CHAPTER 7

MPLS トラフィック エンジニアリング サービスの管理

この章には、さまざまな機能、GUI、およびさまざまなトラフィック エンジニアリング管理タスクを実行するために必要な手順を含む『Cisco Prime Provisioning Traffic Engineering Management』（TEM）製品の詳細な説明が記載されています。

この章の内容は、次のとおりです。

スタートアップ

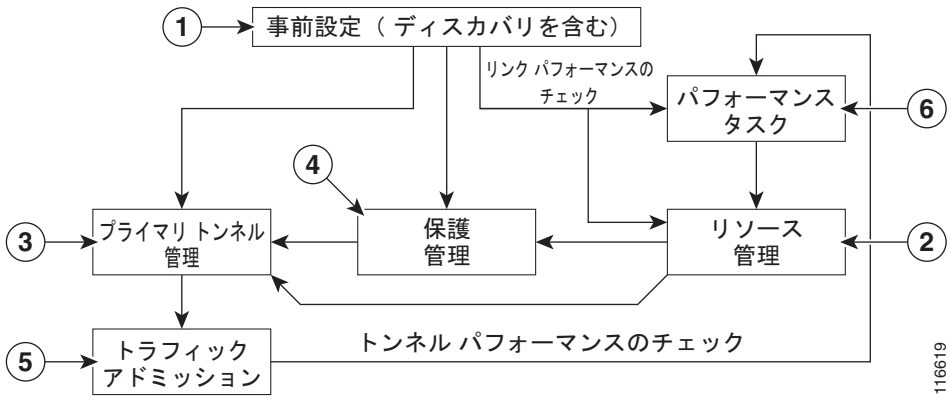
ここでは、Prime Provisioning のインストール手順について説明します。Cisco Prime Provisioning（Prime Provisioning）の一般的なインストール手順は、*『Cisco Prime Provisioning 6.3 Installation Guide』* で説明しています。

内容は次のとおりです。

プロセスの概要

TEM の主要なコンポーネントとフローは、図 7-1 に示されています。

図 7-1　TEM の主要なプロセス フロー

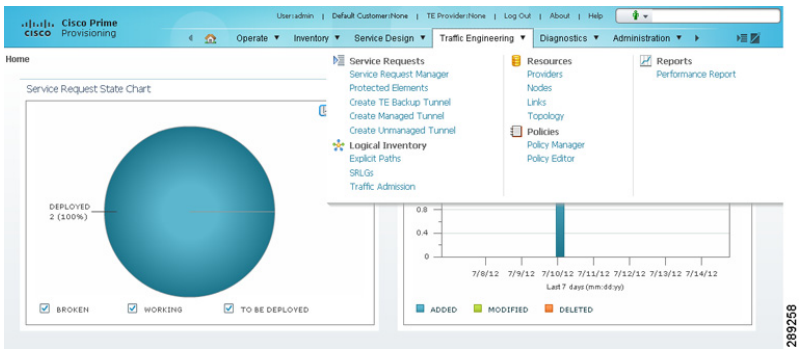


この図には、次のコンポーネントが含まれています。

1. 事前設定：システムで TE ネットワーク情報を収集してから（TE ディスカバリ）、選択したネットワークに TE 設定を導入できるようにする主要パラメータを設定します。（「スタートアップ」（P.7-1）を参照）
2. リソース管理：TE インターフェイスの特定のプロパティを調整してトンネル配置を最適化します。（「TE リソース管理」（P.7-21）を参照）
3. プライマリ トンネル管理：管理対象外（「基本的なトンネル管理」（P.7-28）を参照）または管理対象のプライマリ トンネルを作成および管理します。（「基本的なトンネル管理」（P.7-28）または「高度なプライマリ トンネル管理」（P.7-46）を参照）
4. 保護管理：ネットワークの選択された要素（リンク、ルータ、または SRLG）を障害から保護します。（「高度なプライマリ トンネル管理」（P.7-46）を参照）
5. トラフィック アドミッション：トラフィックをトラフィック エンジニアリングされたトンネルに割り当てます。（「TE トラフィック アドミッション」（P.7-68）を参照）
6. パフォーマンス タスク：簡易ネットワーク管理プロトコル（SNMP）を使用してインターフェイスおよびトンネルの帯域使用率を計算します。（「管理機能」（P.7-72）を参照）

Prime Provisioning ユーザ インターフェイスの [Traffic Engineering] メニューのオプションを図 7-2 に示します。

図 7-2　[Traffic Engineering] メニューのオプション



前提条件と制限事項

現在のリリースの Prime Provisioning には、ここで説明する一定の前提条件および制限事項があります。

一般的なシステムの推奨事項については、*『Cisco Prime Provisioning 6.3 Installation Guide』* を参照してください。

一般的な制限事項

Prime Provisioning の現在のリリースには、次の制限事項があります。

- Prime Provisioning の同時実行ユーザは現在の実装の計画部分でサポートされますが（「複数の同時実行ユーザ」（P.7-118）の項を参照）、ブラウザ セッション属性の制限のため、同じマシンで複数のブラウザを使用することは推奨されません。
- Java アプリケーションおよびアプレットを起動するには、クライアント コンピュータに JRE バージョン 1.6.0_07 以上をインストールする必要があります。これは、Java のコントロール パネルから行えます。Java をまだインストールしていない場合は、[Topology Tool] ページにあるリンクを使用して、Prime Provisioning にバンドルされているバージョンをインストールできます。
- ISC 4.1 リリースよりも前のリポジトリを使用していて、4.1 以降のリポジトリにアップグレードした場合は、サービス要求を展開する前に TE 検出タスクを実行してデバイスからソフトウェア バージョン情報を収集する必要があります。
- 競合を回避するために他のサービス要求を発行する前に、発行されたサービス要求の展開を完了します。この詳細は、トンネル プロビジョニングの項で説明されています。

機能固有の注意事項および制限事項

Prime Provisioning には、次のような機能固有の前提条件と制限事項があります。

- 一部の機能は、特定のライセンスがある場合に限り使用できます。また、ライセンスで提供されるノードの数により、ネットワークのサイズが制限されます。詳細については、「トラフィック エンジニアリング管理の概念」（P.7-115）を参照してください。
- TE ディスカバリ タスクに関連する固有の要件は多数あります。これらについては、「TE ディスカバリの前提条件と制約事項」（P.7-13）に記載されています。
- Prime Provisioning は、単一の OSPF エリアまたは IS-IS レベルを管理します。Prime Provisioning は複数の OSPF エリアもサポートしますが、エリア間のトンネルを検出しません。各 OSPF エリアは単一の TE プロバイダーマッピングされ、エリアごとに別々に検出されます。
- Prime Provisioning は、ポイントツーポイント リンクを使用した MPLS-TE トポロジのみをサポートします。

シスコ デバイス以外のデバイスおよび TEM

Prime Provisioning では、シスコ デバイス以外のデバイスを管理せず、Prime Provisioning は、そのようなデバイスのプロビジョニングに使用できません。

ただし、Prime Provisioning では、シスコ デバイス以外のデバイスを検出してリポジトリに格納します。これらのデバイスを通過するトンネルを設定でき、消費される帯域幅を算入できますが、デバイスのこれ以外の側面は Prime Provisioning によって管理されません。シスコ デバイス以外のデバイスを始点とする TE トンネルは検出されません。

Prime Provisioning GUI のさまざまな部分のさまざまな属性のソートを実行できます。ただし、シスコ デバイス以外のデバイスに対して追加されたサポートのため、[TE Nodes List] ウィンドウの [Device Name] と [MPLS TE ID] に対してソートを実行できません。

サポートされるプラットフォーム

サポートされるデバイスと IOS プラットフォームについては、*『Cisco Prime Provisioning 6.3 Installation Guide』*を参照してください。

エラー メッセージ

Prime Provisioning で TE 計画ツールを使用するときに呼び出される違反と警告は、「警告および違反」（P.7-102）に記載されています。

Prime Provisioning で展開を実行したときに、次のような Elixir 警告メッセージが表示されることがあります。

```
WARNING Elixir.ServiceBlade Unable to load support matrix for the platform or platform
family. The default support matrix is loaded instead for role: TunnelHead.
WARNING Elixir.ConfigManager Attribute - lockdown of Command - Tunnel_PathOption can NOT
be retrieved from the input SR - SKIPPING.
```

ただし、展開は正常に行われ、警告メッセージは無視しても安全です。

事前設定処理の概要

事前設定処理により、システムが TE ネットワーク情報を収集し、選択されたネットワークで TE 設定を展開することを可能にする主要なパラメータが設定されます。

図 7-3 で強調表示されたボックスは、事前設定処理が Prime Provisioning のどこで行われるかを示しています。

図 7-3　Prime Provisioning プロセス図：事前設定

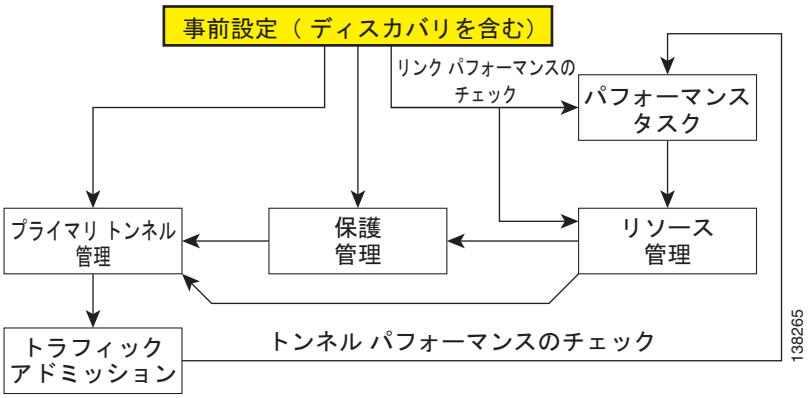
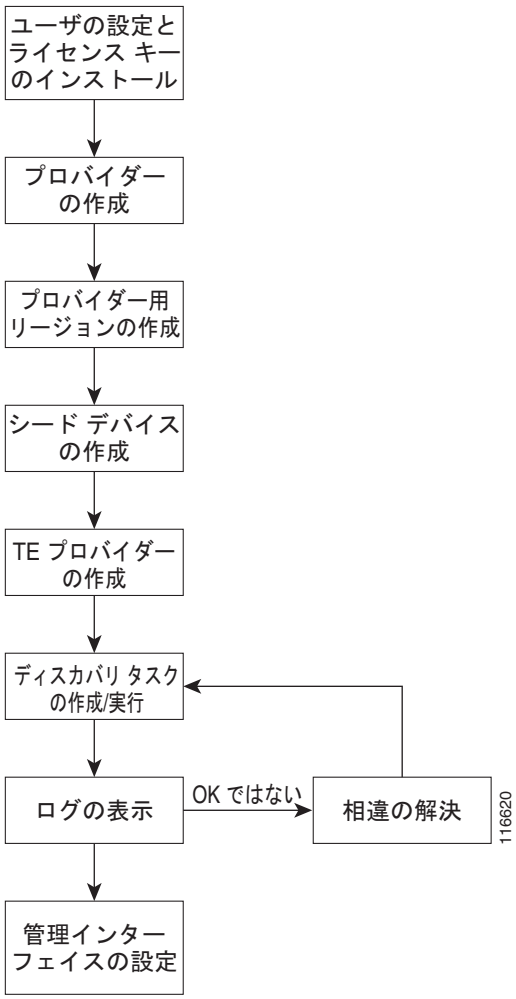


図 7-4 には、事前設定処理の異なる手順が示されています。

図 7-4　事前設定処理



事前設定処理を開始する前に、デバイスの TE ID として使用される IP アドレスに、管理ステーションから正常にアクセスできることを確認することにより、ネットワーク デバイスで MPLS-TE をイネーブルにする必要があります（このステップは TEM によってサポートされていません）。

事前設定処理は、次の手順から構成されます。

1. **新規ユーザの設定およびライセンス キーのインストール**：Prime Provisioning の TEM 機能を実行するには、新規ユーザの作成とライセンス キーのインストールが必要です。これらのキーにより、Prime Provisioning を使用して TE トンネルとリソースを表示および管理できるようになります。（「TEM のセットアップおよびインストール」（P.7-7）を参照）
2. **プロバイダーの作成**：プロバイダーは、複数のオペレータが Prime Provisioning で同時に作業を行えるように設計された概念です（各プロバイダーは異なるネットワークで作業します）。したがって、各プロバイダーを定義してさらにシステムで作業するために参照オペレータとして使用する必要があります （プロバイダーを作成するには、「プロバイダー」（P.2-15）を参照してください）。
3. **プロバイダーのリージョンの作成**：単一のプロバイダーは複数のネットワークを使用できるため、リージョンが重要になります。そのような環境に対応するために、リージョンはさらなる細分化のレベルとして使用されます。（リージョンを作成するには、「プロバイダー リージョン」（P.2-17）を参照してください）。

4. **シード デバイスの作成**：この IOS または IOS XR デバイスは、TE 検出のためのシード ルータになります。ネットワーク ディスカバリ プロセスでは、MPLS TE ネットワーク トポロジを検出するための初期通信ポイントとしてシード ルータを使用します（シード ルータを作成するには、「デバイス」（P.2-1）を参照してください）。
5. **TE プロバイダーの作成**：ネットワークで MPLS TE をサポートしているプロバイダーは、TE プロバイダーとして定義できます。TE ネットワークを管理できるようにするには、TE プロバイダーを作成する必要があります。特定のネットワークに関連付けられたすべての TE 関連データは、一意な TE プロバイダーの下に格納されます。プロバイダーとリージョンは、TE プロバイダーを一意に定義します（「TE プロバイダーの作成」（P.7-8）を参照）。
6. **TE ディスカバリ タスクの実行**：プライマリ トンネルとバックアップ トンネルを作成するために、リポジトリに入力する特定の TE プロバイダーの TE ネットワークを検出します。（「TE ネットワーク検出」（P.7-11）を参照）。
7. **管理インターフェイスの設定**：検出されたデバイスの管理インターフェイスを設定するか、検出されたすべてのデバイスに対する解決方法でサーバ ホスト ファイルを更新します。TE ネットワーク内のデバイスにホスト名でアクセスできない場合にだけ、このステップが必要です（「管理インターフェイスの設定」（P.7-20）を参照）。

（注） シード ルータと通信するために Telnet が選択された場合は、他のネットワーク デバイスにも Telnet を使用する必要があります。同様に、シード ルータに対して SSH が選択された場合、SSH は他のすべてのデバイスに使用する必要があります。

TEM のセットアップおよびインストール

Prime Provisioning を設定する前に、Prime Provisioning ソフトウェアをインストールする必要があります。これを行うには、*『Cisco Prime Provisioning 6.3 Installation Guide』* を参照してください。

新規 Prime Provisioning ユーザを設定する場合は、TE ロールを持つユーザを 1 つ以上作成する必要があります。ステップバイステップの説明については、*『Cisco Prime Provisioning 6.3 Administration Guide』* を参照してください。

ライセンスのインストールに必要な Prime Provisioning ライセンス オプションと手順を含むライセンス情報については、*『Cisco Prime Provisioning 6.3 Administration Guide』* を参照してください。

DCPL プロパティの編集（任意）

Prime Provisioning Dynamic Component Properties Library（DCPL）には、GUI からアクセスできるさまざまなプロパティが含まれます。これらのプロパティの一部は変更できます。

警告 **影響を十分に理解していない限り、DCPL プロパティの変更を試みないでください。**

Prime Provisioning の GUI で、DCPL プロパティは [Administration] > [Hosts] にあります。特定のホストのチェックボックスをオンにして、[Config] ボタンをクリックします。

TEM に関する DCPL プロパティは、次のフォルダにあります。

- [Provisioning] > [Service] > [TE]
- TE

- TE Topology

TE プロバイダーの作成

TE 検出または TE データの操作を行う前に、TE プロバイダーを少なくとも 1 つ作成する必要があります。たとえば、OSPF エリアは TE プロバイダーとして割り当てることができます。これよりも前に、プロバイダーおよびプロバイダー用のリージョンが設定されている必要があります（「事前設定処理の概要」（P.7-4）を参照）。

検出されたルータの場所であるデフォルト リージョンとして、1 つのリージョンを割り当てることができます。これらのルータは、後に任意のリージョンに配置できます。詳細については、*『Cisco Prime Provisioning 6.3 Administration Guide』* の複数のホストの項を参照してください。

TE プロバイダーを作成するには、次のステップを実行します。

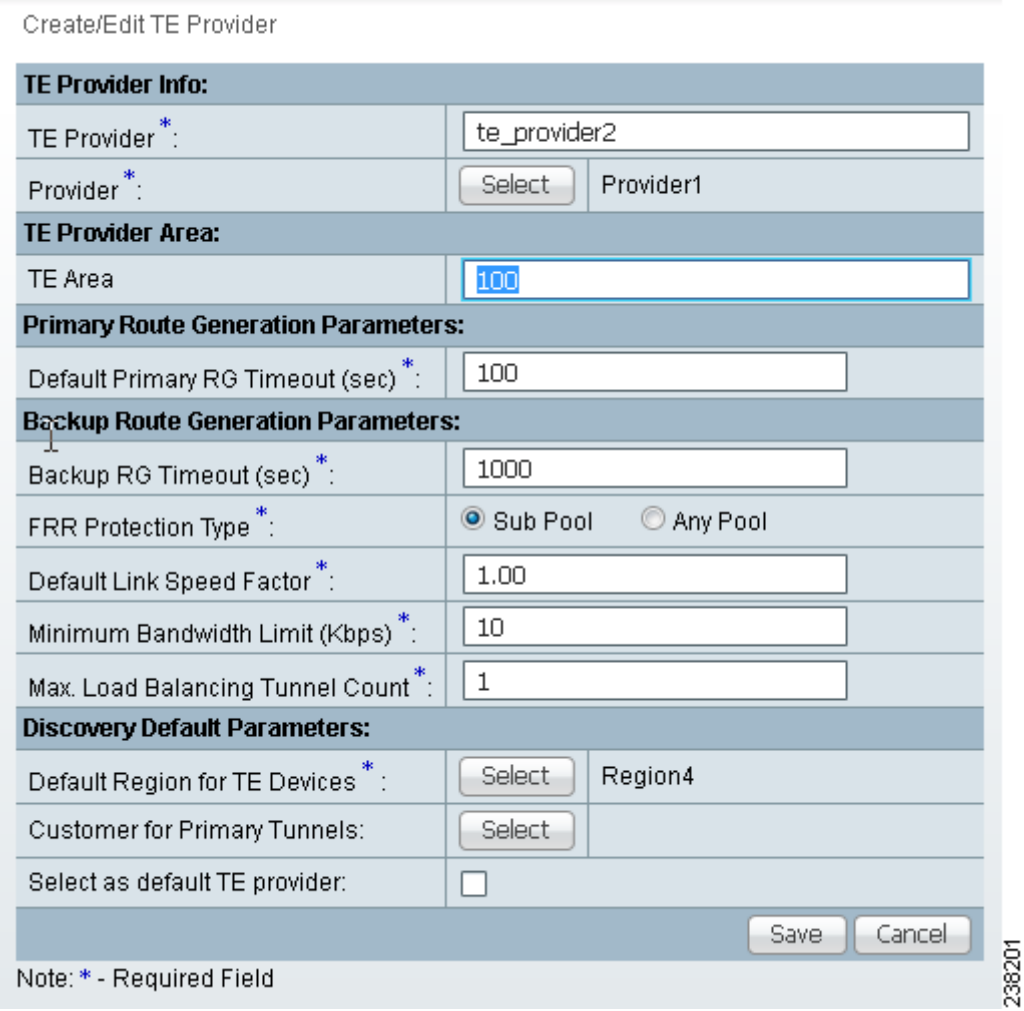
ステップ 1　[Traffic Engineering] > [Providers] を選択します。

[TE Providers] ウィンドウが表示されます。

ステップ 2　[Create] をクリックして TE をプロバイダーを作成します。

[Create/Edit TE Provider] 図 7-5 ウィンドウが表示されます。

図 7-5　Create/Edit TE Provider



[Create/Edit TE Provider] ウィンドウには、次のフィールドが含まれています。

- [TE Area]：TE プロバイダーに割り当てられた OSPF エリア。これは、0 ～ 4294967295 の正の整数または x.x.x.x 形式のドット表記アドレスにすることができます。ここで、x は 0 ～ 255 の間の数値です。
- [Default Primary RG Timeout]：プライマリ トンネルに対するデフォルトの計算タイムアウト。
- [Backup RG Timeout]：バックアップ トンネルの要素あたりの計算のタイムアウト（各保護対象要素に対して、タイマーは、Prime Provisioning が保護を試みる前にゼロにリセットされます）。
- [FRR Protection Type]：Fast Re-Route（FRR）保護タイプ。
  - [Sub Pool]：サブ プールのプライマリ トンネルだけを保護します。
  - [Any Pool]：サブ プールとグローバル プールの両方のプライマリ トンネルを保護します。

  プール タイプの定義については、「トラフィック エンジニアリング管理の概念」（P.7-115）で帯域幅プールの項を参照してください。

- [Default Link Speed Factor]：影響を受けるトンネルを移動するためにリンク速度に適用するデフォルト増倍係数。これは保護する必要があります。リンクの帯域幅は、リンク速度係数によって乗算され、リンクのために予約された RSVP 帯域幅（FRR 保護タイプによって、サブ プールまたはグローバル プール）が差し引かれます。算出された帯域幅は、FRR バックアップ トンネルに使用できます。

  リンク速度係数の解釈：

  1.0 よりも大きい（オーバーブッキング）：リンクよりも多くのバックアップ帯域幅を使用できます。

  1.0 よりも小さい（アンダーブッキング）：リンクよりも少ないバックアップ帯域幅を使用できます。

- [Minimum Bandwidth Limit]：バックアップ トンネルで許可される最小帯域幅。
- [Max. Load Balancing Tunnel Count]：保護対象要素を通じてフローを保護するために必要なバックアップ トンネルの最大数です。ここでは、フローは次のように定義されます。

  保護対象リンクには、2 つのフローがあります（トラフィックのフローが可能な方向ごとに 1 つ）ノードの場合、フローの数は特定のノードのネイバー ノードの数によって決まります。フローは、ネイバー ペアごとに 1 つです。したがって、3 台のネイバー、A、B、および C があるノードには、そのノードを通過する 6 つのフローがあります（A->B、A->C、B->A、B->C、C->A、C->B）

- [Default Region for TE Devices]：デフォルト プロバイダー リージョンは、TE ディスカバリによって、新しく検出されたデバイスに割り当てられます。デバイスがリポジトリにすでに存在し、リージョンが定義されている場合、TE ディスカバリでは、その設定が維持されます。TE ディスカバリ後に、デバイスのリージョンを変更できます。
- [Customer for Primary Tunnels]：プライマリ TE トンネルのカスタマーの名前。

ステップ 3　[TE Provider] フィールドに新規 TE プロバイダーの名前を入力します。

ステップ 4　この TE プロバイダーとしてプロバイダーを選択するには、[Provider] フィールドの隣の [Select] ボタンをクリックします。

[Select Provider] ウィンドウが表示されます。

ステップ 5　オプション ボタンを使用して必要なプロバイダーを選択するか、プロバイダー名に一致する検索基準でプロバイダーを検索し、[Find] をクリックします。

ステップ 6　[Select] をクリックして必要なプロバイダーを選択します。

[Select Provider] ウィンドウが閉じます。選択されたプロバイダー名が、[Provider] フィールドに表示されます。

ステップ 7　[TE Area] フィールドに、TE エリアとして使用する OSPF エリアの番号を指定します。

エリア ID では、ドット表記と 10 進表記の両方がサポートされます。

（注）　TE ディスカバリに使用されるシード ルータがエリア境界ルータでなく、検出時に自動的に読み込まれる場合は、[TE Area] フィールドを空にできます。

TE 検出に使用されるシード ルータに応じて、エリア ID を次のように設定する必要があります。

- **シード ルータが ABR である場合：**TE プロバイダーのエリア ID フィールドが ABR の 2 つ以上のエリアのどれを検出するかを示すよう設定する必要があります。
- **シード ルータが ABR でない場合：**空にします。

（注）　[TE Provider] にエリア ID を設定しなかった場合は、TE ディスカバリによって設定されます。エリア ID は、設定後に変更できません。

ステップ 8　プライマリおよびバックアップのルート生成パラメータを追加します。

FRR（Fast Re-Route）保護タイプがサブ プールと同じである場合、ツールにより生成されたバックアップ トンネルはサブ プール プライマリ トンネルのみを保護します。[Any Pool] の場合、ツールによって生成されるバックアップ トンネルでは、サブプールおよびグローバル プールの両方のプライマリ トンネルを保護します。

Fast Re-Route（FRR）保護プールの詳細については、「トラフィック エンジニアリング管理の概念」（P.7-115）で、帯域幅プールの項を参照してください。

ステップ 9　残りの必須フィールド（「*」とマークされたフィールド）と、必要に応じてオプション フィールドに値を入力します。

ステップ 10　必須の [Default Region for TE Devices] フィールドで、対応する [Select] ボタンをクリックします。

[Region for Create TE Provider] ウィンドウが表示されます。

ステップ 11　オプション ボタンを使用して必要なリージョンを選択します。

ステップ 12　[Select] をクリックして必要なデフォルト リージョンを選択します。

[Region for Create TE Provider] ウィンドウが閉じます。選択されたリージョン名が [Default Region for TE Devices] フィールドに表示されます。

ステップ 13　オプションの [Customer for Primary Tunnels] フィールドで、対応する [Select] ボタンをクリックします。

[Customer for Create TE Provider] ウィンドウが表示されます。

ステップ 14　必要な場合は、オプション ボタンを使用してカスタマーを選択するか、[Show Customers with Customer Name matching] フィールドにカスタマー検索基準を入力してカスタマーを検索し、[Find] をクリックします。

ステップ 15　[Select] をクリックして必要なカスタマーを選択します。

[Select Customer for Create TE Provider] ウィンドウが閉じます。選択されたカスタマー名が、[Create/Edit TE Provider] ウィンドウの [Customer for Primary Tunnels] フィールドに表示されます。

ステップ 16　[Save] をクリックします。

作成された TE プロバイダーは、[TE Provider] ウィンドウに表示され、TE 検出と他の TE 機能を実行するために使用できるようになります。

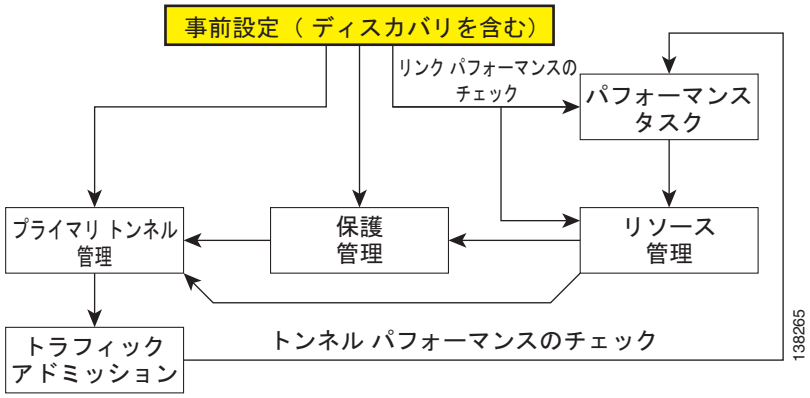
TE プロバイダーを切り替えるには、メニュー ツールバーの上の Prime Provisioning ウィンドウの上部に移動し（図 7-2）、[TE Provider] リンクをクリックします。

TE ネットワーク検出

事前設定処理を完了し、シード ルータの作成を終えれば、特定の TE プロバイダーの TE ネットワークを検出できます。これによって、ネットワーク トポロジがリポジトリに入力されます。また、管理インターフェイスの設定が必要になる場合があります。必要なステップについては、この項で説明します。

図 7-3 で強調表示されているボックスは、Prime Provisioning で行う事前設定のステップを示しています。

図 7-6　Prime Provisioning プロセス図：事前設定



TE 検出プロセスの目的は、TE トポロジ、TE トンネル、明示的パス、およびライブ ネットワークに存在するトンネルへのスタティック ルートをリポジトリに入力することです。

TE 検出プロセスでは、Telnet または SSH のいずれかを使用している MPLS TE ネットワーク トポロジを検出するためにシード デバイスを使用します。ネットワーク内のすべてのトラフィック エンジニアリング ルータは、TE ID を介してアクセス可能にする必要があります。

TE ディスカバリは、1 回または定期的に実行できるスケジュール設定可能なタスクです。リポジトリとネットワークの間の不一致は、ディスカバリ ログに報告されます。サービス状態の情報は、ラベル スイッチド パス（LSP）のログを記録し、サービス要求（SR）状態を更新することにより、段階的に更新されます。

ここでは、次の内容について説明します。

TE ディスカバリの前提条件と制約事項

次の前提条件は、主に TE 検出に適用されます。

一般的な Prime Provisioning の前提条件と制約事項については、「前提条件と制限事項」（P.7-3）を参照してください。

TE 検出の TE ルータへアクセス

TE ディスカバリ タスクを正常に実行するには、シード ルータに管理ステーションから直接アクセスできる必要があります。

すべての TE ルータは、Prime Fulfillment マシンから TE ルータ ID を介してアクセスできる必要があります。多くの場合、これはループバック IP アドレスですが、常にそうであるわけではありません。

Telnet/SSH では、『Cisco Prime Provisioning Traffic Engineering Management』（TEM）管理ステーションから各デバイスへの直接 Telnet/SSH アクセスが必要です。

シード ルータの設定時に Telnet または SSH を選択する方法の手順については、「事前設定処理の概要」（P.7-4）を参照してください。

（注） TE 検出の実行後、デバイスでの RSVP グレースフル リスタートを手動で再設定しないことを推奨します。これは、データベースとの同期に影響を与え、展開が失敗する可能性があります。この場合、新たに TE 検出を実行する必要があります。

大規模ネットワークでのメモリの不足

大規模ネットワーク（250 以上のデバイスまたは 5000 以上のトンネルなど）で TE ディスカバリを実行している場合、または OutOfMemoryException が発生した場合は、メモリ設定を変更することを推奨します。

これを行うには、次のステップを実行します。

ステップ 1　[Administration] > [Hosts] を選択します。

ステップ 2　ホストを選択し、[Config] ボタンをクリックします。

ステップ 3　[watchdog] > [server] > [worker] > [java] > [flags] を選択します。

ステップ 4　プロパティ文字列の最初の部分を変更します。たとえば、デフォルト値 **-Xmx512m** の代わりに **-Xmx1024m** に変更します。

これにより、**TE 検出**タスクのヒープ サイズが増加し、これにより、OutOfMemoryException の問題が解決します。

ステップ 5　**watchdog.server.worker.java.flags** プロパティを元の値に戻し、不要になったときにリソース使用率を減らします。

（注） または、**vpnsc.properties** ファイルの **watchdog.server.worker.java.flags** プロパティを編集することにより、同様にメモリの増加を実現することができます。

IOS XR およびイネーブル パスワード

IOS XR デバイスをシード デバイスとして使用している場合、IOS XR 自体はイネーブル パスワードを必要としませんが、イネーブル パスワードをデバイス レコードに設定する必要があります。このように、ネットワーク内の IOS デバイスは、イネーブル パスワードを必要としませんが、完全に検出することができます。

初期ディスカバリのシード デバイスとして機能する IOS XR デバイスを [Devices] タブ（[Inventory] > [Devices]）から作成する場合は、イネーブル パスワードを指定する必要はありません。TEM では、ログイン可能であり、必要なすべてのデータを取得できます。

ただし、同じネットワークに他の IOS デバイスがある場合、TEM はこれらのデバイスのイネーブル モードを開始できません。その結果、イネーブル モードを開始できないために TEM で収集できない関連データがあるという意味で、これらのデバイスのディスカバリは完全ではありません。これらの他の IOS ルータは、[Devices] ウィンドウでは [unknown] デバイスとして表示されます。

制限事項

同じ TE プロバイダーの同時 TE ディスカバリはサポートされていません。TE プロバイダーごとに、一度に 1 人のユーザのみが TE ディスカバリ タスクを実行できます。

TE 検出タスクの作成

タスク マネージャでは、次の 2 つのタイプの TE ディスカバリ タスクを実行できます。

- 「TE 増分ディスカバリ」（P.7-14）
- 「TE フル ディスカバリ」（P.7-15）

TE 増分ディスカバリ

比較的大きい OSPF エリアで、この再ディスカバリ プロセスは、完了までに長い時間がかかる場合があります。

TE 増分ディスカバリでは、ディスカバリ タスクは、新しいデバイスまたはリンクの追加など、ネットワークで変更が発生するたびに漸次的に実行されます。このため、TE フル ディスカバリよりも、メモリ オーバーヘッドがはるかに小さくなります。

TE ネットワーク上で TE 検出タスクを作成するには、次のステップを実行します。

ステップ 1　[Operate] > [Task Manager] を選択します。

[Task Manager] ウィンドウが表示されます。

ステップ 2　[Create] > [TE Incremental Discovery] を選択します。

[Task Creation] ウィザードが開きます。

ステップ 3　（任意）[Name] および/または [Description] フィールドを変更し、[Next] をクリックします。

[TE Provider] ウィンドウが表示されます。

ステップ 4　TE プロバイダーを選択し、[Next] をクリックします。

[Device/Link Discovery Information] ウィンドウが表示されます。

次のいずれかの操作を実行できます。

- デバイス ディスカバリ：ネットワークに追加された新しいデバイスは、デバイス ディスカバリを使用して検出できます。デバイス ディスカバリでは、シスコ以外のデバイス（ある場合）は、リストから除外されます。

  デバイスは、[Select] ボタンをクリックして選択できます（インベントリに追加されたデバイスのリストが表示されます）。

  ここで、検出する必要があるデバイスは、その管理 IP アドレスとともに追加する必要があるという前提条件があります。デバイスのクレデンシャルは、リポジトリにすでに入力されている他のデバイスのクレデンシャルと同じである必要はありません。デバイスは、TE プロバイダーと同じ OSPF エリアに含まれる場合に限り、検出に成功します。

- リンク ディスカバリ：ネットワークに追加された新しいリンクは、リンク ディスカバリを使用して検出できます。明示的パス、リンクを通過するプライマリおよびバックアップ トンネルも検出されます。

  すでに TE ノードである [End Device A] および [End Device B] をデバイスのリストから選択できます。[Interface A] および [Interface B] を指定する必要があります。

ステップ 5　ネットワークを検出するためのシード デバイスを選択し、[Next] をクリックします。

[Task Schedules] ウィンドウが表示されます。

ステップ 6　次の 2 つの方法のいずれかでタスク スケジュールを作成します。

- すぐに実行するタスクをスケジュールする場合は、[Now] をクリックします。この場合、スケジュール情報が [Task Schedules] のリストに自動的に入力されます。
- このタスクのスケジューラを作成するには、[Create] をクリックします。この場合、[Task Schedule] ウィンドウが表示されます。

ステップ 7　[Task Schedule] ウィンドウで、タスクを実行する時間と頻度を定義するための選択を行います。

（注）　デフォルト設定では、単一の **TE ディスカバリ タスク**をすぐに実行します（[Now]）。

ステップ 8　[OK] をクリックします。

この結果、スケジュールされたタスクが [Task Schedules] テーブルに表示されます。

ステップ 9　[Next] をクリックします。

スケジュールされたタスクの概要が表示されます。

ステップ 10　[Finish] をクリックします。

[Tasks] ウィンドウの作成済みタスクのリストにタスクが追加されます。

TE フル ディスカバリ

TE フル ディスカバリでは、ディスカバリ タスクは、すべてのデバイスが検出されるまで停止せずに動作します。

TE ネットワーク上で TE 検出タスクを作成するには、次のステップを実行します。

ステップ 1　[Operate] > [Task Manager] を選択します。

[Task Manager] ウィンドウが表示されます。

ステップ 2　[Create] > [TE Full Discovery] を選択し、新しいタスクを作成します。

[Create Task] ウィンドウが表示されます。

ステップ 3　（任意）[Name] および/または [Description] フィールドを変更し、[Next] をクリックします。

[Select TE Provider] ウィンドウが表示されます。

ステップ 4　TE プロバイダーを選択し、[Next] をクリックします。

[Select Seed Device] ウィンドウが表示されます。シスコ以外のデバイス（ある場合）は、リストから除外されます。

ステップ 5　ネットワークを検出するためのシード デバイスを選択し、[Next] をクリックします。

[Task Schedules] ウィンドウが表示されます。

ステップ 6　次の 2 つの方法のいずれかでタスク スケジュールを作成します。

- すぐに実行するタスクをスケジュールする場合は、[Now] をクリックします。この場合、スケジュール情報が [Task Schedules] のリストに自動的に入力されます。
- このタスクのスケジューラを作成するには、[Create] をクリックします。この場合、[Task Schedule] ウィンドウが表示されます。

ステップ 7　[Task Schedule] ウィンドウで、タスクを実行する時間と頻度を定義するための選択を行います。

（注）　デフォルト設定では、単一の **TE ディスカバリ タスク**をすぐに実行します（[Now]）。

ステップ 8　[OK] をクリックします。

この結果、スケジュールされたタスクが [Task Schedules] テーブルに表示されます。

ステップ 9　[Next] をクリックします。

スケジュールされたタスクの概要が表示されます。

ステップ 10　[Finish] をクリックします。

[Tasks] ウィンドウの作成済みタスクのリストにタスクが追加されます。

エリア別ディスカバリの管理

エリア別 TE ディスカバリを実行する前に、Prime Provisioning による複数 OSPF エリアの管理方法を理解することは有益です。

このトピックの背景情報については、「トラフィック エンジニアリング管理の概念」（P.7-115）で複数の OSPF エリアの項を参照してください。

このセクションでは、次の操作について説明します。

- 「エリア別 TE 検出の実行」（P.7-16）
- 「ABR を使用したエリア別 TE 検出の実行」（P.7-17）。

エリア別 TE 検出の実行

選択した TE プロバイダーがある領域に対して TE ディスカバリを実行すると、その領域に関連付けられたすべてのトンネルおよび明示的パスが Prime Provisioning データベースにインポートされます。

エリア別 TE ディスカバリを開始するには、次のステップを実行します。

ステップ 1　プロバイダーを作成します。

ステップ 2　リージョンを作成します。

ステップ 3　TE プロバイダーを作成します。

ステップ 4　[Devices] ウィンドウからシード デバイスを作成します。

ステップ 5　[Operate] > [Task Manager] > [Create] > [TE Full Discovery] を選択します。

TE ディスカバリ タスクの名前を指定するか、またはデフォルトを受け入れて、[Next] をクリックします。

ステップ 6　TE プロバイダーを選択し、[Next] をクリックします。

ステップ 7　シード デバイスを選択し、[Next] をクリックします。

ステップ 8　TE ディスカバリからスケジュールを選択し、[Next] をクリックします。

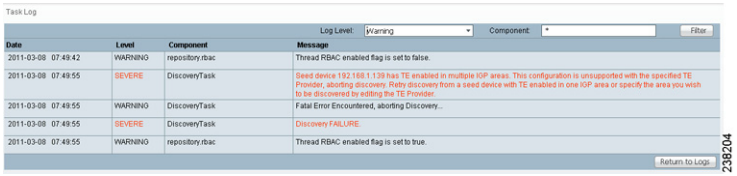
ステップ 9　ディスカバリ タスクの要約を確認します。

受け入れ可能な場合は、[Finish] をクリックして、TE ディスカバリプロセスを開始します。

ABR を使用したエリア別 TE 検出の実行

TE プロバイダー設定でエリア識別子が指定されておらず、シード デバイスが ABR の場合、図 7-7 の警告メッセージが表示されて TE 検出が中断し、TE プロバイダーのエリア識別を指定する、または ABR 以外のデバイスをシードとして使用するように通知します。

図 7-7　TE エリア識別子が指定されていない ABR を使用した TE 検出



TE 検出タスクの検証

TE 検出タスクは、次の 4 つの方法で評価できます。

- Task Logs：ネットワークで発生した変更のサマリー ログを表示します。
- TE トポロジ：リポジトリから最新の TE トポロジを表示します。
- ネットワーク要素の表示：トラフィック エンジニアリング管理 GUI で、[TE Nodes]、[TE Links]、[TE Primary Tunnels] などに移動し、特定のネットワーク要素タイプの状態を確認します。
- 検出されたデバイスの状態の表示：[Service Requests] ウィンドウに移動し、検出されたデバイスの状態が想定どおりかどうかを調べます。

Task Logs

TE 検出ログは、ネットワークの状態をキャプチャし、リポジトリの最新のスナップショットと比較します。

TE 検出タスクのタスク ログを表示するには、次のステップを実行します。

ステップ 1　[Operate] > [Task Logs] を選択します。

[Task Logs] ウィンドウが表示されます。

タスクのステータスが [Status] 列に表示されます。これは自動的に更新され、TE 検出プロセスが完了した時間を通知します。

タスクが完了しておらず、[Auto Refresh] が選択されている場合は、完了するまで表は更新を定期的に続行します。

ステップ 2　特定のタスクのログを表示するには、[Operate] > [Task Manager] に移動し、必要なタスクを選択してから、[View Log] ボタンをクリックします。

TE 検出ログのコピーを、図 7-8 から始まる次のスクリーンショットで示します。この最初の例では、TE ディスカバリによってトポロジ内で発見された TE 対応のデバイスとリンクを示します。各デバイスが識別された後に、エラーの特定を容易にするために、各デバイスに対して、一連のデバッグ、情報、警告、およびエラーのログが作成されます。

（注）　次のスクリーンショットに示すネットワークにおける変更の要約を探すには、ログの下部までスクロールしてください。

図 7-8　TE ディスカバリ タスク ログ - 例 1

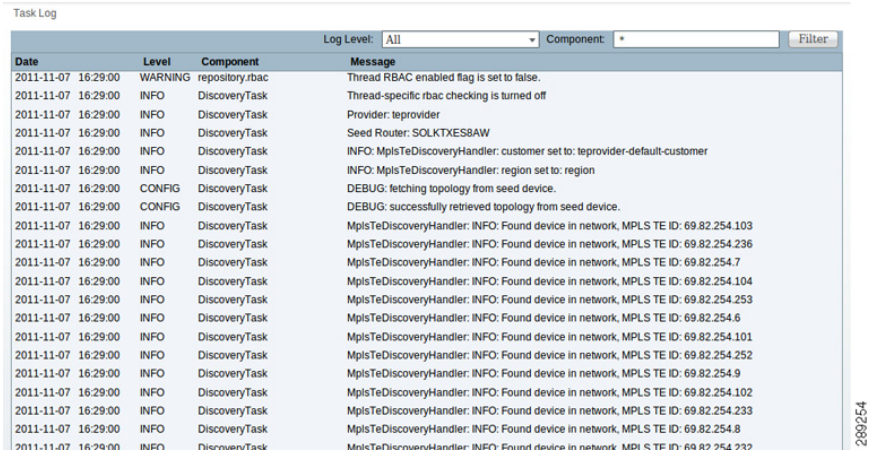


図 7-9 と 図 7-10 には、デバイスのデバッグおよび情報セクションの例を示します。

図 7-9　TE ディスカバリ タスク ログ - 例 2

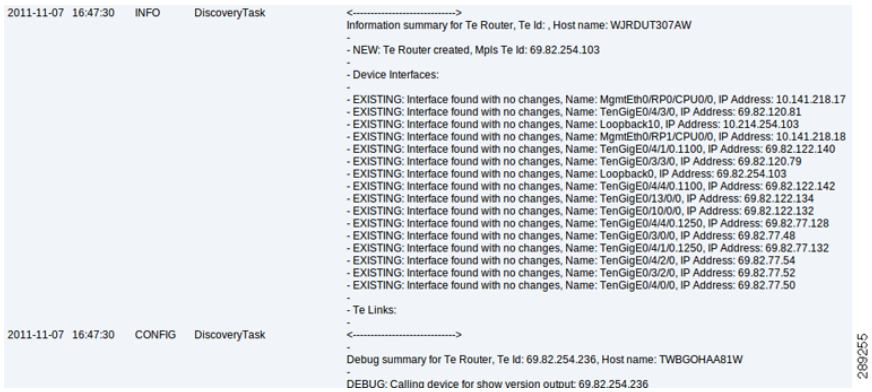
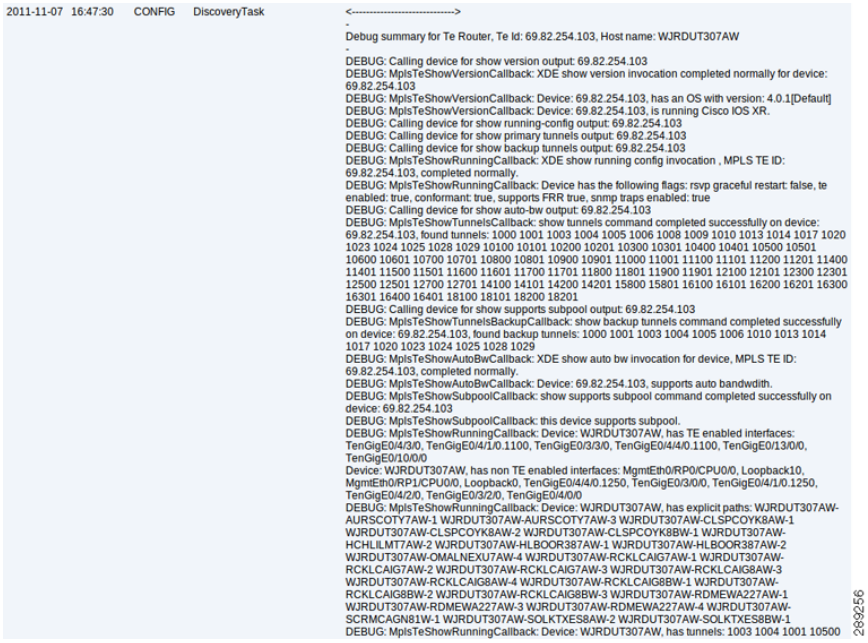


図 7-10　TE ディスカバリ タスク ログ - 例 3



ステップ 3　[Return to Logs] をクリックして、現在のログとオプションを終了し、別のログを開きます。

TE トポロジ

TE トポロジ ツールは、ネットワークの現在の状態の視覚的なスナップショットを提供します。すでにネットワークで行われた変更を判断するために使用することはできません。

ネットワークのトポロジ グラフの生成に必要なステップについては、「TE トポロジ」（P.7-84）を参照してください。

ネットワーク要素の表示

TE ディスカバリを実行した後でネットワークの状態を確認する別の方法は、[Traffic Engineering] メニュー オプションに移動し、確認する要素のタイプを選択することです。

たとえば、TE ディスカバリを実行した後でノードのステータスを確認するには、[Traffic Engineering] > [Nodes] を選択します。TE ノードの更新されたリストを確認し、ネットワーク内のノードを評価します。

[TE Links]、[TE Primary Tunnels]、[TE Backup Tunnels] などについて繰り返します。

管理インターフェイスの設定

トンネル管理操作を開始する前に、管理インターフェイスを設定する必要があります。ただし、このステップは、ネットワーク デバイスが、管理ステーションからホスト名によってアクセスできない場合のみ必要です。

特定のデバイスで管理インターフェイスを設定する方法の詳細については、「デバイス」（P.2-1）を参照してください。

MPLS-TE 管理プロセス

MPLS-TE 管理プロセスには、次のステップが関係します。

1. ネットワーク上で MPLS-TE をイネーブルにし、デバイス TE ID として使用されている IP アドレスが管理ステーションからアクセスできることを確認します（このステップは TEM によってサポートされていません）。
2. MPLS-TE ネットワークの検出するためにリポジトリを準備します。
3. 検出されたデバイスの管理インターフェイスを設定するか、検出されたすべてのデバイスの解決策でサーバ ホスト ファイルを更新します。繰り返しになりますが、ホスト名がすでに管理ステーションからアクセス可能な場合、これは必要ありません。
4. MPLS-TE ネットワークを検出します。

次に、TEM で使用可能な他の MPLR-TE 機能を実行することができます。

（注）　リポジトリが空の場合、または管理 IP アドレスが TE ネットワーク内の現在のデバイスに設定されていない場合、管理ステーションからルータ MPLS TE ID に到達できることを確認してください。つまり、TE 検出プロセスはシード パススルーをサポートしていません。

イーサネット リンクの設定

TEM では、ポイントツーポイント リンクのみサポートされます。POS リンクはデフォルトでポイントツーポイントですが、そうでない場合は、イーサネット リンクをポイントツーポイントとして設定する必要があります。

IOS の場合は、次のコマンドを入力します。

```
(config-if)# ip ospf network point-to-point
```

IOS XR の場合は、次のコマンドを入力します。

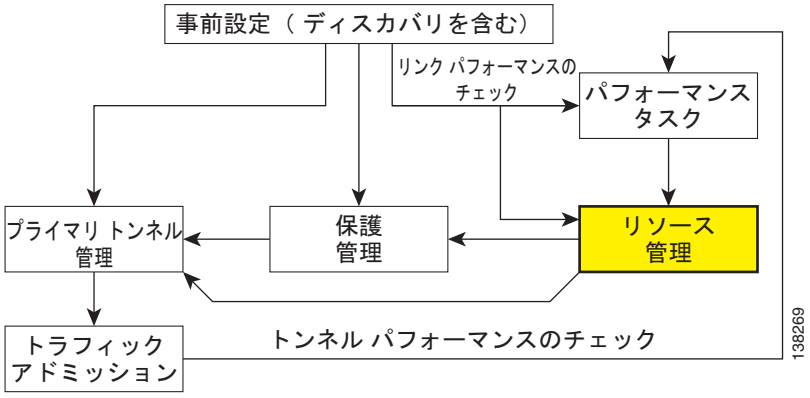
```
# router ospf <id> area <area identifier> interface <name> network point-to-point
```

TE リソース管理

TE リソース管理は、トンネル配置を最適化する TE インターフェイスの特定のプロパティの調整として定義されます。

図 7-3 で強調表示されたボックスは、リソース管理が Prime Provisioning のどこで行われるかを示しています。

図 7-11　Prime Provisioning プロセス図：リソース管理



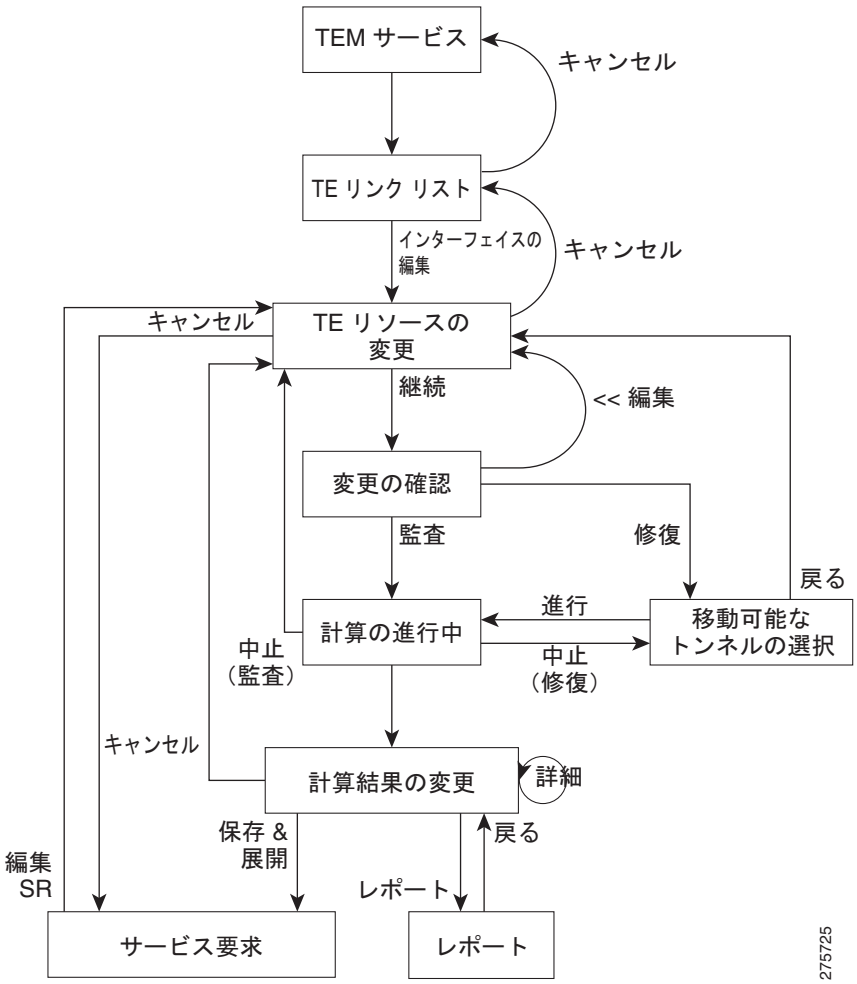
トンネル配置が試行され、十分な帯域幅がない場合は、TE リンクのリソースが変更され、トンネル配置が再試行されることがあります。

ここで述べられているネットワーク リソースは、TE ネットワークのルータ、これらのルータを接続するインターフェイス、RSVP 帯域幅、およびリンクで設定された他のプロパティを意味します。Prime Provisioning は、検出プロセスに依存してリポジトリにネットワーク要素を追加するため、リソース管理を実行する前にリソースを検出する必要があります。

TE リソース管理は、必要に応じて実行する手動プロセスです。元の設定がすでに最適である場合は、リソース管理タスクを行う必要がありません。以降のディスカバリで不一致が見つかったり、保護計画またはプライマリ トンネル配置で期待する結果をなかなか得られなかったりする場合は、リソースを調整する必要があることがあります。

リソース管理プロセスの概要については、図 7-12 を参照してください。

図 7-12　リソース管理プロセス



ここでは、次の内容について説明します。

- 「ネットワーク リソースの変更」（P.7-22）
- 「リンク ステータスの変更」（P.7-24）
- 「TE リンクの削除」（P.7-25）
- 「TE トンネルの削除」（P.7-26）
- 「TE ノードの削除」（P.7-27）。

ネットワーク リソースの変更

リソース管理タスクは、[TE Links List] ウィンドウから主に実行されます。

（注）　説明など特定の属性はこれらのツールで実行する計算に影響を与えず、これらの属性に対する更新は計算結果ウィンドウに表示されません。

TE リンクを変更するには、次の手順を実行します。

ステップ 1　[Traffic Engineering] > [Links] を選択します。

[TE Links List] ウィンドウが表示されます。

リンク リストには、TE ネットワークで現在アクティブなリンクが表示されます。必要に応じ、矢印を使用してページを移動してください。

ステップ 2　リンク リストで必要なリンクを選択します。

（注）　[Admin Status]：リンクが**アップ**なのか**ダウン**なのかを示します。これは Prime Provisioning に対してローカルです ネットワーク インターフェイスのステータスではありません。

ステップ 3　[Edit] > [Interface A] または [Edit] > [Interface B] をクリックして、リンクのいずれかのインターフェイスを編集します。

（注）　編集対象としてシスコ デバイス以外のインターフェイスを選択した場合、[Edit] ウィンドウで加えた変更は ISC リポジトリに保存されますが、導入はされません。

[TE Resource Modification] ウィンドウが表示されます。次のフィールドが含まれます。

- [Max Global (BC0) Reservable]：TE トンネルで予約できる帯域幅の最大量（kbps）。
- [Max Sub Pool (BC1) Bandwidth]：サブプール TE トンネルで予約できる帯域幅の最大量（kbps）。範囲は、1 ～ [Max Global Reservable] の値までです。
- [Attribute Bits]：パスを選択するときに、比較対象の属性をトンネルのアフィニティ ビットにリンクします。有効な値は 0x0 ～ 0xFFFFFFFF で、32 属性（ビット）を表します。属性の値は 0 または 1 です。
- [TE Metric]：リンクの Interior Gateway Protocol（IGP）管理上の重み（コスト）を上書きするために使用されるメトリック。
- [Propagation Delay]：トラフィックがリンクに沿ってヘッド インターフェイスからテール インターフェイスまで移動する時間。
- [Max Delay Increase]：リンクのバックアップ トンネルの伝搬遅延を制約する FRR バックアップ トンネルの計算で使用されます。バックアップ トンネルを生成する場合、リンクの最大遅延の増加によって、遅延の制約を緩めに設定する必要が生じることがあります。これは、保護されているフローと比較して遅延が増加されない場合、バックアップ トンネルのパスを見つけることは困難であるためです。
- [Link Speed Factor]：プライマリ トラフィックおよびバックアップ トラフィックで使用可能なリンク速度の量（パーセンテージ）に対応する増倍係数。通常は 1 に設定されます。

ステップ 4　必要な変更を行い、[Continue] をクリックして確認ページに進み、変更を確認するか、[Cancel] をクリックして変更を保存せずに終了します。

ステップ 5　[Edit] をクリックして編集可能なウィンドウに戻るか、次のいずれかの方法で続行します。

- [Proceed with Changes]：トンネル監査またはトンネル修復を実行します。

  トンネル監査およびトンネル修復の詳細については、「高度なプライマリ トンネル管理」（P.7-46）を参照してください。

  シスコ デバイス以外のデバイスが編集された場合は、[Proceed with Changes] が無効になります。代わりに、[Save & Deploy] が有効になり、変更を保存できます（展開はできません）。
- [Save & Deploy]：行われた変更がトンネル配置に影響を与えない場合は、[Save & Deploy] をクリックして作業を続行します。この場合は、トンネル監査またはトンネル修復を実行する必要がありません。

（注）　[Save & Deploy] をクリックすると、バックグラウンド プロセスが開始されます。別の配置との競合を避けるために、[Save & Deploy] で別の SR を展開する前にサービス要求（SR）の [Requested] および [Pending] 状態が完了するまで待機してください。展開の状態を確認するには、[Operate] > [Service Request Manager] に移動するか、[Operate] > [Task Manager] を開きます。

（注）　Prime Provisioning で、サービス要求（SR）は、TE トラフィック アドミッション SR を除き、[Operate] > [Service Request Manager] ページではなく、一般に各 TE サービスから展開されます。

展開後、SR のステータスは、[Operate] > [Service Request Manager] の SR ウィンドウで表示できます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

SR が [Deployed] 状態にならない場合は、[Task Logs] に移動し、展開ログ（[Operate] > [Task Manager] > [Logs]）を参照してください。タスク ログの詳細については、「Task Logs」（P.7-18）を参照してください。

リンク ステータスの変更

[TE Links List] ウィンドウで、リンクがオフラインになった場合の影響を確認することもできます。この方法は、インターフェイスを実際にシャットダウンする前にリンクからトンネルを移動するために使用できます。

（注）　Prime Provisioning のリンク ステータスはローカルでのみ有効です。ここで説明するリンク ステータスの変更は、ネットワークにプロビジョニングされません。

リンク ステータスを変更するには、次の手順を実行します。

ステップ 1　[Traffic Engineering] > [Links] を選択します。

[TE Links List] ウィンドウが表示されます。

ステップ 2　1 つまたは複数のリンクを選択し、[Change Status] ボタンをクリックします。

ステップ 3　[Enable] または [Disable] を選択して、選択されたリンクを有効または無効にします。

たとえば、[Disable] を選択すると、リンク ステータスが DOWN に変更されます。

同様に、[Enable] を使用してステータスを [UP] に変更します。

ステップ 4　トンネル監査またはトンネル修復を使用して、トンネルの配置に対する影響を評価し、変更を展開するには、[Proceed with Changes] をクリックします。

トンネル監査およびトンネル修復の詳細については、「高度なプライマリ トンネル管理」（P.7-46）を参照してください。

TE リンクの削除

[TE Link List] ウィンドウには削除機能（[Delete] ボタン）があります。この機能では、TE リンクおよびリンクの両端にある TE インターフェイスをリポジトリから削除できます。この場合、ネットワークの物理リンクには変更が加えられません。

リンク削除は、具体的な TE プロバイダーに基づいて選択できます。異なるプロバイダーに属する異なるリンクを削除する場合は、最初に適切なプロバイダーを選択し、次に削除するリンクをマークします。

また、同じプロバイダーの複数のリンクの同時削除もサポートされます。

制約事項

Prime Provisioning の GUI では、TE オブジェクトが使用しているリンクを削除できません。

次のオブジェクトがチェックされます。

- ストリクト明示的パス
- バックアップ トンネルの保護されたインターフェイス
- SRLG
- 保護された要素
- TE リソース SR

パス オプションを通過するプライマリまたはバックアップ トンネルが存在する場合は、エラー レポートが表示されます。それ以外の場合は、関連する上記のオブジェクト セットを削除する確認を求めるメッセージが表示されます。

使用例

この例では、プライマリまたはバックアップ トンネルが通過できるリンクを削除するときに必要な手順を示します。

次のステップを実行します。

ステップ 1　[Traffic Engineering] > [Links] を選択します。

ステップ 2　対応するチェックボックスをオンにしてリンクを選択します。

ステップ 3　[Delete] ボタンをクリックします。

ステップ 4　次の 2 通りの結果が考えられます。

- パス オプションがあるトンネルがリンクを通過します。リンクの削除に失敗し、リンクの削除を再試行する前にこれらのトンネルを再ルーティングまたは削除するよう求められます。この場合は、[TE Links List] ページに移動されます。
- パス オプションがあるトンネルがリンクを通過しません。そのリンクに対して TE に関連するオブジェクトのリストが表示され、TE リンクに関連するオブジェクトの自動削除に同意するか、リンクの削除トランザクションをキャンセルするかを確認するよう求められます。

ステップ 5　必要なすべてのトンネルを再ルーティングするか削除してからリンク削除を試行した場合は、まだ関連しているオブジェクトのリストが表示されます。

ステップ 6　プライマリ トンネルの再ルーティング後または削除後にリストされた関連する TE オブジェクトを削除する場合は、バックアップ リンク保護を提供するトンネルまたは複数のインターフェイスを保護するトンネルが存在する場合のみ、トランザクションの進行状況を示す新しいウィンドウが表示されま

す。バックアップ リンク保護を提供するトンネルまたは複数のインターフェイスを保護するトンネルが存在しない場合は、関連する TE オブジェクト リスト ページから、成功または失敗トランザクションに関する [TE Links] ウィンドウに移動します。

関連する TE オブジェクトに関する次の注意事項を確認してください。

ステップ 7　関連するすべてのオブジェクトが削除されたら、[TE Links List] ウィンドウが表示されます。

関連 TE オブジェクトに関する注意事項

関連する TE オブジェクトは次のいずれかになります。

- リンクを通過しているストリクト明示的パスおよびルーズ明示的パス（ストリクト ホップ タイプのもの）
- リンク保護を提供するバックアップ トンネル

（注）　リンクが SRLG から削除され（SRLG に複数のリンクがある場合）、またはリンクと SRLG の両方が削除されます（削除のためにマークされたリンクが、SRLG 内で唯一のリンクである場合）。

- リソース：SRs
- 保護された要素

上記リストの関連する TE オブジェクトは、リンクが TEM で設定されている方法によって異なります。

たとえば、関連する TE オブジェクトにリンク保護を提供するバックアップ トンネルがある場合は、保護されたインターフェイスが、利用可能な TE リンクに対して適切に更新され、バックアップ トンネル SR が再展開される [Link Deletion Progress] ウィンドウが表示されます。リンク保護を提供するバックアップ トンネルが関連する TE オブジェクトの資格を満たさない場合は、残りの TE オブジェクトが、関連する TE オブジェクトが表示されたウィンドウから自動的に削除されます。

TE トンネルの削除

TE トンネルは、[TE Links List] ウィンドウ、または個々のプライマリ トンネルまたはバックアップ トンネルの SR ウィンドウで削除できます（「プライマリ トンネルの削除」（P.7-40）または「バックアップ トンネルの削除」（P.7-45）を参照）。

[TE Links] ウィンドウで、1 つ以上のトンネルが通過するリンクを削除する必要性が、トンネルを削除する理由である場合があります。

トンネルを [TE Links List] ウィンドウで削除するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [Links] を選択します。

ステップ 2　削除するトンネルのリンクを選択し、[Show Tunnels] ボタンをクリックします。

表示するトンネルのカテゴリを選択できるトンネル フィルタが表示されます（[All]、[Managed]、[Unmanaged]、[Backup]）。

ステップ 3　いずれかのトンネルのカテゴリを選択します。

リンクを通過し、選択したフィルタのカテゴリに属するすべてのトンネルのリストが表示されます。

ステップ 4　削除する 1 つ以上のトンネルを選択し、[Delete] ボタンをクリックします。

新しいプロビジョニング操作の開始によって、選択したトンネルが削除されます。

TE ノードの削除

また、TE ノードを削除することもできます。この処理は、リンクの削除と非常に似ていますが、PE デバイス画面から実行します。対応する PE デバイスを削除することにより、TE ノードを事実上削除します。

TE リンクの場合と同様の制限が適用されます。削除操作は、いかなる TE オブジェクトもノードを使用していない場合にだけ成功します。

制約事項

Prime Provisioning の GUI では、TE オブジェクトが使用しているノードを削除できません。

TE リンクと同様に、次のオブジェクトを確認します。

- ストリクト明示的パス
- バックアップ トンネルの保護されたインターフェイス
- SRLG
- 保護された要素
- TE リソース SR

また、ノードの削除では、いかなる管理対象トンネル、管理対象外トンネル、またはバックアップ トンネルも、そのノードで開始または終了していないことが確認されます。

これらのオブジェクトのいずれかがノードを使用している場合は、ノードを削除しようとすると、エラー メッセージが発生し、ノードとそのインターフェイスが未変更のままになります。

使用例

この機能の例は、TE ルータをネットワークからデコミッションし、大規模なトポロジ変更の一環として 1 つまたは複数の新しい TE ルータに置き換える場合です。

このノードを削除できるようにするためには、次のようなステップが必要です。

1. トンネル修復を使用してこのノードからすべての管理対象トンネルを再ルーティングする。
2. トンネルから離れるパスの一部としてノードを使用して、すべての管理対象外トンネルとバックアップ トンネルを再ルーティングする。
3. ノードを構成するいずれかのインターフェイスを保護するすべてのバックアップ トンネルを削除する。
4. ノードを使用する明示的なパスをすべて削除する。
5. [TE Links List] ウィンドウでリポジトリからノードを削除する。
6. Prime Provisioning の外部で、適切な停止期間内に、ノードのデコミッションを行い、新しいノードをセットアップする。
7. 新しい [TE discovery] タスクを実行する。この結果、新しく追加されたノードがリポジトリに追加される。

8. ネットワークの FRR 要件に応じて、バックアップ計算を使用して新しいノードを保護する。（「バックアップ計算」（P.7-65）を参照）。
9. ネットワーク グルーミング（「グルーミング」（P.7-59）を参照）を実行して、管理対象トンネルを最適化することにより、管理対象トンネルで新規ノードが使用されるようにする。

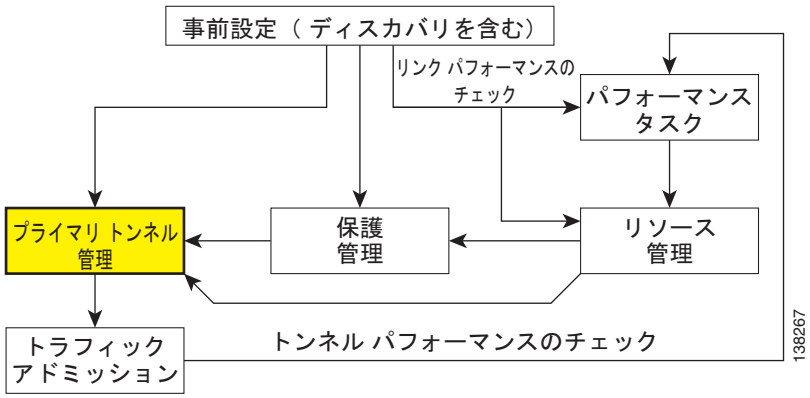
これらの手順が正常に行われると、TE ノードと、そのノードで開始されるすべての TE リンクおよび TE インターフェイスがリポジトリから削除されます。

基本的なトンネル管理

ここでは、Prime Provisioning でプライマリおよびバックアップ トンネルの作成に必要なプロセスについて説明します。トンネルを作成するには、以前の項の説明に従って、特定のステップをまず実行する必要があります。

図 7-3 で強調表示されているボックスは、Prime Provisioning のプライマリ トンネル管理が発生した場所を示します。

図 7-13　Prime Provisioning プロセス図：プライマリ トンネル管理



プライマリ トンネルは、通常操作においてトラフィックを伝送することによって特徴付けられます。可能なパスの優先順位リストがあり、これにより、トラフィックをルーティングすることができます。いずれの時点でも、優先順位の最も高い、使用可能なパスがトラフィックのルーティングに使用されます。これに失敗した場合、トラフィックは通常、より高い優先順位のパスが再び使用可能になるまで、次に使用可能なパスを介してリルートされます。

トンネルを設定する前に、トラフィックを制御する TE ポリシーを定義する必要があります。ルートを確立するために明示的パスが作成され、プライマリ トンネルの場合は、管理対象または管理対象外トンネルのいずれかとして作成されます。

バックアップ トンネルの目的は、ネットワーク内のルーティングが再コンバージェンスされるまで、失敗した要素の周辺の Fast Re-Route（FRR）で保護されたトラフィックを伝送することです。これは、プライマリ トンネルに沿って移動するトラフィックを保護することを意図しています。ロード バランシングの使用を通じて、同じトラフィックを複数のバックアップ トンネルが保護することが考えられます。

ネットワークが再コンバージされない場合は、バックアップ トンネルによる伝送が続行されます。

管理対象トンネルと管理対象外トンネルの違いは、「トラフィック エンジニアリング管理の概念」（P.7-115）の管理対象 / 管理対象外プライマリ トンネルの項で説明します。

帯域幅プールという重要な概念があり、ここからトンネルで帯域幅を予約します。これは、「トラフィック エンジニアリング管理の概念」（P.7-115）の帯域幅プールの項で説明します。

ここでは、次の内容について説明します。

TE ポリシーの作成

プライマリ トンネルを作成するには、各プライマリ トンネルをポリシーに関連付ける必要があります。ポリシーは、複数のトンネルで使用できます。

バックアップ トンネルの場合、このステップは必要ありません。この場合は、「明示的パスの作成」（P.7-30）に進みます。

他の TE ポリシー管理の操作については、「TE ポリシー」（P.7-73）を参照してください。

TE ポリシーは、TE ネットワークを制御する一連のルールで、プライマリ トンネル トラフィックのサービス クラス（たとえば、ゴールド、シルバー、ブロンズ）を定義します。

Prime Provisioning には、管理対象および管理対象外のポリシーの概念があります。管理対象ポリシーの設定 / 保持優先順位は 0/0 であり、保護レベルや最大遅延などの追加のルーティング制約があります。管理対象外ポリシーのトンネルは、システムによってプロビジョニングされますが、システムは展開のみを追跡し、トンネルの操作は追跡しません。管理対象外ポリシーの設定 / 保持優先順位は 0 にできません。

管理対象および管理対象外のプライマリ トンネルの詳細については、「トラフィック エンジニアリング管理の概念」（P.7-115）で、管理対象 / 管理対象外プライマリ トンネルの項を参照してください。

ポリシーは [Service Design] の [Policies] で管理します。**ポリシー** GUI の詳細については、「TE ポリシー」（P.7-73）を参照してください。

TE ポリシーを作成するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [Policy Manager] を選択します。

[Policy Manager] ウィンドウが表示されます。

ステップ 2　[Create] をクリックし、[TE Policy] を選択して新規 TE ポリシーを設定します。

既存のポリシーを編集するには、変更するポリシーを選択し、[Edit] をクリックします。[TE Policy Editor] ウィンドウが表示されます。

（注）　トンネルで使用されているポリシーは変更できません。ただし、使用中のポリシーの名前と所有権は変更できます。

さまざまなウィンドウ要素の説明については、「TE ポリシー」（P.7-73）を参照してください。

ステップ 3　アスタリスク（*）が付いた必須フィールド、および任意フィールドに入力します。

管理対象トンネルの TE ポリシーを使用する場合は、[Managed] チェックボックスがオンであることを確認します。

管理対象トンネルのポリシーを設定する場合は、**設定**および**保持**優先順位が 0（最も高い優先順位）に自動的に設定されます。管理対象外トンネルのポリシーを設定する場合は、希望する**設定**および**保持**優先順位の設定を指定することができます。

ステップ 4　[Save] をクリックします。

明示的パスの作成

パスは、ソース ルータと宛先ルータの間で定義され、これらの間には 1 つ以上のホップがある可能性があります。パスは、明示的パスのオプションで、プライマリ トンネルおよびバックアップ トンネルに対して使用されます。

管理対象トンネルの明示的パスを作成する場合、パスに TE 以外に対応したインターフェイスを含めないでください。TE 以外に対応したインターフェイスを持つパスは、管理対象トンネルおよびバックアップ トンネルのトンネル エディタのトンネル パス選択によるフィルタリングによって除外されます。

明示的パスを作成または編集するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [Explicit Paths] を選択します。

[TE Explicit Path List] ウィンドウが表示されます。

ステップ 2　[TE Explicit Path List] で明示的パスを作成するには、[Create] をクリックします。

[New TE Explicit Path] ウィンドウが表示されます。

明示的パス リストで明示的パスを編集するには、変更する明示的パスを選択し、[Edit] をクリックします。これにより、[TE Explicit Path Editor] ウィンドウが開きます。

（注）　トンネルで使用されている明示的パスは変更できません。ただし、パスを表示するには [Edit] を使用します。

[New TE Explicit Path] ウィンドウには、次の GUI 要素があります。

- [Path Name]：明示的パスの名前。
- [Head Router]：ヘッド ルータの名前。
- [Path Type]：次の 3 タイプの明示的パスがサポートされています。
  - [STRICT]：すべてのストリクト ホップはパスで定義されます。
  - [Loose]：すべてのルーズ ホップ（純粋なルーズ パスまたはルーズ ホップとストリクト ホップの組み合わせ）は、パスで定義されます。

  - [EXCLUDE]：すべての除外ホップはパスで定義されます。
- [Links (table)]：現在のパスに追加されたリンクを示し、次の情報が含まれます。
  - [Device]：パスのリンク元である TE デバイスのホスト名。
  - [Outgoing Interface]：発信元デバイスの発信インターフェイスのインターフェイス名。
  - [Outgoing IP]：発信インターフェイスの IP アドレス。
  - [Next Hop]：ネクスト ホップ デバイスのホスト名。
  - [Incoming Interface]：ネクスト ホップ デバイスの着信インターフェイスの名前。
  - [Incoming IP]：ネクスト ホップ デバイスの着信インターフェイスの IP アドレス。
- [Provision Preference]：**ip explicit-path** コマンドの **next-address** サブコマンドをプロビジョニングするための設定。[Outgoing Interface] または [Incoming Interface] を選択します。
  - [Outgoing Interface]：ルータ上の発信インターフェイス。
  - [Incoming Interface]：ルータ上の着信インターフェイス。

（注） トンネルでパスが使用されている場合、変更することはできません。[Outgoing Interface] および [Incoming Interface] リンクは選択できず、[Provision Preference] 行および [Add Link]、[Delete Link]、および [Save] ボタンは表示されません。

ステップ 3　パス名を指定してヘッド ルータを選択します。

ステップ 4　パス タイプを選択します。

- [Strict]：[Strict] が選択されている場合は、現在のパネルを使用して、宛先に到達するまで 1 つずつ接続されたリンクを一覧表示します。
- [Loose]：[Loose] が選択されている場合、IP アドレスを入力することにより新しいホップが追加されます。[Strict] が選択されている場合は、[TE Links List] からのみ選択することができます。

（注） IOS XR で、ヘッド デバイスが IOS XR 3.4 以降を実行している場合は、[Loose] タイプのみ使用できます。

（注） [Loose] が選択されている場合、ルーズ ホップ定義を 1 つずつ追加する新しいパネルが一覧表示されます。ルーズ明示的パス定義にはストリクト ホップとルーズ ホップの組み合わせを使用できるため、ストリクト ホップを含む柔軟性が、パスに少なくとも 1 つのルーズ ホップが存在するという制約とともに提供されます。

- [Exclude]：[Exclude] を使用することによって、除外する IP アドレスを指定できます。ステップ 6 を参照してください。

ステップ 5　[Strict] が選択された場合、[Add Link] ボタンをクリックして空白行をホップ リスト テーブルに追加します。

[Loose] または [Exclude] を選択した場合は、[Add Hop] ボタンが表示され、このボタンをクリックすると IP アドレスを指定するポップアップ ウィンドウが開きます。

ステップ 6　次に、ヘッド ルータのインターフェイスを選択する必要があります。

パス タイプの選択に応じて、次のいずれかのウィンドウが表示されます。

A. ストリクト パス タイプ：

[Add Link] ボタンをクリックし、次に [Add Interface] をクリックします。[Select Next Hop] ウィンドウが表示されます。

ネクスト ホップ リストには、明示的パスにすでに含まれているものを除き（パス ループを避けるため）、ルータのすべての可能なネクスト ホップが含まれています。

次のホップ リストには、TE インターフェイスおよび最大 1 つの各ルータの TE 以外のインターフェイスが含まれます（ループバック インターフェイスがデバイスの MPLS TE ID として使用されている場合）。TE インターフェイスの場合、[Outgoing Interface] および [Outgoing IP] 列がアプリケーションによって生成されます。

（注） TE 以外のインターフェイスが選択されている場合、[Provision Preference] は [Incoming Interface] に設定されます。プロビジョニング設定は手動で設定できません。

インターフェイスを選択し、[Select] をクリックします。対応するリンク情報が、[Links] テーブルの新しい明示的パスに追加されます。

[New TE Explicit Path] ウィンドウで、受信および発信インターフェイスの両方のフィールドが生成されます。

B. ルーズ パス タイプ：

[Add Hop] ボタンをクリックします。[Loose Hop Definition] ウィンドウが表示されます。

このウィンドウで、必要なルーズ ホップの IP アドレスを指定し、[OK] をクリックします。[Loose Hop Definition] ウィンドウが閉じます。

[New TE Explicit Path] ウィンドウに、追加したルーズ ホップが表示されます。

C. 除外 パス タイプ：

[Add Hop] ボタンをクリックします。[Exclude Hop Definition] ウィンドウが表示されます。

このウィンドウで、必要な除外ホップの IP アドレスを指定し、[OK] をクリックします。[Exclude Hop Definition] ウィンドウが閉じます。

[New TE Explicit Path] ウィンドウに追加された除外ホップが表示されるようになります。

ステップ 7　別のリンクを追加するには、[Add Link] または [Add Hop] をクリックします。

ステップ 8　ストリクト ホップの場合、[Outgoing Interface] または [Incoming Interface] オプション ボタンのいずれかをクリックすることにより、オプションで [Provision Preference] を選択できます。

（注） TE 以外のインターフェイスが存在しない場合にリンクを追加する前に [Provision Preference] を選択しようとすると、[Add Link] プロセスにより [Provision Preference] が無効になり、受信に設定されます。

ステップ 9　作成した TE 明示的パスを保持するには [Save] をクリックし、保存せずに終了するには [Cancel] をクリックします。

明示的パスの削除

Prime Provisioning では、プライマリ/バックアップ トンネルの削除/デコミッション時の明示的パスのデコミッションをサポートしています。これは、IOS XR の場合にのみサポートされます。

このような状況で明示的パスを削除できるかどうかは、他のグローバル アプリケーションによって使用されるかどうかによって異なります。

明示的パスの削除は、プライマリ管理対象/管理対象外トンネル、バックアップ トンネル、および任意の非適合トンネルの両方の SR トンネル削除と関連して行われ、すべてのパス オプション タイプ（STRICT、LOOSE、EXCLUDE）に適用可能です。

トンネル設定の変更により、システム内のトンネルが明示的パスを使用しなくなった場合、明示的パス設定は Prime Provisioning によって自動的に削除されます。この状況は、トンネルを削除した場合、または Prime Provisioning でトンネルをリルートした場合に発生します。

デバイスから明示的パス設定を削除した場合でも、明示的パスはまだ Prime Provisioning データベースには存在しています。データベースに残っているこのような明示的パスは、再使用できます。

Prime Provisioning の外部で（たとえば、デバイス自体の CLI を介して）トンネルをリルートまたは削除した場合、明示的パスは削除されません。ただし、トンネルが明示的パスを使用しなくなるように、トランザクションが Prime Provisioning を使用してトンネルをリルート、削除、変更した場合、その明示的パス設定は自動的にデバイスから削除されます。

プライマリ トンネルの操作

Prime Provisioning を使用することにより、多くのプライマリ トンネルの操作を実行できます。これらについては、次の項で説明します。

プライマリ トンネルの作成

TE ポリシーおよび明示的パスの設定を終えれば、プライマリ トンネルを作成できます。プライマリ トンネルには、次の 2 つのタイプがあります。

- 管理対象プライマリ トンネル
- 管理対象外プライマリ トンネル

以降では、管理対象外プライマリ トンネルを作成する場合の GUI の流れを説明します。これは、管理対象プライマリ トンネルと非常に似ており、わずかな違いについては、「トラフィック エンジニアリング管理の概念」（P.7-115）の管理対象/管理対象外プライマリ トンネルの項で説明されています。

管理対象プライマリ トンネルまたは管理対象外プライマリ トンネルを作成するには、次のステップを実行します。

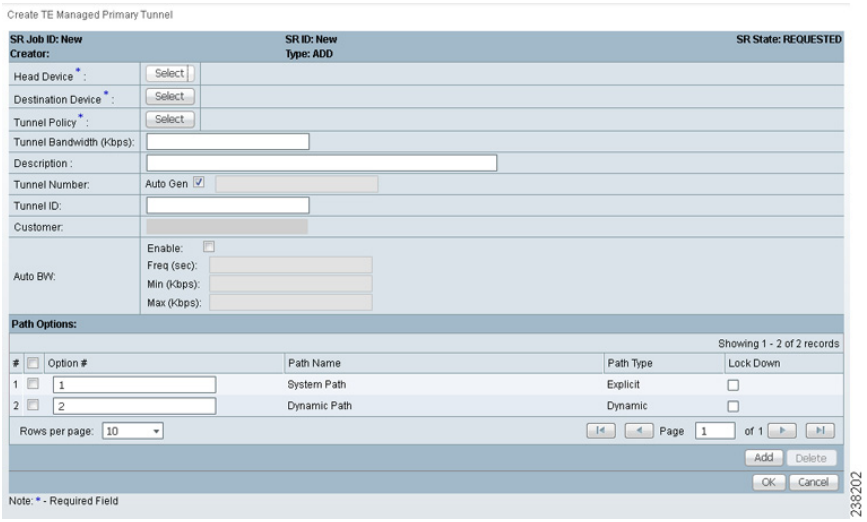
ステップ 1　[Traffic Engineering] を選択します。

ステップ 2　[Create Managed Tunnel] をクリックします。図 7-14 に示すように、[TE Managed Primary Tunnels SR] ウィンドウが表示されます。

または

[Create Unmanaged Tunnel] をクリックします。[TE Unmanaged Primary Tunnels SR] ウィンドウが表示されます。

図 7-14　Create TE Managed Primary Tunnel



次の要素を含む [TE Managed Primary Tunnels SR] ウィンドウが表示されます。

- [Op]：トンネルの SR 操作。次のいずれかになります。
  - [ADD]：新しく追加されたトンネルを示します。
  - [MODIFY]：変更された既存のトンネルを示します。
  - [DELETE]：削除される既存のトンネルを示します。
  - [ADMIT]：トンネル計算によってアドミッションされる既存のトンネルを示します。
- [Tunnel ID]：Prime Provisioning で使用される一意のトンネル識別子。
- [T#]：ヘッド ルータのトンネル番号。
- [Head]：ヘッド ルータのホスト名。
- [Dest]：宛先ルータのホスト名。
- [Policy]：トンネルの TE ポリシー。
- [BW]：トンネル帯域幅。トンネルが auto-bw 対応の場合、[BW] には、トンネル帯域幅と最大自動帯域幅のうち大きい方が示されます。
- [AutoBW]：**true** であれば自動帯域幅がイネーブルにされており、そうでない場合は **false** です。
- [Deploy Status]：トンネル展開ステータス。
- [Verified]：トンネルの検証が成功したかどうかを示します（succeed、failed、または unknown）。
- [Allow Reroute]：再ルーティングが許可されるかどうかを指定します（true または false）。再ルーティングが許可されない場合、トンネルは移動可能に設定できないため、操作によって再ルーティングできません。
- [Head Region]：ヘッド ルータが含まれているリージョン。
- [Tail Region]：テール ルータが含まれているリージョン。

次のアクションを実行できます（ボタン）。

- [Display]：ネットワークのトポロジの表示を開き、選択されたプライマリ トンネルを強調表示します。選択したトンネルは、方向を示す矢印を使用してカラーでマークされます。
- [Details]：トンネルのタイプ、ステータス、LSP、およびその他の情報を提供する [TE Tunnel Details] ウィンドウを開きます。
- [Admit]:選択した事前に検証されていないトンネルを管理対象トポロジにアドミッションします。この機能は、検証が失敗したディスカバリ済みのトンネル、または管理対象外トンネルの移行にのみ使用します。
- [Create]：管理対象プライマリ トンネルを作成します。
- [Edit]：選択したプライマリ トンネルを編集します。
- [Delete]：選択したプライマリ トンネルを削除します。
- [Import]：インポート XML ファイルからトンネル データをインポートします。
- [Placement Tools]：これらのツールは、トンネルに変更を加えていない場合にだけ使用できます。現在のトポロジおよびトンネルに対して次の機能を適用します。
  - [Groom]：最大リンクの使用率を下げるために、ネットワークの管理対象トンネルを分析し、再ルーティングします。
  - [Tunnel Audit]：SRLG またはバックアップ トンネルに対して以前に加えた変更が、管理対象トンネルで制約違反の原因となったかどうかを調べます（これは、管理対象トンネルに FRR 保護の制約がある場合に発生することがあります）。
  - [Tunnel Repair]：[Placement Tools] > [Tunnel Audit] で明らかになった管理対象トンネルの制約違反を修復します。
- [Update Tunnel ID]：対応するトンネルを展開せずに、リポジトリでトンネル ID を直接更新します。
- [Proceed with Changes]：トンネルの変更を確認します。トンネルが作成、削除、またはアドミッションされるか、またはトンネルの属性が変更された場合に、次のいずれかの配置ツールに進むことができます。
  - [Tunnel Audit]：トンネルの変更が原因となった可能性がある制約違反をチェックします。
  - [Tunnel Placement]：新しいトンネルのアドミッションを行い、ネットワークですでにアドミッションされたトンネルを変更します。
  - [Tunnel Repair]：変更を受け入れるためにできるだけ少ない既存のトンネルを移動することにより、既存のトンネルの帯域幅要件または遅延パラメータの変更による不一致を解決します。

管理対象外トンネルのリストでは、管理対象リストの最後の 2 列（[Verified] および [Allow Reroute]）が [Conformance] 列に置き換えられることに注意してください。

次の例では、管理対象外トンネルが作成されます。

ステップ 3　[Create] をクリックします。

[Create TE Unmanaged Primary Tunnel] ウィンドウが表示されます。

[Create TE Managed Primary Tunnel] ウィンドウと [Create TE Unmanaged Primary Tunnel] ウィンドウには、わずかな違いがありますが、次の要素が含まれています。

- [Head Device]：トンネルのヘッド デバイス。
- [Destination Device]：トンネルの宛先デバイス。
- [Tunnel Policy]：トンネルに対して確立されたルールのセット。
- [Tunnel Bandwidth]：トンネルに割り当てられている合計帯域幅。

- [Description]：トンネルの識別に役立つ説明のテキスト。
- [Tunnel Number]：トンネル インターフェイスの名前に対応するトンネル番号。
  - [Auto Gen]：トンネル番号を自動的に生成する場合は、このボックスをオンにします。オンにしない場合は、希望する番号を入力します。

（注）　手動で入力したトンネル番号が小さすぎると、展開の妨げになるおそれがあります。

（注）　MPLS-TE トンネルには、マルチキャスト GRE トンネルと干渉する潜在性があります。Prime Provisioning では、auto-gen を使用して新規トンネルを作成しますが、このトンネル番号は、MDT GRE トンネルによってすでに使用されているおそれがあります。このため、Prime Provisioning は、複雑さを回避するために大きいトンネル番号を使用します。

- [Tunnel ID]：Prime Provisioning で使用される一意のトンネル識別子。
- [Customer]：トンネルに対して選択したカスタマー。
- [Auto BW]：自動帯域幅調整のためにトンネルを設定し、トンネルの帯域幅の調整方法を制御します。
  - [Enable]：自動帯域幅をイネーブルにするには、このボックスをオンにします。
  - [Freq]：帯域幅調整の間隔。
  - [Min]：このトンネルの最小自動帯域幅（kbps 単位）。
  - [Max]：このトンネルの最大自動帯域幅（kbps 単位）。

パス オプション：

- [Option #]：使用可能な明示的パスの連続番号。
- [Path Name]：明示的パスの名前。既存のパスの場合、名前は明示的パス ビューアにリンクする URL です。
  - [System Path]：システム生成の明示的パス。管理対象トンネルでは、最初のパスは明示的パスでなければなりません。トンネルにシステム パスが含まれている場合、計画の機能は、トンネルの最適パスを生成します。
  - [Dynamic Path]：動的パスは、ヘッド ルータによるパスの検出を許可することによってプロビジョニングされます。**dynamic** キーワードは、ルータにプロビジョニングされます。
- [Path Type]：パス オプション タイプ（[Explicit] または [Dynamic]）。
- [Lock Down]：トンネルの再最適化チェックをディセーブルにします。オンにした場合、パスは変更できません。

ステップ 4　[Create TE Unmanaged Primary Tunnel] ウィンドウで [Head Device] を選択するには、対応する [Select] ボタンをクリックし、[Select Device for TE Head Router] ウィンドウを開きます。

ステップ 5　デバイス名を選択し、[Select] をクリックします。

[Select Device for TE Head Router] ウィンドウが閉じられ、[Create TE Unmanaged Primary Tunnel] ウィンドウにプロンプトが戻ります。

ステップ 6　[Create TE Unmanaged Primary Tunnel] ウィンドウで [Destination Device] を選択するには、対応する [Select] ボタンをクリックし、[Select Device for TE Tail Router] ウィンドウを開きます。

ステップ 7　デバイス名を選択し、[Select] をクリックします。

[Select Device for TE Tail Router] ウィンドウが閉じられ、[Create TE Unmanaged Primary Tunnel] ウィンドウにプロンプトが戻ります。

ステップ 8　[Create TE Unmanaged Primary Tunnel] ウィンドウで [Tunnel Policy] を選択するには、対応する [Select] ボタンをクリックして [Select Unmanaged TE Tunnel Policy] ウィンドウを開きます。

（注）　管理対象トンネルを作成するときは、1 つ以上の管理対象トンネル ポリシーが使用可能なことを確認してください。このようになっていない場合は、[Policies]（「TE ポリシーの作成」（P.7-29）を参照）に移動し、[Managed] チェックボックスがオンであることを確認します。

ステップ 9　ポリシーを選択し、[Select] ボタンをクリックします。

これにより、トンネル エディタに戻ります。

ステップ 10　[Add] をクリックし、トンネルのパス オプションを設定します。[Select TE Explicit Path] ウィンドウが表示されます。

[Path Options] には、パス タイプが 2 つ示されます。

[Explicit Path]：次の 3 種類のパスを含む、特定のヘッドから特定の宛先デバイスへの固定パス：[Strict]、[Loose]、および [Exclude]。

[Dynamic Path]：動的パスは、ヘッド ルータによるパスの検出を許可することによってプロビジョニングされます。**dynamic** キーワードは、ルータにプロビジョニングされます。

ステップ 11　ダイナミック パスだけを希望する場合を除き、必要な TE の明示的パスを選択します。

使用可能なものがない場合は、まず設定することができます。これを行うには、「明示的パスの作成」（P.7-30）を参照してください。

ステップ 12　[Select] をクリックします。

選択したパスが、作成ウィンドウの [Path Options] セクションに表示されます。

明示的パス（<*head_device*>-<*destination_device*>）の場合は、パス名をクリックして編集不可の明示的パス ビューアを開くことができます。

さまざまなウィンドウ要素の説明については、「明示的パスの作成」（P.7-30）を参照してください。

ステップ 13　[Create TE Unmanaged Tunnel] ウィンドウで、[OK] をクリックして入力したトンネル情報を受け入れるか、[Cancel] をクリックして終了し、[TE Unmanaged Primary Tunnels SR] ウィンドウに戻ります。

[Op] フィールドに [ADD] を設定した、新規作成した SR を含む [TE Unmanaged Primary Tunnel SR] ウィンドウが表示されます。

（注）　追加したトンネルは、トンネルを選択して [Delete] をクリックすることにより、[ADD] 状態から元の状態に戻すことができます。トンネル リストからトンネルが削除されます。

ステップ 14　[TE Unmanaged Primary Tunnel] ウィンドウで [Save & Deploy]（（注）（P.38）を参照）をクリックして、新規トンネル SR をネットワークに展開するかすべてのトンネルを強制的に展開します。または、プライマリ トンネルをさらに作成または編集してからすべての変更を保存および展開することもできます。

[Save & Deploy] をクリックすると、影響を受ける TE ルータが Prime Provisioning によってロックされます。これにより、SR が終了するまで、その TE ルータを使用する後続のすべての SR はブロックされます。システム内の他の SR は、安全に試行および展開できます。処理中の SR と競合する場合、Prime Provisioning では、単に完了まで待機することを要求します。

展開の状態を確認するには、[Operate] > [Service Request Manager] で [Service Requests] ウィンドウに移動するか、[Operate] > [Task Manager] を開きます。

- [Save & Deploy]：トンネル配置に影響を与えないトンネルの変更をコミットします。ネットワークに対して SR トンネルを保存し、展開するための 2 つのオプションがあります。

- [SR Tunnels Only]：トンネル配置に影響しないトンネルのすべての変更を展開するか、SR に変更が加えられていない場合に、このオプションを使用して、[Requested] 状態または [Invalid] 状態だった SR を再展開します。
- [Force Deploy All Tunnels]：この SR に含まれるすべてのトンネルを強制的に展開します。SR の前回プロビジョニングが失敗し、SR に含まれるすべてのトンネルを強制的に展開する必要がある場合に有用です。

（注）　TE トンネルの展開中に Elixir 警告が表示されることがあります。展開は正常に行われ、警告メッセージは無視しても安全です。

（注）　管理対象トンネルの場合、[Proceed with Changes] ボタンを使用してトンネル配置、トンネル監査、またはトンネル修復（「高度なプライマリ トンネル管理」（P.7-46））を実行するまで、サービス要求を展開できません。

（注）　TE トラフィック アドミッション SR を除き、TE SR は、[Operate] > [Service Request Manager] からではなく、常に特定の [TE SR] ウィンドウからすぐに展開されます。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が表示され、展開済みの SR の状態が表示されます（最初は REQUESTED、次に PENDING、成功した場合は DEPLOYED）。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

SR が [Deployed] 状態にならない場合は、[Task Logs] ウィンドウに移動し、「SR 展開ログ」（P.10-48）の説明に従って展開ログ（[Operate] > [Task Manager] > [Logs]）を参照してください。

[Service Request Manager] ウィンドウからサービス要求を編集する場合は、「プライマリ トンネルの編集」（P.7-38）の説明に従って、[TE Managed Primary Tunnels SR] ウィンドウまたは [TE Unmanaged Primary Tunnels SR] ウィンドウに戻ります。

プライマリ トンネルの編集

プライマリ トンネル属性はプライマリ トンネル エディタで変更できます。

プライマリ トンネル エディタにアクセスする方法は 2 通りあります。

- 管理対象または管理対象プライマリ トンネルの SR ウィンドウから、または
- [Service Requests] ウィンドウから

プライマリ トンネルの SR ウィンドウからのアクセス

プライマリ トンネルの SR ウィンドウ（[TE Managed Primary Tunnels SR] または [TE Unmanaged Primary Tunnels SR] ウィンドウ）からプライマリ トンネル エディタにアクセスするには、次のステップを実行します。

ステップ 1　[Traffic Engineering] を選択します。

ステップ 2　[Create Managed TE Tunnel] をクリックします。図 7-14 の [TE Managed Primary Tunnels SR] ウィンドウが表示されます。

または

[Create Unmanaged TE Tunnel] をクリックします。[TE Unmanaged Primary Tunnels SR] ウィンドウが表示されます。

ステップ 3　トンネル SR を編集するために、編集する SR を選択し、[Edit] をクリックします。

[Edit TE Managed Primary Tunnel] ウィンドウまたは [Edit TE Unmanaged Primary Tunnel] ウィンドウが表示されます。

プライマリ トンネル エディタは、プライマリ トンネル作成 GUI のエディタと同じです。さまざまなウィンドウ要素の説明については、「プライマリ トンネルの作成」（P.7-33）を参照してください。

ステップ 4　必要な変更を加え [OK] をクリックして受け入れるか、[Cancel] をクリックして変更を廃棄します。

[TE Unmanaged Primary Tunnel SR] ウィンドウで、[Op] フィールドが [MODIFY] に変わります。

（注）　変更したトンネルは、トンネルを選択して [Delete] をクリックすることにより、元の状態に戻すことができます。[Op] 列の [MODIFY] フラグが消えます。

ステップ 5　[Save & Deploy] をクリックして、新規トンネル SR をネットワークに展開するかすべてのトンネルを強制的に展開します。または、プライマリ トンネルをさらに作成または編集してからすべての変更を保存および展開することもできます。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が表示され、展開済みの SR の状態が表示されます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

[Service Requests] ウィンドウからアクセス

SR がすでに作成されている場合に [Service Requests] ウィンドウからプライマリ トンネル エディタにアクセスするには、次のステップを実行します。

ステップ 1　[Operate] > [Service Request Manager] を選択します。

ステップ 2　必要なトンネル SR を編集するために、編集する SR を選択し、[Edit] をクリックします。

管理対象トンネルを選択したのか管理対象外トンネルを選択したのかに応じて、[Service Requests] ウィンドウで選択した SR を表示した、[TE Managed Primary Tunnel SR] ウィンドウまたは [TE Unmanaged Primary Tunnel SR] ウィンドウが表示されます。

ステップ 3　トンネル SR を選択し、[Edit] をクリックします。

[Edit TE Unmanaged Primary Tunnel] ウィンドウが表示されます。

「プライマリ トンネルの SR ウィンドウからのアクセス」（P.7-38）に移動し、ステップ 4 から処理を続行します。

プライマリ トンネルの削除

TE トンネルは、[TE Links List] ウィンドウ（「TE トンネルの削除」（P.7-26）を参照）、またはプライマリ トンネルまたはバックアップ トンネルの SR ウィンドウで削除できます。

管理対象または管理対象外のプライマリ トンネルを [TE Managed Primary Tunnels SR] ウィンドウまたは [TE Unmanaged Primary Tunnels SR] ウィンドウから削除するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] を選択します。

ステップ 2　[Create Managed TE Tunnel] をクリックします。[TE Managed Primary Tunnels SR] ウィンドウが表示されます。

または

[Create Unmanaged TE Tunnel] をクリックします。[TE Unmanaged Primary Tunnels SR] ウィンドウが表示されます。

ステップ 3　トンネルを削除するには、削除するトンネルを選択し、[Delete] をクリックします。

[Op] フィールドのステータスが [DELETE] に変わります。

さまざまなウィンドウ要素の説明については、「プライマリ トンネルの作成」（P.7-33）を参照してください。

（注）　削除したトンネルは、トンネルを選択して [Delete] をクリックすることにより、元の状態に戻すことができます。[Op] 列の [DELETE] フラグが消えます。

ステップ 4　[Save & Deploy] をクリックして、新規トンネル SR をネットワークに展開するかすべてのトンネルを強制的に展開します。または、プライマリ トンネルをさらに作成または編集してからすべての変更を保存および展開することもできます。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が表示され、展開済みの SR の状態が表示されます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

バックアップ トンネル操作

Prime Provisioning では、いくつかのバックアップ トンネルの操作を実行できます。これについては、この項で説明します。

「トラフィック エンジニアリング管理の概念」（P.7-115）の「Connectivity Protection (CSPF) Backup Tunnels」は、バックアップ保護を実現する手法の 1 つです。

バックアップ トンネルの作成

バックアップ トンネルの作成方法は、プライマリ トンネルとほぼ同じです。いずれの場合も、対象のルータを通過する既存のパスがすでに存在する場合は、明示的パスの作成は不要です。パスは、パスの帯域幅キャパシティの許す限り、任意の数のトンネルで使用できます。

バックアップ トンネルの作成の前提条件は、明示的パスが存在することです。明示的パスを作成するには、「明示的パスの作成」（P.7-30）を参照してください。

バックアップ トンネルを作成するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [Create TE Backup Tunnel] を選択します。

[TE Protection SR] ウィンドウが表示されます。

[TE Protection SR] ウィンドウには、次の要素が含まれます。

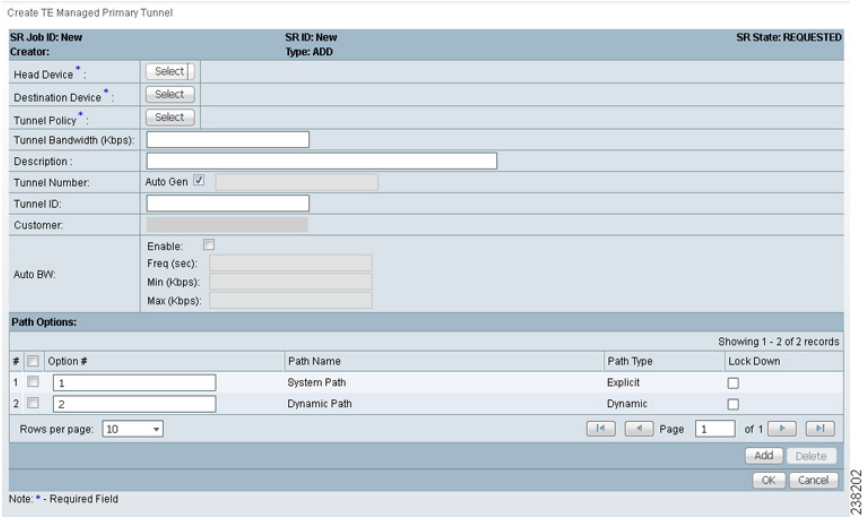
トンネル リストの列には、次の情報が示されます。

- [Op]：トンネルの現在の SR 操作。次のいずれかになります。
  - [ADD]：システムによって計算され、またはユーザによって入力された新規追加トンネルを示します。
  - [MODIFY]：変更された既存のトンネルを示します。
  - [DELETE]：システムの計算によるか、ユーザが開始することによって削除される既存のトンネルを示します。
- [Tunnel ID]：Prime Provisioning で使用される一意のトンネル識別子。
- [T#]：ヘッド ルータのトンネル番号。
- [Head]：ヘッド ルータのホスト名。
- [Dest]：宛先ルータのホスト名。
- [BW Quota]：このバックアップ トンネル保護できる帯域幅の量。ルータでは、LSP の帯域幅の合計が指定された帯域幅の総計を超えないように、このバックアップ トンネルを使用できる LSP を制限できます。複数のバックアップ トンネルがある場合、ルータは最適なアルゴリズムを使用します。
- [Deploy Status]：トンネル展開ステータス。
- [Conformance]：ディスカバリを実行して判明したトンネルの適合性を示します。予約された帯域幅が非ゼロで、保持プライオリティまたはセットアップ プライオリティがゼロの場合、トンネルは不適合です。TEM から入力したトンネルの場合は、常に適合しています。接続保護トンネルは、トンネル帯域幅が 0 で、バックアップ帯域幅が無制限であり、最初のパス オプションが「exclude address」である場合は、Conformant = true とマークされます。それ以外の場合は、Conformant = false とマークされます。
- [Backup Type]：帯域幅によって保護されているバックアップ トンネル（**BW** 保護）または CSPF-routed バックアップ トンネル（**CSPF**）のいずれかにすることができます。これらのバックアップ トンネルのタイプについて詳しくは、「トラフィック エンジニアリング管理の概念」（P.7-115）を参照してください。
- [Head Region]：ヘッド ルータが含まれているリージョン。
- [Tail Region]：テール ルータが含まれているリージョン。

ステップ 2　[Create] をクリックします。

図 7-15 の [Create TE Backup Tunnel] ウィンドウが表示されます。

図 7-15　Create TE Backup Tunnel



[Create TE Backup Tunnel] ウィンドウには次の要素が含まれています。

- [Head Device]：トンネルのヘッド デバイス。
- [Destination Device]：トンネルの宛先デバイス。選択ウィンドウは、ヘッド デバイス選択のウィンドウに非常に似ています。
- [Protected Interface(s)]：このバックアップ トンネルで保護するヘッド ルータ上のインターフェイス。
- [Description]：トンネルの識別に役立つ説明のテキスト。
- [Backup Bandwidth Limit]：バックアップ トンネルによって保護される帯域幅。
  - [Any Pool BW]：サブプールまたはグローバル プールのいずれかを保護するために保留する帯域幅。
  - [Sub Pool (BC1) BW]：サブ プール用に保留する帯域幅。
  - [Global Pool (BC0) BW]：グローバル プール用に保留する帯域幅。

  プール タイプの定義については、「トラフィック エンジニアリング管理の概念」（P.7-115）を参照してください。
- [Tunnel Number]：トンネル インターフェイスの名前に対応するトンネル番号。
  - [Auto Gen]：プロビジョニング時にトンネル番号を生成する場合は、このボックスをオンにします。オンにしない場合は、希望する番号を入力します。

  （注）　手動で入力したトンネル番号が小さすぎると、展開の妨げになるおそれがあります。
- [Tunnel ID]：Prime Provisioning で使用される一意のトンネル識別子。
- [Tunnel Bandwidth]：このバックアップ トンネルで許可される合計帯域幅（表示のみ）。

- [Tunnel Pool Type]：このポリシーのトンネル帯域幅プール タイプ（表示のみ）。プール タイプの定義については、「トラフィック エンジニアリング管理の概念」（P.7-115）を参照してください。
  - [Global Pool (BC0)]：帯域幅はグローバル プールから予約されます。
  - [Sub Pool (BC1)]：帯域幅はサブプールから予約されます。
- [Setup Priority (0-7)]、[Hold Priority (0-7)]、[Affinity]、[Affinity Mask]：手動で作成するすべてのバックアップ トンネルでは、セットアップ プライオリティおよび保持プライオリティがいずれも 0 で、アフィニティ値およびマスクが 0x0 の場合に限り、要素を保護できます。

パス オプション：

- [Option #]：使用可能な明示的パスの連続番号。
- [Path Name]：明示的パスの名前。
- [Path Type]：明示的パス タイプ（[Explicit] または [Dynamic]）。
- [Lock Down]：オンにした場合は、トンネルに対する再最適化検査がディセーブルになります。

ステップ 3　最低限、[Head Device]、[Destination Device]、および [Protected Interface] を選択します。

ゼロより大きい [Backup Bandwidth Limit] も指定してください。必要に応じて他のトンネル情報を追加します。

ステップ 4　[Add] をクリックして、1 つのパスだけを追加します。

[Select TE Explicit Path] ウィンドウが表示されます。

ステップ 5　明示的パスを選択します。

これは既存のパスのヘッドおよび宛先と一致している必要があります。使用可能なものがない場合は、まず設定する必要があります。これを行うには、「明示的パスの作成」（P.7-30）を参照してください。

ステップ 6　[Select] をクリックします。

選択したパスが、[Select TE Explicit Path] ウィンドウに示すように、ページの [Path Options] セクションに表示されます。

明示的パスの場合は、パス名をクリックして明示的パス ビューアを開くことができます。

ステップ 7　[Create TE Backup Tunnel] ウィンドウで、[OK] をクリックして入力したトンネル情報を受け入れるか、[Cancel] をクリックして保存せずにウィンドウを終了します。

[TE Protection SR] ウィンドウで、[Op] フィールドに [ADD] を設定した新規バックアップ トンネルがトンネル リストに追加されています。

（注）　追加したトンネルは、トンネルを選択して [Delete] をクリックすることにより、元の状態に戻すことができます。トンネル リストからトンネルが削除されます。

ステップ 8　[Save & Deploy] をクリックして、新規トンネル SR をネットワークに展開するかすべてのトンネルを強制的に展開します。または、バックアップ トンネルをさらに作成または編集してからすべての変更を保存および展開することもできます。

[Save & Deploy] ボタンには 2 つのオプションがあります。

- [SR Tunnels Only]：トンネル配置に影響しないトンネルのすべての変更を展開するか、SR に変更が加えられていない場合に、このオプションを使用して、[Requested] 状態または [Invalid] 状態だった SR を再展開します。
- [Force Deploy All Tunnels]：この SR に含まれるすべてのトンネルを強制的に展開します。SR の前回プロビジョニングが失敗し、SR に含まれるすべてのトンネルを強制的に展開する必要がある場合に有用です。

[Save & Deploy] をクリックすると、影響を受ける TE ルータが Prime Provisioning によってロックされます。これにより、SR が終了するまで、その TE ルータを使用する後続のすべての SR はブロックされます。システム内の他の SR は、安全に試行および展開できます。処理中の SR と競合する場合、Prime Provisioning では、単に完了まで待機することを要求します。展開の状態を確認するには、[Inventory and Connection Manager] の [Service Requests] ウィンドウに移動するか、[Monitoring] の [Task Manager] を開きます。

（注） TE トンネルの展開中に Elixir 警告が表示されることがあります。展開は正常に行われ、警告メッセージは無視しても安全です。

（注） TE トラフィック アドミッション SR を除き、TE SR は、[Operate] > [Service Request Manager] ページからではなく、常に特定の [TE SR] ウィンドウからすぐに展開されます。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が表示され、展開済みの SR の状態が表示されます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

SR が [Deployed] 状態にならない場合は、[Task Logs] ウィンドウに移動し、「SR 展開ログ」（P.10-48）の説明に従って展開ログ（[Operate] > [Task Manager] > [Logs]）を参照してください。

バックアップ トンネルの編集

バックアップ トンネル属性はバックアップ トンネル エディタで変更できます。

バックアップ トンネル エディタにアクセスする方法は 2 通りあります。

- [Protection SR] ウィンドウからアクセス
- [Service Requests] ウィンドウから

[Protection SR] ウィンドウから

[Protection SR] ウィンドウにアクセスしてバックアップ トンネルを編集するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [Create TE Backup Tunnel] を選択します。

[TE Protection SR] ウィンドウが表示されます。

ステップ 2　トンネル SR を編集するために、編集する SR を選択し、[Edit] をクリックします。

[Edit TE Backup Tunnel] ウィンドウが表示されます。バックアップ トンネル エディタは、バックアップ トンネル作成 GUI のエディタと同じです。さまざまなウィンドウ要素の説明については、「バックアップ トンネルの作成」（P.7-40）を参照してください。

ステップ 3　必要な変更を加えて [OK] をクリックします。

[TE Protection] ウィンドウで [Op] フィールドが [MODIFY] に変わります。

（注）　変更したトンネルは、トンネルを選択して [Delete] をクリックすることにより、元の状態に戻すことができます。[Op] 列の [MODIFY] フラグが消えます。

ステップ 4　[TE Protection SR] ウィンドウで、[Save & Deploy] をクリックして、新規トンネル SR をネットワークに展開するかすべてのトンネルを強制的に展開します。または、バックアップ トンネルをさらに作成または編集してからすべての変更を保存および展開することもできます。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が表示され、展開済みの SR の状態が表示されます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

[Service Requests] ウィンドウから

SR がすでに作成されている場合に [Service Requests] ウィンドウからバックアップ トンネルを編集するには、次のステップを実行します。

ステップ 1　[Operate] > [Service Request Manager] を選択します。

ステップ 2　必要なトンネル SR を編集するために、編集する SR を選択し、[Edit] をクリックします。

[Service Request Manager] ウィンドウで選択した SR を表示している [TE Protection SR] ウィンドウが表示されます。

ステップ 3　トンネル SR を選択し、[Edit] をクリックします。

[Edit TE Backup Tunnel] ウィンドウが表示されます。

「バックアップ トンネルの編集」（P.7-44）に移動し、ステップ 3 から処理を続行します。

バックアップ トンネルの削除

TE トンネルは、[TE Links List] ウィンドウ（「TE トンネルの削除」（P.7-26）を参照）、またはプライマリ トンネルまたはバックアップ トンネルの SR ウィンドウで削除できます。

[TE Protection SR] ウィンドウからバックアップ トンネルを削除するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [Create TE Backup Tunnel] を選択します。

[TE Protection SR] ウィンドウが表示されます。

ステップ 2　トンネル SR を削除するために、削除する SR を選択し、[Delete] をクリックします。

管理対象外トンネルの [Op] フィールドのステータスが [DELETE] に変わります。

さまざまなウィンドウ要素の説明については、「バックアップ トンネルの作成」（P.7-40）を参照してください。

（注）　削除したトンネルは、トンネルを選択して [Delete] をクリックすることにより、元の状態に戻すことができます。[Op] 列の [DELETE] フラグが消えます。

[Save & Deploy] をクリックして、新規トンネル SR をネットワークに展開するかすべてのトンネルを強制的に展開します。または、プライマリ トンネルをさらに作成または編集してからすべての変更を保存および展開することもできます。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が表示され、展開済みの SR の状態が表示されます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

サービス要求の削除

[Service Request Manager] ウィンドウにある [Purge] 操作は、ネットワークに影響を与えることなくリポジトリからサービス要求を削除することを目的としています。

[Purge] ボタンには 2 つのオプションがあります。

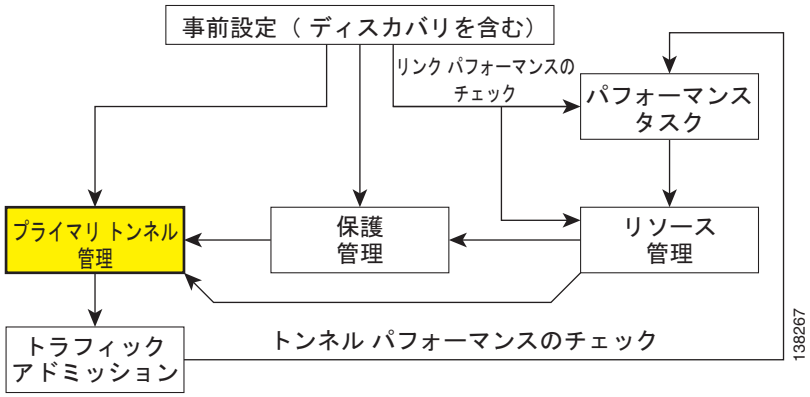
- [Purge]：通常の削除は、[CLOSED] 状態にあるサービス要求のみに使用できます。したがって、TE リソース、TE トンネル、および TE 保護サービス要求に対しては使用できません。これらは撤去できないためです。これらの 3 つのサービス要求タイプは、強制削除のみ可能です。
- [Force Purge]：強制削除では、リポジトリでサービス要求に対する必要な依存関係を検査してから削除が可能になります。したがってサービス要求を削除できない場合は、エラー メッセージが出されます。

高度なプライマリ トンネル管理

「基本的なトンネル管理」（P.7-28）で説明している基本的なトンネル管理ツールに加え、Prime Provisioning では、最適なトンネル配置を実現し、ネットワーク リソースの効率的な使用を保証する、一連の高度なトンネル計画ツールにアクセスできます。

図 7-3 で強調表示されているボックスは、Prime Provisioning のプライマリ トンネル管理が発生した場所を示します。

図 7-16　Prime Provisioning プロセス図：プライマリ トンネル管理



高度なツールは、管理対象のトンネルにのみ使用できます。管理対象トンネルと管理対象外トンネルの違いは、「トラフィック エンジニアリング管理の概念」（P.7-115）の管理対象 / 管理対象外プライマリ トンネルの項で説明します。

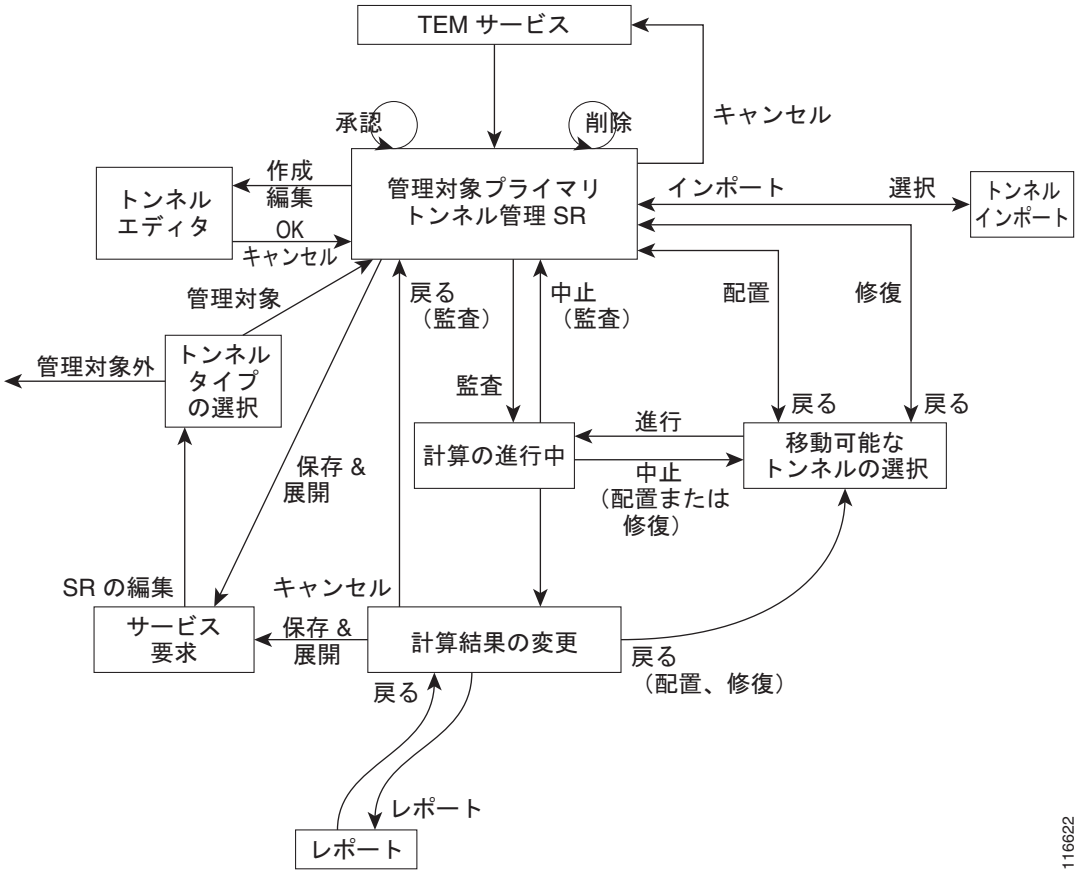
ここでは、次の内容について説明します。

トンネル操作

ここでは、計画ツールを組み込む Prime Provisioning の高度なトンネル操作について説明します。

プライマリ トンネル管理プロセスの概要については、図 7-17 を参照してください。

図 7-17　プライマリ トンネル管理プロセス



[Tunnel Type Selection] で、[Unmanaged] を選択していると [TE Unmanaged Primary Tunnel SR] ウィンドウが表示されます（「基本的なトンネル管理」（P.7-28）を参照）。

図 7-17 のその他のすべての要素は、この項で説明します。

プライマリ トンネルの作成

RG ライセンスがインストールされた状態で TE 管理対象プライマリ トンネルを作成するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] を選択します。

ステップ 2　[Create Managed TE Tunnel] をクリックします。

[TE Managed Primary Tunnels SR] ウィンドウが表示されます。

さまざまなウィンドウ要素の説明については、「プライマリ トンネルの作成」（P.7-33）を参照してください。

ステップ 3　[Create] をクリックします。

[Create TE Managed Primary Tunnel] ウィンドウが表示されます。

さまざまなウィンドウ要素の説明については、「プライマリ トンネルの作成」（P.7-33）を参照してください。

[Path Options] セクションには、3 つのパス タイプ [System Path]、[Explicit Path]、および [Dynamic Path] が示されます。

[System Path] は、Prime Provisioning システムによって生成される明示的パスです（固定）。最初のパスは明示的パスでなければなりません。

[Explicit Path] は、特定のヘッドから特定の宛先デバイスへの固定パスです。

[Dynamic Path] は、ヘッド ルータによるパスの検出を許可することによってプロビジョニングされます。**dynamic** キーワードは、ルータにプロビジョニングされます。

ステップ 4　[Head Device] を選択するために、対応する [Select] ボタンをクリックしてデバイス選択ウィンドウを開きます。

ヘッド デバイスを選択し、[Select] をクリックします。

ステップ 5　[Destination Device] を選択するために、対応する [Select] ボタンをクリックしてデバイス選択ウィンドウを開きます。

テール デバイスを選択し、[Select] を選択します。

ステップ 6　[Tunnel Policy] を選択するために、対応する [Select] ボタンをクリックしてポリシー選択ウィンドウを開きます。

（注）　使用可能なトンネル ポリシーがない場合、その理由は、すべてが管理対象外である可能性があります。管理対象トンネルを作成するには、[Managed] チェックボックスを必ずオンにして、まず、[Service Design] > [Policy Manager]（「ポリシーの作成」（P.7-73）を参照）で管理対象ポリシーを作成します。

[Select Managed TE Tunnel Policy] ウィンドウには、次の要素が含まれています。

- [Policy Name]：TE ポリシー名。
- [Pool Type]：このポリシーのトンネル帯域幅プール タイプ。プール タイプの定義については、「トラフィック エンジニアリング管理の概念」（P.7-115）で帯域幅プールの項を参照してください。
  - [SUB_POOL]：帯域幅は、サブ プールから予約されます。
  - [GLOBAL]：帯域幅は、グローバル プールから予約されます。
- [Setup Priority]：優先する既存のトンネルを判別するために、トンネルの LSP をシグナリングするときに使用される優先順位。有効な値は 0 ～ 7 であり、数字が小さいほど優先順位は高くなります。したがって、セットアップ プライオリティが 0 の LSP は、0 以外の保持プライオリティのすべての LSP より優先されます。
- [Hold Priority]：シグナリングされている他の LSP の方を優先的に取得する必要があるかどうかを決定するため、トンネルの LSP に関連付けられた優先順位。有効な値は 0 ～ 7 であり、数字が小さいほど優先順位は高くなります。
- [Affinity]：トンネルを伝送するリンクで必要な属性値（ビット値は 0 または 1 のいずれか）。
- [Affinity Mask]：チェックする属性値。マスクのビットが 0 の場合、そのビットに対応するリンクの属性値は関連しません。マスクのビットが 1 の場合、そのビットに対するリンクの属性値とトンネルに必要なアフィニティは一致する必要があります。
- [Delayed Constraint]：True または False の値。true の場合、トンネルには、パスが超えてはならない最大遅延があります。
- [FRR Protection]：バックアップ トンネルが存在しており、リンク障害が発生した場合に、MPLS トラフィック エンジニアリング トンネルで、バックアップ トンネルの使用をイネーブルにするために使用します。
  - [None]：バックアップ トンネルは必要ありません。
  - [Best Effort]：可能な場合に、バックアップ トンネルを使用します。

- [Link and SRLG (only managed tunnels)] : FRR バックアップ トンネルで保護されるリンクと SRLG だけを通じて、プライマリ トンネルをルーティングする必要があることを指定します。
- [Link, SRLG and Node (only managed tunnels)] : FRR バックアップ トンネルで保護されるリンク、SRLG、およびノードだけを通じて、プライマリ トンネルをルーティングする必要があることを指定します。

• [MPLS IP Enabled] : MPLS IP が対応するトンネルで設定されているかどうかを示します。

ステップ 7　ゼロより大きいトンネル帯域幅を指定します。

ステップ 8　必要に応じて他のトンネル情報を追加します。

ステップ 9　オプションで、Prime Provisioning によって提供されるシステム パスを使用せずに、明示的パスを指定したい場合は、システム パスを削除し、次に明示的パスを追加します。

このステップの詳細については、「プライマリ トンネルの作成」（P.7-33）を参照してください。

ステップ 10　[Create TE Managed Tunnel] ウィンドウで、[OK] をクリックして入力したトンネル情報を受け入れるか、[Cancel] をクリックして終了し、[TE Managed Primary Tunnels SR] ウィンドウに戻ります。

SR が追加されたことを示す [ADD] を [Op] フィールドに設定した新規トンネルを表示している [TE Managed Primary Tunnel SR] ウィンドウが表示されます。

（注）　追加したトンネルは、トンネルを選択して [Delete] をクリックすることにより、元の状態に戻すことができます。トンネル リストからトンネルが削除されます。

ステップ 11　[TE Managed Primary Tunnel SR] ウィンドウで、より多くのトンネルを作成または編集できます。また、すべての変更が完了した場合は、次のどちらのボタンがアクティブであるかに応じて、次の 2 つの方法のいずれかに進みます（[Save & Deploy] は、[Create] 操作の後は使用できません）。

- [Proceed with Changes] : 入力した変更は、トンネル配置に影響を与えます。SR を保存および展開できるまで、配置ツールに記載されている計画フローのいずれか（「配置ツール」（P.7-54）を参照）を使用して続行するには、これをクリックします。
- [Save & Deploy] : 入力した変更は、トンネル配置に影響を与えません。SR を保存および展開するには、これをクリックします。この機能は、「プライマリ トンネルの作成」（P.7-33）で詳細に説明されています。

[Save & Deploy] をクリックすると、影響を受ける TE ルータが Prime Provisioning によってロックされます。これにより、SR が終了するまで、その TE ルータを使用する後続のすべての SR はブロックされます。システム内の他の SR は、安全に試行および展開できます。処理中の SR と競合する場合、Prime Provisioning では、単に完了まで待機することを要求します。展開の状態を確認するには、[Inventory and Connection Manager] の [Service Requests] ウィンドウに移動するか、[Monitoring] の [Task Manager] を開きます。

（注）　TE トラフィック アドミッション SR を除き、TE SR は、[Inventory and Connection Manager] の [Service Requests] ページではなく、常に特定の [TE SR] ウィンドウから直接展開されます。

ステップ 11 で [Save & Deploy] を選択した場合、[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が開き、展開済みの SR の状態が表示されます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

（注）　TE トンネルの展開中に Elixir 警告が表示されることがあります。展開は正常に行われ、警告メッセージは無視しても安全です。

SR が [Deployed] 状態にならない場合は、[Task Logs] ウィンドウに移動し、「タスク ログ」（P.10-29）の説明に従って展開ログ（[Operate] > [Task Manager] > [Logs]）を参照してください。

プライマリ トンネルの編集

トンネルの作成と編集の唯一の違いは、トンネル エディタでは、ヘッド デバイス、宛先デバイス、およびトンネル番号のフィールドを編集できないことです。それ以外の場合は、同じ属性を作成および編集できます。

入力した変更がトンネル配置に影響するかどうかに応じて、両方ではなく、[Proceed with Changes] または [Save & Deploy] だけが使用可能です。

プライマリ トンネルを編集する場合は、「プライマリ トンネルの編集」（P.7-38）を参照してください。

プライマリ トンネルの削除

1 つ以上のトンネルを削除するには、「プライマリ トンネルの削除」（P.7-40）を参照してください。

プライマリ トンネルのアドミッション

アドミッション機能は、選択した以前検証されていないトンネルを管理対象トポロジにアドミッションします。この機能は、検証が失敗した検出済みのトンネルにのみ使用します。ディスカバリ プロセスでは、トンネルを初めてアドミッションすると想定し、トンネル配置アルゴリズムによって検証が実行されます。

ここでいう検証は、検出された管理対象トンネルをネットワーク トポロジと照合して検証することおよび十分な帯域幅のあるトンネル パスであるかどうかを TEM によって検査すること（いずれもトンネルに指定）を意味します。

一般的に、他のトンネルまたはリンク キャパシティ / 帯域幅の制限の存在が原因で、帯域幅が十分ではない場合、検証が失敗します。

具体的には、これは、優先順位 0 のトンネルが TEM とは独立して作成され、TE 検出タスクが実行された場合に発生する可能性があります。管理対象トンネルの制約の一部を満たさない（つまり、通過するリンクで使用可能な帯域幅より多い帯域幅を予約する）トンネルの場合、TE ディスカバリでは、そのトンネルの「verified」に「false」とマークします。これは、[Admit] ボタンを使用して検証が行われるまで、TEM による管理対象になりません。通常、制約が現在満たされていることを保証するために、これには他のトンネルまたはリソース変更が伴う必要があります。

プライマリ トンネルのアドミッションを行うには、次のステップを実行します。

ステップ 1　[TE Managed Primary Tunnel SR] で、移行する 1 つ以上の未検証のトンネルを選択します。

ステップ 2　[Admit] をクリックします。

未検証のトンネルが検証され、成功した場合は、[Op] 列に [ADMIT] フラグが表示されます。

ステップ 3　[Proceed with Changes] > [Tunnel Placement] を選択して、トンネルを配置できるかどうかを判別します。そうでない場合は、トンネルを編集し、再度試行します。

プライマリ トンネルのインポート

この機能を使用すると、ファイルベースのインポート メカニズムを介してトンネルを一括して更新することができます。データは、管理対象プライマリ トンネル サービス要求に移行されます。

XML インポート ファイルの作成

ファイルからトンネルをインポートするには、まず、システムが提供する文書型定義（DTD）ファイル（「ドキュメント タイプ定義（DTD）ファイル」（P.7-112）を参照）で定義された構造に準拠している XML インポート ファイルを作成します。次に、Prime Provisioning サーバで、同じディレクトリに DTD ファイルとともに XML ファイルを保存します。有効なインポート ファイルを作成するには、提供されたコマンドライン検証ツール（「コマンドライン検証ツール」（P.7-52）を参照）を使用します。

次のファイルは、Prime Provisioning アプリケーションへのデータのインポートに必要であり、インストールに含まれています。

- 次にあるインポート ファイルの DTD ファイル
  < *installedDir*>/ *resources/java/xml/com/cisco/vpnsc/ui/te*
  - **TeImport.dtd**

    （サンプル ファイル **sample.xml** も含まれます）
- <*installedDir*>*/bin* ディレクトリでコマンドライン バリデータを実行するためのシェル スクリプト
  - **ImportTeTunnels**

    使用方法：**importTeTunnels <***importfile***>**

importfile は XML ファイルであり、**TeImport.dtd** をその DTD として指定する必要があります。**TeImport.dtd** は、*importfile* と同じディレクトリにある必要があります。

コマンドライン検証ツール

コマンドライン バリデータの目的は、**TeImport.dtd** に対応する有効なインポート ファイルのオフラインでの作成を支援することです。このツールは、整形式でないファイルおよび DTD によって設定されるルールに準拠していないファイルに関連するエラーを排除するために有用です。

DTD ファイルの使用法については、DTD ファイルのマニュアルを参照してください。

ツールはインポート ファイルを行単位で読み取り、解析時に出力上で各行をエコーし、発生した解析エラーをレポートします。解析および検証は、解析エラーが発生した場合であっても、ファイル構造が意味を持つ限り続行されます。

（注） このツールでは、クロス フィールド検証を行わず、Prime Provisioning アプリケーションの観点からのデータ完全性エラーを検査しません。

インポート手順

ファイルベースのインポート機能は、サービス要求にコミットされていない新規のトンネル、変更されたトンネル、削除されたトンネルが存在しない場合のみイネーブルになります。

多数のトンネルを一度に追加、編集、削除、または移行できます。

インポート手順を開始するには、次のステップを実行します。

ステップ 1　DTD ファイルに準拠した XML インポート ファイルを準備します。

ステップ 2　[Traffic Engineering] に移動します。

ステップ 3　このセッションでまだプロバイダーを選択していない場合は、プロバイダーを選択します。

ステップ 4　[Create Managed TE Tunnel] をクリックします。

[TE Managed Primary Tunnels SR] ウィンドウが表示されます。

ステップ 5　[Import] をクリックし、インポート プロセスを開始します。

[Select Import File] ウィンドウが表示されます。

（注）　[Import] ボタンは、サービス要求にコミットされていない新規のトンネル、変更済みのトンネル、または削除されたトンネルが存在する場合のみイネーブルになります。

[Select Import File] ウィンドウには、[Look in] フィールドに表示されるディレクトリ名の下に、すべての XML ファイルとディレクトリが示されます。

[Look in] フィールドに表示されているデフォルト ディレクトリは、DTD およびサンプル XML ファイルが存在するインストール ディレクトリに対応します。

ステップ 6　インポート操作で使用する、必要な XML ファイルを選択します。

ファイルが解析されます。何らかのエラーが検出された場合は、[Tunnel Import Error Status] ウィンドウに報告されます。

[Tunnel Import Error Status] ウィンドウに、ファイルの URL、最後に変更されたタイムスタンプ、インポート ステータス、およびエラー / 警告メッセージが表示されます。

ステップ 7　インポート操作が失敗した場合は、[Cancel] をクリックして前のウィンドウに戻ります。

部分的に成功した場合は、[Continue] ボタンがイネーブルになるため、エラーおよび警告に対するシステム処置を受け入れる追加のオプションを指定して、インポート操作を続行します。

ステップ 8　ファイルが正常に解析された、または [Continue] をクリックした場合、ファイルのすべての有効なトンネルがサービス要求に追加され、SR ビューで [TE Managed Primary Tunnels SR] ウィンドウが再表示されます。インポートされたトンネルが、適切なトンネル **Op** タイプと表示されます。

計画ストラテジ

計画ツールを使用する主な目的は、ネットワーク上の既存のトラフィックへの影響の発生を最小限にする一方で、ネットワーク全体の最適な利用を実現することです。

ほとんどの場合、次のストラテジを適用できます。

- 既存トラフィックを移動させないで、使用率を最適化しながら新規トラフィックのアドミッションを試行する（配置機能）。これにより、既存のトラフィックを変更せずに、新しいトラフィックに適応することが可能になります。一方で、予約済み帯域使用率は、既存のトンネルを移動しない制約のもとで引き続き最適化されます。
- これが失敗した場合、変更を最小化する同じ新しいトラフィックの既存のトラフィックへのアドミッションを試行し（修復機能）、必要以上に既存のトンネルに影響を与えずに新しいトラフィックを適応できるかどうかを確認します。
- 新しいネットワーク トラフィックの配置が成功したが、希望よりも全体の予約済み帯域使用率が高い場合は、ネットワークのグルーミングを検討してください。
- 修復に失敗する場合は、検討可能な変更の数を制御するパラメータを確認します。また、希望のトラフィックへの指定は変更でき、リソースの変更を実行できます。

このストラテジは、ソリューションを探求するさまざまなアルゴリズムで採用されているさまざまなアプローチを反映します。ただし、他の組み合わせが可能です。

配置ツール

プライマリ トンネルの計画ツールは、変更が管理対象プライマリ トンネルに行われたかどうかによって、[TE Primary Tunnel SR] ウィンドウの [Proceed with Changes] および [Placement Tools] ボタンから使用できます。

- [Proceed with Changes]：トンネルに変更（追加/変更/削除/アドミッション）を加えている場合に使用します。トンネル操作については、「トンネル操作」（P.7-47）を参照してください。次に、いずれかの配置ツールを選択して、システムと照合しながら初期配置を検証して展開を続行します。このボタンは、[Resource Management] でも使用可能です。
- [Placement Tools]：既存のネットワークの計画機能を実行するために使用されます。
  - [Tunnel Audit] オプションは、既存の管理対象プライマリ トンネルの制約ベースの配置と既存のネットワーク トポロジを検証するために使用する必要があります。このオプションを使用して、プライマリ配置の最適性を確認することができます。プライマリ トンネルで「ベスト エフォート」より上の保護レベルが必要な場合は、保護ネットワークで変更が行われた後に、監査を実行することも重要です。監査の結果が警告/違反の場合は、[Tunnel Repair] オプションを使用して、ソリューションを見つけることができます。
  - [Groom] オプションは、プライマリ配置の最適化に使用します。すべてのプライマリの計算において、帯域幅プールの最適性および使用率を表示する品質レポートが生成されます。まず、トンネル監査を実行して、ネットワークでグルーミングが必要かどうかを判断することができます。

計画ツールの詳細については、次の項で説明します。

（注）　配置ツール（auto-bw frequency など）でサポートされていないトンネル属性がサポートされている属性とあわせて変更された場合は、[TE Computation Results] ウィンドウに属性が正しく表示されます。ただし、サポートされていない属性のみが変更された場合、[TE Computation Results] ウィンドウには行われていない変更のみが表示され、変更を展開できないように [Save & Deploy] ボタンはグレー表示されます。

トンネル監査

トンネルの変更または TE リソースの変更の任意のタイプの変更が必要な場合は、変更によって生じる不一致（ある場合）を判断するためにトンネル監査が実行されます。また、トンネル監査は、ネットワーク利用の最適化を確認するためにいつでも使用できます。

監査は、プライマリ トンネル ウィンドウからか [TE Links List] ウィンドウから実行できます。（「TE リソース管理」（P.7-21）を参照）。

作成したトンネルで監査を実行するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] を選択します。

ステップ 2　[Create Managed Tunnel] をクリックします。

[TE Managed Primary Tunnels SR] ウィンドウが表示されます。

トンネル監査は、次の 2 つの方法で使用できます。

- 1 つ以上のトンネルを作成したか、その属性を変更した場合は（「プライマリ トンネルの作成」（P.7-48）を参照）、[Proceed with Changes] を選択することによってトンネル監査をアクティブにできます。
- 変更が行われていない場合、[Placement Tools] を選択することによってトンネル監査にアクセスできます。

この例では、新規プライマリ トンネル SR が作成されています。

[TE Managed Primary Tunnel SR] ウィンドウが表示されます。

ステップ 3　[Proceed with Changes] > [Tunnel Audit] を選択します。

[Computation In Progress] ウィンドウが一時的に表示されます。[TE Primary Tunnel Computation Results - Changes] ウィンドウが表示されます。

このウィンドウには、次の要素が含まれます。

[Status] セクション（上部）

- [Computation Status]：計算が、成功したか、または失敗したかを示します。
- [Tunnels]：
  - [unplaced]：合計内で、配置されていないトンネルの数。
  - [moved]：移動されたトンネルの数。
- [Bandwidth - unplaced]：すべての既存および新規トンネルの合計帯域幅の内、配置されていないトンネル帯域幅の量。
- [Global Util.]：グローバル プール帯域利用率。

  使用率の値は、次のいずれかです。
  - [Global Pool]：さまざまなグローバル プール属性の比較データ。
  - [Sub Pool]：さまざまなサブ プール属性の比較データ。
  - [Median]：すべてのリンクを使用率で順序付けした場合に、中間であるリンクの使用率。
  - [Max. Modifiable]：通過する移動可能なトンネルがあり、最も使用されているリンクの使用率の値。
  - [Mean]：ネットワーク全体の平均リンク使用率。
  - [Max.]：トポロジ内で最も使用されているリンクの使用率の値。
- [Sub Pool Util.]：サブプール帯域利用率。
- [Solution]：生成されたソリューションの使用率。
- [Original]：元の配置の使用率。

[Changes] セクション（左方）

- [Changes]：変更の合計数の内、実現した変更の数。
  - [Achieved]：特定の変更が成功したかどうかを示します（[Yes] または [No]）。
  - [Origin]：変更の実行元。[user]（ユーザによる変更）または [compute]（トンネルの再ルーティングなどの計算による変更）にすることができます。
  - [Type]：要求された変更のタイプ（[Tunnel Add Change]、[Tunnel Modify Change]、[Tunnel Remove Change]、または [Element Modify Change]）。
  - [Object ID]：トンネルまたはリンクの ID。

（注）　説明など特定の属性は配置ツールの実行する計算に影響せず、これらの属性に対する更新は計算結果ウィンドウに表示されません。

ステップ 4　トンネルの詳細情報を取得し、変更要求が達成されたかどうかを確認するには、具体的なトンネルを選択し、[Details] をクリックします。

qualityReport は常に生成されます。計算が正常に完了すると、これはレポートのみになります。

警告または違反が発生した場合は、1 つ以上の警告または違反のレポートも生成されます。

ステップ 5　監査レポートを表示するには、[View Report] をクリックします。

場合によっては、qualityReport と違反レポートの両方が生成されます。

ステップ 6　**qualityReport** の内容を表示するには、**qualityReport** を選択し、[Details] ボタンをクリックします。

右ウィンドウ ペインの qualityReport フィールドには、次の要素が含まれます。

[Status] セクション（上）：上に説明があります。

[Report] セクション（左）：

- [Report Type]：**qualityReport**（毎回生成されます）、警告レポート、および違反レポートの 3 種類の基本的なレポート タイプがあります。
- [Summary Info]：レポートの結果に関するサマリー情報。

[Information] セクション（右）

- [Report Type]：上記の説明を参照してください。
- [Description]：レポートに関する特定の情報。
- [Achievement]：計算の試行やソリューションの成功または失敗（**SUCCESS** または **CONSTRAINT_VIOLATIONS_REPORTED**）。
- [Solution]：ソリューションが見つかったかどうかを示します（**SOLUTION_FOUND**、**PARTIAL_SOLUTION_FOUND** または **NO_SOLUTION_FOUND**）。
- [Termination]：計算が完了したかどうかを示します。
  - [COMPLETED]：計算の処理は、制限時間の前に完了しました。
  - [TIMED_OUT]：計算の処理は、時間制限内に完了できませんでした。表示されるソリューションは、使用可能な時間内に検出できた最善のソリューションです。
- [Optimality]：計算が最適であったかどうかを示します。
  - **OPTIMAL_FOR_ALL_CRITERIA**：生成されるソリューションは、すべての最適化基準で最適であることが実証されています。
  - **NO_OPTIMALITY_PROOF**：ソリューションの最適性が不明です。
  - **OPTIMAL_FOR_DEMAND_SELECTION**：生成されたソリューションは、配置された合計帯域幅に関して最適であることが証明されましたが、使用率の最適性は不明です。

OPTIMAL_FOR_SUB_POOL_PATH_SELECTION：生成されたソリューションは、配置された合計帯域幅と最大サブ プール使用率に関して最適であることが証明されましたが、グローバル プールの使用率に関して最適であることは証明されませんでした。

ステップ 7　違反レポートの内容を表示するには、違反レポートを選択し、[Details] ボタンをクリックします。

[TE Primary Tunnel Computation Results - Report]（詳細）ウィンドウが表示されます。

各レポートの右側のウィンドウ ペインのレポート フィールドについては、「警告および違反」（P.7-102）を参照してください。

ステップ 8　[View Result] をクリックして [Changes] ウィンドウに戻ります。

提示された変更が行われた場合は、[Save & Deploy] をクリックして実現可能な変更をリポジトリに保存し、ネットワークにトンネルの変更を実装します。

（注）　[Save & Deploy] では、実現不可能な変更は破棄されます。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が表示され、展開済みの SR の状態が表示されます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

トンネル配置

配置機能は、ネットワークへの新規のトンネルのアドミッション、およびネットワークへのアドミッションがすでに行われている変更をサポートしています。 Prime Provisioning は、ネットワーク利用が最適化される方法で、変更の実装を試行します。

作成したトンネルを配置するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] を選択します。

ステップ 2　[Create Managed TE Tunnel] をクリックします。

[TE Managed Primary Tunnels SR] ウィンドウが表示されます。

ステップ 3　1 つ以上のトンネルを作成したか、その属性を変更した場合は（「プライマリ トンネルの作成」（P.7-48）を参照）、[Proceed with Changes] > [Tunnel Placement] を選択します。

[Movable Tunnel Selection (Placement)] ウィンドウが表示されます。

ステップ 4　移動可能または移動不能な管理対象トンネルを設定します。

新規のトンネルのアドミッションを行う場合は、既存のトンネルを移動（リルート）できるかどうかを指定できます。ユーザが設定できます。デフォルトでは、管理対象トンネルは移動不能です。

ステップ 5　[Proceed] をクリックします。

[Computation In Progress] ウィンドウが一時的に表示されます。[TE Primary Tunnel Computation Results - Changes] ウィンドウが表示されます。

（注）　説明など特定の属性は配置ツールの実行する計算に影響せず、これらの属性に対する更新は計算結果ウィンドウに表示されません。

ステップ 6　トンネルの詳細情報を取得し、配置要求が達成されたかどうかを確認するには、具体的なトンネルを選択し、[Detail] をクリックします。

ウィンドウの右側に、[Detail] セクションが表示されます。

配置リクエストが正常に完了した場合（[Achieved] : yes）、[Detail] ペインには選択可能な計算済みの**パス**が含まれます。

パス情報を表示するには、計算された [Path] フィールドの青色のリンクをクリックします。[TE Explicit Path] ウィンドウが表示されます。

ステップ 7　配置レポートを表示するには、[Changes] ウィンドウの [View Report] をクリックします。

[TE Primary Tunnel Computation Results - Report] ウィンドウが表示されます。

qualityReport は常に生成されます。計算が正常に完了すると、これはレポートのみになります。

警告または違反が発生した場合は、1 つ以上の警告または違反のレポートも生成されます。

ステップ 8　配置レポートの内容を表示するには、レポートのいずれかを選択し、[Details] ボタンをクリックします。

qualityReport の場合、[TE Primary Tunnel Computation Results - Report]（詳細）ウィンドウが右側のレポート ペインに表示されます。

ステップ 9　[View Result] をクリックして [Changes] ウィンドウに戻り、[Save & Deploy] をクリックして変更をリポジトリに保存し、トンネルの変更をネットワークに実装します。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が表示され、展開済みの SR の状態が表示されます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

トンネル修復

既存のトンネルの帯域幅要件または遅延パラメータに変更が行われると、トンネル配置に不一致が生じます。トンネル修復を実行して、このような不一致に対処できます。トンネル修復は、できるだけ少ない既存のトンネルを移動して、変更に対応できるようにすることを目的としています。

修復操作は、プライマリ トンネル ウィンドウからか [TE Links List] ウィンドウから実行できます（「TE リソース管理」（P.7-21）を参照）。

次では、編集済みトンネルの修復を行います。

ステップ 1　[Traffic Engineering] > [Create Managed Tunnel] を選択します。

[TE Managed Primary Tunnels SR] ウィンドウが表示されます。

トンネル修復は、次の 2 つの方法で使用できます。

- 1 つ以上のトンネルを作成したか、トンネルの属性を変更した場合は（「プライマリ トンネルの作成」（P.7-48）を参照）、[Proceed with Changes] > [Tunnel Repair] を選択することによってトンネル修復をアクティブにできます。
- 変更が行われていない場合、トンネル修復には、[Placement Tools] > [Tunnel Repair] を選択してアクセスできます。

ステップ 2　この例では、新規プライマリ トンネル SR が作成されています。

[TE Managed Primary Tunnels SR] ウィンドウから変更したトンネル上でトンネル修復を実行します。これには、次のように移動します。

[Proceed with Changes] > [Tunnel Repair]

[Movable Tunnel Selection] ウィンドウが表示されます。

ステップ 3　移動可能にする必要のあるトンネルを設定します。

トンネル修復は、必要な場合に限り、既存のトンネルを移動します。トンネル修復で移動しない特定のトンネルがある場合は、そのトンネルを移動可能なトンネルの選択リストから明示的に除外する必要があります。

[Maximum number of tunnel moves] フィールドを使用して、受け入れ可能なトンネル移動の最大数の制限を指定することもできます。

（注）　デフォルトでは、変更済のトンネルを移動可能に設定する必要はありません。

ステップ 4　[Proceed] をクリックします。

[Computation In Progress] ウィンドウが一時的に表示されます。[TE Primary Tunnel Computation Results - Changes] ウィンドウが表示されます。

（注）　説明など特定の属性は配置ツールの実行する計算に影響せず、これらの属性に対する更新は計算結果ウィンドウに表示されません。

ステップ 5　トンネルの詳細情報を取得し、変更要求が達成されたかどうかを確認するには、具体的なトンネルを選択し、[Detail] をクリックします。

ウィンドウの右側に、[Detail] セクションが表示されます。

ステップ 6　修復レポートを表示するには、[View Report] をクリックします。

[TE Primary Tunnel Computation Results - Report] ウィンドウが表示されます。

qualityReport は常に生成されます。計算が正常に完了すると、これはレポートのみになります。

警告または違反が発生した場合は、1 つ以上の警告または違反のレポートも生成されます。

ステップ 7　修復レポートの内容を表示するには、[Details] ボタンをクリックします。

qualityReport の場合、[TE Primary Tunnel Computation Results - Report]（詳細）ウィンドウが表示されます。

各レポートの右側のウィンドウ ペインのレポート フィールドについては、「警告および違反」（P.7-102）を参照してください。

ステップ 8　[View Result] をクリックして [Changes] ウィンドウに戻り、[Save & Deploy] をクリックして変更をリポジトリに保存し、トンネルの変更をネットワークに実装します。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が表示され、展開済みの SR の状態が表示されます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

グルーミング

グルーミングは、ネットワーク要素に関してトンネルのパスを分析することと、リソース割り当てを最適化することを目的としています。

グルーミングは、変更要求が作成されている場合は使用できません。その場合は、[Proceed with Changes] の下の配置ツールだけが使用可能です。

ネットワークでグルーミングを実行するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [Create Managed TE Tunnel] を選択します。

[TE Managed Primary Tunnels SR] ウィンドウが表示されます。

ステップ 2　次に移動して、グルーミングを実行します。

[Placement Tools] > [Groom]

[Movable Tunnel Selection] ウィンドウが表示されます。

ステップ 3　移動可能にする必要のあるトンネルを設定します。

トンネル修復では、グルーミングは必要な場合にのみ既存のトンネルを移動します。グルーミング処理で移動しない特定のトンネルがある場合は、そのトンネルを移動可能なトンネルの選択リストから明示的に除外する必要があります。

ステップ 4　[Proceed] をクリックします。

[Computation In Progress] ウィンドウが一時的に表示されます。[TE Primary Tunnel Computation Results - Changes] ウィンドウが表示されます。

（注）　説明など特定の属性は配置ツールの実行する計算に影響せず、これらの属性に対する更新は計算結果ウィンドウに表示されません。

ステップ 5　グルーミングの詳細情報を取得し、グルーミングが成功したかどうかを確認するには、具体的なトンネルを選択し、[Detail] をクリックします。

ウィンドウの右側に、[Detail] セクションが表示されます。

ステップ 6　グルーミング レポートを表示するには、[View Report] をクリックします。

[TE Primary Tunnel Computation Results - Report] ウィンドウが表示されます。

qualityReport は常に生成されます。計算が正常に完了すると、これはレポートのみになります。

警告または違反が発生した場合は、1 つ以上の警告または違反のレポートも生成されます。

ステップ 7　グルーミング レポートの内容を表示するには、[Details] ボタンをクリックします。

qualityReport の場合、[TE Primary Tunnel Computation Results - Report]（詳細）ウィンドウが表示されます。

各レポートの右側のウィンドウ ペインのレポート フィールドについては、「警告および違反」（P.7-102）を参照してください。

ステップ 8　[View Result] をクリックして [Changes] ウィンドウに戻り、[Save & Deploy] をクリックして変更をリポジトリに保存し、トンネルの変更をネットワークに実装します。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が表示され、展開済みの SR の状態が表示されます。

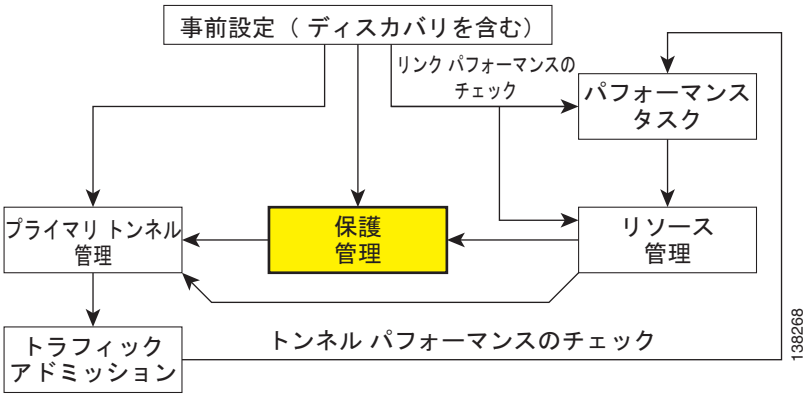
サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

保護計画

ここでは、自動保護ツールを使用してネットワーク要素の保護を作成および管理するプロセスについて説明します。基本的なツールを使用するこのプロセスについては、「基本的なトンネル管理」（P.7-28）を参照してください。

図 7-18 で強調表示されたボックスは、保護管理が Prime Provisioning のどこで行われるかを示しています。

図 7-18　Prime Provisioning プロセス図：保護管理



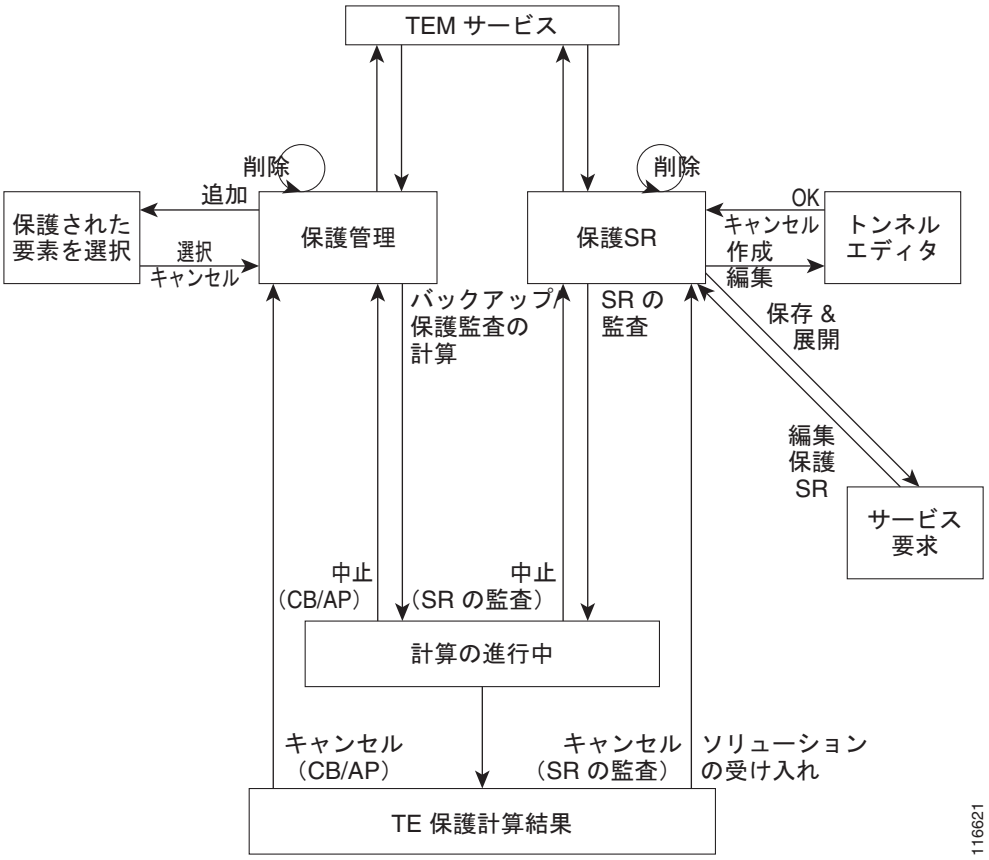
保護計画では、ネットワーク内の選択した要素（リンク、ルータ、または SRLG）を障害から保護することを目的としています。

最初の手順では、保護する必要がある要素を特定し、保護ツールを呼び出して、保護されたトンネルを計算します。計算によって、システムは、要素を保護する一連のトンネル、または保護できなかった理由を判断するために役立つ一連の違反と警告のいずれかとともに、各要素に対して応答します。

正常に保護された要素の場合は、トンネルをネットワークに展開できます。保護できない要素の場合は、保護が無視されるか、保護の場合に制約が変更されます。より具体的には、要素に関連付けられたリンクの TE 帯域幅設定が変更され、変更されたネットワークで保護の計算が再実行されます。

保護管理プロセスの概要は、図 7-19 で提供されます。

図 7-19　保護管理プロセス



ここでは、次の内容について説明します。

- 「SRLG 操作」（P.7-62）
  - 「SRLG の作成」（P.7-63）
  - 「SRLG の編集」（P.7-63）
  - 「SRLG の削除」（P.7-63）
- 「要素保護の設定」（P.7-64）
- 「保護ツール」（P.7-64）
  - 「バックアップ計算」（P.7-65）
  - 「保護監査」（P.7-66）
  - 「監査 SR」（P.7-67）。

SRLG 操作

リンクの物理的特性が同一になることがあります（同じコンジットに物理的に存在する場合や同じハードウェアに接続される場合など）。この結果、単一の障害発生時に、これらのリンクがグループとして失敗することがあります。共有リスク リンク グループ（SRLG）は、一緒に失敗することがあるリンクを特定してこの問題を解決します。

SRLG の変更（作成、編集、削除）後に、[TE Protection Management] ウィンドウで保護計画機能を使用して、適切な保護がネットワークで利用可能になるようにします。

SRLG の作成

SRLG の作成は、共有リスク リンク グループが特定され、共有リスク リンク グループを保護する必要がある場合にのみ必要です。

SRLG を作成するには、次の手順を実行します。

ステップ 1　[Traffic Engineering] > [SRLGs] を選択します。

[TE SRLG List] ウィンドウが表示されます。

ステップ 2　[TE SRLG List] で SRLG を作成するには、[Create] をクリックします。

[TE SRLG Editor] ウィンドウが表示されます。

ステップ 3　[SRLG Name] を指定します。

ステップ 4　[Add Link] をクリックします。

SRLG ウィンドウに関連付けられたリンクが表示されます。

ステップ 5　1 つまたは複数のリンクを選択し、[Select] をクリックします。

対応するリンク情報がリンク リストに追加され、[Select] ウィンドウが閉じられて、SRLG エディタに戻ります。

ステップ 6　[Save] をクリックして SRLG を保存します。

これにより、SRLG エディタが閉じられ、新しく作成された SRLG がリストされた [TE SRLG List] がアクティブ ウィンドウとして表示されます。

SRLG の編集

SRLG を編集するには、次の手順を実行します。

ステップ 1　[Traffic Engineering] > [SRLGs] を選択します。

[TE SRLG List] ウィンドウが表示されます。

ステップ 2　TE SRLG リストの SRLG を編集するために、[TE SRLG List] ウィンドウから変更する SRLG を選択し、[Edit] をクリックします。

[TE SRLG Editor] ウィンドウが表示されます。

ステップ 3　[Add Link] と [Remove Link] を使用して、選択された SRLG の必要なリンク セットに調整します。

ステップ 4　変更を保存するには、[Save] をクリックします。

SRLG の削除

SRLG を削除するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [SRLGs] を選択します。

[TE SRLG List] ウィンドウが表示されます。

ステップ 2　[TE SRLG List] で SRLG を削除するために、[TE SRLG List] ウィンドウから削除する SRLG を選択し、[Delete] をクリックします。[Delete Confirm] ウィンドウが表示されます。

ステップ 3　[Delete] をクリックして確認します。

[Delete Confirm] ウィンドウが閉じられます。[TE SRLG List] ウィンドウが更新されると、削除された SRLG は SRLG リストに表示されなくなります。

要素保護の設定

保護計算を行う前に、ネットワーク要素の保護を設定する必要があります。

ネットワーク要素保護を設定するには、次の手順を実行します。

ステップ 1　[Traffic Engineering] > [Protected Elements] を選択します。

[TE Protection Management] ウィンドウが表示されます。

[Protection Status] フィールドの説明

[Protection Status]：表示される保護ステータスは、監査が最後に実行された時間から決定されます。監査は、ユーザによって明示的に、または保護 SR が展開されたときに、実行されます。保護ステータスは、ネットワーク要素ごとに示され、[Protected]、[Not Fully Protected]、または [Unknown] のいずれかです。保護ステータスに基づいて要素をソートするには、列ヘッダー [Protected] をクリックします。

ステップ 2　最初に、保護する必要があるネットワーク要素を決定します。

[TE Protection Management] ウィンドウで、[Add] をクリックして保護要素（リンク、ノード、または SRLG）を追加します。[The Select Protection Elements] ウィンドウが表示されます。

シスコ デバイス以外のデバイスに接続されたリンクは保護できず、[Select] 保護要素ウィンドウに表示されません。同様に、シスコ デバイス以外のデバイスと、シスコ デバイス以外のデバイスへのリンクを含む SRLG は保護できず、選択から除外されます。

ステップ 3　保護する 1 つ以上の要素を選択し、[Select] をクリックします。

[Select Protection Element] ウィンドウが閉じられ、[TE Protection Management] ウィンドウが再び表示されます。

次に、適用すべき保護ツールを決定します。これらについては、「保護ツール」（P.7-64）に記載されています。

保護ツール

「基本的なトンネル管理」（P.7-28）で説明するように、バックアップ トンネルの手動の作成に依存しているため、比較的大きく、複雑なネットワークに限らず、独自の制約が生じます。

Prime Provisioning で利用可能な保護ツールは、指定されたネットワーク要素の保護を自動的に計算して確認する複数のツールを提供します。

（注）　説明など特定の属性はこれらのツールで実行する計算に影響を与えず、これらの属性に対する更新は計算結果ウィンドウに表示されません。

バックアップ計算

バックアップ計算は、指定されたネットワーク要素を保護するために必要なバックアップ トンネルを Prime Provisioning に自動計算させるために使用します。手動処理については、「基本的なトンネル管理」（P.7-28）で説明されています。

バックアップ計算を実行するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [Protected Elements] を選択します。

ステップ 2　「要素保護の設定」（P.7-64）の説明に従って、必要な保護要素を設定します。

ステップ 3　選択された要素に対してのみバックアップ計算を実行する場合は、バックアップ パスを計算する 1 つまたは複数の要素を選択します。

ステップ 4　[Compute Backup] をクリックし、次のいずれかを選択します。

- All Elements
- Selected Elements

最初に [Computation In Progress] ウィンドウが表示され、次に、[TE Protection Computation Results] ウィンドウが表示されます。

[Element:] テーブルには、保護計算に含まれている各要素の計算結果が表示されます。各要素のステータスは、テーブルの要素ごとに最低 1 行に示されています。ステータスが無効の場合、テーブルには、警告または違反ごとに 1 行が含まれます。

[Element]：テーブルには、次の列があります。

- [Element Name]：保護するネットワーク要素の名前。
- [Type]：ネットワーク要素のタイプ（ノード、リンク、または SRLG）。
- [Report]：計算エンジンから報告されたときに、要素に関連付けられた警告または違反（存在する場合）。
- [Status]：ネットワーク要素の計算のステータス。
  - [Valid Tunnels]：要素はバックアップ トンネルによって十分に保護されています。
  - [InvalidTunnels]：保護監査は、要素が既存のバックアップ トンネルによって十分に保護されていないことを検出しました。
  - [No Solution Exists]：バックアップ計算は、完全に要素を保護することができないことを証明しました。

（注）　説明など特定の属性は保護ツールの実行する計算に影響せず、これらの属性に対する更新は計算結果ウィンドウに表示されません。

ステップ 5　特定の警告または違反に対応する行を選択して [Detail] をクリックします。詳細説明が右ペインに表示され、選択した項目に関連付けられているバックアップ トンネルが下部ペインに表示されます。

警告と違反の説明については、「警告および違反」（P.7-102）を参照してください。

[Protection Type] 列の説明

- [Protection Type]：トンネルのアクティブ化による保護の副次的効果。次の 3 つの保護タイプがあります。
  - [Protection tunnels]：指定された要素を保護するためにアクティブにできるトンネル。
  - [Side-effect tunnels]：隣接する要素を保護するためにアクティブになるが、指定された要素に障害が発生した場合にもアクティブになるトンネル。
  - [Activated tunnels]：指定した要素に障害が発生した場合にアクティブになり、指定した要素またはネイバーを保護する場合と保護しない場合があるトンネル。

[Backup Tunnel] テーブルには、必要な新規保護トンネルおよび各要素について保持または削除する必要のあるすべての既存トンネルが表示されます。

ステップ 6　提示された保護ソリューションが受入可能であれば、[Accept Solution] をクリックします。

[TE Protection SR] ウィンドウが表示され、システムにより計算されたすべてのトンネルの追加および削除が示されます。

さまざまなウィンドウ要素の説明については、「バックアップ トンネルの作成」（P.7-40）を参照してください。

オプションで、トンネルの変更をここで行い、[Audit SR] を実行して、展開する前に保護の必要なレベルを設定することができます（「監査 SR」（P.7-67）を参照）。

ステップ 7　[Save & Deploy] をクリックして、新しいトンネル SR をネットワークに展開します。

[Save & Deploy] をクリックすると、影響を受ける TE ルータが Prime Provisioning によってロックされます。これにより、SR が終了するまで、その TE ルータを使用する後続のすべての SR はブロックされます。システム内の他の SR は、安全に試行および展開できます。処理中の SR と競合する場合、Prime Provisioning では、単に完了まで待機することを要求します。展開の状態を確認するには、[Inventory and Connection Manager] の [Service Requests] ウィンドウに移動するか、[Monitoring] の [Task Manager] を開きます。

（注）　TE トラフィック アドミッション SR を除き、TE SR は、[Inventory and Connection Manager] の [Service Requests] ページではなく、常に特定の [TE SR] ウィンドウから直接展開されます。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が開き、展開済みの SR の状態が表示されます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

SR が [Deployed] 状態にならない場合は、[Task Logs] ウィンドウに移動し、「SR 展開ログ」（P.10-48）の説明に従って展開ログ（[Monitoring] > [Task Manager] > [Logs]）を参照してください。

保護監査

P.65 で説明されたバックアップ計算ツールとは異なり、保護監査ではバックアップ ソリューションの作成が試行されません。保護監査では、現在の一連のバックアップ トンネルによる指定されたネットワーク要素の保護について検証を試み、検出されたすべての警告および違反を報告します。TE リンクまたは SRLG メンバーシップのリソースなどの TE トポロジで変更がコミットされた場合は、必ず保護監査を実行して、すべての要素の保護ステータスを確認することを推奨します。

計算は、バックアップ計算と同じ計算結果ページに表示されます。計算結果ページから戻ると、[TE Protection Management] ウィンドウの [Protection Status] 列が更新され、各要素の保護のレベルが示されます。

この項では、1 つまたは複数のネットワーク要素に対して保護監査を実行するために必要な手順について説明します。

保護監査を実行するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [TE Protected Elements] を選択します。

[TE Protection Management] ウィンドウが表示されます。

[Protection Status] フィールドの説明

[Protection Status] : 表示される保護ステータスは、監査が最後に実行された時間から決定されます。監査は、ユーザによって明示的に、または保護 SR が展開されたときに、実行されます。保護ステータスは、ネットワーク要素ごとに示され、[Protected]、[Not Fully Protected]、または [Unknown] のいずれかです。保護ステータスに基づいて要素をソートするには、列ヘッダー [Protected] をクリックします。

ステップ 2　選択された要素に対してのみ保護監査を実行する場合は、バックアップ パスを計算する 1 つまたは複数のトンネルを選択します。

[Audit Protection] をクリックし、次のいずれかを選択します。

- All Elements
- Selected Elements

[Computation In Progress] ウィンドウが表示されます。

次に、[TE Protection Computation Results] ウィンドウが表示されます。

さまざまなウィンドウ要素の説明については、「バックアップ計算」（P.7-65）を参照してください。

（注）　説明など特定の属性は保護ツールの実行する計算に影響せず、これらの属性に対する更新は計算結果ウィンドウに表示されません。

ステップ 3　特定の要素のバックアップ トンネルを表示するには、要素を選択し、[Details] をクリックします。

[TE Protection Computation Results] ウィンドウが表示されます。

さまざまなウィンドウ要素の説明については、「バックアップ計算」（P.7-65）を参照してください。

ステップ 4　特定の警告または違反に対応する行を選択して [Details] をクリックします。詳細説明が右ペインに表示され、選択した項目に関連付けられているバックアップ トンネルが下部ペインに表示されます。

警告または違反に関連付けられたトンネルには、下部ペインにある [Backup Tunnels] テーブルの [Report] 列でフラグが付けられます。

監査はソリューションではなく評価を提供するため、[Accept Solution] ボタンはグレー表示されます。

警告と違反の説明については、「警告および違反」（P.7-102）を参照してください。

ステップ 5　[Cancel] をクリックして、[TE Protection Management] ウィンドウに戻ります。

保護ステータスが [Protection Status] 列で更新されます。

監査 SR

監査 SR では、[TE Protection Management] ウィンドウのすべての要素の保護を [TE Protection SR] ウィンドウのバックアップ トンネルに対して監査します。

この機能は、展開前に、[TE Protection SR] ウィンドウで、手動で追加、変更、および削除したトンネルに対する保護を監査するために使用できます。

TE バックアップ トンネル SR を監査するには、次の手順を実行します。

ステップ 1　[Traffic Engineering] を選択します。

ステップ 2　[Create TE Backup Tunnel] をクリックします。

[TE Protection SR] ウィンドウが表示されます。さまざまなウィンドウ要素の説明については、「バックアップ トンネルの作成」（P.7-40）を参照してください。

ステップ 3　保護 SR を監査するために [Audit SR] をクリックします。

（注）　監査 SR は、[TE Protection Management] ウィンドウに要素がある場合のみ有効になります。[TE Protection Management] ウィンドウに要素がない場合は、[Audit SR] ボタンが無効になります（グレー表示されます）。

FRR 監査プロセスが開始され、[TE Protection Computation Results] ウィンドウが表示されます。

このプロセスの残りの説明については、「保護監査」（P.7-66）を参照してください。これらの 2 つのプロセスでは、詳細ウィンドウとレポート ウィンドウはまったく同じです。

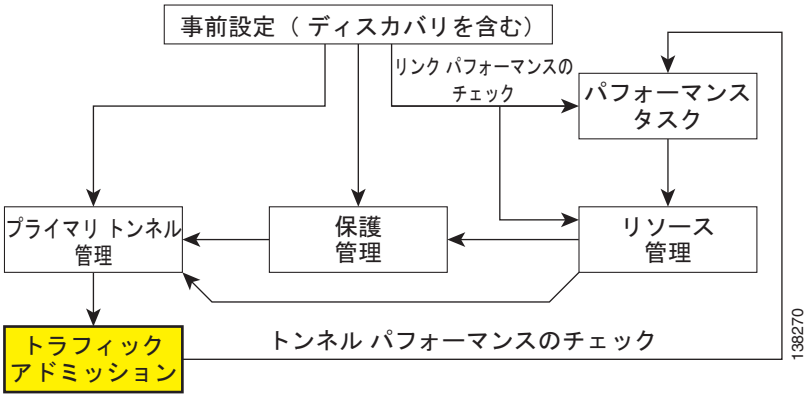
TE トラフィック アドミッション

TE トラフィック アドミッションは、TE トンネルでサービスを有効にするための最初のステップです。トラフィックをトンネルに転送して基本 IP 接続を提供するために使用できるメカニズムは多数存在します。現在の実装では、『Cisco Prime Provisioning Traffic Engineering Management』（Prime Provisioning）トンネルの存在をルーティング プロトコルに通知するために、スタティック ルーティングと自動ルート通知の両方が使用されます。自動ルート通知は、ルーティング プロトコル計算の一部としても使用できます。

TE トラフィック アドミッション ツールは、トラフィック エンジニアリングされたトンネルにトラフィックを割り当てるために使用されます。

図 7-3 で強調表示されているボックスは、Prime Provisioning TE トラフィック アドミッションが発生する場所を示しています。

図 7-20　Prime Provisioning プロセス図 : TE トラフィック アドミッション



スタティック ルーティングは、おそらく、トラフィックをトンネルに転送する最も簡単な方法です。ターゲット宛先プレフィックスと一致するトラフィックは、特定のトンネルにルーティングされます。

これにより、トラフィックを特定のトンネルに転送するという基本的な目的は達成されますが、このアプローチには制約があります。第 1 に、ディファレンシエーテッド サービス クラス（CoS）の処置の提供は、宛先ベースの CoS に制限されます。各ソース PE は複数のトラフィック フローの集約ポイントとして機能し、トンネルへは一般的なルーティングを通してアクセスするため、どのトラフィックが宛先への優先処置を受信するかを制限する方法はありません。第 2 に、スタティック ルーティング メカニズムでは各 PE ルータによって処理できる大量のサブネットのキャプチャに加えて、これらの各サブネットに対する CoS の処置もキャプチャできる必要があるため、通常は、スケーラブルなソリューションにはなりません。

スタティック ルーティングは、宛先によって CoS 処理を区別する必要がない場合に、最適に動作します。つまり、1 つ以上の特定のプレフィックス宛てのすべてのパケットは、すべて同じ CoS を受信します。

ここでは、次の内容について説明します。

- 「TE トラフィック アドミッション SR の作成」（P.7-69）
- 「TE トラフィック アドミッション SR の展開」（P.7-71）
- 「その他のトラフィック アドミッション SR の操作」（P.7-72）
- 「SR 状態の表示」（P.7-72）。

TE トラフィック アドミッション SR の作成

Cisco ISC TEM の TE トラフィック アドミッション ツールでは、トンネルが TE プロバイダーと関連付けられており、TE アドミッション SR とまだ関連付けられていない場合に、プライマリ トンネル（管理対象または管理対象外）だけが表示されます。つまり、このツールでは、現時点でいずれのトラフィックも伝送していない、トンネル宛ての新規トラフィックだけをアドミッションすることを想定しています。

TE トラフィック アドミッション SR を作成するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] を選択します。

ステップ 2　[TE Traffic Admission] をクリックします。

[TE Traffic Admission Tunnel Selection] ウィンドウが表示されます。

（注） このウィンドウが開かない場合は、TE プロバイダーに関連付けられているトンネルがないか、TE プロバイダーに関連付けられているすべてのトンネルが TE アドミッション SR とすでに結びつけられているかのいずれかです。

[TE Traffic Admission Tunnel Selection] ウィンドウには、アドミッション SR と関連付けられていない、管理対象および管理対象外の両方を含むすべてのプライマリ トンネルがリストされます。

[Deploy Status] には、[Pending]、[Deployed]、または [Functional] を指定できます。

（注） バックアップ トンネルは、[TE Traffic Admission Tunnel Selection] ウィンドウに表示されません。

ステップ 3　対応するオプション ボタンをクリックして TE トンネルを選択し、[Select] をクリックします。

[TE Traffic Admission SR] ウィンドウが表示されます。

[TE Traffic Admission SR] メイン ウィンドウには、次のフィールドが含まれています。

- [Tunnel]：トンネル名。
- [Description]：サービス要求の説明。
- [EXP]（IOS デバイスだけ）：CBTS のクラス マーキング ビット。
- [Policy]（IOS XR デバイスだけ）：PBTS のポリシー マーキング ビット。
- [Autoroute announce]：Interior Gateway Protocol（IGP）で、拡張最短パス優先（SPF）の計算に（トンネルがアップの場合）トンネルを使用することを指定します。
  - [On]：自動ルート通知はイネーブルになります。
  - [Off]：自動ルート通知はディセーブルになります。
- [Autoroute Metric]：マルチ プロトコル ラベル スイッチング（MPLS）のトラフィック エンジニアリング トンネル メトリックを指定するために使用します。これは、Interior Gateway Protocol（IGP）の拡張 Shortest Path First（SPF）の計算で使用されます。
  - [Absolute]：絶対メトリック モード。正のメトリック値を入力できます。
  - [Relative]：相対メトリック モード。正、負、またはゼロの値を入力できます。
- [Static Routes]：トンネルが使用するスタティック ルートが表示されます。
- [Destination]：トンネルの宛先に対するスタティック ルートの名前。
- [Distance]：アドミニストレーティブ ディスタンス（コスト）。

（注） PBTS 属性などの TE トラフィック アドミッション SR 属性が Prime Provisioning の外部で変更されて TE ディスカバリ タスクが実行される場合、ディスカバリ タスク ログでは不一致警告が報告されず、リポジトリはデバイスからの新規設定で更新されます。

ステップ 4　フォームの入力時に、[Autoroute Announce] を [On] に設定した場合は、[Autoroute Metric] を [Absolute] または [Relative] のどちらにするかを指定します。

ステップ 5　オプションの自動ルート メトリックも設定できます。

相対メトリックの場合、範囲は -10 ～ 10、絶対メトリックの場合、範囲は 1 ～ 2147483647 です。

（注） CBTS は IOS、PBTS は IOS XR でサポートされます。トンネル ヘッド ルータが IOS XR を実行している場合、[EXP] フィールドは表示される、[PBTS] フィールドに置き換えられます。

[Add] ボタンをクリックすると、[Add TE Static Route] ウィンドウが表示されます。

ステップ 6　[Add TE Static Route] ウィンドウで、**宛先** IP アドレス（w.x.y.z/n）の最小値を指定します。

オプションで、アドミニストレーティブ **ディスタンス**を指定します。1 つ以上のスタティック ルートを定義するか、代わりに自動ルートを定義するかのいずれかを行うことを推奨します。

ステップ 7　エントリを受け入れるには [OK] をクリックし、ウィンドウを閉じるには [Cancel] をクリックします。

メイン [TE Traffic Admission SR] ウィンドウで、別の TE スタティック ルートを追加するか、既存のルートを編集することができます。

ステップ 8　[Save] をクリックして、サービス要求を保存します。

[Service Requests] ウィンドウが表示され、TE トラフィック アドミッション SR が [REQUESTED] 状態になり、操作タイプが [ADD] に設定されていることがわかります。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

[Service Requests] ウィンドウからサービス要求を展開する場合は、「TE トラフィック アドミッション SR の展開」（P.7-71）を参照してください。

TE トラフィック アドミッション SR の展開

TE アドミッション SR は、[TE Primary Tunnel SR]、[Backup Tunnel SR]、[TE Resource Modification] ウィンドウではなく、一般的な [Service Requests Manager] ウィンドウから展開する必要があります。

TE アドミッション SR を展開するには、次のステップを実行します。

ステップ 1　[Operate] > [Service Request Manager] を選択します。

[Service Requests] ウィンドウが表示されます。

[Service Requests] ウィンドウには、次の要素が含まれています。

- [Job ID]：SR のジョブ ID。
- [Data Files]：このフィールドは、テンプレートを使用した変数の置換に使用され、現在、TEM SR には適用されません。
- [State]：トンネル状態が [DEPLOYED] または [NOT DEPLOYED] であるか、および [Conformed] または [Not Conformed] であるかを示します。
- [Type]：要求を発行したサービスを示すサービス要求のタイプ。使用可能なサービス タイプの詳細については、このマニュアルのサービス要求の管理の部分を参照してください。
- [Operation Type]：トンネル上の SR 操作。[ADD]、[MODIFY]、[DELETE]、または [ADMIT] のいずれかになります。現在の SR のトンネルにのみ適用できます。
- [Creator]：SR を作成したユーザの ID。
- [Customer Name]：SR が適用されるカスタマーの名前。
- [Policy Name]：SR に関連付けられたポリシーの名前。
- [Last Modified]：SR の最終変更日時。
- [Description]：ユーザが指定した SR の説明。

ステップ 2　目的のサービス要求を選択し、[Deploy] をクリックします。

[Deploy] ボタンの下にドロップダウン メニューが表示されます。ドロップダウン メニューで、[Deploy] または [Force Deploy] を選択します。正常に展開されると、SR の [State] が [Deployed] に変わります。

[Service Requests] ウィンドウ（[Operate] > [Service Request Manager]）が表示され、展開済みの SR の状態が表示されます。

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

その他のトラフィック アドミッション SR の操作

他のサービス要求と異なり、TE トラフィック アドミッション SR は、[Service Requests] ウィンドウでデコミッションできます。

TE トラフィック アドミッション サービス要求の編集およびデコミッション操作は、[Service Requests Manager] ウィンドウで処理されます。これらの操作については、このガイドでサービス要求の管理に関する部分で説明します。

SR 状態の表示

サービス リクエストの状態を表示するには、[Operate] > [Service Request Manager] に移動します。

SR が [Deployed] 状態にならない場合は、[Task Logs] ウィンドウに移動し、の説明に従って展開ログ（[Operate] > [Task Manager] > [Logs]）を参照してください。「SR 展開ログ」（P.10-48）

管理機能

『Cisco Prime Provisioning Traffic Engineering Management』（TEM）のいくつかの管理機能は、Prime Provisioning と共通です。これらの機能を使用する手順については、*『Cisco Prime Provisioning 6.3 Administration Guide』* から詳細に説明されています。

ここでは、TE 固有の管理機能だけを示します。

ここでは、次の内容について説明します。

TE のユーザ ロール

TE のユーザ ロールは、事前に定義されたロールまたは一連の権限を定義するユーザ指定ロールです。Prime Provisioning のユーザ ロールとその使用方法の詳細については、*『Cisco Prime Provisioning 6.3 Administration Guide』* を参照してください。

[User Roles] ウィンドウにアクセスし、TE のユーザ ロールを指定するには、[Administration] > [Roles] を選択します。[User Roles] ウィンドウが表示されます。

事前定義された TEM ユーザ ロールには次の 2 つがあります。

- **TERole**：TEM 操作へのすべての権限を与えます。
- **TEServiceOpRole**：TE アドミッション SR のみを管理する権限を与えます。

TE ポリシー

ポリシーは、一般的なトンネル属性を定義するために使用されます。帯域幅プール、保持およびセットアップ優先度、アフィニティ ビットなどの属性は、以下で説明されているように、ポリシーの作成時に手動で設定します。

この項では、次のポリシー操作について説明します。

- 「ポリシーの作成」（P.7-73）
- 「ポリシーの編集」（P.7-75）
- 「ポリシーの削除」（P.7-76）

ポリシーの作成

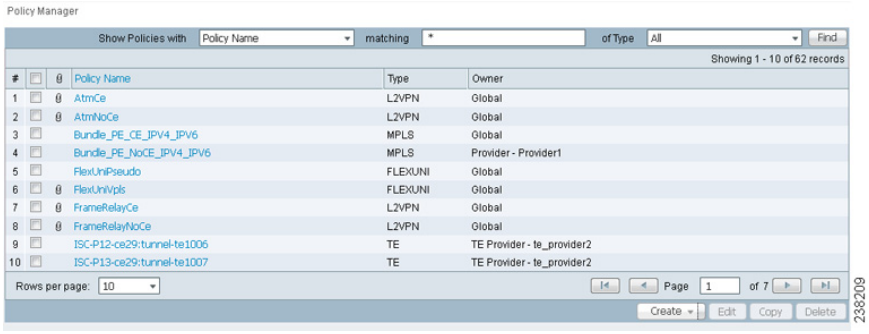
Prime Provisioning では、TE 固有のポリシーを他のポリシーと同様に作成できます。

TE ポリシーを作成するには、次のステップを実行します。

ステップ 1　[Service Design] > [Policy Manager] を選択します。

図 7-21 の [Policy Manager] ウィンドウが表示されます。

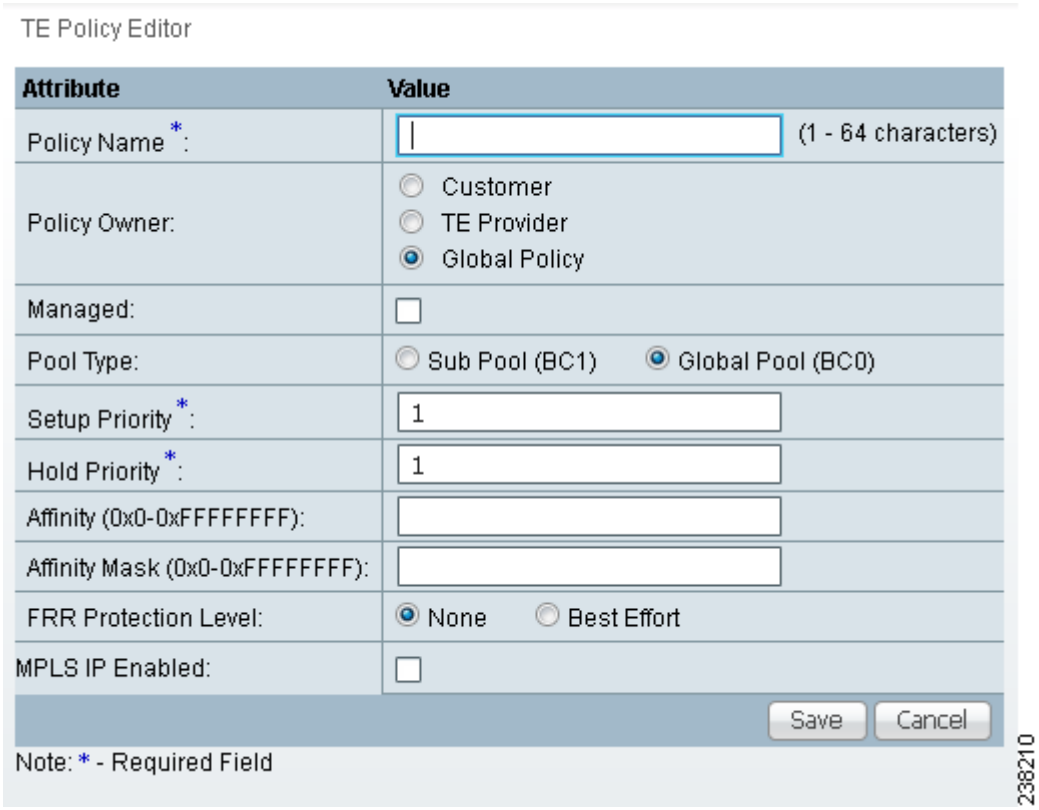
図 7-21　Policy Manager



ステップ 2　[Create] をクリックし、[TE Policy] を選択して新規 TE ポリシーを設定します。

図 7-22 の [TE Policy Editor] ウィンドウが表示されます。

図 7-22　TE Policy Editor



[TE Policy Editor] ウィンドウには、次のフィールドが含まれます。

- [Policy Name]：ユーザが選択する TE ポリシーの名前。

- [Owner]：TE ポリシーの所有者。
- [Managed]：このチェックボックスをオンにすると、ポリシーが管理対象トンネルにより使用されます。オンにした場合は、セットアップ プライオリティおよび保持プライオリティの両方にゼロが設定されて、編集不可になります。このチェックボックスがオフの場合は、セットアップおよび保持の優先度を 1 ～ 7 の値に設定できます。

  [Managed] チェックボックスをクリックすると、[FRR Protection Level]（Fast Re-Route）の 2 つの追加保護レベルに対応する TE Policy Editor のいくつかの特別なフィールドと新しいフィールド [Delay Constraint] が追加されます。
- [Pool Type]：このポリシーのトンネル帯域幅プール タイプ。プール タイプの定義については、「トラフィック エンジニアリング管理の概念」（P.7-115）で帯域幅プールの項を参照してください。
  - [Sub Pool (BC1)]：帯域幅はサブプールから予約されます。
  - [Global Pool (BC0)]：帯域幅はグローバル プールから予約されます。
- [Setup Priority]：優先する既存のトンネルを判別するために、トンネルの LSP をシグナリングするときに使用される優先順位。有効な値は 0 ～ 7 であり、数字が小さいほど優先順位は高くなります。したがって、セットアップ プライオリティが 0 の LSP は、0 以外の保持プライオリティのすべての LSP より優先されます。
- [Hold Priority]：シグナリングされている他の LSP の方を優先的に取得する必要があるかどうかを決定するため、トンネルの LSP に関連付けられた優先順位。有効な値は 0 ～ 7 であり、数字が小さいほど優先順位は高くなります。
- [Affinity]：トンネルを伝送するリンクで必要な属性値（ビット値は 0 または 1 のいずれか）。
- [Affinity Mask]：確認する属性値を決定します。マスクのビットが 0 の場合、そのビットに対応するリンクの属性値は関連しません。マスクのビットが 1 の場合、そのビットに対するリンクの属性値とトンネルに必要なアフィニティは一致する必要があります。
- [FRR Protection Level]：プライマリ トンネルで必要な高速再ルーティング保護のレベル。
  - [None]：バックアップ トンネルは必要ありません。
  - [Best Effort]：可能な場合に、バックアップ トンネルを使用します。
  - [Link & SRLG]：プライマリ トンネルは FRR 保護されたリンクまたは SRLG だけを通過する必要があります。
  - [Link, SRLG & Node]：プライマリ トンネルは、中間ノードと、FRR 保護されたリンクまたは SRLG だけを通過する必要があります。
- [MPLS IP Enabled]：**mpls ip** コマンド（有効な場合）でトンネルを設定します。

ポリシーの編集

ポリシーは、トンネルに関連付けられていない場合にのみ編集できます。

TE ポリシーを編集するには、次のステップを実行します。

ステップ 1　[Service Design] > [Policy Manager] を選択します。

図 7-22 の [Policies] ウィンドウが表示されます。

ステップ 2　必要なポリシーを選択し、[Edit] をクリックします。

[TE Policy Editor] ウィンドウが表示されます。ポリシー エディタについては、「ポリシーの作成」（P.7-73）で説明されています。作成プロセスと編集プロセスの唯一の違いは、ポリシーの編集時にポリシー名と所有者を編集できないことです。

ステップ 3　ポリシー属性に適切な変更を加え、[Save] をクリックします。

保存操作が正常に行われた場合は、新しい TE ポリシーが [Policies] ウィンドウに表示されます。成功しない場合は、発生したエラーのタイプと修正可能な場合の修正措置が [Status] ボックスに示されます。

ポリシーの削除

ポリシーは、トンネルに関連付けられていない場合にのみ削除できます。

TE ポリシーを削除するには、次のステップを実行します。

ステップ 1　[Service Design] > [Policy Manager] を選択します。

図 7-22 の [Policies] ウィンドウが表示されます。

ステップ 2　必要なポリシーを選択し、[Delete] をクリックします。

[Confirm Delete] ウィンドウが表示されます。

ステップ 3　削除とマークされたポリシーのチェックボックスをオンにし、[OK] をクリックします。

[Policies] ウィンドウが更新され、選択されたポリシーが非表示になります。

TE タスク

Prime Provisioning には、現時点では、他のタスクと同様な方法で使用する TE 固有のタスクが 3 つあります。

- [TE Discovery (Full and Incremental)] : TE ネットワークからデータをリポジトリに入力します。不一致が調整または報告されます。
- [TE Functional Audit] : 特定の状態において、TE プライマリまたはバックアップ SR で機能監査を実行します。
- [TE Interface Performance] : インターフェイスまたはトンネルの帯域使用率を計算します。

この項では、TE 機能監査および TE インターフェイス パフォーマンス タスクの作成方法について説明します。TE 検出タスクの作成方法は、「TE ネットワーク検出」（P.7-11）に記載されています。

TE タスクの作成

TE タスクは、Task Manager で管理されます。ISC Task Manager にアクセスするには、[Operate] > [Task Manager] を選択します。

[Tasks] ウィンドウが表示されます。

[Tasks] ウィンドウのウィンドウ要素の詳細については、「タスク マネージャ」（P.10-25）を参照してください。

このページには、実行されたすべての収集および展開タスクが表示されます。タスクは 1 回だけ行うようにスケジュールしたり、複数回行うようにスケジュールしたりできることに注意してください。スケジュールは、タスクを選択し、[Schedules] をクリックして表示できます。

TE 機能監査タスクの作成

SR の各トンネルに対して、TE 機能監査タスクはルータで現在使用されている LSP とリポジトリに格納された LSP を照合します。

- [tunnel down]：無視します（オンにしません）。
- [tunnel up]：ルータで使用されている LSP とリポジトリに格納された LSP を照合します。
  - これらの LSP が同じ場合、トンネルと SR は両方とも [Functional] に設定されます。
  - 異なる場合は、トンネルおよび SR の両方に [Broken] が設定されます。
- [tunnel missing from router]：SR はそのまま通過します。トンネルの状態は、Lost に設定されます。

このタスクでは、次のいずれかの状態でない TE プライマリまたはバックアップ SR に対してのみ機能監査を実行します。

- **Closed**
- **Requested**
- **Invalid**
- **Failed Deploy**

サービス要求の操作に関する詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

TE 機能監査タスクを作成するには、次のステップを実行します。

ステップ 1　[Operate] > [Task Manager] を選択します。

ステップ 2　[Audit] > [TE Functional Audit] をクリックして [Create Task] ウィンドウを開きます。

[Create Task] ウィンドウのウィンドウ要素の詳細については、「タスク マネージャ」（P.10-25）を参照してください。

ステップ 3　必要に応じて [Name] または [Description] フィールドの内容を変更し、[Next] をクリックします。

[Task Service Requests] ウィンドウが表示されます。

ステップ 4　[Add] をクリックしてタスク サービス要求を追加します。

[Select Service Request(s)] ウィンドウが表示されます。

ステップ 5　[Select] ボタンを使用して SR を選択します。

（注）　タイプ TE トンネルまたは TE 保護の SR のみが受け入れられます。

[Selected Service Request(s)] ウィンドウが閉じられ、選択されたタスクが [Task Service Requests] ウィンドウに表示されます。他の SR を追加するには、ステップ 4 とステップ 5 を繰り返します。

ステップ 6　[Task Service Requests] ウィンドウで、[Next] をクリックします。

[Task Schedules] ウィンドウが表示されます。

ステップ 7　[Now] をクリックしてタスクをすぐに開始するか、[Create] をクリックしてタスク スケジュールを作成します。

[Now] を選択すると、行が [Task Schedules] ウィンドウに追加されます。[Create] を選択すると、[Task Schedule] ウィンドウが表示されます。

ステップ 8　[Task Schedule] ウィンドウで、タスクを実行するタイミングと頻度を指定します。

ステップ 9　[OK] をクリックします。

この結果、スケジュールされたタスクが [Task Schedules] テーブルに表示されます。

（注）　デフォルト設定では、単一の TE 機能監査タスクをすぐに実行します（[Now]）。

ステップ 10　[Next] をクリックします。

[Task Schedule] ウィンドウの作成済みタスクのリストに新しいタスクが表示されます。スケジュールされたタスクの概要が表示されます。

ステップ 11　[Finish] をクリックします。

[Tasks] ウィンドウの作成済みタスクのリストにタスクが追加されます。

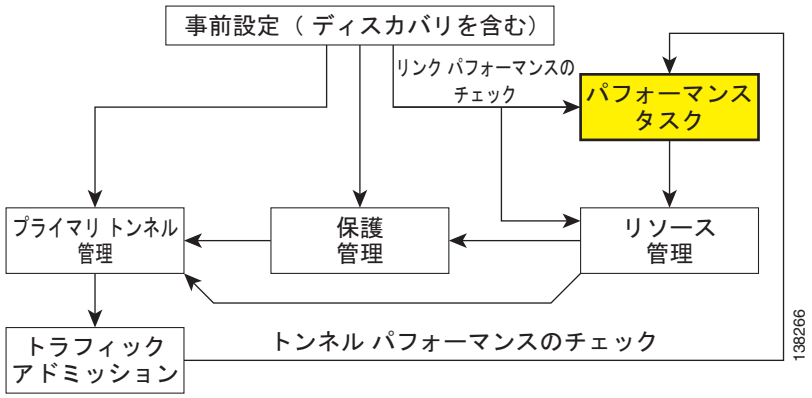
作成済みタスクのタスク ログを表示する場合は、「タスク ログの表示」（P.10-48）を参照してください。

TE インターフェイス パフォーマンス タスクの作成

このタスクでは、簡易ネットワーク管理プロトコル（SNMP）を使用してインターフェイスおよびトンネルの帯域使用率を計算します。

図 7-3 で強調表示されたボックスは、トラフィック アドミッションが Prime Provisioning のどこで行われるかを示しています。

図 7-23　Prime Provisioning プロセス図：TE インターフェイス パフォーマンス



使用率の計算は、測定するオブジェクトのデータの表現方法に依存します。インターフェイス使用率は、ネットワーク使用率に使用される主要な測定単位です。MIB-II 変数はカウンタとして格納されるため、2 つのポーリング サイクルを測定し、その差を計算する必要があります（つまり、方程式で使用される差分）。

次の 3 つの変数が必要です。

- タスク時間：タスクが実行される時間の長さ（秒単位）
- 頻度：データが収集される頻度（秒単位）
- 間隔：2 つのポーリング サイクル間の差（ミリ秒単位）

計算式で使用される変数の説明は次のとおりです。

- 差分（着信トラフィック）：SNMP 入力オブジェクトを収集する 2 つのポーリング サイクル間の差分であり、トラフィックの着信単位の数を表します。
- 差分（発信トラフィック）：SNMP 出力オブジェクトを収集する 2 つのポーリング間隔の差分で、トラフィックの発信単位の数を表します。
- 帯域幅：インターフェイスの速度。

次の式を使用して入力使用率と出力使用率を別々に測定する方式により、さらに高い精度を得られます。

$$\text{入力使用率} = \frac{\text{差分（着信トラフィック）} \times 8 \times 100}{\text{（差分の秒数）} \times \text{帯域幅}}$$

$$\text{出力使用率} = \frac{\text{差分（発信トラフィック）} \times 8 \times 100}{\text{（差分の秒数）} \times \text{帯域幅}}$$

TE インターフェイス パフォーマンス タスクを作成するには、次のステップを実行します。

ステップ 1　[Operate] > [Task Manager] を選択します。

ステップ 2　[Create] > [TE Interface Performance] をクリックして、新しい TE インターフェイス パフォーマンス タスクに対して [Create Task] ウィンドウを開きます。

[Create Task] ウィンドウのウィンドウ要素の詳細については、「タスク マネージャ」（P.10-25）を参照してください。

ステップ 3　必要に応じて名前と説明を変更し、[Next] をクリックします。

[Select TE Provider] ウィンドウが表示されます。

ステップ 4　オプション ボタンをクリックして TE プロバイダーを選択します。

ステップ 5　[Next] をクリックします。

[TE Performance Collection] ウィンドウが表示されます。

ステップ 6　[Task Duration]、[Task Frequency]、および [Task Interval] の各フィールドに必要な値を入力します。

（注）　[Task Interval] フィールドの設定値が小さすぎる場合は、MIB を更新できず、TE パフォーマンス レポートでトラフィックが示されません。IOS ルータ上のトンネルまたはリンクの場合は、間隔に 1000 ms を設定することを推奨します。IOS XR ルータの場合は、間隔に 5000 ms を設定することを推奨します。お使いの特定の環境に合わせてこれらの値を調整する必要がある場合があることに注意してください。

ステップ 7　[Add] ボタンを使用して、インターフェイス パフォーマンス タスクを実行するトンネルまたはリンクを選択します。

- [TE Tunnel] : TE トンネルを追加します。[Select Tunnel(s)] ウィンドウが表示されます。
- [TE Link] : TE リンクを追加します。[Select Link(s)] ウィンドウが表示されます。

ステップ 8　1 つまたは複数のトンネルおよびリンクを選択し、[Next] をクリックします。

選択されたトンネルおよびリンクは、[TE Performance Collection] ウィンドウの [Targets] リストに追加されます。[Task Schedules] ウィンドウが表示されます。

ステップ 9　[Now] または [Create] をクリックしてタスク スケジュールを作成します。

[Create] を選択してスケジュールをカスタマイズする場合は、[Task Schedule] ウィンドウが表示されます（[Now] の場合、このステップはスキップされます）。

（注）　デフォルト設定では、単一の TE インターフェイス パフォーマンス タスクをすぐに実行します（[Now]）。

ステップ 10　[Task Schedule] ウィンドウで、タスクを実行する時間と頻度を定義するための選択を行います。

ステップ 11　[OK] をクリックします。

この結果、スケジュールされたタスクが [Task Schedules] テーブルに表示されます。

ステップ 12　[Next] をクリックします。

スケジュールされたタスクの概要が表示されます。

ステップ 13　[Finish] をクリックします。

[Tasks] ウィンドウの作成済みタスクのリストにタスクが追加されます。

TE インターフェイス パフォーマンス タスクに対して生成された TE パフォーマンス レポートを表示するには、「TE パフォーマンス レポート」（P.10-49）を参照してください。

作成済みタスクのタスク ログを表示する場合は、「タスク ログの表示」（P.10-48）を参照してください。

SR 履歴およびコンフィグレット

個々のサービス要求に関連する履歴とコンフィグレットは、[Service Requests] ウィンドウでサービス要求を選択し、[Details] ボタンをクリックして表示できます。

サービス要求の履歴は、実質的に状態の変更レポートです。SR に関連付けられた要素が遷移したさまざまな状態がリストされ、これらの状態の遷移に関する詳細が報告されます。

サービス要求に関連付けられたデバイスのコンフィグレットは、スクロール可能な単純なテキスト形式で保存されます。

これらの機能についておよびサービス要求を管理する方法の詳細については、このマニュアルのサービス要求の管理の部分を参照してください。

ロック メカニズムの管理

データベース更新を伴うタスクの実行は、リソースに影響し、したがってトンネル計算の結果に影響することがあるため、更新の前にタスクによってシステムがロックし、更新の完了時に解放します。何らかの理由でロックがリリースされない場合は、ロックを必要とする他の更新がブロックされます。

ロック機能は、相互に矛盾する計画アクティビティを同時にデータベースにコミットさせないことを目的としています。つまり、各ユーザがリポジトリの同じスナップショットを取得し、計算を実行して結果をコミットしようとした場合に、ロック メカニズムは、コミットを同期するため、および他のコミットが原因で無効になるコミットをなくすために有用です。

システムが長時間ロックされる場合、管理者は、計画タスクを長時間実行しているユーザの存在を確認し、システムをロックしたプロセスをメモして報告する必要があります。管理者は、システムを使用しているユーザがいないことを確認し、ロック マネージャを使用してロックを解除できます。

Prime Provisioning には、2 種類のロックがあります。

- TE プロバイダー ロック：管理対象トンネル、バックアップ トンネル、リソース SR、および TE 検出をロックします。
- TE ルータ ロック：管理対象外トンネルをロックします。

各システム ロックは、TE プロバイダーにリンクされます。次に、各システム ロックをロック解除する手順を示します。

TE プロバイダー ロックのロック解除

TE プロバイダーをロック解除するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [Providers] を選択します。

[TE Providers] ウィンドウが表示されます。

ステップ 2　対応するチェックボックスをオンにして、ロックされている TE プロバイダーを選択します。

ステップ 3　[Manage Lock] をクリックします。

[System Lock Management] ウィンドウが表示されます。

このウィンドウのテキスト フィールドは読み取り専用です。

ステップ 4　ロックを解除するために [Unlock] ボタンをクリックします。

[System Lock Management] ウィンドウが閉じられ、[TE Providers] ウィンドウの [System Lock Status] フィールドが適宜更新されます。

TE ルータ ロックのロック解除

TE ルータ ロックをロック解除するには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [Nodes] を選択します。

[TE Nodes List] ウィンドウが表示されます。

ステップ 2　対応するチェックボックスをオンにして、ロックされている TE ノードを選択します。

ステップ 3　[Manage Lock] をクリックします。

[System Lock Management] ウィンドウが表示されます。このウィンドウのテキスト フィールドは読み取り専用です。

ステップ 4　ロックを解除するために [Unlock] ボタンをクリックします。

[System Lock Management] ウィンドウが閉じられ、[TE Nodes List] ウィンドウの [System Lock Status] フィールドが適宜更新されます。

操作エラーのロック

TEM では、保存操作および導入操作の間、TE プロバイダーまたは TE ルータ オブジェクトをそれぞれロックして、データベースの一貫性を保ちます。

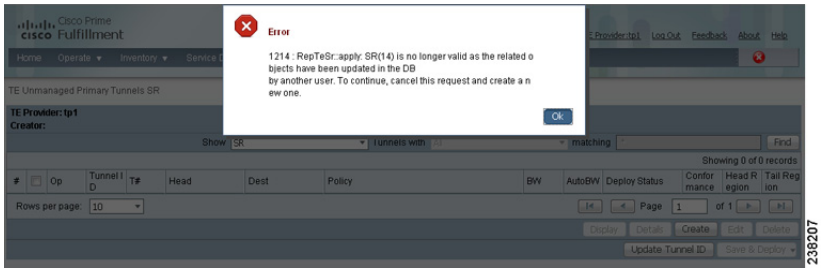
この項では、次のエラーについて説明します。

- 「ロックされたオブジェクトの変更」（P.7-82）
- 「ロックが解放されたオブジェクトの変更」（P.7-83）
- 「関連 TE オブジェクトのあるリンクの削除」（P.7-83）
- 「関連 TE オブジェクトのないリンクの削除」（P.7-84）

ロックされたオブジェクトの変更

ロックされたオブジェクトを変更しようとした場合は、別のユーザによって変更中であるため、オブジェクトを変更できないと通知されます。図 7-24 のエラー メッセージが表示されます。

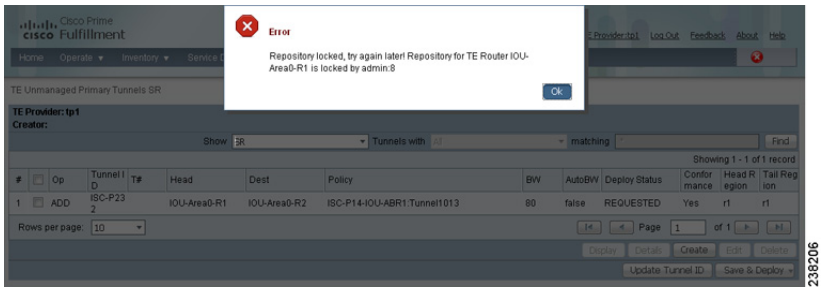
図 7-24　ロックされたオブジェクトの変更



ロックが解放されたオブジェクトの変更

ロックの解放後にオブジェクトを変更しようとした場合、Prime Provisioning では、現在作業中のオブジェクトのバージョンが最新であるかどうかをチェックします。バージョンが最新でない場合は、データが最新でないため、オブジェクトの新しいバージョンで再び作業を始めるよう指示されます。
図 7-25 のエラー メッセージが表示されます。

図 7-25　ロックが解放されたオブジェクトの変更

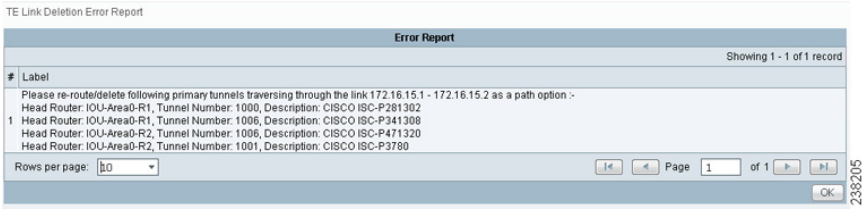


関連 TE オブジェクトのあるリンクの削除

明示的パスと関連付けられているリンクや、トンネルが通過しているリンクは削除できません。

1 つまたは複数のオブジェクトが関連付けられたリンクを削除しようとすると、図 7-26 のエラー メッセージが表示されます。

図 7-26　関連 TE オブジェクトのあるリンクの削除

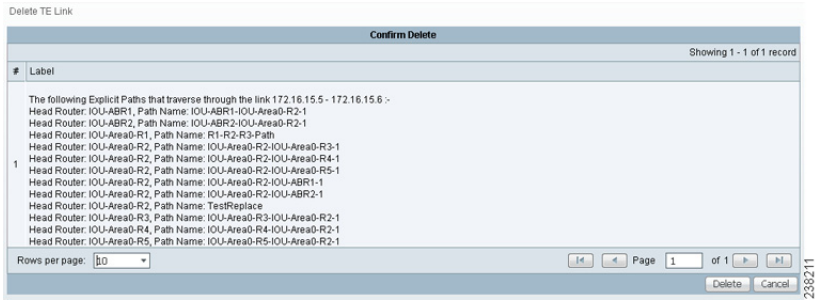


関連 TE オブジェクトのないリンクの削除

トンネルが通過していないリンクは、明示的パスと関連付けられていても削除できます。

このようなリンクを削除しようとしたときに、図 7-27 示すレポートのタイプが表示されます。

図 7-27　関連 TE オブジェクトのないリンクの削除



TE トポロジ

TE トポロジ ツールは、Cisco Prime Provisioning Web クライアントを通じてネットワーク設定のグラフィカル ビューを提供します。デバイス、リンク、およびトンネルなどさまざまなネットワーク要素がグラフィカルに表示されます。Prime Provisioning では識別できないが、TE 検出ツールでネットワークの一部として検出されたデバイスも表示されます。

TE トポロジ ツールには、[Traffic Engineering] メニューからアクセスします。

TE トポロジ ツールは、リポジトリに含まれるデータに基づいて TE ネットワークを視覚化するために使用されます。この目的のために、グラフ レイアウトに対するアルゴリズムの適用、マップのインポートなど、表示を操作するさまざまな方法が用意されています。

このツールは、ブラウザ内の Java アプレットを介して TE トポロジを表示する TE トポロジ インターフェイス アプレットからアクセスします。

ここでは、トポロジ ツールを使用する方法について説明します。

内容は次のとおりです。

TE トポロジ インターフェイス アプレットの使用

TE トポロジ インターフェイス アプレット（トポロジ アプレット）は、ネットワークおよびネットワークに存在しているトンネルを視覚化する手段を備えています。Web ベースの GUI は、ネットワーク情報を視覚化する主要な手段です。トポロジ アプレットでは単に Web ベースの GUI を拡張してさまざまなプレゼンテーション形式を実現します。

トポロジ アプレットを介して次の機能が提供されます。

- TE トポロジのレンダリング
- ネットワーク要素の強調表示
- トンネル オーバーレイ（管理対象外、プライマリ、およびバックアップ）
- トポロジ レイアウトのパーシステンス
- Web ページ コンテンツとの統合

トポロジ アプレットにアクセスするには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [Topology] を選択します。

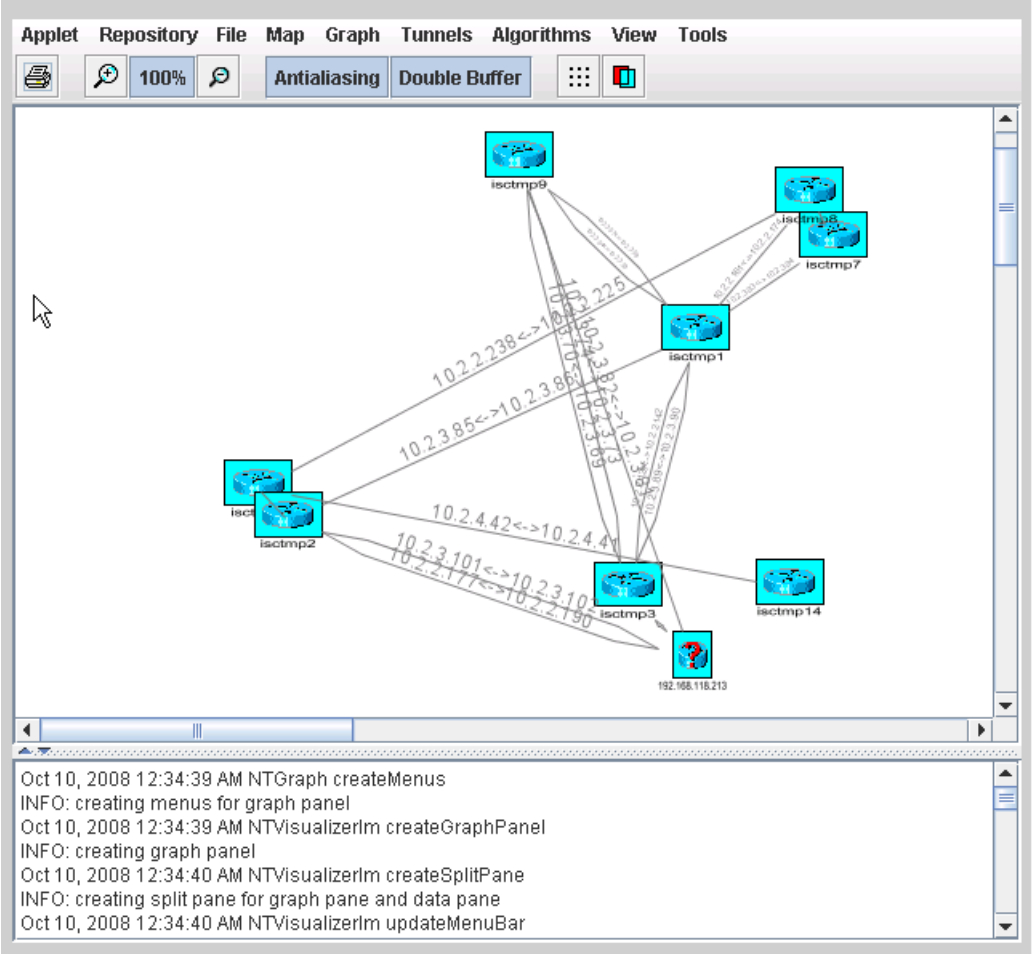
ステップ 2　[TEM Topology Interface Applet] をクリックします。

トポロジ アプレットのセキュリティ証明書をまだ受け入れていないために、セキュリティ警告ウィンドウが表示されることがあります。

ステップ 3　[Yes] または [Always] をクリックして、セキュリティ証明書の信頼性を受け入れます。

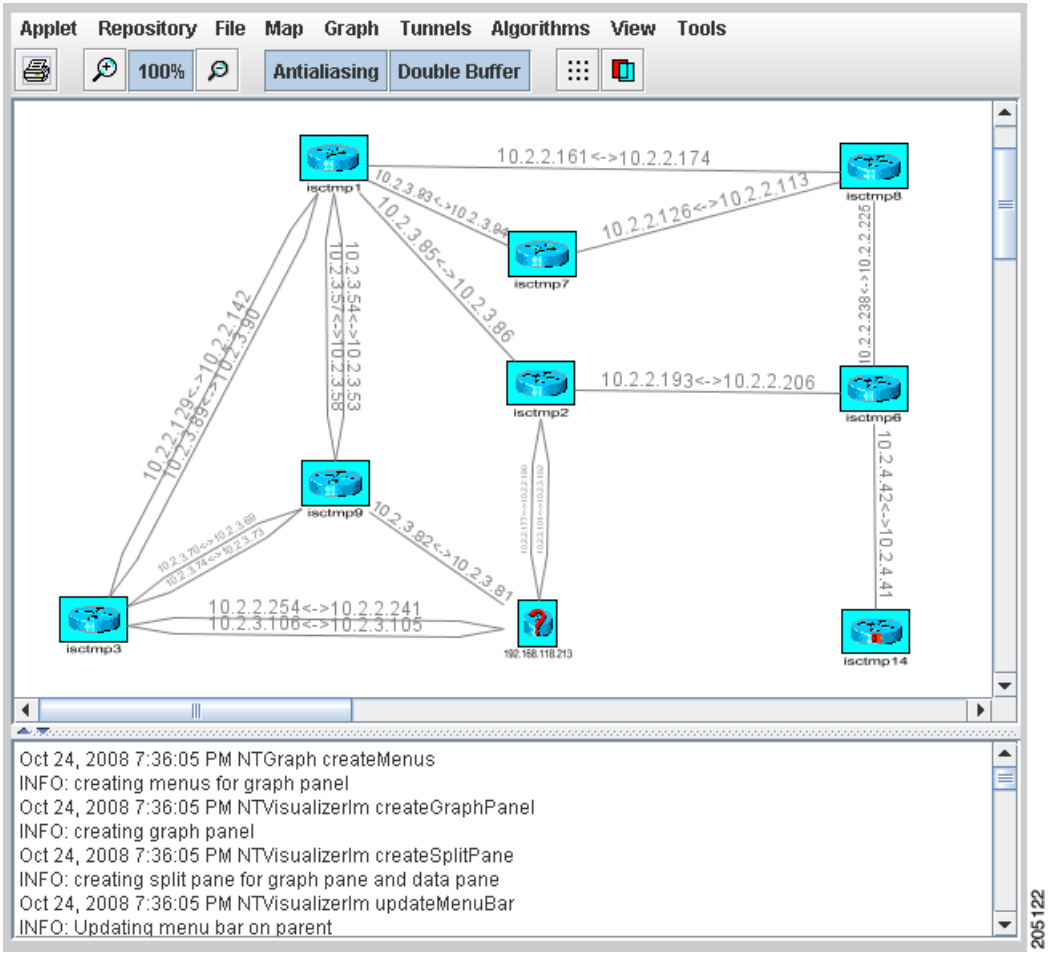
図 7-28 の [Topology Display] アプレット ウィンドウが表示されます。

図 7-28　順序付けられていない状態のトポロジ表示アプレット



好みに合わせてノードを配置し終えると、トポロジ表示は図 7-29 のようになります。

図 7-29　トポロジ表示アプレットとユーザが編成したトポロジ



レイアウトの表示および保存

[Repository] メニューの 2 つの操作 [Layout Graph] および [Save Graph Layout] を使用して、ネットワーク グラフの現在のレイアウトを表示または保存します。

グラフ レイアウトを生成する前に、各ネットワーク デバイスの座標を設定する必要があります。そうでない場合、グラフはランダムにレイアウトされます。

- [Layout Graph]：グラフはリポジトリからレイアウトされます。すでにグラフ レイアウトが存在する場合、[Clear Graph Layout] 確認ボックスで [Yes] をクリックすると、そのレイアウトはクリアされます。レイアウトが以前に保存されていない場合は、リポジトリの内容のランダムなレイアウトが取得されます。以前にレイアウトを保存した場合は、保存されたレイアウトが再描画されます。
- [Save Graph Layout]：現在のグラフ レイアウトを保存します。そうすることで、[Layout Graph] またはトポロジ アプレットを閉じると常にグラフ レイアウトがクリアされ、アプレットの再起動時に同じレイアウトが作成されるように保証されます。マップが使用された場合、そのマップも再描画されます。

マップの使用

各ビューには、マップを 1 つ関連付けることができます。現在、トポロジ ビューアでは、Environmental Systems Research Institute, Inc.（ESRI）のシェープ形式のマップのみサポートされています。以降の章では、マップをロードし、マップ レイヤと各マップに関連付けられているデータを選択的に表示する方法について説明します。

マップの機能は、[Topology] ウィンドウの [Map] メニューからアクセスします。

[Map] メニューにアクセスするには、次のステップを実行します。

ステップ 1　[Traffic Engineering] > [TE Topology] を選択します。

ステップ 2　[TM Topology Interface Applet] を起動します。

ネットワークのリンクとノード データがリポジトリにすでに存在する場合、進行状況レポートは、対応するデータがロードされるときに、さまざまなネットワーク要素を示します。

ステップ 3　[Map] メニューを選択します。

メニューが表示されます。

[Map] メニューでは、次に説明するように、マップをロードまたはクリア（削除）できます。

マップのロード

表示されたデバイスの物理的な位置を表示したバックグラウンド マップの設定が必要になることがあります。マップをロードするには、次のステップを実行します。

ステップ 1　メニュー バーで、[Map] > [Load] を選択します。

Web マップ サーバが動作している場合は、[Map Chooser] ウィンドウが表示されます。

ステップ 2　[Map Chooser] ウィンドウで必要な選択を行います。

ウィンドウの右側部分には、小さいコントロール パネルがあり、マップを表示する投影法を選択できます。マップの投影では、平面に球体がマップされます。一般的な投影法には、メルカトル、ランベルト、およびステレオ投影があります。

投影法の詳細については、次の場所にある、Eric Weisstein による「World of Mathematics」の「Map Projections」の項を参照してください。

http://mathworld.wolfram.com/topics/MapProjections.html

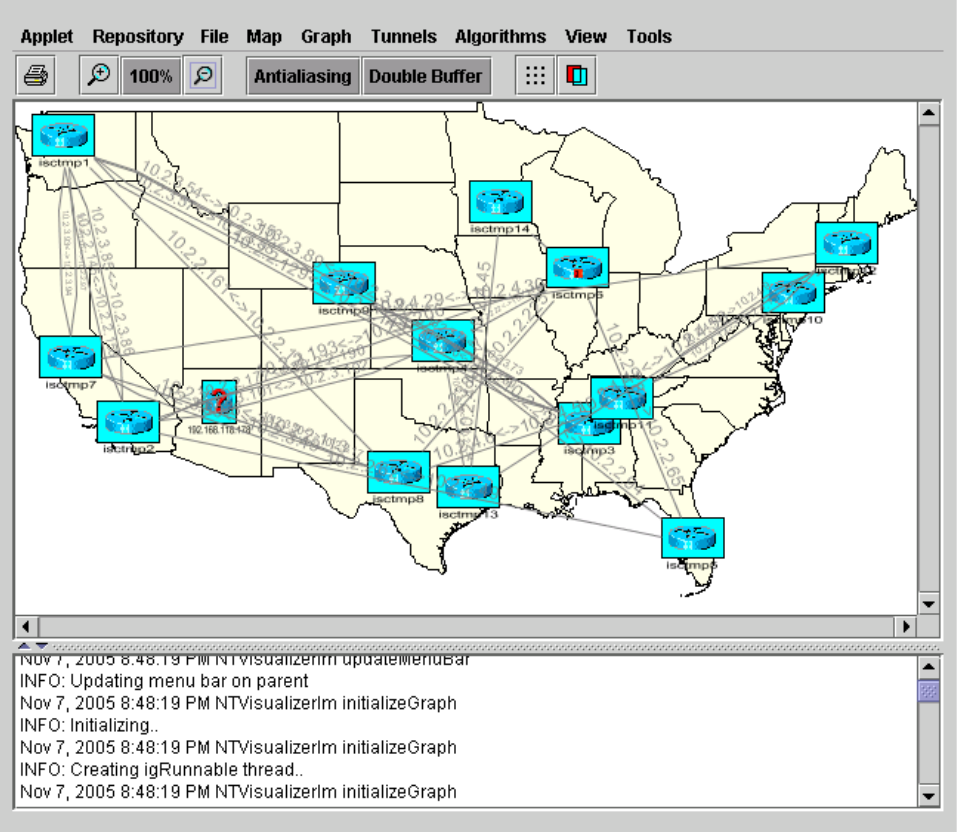
必要に応じて、[Longitude Range] フィールドと [Latitude Range] フィールドの設定を変更します。

ステップ 3　マップ ファイルを選択し、[Open] をクリックして、マップをロードします。

マップ ファイルを選択し、[Open] ボタンをクリックすると、ファイルのロードが開始されます。マップは複数コンポーネントで構成されている場合があるため、ロードされたマップ ファイルの部分を通知する進捗ダイアログが表示されます。

図 7-30 のようなマップが表示されます。

図 7-30　ロードされたマップ



ステップ 4　トポロジ ビューの表示内容を操作するには、[Topology Display] ウィンドウのメニューで、各種機能を使用します。一部については、以降で説明します。

新規マップの追加

トポロジ ツールで使用できるように、マップの選択肢に独自のマップを追加することが必要になる場合があります。これは、マップ ファイルを **$ISC_HOME/resources/webserver/tomcat/webapps/ipsc-maps/data** ディレクトリまたは、Prime Provisioning インストール内のサブディレクトリに配置することによって行います。この例をわかりやすく説明するために、クイーンズランド州の州都ブリスベンの郊外にあるトゥーウォンのマップを追加するとします。最初のステップとして、マップ ベンダーからマップを入手します。すべてのマップは ESRI シェープ ファイル形式でなければなりません（『**ESRI Shapefile Technical Description**』を参照）。また、各シェープ ファイルにはデータ ファイルを付属させることもできます。データ ファイルには、オブジェクト、およびシェープ ファイル内に含まれている対応するシェープに関する情報が含まれます。ベンダーが次の 4 つのファイルを提供しているとします。

- toowong_city.shp
- toowong_city.dbf
- toowong_street.shp
- toowong_street.dbf

マップのレイヤに関する情報を TE トポロジ ツールに伝える .map ファイルを作成する必要があります。この例では、City と Street という 2 つのレイヤがあります。マップ ファイル（たとえば、Toowong.map）は、次のような内容になります。

```
toowong_city
toowong_street
```

このファイルには、トゥーウォンのマップを構成するレイヤがすべてリストされます。最初のファイルがバックグラウンド レイヤになり、他のレイヤは先行するレイヤの上に配置されるため、順序が重要です。

シェープ ファイルとデータ ファイルを取得し、マップ ファイルを書き込んでから、5 つのファイルすべてを **$ISC_HOME/resources/webserver/tomcat/webapps/ipsc-maps/data** ディレクトリに配置します。マップ ファイルはすべて、このフォルダに配置する必要があります。これが終了すると、自動的にトポロジ ビューアからこのマップにアクセスできるようになります。

マップのクリア

アクティブなマップをクリアするには、[Map] > [Clear] を選択します。

この機能を使用してアクティブ マップをクリア（削除）することにより、ノードおよびリンクだけが対応するネットワークに残る状態にします。

強調表示および属性の使用

[Graph] メニューは、グラフを管理し、操作するさまざまなツールへのアクセスを提供します。

JavaServer Pages を使用してノード、リンク、およびトンネルのリストを参照します。JSP ページからウィンドウの下部にある [display] ボタンを選択して要素を強調表示します。

[Graph] メニューのツールは、トポロジの表示を変更します。

これらについては、次の項を参照してください。

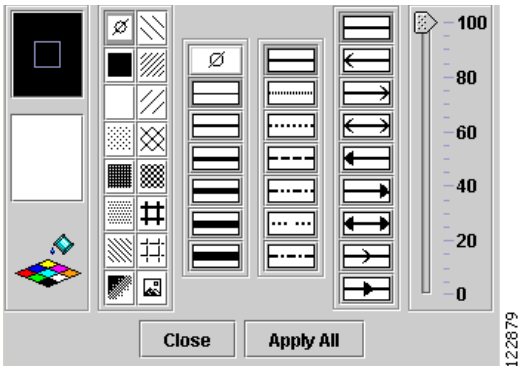
強調表示の解除

[Clear Highlighting] は、サブメニューにリストされている特定の要素で、強調表示を解除します。

属性の追加 / 変更

[Graph] メニューから [Attributes] を選択すると、図 7-31 の [Graphic Attributes] ウィンドウが表示されます。

図 7-31　Graphic Attributes



属性の追加 / 変更ツールは、次のように使用します。

ステップ 1　トポロジ表示にあるグラフ要素（ノードまたはリンク）を選択します。

複数の要素を選択するには、Ctrl/Shift を使用します。

ステップ 2　[Graph] > [Attributes] を選択し、[Graphic Attributes] ウィンドウを開きます。

ステップ 3　目的の属性を変更し、[Apply All] をクリックします。

（注）　選択したリンク（ステップ 1）だけが影響を受けます。

現在のグラフ レイアウトのクリア

現在のビューからトポロジ グラフを削除するには、[Graph] メニューの [Clear] 機能を使用します。

[Repository] メニューの [Layout Graph] でもグラフは削除されますが、[Layout Graph] ではグラフのクリアに加えて、リポジトリに最後に保存されたグラフの再作成も行われます。

[AntiAlias]、[BackingStore]、[DoubleBuffer] の使用

[Graph] メニューの [AntiAlias] は、パフォーマンスを犠牲にして、より滑らかなラインと気持ちのよい外観を生み出すために使用します。

[BackingStore] では、バックグラウンドになるとグラフィック コンテンツを自動的に保存し、フォアグラウンドに戻るとそれを再生成することができます。これによって、不必要な更新を回避できます。

[DoubleBuffer] は、グラフに要素をドラッグするためのダブルバッファリングを有効にします。

アルゴリズムの使用

[Algorithms] メニューでは、さまざまなアルゴリズムを使用して、グラフィック レイアウトを拡張する、およびそれ以外の場合は変更することができます。

（注）　アルゴリズムは、ノードがリンクと相互接続されている場合に限り機能します。

[Spring] は、重みに基づいてグラフィック レイアウトを最適化するグラフ レイアウト アルゴリズムです。

[Randomize] は現在のトポロジ レイアウトのノードをランダムに再配置します。

重複したリンクがある場合は、[Optimize Links] を選択してレイアウトを最適化できます。

スプリング設定は、ユーザの好みに従ってトポロジ表示の外観を拡張する場合に使用します。[Spring Settings] を選択すると、[Spring Settings] ウィンドウが表示されます。

サンプル コンフィグレット

この項に含まれるコンフィグレットは、特定のサービスおよび機能向けに Prime Provisioning によって生成された CLI を示しています。各コンフィグレット例では、次の情報を提供します。

- サービス
- 機能
- デバイス設定（ネットワーク ロール、ハードウェア プラットフォーム、デバイスの関係、およびその他の関連情報）
- 設定内の各デバイス用のサンプル コンフィグレット
- コメント

この項のすべてのサンプルでは、MPLS-TE コアの存在を想定しています。

（注）　Prime Provisioning によって生成されるコンフィグレットは、プロビジョニングする必要のある要素と現在デバイス上に存在する要素の差分にすぎません。つまり、関連する CLI がすでにデバイス上に存在する場合、その CLI は関連コンフィグレットには示されません。

ここでは、Cisco Prime Provisioning でのトラフィック エンジニアリング サービス プロビジョニングのコンフィグレットの例について説明します。

内容は次のとおりです。

プライマリ トンネル コンフィグレット（IOS）

設定

- サービス：MPLS-TE プライマリ トンネル
- 機能：プライマリ トンネルを導入するための MPLS TE コンフィグレット（IOS）
- デバイス設定：IOS 12.0(32)S を稼働する CISCO12410

コンフィグレット

IOS デバイスの設定	コメント
! **Explicit path:** ip explicit-path name isctmp2-isctmp8-1 enable next-address 10.2.2.145 next-address 10.2.2.174 !	指定したネクスト アドレス（トンネルが経由するストリクト パスを示す）によって明示的パスを作成します。 この明示的パスは、前述したプライマリ トンネルにより使用されます。
! **Primary tunnel:** interface Tunnel1000 description CISCO ISC-P24 ip unnumbered Loopback0 no ip directed-broadcast tag-switching ip tunnel destination 192.168.118.183 tunnel mode mpls traffic-eng tunnel mpls traffic-eng priority 0 0 tunnel mpls traffic-eng bandwidth 10 tunnel mpls traffic-eng affinity 0x0 mask 0x0 tunnel mpls traffic-eng path-option 1 explicit name isctmp2-isctmp8-1 tunnel mpls traffic-eng path-option 2 dynamic tunnel mpls traffic-eng record-route !	次の属性を使用して TE プライマリ トンネルを作成します。 - タグ スイッチング：このコマンドが生成されているのは、ポリシーで「mpls ip」フラグがイネーブルになっているためです。これにより、MPLS VPN トラフィックに対して TE トンネルを使用できるようになります。 - 宛先 192.168.118.183 - TE カプセル化 - セットアップ プライオリティと保持プライオリティはともに 0 - 帯域幅のグローバル プールは 10 kbps - トンネル アフィニティは 0x0 - 明示的な最初のパス オプション - 動的な 2 番目のパス オプション

帯域幅保護バックアップ トンネル コンフィグレット（IOS）

設定

- サービス：MPLS-TE と FRR（Fast Re-Route）
- 機能：このトンネルは、リンクまたはノードのいずれかの障害発生時にプライマリ トンネル トラフィックを保護します。
- デバイス設定：IOS 12.0(32)S を稼働する CISCO12410

コンフィグレット

IOS デバイスの設定	コメント
! Explicit path: ip explicit-path name isctmp5-isctmp4-1 enable next-address 10.2.2.145 next-address 10.2.2.174 !	指定したネクスト アドレス（トンネルが経由するストリクト パスを示す）によって明示的パスを作成します。 この明示的パスは、前述したバックアップ トンネルにより使用されます。
! Backup tunnel: interface Tunnel1001 description CISCO ISC-B30 ip unnumbered Loopback0 tunnel destination 192.168.118.213 tunnel mode mpls traffic-eng tunnel mpls traffic-eng backup-bw sub-pool 30000 tunnel mpls traffic-eng priority 0 0 tunnel mpls traffic-eng affinity 0x0 mask 0x0 tunnel mpls traffic-eng path-option 1 explicit name isctmp5-isctmp4-1 tunnel mpls traffic-eng record-route !	次の属性を使用して TE バックアップ トンネルを作成します。 - 宛先 192.168.118.213 - TE カプセル化 - サブプールの帯域幅を 30000 kbps 保護 - セットアップ プライオリティと保持プライオリティはともに 0 - トンネル アフィニティは 0x0 - 明示的な最初のパス オプション
interface POS0/1 mpls traffic-eng backup-path tunnel 1001 !	バックアップ トンネル 1001 でインターフェイス POS0/1 を保護

接続保護バックアップ トンネル コンフィグレット（IOS）

設定

- サービス：MPLS-TE と FRR（Fast Re-Route）
- 機能：接続保護バックアップ トンネルおよび関連する除外アドレス パスを導入するための MPLS TE コンフィグレット（IOS）
- デバイス設定：IOS 12.0(32)S を稼働する CISCO12410

コンフィグレット

IOS デバイスの設定	コメント
! **Explicit path:** ip explicit-path name L47-excl enable exclude-address 192.168.1.18 ! !	除外アドレス（パスで回避する必要がある IP アドレスを示す）によって明示的パスを作成します。この明示的パスは、前述したバックアップ トンネルにより使用されます。

! **Backup tunnel:**
interface Tunnel1000
  description CISCO ISC-B1
  ip unnumbered Loopback0
  tunnel mode mpls traffic-eng
  tunnel destination 10.52.96.38
  tunnel mpls traffic-eng priority 0 0
  no tunnel mpls traffic-eng bandwidth
  tunnel mpls traffic-eng path-option 1
explicit name L47-excl
  tunnel mpls traffic-eng affinity 0x0 mask
0x0
  tunnel mpls traffic-eng backup-bw
sub-pool unlimited
  tunnel mpls traffic-eng record-route
!
	次の属性を使用して TE バックアップ トンネルを作成します。
	- 宛先 10.52.96.38
	- TE カプセル化
	- セットアップ プライオリティと保持プライオリティはともに 0
	- バックアップ トンネルによる帯域幅の予約なし
	- 明示的な最初のパス オプション
	- トンネル アフィニティは 0x0
	- サブプール保護のためのバックアップ帯域幅は無制限

interface ATM4/0.1 point-to-point mpls traffic-eng backup-path Tunnel1000	ATM インターフェイスにバックアップ パスを設定します。

CBTS を使用した TE トラフィック アドミッション コンフィグレット（IOS）

設定

- サービス：TE トラフィック アドミッション
- 機能：Class-Based Tunnel Selection（CBTS; クラスベース トンネル選択）を使用してトラフィックをアドミッションするための MPLS TE コンフィグレット（IOS）
- デバイス設定：IOS 12.0(32)S を稼働する CISCO12410

コンフィグレット

IOS デバイスの設定	コメント
! **TE Traffic Admission using CBTS:** interface Tunnel1000 tunnel mpls traffic-eng exp 1 2 3 ! ! **Static route:** ip route 192.168.118.189 255.255.255.255 Tunnel1000	EXP ビット 1、2 または 3 のトラフィックを選択した場合のクラスベース トンネル選択 スタティック ルートを作成し、192.168.118.189 宛ての全トラフィックを上記で設定したトンネル 1000 に向けて許可します。

次に、上記の項目は、「プライマリ トンネル コンフィグレット（IOS）」（P.7-93）のような既存のプライマリ トンネルに展開されます。

TE トラフィック アドミッション コンフィグレット（IOS）

設定

- サービス：TE トラフィック アドミッション
- 機能：TE トラフィック アドミッションの MPLS TE コンフィグレット（IOS）
- デバイス設定：IOS 12.2(33)SRA を稼働する OSR-7609

コンフィグレット

IOS デバイスの設定	コメント

! **TE Traffic Admission:**
interface Tunnel1000
  tunnel mpls traffic-eng autoroute announce
  tunnel mpls traffic-eng autoroute metric relative 0
	相対メトリック 0（デフォルト）を使用した自動ルート通知

次に、上記の項目は、「プライマリ トンネル コンフィグレット（IOS）」（P.7-93）のような既存のプライマリ トンネルに展開されます。

プライマリ トンネル コンフィグレット（IOS XR）

設定

- サービス：MPLS-TE プライマリ トンネル
- 機能：プライマリ トンネルを導入するための MPLS TE コンフィグレット（IOS XR）
- デバイス設定：IOS XR 3.7.0 を稼働する CISCO12406

コンフィグレット

IOS デバイスの設定	コメント
! **Explicit path:** explicit-path name isctmp12-isctmp7-1 index 1 next-address ipv4 unicast 10.163.25.109 index 2 next-address ipv4 unicast 10.163.25.106 !	指定したネクスト アドレス（トンネルが経由するストリクト パスを示す）によって明示的パスを作成します。この明示的パスは、前述したプライマリ トンネルにより使用されます。
! **Primary tunnel:** interface tunnel-te133 description CISCO ISC-P2 ipv4 unnumbered Loopback0 priority 0 0 signalled-bandwidth 13 destination 192.168.118.214 fast-reroute path-option 1 explicit name isctmp12-isctmp7-1 path-option 2 dynamic record-route !	次の属性を使用して TE プライマリ トンネルを作成します。 - 宛先 192.168.118.214 - TE カプセル化 - セットアップ プライオリティは 0 - 保持プライオリティは 0 - グローバル プールから 13 kbps 予約 - トンネル アフィニティは 0x0 - 明示的な最初のパス オプション - 動的な 2 番目のパス オプション - トンネルで FRR をイネーブル化
mpls ldp interface tunnel-te 133 !	トンネル インターフェイスで LDP（ラベル配布プロトコル）をイネーブルにします。このコマンドが生成されているのは、ポリシーで「mpls ip」フラグがイネーブルになっているためです。これにより、MPLS VPN トラフィックに対して TE トンネルを使用できるようになります。

帯域幅保護バックアップ トンネル コンフィグレット（IOS XR）

設定

- サービス：MPLS-TE と FRR（Fast Re-Route）
- 機能：バックアップ トンネルを導入するための MPLS TE コンフィグレット（IOS XR）
- デバイス設定：IOS XR 3.7.0 を稼働する CISCO12406

コンフィグレット

IOS デバイスの設定	コメント
! **Explicit path:** explicit-path name isctmp8-isctmp9-1 index 1 next-address ipv4 unicast 10.163.25.109 index 2 next-address ipv4 unicast 10.163.25.106 ! ! **Backup tunnel:** interface tunnel-te1009 description CISCO ISC-B1411 ipv4 unnumbered Loopback0 priority 0 0 backup-bw 9600000 destination 10.163.24.131 path-option 1 explicit name isctmp8-isctmp9-1 record-route affinity 0 mask 0 ! mpls traffic-eng interface POS0/1/0/1 backup-path tunnel-te 1009	指定したネクスト アドレス（トンネルが経由するストリクト パスを示す）によって明示的パスを作成します。この明示的パスは、前述したバックアップ トンネルにより使用されます。 次の属性を使用して TE バックアップ トンネルを作成します。 - 宛先 10.163.24.131 - TE カプセル化 - 任意のプールの帯域幅を 9600000 kbps 保護 - セットアップ プライオリティと保持プライオリティは 0 - トンネル アフィニティは 0x0 - 明示的な最初のパス オプション

接続保護バックアップ トンネル コンフィグレット（IOS XR）

設定

- サービス：MPLS-TE と FRR（Fast Re-Route）
- 機能：接続保護バックアップ トンネルおよび関連する除外アドレス パスを導入するための MPLS TE コンフィグレット（IOS XR）
- デバイス設定：IOS XR 3.7.0 を稼働する CISCO12406

コンフィグレット

IOS デバイスの設定	コメント

! **Explicit path:**
explicit-path name L96-excl
  index 1 exclude-address ipv4 unicast 192.168.1.42
!
!
! **Backup tunnel:**
interface tunnel-te1000
  description CISCO ISC-B2
  ipv4 unnumbered Loopback0
  destination 10.52.96.37
  priority 0 0
  no signalled-bandwidth 0
  path-option 1 explicit name L96-excl
  affinity 0 mask 0
  backup-bw sub-pool unlimited
  record-route
!
mpls traffic-eng
  interface POS0/1/0/2
  backup-path tunnel-te 1000
!
	除外アドレス（パスで回避する必要がある IP アドレスを示す）によって明示的パスを作成します。この明示的パスは、前述したバックアップ トンネルにより使用されます。
	次の属性を使用して TE バックアップ トンネルを作成します。
	- 宛先 10.52.96.37
	- TE カプセル化
	- セットアップ プライオリティは 0
	- 保持プライオリティは 0
	- 明示的な最初のパス オプション
	- トンネル アフィニティは 0x0
	- 無制限のサブプールがバックアップ帯域幅として機能
	
	トンネル 1000 でインターフェイス POS0/1/0/2 を保護

PBTS を使用した TE トラフィック アドミッション コンフィグレット（IOS XR）

設定

- サービス：TE トラフィック アドミッション
- 機能：ポリシーベース トンネル選択（PBTS）を使用してトラフィックをアドミッションするための MPLS TE コンフィグレット（IOS XR）
- デバイス設定：IOS XR 3.7.0 を稼働する CISCO12406

コンフィグレット

IOS デバイスの設定	コメント

! **TE Traffic Admission using PBTS:**
interface tunnel-te133
  autoroute announce
  autoroute metric absolute 100
  policy-class 2
!
	絶対メトリック 100 を使用した自動ルート通知

次に、上記の項目は、「プライマリ トンネル コンフィグレット（IOS XR）」（P.7-98）のような既存のプライマリ トンネルに展開されます。

TE トラフィック アドミッション コンフィグレット（IOS XR）

設定

- サービス：TE トラフィック アドミッション
- 機能：TE トラフィック アドミッションの MPLS TE コンフィグレット（IOS XR）
- デバイス設定：IOS XR 3.7.0 を稼働する CISCO12406

コンフィグレット

IOS XR デバイス設定	コメント

! **TE Traffic Admission Using Static Route:**
router static
  address-family ipv4 unicast
  1.2.3.4/32 tunnel-te 1000 123
  !
!
	スタティック ルートを使用してトンネル 1000 に TE トラフィック アドミッションを設定

次に、上記の項目は、「プライマリ トンネル コンフィグレット（IOS XR）」（P.7-98）のような既存のプライマリ トンネルに展開されます。

警告および違反

このセクションは、Prime Provisioning で計画ツール（計算エンジン）を使用する場合に、呼び出されることがある違反と警告を示します。

警告と違反は、計画ツールに関連付けられます（「トラフィック エンジニアリング管理の概念」（P.7-115）の計画ツールの項を参照）。これらは、次の状況で発生します。

- プライマリ管理対象トンネルの監査、配置、修復、または調整の試行時。
- 選択したネットワーク要素（リンク、ルータ、または SRLG）の保護の試行時。ここでは、これらが、失敗した保護の原因の判断に役立ちます（「保護計画」（P.7-60）を参照）。

  特定の要素を保護できるかどうかを判断する場合にオフライン バックアップのルート生成が呼び出されると、バックアップ ルート ジェネレータは、各要素と、一連の要素を保護するトンネルまたは要素を保護できなかった理由の判断に役立つ一連の違反および警告のいずれかに応答します。

（注） 以下、用語 DirectedLink はルータ インターフェイスを示します。

ここでは、次の内容について説明します。

警告

このクラスの特徴は、すべてのレポートが警告であることです。警告は保護パスの計算の妨げにならないという点で、違反に比べて深刻でないと見なされます。

保護計算の警告

WarningFixVetoed

この要素の修正により、ネイバー要素が保護されなくなりました。この修正は拒否され、変更は提示されません。

WarningRouterNotConformant

この要素またはいずれかの隣接ルータはプロトコルに適合していません。したがって、保護できません。

フィールド：

- [Report Type]：レポート タイプの名前。
- [Description]：違反によって通知された問題の説明。
- [Non-conformant router]：トラフィック エンジニアリングをサポートしないルータ。

WarningTunnelBandwidthQuotaTooSmall

この要素を保護するバックアップ トンネルの帯域幅が、許容される最小の帯域幅キャパシティを下回っています。

フィールド：

- [Minimum allowed bandwidth quota]：当該の要素の保護に許可された最小帯域幅。
- [Actual tunnel bandwidth quota]：バックアップ トンネルの実際の帯域幅。

WarningTunnelNumberTooLarge

この要素を通過するフローに対するバックアップ トンネルが多すぎます。

フィールド：

- [Maximum tunnel number allowed]：特定のネットワーク要素に対して許可されるトンネルの最大数。
- [Actual Tunnel Count]：このネットワーク要素に課されるトンネルの実際の数。
- [Flow]：
  - [Maximum Bandwidth]：保護する必要のあるトラフィック フローの最大帯域幅。
  - [Head Links]：このフローの保護済みインターフェイス。
  - [Through Router]：通常のトラフィック フローが通過する保護済みデバイス。保護済みの要素がリンクである場合は、[Through Router] フィールドは表示されません。
  - [Tail Router]：宛先（テール）ルータのホスト名。
  - [Type]（NHop、NNHop）：ネクスト ホップ タイプ。リンク（ルータを介さない）の場合は [NHOP] で、ノードの場合は [NNHOP] です。

WarningZeroProtectedFlow

この要素を通過するフローはバックアップ トンネルによって保護されていますが、最大フローが 0 です。

フィールド：

- [Flow]：
  - [Maximum Bandwidth]：要素で使用可能な最大帯域幅。
  - [Head Links]：このフローの保護済みインターフェイス。
  - [Through Router]：通常のトラフィック フローが通過する保護済みデバイス。保護済みの要素がリンクである場合は、[Through Router] フィールドは表示されません。
  - [Tail Router]：宛先（テール）ルータのホスト名。
  - [Type]（NHop、NNHop）：ネクスト ホップ タイプ。リンク（ルータを介さない）の場合は [NHOP] で、ノードの場合は [NNHOP] です。

違反

このクラスの特徴は、すべてのレポートが違反であることです。警告と異なり保護パスの計算の妨げとなるため、これらは警告よりも「深刻」であると見なされます。

初期配置計算違反

ViolationFrrProtectionInadequate

トンネルの FRR 保護は、指定された保護レベルを満たしていません。

フィールド：

- [Report Type]：レポート タイプの名前。
- [Description]：違反によって通知された問題の説明。
- [Required FRR Protection Level]：バックアップ トンネルが存在しており、リンク障害が発生した場合に、MPLS トラフィック エンジニアリング トンネルで、バックアップ トンネルの使用をイネーブルにするために使用します。可能なレベルは、[None]、[Best Effort]、[Link and SRLG]、および [Link, SRLG and Node] です。
- [Primary Tunnel]：
  - [Name]：名前とトンネル番号で構成されたトンネル識別子。
  - [Head]：ヘッド ルータのホスト名。
  - [Tail]：宛先（テール）ルータのホスト名。
- [Path]：トンネルパス。
  - [Node]：デバイスのホスト名。保護レベルが [Link, SRLG & Node] の場合に限り表示されます。
  - [Protected (Node)]：各ノードが保護されている（[Yes]）か、保護されていない（[No]）かを示します。保護レベルが [Link, SRLG & Node] の場合に限り表示されます。
  - [Link Label]：リンクのインターフェイスの IP アドレス。
  - [Protected (Link)]：各リンクが保護されている（[Yes]）か、保護されていない（[No]）かを示します。

ViolationInconsistentResourceAttributeChanges

リソース上の 1 つ以上の属性を変更しようとするトポロジ変更が原因で、属性のペアの 1 つが一致しなくなります。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Resource]：
  - [Id]：ネットワーク リソースを表すヘッド デバイスまたはヘッド インターフェイスの ID。
  - [Type]：リソース デバイスまたはインターフェイス。
- [Attributes]：
  - [Attribute]：一致していない属性の名前。
  - [New Value]：ユーザが指定する新規属性値。

ViolationInconsistentTunnelAttributeChanges

トンネル上の 1 つ以上の属性を変更しようとするトンネル変更が原因で、属性のペアの 1 つが一致しなくなります。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Tunnel]：
  - [Name]：名前とトンネル番号で構成されたトンネル識別子。
  - [Head]：ヘッド ルータのホスト名。
  - [Tail]：宛先（テール）ルータのホスト名。
- [Attributes]：
  - [Attribute]：一致していない属性の名前。
  - [New Value]：ユーザが指定する新規属性値。

ViolationLinkAffinityMismatch

プライマリ トンネルのパスに含まれている有向リンクの少なくとも 1 つに、トンネルのアフィニティ ビットおよびマスクと一致する属性フラグがありません。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Primary Tunnel]：
  - [Name]：名前とトンネル番号で構成されたトンネル識別子。
  - [Head]：ヘッド ルータのホスト名。
  - [Tail]：宛先（テール）ルータのホスト名。
  - [Affinity Bits/Mask]：トンネルのアフィニティ ビットおよびマスク。
- [Path]：トンネル パスの名前。
  - [Outgoing Interface]：発信インターフェイスのホスト名や IP アドレス。
  - [Attribute Flags]：比較する属性とトンネルのアフィニティ ビットをリンクします。有効なパスを持たせるには、すべてが同一でなければなりません。少なくとも 1 つが異なる場合、違反がトリガーされます。

ViolationLinkPoolOversubscribed

有向リンクに指定された帯域幅プールが、パススルーするプライマリ トンネルによってオーバー サブスクライブされました。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Directed Link]：
  - [Head Device/Interface]：ヘッド デバイスのホスト名およびインターフェイスの IP アドレス。
  - [Tail Device/Interface]：宛先（テール）デバイスまたはインターフェイスのホスト名。
  - [Pool]：グローバル プールまたはサブプール。
  - [Pool Bandwidth]：リンク上で割り当てられたグローバル プールまたはサブプールの帯域幅。
- [Primary Tunnel (table)]：リンク リソースを使用しているトンネルの数を指定します。
  - [Name]：名前とトンネル番号で構成されたトンネル識別子。
  - [Head]：ヘッド ルータのホスト名。
  - [Tail]：宛先（テール）ルータのホスト名。
  - [Bandwidth]：トンネルの合計帯域幅。
  - [Pool]：グローバル プールまたはサブプール。
  - [Path]：トンネル パスの名前。

ViolationMaxReRoutesExceeded

このソリューションのプライマリ トンネル リルートの数は、指定された最大数を超えています。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Number of re-routes in solution]：計算エンジンによって推奨されたリルートの数。
- [Specified maximum number of re-routes]：許容されるリルートの最大数。

ViolationNoPathInLayout

トポロジにすでに配置されている他のプライマリ トンネルがある場合、要求したプライマリ トンネルに正規パスは使用できません。（注）ユーザ要求のパスに示されたこの違反は、他のプライマリ トンネルが存在するために、要求したパスにプライマリ トンネルを配置できなかったことだけを意味します。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Requested Primary Tunnel]：
  - [Name]：名前とトンネル番号で構成されたトンネル識別子。
  - [Head]：ヘッド ルータのホスト名。
  - [Tail]：宛先（テール）ルータのホスト名。
  - [Bandwidth]：トンネルの合計帯域幅。
  - [Requested Path]：トンネルのユーザ指定のパス。

- [Pool]：グローバル プールまたはサブプール。
- [FrrProtection]：可能な保護レベルは、[None]、[Best Effort]、[Link and SRLG]、および [Link, SRLG and Node] です。
- [Propagation Delay]：トラフィックがリンクに沿ってヘッド インターフェイスからテール インターフェイスまで移動する時間。
- [AffinityBits/Mask]：トンネルのアフィニティ ビットおよびマスク。

ViolationNoPathInTopology

トポロジに配置されている他のプライマリ トンネルにかかわらず、要求したプライマリ トンネルに有効なパスは使用できません。（注）ユーザ要求のパスに示されたこの違反は、他のトンネルとは関係なく、要求したパスにプライマリ トンネルを配置できなかったことだけを意味します。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Requested Primary Tunnel]：
  - [Name]：名前とトンネル番号で構成されたトンネル識別子。
  - [Head]：ヘッド ルータのホスト名。
  - [Tail]：（宛先）テール ルータのホスト名。
  - [Bandwidth]：トンネルの合計帯域幅。
  - [Requested Path]：トンネルのユーザ指定のパス。
  - [Pool]：グローバル プールまたはサブプール。
  - [FrrProtection]：可能な保護レベルは、[None]、[Best Effort]、[Link and SRLG]、および [Link, SRLG and Node] です。
  - [Propagation Delay]（任意）：トラフィックが要求されたパスに沿って移動するときに許容される最大時間。
  - [AffinityBits/Mask]：トンネルのアフィニティ ビットおよびマスク。

ViolationNoTunnelForDemand

ネットワークにはこのトンネルで使用できる有効なパスはありますが、要求されたプライマリ トンネルを実装しているパスはありません。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Requested Primary Tunnel]：
  - [Name]：名前とトンネル番号で構成されたトンネル識別子。
  - [Head]：ヘッド ルータのホスト名。
  - [Tail]：宛先（テール）ルータのホスト名。
  - [Bandwidth]：トンネルの合計帯域幅。
  - [Requested Path]：トンネルのユーザ指定のパス。
  - [Pool]：グローバル プールまたはサブプール。

- [FrrProtection]：可能な保護レベルは、[None]、[Best Effort]、[Link and SRLG]、および [Link, SRLG and Node] です。
- [Propagation Delay]（任意）：トラフィックが要求されたパスに沿って移動するときに許容される最大時間。
- [AffinityBits/Mask]：トンネルのアフィニティ ビットおよびマスク。

ViolationPathMismatch

プライマリ トンネルのパスが、ユーザ指定パスに指定されたパスと異なります。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Primary Tunnel]：
  - [Name]：名前とトンネル番号で構成されたトンネル識別子。
  - [Head]：ヘッド ルータのホスト名。
  - [Tail]：宛先（テール）ルータのホスト名。
  - [Actual Path]：違反と関連付けられたトンネルの実際のパス。
  - [Requested Path]：トンネルのユーザ指定のパス。

ViolationPathNotConnected

プライマリ トンネルのパスが「接続」されていません。つまり、アップ管理ステータスのリンクによる接続シーケンスがトンネルのヘッドとテールの間に形成されていないか、ループを含んでいます。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Primary Tunnel]：
  - [Name]：名前とトンネル番号で構成されたトンネル識別子。
  - [Head]：ヘッド ルータのホスト名。
  - [Tail]：宛先（テール）ルータのホスト名。
  - [Path]：トンネル パスの名前。

ViolationPathUsesMissingLinks

トンネル変更により、パスまたは「ユーザ要求のパス」がこのトポロジに存在しない 1 つ以上の有向リンクを使用するようにトンネルを作成または変更しようとしています。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Primary Tunnel]：
  - [Name]：名前とトンネル番号で構成されたトンネル識別子。
  - [Head]：ヘッド ルータのホスト名。
  - [Tail]：宛先（テール）ルータのホスト名。
  - [Change Type]：[Add Tunnel] または [Modify Tunnel]。

- [Path Type]：[Requested] または [Actual]。
- [Path]：トンネル パスの名前。
- [Outgoing Interface]：リンクが欠落しているかどうかに従い [Yes] または [No]。
- [Incoming Interface]：リンクが欠落しているかどうかに従い [Yes] または [No]。

ViolationPrimaryTunnelDelayTooLong

プライマリ トンネルの伝搬遅延は、指定されている [Maximum Propagation Delay] を超えています。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Required Max Propagation Delay]：トラフィックが要求したパスに沿って移動するときに許容される最大時間。
- [Primary Tunnel]：
  - [Name]：名前とトンネル番号で構成されたトンネル識別子。
  - [Head]：ヘッド ルータのホスト名。
  - [Tail]：宛先（テール）ルータのホスト名。
  - [Path]：トンネル パスの名前。
  - [Actual Propagation Delay]（テーブル）：トラフィックがパス全体の各リンクに沿って移動するときにかかる時間。

    - [Link]：パス内のリンク セグメント。

    - [Propagation Delay]：トラフィックが各リンク セグメントを移動する時間。

ViolationResourceIdUnknown

ID を指定してリソース（リンク、ルータ、または SRLG）を削除または変更しようとしたときに、指定された ID のリソースが存在していません。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Resource to be removed]：
  - [Id]：ネットワーク リソースを表すヘッド デバイスまたはヘッド インターフェイスの ID。
  - [Type]：リソース デバイスまたはインターフェイス。

ViolationTunnelIdInUse

すでに存在している ID を指定してプライマリ トンネルを追加しようとしています。

フィールド：

- [Report Type]：品質レポート、警告レポート、または違反レポート。
- [Description]：違反によって通知された問題の説明。
- [Tunnel to Add]：
  - [Name]：名前とトンネル番号で構成されたトンネル識別子。
  - [Head]：ヘッド ルータのホスト名。

  - [Tail] : 宛先（テール）ルータのホスト名。
- 既存のトンネル：
  - [Name] : 名前とトンネル番号で構成されたトンネル識別子。
  - [Head] : ヘッド ルータのホスト名。
  - [Tail] : 宛先（テール）ルータのホスト名。

ViolationTunnelIdUnknown

ID を指定してプライマリ トンネルの削除または変更しようとしたときに、指定された ID のトンネルが存在していません。

フィールド：

- [Report Type] : 品質レポート、警告レポート、または違反レポート。
- [Description] : 違反によって通知された問題の説明。
- [Tunnel to Remove] :
  - [Id] : Prime Provisioning で使用される一意のトンネル識別子。

保護計算違反

ViolationAggregateBandwidthOnLink

この要素は、このリンクを通過しますが、バックアップ トンネルの帯域幅に設定されている最大帯域幅クォータは、このリンクのバックアップ帯域幅を超えています。

フィールド：

- [Required Bandwidth]（トンネル起因）：リンク上のトンネルの必須帯域幅。
- [Link] :
  - [Backup Bandwidth] : リンクの使用可能な合計帯域幅。
  - [Head Router] : ヘッド ルータのホスト名。
  - [Head Interface] : ヘッド インターフェイスの IP アドレス。
  - [Tail Router] : 宛先（テール）ルータのホスト名。
  - [Tail Interface] : 宛先（テール）インターフェイスの IP アドレス。
  - [Label] : リンク上のインターフェイスの IP アドレス。
  - [Admin Status] : リンクが**アップ**なのか**ダウン**なのかを示します。

ViolationBadBackupTunnel

トンネルは、この要素越しのフローを保護しません。

ViolationBandwidthProtectionMismatch

フローを保護しているすべてのトンネルのトンネル バックアップ帯域幅クォータの合計は、フローの最大帯域幅と一致していません。

フィールド：

- [Protected bandwidth] : 保護パスの保護可能な帯域幅。
- [Flow] :
  - [Maximum Bandwidth] : 要素で使用可能な最大帯域幅。

- [Head Links]：このフローの保護済みインターフェイス。
- [Through Router]：通常のトラフィック フローが通過する保護済みデバイス。保護済みの要素がリンクである場合は、[Through Router] フィールドは表示されません。
- [Tail Router]：宛先（テール）ルータのホスト名。
- [Type]（NHop、NNHop）：ネクスト ホップ タイプ。リンク（ルータを介さない）の場合は [NHOP] で、ノードの場合は [NNHOP] です。

ViolationLinkLevelTunnelDelayTooLarge

バックアップ トンネルの遅延は許容値を超えています。

フィールド：

- [Maximum allowed delay]：バックアップ トンネルで許容される最大遅延。
- [Actual delay of tunnel]：バックアップ トンネルの実際の遅延。

ViolationNoBackupTunnels

要素を通過するこのフローを保護しているバックアップ トンネルはありません。

フィールド：

- [Flow]：
  - [Maximum Bandwidth]：要素で使用可能な最大帯域幅。
  - [Head Links]：このフローの保護済みインターフェイス。
  - [Through Router]：通常のトラフィック フローが通過する保護済みデバイス。保護済みの要素がリンクである場合は、[Through Router] フィールドは表示されません。
  - [Tail Router]：宛先（テール）ルータのホスト名。
  - [Type]（NHop、NNHop）：ネクスト ホップ タイプ。リンク（ルータを介さない）の場合は [NHOP] で、ノードの場合は [NNHOP] です。

ViolationPassesThroughSRLG

バックアップ トンネルは、Shared Risk Link Group（SRLG; 共有リスク リンク グループ）に含まれるリンクから開始されているこの要素を通過するフローを保護しています。一方、このトンネルは、同じ SRLG 内の別のリンクも通過しています。

フィールド：

- [Link]：
  - [Backup Bandwidth]：リンクの使用可能な合計帯域幅。
  - [Head Router]：ヘッド ルータのホスト名。
  - [Head Interface]：ヘッド インターフェイスの IP アドレス。
  - [Tail Router]：宛先（テール）ルータのホスト名。
  - [Tail Interface]：宛先（テール）インターフェイスの IP アドレス。
  - [Label]：リンク上のインターフェイスの IP アドレス。
  - [Admin Status]：リンクが**アップ**なのか**ダウン**なのかを示します。
- [SRLG]：ユーザ定義の SRLG 名。
- [Flow]：
  - [Maximum Bandwidth]：要素で使用可能な最大帯域幅。

- [Head Links]：このフローの保護済みインターフェイス。
- [Through Router]：通常のトラフィック フローが通過する保護済みデバイス。保護済みの要素がリンクである場合は、[Through Router] フィールドは表示されません。
- [Tail Router]：宛先（テール）ルータのホスト名。
- [Type]（NHop、NNHop）：ネクスト ホップ タイプ。リンク（ルータを介さない）の場合は [NHOP] で、ノードの場合は [NNHOP] です。

ViolationUsesFailedElement

この要素を保護するバックアップ トンネルでもこの要素を使用しています。

ドキュメント タイプ定義（DTD）ファイル

ドキュメント タイプ定義（DTD）ファイルは、Prime Provisioning へのバルク データ インポート用の XML インポート ファイルに必要なルールを提供します。

Prime Provisioning へのトンネルのインポート方法の手順については、「プライマリ トンネルのインポート」（P.7-52）を参照してください。

ここでは、次の内容について説明します。

DTD ファイル

これは、Prime Provisioning に付属している DTD ファイルです。

```
<?xml version="1.0" encoding="UTF-8"?>

<!-- Data Definition for file based tunnel import -->

<!-- Import File Structure -->
<!ELEMENT IMPORT_DATA (TUN_ADD|TUN_CHANGE|TUN_DELETE|TUN_MIGRATE)+ >

<!-- Notes on attributes:
     importId:must be unique within the file,
          it is alphanumeric, must begin with alpha character,
          and no special character
     head, tail:hostname of valid TE enabled device
     policy:name of existing managed tunnel policy
     bw: must be numeric and values between 0-2147483647
     tnum:is the number portion of a tunnel interface
          E.g. for "interface tunnel3", use tnum="3"
          must be numeric and values between 0-65535
-->


<!-- Tunnel Add

   - #IMPLIED attributes are optional, if not specified, defaults to null
   - If tnum is not specified, system will generate tunnel number
   - To enable auto bandwidth, specify AUTOBW element
```

```
   - bw is required if autobw is not enabled
   - By default, tunnel will be created with a system path and a dynamic path

-->

<!ELEMENT TUN_ADD (AUTOBW?)>
<!ATTLIST TUN_ADD
         importId ID #REQUIRED
    head CDATA #REQUIRED
    tail CDATA #REQUIRED
    policy CDATA #REQUIRED
    bw CDATA #IMPLIED
    tnum CDATA #IMPLIED>


<!-- Tunnel Change

  - #IMPLIED attributes are optional, if not specified, value on existing
    tunnel is kept
  - To enable auto-bw, or to change auto-bw parameters, specify AUTOBW element
  - To disable auto-bw, set disableAutoBw="yes" and do not specify AUTOBW element
  - Existing tunnel path cannot be changed directly, setting reroutable="true"
    will enable system to reroute the tunnel if necessary

-->

<!ELEMENT TUN_CHANGE (AUTOBW?)>
<!ATTLIST TUN_CHANGE
         importId ID #REQUIRED
    head CDATA #REQUIRED
    tnum CDATA #REQUIRED
    policy CDATA #IMPLIED
    bw CDATA #IMPLIED
    disableAutoBw (yes) #IMPLIED
    reroutable (true|false) #IMPLIED>


<!-- Tunnel Delete

  - all attributes are required to identify tunnel to be deleted

-->

<!ELEMENT TUN_DELETE EMPTY>
<!ATTLIST TUN_DELETE
         importId ID #REQUIRED
    head CDATA #REQUIRED
    tnum CDATA #REQUIRED>


<!-- Tunnel Migrate

  - #IMPLIED attributes are optional, if not specified, value on existing
    tunnel is kept
  - All comments under Tunnel Change (above) applies to Tunnel Migrate
  - only unmanaged primary tunnel can be migrated
  - for tunnels with unmanaged tunnel policy, must specify a managed policy
  - for tunnels that was non-conformant:
         . if bw was zero, specify a new bw or enable auto-bw
         . if path was dynamic or non-conformant, the path options will be
           replaced with a system path and a dynamic path, and reroutable will
           be set to true.
  - reroutable attribute applicable only for tunnel that had a conformant first
         explicit path (i.e. explicit path with no loopback)
```

```
-->

<!ELEMENT TUN_MIGRATE (AUTOBW?)>
<!ATTLIST TUN_MIGRATE
         importId ID #REQUIRED
    head CDATA #REQUIRED
    tnum CDATA #REQUIRED
         policy CDATA #IMPLIED
         bw CDATA #IMPLIED
    disableAutoBw (yes) #IMPLIED
         reroutable (true|false) #IMPLIED>


<!-- Auto Bandwdith

  - #IMPLIED attributes are optional, if not specified, value is set to null
    for TUN_ADD and existing value is kept TUN_CHANGE
  - maxBw is required when used in TUN_ADD or if existing tunnel is not auto-bw
    enabled
  - minBw and maxBw must be numeric and values between 0-2147483647
  - maxBw must be greater than minBw if specified
  - freq must be numeric and values between 300-604800

-->

<!ELEMENT AUTOBW EMPTY>
<!ATTLIST AUTOBW
    freq CDATA #IMPLIED
    minBw CDATA #IMPLIED
    maxBw CDATA #IMPLIED>
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE IMPORT_DATA SYSTEM "TeImport.dtd">

<IMPORT_DATA>

<!--  Add New Managed Tunnel -->
<TUN_ADD importId="a1" head="isctmp3" tail="isctmp1" policy="mgdPolicy" bw="400" />
<TUN_ADD importId="a2" head="isctmp2" tail="isctmp9" policy="mgdPolicy" >
  <AUTOBW freq="300" minBw="100" maxBw="200"/>
</TUN_ADD>

<!--  Modify Existing Tunnel -->
<TUN_CHANGE importId="c1" head="isctmp2" tnum="200" bw="30" />
<TUN_CHANGE importId="c2" head="isctmp4" tnum="2" policy="mgdPolicy" reroutable="true"/>
<TUN_CHANGE importId="c3" head="isctmp5" tnum="46">
  <AUTOBW freq="300" minBw="100" maxBw="200"/>
</TUN_CHANGE>
<TUN_CHANGE importId="c4" head="isctmp2" tnum="200" bw="30" disableAutoBw="yes"/>

<!--  Delete Existing Tunnel -->
<TUN_DELETE importId="d1" head="isctmp3" tnum="45"/>

<!--  Migrate Tunnel -->
<TUN_MIGRATE importId="m1" head="isctmp2" tnum="3" policy="mgdPolicy"/>
<TUN_MIGRATE importId="m2" head="isctmp5" tnum="1" policy="mgdPolicy"/>

</IMPORT_DATA>
```

例

次に、「DTD ファイル」（P.7-112）で指定した DTD ファイルに準拠する、トンネル インポートの XML ファイルの例を示します。これは、追加、変更、削除、および移行操作の各サンプル ブロックで構成されています。

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE IMPORT_DATA SYSTEM "TeImport.dtd">

<IMPORT_DATA>

<!--  Add New Managed Tunnel -->
<TUN_ADD importId="a1" head="isctmp3" tail="isctmp1" policy="mgdPolicy" bw="400" />
<TUN_ADD importId="a2" head="isctmp2" tail="isctmp9" policy="mgdPolicy" >
  <AUTOBW freq="300" minBw="100" maxBw="200"/>
</TUN_ADD>

<!--  Modify Existing Tunnel -->
<TUN_CHANGE importId="c1" head="isctmp2" tnum="200" bw="30" />
<TUN_CHANGE importId="c2" head="isctmp4" tnum="2" policy="mgdPolicy" reroutable="true"/>
<TUN_CHANGE importId="c3" head="isctmp5" tnum="46">
  <AUTOBW freq="300" minBw="100" maxBw="200"/>
</TUN_CHANGE>
<TUN_CHANGE importId="c4" head="isctmp2" tnum="200" bw="30" disableAutoBw="yes"/>

<!--  Delete Existing Tunnel -->
<TUN_DELETE importId="d1" head="isctmp3" tnum="45"/>

<!--  Migrate Tunnel -->
<TUN_MIGRATE importId="m1" head="isctmp2" tnum="3" policy="mgdPolicy"/>
<TUN_MIGRATE importId="m2" head="isctmp5" tnum="1" policy="mgdPolicy"/>

</IMPORT_DATA>
```

トラフィック エンジニアリング管理の概念

この章では、Cisco Prime Provisioning の概要と、このマニュアルで使用されるいくつかの概念について説明します。この章の内容は、次のとおりです。

– 「ポリシーベース トンネル選択」（P.7-123）。

Prime ProvisioningTEM の概要

TEM は、Prime Provisioning のトラフィック エンジニアリング管理モジュールです。トラフィックの Service Level Agreement（SLA; サービス レベル契約）に基づく保証の提供を目的として Multiprotocol Label Switching Traffic Engineering（MPLS TE; マルチプロトコル ラベル スイッチング）プライマリ トンネルおよびバックアップ トンネルを管理するためのツールです。帯域幅保護管理、ネットワーク検出、および MPLS TE の設定のサポートを提供します。また、高度なプライマリ パス計算ツールや要素保護のためのバックアップ トンネル計算機能など、多くの強力な計画ツールが含まれています。

予測可能性の要件、QoS 要件に適合するトラフィック フロー、および保証帯域幅による迅速な復旧をサポートするための MPLS TE メカニズムを搭載しており、厳格な SLA パフォーマンス基準（アベイラビリティ、遅延、ジッター）を確実に満たします。

Prime Provisioning の機能

Prime Provisioning は、さまざまな MPLS TE プライマリ管理機能を追加します。

- トンネル監査：トンネルの変更後に不一致を検出します。
- トンネル アドミッション：新しいトンネルをネットワークに受け入れます。
- トンネル修復：ネットワークやサービスの変更後にトンネルの不一致を解決します。
- ネットワーク グルーミング：ネットワーク全体の利用を最適化します。

さらに、Prime Provisioning は次のような Prime Provisioning 機能との連携および統合も実現します。

- サービス アクティベーション フォーカス
- 他の Prime Provisioning モジュールとの統合
- データ パーシステンス
- ユーザの目的のロギング
- サービス状態の管理
- サービスの監査
- Web ベースの GUI
- Role Based Access Control（RBAC; ロール ベース アクセス コントロール）

Prime ProvisioningTEM の基礎

Prime Provisioning の動作方法を理解するには、最初に特定の重要な概念を知っておく必要があります。

管理対象 / 管理対象外プライマリ トンネル

Prime Provisioning では、管理対象トンネルの概念が TE 計画アクティビティの中心にあります。

次の違いを理解しておくことが重要です。

- 管理対象 TE トンネル：

  - （設定/保持）優先順位が 0
  - 0 以外の RSVP 帯域幅
  - 明示的な最初のパス オプション
  - 自動帯域幅には最大値が必要
- 管理対象外トンネル：他のすべてのトンネル。

Prime Provisioning のグラフィカル ユーザ インターフェイス（GUI）には、管理対象トンネルと管理対象外トンネルを操作するための別個のエントリ ポイントがあります。

Conformant/Non-Conformant トンネル

Conformant トンネルと Non-Conformant トンネルについて理解することは、Prime Provisioning を効率的に使用するために不可欠です。

Prime Provisioning は Conformant トンネルのみを作成できます。Non-conformant トンネルは、TE 検出プロセスを介して導入できます（ユーザ ガイドの「TE ネットワーク検出」（P.7-11）を参照）。

Conformant/Non-Conformant トンネルの定義

Prime Provisioning の設計では、Conformant トンネルと Non-Conformant トンネルは明確に区別されています。

- Conformant トンネル：Prime Provisioning の TE 管理パラダイム（下記を参照）を満たす正常に動作するトンネルです。管理対象トンネルは Conformant トンネルにのみなることができます。0 以外の優先順位の管理対象トンネルも Conformant トンネルになることができます。ただし、Conformant トンネルは必ずしも管理対象トンネルではありません。

  接続保護トンネルは、トンネル帯域幅が 0 で、バックアップ帯域幅が無制限であり、最初のパス オプションが「exclude address」である場合は、Conformant = true とマークされます。BW 保護設定では、トンネルに 0 以外のバックアップ帯域幅、およびストリクト パス オプション 1 が定義されている必要があります。
- Non-Conformant トンネル：Prime Provisioning の帯域幅保証を満たす能力に影響する可能性のある TE トンネルです。自動帯域幅に最大帯域幅が未設定、プリエンプションの可能性、ダイナミック パスなど、未知の帯域幅要件が原因で発生することがあります。優先順位が 0 である管理対象外トンネルも Non-Conformant トンネルになることがあります。

  次に、Non-Conformant トンネルの例を示します。
  - 設定および保持優先順位が 0 で、最初のパス オプションが明示パスであるが、帯域幅は 0 であるトンネル
  - 設定および保持優先順位が 0 で、帯域幅は 0 以外であるが、最初のパス オプションがダイナミック パスであるトンネル
  - 設定および保持優先順位が 0 で、明示パス オプションが 1 であり、自動帯域幅の最大値が定義されていないトンネル
  - Conformant = false とマークされた接続保護トンネルは、バックアップ トンネルのために予約されており、トンネル帯域幅 0、無制限のバックアップ帯域幅、最初のパス オプション「exclude address」のいずれも設定されていません。

  上記のトンネルは、なぜ Non-Conformant なのでしょうか。Prime Provisioning は、設定および保持優先順位が 0 であるトンネルをすべて管理し、それらが通過するリンクがいずれも十分な帯域幅を持ち、アフィニティが一致、TE ポリシーに定義された遅延または FRR 制約に違反しないことを確認するからです。

ただし、トンネルのパスがダイナミック パスであるか、トンネルが必要とする帯域幅の量が定義されていない場合、Prime Provisioning はトンネルの管理に必要な情報を得られないため、そのトンネルを Non-Conformant とマークします。すべての Non-Conformant トンネルは [TE Unmanaged Primary Tunnels SR] ウィンドウに表示されます。

Non-Conformant トンネルの管理

Non-Conformant トンネルは、SLA 違反の原因となる可能性があるだけでなく、管理対象トンネルに悪影響（帯域幅を奪うなど）を与えるおそれもあることを理解しておくことが重要です。

ただし、Non-Conformant トンネルが検出されると、警告がログに記録されます。Prime Provisioning は、Non-Conformant トンネルを追跡して廃棄します。

したがって、Conformant トンネルの方が望ましいと言えます。Conformant トンネルによって、システムは管理対象トンネルの帯域幅保証を提供できます。管理対象外の Non-Conformant トンネルは、必要な帯域幅を提供したりしなかったりするため、帯域幅保証は提供されません。

Non-Conformant トンネルがある場合は、設定および保持優先順位を 0 以外の値に変更する（管理対象トンネルに対するプリエンプション処理を実行できないようにするため）か、管理対象トンネルに移行させてツールが適切な明示パスを検出できるようにします。

複数の同時実行ユーザ

以前のリリースでは、TEM は単一の GUI ユーザしかサポートしていませんでした。本リリースは、ブラウジング、更新、プロビジョニングのいずれの操作においても複数の同時実行ユーザをサポートします。

管理対象トンネルと管理対象外トンネルの同時使用

複数ユーザ機能が TEM にどのように実装されているかを理解するためには、Managed トンネルと Unmanaged トンネルの違いを理解することが重要です。これについては、「管理対象 / 管理対象外プライマリ トンネル」（P.7-116）で説明しています。

複数のユーザのサポートでは管理対象および管理対象外トンネルの処理方法に重要な違いがあります。

- 管理対象トンネルは、すべて SR によってカプセル化されます。SR の操作により、Router Generator サーバによるパス計算の後にスナップショット内のすべてのオブジェクトが最適化される可能性があります。
- 管理対象外トンネルの場合、SR はトンネルヘッド エンド ルータとして定義されます。そのため、管理対象外トンネルには、いくつかの制限があります。たとえば、2 人のユーザが同じデバイスで同時にプロビジョニングすることはできません。
- TEM は、管理対象外トンネル SR が同じデバイスで同時にプロビジョニングすることを許可しませんが、管理対象外トンネル SR による複数のデバイスでの同時プロビジョニングはサポートします。
- 管理対象トンネルは、すべて各 TE プロバイダーの共有管理対象 TE トンネル SR 内に存在します。管理対象外トンネルの場合は、ヘッド デバイスごとに別個の管理対象外 TE トンネル サービス要求が作成されます。TEM は、1 つの TE プロバイダーにつき複数の SR をサポートします。

複数の TEM ユーザが TEM でブラウジングおよびプロビジョニングを実行できます。最大 20 人までの同時ユーザがサポートされ、そのうちの 7 人までがプロビジョニング タスクを実行できます。

以前は、管理対象と管理対象外の両方のプライマリ トンネルがすべて TE プロバイダーごとに 1 つの TE トンネル SR に存在していました。現在は、管理対象トンネルへの複数の同時変更を可能にするために、TE トンネル SR が TE プロバイダーあたり 1 つの管理対象トンネル SR とヘッド TE ルータあたり 1 つの管理対象外トンネル SR に分割されています。

同じ SR で並行プロビジョニングを行うことはできませんが、管理対象外トンネルについては SR がルータ レベルで存在するため、管理対象外トンネルを同時に複数のルータにプロビジョニングすることができます。

ロッキング メカニズム

管理対象外トンネルをプロビジョニングすると、そのトンネルのヘッド TE ルータがロックされます。ロックされていることは、[TE Nodes] ウィンドウの [System Lock Status] 列で確認できます。ロッキングによって、プロビジョニング タスクが完了し、TE ルータのロックが解除されるまで、他のユーザはそのルータにどのような種類のトンネルも配置できなくなります。

ロッキング メカニズムは、バックアップ トンネル、リソース SR、リンク削除、TE トラフィック アドミッションなどの Prime Provisioning 機能にも適用されます。リソース SR には、明示パスの削除/編集、保護要素の削除、SRLG の削除/編集などが含まれます。

リンク削除の場合、一定レベルのインテリジェンス機能が組み込まれています。ユーザまたは Prime Provisioning によって再ルーティングまたは削除できるトンネルが存在せず、TE 関連オブジェクトだけが残っている場合、リンクを削除するためには、ユーザによる介入が必要となります。このとき、削除対象として選択されたインターフェイスを保護するバックアップ トンネルがある場合は、バックアップ トンネルを配置する操作の実行中、ロッキング メカニズムが働きます。TE リンクの削除の詳細については、ユーザ ガイドの 「TE リンクの削除」（P.7-25）を参照してください。

発生する可能性のあるエラーについては、ユーザ ガイドの 「操作エラーのロック」（P.7-82）を参照してください。

管理対象プライマリ トンネルまたはバックアップ トンネルをプロビジョニングすると、そのトンネルに関連付けられている TE プロバイダーがロックされます。ロックされていることは、[TE Provider] ウィンドウの [System Lock Status] 列で確認できます。TE プロバイダー レベルのロックによって、トンネルがどの TE ルータを起点としているかに関係なく、別のユーザがその TE プロバイダーでトンネルを変更することを防止できます。

管理対象トンネルおよびバックアップ トンネルのロッキング メカニズムと管理対象外トンネルのロッキング メカニズムが異なるのは、管理対象トンネルとバックアップ トンネルがすべての制約を満たす最適なルートを見つけるためにパス生成アルゴリズムを使用し、そのアルゴリズムが、ルーティング決定基準として、TE トポロジとそこに含まれるすべてのトンネルの安定したグローバル ビューを必要とするからです。これを実現する唯一の方法は、一度に 1 人のユーザだけが変更を実行できるようにすることです。

Prime Provisioning のロッキング メカニズムを管理する方法の詳細については、ユーザ ガイドの 「ロック メカニズムの管理」（P.7-81）を参照してください。

複数の OSPF 領域

Prime Provisioning は、複数の Open Shortest Path First（OSPF）内での TE トンネルの検出、管理、プロビジョニングをサポートします。

Prime Provisioning の管理対象となるのは、OSPF 領域の範囲内にあるプライマリ TE トンネルとバックアップ TE トンネルだけです。複数の OSPF 領域にまたがる検出および作成はサポートしていません。

Prime Provisioning では、OSPF 領域は TE プロバイダーによって表されます。領域を TE プロバイダーに割り当てた後で変更することはできません。1 つの Prime Provisioning プロバイダーに複数の TE プロバイダーを関連付けることができます。

TE 検出に適したデバイス

複数の OSPF 領域があるネットワークでは、各 OSPF 領域が TE プロバイダーで表されるため、OSPF 領域内のどのルータでも TE 検出に使用できます。1 つのプロバイダーに属する複数の TE プロバイダー（複数の OSPF 領域）を使用することにより、複数の領域にまたがる L3VPN のプロビジョニングが可能になります。

（注）　Prime Provisioning は、複数の領域にまたがる TE トンネル（ある領域にヘッド ルータがあり、別の領域にテール ルータがあるトンネル）を検出またはプロビジョニングしません。

複数の領域があるネットワークを検出するためには、TE 検出を使用して各領域を順に検出する必要があります（ユーザ ガイドの「TE ネットワーク検出」（P.7-11）を参照）。シード ノードは、Area Border Router（ABR; エリア境界ルータ）を含め、領域内のどのデバイスでもかまいません。

TE 検出と TE 領域 ID

TE 検出には TE プロバイダーが関連付けられ、各 TE プロバイダーには領域が割り当てられます。この領域は TE プロバイダーの作成プロセスで割り当てられます（ユーザ ガイドの「TE プロバイダーの作成」（P.7-8）を参照）。この領域は単純な整数値またはドット付き 10 進表記（領域 0.6.0.0 など）です。

TE プロバイダー オブジェクトは、作成時の指定または検出時の自動入力によって対象とする領域を認識し、ドット表記と 10 進表記の変換に対応します。デフォルトはネットワークで使用されている表記です。

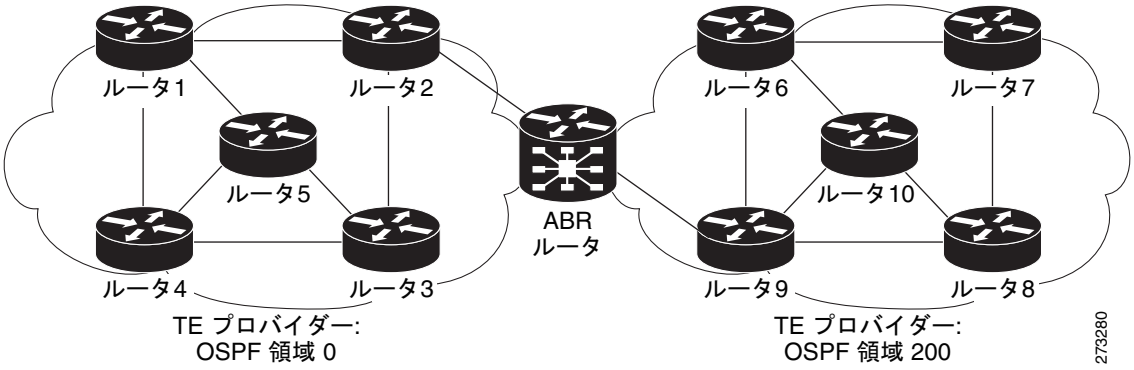
選択した TE プロバイダーがある領域に対して検出を実行すると、その領域に関連付けられたすべてのトンネルおよび明示パスが Prime Provisioning データベースにインポートされます。領域単位の検出の実行手順については、ユーザ ガイドの「エリア別ディスカバリの管理」（P.7-16）を参照してください。

複数の OSPF 領域があるネットワークの例

TE プロバイダー内の TE ルータを複数のリージョン（地域など）に割り当てることにより、デバイスを論理的な基準に基づいてリージョンにグループ化できます。また、Prime Provisioning ではリージョンに基づくフィルタリングが可能です。オブジェクトを特定のリージョンに割り当てるには、検出の実行後、[Inventory] > [Provider Devices] から手動で行います。PE デバイスのリージョンは、[Select Region] ポップアップ ウィンドウで変更できます。

次の図 7-32 に示す例では、2 つの TE プロバイダーがそれぞれ 1 つの Prime Provisioning プロバイダー内に作成され、視覚化された 1 つの OSPF 領域を担当します。

図 7-32　複数の OSPF 領域があるネットワーク



TE の管理方法については、ユーザ ガイドの 「TE プロバイダーの作成」（P.7-8）を参照してください。

帯域幅プール

各 TE 対応のインターフェイスの帯域幅には、ネストされた複数の帯域幅プールが割り当てられます。現在、IOS は、グローバル プールとサブ プールという 2 種類の帯域幅プールをサポートしています。

帯域幅プールについての理解を深めるために、図 7-33 を参照してください。

図 7-33　帯域幅プール

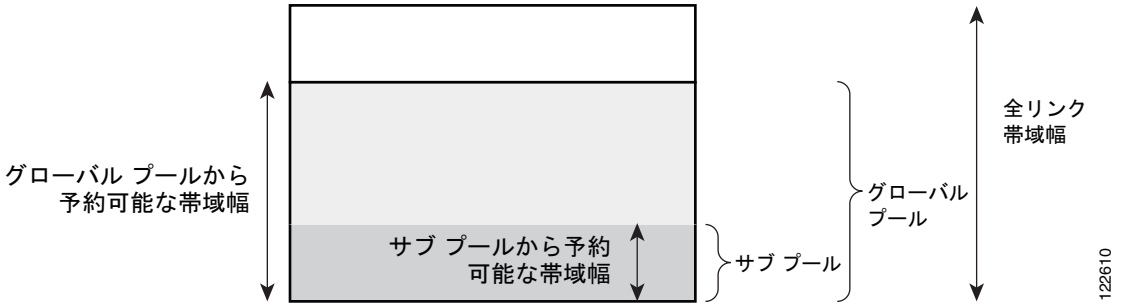


図 7-33 に示すように、サブ プールはグローバル プール内にネストされています。したがって、プライマリ トンネルがサブ プールから帯域幅を予約すると、同じ帯域幅がグローバル プールでも予約されます。

サブ プールでの帯域予約（プライマリ トンネル）は、合計でサブ プールのサイズを超えてはなりません。同様に、グローバル プールでの帯域予約は、合計でグローバル プールのサイズを超えてはなりません。

計画ツール

ここでは、トラフィック エンジニアリングされたネットワークの改善計画を What-If シナリオを基づいて評価するためのツールについて説明します。

計画ツールには、次の機能が含まれます。

- プライマリ計画ツール：

  - トンネル監査：トンネルまたはリソースの変更が提案されているかどうかにかかわらず、既存のネットワークのプライマリ配置に不一致がないかどうか調べます。
  - トンネル配置：通常は、新しいトンネルに使用します。トンネル配置機能では、新しいルートを生成できます。この機能は、それまでパスがなく、配置することが必要なトンネルに使用できます。
  - トンネル修復：トンネル監査の実行後（問題が検出された場合）に実行します。トンネル修復機能には再ルーティング機能があり、トンネルの移動に使用できます。
  - グルーミング：ネットワーク全体を対象とする最適化ツールです。これは、トンネル属性が変更されていない場合にだけ利用できます。
- 保護計画ツール：
  - 監査 SR：手動で追加、変更、削除されたバックアップ トンネルについて、配置前に保護の状態を調べます。
  - バックアップ計算：選択されたネットワーク要素に最適なバックアップ トンネルを自動的に計算します。
  - 保護監査：選択された要素の保護を既存のバックアップ トンネルの観点から監査します。

これらの計画ツールは Prime Provisioning に完全に統合されており、次のような GUI のさまざまな場所から使用できます。

- TE Protected Elements（Compute Backup および Audit Protection）
- Create Managed TE Tunnel（Tunnel Audit、Tunnel Placement、Tunnel Repair、Grooming）
- Create TE Backup Tunnel（Audit SR）

接続保護（CSPF）バックアップ トンネル

TEM によって作成される帯域幅保護のバックアップ トンネルに加え、一連の CSPF-routed バックアップ トンネルも Prime Provisioning 内に作成できます。CSPF-routed バックアップ トンネルは、[TE Protection SR] ウィンドウで管理します。

接続保護バックアップ トンネルは「exclude-address」明示的パスを使用します。この明示パスは [TE Explicit Path List] ウィンドウで作成します。exclude address パスは、パスが使用するホップではなくパスが回避するホップを示す点で strict パスと異なります。どのパスが最適であるかはルータ上の CSPF アルゴリズムによって決定されますが、このアルゴリズムには exclude address パス設定のホップを使用できないという制約があります。この種のパスは、特にバックアップ トンネルで役に立ちます。exclude address パスが回避する必要のあるインターフェイスは、バックアップ トンネルの保護対象である可能性があるからです。

Prime Provisioning では、これらのバックアップ トンネルに無制限のバックアップ帯域幅が設定されます。無制限とは帯域幅が保証されないことを意味しますが、障害発生時に使用可能な最大限の帯域幅が使用されます。そのため、帯域幅保護は実質的にベスト エフォートです。ただし、接続は保証されます。接続保護バックアップ トンネルは、帯域幅保護バックアップ トンネルへの追加または代替として使用できます。

帯域幅保護バックアップ トンネルと接続保護バックアップ トンネルには、次のような違いがあります。

- 帯域幅保護バックアップ トンネルの最初のパス オプションはストリクト明示パスであるのに対し、接続保護バックアップ トンネルの最初のパス オプションは exclude address 明示パスです。
- 帯域幅保護バックアップ トンネルにはバックアップ帯域幅が定義されているのに対し、接続保護バックアップ トンネルでは無制限のバックアップ帯域幅がベスト エフォート方式で使用されます。

- 帯域幅保護バックアップ トンネルは、最適なバックアップ トンネルを生成して既存のトンネルが要素を完全に保護することを確認するルート ジェネレータ アルゴリズムに渡されるのに対し、接続保護バックアップ トンネルはルート ジェネレータ アルゴリズムに渡されないため、トンネルが目的を果たしていることをユーザが確認する必要があります。

クラスベース トンネル選択

マルチプロトコル ラベル スイッチング トラフィック エンジニアリング Class-Based Tunnel Selection（CBTS; クラスベース トンネル選択）を使用すると、同一トンネル ヘッド エンドと同一テール エンド間でさまざまな TE トンネルに、さまざまなサービス クラス（CoS）値を指定して、トラフィックを動的にルーティングおよび転送できます。パケットの CoS 値は EXP ビット内にあります。8 個の EXP ビットがあり、0 ～ 7 の番号が付いています。

同一ヘッド エンドから同一テール エンドへの TE（または DS-TE）トンネルは、複数の CoS 値を持つように設定できます。設定後、CBTS は、次の要件を満たすトンネルに各パケットを動的にルーティングして転送します。

- 標準の自動ルートまたはスタティック ルートを使用してトラフィック アドミッションの対象として選択されている。
- EXP ビットがパケットの EXP ビットと一致している。

したがって、CBTS は、TE トンネルへの直接のトラフィック アドミッションではなく、トラフィックが TEM でサポートされる自動ルートまたはスタティック ルート メカニズムによってトンネルに入る前に満たす必要のある追加の基準です。

CBTS は DS-TE トンネル経由でダイナミック ルーティングを行い、設定が最小限で済むので、大規模なネットワークにおいて DS-TE の配置が大幅に軽減されます。CBTS は、すべての CoS 値をさまざまな種類のトンネルに配布できます。

CBTS 機能には次の制限があります。

- 1 つの宛先について、同じテール エンドで終端するトンネルを使用してすべての CoS 値が伝送されます。すべての CoS 値がトンネルで伝送されるか、またはトンネルでまったく値が伝送されないかのいずれかです。したがって、1 つの宛先について、一部の CoS 値を DS-TE トンネルでマッピングし、その他の CoS 値を最短パス優先（SPF）ラベル配布プロトコル（LDP）または SPF IP パスでマッピングすることはできません。
- CBTS では、複数のトンネルで特定の EXP 値のロードバランスを図ることはできません。2 つ以上のトンネルが特定の experimental（EXP）値を伝送するように設定されている場合、CBTS はその中から 1 つのトンネルを選択して、この EXP 値を伝送します。
- Any Transport over MPLS（AToM）、MPLS TE Automesh、または Label-Controlled（LC）-ATM では、CBTS の動作はサポートされません。

グローバル スタティック ルートを使用してトンネルへのトラフィック アドミッションが行われ、特定の宛先に対し、管理上の重みが同じであるトンネルが複数ある場合は、CBTS 属性がトンネルの選択基準となります （上記の CBTS でのロードバランスに関する説明を参照してください）。

ポリシーベース トンネル選択

マルチプロトコル ラベル スイッチング トラフィック エンジニアリング Policy-Based Tunnel Selection（PBTS; ポリシーベース トンネル選択）を使用すると、トラフィックを同一トンネル ヘッド エンドと同一テール エンド間でさまざまな TE トンネルにポリシーに基づいて動的にルーティングおよび転送できます。ルーティング アルゴリズムは、フォワーディング ルックアップの前にヘッドエンド ルータの入力インターフェイスで実行されます。

Prime Provisioning の PBTS 実装では、トラフィックはインターフェイス コマンド policy-class を使用して特定の TE トンネルに転送されます。CBTS は IOS デバイスを対象としていますが、PBTS は IOS XR デバイス用に厳密に設計されています。

CBTS と同じように、PBTS は、TE トンネルへの直接のトラフィック アドミッションではなく、トラフィックが TEM でサポートされる自動ルートまたはスタティック ルート メカニズムによってトンネルに入る前に満たす必要のある追加の基準です。

（注） Prime Provisioning は、ポリシー クラスをプロビジョニングするわけではなく、トンネルに既存のポリシー クラスを関連付けるだけです。そのためには、policy-class 属性を 1 ～ 7 の値に設定します。

CBTS の詳細については、「クラスベース トンネル選択」（P.7-123）を参照してください。

PBTS および IOS XR の一般的な情報については、http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.7/mpls/configuration/guide/gc37te.html#wp1325561 を参照してください。