APPENDIX E

インベントリ - ディスカバリ

この付録では、ディスカバリ機能を使用して Prime Provisioning プロビジョニング プロセスのためにデバイス、接続、サービスを検出する方法について説明します。次の事項について説明します。

Prime Provisioning ディスカバリの概要

Prime Provisioning ディスカバリ機能は、既存のネットワーク（Prime Provisioning の導入より先に存在していたサービスを持つネットワーク）での Prime Provisioning のインストールに役立つよう設計されています。Prime Provisioning ディスカバリは、サービスの検出とデータベースとの同期とを繰り返し実行するメカニズムではありません。初回のディスカバリが完了した後のプロビジョニングは、すべて Prime Provisioning を使用して実行する必要があります。Prime Provisioning を使用せずにサービスを直接プロビジョニングすると、サービスは Prime Provisioning から認識されず、Prime Provisioning によってこれらのサービスに上書きや競合が発生する可能性があります。このため、
Prime Provisioning 以外でプロビジョニングされたサービスはすべて、グラフィカル ユーザ インターフェイス（GUI）またはアプリケーション プログラム インターフェイス（API）によって

Prime Provisioning にプロビジョニングすることで Prime Provisioning に展開する必要があります。これをエコー モードで実行することで、ネットワークと Prime Provisioning データベースとの同期が後続のコンフィギュレーション監査によって確認されます。

通常、Prime Provisioning でプロビジョニング可能なサブセットだけが検出されます。
Prime Provisioning でプロビジョニングできないタイプのサービスは検出できません。

Prime Provisioning によって、ご使用の MPLS VPN または L2VPN メトロ イーサネット ネットワークを構成するデバイス、接続、サービスを検出してネットワーク デバイスのインベントリを作成するプロセスを効率良く進められます。

（注） サービス ディスカバリは、ネットワーク内のさまざまな要素の影響を受ける、複雑な操作です。元のネットワーク コンフィギュレーションは、サービスのプロビジョニング時に Prime Provisioning が使用したルールに従って実行されたものである必要があります。そうでない場合、ディスカバリ中にエラーが発生することがあります。特定のネットワークでは多数の設定が可能であるため、サービス ディスカバリ プロセスをコミットする前に、シスコのアカウント チームまたはシスコ アドバンスド サービスに連絡して、サポートを受けることを強く推奨します。

サービス ディスカバリを実行するユーザは、全体的なネットワーク トポロジを十分把握し、PE、N-PE、U-PE、PE-AGG、CE といったネットワーク用語についての知識があり、Prime Provisioning での NPC やメトロ イーサネット/MPLS サービスの定義について理解している必要があります。

Prime Provisioning は、管理ユーザだけに対してディスカバリ プロセスをサポートします。

Prime Provisioning ディスカバリ機能は、Prime Provisioning アプリケーション スイートに含まれる次の 3 つのアプリケーションのリポジトリ読み込みに使用できます。

- Prime Provisioning MPLS VPN Management
- Prime Provisioning L2VPN Management
- Prime Provisioning Prime Diagnostics

（注） サービス ディスカバリは、Secure Shell version 2（SSHv2; セキュア シェル バージョン 2）をターミナル セッション プロトコルとしてサポートしていません。MPLS および L2VPN のサービス ディスカバリは、IOS XR が稼働中のデバイスをサポートしていません。

Prime Provisioning のデバイスにホスト名だけが割り当てられている場合、Prime Provisioning デバイスでは、IP 管理アドレスまたはドメイン名が設定されていません。ディスカバリでは、同じホスト名のデバイスが IP 管理アドレスで検出された場合やデバイス エディタで手動作成された場合、そのデバイスによる Prime Provisioning リポジトリへのコミットが失敗することがあります。この失敗の原因は、両方のデバイスにドメイン名が設定されていないため、既存の Prime Provisioning デバイスで一致判定がなされてしまうことにあります。

回避策として、次の 1. または 2. のいずれかを実行します。

1. ディスカバリの前に既存の Prime Provisioning 内デバイスを編集し、管理 IP アドレスを追加しておく。これにより、ディスカバリはそのデバイスを重複として扱い、デバイス エディタでは読み取り専用としてマークします。

   または

2. ディスカバリ中に、検出されたデバイスにデバイス エディタを使用してドメイン名を入力する。これにより、ディスカバリはそのデバイスを新しいデバイスとして扱うようになります。

Prime Provisioning トラフィック エンジニアリング管理には、独自のディスカバリ インターフェイスおよびプロセスがあります。この点については、*『Cisco Prime Provisioning 6.3 User Guide』*の TE ネットワーク検出で説明されています。

複数のサービス ディスカバリ プロセスがサポートされており、前のステップの任意の場所から再開できます。複数のサービス ディスカバリ プロセスのサポートによって、ネットワークの増分ディスカバリが可能になります。前のステップから再開する機能は、選択した以前のステップまでディスカバリ プロセスをロールバックするために役立ちます。これにより、ディスカバリ プロセス全体を最初から再開する代わりに、そのステップから検出を再開できます。ディスカバリ データ収集から再開すると、データ収集が必要なデバイスを選択するよう求められます。

既存の VPN リンクでは増分ディスカバリが発生します。既存の VPN はディスカバリ GUI では編集できません。既存の VPN リンクは、コミット中バイパスされます。

MPLS および L2VPN サービス ディスカバリでは、同期は行われません。変更はすべて Prime Provisioning ユーザ インターフェイスを使用して手動で実行する必要があります。新しい VPN だけが検出されます。また、変更された既存の NPC や競合が発生している NPC のサービスも検出されません。

Prime Provisioning へのコミットは、各ステップの後ではなく、ディスカバリ フェーズの終了時だけに発生します。検出ワークフローの中で、ディスカバリ プロセスが Prime Provisioning の状態を変更することはありません。ユーザが検出されたデバイスとサービスを Prime Provisioning にコミットできるのは、ワークフローの最後だけです。

ディスカバリ プロセスは、ネットワーク トポロジの検出方法に関して、複数の選択肢を提供します。

3. Prime Provisioning MPLS VPN Management または Prime Provisioning L2VPN Management をプロビジョニングするためにディスカバリを実行している場合は、次の 3 つのディスカバリ方式から選択できます。

   a. CDP ディスカバリ

      Cisco Discovery Protocol（CDP）を使用して、**policy.xml** ファイルで指定する IP アドレスを持つ、最初のデバイスに接続されているデバイスを検出できます。

   b. デバイス / トポロジ・ベースのディスカバリ

      デバイス / トポロジ ベースの方式を使用できます。この方式では、デバイスおよび NPC トポロジの情報を指定する XML ファイルを使用します。

   c. インポート コンフィギュレーション ファイル ベース

      インポート コンフィギュレーション ファイル ベースの方式を使用できます。この方式は、検出するデバイスのコンフィギュレーション ファイルが格納されているサーバのディレクトリと、NPC を自動作成するために使用されるデバイス接続情報を含む XML ファイルを使用します。

4. MPLS VPN トポロジ、L2VPN（Metro Ethernet）トポロジ、またはその両方を検出するために、ネットワーク トポロジを選択できます。

   L2VPN（Metro Ethernet）ディスカバリを選択した場合は、MPLS コアの Metro Ethernet、イーサネット コアの Metro Ethernet、または混合コアの両方の組み合わせのいずれかを検出できます。混合コアでは、L2VPN サービスは、MPLS コア全体を対象とすることも、ローカル イーサネット ドメインだけに制限することもできます（ローカル スイッチド サービス）。イーサネット ドメインにわたって N-PE デバイスを通過しないローカル スイッチド サービスも検出できます。図 E-1 には、混合コアを示します。

図 E-1　混合コア

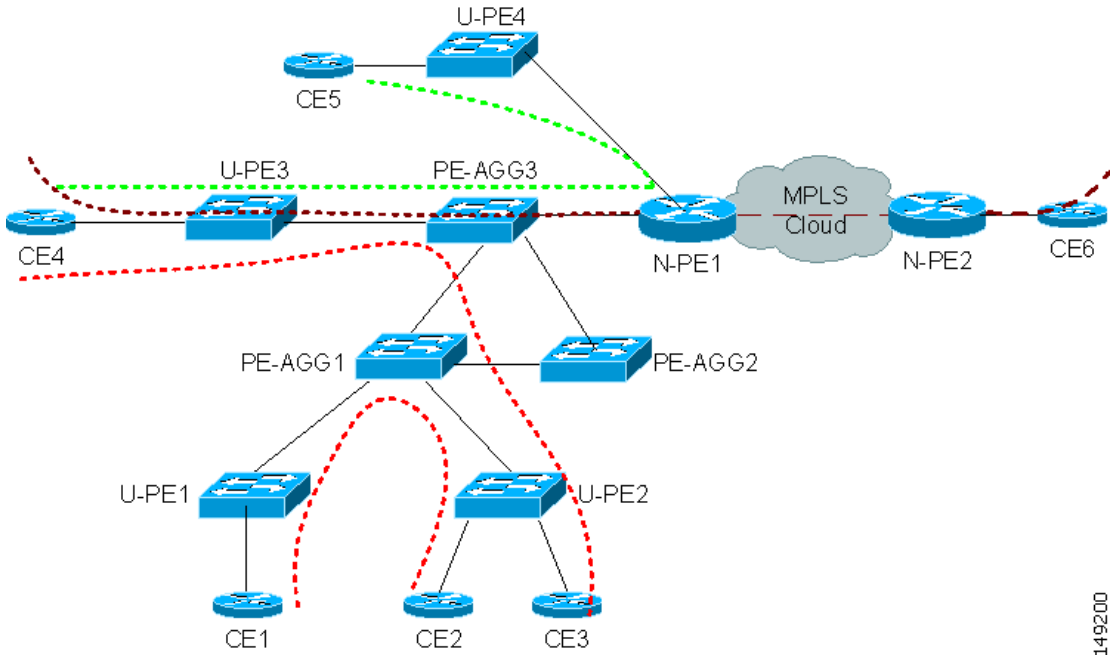


図 E-2 に、ディスカバリ プロセスの各フェーズを示します。

図 E-2　Prime Provisioning のディスカバリ ステップ

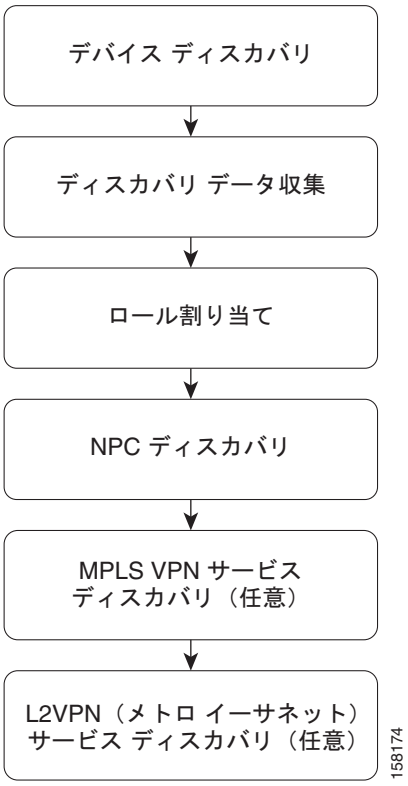


表 E-1 では、ディスカバリ プロセスのフェーズについて説明します。

表 E-1　ディスカバリ プロセスのステップ

ステップ	説明
デバイス ディスカバリ	MPLS VPN またはメトロ イーサネット トポロジあるいはその両方でデバイスを検出します。
ディスカバリ データ収集	検出されたデバイスの IOS コンフィギュレーションを収集します。
ロール割り当て	rules.xml に基づいて検出されたデバイスのロール割り当てが実行され、N-PE、U-PE、または CE として、デバイスのロールを編集するよう求められます。 **（注）** サンプルは $PRIMEP_HOME/resources/discovery/data/ にあります。rules.xml（ここに rules.xml ファイルが保持されている必要がある）。
NPC ディスカバリ	検出された NPC を表示し、NPC の追加または削除を許可します。
MPLS VPN ディスカバリ	MPLS VPN ネットワークのトポロジを検出し、必要に応じてその変更を許可します。 **（注）** Prime Provisioning Discovery with Prime Diagnostics を使用している場合、MPLS VPN ディスカバリ ステップは必要ありません。
L2VPN（Metro Ethernet）ディスカバリ	Metro Ethernet ネットワークのトポロジを検出し、必要に応じてその変更を許可します。 **（注）** Prime Provisioning Discovery with Prime Diagnostics を使用している場合、（L2VPN）Metro Ethernet ディスカバリ ステップは必要ありません。

次のディスカバリ操作は、Prime Provisioning でサポートされていません。

- IOS XR が動作しているデバイスでの MPLS VPN サービスの初回ディスカバリ
- MPLS VPN サービスへのイーサネット アクセス（U-PE、PE-AGG）の初回ディスカバリ
- VRF lite/MVRF の初回ディスカバリ
- マルチキャスト設定の VRF の初回ディスカバリ
- 固有ルート識別子を持つ MPLS VPN サービスの初回ディスカバリ
- インターフェイスに関連付けられていない VRF の初回ディスカバリ
- 1 つのインターフェイスに関連付けられ、検出されるデバイス間で他の VRF が稼働していない VRF の初回ディスカバリ。
- 検出されたエクストラネット（ユーザが手動で VPN を分割する場合を除く）
- ループバック インターフェイスに接続されている MPLS VPN/MLS VRF のディスカバリ

- Cisco 7600 シリーズ ルータの 12.2(33) SRB で導入された新しいイーサネット サービス インスタンス（EVC）の構文を使用しているサービスの初回ディスカバリ
- IOS XR が動作しているデバイスでの L2VPN サービスの初回ディスカバリ
- アクセス ポートを備えた ERS および ERMS サービスのディスカバリ（VLAN アクセスによるディスカバリだけをサポート）
- ATM やフレームリレー サービスのディスカバリ（イーサネット サービスのディスカバリだけをサポート）
- 段階的な NPC 同期
- 不一致の管理を含む再同期

Prime Provisioning ディスカバリのテクニカル ノート

ここでは、Prime Provisioning ディスカバリ プロセスに関する技術的なヒント、一般情報、および制約事項を示します。

Prime Provisioning ディスカバリ機能は、Prime Provisioning アプリケーション スイートに含まれる次の 3 つのアプリケーションのリポジトリ読み込みに使用できます。

- Prime Provisioning MPLS VPN Management
- Prime Provisioning L2VPN Management
- Prime Provisioning Prime Diagnostics

ステップは全体としてよく似ていますが、ディスカバリのタイプによってワークフローにいくつかの違いがあります。これらについては、各 Prime Provisioning アプリケーションに関する項で説明します。

- 「Prime Provisioning ディスカバリの Prime Provisioning MPLS VPN Management との使用」（P.E-7）
- 「Prime Provisioning ディスカバリの Prime Provisioning L2VPN Management との使用」（P.E-8）
- 「Prime Provisioning ディスカバリの Prime Provisioning Prime Diagnostics との使用」（P.E-8）
- 「Prime Provisioning トラフィック エンジニアリング管理による Prime Provisioning ディスカバリの使用」（P.E-9）

（注） Prime Provisioning トラフィック エンジニアリング管理には、独自のディスカバリ インターフェイスおよびプロセスがあります。

この点については、*『Cisco Prime Provisioning 6.3 User Guide』* の TE ネットワーク検出で説明されています。

Prime Provisioning トラフィック エンジニアリング管理と Prime Provisioning MPLS VPN Management の両方を含むインストール環境での Prime Provisioning ディスカバリの使用に関するテクニカル ノートについては、「Prime Provisioning トラフィック エンジニアリング管理による Prime Provisioning ディスカバリの使用」（P.E-9）を参照してください。

一般的な注意点

Prime Provisioning ディスカバリを実行する前に、次の点に注意してください。

- ディスカバリを実行する前に、Prime Provisioning GUI を使用して、プロバイダー、カスタマー、およびリソース プールを作成できます。
- 検出ワークフロー インターフェイスを制御できるのは、一度に 1 ユーザだけです。
- この章の手順には、「汎用」な手順を示します。特定のアプリケーションのライセンスがない場合は、Prime Provisioning ディスカバリのスタート画面に、そのアプリケーションの選択肢が表示されません。
- ディスカバリの終了後に、「手動」のデバイスの収集を実行します。
- ディスカバリ プロセスを開始した後、[Discovery Workflow] ウィンドウに [Restart] ボタンが表示されます。[Restart] ボタンをクリックすると、完了したステップのドロップダウン リストがポップ アップ表示されます。ステップを選択し、そのステップから再開できます。
- 初期化から再開すると、現在のディスカバリ プロセスが中止されます。
- Role Based Access Control（RBAC）を使用したディスカバリは、サポートされていません。

ディスカバリのログ ファイルの使用

ログ ファイルは、ディスカバリ プロセスの各フェーズに対して書き込まれます。[Discovery Workflow] ウィンドウの各ディスカバリ フェーズの概要の横にある [Log] 列で、[View] をクリックして、ログ ファイルを表示できます。

ログ ファイルは、ディスカバリ ステップが失敗したイベントに関して役立つ情報を提供します。

Prime Provisioning ディスカバリの Prime Provisioning MPLS VPN Management との使用

ディスカバリ プロセスを実行して、Prime Provisioning MPLS VPN Management で使用するために MPLS VPN ネットワークを検出する場合は、次の点に注意してください。

- ディスカバリ プロセスの主要なすべてのステップを実行する必要があります。
- CDP ディスカバリ、デバイス / トポロジ、またはインポート コンフィギュレーション ファイル ベースのディスカバリを使用できます。デバイス / トポロジまたはインポート コンフィギュレーション ファイル ベースのディスカバリを使用するを推奨します。
- Prime Provisioning はパーシャル メッシュ VPN トポロジをサポートしていません。ディスカバリ プロセスがパーシャル メッシュ VPN を検出した場合、より小さな単位（通常は完全メッシュ VPN とハブ アンド スポーク VPN の組み合わせ）にパーシャル メッシュ VPN を分割する必要があります。
- 自動ディスカバリ プロセスの完了後に、検出されたすべてのデバイスに対して、[Operate] > [Tasks] > [Task Manager] > [Collect Config] のタスクをスケジューリングし、実行する必要があります。

（注）　MPLS サービス ディスカバリでは、同期は行われません。変更はすべて Prime Provisioning ユーザ インターフェイスを使用して手動で実行する必要があります。新しい VPN だけが検出されます。また、変更された既存の NPC や競合が発生している NPC のサービスも検出されません。

Prime Provisioning ディスカバリの Prime Provisioning L2VPN Management との使用

ディスカバリ プロセスを実行して、Prime Provisioning L2VPN Management を使用してプロビジョニングおよび管理される L2VPN ネットワークを検出する場合は、次の点に注意してください。

- ディスカバリ プロセスの主要なすべてのステップを実行する必要があります。
- CDP ディスカバリ、デバイス / トポロジ、またはインポート コンフィギュレーション ファイル ベースのディスカバリを使用できます。デバイス / トポロジまたはインポート コンフィギュレーション ファイル ベースのディスカバリを使用するを推奨します。
- 新しい L2VPN サービスは、Prime Provisioning にあるサービスと比較して、次のいずれかが見つかった場合に検出されます。
  - イーサネット コア（イーサネット アクセス ドメイン）内の新しい仮想 LAN ID（VLAN ID）
  - MPLS コアの Virtual Private Wire Services（VPWS）サービスに対する新しい Virtual Circuit Identifier（VC ID）。
  - MPLS コアの Virtual Private LAN Service（VPLS）サービスに対する新しい VPLS Forwarding Instance Identifier（VFI ID）。
- Prime Provisioning L2VPN Management のディスカバリ プロセスは、MPLS コア、イーサネット コア、またはその両方の Metro Ethernet を検出できます。
- Prime Provisioning L2VPN Management のために NPC ディスカバリ ステップを実行する前に、N-PE デバイスのアクセス ドメインを指定する必要があります。
- Existing Modified または Conflicting としてマークされた NPC で設定済みの新しいリンクは、検出されません。
- 自動ディスカバリ プロセスの完了後に、検出されたすべてのデバイスに対して、[Task Manager] > [Collect Config] のタスクをスケジューリングし、実行する必要があります。

（注） L2VPN サービス ディスカバリでは、同期は行われません。変更はすべて Prime Provisioning ユーザ インターフェイスを使用して手動で実行する必要があります。新しい VPN だけが検出されます。また、変更された既存の NPC や競合が発生している NPC のサービスも検出されません。

Prime Provisioning ディスカバリの Prime Provisioning Prime Diagnostics との使用

ディスカバリ プロセスを実行して、Prime Diagnostics で使用するために MPLS VPN ネットワークを検出する場合は、次の点に注意してください。

- CDP ディスカバリ、デバイス / トポロジ、またはインポート コンフィギュレーション ファイル ベースのディスカバリを使用できます。デバイス / トポロジまたはインポート コンフィギュレーション ファイル ベースのディスカバリを使用するを推奨します。
- Prime Provisioning Prime Diagnostics では、デバイスの検出、ディスカバリ データ収集、およびロールの割り当てのステップだけを実行する必要があります。NPC ディスカバリ ステップまたはサービス ディスカバリ ステップを実行する必要はありません。ただし、NPC ディスカバリ プロセスを実行させることはできます。

  Prime Provisioning ディスカバリの Prime Provisioning Prime Diagnostics との使用に必要なステップのフローチャートについては、図 E-5 を参照してください。

- Prime Provisioning Prime Diagnostics を使用している場合は、通常、P および PE デバイスだけを検出する必要があります。したがって、検出したデバイスに対してロール割り当てのステップを実行する場合は、P および PE デバイスだけにロールを割り当てる必要があります。

（注）　CE デバイスを検出する場合は、CE ロールを割り当てる必要があります。

- 自動ディスカバリ プロセスの完了後に、検出されたすべてのデバイスに対して、[Task Manager] > [Collect Config] のタスクをスケジューリングし、実行する必要があります。

Prime Provisioning トラフィック エンジニアリング管理による Prime Provisioning ディスカバリの使用

通常、Prime Provisioning トラフィック エンジニアリング管理を使用している場合、Prime Provisioning ディスカバリ プロセスを実行する必要はありません。Prime Provisioning トラフィック エンジニアリング管理には、独自のディスカバリ プロセスがあります。このプロセスは、*『Cisco Prime Provisioning 6.3 User Guide』* の TE ネットワーク検出で説明されています。

ただし、Prime Provisioning Traffic Engineering Management（TEM）と Cisco IP solution Center MPLS VPN Management の*両方*を稼働させている場合、Prime Provisioning MPLS VPN Management のためにディスカバリ プロセスを実行する必要があります。

次の点に注意してください。

- 1 つのリージョン（デフォルト リージョン）が TEM のために使用されます。
- また、MPLS VPN Management のために Prime Provisioning ディスカバリを実行している場合は、この章で説明したディスカバリ ワークフローを*先に*実行し、Prime Provisioning トラフィック エンジニアリング管理プロセスを後で実行します。

ディスカバリのタスクの概要（Prime Provisioning MPLS VPN Management および L2VPN Management）

図 E-3 には、Prime Provisioning MPLS VPN Management または Prime Provisioning L2VPN Management アプリケーションで使用されるディスカバリ プロセスの一般的なワークフロー図を示します。

（注）　図 E-5 には、Prime Diagnostics アプリケーションで使用されるディスカバリ プロセスの一般的なワークフロー図を示します。

図 E-3　Prime Provisioning MPLS VPN Management または Prime Provisioning L2VPN Management でのディスカバリの基本ワークフロー

表 E-2 では、Prime Provisioning MPLS VPN Management および Prime Provisioning L2VPN Management のためのディスカバリ ワークフローの各タスクについて説明します。

表 E-2　MPLS VPN および L2VPN Management のディスカバリ ステップの説明

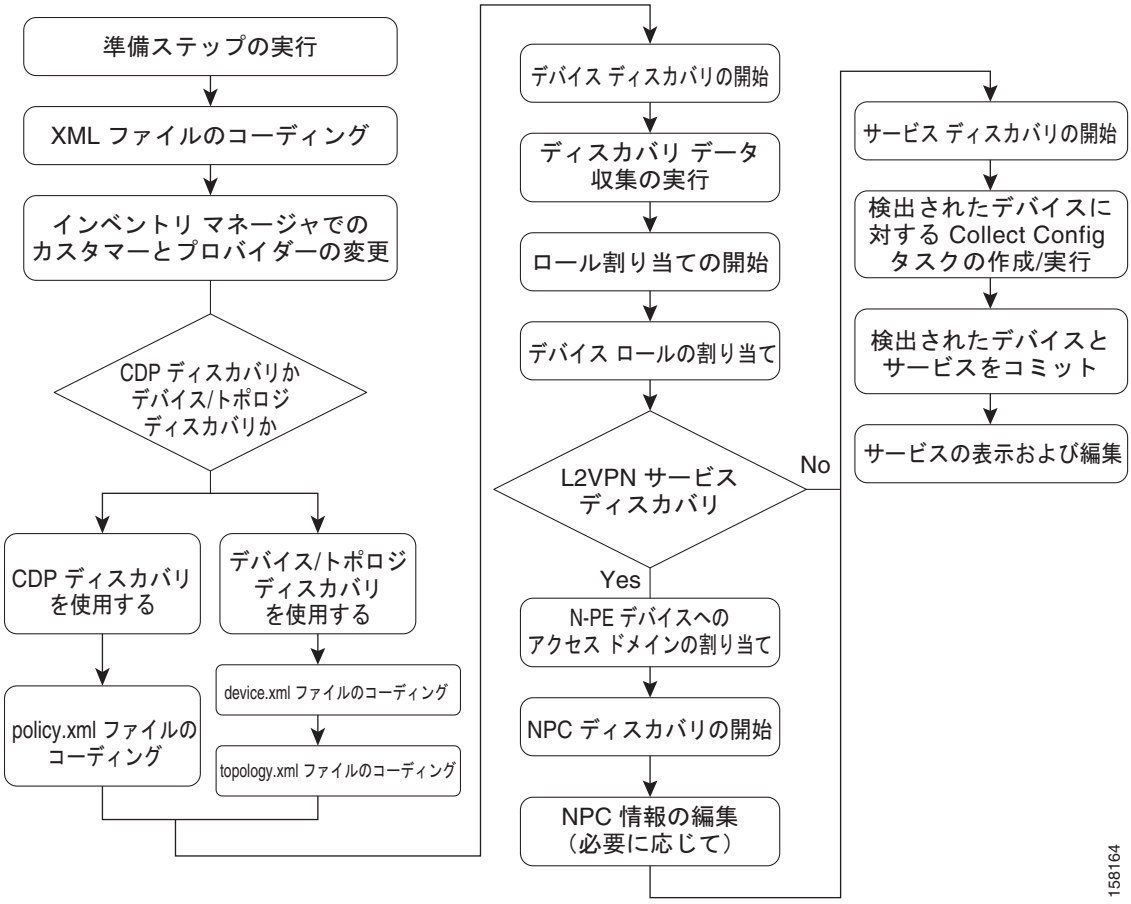
ステップ	説明
ステップ 1：準備ステップの実行	Prime Provisioning ディスカバリに必要な準備ステップを実行します。「ステップ 1：予備ステップの実行」（P.E-16）を参照してください。 • システム要件の確認 「システム要件の確認」（P.E-17）を参照してください。 • ライセンスのインストール 「ライセンスのインストール」（P.E-17）を参照してください。 • （CDP ディスカバリのみ）一意の TIBCO ポートが定義されていることの確認 「（CDP ディスカバリのみ）一意の TIBCO ポートが定義されていることの確認」（P.E-18）を参照してください。 • （CDP ディスカバリのみ）CDP がディスカバリ対象デバイスで実行されていることの確認 「（CDP ディスカバリのみ）CDP がディスカバリ対象デバイスで実行されていることの確認」（P.E-19）を参照してください。 • ディスカバリに必要な XML ファイルのコーディング 「ディスカバリに必要な XML ファイルのコーディング」（P.E-20）を参照してください。
ステップ 2：デバイス ディスカバリの実行	• デバイス ディスカバリの開始 「デバイス ディスカバリの開始」（P.E-27）を参照してください。 • デバイス ディスカバリの完了後に、デバイスのパスワードを入力します。 デバイスのパスワードの入力については、「パスワード属性の設定（必須ステップ）」（P.E-31）を参照してください。 • 必要に応じて、他のデバイス情報を入力します。 「一般デバイス属性の設定」（P.E-32）および「Cisco CNS 属性の設定」（P.E-33）を参照してください。
ステップ 3：ディスカバリ データ収集の実行	コンフィギュレーションの収集を開始します。このステップに必要な入力はありません。「ステップ 3：ディスカバリ データ収集の実行」（P.E-33）を参照してください。
ステップ 4：ロール割り当ての実行	各デバイスにデバイス ロールを割り当てます。「ステップ 4：ロール割り当ての実行」（P.E-34）を参照してください。

表 E-2　MPLS VPN および L2VPN Management のディスカバリ ステップの説明 （続き）

ステップ	説明
ステップ 5：NPC ディスカバリの実行	イーサネット コアの Metro Ethernet ネットワークを検出する場合は、必要な準備ステップを実行します。「メトロ イーサネット ネットワークの NPC ディスカバリ完了前の準備ステップ」（P.E-43）を参照してください。 • NPC ディスカバリの実行 「ステップ 5：NPC ディスカバリの実行」（P.E-43）を参照してください。 • 必要に応じて、NPC を変更または追加します。 「NPC へのデバイスの追加」（P.E-46）、「リングの追加」（P.E-46）、「デバイスの挿入」（P.E-46）、「リングの挿入」（P.E-47）、または「デバイスやリングの削除」（P.E-47）を参照してください。
ステップ 6：MPLS VPN サービス ディスカバリの実行（任意）	MPLS VPN サービス ディスカバリを開始します。「ステップ 6：MPLS VPN サービス ディスカバリの実行（任意）」（P.E-47）を参照してください。 このステップは、Prime Provisioning MPLS VPN Management アプリケーションで必要です。 **（注）** Prime Provisioning L2VPN Management アプリケーションや Prime Provisioning Prime Diagnostics アプリケーションの場合、このステップは必要ありません。
ステップ 7：L2VPN サービス ディスカバリの実行（任意）	L2VPN サービス ディスカバリを開始します。「ステップ 7：L2VPN（メトロ イーサネット）サービス ディスカバリの実行（任意）」（P.E-53）を参照してください。 このステップは、Prime Provisioning L2VPN Management アプリケーションで必要です。 **（注）** Prime Provisioning MPLS VPN Management アプリケーションや Prime Provisioning Prime Diagnostics アプリケーションの場合、このステップは必要ありません。
ステップ 8：検出されたデバイスとサービスの Prime Provisioning リポジトリへのコミット	検出されたデバイスとサービスを Prime Provisioning リポジトリにコミットします。このステップの前に、検出ワークフローは検出されたデバイスとサービスを、検出ワークフローの最後のステップでだけ Prime Provisioning にコミットされる一時リポジトリに格納します。
ステップ 9：検出されたデバイスのコンフィギュレーション収集タスクの作成および実行	[Prime Provisioning Start] ページから、[Operate] > [Tasks] > [Task Manager] と選択します。[Collect Config] タスクを選択し、デバイス ディスカバリ ステップで検出されたデバイスすべてを選択してから、タスクを送信します。 「ステップ 9：検出されたデバイスへのコンフィギュレーション収集タスクの作成と実行」（P.E-60）を参照してください。
ステップ 10：サービスの表示と編集	検出されたサービスは保留状態になり、[Deployed] 状態に移行するにはコンフィギュレーション監査を実行する必要があります。「ステップ 10：サービスの表示と編集」（P.E-61）を参照してください。

各ステップで、追加のタスクを実行し、選択を行う必要があります。図 E-4 には、ディスカバリ ワークフローのすべてのステップを説明する詳細フローチャートを示します。

図 E-4　ディスカバリ ステップの詳細図（Prime Provisioning MPLS VPN Management および Prime Provisioning L2VPN Management）



Prime Diagnostics の Prime Provisioning ディスカバリ ステップの概要

図 E-5 では、Prime Diagnostics アプリケーションでの Prime Provisioning に対する基本ディスカバリ ステップを示します。Prime Diagnostics では、Prime Provisioning MPLS VPN Management および Prime Provisioning L2VPN Management で必要ないくつかのステップは必要ありません。

図 E-5　Prime Diagnostics アプリケーションのディスカバリ ワークフロー

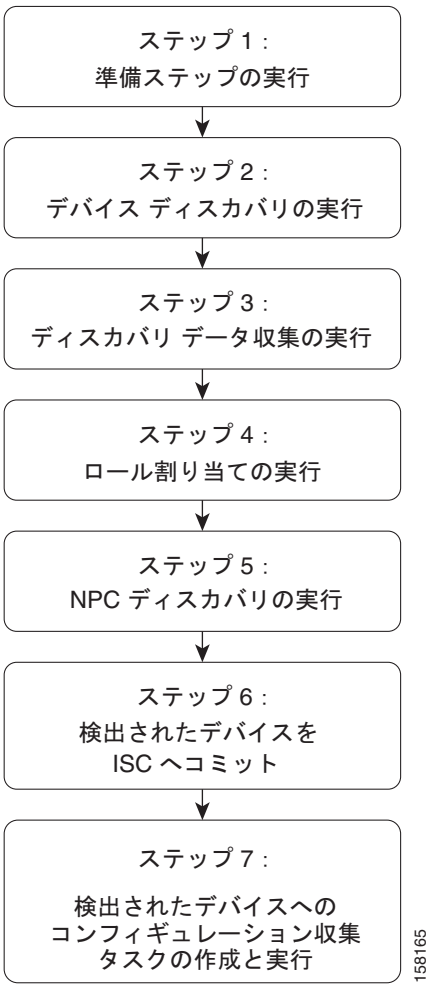


表 E-3　Prime Diagnostics のディスカバリ ステップの説明

ステップ	説明
ステップ 1：準備ステップの実行	Prime Provisioning ディスカバリに必要な準備ステップを実行します。 • システム要件の確認 「システム要件の確認」（P.E-17）を参照してください。 • ライセンスのインストール 「ライセンスのインストール」（P.E-17）を参照してください。 • ディスカバリに必要な XML ファイルのコーディング 具体的な手順については、次の項を参照してください。 – 「ディスカバリに必要な XML ファイルのコーディング」（P.E-20）。
ステップ 2：デバイス ディスカバリの実行	• デバイス ディスカバリの開始 「デバイス ディスカバリの開始」（P.E-27）を参照してください。 • デバイス ディスカバリの完了後に、デバイスのパスワードを入力します。 デバイスのパスワードの入力については、「パスワード属性の設定（必須ステップ）」（P.E-31）を参照してください。 • 必要に応じて、他のデバイス情報を入力します。 「一般デバイス属性の設定」（P.E-32）および「Cisco CNS 属性の設定」（P.E-33）を参照してください。
ステップ 3：ディスカバリ データ収集の実行	コンフィギュレーションの収集を開始します。このステップに必要な入力はありません。「ステップ 3：ディスカバリ データ収集の実行」（P.E-33）を参照してください。

表 E-3　Prime Diagnostics のディスカバリ ステップの説明 （続き）

ステップ	説明
ステップ 4：ロール割り当ての実行	各デバイスにデバイス ロールを割り当てます。 「ステップ 4：ロール割り当ての実行」（P.E-34）を参照してください。 Prime Diagnostics の場合、検出されるのは通常 P および PE だけで、割り当てるのも P および PE ロールだけです。しかし、CE が検出された場合、CE デバイスには CE ロールを割り当てます。 **（注）** Prime Diagnostics の NPC を編集する必要はありませんが、ロール割り当てを実行した後に、このステップを完了する必要があります。
ステップ 5：検出されたデバイスのコンフィギュレーション収集タスクの作成および実行	[Prime Provisioning Start] ページから、[Operate] > [Tasks] > [Task Manager] と選択します。[Collect Config] タスクを選択し、デバイス ディスカバリ ステップで検出されたデバイスすべてを選択してから、タスクを送信します。 「ステップ 8：検出されたデバイスとサービスの Prime Provisioning リポジトリへのコミット」（P.E-60）を参照してください。

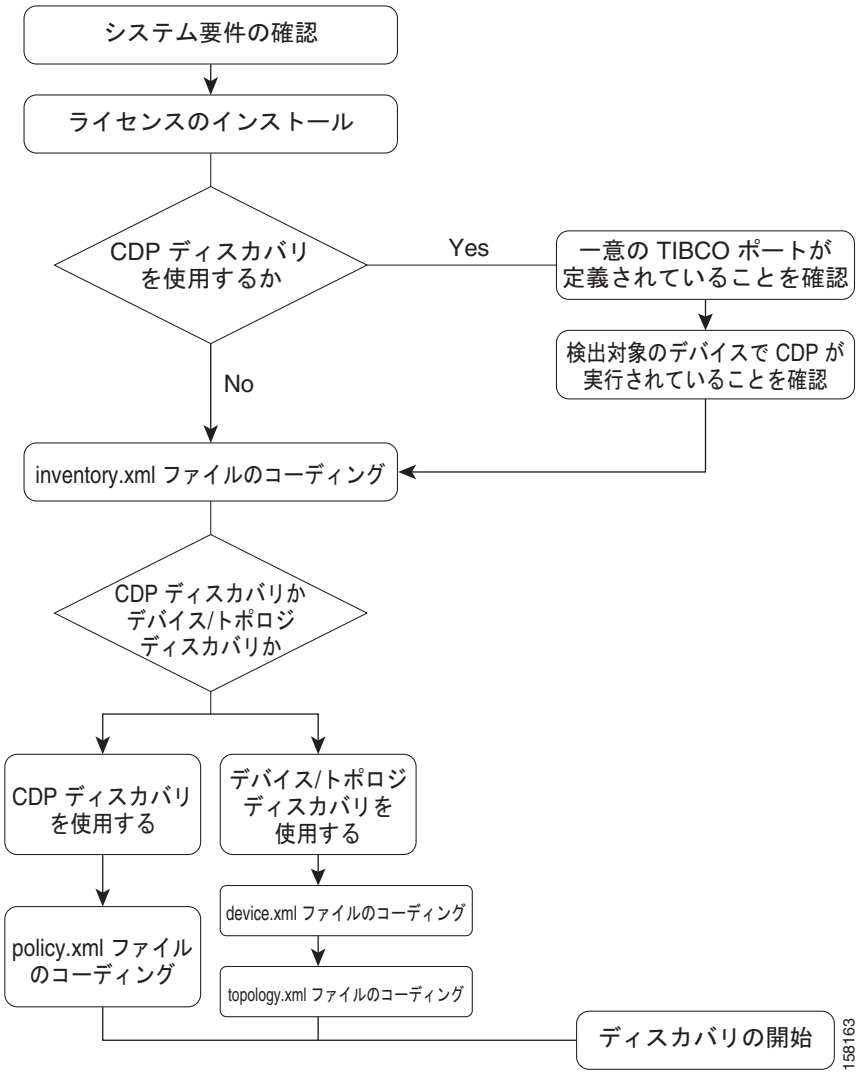
ステップ 1：予備ステップの実行

Prime Provisioningディスカバリ プロセスを開始する前に、次の準備ステップを完了します。

- システム要件の確認
- ライセンスのインストール
- 大規模ネットワークでのディスカバリ
- （CDP ディスカバリのみ）一意の TIBCO ポートが定義されていることの確認
- （CDP ディスカバリのみ）CDP がディスカバリ対象デバイスで実行されていることの確認
- ディスカバリに必要な XML ファイルのコーディング

図 E-6 に、Prime Provisioning ディスカバリの準備ステップの概要を示します。

図 E-6　ディスカバリの準備ステップの概要



システム要件の確認

インストールの計画前に Prime Provisioning のシステム要件を十分に確認し、インストールを成功させるために必要なハードウェアとソフトウェアがすべて揃っていることを確認することを推奨します。

Prime Provisioning に対するシステムの推奨事項および要件は、*『Cisco Prime Provisioning 6.3 Installation Guide』*の第 1 章「System Recommendations」と、*『Cisco Prime Provisioning 6.3 Release Notes』* に示されています。

ライセンスのインストール

検出を開始する前に、適切なライセンス（アクティベーションと VPN ライセンスの両方）をインストールする必要があります。また、各ライセンスは、すべての検出されうるオブジェクトを処理するために、十分な規模にする必要があります。ライセンスのインストールの詳細については、*『Cisco Prime Provisioning 6.3 Installation Guide』* の第 2 章の「Installing License Keys」項、「Installing and Logging In to Prime Provisioning」を参照してください。

大規模ネットワークでのディスカバリ

トポロジが複雑な大規模なネットワークを検出するには、次のように 2 つの DCPL プロパティをリセットすることを推奨します。

ステップ 1　Dynamic Component Properties Library（DCPL）プロパティに移動する方法については、Appendix B, “Property Settings” を参照してください。

ステップ 2　プロパティ **watchdog\server\discovery\heartbeat\timeout** に移動し、このプロパティを **180000 milliseconds**（3 分）に設定します。

ステップ 3　プロパティ **watchdog\server\discovery\java\flags** に移動し、このプロパティを **-Xmx3072m -XX:PermSize=256m -XX:MaxPermSize=512m** に設定します。

ステップ 4　Prime Provisioning サーバを再起動します。

ヒープとは、L2VPN と Metro Ethernet、レイヤ 3 MPLS VPN、および TEM コンポーネントに対するメモリ セグメントのブロックです。これは、Java Virtual Machine（JVM）プロセスによる使用のために実行時に割り当てられます。これは、大規模な展開では、増大させる必要が生じることがあります。**httpd** プロセスが再起動する場合、次のようにヒープのサイズを大きくします。

ステップ 1　**cd $PRIMEP_HOME/bin**

ステップ 2　**vi tomcat.sh**

ステップ 3　**-Xmx** がある行を検索し、より高い値を指定します。

ステップ 4　**-Xmx512m** を **-Xmx1024m** または **-Xmx2048m** に置き換えて、ヒープ サイズを 1GB または 2GB に設定します。

ステップ 5　**tomcat.sh** ファイルを保存します。

ステップ 6　**stopall** と入力して Prime Provisioning サーバを停止します。

ステップ 7　Prime Provisioning サーバを起動するために **startwd** と入力します。

（CDP ディスカバリのみ）一意の TIBCO ポートが定義されていることの確認

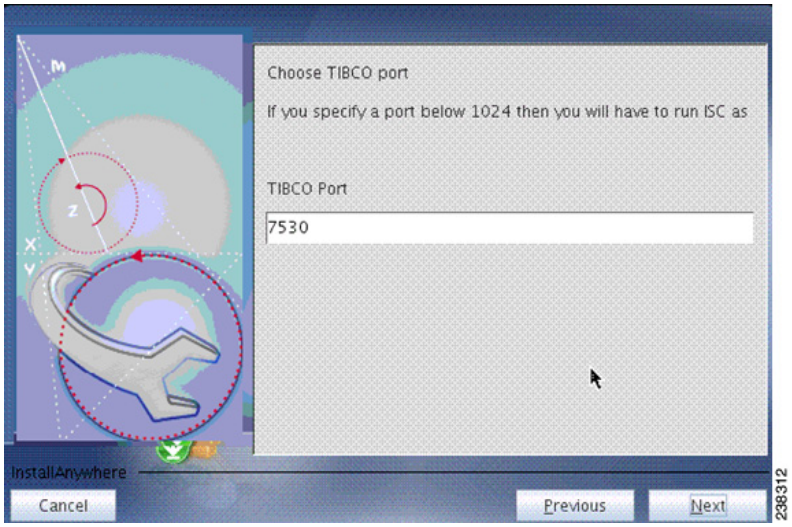
ネットワーク トポロジのディスカバリに CDP ディスカバリを使用している場合、TIBCO ポートが一意であることを確認します。一意でない場合、CDP ディスカバリは失敗します。

インストール プロセスの開始時に「カスタム」インストール タイプを選択した場合は、インストール中に、TIBCO ポートを指定できます。それ以外の場合、インストールされるデフォルト ポートは 7530 です。[Choose TIBCO Port] ダイアログで TIBCO ポートを指定します。

指定するポート番号は、ネットワーク全体で一意である必要があり、その他の Prime Provisioning インストールで同じポートを使用することはできません。

図 E-7 には、[Choose TIBCO Port] ダイアログを示します。

図 E-7　Choose TIBCO Port



Tibco ポートは、インストールの後に、Appendix B, “Property Settings” で指定する Dynamic Component Properties Library エントリの /SYSTEM/tibco/port を修正することにより、インストール後に変更できます。

（CDP ディスカバリのみ）CDP がディスカバリ対象デバイスで実行されていることの確認

CDP ディスカバリを使用する場合は、**show cdp** コマンドを使用して、ディスカバリの対象となるすべてのデバイスで CDP が実行されていることを確認します。

例 E-1 に示すように、デバイスごとに、**show cdp** コマンドを入力します。

例 E-1　show cdp コマンド：

```
Router# show cdp
Global CDP information:
        Sending CDP packets every 120 seconds
        Sending a holdtime value of 180 seconds
        Sending CDPv2 advertisements is enabled
Router#
```

（注）　複数の IP アドレスが設定されているデバイスに対して CDP ディスカバリを実行する場合は、CDP ディスカバリによって、管理 IP アドレス以外の IP アドレスが検出される場合があります。検出された IP アドレスが Prime Provisioning サーバからアクセスできない場合、CDP ディスカバリを使用して、そのデバイスを検出することはできません。

ディスカバリに必要な XML ファイルのコーディング

Prime Provisioning ディスカバリの実行前に、ディスカバリ プロセスに必要な XML ファイルをコーディングしておく必要があります。CDP ディスカバリまたはデバイス / トポロジ ベースのディスカバリのいずれを使用するかに応じて、異なるファイルのセットが必要です。

表 E-4 では、XML ファイルについて説明し、各タイプのディスカバリ方式に対して必要なファイルを示します。

表 E-4　Prime Provisioning ディスカバリで使用される XML ファイル

XML ファイル	説明	CDP ディスカバリに必要	デバイス / トポロジ ベースのディスカバリに必要
policy.xml	指定シード デバイスから到達可能な 1 つ以上のシード IP アドレスおよびデバイス ディスカバリ プロセスの最大ホップ カウントを指定します。	Yes	No
device.xml	デバイスの IP アドレスとオブジェクト ID（OID）など、デバイスを位置づけるための情報を指定します。	No	Yes
topology.xml	MPLS VPN またはメトロ イーサネット トポロジあるいはその両方で使用される NPC の構築に使用する情報を指定します。	No	Yes

（注）　XML ファイルのコーディングが正しいことを確認します。ファイルにエラーがある場合、ディスカバリ プロセスを再実行する必要が生じる場合があります。

サンプル XML ファイル

Prime Provisioning の初回インストールでは、独自の XML ファイルのコーディングで開始点として使用できるサンプル XML ファイルが提供されます。サンプル XML ファイルは、次のディレクトリにあります。

<*install_directory*>/resources/discovery/sample

ここで、<*install_directory*> は、Prime Provisioning インストール プログラムによって要求されたときに指定したインストール ディレクトリです。

policy.xml ファイルのコーディング

policy.xml ファイル：

- CDP ディスカバリに必要です。
- Prime Provisioning MPLS VPN Management、Prime Provisioning Carrier Ethernet、L2VPN Management、Prime Diagnostics で必要です。
- デバイス / トポロジ ベースのディスカバリでは必要ありません。
- Prime Provisioning Traffic Engineering Management では必要ありません。
- シード デバイスの近くのデバイスを検出するために CDP プロトコルが使用するシード IP アドレスを提供します。

例 E-2 は、Prime Provisioning インストール時に準備されているサンプル **policy.xml** ファイルです。

例 E-2　　サンプル policy.xml ファイル

```
<?xml version='1.0' encoding='UTF-8'?>
<DISCOVERY_POLICY overwrite_existing_policy="true">
  <DISCOVERY_METHOD>
    <CDP ipaddress="209.168.133.232" hop="1"/>
  </DISCOVERY_METHOD>
  <SNMP_COMMUNITY>
    <RO_COMMUNITY>
      <COMMUNITY community="public"/>
    </RO_COMMUNITY>
    <RW_COMMUNITY>
      <COMMUNITY community="private"/>
    </RW_COMMUNITY>
  </SNMP_COMMUNITY>

</DISCOVERY_POLICY>
```

ネットワークのコア セグメントのエッジで、PE ルータの反対側に追加のルータがある場合、これらのデバイスを検出するために複数のシード IP アドレスを指定できます。

例 E-3 は、2 つのシード IP アドレスを持つ **policy.xml** ファイルです。

例 E-3　　2 つの IP アドレスを持つ Policy.xml ファイル

```
<?xml version='1.0' encoding='UTF-8'?>
<DISCOVERY_POLICY overwrite_existing_policy="true">
  <DISCOVERY_METHOD>
    <CDP ipaddress="209.168.133.241" hop="8"/>
  </DISCOVERY_METHOD>
  <DISCOVERY_METHOD>
    <CDP ipaddress="209.168.133.244" hop="8"/>
  </DISCOVERY_METHOD>
  <SNMP_COMMUNITY>
    <RO_COMMUNITY>
      <COMMUNITY community="public"/>
    </RO_COMMUNITY>
    <RW_COMMUNITY>
      <COMMUNITY community="private"/>
    </RW_COMMUNITY>
  </SNMP_COMMUNITY>

</DISCOVERY_POLICY>
```

表 E-5 で、**policy.xml** ファイルで使用する XML タグについて説明します。

表 E-5　policy.xml ファイルで使用する XML タグと属性

タグ	説明
<DISCOVERY_METHOD>	**<DISCOVERY_METHOD>** タグを開始します。 **<DISCOVERY_METHOD>** タグには **<CDP>** タグを含める必要があります。
<CDP>	**<CDP>** タグを開始します。**<CDP>** タグは、シード IP アドレスとホップ カウントを指定します。 **<CDP>** タグには、次の属性を含める必要があります。 • **ipaddress** • **hop**
ipaddress	シード デバイスの IP アドレスを指定します。**<CDP>** タグの必須属性です。
hop	デバイスを検出するときに、ipaddress 属性によって指定されたデバイスから何ホップまでを対象とするかを指定します。**<CDP>** タグの必須属性です。

サンプル **policy.xml** ファイルの編集は、次のステップを実行します。

ステップ 1　サンプル ファイルを編集し、**ipaddress** XML 属性で指定された IP アドレスを、ご使用のネットワークの適切な IP アドレスに置き換えます。

この IP アドレスは、Prime Provisioning ホストから到達可能なデバイスです。それぞれのシード デバイスについて、出発点でアクセス可能なインターフェイスが設定されます。管理インターフェイスが必要なためです。管理インターフェイスは、Prime Provisioning ホストがデバイスに到達するために使用する、デバイス上のアドレスです。

（注）　複数の IP アドレスを指定できます。これは、1 つのネットワーク ドメインが、ネットワークのコア セグメントのエッジで、PE ルータの反対側にある場合に便利です。

ステップ 2　**hop** 属性で指定されたホップ カウントを編集し、ディスカバリ プロセスが初期化されるときに使用されるホップ カウントを指定します。

シード デバイスとホップ カウントを選択する場合は、ネットワークの大規模なセクションに到達できるシード デバイスを選択します。これらのデバイスによって、管理対象ネットワーク全体にアクセスすることができると考えられるまで、1 つ以上のシード デバイスを選択します。

通常、Point Of Presence（POP）ルータを選択できます。シード デバイスの集合としてネットワークのすべての POP を選択し、適切な数のハブを配置した場合、管理対象ネットワーク全体が検出されます。

ホップ カウント数を選ぶには、関連付けられた POP から最も遠い CE まで移動するときに、その間にあるデバイスの数を数えます。シードとして POP を選択している場合、この値が N であれば、ハブの数は N+1 です。

ステップ 3　シード デバイスに IP アドレスを追加する必要がある場合は、追加の **<DISCOVERY_METHOD>** タグをコーディングします。

追加の **<DISCOVERY_METHOD>** タグには、**<CDP>** タグを含めます。

各 **<CDP>** タグでは、**ipaddress** 属性で IP アドレスを指定し、**hops** 属性でホップ カウントを指定します。

ステップ 4　**policy.xml** ファイルを Prime Provisioning ホストの適切なディレクトリに保存します。

ディスカバリ プロセスの実行中、プロセスは出発点デバイスを CDP テーブルに問い合わせます。このテーブルから、すべてのデバイスの CDP 情報が問い合わせされます。このプロセスは、開始点から最大ホップ カウントに達するまで続きます。CDP ベースの方法で検出されるのは CDP が稼働中のデバイスだけであることに注意してください。

device.xml ファイルのコーディング

device.xml ファイル：

- デバイス / トポロジ ベースのディスカバリで必要です。
- CDP ベースのディスカバリでは必要ありません。
- Prime Provisioning MPLS VPN Management、Prime Provisioning Carrier Ethernet、L2VPN Management、Prime Diagnostics で必要です。
- Prime Provisioning Traffic Engineering Management では必要ありません。
- デバイスの IP アドレスとオブジェクト ID（OID）など、デバイスを位置づけるための情報を指定します。

例 E-4 に **device.xml** ファイルの例を示します。サンプル ファイルを例として使用し、編集したファイルを適切なディレクトリに保存します。

例 E-4　　サンプル device.xml ファイル

```
<network>
<device>
<device-name>mlpe8</device-name>
<ip-address>209.168.133.244</ip-address>
<system-object-id>.1.3.6.1.4.1.9.1.509</system-object-id>
<snmp-info>
<ro-community>public</ro-community>
</snmp-info>
</device>

<device>
<device-name>mlsw11</device-name>
<ip-address>209.168.133.170</ip-address>
<system-object-id>.1.3.6.1.4.1.9.1.574</system-object-id>
<snmp-info>
<ro-community>public</ro-community>
</snmp-info>
</device>

<device>
<device-name>mlsw16</device-name>
<ip-address>209.168.133.175</ip-address>
<system-object-id>.1.3.6.1.4.1.9.1.574</system-object-id>
<snmp-info>
<ro-community>public</ro-community>
</snmp-info>
</device>

<device>
<device-name>mlsw17</device-name>
<ip-address>209.168.133.176</ip-address>
```

```
<system-object-id>.1.3.6.1.4.1.9.1.574</system-object-id>
<snmp-info>
<ro-community>public</ro-community>
</snmp-info>
</device>

</network>
```

表 E-6 で、**device.xml** ファイルで使用する XML タグについて説明します。

表 E-6　device.xml ファイルで使用する XML タグ

タグ	説明
<device>	**<device>** タグを開始します。**<device>** タグには、次のタグを含める必要があります。 • **<device-name>** • **<ip-address>** 次のタグは、**<device>** タグ内で使用する任意のタグです。 • **<system-object-id>** • **<snmp-info>**
<device-name>	デバイス名を指定します。**<device>** タグ内で必須です。
<ip-address>	デバイスの IP アドレスを指定します。**<device>** タグ内で必須です。
<system-object-id>	（任意）使用するとデバイスに SNMP Object ID（OID; オブジェクト ID）を指定できます。これを指定すると、**<device>** タグ内に指定されます。
<snmp-info>	デバイスの SNMP 情報を指定します。**<snmp-info>** タグには、**<ro-community>** タグを含める必要があります。**<device>** タグ内では任意です。
<ro-community>	デバイスの SNMP アクセスのレベルを指定します。通常は「public」とします。**<snmp-info>** タグ内で必須です。
注：SNMPv3 はサポートされていません。	

次のステップに従って、**device.xml** ファイルをコーディングします。

ステップ 1　インストール時に準備されている **device.xml** ファイルを編集します。

ステップ 2　Prime Provisioning で検出するデバイスのそれぞれに、**<device>** エントリをコーディングします。

各 **<device>** エントリには、次のタグを含める必要があります。

- デバイス名を指定する **<device-name>** タグ。
- デバイスの IP アドレスを指定する **<ip-address>** タグ。
- デバイスの OID を指定する **<system-object-id>** タグ（任意）。
- **<ro-community>** 情報を指定する **<snmp-info>** タグ。

ステップ 3　**device.xml** ファイルを Prime Provisioning ホストの適切なディレクトリに保存します。

topology.xml ファイルのコーディング

topology.xml ファイルについて：

- デバイス / トポロジ ベースのディスカバリで必要です。
- CDP ベースのディスカバリでは必要ありません。
- Prime Provisioning MPLS VPN Management、Prime Provisioning Carrier Ethernet、L2VPN Management、Prime Diagnostics の Prime Provisioning ディスカバリ実行に必要です。
- Prime Provisioning Traffic Engineering Management では必要ありません。
- デバイスの IP アドレスとオブジェクト ID（OID）など、デバイスを位置づけるための情報を指定します。

topology.xml ファイルは、ディスカバリ プロセスで使用するディスカバリ プロトコルを指定し、各接続に対して、開始 IP アドレス、開始インターフェイス、エンド デバイス、および最後のインターフェイスを指定します。

例 E-5 には、サンプル **topology.xml** ファイルを示します。サンプル ファイルを例として使用し、編集したファイルを適切なディレクトリに保存します。

例 E-5　サンプル topology.xml ファイル

```
<topology>
<connection discovery-protocol="CDP" fromDevice="mlsw19"  fromIP="209.168.133.178"
fromInterface="GigabitEthernet1/1/2"   toDevice="mlsw21"  toIP="209.168.133.220"
toIF="GigabitEthernet1/1/1" >
</connection>

<connection discovery-protocol="CDP" fromDevice="mlsw19"  fromIP="209.168.133.178"
fromInterface="FastEthernet1/0/23"   toDevice="mlsw21"  toIP="209.168.133.220"
toIF="FastEthernet1/0/24" >
</connection>

<connection discovery-protocol="CDP" fromDevice="mlsw19"  fromIP="209.168.133.178"
fromInterface="FastEthernet
1/0/24"   toDevice="mlsw18"  toIP="209.168.133.177"  toIF="FastEthernet1/0/23" >
</connection>

<connection discovery-protocol="CDP" fromDevice="mlsw19"  fromIP="209.168.133.178"
fromInterface="FastEthernet1/0/22"   toDevice="mlsw22"  toIP="209.168.133.221"
toIF="FastEthernet1/0/24" >
</connection>

</topology>
```

表 E-7 で、**topology.xml** ファイルで使用する XML タグについて説明します。

表 E-7　topology.xml ファイルで使用する XML タグと属性

タグ	説明
<connection>	**<connection>** タグを開始します。**<connection>** タグでは、次の属性を指定する必要があります。 • **discovery-protocol** • **fromDevice** • **FromIP** • **FromInterface** • **toDevice** • **toIP** • **toIF**
discovery-protocol	ネットワーク トポロジを検出する際に使用する検出プロトコルを指定します。通常は「CDP」です。
fromDevice	名前付き物理回線の開始元のデバイス名を指定します。**<connection>** タグの必須属性です。
FromIP	名前付き物理回線の開始元デバイスの管理 IP アドレスを指定します。**<connection>** タグの必須属性です。
FromInterface	名前付き物理回線の開始元のデバイス インターフェイス名を指定します。**<connection>** タグの必須属性です。
toDevice	名前付き物理回線の接続先デバイス名を指定します。**<connection>** タグの必須属性です。
toIP	名前付き物理回線の接続先デバイスの管理 IP アドレスを指定します。**<connection>** タグの必須属性です。
toIF	名前付き物理回線の接続先デバイス上で、デバイス インターフェイスを指定します。 **<connection>** タグの必須属性です。

次のステップに従って、**topology.xml** ファイルをコーディングします。

ステップ 1　インストール時に準備されている **topology.xml** ファイルを編集します。

ステップ 2　Prime Provisioning で検出する NPC 接続のそれぞれに、**<connection>** エントリをコーディングします。

各 **<connection>** エントリには、次のタグを含める必要があります。

- CDP プロトコルを指定する **discovery-protocol** 属性。
- NPC の開始元のデバイスを指定する **fromDevice** 属性。
- NPC の開始元の管理 IP アドレスを指定する **FromIP** 属性。
- NPC の開始元のデバイス インターフェイスを指定する **FromInterface** 属性。
- NPC の接続先デバイスの名前を指定する **toDevice** 属性。

- NPC の接続先デバイスの管理 IP アドレスを指定する **toIP** 属性。
- NPC の接続先デバイス上のインターフェイス名を指定する **toIF** 属性。

ステップ 3　**topology.xml** ファイルを Prime Provisioning ホストの適切なディレクトリに保存します。

ステップ 2：デバイス ディスカバリの実行

この項では、デバイス ディスカバリ プロセスの開始方法と、デバイス コンフィギュレーションの編集方法について説明します。

デバイス ディスカバリの開始

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　Prime Provisioning にログインします。

ステップ 2　[Inventory] > [Physical Inventory] > [Discovery] とクリックします。

[Device Discovery — CDP Fields] ウィンドウが表示されます。

初期状態では、ディスカバリ方式として [CDP] が選択され、この方式に必要な入力内容がウィンドウに表示されています。

編集可能な [Output Device File] フィールドはオプションで、検出されたデバイスの XML ファイルにデフォルトで設定されています。このファイルは、[Device/Topology] オプション ボタンを選択してデバイス/トポロジ オプションを使用したディスカバリの再実行を行う場合の入力 [Devices File] となります。

編集可能な **Output Connection File** は任意であり、CDP デバイス ディスカバリ中に書き込まれるデバイス接続情報を含む XML ファイルにデフォルト設定されます。このファイルは、[Device/Topology] オプション ボタンを選択してデバイス/トポロジ オプションを使用したディスカバリの再実行を行う場合の入力 [NPC Topology File] となります。

ステップ 3　ディスカバリ方式を選択します。

- Cisco Discovery Protocol（CDP）方式を使用するには、[CDP] オプション ボタンをクリックします。
- デバイス/トポロジ方式を使用するには、[Device/Topology] ボタンをクリックします。
- インポート コンフィギュレーション ファイル方式を使用するには、[Import Configuration Files] ボタンをクリックします。

必須の [Directory] フィールドは、検出するデバイスのコンフィギュレーション ファイルが格納された、サーバ上のディレクトリです。これらのファイルの形式は、*必ず* <*filename*>**.cfg** である必要があります。

[NPC Topology File] フィールドの内容は、NPC を自動作成するために使用するデバイス接続情報が含まれている XML ファイルです。

（注） サービス ディスカバリ中、プロバイダー、リージョン、カスタマー、サイトは自動作成されません。そのため、サービス ディスカバリの実行前に手動で作成しておく必要があります。Prime Provisioning のプロビジョニングでリソース プールが使用される場合、アクセス ドメインとリソース プールはサービス ディスカバリの実行前に手動で作成しておく必要があります。

ステップ 4　[Discovery] ウィンドウで、表 E-8 に示す設定を指定します。

表 E-8　ディスカバリ設定

設定	説明
Name	このフィールドには、ワークフロー名に対して選択した一意の名前を入力します。このフィールドに名前を入力しない場合、システムが一意の名前を生成します。
CDP	このオプション ボタンをクリックして、Cisco Discovery Protocol（CDP）をディスカバリ方式として選択します。
Policy File	[CDP] ボタンをクリックした場合、**policy.xml** ファイルのパスをここで指定します。このファイルは、ディスカバリ プロセスで出発点として使用する 1 つ以上のデバイスの IP アドレスを指示する XML ファイルです。 **policy.xml** ファイルの詳細については、「policy.xml ファイルのコーディング」（P.E-20）を参照してください。
Output Device File	この編集可能なフィールドの設定は任意で、検出されたデバイスの XML ファイルにデフォルト設定されています。このファイルは、[Device/Topology] オプションを使用したディスカバリの再実行を行う場合の入力 [Devices File] にできます。
Output Connection File	この編集可能なフィールドの設定は任意で、CDP デバイス ディスカバリの間に書き込まれたデバイス接続情報を含む XML ファイルにデフォルト設定されています。このファイルは、[Device/Topology] オプションを使用したディスカバリの再実行を行う場合の入力 [NPC Topology File] にできます。
Device/Topology	このオプション ボタンをクリックして、ディスカバリ方式としてデバイス / トポロジを選択します。

表 E-8　ディスカバリ設定 （続き）

設定	説明
Devices File	[Device/Topology] ボタンをクリックした場合、**device.xml** ファイルのパスをここで指定します。このファイルには、IP アドレスや OID など、ネットワーク内でデバイスを位置づけるための情報が含まれています。 **device.xml** ファイルの詳細については、「device.xml ファイルのコーディング」（P.E-23）を参照してください。
NPC Topology File	オプションのこの [Device/Topology] ボタンをクリックした場合、**topology.xml** ファイルのパスをここで指定します。このファイルには、ネットワークの NPC トポロジを判定するために使用される情報が含まれます。 **topology.xml** ファイルの詳細については、「topology.xml ファイルのコーディング」（P.E-25）を参照してください。
Import Configuration Files	このオプション ボタンをクリックして、ディスカバリ方式としてインポート コンフィギュレーション ファイルを選択します。
Directory	この必須フィールドは、検出するデバイスのコンフィギュレーション ファイルが格納された、サーバ上のディレクトリです。これらのファイルの形式は、*必ず*<*filename*>**.cfg** である必要があります。
NPC Topology File	このフィールドには、NPC を自動作成するために使用するデバイス接続情報の XML ファイルが含まれます。
MPLS VPN	MPLS VPN サービスでデバイスを検出するには、[MPLS VPN] オプション ボタンをクリックします。
L2VPN (Metro Ethernet) Discovery	メトロ イーサネット サービスで使用されるレイヤ 2 デバイスを検出するには、[L2VPN (Metro Ethernet) Discovery] オプション ボタンをクリックします。

ステップ 5　[Start] ボタンをクリックします。

ディスカバリ プロセスが開始され、[Discovery Workflow] ウィンドウが表示されます。

データ ペインの [Workflow] カテゴリに、現在のディスカバリ要求や検出ワークフローについての名前情報が表示されます。

[Restart] ボタンをクリックすると、完了したステップのドロップダウン リストが表示されます。ステップを選択すると、そのステップから再開します。

左側の列で、[Current Request] には現在実行中のディスカバリ要求や検出ワークフローが表示されます。現在実行中のディスカバリ要求やワークフローがない場合、初期化ウィンドウが開いて新規のディスカバリ要求やワークフローを作成できます。

左側の列で、[Previous Requests] には検出された要求やワークフローがすべてリストされます。ディスカバリ要求や検出ワークフローそれぞれについて、ステータスやログを参照できます。

[Discovery Workflow] ウィンドウには、デバイス ディスカバリの各フェーズの進行状況が表示されます。

- このウィンドウが最初に開いたとき、ステータス インジケータは黄色で、デバイス ディスカバリ プロセスが初期化中（[Initializing]）であることを示します。
- その後、ステータス インジケータはプロセスが進行中（[In Progress]）であることを示します。
- ディスカバリ プロセスが完了すると、ディスプレイには検出されたデバイス数が表示され、ステータス インジケータはオレンジに変わり、入力待ち（[Pending Input]）であることを示します。

ウィンドウ下部の [Progress] エリアには、検出されたデバイス数が表示されます。

ウィンドウの右下には、[Restart] ボタンがあります。このボタンをクリックすると、ディスカバリ プロセス全体を再起動できます。ただし、ディスカバリ プロセスを再起動すると、ディスカバリの再起動前の作業内容はすべて失われます。

（注） ディスカバリ プロセスの各フェーズ後に、プロセスにエラーがないことを確認するためにログ ファイルをチェックします。具体的な手順については、「ディスカバリのログ ファイルの使用」（P.E-7）を参照してください。

デバイス コンフィギュレーションの編集

ネットワークのデバイスの初回ディスカバリ終了後、Prime Provisioning のデバイスについての情報を編集する必要があります。こうすることで、ディスカバリ プロセスはネットワーク トポロジを判定し、サービス要求を生成するために必要となる、デバイスについてのコンフィギュレーション情報を収集できます。

デバイス コンフィギュレーションの編集には、次のようなステップがあります。

- パスワード属性の設定（必須ステップ）
- 一般デバイス属性の設定
- Cisco CNS 属性の設定

デバイス コンフィギュレーションを編集するには、次のステップを実行します。

ステップ 1　デバイス ディスカバリが [Pending Input] であると [Discovery Workflow] ウィンドウに表示されたら、[Continue] ボタンをクリックします。

[General Attributes - Devices] ウィンドウが表示されます。

[General Attributes - Devices] ウィンドウでは、次の作業が実行できます。

1. デバイスを削除する。

   デバイスのリストに設定対象でないデバイスがある場合、ステップ 4 の説明に従って削除できます。

2. 各デバイスに次のグループの属性を設定する。

   – [General Attributes] : 一般属性には、デバイスのホスト名、デバイス タイプ、管理 IP アドレスやその他の設定が含まれます。

[General Attributes - Devices] ウィンドウに表示されたデフォルトの属性を使用することも、必要に応じて変更することも可能です。

一般属性のリストについては、「一般デバイス属性の設定」（P.E-32）を参照してください。

- [Password Attributes]：パスワード 属性には、デバイスのユーザ名とパスワード、およびデバイスのイネーブル ユーザ名とイネーブル パスワードが含まれます。これらの属性の設定は*必須*です。
- [CNS Attributes]：デバイスが CNS デバイスの場合、CNS 属性を設定します。

ステップ 2　ウィンドウに表示されたデバイスのフィルタリングを行うには、表示させるデバイス名の一部をアスタリスク（*）を前か後に付けて入力し、[Find] ボタンをクリックします。

[Find] フィールドにアスタリスクが表示されている場合、すべてのデバイスが表示されます。

[Find] フィールドの設定は、すべての属性ウィンドウに適用されます。

ステップ 3　属性エリアの 1 つを表示するよう変更するには、ウィンドウ下部の [Attributes] ボタンをクリックし、プルダウン リストで表示する属性エリアを選択します。

- デバイスを設定するために使用するプロトコル（コンフィギュレーション アクセス プロトコル）といった、デバイスの一般属性を変更する必要がある場合、最初に表示されるウィンドウでこの操作を実行できます。

  [General Attributes - Devices] ウィンドウが現在のウィンドウでない場合、[Attributes] ボタンをクリックし、プルダウン リストから [General Attributes] を選択します。

  一般属性の設定については、「パスワード属性の設定（必須ステップ）」（P.E-31）を参照してください。

- パスワード属性を設定するには、[Attributes] ボタンをクリックし、プルダウン リストから [Password Attributes] を選択します。

  パスワード属性の設定については、「パスワード属性の設定（必須ステップ）」（P.E-31）を参照してください。

（注）　この手順は必須です。コンフィギュレーション収集をイネーブルにするには、パスワード属性の設定が*必須*です。

- CNS 属性の変更が必要な場合、「Cisco CNS 属性の設定」（P.E-33）を参照してください。

ステップ 4　1 つ以上のデバイスを削除するには、次のステップを実行します。

a.　削除する各デバイスの横にあるチェックボックスをオンにします。

複数のデバイスを削除する必要がある場合、デバイスのリストの見出し横にあるチェックボックスをオンにします。リストのすべてのデバイスが選択されます。その後、削除しないデバイスのチェックを外します。

b.　デバイスを削除するには、[Delete] ボタンをクリックします。

パスワード属性の設定（必須ステップ）

コンフィギュレーション収集フェーズを正しく完了させるには、各デバイスへのパスワード属性の設定が*必須*です。パスワード属性を設定するには、次のステップを実行します。

ステップ 1　[Password Attributes] ウィンドウが現在のウィンドウでない場合、[Attributes] ボタンをクリックし、プルダウン リストから [Password Attributes] を選択します。

[Password Attributes] ウィンドウが表示されます。

ステップ 2　設定対象のデバイスとパスワード属性を選択するには、次のステップを実行します。

a. 設定対象のパスワード属性を持つデバイス横のチェックボックスをオンにします。

いくつかのデバイスが同じパスワード属性を持つ場合、複数のチェックボックスをオンにできます。すべてのデバイスが同じパスワード属性を持つ場合、見出し行の左にあるチェックボックスをオンにして、リスト内のすべてのデバイスを選択できます。このチェックボックスがオンになっている場合、オフにすることですべてのデバイスの選択を解除できます。

b. 設定するパスワード属性を選択するには、見出し行の属性名の横にあるチェックボックスを 1 つ以上オンにします。

ステップ 3　[Edit] ボタンをクリックします。

ステップ 4　デバイスについて、次の情報を入力します。

- [Login Password] : デバイスのログイン パスワードを入力します。
- [Login User] : デバイスのユーザ名を入力します。
- [Enable User] : イネーブル権限を持つユーザ名を入力します。
- [Enable Password] : イネーブル ユーザのイネーブル パスワードを入力します。

ステップ 5　[Save] をクリックします。

入力した情報が [Password Attributes] ウィンドウに表示されます。

一般デバイス属性の設定

デバイス ディスカバリ プロセスが完了すると、[General Attributes - Devices] ウィンドウに各デバイスの現在の一般属性設定が表示されます。

デバイスの一般属性を変更するには、次のステップを実行します。

ステップ 1　変更する属性をクリックします。

選択した属性の [Edit Attributes] ダイアログボックスが開きます。

ステップ 2　ダイアログボックスに、属性の新しい設定を指定します。

一般デバイス属性には、次の内容が含まれます。

- [Host Name] : 先頭と最後の文字に使用できるのは英字、数字、または下線で、中間の文字として使用できるのは英字、数字、下線、スペース、ハイフン、ドットだけです。このフィールドは必須であり、ターゲット ルータ デバイスで設定されている名前と一致させる必要があります。256 文字に制限されています。
- [Device Type] : デバイス タイプは [Cisco Router] です。
- [Device Description]（このウィンドウでは編集不可）: デバイスのタイプ、位置やその他サービス プロバイダーのオペレータに役立つ情報など、デバイスに関係する情報を何でも含められます。80 文字に制限されています。
- [Management Address] : Prime Provisioning がターゲット ルータ デバイスの設定に使用する、デバイスの有効な IP アドレス。この IP アドレスは、Prime Provisioning ホストから到達可能である必要があります。

- [Domain Name]：先頭と最後の文字に使用できるのは英字、数字、または下線で、中間の文字として使用できるのは英字、数字、下線、スペース、ハイフン、ドットだけです。名前は、ターゲット ルータ デバイスのドメイン名と一致させる必要があります。
- [Config Access Protocol]：コンフィギュレーションのアップロードおよびダウンロード用のアクセス プロトコルを管理します。[Telnet]、[Terminal]、[TFTP]、[RCP] から選択できます。

Cisco CNS 属性の設定

デバイスの 1 つが Cisco CNS デバイスの場合、次のステップに従って CNS 属性を設定します。

ステップ 1　[CNS Attributes] ウィンドウが現在のウィンドウでない場合、[Attributes] ボタンをクリックし、プルダウン リストから [CNS Attributes] を選択します。

[CNS Attributes] ウィンドウが表示されます。

[Terminal Server] 列はエッジ ルータのプロビジョニングに使用可能なワークステーションを表すデバイスを指定し、[Port Number] 列はターミナル サーバが使用するポート番号を指定します。

ステップ 2　既存の [Event Identification] 項目をクリックします。

イベント識別の [Edit Attributes] ダイアログボックスが開きます。

ステップ 3　[Event Identification] 属性のドロップダウン リストから、イベント識別を選択できます。これは [CNS Identification] フィールドの内容が HOST NAME か CNS ID かを示します。デフォルト：[HOST NAME]。

。

デバイス コンフィギュレーションの保存

デバイス コンフィギュレーションを変更した後、[Continue] ボタンをクリックします。

[Device Discovery] インジケータがグリーンに変わり、デバイス ディスカバリの完了（[Complete]）を示します。

ディスカバリ データ収集フェーズが自動的に始まります。

ステップ 3：ディスカバリ データ収集の実行

デバイス コンフィギュレーション設定を保存すると、デバイス ディスカバリのディスカバリ データ収集フェーズが自動的に始まります。

Cisco Prime Provisioning がデバイス コンフィギュレーションを収集している間、ディスカバリ データ収集インジケータはイエローになり、プロセスが進行中（[In Progress]）であることを示します。

ディスカバリ データ収集フェーズが完了すると、インジケータはグリーンに変わり、プロセスの完了（[Complete]）を示します。これでデバイス ロールの割り当ての準備ができました。

ステップ 4：ロール割り当ての実行

デバイス ディスカバリのディスカバリ データ収集フェーズ完了後、[Discovery Workflow] ウィンドウは、ロール割り当てフェーズが入力待ち（[Pending Input]）であることを示します。

ディスカバリ データ収集から再開すると、ディスカバリ データ収集対象デバイスを選択するよう求められます。

デバイス ロールを割り当てるには、次のステップを実行します。

- デバイス ロール割り当ての開始
- デバイス割り当て表示の変更
- デバイス割り当ての変更
- デバイス ロールの決定
- CE デバイス ロールの割り当て
- PE デバイス ロールの割り当て

ここでは、これらのステップについて説明します。

デバイス ロール割り当ての開始

次のステップを実行して、デバイス ロール割り当てを開始します。

ステップ 1　[Discovery Workflow] ウィンドウで、[Continue] をクリックします。

[Role Assignment - Un-assigned Devices] ウィンドウが表示されます。

[Role Assignment - Un-assigned Devices] ウィンドウでは、単一のデバイスを選択した場合、直接デバイス ロールを割り当てるよう求められます。複数のデバイスを選択した場合は、[Role Assignment - CEs] ウィンドウと [Role Assignment - PEs] ウィンドウのいずれかが表示されます。これらのウィンドウで、必要なデバイス ロールを指定できます。

ステップ 2　デバイスの表示方法を変更するには、次の項「デバイス割り当て表示の変更」（P.E-34）を参照してください。

デバイス割り当て表示の変更

次の方法で、[Role Assignment] ウィンドウのデバイス表示方法を変更できます。

- [Role Assignment] ウィンドウ下部のプルダウン リストを使って、未割り当てデバイス、PE デバイス、CE デバイスの表示を切り替えられます。
- ウィンドウ上部にある [Show devices with] の選択と [matching] フィールドを使用して、表示されるデバイスの範囲を変更できます。

表示されるデバイスのカテゴリを変更するには、次のステップを実行します。

ステップ 1　表示されるデバイスのカテゴリを変更するには、[Role Assignment] ウィンドウ下部のプルダウン リストから値を選択します。

- PE デバイスを表示するには、[PEs] を選択します。

- CE デバイスを表示するには、[CEs] を選択します。
- 未割り当てデバイスを表示するには、[Un-assigned Devices] を選択します。

ステップ 2　表示されるデバイスの範囲を変更するには、ウィンドウ上部にある [Show devices with] の選択と [matching] フィールドを組み合わせて使用します。

- ホスト名順にデバイスをリストするには、[Device Host Name] を選択して [matching] フィールドに検索する値を入力してから、[Find] をクリックします。
- ドメイン名順にデバイスをリストするには、[Device Domain Name] を選択して [matching] フィールドに検索する値を入力してから、[Find] をクリックします。
- 管理 IP アドレス順にデバイスをリストするには、[Management IP Address] を選択して [matching] フィールドに検索する値を入力してから、[Find] をクリックします。

[matching] フィールドの値は、表示されるデバイスを制御するサーチ マスクを指定します。アスタリスク（*）は、選択された検索条件にあてはまるすべてのデバイスを指定します。アスタリスクが後に付いた文字列を指定すると、その文字列で始まるホスト名、ドメイン名、管理 IP アドレスを持つすべてのデバイスを表示します。アスタリスクが前に付いた文字列を指定すると、その文字列で終わるホスト名、ドメイン名、管理 IP アドレスを持つすべてのデバイスを表示します。

検索文字列内には、複数のワイルドカード（アスタリスク）値を指定できます。たとえば、ホスト名の一部に「ce」を含むデバイスすべてを表示するには、[matching] フィールドに「*ce*」と入力します。

表示内容は、選択によって変わります。たとえば、2 台のデバイスに CE ロールが割り当てられている場合は、[Role Assignment - CEs] ウィンドウが表示されます。

デバイス割り当ての変更

デバイス ディスカバリ プロセスで、誤ったデバイス ロールがデバイスのグループに割り当てられる場合があります。たとえば、PE となるはずのデバイスに CE が割り当てられることがあります。

この場合、次のステップを実行します。

- PE と表示されるはずのデバイスの一部が [Role Assignment - PEs] ウィンドウにリストされない場合、[Role Assignment - Unassigned Devices] ウィンドウと [Role Assignment - CEs] ウィンドウを確認し、デバイスを PE デバイスとして割り当てます。
  - [Role Assignment - CEs] ウィンドウに移動し、PE デバイスとなるはずのデバイスをすべて選択します。
  - [Assign as PEs] ボタンをクリックします。

    [Role Assignment - PEs] ウィンドウが表示され、PE として割り当てたデバイスがリストされるようになります。
- 希望どおりに割り当てられていない他のデバイスがあれば、必要に応じて基本デバイス割り当てを変更します。

個別および一括でのデバイス割り当て

ロール割り当て用のウィンドウでは、単一のデバイスにデバイス ロールを割り当てることも、一括割り当てを使用する（複数のデバイスを選択してすべてに同じロールを割り当てる）こともできます。

単一のデバイスにデバイス ロールを割り当てる場合、[Site] や [Region] といった他のデバイス属性も割り当てられます。ただし、一括でデバイス ロールを割り当てる場合は、同時に他の属性を割り当てられません。他の属性は、後から [PEs] または [CEs] ウィンドウに移動して割り当てることになります。

デバイス ロールの決定

デバイス割り当ての目的は、プロバイダーのネットワークで検出されたデバイスを、2 つの一般的なグループに区分することです。

- プロバイダー関連デバイス：プロバイダー エッジ（PE）デバイス

  PE ロールの割り当て（U-PE、N-PE、P、PE-AGG）については、「PE ロールの割り当て」（P.E-36）を参照してください。

- カスタマー関連デバイス：カスタマー エッジ（CE）デバイス

  CE ロールの割り当てについては、「CE ロールの割り当て」（P.E-39）を参照してください。

PE デバイスでは、次の注意事項に従ってデバイス ロールを決定します。

- コア ドメインの中央に位置するデバイスを P デバイスとして割り当てます。
- VPN サービスのユーザとインターフェイスが設定されているデバイスは、すべて U-PE デバイスとして割り当てます。これらのデバイスが、ドメインのカスタマー方向エッジにあるデバイスです。
- MPLS コア ドメインまたは L2VPN コア ドメインのエッジにあるデバイスすべてを、N-PE デバイスとして割り当てます。
- デバイス リング内のデバイス、または複数の U-PE デバイスに接続するデバイスを、PE-AGG デバイスとして割り当てます。

  CE デバイスでは、CE ロールの割り当てについての項にある CE ロールの説明（「CE ロールの割り当て」（P.E-39））の特定情報を参照してください。

PE ロールの割り当て

あるデバイスを PE デバイスとして割り当てるには、次のステップを実行します。

ステップ 1　[Role Assignment - Un-assigned Devices] ウィンドウで、PE として割り当てるデバイスを選択します。

- デバイスを選択するには、デバイス名の横のチェックボックスをオンにします。
- デバイスの選択を解除するには、デバイス名の横のチェックボックスをオフにします。

ステップ 2　[Assign as PE(s)] ボタンをクリックします。

ステップ 3　[Assign as PE] ウィンドウで、PE に必要な情報を割り当てます。

a. PE リージョン名を割り当てるには、[Select] ボタンをクリックします。

[PE Region Name] ウィンドウが表示されます。

b. [PE Region Name] ウィンドウで、割り当てるリージョン名の横のオプション ボタンをクリックし、[Select] をクリックします。

[PE Region] フィールドにリージョン名が表示された状態で [Assign as PE] ウィンドウが表示されます。

c. PE ロールを割り当てるには、プルダウン リストから [PE Role] フィールドの値を選択します。

PE ロールは、PE ルータの構造上の役割を指定します。デバイスが属するネットワーク層に基づいて PE ロールを割り当てます。

次の PE ロールを選択できます。

- [N-PE]：ドメインのエッジにある（エッジ レイヤ内）デバイスを、ネットワーク側プロバイダー エッジ（N-PE）デバイスとして割り当てます。
- [U-PE]：ユーザ方向のプロバイダー エッジ内のデバイスを、U-PE デバイスとして割り当てます。
- [P]：コア ドメインの中央に位置するデバイスをプロバイダー コア（P）デバイスとして割り当てます。
- [PE-AGG]：集約レイヤ内のデバイスを Provider Edge Aggregation（PE-AGG）デバイスとして割り当てます。

d. [OK] をクリックします。

指定した値が表示された状態で [Role Assignment - PEs] ウィンドウが表示されます。

PE ロールの編集

1 つ以上のデバイスが PE デバイスとして割り当てられ、[Role Assignment - PEs] ウィンドウに表示された後、PE ロールを編集できます。[Assign as PE] ウィンドウで値が割り当てられなかった場合でも、PE ロールを編集できます。

（注） PE ロールの割り当ては必須ではありません。ただし、予期しない動作の防止のために推奨されています。

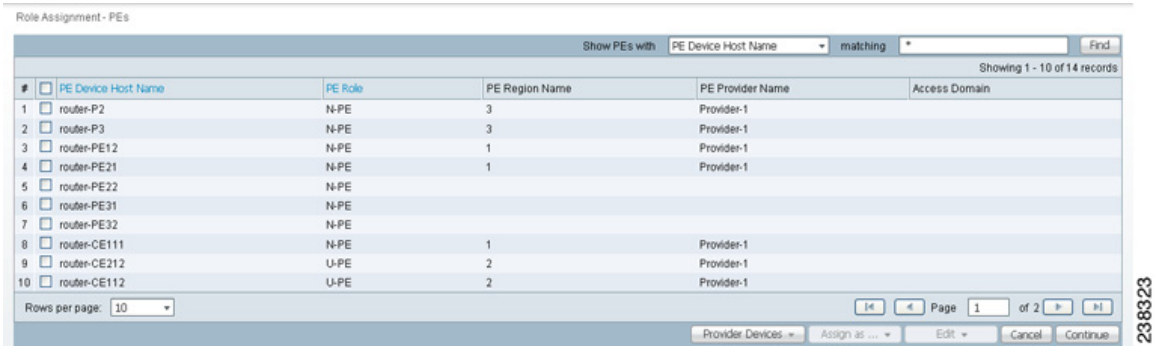
PE デバイスのロール割り当ての値を編集するには、次のステップを実行します。

ステップ 1　デバイス ディスカバリのロール割り当てフェーズがアクティブな間に、[Role Assignment - PEs] ウィンドウを選択します。

[Role Assignment - Un-assigned Devices] または [Role Assignment - CEs] ウィンドウがアクティブの場合、ウィンドウ下部のプルダウンリストから [Role-Assignment - PEs] を選択します。

[Role Assignment - PEs] ウィンドウが表示されます（図 E-8 を参照）。

図 E-8　[Role Assignment - PEs] ウィンドウ



このウィンドウでは、次の列によるソートが無効なことに注意してください。

- PE Device Host Name
- PE Provider Name
- PE Region Name

図 E-8 のウィンドウ例では、PE の 1 つにロール情報が割り当てられています。他の 2 つの PE は、PE として割り当てられていますが、ロール情報は割り当てられていません。PE の情報はすべて、情報が入力されているかどうかにかかわらず編集可能です。

ステップ 2　編集する 1 つ以上の PE を選択します。

- 特定の PE を選択するには、デバイス名の横のチェックボックスをオンにします。
- ウィンドウ内のすべての PE を選択するには、見出し行のチェックボックスをオンにします。

ステップ 3　PE ロールを編集するには、次のステップを実行します。

a. ウィンドウ下部にある [Edit] ボタンをクリックし、プルダウン リストから [PE Role] を選択します。

PE ロールを選択するよう求められます。

b. プルダウン リストから [PE Role] フィールドの値を選択し、PE ロールを割り当てます。

次の PE ロールを選択できます。

- [N-PE]：エッジ レイヤ内のデバイスをネットワーク側プロバイダー エッジ（N-PE）デバイスとして割り当てます。
- [U-PE]：ユーザ方向のプロバイダー エッジ内のデバイスを、U-PE デバイスとして割り当てます。
- [P]：コア レイヤ内のデバイスをプロバイダー コア（P）デバイスとして割り当てます。
- [PE-AGG]：集約レイヤ内のデバイスを Provider Edge Aggregation（PE-AGG）デバイスとして割り当てます。

指定した PE ロールが [Role Assignment - PEs] ウィンドウに表示されます。

ステップ 4　PE プロバイダー名や PE リージョン名を編集するには、次のステップを実行します。

a. ウィンドウ下部にある [Edit] ボタンをクリックし、プルダウン リストから [Region/Provider] を選択します。

リージョン名を入力するよう求められます。

b. ポップアップ ウィンドウにリストされたリージョン名のいずれかを横のオプション ボタンをクリックして選択してから、[Select] ボタンをクリックします。

指定したリージョン名と、関連付けられたプロバイダー名が [Role Assignment - PEs] ウィンドウに表示されます。

CE ロールの割り当て

あるデバイスを CE デバイスとして割り当てるには、次のステップを実行します。

ステップ 1　[Role Assignment - Un-assigned Devices] ウィンドウで、CE として割り当てるデバイスを選択します。

- デバイスを選択するには、デバイス名の横のチェックボックスをオンにします。
- デバイスの選択を解除するには、デバイス名の横のチェックボックスをオフにします。

ステップ 2　[Assign as CE(s)] ボタンをクリックします。[Assign as CE] ウィンドウが表示されます。

ステップ 3　[Assign as CE] ウィンドウで、CE に必要な情報を割り当てます。

a. カスタマー名（必須フィールド）を割り当てるには、[Select] ボタンをクリックします。

[Customer Name] ウィンドウが表示されます。

b. カスタマー名を割り当てるには、割り当てるカスタマー名の横のオプション ボタンをクリックし、[Select] ボタンをクリックします。

指定したカスタマー名が表示された状態で [Assign as CE] ウィンドウが表示されます。

c. CE 管理タイプを割り当てるには、プルダウン リストから [CE Management Type] の値を選択します。

CE 管理タイプは、CE ルータの構造上の役割を指定します。デバイスが属するネットワーク層に基づいて CE 管理タイプを割り当てます。

次の CE 管理タイプを選択できます。

- [MANAGED-REGULAR]：デフォルトの CE ロール割り当てです。プロバイダーに管理させる CE にこのロールを割り当てます。CE は Prime Provisioning サーバから到達可能である必要があります。このロールを割り当てると、インベントリ マネージャ インターフェイスでルータを作成するときに、ルータ コンフィギュレーションが自動的にダウンロードされます。
- [UNMANAGED]：手動で管理するデバイスにこのロールを割り当てます。このロールを割り当てると、新しいデバイスの作成時にデバイス コンフィギュレーションは自動で割り当てられず、デバイスを手動で設定する必要があります。プロバイダーは管理対象外 CE を直接プロビジョニングできません。[Unmanaged] を選択すると、プロバイダーは Prime Provisioning を使用してコンフィギュレーションを生成した後、コンフィギュレーションを CE に配置するようカスタマーに送ることができます。
- [MANAGED-MGMT-LAN]：デバイス管理が PE コンフィギュレーションにリンクすることを示します。新規デバイスが作成されると、コンフィギュレーションが自動的にダウンロードされます。管理対象の Management LAN や Management CE（MCE; 管理 CE）は管理対象の CE ルータのように設定されますが、存在するのはプロバイダー空間内です。通常、MCE は、Network Operations Center（NOC; ネットワーク オペレーション センター）ゲートウェイ ルータとして機能します。
- [UNMANAGED-MGMT-LAN]：デバイス管理が PE コンフィギュレーションに関連付けられているが、新規デバイス作成時にコンフィギュレーションが自動でダウンロードされないことを示します。管理対象外の Management LAN や MCE は管理対象外 CE ルータのように設定

されますが、存在するのはプロバイダー空間内です。通常、MCE は、Network Operations Center（NOC; ネットワーク オペレーション センター）ゲートウェイ ルータとして機能します。

- [DIRECT-CONNECTED-REGULAR]：ほとんどの場合、CE は PE ルータに接続されます。この場合、CE はワークステーションまたはその他のデバイスに接続されます。
- [DIRECT-CONNECTED-MGMT-HOST]：ほとんどの場合、CE は PE ルータに接続されます。このケースでは、CE は Prime Provisioning の存在するワークステーションや他のデバイスに接続されます。
- [MULTI-VRF]：PE と CE との間に VPN Routing/Forwarding（VRF; VPN ルーティング/転送）インスタンスであるデバイスが存在することを示します。Multi-VRF CE（MVRFCE; マルチ VRF CE）はカスタマーの所有ですが、プロバイダー空間に存在します。PE からのオフロード トラフィックに使用されます。
- [UNMANAGED-MULTI-VRF]：管理対象外のマルチ VRF CE は、管理対象外の CE のようにプロビジョニングされます（プロバイダーによってコンフィギュレーションのアップロードやデバイスへのアップロードが行われない）。これはカスタマーの所有であり、プロバイダー空間に存在します。

d. [OK] をクリックします。

指定した値が表示された状態で [Role Assignment - CEs] ウィンドウが表示されます。

（注） この時点で、[CE Site] の値は未割り当てです。この値を割り当てるには、設定を編集する必要があります。このタスクについては、「CE ロールの編集」（P.E-40）を参照してください。

CE ロールの編集

1 つ以上のデバイスが CE デバイスとして割り当てられ、[Role Assignment - CEs] ウィンドウに表示された後、CE ロールを編集できます。[Assign as CE] ウィンドウで値が割り当てられなかった場合でも、CE ロールを編集できます。

CE デバイスのロール割り当ての値を編集するには、次のステップを実行します。

ステップ 1　デバイス ディスカバリのロール割り当てフェーズがアクティブな間に、[Role Assignment - CEs] ウィンドウを選択します。

[Role Assignment - Un-assigned Devices] または [Role Assignment - PE] ウィンドウがアクティブの場合、ウィンドウ下部のプルダウンリストから [Role-Assignment - CEs] を選択します。

[Role Assignment - CEs] ウィンドウが表示されます。

図 E-9　[Role Assignment - CEs] ウィンドウ

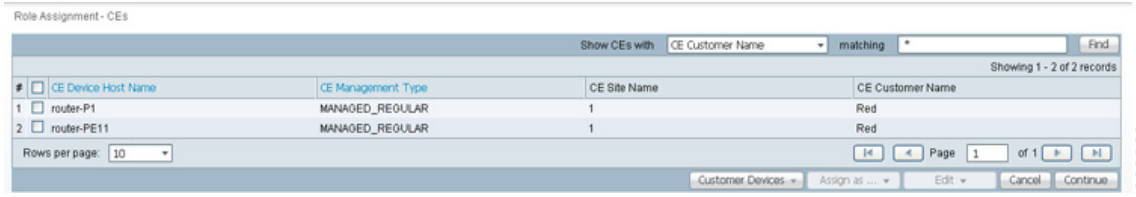


図 E-9 に示した [Role Assignment - CEs] ウィンドウでは、CE のうち 2 つにはロール割り当て情報が割り当てられ、2 つには情報が割り当てられていません。CE の情報はすべて、情報が入力されているかどうかにかかわらず編集可能です。

このウィンドウでは、次の列によるソートが無効なことに注意してください。

- CE Device Host Name
- CE Site Name
- CE Customer Name

ステップ 2　編集する 1 つ以上の CE を選択します。

- 特定の CE を選択するには、デバイス名の横のチェックボックスをオンにします。
- ウィンドウ内のすべての CE を選択するには、見出し行のチェックボックスをオンにします。

ステップ 3　カスタマー名を編集するステップは、次のとおりです。

a. ウィンドウ下部にある [Edit] ボタンをクリックし、プルダウン リストから [Customer] を選択します。

カスタマー名を選択するよう求められます。

b. カスタマー名を選択するには、表示されたいずれかのカスタマー名の横のオプション ボタンをクリックし、[Select] ボタンをクリックします。

指定したカスタマー名が表示された状態で [Role Assignment - CEs] ウィンドウが表示されます。

ステップ 4　CE 管理タイプを編集するステップは、次のとおりです。

a. 編集する 1 つ以上の CE を選択します。

b. ウィンドウ下部にある [Edit] ボタンをクリックし、プルダウン ウィンドウから [CE Management Type] を選択します。

CE 管理タイプは、CE ルータの構造上の役割を指定します。デバイスが属するネットワーク層に基づいて CE 管理タイプを割り当てます。

次の CE 管理タイプを選択できます。

- [MANAGED-REGULAR]：デフォルトの CE ロール割り当てです。プロバイダーに管理させる CE にこのロールを割り当てます。CE は Prime Provisioning サーバから到達可能である必要があります。このロールを割り当てると、インベントリ マネージャ インターフェイスでルータを作成するときに、ルータ コンフィギュレーションが自動的にダウンロードされます。
- [UNMANAGED]：手動で管理するデバイスにこのロールを割り当てます。このロールを割り当てると、新しいデバイスの作成時にデバイス コンフィギュレーションは自動で割り当てられず、デバイスを手動で設定する必要があります。プロバイダーは管理対象外 CE を直接プロビジョニングできません。[Unmanaged] を選択すると、プロバイダーは Prime Provisioning を使用してコンフィギュレーションを生成した後、コンフィギュレーションを CE に配置するようカスタマーに送ることができます。

- [MANAGED-MGMT-LAN] : デバイス管理が PE コンフィギュレーションにリンクすることを示します。新規デバイスが作成されると、コンフィギュレーションが自動的にダウンロードされます。管理対象の Management LAN や Management CE（MCE; 管理 CE）は管理対象の CE ルータのように設定されますが、存在するのはプロバイダー空間内です。通常、MCE は、Network Operations Center（NOC; ネットワーク オペレーション センター）ゲートウェイ ルータとして機能します。
- [UNMANAGED-MGMT-LAN] : デバイス管理が PE コンフィギュレーションに関連付けられているが、新規デバイス作成時にコンフィギュレーションが自動でダウンロードされないことを示します。管理対象外の Management LAN や MCE は管理対象外 CE ルータのように設定されますが、存在するのはプロバイダー空間内です。通常、MCE は、Network Operations Center（NOC; ネットワーク オペレーション センター）ゲートウェイ ルータとして機能します。
- [DIRECT-CONNECTED-REGULAR] : ほとんどの場合、CE は PE ルータに接続されます。この場合、CE はワークステーションまたはその他のデバイスに接続されます。
- [DIRECT-CONNECTED-MGMT-HOST] : ほとんどの場合、CE は PE ルータに接続されます。このケースでは、CE は Prime Provisioning の存在するワークステーションや他のデバイスに接続されます。
- [MULTI-VRF] : PE と CE との間に VPN Routing/Forwarding（VRF; VPN ルーティング / 転送）インスタンスであるデバイスが存在することを示します。Multi-VRF CE（MVRFCE; マルチ VRF CE）はカスタマーの所有ですが、プロバイダー空間に存在します。PE からのオフロード トラフィックに使用されます。
- [UNMANAGED-MULTI-VRF] : 管理対象外のマルチ VRF CE は、管理対象外の CE のようにプロビジョニングされます（プロバイダーによってコンフィギュレーションのアップロードやデバイスへのアップロードが行われない）。これはカスタマーの所有であり、プロバイダー空間に存在します。

c. [Select] をクリックします。

指定した CE 管理タイプが表示された状態で [Role Assignment - CEs] ウィンドウが表示されます。

ステップ 5　サイト名の指定や既存のサイト名の編集を行うには、次のステップを実行します。

a. 編集する 1 つ以上の CE を選択します。

b. ウィンドウ下部にある [Edit] ボタンをクリックし、プルダウン ウィンドウから [Site] を選択します。

[Site Name] ウィンドウが表示されます。

c. [Site Name] ウィンドウで、割り当てるサイト名の横のオプション ボタンをクリックし、[Select] ボタンをクリックします。

指定したサイト名が表示された状態で [Role Assignment - CEs] ウィンドウが表示されます。

ロール割り当て情報の保存

デバイスへのロールの割り当てが終わったら、[Continue] ボタンをクリックします。

[Role Assignment Discovery] インジケータがグリーンに変わり、ロール割り当ての完了（[Complete]）を示します。

これでデバイス ディスカバリの NPC ディスカバリ フェーズ開始の準備ができました。

ステップ 5：NPC ディスカバリの実行

デバイス ディスカバリのロール ディスカバリ フェーズ完了後、[Discovery Workflow] ウィンドウは、NPC ディスカバリ フェーズが入力待ち（[Pending Input]）であることを示します。

検出された NPC のリストを参照したり、必要に応じて NPC を削除したりするには、次の一般的なステップを実行します。

- *イーサネット コアのメトロ イーサネット ネットワーク トポロジ*を検出する場合、「メトロ イーサネット ネットワークの NPC ディスカバリ完了前の準備ステップ」（P.E-43）に説明されているステップを実行します。
- 「NPC 割り当ての開始」（P.E-44）で説明されている NPC 割り当てのステップを完了させます。
- 必要であれば、「NPC へのデバイスの追加」（P.E-46）や次の項で説明されているように、NPC の追加や変更のためのステップを完了させておきます。

メトロ イーサネット ネットワークの NPC ディスカバリ完了前の準備ステップ

イーサネット コアのメトロ イーサネット トポロジを検出する場合、次のステップを実行します。

- 1 つ以上のアクセス ドメインを作成し、デバイス ディスカバリ フェーズで検出されたデバイスをアクセス ドメインに割り当てます。
- 最低 1 つのリソース プールを作成します。
- 各デバイスの「Inter-N-PE インターフェイス」を編集します。

これらのステップは、Service Inventory インターフェイスの Inventory and Connection Manager（[Service Inventory] > [Inventory and Connection Manager]）を使用して実行します。

アクセス ドメインの作成

アクセス ドメインを作成し、検出されたデバイスをドメインに追加するには、次のステップを実行します。

ステップ 1　[Prime Provisioning Start] ページで、[Service Inventory] を選択します。

ステップ 2　[Service Inventory] ウィンドウで、[Inventory and Connection Manager] を選択します。

[Inventory and Service manager] ウィンドウが開きます。

ステップ 3　ウィンドウの左側領域で、[Access Domains] を選択します。

[Access Domains] ウィンドウが表示されます。

ステップ 4　1 つ以上のアクセス ドメインを作成し、L2VPN メトロ イーサネット トポロジ内のデバイスを作成したアクセス ドメインに割り当てます。

アクセス ドメインの作成の詳細については、の第 2 章「Prime Provisioning を設定する前に」「アクセス ドメインの作成」（P.2-43）の項を参照してください。

リソース プールの作成

リソース プールを作成するには、次のステップを実行します。

ステップ 1　[Prime Provisioning Start] ページで、[Service Inventory] を選択します。

ステップ 2　[Service Inventory] ウィンドウで、[Inventory and Connection Manager] を選択します。

[Inventory and Service manager] ウィンドウが開きます。

ステップ 3　ウィンドウの左側領域で、[Resource Pools] を選択します。

[Resource Pools] ウィンドウが表示されます。

ステップ 4　リソース プールを作成します。

ステップ 5　[Pool Type] で [VLAN] が選択されていることを確認します。

ステップ 6　[Start] の値として 2 を入力します。

ステップ 7　[Pool Size] の値には、リソース プール内のデバイス数に対応できる、十分に大きな値（500 など）を入力します。

リソース プールの作成の詳細については、第 2 章「Prime Provisioning を設定する前に」の「リソース プール」（P.2-46）の項を参照してください。

Inter-N-PE インターフェイスの編集

ご使用のメトロ イーサネット トポロジ内のデバイス用に「Inter N-PE」インターフェイスを編集するには、次のステップを実行します。

（注）　これらのステップが必要なのは、PE デバイスがリポジトリ内にすでに存在している場合だけです。

ステップ 1　[Prime Provisioning Start] ページで、[Service Inventory] を選択します。

ステップ 2　[Service Inventory] ウィンドウで、[Inventory and Connection Manager] を選択します。

[Inventory and Service manager] ウィンドウが開きます。

ステップ 3　ウィンドウの左側領域で、[PE Devices] を選択します。

[PE Devices] ウィンドウが表示されます。

ステップ 4　トポロジ内の各 PE デバイスを選択し、次の操作を実行します。

a.　[Edit] ボタンをクリックします。

[Edit PE] ウィンドウが表示されます。

b.　デバイスが接続されている各デバイスへのインターフェイスを見つけます。

c.　各インターフェイスについて、[Metro Ethernet] 列の [Any] を [None] に変更します。

d.　変更を保存します。

次の項「NPC 割り当ての開始」（P.E-44）へ進み、NPC 割り当ての開始のステップを実行します。

NPC 割り当ての開始

次のステップを実行して、NPC 割り当てを開始します。

ステップ 1　[Discovery Workflow] ウィンドウで、[Continue] をクリックします。

[Named Physical Circuits] ウィンドウが表示されます。

[Named Physical Circuits] ウィンドウは、初期状態では検出された回線すべてを表示しています。

この時点で、必要に応じて NPC を作成、追加、または削除できます。

[State] 列には次のカテゴリがあります。

- [New]：Prime Provisioning に対応する NPC が存在しない。新しい NPC だけが Prime Provisioning にコミットされます。
- [Existing]：検出された NPC は Prime Provisioning の NPC と同一です。
- [Existing Modified]：Prime Provisioning の NPC とは送信元とエンドポイントは同じですが、1 つ以上の中間リンクが異なります。
- [Conflicting]：検出された NPC と Prime Provisioning の NPC とが競合しています。

Named Physical Circuit（NPC; 名前付き物理回線）は、CPE または U-PE と N-PE との間の物理的な接続を表す名前付き回線です。NPC の中間ノードは U-PE と PE-AGG のいずれかです。これらは、環状に接続でき、デバイスの環を形成します。これは、NPC リングと呼ばれるエンティティによって表されます。NPC リングはデバイスと名前付き物理回線とのリング型トポロジを表します。NPC を作成するには、送信元 CPE/U-PE と宛先 N-PE とがどのように接続されているかを指定し、中間ノードを指定する必要があります。

ステップ 2　NPC を定義する必要がある場合、次のステップを実行します。

a.　[Named Physical Circuits] ウィンドウで、[Create] をクリックします。

[Create a Physical Circuit] ウィンドウが表示されます。

初期状態では、NPC リストは空です。

b.　[Add Device] ボタンをクリックします。

[Select a Device] ウィンドウが表示されます。

ステップ 3　このウィンドウで、デバイスのオプション ボタンをクリックしてから [Select] ボタンをクリックします。

初期デバイスが追加された状態で [Create a Named Physical Circuit] ウィンドウが開きます。

ウィンドウのボタンがアクティブに変わります。

c.　画面上のデバイスをクリックし、次のいずれかの処理を選択します。

- デバイスを挿入するには、[Insert Device] ボタンをクリックします。
- リングを挿入するには、[Insert Ring] ボタンをクリックします。
- デバイスを追加するには、[Add Device] ボタンをクリックします。
- リングを追加するには、[Add Ring] ボタンをクリックします。
- 既存のデバイスやリングを削除するには、デバイスを選択して [Delete] ボタンをクリックします。

ステップ 4　詳細は、次の項を参照してください。

NPC へのデバイスの追加

ステップ 1　[Create a Named Physical Circuit] ウィンドウで着信インターフェイスを選択するには、[Select Incoming Interface] をクリックします。

[Select Device Interface] ウィンドウが表示されます。このウィンドウには、選択されたデバイス上のインターフェイスが表示されています。

ステップ 2　リストでインターフェイス横のオプション ボタンをクリックし、[Select] ボタンをクリックします。

選択されたインターフェイスが [Create a Named Physical Circuit] ウィンドウに表示されます。

ステップ 3　発信インターフェイスを選択するには、[Select Outgoing Interface] をクリックします。

デバイス上に設定されているインターフェイスのリストが表示されます。

ステップ 4　リストでインターフェイス横のオプション ボタンをクリックし、[Select] ボタンをクリックします。

発信インターフェイスが [Create a Named Physical Circuit] ウィンドウに表示されます。

ステップ 5　必要に応じて追加デバイスを選択し、着信インターフェイスまたは発信インターフェイスあるいはその両方を指定します。

ステップ 6　完了後、[Create a Named Physical Circuit] ウィンドウの [Save] ボタンをクリックします。

リングの追加

現在選択されているデバイスの前にリングを追加するには、次のステップを実行します。

（注）　リングの増分サービス ディスカバリはサポートされていません。

ステップ 1　[Create a Named Physical Circuit] ウィンドウで、[Add Ring] をクリックします。

[Select NPC Rings] ウィンドウが表示されます。ネットワーク トポロジ内に存在するリングは、すべてこのウィンドウに表示されます。

ステップ 2　ウィンドウにリストされたリング横のオプション ボタンをクリックし、[Select] ボタンをクリックします。

選択されたリングが [Create a Named Physical Circuit] ウィンドウに表示されます。

デバイスの挿入

トポロジ内の最後のデバイスの後にデバイスを挿入するには、次のステップを実行します。

ステップ 1　[Create a Named Physical Circuit] ウィンドウで、[Insert Device] ボタンをクリックします。

[Select a Device] ウィンドウが表示されます。

ステップ 2　挿入するデバイスの横にあるチェックボックスをオンにし、[Select] ボタンをクリックします。

デバイスが [Create a Named Physical Circuit] ウィンドウに表示されます。

ステップ 3　[select incoming interface] をクリックします。

選択されたデバイス上のインターフェイスのリストが表示されます。

ステップ 4　選択するインターフェイス横のチェックボックスをオンにし、[Select] をクリックします。

選択されたインターフェイスがインターフェイスのリストに表示されます。

リングの挿入

トポロジ内の最後のデバイスの後にリングを挿入するには、次のステップを実行します。

ステップ 1　[Create a Named Physical Circuit] ウィンドウで、[Insert Ring] ボタンをクリックします。

現在すでに存在するリングのリストが表示されます。

ステップ 2　リングのリストで、挿入するリング横のチェックボックスをオンにし、[Select] をクリックします。

選択したリングが [Create a Named Physical Circuit] ウィンドウに表示されます。

デバイスやリングの削除

デバイスやリングを削除するには、[Create a Named Physical Circuit] ウィンドウでデバイスまたはリングを選択し、[Delete] ボタンをクリックします。

デバイスが削除された状態で [Create NPC] ウィンドウが表示されます。

NPC コンフィギュレーションの保存

選択した 2 つのデバイス間の接続を設定した後、次のステップに従って NPC コンフィギュレーションを保存します。

ステップ 1　[Create a Named Physical Circuit] ウィンドウで、[Save] をクリックします。

NPC プロセスが NPC コンフィギュレーションを検証します。

ステップ 2　[Continue] をクリックして続行します。

NPC ディスカバリが完了になった状態でワークフロー ウィンドウが表示されます。

ステップ 6：MPLS VPN サービス ディスカバリの実行（任意）

デバイス ディスカバリの NPC ディスカバリ フェーズの完了後、ディスカバリ プロセス開始時に [MPLS VPN Discovery] を選択していた場合、NPC ディスカバリ フェーズは完了と表示され、MPLS VPN ディスカバリ ステップが入力待ち（[Pending Input]）と表示されます。

MPLS VPN ディスカバリ ユーザ インターフェイスを使用して、検出された MPLS VPN のコンフィギュレーションを開始する準備ができました。MPLS VPN サービスを設定するには、次のステップを実行します。

（注）　MPLS のサービス ディスカバリは、IOS XR が稼働中のデバイスをサポートしていません。

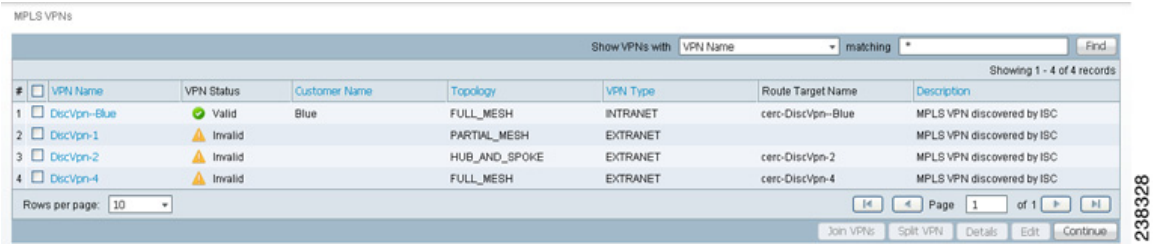
ステップ 1　[Discovery Workflow] ウィンドウで、[Continue] をクリックします。

[MPLS VPNs] ウィンドウが表示され、検出された MPLS VPN がリストされます。検出された MPLS VPN のステータスは、次のように表示されます。

- 検出された MPLS の MPLS VPN トポロジが有効で、Prime Provisioning リポジトリに保存できる状態の場合、[VPN Status] は [Valid] VPN として表示され、ステータス インジケータはグリーンになります。
- 検出された MPLS の MPLS VPN トポロジが無効（トポロジがパーシャル メッシュ）の場合、カスタマー割り当てが行われていない場合、および無効なルート ターゲットが含まれている場合、[VPN Status] は [Invalid] VPN として表示され、ステータス インジケータはイエローになります。パーシャル メッシュ トポロジ VPN は Prime Provisioning ではサポートされていないため、フル メッシュまたはハブ アンド スポークあるいはその両方のコンポーネントに分割する必要があります。

図 E-10 に示す [MPLS VPN] ウィンドウには、無効な MPLS VPN が表示されています（トポロジがパーシャル メッシュで、カスタマー名が空白）。

図 E-10　無効な MPLS VPN が存在する [MPLS VPNs] ウィンドウ



（注）　MPLS VPN ディスカバリ プロセスでパーシャル メッシュ トポロジの MPLS VPN が検出された場合、VPN をサポートされているトポロジ（ハブ アンド スポークやフル メッシュ）の複数の個別 VPN に分割する必要があります。

ステップ 2　次のいずれかを実行します。

- [MPLS VPNs] ウィンドウの表示を変更する場合、別の表示オプションを選択します。

  MPLS VPN の表示オプションについては、「MPLS VPN 表示のフィルタリング」（P.E-49）を参照してください。
- MPLS VPN が有効であり、現時点で MPLS VPN トポロジに変更を加える必要がない場合、[Continue] をクリックして、検出されたトポロジに基づいた MPLS VPN サービスを作成します。
- 検出された MPLS VPN に 1 つ以上無効なものがある場合、次のステップを完了させる必要があります。
  - **VPN の分割**：無効な VPN を選択し、[Split VPN] ボタンをクリックします。

手順については、「VPN の分割」（P.E-49）を参照してください。

– **新規 VPN を作成しルート ターゲットを追加**：分割した VPN 内のデバイスを含む新規 VPN を作成し、それぞれの新規 VPN にルート ターゲットを追加する必要があります。

手順については、「VPN の作成」（P.E-51）を参照してください。

MPLS VPN 表示のフィルタリング

[MPLS VPNs] ウィンドウの表示方法を変更するには、次のステップを実行します。

ステップ 1　[Show VPNs with] フィールド横のメニューをプルダウンします。

VPN のリストを [VPN Name]、[Customer Name]、[Topology]、[VPN Type]、[Description] でフィルタリングできます。

ステップ 2　選択したカテゴリ内に表示される VPN を制限するには、[Matching] フィールドに値を入力します。

[matching] フィールドの値は、表示されるサイトを制御するサーチ マスクを指定します。アスタリスク（*）は、選択された検索条件にあてはまるすべてのサイトを指定します。アスタリスクが後に付いた文字列を指定すると、[Show VPNs with] フィールドで指定された要素で始まるサイトすべてが表示されます。

検索文字列内には、複数のワイルドカード（アスタリスク）値を指定できます。たとえば、カスタマー名の一部に「cisco」が含まれる VPN をすべて表示するには、[matching] フィールドに「*cisco*」と入力します。

選択された条件に合致する VPN が表示されるようになります。

VPN の分割

場合によっては、MPLS VPN ディスカバリ プロセスを完了させて MPLS VPN サービスを実際に作成する前に、既存の MPLS VPN の分割が必要になる場合があります。

たとえば、次のように入力します。

- MPLS サービス ディスカバリ プロセスで無効な MPLS VPN（パーシャル メッシュ トポロジの MPLS VPN）が検出された場合、VPN をサポートされているトポロジ（ハブ アンド スポークやフル メッシュ）の複数のルート ターゲットに分割する必要があります。
- 処理の必要に応じて、MPLS VPN を分割してトポロジを変更することも選択できます。一度に分割できる VPN は 1 つだけです。

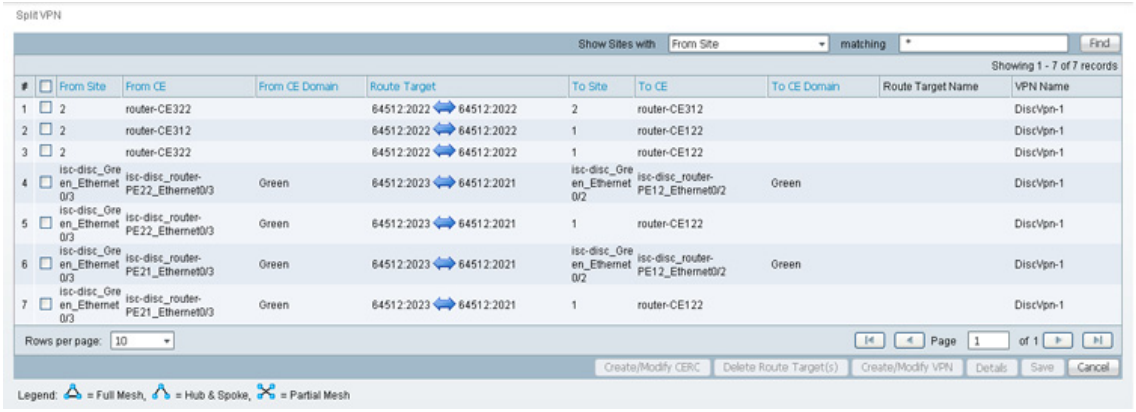
VPN を分割するステップは、次のとおりです。

ステップ 1　[MPLS VPNs] ウィンドウで、分割する VPN の横のチェックボックスをオンにします。

ステップ 2　[Split VPN] ボタンをクリックします。

[Split VPN] ウィンドウが表示されます（図 E-11 を参照）。

図 E-11　[Split VPN] ウィンドウ



ステップ 3　[Split VPN] ウィンドウで、リンクをいくつか選択します。

ハブ アンド スポークまたはフル メッシュ トポロジを構成するリンクを選択します。

たとえば、図 E-11 に示した [Split VPN] ウィンドウでは、最初の 3 つのリンクはすべて **1:102** のルート ターゲットを持ち、フル メッシュ トポロジを形成しています。

残り 2 つのリンクは、**1:106** および **1:105** というルート ターゲットを持っています。これらのリンクは、共同でハブ アンド スポーク トポロジを形成しています。

この VPN を分割するためには、最初の 3 つのリンクが 1 つのルート ターゲットに、残り 2 つのリンクが別のルート ターゲットに関連付けられる必要があります。その後、VPN ごとに 1 つのルート ターゲットの場合の Prime Provisioning ベスト プラクティス表記法に従って、VPN を 2 つの別々の VPN に分割できます。

ステップ 4　[Create/Modify CERC] ボタンをクリックします。

ルート ターゲット名を入力するよう求められます。

ステップ 5　新しいルート ターゲット名を入力して [Save] ボタンをクリックします。

ステップ 6　無効な VPN に含まれる残りのデバイスについても、これらのステップを繰り返します。

たとえば、図 E-11 に示すトポロジでは、ルート ターゲット **1:106 ～ 1:105** を持つデバイスを選択します。

ステップ 7　[Create/Modify CERC] ボタンをクリックします。

ステップ 8　ルート ターゲット名を入力するよう求められたら、新しいルート ターゲット名を入力し、[Save] ボタンをクリックします。

[Split VPNs] ウィンドウが再度表示され、ウィンドウには作成された新しいルート ターゲットが表示されています。

この例では、2 つの新しいルート ターゲットが作成され（**valid_cerc_one** と **valid_cerc_two**）、有効なトポロジであることに注意してください。最初のルート ターゲット **valid_cerc_one** はフル メッシュ トポロジ、2 番めのルート ターゲット **valid_cerc_two** はハブ アンド スポーク トポロジです。

ステップ 9　[Save] ボタンをクリックします。

次のステップに進んで、VPN を作成し VPN にルート ターゲットを追加する準備ができました。

VPN の作成

ルート ターゲットを作成した後、VPN を作成してルート ターゲットを追加する必要があります。

VPN を作成するステップは、次のとおりです。

ステップ 1　[Split VPN] ウィンドウで、[Create/Modify VPN] を選択します。

[Create New VPN] ウィンドウが表示されます。

ステップ 2　VPN に割り当てるルート ターゲットを選択します。

ステップ 3　[VPN Name] フィールドに VPN の名前を入力します。

この例では、**vpn_one** と入力します。

ステップ 4　[Assign VPN Name] ボタンをクリックします。

ステップ 5　[Save] をクリックします。

VPN が作成され、[Split VPN] ウィンドウの [VPN Name] フィールドに表示されます。

ステップ 6　必要に応じて、さらに VPN を作成します。

「VPN の分割」（P.E-49）のサンプル ウィンドウに示すルート ターゲットへと進むには、VPN が作成され、ルート ターゲットが割り当てられている必要があります。次の手順を実行します。

a.　[Split VPN] ウィンドウで、[Create/Modify VPN] をクリックします。

b.　[Create VPN] ウィンドウで、別の VPN を作成し、ルート ターゲットを割り当てます。

例の画面では、2 番めのルート ターゲット（**valid_cerc_two**）を新規作成された VPN に選択します。

ステップ 7　VPN の作成が完了したら、[Split VPN] ウィンドウの [Save] ボタンをクリックします。

[MPLS VPNs] ウィンドウが表示されます。

（注）　例では、VPN のうち 1 つが [Valid] と表示され、ステータス インジケータがグリーンになっています。しかし、ウィンドウ内のその他の VPN は [Invalid] と表示され、インジケータはイエローです。

このような状況が発生する場合があるのは、MPLS ディスカバリ プロセスがデータを完全には検証できないからです。このような状況でも、サービス ディスカバリ プロセスを継続し、MPLS VPN サービスを作成できます。ただし、プロセスでは無効な VPN がスキップされるため、Prime Provisioning プロビジョニング コマンドを使用して VPN サービスを手動設定する必要があります。

ステップ 8　カスタマーを各 VPN に割り当てるには、次のステップを実行します。

a.　[MPLS VPNs] ウィンドウの VPN エントリを選択し、[Edit] ボタンをクリックします。

[Edit VPN] ウィンドウが表示されます。

b.　[Customer Name] フィールドの横にある [Select] ボタンをクリックします。

カスタマー名のリストが表示されます。

c.　カスタマー名の横にあるオプション ボタンをクリックし、[Select] をクリックします。

d.　ルート ターゲットの名前を変更するには、[Rename] をクリックして変更します。

e.　[Save] をクリックします。

[MPLS VPNs] ウィンドウにカスタマー名が表示されます。

（注） 場合によっては、有効に思える VPN が無効と表示されることがあります。そのような VPN の処理はスキップされます。この場合、Prime Provisioning プロビジョニング コマンドを使用して手動で設定する必要があります。

ステップ 9 VPN の編集完了後、[Continue] ボタンをクリックして MPLS VPN サービス作成プロセスを開始します。

VPN リンクの詳細の表示

検出された VPN の詳細を表示するには、次のステップを実行します。

ステップ 1 [MPLS VPNs] ウィンドウから詳細事項を表示させる VPN を選択し、[Details] ボタンをクリックします。

[MPLS VPN Links] ウィンドウが表示されます。

ステップ 2 表示される MPLS VPN リンクをフィルタリングするには、[Show Sites with] フィールドのプルダウンリストから値を選択します。

VPN のリストを [From Site]、[From CE]、[From CE Domain]、[Route Target]、[To Site]、[To CE]、[To CE Domain] でフィルタリングできます。

[matching] フィールドの値は、表示されるサイトを制御するサーチ マスクを指定します。アスタリスク（*）は、選択された検索条件にあてはまるすべてのサイトを指定します。アスタリスクが後に付いた文字列を指定すると、[Show Sites with] フィールドで指定された要素で始まるサイトすべてが表示されます。

検索文字列内には、複数のワイルドカード（アスタリスク）値を指定できます。たとえば、[From CE] 名に「realtime」が含まれるサイトすべてを表示するには、[Show Sites with] フィールドで [From CE Name] を選択してから、[matching] フィールドに「*realtime*」と入力します。

指定したリンクだけが表示された状態に変わります。

MPLS VPN の保存と MPLS VPN サービスの作成開始

検出された MPLS VPN の [MPLS VPNs] ウィンドウでのデータ編集が完了した後、[Continue] ボタンをクリックします。

ディスカバリ プロセスが VPN サービスを作成します。プロセスが完了すると、[Discovery Workflow] ウィンドウには MPLS VPN ディスカバリ プロセスが完了（[COMPLETE]）したことが表示され、ステータス インジケータはグリーンになります。

ディスカバリ プロセス開始前に [Discovery] ウィンドウで [L2VPN (Metro Ethernet) Discovery] も選択していた場合、キャリア イーサネット サービス ディスカバリに進めるようになります。

ステップ 7 : L2VPN（メトロ イーサネット）サービス ディスカバリの実行（任意）

ディスカバリ プロセス開始前に [Discovery] ウィンドウで [L2VPN (Metro Ethernet) Discovery] を選択していた場合、前のステップが完了すると、[Discovery Workflow] ウィンドウに [L2VPN (Metro Ethernet) Discovery] が [Pending Input] と表示されます。

メトロ イーサネット サービス 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。

（注） L2VPN サービス ディスカバリは、IOS XR 稼働中のデバイスをサポートしておらず、EVC CLI フレームワークを使用して定義されたサービスを検出しません。

ステップ 1　メトロ イーサネット サービス ディスカバリを開始する前に、次のステップを実行します。

a. [Service Inventory] > [Inventory and Connection Manager] と選択します。

b. [Inventory and Connection Manager] ウィンドウ左にあるタスク ペインで、[Access Domains] を選択します。

c. メトロ イーサネット トポロジ内の N-PE デバイスのいずれかに、アクセス ドメインを作成します。

詳細については、第 2 章「Prime Provisioning を設定する前に」「アクセス ドメインの作成」（P.2-43）の項を参照してください。

d. [Service Inventory] > [Inventory and Connection Manager] と選択します。

e. [Inventory and Connection Manager] ウィンドウ左にあるタスク ペインで、[Resource Pools] を選択します。

f. 作成したアクセス ドメインのそれぞれにリソース プールを作成します。

詳細については、第 2 章「Prime Provisioning を設定する前に」「リソース プール」（P.2-46）の項を参照してください。

g. [Service Inventory] > [Discovery] と選択します。

[Discovery Workflow] ウィンドウに、[L2VPN (Metro Ethernet) Discovery] プロセスが [Pending Input] と表示されます。

ステップ 2　[Continue] をクリックします。

[L2VPN Discovery (Ethernet Services)] ウィンドウが表示されます。

ステップ 3　次のいずれかのアクションを選択します。

- [View/Edit Discovered Layer 2 Services grouped by VPN]: 検出された L2VPN サービスを表示し、必要に応じて編集できます。
- [View/Edit Discovered Layer 2 End to End Wires]: 検出されたレイヤ 2 エンドツーエンド回線を表示し、必要に応じて編集できます。
- [View/Edit Discovered Layer 2 VPLS Links] : 検出されたレイヤ 2 Virtual Private LAN Service（VPLS; 仮想プライベート LAN サービス）リンクを表示し、必要に応じて編集できます。

この章の次の項で、各アクションについて説明します。

VPN によるグループ化表示された検出済みレイヤ 2 サービスの表示

検出されたレイヤ 2 サービスを VPN によってグループ化して表示するには、次のステップを実行します。

ステップ 1　[L2VPN Discovery (Ethernet Services)] ウィンドウで、[VPNs] ボタンをクリックします。

[L2VPNs] ウィンドウが表示されます。

[L2VPNs] ウィンドウでは、次のタスクが実行できます。

- レイヤ 2 VPN についての詳細情報を表示する。

  このタスクは、このステップの次のステップで説明します。

- 既存の Layer 2 VPN の設定情報編集ウィンドウを表示する。

  詳細な手順については、「VPN によるグループ化表示された検出済みレイヤ 2 サービスの編集」（P.E-54）を参照してください。

- 既存のレイヤ 2 VPN を削除する。

  このタスクについては、「VPN によるグループ化表示された検出済みレイヤ 2 サービスの削除」（P.E-55）を参照してください。

ステップ 2　レイヤ 2 サービスについての詳細情報を参照するには、詳細を表示させる VPN の横にあるチェックボックスをオンにしてから、[Details] ボタンをクリックします。

[L2VPN Details] ウィンドウが表示されます。

[L2VPN Details] ウィンドウには、User-Network Interface（UNI; ユーザネットワーク インターフェイス）など、検出された VPN の詳細が表形式で表示されます。

ステップ 3　リンク詳細の参照後、[Close] ボタンをクリックします。

VPN によるグループ化表示された検出済みレイヤ 2 サービスの編集

検出されたレイヤ 2 VPN サービスを編集して、サービスに適用されるポリシーを変更できます。レイヤ 2 VPN サービスを編集するには、次のステップを実行します。

ステップ 1　[L2VPNs] ウィンドウで、編集する VPN の横にあるチェックボックスをオンにし、[Edit] ボタンをクリックします。

[Edit VPN] ウィンドウが表示されます。

ステップ 2　VPN 名を編集するには、新しい VPN 名を [VPN Name] フィールドに入力します。

ステップ 3　カスタマー名を編集するステップは、次のとおりです。

a.　カスタマー名の横にある [Select] ボタンをクリックします。

カスタマーのリストが表示されます。

b.　設定する新しいカスタマー名の横にあるオプション ボタンをクリックします。

c.　[Save] ボタンをクリックします。

[Metro Ethernet End to End Wires] ウィンドウに、新しい VPN 名またはカスタマー名あるいはその両方が表示されます。

VPN によるグループ化表示された検出済みレイヤ 2 サービスの削除

レイヤ 2 サービスを削除するには、次のステップを実行します。

ステップ 1　[L2VPNs] ウィンドウで、削除する VPN の横にあるチェックボックスをオンにし、[Delete] ボタンをクリックします。

次のメッセージが表示されます。

```
Links/End to End wires associated with all selected VPNs will be deleted as a result of
this operation. Do you really want to Delete?
```

ステップ 2　VPN を削除してよいことを確認し、[OK] をクリックします。削除しない場合、[Cancel] をクリックします。

[OK] をクリックした場合、VPN および関連付けられたリンクとエンドツーエンド回線が削除されます。

検出済みレイヤ 2 VPN サービスを使用するポリシーの編集

検出されたレイヤ 2 VPN サービスを編集して、サービスに適用されるポリシーを変更できます。レイヤ 2 VPN サービスを編集するには、次のステップを実行します。

ステップ 1　[L2VPNs Details] ウィンドウで、VPN に関連付けられた UNI の横にあるチェックボックスをオンにし、[Edit] ボタンをクリックします。

[Edit Link Policy] ウィンドウが表示されます。

ステップ 2　サービスのリンク ポリシーを変更するには、次のステップを実行します。

a.　[Policy Name] フィールドの横にある [Policy] ボタンをクリックします。

ポリシーのリストが表示されます。

[Show VPN policies with] フィールドのプルダウン リストからフィルタを選択したり、[Matching] フィールドにサーチ マスクを入力したりして、ポリシー リストを変更できます。

ポリシー リストを [Policy Name]、[Customer Name]、[Provider Name]、[Global policy name] でフィルタリングできます。[Matching] フィールドに値を入力して、選択したカテゴリのうち表示されるポリシーのリストを制限することも可能です。

ステップ 3　サービスを適用するポリシーの横にあるオプション ボタンをクリックし、[Select] をクリックします。

ステップ 4　次のいずれかを実行します。

- [Save] をクリックして変更を保存します。
- [Cancel] をクリックすると、変更がキャンセルされます。

検出されたレイヤ 2 エンドツーエンド回線の表示

検出されたレイヤ 2 エンドツーエンド回線を表示するには、次のステップを実行します。

ステップ 1　[L2VPN Discovery (Ethernet Services)] ウィンドウで、[End-End Wires] ボタンをクリックします。

[Metro Ethernet End to End Wires] ウィンドウが表示されます。

[Metro Ethernet End to End Wires] ウィンドウでは、次のタスクを実行できます。

- メトロ イーサネット エンドツーエンド回線の詳細情報を表示する。

  このタスクは、このステップの次のステップで説明します。

- エンドツーエンド回線に関連付けられた VPN を編集する。

  このタスクについては、「エンドツーエンド回線に関連付けられた VPN の編集」（P.E-56）を参照してください。

- 既存のエンドツーエンド回線を 2 本のエンドツーエンド回線に分割する。

  このタスクについては、「レイヤ 2 サービス エンドツーエンド回線の分割」（P.E-57）を参照してください。

- 複数の既存エンドツーエンド回線を 1 本のエンドツーエンド回線に統合する。

  このタスクについては、「レイヤ 2 サービス エンドツーエンド回線の統合」（P.E-57）を参照してください。

- 既存のエンドツーエンド回線を削除する。

  このタスクについては、「検出されたレイヤ 2 エンドツーエンド回線の表示」（P.E-55）を参照してください。

ステップ 2　レイヤ 2 サービスについての詳細情報を参照するには、詳細を表示させる UNI の横にあるチェックボックスをオンにしてから、[Details] ボタンをクリックします。

ステップ 3　リンク詳細の参照後、[Close] ボタンをクリックします。

ステップ 4　エンドツーエンド回線内のインターフェイスの詳細を表示する場合、[AC1 UNI] または [AC2 UNI] フィールドのいずれかのインターフェイス名をクリックします。

インターフェイス名をクリックすると、[Interface Detail] ウィンドウが表示されます。[Interface Detail] ウィンドウは、選択されたインターフェイスについて、インターフェイスが位置するホストのホスト名やインターフェイスで使用されるカプセル化のタイプ、インターフェイスで使用されるスイッチ モードといった詳細情報を表示します。

ステップ 5　インターフェイスの詳細の参照後、[Close] ボタンをクリックします。

エンドツーエンド回線に関連付けられた VPN の編集

[Metro Ethernet End to End Wires] ウィンドウから、エンドツーエンド回線に関連付けられた VPN を編集することも可能です。

エンドツーエンド回線に関連付けられた VPN を編集するには、次のステップを実行します。

ステップ 1　[Metro Ethernet End to End Wires] ウィンドウで、[VPN name] フィールドに表示された VPN 名をクリックします。

[Edit VPN] ウィンドウが表示されます。

ステップ 2　VPN 名を編集するには、新しい VPN 名を [VPN Name] フィールドに入力します。

ステップ 3　カスタマー名を編集するステップは、次のとおりです。

a.　カスタマー名の横にある [Select] ボタンをクリックします。

カスタマーのリストが表示されます。

b. 設定する新しいカスタマー名の横にあるオプション ボタンをクリックします。

c. [Save] ボタンをクリックします。

[Metro Ethernet End to End Wires] ウィンドウに、新しい VPN 名またはカスタマー名あるいはその両方が表示されます。

レイヤ 2 サービス エンドツーエンド回線の分割

既存のエンドツーエンド回線を、関連付けられた VPN から切り離し、新しい VPN に関連付けることが可能です。

エンドツーエンド回線を既存の VPN から分離するには、次のステップを実行します。

ステップ 1　[Metro Ethernet End to End Wires] ウィンドウで、VPN から分離させるエンドツーエンド回線エントリの横にあるチェックボックスをオンにします。

（注） エンドツーエンド回線に関連付けられた VPN の ID が 1 つだけである場合、回線上で分離アクションを実行できません。

ステップ 2　[Split] ボタンをクリックします。

続行確認メッセージが表示されます。

ステップ 3　プロセスを続行する場合、[OK] をクリックします。

エンドツーエンド回線は分割され、2 つの新しい VPN と関連付けられます。これらの VPN の名前は、既存の VPN 名の後ろに新しい番号を付加する方法で作成されます。

レイヤ 2 サービス エンドツーエンド回線の統合

2 本の既存エンドツーエンド回線を単一の VPN に統合できます。

2 本の既存エンドツーエンド回線を統合するには、次のステップを実行します。

ステップ 1　[Metro Ethernet End to End Wires] ウィンドウで、統合する複数のエンドツーエンド回線エントリの横にあるチェックボックスをオンにします。

続行確認メッセージが表示されます。

ステップ 2　プロセスを続行する場合、[OK] をクリックします。

選択されたエンドツーエンド回線が新しい VPN に統合されます。この VPN の名前は、最も大きな番号が付いた既存の VPN 名に新しい番号を付加する方法で作成されます。

レイヤ 2 サービス エンドツーエンド回線の削除

既存のエンドツーエンド回線を削除するには、次のステップを実行します。

ステップ 1　[Metro Ethernet End to End Wires] ウィンドウで、削除する 1 本以上のエンドツーエンド回線エントリの横にあるチェックボックスをオンにします。

続行確認メッセージが表示されます。

ステップ 2　プロセスを続行する場合、[OK] をクリックします。

選択したエンドツーエンド回線が削除されます。回線に関連付けられた接続回線もすべて削除されます。

ステップ 3　[Close] をクリックして [Metro Ethernet End to End Wires] ウィンドウを閉じます。

検出されたレイヤ 2 VPLS リンクの表示

検出されたレイヤ 2 VPLS リンクを表示するには、次のステップを実行します。

ステップ 1　[L2VPN Discovery (Ethernet Services)] ウィンドウで、[VPLS Links] ボタンをクリックします。

[VPLS Links] ウィンドウが表示されます。

[VPLS Links] ウィンドウでは、次のタスクが実行できます。

- VPLS リンクの詳細情報を表示する。

  このタスクは、このステップの次のステップで説明します。

- 既存の VPLS リンクの設定情報編集ウィンドウを表示する。

  詳細な手順については、「検出されたレイヤ 2 VPLS リンクの編集」（P.E-58）を参照してください。

- 既存のレイヤ 2 VPN を削除する。

  このタスクについては、「検出されたレイヤ 2 VPLS リンクの削除」（P.E-59）を参照してください。

ステップ 2　VPLS リンクについての詳細情報を参照するには、詳細を表示させる VPLS link の横にあるチェックボックスをオンにしてから、[Details] ボタンをクリックします。

[VPLS Link Detail] ウィンドウが表示されます。

[VPLS Link Detail] ウィンドウには、検出された VPN とそのリンク プロパティが表示されます。

ステップ 3　リンク詳細の参照後、[Close] ボタンをクリックします。

検出されたレイヤ 2 VPLS リンクの編集

検出されたレイヤ 2 VPLS リンクを編集して、サービスに適用されるポリシーを変更できます。レイヤ 2 VPLS リンクを編集するには、次のステップを実行します。

ステップ 1　[VPLS Links] ウィンドウで、編集する VPLS リンクの横にあるチェックボックスをオンにし、[Edit] ボタンをクリックします。

[Edit Link Policy] ウィンドウが表示されます。

ステップ 2　リンクのリンク ポリシーを変更するには、次のステップを実行します。

a. [Policy Name] フィールドの横にある [Policy] ボタンをクリックします。

ポリシーのリストが表示されます。

[Show VPN policies with] フィールドのプルダウン リストからフィルタを選択したり、[Matching] フィールドにサーチ マスクを入力したりして、ポリシー リストを変更できます。

ポリシー リストを [Policy Name]、[Customer Name]、[Provider Name]、[Global policy name] でフィルタリングできます。[Matching] フィールドに値を入力して、選択したカテゴリのうち表示されるポリシーのリストを制限することも可能です。

ステップ 3　サービスを適用するポリシーの横にあるオプション ボタンをクリックし、[Select] をクリックします。

ステップ 4　次のいずれかを実行します。

- [Save] をクリックして変更を保存します。
- [Cancel] をクリックすると、変更がキャンセルされます。

検出されたレイヤ 2 VPLS リンクの削除

VPLS リンクを削除するステップは、次のとおりです。

ステップ 1　[VPLS Links] ウィンドウで、削除する VPLS リンクの横にあるチェックボックスをオンにし、[Delete] ボタンをクリックします。

次のメッセージが表示されます。

```
The selected link(s) will be deleted. Do you really want to Delete?
```

ステップ 2　VPLS を削除してよいことを確認し、[OK] をクリックします。削除しない場合、[Cancel] をクリックします。

[OK] をクリックすると、VPLS リンクが削除されます。

ステップ 3　[Close] をクリックして、[VPLS links] ウィンドウを閉じます。

L2VPN メトロ イーサネット ポリシーの保存とサービスの作成開始

検出された L2VPN メトロ イーサネット トポロジの参照や編集が終了した後、[Close] ボタンをクリックして [L2VPN Discovery (Ethernet Services)] ウィンドウに戻ります。

[Continue] ボタンをクリックして、L2VPN サービス ディスカバリ プロセスを開始します。

[Discovery Workflow] ウィンドウが表示され、L2VPN サービス ディスカバリ プロセスが進行中（[In Progress]）であることを示します。ステータス インジケータはイエローです。

L2VPN サービス ディスカバリ プロセスが完了すると、ステータス インジケータはグリーンに変わり、[Discovery Workflow] ウィンドウは L2VPN サービス ディスカバリ プロセスが完了した（[Complete]）ことを示します。

ステップ 8：検出されたデバイスとサービスの Prime Provisioning リポジトリへのコミット

[Continue] ボタンをクリックして、検出されたデバイスとサービスを Prime Provisioning リポジトリにコミットします。このステップの前に、検出ワークフローは検出されたデバイスとサービスを、検出ワークフローの最後のステップでだけ Prime Provisioning にコミットされる一時リポジトリに格納します。

ステップ 9：検出されたデバイスへのコンフィギュレーション収集タスクの作成と実行

サービスの表示と編集の前に、次のステップに従ってデバイスのコンフィギュレーション作成タスクを実行します。

（注）　コンフィギュレーション作成タスクについて詳しくは、「タスク」（P.10-25）の第 10 章「モニタリング」の項を参照してください。

ステップ 1　[Prime Provisioning Start] ページで、[Monitoring] を選択します。

[Monitoring] ウィンドウが表示されます。

ステップ 2　[Task Manager] を選択します。

[Tasks] ウィンドウが表示されます。

ステップ 3　[Create] ボタンをクリックし、プルダウン リストから [Collect Config] を選択します。

[Create Task] ウィンドウが表示されます。

ステップ 4　[Next] ボタンをクリックします。

[Collect Config Task] ウィンドウが表示されます。

ステップ 5　[Collect Config Task] ウィンドウで、次のステップに従ってコンフィギュレーション収集タスクを作成し、実行します。

a. [Select/Deselect] ボタンをクリックします。

ディスカバリ プロセスで検出されたデバイスをリストしたダイアログ ウィンドウが表示されます。

b. リストに表示されたデバイスをすべて選択します。

c. [Select] ボタンをクリックします。

再度 [Collect Config Task] ウィンドウが表示されます。

d. 必要に応じてコンフィギュレーション収集タスクの詳細設定を指定します。

e. [Submit] ボタンをクリックします。

次の項（「ステップ 10：サービスの表示と編集」（P.E-61））で説明する、サービスの表示と編集の準備ができました。

ステップ 10：サービスの表示と編集

MPLS VPN または L2VPN メトロ イーサネット サービスあるいはその両方の作成プロセスが成功すると、作成されたサービスを表示させ、サービス要求エディタを使用して変更できます。

L2VPN サービスを表示するには、次のステップを実行します。

ステップ 1　[Service Inventory] ウィンドウが現在アクティブになっていない場合、[Operate] > [Service Request] > [Service Request Manager] とクリックします。

[Service Request Manager] ウィンドウが表示されます。

必要に応じて、[Service Requests] ウィンドウに表示されているサービス要求を変更できます。

（注）　このプロセスの一部として MPLS VPN を編集する必要がある場合、「VPN の分割」（P.E-49）、「VPN の作成」（P.E-51）、「VPN リンクの詳細の表示」（P.E-52）、および「MPLS VPN の保存と MPLS VPN サービスの作成開始」（P.E-52）を参照してください。

ステップ 2　L2VPN メトロ イーサネット ネットワークのためのサービス要求変更について詳しくは、*『Cisco Prime Provisioning 6.3 User Guide』* を参照してください。

ステップ 3　このリリースについての一般的な情報については、リリース付属の *『Cisco Prime Provisioning 6.3 Release Notes』* を参照してください。