CHAPTER 2

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、本章で説明します。

図 2-1 で強調表示されているボックスは、TEM で行う事前設定のステップを示しています。

図 2-1　　TEM プロセス図：事前設定

この章の内容は、次のとおりです。

- 「概要」（P.2-2）
- 「TE 検出の前提条件と制約事項」（P.2-2）
  - 「TE 検出の TE ルータへアクセス」（P.2-2）
  - 「大規模ネットワークでのメモリの不足」（P.2-3）
  - 「IOS XR およびイネーブル パスワード」（P.2-3）
- 「TE 検出タスクの作成」（P.2-3）
- 「エリア別ディスカバリの管理」（P.2-8）
  - 「エリア別 TE 検出の実行」（P.2-8）
  - 「ABR を使用したエリア別 TE 検出の実行」（P.2-9）
- 「TE 検出タスクの検証」（P.2-9）
  - 「タスク ログ」（P.2-10）
  - 「TE トポロジ」（P.2-14）

– 「ネットワーク要素の表示」（P.2-14）
- 「管理インターフェイスの設定」（P.2-14）
  – 「MPLS-TE 管理プロセス」（P.2-14）
  – 「イーサネット リンクの設定」（P.2-15）

概要

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 検出は、1 回または定期的に実行するようにできる、スケジュール可能なタスクです。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。

TE 検出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 TEM 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.1-2）を参照してください。

TE 検出の TE ルータへアクセス

TE 検出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、ISC 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 の場合は、Cisco IP Solution Center Traffic 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.1-4）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（たとえば、250 を超えるデバイスまたは 5000 を超えるトンネル）で TE 検出を実行する場合、または OutOfMemoryException が発生した場合は、次のことを実行します。

ステップ 1　[Administration] > [Control Center] > [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（[Service Inventory] > [Inventory and Connection Manager] > [Devices]）から作成する場合は、厳密には、イネーブル パスワードを指定する必要はありません。Cisco ISC 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、Cisco ISC 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 Cisco ISC 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

同時 TE 検出はサポートされていません。一度に 1 人のユーザのみが **TE 検出**タスクを実行できます。

TE 検出タスクの作成

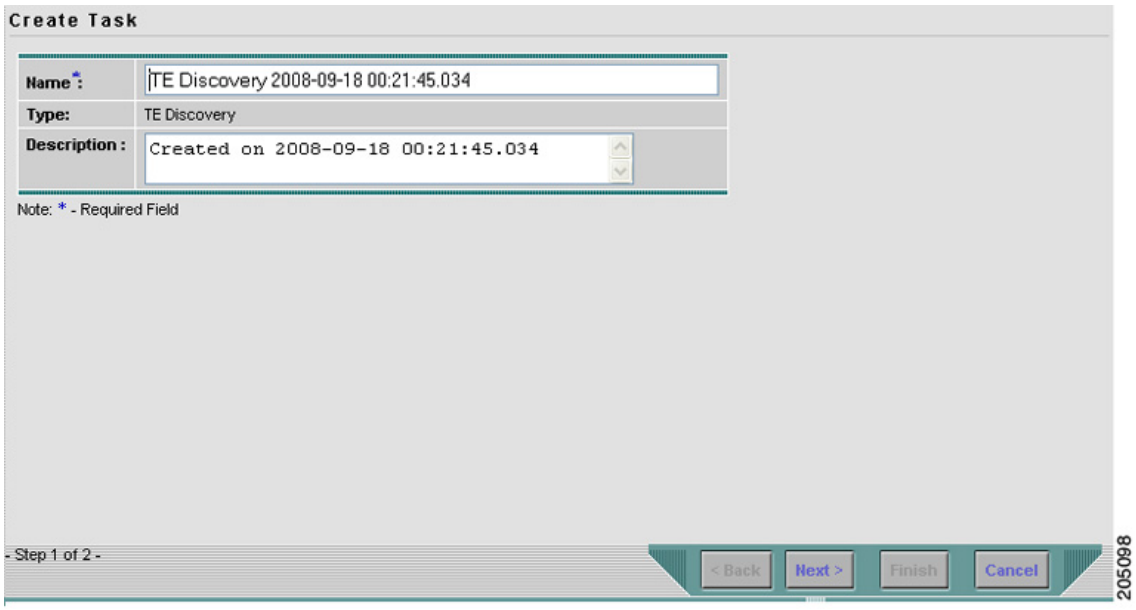
TE ネットワーク上で TE 検出タスクを作成するには、次のステップを実行します。

ステップ 1　[Monitoring] > [Task Manager] を選択します。図 2-2 に示すウィンドウが表示されます。

図 2-2　　タスク

ステップ 2　[Create] > [TE Discovery] を選択し、新しいタスクを作成します。
図 2-3 に示すウィンドウが表示されます。

図 2-3　　TE 検出タスクの作成（ステップ 1）



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。
図 2-4 の [Select TE Provider] ウィンドウが表示されます。

図 2-4　Select TE Provider

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。

図 2-5 の [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。

図 2-5　Select Seed Device

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。

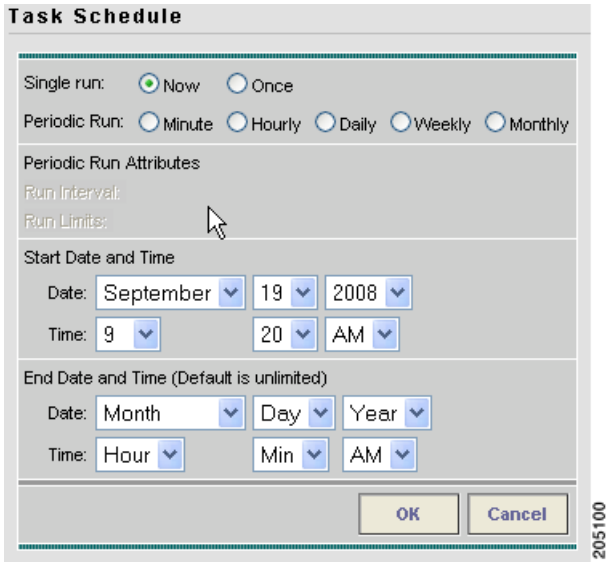
図 2-6 の [Task Schedules] ウィンドウが表示されます。

図 2-6　スケジュールを作成する前の TE 検出の [Task Schedules] ウィンドウ

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（図 2-8）。
- 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、図 2-7 の [Task Schedule] ウィンドウが表示されます。

図 2-7　Task Schedule



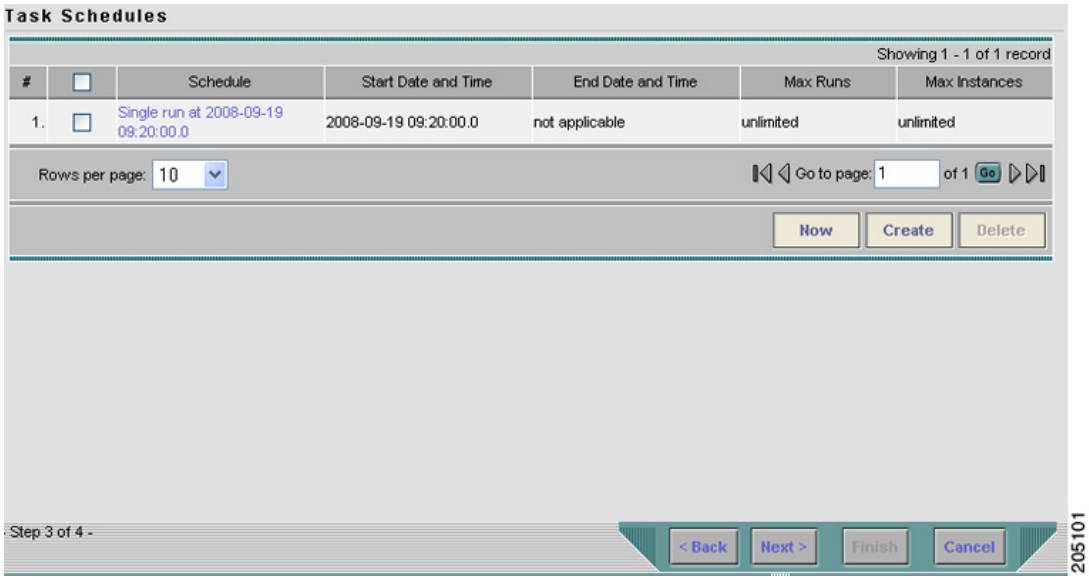
ステップ 7　[Task Schedule] ウィンドウで、タスクを実行する時間と頻度を定義するための選択を行います。

（注）　デフォルト設定では、単一の **TE 検出**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。

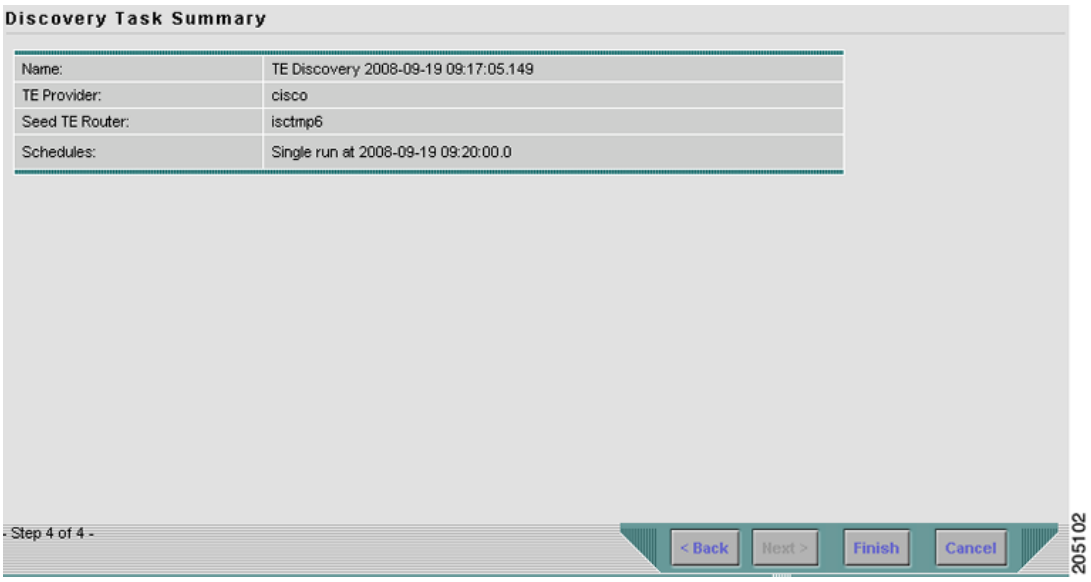
図 2-8 に示すように、スケジュールに入れたタスクが [Task Schedules] テーブルに表示されるようになりました。

図 2-8　スケジュールを作成した後の TE 検出の [Task Schedules] ウィンドウ



ステップ 9　[Next] をクリックします。図 2-9 の、スケジュールに入れたタスクの要約が表示されます。

図 2-9　Discovery Task Summary



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（図 2-2）。

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、TEM 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説明については、「複数の OSPF 領域」（P.F-5）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。

- 「エリア別 TE 検出の実行」（P.2-8）
- 「ABR を使用したエリア別 TE 検出の実行」（P.2-9）。

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 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的パスが ISC データベースにインポートされます。

エリア別 TE 検出を開始するには、次のステップを実行します。

ステップ 1　ISC プロバイダーを作成します。

ステップ 2　ISC 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　[Monitoring] > [Task Manager] > [Create] > [TE Discover] を選択します。

TE 検出の名前を指定するか、デフォルト値をそのまま使用し、[Next] を押します。

ステップ 6　TE プロバイダーを選択し、[Next] を押します。

ステップ 7　シード デバイスを選択し、[Next] を押します。

ステップ 8　TE 検出からスケジュールを選択し、[Next] を押します。

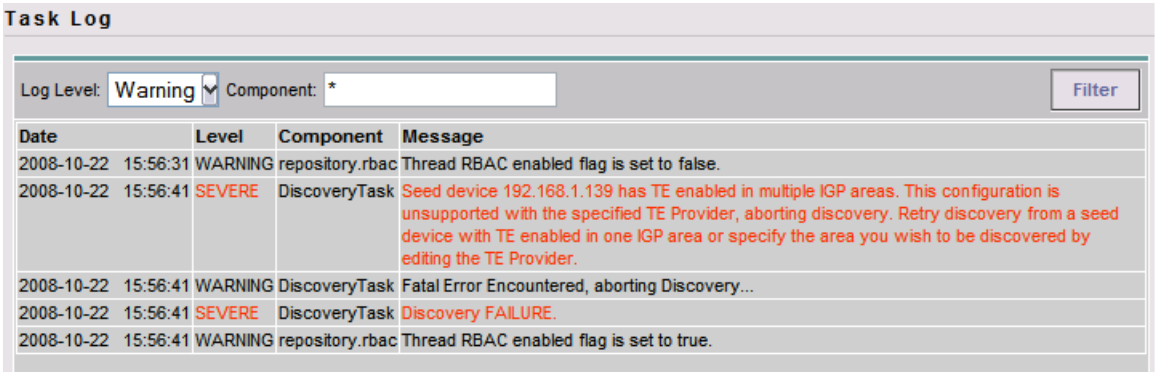
ステップ 9　ディスカバリ タスクの要約を確認します。

受け入れ可能な場合は、[Finish] を押して、TE 検出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 2-10 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 2-10　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。

- タスク ログ：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。

タスク ログ

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　[Monitoring] > [Task Manager] を選択します。

ステップ 2　[Tasks] ウィンドウの左側にある目次の [Logs] を選択します。

図 2-11 の [Task Logs] ウィンドウが表示されます。

図 2-11　[Task Logs] : TE 検出

さまざまなウィンドウ要素の説明については、「TE タスク ログ」（P.B-67）を参照してください。

各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 3　特定のタスクのログを表示するには、[Action] 列でログ名をクリックします。

TE 検出ログのコピーを、図 2-12 から始まる次のスクリーンショットで示します。

（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 2-12　TE 検出タスク ログ：デバイス/インターフェイス

```
[Step 1 of 6] Process Device(s)/Interface(s)

  ADD: Device(s)/Interface(s) to Repository:


  SKIP: Matching Device(s)/Interface(s) in Repository:

           1.  isctmpl2., TEID: 192.168.118.168, Vendor: Cisco
           1.1.  POS0/1/0/1  --  10.2.4.13

           2.  isctmpl3., TEID: 192.168.118.171, Vendor: Cisco
           2.1.  GigabitEthernet2/0/0  --  10.2.4.46
           2.2.  GigabitEthernet1/0/0  --  10.2.4.50

           3.  isctmpl., TEID: 192.168.118.176, Vendor: Cisco
           3.1.  FastEthernet3/1/0  --  10.2.3.93
           3.2.  FastEthernet1/1/0  --  10.2.2.110
           3.3.  FastEthernet3/0/1  --  10.2.3.89
           3.4.  FastEthernet2/1/0  --  10.2.3.54
           3.5.  FastEthernet2/1/1  --  10.2.3.57
```

138911

図 2-13　TE 検出タスク ログ：リンク

図 2-14　TE 検出タスク ログ：明示的パス

```
[Step 3 of 6] Process Explicit Path(s)

  ADD: Explicit Path(s) to Repository:

           1.  isctmpl1.
           1.1.  pl1-p8: 10.2.4.5 :
           1.2.  pl1-pl2-p7-p8: 10.2.4.14 : 10.2.4.29 : 10.2.3.49 :
           1.3.  isctmpl1-isctmp8-1: 10.2.4.13 : 10.2.4.30 : 10.2.2.126 :
           1.4.  isctmpl1-isctmpl2-1: 10.2.4.9 :

           2.  isctmpl0.
           2.1.  pl0-pl2-pl1: 10.2.4.21 : 10.2.4.10 :
           2.2.  pl0-pl2-p7-p1: 10.2.4.21 : 10.2.4.30 : 10.2.2.110 :
           2.3.  loopback-pl0-pl2-pl1: 192.168.118.168 : 192.168.118.166 :

           3.  isctmpl2.
           3.1.  pl2-p7-p8-pl1: 10.2.4.30 : 10.2.2.126 : 10.2.4.6 :
           3.2.  isctmpl2-isctmp5-1: 10.2.4.50 : 10.2.4.54 : 10.2.2.81 :

           4.  isctmp8.
           4.1.  isctmp8-isctmp7-1: 10.2.2.113 :
```

138913

図 2-15　TE 検出タスク ログ：プライマリ トンネル

```
[Step 4 of 6] Process Primary Tunnel(s)

  ADD: Primary Tunnel(s) to Repository:

           1.  tunnel-te2 : isctmpl1  --  isctmpl0
           2.  tunnel-te1000 : isctmpl1  --  isctmpl
           3.  tunnel-te1 : isctmpl0  --  isctmp6
           4.  tunnel-te2 : isctmpl0  --  isctmpl
           5.  tunnel-te133 : isctmpl2  --  isctmp7
           6.  tunnel-te212 : isctmpl2  --  isctmp7
           7.  tunnel-te1000 : isctmpl2  --  isctmp2
           8.  tunnel-te1001 : isctmpl2  --  isctmp2
           9.  Tunnel2 : isctmpl  --  isctmp8
           10.  Tunnel3 : isctmpl  --  isctmp5
           11.  Tunnel138 : isctmpl  --  isctmp3
           12.  Tunnel300 : isctmpl  --  isctmp2
           13.  Tunnel1000 : isctmpl  --  isctmpl1
           14.  Tunnel2000 : isctmpl  --  isctmp2


  SKIP: Matching Primary Tunnel(s) in Repository:
```

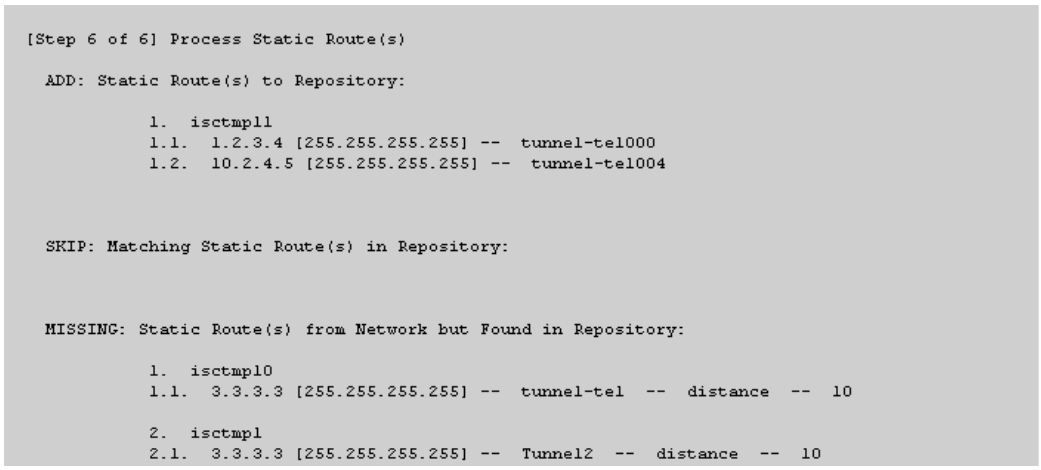
138914

図 2-16　TE 検出タスク ログ：バックアップ トンネル

```
[Step 5 of 6] Process Backup Tunnel(s)

  ADD: Backup Tunnel(s) to Repository:

           1.  tunnel-te1002 : isctmpl1  --  isctmp8
           2.  tunnel-te1005 : isctmpl1  --  isctmpl2
           3.  tunnel-te1000 : isctmpl2  --  isctmp5


  SKIP: Matching Backup Tunnel(s) in Repository:



  MISSING: Backup Tunnel(s) from Network but Found in Repository:

           1.  tunnel-te3 : isctmpl1  --  isctmpl2
           2.  tunnel-te1001 : isctmpl1  --  isctmp8
           3.  Tunnel2 : isctmpl3  --  isctmpl2
           4.  Tunnel1 : isctmpl  --  isctmp2
           5.  Tunnel4 : isctmpl  --  isctmp2
           6.  Tunnel5 : isctmpl  --  isctmp3
```

138915

図 2-17　TE 検出タスク ログ：スタティック ルート



TE 検出タスク ログのウィンドウは、TE ネットワークにおける特定のイベントを説明する各セクションに分類されています。

- **TE 検出**タスクが最初に実行されたときにリポジトリに記録されたネットワークの状態
- **TE ディスカバリ** タスクが前回実行されて以降に実施されたネットワークの変更（リポジトリ差分）

ネットワークにおける変更の要約は 6 ステップで報告されます。

1. デバイス/インターフェイス（図 2-12）。
2. リンク（図 2-13）。
3. 明示的パス（図 2-14）。
4. プライマリ トンネル（図 2-15）。
5. バックアップ トンネル（図 2-16）。
6. スタティック ルート（図 2-17）。

図に示すように、各ステップは、次のレポート カテゴリに含まれる変更をログ テーブルに表示します。

- ADD：このセクションは、**TE 検出**タスクがリポジトリに追加した要素をリストします。最初のディスカバリでは、事前にリポジトリに存在する要素がないため、すべての要素が ADD セクションに含まれます。以降のディスカバリのたびに、ADD セクションは、Cisco ISC TEM に依存しないディスカバリ以降のネットワークに追加されている要素をリストします。このように、ADD の機能は、これらの要素を追加することにより、リポジトリとネットワークを同期します。
- SKIP：このセクションは、ネットワークとリポジトリの両方に存在する要素をリストし、すべて等しい属性を持ちます。これらの要素は、Cisco ISC TEM とは独立して削除または変更されていないことを示しています。
- MISSING：このセクションは、リポジトリに存在するがネットワークには存在しない要素をリストし、これらが **Cisco ISC TEM** とは独立して削除されたことを意味します。これは、不一致の修正にさらに調査が必要であることを示しています。
- MISMATCH：このセクションは、ネットワークとリポジトリの両方に存在する要素をリストしますが、1 つ以上の属性が等しくありません。これらの要素は、Cisco ISC TEM とは独立して変更されており、調査して問題を修正する必要があることを意味しています。

- MODIFY：このセクションは、ネットワークと同期するために、**TE 検出**タスクの前回の実行から変更されたリポジトリ内の属性を持つネットワーク要素をリストします。これらは通常、トンネルを設定した時間などの動的属性です。

ステップ 4　[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、第 10 章「TE トポロジ」を参照してください。

ネットワーク要素の表示

TE 検出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 Management Services] ウィンドウに移動し、確認する要素のタイプを選択することです。

たとえば、TE 検出を実行した後でノードのステータスを確認するには、[Service Inventory] > [Inventory and Connection Manager] > [Traffic Engineering Management] > [TE 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。

特定のデバイスにおける管理インターフェイスの設定方法の詳細については、『*Cisco IP Solution Center Infrastructure Reference, 6.0*』の、作成中のデバイスのセクション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 Cisco ISC 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、Cisco ISC 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

Cisco ISC 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
```