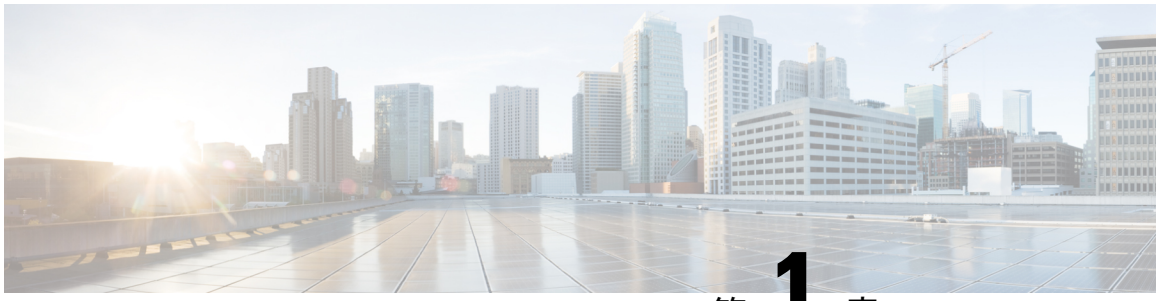
Cisco Crosswork Network Controller 7.2 ネットワーク帯域幅管理

最終更新：2026 年 4 月 16 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/

© 2026 Cisco Systems, Inc. All rights reserved.

目 次



第 1 章

ネットワーク帯域幅管理

ネットワーク帯域幅管理機能パック

サービスプロバイダーは、信頼性の高い高品質のネットワークサービスを顧客に提供するというプレッシャーに直面しています。従来、帯域幅管理は手動でリアクティブなプロセスであり、新たな問題に迅速に対応することが困難でした。

最も重要な問題の 1 つがネットワークの輻輳です。輻輳リンク、長い遅延、およびその他の障害は、サービスの品質に悪影響を与え、エンドカスタマーエクスペリエンスを低下させます。ネットワークの問題が解消されない場合、サービスレベル契約（SLA）の遵守が困難になり、最悪の場合は、SLA 違反、契約違反、およびブランド評価の低下につながる可能性があります。

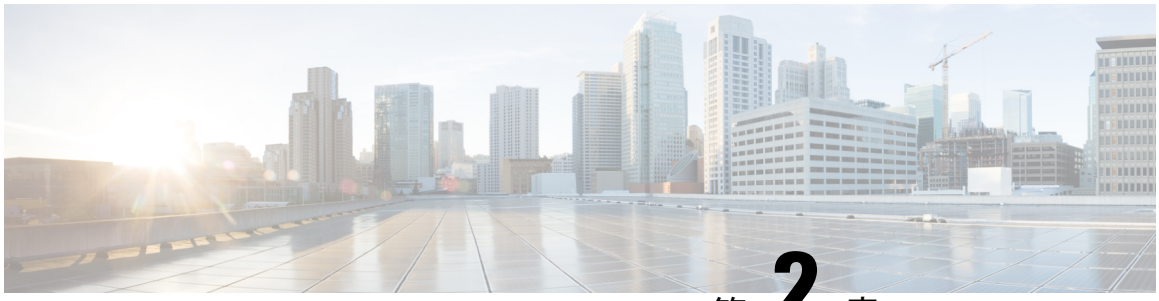
これらの課題を解決するために、ネットワークオペレータは、帯域幅を最適化し、手動介入を削減し、重要なリンクが常に輻輳を回避するのに十分なキャパシティを確保する自動化ツールを必要としています。Crosswork Network Controller は、帯域幅管理とトラフィック エンジニアリングを合理化するように設計された一連の機能パックで、これらのニーズに対応します。

- **ローカル輻輳緩和（LCM）**：帯域幅管理と輻輳緩和のための戦術的なソリューションです。LCM は、包括的なトラフィックマトリックスや高度な計画を必要とせずに、デバイスの輻輳の問題に直接対処するのに最適です。
- **SR 回線型マネージャ（CSM）**：重要なサービス用に帯域幅を事前に予約できる戦略的なトラフィック エンジニアリング ソリューションであり、優先順位の高いサービスに関する輻輳の問題を完全に回避できます。
- **オンデマンド帯域幅（BWoD）**：回線型 SR-TE サービスによって提供される厳密な帯域幅保証とは対照的に、SR ポリシー用のソフト帯域幅保証サービスを提供するソリューションです。BWoD では、設定に応じて、SR ポリシー用の帯域幅予約またはベストエフォート帯域幅パスが提供されます。

（注） CSM と BWoD の機能パックは相互に排他的で、一度に 1 つの機能パックのみ有効にできます。

機能パックの要件

- 機能パックを使用するための正しいライセンスパッケージがあることを確認します。
- 一部の機能や設定にアクセスするユーザーには、管理者ロールまたは特定のデバイスアクセスグループ権限が割り当てられている必要があります。RBAC およびユーザーロールの詳細については、『Cisco Crosswork Network Controller Administration Guide』を参照してください。



第 2 章

SR 回線型マネージャ（CSM）

回線型マネージャ

回線型マネージャは、大規模ネットワークにおける回線型 SR-TE ポリシーパスの帯域幅を考慮したパスの計算と管理を提供します。これは、次の機能を提供するネットワーク管理ツールです。

- 一元化されたブックキーピングを実行して、ネットワーク全体の帯域幅リソースを追跡し、割り当てます。
- コミットされた帯域幅の要件とサービスレベルの制約を満たすポリシーパスを計算します。
- 帯域幅リソースレベルをモニターし、リソースが不足しているエリアを特定できるようにします。
- ネットワークトポロジマップ上で回線型 SR-TE ポリシーを管理および可視化し、適切なフェールオーバー、保護、および双方向動作を保証します。

回線型 SR-TE ポリシーを使用する利点

回線型 SR-TE ポリシーの主な利点は次のとおりです。

- 保証された帯域幅と保護されたパスを使用して、優先順位の高い重要なサービスの信頼性の高い双方向トランスポートを確保します。
- 追加のプロトコルを必要とせずに、一元化された帯域幅予約とポリシー管理により、ネットワーク運用を簡素化します。
- 自動的に計算された現用パス、保護パス、および復元パスを使用して、迅速なサービス復旧を実現します。
- ネットワーク負荷が変化した場合でもサービスレベル契約（SLA）を維持します。
- 中間ルータでのネットワーク状態のメンテナンスが必要ありません。
- ネットワーク全体の帯域幅リソース割り当ての明確な可視性と制御を提供します。

回線型 SR-TE ポリシーに関する重要な考慮事項

回線型SR-TEは、ポリシー属性の互換性などの特定の設定要件と動作の制約事項に従います。

回線型 SR-TE ポリシープロビジョニングのアクセス要件

回線型 SR-TE ポリシーをプロビジョニングするには、デバイスアクセスグループと割り当てられたロールに基づいた、ヘッドエンドデバイスへの書き込みアクセス権が必要です。回線型 SR-TE 管理ユーザーのみが 回線型 SR-TE 構成設定を変更できます。ロールベース アクセス コントロール（RBAC）およびタスク権限の詳細については、『Cisco Crosswork Network Controller Administration Guide』を参照してください。

属性の制約

デバイスのコマンド ライン インターフェイス（CLI）で、またはネットワーク サービス オーケストレーション（NSO）を使用したCrosswork Network Controller UI プロビジョニングで回線型 SR-TE ポリシーを作成するときに、ポリシー属性値を設定します。デバイスの CLI 設定例を表示するには、回線型 SR ポリシーの設定 （12 ページ）を参照してください。

次の表に、各ポリシー属性の要件と、変更が各属性に及ぼす影響を示します。リストされているすべての属性は、制約として機能します。各属性は、Crosswork Network Controller が回線型パスホップの計算を管理するために使用する設定要素と連携します。各値は、パスの計算または最適化に対する制約として機能し、必要なパスプロパティを定義するか、潜在的なパスオプションを除外します。

表 *1*：属性の制約

属性	説明
ポリシーのパス保護	パス保護の制約は、回線型 SR-TE ポリシーの両側に必要です。

属性	説明

帯域幅の制約	• 帯域幅の制約は必須であり、回線型 SR-TE ポリシーの両側で同じである必要があります。帯域幅の変更は、既存のポリシーに適用でき、次のような結果をもたらします。
	  • 両側で新しい帯域幅を設定すると、システムは再計算せずにパスを評価します。
	  • 新しい帯域幅の方が高い場合、システムが現在のパスに十分なリソースがあるかどうかチェックします。すべてのパスが新しい帯域幅に対応できる場合、更新された帯域幅値を持つ同じパスが返され、パス計算クライアント（PCC）が成功したことが示されます。いずれかのパスが新しい帯域幅をサポートできない場合、古い帯域幅の値が返され、失敗したことが示されます。この評価は、帯域幅が再度変更された場合にのみ再試行されます。
	  • 帯域幅の方が低い場合、システムが新しい帯域幅値を使用して同じパスを返し、成功したことが PCC に示されます。
	• ポリシーの詳細を表示すると、ユーザーインターフェイスの各候補パスの下に要求された帯域幅と予約済みの帯域幅の両方が表示されます。各値は、要求された帯域幅が増加し、1 つ以上のパスで使用可能な回線型プール帯域幅が不足している場合は異なる可能性があります。

候補パスとロール	• 現用パスは、優先順位が最も高い候補（CP）パスとして定義されます。 • 保護パスは、優先順位が 2 番目に高い CP として定義されます。 • 復元パスは、優先順位が最も低い CP として定義されます。ヘッドエンドには `backup-inligible` が設定されている必要があります。 • 各方向で同じロールの CP については、CP の優先順位が同じである必要があります。
双方向パス	• すべてのパスを相互ルーティングとして設定する必要があります。 • 両側にある同じロールのパスには、グローバルに一意の同じ双方向アソシエーション ID が必要です。

属性	説明
分離	ディスジョイントポリシーは、2 つの送信元ノードから 2 つの宛先ノードへのトラフィックをディスジョイントパスに沿って誘導する 2 つのセグメントのリストを計算するために使用されます。ディスジョイントタイプは、2 つの計算されたパスで共有すべきではないリソースのタイプを指します。 • サポートされているディスジョイントパスのタイプは次のとおりです。 • [リンク（Link）]：計算されたパス上でリンクが共有されません。 • [ノード（Node）]：計算されたパス上でノードが共有されません。 • [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ません。これらのリンクは共通のリソースに依存しているため、同じ障害が発生する可能性があります。この設定では、現用パスと保護パスが同じ SRLG に属するリンクを使用でき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ません。 • 使用される分離タイプは、同じポリシーの両方向で同じである必要があります。 • 同じ PCC 上の現用パスと保護パスは、同じ分離アソシエーション ID と分離タイプを使用する分離制約で設定する必要があります。 • ある方向の現用パスと保護パスのペアの分離アソシエーション ID は、反対方向の対応するペアと比較して一意である必要があります。 • 復元パスには分離制約を設定できません。 • Crosswork Network Controller では厳密なフォールバック動作に従い、すべての現用パスと保護パスの分離が計算されます。つまり、ノードタイプの分離が設定されていて、使用可能なパスがない場合、システムでは制限の緩いリンクタイプの分離パスは自動的に計算されません。
メトリックタイプ	TE、IGP、ホップカウント、および遅延メトリックタイプのみがサポートされています。メトリックタイプは、両方向の現用パス、保護パス、および復元パスと一致する必要があります。

属性	説明
セグメントの制約	• すべての現用パス、保護パス、および復元パスには、次のセグメントの制約が必要です。 • protection unprotected-only • adjacency-sid-only • リンク障害が発生しても永続性を確保するには、回線型SR-TEポリシーで使用可能なすべてのインターフェイスで静的隣接関係 SID を設定します。

サポートされていない設定

次の設定はサポートされていません。

- メトリック境界
- SID-Algo の制約
- IOS XR 7.8.x を実行しているデバイスの部分的なリカバリ
- 色は同じでエンドポイント IP アドレスが異なる同じノード間の複数の回線型 SR-TE ポリシー。
- 高可用性ペアの PCE 間の状態同期設定

パス計算と復帰の動作

回線型 SR-TE ポリシーの正常なプロビジョニングと継続性は、パス計算プロセスと、復旧および復元シナリオの正確な処理の両方に依存します。パス計算によって、帯域幅、保護、および制約の要件を満たす候補パスをシステムが確立する方法が決定されます。パス復帰ロジックは、ネットワークイベントおよび復旧に応答して、現用パス、保護パス、復元パス間の遷移を制御します。

パス計算の動作

SR 回線型マネージャ（CSM）は、完全な双方向のパス保護された一連の候補パス（両側の現用パスと保護パスを含む）が委任されて初めて、回線型ポリシーのパスを計算します。

- **帯域幅の可用性とパスの委任**：パス計算は、帯域幅の可用性に依存します。帯域幅が不足しているためパスが確立できない場合、SR 回線型マネージャ はソリューションが見つかるか、回線型 SR-TE が無効になるまで 30 分ごとに再試行します。
- **復元パスの計算**：現用パスと保護パスがダウンして初めて復元パスが計算されます。設定可能な遅延タイマーを使用して、委任後の待機期間を設定します。これにより、トポロジとポリシーの状態の変更が計算の前に伝達されます。

- **パスの最適化と制限事項**：トポロジまたはLSP状態の変更および定期的なイベントでは、自動パス再最適化を使用できません。必要に応じて、パス設定を手動で調整する必要があります。
- **サポートされているパス計算シナリオ**：パス計算では、エリア内/エリア間およびIGP ドメイン内/ IGP ドメイン間のシナリオがサポートされています。AS 間のパスの計算はサポートされていないため、そのような場合は手動での設定が必要です。

パス復帰

復帰動作

復帰動作は、保護パスと復元パスの WTR ロックタイマーオプションの設定によって制御されます（現用パスには関係ありません）。

- ロックなし設定：デフォルトの 5 分間のロック後に復帰
- 期間の指定がないロック：復帰なし
- ロック期間：指定した秒数後に復帰

復帰ロジック

パスの復帰は、現用パス、保護パス、復元パスの初期状態と、各パスに影響するイベントによって異なります。次の表のシナリオに、一般的な復帰動作の例を示します。

表 *2:* パスの復帰のシナリオ

初期状態	イベント	動作
現用パスがダウン、保護パスがアップ/アクティブ	現用パスが復旧する	**1.** 現用パスがアップ/スタンバイ状態に回復します。 **2.** WTR タイマーが切れた後、各 PCC によって現用パスがアクティブに移行します。 **3.** 保護パスがアップ/スタンバイに移行します。
現用パスがダウン、保護パスがダウン、復元パスがアップ/アクティブ	現用パスが復旧し、保護パスが復旧する	**1.** 現用パスが回復し、アップ/アクティブになります。 **2.** 復元パスが削除されます。 **3.** 保護パスが回復し、アップ/スタンバイになります。

初期状態	イベント	動作
現用パスがダウン、保護パスがダウン、復元パスがアップ/アクティブ	保護パスが復旧し、現用パスが復旧する	サイド A：現用パス障害はローカル障害です（SegList の最初の Adj SID が**無効**です）。 **1.** 保護パスが回復し、アップ/アクティブになります。 **2.** 復元パスが削除されます。 **3.** 現用パスが回復し、アップ/スタンバイになります。 **4.** WTR タイマーが切れた後、各 PCC によって現用パスがアクティブに移行し、保護パスがアップ/スタンバイに移行します。 サイド Z：現用パス障害はリモート詳細です（SegList の最初の Adj SID が**有効**）。 **1.** 保護パスは回復しますが、起動せず、復元パスはアップ/アクティブのままです。 **2.** 現用パスが回復し、アップ/アクティブになります。 **3.** 復元パスが削除されます。 **4.** 保護パスがアップ/スタンバイになります。

CS SR-TE ポリシー可視化ワークフローのセットアップ

CS SR-TE ポリシーが正しい帯域幅の詳細で表示されるようにするには、次の手順を実行します。

手順

ステップ 1 SR CSM の有効化 （10 ページ）。

ステップ 2 デバイス上で、回線型 SR ポリシーの設定 （12 ページ）を実行します。

ステップ 3 CS SR-TE ポリシーが [トラフィックエンジニアリング（Traffic Engineering）] テーブルに表示されていることを確認します。

[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）] > **[トラフィックエンジニアリング（Traffic Engineering）]** > **[SR-MPLS]** > **[回線型（Circuit-style）]** を選択します。

ステップ 4 トポロジマップから、参加している CS SR-TE ノードをクリックし、最初の手順で定義した予約済み帯域幅プールの設定が適切に構成されていることを確認します。

[リンク（Links）] > ***[link-type-entry]*** > **[トラフィックエンジニアリング（Traffic Engineering）]** > **[全般（General）]** の順に選択します。回線型 SR-TE ポリシーの帯域幅使用率の確認 （14 ページ） を参照してください。

SR CSM の有効化

トポロジマップで回線型 SR-TE ポリシーを管理および可視化するには、まず SR-CSM を有効にし、帯域幅設定を行う必要があります。CSM が有効になっている場合、要求された帯域幅と、2 つのノード間の回線型 SR ポリシーの設定で定義されているその他の制約を使用して、最適なフェールオーバーの双方向パスが計算されます。

SR 回線型マネージャを有効にするには、次の手順を実行します。

Before you begin

CSM と BWoD の両方を同時に有効にすることはできません。BWoD が有効になっている場合は、CSM を有効にする前に BWoD を無効にする必要があります。

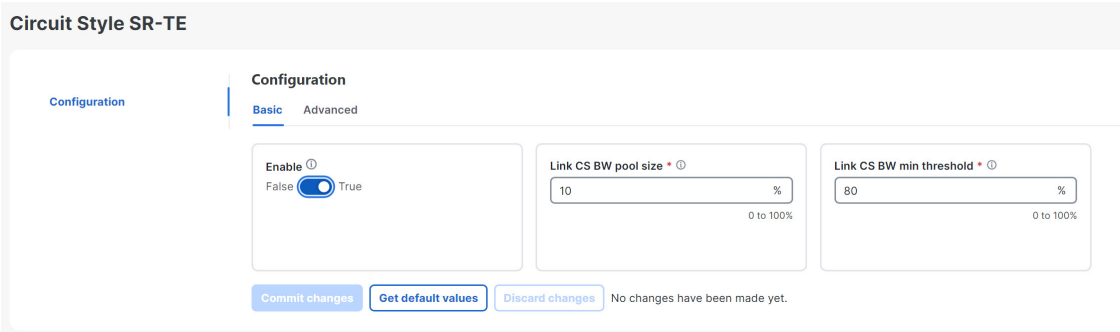
（注） また、関連する機能パック（BWoD または CSM）を無効にする前に、ネットワークからそれぞれのポリシーを削除することを推奨します。ポリシーが無効な機能パックに残っている場合、新しいポリシー委任で問題が発生し、処理時間が長くなる可能性があります。

手順

ステップ 1 メインメニューから、**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）]** > **[回線型SR-TE（Circuit Style SR-TE）]** > **[設定（Configuration）]** > **[基本（Basic）]**の順に選択します。

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

図 *1* : 基本回線型 *SR-TE* 設定



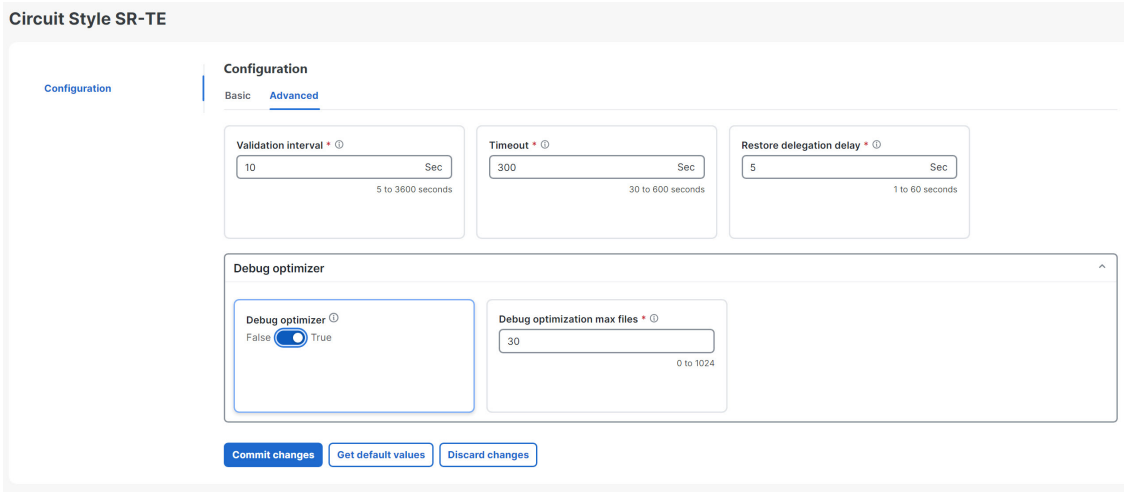
ステップ 3 必要な帯域幅プールサイズとしきい値情報を入力します。その他のフィールド情報がこの表に記載されています。帯域幅予約制限を超過することの影響 （22 ページ）を参照してください。

フィールド	説明
リンク CS BW プールサイズ（Link CS BW pool size）	回線型 SR-TE ポリシー用に予約可能な各リンクの帯域幅の割合。
リンク CS BW 最小しきい値（Link CS BW min threshold）	Crosswork Network Controller でしきい値超過イベント通知が生成されるリンク CS BW プール使用率の割合。

ステップ 4 [変更を確定（Commit changes）] をクリックして、基本設定を保存します。

ステップ 5 [詳細（Advanced）] タブをクリックして、追加の CS-SR 設定値を表示します。その他のフィールド情報がこの表に記載されています。

図 2 : 回線型 *SR-TE* 設定：*[詳細（Advanced）]* タブ



フィールド	説明
検証間隔（Validation interval）	これは、委任されていないポリシー用に予約されている帯域幅が回線型SR-TE ポリシー帯域幅プールに返される前に、CSM ポリシーが待機する間隔です。
タイムアウト	CSM がしきい値超過アラームを生成する前に委任要求を待機する期間。
委任の復元の遅延（Restore delegation delay）	CSM が復元パスの委任を処理する前に一時停止する期間。

フィールド	説明
デバッグオプティマイザ（Debug optimizer）	スイッチを[True]に切り替えて、すべてのCS-SRポリシーのデバッグオプティマイザをオンにします。デバッグオプティマイザは、指定した最大ファイル数までルートを計算するたびに、ログファイルを Crosswork Network Controller ファイルシステムに書き込みます。
デバッグ最適化最大ファイル数（Debug optimization max files）	デバッグオプティマイザが書き込むログファイルの最大数を入力します。最大数に達すると、オプティマイザは既存のファイルを上書きします。

ステップ 6 詳細設定値の入力が完了したら、[変更を確定（Commit changes）] をクリックして設定を保存します。

次のタスク

回線型 SR ポリシー設定は、デバイス上で手動で設定するか（「回線型 SR ポリシーの設定」を参照）、または Crosswork Network Controller を使用して設定します。

回線型 SR ポリシーの設定

回線型 SR ポリシーの設定には、接続先エンドポイント、要求された帯域幅の量、および双方向属性を含める必要があります（追加の要件や注目すべき制約については、回線型 SR-TE ポリシーに関する重要な考慮事項 （4 ページ）を参照してください）。設定には、Performance Measurement Liveness（PM）プロファイルも含める必要があります。PM プロファイルを使用すると、候補パスの活性状態が適切に検出され、パス保護が効果的に実行されます。PCC では最初の SID を過ぎると検証されないため、回線型 SR ポリシー候補パス障害がセグメントリストの最初のホップでない場合、PM がないとパス保護は実行されません。詳細については、「Configuring SR Policy Liveness Monitoring」を参照してください。

手順

ステップ 1 該当する場合は、PM 設定用にデバイスのハードウェアモジュールを有効にします。

例：

```
hw-module profile offload 4
reload location all
```

ステップ 2 PM プロファイルを設定します。

例：

```
performance-measurement
  liveness-profile sr-policy name CS-active-path
    probe
      tx-interval 3300
    !
```

```
    npu-offload enable   !! Required for hardware Offload only
    !
  !
  liveness-profile sr-policy name CS-protect-path
    probe
      tx-interval 3300
    !
    npu-offload enable   !! Required for hardware Offload only
    !
  !
!
```

ステップ 3 PM プロファイルを使用して回線型 SR ポリシーを設定します。CSM で 回線型 SR-TE ポリシーを管理するには、例に示されているすべての設定が必要です。ユーザーが定義したエントリは斜体で表示されます。追加の要件や注目すべき制約については、回線型 SR-TE ポリシーに関する重要な考慮事項 （4 ページ）を参照してください。

例：

```
segment-routing
  traffic-eng
    policy cs1-cs4
      performance-measurement
        liveness-detection
          liveness-profile backup name CS-protect  !! Name must match liveness profile defined for
 Protect path
          liveness-profile name CS-active  !! Name must match liveness profile defined for Active
path
      !
      !
      bandwidth 10000
      color 1000
      end-point ipv4 192.168.20.4
      path-protection
      !
      candidate-paths
        preference 10
          dynamic
            pcep
          !
            metric
             type igp
            !
           !
          backup-ineligible
          !
          constraints
            segments
              protection unprotected-only
              adjacency-sid-only
            !
          !
          bidirectional
            co-routed
            association-id 1010
            !
          !
        preference 50
          dynamic
            pcep
            !
```

```
        metric
          type igp
          !
        !
      constraints
        segments
          protection unprotected-only
          adjacency-sid-only
          !
        disjoint-path group-id 3
        type node, srlg, or link
        !
        bidirectional
          co-routed
          association-id 1050
          !
       !
    preference 100
      dynamic
        pcep
       !
      metric
       type igp
       !
      !
      constraints
        segments
          protection unprotected-only
          adjacency-sid-only
         !
        disjoint-path group-id 3
        type node, srlg, or link
        !
        bidirectional
          co-routed
          association-id 1100
          !
        !
      !
    !
  !
!
```

回線型 SR-TE ポリシーの帯域幅使用率の確認

次の手順を実行して、予約済み帯域幅プールの設定（CSMを有効にすると定義されます。SR CSM の有効化 （10 ページ）を参照）が正しく設定されていることを確認します。また、現在の 回線型 SR-TE 帯域幅使用率と、まだ使用可能な量を確認できます。

手順

ステップ 1 メインメニューから、**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）] > [トラフィックエンジニアリング（Traffic Engineering）] > [SR-MPLS]** の順に選択し、[回線型（Circuit Style）]

ミニダッシュレットをクリックします。[トラフィックエンジニアリング（Traffic engineering）]テーブルには、すべての 回線型 SR-TE ポリシーが一覧表示されます。

ステップ 2 目的の 回線型 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。

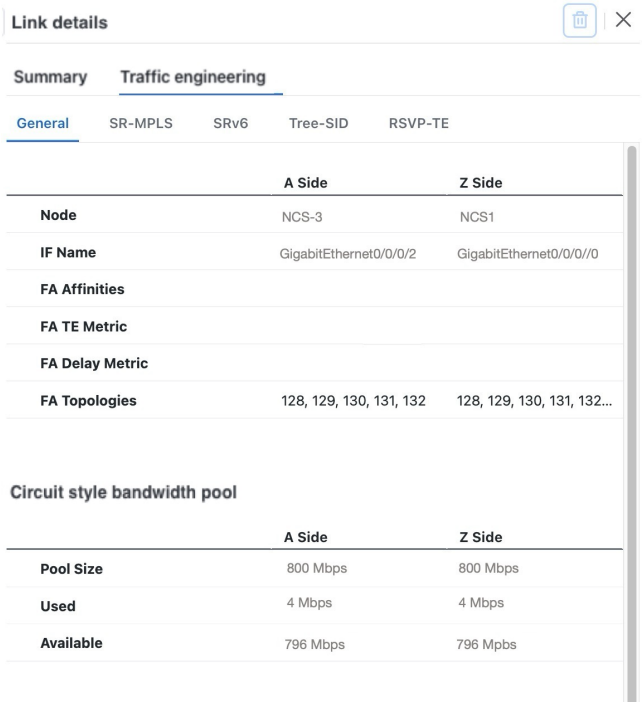
ステップ 3 トポロジマップから、参加している 回線型 SR-TE ポリシーノードをクリックします。

ステップ 4 [デバイスの詳細（Device details）] ページで、**[リンク（Links）]** > ***[link-type-entry]*** > **[トラフィックエンジニアリング（Traffic Engineering）]** > **[全般（General）]** の順にクリックします。

[回線型帯域幅プール（Circuit Style bandwidth pool）] で、次を確認できます。

- 予約済み帯域幅プールのサイズ
- 現在使用されている帯域幅の量
- 回線型 SR-TEポリシーに割り当てられていて、まだ使用可能な帯域幅の量。

図 *3 : CS SR* ポリシー帯域幅プール



この例では、予約済み帯域幅プールサイズを、NCS-3 および NCS1 に対して 800 Mbps と表示します。構成済みの設定は、帯域幅プールサイズの 80% として事前に定義されています。インターフェイスは 1 Gbps であるため、これらのインターフェイスの 回線型 SR-TE ポリシーの帯域幅の 80% が CSM によって正しく割り当てられていることを確認できます。

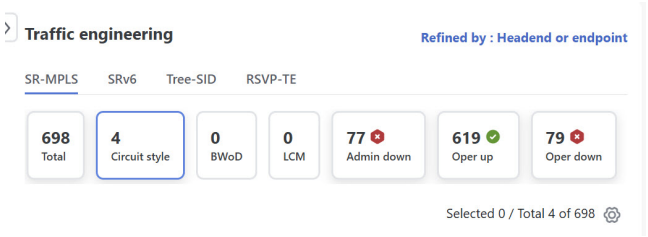
回線型 SR-TE ポリシー情報の表示

回線型 SR-TE ポリシー情報を表示するには、次の手順を実行します。

手順

ステップ 1 メインメニューから、**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）]** > **[トラフィックエンジニアリング（Traffic Engineering）]** > **[SR-MPLS]**の順に選択し、[回線型（Circuit Style）]をクリックします。

図 *4*: 回線型ダッシュレット

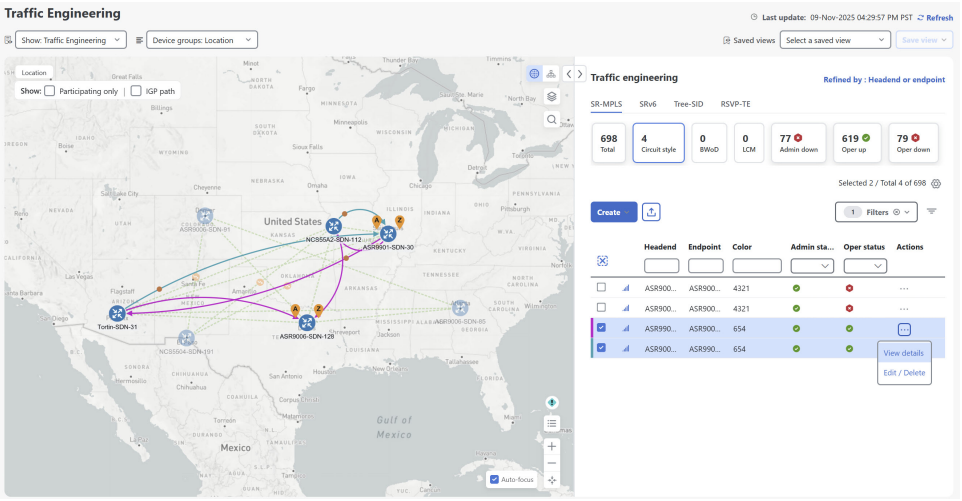


テーブルには、すべての回線型 SR-TE ポリシーが一覧表示されます。

ステップ 2 [アクション（Actions）]列で、いずれかの回線型 SR-TE ポリシーに対して ··· > [詳細の表示（View Details）]の順に選択します。

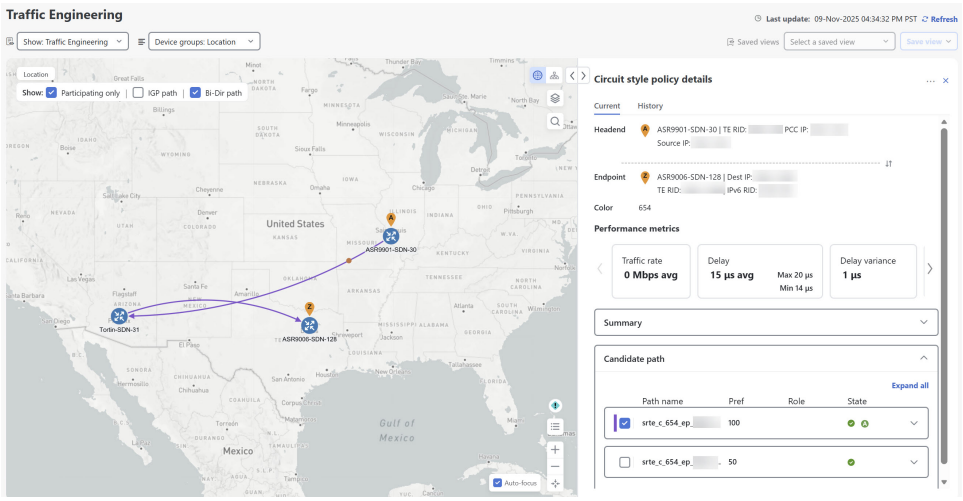
（注）
デバイスで直接作成された 回線型 SR-TE ポリシーの設定は、編集または削除できません。

図 *5*: 回線型 *SR-TE* ポリシーの詳細の表示



サイドパネルに [回線型ポリシーの詳細（Circuit style policy details）] ページが表示されます。デフォルトでは、「アクティブ」状態の候補パスがトポロジマップに表示されます。アクティブな状態は、[状態（State）]の下に緑色の「A」アイコン付きで示され、現在動作中のアクティブなパスであることが示されています。また、このマップでは、[双方向パス（Bi-Dir path）] チェックボックスがデフォルトでオンになっており、双方向パスが表示されます。[候補パス（Candidate path）] リストには、ステータスがアクティブな候補パス（トラフィックを受け取るパス）とその他の候補パスが表示されます。

図 *6 : CS-SR* ポリシーの詳細の概要



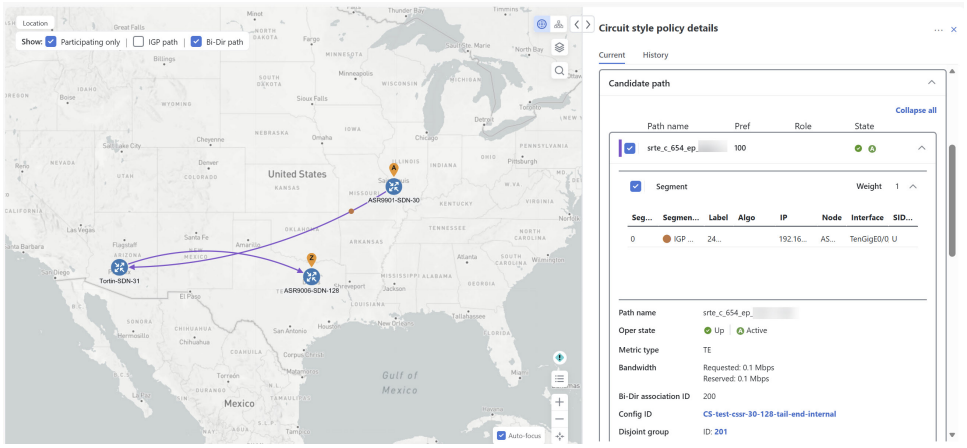
（注）
帯域幅の制約値は、値が増え、すべての現用および保護候補パスの要求を満たせる十分なリソースが存在しない場合、要求した帯域幅と異なる場合があります。

ステップ 3 候補パス設定の詳細を表示します。

a) [回線型ポリシーの詳細（Circuit style policy details）] ウィンドウでは、ドリルダウンして候補パスに関する詳細情報を表示できます。また、URL をコピーして、詳細情報を他のユーザーと共有できます。

動作状態（Oper state）が「アップ（Up）」の現用パス（最も優先度の高いパス）は常に、トラフィックを受け取ることを示すアクティブな状態になります（CSM パス障害管理 （26 ページ）を参照）。現用パスがダウンすると、保護パスがアクティブになります。この例では、保護パス（優先順位 50）がアクティブであり、トポロジマップに表示されます。[すべて展開（Expand all）] をクリックして、両方のパスに関する詳細情報を表示します。

図 7: トポロジマップ上の候補パス

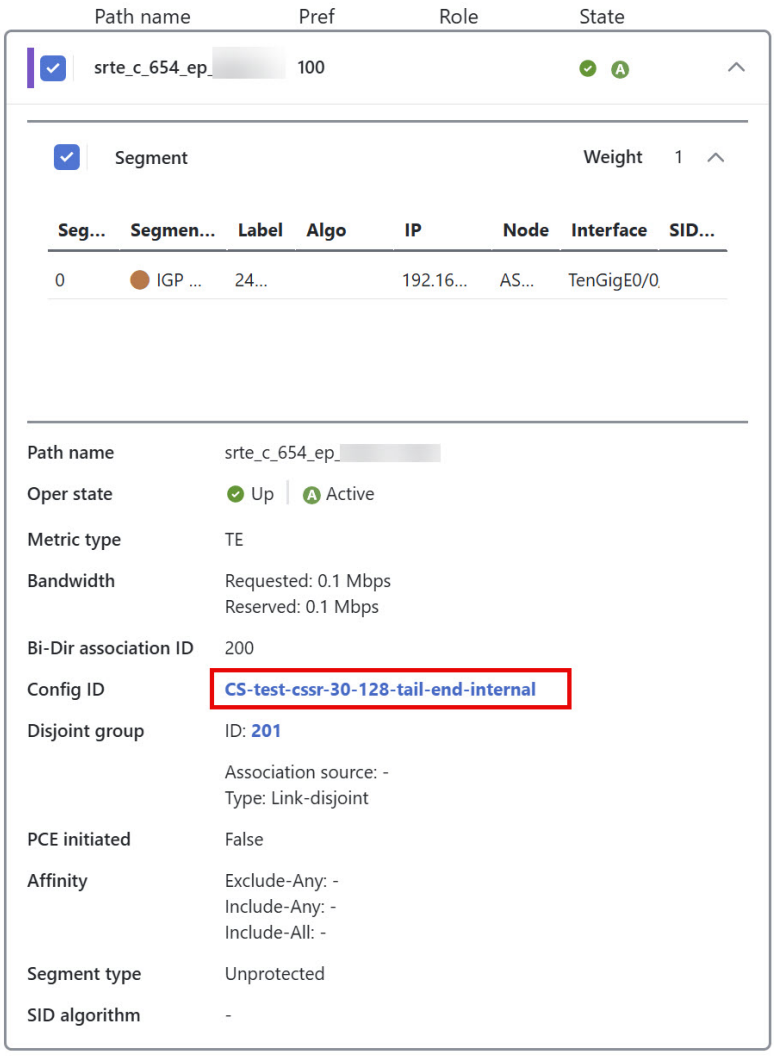


（注）

- 1 番目の優先パスは紫色のリンクで表示されます。
- 2 番目の優先パスは青色のリンクで表示されます。
- 3 番目の優先パスはピンク色のリンクで表示されます。

Crosswork Network Controller を使用して回線型 SR-TE ポリシーを設定した場合は、回線型 SR-TE ポリシーの設定を表示するオプションがあります。設定を表示するには、[設定ID（Config ID）] の横にあるリンクをクリックします。

図 *8* : 候補パスの詳細での *[*設定*ID*（*Config ID*）*]*

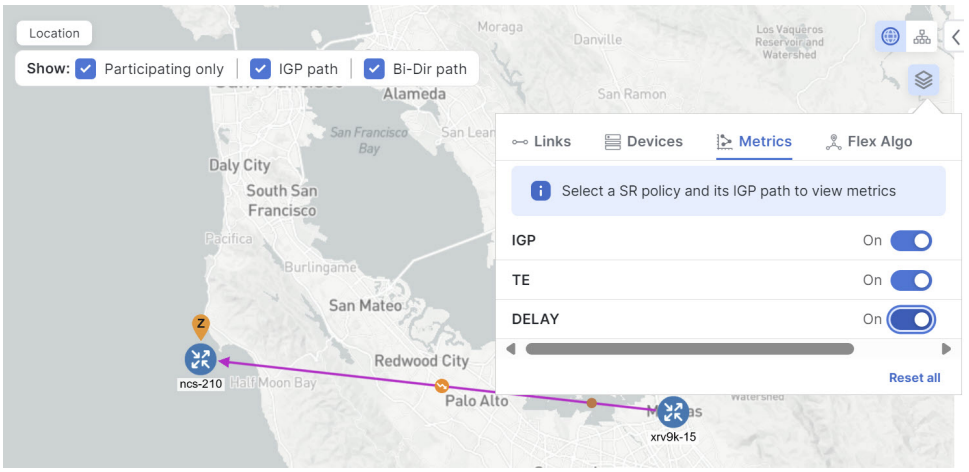


次に、回線型ポリシーの設定例を示します。CS-SR ポリシーの設定については、回線型 SR ポリシーの設定 （12 ページ）を参照してください。

図 *9 :* 回線型ポリシーの設定例

ステップ 4 選択した回線型SR-TEポリシーのエンドポイント間の物理パスとメトリックを表示するには、をクリックして該当するメトリックをオンにし、[IGPパス（IGP path）] チェックボックスをオンにします。

図 *10 : IGP* メトリック



回線型 SR-TE ポリシーを再計算するための CSM のトリガー

回線型 SR-TE ポリシーは本質的に静的です。つまり、パスが計算されると、パスに影響を与える可能性のあるトポロジまたは動作ステータスの変更に基づいて自動的に再最適化されません。ポリシーの動作ステータスがダウンからアップになった後、または帯域幅サイズと要件の変更が設定された場合は、現用パスと保護パス（復元パスを除く）を再最適化できます。

回線型 SR-TE ポリシーの再計算を手動でトリガーするには、次の手順を実行します。

手順

ステップ 1 メインメニューから、**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）] > [トラフィックエンジニアリング（Traffic Engineering）] > [SR-MPLS]** の順に選択し、[回線型（Circuit Style）] ミニダッシュレットをクリックします。[トラフィックエンジニアリング（Traffic engineering）] テーブルには、すべての 回線型 SR-TE ポリシーが一覧表示されます。

ステップ 2 [アクション（Actions）] 列で、CSM がパスを再計算する 回線型 SR-TE ポリシーに対して … > [詳細の表示（View Details）] の順に選択します。

ステップ 3 右上隅にある … > [再最適化（Reoptimize）] を選択します。

帯域幅予約制限を超過することの影響

CSM はネットワークで使用可能で予約可能な帯域幅を検出して更新します。CS SR-TE ポリシーに提供されるすべての帯域幅予約のアカウンティングを維持し、すべてのインターフェイスの予約済み帯域幅の合計がネットワーク全体のリソースプール（帯域幅プールサイズ）以下に保たれるようにします。帯域幅が設定されたプールまたはしきい値のいずれかを超えると、システムは次の方法で応答します。

- 可視性と操作応答のためにしきい値超過イベント通知を生成します。
- リソースが利用可能になるまで、ポリシーの確立または帯域幅の増加を拒否します。
- ソリューションが見つかるか、ポリシーが無効になるまで、定期的に（たとえば 30 分ごとに）パス計算を繰り返し再試行します。

例：帯域幅使用率が定義されたしきい値を超えた場合

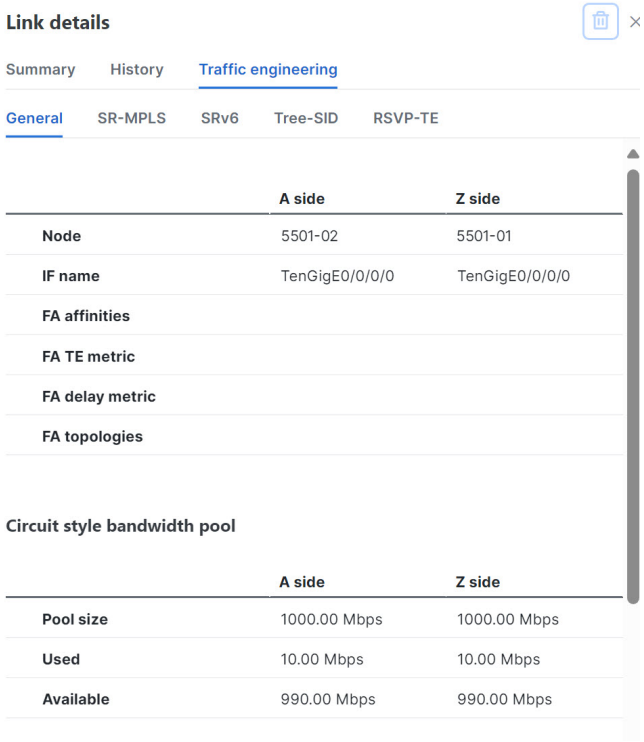
この例では、予約済み帯域幅の設定が次のようになっているとします。

- リンク CS 帯域幅プールサイズ：10%
- リンク CS 帯域幅の最小しきい値：10%

この例では、10 Gbps イーサネット インターフェイスの帯域幅プールサイズは 1 Gbps で、アラームしきい値は 100 Mbps（プールサイズの 10%）に設定されています。

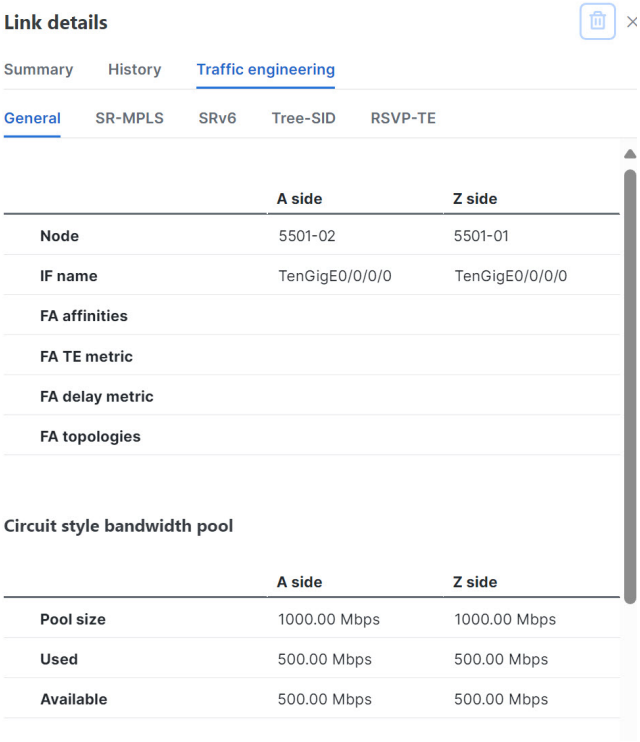
1. ノード 5501-02 からノード 5501-01（r02 - r01）への 回線型 SR-TE ポリシーは、100 Mbps の帯域幅で作成されます。

図 *11 : CS-SR* ポリシー *10 Mbps* アップ



2. その後、ポリシーに設定された要求帯域幅が 500 Mbps に増え、CSM は、既存のパスに沿った追加の帯域幅が使用可能であると判断し、帯域幅を予約します。

図 *12 : CS-SR* ポリシー *500 Mbps* アップ



3. 更新されたポリシーでの帯域幅使用率（500 Mbps）が、設定されたプール使用率のしきい値（100 Mbps）を超えているため、イベントがトリガーされます。

図 *13 :* しきい値アラート

例：帯域幅プールサイズと使用率を超えた場合

この例では、予約済み帯域幅の設定が次のようになっているとします。

- リンク CS 帯域幅プールサイズ：10%
- リンク CS 帯域幅の最小しきい値：90%

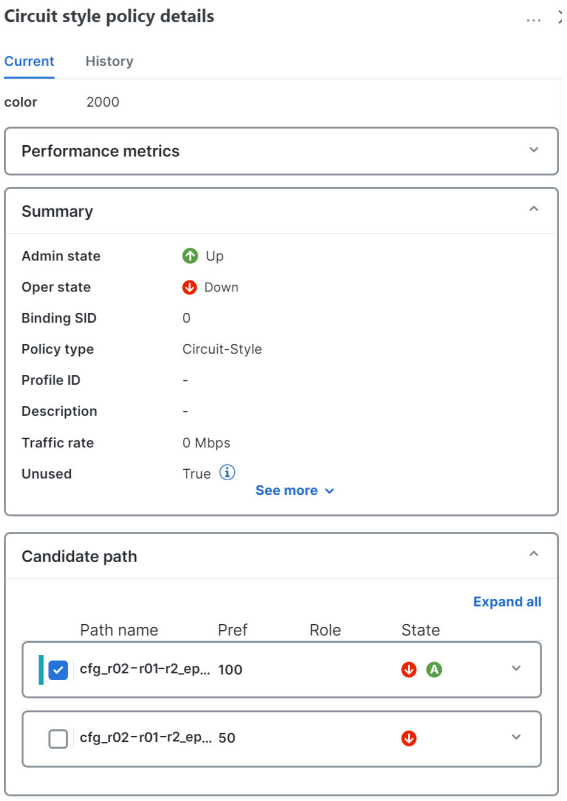
この例では、10 Gbps イーサネット インターフェイスの帯域幅プールサイズは 1 Gbps で、アラームしきい値は 900 Mbps に設定されています。

1. ノード 5501-02 からノード 5501-01（r02 - r01）への既存の 回線型 SR-TE ポリシーでは、500 Mbps の帯域幅が使用されます。

2. その後、ノード 5501-02 からノード 5501-01、5501-2（r02 - r01 - r2）へのパスで 750 Mbps の帯域幅を必要とする新しいポリシーが要求されます。既存のポリシーとこの新しいポリシーの合計が帯域幅プールサイズとアラームしきい値の 1 Gbps（750 Mbps + 500 Mbps = 1250 Mbps）を超えるため、次の動作が発生します。

   - 新しい CS-SR ポリシー **r02 - r01 - r2** が作成されましたが、CSM が新しいポリシーのパスを計算できないため、運用上ダウン状態のままです。CSM は、帯域幅要件を満たすパスを見つけるために 30 分ごとに再試行します。

     図 *14 : CS-SR* ポリシーが帯域幅プールサイズを超過



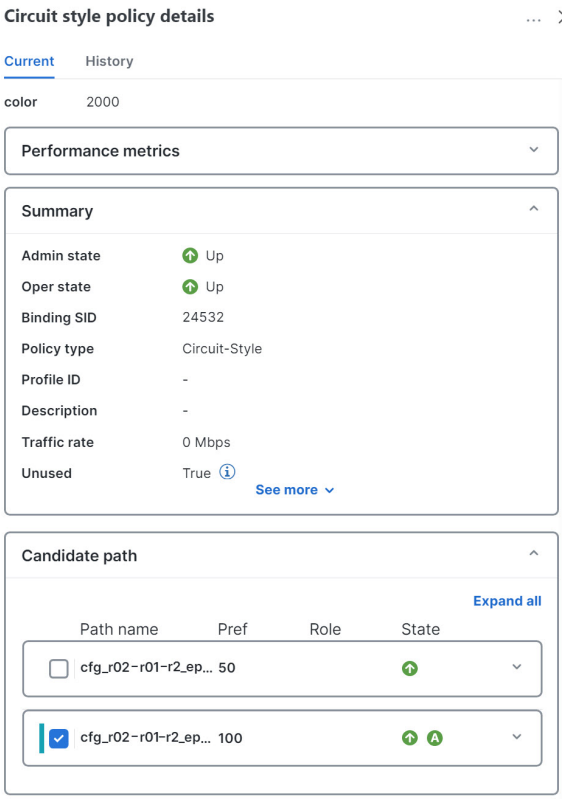
   - アラートがトリガーされます。

     図 *15 :* しきい値アラート

3. その後、回線型 SR-TE ポリシー（r02 - r01- r2）が更新され、10 Mbps のみ必要になり、次の動作が発生します。

- 2 つのポリシーに必要な合計帯域幅（10 Mbps + 500 Mbps = 510 Mbps）は、帯域幅プールサイズ（1 Gbps）よりも少ないため、回線型 SR-TE ポリシー（**r02 - r01 - r2**）は、CSM によって計算されたパスを受け取り、運用上アップ状態になります。

図 *16*：更新された *CS-SR* ポリシーの運用状態



- 帯域幅が削減された 2 番目の回線型 SR-TE ポリシーには CSM によってパスが提供されるため、アラートはクリアされます。

図 *17*：クリアされたアラート

CSM パス障害管理

Crosswork Network Controller は、完全な双方向のパス保護された一連の候補パスが委任されて初めて、回線型SR-TEポリシーのパスを計算します。パス障害時に使用される候補パスには、次の 3 タイプがあります。

- **現用**：優先順位値が最も高い候補パスです。

- **保護**：2 番目に優先順位値が高い候補パスです。現用パスがダウンすると、（優先順位値が低い）保護パスがアクティブになります。現用パスが回復しても、デフォルトのロック期間が経過するまで、保護パスはアクティブのままになります。
- **復元**：優先順位値が最も低い候補パスです。Crosswork Network Controller は、現用パスと保護パスがダウンして初めて復元パスを計算します。復元パスが両側から委任された後、パスが計算されるまで待機する時間を制御できます（SR CSM の有効化 （10 ページ）を参照）。この遅延により、トポロジとポリシーの状態変更によって復元パスの委任がトリガーされた場合、それらの変更が Crosswork Network Controller に完全に伝達されます。

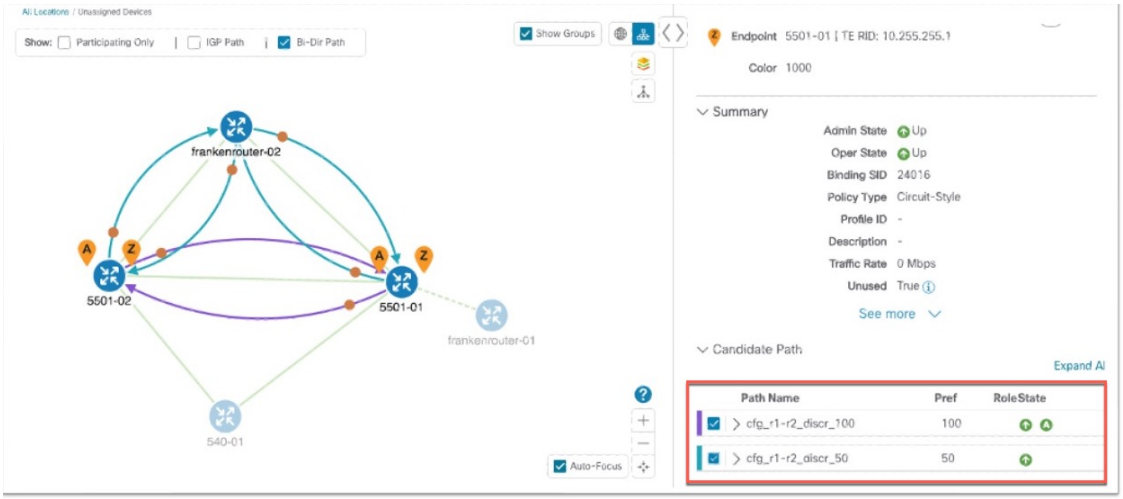
パス障害に効果的に対応し、現用パスから保護パスへの切り替えを実行するために、パフォーマンス測定（PM）を設定できます。詳細については、回線型 SR ポリシーの設定 （12 ページ）を参照してください。

例

（注） 以下の図はデモンストレーションのみを目的としており、ワークフローコンテンツ内で説明されている正確な UI やデータを常に反映しているとは限りません。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。

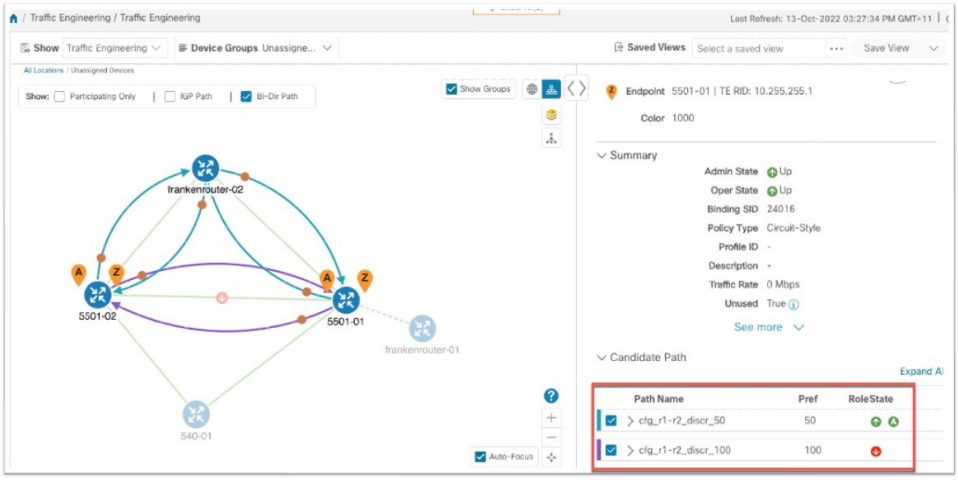
次の画像は、回線型 SR-TE ポリシーの現用パスと保護パスが動作していることを示しています。アクティブなパスは「A」アイコンで示されます。

図 *18 :* 初期候補パス



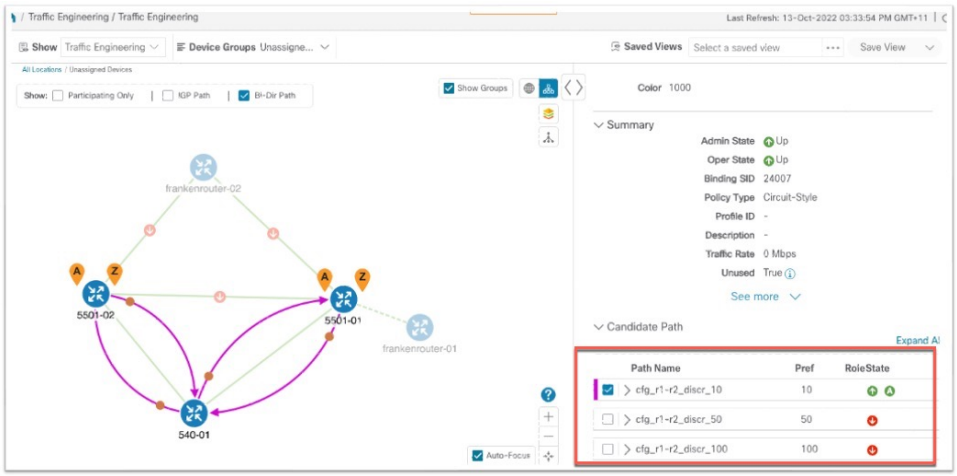
アクティブ状態の現用パスがダウンすると、保護パスはすぐに「アクティブ」になります。現用パスが回復すると、保護パスがアップ/スタンバイに移行し、現用パス（この例ではプリファレンスが 100）がアクティブになります。

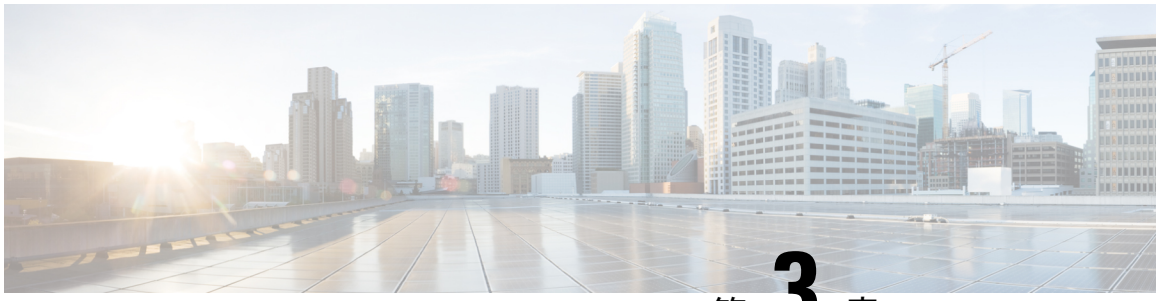
図 *19* : 保護パスがアクティブになる



現用パスと保護パスの両方がダウンした場合、CSM によって復元パスが計算されてアクティブになります。復元パスは、この特定のシナリオでのみ表示されます。この例では復元パスの最も低い優先順位値は 10 です。現用パスまたは保護パスが再び動作可能になると、復元パスはトポロジマップに表示されなくなり、**候補パス**リストから削除されます。

図 *20* : 復元パス





第 3 章

ローカル輻輳緩和（LCM）

ローカル輻輳緩和

ローカル輻輳緩和は、次のネットワーク最適化技術です。

- 指定したインターフェイスしきい値で定義された輻輳をモニターし、インターフェイスの使用率とトラフィックしきい値をモニターすることで、（トリガーされるイベントではなく）設定可能なケイデンスでの輻輳を検出します。
- 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から最小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。
- 輻輳を緩和しながら可能な限り多くのトラフィックを元のIGPパスに維持することを目指します。
- ドメイン内の周辺インターフェイスにおいてローカル化された緩和推奨事項（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。完全なトラフィックマトリックスを必要とせず、ネットワーク内のエッジツーエッジのトラフィックフローをシミュレートしません。
- ユーザーが戦術的トラフィック エンジニアリング（TTE）SR ポリシー展開をコミットする前に、LCM推奨事項を視覚的にプレビューできます（手動モードで使用可能な機能）。

- 指定されたしきい値に基づいて、gRPC MSL に完全準拠したデバイスの複数セグメントリスト（MSL）ポリシーを自動的に展開できます（自動モードで使用可能な機能）。
- ネットワーク障害のリスクを軽減するために、ダウン、失敗、またはコミットされていない LCM TTE ポリシーの自動削除をサポートします（LCM 設定オプション （62 ページ）の「**自動修復ソリューション**」および「**隣接ホップタイプ**」を参照）。
- SNMP を介して TTE SR ポリシーおよびインターフェイスカウンタが収集されるため、セグメント ルーティング トラフィック マトリックス（SR-TM）は必要ありません。
- パス計算が単純で特定のネットワーク要素に限定されるため、複数の IGP エリアを持つ大規模なネットワークでの拡張性と適用可能性を考慮して設計されています。

ネットワークで LCM を使用する方法については例：ローカルインターフェイスでの輻輳の緩和 （55 ページ）を参照してください。

LCM - デバイスおよびネットワークの要件

これらの要件を満たすことで、LCM はネットワークトラフィックに対する完全な可視性と、トラフィックを効果的にステアリングする機能が保証されます。

LCM のトラフィックモニタリングの有効化

LCM で輻輳を適切に評価するためには、インターフェイスおよびヘッドエンド SR-TE ポリシー トラフィック測定値のトラフィック統計が必要です。

LCM がこれらのトラフィック統計を受信していることを確認するには、次の手順を実行します。

手順

ステップ 1 **SNMP または gNMI を有効にします**：トラフィックをモニターするデバイス（ヘッドエンドデバイスを含む）で SNMP または gNMI を有効にします。各プロトコルの設定方法の詳細については、各デバイスのプラットフォーム コンフィギュレーション ガイド（例：「Configuring SNMP support」）を参照してください。

ステップ 2 **デバイスの到達可能性を確認する**：すべてのモニター対象デバイスが Crosswork Data Gateway から到達可能であることを確認します。

LCM の使用に関する厳密な SID ラベルの有効化

LCM ドメイン内のすべてのデバイスで、厳密な SID が有効になっている必要があります。Cisco IOS XR および XE を実行しているデバイスで厳密な SID を設定するには、この例の手順を実行します。

LCM がこれらのトラフィック統計を受信していることを確認するには、次の手順を実行します。

手順

ステップ 1 LCM ドメイン内のすべてのデバイスに対して厳密な SID ラベルを有効にします。

ISIS を使用した Cisco IOS XR

```
router isis core
interface Loopback0
address-family ipv4 unicast
prefix-sid absolute 16003
prefix-sid strict-spf absolute 16503
!
address-family ipv6 unicast
!
!
```

OSPF を使用した Cisco IOS XR

```
router ospf 100
area 0
mpls traffic-eng
segment-routing mpls
interface Loopback0
passive enable
prefix-sid absolute 16002
prefix-sid strict-spf absolute 16502
!
```

Cisco IOS XE

```
segment-routing mpls
!
connected-prefix-sid-map
address-family ipv4
<ipv4-address> absolute 16010 range 1
exit-address-family
address-family ipv4 strict-spf
<ipv4-address> absolute 16510 range 1
exit-address-family
!
!
```

ステップ 2 一貫した SRGB でセグメントルーティングを有効にします。

ヘッドエンドデバイスでセグメントルーティングを有効にし、すべてのデバイスが以下の状態であることを確認します。

- 同じデフォルトの SRGB 範囲または指定されたカスタム範囲を使用している。

- ラベルスタックの深さに制限を課すデバイスがパスに沿って存在する場合 、最大 SID 深度が明示的に設定されている。

```
segment-routing
global-block 16000 80000
traffic-eng
maximum-sid-depth 8
```

ステップ 3 **厳密な SID ラベルを使用して SR-TE ポリシーを設定します。**

既存の SR ポリシーがある場合は、厳密な SPF SID ラベルを使用するようにヘッドエンドデバイスを設定する必要があります。

PCC によって開始または計算された SR ポリシーの場合

```
segment-routing
traffic-eng
policy srte_c_8000_ep
color 8000 end-point ipv4 <ipv4-address>
candidate-paths
preference 100
dynamic
metric
type igp
!
!
constraints
segments
sid-algorithm 1
```

PCE によって計算または委任された SR ポリシーの場合

```
policy srte_c_8001_ep_198.19.1.4
color 8001 end-point ipv4 198.19.1.4
candidate-paths
preference 100
dynamic
pcep
!
metric
type igp
```

厳密な SID のみを持つパスを返す PCE 設定

```
pce
segment-routing
strict-sid-only
```

自動ルートを使用したトラフィックステアリングの有効化

ヘッドエンドデバイスは、自動ルートステアリングを使用した 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。この機能は Cisco IOS XR デバイスでサポートされ、gRPC ポリシープロビジョニングを使用して Cisco Crosswork Network Controller 7.2 を介してプロビジョニングされます。ヘッドエンドデバイスが Cisco NCS デバイスであり、ネットワークに L2VPN トラフィックがある場合、LCM は正常に動作しないことに注意してください。

自動ルートを使用して 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、次の手順を実行します。

手順

ステップ 1 適切な PCC プロファイルの下で、`include ipv4 all` および `force-sr-include` を使用してヘッドエンドデバイスを設定します。

設定例

```
segment-routing
traffic-eng
pcc
profile 10      ! Profile ID must match the value in LCM Configuration > Basic > Profile ID
autoroute
include ipv4 all
force-sr-include
```

（注）
PCC プロファイルで設定されたプロファイル ID は、[LCM設定（LCM Configuration）] ページで設定されたプロファイル ID オプションと一致する必要があります。

プロファイル ID は、PCE がプロビジョニングした SR-TE ポリシーに関連付けられた PCC プロファイルを識別します。この ID には 1 ～ 65,535 の任意の整数を指定できますが、PCE がポリシーをインスタンス化するために使用するプロファイル ID と一致させる必要があります。値が一致しない場合、ポリシーはアクティブ化されません。たとえば、PCE がプロファイル ID 10 のポリシーをプロビジョニングする場合、そのポリシーの autoroute アナウンスを有効にするには、ヘッドエンドルータで `segment-routing traffic-eng pcc profile 10 autoroute force-sr-include` を設定する必要があります。

ステップ 2 詳細については、各デバイスのプラットフォーム コンフィギュレーション ガイド（たとえば、『*Segment Routing Configuration Guide, Cisco IOS XE 17 (Cisco ASR 920 Series)*』）を参照してください。

等コストマルチパスサポート

ヘッドエンドデバイスは、複数のパラレル SR-TE ポリシー全体で等コストマルチパス（ECMP）をサポートする必要があります。デバイスが ECMP で SR-TE ポリシーをサポートできることを確認するには、次のことを確認します。

- **セグメントルーティングが有効になっている**：SR-TE ポリシーのヘッドエンドルータとテールエンドルータの SRGB と一致する SRGB を使用して、セグメントルーティングが設定されていることを確認します。

  `show segment-routing mpls state` で確認

- **BGP-LS が有効になっている**：ヘッドエンドルータとテールエンドルータからリンクステート情報をアドバタイズして受信するように BGP-LS が設定されていることを確認します。

  `show bgp link-state link-state` でステータスを確認

`show bgp link-state link-state database` でリンクステート情報を確認

- **ECMP が有効になっている**：複数の等コストパス間でトラフィックをロードバランシングするように ECMP が有効化および設定されていることを確認します。

  `show ip route` で ECMP ルートを確認

  `show ip cef` で ECMP ロードバランシング アルゴリズムを確認

gRPC ポリシー管理のためのデバイスの準備

LCM の効率を最大化し、パフォーマンスを向上させるために、LCM は重み付けマルチセグメントリスト（MSL）を使用して SR-TE ポリシーをプロビジョニングできます。このアプローチにより、LCM ソリューションは通常、複数の重み付けセグメントリストを含む単一のポリシーで構成され、並列ポリシーを使用せずにトラフィックの迂回が可能になります。

重み付け MSL LCM ポリシーには、レガシーの PCE によって開始されたメソッドではなく gRPC ポリシープロビジョニングが必要であり、IOS XR バージョン 25.3.1 以降を実行しているシスコデバイスでのみサポートされています。このセクションでは、参加しているすべてのデバイスでこれらの高度な機能をサポートするために必要な追加の設定と要件について説明します。

- 対象ドメイン内のすべてのデバイスで gRPC を有効にします。
- SR MSL ポリシーを BGP-LS ピアおよび PCE ネイバーにアドバタイズします。
- PCEP での MSL ポリシーのレポートを防止します。
- デバイスに gRPC プロトコル接続を追加します。
- 「grpc_msl」または「GRPC_MSL」タグを作成してデバイスに割り当てます。

（注） MSL ポリシー展開をサポートするために、gRPC ポートが有効になっているデバイスがすべての Crosswork Network Controller ノードからアクセスできることを確認します。

自動モードを利用し、SR-TE で複数のセグメントリストをサポートするには、次の手順を実行します。

手順

ステップ 1 SR-TE ポリシーレポート用に gRPC を有効にする

IOS XR バージョン 25.3.1 より後を実行しているデバイスで、gRPC を有効にしてポリシーサービスと通信を許可します。

```
RP/0/RP0/CPU0:L1-NCS5501#sh running-config grpc
grpc
  segment-routing
    traffic-eng
```

```
    policy-service
  !
!
port 57400
no-tls
```

ステップ 2 BGP-LS ピアおよび PCE ネイバーに SR MSL ポリシーをアドバタイズする

完全な可視性を提供し、ネットワーク オーケストレーションをサポートするには、SR MSL ポリシーをピアと PCE ネイバーの両方に BGP-LS を介してアドバタイズする必要があります。これには、リンクステートデータベースへの SR MSL ポリシーのレポートの有効化と、リンクステート アドレス ファミリ内の PCE ネイバーとの BGP セッションの設定が含まれます。

a) **BGP-LS ピアへの SR MSL ポリシーのレポートを有効にする**

アクティブと非アクティブの両方の SR MSL ポリシーをリンクステートデータベースにレポートするようにルータを設定します。これにより、ポリシーを BGP-LS を介してコントローラまたはピアにアドバタイズできます。設定済みのすべての SR MSL ポリシーのレポートを有効にするには、次の設定スニペットを使用します。

```
RP/0/RP0/CPU0:L1-NCS5501#sh running-config segment-routing traffic-eng distribute link-state
segment-routing
  traffic-eng
    distribute link-state
      report-candidate-path-inactive
    !
  !
!
```

b) **BGP-LS を介して PCE ネイバーに SR MSL ポリシーをアドバタイズする**

PCE ネイバーとの BGP セッションを確立し、リンクステート アドレス ファミリを設定して、PCE がルータからすべての SR MSL ポリシーを受信して学習できるようにします。

（注）
交換を成功させるには、リンクステート アドレス ファミリがヘッドエンドと PCE の両方で設定されている必要があります。

```
RP/0/RP0/CPU0:L1-NCS5501#sh running-config router bgp
router bgp 60
  neighbor <NEIGHBOR_IP>   ! PCE neighbor
    remote-as 60
    update-source Loopback0
    address-family ipv4 unicast
      next-hop-self
    !
    address-family ipv6 unicast
    !
    address-family link-state link-state. ! Enable BGP-LS for SR MSL policy advertisement
    !
  !
```

ステップ 3 PCEP での MSL ポリシーのレポートを防止する

PCEP は MSL ポリシーを完全にはサポートしていないため（アドバタイズするのは単一のセグメントリストだけであるため、運用上の問題を引き起こす可能性があります）、ヘッドエンドルータの PCC 設定から

report-all コマンドを削除することを推奨します。この設定を使用して、SR MSL ポリシーが PCEP を介してレポートされなくなるようにします。

```
RP/0/RP0/CPU0:L4-NCS560#sh running-config segment-routing traffic-eng pcc
segment-routing
  traffic-eng
    pcc
      source-address ipv4 192.100.0.4
      pce address ipv4 100.100.0.1
        precedence 25
      !
      pce address ipv4 100.100.0.2
        precedence 50
      !
      !  Remove the following line to prevent reporting MSL policies to PCE
      !  report-all
      redundancy pcc-centric
      profile 1981
        autoroute
          include ipv4 all
          force-sr-include
        !
      !
    !
  !
!
```

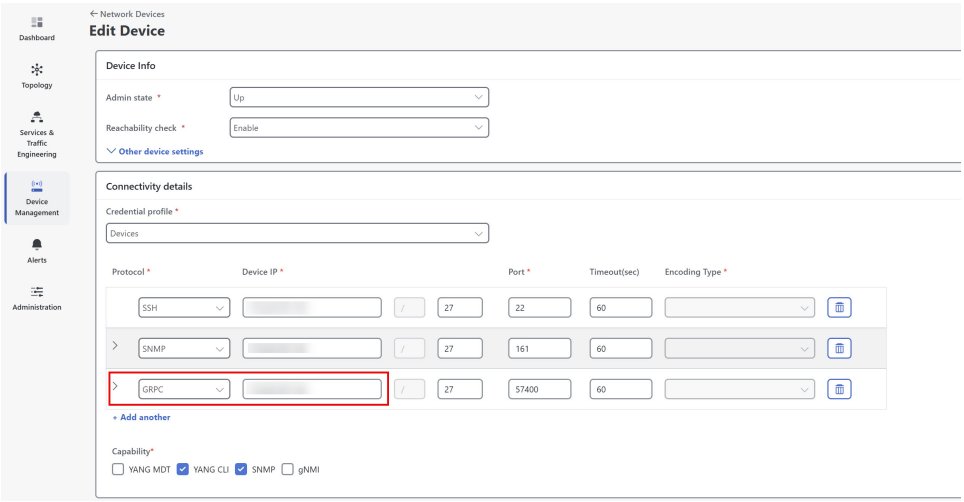
ステップ 4　gRPC プロトコル接続を追加する

[デバイス管理（Device Management）] で、対象ドメイン内のすべてのデバイスに gRPC プロトコル接続が設定されていることを確認します。

a) **[デバイス管理（Device Management）] > [ネットワークデバイス（Network Devices）]** に移動して、デバイス クレデンシャル プロファイルに gRPC プロトコルを追加できます。

b) 必要に応じて各デバイスを編集し、gRPC 接続の詳細を追加します。

図 *21 : gRPC* 接続の詳細のデバイスの編集



ステップ 5　「grpc_msl」または「GRPC_MSL」タグを作成してデバイスに割り当てる

（注）

このタグが存在する場合にのみ、LCM は MSL ポリシーを展開します。自動モードでは、PCE によって開始されたポリシーはサポートされません。手動モードでは、タグがない場合、LCM は PCE によって開始されたポリシーを展開します。

a) **[管理（Administration）]** > **[タグ管理（Tag Management）]** > を選択します。これにより、[タグの追加（Add tags）] ペインが表示されます。
b) [タグカテゴリの選択（Select tag category）] ドロップダウンリストからタグカテゴリを選択するか、テキストフィールドに新しいカテゴリの名前を入力して、[追加（Add）] をクリックします。
c) [<カテゴリ名>のタグを追加（Add tags for <category name>）] で、「grpc_msl」または「GRPC_MSL」タグを作成し、Enter キーを押します。
d) [保存（Save）] をクリックします。
e) **[デバイス管理（Device Management）]** > **[ネットワークデバイス（Network Devices）]** に移動し、タグ付けするデバイスを選択します。
f) をクリックします。これにより、[タグの編集（Edit tags）] ペインが表示されます。
g) [タグの関連付け（Associate tag）] フィールドに、作成した「grpc_msl」または「GRPC_MSL」タグを入力します。
h) 検索結果リストのタグをクリックして、デバイスに関連付けます。
i) [保存（Save）] をクリックします。

LCM を使用する際の重要な考慮事項

LCM ドメインの適切なセットアップ、最適な運用、および安全な管理を確保するために、これらの重要な考慮事項を確認してください。

ユーザーロールと権限

- LCM を設定して推奨事項をコミットする前に、ユーザーロールにドメインの LCM タスク権限が付与されていることを確認してください。RBAC およびユーザーロールの詳細については、『Cisco Crosswork Network Controller Administration Guide』を参照してください。
- デバイスアクセスグループ（DAG）アクセスは、LCM ではサポート**されていません**。LCM タスク権限を持つユーザーは、そのドメイン内のデバイスに対する DAG アクセス権の有無に関係なく、LCM の推奨事項を設定およびコミットできます。

サポートされるネットワーク機能と制限

- LDP ラベル付きトラフィックは、LCM 自動ルート TTE SR ポリシーにステアリングしないでください。LCM は、LDP ラベル付きトラフィックをサポートしていません。
- 不完全なトラフィック測定では計算が不正確になる可能性があるため、ツリー SID ポリシーを使用するネットワークでは LCM を使用しないでください。

ドメイン管理とデバイスのサポート

- 効率的なLCM運用を実現するため、ドメインは最大2,000デバイスに制限してください。ドメインは、BGP-LSアドバタイズメントに使用されるPCCルータの設定（リンクステートインスタンス ID）から IGP プロセスとドメイン ID によって識別されます。
- LCM 推奨ソリューションでは、単一ドメイン内のリソースのみが使用されます。
- 意図的または意図せずに、ドメインインターフェイスまたはリンクが削除されるか、ダウン状態（LINK_DOWN 状態）になった場合、LCM 設定とドメイン UI カード（LCM の設定 （61 ページ）を参照）はリンクがエージアウトするまで使用可能であり、回復時間は最大 4 時間です。
- 自動エージング期間の前にドメインを強制的に削除する必要がある場合は、UI からリンクを手動で削除します。ドメインは、最後のリンクが削除されるまで「削除準備完了」のままになります。

トラフィックの評価と統計

- LCMは、1分以上の設定可能な頻度で定期的にネットワーク使用率を評価します。デフォルトは 10 分です。この頻度は応答性を高めるために低く設定できますが、通常は SNMP のポーリング間隔以上に設定されます。
- トラフィック統計の収集間隔は、トポロジの変更や、インターフェイスとLSPトラフィックの測定値に影響を与える LSP 展開に対して LCM が応答する速さに影響します。変更を完全に反映するには、推奨事項の統計の収集間隔に LCM の評価間隔を加えた時間の、最大で 2 倍の時間が LCM でかかる場合があるので注意してください。この間にトラフィック測定値が更新され、最終的に Crosswork Network Controller で完全に収束するにつれて、LCM の推奨事項が改善される場合があります。

ECMP 処理と最適化の利用資格

- LCM は、パラレル TTE SR ポリシー全体で ECMP を使用し、トラフィックのほぼ均等な分割を想定します。実際のECMPの動作は、トラフィックのパターンや集約によって異なります。LCM は、過剰な不均一 ECMP を検出して通知するように設定できます。
- 不均一な ECMP の影響を軽減するために、LCM ではオーバープロビジョニング係数が使用されます。詳細については、「LCM の設定」を参照してください。
- 既存の SR-TE ポリシーから LCM TTE SR ポリシーにトラフィックをステアリングしないでください。既存の非 LCM SR-TE ポリシーで通常の Algo-0 プレフィックス SID を使用しないようにしてください。このトラフィックがLCM TTE SR ポリシーに誘導されないようにするために、Algo-1 Strict、Flexible Algorithm、または隣接関係 SID の任意の組み合わせが推奨されます。

高可用性（HA）および SR-PCE の動作

- HA スイッチオーバー後、システムが安定したら、以前にモニターされていた欠落しているインターフェイスを手動で追加したり、ドメイン構成オプションを更新したりできます。インターフェイスの欠落は、最後のクラスタデータの同期後に追加された場合に発生することがあります。

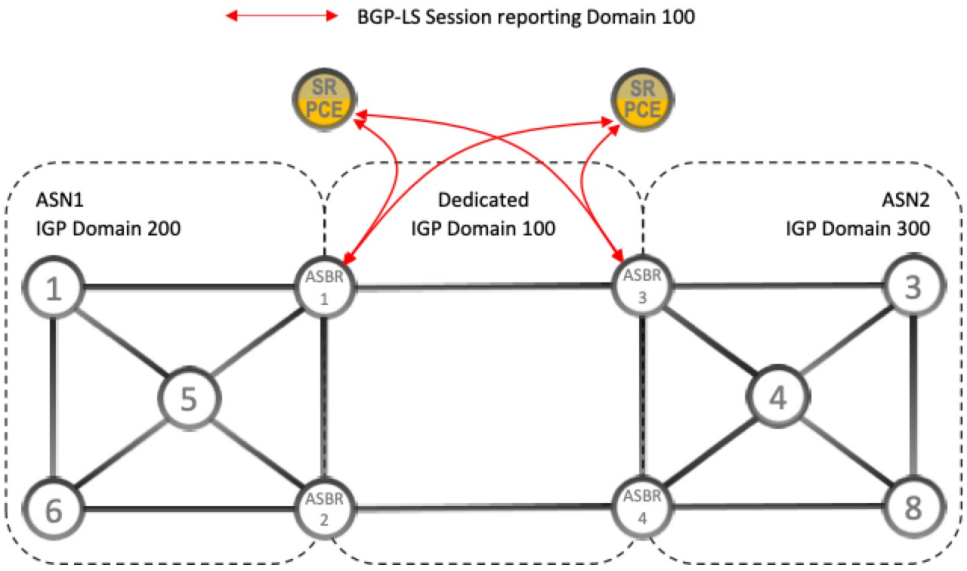
- SR-PCE がダウンすると LCM は休止状態に入り、すべての SR-PCE が再接続されて、関連するトポロジがトポロジサービスと完全に同期されるまで休止状態のままになります。LCM は、SR-PCE 冗長性セットの状態を把握できません。

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

ドメイン間遅延最適化 SR ポリシーパス計算とは、データ移動の遅延やレイテンシを最小限に抑えるために、SR-PCE を使用して異なるネットワーク（自律システム）間の最適なルートを見つけるプロセスを指します。このアプローチは、出力ピアエンジニアリング（EPE）がサポートされていない場合に特に重要です。

- **専用IGPインスタンス**：この計算をサポートするために、異なる自律システム番号（ASN）を介して、専用の内部ゲートウェイプロトコル（IGP）インスタンスを自律システム境界ルータ（ASBR）間に設定できます。
- **トポロジレポート**：正確なトポロジ検出には、BGP-LS（ボーダー ゲートウェイ プロトコル リンク ステート）を介してトポロジをレポートする ASBR を特定することが重要です。
- **BGP-LS 設定**：専用 AS 間 IGP（例：ドメイン 100）に参加している各 AS の少なくとも 1 つの ASBR で、各 ASBR 間の IGP を報告する BGP-LS が有効になっている必要があります。
- **BGP-LS 識別子**：各 ASBR は、ドメインをレポートするために同じ BGP-LS 識別子を使用する必要があります。
- **複数 ASBR のサポート**：AS ごとに複数の ASBR が BGP-LS トポロジをレポートできるため、トポロジレポートには柔軟性があります。

図 *22 : BGP-LS* セッション報告ドメイン *100*

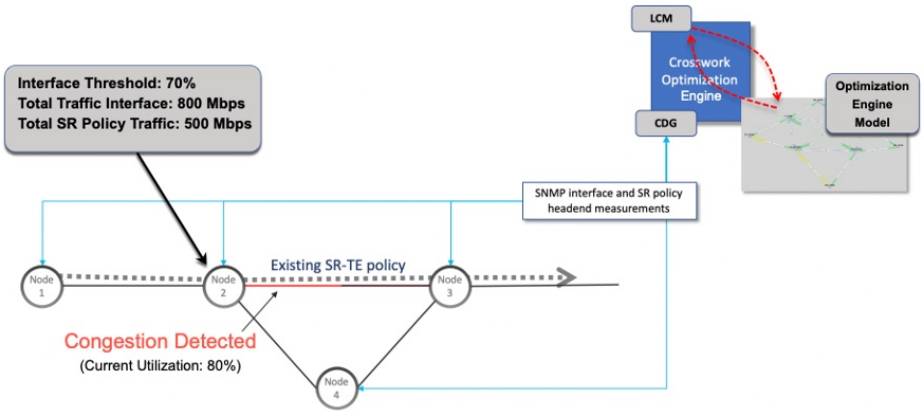


LCM 計算のワークフロー

process_summary

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するまでのプロセスについて説明します。計算はドメイン単位で実行されるため、大規模なネットワークの拡張性が向上し、計算が高速になります。

図 *23 : LCM* の設定ワークフローの例



process_workflow

1. **ネットワーク状態の分析**：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。この例では、

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

2. **対象トラフィックの計算**：LCMは、転送対象となるトラフィックの量を計算します。LCMは、既存の SR ポリシーや RSVP-TE トンネルでルーティングされていないトラフィック（ラベルなし、IGP ルーティング、または FlexAlgo-0 SID 経由で転送されていないトラフィックなど）のみを転送します。SR-TEポリシー内のトラフィックは、LCM計算から除外され、元のプログラムされたパスを通過し続けます。

   LCMは、インターフェイスの合計トラフィックから、インターフェイスを通過するすべてのSR-TEポリシーのトラフィック統計情報の合計を差し引くことにより、転送対象のトラフィックを計算します。

   インターフェイス トラフィックの合計 - SR ポリシートラフィックおよび RSVP-TE トンネル = 最適化できる対象トラフィック

   このプロセスでは、SR ポリシーの ECMP 分割を考慮して、SR ポリシートラフィックを適切にアカウンティングする必要があります。この例では、輻輳したノード 2 の合計トラフィックは 800 Mbps であり、ノード 2 を介して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。したがって、LCM が転送できる合計トラフィックは 800 Mbps - 500 Mbps = 300 Mbps です。

3. **トラフィックの転送量計算**：LCM は、合計のインターフェイス 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トラフィック量を判定します。この例では、LCM は、300 Mbps のうちの 100 Mbps（対象トラフィック）を別のパスにルーティングする必要があります。

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

4. **オーバープロビジョニング係数（OPF）**：OPFは、ソリューションの計算中に輻輳しきい値から差し引かれるパーセンテージを表し、使用率のヘッドルームを確保して、不規則なECMP トラフィック分散を考慮します。たとえば、輻輳しきい値が 80% で OPF が 3% の場合、オプティマイザはソリューションを計算するときに77%の有効しきい値を使用します。OPF は、[LCM Configuration] ウィンドウの [Advanced] タブで設定できます。詳細については、LCM の設定 （61 ページ）を参照してください。

5. **TTE SR ポリシーの決定**：

   - **複数の並列戦術 SR-TE ポリシー**：

     LCMは、トラフィック分割比率に基づいて必要なTTE SRポリシーの数とそのパスを計算します。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必要なTTE SRポリシーの数が決まります。

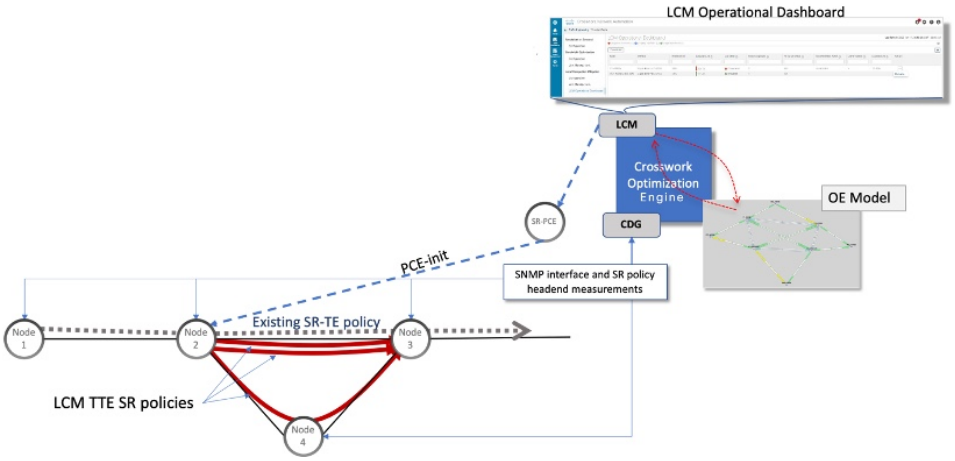
     この例では、LCMは輻輳したリンクから対象トラフィックの合計の1/3（300 Mbpsのうち100 Mbps）を転送する必要があります。LCMは完全なECMPを想定し、このトラフィック分割には3つの戦術的SR-TEポリシーが必要だと予測します。1つの戦術的SR-TEポリシーが転送パスをとり、2つの戦術的SR-TEポリシーが元のパスをとります。ノード2とノード4の間のパスに十分な容量があります。したがって、LCMで

は、SR-PCE を介してノード 2 からノード 3 に 3 つの TTE SR ポリシー（それぞれ約 100 Mbps をルーティングすると想定）を展開することを推奨しています。

- 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）] に表示されます。

図 *24 : LCM* の推奨例



- **重み付けセグメントリストが複数含まれる単一 TTE SR ポリシー**：

LCMは、複数の重み付けセグメントリストを含む、輻輳インターフェイスごとに単一の戦術的な SR-TE ポリシーを計算します。各セグメントリストは個別のパスに対応し、重み付けによって各パスに誘導される合計トラフィックの割合が決まります。このアプローチでは、トラフィックをほぼ均等に分割する複数の並列SR-TEポリシーを展開する代わりに、LCMは重み付けを使用して、最短パスと1つ以上の迂回パスでのトラフィック配信を正確に制御します。これにより、必要なポリシーの数が削減され、並列ポリシーによって引き起こされるダウンストリームECMPの影響が排除されます。

この例では、複数の並列戦術的 SR-TE ポリシーを展開する代わりに、LCM は単一の戦術的SR-TEポリシーを作成します。このポリシーには、トラフィック配信を正確に制御するために 2 つの重み付けセグメントリストが含まれています。

- 一方のセグメントリストは、ノード 2 からノード 3 への最短の IGP パスに対応し、約 200 Mbps（対象トラフィックの 3 分の 2）を伝送するように重み付けされています。
- もう一方のセグメントリストは、ノード 4 を経由する迂回パスに対応し、約 100 Mbps（対象トラフィックの 3 分の 1）を伝送するように重み付けされています。

このアプローチにより、ポリシー管理が簡素化され、複数の並列ポリシーに比べてトラフィックエンジニアリングをより細かく制御できます。トラフィックパターンが変

化すると、LCMはポリシーを追加または削除することなく、この単一ポリシー内のセグメントリストの重み付けを動的に調整できます。これにより、管理が簡素化されます。

6. **モニタリングと調整**：LCMは展開されたTTEポリシーを継続的にモニターし、[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を推奨します。LCMは、展開されたTTE RSポリシーが削除された後も緩和されたインターフェイスに輻輳が発生しない場合（保留マージンを除く）、ポリシーを削除することを推奨します。これにより、LCMの操作全体で不必要なTTE SRポリシーのチャーンを回避できます。

LCM 動作のモニター

LCM ダッシュボードとそのモニタリングロールは以下のとおりです。

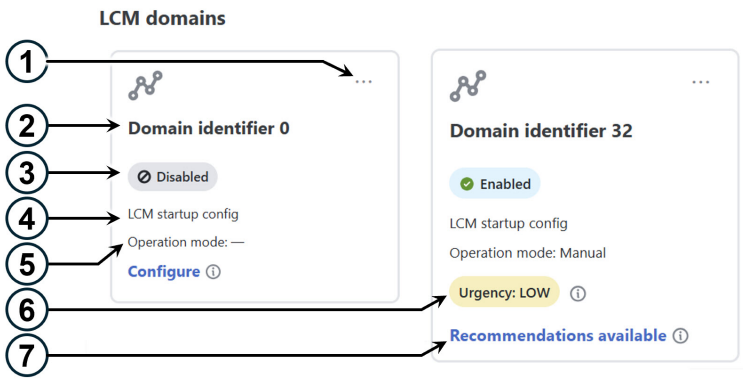
- [LCMドメインダッシュボード（LCM domain dashboard）]：検出されたすべてのドメインと、ドメイン識別子、LCM ステータス、設定の説明、動作モード、緊急レベルなどの重要な情報が表示されます。また、LCM が設定されていない場合の設定リンクや、輻輳が検出された場合の TTE ポリシー推奨事項を表示するリンクも提供されます。
- [LCM運用ダッシュボード（LCM Operational Dashboard）]：設定された使用率しきい値で定義された輻輳インターフェイスを表示します。
- [LCM操作履歴（LCM operational history）]：評価、コミット、一時停止、再開、緩和状態、低下状態などの各主要 LCM イベント後に、詳細なタイムスタンプ付きスナップショットが表示され、輻輳管理アクティビティの時系列かつ視覚的な記録として機能します。

ネットワークで LCM を使用する方法については、例：ローカルインターフェイスでの輻輳の緩和 （55 ページ）のトピックを参照してください。

LCM ドメインダッシュボード

LCM ドメインダッシュボード（**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）]>[ローカル輻輳緩和（Local Congestion Mitigation）]**）には、Crosswork Network Controllerによって検出されたすべてのドメインが表示されます。ドメインは、IGPプロセスに割り当てられる識別子です。

図 *25 : LCM* ドメインダッシュボード



引き出し線番号	説明
1	**メインメニュー**：以下のページに移動できます。 • 運用ダッシュボード（Operational dashboard） • 操作履歴（Operational history） • インターフェイスのしきい値（Interface thresholds） • 設定（Configuration）
2	**ドメイン識別子**：ドメイン ID は、BGP-LS で IGP をアドバタイズするために使用するルータ設定（`link-state instance-id`）から取得されます。
3	**LCM ステータス**：ドメインで LCM が有効になっているか、または削除可能かどうかを示します。
4	**LCM 設定の説明**：説明は、[LCMの設定（LCM Configuration）] ページで定義されます。デフォルトの説明は「LCM startup config」です。
5	**操作モード**：LCM が自動モードで実行されているか、手動モードで実行されているかを示します。デフォルトは手動モードです。 • [自動モード（Automated mode）]：LCM は、ユーザーが設定したしきい値に基づいて TE トンネルの推奨事項を自動的に展開します。自動モードは、gRPC MSL に完全準拠したドメインでのみサポートされています。 • [手動モード（Manual Mode）]：このオプションを使用する場合、ユーザーは [LCM運用ダッシュボード（LCM Operational Dashboard）] を確認し、TE トンネルの推奨事項をコミットするかどうか決める必要があります。

引き出し線番号	説明
6	[緊急性（Urgency）]：推奨事項の展開またはアクションの重要性を示します。 • [低（Low）]：LCM インスタンス化ポリシーが不要になったために削除できること、または変更が不要であることを示します。 • [中（Medium）]：新規または変更された推奨事項を示します。 • [高（High）]：ネットワーク障害と推奨事項を展開する必要があることを示します。これは、[自動修復ソリューション（Auto repair solution）] の詳細オプションが有効になっている場合に自動的に対処できる候補です。LCM の設定（61 ページ）を参照してください。 [休止（Dormant）]：ドメインが非アクティブの場合に、このステータスが表示されます。LCM は、休止状態のドメインに何の操作も実行しません。
7	**設定**：このリンクは、LCM がまだ設定されていない場合に表示されます。[設定（Configure）] をクリックして、[LCMの設定（LCM Configuration）] ページに移動します。 **使用可能な推奨事項**：このリンクは、LCM が輻輳を検出し、TTE ポリシーの推奨事項がある場合に表示されます。LCMの推奨事項を表示するには、リンクをクリックして [LCM運用ダッシュボード（LCM Operational Dashboard）] に移動します。 **削除**：ドメインカードを LCM モニタリング対象から削除できることを示します。

LCM 運用ダッシュボード

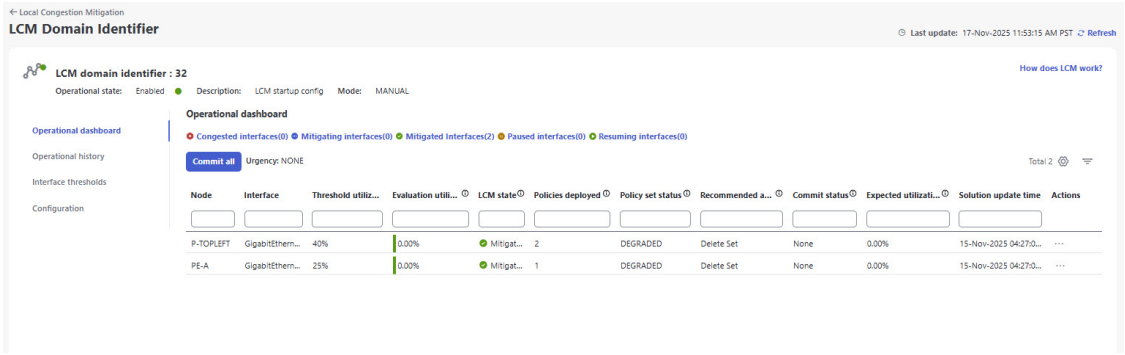
LCM 運用ダッシュボードでは、輻輳を軽減するためのトラフィック エンジニアリング ポリシーとパスの推奨をプレビューできます。輻輳インターフェイスとは、設定された使用率しきい値を超えているインターフェイスです。

LCM 運用ダッシュボードへのアクセス

LCM 運用ダッシュボードにアクセスするには：

1. メインメニューから、**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）]** > **[ローカルでの輻輳緩和（Local Congestion Mitigation）]** > ***[Domain-ID]*** > ··· > **[運用ダッシュボード（Operational dashboard）]** を選択します。

図 *26 : LCM* 運用ダッシュボード



各インターフェイスには、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。

2. 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。[アクション（Action）] 列には、次のオプションがあります。

   - [ソリューションのプレビュー（Preview solution）]：このオプションを選択すると、[推奨TTEポリシーのプレビュー（Recommended TTE policies preview）] ページが開き、輻輳を軽減するために LCM が提案したポリシーが表示されます。MSL ポリシーをサポートするヘッドエンドの場合、MSL ベースのポリシーが推奨ソリューションとして表示される場合があります。
   - [展開されたポリシーの表示（View deployed policies）]：このオプションにより、[トラフィックエンジニアリング - LCM展開済みポリシー（Traffic Engineering - LCM deployed policy）] ページが開き、輻輳を緩和するために展開されたさまざまなポリシーが表示されます。[アクション（Actions）] メニューの各ポリシーの [詳細の表示（View details）] をクリックすると、さまざまなパスとセグメントが詳細なポリシー情報とともに表示されます。
   - [再開（Resume）] / [一時停止（Pause）]：インターフェイスを一時停止または再開します。

LCM の状態とダッシュボードの動作

[緩和状態（Mitigated state）]：LCM が緩和状態のとき、ダッシュボードには、以前の輻輳に対処するために現在展開されているポリシーの数が表示されます。また、推奨アクションも示されます。たとえば、「セットの削除（Delete Set）」推奨事項は、今後輻輳が予想されないためこれらのポリシーを削除することを示します。[コミットステータス（Commit status）] は、推奨事項がコミットされていない場合は [なし（None）]、適用されている場合は [コミット済み（Committed）] と表示されます。

[輻輳状態（Congested state）]：LCM が輻輳を検出すると、状態が [輻輳（Congested）] に変わります。ダッシュボードには輻輳を修復するための推奨アクションが表示されます。たとえば、「セットの作成（Create Set）」推奨事項は新しいポリシーの展開を推奨します。コミット

する前に、[アクション（Actions）] メニュー（…）>[ソリューションのプレビュー（Preview solution）]）から新しいソリューションをプレビューできます。

（注） LCM がソリューションを見つけられない場合（[推奨処置（Recommended Action）] : [ソリューションなし（No Solution）]）、[LCM設定（LCM configuration）] で有効になっている制約が原因の可能性があります。詳細については、「LCM の設定 （61 ページ）」を参照してください。

[一時停止状態（Paused state）] : LCM が一時停止状態のとき、[操作履歴（Operational history）]LCM 操作履歴 （47 ページ） に 2 つのイベントが表示されます。1 つは、削除対象のポリシーの評価に関するものであり、もう 1 つはその削除のコミットに関するものです。同様に、ポリシーを再開する際は、評価イベントが新しいコミットイベントの前に行われます。LCM が輻輳チェック一時停止間隔にある場合、操作履歴に再開イベントが表示されますが、間隔が経過するまで待機してから新しいソリューションを計算します。

推奨事項はセットとして展開されるため、変更を適用するには [すべてをコミット（Commit all）] をクリックする必要があります。

LCM 操作履歴

LCM 操作履歴は、ネットワーク内の LCM の過去のアクションを確認および分析するための強力な手段です。イベントは、評価中、ポリシーのコミットまたは削除時、インターフェイスの一時停止または再開時、輻輳状態の変更時など、主要なポイントで生成されます。主要な LCM イベントが発生するたびに詳細なタイムスタンプ付きスナップショットを取得することで、輻輳管理アクティビティの視覚的な時系列レコードが得られます。ノードおよびインターフェイスごとにデータをフィルタ処理して、関連するイベントをすばやく見つけることができます。履歴レコードは、構成可能な設定に基づいて保持されます（デフォルトは 30 日）。この履歴により、次の情報が示されることで、監査、トラブルシューティング、および運用のレビューが可能になります。

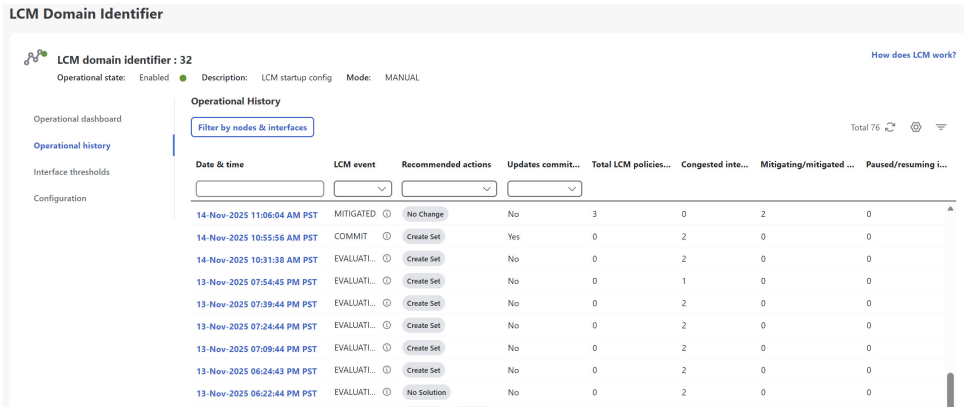
- 各イベントの日時
- LCM イベントのタイプ（コミット、低下、評価、緩和、一時停止、および再開）
- イベントの結果に基づく推奨アクションまたは次のステップ
- 推奨される変更がネットワークに展開されたかどうかを示す、コミット済みの設定の更新
- 展開された LCM ポリシーの総数
- 輻輳インターフェイスの数
- 緩和中/緩和済みインターフェイスの数
- 一時停止/再開中インターフェイスの数
- イベントリストを特定のノードおよびインターフェイスに絞り込むためのフィルタリングオプション

LCM 操作履歴へのアクセス

LCM 操作履歴を表示するには、次の手順を実行します。

1. メインメニューから、**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）] > [ローカルでの輻輳緩和（Local Congestion Mitigation）] >** [Domain-ID] > ··· **> [操作履歴（Operational history）]** を選択します。

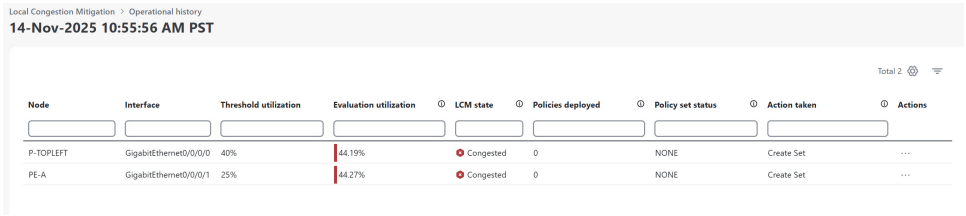
図 *27 : LCM* 操作履歴



テーブルの行には、LCM イベントの操作履歴が表示されます。イベントが一時停止すると、ユーザーの操作があるまで、一時停止状態が継続します。運用ダッシュボードで一時停止したポリシーを確認し、必要に応じて再開できます。

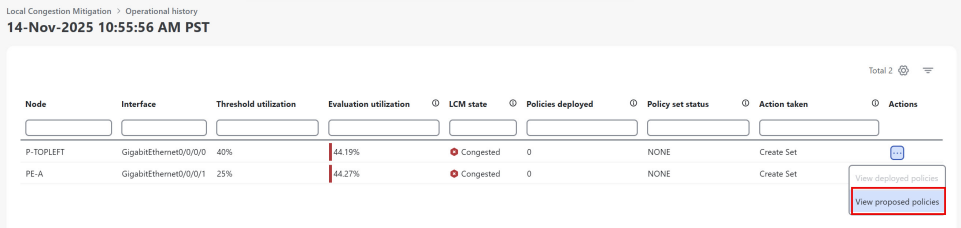
2. テーブル内の任意のイベントをクリックすると、特定の時点のダッシュボードの状態とそのイベントの結果としてのダッシュボードの状態を確認できます。LCM 操作履歴によって提供される情報をより詳しく理解するには、上の画像の 2 行目のイベント（[2025年11月14日10時55分56秒PST（14-Nov-2025 10:55:56 AM PST）]）をクリックしてください。イベントの詳細が表示されます。このページでは、インターフェイスが 44% の使用率で輻輳していることが確認できます。

図 *28 :* 操作履歴イベントスナップショット



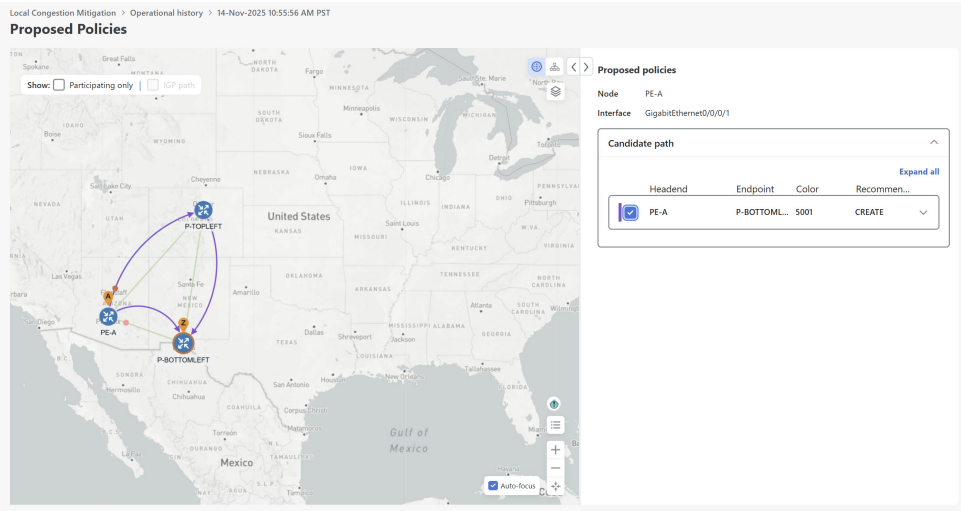
3. [アクション（Actions）]列の ··· をクリックし、[提案されたポリシーの表示（View proposed policies）] を選択すると、生成されたソリューションでポリシーが可視化されます。これにより、過去のイベントのより適切なインサイトが得られます。

図 *29* : 操作履歴イベントスナップショット - アクション



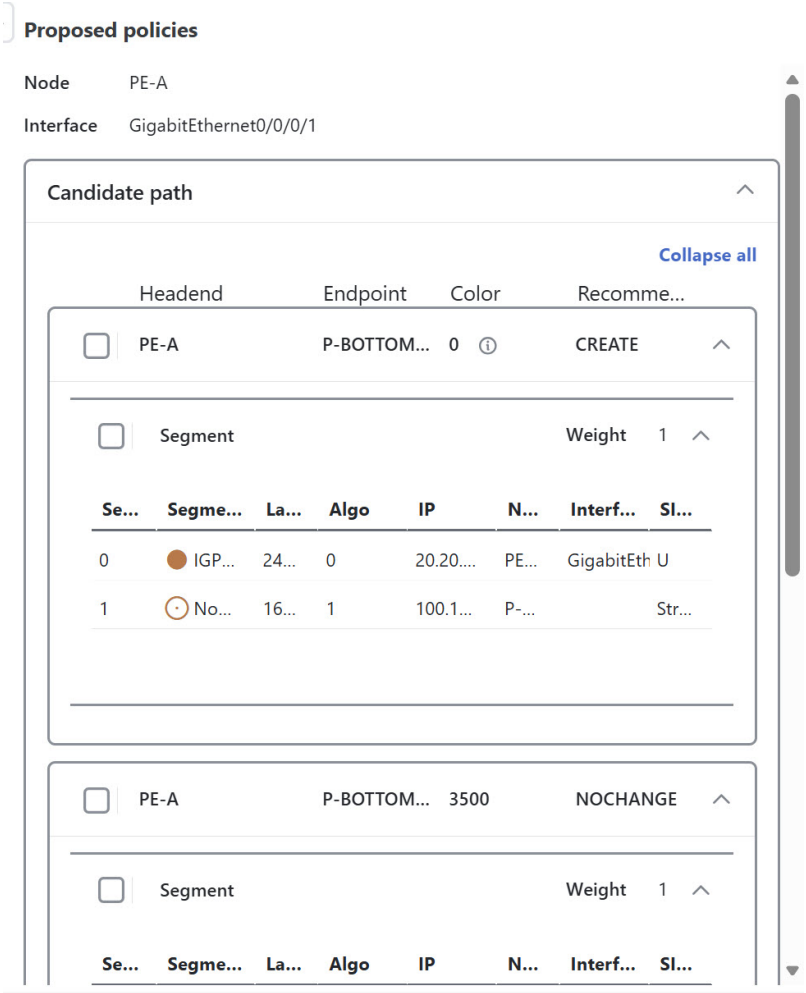
[提案されたポリシー（Proposed policies）] ページには、そのイベントの輻輳を緩和するために提案されたポリシーが表示されます。

図 *30* : 操作履歴イベントスナップショット - 提案されたポリシー



4. [候補パス（Candidate Path）] エリアで、[すべて展開（Expand All）] をクリックして、提案されたポリシーをセグメントリストの詳細とともに表示します。MSL ポリシーをサポートするヘッドエンドの場合、提案されたソリューションとして MSL ベースのポリシーが表示される場合があります。

図 *31* : 複数のセグメントリストを持つ提案されたポリシー



LCM ソリューションイベント

LCM によるイベントの生成は、評価の状態、ユーザーアクション、および輻輳チェック間隔と密接に関連しています。

表 *3 : LCM* ソリューションイベントと説明

LCM イベント	説明
評価	LCMが輻輳を検出して緩和ポリシーを計算した後に、新しい推奨事項があることを示します。この段階では、ソリューションを一時停止またはコミットできます。 輻輳チェックの一時停止間隔が経過すると、実行されたアクションに応じて、輻輳が解決された場合は緩和状態、問題が解決しない場合は低下状態に変わります。 （注） ポリシープレビューの色はコミット後に変更される場合があります。
Commit	輻輳を緩和するために、推奨事項がコミット（展開）されていることを示します。 （注） 別のポリシーで使用されている場合、ポリシープレビューの色が変更されることがあります。
低下（Degraded）	緩和ソリューションによってインターフェイスの輻輳が完全に解決されていないか、コミットされたポリシーにもかかわらず輻輳が悪化していることを示します。
緩和（Mitigated）	輻輳チェックの一時停止間隔が経過した後に、コミットされた推奨事項によって輻輳が正常に解決されたことを示します。インターフェイスの輻輳は解消されました。
一時停止	ソリューションを一時停止する要求を受信したことを示します。インターフェイスは、緩和計算から一時的に除外されています。 一時停止すると、操作履歴に 2 つのイベントがトリガーされます。1 つは、削除対象のポリシーの**評価**を示すものであり、もう 1 つはその削除の**コミット**に関するものです。LCMは、ソリューションを計算する前に、輻輳チェックの一時停止間隔が経過するまで待機します。ユーザーは後でインターフェイスを再開できます。このとき、再開イベントも生成されます。
復帰（Resume）	ソリューションを再開する要求を受信したことを示します。インターフェイスは、緩和計算に再度含まれます。操作履歴では、コミットイベントの前に評価イベントが表示されます。LCMが輻輳チェック一時停止間隔にある場合、操作履歴に再開イベントが表示されますが、間隔が経過するまで待機してからソリューションを計算します。

LCM からのインターフェイスの一時的な除外

自動モードまたは手動モードで、軽減のために LCM にインターフェイスを含めるのを一時的に停止できます。インターフェイスは一時停止されると、推奨項目の一部とは見なされなくなり、そのインターフェイスが参加している既存のソリューションはすべて削除されます。自動モードでの操作の一時停止は、次のような多くの使用例で必要になる場合があります。

- 展開されたソリューションで意図した解決につながらない場合
- ECMP トラフィックが不均一な場合
- トラフィックを伝送しないポリシーがある場合
- インターフェイスが異なるソリューション間で継続的にスロットリングしている場合

次のような特定の異常が検出されると、LCM によってインターフェイスが自動的に一時停止されることがあります。

- LCM SR ポリシートラフィックがない
- LCM ポリシートラフィックの過剰な不均衡
- 1 時間あたりの過剰な LCM 振動や削除数

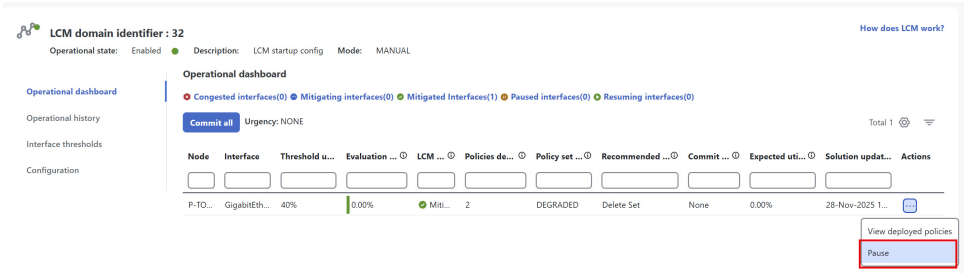
このような状況では、ユーザーは修正処置を実行し、手動でインターフェイスを再開できます。

インターフェイスの一時停止と再開

[LCM運用ダッシュボード（LCM Operational Dashboard）] の [アクション（Actions）] 列で、LCM 計算から除外するインターフェイスに対して [一時停止（Pause）] を選択します。LCM 計算にインターフェイスを再度含めるには、[再開（Resume）] を選択します。

（注） 複数のインターフェイスを同時に一時停止すると、要求がタイムアウトする可能性がありますが、各要求はキューに入り、ダッシュボードに表示されます。

図 *32 :* インターフェイスの一時停止



輻輳の自動緩和

LCM 自動モードでは、ネットワークに自動的に変更を加えることで、ユーザーの介入なしでシステムを稼働させることができます。すべてのデバイスがgRPCMSLに完全準拠しているドメインにおいて、ネットワーク輻輳の継続的なクローズドループ検出および緩和が可能になります。この要件を満たすために、対象ドメイン内の各デバイスは gRPC プロトコル接続をサポートし、準拠を示すgRPCMSLタグが適用されている必要があります。自動モードを有効にすると、システムはネットワーク輻輳をモニターし、設定されたしきい値に基づいて輻輳を軽減するために、複数セグメントリスト（MSL）ポリシーを自動的に適用または削除し、手動介入の必要性を減らします。

（注） 自動モードでは、LCM は複数セグメントリスト（MSL）ポリシーのみを展開できます。PCE によって開始されたポリシーはサポートされていません。

LCM は、自動モードで自動修復ソリューションも適用します。輻輳を緩和するだけでなく、ネットワークの問題を特定し、積極的に対処します。

自動モードには、過剰なソリューション振動を検出するための保護策が含まれています。設定されたしきい値を超える緩和ポリシーの展開と削除がインターフェイスで繰り返し発生した場合、システムはネットワークの安定性を維持するために、そのインターフェイスの自動アクションを自動的に一時停止します。

Before you begin

- 対象ドメイン内のすべてのデバイスが gRPC 対応になるように、gRPC ポリシー管理のためのデバイスの準備 （34 ページ）内のすべての要件を満たします。
- 「grpc_msl」または「GRPC_MSL」タグを作成し、[タグ管理（Tag Management）] で準拠デバイスに割り当てていることを確認します。

（注） このタグが存在する場合にのみ、LCM は MSL ポリシーを展開します。自動モードでは、PCE によって開始されたポリシーはサポートされません。手動モードでは、タグがない場合、LCM は PCE によって開始されたポリシーを展開します。

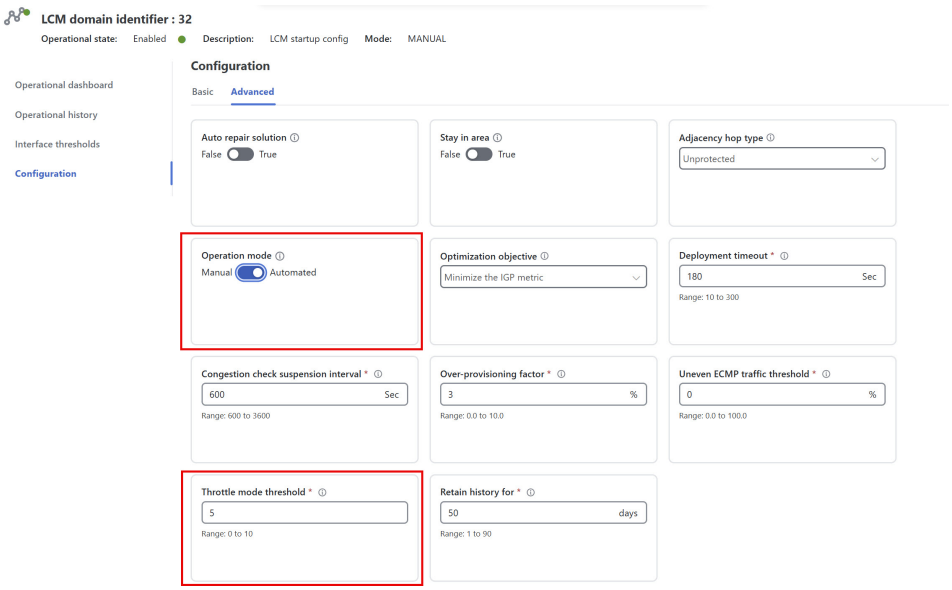
自動モードを有効にするには、次の手順を実行します。

手順

ステップ 1 メインメニューから、**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）]** > **[ローカルでの輻輳緩和（Local Congestion Mitigation）]** > **[LCM-Domain-Card]** を選択します。 をクリックし、[設定（Configuration）] を選択します。

ステップ 2 [詳細（Advanced）] タブで、[動作モード（Operation mode）] オプションを [自動（Automated）] に切り替えます。ドメイン内のデバイスに「grpc_msl」または「GRPC_MSL」タグがない場合、または gRPC が設定されていない場合、システムは自動モードを有効にせず、非準拠デバイスのリストを表示します。

図 *33 : LCM* 設定 - *[自動（Automated）]* モード



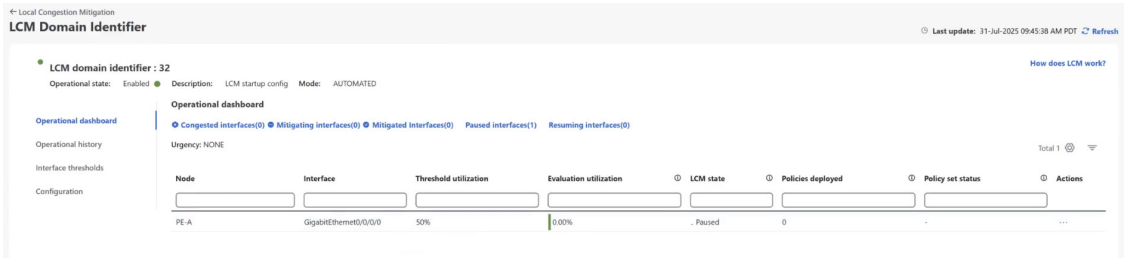
ステップ 3 [スロットルモードしきい値（Throttle mode threshold）] フィールドは、LCM が 1 時間以内にインターフェイスでソリューションを適用または削除できる最大回数です。いずれかのインターフェイスでのポリシー変更がこのしきい値を超えると、LCM はそのインターフェイスの自動アクションを一時停止し、ネットワークの安定性を維持するための新しいソリューションの提案を停止します。一時停止したイベントは、ユーザーが介入するまでこの状態のままです。必要に応じて、一時停止したポリシーを運用ダッシュボードから確認および再開できます。値を 0 に設定すると、振動検出が無効になります。

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。設定の変更をコミットすると、モニター対象インターフェイスで輻輳が発生した場合、LCM は [LCM運用ダッシュボード（LCM Operational Dashboard）] に推奨事項を表示します。

[LCM運用ダッシュボード（LCM Operational Dashboard）] には、ドメインに関連付けられている現在のインターフェイスと緩和ステータスが表示されます。自動モードでは、輻輳を継続的にモニターし、設定されたしきい値に基づいて必要に応じて MSL ポリシーを展開または削除します。

必要に応じて、展開されたポリシーと一時停止されたインターフェイスも確認できます。

図 *34 : LCM* 運用ダッシュボード



例：ローカルインターフェイスでの輻輳の緩和

この例では、LCM を有効にし、インターフェイスの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。この例では、次の手順について説明します。

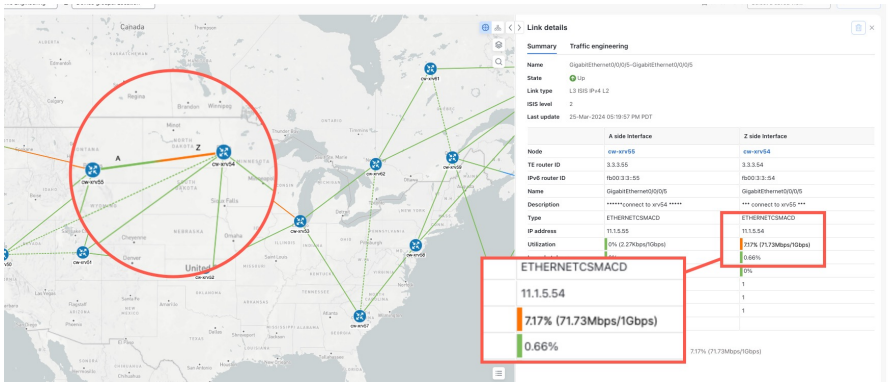
1. 輻輳していないネットワークトポロジを表示します。
2. 個々のインターフェイスの使用率のしきい値を設定します。
3. LCM を有効にし、手動モードで設定します。これにより、推奨される TTE ポリシーを展開するかどうかを決定する前に確認できます。
4. LCM が輻輳を検出した後、[運用ダッシュボード（Operational dashboard）] で推奨事項を表示します。
5. 推奨される LCM TTE ポリシーをトポロジマップで視覚的にプレビューします。
6. すべての推奨される LCM TTE ポリシーをコミットして展開し、輻輳を緩和します。
7. LCM TTE ポリシーが正常に展開されていることを確認します。

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

手順

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。この例では、ノード cw-xrv54 の使用率が 7.17% であることに注意してください。

図 *35 :* 初期使用率



ステップ 2 個別のインターフェイスしきい値の定義

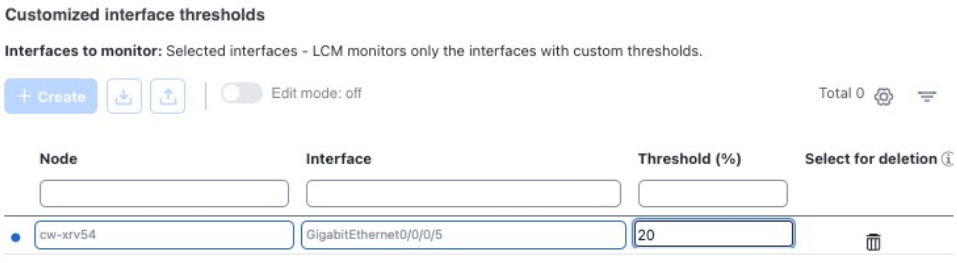
LCM では、すべてのインターフェイスに使用できるグローバル使用率のしきい値を設定できます。トラフィック使用率がしきい値を超えると、LCMは輻輳を修正するためにバイパスポリシーを見つけようとします。[LCMの設定（LCM Configuration）] ページでグローバル使用率のしきい値を設定します。ただし、個々のインターフェイスに異なるしきい値を定義する場合は、LCM を有効にする前に、[カスタマイズされたインターフェイスのしきい値（Customized interface threshold）] ページでそれらを定義することをお勧めします。

a) この例では、個々のインターフェイスのしきい値を定義します。[カスタマイズされたインターフェイスのしきい値（Customized interface threshold）] ページに移動します（**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）]** > **[ローカル輻輳緩和（Local Congestion Mitigation）]** > [ドメイン識別子（Domain-Identifier）] > ··· > **[インターフェイスのしきい値（Interface thresholds）]**）。インターフェイスを個別に追加したり、カスタムの使用率しきい値を持つノードとインターフェイスのリストを含む CSV ファイルをアップロードしたりできます。詳細については、「個別のインターフェイスしきい値の追加 （68 ページ）」を参照してください。

次の例を参照してください。インターフェイス GigabitEthernet0/0/0/1 を使用する cw-xrv54 の定義済みしきい値は 20% です。

（注）
この例の使用率のしきい値は非常に低く、ラボ環境での使用に最適です。

図 *36 :* カスタマイズされたインターフェイスのしきい値



（注）

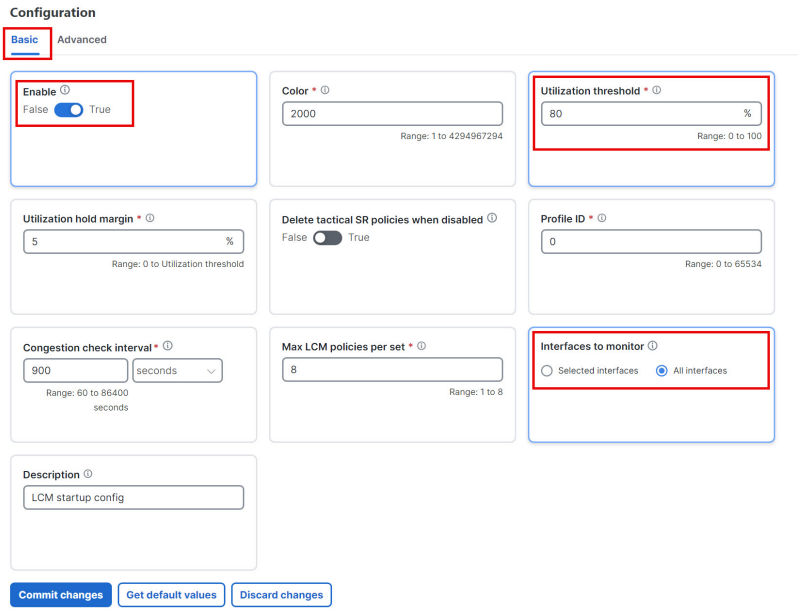
デフォルトでは、LCM はすべてのインターフェイスを監視します。対象には、このページにインポートされた個々のしきい値が含まれます。残りのインターフェイスは、[LCMの設定（LCM Configuration）] ページで定義されたグローバルな [使用率のしきい値（Utilization threshold）] を使用して監視されます。

b) インターフェイスを追加し、しきい値を定義したら、[保存（Save）] をクリックします。

ステップ 3 LCM を有効にし、グローバル使用率のしきい値を設定します。

a) メインメニューから、**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）]** > **[ローカル輻輳緩和（Local Congestion Mitigation）]** > [ドメイン識別子（Domain-Identifier）] を選択し、[設定（Configuration）] をクリックします。[有効化（Enable）] スイッチを [True] に切り替え、他の LCM オプションを設定します。この例ではグローバルしきい値は 80% に設定され、[監視するインターフェイス（Interfaces to monitor）] > [すべてのインターフェイス（All interfaces）] オプションが選択されています。[詳細設定（Advanced）] タブで、[動作モード（Operation Mode）] が [手動（Manual）] に設定されています。すべての使用できるオプションの詳細については、LCM の設定 （61 ページ）を参照してください。

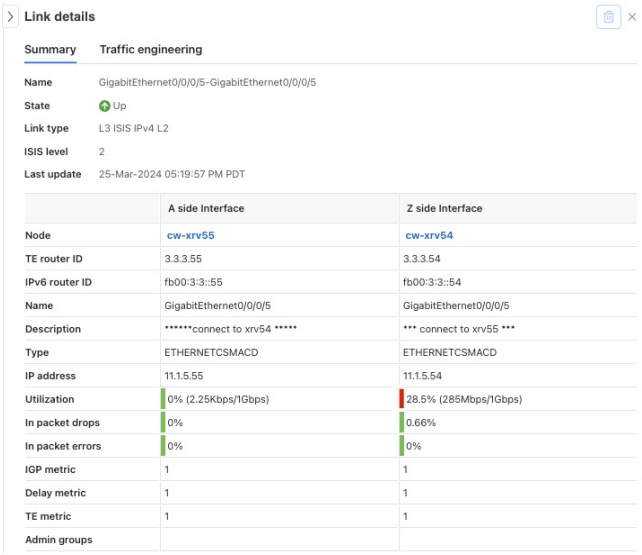
図 *37 : LCM* 設定ページ



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

ステップ 4 しばらくすると、GigabitEthernet0/0/0/5 インターフェイスのノード cw-xrv54 に対して 20% で定義されたカスタム LCM しきい値を超える輻輳が発生します。

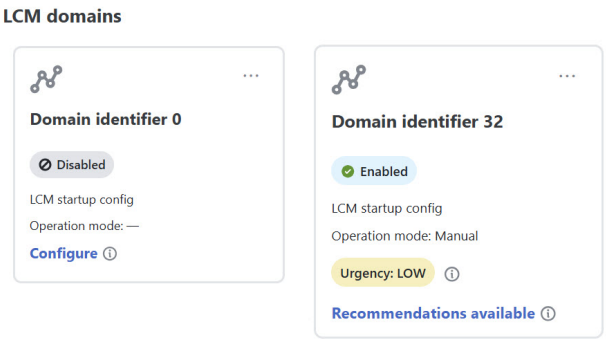
図 *38*：確認された輻輳



ステップ 5 [LCM Operational Dashboard] で TTE SR ポリシーの推奨事項を表示します。

a) **[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）] > [ローカル輻輳緩和（Local Congestion Mitigation）]** に移動します。輻輳が検出されると、ドメインには緊急度のタイプと利用可能な推奨事項が表示されます。疑問符アイコンをクリックすると、緊急度のタイプと、最新の推奨事項が提示された時期に関する詳細が表示されます。

図 *39*：検出された輻輳と *LCM* の推奨事項



b) （オプション）LCM イベントを表示します。

Crosswork Network Controller UI の右上隅から > [イベント（Events）] タブをクリックして、LCM イベントを表示します。このウィンドウをモニターして、発生したLCMイベントを表示することもできます。LCM の推奨事項、コミットアクション、および例外のイベントを確認する必要があります。

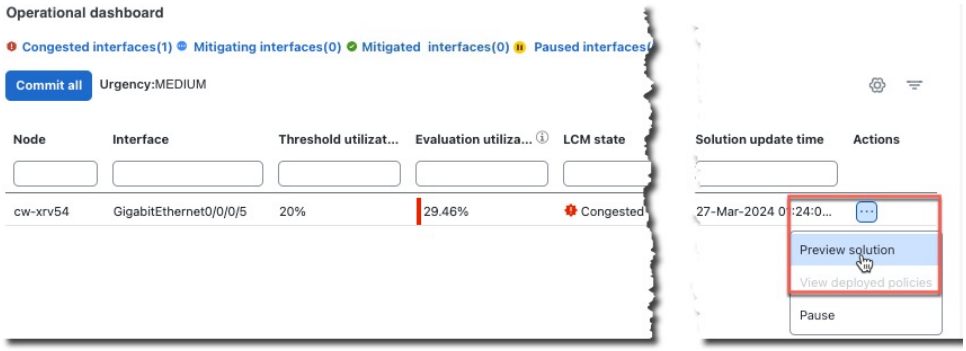
c) [運用ダッシュボード（Operational Dashboard）] を開きます（**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）] > [ローカルでの輻輳緩和（Local Congestion Mitigation）]** > [ドメイン識別子（Domain-Identifier）] > > **[運用ダッシュボード（Operational Dashboard）]**）。

cw-xrv54 の使用率が 20% を超えていて、29.46% であることがダッシュボードに表示されます。[推奨処置（Recommended action）] 列では、LCM により、インターフェイスの輻輳に対処するために TTE ポリシーのソリューションセット（[推奨処置（Recommended action）] : [セットの作成（Create set）]）を展開することが推奨されています。詳細については、LCM 動作のモニター （43 ページ）を参照してください。

（注）
LCM がソリューションを見つけられない場合（[推奨処置（Recommended action）] : [ソリューションなし（No solution）]）、LCM の設定（LCM の設定 （61 ページ））時に有効にした制約が原因の可能性があります。

d) TTE ポリシーをコミットする前に、各 TTE ポリシー ソリューション セットの展開をプレビューできます。[アクション（Actions）] 列で … をクリックし、[解決策のプレビュー（Preview solution）] を選択します。

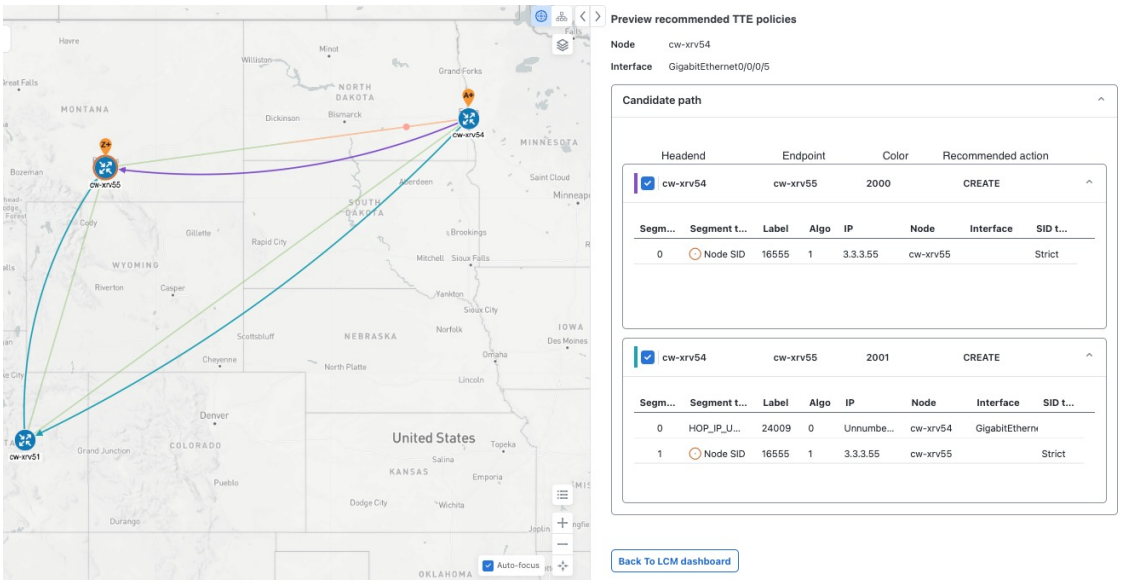
図 *40* : ソリューションのプレビュー



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。[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。各ポリシーを展開して、個々のセグメントを表示できます。ネットワークへの潜在的な影響を検討してから、LCM が推奨するバイパスポリシーを展開するかどうかを決定できます。

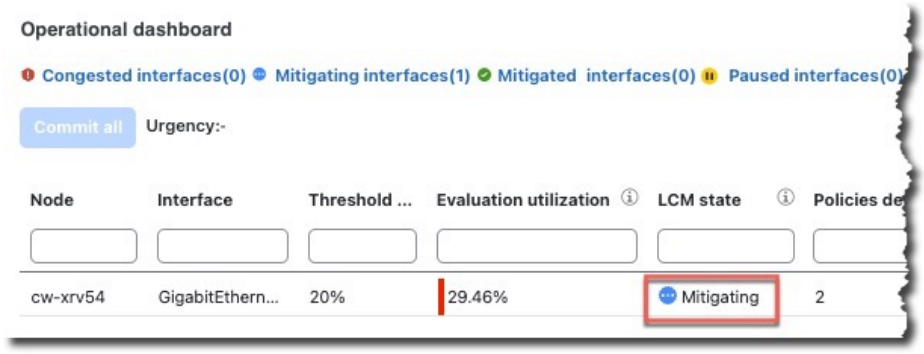
次の図は、ノード cw-xrv54 の推奨 TTE ポリシーを示しています。

図 *41 : LCM TTE* 展開のプレビュー



e) マップ上で推奨される TTE ポリシーを確認したら、[運用ダッシュボード（Operational dashboard）] に戻り、[すべて確定（Commit all）] をクリックします。[LCMの状態（LCM state）] 列が [緩和中（Mitigating）] に変化します。

図 *42 : [*緩和中（*Mitigating*）*]* 状態



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

ステップ 6 TTE SR ポリシーの展開を検証します。

a) > [Events] タブをクリックします。[Events] ウィンドウに表示される LCM イベントを確認します。

（注）

Crosswork Network Controller は、ユーザーが有効にしたポリシーと機能に基づいて検出されたネットワークイベントを報告します。たとえば、リンクがドロップしたことで SR-TE ポリシーがダウンした場合や、LCM が輻輳を検出した場合は、イベントが表示されます。これらのアラートは UI で報告され、必要に応じてサードパーティのアラート/モニタリングツールに転送できます。

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

（注）
LCM の状態が変化するまでに、SNMP パターンの 2 倍の時間がかかります。

c) トポロジマップを表示して、TTE ポリシーの展開を確認します。

[アクション（Actions）] 列の … をクリックし、[展開されたポリシーを表示（View deployed policies）] を選択します。展開されたポリシーは、トポロジマップ内で強調表示されます。

ステップ 7 LCM の推奨に従って TTE SR ポリシーを削除します。

a) しばらくすると、展開された TTE SR ポリシーが不要になる場合があります。これは、LCM によって開始された TTE トンネルがなくても、使用率がしきい値を下回り続ける状況が続く場合に発生します。この場合、LCM は TTE SR ポリシーセットを削除するための新しい推奨処置を生成します。

b) 以前に展開された TTE SR ポリシーを削除するには、[すべて確定（Commit all）] をクリックします。

c) トポロジマップと [SRポリシー（SR Policy）] テーブルを表示して、削除を確認します。

このシナリオでは、LCM を使用してネットワークトラフィックの輻輳を緩和する方法を確認しました。LCM は、追跡と計算を自動化して手動の作業を削減しますが、輻輳を軽減するための推奨事項を実行するかどうかを制御できます。推奨事項をプレビューし、ネットワークへの潜在的な影響を評価してから、推奨事項を展開できます。トラフィックパターンが変化すると、LCM は展開された TTE SR-TE ポリシーを継続的にモニターし、引き続き必要かどうかを判断します。ポリシーが不要になった場合、LCM はポリシーを削除することを推奨します。

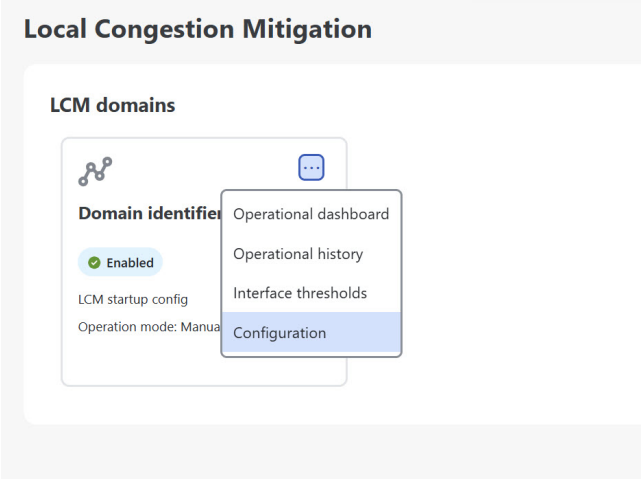
LCM の設定

LCM を有効にして設定するには、次の手順を実行します。

手順

ステップ 1 メインメニューから、**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）] > [ローカルでの輻輳緩和（Local Congestion Mitigation）] [> Domain-identifier-card]** を選択します。⋯ をクリックし、次に **[Configuration]** をクリックします。

図 *43 : LCM* の設定



ステップ 2 [有効化（Enable）] を [はい（True）] に設定します。

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については、LCM 設定オプション （62 ページ）セクションを参照してください。

ステップ 4 設定を保存するには、[変更のコミット（Commit changes）] をクリックします。モニター対象インターフェイスで輻輳が発生した場合、LCM は [LCM運用ダッシュボード（LCM Operational dashboard）] に推奨事項を表示します。LCM は新しい TTE ポリシーを自動的にコミットまたは展開しないことに注意してください。推奨される TTE ポリシーをプレビューし、コミットしてネットワークに展開するかどうかを決定できます。

（注）
LCM が有効になっているのに解決策が見つからない場合（[推奨処置（Recommended action）] : [解決策なし（No solution）]）、このページで有効になっている制約が原因である可能性があります。

LCM 設定オプション

これらの表は、UI で使用可能な LCM 設定オプションに関する情報を提供します。

- 基本 LCM 設定
- LCM の詳細設定

LCM の基本オプション

表 *4 :* 基本設定オプション

オプション	説明
Enable	LCM 機能パックを有効または無効にします。

オプション	説明
Color	この値から始まる SR ポリシーに順番にカラー値を割り当てます。
使用率のしきい値（Utilization threshold）	インターフェイスが輻輳していると LCM が判断する使用率を設定します。この値は、[カスタマイズされたインターフェイスのしきい値（Customized interface thresholds）] ページで個々のインターフェイスにしきい値を指定しない限り、すべてのインターフェイスに適用されます。
使用率保留マージン（Utilization hold margin）	この値は、展開された戦術的 SR ポリシーの削除を抑制します。たとえば、使用率しきい値が 90% で、使用率保留マージンが 5% の場合、戦術的 SR ポリシーが配置されていない状態でインターフェイスの合計使用率が 85%（90 - 5）を下回る場合にのみ、戦術的 SR ポリシーがネットワークから削除されます。
無効化されたときに戦術的SRポリシーを削除（Delete Tactical SR Policies when Disabled）	LCM が無効の場合、展開されたすべての戦術的 SR ポリシーを削除します。
プロファイル ID	LCM ポリシーへのトラフィックステアリングを有効にするために必要な設定です。autoroute（LCM が作成する戦術的な SR-TE ポリシーへのトラフィックのステアリング）は、（プロファイル ID を autoroute 機能に関連付ける PCC 上の設定と一致させるために）ここで設定した適切な [Profile ID] オプションを介して SR-TE ポリシーに適用されます。
輻輳確認間隔（Congestion check interval）（秒）	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、変更する必要があるかどうかを判断します。たとえば、間隔が 600 秒（10 分）に設定されている場合、LCM は 10 分ごとにネットワークを評価して新しい輻輳を確認し、新しい推奨事項、または既存の推奨事項に対する変更が必要かどうかを判断します。変更の例としては、以前に推奨された個々のポリシーの削除や更新などがあります。このオプションは通常、SNMP ポーリング頻度以上に設定されますが、トラフィック収集間隔によって課される範囲内で応答性を向上させるために、60 秒という低い値に設定することもできます。
セットあたりの最大 LCMポリシー（Max LCM policies per set）	単一のインターフェイスを緩和するために使用される戦術的ポリシーの最大数です。

オプション	説明
監視するインターフェイス（Interfaces to monitor）	デフォルトでは、[選択されたインターフェイス（Selected interfaces）] に設定され、[カスタマイズされたインターフェイスのしきい値（Customized interface thresholds）] ページ（**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）] > [ローカル輻輳緩和（Local Congestion Mitigation）] > [ドメイン識別子（domain-identifier）]** > ··· > **[インターフェイスのしきい値（Interface thresholds）]**）で CSV ファイルをインポートして、しきい値を個々のインターフェイスに追加する必要があります。[カスタマイズされたインターフェイスのしきい値（Customized interface thresholds）] ページで定義されたインターフェイスのみが監視されます。[すべてのインターフェイス（All interfaces）] に設定すると、LCM は、[カスタマイズされたインターフェイスのしきい値（Customized interface thresholds）] ページでアップロードされたカスタムしきい値を持つインターフェイスと、このページで設定された [使用率のしきい値（Utilization threshold）] 値を使用している残りのインターフェイスを監視します。
説明	ドメイン識別子の説明です。

LCM の詳細オプション

表 *5:* 詳細設定オプション

オプション	説明
自動修復ソリューション（Auto repair solution）	[はい（True）] に設定すると、LCM はダウン、失敗、またはコミットされていない LCM TTE ポリシーを自動的に削除します。これは、主にポリシーの障害に対処するためのオプションです。 このオプションが無効で、[LCM運用ダッシュボード（LCM Operational Dashboard）] に表示される推奨の [緊急（Urgency）] ステータスが [高（High）] の場合、推奨されるソリューションは [自動修復ソリューション（Auto repair solution）] の候補です。これは、ソリューションが展開されていない場合にネットワーク障害が発生する可能性が高いことを意味します。
エリアに留まる（Stay in area）	バイパス LSP パスを制限して、OSPF の緩和エリアまたは ISIS のレベル内に留まるようにします。

オプション	説明
隣接ホップタイプ（Adjacency hop type）（秒）	[保護（Protected）] に設定すると、LCM は保護された隣接関係 SID を使用して SR ポリシーを作成します。これにより、トポロジに依存しないループフリー代替（TI-LFA）で隣接関係の障害のパスを計算できます。 このオプションは、LCM が動作している同じ IGP エリア内のすべてのノードが厳密な SPF SID 対応である場合にのみ、[Protected] に設定する必要があります。
動作モード	• [自動モード（Automated mode）]：このオプションを使用すると、LCM は、ユーザーが設定したしきい値に基づいて TE トンネルの推奨事項を自動的に展開できます。 • [手動モード（Manual Mode）]：このオプションを使用する場合、ユーザーは [LCM運用ダッシュボード（LCM Operational Dashboard）] を確認し、TE トンネルの推奨事項をコミットするかどうか決める必要があります。
最適化の目的	LCM は、最小化するために選択されたメトリックタイプに基づいて戦術的な SR ポリシーを計算します。
展開のタイムアウト（Deployment timeout）	戦術的な SR ポリシーの展開を確認するために許可される最大秒数を入力します。
輻輳チェック抑制間隔（Congestion check suspension interval）（秒）	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。
オーバープロビジョニング係数（Over-provisioning factor）（OPF）	このオプションは、計算中に輻輳しきい値を設定されたパーセンテージだけ下げて、使用率にマージンを提供し、不規則な ECMP トラフィック分散を考慮します。たとえば、輻輳しきい値が 80% で OPF が 3% の場合、オプティマイザはソリューションを計算するときに 77% の有効しきい値を使用します。デフォルト値は 0 です
不均一なECMPトラフィックしきい値（Uneven ECMP Traffic Threshold）	ソリューション バイパス トンネル全体の不均一な量のトラフィックを検出する感度のパーセンテージです。
スロットルモードしきい値（Throttle mode threshold）	自動モード時に、インターフェイスが自動的に一時停止するまでに LCM がソリューション間でスロットルを行う 1 時間あたりの回数を入力します。

オプション	説明
履歴の保持期間（Retain history for）	データが削除されるまでに収集および保持される期間です。デフォルト値は 30 日です。削除プロセスは 24 時間ごとに、または設定された保持時間に変更がある場合に発生します。
デバッグオプティマイザ（Debug optimizer）	デバッグオプティマイザが Crosswork Network Controller ファイルシステムにプランファイルをログ記録できるようにします。ファイルは [デバッグオプティマイザ最大計画ファイル（Debug opt max plan files）] で指定した最大ファイル数で保存されます。
最大セグメントホップ（Maximum segment hops）	このオプションを使用する前に、特定の MSD 値を割り当てるデバイスタググループを作成する必要があります。タグの作成とデバイスへのタグの割り当てについては、『Cisco Crosswork Network Controller Administration Guide』を参照してください。 バイパス TTE ポリシーを計算する場合、LCM は指定されたデバイスタグの有効な最大 SID 深度（MSD）値（ここで入力）を使用します。特定の MSD 値を持つデバイスタグを 5 つまで割り当てることができます。 値が **0** の場合、解決にはなりません。**0** の値を設定した場合は LCM 監視と同等になり、推奨事項を提供せずにネットワークに輻輳があることを示します。 システムは、SR-PCE から各プラットフォームの MSD を学習し、IGP および BGP-LS のハードウェア制限をアドバタイズします。これは、サービス/トランスポート/特殊ラベルを除いて適用できるハードウェア制限を表します。したがって、この新しいオプションを使用して、アドバタイズされた MSD 値よりも小さい値を割り当てることができ、LCM はバイパス TTE ポリシーの計算にその値を使用できます。デバイスの MSD 値を表示するには、[トラフィックエンジニアリング（Traffic Engineering）] トポロジマップに移動し、そのデバイスをクリックします。[デバイスの詳細（Device details）] ページで、**[SR-MPLS]** > > **[プレフィックス（Prefixes）]** > **[すべて展開（Expand all）]** をクリックします。
アフィニティ	アフィニティを使用して特定の基準に基づいてデータをルーティングすることにより、リンクを含めるか除外するように LCM を設定できます。たとえば、アフィニティが除外される場合、LCM はそのアフィニティを持たないパスを使用してトラフィックを転送することにより、輻輳リンクを緩和しようとします。アフィニティ名のリストを表示するには、アフィニティをデバイスであらかじめ設定し、Crosswork ネットワークコントローラ UI を使用してマッピングする必要があります。例：Cisco IOS-XR のアフィニティ設定 （67 ページ）およびリンクアフィニティの設定 （67 ページ）を参照してください。

リンクアフィニティの設定

リンクアフィニティは、リンクに関連付けられた属性またはタグです。リンクアフィニティは、帯域幅の可用性、遅延、コストなどの特定の基準に基づいて、優先パスに沿ってトラフィックを誘導するのに役立ちます。インターフェイスのアフィニティ構成は、単にいくつかのビットをオンにします。これは32ビット値で、各ビット位置（0ー31）はリンク属性を表します。アフィニティマッピングは、特定のタイプのサービスプロファイルを表す色にすることができます（たとえば、低遅延、高帯域幅など）。Crosswork ネットワークコントローラ は、プロビジョニング中にビット情報を SR-PCE に送信します。

ポリシーパスのプロビジョニング時に LCM に考慮させるアフィニティがある場合は、次の手順を実行します。

手順

ステップ 1 デバイスでアフィニティを設定します。「例：Cisco IOS-XR のアフィニティ設定 （67 ページ）」を参照してください。

ステップ 2 Crosswork Network Controller でのアフィニティの追加 （67 ページ）。

ステップ 3 高度なアフィニティオプションを使用して、LCM の設定 （61 ページ）を実行します。

例：Cisco IOS-XR のアフィニティ設定

デバイスにアフィニティ設定を適用する方法はいくつかあります。

特定のデバイスの Segment Router 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。

Cisco IOS-XR のアフィニティ設定例

```
segment-routing
traffic-eng
interface GigabitEthernet0/0/0/1
affinity
name red
name blue
affinty-map
name red bit-position 1
name blue bit-position 5
```

Crosswork Network Controller でのアフィニティの追加

Crosswork ネットワークコントローラ はデバイスのアフィニティ名を収集しません。リンクアフィニティを使用しやすくするために、デバイスで使用されているものと同じ名前とビットを使用して Crosswork ネットワークコントローラ でアフィニティマッピングを定義します。ア

フィニティ名がマッピングされていない場合、UI にはアフィニティ名が「UNKNOWN」と表示されます。

アフィニティを追加するには、以下の手順を実行します。

Before you begin

デバイスでアフィニティを設定し、メモします。

手順

ステップ 1 メインメニューから、**[管理（Administration）] > [設定（Settings）] > [トラフィックエンジニアリング（Traffic Engineering）] > [アフィニティ（Affinity）] > [TEリンクアフィニティ（TE Link Affinities）]** を選択します。LCM の設定時にアフィニティを定義することもできます（[制約（Constraints）] > [アフィニティ（Affinity）] フィールドの [マッピングの管理（Manage Mapping）] をクリック）。

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

ステップ 3 名前と割り当てるビット位置を入力します。

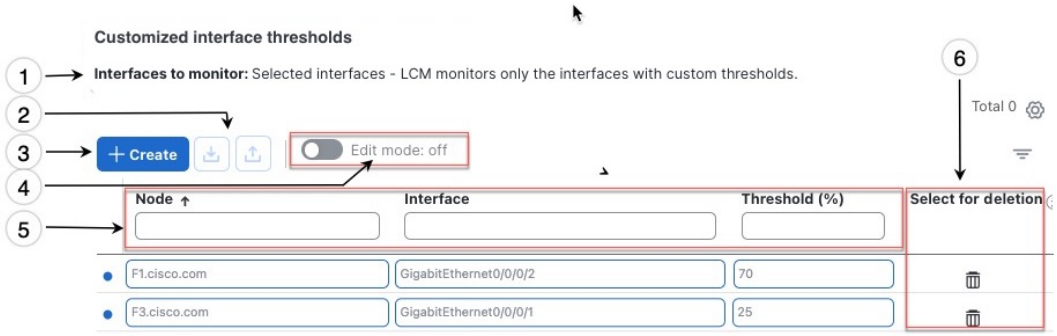
図 *44*：アフィニティ

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

個別のインターフェイスしきい値の追加

ネットワークにはさまざまなリンク（10G、40G、100G）があり、異なるしきい値を設定する必要があります。[カスタマイズされたインターフェイスのしきい値（Customized interface thresholds）] ページでは、個々のしきい値を管理し、ノードとインターフェイスに割り当てることができます。

図 *45* : カスタマイズされたインターフェイスのしきい値



引き出し線番号	説明
1	**監視するインターフェイス**：[LCMの設定（LCM Configuration）]LCM の設定 （61 ページ）ページで現在設定されているオプションを表示します。
2	**CSV ファイルのインポート**：現在テーブルにあるすべてのインターフェイスは、インポートする CSV ファイルのデータに置き換えられます。 **CSV ファイルのエクスポート**：すべてのインターフェイスが CSV ファイルにエクスポートされます。エクスポートするデータをフィルタリングすることはできません。
3	[+作成（+Create）]：このボタンをクリックして、新しいインターフェイスのしきい値行を追加します。
4	[編集モード（Edit mode）]：[編集モード（Edit mode）] が [オン（ON）] の場合、1 つのセッションで複数のフィールドを編集して、[保存（Save）] をクリックできます。
5	**フィルタ**：デフォルトでは、この行はコンテンツをフィルタするテキストを入力するために使用できます。
6	[削除対象の選択（Select for deletion）]：行を削除するには、 をクリックします。[編集モード（Edit mode）] が [オン（ON）] の場合、削除する複数の行をチェックしてから、[保存（Save）] をクリックできます。

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。

手順

ステップ 1 メインメニューから、**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）]** > **[ローカルでの輻輳緩和（Local Congestion Mitigation）]** > **[ドメイン識別子（Domain-identifier）]** > ··· > **[イ**

ンターフェイスのしきい値（Interface thresholds）] を選択します。インターフェイスの追加方法を選択します。

- [CSVファイルのインポート（Import CSV File）]：CSV ファイルを編集してインターフェイスとしきい値のリストを含め、後でファイルを LCM にインポートします。
- [新しいインターフェイスの追加（Add new interface）]：個々のインターフェイスとしきい値を手動で追加します。

ステップ 2 CSV ファイルをインポートする場合は次の手順を実行します。

a) [サンプル設定ファイルのダウンロード（Download sample configuration file）] リンクをクリックします。
b) [キャンセル（Cancel）] をクリックします。
c) ダウンロードした構成ファイル（LCMLinkManagementTemplate.csv）を開き、編集します。サンプルテキストを特定のノード、インターフェイス、およびしきい値情報に置き換えます。
d) ファイルの名前を変更して保存します。
e) [カスタマイズされたインターフェイスのしきい値（Customized interface thresholds）] ページに戻ります。
f) [CSVファイルのインポート（Import CSV file）] をクリックして、編集した CSV ファイルに移動します。
g) [インポート（Import）] をクリックします。

ステップ 3 個々のインターフェイスを手動で追加する場合は次の手順を実行します。

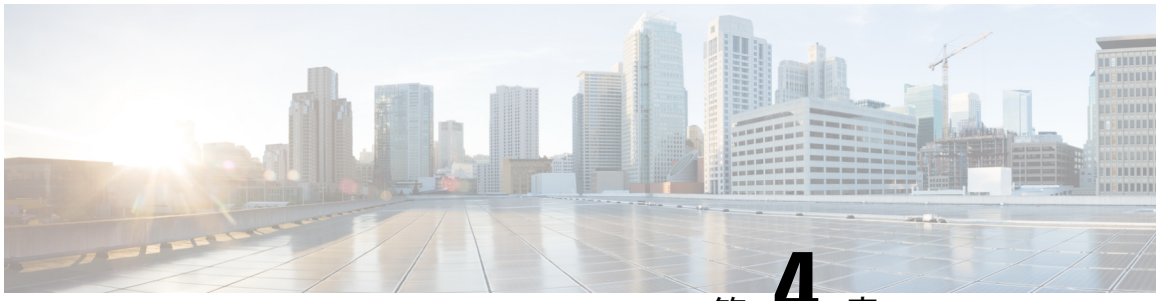
a) 最初の空の行をクリックし、適切なノード、インターフェイス、およびしきい値を入力します。

図 *46*：最初のインターフェイスの追加

b) [+作成（+ Create）] をクリックして、インターフェイスを追加します。

ステップ 4 [カスタマイズされたインターフェイスのしきい値（Customized interface thresholds）] ページに情報が正しく表示されることを確認します。

（注）
テーブルを更新するには、編集モードをオンにするか、テーブル内の現在のすべてのデータを置き換える CSV ファイルをインポートします。



第 4 章

オンデマンド帯域幅（BWoD）

オンデマンド帯域幅

帯域幅オンデマンド（BWoD）は、次の機能を持つ帯域幅対応パス計算要素（PCE）です。

- SR-PCE と統合して、要求された帯域幅要件を満たす SR ポリシーパスを計算します。
- 特定のユーザー定義インテントに基づいてネットワーク内のエンドポイント間にパスを作成し、ネットワーク条件が変化してもこれらの帯域幅保証を動的に維持します。
- PCC によって開始された（PCE によって委任された）ポリシーと PCE によって開始されたポリシーの両方をサポートし、SR ポリシーに対してソフトな帯域幅の保証を提供します。

BWoD の主な機能

BWoD の主な機能は次のとおりです。

- **インテントベースのパス計算**：BWoD は、IGP コスト、TE メトリック、または遅延の最小化などのユーザー定義インテントに基づいて SR ポリシーパスを作成します。
- **継続的なモニタリングと再最適化**：BWoD は、ネットワーク条件を継続的にモニターし、BWoD パスを自動的に再最適化して、いずれかのインターフェイス上の BWoD トラフィックの合計が設定されたしきい値パーセンテージを超えないようにします。

（注） ここで説明する機能は、特定のライセンスオプションでのみ使用できます。

BWoD の制限事項

BWoD はインターフェイスの総使用率を追跡しないため、BWoD と非 BWoD のトラフィック合計がキャパシティを超えた場合でも、インターフェイスが輻輳する可能性があります。さらに、BWoD では BWoD SR ポリシーに入るトラフィックの総量は強制されません。BWoD ポリシーは、トラフィック配信が均等であることを前提として等コストマルチパス（ECMP）パスを通過する可能性がありますが、実際の ECMP 配信は、特に大規模なフローでは不規則である可能性があります。

BWoD を使用する際の重要な考慮事項

BWoD を使用する場合は、次の情報を考慮してください。

- デバイスアクセスグループと割り当てられたユーザーロールに基づいた、ヘッドエンドデバイスへの書き込みアクセス権が必要です。BWoD 管理ユーザーのみが BWoD 構成設定を変更できます。『Cisco Crosswork Network Controller Administration Guide』を参照してください。
- 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。
- BWoD は、予期しないエラーが発生した場合、ネットワークの中断を回避するために BWoD 自体を無効化します。
- Optimization Engine の再起動またはトポロジサービスからのトポロジの再構築が原因で Optimization Engine モデルが使用できなくなると、BWoD は一時的に動作を停止します。この期間中の BWoD への要求は拒否されます。モデルが使用可能になり、BWoD が Optimization Engine から 2 つのトラフィック更新を受信すると、BWoD は通常の動作を再開します。
- [ポリシー違反（Policy Violation）] 詳細フィールドが [厳格（Strict）] に設定されている場合、SR ポリシートラフィックのオプションは [要求された最大測定値（Max Measured Requested）] に設定する必要があります。
- 高可用性セットアップでのスイッチオーバー後、最後のクラスタデータ同期後に作成された BWoD ポリシーは管理できなくなり、孤立した TE ポリシーと見なされます。Crosswork Network Controller 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（[管理（Administration）] > [アラーム（Alarms）]）。API を使用して、孤立したポリシーをクリアして管理可能できるようにできます。詳細については、DevNet の API ドキュメントを参照してください。

PCC によって開始された BWoD SR-TE のポリシー

PCC によって開始された BWoD SR-TE のポリシーは、次のトラフィック エンジニアリング ポリシーです。

- デバイスが帯域幅要件をローカルに設定できるようにします。

- パス計算を外部 SR-PCE に委任します。
- 帯域幅の制約に基づいて、トラフィック エンジニアリング パスを継続的に最適化およびモニターします。

BWoD は、Crosswork Network Controller 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、SR-PCE BWoD REST API への永続的な接続を維持します。これは、帯域幅が制約された SR-TE ポリシー用の PCE として登録されます。帯域幅の制約を完全に満たすことができない場合、BWoDはベストエフォートパスを計算し、それに応じてイベントを発行します。BWoDは、ネットワーク全体の帯域幅の保証を維持するためのパスのモニターと再最適化も行います。

PCC によって開始された BWoD SR-TE のポリシーの動作

process_summary

このプロセスに関与する主要なコンポーネントは次のとおりです。

- **パス計算クライアント（PCC）**：BWoD SR-TE ポリシーを設定して開始し、パス計算を SR-PCE に委任します。
- **SR パス計算要素（SR-PCE）**：PCC から委任されたポリシーを受信し、帯域幅要件を調整し、BWoD 機能と対話します。
- **BWoD モジュール**：帯域幅の制約を満たすための制約ベースのパス計算を実行し、セグメントリストを返し、必要に応じてポリシーステータスを更新します。

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。

process_workflow

図 *47 : PCC* によって開始された *BWoD SR-TE* のポリシー

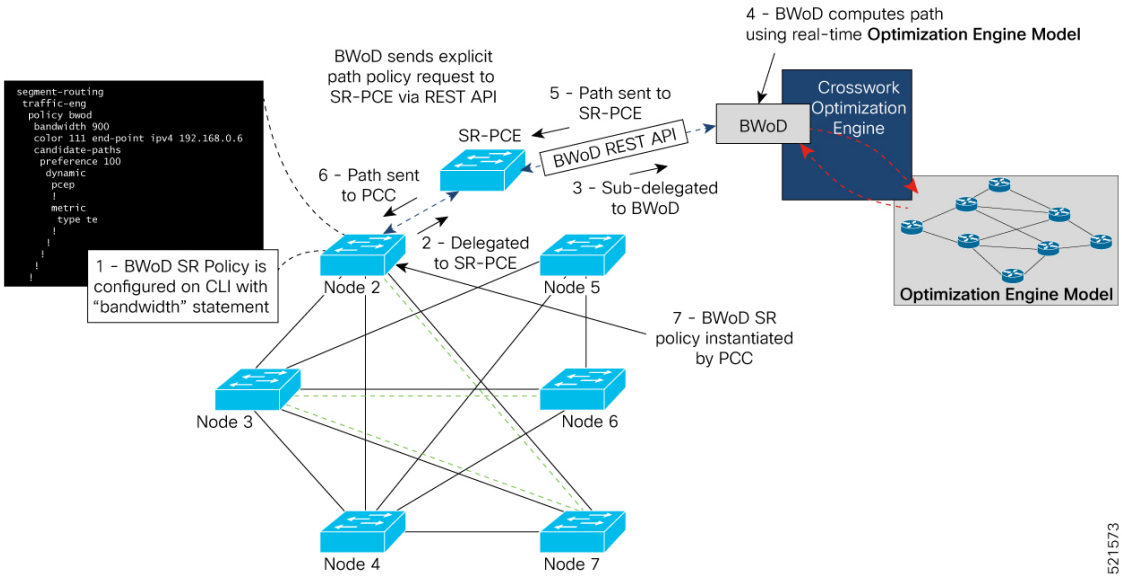


表 *6 : PCC* によって開始された *BWoD SR-TE* のポリシー

引き出し線番号	ワークフロー

1	ユーザーは CLI を使用して PCC で BWoD SR-TE ポリシーを設定し、帯域幅、エンドポイント、候補パス、および制約事項を指定します。次に例を示します。
	`segment-routing`
	`  traffic-eng`
	`  policy bwod`
	`  bandwidth 900`
	`  color 100`
	`  end-point ipv4 1.1.1.2`
	`  candidate-paths`
	`  preference 100`
	`  dynamic`
	`  pcep`
	`  !`
	`  metric`
	`  type te`
	`  !`
	`  !`
	`  constraints`
	`  affinity`
	`  exclude-any`
	`  name RED`
	`  !`
	`  !`
	`  !`
	`!`

引き出し線番号	ワークフロー
2	設定がコミットされると、PCC はパスの計算を SR-PCE に委任します。
3,4	SR-PCE は、要求された帯域幅の制約を満たすパスを計算しようとする BWoD にポリシーを委任します。
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

Before you begin

CSM と BWoD の両方を同時に有効にすることはできません。CSM が有効になっている場合は、BWoD を有効にする前に CSM を無効にする必要があります。

（注） 関連する機能パック（BWoD または CSM）を無効にする前に、ネットワークからそれぞれのポリシーを削除することを推奨します。ポリシーが無効な機能パックに残っている場合、新しいポリシー委任で問題が発生し、処理時間が長くなる可能性があります。

オンデマンドで帯域幅を設定し、BWoD SR ポリシーを作成するには、次の手順を実行します。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。

手順

ステップ 1 メインメニューから、**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）] > [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 必要なオプションを設定します。各フィールドの説明については、「BWoD 設定オプション」セクションを参照してください。

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、**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）]** > **[トラフィックエンジニアリング（Traffic Engineering）]** > **[SR-MPLS]** タブの順に選択し、[作成（Create）] > [PCEによって開始（PCE Init）] をクリックします。

ステップ 6 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 7 該当する場合は、[SIDアルゴリズム（SID Algorithm）] フィールドにフレキシブルアルゴリズムの制約を入力します。値はデバイスで定義されているフレキシブルアルゴリズムに対応し、128 ～ 255 の範囲が Cisco IOS XR によって適用されます。Crosswork Network Controller は、この SID を持つパスを見つけようとします。SID の制約のあるパスが見つからない場合、プロビジョニングされたポリシーは、条件が満たされるまで運用停止状態のままになります。

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 設定オプション

これらの表は、UI で使用可能な BWoD 設定オプションに関する情報を提供します。

- BWoD の基本設定
- BWoD の詳細設定

BWoD の基本オプション

表 7: 基本設定オプション

オプション	説明
Enable	BWoD 機能パックを有効または無効にします。
主な目的	ポリシーを最適化する際の主な目的を設定します。 • [使用可能な帯域幅の最大化（Maximize available bandwidth）]：ネットワーク全体で使用可能な帯域幅を最大化する SR ポリシーパスを計算します。この設定は、一般に、パスが長くなる可能性があっても使用可能なネットワークキャパシティを最大化しようとします。 • [メトリックの最小化（Metric minimization）]：選択したメトリックを最小化する SR ポリシーパスを計算します。通常、この設定ではメトリックタイプに対して使用可能なパスが最短になります。

オプション	説明
リンク使用率	輻輳の制約（パーセンテージ）を設定します。委任されたポリシーのパスを検索する場合、[オンデマンド帯域幅（Bandwidth on Demand）]により、この使用率しきい値を超える可能性のあるパスを回避し、トラフィックが輻輳リンクを通過しないようにします。さらに、インターフェイスがこの値を超えると、システムは最適化をトリガーしてトラフィックを再配布し、輻輳を緩和します。
再最適化間隔（Re-optimization interval）（秒）	ネットワーク条件が変更された場合にパスを再最適化できるまでの最小時間（秒単位）を設定します。これはカウントダウンタイマーとして機能します。BWoDポリシーは、再最適化を許可する前に、この期間が経過するまで待機します。
メトリック再最適化時間（Metric re-optimization time）	メトリック改善のためにパスを再最適化できるようになるまでの時間（秒単位）を設定します。帯域幅の要件が満たされていても、より優れたIGPまたはTEパスが使用可能な場合、BWoDはこのタイマーの期限が切れるまで待機してから再最適化します。これにより、頻繁なパス変更や不要な再最適化を防ぐことができます。

BWoD の詳細オプション

表 *8*：詳細設定オプション

オプション	説明
SR ポリシートラフィック（SR policy traffic）	各ポリシーの帯域幅の最適化を計算する方法を決定します。 • [測定結果（Measured）]：BWoD でプロビジョニングされた SR ポリシーの現在測定済みトラフィックを最適化計算に使用します。 • [要求された最大測定値（Max measured requested）]：BWoD でプロビジョニングされた SR ポリシーで現在測定されたトラフィックと、最適化計算用に要求された帯域幅の量との間の最大値を使用します。
スロットルの更新（Update throttle）（秒）	更新間で待機する時間（秒単位）を設定します。スロットルを無効にするには、0 に設定します。

オプション	説明
オプティマイザイベントしきい値（Optimizer event threshold）（秒）	オプティマイザが指定された時間（秒単位）よりも長く実行された場合、UI にアラートを送信します。 （注） 大規模環境では、オプティマイザの実行がデフォルトの実行時間制限（60秒）を超える場合があります。内部テストにおいて、ポリシーが 100 個単位でプロビジョニングされる展開では、[オプティマイザイベントしきい値（Optimizer event threshold）] を 240 秒に設定し、[オプティマイザ実行時間制限（Optimizer run time limit）] を 300 秒に設定することは効果がありました。1,000 以上のポリシーが展開される環境では、これらの値をさらに増やす必要がある場合があります。最適なパフォーマンスを確保するには、展開の規模に基づいてこれらのパラメータを調整します。
オプティマイザ実行時間制限（Optimizer run time limit）（秒）	BWoD オプティマイザの最大許容実行時間（秒単位）を設定します。 （注） 大規模環境では、オプティマイザの実行がデフォルトの実行時間制限（60秒）を超える場合があります。内部テストにおいて、ポリシーが 100 個単位でプロビジョニングされる展開では、[オプティマイザイベントしきい値（Optimizer event threshold）] を 240 秒に設定し、[オプティマイザ実行時間制限（Optimizer run time limit）] を 300 秒に設定することは効果がありました。1,000 以上のポリシーが展開される環境では、これらの値をさらに増やす必要がある場合があります。最適なパフォーマンスを確保するには、展開の規模に基づいてこれらのパラメータを調整します。
ポリシー違反（Policy violations）	新しいポリシーがプロビジョニングされてポリシー違反が検出されたときに、BWoD がどのように応答するかを決定します。
厳密なSIDを優先（Prefer strict SIDs）	有効にすると、セグメントリストを導出するときに厳密な SID が優先されます。LCM との互換性を保つために必要です。
デバッグオプティマイザ（Debug optimizer）	Crosswork Network Controller ファイルシステムへのオプティマイザ プラン ファイルのログ記録を有効にします。保存されるファイルの数は、[デバッグオプティマイザ最大計画ファイル（Debug opt max plan files）] 設定によって制限されます。

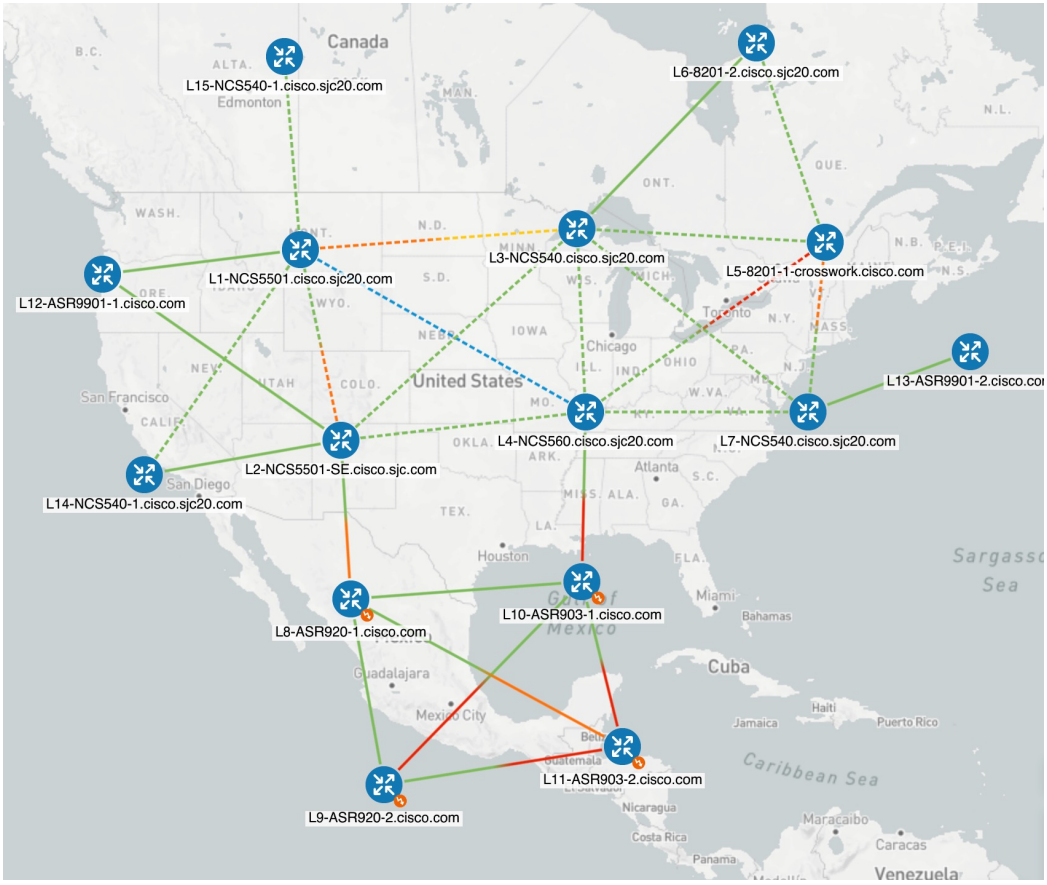
インテントベースの帯域幅の要件を維持するための SR-TE ポリシーのプロビジョニングの例

この例では、次の内容を示します。

- オンデマンド帯域幅（BWoD）を有効にして設定する方法
- BWoD ポリシーの作成方法
- BWoD によるパスの計算方法
- ポリシー違反オプションが Loose または Strict に設定されている場合に、BWoD が新しいポリシーを計算する方法。

この例では、ネットワーク使用率の上限を 80% にしながら、同じヘッドエンド（L1-NCS5501.cisco.sjc20.com）とエンドポイント（L5-8201-1-crosswork.cisco.com）を使用して、異なる帯域幅（700 Mbps と 1000 Mbps）で 3 つの BWoD ポリシーが作成されます。すべてのインターフェイスのキャパシティは **1 Gbps** です。

図 *48 :* 初期 *BWoD* トポロジ



手順

ステップ 1 BWoD を有効にして設定します。

（注）

CSM と BWoD の両方を同時に有効にすることはできません。CSM が有効になっている場合は、BWoD を有効にする前に CSM を無効にする必要があります。関連する機能パック（BWoD または CSM）を無効にする前に、ネットワークからそれぞれのポリシーを削除することを推奨します。ポリシーが無効な機能パックに残っている場合、新しいポリシー委任で問題が発生し、処理時間が長くなる可能性があります。

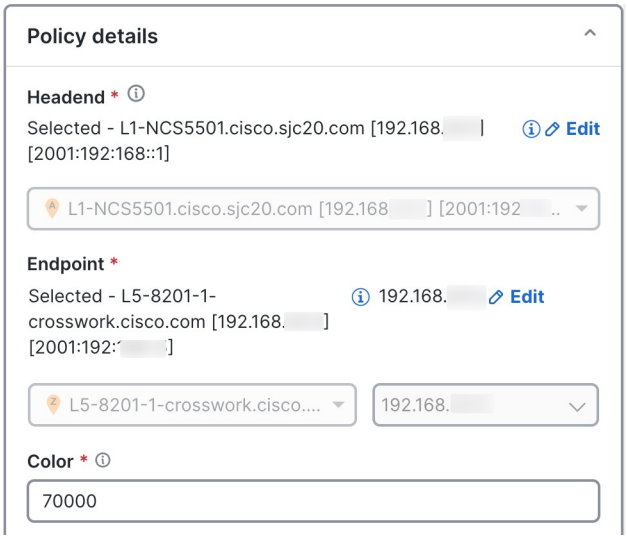
a) メインメニューから、**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）]** > **[オンデマンド帯域幅（Bandwidth on Demand）]** > **[設定（Configuration）]** を選択します。
b) [有効化（Enable）] を [はい（True）] に設定し、[リンク使用率（Link utilization）] フィールドに 80 と入力し、[詳細設定（Advance）] > [ポリシー違反（Policy Violations）] が [緩やか（Loose）] に設定されていることを確認します。他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 最初の PCE 開始 BWoD SR-TE ポリシーを作成します。

a) メインメニューから、**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）]** > **[トラフィックエンジニアリング（Traffic Engineering）]** > **[SR-MPLS]** タブの順に選択し、[作成（Create）] > [PCEによって開始（PCE Init）] をクリックします。
b) 必要なポリシーの詳細を入力します。この例では、次の値を使用してポリシーを作成します。

- ヘッドエンド：**L1-NCS5501.cisco.sjc20.com**
- エンドポイント：**L5-8201-1-crosswork.cisco.com**
- 色：**70000**

図 *49*：ポリシーの詳細

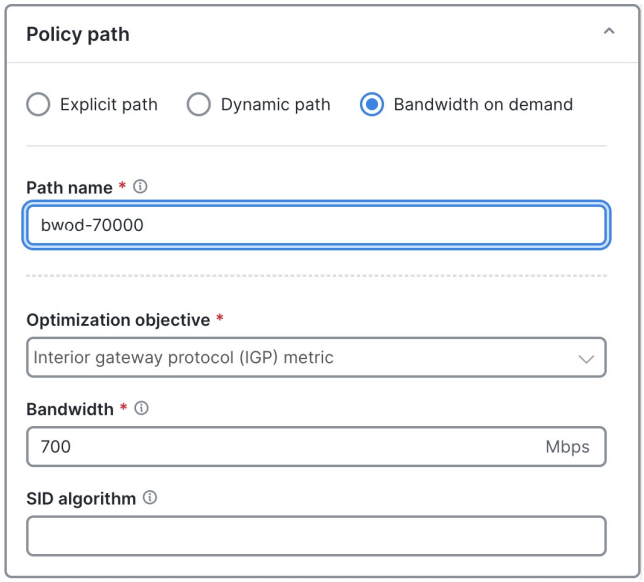


c) [ポリシーパス（Policy path）] 領域で、[オンデマンド帯域幅（Bandwidth on demand）] をクリックし、必要なポリシーパスの詳細を入力します。この例では、次の値を使用します。

- パス名：**bwod-70000**
- 最適化の目標：**内部ゲートウェイプロトコル（IGP）メトリック**

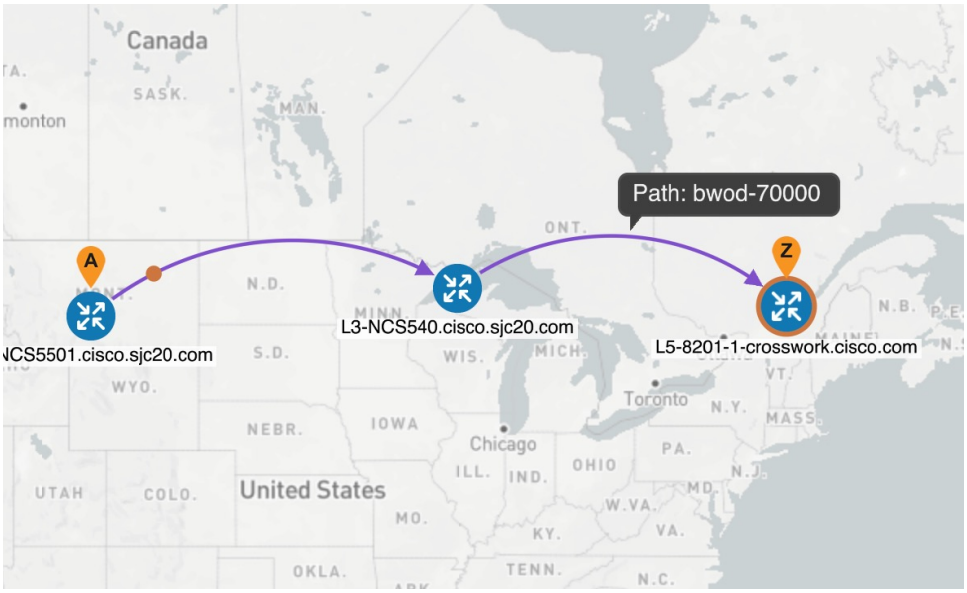
- 帯域幅：**7000 Mbps**

図 *50* : ポリシーパスの詳細



d) [プレビュー（Preview）] をクリックします。BWoD では、別の BWoD ポリシーによって予約されている現在のインターフェイス使用率のみが考慮されます。それ以外の場合、BWoD は計算でインターフェイスのキャパシティのみを考慮します。この例では、すべてのインターフェイスのキャパシティが 1 Gbps です。既存の BWoD ポリシーがないため、BWoD はすべてのノードのキャパシティを考慮し、最短ルートを選択します。

図 *51* : 最初の *BWoD* ポリシー（*bwod-70000*）



e) 提案された BWoD 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、**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）]** > **[トラフィックエンジニアリング（Traffic Engineering）]** > **[SR-MPLS]**の順に選択します。

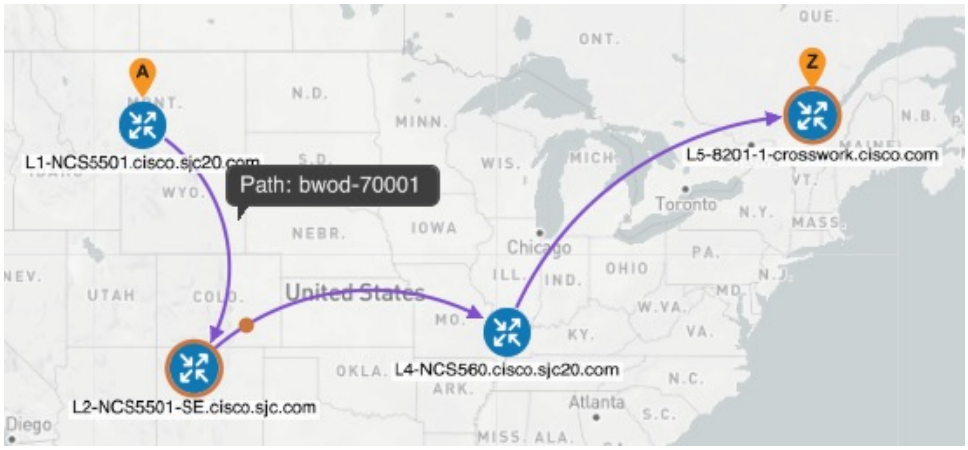
b) 新しい BWoD SR-TE ポリシーを選択し、SR ポリシーの詳細を表示します（[詳細の表示（View details）] をクリックして選択します）。

ステップ 4 2 番目の BWoD ポリシーを作成します。この例では、次の値を使用します。

- ヘッドエンド：**L1-NCS5501.cisco.sjc20.com**
- エンドポイント：**L5-8201-1-crosswork.cisco.com**
- 色：**70001**
- パス名：**bwod-70001**
- 最適化の目標：**内部ゲートウェイプロトコル（IGP）メトリック**
- 帯域幅：**700 Mbps**

BWoD は、既存の BWoD ポリシー（bwod-70000）とその帯域幅要件をインターフェイス キャパシティの計算で考慮します。したがって、bwod-70001 ポリシー用の新しいパスが作成されます。

図 *52 :* 新しい *bwod-70001* ポリシー



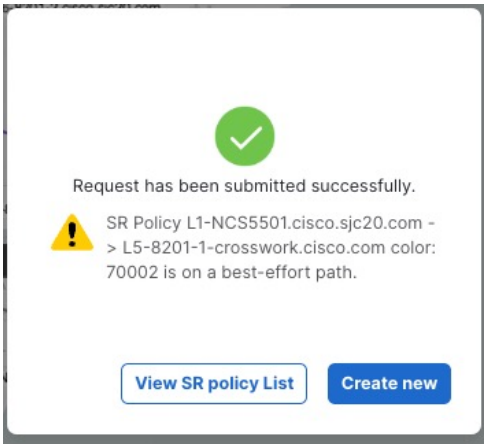
ステップ 5 3 番目の BWoD ポリシーを作成します。この例では、次の値を使用します。

- ヘッドエンド：**L1-NCS5501.cisco.sjc20.com**
- エンドポイント：**L5-8201-1-crosswork.cisco.com**
- 色：**70002**
- パス名：**bwod-70002**
- 最適化の目標：**内部ゲートウェイプロトコル（IGP）メトリック**

- 帯域幅：**1000 Mbps**

BWoD では以前のすべての BWoD ポリシー要件が考慮され、BWoD ポリシー違反オプションが [緩やか（Loose）] に設定されているため、BWoD は bwod-70002 ポリシーのベストエフォートパスを作成します。新しいポリシーをプロビジョニングすると、次のメッセージが表示されます。

図 *53* : ベストエフォートメッセージ



bwod-7000 および bwod-70001 の既存のパスは、新しい bwod-70002 ポリシーに対応するために移動されることに注意してください。

図 *54* : *Loose* オプションを使用した *BWoD* ポリシー

ステップ 6 BWoDポリシー違反オプションを、[厳格（Strict）] に変更します（**[サービスとトラフィックエンジニアリング（Services & Traffic Engineering）] > [オンデマンド帯域幅（Bandwidth on Demand）] > [設定（Configuration）] > [詳細設定（Advanced）]**）。

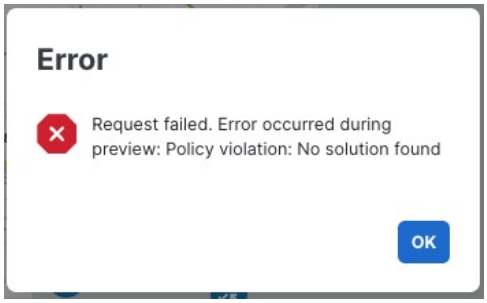
ステップ 7 4 番目の BWoD ポリシーを作成します。この例では、次の値を使用します。

- ヘッドエンド：**L1-NCS5501.cisco.sjc20.com**

- エンドポイント：**L5-8201-1-crosswork.cisco.com**
- 色：**70003**
- パス名：**bwod-70003**
- 最適化の目標：**内部ゲートウェイプロトコル（IGP）メトリック**
- 帯域幅：**1000 Mbps**

BWoD ポリシー違反オプションが [厳格（Strict）] に設定されているため、BWoD は既存の BWoD ポリシーを上書きできず、追加の 1000 Mbps ポリシーを要求すると、「ソリューションが見つかりません（No solution found）」というメッセージが表示されます。

図 *55 :* ソリューションが見つかりません



BWoD エラーメッセージ

次に、BWoD の最も一般的ないくつかのエラー状態とその考えられる修正処置を示します。

表 *9*：エラーイベントメッセージ

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

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。