



回線/VC のプロビジョニング

- での回線/VC のプロビジョニング [Cisco EPN Manager](#) (1 ページ)
- キャリア イーサネット ネットワークの EVC のプロビジョニング (11 ページ)
- セグメント ルーティング (30 ページ)
- 光/DWDM ネットワークの回線のプロビジョニング (37 ページ)
- L3VPN サービスのプロビジョニング (69 ページ)
- 回線エミュレーション サービスのプロビジョニング (96 ページ)
- MPLS トラフィック エンジニアリング サービスのプロビジョニング (108 ページ)
- 回線/VC プロファイル (134 ページ)
- QoS プロファイルの作成 (135 ページ)
- 顧客の作成 (137 ページ)
- アンマネージド エンドポイントを使用した回線/VC のプロビジョニング (137 ページ)
- テンプレートを使用した回線/VC の拡張 (138 ページ)
- 設定例：CLI テンプレートを使用した回線/VC の拡張 (139 ページ)
- 設定例：ロールバック テンプレート (144 ページ)
- 設定例：インタラクティブ テンプレート (146 ページ)
- プロビジョニング障害の syslog (147 ページ)

での回線/VC のプロビジョニング **Cisco EPN Manager**

回線/VCの作成とプロビジョニングのプロセスは、サポートされているすべてのテクノロジーで類似しており、次の手順が含まれています。

- 回線/VC のエンドポイントの指定。
- 回線/VC の設定パラメータの定義。

Cisco EPN Manager でのプロビジョニング サポートの詳細な概要については、[回線/VC のプロビジョニング \(1 ページ\)](#) 参照してください。

新しい回線/VC を作成してプロビジョニングするには、次の手順を実行します。

- ステップ 1** 左側のサイドバーから、[マップ (Maps)] > [トポロジ マップ (Topology Maps)] > [ネットワーク トポロジ (Network Topology)] を選択します。
- ステップ 2** [デバイスグループ (Device Groups)] ボタンをクリックし、必要なデバイスグループを選択して、[ロード (Load)] をクリックします。
- ステップ 3** [デバイス グループ (Device Groups)] ポップアップ ウィンドウを閉じます。
- ステップ 4** [ネットワーク トポロジ (Network Topology)] ウィンドウで [回線/VC (Circuits/VCs)] タブをクリックします。
- ステップ 5** [+] アイコンをクリックします。マップ右側の新しいペインにプロビジョニングウィザードが表示されません。
- (注) または、[設定 (Configuration)] > [ネットワーク (Network)] > [サービス プロビジョニング (Service Provisioning)] を選択してプロビジョニング ウィザードを表示します。
- ステップ 6** [テクノロジー (Technology)] ドロップダウンリストから必要なテクノロジーを選択します。たとえば、光/DWDM ネットワークの回線を作成する場合は、[光 (Optical)] を選択します。
- ステップ 7** [サービスタイプ (Service Type)] 領域で、作成する回線/VCのタイプを選択します。たとえば、光/DWDM ネットワーク用の回線/VC を作成する場合は、OCHNC WSON、OCHCC WSON、OCH-Trail WSON、OCH-Trail UNI、ODU UNI、ODU トンネル、OPU over ODU など、さまざまな回線タイプがあります。
- ステップ 8** さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、[プロファイルの選択 (Select Profile)] ドロップダウンリストから必要なプロファイルを選択します。回線/VC プロファイル (134 ページ) を参照してください。
- ステップ 9** [次へ (Next)] をクリックして [カスタマー サービスの詳細情報 (Customer Service Details)] ページに移動します。
- ステップ 10** (オプション) 回線/VC の作成対象顧客を選択します。リストに顧客が表示されない場合は、[インベントリ (Inventory)] > [その他 (Other)] > [顧客 (Customers)] に移動し、プロビジョニングウィザードに移動して回線/VC のプロビジョニングを開始します。
- ステップ 11** サービス名と説明を入力します。
- ステップ 12** [展開アクション (Deployment Action)] ドロップダウンリストから、回線/VCの属性を定義した後に実行するアクションを選択します。次のオプションがあります。
- [プレビュー (Preview)] : 各デバイスで生成された CLI を表示します。CLI を確認して、属性を編集するか、展開を進めるかを決定できます。
 - [展開 (Deploy)] : プロビジョニング ウィザードの最後のページで [送信 (Submit)] をクリックした直後に関連するデバイスに設定を展開します。
- 次のいずれかの展開オプションをクリックします。
- [今すぐ展開 (Deploy Now)] : プロビジョニング順序を直接展開します。
 - [後で展開 (Deploy Later)] : 作成されたプロビジョニング順序を保存します。同じ順序は、後で展開できます。プロビジョニング順序を再展開するには、左側のペインの下部にある回線/VC のリンクをクリックします。

- [展開のスケジュール (Schedule Deployment)] : 指定した時間に、今後の展開の順序を保存します。プロビジョニング順序をスケジュールし、スケジュールした時刻に展開するジョブの順序を作成します。必要に応じて、[ジョブ スケジューラ (Job Scheduler)] ダイアログボックスで順序をプロビジョニングする日付と時刻を指定できます。

この [展開のスケジュール (Schedule Deployment)] オプション ボタンをクリックした場合は、次を指定します。

- [スケジュール時刻の展開 (Deploy Schedule Time)] : プロビジョニング順序の展開のスケジュール時刻を指定します。
- [サーバ時刻 (Server Time)] : 現在のサーバ時刻を表示します。

プロビジョニング順序をスケジュールし、保存する方法の詳細については、次を参照してください。
[プロビジョニング順序の保存とスケジュール \(105 ページ\)](#)

- ステップ 13** [次へ (Next)] をクリックしてエンドポイントを選択し、選択したテクノロジーに基づいて属性を定義します。
- ステップ 14** [送信 (Submit)] をクリックします。選択した展開アクションに応じて、関連するアクションが実行されます。つまり、設定のプレビューを選択した場合は、設定を表示できるプレビューページが表示され、その後に [展開 (Deploy)] をクリックします。展開を選択した場合、設定は関連するデバイスに直接展開されます。
- ステップ 15** (オプション) [このビューのままにする (Leave this View)] ボタンをクリックして Cisco EPN Manager を引き続き使用し、サービスの展開をバックグラウンドで続行できるようにします。

(注) デバイスがビジー状態の場合、サービスを展開する Cisco EPN Manager からの要求は、その要求がタイムアウトする事前に設定された時間まで待機します。この設定を変更するには、[サービス展開のタイムアウト値の設定 \(4 ページ\)](#) を参照してください。

回線/VC が、[ネットワーク トポロジ (Network Topology)] ウィンドウの [回線/VC (Circuits/VCs)] ペインのリストに追加されているはずですが、プロビジョニング状態を確認するには、回線/VC 名の横にある [i] アイコンをクリックし、[回線/VC 360 (Circuit/VC 360)] ビューを表示します。

さまざまなテクノロジーに対して回線/VCを作成し、プロビジョニングする方法については、次を参照してください。

- [キャリア イーサネット ネットワークの EVC のプロビジョニング \(11 ページ\)](#)
- [光/DWDM ネットワークの回線のプロビジョニング \(37 ページ\)](#)
- [L3VPN サービスのプロビジョニング \(69 ページ\)](#)
- [回線エミュレーション サービスのプロビジョニング \(96 ページ\)](#)
- [MPLS トラフィック エンジニアリング サービスのプロビジョニング \(108 ページ\)](#)

保存されたプロビジョニング順序は、[管理 (Administration)] > [ダッシュボード (Dashboards)] > [ジョブ ダッシュボード (Job Dashboard)] > [プロビジョニング (Provisioning)] から [計画済み回線/VC (Planned Circuits/VCs)] タブに表示できます。

[最後の実行の統計 (Last run stat)] フィールドの [I] アイコンをクリックし、設定とデバイスの詳細を表示します。

サービス展開のタイムアウト値の設定

デバイスにサービスを展開すると、デバイスが事前に占有されているか、またはビジー状態の場合は、作成されたサービス要求は事前に設定された時間まで待機して、サービスを展開するための「デバイスロック」を取得します。デフォルトでは、タイムアウト値は60分に設定されます。

デフォルトのタイムアウト値を変更するには、次の手順を実行します。

ステップ 1 左側のサイドバーから **Administration > Settings > System Settings** を選択します。

ステップ 2 [回線/VC (Circuits/VCs)] セクションを展開し、[展開設定 (Deployment Settings)] をクリックします。

ステップ 3 必要なタイムアウト値を分単位で設定します。

Cisco EPN Manager は、サービスを展開するためのデバイスロックを取得するために指定された時間まで待機します。この時間以内にロックが取得されなかった場合、サービス展開操作は失敗します。

回線アクティベーション待機タイムアウト値の設定

回線アクティベーション待機タイムアウトまでプロビジョニングシステムが待機する最大時間間隔を設定できます。

ステップ 1 左側のサイドバーから **Administration > Settings > System Settings** を選択します。

ステップ 2 [回線/VC (Circuits/VCs)] セクションを展開し、[展開設定 (Deployment Settings)] をクリックします。

ステップ 3 [回線アクティベーション待機タイムアウト (Circuit Activation Wait Timeout)] フィールドで、必要なタイムアウト値を分単位で設定します。

デフォルトのタイムアウト値は5分です。

展開が失敗した場合の動作

回線/VC を展開すると、Cisco EPN Manager は回線/VC のタイプに基づいて、参加しているデバイスでの設定変更を実行します。設定変更がデバイスに正常に展開された場合にのみ、回線/VC は正常にプロビジョニングされたと見なされます。参加しているデバイスのいずれかで設定変更の展開が失敗した場合は、Cisco EPN Manager がこれまでにデバイスで行われたすべての設定変更をロールバックします。

参加しているデバイスのいずれかで設定変更の展開が失敗した場合は、プロビジョニングウィザードで[再展開 (Redeploy)]をクリックできます。再展開アクションは、同じ設定で展開を再試行します。



(注) [再展開 (Redeploy)] ボタンは、OCHNC WSON、OCHCC WSON、OCHCC、OCH-Trail WSON、OCH-Trail、Media Channel NC SSON、Media Channel Trail SSON、Media Channel CC SSON 光回線でサポートされています。

展開アクションでは、次のシナリオのいずれかが発生する可能性があります。

- 参加しているすべてのデバイスで展開が成功し、ロールバックは開始されない：このシナリオでは、すべてのデバイスが正常に設定され、回線のプロビジョニングが成功します。
- 展開が失敗して、ロールバックが開始され、成功する：このシナリオでは、複数のデバイスを設定したときに、デバイスのいずれかで設定が失敗します。障害は、たとえば、デバイスが設定を拒否したなど、さまざまな理由が原因となる可能性があります。Cisco EPN Manager は障害を識別し、すべてのデバイスで行われたすべての設定変更を正常にロールバックします。このシナリオでは、すべてのデバイス設定が展開前の状態に復元されます。

順番に回線をプロビジョニングするように設定された3つのデバイス (A、B、およびC) を使用した例を以下に示します。デバイス A では設定変更が正常に展開されますが、デバイス B では展開が失敗します。Cisco EPN Manager は、失敗を検出して、デバイス B および C の以降の設定を中止します。また、プロビジョニングの逆順で設定をロールバックします。つまり、最初にデバイス B をロールバックしてからデバイス A をロールバックします。3つのデバイスで順に実行されるアクションを以下に示します。

- デバイス C：まだ変更がデバイスに展開されていないため、デバイス C に対するロールバックは必要ありません。これは、設定変更がデバイス C に送信される前に、デバイス B で設定の失敗が検出されたことを意味します。
 - デバイス B：Cisco EPN Manager は、展開が失敗する前にこのデバイスで行われた設定変更があるかどうかをチェックします。変更がある場合は、このデバイスの部分的な設定が削除され、デバイスが以前の設定にロールバックされます。
 - デバイス A：Cisco EPN Manager は、デバイス A で完全なロールバックを実行します。正常に展開されたすべての設定変更が削除され、デバイスは以前の設定にロールバックされます。
- 展開が失敗して、ロールバックが開始されたが、失敗した：このシナリオでは、参加しているデバイスのいずれかで設定の展開が失敗すると、Cisco EPN Manager がロールバックを実行しますが、1つ以上のデバイス上のロールバックが失敗します。この場合、ロールバックが失敗したデバイスには部分的な設定が残ります。

たとえば、デバイス A および B で設定変更が正常に展開され、デバイス C で展開が失敗した場合です。Cisco EPN Manager は、失敗を特定して、プロビジョニングの逆順でロー

ロールバックを開始します。つまり、デバイス C、デバイス B、デバイス A の順にロールバックします。3 つのデバイスで順に実行されるアクションを以下に示します。

- デバイス C : Cisco EPN Manager はデバイス C で正常にロールバックを実行します。
- デバイス B : デバイス B でロールバックを試みると、デバイス接続が失われ、デバイス上に部分的な設定が残される可能性があります。
- デバイス A : Cisco EPN Manager は、デバイス B でロールバックが失敗しても、デバイス A のロールバックを実行します。



(注) ロールバックは、他のさまざまな理由で失敗することがあります。

プロビジョニングウィザードで、設定をプレビューしてから、[展開 (Deploy)] をクリックします。展開が失敗すると、参加している各デバイスのロールバック設定とステータスが表示されます。[デバイス (Device(s))] ドロップダウンリストで、ロールバック設定とステータスを表示するデバイスを選択します。

次の図に、各デバイスのロールバック設定とロールバック ステータスを示します。

Deploy: Failure

Service Name: EVPL_withQOS

Service Type: EVPL

Device(s): NCS4206-120.81

Attempted Configuration

```

ethernet cfm domain EVC level 4
service number 41 evc EVPL_withQOS
continuity-check
continuity-check interval 1s
ethernet evc EVPL_withQOS
oam protocol cfm domain EVC
class-map match-all test_1
match cos 3
policy-map pol_123
class test_1
police cir 900m
conform-action transmit
exceed-action drop
interface pseudowire177
encapsulation mpls
control-word include
neighbor 192.168.0.145 159
mtu 1508
interface GigabitEthernet0/0/7
no ethernet lmi interface
ethernet uni id Testuni23
service instance 5 ethernet EVPL_withQOS
    
```

Status

```

Command returned an error : customizedError
config
Enter configuration commands, one per line. End with CNTL/Z.
NCS4206-120.81(config)#ethernet cfm domain EVC level 4
NCS4206-120.81(config-ecfm)#service number 41 evc EVPL_withQOS
NCS4206-120.81(config-ecfm-srv)#continuity-check
NCS4206-120.81(config-ecfm-srv)#continuity-check interval 1s
NCS4206-120.81(config-ecfm-srv)#ethernet evc EVPL_withQOS
NCS4206-120.81(config-ecfm-srv)#oam protocol cfm domain EVC
    
```

Rollback Configuration

```

interface GigabitEthernet0/0/7
no service instance 5 ethernet EVPL_withQOS
no interface pseudowire177
ethernet evc EVPL_withQOS
no oam protocol cfm
ethernet cfm domain EVC level 4
no service number 41 evc EVPL_withQOS
class-map match-all test_1
no match cos 3
policy-map pol_123
class test_1
no police cir 900000000
police cir 9000000
conform-action transmit
exceed-action drop
interface GigabitEthernet0/0/7
no ethernet uni id Testuni23
ethernet lmi interface
ethernet uni id Testuni23
    
```

Rollback Success

1	[試みた設定 (Attempted Configuration)] : [デバイス (Device(s))] ドロップダウンリストで選択されたデバイスに展開された設定を表示します。
2	[展開ステータス (Deployment Status)] : 選択されたデバイスの展開ステータスを表示します。展開が成功すると、[成功 (Success)] というステータスが表示されます。展開が失敗すると、失敗に関する情報が提供されます。

3	[ロールバック設定 (Roll back Configuration)] : ロールバックが自動的に試みられる設定を表示します。
4	[ロールバック ステータス (Roll back Status)] : 選択されたデバイスのロールバックステータスを表示します。ロールバックが成功すると、[成功 (Success)] というステータスが表示されます。ロールバックが失敗すると、失敗に関する情報が提供されます。この情報を使用して、デバイスの部分的な設定を手動でクリーンアップすることができます。

[削除 (Delete)] をクリックして、失敗した展開をこのウィンドウから削除することもできます。

また、拡張テーブル内の [回線/VC (Circuits/VCs)] タブと [削除済み回線/VC (Deleted Circuits/VCs)] タブの [プロビジョニング (Provisioning)] 列の横にある [i] アイコンをクリックして回線/VCに参加している各デバイスの設定、設定エラー、ロールバック設定、およびロールバック設定エラーの詳細を表示することもできます。[i] アイコンは、[なし (None)] を除くすべてのプロビジョニング状態で使用できます。拡張テーブルへのアクセス方法については、[ネットワーク トポロジマップからのアラーム、ネットワーク インターフェイス、回線/VC、およびリンクの詳細テーブルの表示](#)を参照してください。

展開とロールバックの失敗をトラブルシューティングする方法については、[構成導入の失敗およびロールバックの失敗のトラブルシューティング \(8 ページ\)](#) を参照してください。

構成導入の失敗およびロールバックの失敗のトラブルシューティング

以下に、導入またはロールバックの失敗をトラブルシューティングするためのヒントを示します。

- 導入は失敗するが、ロールバックは成功する場合：構成導入が失敗しても、ロールバックは自動的に開始され、結果が結果ページに表示されます。各デバイスの結果ページに表示される試行された設定とエラーメッセージを分析し、展開の失敗の根本原因を特定します。

導入の失敗の原因として、次の問題が考えられますが、これらに限定されません。

- プロビジョニング ウィザードでサービス パラメータに無効な値が入力されました。たとえば、サービス ID はすでに存在しているか、生成された CLI にセマンティックエラーがある可能性があります。
- デバイスに到達できない、デバイスパスワードが変更された、などのデバイスの問題があります。

この場合は、導入に失敗した回線を（作成時に指定した名前）で特定し、その回線を編集してプロビジョニングを再試行する必要があります。値を変更するサービスパラメータが編集できない場合は、回線を削除して新しい回線を作成します。



(注) 回線を削除する前に、使用されていないことを確認します。

- 導入とロールバックの両方が失敗する場合：この場合は、次の手順を実行します。
 1. デバイスに到達可能であることを確認し、デバイスの再同期を実行します。
 2. 前の導入で報告されたデバイスの問題があれば、問題を修正します。
 3. 回線を編集し、必要に応じて属性を更新して、回線の導入を再試行します。
 4. 導入が失敗すると、Cisco EPN Manager はロールバックを開始します。
 5. ロールが再び失敗した場合は、ロールバックの失敗の原因を特定します。
 6. 失敗の原因を特定するには、構成とロールバック トランザクションの詳細、サービス導入の試行の履歴、および回線/VC 360 度ビューに表示されるロールバック試行を使用できます。回線/VC の情報をすばやく取得する：[回線/VC 360 (Circuit/VC 360)]ビューを参照してください。
 7. 手動でデバイスに保存されている部分構成を削除します。

また、シスコ担当者に問い合わせ、設定の展開の失敗とロールバックの失敗の根本原因を分析し、特定することもできます。

WAN 自動化エンジンの統合

Cisco WAN Automation Engine と Cisco EPN Manager の統合

Cisco WAN Automation Engine (WAE) のプラットフォームは、ソフトウェア モジュールを相互接続し、ネットワークと通信し、外部アプリケーションとインターフェイスする API を提供するオープンでプログラマブルなフレームワークです。

Cisco WAE は、ネットワークの継続的なモニタリングと分析およびネットワーク上のトラフィック需要に基づく現在のネットワークのモデルを作成および維持するためのツールを提供します。このネットワークモデルには、トポロジ、設定、トラフィック情報など、特定の時点でのネットワークに関するすべての関連情報が含まれています。この情報は、トラフィック要求、パス、ノードとリンクの障害、ネットワークの最適化、またはその他の変更によるネットワークへの影響を分析するための基礎として使用できます。



(注) 詳細については、『Cisco WAN Automation Engine (WAE) Installation Guide』と『Cisco WAN Automation Engine (WAE) User Guide』を参照してください。

Cisco EPN Manager では、明示的なパスを持つ単方向トンネルまたは双方向トンネルを作成すると、WAN Automation Engine (WAE) との統合により、Cisco EPN Manager から自動的に REST コールを使用して明示的なパスが提供されます。そのため、明示的なパスを手動で入力する必

要がなくなります。WAE は、可能なネットワーク パスのリストを表示し、適切なパスを選択できるようにします。

WAE パラメータの設定

WAE パスの詳細を指定するには、次の手順を実行します。

始める前に

WAE パラメータを設定することを確認します。

1. [管理 (Administration)] > [設定 (Settings)] > [システム設定 (System Settings)] を選択します。
2. 回線 VC を展開し、[WAE サーバ設定 (WAE Server Settings)] を選択します。
3. 関連する WAE の詳細 (バージョン 7.1.3 以降) とフィールドの詳細 ([WAEサーバIP (WAE Server IP)], [WAEポートアドレス (WAE Port Address)], [WAEサーバユーザ名 (WAE Server User Name)], [WAEサーバパスワード (WAE Server Password)], [WAEネットワーク名 (WAE Network Name)] など) を入力します。
4. [保存 (Save)] をクリックして WAE サーバの設定を保存するか、または [デフォルトにリセット (Reset to Defaults)] をクリックしてデフォルト値を使用します。

-
- ステップ 1** 必要なパラメータを持つ単方向トンネルまたは双方向トンネルを作成します。詳細については、[MPLS TE トンネルの作成とプロビジョニング \(118 ページ\)](#) を参照してください。
- ステップ 2** [パスの制約の詳細 (Path Constraints Details)] 領域で、パスのタイプを [動作中 (Working)] または [保護済み (Protected)] のいずれかとして選択します。フィールドと属性の説明については、[パスの制約の詳細に関するフィールド参照 : MPLS TE トンネル \(130 ページ\)](#) を参照してください。
- ステップ 3** 必要に応じて [新しいパス (New Path)] チェックボックスをオンにして、[WAEサーバからパスを選択 (Choose Path from WAE server)] チェックボックスをオンにします。
- ステップ 4** [WAE サーバからパスを選択 (Choose Path from WAE server)] チェックボックスをオンにします。EPNM マネージャは、WAE ネットワークを取得するために REST 要求を WAE に送信します。WAE は可能なネットワークのリストを返します。
- ステップ 5** [WAE ネットワークの選択 (Select WAE Network)] ドロップダウン リストから、ネットワークを選択します。EPNM マネージャは、送信元、宛先、ネットワークなどの必要なすべてのパラメータを持つ REST 設定要求を WAE に送信します。返される最大パスのデフォルト値は 2 です。WAE は、要求を満たす可能性のあるパスのリストを表示します。
- ステップ 6** [WAE パスの選択 (Select WAE Path)] ドロップダウン リストから、返された適切なパスを選択します。EPNM は、マップ上に選択したパス オーバーレイを表示します。
- ステップ 7** [パス名 (Path Name)] フィールドにパスの名前を入力します。最後に選択したパスを明示的なパスとして使用して、順序のプロビジョニングを続行できます。
-

キャリアイーサネットネットワークの EVC のプロビジョニング

- [Cisco EPN Manager キャリアイーサネットプロビジョニングサポートの概要](#) (11 ページ)
- [EVC プロビジョニングの前提条件](#) (12 ページ)
- [新規キャリアイーサネット EVC の作成およびプロビジョニング](#) (13 ページ)
- [EVPN VPWS 技術を使用した新しいキャリアイーサネット EVC の作成とプロビジョニング](#) (17 ページ)
- [複数の UNI を使用した EVC の作成およびプロビジョニング](#) (19 ページ)

Cisco EPN Manager キャリアイーサネットプロビジョニングサポートの概要

このトピックでは、Cisco EPN Manager におけるキャリアイーサネットサービスプロビジョニングサポートの概要を示します。さまざまなタイプの EVC とサポートされる基盤ネットワークの詳細については、[回線/VC の検出およびプロビジョニングの概要](#)を参照してください。

Cisco EPN Manager は、次のタイプのポートベースおよび VLAN ベースの VC のプロビジョニングをサポートします。

- E-line : イーサネット専用回線 (EPL) とイーサネット仮想専用回線 (EVPL) 。 [E-Line](#)を参照してください。
- E-LAN : EP-LAN と EVP-LAN 。 [E-LAN](#)を参照してください。
- E-Access : Access EPL と Access EVPL 。 [E-Access](#)を参照してください。
- E-TREE : EP-TREE と EVP-TREE 。 [E-Tree](#)を参照してください。
- EVPN 仮想プライベートワイヤサービス (VPWS) 。 [EVPN 仮想プライベートワイヤサービス \(VPWS\)](#) を参照してください。

Cisco EPN Manager は、EVC の作成時に使用可能な次の補足プロビジョニング機能をサポートします。

- UNI のプロビジョニング : EVC ごとに、参加する UNI の属性を定義する必要があります。EVC の作成中にこれを行うか、または EVC の作成プロセスとは無関係に UNI をプロビジョニングできます。 [UNI としてのデバイスおよびインターフェイスの設定](#) (28 ページ) を参照してください。
- ENNI のプロビジョニング : E-Access 回線の場合、ENNI の属性を定義する必要があります。EVC の作成中にこれを行うか、または EVC の作成プロセスとは無関係に ENNI をプロビジョニングできます。 [デバイスとインターフェイスを ENNI として設定する](#) (29 ページ) を参照してください。
- QoS プロファイル : QoS プロファイルを作成して VC に適用できます。 [QoS プロファイルの作成](#) (135 ページ) を参照してください。

- EVC属性のプロファイル：EVCのすべての必須属性を含むプロファイルを作成できます。これらのプロファイルをEVCの作成中に選択して、EVCの属性を定義できます。各EVCの属性を個別に定義する必要はありません。回線/VCプロファイル（134ページ）を参照してください。

EVC プロビジョニングの前提条件

EVC をプロビジョニングする前に、次の前提条件を満たしている必要があります。

1. EVC をプロビジョニングする前にデバイスの間の通信をセットアップする必要があります。
 - MPLS エンドツーエンド ネットワークでは、ラベル配布プロトコル（LDP）をネットワーク全体でセットアップし、各デバイスに LDP ID を指定する必要があります。これにより、MPLS ネットワークのピアのラベルスイッチルータ（LSR）は、ホップバイホップ転送をサポートするためにラベルバインド情報を交換できます。または、MPLS トラフィック エンジニアリングまたはセグメントルーティングを使用して MPLS エンドツーエンド接続を実現できます。具体的には、単方向または双方向の TE トンネルを介した EVC（P2P タイプのみ）プロビジョニングがサポートされます。TE トンネルを介した CEm プロビジョニングと SR ポリシーを介したプロビジョニングもサポートされています。
 - イーサネットアクセスがある場合、つまり、すべてのデバイスが MPLS に対応しているわけではない場合は、イーサネット アクセス スイッチを MPLS スイッチに接続するように G.8032 リングまたは ICCP-SM を設定する必要があります。
 - CDP または LLDP は、イーサネット リンク検出を有効にするように、G.8032 リング内のリンク上に設定する必要があります。
2. ICCP-SM と G.8032 ネットワーク上に EVC をプロビジョニングするには、すべての VLAN（1 から 4095 まで）をプライマリまたはセカンダリ VLAN として設定する必要があります。
3. EVC をプロビジョニングするデバイスのインベントリ収集の状態は [完了（Completed）] である必要があります。これを確認するには **Inventory > Network Devices** に移動し、[最新のインベントリ収集ステータス（Last Inventory Collection Status）] 列のステータスを確認します。
4. システムに顧客を作成して、回線/VC の作成およびプロビジョニングプロセス中に顧客に回線/VC を関連付けられるようにすることができます。左側のサイドバーで **Inventory > Other > Customers** を選択し、顧客を作成および管理します。
5. EVC でインターフェイスを使用する場合は、インターフェイスのデフォルト設定をリセットすることをお勧めします。グローバルコンフィギュレーションモードでは、各インターフェイスで次のコマンドを設定します。

```
default interface 'interface-name'
```

6. ME3600 と ME3800 デバイスでは、サービス インスタンスは、VLAN が許可されていないトランク ポートでのみ設定できます。インターフェイスで次のコマンドを設定し、Cisco EPN Manager でデバイスを再同期します。

```
interface GigabitEthernetXX/XX
switchport trunk allowed vlan none
switchport mode trunk
```

7. EVPN の使用時に EPL および EVPN サービスをプロビジョニングするには、デバイス設定の [BGP] セクションで次のコマンドを定義します。このコマンドを設定しない場合、EVPN サービスのプロビジョニング時にデバイスは表示されません。

```
address-family l2vpn evpn
```

新規キャリア イーサネット EVC の作成およびプロビジョニング

EVC はトポロジマップのコンテキストで作成します。トポロジマップとプロビジョニングウィザードにアクセスするには、左側のサイドバーから **[構成 (Configuration)]** > **[ネットワーク (Network)]** > **[サービス プロビジョニング (Service Provisioning)]** の順に選択します。または、次の手順での説明に従ってトポロジマップからプロビジョニングウィザードを開くこともできます。

EVC を作成してプロビジョニングするプロセスは、サポートされているすべての EVC タイプで同様であり、次の作業が含まれます。

- EVC のエンドポイント (UNI および ENNI) を指定します。
- 回線/VC の設定パラメータを定義します。

サービスがプロビジョニングされた後は、サービスを編集し、A エンドポイントまたは Z エンドポイントを更新または変更できます。

エンドポイントの変更は、EPL や EVPL などの E 回線サービスでサポートされています。変更できるのは管理対象エンドポイントと、フル サービスまたは部分的サービスのみです。

サービスの変更中に、既存の UNI に異なるデバイスか、または異なるポートを持つ同じデバイスがある場合は、既存の他の UNI に変更できます。

これには次のような制約があります。

- 1 回のサービス変更で、両端のエンドポイントを変更することはできません。
- スタンドアロン UNI ウィザードを使用して UNI を作成し、EPL サービスまたは EVPL サービスの変更に使用します。
- サービスの変更中に新しい UNI を作成することはできません。

始める前に

EVC をプロビジョニングする前に満たす必要がある前提条件については、[EVC プロビジョニングの前提条件 \(12 ページ\)](#) を参照してください。

新しい EVC を作成するには、次の手順に従います。

- ステップ 1** 左側のサイドバーから、[マップ (Maps)] > [トポロジマップ (Topology Maps)] > [ネットワーク トポロジ (Network Topology)] の順に選択します。
- ステップ 2** ツールバーで [デバイス グループ (Device Group)] ボタンをクリックし、マップに表示するデバイスのグループを選択します。
- ステップ 3** [回線/VC (Circuits/VCs)] タブで、[+] アイコンをクリックします。これにより、マップの右側に新しいペインが開き、[プロビジョニング ウィザード (Provisioning Wizard)] が表示されます。
- ステップ 4** [テクノロジー (Technology)] ドロップダウンリストで **Carrier Ethernet** を選択すると、Cisco EPN Manager は [サービス タイプ (Service Type)] 領域に関連する回線/VC タイプのリストを表示します。たとえば、キャリアイーサネット サービス タイプには EPL、EVPL、EP-LAN などが含まれます。
- ステップ 5** [サービス タイプ (Service Type)] リストから、作成する回線/VC のタイプを選択します。
- ステップ 6** さまざまなサービスの属性を設定するプロファイルを定義している場合、[プロファイルの選択 (Select Profile)] ドロップダウンリストから必要なプロファイルを選択します。[回線/VC プロファイル \(134 ページ\)](#) を参照してください。
- ステップ 7** **Next** をクリックして [サービスの詳細 (Service Details)] ページに移動します。
- ステップ 8** (オプション) EVC の作成対象顧客を選択します。リストに顧客が表示されない場合は **Inventory > Other > Customers** に移動し、システムで顧客を作成してからプロビジョニング ウィザードを再起動します。
- ステップ 9** サービスの詳細を入力します。フィールドと属性の説明については、[サービス詳細の参考資料 \(22 ページ\)](#) を参照してください。
- ステップ 10** E-Line EVC、E-Tree EVC、E-LAN EVC の場合：必要に応じて、EVC で障害およびパフォーマンス モニタリングを可能にするサービス OAM を設定します。E-Line EVC の場合：[サービス OAM (Service OAM)] オプションを有効にするには、[CFM の有効化 (Enable CFM)] チェックボックスをオンにします。その後、新しい CFM ドメインを作成するか、または E 回線 EVC の既存のドメインを選択することができます。[サービス OAM \(27 ページ\)](#) を参照してください。プラスアイコンをクリックして [サービス OAM (Service OAM)] テーブルに行を追加し、該当する列に値を入力します。E-Tree EVC の場合、方向 (リーフからルート、ルートからリーフ、またはルートからルート) を指定する必要があります。
- たとえば EVPL/EPL サービスの場合、ポイントツーポイント サービスまたはマルチポイントサービスを昇格させ、調整する場合は、[CFM ドメイン名 (CFM Domain name)]、[CFM ドメインレベル (CFM Domain level)]、および [メンテナンス (Maint)] などの CFM パラメータを有効にします。関連付けられた [名前のタイプ (Name Type)] フィールド、[ITU キャリアコード (ITU Carrier Code)] フィールド、[ITU MEG ID コード (ITU MEG ID Code)] フィールド、[継続性チェック間隔 (Continuity check interval)] フィールド。CFM パラメータは、サービス昇格時に検出されたバージョンから読み取られます。検出されたバージョンか、またはプロビジョニングされたバージョンとの調整を実行できます。
- (注) デフォルトでは、[メンテナンス関連名 (Maint Assoc Name)] として IEEE が選択されています。[メンテナンス (Maint)] で [ITU] が選択されている場合。関連付けられた [名前のタイプ (Name Type)] ドロップダウンリスト、[ITU キャリアコード (ITU Carrier Code)]、および [ITU MEG ID コード (ITU MEG ID code)] が表示されます。
- ステップ 11** [展開アクション (Deployment Action)] フィールドに、ECV の作成プロセス完了時のアクションを指定します。実際に展開する前に、該当するデバイスに展開される設定のプレビューを表示するように指定することも、完了時にすぐに設定を展開するように指定することもできます。

ステップ 12 **Next** をクリックして UNI を定義するページに移動します。E-Access の場合、ENNI を定義するページもあります。

ステップ 13 UNI として機能するデバイスとインターフェイスを識別します。

(注) エンドポイントのいずれかが、Cisco EPN Manager で管理されないデバイス上のインターフェイスである場合、[管理対象外 (Unmanaged)]チェックボックスをオンにして、その管理対象外デバイスの情報を入力します。アンマネージドエンドポイントを使用した回線VCのプロビジョニング (137 ページ) を参照してください。

- デバイス上で必要なインターフェイスを既に設定している場合は、**Create New UNI** チェックボックスをオフにして、関連する UNI 名をリストから選択します。

(注) リスト内の UNI 名は、UNI の作成時に選択したサービスとオプションによって異なります。

- EPL、Access EPL、EP LAN、および EP Tree サービスの場合は、作成時に [すべてを1つにバンドリング (All To One Bundling)] オプションが選択された UNI のみが表示されます。
 - EVPL、Access EVPL、および EVP Tree サービスの場合、[多重化 (Multiplexing)] オプションまたは [バンドリング (Bundling)] オプション、またはその両方が作成時に選択された UNI のみがリストされます。
- 新しい UNI を作成するには、次の手順を実行します。

- **Create New UNI** チェックボックスがオンになっていることを確認します。
- [UNI 名 (UNI Name)] フィールドに、UNI を簡単に識別できるような UNI 名を入力します。
- [デバイス (Device)] フィールドのリストからデバイスを選択するか、マップ内のデバイスをクリックして選択し、[デバイス (Device)] フィールドに取り込みます。選択したデバイスのポートのリストが表示されます。
- [ポート (Port)] テーブルから必要なポートを選択します。ポートを UNI に使用できない場合は、[ポート (Port)] テーブルの UNI 名の横にアラートアイコンが表示され、ポートが選択できない理由が示されます。

(注) UNI の作成時に選択したデバイスは、マップ内でオレンジ色の丸で囲われます。オレンジの円の上に UNI 名が表示されます。ポイントツーポイント EVC の場合、オレンジの円に、これが A 側または Z 側のどちらのエンドポイントであるかを示すラベルが付けられます。

ステップ 14 新しい UNI を作成している場合は、新しい UNI の詳細を入力します。フィールドと属性の説明については、**新規 UNI の詳細リファレンス (23 ページ)** を参照してください。

ステップ 15 UNI サービスの詳細を入力します。フィールドと属性の説明については、**UNI サービス詳細の参照 (24 ページ)** を参照してください。

ステップ 16 H-VPLS をコアテクノロジーとして使用する E-LAN EVC および E-TREE EVC の場合、プライマリ ハブとセカンダリ ハブとして機能するデバイスをそれぞれ選択します。

- ステップ 17** E 回線 EVC の場合：[疑似回線設定 (Pseudowire Settings)] ページで、次のようにして EVC が経由する TE トンネルを選択できます。
1. [静的優先パス (Static Preferred Path)] チェックボックスをオンにして、サービスの静的ルートを割り当てます。
 2. [優先パスタイプ (Preferred Path Type)] に [双方向 (Bidirectional)] または [単方向 (Unidirectional)]、あるいは [SR ポリシー (SR Policy)] を選択します。
 3. [優先パス (Preferred Path)] ドロップダウンリストから、必要な双方向 TE トンネルを選択します。このリストには、EVC のエンドポイント間にすでに存在する双方向 TE トンネルのすべてが示されます。

(注) このフィールドが有効になるのは、[優先パスタイプ (Preferred Path Type)] として [双方向 (Bidirectional)] を選択した場合のみです。
 4. [優先パス (A-Z) (Preferred Path (A-Z))] および [優先パス (Z-A) (Preferred Path (Z-A))] ドロップダウンリストのそれぞれから、必要な単方向 TE トンネルを選択します。

(注) これらのフィールドは、[優先パスタイプ (Preferred Path Type)] に [単方向 (Unidirectional)] を選択したときのみ使用できます。
 5. 優先パスが使用できない場合にデフォルトパスが使用されるようにするには、[LDP へのフォールバックを許可 (Allow Fallback to LDP)] チェックボックスをオンにします。

(注) エンドポイント間にトンネルが存在しない場合、[優先パス (Preferred Path)] および [LDP へのフォールバックを許可 (Allow Fallback to LDP)] オプションは無効になります。
 6. 接続の両側で疑似回線ペイロードを識別するためにコントロールワードが使用されるようにするには、[送信コントロールワード (Send Control Word)] チェックボックスをオンにします。
 7. イーサネット、VLAN、または IP のいずれかを使用する相互接続サイトが必要な場合は、[相互接続オプション (Interworking Option)] を選択します。EVC のいずれかのエンドポイントが管理対象外デバイスである場合は、このオプションを有効にする必要があります。
 8. 疑似回線に必要な帯域幅を入力します。
 9. [PW ID] フィールドには、ポイントツーポイント サービスの疑似回線の設定に表示する識別子を入力します。

(注) 疑似回線 (PW) の ID は、PW ID のリソース プールから自動的に割り当てられます。PW ID 値は、サービスの作成時にのみ変更できます。EVC サービスの変更時にこの値を編集することはできません。入力された PW ID が既にサービスに割り当てられている場合は、エラーメッセージが表示されます。
- ステップ 18** (オプション) サービスに参加するデバイス上に設定する追加の CLI コマンドをテンプレートに追加する場合は、[サービス テンプレート (Service Template)] ページを使用します。詳細については、[テンプレートを使用した回線/VC の拡張 \(138 ページ\)](#) を参照してください。
- ステップ 19** 回線/VC に必要な情報をすべて入力したら、**Submit** をクリックします。デバイスに展開される CLI のプレビューを表示することを選択した場合は、プレビューが表示されます。この場合、属性の編集 (Edit

Attributes)] をクリックすることで、属性を変更できます。そうでない場合は、すぐに設定がデバイスに展開されます。

ステップ 20 回線/VC が、[ネットワーク トポロジ (Network Topology)] ウィンドウの [回線/VC (Circuits/VCs)] タブのリストに追加されているはずで

設定の展開が失敗した場合は、[展開が失敗した場合の動作 \(4 ページ\)](#) を参照してください。

EVPN VPWS 技術を使用した新しいキャリアイーサネット EVC の作成とプロビジョニング

EVPN を使用してキャリアイーサネット EVC を作成してプロビジョニングするには、次の手順を実行します。

始める前に

EVC をプロビジョニングする前に満たす必要がある前提条件については、[EVC プロビジョニングの前提条件 \(12 ページ\)](#) を参照してください。

- ステップ 1** 左側のサイドバーから、[マップ (Maps)] > [トポロジ マップ (Topology Maps)] > [ネットワーク トポロジ (Network Topology)] の順に選択します。
- ステップ 2** ツールバーで [デバイス グループ (Device Group)] ボタンをクリックし、マップに表示するデバイスのグループを選択します。
- ステップ 3** [回線/VC (Circuits/VCs)] タブで、[+] アイコンをクリックします。これにより、マップの右側に新しいペインが開き、[プロビジョニング ウィザード (Provisioning Wizard)] が表示されます。
- ステップ 4** [テクノロジー (Technology)] ドロップダウンリストで **Carrier Ethernet** を選択すると、Cisco EPN Manager は [サービス タイプ (Service Type)] 領域に関連する回線/VC タイプのリストを表示します。EVPN は、キャリアイーサネットのサービスタイプ EPL および EVPL でサポートされています。
- ステップ 5** [サービス タイプ (Service Type)] リストから、作成する回線/VC のタイプを選択します。
- ステップ 6** さまざまなサービスの属性を設定するプロファイルを定義している場合、[プロファイルの選択 (Select Profile)] ドロップダウン リストから必要なプロファイルを選択します。[回線/VC プロファイル \(134 ページ\)](#) を参照してください。
- ステップ 7** **Next** をクリックして [サービスの詳細 (Service Details)] ページに移動します。
- ステップ 8** (オプション) EVC の作成対象顧客を選択します。リストに顧客が表示されない場合は **Inventory > Other > Customers** に移動し、システムで顧客を作成してからプロビジョニング ウィザードを再起動します。
- ステップ 9** サービスの詳細を入力します。フィールドと属性の説明については、[サービス詳細の参考資料 \(22 ページ\)](#) を参照してください。
- ステップ 10** [EVPN を使用 (Use EVPN)] チェックボックスをオンにします。
- ステップ 11** E-Line EVC の場合：必要に応じて、EVC で障害およびパフォーマンスのモニタリングを可能にするサービス OAM を設定します。[CFM の有効化 (Enable CFM)] チェックボックスをオンにしてサービス OAM オプションを有効にします。その後、新しい CFM ドメインを作成するか、または E 回線 EVC の既存のドメインを選択することができます。[サービス OAM \(27 ページ\)](#) を参照してください。プラス アイコ

ンをクリックして [サービス OAM (Service OAM)] テーブルに行を追加し、該当する列に値を入力します。

(注) ICC ベースの CFM は、EVPN ではサポートされていません。

ステップ 12 [展開アクション (Deployment Action)] フィールドに、ECV の作成プロセス完了時のアクションを指定します。実際に展開する前に、該当するデバイスに展開される設定のプレビューを表示するように指定することも、完了時にすぐに設定を展開するように指定することもできます。

ステップ 13 UNI として機能するデバイスとインターフェイスを識別します。

(注) EVPN は、管理対象外デバイスをサポートしていません。

[サービスの詳細 (Service Detail)] ページの [EVPN を使用 (Use EVPN)] チェックボックスをオンにすると、EVPN をサポートするデバイスのみが [UNI A] ページと [UNI Z] ページに表示されます。

- デバイス上で必要なインターフェイスを既に設定している場合は、**Create New UNI** チェックボックスをオフにして、関連する UNI 名をリストから選択します。

(注) リスト内の UNI 名は、UNI の作成時に選択したサービスとオプションによって異なります。

- EPL、Access EPL、EPE LAN、および EP Tree サービスの場合は、作成時に [すべてを1つにバンドリング (All To One Bundling)] オプションが選択された UNI のみが表示されます。
- EVPL、Access EVPL、および EVP Tree サービスの場合、[多重化 (Multiplexing)] オプションまたは [バンドリング (Bundling)] オプション、またはその両方が作成時に選択された UNI のみがリストされます。

- 新しい UNI を作成するには、次の手順を実行します。

- **Create New UNI** チェックボックスがオンになっていることを確認します。
- [UNI 名 (UNI Name)] フィールドに、UNI を簡単に識別できるような UNI 名を入力します。
- [デバイス (Device)] フィールドのリストからデバイスを選択するか、マップ内のデバイスをクリックして選択し、[デバイス (Device)] フィールドに取り込みます。選択したデバイスのポートのリストが表示されます。
- [ポート (Port)] テーブルから必要なポートを選択します。ポートを UNI に使用できない場合は、[ポート (Port)] テーブルの UNI 名の横にアラートアイコンが表示され、ポートが選択できない理由が示されます。

(注) UNI の作成時に選択したデバイスは、マップ内でオレンジ色の丸で囲われます。オレンジの円の上に UNI 名が表示されます。ポイントツーポイント EVC の場合、オレンジの円に、これが A 側または Z 側のどちらのエンドポイントであるかを示すラベルが付けられます。

ステップ 14 新しい UNI を作成している場合は、新しい UNI の詳細を入力します。フィールドと属性の説明については、**新規 UNI の詳細リファレンス (23 ページ)** を参照してください。

- ステップ 15** UNI サービスの詳細を入力します。フィールドと属性の説明については、[UNI サービス詳細の参照 \(24 ページ\)](#) を参照してください。
- ステップ 16** E-Line EVC の場合 : [EVPNの設定 (EVPN Settings)] ページで、次の手順を実行します。
1. [EVPN インスタンス (EVI) ID (EVPN Instance (EVI ID))] は事前に入力されています。この値は必要に応じて変更できます。
 2. [RD 値 (RD Value)] を指定するには、[自動 RD (Auto RD)] チェックボックスをオフにします。
 3. [RT のインポート (Import RT)] および [RT のエクスポート (Export RT)] の値を指定するには、[自動 RT (Auto RT)] チェックボックスをオフにします。
(注) [RT のインポート (Import RT)]、[RT のエクスポート (Export RT)]、[RD]、および [コントロールワード (Control Word)] は、使用した EVI ID が他のそのサービスにも関連付けられていない場合にのみ編集できます。
 4. 接続の両側でパイロットを識別するためにコントロールワードを使用するには、[コントロールワード (Control Word)] チェックボックスをオンにします。
 5. Z エンド AC 識別子と A エンド AC 識別子は事前に入力されています。これらの値は必要に応じて変更できます。
 6. [静的優先パス (Static Preferred Path)] チェックボックスを選択して A ~ Z または Z ~ A の優先パスを指定し、SR ポリシーを指定できます。
 7. 優先パスが使用できない場合にデフォルト パスが使用されるようにするには、[LDP へのフォールバックを許可 (Allow Fallback to LDP)] チェックボックスをオンにします。
(注) エンドポイント間にトンネルが存在しない場合、[優先パス (Preferred Path)] および [LDP へのフォールバックを許可 (Allow Fallback to LDP)] オプションは無効になります。
- ステップ 17** (オプション) サービスに参加するデバイス上に設定する追加の CLI コマンドをテンプレートに追加する場合は、[サービス テンプレート (Service Template)] ページを使用します。詳細については、[テンプレートを使用した回線/VC の拡張 \(138 ページ\)](#) を参照してください。
- ステップ 18** 回線/VC に必要な情報をすべて入力したら、**Submit** をクリックします。デバイスに展開される CLI のプレビューを表示することを選択した場合は、プレビューが表示されます。この場合、属性の編集 (Edit Attributes)] をクリックすることで、属性を変更できます。そうでない場合は、すぐに設定がデバイスに展開されます。
- ステップ 19** 回線/VC が、[ネットワーク トポロジ (Network Topology)] ウィンドウの [回線/VC (Circuits/VCs)] タブのリストに追加されているはずですが。

複数の UNI を使用した EVC の作成およびプロビジョニング

Cisco EPN Manager では、マルチポイント EVC (E-LAN および E-Tree) を作成してプロビジョニングするプロセスで、複数の UNI の作成/選択がサポートされています。



(注) VPLS をコア テクノロジーとして使用する EVC の場合、同じデバイス上に複数の UNI を設定できますが、H-VPLS ベースの EVC の場合はその限りではありません。

始める前に

EVC をプロビジョニングする前に満たす必要がある前提条件については、[EVC プロビジョニングの前提条件 \(12 ページ\)](#) を参照してください。

新しい EVC を作成するには、次の手順に従います。

- ステップ 1** 左側のサイドバーのメニューから、[**マップ (Maps)**] > [**トポロジ マップ (Topology Maps)**] > [**ネットワーク トポロジ (Network Topology)**] の順に選択します。
- [**ネットワーク トポロジ (Network Topology)**] ウィンドウが開きます。
- ステップ 2** ツールバーで [**デバイス グループ (Device Groups)**] をクリックし、マップ上に表示するデバイスのグループを選択します。
- ステップ 3** [**回線/VC (Circuits/VCs)**] タブをクリックします。
- ステップ 4** [**回線/VC (Circuits/VCs)**] ペインのツールバーで、[**+**] (作成) アイコンをクリックします。
- マップの右側に新しいペインが開き、[**プロビジョニング ウィザード (Provisioning Wizard)**] が表示されます。
- ステップ 5** [**テクノロジーの選択 (Select Technology)**] ドロップダウンリストで **Carrier Ethernet** を選択します。
- ステップ 6** [**サービス タイプ (Service Type)**] リストから、マルチポイント EVC タイプを選択します。
- ステップ 7** さまざまなサービスの属性を設定するプロファイルを定義している場合、[**プロファイルの選択 (Select Profile)**] ドロップダウンリストから必要なプロファイルを選択します。[回線/VC プロファイル \(134 ページ\)](#) を参照してください。
- ステップ 8** **Next** をクリックして [**サービスの詳細 (Service Details)**] ページに移動します。
- ステップ 9** EVC を作成する対象の顧客を選択します。リストに顧客が表示されない場合は **Inventory > Other > Customers** に移動し、システムで顧客を作成してからプロビジョニング ウィザードを再起動します。
- ステップ 10** サービスの詳細を入力します。フィールドと属性の説明については、[サービス詳細の参考資料 \(22 ページ\)](#) を参照してください。
- ステップ 11** [**展開アクション (Deployment Action)**] フィールドに、ECV の作成プロセス完了時のアクションを指定します。実際に展開する前に、該当するデバイスに展開される設定のプレビューを表示するように指定することも、完了時にすぐに設定を展開するように指定することもできます。
- ステップ 12** [**次へ (Next)**] をクリックして UNI を定義するページに進みます。
- ステップ 13** [**マルチ UNI (Multi UNI)**] 領域でプラスアイコンをクリックし、最初の UNI をテーブルに追加します。UNI にはデフォルトの名前が付けられて、自動的にテーブル内で選択された状態になります。プラスアイコンをクリックするたびに、新しい UNI がテーブルに追加されます。
- または、マップ内のデバイスをクリックして新しい UNI をテーブルに追加することもできます。この場合、新規 UNI の詳細の [**デバイス (Device)**] フィールドに、そのデバイスの名前が取り込まれます。

ステップ 14 テーブルから、属性を定義または編集する UNI を選択します。

ステップ 15 UNI として機能するデバイスとインターフェイスを識別します。

- 既存の UNI を使用する場合、[新規 UNI の作成 (Create New UNI)] チェックボックスをオフにして、リストから該当する UNI 名を選択します。

(注) リスト内の UNI 名は、UNI の作成時に選択したサービスとオプションによって異なります。

- EPL、Access EPL、EP LAN、および EP Tree サービスの場合は、作成時に [すべてを1つにバンドリング (All To One Bundling)] オプションが選択された UNI のみが表示されます。
- EVPL、Access EVPL、および EVP Tree サービスの場合、[多重化 (Multiplexing)] オプションまたは [バンドリング (Bundling)] オプション、またはその両方が作成時に選択された UNI のみがリストされます。

- 新しい UNI を定義するには、次の手順に従います。

- [新規 UNI の作成 (Create New UNI)] チェックボックスがオフにされていることを確認します。
- [UNI 名 (UNI Name)] フィールドに、UNI を簡単に識別できるような UNI 名を入力します。
- [デバイス (Device)] フィールドで、リストからデバイスを選択します。選択したデバイスのポートのリストが表示されます。
- [ポート (Port)] テーブルから必要なポートを選択します。ポートを UNI に使用できない場合は、[ポート (Port)] テーブルの UNI 名の横にアラートアイコンが表示され、ポートが選択できない理由が示されます。

ステップ 16 新しい UNI を作成している場合は、新しい UNI の詳細を入力します。新規 UNI の詳細は、[マルチ UNI (Multi UNI)] テーブルで現在選択されている UNI に関するものです。フィールドと属性の説明については、[新規 UNI の詳細リファレンス \(23 ページ\)](#) を参照してください。

ステップ 17 UNI サービスの詳細を入力します。フィールドと属性の説明については、[UNI サービス詳細の参照 \(24 ページ\)](#) を参照してください。[次へ (Next)] をクリックします。

ステップ 18 エンドポイントのいずれかが Cisco EPN Manager で管理されないデバイス上のインターフェイスである場合、[管理対象外 (Unmanaged)] ページでその管理対象外デバイスの情報を入力します。[アンマネージドエンドポイントを使用した回線/VC のプロビジョニング \(137 ページ\)](#) を参照してください。

ステップ 19 これはオプションです。テンプレートに、サービスに参加するデバイス上に設定する追加の CLI コマンドを付加する場合は、[サービス テンプレート (Service Template)] ページを使用します。詳細については、[テンプレートを使用した回線/VC の拡張 \(138 ページ\)](#) を参照してください。

ステップ 20 回線/VCに必要な情報をすべて入力したら、[送信 (Submit)] をクリックします。デバイスに展開される CLI のプレビューを表示することを選択した場合は、プレビューが表示されます。この場合、属性の編集 (Edit Attributes)] をクリックすることで、属性を変更できます。そうでない場合は、すぐに設定がデバイスに展開されます。

ステップ 21 回線/VC が、[ネットワーク トポロジ (Network Topology)] ウィンドウの [回線/VC (Circuits/VCs)] ペインのリストに追加されているはずですが。

サービス詳細の参考資料

次の表に、サービス レベルの EVC を定義する属性を示し、それらについて説明します。すべての属性がすべての EVC タイプに関連するわけではないことに注意してください。

表 1: サービスの詳細

属性	説明
サービス名 (Service Name)	回線/VC を特定する一意の名前。
サービスの説明 (Service Description)	VC を識別するのに役立つ VC の説明。
サービス タイプ (Service Type)	作成するサービスのタイプに基づいて事前に入力されています (EPL、EVPL、EP-LAN など)。
EVPN を使用 (Use EVPN)	EVPN ベースのコネクションを作成できます。
サービス MTU	VC を通過するフレームの最大サイズ (バイト単位)。値は 64 ~ 65535 です。サービス MTU は、サービスのすべての UNI で定義された MTU 以下である必要があります。
コアテクノロジー	VPLS または H-VPLS。マルチポイント EVC のコア テクノロジーを参照してください。 (注) VPLS または H-VPLS の場合は、プロビジョニング ウィザードを使用して最大 20 台のデバイスをプロビジョニングできます。
VPN ID	マルチポイント EVC に関連します (VPLS と H-VPLS の両方)。このフィールドには、次の使用可能な擬似回線の ID が自動的に入力されます。この ID は、EVC の作成プロセス中に変更できます (有効な値の範囲: 1 ~ 4294967295)。EVC の変更時には、ID は編集できません。 (注) VPN ID はネットワーク全体で一意に使用されます。つまり、2 つのサービスで同じ VPN ID が使用されることはありません。また、擬似回線の競合を回避するため、ネットワークですでに設定されている擬似回線 ID を VPN ID に使用することはできません。VPN ID 値が [PW ID] フィールドに表示されます。サービスの作成および変更時にマルチポイントサービスの PW ID 値を変更することはできません。

属性	説明
PW ID	マルチポイント EVC およびポイントツーポイント EVC に関連します。このフィールドには、次の使用可能な擬似回線の ID が自動的に入力されます。この ID を編集し、EVC 作成プロセス時にポイントツーポイント EVC の場合にのみ値（有効値範囲：1～4294967295）を割り当てることができます。EVC の変更時には、ID は編集できません。 (注) PW ID はネットワーク全体で一意に使用されます。つまり、2つのサービスで同じ PW ID が使用されることはありません。
バンドリング	この VC で複数の VLAN を有効にします。複数の CE-VLAN ID は、1つの EVC にバンドルされます。
CE-VLAN ID の保持	出力サービスフレームの CE-VLAN ID が対応する入力サービスフレームの CE-VLAN ID と同じ値であることを確認します。バンドリングが有効な場合、これを有効にする必要があります。
CE-VLAN ID CoS の保持	出力サービスフレームの CE-VLAN CoS が対応する入力サービスフレームの CE-VLAN CoS と同じ値であることを確認します。CoS マーキングは変更できません。

新規 UNI の詳細リファレンス

次の表に、UNIとして指定されているポートに関連する属性とその説明をリストします。すべての属性がすべての EVC タイプに関連するわけではないことに注意してください。

表 2: 新規 UNI の詳細 (New UNI Details)

属性	説明
[MTU]	インターフェイスを通過するパケットの最大伝送サイズ (バイト単位)。UNI の MTU は、サービス レベルで定義された MTU 以上でなければなりません。
自動ネゴシエーション (Auto Negotiation)	速度とデュプレックスモードを自動的にネゴシエートするには、このチェックボックスをオンにします。
速度	ポートの速度。ポートでサポートされている場合は、速度を下げるできます。 (注) [自動ネゴシエーション (Auto Negotiation)] チェックボックスをオンにすると、このフィールドは使用できません。

属性	説明
デュプレックス モード (Duplex Mode)	<ul style="list-style-type: none"> • [全二重 (Full Duplex)] : UNI と顧客のアクセス スイッチ間で、どちらの側も全二重をサポートしていると仮定して、双方向の同時通信を使用します。一方の側が全二重をサポートしていない場合、ポートはダウンします。 • [自動ネゴシエーション (Auto-Negotiation)] : サポートされている内容に応じて、2つのデバイス間で合意されたモードを使用します。全二重が試行されますが、一方のデバイスがそれをサポートしていない場合、半二重が使用されます。 <p>(注) [自動ネゴシエーション (Auto Negotiation)] チェックボックスをオンにすると、このフィールドは使用できません。</p>
[サービス多重化 (Service Multiplexing)]	UNI が複数の EVC インスタンスに参加できるようにします。
[UNI 許可バンドリング (UNI Allows Bundling)]	バンドルを有効にして、UNI が VC に参加できるようにします。バンドルについては、以下を参照してください: サービス詳細の参考資料 (22 ページ)
[タグなし CE-VLAN ID (Untagged CE-VLAN ID)]	タグなしトラフィックに割り当てられた CE-VLAN の ID。
[入力/出力 QoS プロファイル (Ingress/Egress QoS Profile)]	UNI の入力または出力トラフィックに必須の QoS プロファイルを選択します。プロファイルの一覧には、デバイスで設定され、システムによって検出されるポリシーマップおよびユーザ定義の QoS プロファイルが含まれます。QoS プロファイルの作成方法については、 QoS プロファイルの作成 (135 ページ) を参照してください。
[UNI QoS プロファイル (UNI QoS Profile)]	UNI 自体の QoS プロファイルを適用して、UNI の帯域幅プロファイルおよびその他の QoS 属性を定義します。UNI レベルで QoS プロファイルを適用する場合は、サービス レベルで QoS プロファイルを適用しないでください。
[リンク OAM の有効化 (Enable Link OAM)]	IEEE 803.1ah リンクの操作とメンテナンスを有効にします。リンク OAM が有効になっている場合は、この UNI と顧客のアクセス スイッチ間のリンクの状態に関連するイベントが表示されます。
[リンク管理の有効化 (Enable Link Management)]	顧客アクセス スイッチがこの UNI、VLAN ID、UNI 上のサービスなどに関する情報を取得できるようにします。

UNI サービス詳細の参照

次の表に、UNI に関連する EVC の属性 (EVC がこの UNI でどのように動作するか、など) の一覧と説明を示します。すべての属性がすべての EVC タイプに関連しているとは限りません。



(注) QinQ 属性については、選択したデバイスでサポートされている属性のみがウィザードに表示されます。

表 3: UNI サービス詳細

属性	説明	その他の情報
入力/出力サービス QoS プロファイル (Ingress/Egress Service QoS Profile)	<p>UNI の入力または出力トラフィックに必須の QoS プロファイルを選択します。プロファイルの一覧には、デバイスで設定され、システムによって検出されるポリシー マップおよびユーザ定義の QoS プロファイルが含まれます。</p> <p>(注) リリース 4.0.0 以降では、独立した列 ([Sub-Policy]) は、値 True を表示することによって、特定のポリシーがサブポリシーであるかどうかを示します。サブポリシーではないポリシーの場合は、関連付けられている [Sub-Policy] 列に値 NA が表示されます。</p> <p>QoS プロファイルの作成方法については、QoS プロファイルの作成 (135 ページ) を参照してください。</p>	
レイヤ 2 制御プロトコル プロファイル (Layer 2 Control Protocol Profile)	さまざまな通信プロトコルの処理方法を決定するプロファイル。さまざまなプロトコルを使用するフレームは、トンネル化、ドロップ、またはピアリングされます。詳細については、MEF 6.1 を参照してください。	
指定	E-Tree の場合：VC の UNI のロール（リーフまたはルート）を選択します。	
ルートを指定したポイントツーポイント接続の使用 (Use point to point connection with Root)	E-Tree の場合：UNI がリーフとして指定された場合、このチェックボックスを選択して、ルートとリーフ間のアクティブな疑似回線を作成できます。このチェックボックスは、単一デバイスに複数のエンドポイントが存在する場合またはサービスに複数のルートが存在する場合は表示されません。	
一致 (Match)	<p>UNI を入力するためにトラフィックに必要なタギングのタイプを選択します。</p> <ul style="list-style-type: none"> • Dot1q：サービス インスタンスへのインターフェイスの 802.1q フレーム入力のマッピング。 • Dot1ad：サービス インスタンスへのインターフェイスの 802.1ad フレーム入力のマッピング。 • デフォルト (Default)：このポートの他のどの VC にも割り当てられないトラフィック。 • タグなし (Untagged)：VLAN タグがないフレーム 	Dot1AD は、15.3(3) ソフトウェア バージョンを実行している ME3600 デバイスではサポートされません。

属性	説明	その他の情報
VLAN の自動割り当て	UNI に VLAN ID を自動的に割り当てるには、このチェックボックスをオンにします。	
VLAN	VLAN ID。1 ～ 4094 の整数。ハイフンまたはカンマで区切られた一連の VLAN ID を使用して VLAN ID の範囲を入力できます。	[VLAN の自動割り当て (Auto Allocate VLAN)] チェックボックスをオンにした場合、このフィールドは使用できません。
内部 VLAN (Inner VLAN(s))	VLAN タギングの第 2 レベルの VLAN ID。1 ～ 4094 の整数。ハイフンまたはカンマで区切られた一連の VLAN ID を使用して VLAN ID の範囲を入力できます。	
タグなしバンドル (Untagged Bundled)	VLAN タグのないトラフィックを VLAN タグ付きのフレームとともにバンドルできます。	
優先順位タグ付きバンドル (Priority Tagged Bundled)	優先順位タグ付きトラフィックを VLAN タグ付きフレームとともにバンドルできます。	
完全一致 (Exact)	サービスによる伝送対象として一致していない追加の VLAN タグが付けられたトラフィックのアドミタンスを防止します。	IOS-XR デバイスにのみ適用されます。
外部 VLAN CoS (Outer VLAN CoS)	フレームに関連付ける必要がある外部 VLAN サービス クラス ID。CoS ID は、0 ～ 7 の範囲の整数です。	IOS デバイスにのみ適用されます。
内部 VLAN CoS (Inner VLAN CoS)	フレームに関連付ける必要がある内部 VLAN サービス クラス ID。CoS ID は、0 ～ 7 の範囲の整数です。	IOS デバイスにのみ適用されます。
E-Type	サービスを指定された EtherType のフレームのみ伝送するように制限します。 <ul style="list-style-type: none"> • IPv4 • IPv6 • PPPoE-All • PPPoE-Discovery • PPPoE-Session 	IOS デバイスにのみ適用されます。

属性	説明	その他の情報
定義書き換えアクション (Rewrite Definition Action)	<p>フレームが UNI に入ったときに実行するカプセル化調整。</p> <ul style="list-style-type: none"> なし ポップ (Pop) : 入力フレームから 1 個または 2 個の VLAN タグを削除し、出力で追加します。 プッシュ (Push) : 入力フレームから 1 個または 2 個の VLAN タグ (Dot1q または Dot1ad タグ) を追加し、出力で削除します。 変換 (Translate) : VLAN タグを新しい VLAN タグ (Dot1q または Dot1ad タグ) で置き換えます。変換は、1:1、1:2、2:1、または 2:2 です。 	変換アクションは、IOS-XR デバイスにのみ適用されます。

サービス OAM

サービス レベルで、EVC のモニタリングとトラブルシューティングを可能にする EOAM (Ethernet Operations, Administration and Management) パラメータを定義できます。実際には、EVC のエンドポイント上の接続障害管理 (CFM) コンポーネントを設定することになります。

ポイントツーポイント EVC では、一方向 (UNI A から UNI Z へなど) または双方向で OAM パラメータを定義できます。マルチポイント EVC では、送信元と送信先の MEP グループを定義してから、EVC エンドポイントを特定の MEP グループに関連付けることができます。

CFM の詳細とデバイス レベルの CFM 設定については、[EOAM の障害とパフォーマンスのモニタリングを設定する](#)を参照してください。

次のように、プロビジョニング ウィザードの [カスタマー サービスの詳細 (Customer Service Details)] ページの [サービス OAM (Service OAM)] セクションを使用して、モニタするサービス フレームの仕様を定義し、そのフレームに適用する OAM プロファイルを定義します。

- [送信元 (From)] : EVC を経由するトラフィック フローの送信元。
- [送信先 (To)] : EVC を経由するトラフィック フローの送信先。
- [方向 (Direction)] (E ツリーのみ) : リーフとルート間またはルートからルートへのトラフィック フローの方向。



(注) [送信元 (From)] フィールドと [送信先 (To)] フィールドに入力すると、MEP グループ、つまり、順序付けされた UNI のセットが作成されます。ウィザードの次のページで、UNI をこれらの MEP グループの 1 つに関連付けます。

- [CoS] : フレームに関連付ける必要のあるサービス クラス識別子。
- [OAM プロファイル (OAM Profile)] : パフォーマンス モニタリングを有効にするためにフレームに適用する必要のある OAM 属性のセット。次の OAM プロファイルを選択に使用できます。

- パフォーマンスモニタリング1：コミュニティチェックと合成損失測定を有効にします。このプロファイルは、ポイントツーポイントとマルチポイントの両方の EVC をサポートします。
- [パフォーマンス モニタリング 2 (Performance Monitoring 2)]：コミュニティチェック、合成損失測定、およびシングルエンド遅延測定を有効にします。このプロファイルは、ポイントツーポイントとマルチポイントの両方の EVC をサポートします。
- [パフォーマンス モニタリング 3 (Performance Monitoring 3)]：コミュニティチェック、合成損失測定、およびデュアルエンド遅延測定を有効にします。このプロファイルは、ポイントツーポイントとマルチポイントの両方の EVC をサポートします。
- [パフォーマンス モニタリング 3 (Performance Monitoring 3)]：コミュニティチェック、合成損失測定、およびデュアルエンド遅延測定を有効にします。このプロファイルは、フレームサイズ 64 (損失および遅延)、履歴間隔 2 (遅延) および 5 (損失)、集約間隔 60 をサポートします。
- [パフォーマンス モニタリング 4 (Performance Monitoring 4)]：コミュニティチェック、合成損失測定、およびデュアルエンド遅延測定を有効にします。このプロファイルは、フレームサイズ 152 (損失および遅延)、履歴間隔 10、集約間隔 300 (5 分間のサンプル) をサポートします。
- [コミュニティチェック間隔 (Continuity Check Interval)]：コミュニティチェックメッセージの間隔。

UNI としてのデバイスおよびインターフェイスの設定

ユーザネットワークインターフェイス (UNI) は、サブスクライバ (カスタマーエッジ (CE)) の責任とサービスプロバイダー (プロバイダーエッジ (PE)) の責任とを分ける、物理的な責任分界点です。

UNI は EVC のエンドポイントの境界を定めるため、デバイスのインターフェイスを UNI として設定することは、VC プロビジョニングで不可欠の部分となります。UNI は、VC の作成時に設定できます。あるいは、VC の作成とは別の UNI を設定することもできます。設定した UNI は、VC の作成時に使用可能になります。

UNI を設定するには、次の手順に従います。

- ステップ 1 新規キャリアイーサネット EVC の作成およびプロビジョニング (13 ページ) の説明に従って、プロビジョニングウィザードにアクセスします。
- ステップ 2 [テクノロジーの選択 (Select Technology)] ドロップダウンリストから **Carrier Ethernet** を選択します。
- ステップ 3 [サービスタイプ (Service Types)] リストから **UNI** を選択します。
- ステップ 4 **Next** をクリックして [カスタマーサービスの詳細 (Customer Service Details)] ページに移動します。
- ステップ 5 UNI の一意の名前と説明を入力し、必要に応じて顧客を関連付けます。
- ステップ 6 UNI のサービス属性を次のように定義します。

- [すべてを 1 つにバンドル (All to One Bundling)]：UNI を VC 専用にするポートベースの VC の場合。有効にすると、すべての CE-VLAN ID が 1 つの VC にバンドルされます。[すべてを 1 つにバン

ドル (All to One Bundling)] を選択すると、[多重化 (Multiplexing)] と [バンドリング (Bundling)] は選択できなくなります。

- [サービス多重化 (Service Multiplexing)] : UNI を複数の VC で共有する VLAN ベースの VC の場合、有効にすると、UNI を複数の EVC インスタンスに参加させることができます。
- [バンドリング (Bundling)] : UNI に複数の VLAN を使用することができます。複数 CE-VLAN ID が 1 つの EVC にバンドルされます。

- ステップ 7** [展開 (Deploy)] で、完了時にただちに UNI を展開するか、デバイスに展開する前に CLI のプレビューを表示するかを選択します。
- ステップ 8** **Next** をクリックして [UNI の詳細 (UNI Details)] 定義ページに移動します。
- ステップ 9** UNI として設定するデバイスとポートを選択します。
- ステップ 10** [新規 UNI の詳細リファレンス \(23 ページ\)](#) の説明に従って、UNI の属性を設定します。
- ステップ 11** **Submit** をクリックします。完了時に回線を展開するように選択していた場合は、ジョブが作成され、必要な CLI がデバイスに展開されます。実際にデバイスに展開する前に CLI のプレビューを表示することを選択した場合、この時点でプレビューが表示されます。CLI を確認します。属性のいずれかを変更する場合は、[属性の編集 (Edit Attributes)] をクリックします。それ以外の場合は、**Deploy** をクリックします。

デバイスとインターフェイスを ENNI として設定する

External Network to Network Interface (ENNI) は、各オペレータ ネットワークが別々の管理認証局の制御下にある 2 つの Metro Ethernet Network (MEN) 間のインターフェイスである参照ポイントを指定します。ENNI は、サービスの特性を維持しながら、複数のオペレータ MEN 全体でのイーサネットサービスの拡張をサポートするように設計されています。

E アクセス VC をプロビジョニングする場合は、隣接するネットワーク経由でトラフィックを伝送する ENNI を定義する必要があります。ENNI の設定は VC 作成プロセスで行うことができます。または、VC 作成とは無関係に ENNI を設定できます。このような ENNI は VC 作成中に選択できます。

ENNI を設定するには、次の手順を実行します。

- ステップ 1** [新規キャリアイーサネット EVC の作成およびプロビジョニング \(13 ページ\)](#) の説明に従って、プロビジョニング ウィザードにアクセスします。
- ステップ 2** [テクノロジーの選択 (Select Technology)] ドロップダウンリストから **Carrier Ethernet** を選択します。
- ステップ 3** [サービス タイプ (Service Types)] リストから **ENNI** を選択します。
- ステップ 4** **Next** をクリックして [カスタマー サービスの詳細 (Customer Service Details)] ページに移動します。
- ステップ 5** ENNI の一意の名前と説明を入力し、必要に応じて、顧客/オペレータに関連付けます。
- ステップ 6** [展開 (Deploy)] で、ENNI を完了時にすぐに展開するか、最初にデバイスに展開する CLI のプレビューを表示するかを選択します。

ステップ7 **Next** をクリックして、[ENNI の詳細 (ENNI Details)] 定義ページに移動します。

ステップ8 ENNI として設定するデバイスとポートを選択します。

ステップ9 ENNI に関する次のパラメータを定義します。

- **MTU** : インターフェイスを通過するパケットのバイト単位の最大伝送サイズ。ENNI の MTU は 1526 より大きくする必要があります。
- **速度** : これがサポートされている場合、必要に応じて、ポートの速度を抑えることができます。

ステップ10 **Submit** をクリックします。完了時に回線を展開するように選択していた場合は、ジョブが作成され、必要な CLI がデバイスに展開されます。実際にデバイスに展開する前に、CLI のプレビューを表示するように選択していた場合は、ここでプレビューが表示されます。CLI を確認します。属性のいずれかを変更する場合は、[属性の編集 (Edit Attributes)] をクリックします。それ以外の場合は、**Deploy** をクリックします。

セグメントルーティング

セグメントルーティングの設定

セグメントルーティング (SR) は、送信元ルーティングを実行するための柔軟でスケーラブルな方法です。送信元ルータは、明示的パスまたは内部ゲートウェイプロトコル (IGP) 最短パスのいずれかを選択し、パケットヘッダー内のパスをセグメントの順序付きリストとしてエンコードします。セグメントは、ネットワークの宛先への完全なルートを形成するためにルータを組み合わせることができるサブパスを表しています。各セグメントは、新しい IGP 拡張機能を使用してネットワーク全体に配布されるセグメント識別子 (SID) で識別されます。

各ルータ (ノード) と各リンク (隣接関係) には関連付けられた SID があります。ノードセグメント識別子はグローバルに一意であり、IGP で決定されたルータへの最短パスを表します。ネットワーク管理者は各ルータに予約されたブロックからノード ID を割り当てます。一方、隣接関係セグメント ID はローカルで有効なものであり、出力インターフェイスなどの隣接ルータに固有の隣接関係を表します。ルータは、ノード ID の予約済みブロック外の隣接関係識別子を自動的に生成します。MPLS ネットワークでは、セグメント識別子は MPLS ラベルスタックエントリとしてエンコードされます。セグメント ID は指定したパスに沿ってデータを移動します。ノードセグメントはマルチホップパスを使用できますが、隣接関係セグメントはワンホップパスです。



(注) SR ポリシー視覚化オーバーレイは、サブインターフェイスではサポートされていません。

セグメントルーティングポリシーの作成とプロビジョニング

SR ポリシーを作成し、プロビジョニングするには、次の手順を実行します。

始める前に

SR ポリシーのプロビジョニングの前に、次の前提条件が満たされていることを確認します。

- デバイス上とルータプロトコルレベル (ISIS / OSPF) で MPLS TE が有効になっている。
- SR-TE は、traffic-eng の優先オプションとして設定されていなければならない。
- ブロックレベルとループバックインターフェイスのラベル割り当て

-
- ステップ 1** 左側のプレーンで、[マップ (Maps)] > [トポロジマップ (Topology Maps)] > [ネットワークトポロジ (Network Topology)] を選択します。
- ステップ 2** ツールバーで [デバイスグループ (Device Group)] ボタンをクリックし、マップに表示されるデバイスのグループを選択します。
- ステップ 3** [回線/VC (Circuits/VCs)] タブで、[+] アイコンをクリックします。これにより、マップの右側に新しいペインが開き、[プロビジョニングウィザード (Provisioning Wizard)] が表示されます。
- ステップ 4** [テクノロジー (Technology)] ドロップダウンリストで **Segment Routing** を選択すると、Cisco EPN Manager は [サービスタイプ (Service Type)] 領域に関連する回線/VC タイプのリストを表示します。
- ステップ 5** [サービスタイプ (Service Type)] リストで、[SR ポリシー (SR Policy)] を選択します。
- ステップ 6** さまざまなサービスの属性を設定するプロファイルを定義している場合、[プロファイルの選択 (Select Profile)] ドロップダウンリストから必要なプロファイルを選択します。[回線/VC プロファイル \(134 ページ\)](#) を参照してください。
- ステップ 7** **Next** をクリックして [サービスの詳細 (Service Details)] ページに移動します。
- ステップ 8** (オプション) ポリシーの作成対象の顧客を選択します。リストに顧客が表示されない場合は **Inventory > Other > Customers** に移動し、システムで顧客を作成してからプロビジョニングウィザードを再起動します。
- ステップ 9** サービスの詳細を入力します。
- サービスの詳細は、[Activate] チェックボックス、[Name]、および [Description] で構成されます。[Activate] チェックボックスを使用して、ポリシーの動作ステータスを [Up] または [Down] に設定します。
- ステップ 10** ポリシーの詳細を入力します。詳細については、[\[ポリシーの詳細 \(Policy Details\)\] のフィールドリファレンス : SR ポリシー \(32 ページ\)](#) を参照してください。
- ステップ 11** [自動ルートの設定 (Autoroute Settings)] の詳細を入力します。詳細については、[\[自動ルート設定の詳細 \(Autoroute Settings Details\)\] のフィールドリファレンス : SR ポリシー \(32 ページ\)](#) を参照してください。
- ステップ 12** [デプロイアクション (Deployment Action)] フィールドに、ポリシー作成プロセス終了時のアクションを指定します。実際に展開する前に、該当するデバイスに展開される設定のプレビューを表示するように指定することも、完了時にすぐに設定を展開するように指定することもできます。詳細については、[プロビジョニング順序の保存とスケジュール \(105 ページ\)](#) を参照してください。
- ステップ 13** **Next** をクリックして、[パスおよび制約の詳細 (Path and Constraint Details)] ページに移動します。
- ステップ 14** [候補パス (Candidate Paths)]、[パスの詳細 (Path Details)]、および [パスの制約の詳細 (Path Constraint Details)] を指定します。詳細については、[パスおよび制約の詳細のフィールド参照 : SR ポリシー \(33 ページ\)](#) を参照してください。

ステップ 15 **Next** をクリックし、[テンプレートの詳細 (Template Details)] ページに移動します。テンプレートの詳細については、[テンプレートを使用した回線/VC の拡張 \(138 ページ\)](#) を参照してください。

ステップ 16 [送信 (Submit)] をクリックします。選択した展開アクションに応じて、関連するアクションが実行されます。つまり、設定のプレビューを選択した場合は、設定を表示できるプレビューページが表示され、その後に [展開 (Deploy)] をクリックします。展開を選択した場合、設定は関連するデバイスに直接展開されます。

[ポリシーの詳細 (Policy Details)] のフィールドリファレンス : SR ポリシー

次の表に、セグメントルーティングポリシーを作成するためのポリシーの詳細を定義する属性のリストを示し、説明します。

表 4: [ポリシーの詳細 (Policy Details)] セクションの参照 : SR ポリシー

属性	説明
ポリシー名	ポリシー名を入力します。
ヘッドエンド (Head End)	ドロップダウンリストからヘッドエンドを選択します。
カラー	カラー値の範囲は 1 ~ 4294967295 です。
エンドポイント (End Point)	ドロップダウンリストからエンドポイントを選択します。
明示的なバインド SID	明示的なバインド SID (Explicit Binding SID) の範囲は 16 ~ 1048575 です。
帯域幅 (Bandwidth)	帯域幅の値の範囲は [帯域幅の単位 (Bandwidth Unit)] フィールドで選択した値によって異なります。
帯域幅の単位 (Bandwidth Unit)	ドロップダウンリストから値を選択します。使用可能なオプションは、[Kbps]、[Mbps]、および [Gbps] です。



(注) [帯域幅 (Bandwidth)] フィールドと [帯域幅の単位 (Bandwidth Unit)] フィールドは [ダイナミックとPCE (Dynamic With PCE)] パスタイプにのみ適用されます。

[自動ルート設定の詳細 (Autoroute Settings Details)] のフィールドリファレンス : SR ポリシー

次の表に、セグメントルーティングポリシーを作成するための自動ルート設定の詳細を定義する属性のリストを示し、説明します。

表 5: [自動ルート設定の詳細 (Autoroute Settings Details)] セクションの参照：SR ポリシー

属性	説明
自動メトリックモード (Auto Metric Mode)	ドロップダウンリストから値を選択します。使用可能なオプションは [一定 (Constant)] および [相対 (Relative)] です。
自動メトリック値 (Auto Metric Value)	[自動メトリックモード (Auto Metric Mode)] フィールドで選択した値に応じて、自動メトリック値 (Auto Metric Value) の範囲が変わります。[一定 (Constant)] の場合、範囲は 1 ~ 2147483647 です。[相対 (Relative)] の場合、範囲は -10 ~ 10 です。
すべてのプレフィックスを許可 (Allow All Prefixes)	すべての IP プレフィックスを許可する場合は、このチェックボックスをオンにします。
許可プレフィックス (Allowed Prefixes)	このフィールドは [すべてのプレフィックスを許可 (Allow All Prefixes)] チェックボックスをオンにしていない場合のみ表示されます。必要なプレフィックスをテーブルに追加します。

パスおよび制約の詳細のフィールド参照：SR ポリシー

次の表に、セグメントルーティング ポリシーを作成するためのパス制約の詳細を定義する属性のリストを示し、説明します。

表 6: [パス制約の詳細 (Path Constraint Details)] セクションの参照：SR ポリシー

属性	説明
候補パス (Candidate Paths)	
Path Type	SR ポリシーに必要なパスを選択します。値は、[ダイナミック (Dynamic)]、[明示的 (Explicit)]、および [ダイナミックとPCE (Dynamic With PCE)] です。
設定	候補パスの設定値の範囲は 1 ~ 65535 です。
[ダイナミック (Dynamic)] および [ダイナミックとPCE (Dynamic With PCE)] パスタイプのパスの詳細：	
メトリックタイプ	必要な [メトリックタイプ (Metric Type)] を選択します。値は、[IGP]、[遅延 (Latency)]、[TE]、および [ホップ数 (HopCount)] です。
メトリックマージンタイプ (Metric Margin Type)	必要な [メトリックマージンタイプ (Metric Margin Type)] を選択します。値は [絶対 (Absolute)] および [相対 (Relative)] です。
メトリックマージン値 (Metric Margin Value)	[メトリックマージン値 (Metric Margin Value)] の範囲は 0 ~ 2147483647 です。

属性	説明
SID の上限 (Max SID Limit)	[SIDの上限 (Max SID Limit)] は 1 ~ 255 です。
[明示的 (Explicit)] パスタイプのパスの詳細 :	
新しいセグメントリスト (New Segment List)	新しいセグメントリストを作成する場合は、このチェックボックスをオンにします。
セグメントリスト名 (Segment List Name)	このフィールドは [新しいセグメントリスト (New Segment List)] チェックボックスがオンになっている場合に表示されます。
既存のセグメントリスト (Existing Segment List)	このフィールドは [New Segment List] チェックボックスがオフになっている場合に表示されます。ドロップダウンリストからセグメントリストを選択します。
Weight	重みの範囲は 1 ~ 4294967295 です。
<p>(注) パスの詳細を入力する場合は、[+] アイコンをクリックし、[セグメントリスト名 (Segment List Name)] と [重み (Weight)] を入力して、セグメントリストに詳細を追加する必要があります。</p> <p>[新しいセグメントリスト (New Segment List)] チェックボックスがオンになっている場合は、セグメントテーブルがアクティブになり編集できます。</p> <ul style="list-style-type: none"> • [+] をクリックしてセグメントを追加できます。[インデックス (Index)] の値を入力し、[デバイス (Device)]、[セグメントタイプ (Segment Type)]、および [インターフェイス (Interface)] をそれぞれのドロップダウンリストから選択します。 • セグメントを複数追加した場合は、セグメントウィンドウで上矢印または下矢印を使用して目的のキューに配置できます。 • セグメントを作成中の場合にのみ、セグメントウィンドウでセグメントを編集または削除することもできます。作成したセグメントリストは、その後変更できません。 • また、ラベルが割り当てられていないインターフェイスにラベルを割り当てることもできます。 	
パスの制約の詳細 (Path Constraint Details)	
アフィニティ操作 (Affinity Operation)	適切なアフィニティ操作を個別に選択し、関連する詳細を指定します。値は、[いずれかを除外する (Exclude-Any)]、[いずれかを含める (Include-Any)]、および [すべて含める (Include-All)] です。

属性	説明
いずれかのアフィニティ名を除外する (Exclude Any Affinity Names)	ドロップダウンリストから名前を選択します。
いずれかのアフィニティ名を含める (Include Any Affinity Names)	このフィールドは[いずれかを含める (Include-Any)]が選択されている場合に表示されます。ドロップダウンリストから、追加するアフィニティ名を選択します。
すべてのアフィニティ名を含める (Include All Affinity Names)	このフィールドは[すべて含める (Include-All)]が選択されている場合に表示されます。ドロップダウンリストから、追加するアフィニティ名を選択します。
SID アルゴリズム (SID Algorithm)	[SIDアルゴリズム (SID Algorithm)] の範囲は 128 ~ 255 です。
ディスジョイントグループのタイプ (Disjoint Group Type)	ドロップダウンリストから値を選択します。値は、[リンク (Link)]、[ノード (Node)]、[Srlg]、および [Srlg-Node] です。
ディスジョイントグループ ID (Disjoint Group Id)	[グループIDの分離 (Disjoint Group Id)] の範囲は 1 ~ 65535 です。
ディスジョイントサブグループ ID (Disjoint Sub Group Id)	[ディスジョイントサブグループID (Disjoint Sub Group Id)] の範囲は 1 ~ 65535 です。

セグメントルーティングポリシーを使用したキャリアイーサネットサービスの作成とプロビジョニング

Cisco EPN Manager は、セグメントルーティングトラフィックエンジニアリング (SR-TE) ポリシーを使用して、EPL のプロビジョニング、EVPL、アクセス EPL、アクセス EVPL キャリアイーサネットのポイントツーポイントサービスをサポートしています。CE サービスの変更時に SR-TE ポリシーを変更できます。回線/VC 360* の [関連回線/VC (Related Circuits/VC)] タブを使用して、このサービスに関連付けられた SR ポリシーを表示できます。SR ポリシーの場合、バックアップパスの可視化はオーバーレイで使用できます。[バックアップパスの表示 (Show Backup Path)] を展開し、除外するノードまたはリンクを選択できます。[適用 (Apply)] をクリックすると、新しいバックアップパスが表示されます。

SR ポリシーを使用して EVPL サービスを作成およびプロビジョニングするには、次の手順を実行します。

- ステップ 1** 左側のプレーンで、[マップ (Maps)]>[トポロジマップ (Topology Maps)]>[ネットワーク トポロジ (Network Topology)]を選択します。
- ステップ 2** ツールバーで[デバイス グループ (Device Group)] ボタンをクリックし、マップに表示するデバイスのグループを選択します。
- ステップ 3** [回線/VC (Circuits/VCs)] タブで、[+] アイコンをクリックします。これにより、マップの右側に新しいペインが開き、[プロビジョニング ウィザード (Provisioning Wizard)] が表示されます。
- ステップ 4** [テクノロジー (Technology)] ドロップダウンリストで **Carrier Ethernet** を選択すると、Cisco EPN Manager は [サービス タイプ (Service Type)] 領域に関連する回線/VC タイプのリストを表示します。たとえば、キャリアイーサネット サービス タイプには EPL、EVPL、EP-LAN などが含まれます。
- ステップ 5** [サービス タイプ (Service Type)] リストから、作成する回線/VC のタイプを選択します。たとえば、EVPL などです。
- ステップ 6** さまざまなサービスの属性を設定するプロファイルを定義している場合、[プロファイルの選択 (Select Profile)] ドロップダウン リストから必要なプロファイルを選択します。[回線/VC プロファイル \(134 ページ\)](#) を参照してください。
- ステップ 7** **Next** をクリックして [サービスの詳細 (Service Details)] ページに移動します。
- ステップ 8** (オプション) EVPL の作成対象顧客を選択します。リストに顧客が表示されない場合は **Inventory > Other > Customers** に移動し、システムで顧客を作成してからプロビジョニング ウィザードを再起動します。
- ステップ 9** サービスの詳細を入力します。フィールドと属性の説明については、[サービス詳細の参考資料 \(22 ページ\)](#) を参照してください。
- ステップ 10** [次へ (Next)] をクリックします。
- ステップ 11** [展開アクション (Deployment Action)] フィールドに、EVPL 作成プロセス完了時のアクションを指定します。実際に展開する前に、該当するデバイスに展開される設定のプレビューを表示するように指定することも、完了時にすぐに設定を展開するように指定することもできます。詳細については、[プロビジョニング順序の保存とスケジュール \(105 ページ\)](#) を参照してください。
- ステップ 12** **Next** をクリックして UNI を定義するページに移動します。E-Access の場合、ENNI を定義するページもあります。
- ステップ 13** UNI として機能するデバイスとインターフェイスを識別します。
- (注) エンドポイントのいずれかが、Cisco EPN Manager で管理されないデバイス上のインターフェイスである場合、[管理対象外 (Unmanaged)] チェックボックスをオンにして、その管理対象外デバイスの情報を入力します。[アンマネージド エンドポイントを使用した回線/VC のプロビジョニング \(137 ページ\)](#) を参照してください。
- ステップ 14** 新しい UNI を作成している場合は、新しい UNI の詳細を入力します。フィールドと属性の説明については、[新規 UNI の詳細リファレンス \(23 ページ\)](#) を参照してください。
- ステップ 15** UNI サービスの詳細を入力します。フィールドと属性の説明については、[UNI サービス詳細の参照 \(24 ページ\)](#) を参照してください。
- ステップ 16** エンドポイントのいずれかが、Cisco EPN Manager で管理されないデバイス上のインターフェイスである場合、[管理対象外 (Unmanaged)] チェックボックスをオンにして、その管理対象外デバイスの情報を入力します。詳細については、[アンマネージド エンドポイントを使用した回線/VC のプロビジョニング \(137 ページ\)](#) を参照してください。

- ステップ 17** H-VPLS をコア テクノロジーとして使用する E-LAN EVC および E-TREE EVC の場合、プライマリ ハブ とセカンダリ ハブとして機能するデバイスをそれぞれ選択します。
- ステップ 18** E 回線 EVC、E アクセス EVC の場合：[疑似回線の設定 (Pseudowire Settings)] ページで、次のようにして EVC が経由するセグメントルーティングの SR-TE ポリシーを選択できます。
1. [静的優先パス (Static Preferred Path)] チェックボックスをオンにして、サービスの静的ルートを割り当てます。
(注) E アクセスの場合、このチェックボックスは表示されません。
 2. [SR ポリシー (SR Policy)] オプション ボタンをクリックします。
 3. [優先パス (A-Z) (Preferred Path (A-Z))] および [優先パス (Z-A) (Preferred Path (Z-A))] ドロップダウンリストのそれぞれから SR-TE ポリシーを選択します。
(注) [優先パス (A ~ Z) (Preferred Path (A-Z))] と [優先パス (Z ~ A) (Preferred Path (Z-A))] はどちらもオプションのフィールドです。
 4. [新規キャリアイーサネット EVC の作成およびプロビジョニング \(13 ページ\)](#) でステップ 5 ~ 8 を繰り返します。
- ステップ 19** [新規キャリアイーサネット EVC の作成およびプロビジョニング \(13 ページ\)](#) でステップ 20 ~ 22 を繰り返します。

光/DWDM ネットワークの回線のプロビジョニング

- [Cisco EPN Manager 光/DWDM ネットワーク プロビジョニング サポートの概要 \(37 ページ\)](#)
- [光回線のプロビジョニングの前提条件 \(39 ページ\)](#)
- [OCH 回線の作成とプロビジョニング \(40 ページ\)](#)
- [NCS 1004 デバイスを直接接続する OCH トレール回線の作成とプロビジョニング \(49 ページ\)](#)
- [互いに異なる 2 つの OCH トレール UNI 回線の作成およびプロビジョニング \(51 ページ\)](#)
- [メディア チャネル グループ SSON 回線の作成とプロビジョニング \(53 ページ\)](#)
- [メディア チャネル SSON 回線の作成とプロビジョニング \(55 ページ\)](#)
- [OTN 回線の作成とプロビジョニング \(60 ページ\)](#)
- [ODU 回線の作成とプロビジョニング \(67 ページ\)](#)

Cisco EPN Manager 光/DWDM ネットワーク プロビジョニング サポートの概要

Cisco EPN Manager は、高密度波長分割多重 (DWDM) 光チャネル (OCH) の回線タイプのプロビジョニングをサポートします。DWDM の光技術は、既存の光ファイババックボーン上の帯域幅を広げるために使用されます。これは同じ光ファイバ上で異なる波長の複数の信号を同

時に結合して送信します。実際には、1つの光ファイバが複数の仮想光ファイバに変換されます。

Cisco EPN Manager は、次の光回線をサポートします。

- 高密度波長分割多重 (DWDM) 光チャネルの (OCH) 回線 : 以下は、光チャネルのさまざまな回線タイプです。
 - 光チャネル ネットワーク接続 (OCHNC) WSON : OCHNC WSON 回線は、指定された C バンド波長で2つの光ノード間の接続を確立します。詳細については、[Optical Channel Network Connection \(OCHNC\) WSON](#)を参照してください。
 - 光チャネル クライアント接続 (OCHCC) WSON : OCHCC WSON 回線は、OCHNC WSON を拡張して、送信元クライアントポートから TXP/MXP カードの接続先クライアントポートへの光接続を作成します。詳細については、[光チャネル クライアント接続 \(OCHCC\) WSON](#)を参照してください。
 - 光チャネル (OCH) トレール WSON : OCH トレール WSON 回線は、OCHCC WSON 回線を伝送します。詳細については、[光チャネル \(OCH\) トレール WSON](#)を参照してください。
 - NCS 1002、NCS 55xx、および ASR 9K デバイスを接続する光チャネル (OCH) トレール : この OCH トレール回線は、NCS 1002、NCS 55xx、または ASR 9K デバイスの送信元トランク ポートから別の同様なデバイスの宛先トランク ポートへの光接続を作成します。詳細については、[NCS 1002、NCS 55xx、および ASR 9K デバイスを接続する光チャネル \(OCH\) トレール](#)を参照してください。
 - 光チャネル (OCH) トレールのユーザ/ネットワーク間インターフェイス (UNI) : OCH トレールの UNI 回線は、Cisco NCS 2000 シリーズのデバイスと Cisco NCS 4000 シリーズのデバイス間の接続を確立します。詳細については、[光チャネル \(OCH\) トレールのユーザ/ネットワーク間インターフェイス \(UNI\)](#) を参照してください。
 - スペクトラム スイッチド光ネットワーク (SSON) : SSON 回線を使用すると、スパン内のより多くのチャンネルを表示できます。SSON 機能を使用すると、回線をメディア チャンネル グループ内に作成した場合に、回線が互いに近くに配置されます。詳細については、[Spectrum Switched Optical Network \(SSON\) 回線](#)を参照してください。
- 光トランスポート ネットワーク (OTN) : OTN 回線は、Resource Reservation Protocol (RSVP) シグナリングを使用して、イングレスとイーグレスのノード間に静的または動的に確立できます。詳細については、[光トランスポート ネットワーク \(OTN\) 回線](#)を参照してください。
 - 光チャネルデータユニットユーザ/ネットワーク間インターフェイス (ODU UNI) : ODU UNI 回線は、OTN アーキテクチャを経由する実際のエンドツーエンドのクライアントサービスを表します。詳細については、[光チャネルデータユニットのユーザ/ネットワーク間インターフェイス \(ODU UNI\)](#) を参照してください。

- 光チャネルデータユニット (ODU) トンネル : ODU トンネル回線は、ODU UNI を伝送します。詳細については、[光チャネルデータユニット \(ODU\) トンネル](#)を参照してください。
- 光チャネルデータユニット (ODU) を介した光チャネルペイロードユニット (OPU) : ODU を介した OPU 回線は、2つの顧客指定宅内間の高帯域幅のポイントツーポイント接続を提供します。これらの回線は、ODU UNI 回線を使用して、ネットワーク経由でクライアント信号を伝送します。詳細については、[Optical Channel Payload Unit \(OPU\) Over Optical Channel Data Unit \(ODU\)](#) を参照してください。
- 光チャネルデータユニットのユーザ/ネットワークインターフェイス (ODU UNI) ヘアピン : ODU UNI ヘアピン回線は ODU UNI 回線に似ていますが、管理プレーンで作成され、送信元と宛先は同じデバイスですが、インターフェイスが異なる内部ノード回線です。詳細については、[光チャネルデータユニットのユーザ/ネットワーク間インターフェイス \(ODU UNI\) ヘアピン](#)を参照してください。
- 光チャネルデータユニット (ODU) : 光チャネルデータユニット (ODU) は、OTU コントローラのサブコントローラとして作成されます。ODU には、光チャネルをサポートするメンテナンス機能と操作機能の情報が含まれています。詳細については、[光チャネルデータユニット \(ODU\)](#) を参照してください。

光回線のプロビジョニングの前提条件

以下は光回線をプロビジョニングするための前提条件です。

- Cisco EPN Manager は、Wavelength Switched Optical Network (WSON) 回線と非 WSON 回線の両方をサポートします。ただし、非 WSON 回線については、Cisco EPN Manager は回線オーバーレイ、回線 360 ビュー、マルチレイヤトレース ビュー、および回線の詳細が含まれる回線検出のみをサポートします。Cisco EPN Manager は、非 WSON 回線のプロビジョニング、アクティブ化、非アクティブ化、保護切り替えアクション、および変更をサポートしていません。
- デバイス間の通信は、光回線をプロビジョニングする前にセットアップする必要があります。
- 光回線をプロビジョニングするデバイスのインベントリ収集の状態は[完了 (Completed)] である必要があります。これを確認するには、[インベントリ (Inventory)] > [デバイス管理 (Device Management)] > [ネットワーク デバイス (Network Devices)] に移動し、[最後のインベントリ収集ステータス (Last Inventory Collection Status)] 列でステータスを確認します。
- DWDM グリッドユニットは、波長または周波数に設定する必要があります。これには、[管理 (Administration)] > [設定 (Settings)] > [システム設定 (System Settings)] > [回線/VC 表示 (Circuits/VCS Display)] を選択し、[DWDM グリッド単位 (DWDM Grid Unit)] エリアで [波長 (ナノメートル (nm)) (Wavelength (Nanometer (nm)))] または [周波数 (テラヘルツ (THz)) (Frequency (Terahertz (THz)))] を選択します。
- ソフトウェアバージョン 10.7 以降で動作している NCS 2000 シリーズのデバイスを使用して OCHNC またはメディアチャネル NC 回線をプロビジョニングする前に、シスコのトラ

nsポートコントローラ（CTC）または Cisco EPN Manager のいずれかで UNI 設定を必ず作成してください。

- 必要に応じて、システムに顧客を作成し、回線/VCの作成およびプロビジョニングプロセス中に顧客に回線/VCを関連付けられるようにする必要があります。左のサイドバーから **[インベントリ (Inventory)]** > **[その他 (Other)]** > **[顧客 (Customers)]** を選択して、顧客を作成および管理します。

OCH 回線の作成とプロビジョニング

OCH 回線をプロビジョニングするには、次の手順に従います。

始める前に

オプティカル回線をプロビジョニングする前の前提条件については、[光回線のプロビジョニングの前提条件 \(39 ページ\)](#) を参照してください。

-
- ステップ 1** 左側のサイドバーから、**[マップ (Maps)]** > **[トポロジ マップ (Topology Maps)]** > **[ネットワーク トポロジ (Network Topology)]** の順に選択します。
- ステップ 2** **[デバイス グループ (Device Groups)]** をクリックして、OCH 回線を作成する場所を選択します。
- ステップ 3** **[デバイス グループ (Device Groups)]** ポップアップ ウィンドウを閉じます。
- ステップ 4** **[ネットワーク トポロジ (Network Topology)]** ウィンドウで **[回線/VC (Circuits/VCs)]** をクリックします。
- ステップ 5** **[回線/VC (Circuits/VCs)]** タブをクリックし、**[回線/VC (Circuits/VCs)]** ペイン ツールバーで **[+]** (**[作成 (Create)]**) アイコンをクリックします。マップの右側の新しいペインでプロビジョニング ウィザードが開きます。
- プロビジョニング ウィザードを表示するもう 1 つの方法として、**[設定 (Configuration)]** > **[ネットワーク (Network)]** > **[サービス プロビジョニング (Service Provisioning)]** の順に選択する方法があります。
- ステップ 6** **[テクノロジー (Technology)]** ドロップダウン リストから **[光 (Optical)]** を選択すると、Cisco EPN Manager は関連する回線タイプのリストを **[サービス タイプ (Service Type)]** 領域に表示します。たとえば、OCH 回線の **[光 (Optical)]** サービスタイプには、**[OCHNC WSON]**、**[OCHCC WSON]**、**[OCH-Trail]**、**[OCH-Trail WSON]** および **[OCH-Trail UNI]** があります。
- ステップ 7** **[サービス タイプ (Service Type)]** エリアで、作成する OCH 回線のタイプを選択します。
- ステップ 8** さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、**[プロファイルの選択 (Select Profile)]** ドロップダウン リストから必要なプロファイルを選択します。[回線/VC プロファイル \(134 ページ\)](#) を参照してください。
- ステップ 9** **[次へ (Next)]** をクリックして **[顧客セクション (Customer Section)]** ページに移動します。
- ステップ 10** (オプション) 回線の作成対象顧客を選択します。リストに顧客が表示されない場合は、**[インベントリ (Inventory)]** > **[その他 (Other)]** > **[顧客 (Customers)]** の順に移動し、システムで顧客を作成してから、プロビジョニング ウィザードを再起動します。
- ステップ 11** **[顧客セクション (Customer Section)]** ページに回線名とその説明を入力します。
- ステップ 12** **[次へ (Next)]** をクリックして **[回線セクション (Circuit Section)]** ページに移動します。

(注) 光サービスタイプとして OCH-Trail UNI を選択すると、[エンドポイントセクション (Endpoint Section)] ページが最初に表示され、その後 [回線セクション (Circuit Section)] ページが表示されます。

ステップ 13 回線の詳細を入力します。フィールドと属性の説明については、**OCH 回線タイプの [回線 (Circuit)] セクションリファレンス (42 ページ)** を参照してください。

ステップ 14 [次へ (Next)] をクリックして [エンドポイントセクション (Endpoint Section)] ページに移動します。

ステップ 15 [帯域幅 (Bandwidth)] ドロップダウンリストから帯域幅を選択します。

ステップ 16 [エンドポイント (Endpoint)] テーブルの行を選択し、マップでデバイスをクリックします。選択したデバイスの名前が [デバイス名 (Device Name)] 列に読み込まれます。[エンドポイント (Endpoint)] テーブルの行をクリックして、[デバイス名 (Device Name)]、[終端ポイント (Termination Point)]、[ポートの追加/ドロップ (Add/Drop Port)]、[OCH トレール (OCH-Trail)]、および [サイド (Side)] の各列を編集することもできます。[サイド (Side)] 列は、選択したポートに基づいて自動的に設定されます。選択した回線タイプと互換性があり、使用可能なネットワーク要素だけが表示されます。

同じ FEC モードのエンドポイントを選択します。異なる FEC モードのエンドポイントを選択すると、エラーメッセージが表示されます。

(注) [ポートの追加 (Add Port)] 列と [ポートのドロップ (Drop Port)] 列は、OCHNC WSON 回線の場合にのみ使用可能です。[ポートの追加 (Add Port)] 列に追加する必要があるポートを選択すると、[ポートのドロップ (Drop Port)] 列と [サイド (Side)] 列の値が自動的に設定されます。また、[ポートのドロップ (Drop Port)] 列の値を手動で編集することもできます。

ステップ 17 OCH 回線のトレールの多様性を選択します。作成する OCH 回線と選択するトレールは異なります。

(注) 作成したトレールの多様性を変更または削除することはできません。

ステップ 18 [次へ (Next)] をクリックして [制約セクション (Constraints Section)] ページに進みます。

ステップ 19 マップでデバイスノードまたはリンクをクリックし、[制約 (Constraints)] テーブルに追加します。あるいは、テーブルツールバーで「+」ボタンをクリックし、新しい行をテーブルに追加し、[ノード/リンク名 (Node/Link Name)]、[包含/除外 (Include/Exclude)]、および [ルート (Route)] 列を編集することもできます。選択した回線タイプと互換性があるネットワーク要素とリンクだけが表示されます。

(注) 行が編集モードになっている場合は、マップのデバイスまたはリンクをクリックして [制約 (Constraints)] テーブルの列にデータを読み込むことはできません。OCHCC トレール WSON 回線には、次のルートの制約条件が適用されます。

- 変更されたルートの制約事項は、すぐには回線に適用されませんが、再ルーティングが必要になる場合があります。ただし、変更は次のルート操作または復元時に適用されます。
- [回線オーバーレイ (Circuit Overlay)] には現在のルートに適用可能な制約事項のみが表示され、**回線の編集**ウィザードには現在設定されている制約事項が表示されます。
- **回線の編集**ウィザードには、回線オーバーレイを使用して表示される制約事項アイコンとは異なる制約事項を表示する制約事項テーブルが含まれています。

OCH 回線タイプの [回線 (Circuit)] セクションリファレンス

- 回線の変更中に、ドロップダウンリストから [アクションの再ルーティング (Reroute Actions)] を選択できます。リストから [なし (None)]、[動作パス (Working Path)]、または [保護パス (Protection path)] を選択できます。
- 関連する OTS リンクを作業パスに含めたり除外したりするには、ソースリンクターミネーションポイントを選択し、光学次数を制約として OTS リンクターミネーションポイントを選択します。たとえば、3つのノード (A、B、およびC) がすべて接続されており、回線の送信元ノードと宛先ノードがそれぞれ A と B である 3 ノードトポロジについて考えてみます。B と C を接続する作業パスリンクを含める場合は、制約を選択するときに、C に接続する光学次数とともにリストされているリンクターミネーションポイントを選択します。たとえば、ノード B の光学次数 1 を使用して C を接続する場合、制約として B-1 を選択します。このシナリオは、作業パスにリンクを含めるか除外する場合に適用できます。

ステップ 20 [次へ (Next)] をクリックして [異種波長セクション (Alien Wavelength Section)] ページに移動します。送信元ノードと宛先ノードのカード、トランクモード、FEC モードなどの現在の異種波長の設定が表示されます。送信元ノードと宛先ノードの異種波長に新しい設定を作成できます。

(注) [異種波長セクション (Alien Wavelength Section)] は、OCHNC WSON 回線を作成する場合のみ使用できます。

ステップ 21 [今すぐ作成 (Create Now)] をクリックして回線を作成します。デバイスに展開する前に TL1 または CLI コマンドのプレビューを表示することを選択した場合、[プレビュー (Preview)] をクリックするとプレビューが表示されます。この場合、設定をデバイスに展開するかキャンセルするかを選択できますが、属性を編集することはできません。

ステップ 22 [ネットワークトポロジ (Network Topology)] ウィンドウの [回線/VC (Circuits/VCs)] ペインのリストに、回線が追加されます。プロビジョニング状態を確認するには、回線/VC 名の横にある [i] アイコンをクリックし、[回線/VC 360 (Circuit/VC 360)] ビューを表示します。

OCH 回線タイプの [回線 (Circuit)] セクションリファレンス

次の表に、OCH 回線タイプを定義する属性とその説明をリストします。

表 7: 回線 (Circuit) セクションリファレンス : OCH 回線タイプ

属性	説明	有効
[回線詳細 (Circuit Details)]		
ラベル (Label)	回線を識別する一意の名前。	
状態	<p>回線の管理状態。値は次のとおりです。</p> <ul style="list-style-type: none"> • [サービス中 (In Service)] : 回線はサービス中で、トラフィックを伝送できます。 • [サービス停止中 (Out of Service)] : 回線が停止し、トラフィックを伝送できません。 	すべての OCH 回線タイプ。

属性	説明	有効
双方向	双方向回線を作成するには、このチェックボックスをオンにします。	OCHCC WSON および OCH Trail WSON 回線タイプ。
[アクティベーションの待機 (Wait For Activation)]	回線アクティベーションの設定時間を待機するには、このチェックボックスをオンにします。	OCHCC WSON および OCH Trail WSON 回線タイプ。
Protection	<p>回線の保護機構。Cisco EPN Manager は、選択した回線タイプに基づいて、次の保護メカニズムをサポートします。</p> <ul style="list-style-type: none"> • [なし (None)] : 保護されていない回線の場合、この値はすべての OCH 回線タイプに使用できます。 • [PSM] : 保護スイッチモジュール (PSM) カードが TXP カードに接続されている場合。この値は、回線タイプが OCHNC WSON または OCHCC WSON であるときに使用できます。 • [Y字型ケーブル (Y-Cable)] : トランスポンダまたはマックスポンダカードが回線を保護する場合。この値は回線タイプが OCHCC WSON であるときに使用できます。 • [スプリッタ (Splitter)] : MXPP/TXPP カードが使用されている場合。回線の送信元と宛先は、MXPP_MR_2.5G カードおよび TXPP_MR_2.5G カード上にあります。これらのカードは、スプリッタ (回線レベル) の保護 (通常は TXPP または MXPP トランスポンダカード上のトランク保護) を提供します。この値は回線タイプが OCHCC WSON であるときにのみ使用できます。 	OCHNC WSON 回線タイプ。
[ルート プロパティ (Route Properties)]		
[トンネルと異なる (Diverse From Tunnel)]	トンネルを選択し、プロビジョニングする回線でそのトンネルが使用されないことを確認します。これにより、トンネルに障害がある場合に、同じトンネルが他の回線で使用されなくなります。	[相互ダイバーシティ (Mutual Diversity)] チェックボックスがオフの場合の OCH-Trail UNI 回線タイプ。

属性	説明	有効
検証	<p>回線の検証モード。値は次のとおりです。</p> <ul style="list-style-type: none"> • [フル (Full)] : 回線の検証結果が承認しきい値以上になると回線が作成されます。 • [なし (None)] : 承認しきい値を考慮せずに回線が作成されます。 	すべての OCH 回線タイプ。
[承認しきい値 (Acceptance Threshold)]	<p>OCH 保護回線に設定された保護承認しきい値。値は次のとおりです。</p> <ul style="list-style-type: none"> • [緑 (Green)] : 復元失敗の危険性が 0% であることを示します。 • [黄 (Yellow)] : 復元失敗の危険性が 0% ~ 16% の間であることを示します。 • [オレンジ (Orange)] : 復元失敗の危険性が 16% ~ 50% の間であることを示します。 • [赤 (Red)] : 復元失敗の危険性が 50% を超えていることを示します。 	[検証 (Validation)] フィールドが [フル (Full)] に設定されている場合のすべての OCH 回線タイプ。
[保護の承認しきい値 (Protect Acceptance Threshold)]	<p>OCH 保護回線に設定された保護承認しきい値。値は次のとおりです。</p> <ul style="list-style-type: none"> • [緑 (Green)] : 復元失敗の危険性が 0% であることを示します。 • [黄 (Yellow)] : 復元失敗の危険性が 0% ~ 16% の間であることを示します。 • [オレンジ (Orange)] : 復元失敗の危険性が 16% ~ 50% の間であることを示します。 • [赤 (Red)] : 復元失敗の危険性が 50% を超えていることを示します。 	<p>次の場合の OCHNC WSON 回線タイプ:</p> <ul style="list-style-type: none"> • [保護 (Protection)] フィールドが [PSM]、[Y 字型ケーブル (Y-Cable)]、または [スプリッタ (Splitter)] に設定されている。 • [検証 (Validation)] フィールドが [フル (Full)] に設定されている。
[パスアラームを無視 (Ignore Path Alarms)]	パスアラームを無視するには、このチェックボックスをオンにします。	OCHCC WSON、OCHNC WSON、および OCH-Trail WSON 回線タイプ。

属性	説明	有効
[再生成を許可 (Allow Regeneration)]	ネットワーク要素が信号を再生成できるようにするには、このチェックボックスをオンにします。	すべての OCH 回線タイプ。
[復元 (Restoration)]	障害が発生した OCH 回線を新しいルートに復元するには、このチェックボックスをオンにします。	すべての OCH 回線タイプ。
[プライオリティ (Priority)]	障害が発生した OCH 回線の復元操作に優先順位を付けます。値は [高 (High)]、[プライオリティ 1 (Priority 1)]、[プライオリティ 2 (Priority 2)]、[プライオリティ 3 (Priority 3)]、[プライオリティ 4 (Priority 4)]、[プライオリティ 5 (Priority 5)]、[プライオリティ 6 (Priority 6)]、および [低 (Low)] です。	[復元 (Restoration)] チェックボックスがオンの場合のすべての OCH 回線タイプ。
[復元の検証 (Restoration Validation)]	復元操作の検証モード。値は次のとおりです。 <ul style="list-style-type: none"> • [なし (None)] : 復元の承認しきい値を考慮せずに回線が作成されます。 • [継承 (Inherited)] : 復元される回線は、プライマリ回線から検証と承認のしきい値を継承します。 • [フル (Full)] : 復元の検証結果が復元の承認しきい値以上になると回線が作成されます。 	[復元 (Restoration)] チェックボックスがオンの場合のすべての OCH 回線タイプ。
[復元の承認しきい値 (Restoration Acceptance Threshold)]	OCH 回線の復元操作に設定された承認しきい値。値は次のとおりです。 <ul style="list-style-type: none"> • [緑 (Green)] : 復元失敗の危険性が 0% であることを示します。 • [黄 (Yellow)] : 復元失敗の危険性が 0% ~ 16% の間であることを示します。 • [オレンジ (Orange)] : 復元失敗の危険性が 16% ~ 50% の間であることを示します。 • [赤 (Red)] : 復元失敗の危険性が 50% を超えていることを示します。 	次の場合のすべての OCH 回線タイプ : <ul style="list-style-type: none"> • [復元 (Restoration)] チェックボックスがオンになっている。 • [復元検証 (Restoration Validation)] フィールドが [フル (Full)] に設定されている。

属性	説明	有効
[復元保護の承認しきい値 (Restoration Protect Acceptance Threshold)]	<p>OCH 回線の復元操作に設定された保護の承認しきい値。値は次のとおりです。</p> <ul style="list-style-type: none"> • [緑 (Green)] : 復元失敗の危険性が 0 % であることを示します。 • [黄 (Yellow)] : 復元失敗の危険性が 0 % ~ 16 % の間であることを示します。 • [オレンジ (Orange)] : 復元失敗の危険性が 16 % ~ 50 % の間であることを示します。 • [赤 (Red)] : 復元失敗の危険性が 50 % を超えていることを示します。 	<p>次の場合の OCHNC WSON 回線タイプ:</p> <ul style="list-style-type: none"> • [保護 (Protection)] フィールドが [PSM]、[Y 字型 ケーブル (Y-Cable)]、または [スプリッタ (Splitter)] に設定されている。 • [復元 (Restoration)] チェックボックスがオンになっている。 • [復元検証 (Restoration Validation)] フィールドが [フル (Full)] に設定されている。
[元に戻す (Revert)]	<p>障害が修正された後、復元されたパスから元のパスに回線に戻します。値は [なし (None)]、[手動 (Manual)]、および [自動 (Automatic)] です。</p>	<p>[復元 (Restoration)] チェックボックスがオンになっている場合の OCHCC WSON、OCHNC WSON、OCH-Trail、および OCH-Trail WSON 回線タイプ。</p>

属性	説明	有効
[ソーク時間 (Soak Time)]	障害が修正された後、元のパスに切り替わるまでに、復元されたパス上の回線が待機する期間。	[元に戻す (Revert)] が [手動 (Manual)] または [自動 (Automatic)] に設定されている場合の OCHCC WSON、OCHNC WSON、OCH-Trail、および OCH-Trail WSON 回線タイプ。
[管理状態 (Admin State)]	回線の管理状態として [アップ (Up)] または [ダウン (Down)] を選択します。これは、回線の動作可能性に影響を及ぼし、回線を有効化するか無効化するかが決定されます。	OCH-Trail UNI 回線タイプ。
[優先波長プロパティ (Preferred Wavelength Properties)]		
[波長オプション (Wavelength Options)]	回線の波長オプション。値は [設定しない (Do Not Set)]、[デフォルトに設定 (Set To Default)]、および [優先波長を設定 (Set Preferred Wavelength)] です。	OCH-Trail UNI 回線タイプ。
[作業ポートのプロパティ (Work Port Properties)]		
[自動プロビジョニング (Auto Provisioning)]	自動プロビジョニング機能を有効にするには、このチェックボックスをオンにします。	すべての OCH 回線タイプ

属性	説明	有効
[C バンド (C Band)]	<p>回線をプロビジョニングするための従来の波長ウィンドウ。値は次のとおりです。</p> <ul style="list-style-type: none"> • [奇数 (Odd)] : ITU グリッドの奇数位置。 • [偶数 (Even)] : ITU グリッドの偶数位置。 	<ul style="list-style-type: none"> • [自動プロビジョニング (Restoration)] チェックボックスがオンになっている場合のすべての OCHCC WSON、OCHNC WSON、および OCH-Trail WSON 回線タイプ。 • [波長オプション (Wavelength Options)] が [優先波長を設定 (Set Preferred Wavelength)] に設定されている場合の OCH-Trail UNI 回線タイプ。
[波長/周波数 (Wavelength/Frequency)]	<p>回線の波長または周波数。この値は、選択した C バンドに適用されます。</p> <p>(注) DWDM グリッド単位を波長または周波数に設定する必要があります。これには、[管理 (Administration)] > [設定 (Settings)] > [システム設定 (System Settings)] > [回線/VC 表示 (Circuits/VCs Display)] を選択し、[DWDM グリッド単位 (DWDM Grid Unit)] エリアで [波長 (ナノメートル (nm)) (Wavelength (Nanometer (nm)))] または [周波数 (テラヘルツ (THz)) (Frequency (Terahertz (THz)))] を選択します。</p>	[C バンド (C Band)] フィールドが [奇数 (Odd)] または [偶数 (Even)] に設定されている場合のすべての OCH 回線タイプ。

属性	説明	有効
[優先/必須 (Preferred/Required)]	[C バンド (C Band)] フィールドと [波長/周波数 (Wavelength/Frequency)] フィールドで設定した値が、回線をプロビジョニングするときに優先される値であるか必須の値であるかを決定するために選択します。	[自動プロビジョニング (Auto Provisioning)] チェックボックスがオフの場合のすべての OCH 回線タイプ。
[保護ポートのプロパティ (Protect Port Properties)]		
[作業ポートからコピー (Copy from Work Port)]	[作業ポートのプロパティ (Work Port Properties)] セクションで設定した値をコピーするには、このチェックボックスをオンにします。	[保護 (Protection)] フィールドが [PSM]、[Y 字型ケーブル (Y-Cable)]、または [スプリッタ (Splitter)] に設定されている場合のすべての OCH 回線タイプ。

NCS 1004 デバイスを直接接続する OCH トレール回線の作成とプロビジョニング

NCS 1004 デバイスを直接接続する OCH トレール回線を作成してプロビジョニングするには、次の手順を実行します。

始める前に

光回線をプロビジョニングする前に満たす必要がある前提条件については、[光回線のプロビジョニングの前提条件 \(39 ページ\)](#) を参照してください。

- ステップ 1 左側のサイドバーから、[マップ (Maps)] > [トポロジマップ (Topology Maps)] > [ネットワークトポロジ (Network Topology)] の順に選択します。
- ステップ 2 [デバイスグループ (Device Groups)] をクリックして、OCH 回線を作成する場所を選択します。
- ステップ 3 [デバイスグループ (Device Groups)] ポップアップ ウィンドウを閉じます。
- ステップ 4 [ネットワークトポロジ (Network Topology)] ウィンドウで [回線/VC (Circuits/VCS)] をクリックします。
- ステップ 5 [回線/VC (Circuits/VCS)] タブをクリックし、[回線/VC (Circuits/VCS)] ペインツールバーで [+] ([作成 (Create)]) アイコンをクリックします。マップの右側の新しいペインでプロビジョニングウィザードが開きます。

プロビジョニング ウィザードを表示するもう 1 つの方法として、[設定 (Configuration)] > [ネットワーク (Network)] > [サービス プロビジョニング (Service Provisioning)] の順に選択する方法があります。

- ステップ 6** [テクノロジー (Technology)] ドロップダウンリストから [光 (Optical)] を選択すると、Cisco EPN Manager は関連する回線タイプのリストを [サービス タイプ (Service Type)] 領域に表示します。たとえば、OCH 回線の [光 (Optical)] サービス タイプには、[OCHNC WSON]、[OCHCC WSON]、[OCH-Trail WSON]、および [OCH-Trail UNI] があります。
- ステップ 7** [サービス タイプ (Service Type)] エリアで、作成する OCH 回線のタイプを選択します。
- ステップ 8** さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、[プロファイルの選択 (Select Profile)] ドロップダウンリストから必要なプロファイルを選択します。回線/VC プロファイル (134 ページ) を参照してください。
- ステップ 9** [次へ (Next)] をクリックして [顧客セクション (Customer Section)] ページに移動します。
- ステップ 10** (オプション) 回線の作成対象顧客を選択します。リストに顧客が表示されない場合は、[インベントリ (Inventory)] > [その他 (Other)] > [顧客 (Customers)] の順に移動し、システムで顧客を作成してから、プロビジョニング ウィザードを再起動します。
- ステップ 11** [顧客セクション (Customer Section)] ページに回線名とその説明を入力します。
- ステップ 12** [次へ (Next)] をクリックして [回線セクション (Circuit Section)] ページに移動します。
- (注) 光サービス タイプとして OCH-Trail UNI を選択すると、[エンドポイントセクション (Endpoint Section)] ページが最初に表示され、その後 [回線セクション (Circuit Section)] ページが表示されます。
- ステップ 13** 回線の詳細を入力します。フィールドと属性の説明については、OCH 回線タイプの [回線 (Circuit)] セクション リファレンス (42 ページ) を参照してください。
- ステップ 14** [次へ (Next)] をクリックして [エンドポイントセクション (Endpoint Section)] ページに移動します。
- ステップ 15** [エンドポイント (Endpoint)] テーブルの行を選択し、マップでデバイスをクリックします。選択したデバイスの名前が [デバイス名 (Device Name)] 列に読み込まれます。あるいは、[エンドポイント (Endpoint)] テーブルの行をクリックして、[デバイス名 (Device Name)]、[終端ポイント (Termination Point)]、[ポートの追加/ドロップ (Add/Drop Port)]、[OCH トレール (OCH-Trail)]、および [サイド (Side)] の各列を編集できます。[サイド (Side)] 列は、選択したポートに基づいて自動的に設定されます。選択した回線タイプと互換性があり、使用可能なネットワーク要素だけが表示されます。
- (注) [ポートの追加 (Add Port)] 列と [ポートのドロップ (Drop Port)] 列は、OCHNC WSON 回線の場合にのみ使用可能です。[ポートの追加 (Add Port)] 列に追加する必要があるポートを選択すると、[ポートのドロップ (Drop Port)] 列と [サイド (Side)] 列の値が自動的に設定されます。また、[ポートのドロップ (Drop Port)] 列の値を手動で編集することもできます。
- ステップ 16** OCH 回線のトレールの多様性を選択します。作成する OCH 回線と選択するトレールは異なります。
- (注) 作成後にトレールの多様性を変更または削除することはできません。
- ステップ 17** [次へ (Next)] をクリックして [制約セクション (Constraints Section)] ページに進みます。
- ステップ 18** マップでデバイス ノードまたはリンクをクリックし、[制約 (Constraints)] テーブルに追加します。あるいは、テーブル ツールバーで「+」ボタンをクリックし、新しい行をテーブルに追加し、[ノード/リンク

名 (Node/Link Name)]、[包含/除外 (Include/Exclude)]、および[ルート (Route)]列を編集することもできます。選択した回線タイプと互換性があるネットワーク要素とリンクだけが表示されます。

(注) 行が編集モードになっている場合は、マップのデバイスまたはリンクをクリックして [制約 (Constraints)] テーブルの列にデータを読み込むことはできません。OCHCC トレール WSON 回線には、次のルートの制約条件が適用されます。

- 変更されたルートの制約事項は、すぐには回線に適用されませんが、再ルーティングが必要になる場合があります。ただし、変更は次のルート操作または復元時に適用されます。
- [回線オーバーレイ (Circuit Overlay)] には現在のルートに適用可能な制約事項のみが表示され、**回線の編集**ウィザードには現在設定されている制約事項が表示されます。
- **回線の編集**ウィザードには、回線オーバーレイを使用して表示される制約事項アイコンとは異なる制約事項を表示する制約事項テーブルが含まれています。

ステップ 19 [次へ (Next)] をクリックして [異種波長セクション (Alien Wavelength Section)] ページに移動します。送信元ノードと宛先ノードのカード、トランク モード、Fec モードなどの現在の異種波長の設定が表示されます。送信元ノードと宛先ノードの異種波長に新しい設定を作成できます。

(注) [異種波長セクション (Alien Wavelength Section)] は、OCHNC WSON 回線を作成する場合にのみ使用できます。

ステップ 20 [今すぐ作成 (Create Now)] をクリックして回線を作成します。デバイスに展開する前に TL1 または CLI コマンドのプレビューを表示することを選択した場合、[プレビュー (Preview)] をクリックするとプレビューが表示されます。この場合、設定をデバイスに展開するかキャンセルするかを選択できますが、属性を編集することはできません。

ステップ 21 [ネットワーク トポロジ (Network Topology)] ウィンドウの [回線/VC (Circuits/VCs)] ペインのリストに、回線が追加されます。プロビジョニング状態を確認するには、回線/VC 名の横にある [i] アイコンをクリックし、[回線/VC 360 (Circuit/VC 360)] ビューを表示します。

互いに異なる 2 つの OCH トレール UNI 回線の作成およびプロビジョニング

互いに異なる 2 つの OCH トレール UNI 回線を作成するには、この手順を使用します。両方の回線の始点は同じデバイスにする必要があります。プロビジョニングウィザードを使用して、1 つのウィンドウで両方の回線を迅速に作成することができます。

始める前に

オプティカル回線をプロビジョニングする前に満たす必要がある前提条件については、[光回線のプロビジョニングの前提条件 \(39 ページ\)](#) を参照してください。

ステップ 1 左側のサイドバーから、[マップ (Maps)] > [トポロジマップ (Topology Maps)] > [ネットワーク トポロジ (Network Topology)] の順に選択します。

- ステップ 2** [デバイス グループ (Device Groups)] をクリックして、OCH 回線を作成する場所を選択します。
- ステップ 3** [デバイス グループ (Device Groups)] ポップアップ ウィンドウを閉じます。
- ステップ 4** [ネットワーク トポロジ (Network Topology)] ウィンドウで [回線/VC (Circuits/VCs)] をクリックします。
- ステップ 5** [回線/VC (Circuits/VCs)] タブをクリックし、[回線/VC (Circuits/VCs)] ペイン ツールバーで [+] ([作成 (Create)]) アイコンをクリックします。マップの右側の新しいペインでプロビジョニング ウィザードが開きます。
- プロビジョニング ウィザードを表示するもう1つの方法として、[設定 (Configuration)] > [ネットワーク (Network)] > [サービス プロビジョニング (Service Provisioning)] の順に選択する方法があります。
- ステップ 6** [テクノロジー (Technology)] ドロップダウン リストから、[オプティカル (Optical)] を選択します。
- ステップ 7** [サービス タイプ (Service Type)] 領域で、[OCH トレール UNI (OCH-Trail UNI)] を選択します。
- ステップ 8** さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、[プロファイルの選択 (Select Profile)] ドロップダウンリストから必要なプロファイルを選択します。[回線/VC プロファイル \(134 ページ\)](#) を参照してください。
- ステップ 9** [次へ (Next)] をクリックして [顧客セクション (Customer Section)] ページに移動します。
- ステップ 10** 互いに異なる2つのOCHトレールUNI回線を作成するには、[相互ダイバーシティ (Mutual Diversity)] チェックボックスをオンにします。
- ステップ 11** [顧客セクション (Customer Section)] ページで、回線の名前と説明を入力します。
- ステップ 12** [次へ (Next)] をクリックして [エンドポイントセクション (Endpoint Section)] ページに移動します。
- ステップ 13** [エンドポイント (Endpoint)] テーブルの行を選択し、マップでデバイスをクリックします。選択したデバイスの名前が [デバイス名 (Device Name)] 列に読み込まれます。または、[エンドポイント (Endpoint)] テーブル内の行をクリックしてデバイス名とインターフェイスを編集することもできます。
- (注) 行が編集モードになっていると、マップ内のデバイスをクリックしても、[デバイス名 (Device Name)] 列に名前は取り込まれません。
- ステップ 14** [次へ (Next)] をクリックして [回線セクション (Circuit Section)] ページに進みます。
- ステップ 15** 回線の詳細を入力します。フィールドと属性の説明については、[OCH 回線タイプの \[回線 \(Circuit\)\] セクション リファレンス \(42 ページ\)](#) を参照してください。
- ステップ 16** [次へ (Next)] をクリックして [制約セクション (Constraints Section)] ページに進みます。
- ステップ 17** マップでデバイス ノードまたはリンクをクリックし、[制約 (Constraints)] テーブルに追加します。あるいは、テーブル ツールバーで 「+」 ボタンをクリックし、新しい行をテーブルに追加し、[ノード/リンク名 (Node/Link Name)]、[包含/除外 (Include/Exclude)]、および [ルート (Route)] 列を編集することもできます。選択した回線タイプと互換性があるネットワーク要素とリンクだけが表示されます。
- (注) 行が編集モードになっている場合は、マップのデバイスまたはリンクをクリックして [制約 (Constraints)] テーブルの列にデータを読み込むことはできません。
- ステップ 18** [次へ (Next)] をクリックします。2番目の回線の [顧客セクション (Customer Section)] ページが表示されます。
- ステップ 19** ステップ 11 からステップ 17 を繰り返して2番目の回線を作成します。

- ステップ 20** [今すぐ作成 (Create Now)] をクリックして回線を作成します。デバイスに展開する前に TL1 または CLI コマンドのプレビューを表示することを選択した場合、[プレビュー (Preview)] をクリックするとプレビューが表示されます。この場合、設定をデバイスに展開するかキャンセルするかを選択できますが、属性を編集することはできません。
- ステップ 21** 回線が、[ネットワーク トポロジ (Network Topology)] ウィンドウの [回線/VC (Circuits/VCS)] ペインのリストに追加されているはずですが、プロビジョニングの状態を確認するには、回線/VC 名の横にある [i] アイコンをクリックして [回線/VC 360 (Circuit/VC 360)] ビューを表示します。

メディア チャネル グループ SSON 回線の作成とプロビジョニング

メディア チャネル グループの SSON 回線を作成し、プロビジョニングするには、次の手順を実行します。

始める前に

光回線をプロビジョニングする前に満たす必要がある前提条件については、[光回線のプロビジョニングの前提条件 \(39 ページ\)](#) を参照してください。

- ステップ 1** 左側のサイドバーから、[マップ (Maps)] > [トポロジ マップ (Topology Maps)] > [ネットワーク トポロジ (Network Topology)] を選択します。
- ステップ 2** [デバイス グループ (Device Groups)] をクリックして、メディア チャネル グループの SSON 回線を作成する場所を選択します。
- ステップ 3** [デバイス グループ (Device Groups)] ポップアップ ウィンドウを閉じます。
- ステップ 4** [ネットワーク トポロジ (Network Topology)] ウィンドウで [回線/VC (Circuits/VCS)] をクリックします。
- ステップ 5** [回線/VC (Circuits/VCS)] タブをクリックし、[回線/VC (Circuits/VCS)] ペインツールバーで [+] ([作成 (Create)]) アイコンをクリックします。マップの右側の新しいペインでプロビジョニング ウィザードが開きます。
- プロビジョニング ウィザードを表示するもう 1 つの方法として、[設定 (Configuration)] > [ネットワーク (Network)] > [サービス プロビジョニング (Service Provisioning)] の順に選択する方法があります。
- ステップ 6** [テクノロジー (Technology)] ドロップダウンリストから [光 (Optical)] を選択すると、Cisco EPN Manager は関連する回線タイプのリストを [サービス タイプ (Service Type)] 領域に表示します。
- ステップ 7** [サービス タイプ (Service Type)] 領域で、[メディア チャネル グループの SSON (Media Channel Group SSON)] を選択します。
- ステップ 8** さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、[プロファイルの選択 (Select Profile)] ドロップダウンリストから必要なプロファイルを選択します。[回線/VC プロファイル \(134 ページ\)](#) を参照してください。
- ステップ 9** [次へ (Next)] をクリックして [顧客セクション (Customer Section)] ページに移動します。

- ステップ 10** (オプション) 回線の作成対象顧客を選択します。リストに顧客が表示されない場合は、[インベントリ (Inventory)] > [その他 (Other)] > [顧客 (Customers)] の順に移動し、システムで顧客を作成してから、プロビジョニングウィザードを再起動します。
- ステップ 11** [顧客セクション (Customer Section)] ページに回線名とその説明を入力します。
- (注) [回線名 (Circuit Name)] フィールドには最大 80 文字を使用することができます。
- ステップ 12** [次へ (Next)] をクリックして[エンドポイントセクション (Endpoint Section)] ページに移動します。
- ステップ 13** [エンドポイント (Endpoint)] テーブルの行を選択し、マップでデバイスをクリックします。選択したデバイスの名前が [デバイス名 (Device Name)] 列に読み込まれます。あるいは、[エンドポイント (Endpoint)] テーブルの行をクリックして、[デバイス名 (Device Name)]、[終端ポイント (Termination Point)]、[ポートの追加 (Add Port)]、および[ポートのドロップ (Drop Port)] の各列を編集します。選択した回線タイプと互換性があり使用可能なネットワーク要素だけが表示されます。
- (注) 行が編集モードになっていると、マップ内のデバイスをクリックしても、[デバイス名 (Device Name)] 列に名前は取り込まれません。
- ステップ 14** [次へ (Next)] をクリックして[回線セクション (Circuit Section)] ページに進みます。
- ステップ 15** 必要な回線幅を選択します。
- ステップ 16** [中央波長/周波数のプロパティ (Central Wavelength/Frequency Properties)] を設定するには、次のいずれかを実行します。
- [自動プロビジョニング (Auto Provisioning)] チェックボックスをオンにします。
 - 回線に必要な波長を選択して、[優先 (Preferred)] オプションまたは[必須 (Required)] オプションを選択し、[波長 (Wavelength)] フィールドに設定した値が回線をプロビジョニングするために優先されるか、または必須であるかを特定します。
- ステップ 17** [次へ (Next)] をクリックして[制約セクション (Constraints Section)] ページに進みます。
- ステップ 18** マップでデバイスノードまたはリンクをクリックし、[制約 (Constraints)] テーブルに追加します。あるいは、テーブルツールバーで「+」ボタンをクリックし、新しい行をテーブルに追加し、[ノード/リンク名 (Node/Link Name)]、[包含/除外 (Include/Exclude)]、および[ルート (Route)] 列を編集することもできます。選択した回線タイプと互換性があるネットワーク要素とリンクだけが表示されます。
- (注) 行が編集モードになっている場合は、マップのデバイスまたはリンクをクリックして[制約 (Constraints)] テーブルの列にデータを読み込むことはできません。
- [光プロパティ (Optical Properties)] で、[復元 (Restoration)] チェックボックスがオンになっており、[もとに戻す (Revert)] が[なし (None)] に設定されている場合は、[代替制約事項 (Alternate Constraints)] チェックボックスを選択できます。
- ステップ 19** [今すぐ作成 (Create Now)] をクリックして、回線を作成します。デバイスに展開される TL1 または CLI コマンドのプレビューを表示する場合、[プレビュー (Preview)] をクリックするとプレビューが表示されます。この時点で、設定をデバイスに展開するか、またはキャンセルすることができますが、属性を編集することはできません。

[ネットワーク トポロジ (Network Topology)] ウィンドウの [回線/VC (Circuits/VCs)] ペインのリストに、回線が追加されます。プロビジョニング状態を確認するには、回線/VC名の横にある [i] アイコンをクリックし、[回線/VC 360 (Circuit/VC 360)] ビューを表示します。

メディア チャネル SSON 回線の作成とプロビジョニング

メディア チャネルの SSON 回線を作成し、プロビジョニングするには、次の手順を実行します。

始める前に

- メディア チャネル SSON 回線をメディア チャネル グループに関連付けるために、メディア チャネル グループの SSON が既に作成されていることを確認します。[メディア チャネル グループ SSON 回線の作成とプロビジョニング \(53 ページ\)](#) を参照してください。
- 光回線をプロビジョニングする前に満たす必要がある前提条件については、[光回線のプロビジョニングの前提条件 \(39 ページ\)](#) を参照してください。

-
- ステップ 1** 左側のサイドバーから、[マップ (Maps)]>[トポロジ マップ (Topology Maps)]>[ネットワーク トポロジ (Network Topology)] を選択します。
 - ステップ 2** [デバイス グループ (Device Groups)] をクリックして、メディア チャネルの SSON 回線を作成する場所を選択します。
 - ステップ 3** [デバイス グループ (Device Groups)] ポップアップ ウィンドウを閉じます。
 - ステップ 4** [ネットワーク トポロジ (Network Topology)] ウィンドウで [回線/VC (Circuits/VCs)] をクリックします。
 - ステップ 5** [回線/VC (Circuits/VCs)] タブをクリックし、[回線/VC (Circuits/VCs)] ペイン ツールバーで [+] ([作成 (Create)]) アイコンをクリックします。マップの右側の新しいペインでプロビジョニング ウィザードが開きます。
プロビジョニング ウィザードを表示するもう 1 つの方法として、[設定 (Configuration)]>[ネットワーク (Network)]>[サービス プロビジョニング (Service Provisioning)] の順に選択する方法があります。
 - ステップ 6** [テクノロジー (Technology)] ドロップダウンリストから [光 (Optical)] を選択すると、Cisco EPN Manager は関連する回線タイプのリストを [サービス タイプ (Service Type)] 領域に表示します。たとえば、メディア チャネル SSON 回線の光サービスタイプには、[メディア チャネル NC SSON (Media Channel NC SSON)]、[メディア チャネル トレール SSON (Media Channel Trail SSON)]、および [メディア チャネル CC SSON (Media Channel CC SSON)] などがあります。
 - ステップ 7** [サービス タイプ (Service Type)] 領域で、作成するメディア チャネルの SSON 回線のタイプを選択します。
 - ステップ 8** さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、[プロファイルの選択 (Select Profile)] ドロップダウンリストから必要なプロファイルを選択します。[回線/VC プロファイル \(134 ページ\)](#) を参照してください。
 - ステップ 9** [次へ (Next)] をクリックして [顧客セクション (Customer Section)] ページに移動します。

- ステップ 10** (オプション) 回線の作成対象顧客を選択します。リストに顧客が表示されない場合は、[インベントリ (Inventory)] > [その他 (Other)] > [顧客 (Customers)] の順に移動し、システムで顧客を作成してから、プロビジョニングウィザードを再起動します。
- ステップ 11** [顧客セクション (Customer Section)] ページに回線名とその説明を入力します。
- (注) メディアチャネル NC SSON およびメディアチャネルトレール SSON 回線の場合、[回線名 (Circuit Name)] フィールドに使用できるのは最大 77 文字のみです。77 文字のうち、3 文字はキャリアサフィックス用に予約されています。
- メディアチャネル CC SSON 回線の場合、[回線名 (Circuit Name)] フィールドには最大 71 文字を使用できます。
- ステップ 12** [次へ (Next)] をクリックして [エンドポイントセクション (Endpoint Section)] ページに移動します。
- ステップ 13** [エンドポイント (Endpoint)] テーブルの行を選択し、マップでデバイスをクリックします。選択したデバイスの名前が [デバイス名 (Device Name)] 列に読み込まれます。あるいは、[エンドポイント (Endpoint)] テーブルの行をクリックして、[デバイス名 (Device Name)] 列および [終端ポイント (Termination Point)] 列を編集します。[サイド (Side)] 列は、選択した終端ポイントに基づいて自動的に設定されます。選択した回線タイプと互換性があり、使用可能なネットワーク要素だけが表示されます。
- (注) [MCHトレール名 (MCH-Trail Name)] 列は、メディアチャネル CC SSON 回線を作成する場合にのみ使用できます。
- ステップ 14** MCH 回線のメディアチャネルの種類を選択します。作成する MCH 回線と選択するメディアチャネルは異なります。
- (注) 作成後にメディアチャネルの種類を変更または削除することはできません。
- ステップ 15** [次へ (Next)] をクリックして [回線セクション (Circuit Section)] ページに移動します。
- (注) メディアチャネル CC SSON 回線では、[エンドポイント (Endpoints)] テーブルに MCH トレーン名を入力した場合、[回線セクション (Circuit Section)] ページは使用できません。
- ステップ 16** メディアチャネル SSON 回線を関連付けるメディアチャネルグループを選択します。
- ステップ 17** 回線の詳細を入力します。フィールドと属性の説明については、[メディアチャネル SSON 回線タイプの回線セクションリファレンス \(57 ページ\)](#) を参照してください。
- ステップ 18** [次へ (Next)] をクリックして [制約セクション (Constraints Section)] ページに進みます。
- ステップ 19** マップでデバイスノードまたはリンクをクリックし、[制約 (Constraints)] テーブルに追加します。あるいは、テーブルツールバーで「+」ボタンをクリックし、新しい行をテーブルに追加し、[ノード/リンク名 (Node/Link Name)]、[包含/除外 (Include/Exclude)]、および [ルート (Route)] 列を編集することもできます。選択した回線タイプと互換性があるネットワーク要素とリンクだけが表示されます。
- (注) 行が編集モードになっている場合は、マップのデバイスまたはリンクをクリックして [制約 (Constraints)] テーブルの列にデータを読み込むことはできません。
- ステップ 20** [今すぐ作成 (Create Now)] をクリックして、回線を作成します。デバイスに展開される TL1 または CLI コマンドのプレビューを表示する場合、[プレビュー (Preview)] をクリックするとプレビューが表示さ

れます。この時点で、設定をデバイスに展開するか、またはキャンセルすることができますが、属性を編集することはできません。

[ネットワーク トポロジ (Network Topology)] ウィンドウの [回線/VC (Circuits/VCs)] ペインのリストに、回線が追加されます。プロビジョニング状態を確認するには、回線/VC名の横にある [i] アイコンをクリックし、[回線/VC 360 (Circuit/VC 360)] ビューを表示します。

メディア チャネル SSON 回線タイプの回線セクション リファレンス

次の表に、メディア チャネル SSON 回線のタイプを定義する属性のリストと説明を示します。

表 8: [回線セクション (Circuit Section)] のリファレンス : メディア チャネル SSON 回線のタイプ

属性	説明	有効
中心波長/周波数のプロパティ		
自動プロビジョニング (Auto Provisioning)	このチェックボックスをオンにすると、回線の波長または周波数のプロパティが自動的に設定されます。	すべてのメディア チャネル SSON 回線のタイプ。
波長 (nm) (Wavelength (nm))	回線の波長または周波数。 (注) DWDM グリッド単位を波長または周波数に設定する必要があります。これには、[管理 (Administration)] > [設定 (Settings)] > [システム設定 (System Settings)] > [回線/VC 表示 (Circuits/VCs Display)] を選択し、[DWDM グリッド単位 (DWDM Grid Unit)] エリアで [波長 (ナノメートル (nm)) (Wavelength (Nanometer (nm)))] または [周波数 (テラヘルツ (THz)) (Frequency (Terahertz (THz)))] を選択します。	[自動プロビジョニング (Auto Provisioning)] チェックボックスがオフの場合のすべてのメディア チャネル SSON 回線のタイプ。
優先/必須 (Preferred/Required)	[波長 (Wavelength)] フィールドで設定した値が、回線をプロビジョニングするときに優先される値であるか必須の値であるかを決定するために選択します。	[自動プロビジョニング (Auto Provisioning)] チェックボックスがオフの場合のすべてのメディア チャネル SSON 回線のタイプ。
光プロパティ (Optical Properties)		

属性	説明	有効
検証	<p>回線の検証モード。値は次のとおりです。</p> <ul style="list-style-type: none"> • [フル (Full)] : 回線の検証結果が承認しきい値以上になると回線が作成されます。 • [なし (None)] : 承認しきい値を考慮せずに回線が作成されます。 	すべてのメディアチャネル SSON 回線のタイプ。
承認しきい値 (Acceptance Threshold)	<p>回線に設定された保護承認しきい値。値は次のとおりです。</p> <ul style="list-style-type: none"> • [緑 (Green)] : 復元失敗の危険性が 0% であることを示します。 • [黄 (Yellow)] : 復元失敗の危険性が 0% ~ 16% の間であることを示します。 • [オレンジ (Orange)] : 復元失敗の危険性が 16% ~ 50% の間であることを示します。 • [赤 (Red)] : 復元失敗の危険性が 50% を超えていることを示します。 	[検証 (Validation)] フィールドが [フル (Full)] に設定されている場合のすべてのメディアチャネル SSON 回線タイプ。
[パスアラームを無視 (Ignore Path Alarms)]	パスアラームを無視するには、このチェックボックスをオンにします。	すべてのメディアチャネル SSON 回線のタイプ。
[再生成を許可 (Allow Regeneration)]	ネットワーク要素が信号を再生成できるようにするには、このチェックボックスをオンにします。	すべてのメディアチャネル SSON 回線のタイプ。
復元 (Restoration)	障害が発生したメディアチャネル SSON 回線を新しいルートに復元するには、このチェックボックスをオンにします。	すべてのメディアチャネル SSON 回線のタイプ。
プライオリティ (Priority)	障害が発生した回線の復元操作に優先順位を付けます。値は [高 (High)]、[プライオリティ 1 (Priority 1)]、[プライオリティ 2 (Priority 2)]、[プライオリティ 3 (Priority 3)]、[プライオリティ 4 (Priority 4)]、[プライオリティ 5 (Priority 5)]、[プライオリティ 6 (Priority 6)]、および [低 (Low)] です。	[復元 (Restoration)] チェックボックスがオンの場合のすべてのメディアチャネル SSON 回線タイプ。

属性	説明	有効
[復元の検証 (Restoration Validation)]	復元操作の検証モード。値は次のとおりです。 <ul style="list-style-type: none"> • [なし (None)] : 復元の承認しきい値を考慮せずに回線が作成されます。 • [継承 (Inherited)] : 復元された回線は、プライマリ回線から検証と承認のしきい値を継承します。 • [フル (Full)] : 復元の検証結果が復元の承認しきい値以上になると回線が作成されます。 	[復元 (Restoration)] チェックボックスがオンの場合のすべてのメディア チャネル SSON 回線タイプ。
[復元の承認しきい値 (Restoration Acceptance Threshold)]	回線の復元操作に設定された承認しきい値。値は次のとおりです。 <ul style="list-style-type: none"> • [緑 (Green)] : 復元失敗の危険性が 0% であることを示します。 • [黄 (Yellow)] : 復元失敗の危険性が 0% ~ 16% の間であることを示します。 • [オレンジ (Orange)] : 復元失敗の危険性が 16% ~ 50% の間であることを示します。 • [赤 (Red)] : 復元失敗の危険性が 50% を超えていることを示します。 	次の場合のすべてのメディア チャネル SSON 回線タイプ。 <ul style="list-style-type: none"> • [復元 (Restoration)] チェックボックスがオンになっている。 • [復元検証 (Restoration Validation)] フィールドが [フル (Full)] に設定されている。
[元に戻す (Revert)]	障害が修正された後、復元されたパスから元のパスに回線に戻します。値は [なし (None)]、[手動 (Manual)]、および [自動 (Automatic)] です。	[復元 (Restoration)] チェックボックスがオンの場合のすべてのメディア チャネル SSON 回線タイプ。
[ソーク時間 (Soak Time)]	障害が修正された後、元のパスに切り替わるまでに、復元されたパス上の回線が待機する期間。	[元に戻す (Revert)] オプションが [手動 (Manual)] または [自動 (Automatic)] に設定されている場合、すべてのメディア チャネル SSON 回線タイプ。

OTN 回線の作成とプロビジョニング

OTN 回線をプロビジョニングするには、次の手順に従います。

始める前に

光回線をプロビジョニングする前に満たしている必要がある前提条件については、[光回線のプロビジョニングの前提条件 \(39 ページ\)](#) を参照してください。

-
- ステップ 1** 左側のサイドバーのメニューから、[マップ (Maps)] > [トポロジ マップ (Topology Maps)] > [ネットワーク トポロジ (Network Topology)] の順に選択します。
- ステップ 2** [デバイス グループ (Device Groups)] をクリックして、OTN 回線を作成する場所を選択します。
- ステップ 3** [ネットワーク トポロジ (Network Topology)] ウィンドウで [回線/VC (Circuits/VCs)] をクリックします。
- ステップ 4** [回線/VC (Circuits/VCs)] タブをクリックし、[回線/VC (Circuits/VCs)] ペインツールバーで [+] ([作成 (Create)]) アイコンをクリックします。マップの右側の新しいペインでプロビジョニング ウィザードが開きます。
- プロビジョニング ウィザードを表示するもう 1 つの方法として、[設定 (Configuration)] > [ネットワーク (Network)] > [サービス プロビジョニング (Service Provisioning)] の順に選択する方法があります。
- ステップ 5** [テクノロジー (Technology)] ドロップダウンリストから [光 (Optical)] を選択すると、Cisco EPN Manager は関連する回線タイプのリストを [サービス タイプ (Service Type)] 領域に表示します。たとえば、OTN 回線のサービス タイプには、[ODU UNI]、[ODU トンネル (ODU Tunnel)]、[OPU over ODU]、および [ODU UNI ヘアピン (ODU UNI Hairpin)] があります。
- ステップ 6** [サービス タイプ (Service Type)] エリアで、作成する OTN 回線のタイプを選択します。
- ステップ 7** さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、[プロファイルの選択 (Select Profile)] ドロップダウンリストから必要なプロファイルを選択します。[回線/VC プロファイル \(134 ページ\)](#) を参照してください。
- ステップ 8** [次へ (Next)] をクリックして [顧客の詳細 (Customer Details)] ページに移動します。
- ステップ 9** (オプション) 回線の作成対象顧客を選択します。リストに顧客が表示されない場合は、[インベントリ (Inventory)] > [その他 (Other)] > [顧客 (Customers)] の順に移動し、システムで顧客を作成してから、プロビジョニング ウィザードを再起動します。
- ステップ 10** [顧客の詳細 (Customer Details)] ページに回線名とその説明を入力します。
- ステップ 11** [次へ (Next)] をクリックして [回線の詳細 (Circuit Details)] ページに移動します。
- ステップ 12** 回線の詳細を入力します。フィールドと属性の説明については、[OTN 回線タイプの回線セクション参照 \(61 ページ\)](#) を参照してください。
- ステップ 13** [次へ (Next)] をクリックして [エンドポイント セクション (Endpoint Section)] ページに移動します。
- ステップ 14** [エンドポイント (Endpoint)] テーブルの行を選択し、マップでデバイスをクリックします。選択したデバイスの名前が [デバイス名 (Device Name)] 列に読み込まれます。あるいは、[エンドポイント (Endpoint)] テーブルの行をクリックして、[デバイス名 (Device Name)] および [インターフェイス/終端ポイント (Interface/Termination Point)] 列を編集します。選択した回線タイプと互換性があり使用可能なネットワーク要素だけが表示されます。

(注) 行が編集モードになっている場合は、マップのデバイスをクリックして [デバイス名 (Device Name)] 列にデータを読み込むことはできません。

ステップ 15 回線の保護タイプとパスオプションを入力します。フィールドと属性の説明については、[OTN回線タイプの \[エンドポイント \(Endpoint\)\] セクションリファレンス \(63 ページ\)](#) を参照してください。

ステップ 16 [今すぐ作成 (Create Now)] をクリックして、回線を作成します。デバイスに展開される TL1 または CLI コマンドのプレビューを表示することを選択した場合、[プレビュー (Preview)] をクリックするとプレビューが表示されます。TL1 または CLI コマンドのプレビューを確認したら、設定をデバイスに展開するか、またはプロビジョニング操作をキャンセルできます。

[ネットワーク トポロジ (Network Topology)] ウィンドウの [回線/VC (Circuits/VCs)] タブのリストに、回線が追加されます。プロビジョニング状態を確認するには、回線/VC名の横にある [i] アイコンをクリックし、[回線/VC 360 (Circuit/VC 360)] ビューを表示します。

OTN 回線タイプの回線セクション参照

次の表に、OTN 回線タイプを定義する属性の一覧と説明を示します。

表 9: 回線セクション参照 : OTN 回線タイプ

属性	説明	有効
回線プロパティ		
Bandwidth	OTN 回線を提供するために必要な帯域幅。 帯域幅とサービス タイプ フィールドの値のマッピングについては、 表 11: 値のマッピング : ODU UNI 回線の帯域幅とサービス タイプ を参照してください。	すべての OTN 回線タイプ。
A エンド : オープンエンド (A-End Open Ended)	送信元エンドポイントがクライアントのペイロードコントローラではなく ODU サブコントローラに接続されているオープンエンド回線を作成するには、このチェックボックスをオンにします。 (注) このチェックボックスをオンにすると、Cisco NCS 4000 デバイスに ODU サブコントローラが展開されません。デバイスを Cisco EPN Manager に追加する前に Cisco NCS 4000 デバイスで ODU サブコントローラを設定する必要があります。オープンエンド ODU UNI、および Cisco NCS 4000 デバイスで ODU サブコントローラを設定する方法については、 オープンエンドの ODU UNI を参照してください。	帯域幅フィールドが ODU0、ODU1、ODU2、または ODU2E に設定されている場合、ODU UNI 回線タイプ。

属性	説明	有効
Zエンド： オープンエンド (Z-End Open Ended)	宛先エンドポイントがクライアントのペイロードコントローラではなく ODU サブコントローラに接続されているオープンエンド回路を作成するには、このチェックボックスをオンにします。 (注) このチェックボックスをオンにすると、Cisco NCS 4000 デバイスに ODU サブコントローラが展開されません。デバイスを Cisco EPN Manager に追加する前に Cisco NCS 4000 デバイスで ODU サブコントローラを設定する必要があります。オープンエンド ODU UNI、および Cisco NCS 4000 デバイスで ODU サブコントローラを設定する方法については、 オープンエンドの ODU UNI を参照してください。	帯域幅フィールドが ODU0、ODU1、ODU2、または ODU2E に設定されている場合、ODU UNI 回線タイプ。
サービスタイプ (Service Type)	選択した帯域幅でサポートされているサービスタイプ。帯域幅とサービスタイプフィールドの値のマッピングについては、 表 11：値のマッピング：ODU UNI 回線の帯域幅とサービスタイプ を参照してください。	ODU UNI 回線タイプ。
ルート プロパティ (Route Properties)		
ビットレート	1 秒あたりのビット数の合計。	帯域幅フィールドが ODUFLEX に設定されている場合、すべての OTN 回線タイプ (ODU UNI ヘアピンを除く)。
フレーミングタイプ (Framing Type)	要求されたサービスの基本信号。値は次のとおりです。 <ul style="list-style-type: none"> • CBR：固定ビットレート。 • GFP-F 固定 (GFP-F-Fixed)：固定のフレームマップ型ジェネリックフレーミングプロシージャ。 	帯域幅フィールドが ODUFLEX に設定されている場合、すべての OTN 回線タイプ (ODU UNI ヘアピンを除く)。

属性	説明	有効
ルートを記録 (Record Route)	回線ルートを記録するには、このチェックボックスをオンにします。	すべての OTN 回線タイプ (ODU UNI へアピンを除く)。

OTN 回線タイプの [エンドポイント (Endpoint)] セクション リファレンス

次の表に、OTN 回線タイプの保護タイプおよびパス オプションを定義する属性をリストして説明します。

表 10: [エンドポイント (Endpoint)] セクション リファレンス : OTN 回線タイプ

属性	説明	有効
エンドポイント		
デバイス名 (Device Name)	回線の A エンド デバイス と Z エンド デバイス。 (注) ODU UNI へアピン回線では、A エンド と Z エンド が同じデバイスになりますが、終端地点が異なります。	すべての OTN 回線タイプ。
インターフェイス (Interface)	A エンド デバイス と Z エンド デバイスの インターフェイス 名。	ODU UNI 回線。
終端地点	カードの終端地点。	OPU over ODU および ODU UNI へアピン回線。

属性	説明	有効
[保護タイプ (Protection Type)]	<p>OTN 回線の保護タイプ。値は次のとおりです。</p> <ul style="list-style-type: none"> • [1+0]：非保護カード。現用パスで障害が検出されると、データが失われます。 • [1+1]：プライマリパスとセカンダリパスの両方がトラフィックをエンドツーエンドで伝送し、受信者は両方のトラフィックを受信して比較します。あるパスで出力ノードが障害を検出すると、トラフィックは影響を受けていないパスに切り替えられます。 • [1+R]：プライマリパスで障害が発生すると、復元されたパスが計算され、トラフィックは復元されたパスに切り替えられます。プライマリパスが復帰不可能な場合、復元されたパスは新しいプライマリパスになります。 • [1+1+R]：プライマリパスとセカンダリパスの両方でトラフィックが伝送されます。あるパスで出力ノードが障害を検出すると、トラフィックは影響を受けていないパスに切り替えられます。復元されたパスが計算され、トラフィックは復元されたパスに切り替えられます。プライマリパスまたはセカンダリパスが復帰不可能な場合、復元されたパスは新しいプライマリパスまたはセカンダリパスになります。 <p>(注) この保護タイプは、Cisco NCS 4000 シリーズデバイスではサポートされていません。</p>	すべての OTN 回線タイプ (ODU UNI へアピンを除く)。
[トンネル ID と異なる (Diverse From Tunnel ID)]	トンネルを選択し、プロビジョニングする回線でそのトンネルが使用されないことを確認します。これにより、トンネルに障害がある場合に、同じトンネルが他の回線で使用されなくなります。	すべての OTN 回線タイプ (ODU UNI へアピンを除く)。
<p>[動作中のパス (Working Path)]、[保護パス (Protected Path)]、および [復元パス (Restored Path)]</p> <p>[保護パス (Protected Path)] フィールドグループは、[保護タイプ (Protection Type)] フィールドが [1+1] または [1+1+R] に設定されている場合に限り、すべての OTN 回線タイプ (ODU UNI へアピンを除く) で使用できます。</p> <p>[復元パス (Restored Path)] フィールドグループは、[保護タイプ (Protection Type)] フィールドが [1+R] または [1+1+R] に設定されている場合に限り、すべての OTN 回線タイプ (ODU UNI へアピンを除く) で使用できます。</p>		

属性	説明	有効
タイプ (Type)	回線の現用パスまたは保護パスのタイプを選択します。値は [ダイナミック (Dynamic)] および [明示的 (Explicit)] です。	すべての OTN 回線タイプ (ODU UNI へアピンを除く)。
新規作成 (New)	回線の新しい明示的な作業パスまたは保護パスを作成するには、このチェックボックスをオンにします。	[タイプ (Type)] フィールドが [明示的 (Explicit)] に設定されている場合のすべての OTN 回線タイプ (ODU UNI へアピンを除く)。
[既存の EP を 選択 (Select Existing EP)]	回線の既存の明示的な現用パスまたは保護パスを選択します。	[タイプ (Type)] フィールドが [明示的 (Explicit)] に設定されており、[新規作成 (New)] チェックボックスがオフになっている場合のすべての OTN 回線タイプ (ODU UNI へアピンを除く)。

属性	説明	有効
新しい名前 (New Name)	作成する明示的なパスの名前を入力します。[新しい名前 (New Name)] フィールドの下のテーブルで、[+] ボタンをクリックしてテーブルに新しい行を追加し、デバイスを選択して、そのデバイスのインターフェイスとして明示的なパスコントロールを選択します。	[タイプ (Type)] フィールドが [明示的 (Explicit)] に設定されており、[新規作成 (New)] チェックボックスがオンになっている場合のすべての OTN 回線タイプ (ODU UNI へアピンを除く)。
<p>[保護のプロファイル (Protection Profile)]</p> <p>[保護プロファイル (Protection Profile)] フィールドグループは、[保護タイプ (Protection Type)] フィールドが [1+1]、[1+R]、または [1+1+R] に設定されており、有効な A エンドデバイスが選択されている場合に限り、すべての OTN 回線タイプ (ODU UNI へアピンを除く) で使用できます。</p>		
[保護のプロファイル (Protection Profile)]	<p>回線の保護を管理するために使用されるプロファイル。この保護プロファイルは、回線の A エンドノードで設定する必要があります。</p> <p>(注) デバイスに設定されている保護プロファイルを入力できます。</p> <p>保護タイプ、SNC、ホールドオフ、復元待ち、回線復帰などの保護プロファイルの詳細が表示されます。</p>	

ODU UNI 回線の帯域幅とサービス タイプの値のマッピング

次の表に、ODU UNI 回線の帯域幅とサービス タイプ フィールドの値のマッピングを示します。

表 11: 値のマッピング : ODU UNI 回線の帯域幅とサービス タイプ

Bandwidth	サービス タイプ (Service Type)
ODU0	• イーサネット OPU0 GMP

Bandwidth	サービス タイプ (Service Type)
ODU1	<ul style="list-style-type: none"> • OTN OPU1 • Sonet OPU1 BMP • SDH OPU1 BMP
ODU1E	<ul style="list-style-type: none"> • イーサネット OPU1e BMP • OTN OPU1e
ODU1F	<ul style="list-style-type: none"> • OTN OPU1f
ODU2	<ul style="list-style-type: none"> • イーサネット OPU2 GFP_F • イーサネット OPU2 GFP_F_EXT • イーサネット OPU2 WIS • OTN OPU2 • Sonet OPU2 AMP • Sonet OPU2 BMP • SDH OPU2 AMP • SDH OPU2 BMP
ODU2E	<ul style="list-style-type: none"> • イーサネット OPU2e BMP • OTN OPU2e
ODU2F	<ul style="list-style-type: none"> • OTN OPU2f
ODU4	<ul style="list-style-type: none"> • OTN OPU4 • イーサネット OPU4 GFP_F • イーサネット OPU4 GMP
ODUFLEX	<ul style="list-style-type: none"> • OTN OPUFlex • イーサネット OPUFlex GFP_F

ODU 回線の作成とプロビジョニング

ODU 回線を作成し、プロビジョニングするには、次の手順を実行します。

始める前に

- 光回線をプロビジョニングする前に満たす必要がある前提条件については、[光回線のプロビジョニングの前提条件 \(39 ページ\)](#) を参照してください。
- デバイス間に管理対象リンクを作成します。[トポロジマップへのリンクの手動による追加](#) を参照してください。

ステップ 1 左側のサイドバーから、[マップ (Maps)] > [トポロジマップ (Topology Maps)] > [ネットワーク トポロジ (Network Topology)] を選択します。

- ステップ 2** [デバイス グループ (Device Groups)] をクリックして、ODU 回線を作成する場所を選択します。
- ステップ 3** [デバイス グループ (Device Groups)] ポップアップ ウィンドウを閉じます。
- ステップ 4** [ネットワーク トポロジ (Network Topology)] ウィンドウで [回線/VC (Circuits/VCs)] をクリックします。
- ステップ 5** [回線/VC (Circuits/VCs)] タブをクリックし、[回線/VC (Circuits/VCs)] ペイン ツールバーで [+] ([作成 (Create)]) アイコンをクリックします。マップの右側の新しいペインでプロビジョニング ウィザードが開きます。
- プロビジョニング ウィザードを表示するもう 1 つの方法として、[設定 (Configuration)] > [ネットワーク (Network)] > [サービス プロビジョニング (Service Provisioning)] の順に選択する方法があります。
- ステップ 6** [テクノロジー (Technology)] ドロップダウン リストから [光 (Optical)] を選択すると、Cisco EPN Manager は関連する回線タイプのリストを [サービス タイプ (Service Type)] 領域に表示します。
- ステップ 7** [サービス タイプ (Service Type)] 領域で、[ODU] を選択します。
- ステップ 8** さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、[プロファイルの選択 (Select Profile)] ドロップダウン リストから必要なプロファイルを選択します。[回線/VC プロファイル \(134 ページ\)](#) を参照してください。
- ステップ 9** [次へ (Next)] をクリックして [顧客セクション (Customer Section)] ページに移動します。
- ステップ 10** (オプション) 回線の作成対象顧客を選択します。リストに顧客が表示されない場合は、[インベントリ (Inventory)] > [その他 (Other)] > [顧客 (Customers)] の順に移動し、システムで顧客を作成してから、プロビジョニング ウィザードを再起動します。
- ステップ 11** [顧客セクション (Customer Section)] ページに回線名とその説明を入力します。
- ステップ 12** [次へ (Next)] をクリックして [回線セクション (Circuit Section)] ページに移動します。
- ステップ 13** 回線には、次のいずれかの保護タイプを選択します。
- [なし (None)] : 回線の保護タイプなし。
 - [1+1] : プライマリパスとセカンダリパスの両方でトラフィックをエンドツーエンドに伝送します。受信側はプライマリパスとセカンダリパスの両方からトラフィックを受信し、両方のトラフィックを比較します。あるパスで出力ノードが障害を検出すると、トラフィックは影響を受けていないパスに切り替えられます。
- (注) 保護タイプとして [1+1] を選択した場合、[接続モード (Connection Mode)] はデフォルトで [SNC-N] に設定されます。
- ステップ 14** 回線に必要な [復帰時間 (Reversion Time)] と [保留タイマー (Hold off Timer)] を選択します。
- (注) これらのフィールドは、保護タイプとして [1+1] を選択した場合にのみ使用できます。
- ステップ 15** [次へ (Next)] をクリックして [エンドポイント セクション (Endpoint Section)] ページに移動します。
- ステップ 16** [エンドポイント (Endpoint)] テーブルの行を選択し、マップでデバイスをクリックします。選択したデバイスの名前が [デバイス名 (Device Name)] 列に読み込まれます。あるいは、[エンドポイント (Endpoint)] テーブルの行をクリックして、[デバイス名 (Device Name)] 列および [終端ポイント (Termination Point)] 列を編集します。選択した回線タイプと互換性があり使用可能なネットワーク要素だけが表示されます。

(注) 行が編集モードになっていると、マップ内のデバイスをクリックしても、[デバイス名 (Device Name)] 列に名前は取り込まれません。

ステップ 17 [次へ (Next)] をクリックして [制約セクション (Constraints Section)] ページに移動します。

ステップ 18 マップでデバイスノードをクリックし、[制約 (Constraints)] テーブルに追加します。あるいは、テーブルツールバーで [+] ボタンをクリックし、新しい行をテーブルに追加し、[ノード/リンク名 (Node/Link Name)]、[包含/除外 (Include/Exclude)]、および[ルート (Route)] 列を編集することもできます。ODU 回線タイプと互換性があるネットワーク要素のみが表示されます。

(注) ODU 回線の制約事項としてリンクを指定することはできません。

ステップ 19 (オプション) [パスの計算 (Calculate Path)] をクリックして、選択したエンドポイント間に有効な動作中のパスがあるかどうかを確認します。選択したエンドポイント間に有効な動作中のパスが存在する場合、パスはトポロジマップに「W」ラベルで表示されます。選択したエンドポイント間に有効な動作中のパスが存在しない場合は、選択したエンドポイント間に動作中のパスを確立できない理由を表示する [パスの計算結果 (Path Calculation Result)] セクションが表示されます。

ステップ 20 [今すぐ作成 (Create Now)] をクリックして、回線を作成します。デバイスに展開される TL1 または CLI コマンドのプレビューを表示する場合、[プレビュー (Preview)] をクリックするとプレビューが表示されます。この時点で、設定をデバイスに展開するか、またはキャンセルすることができますが、属性を編集することはできません。

[ネットワーク トポロジ (Network Topology)] ウィンドウの [回線/VC (Circuits/VCS)] ペインのリストに、回線が追加されます。プロビジョニング状態を確認するには、回線/VC 名の横にある [i] アイコンをクリックし、[回線/VC 360 (Circuit/VC 360)] ビューを表示します。

L3VPN サービスのプロビジョニング

- [サポートされている L3VPN サービス](#)
- [L3VPN プロビジョニングの機能と制限事項 \(71 ページ\)](#)
- [L3VPN プロビジョニングの前提条件 \(72 ページ\)](#)
- [L3VPN サービスの検出 \(73 ページ\)](#)
- [新規 L3VPN サービスの作成およびプロビジョニング \(74 ページ\)](#)
- [L3VPN サービスの詳細表示 \(91 ページ\)](#)
- [L3VPN および VRF の変更 \(94 ページ\)](#)
- [L3VPN サービスへの VRF の追加およびコピー \(95 ページ\)](#)
- [設定例 : L3VPN サービスのプロビジョニング \(89 ページ\)](#)

サポートされている L3VPN サービス

MPLS レイヤ 3 VPN はプライベート IP ネットワークを形成します。顧客はプロバイダー エッジ (PE) ルータの IP ピアとして機能するカスタマーエッジ (CE) ルータを介してネットワークに接続します。

仮想ルーティングおよび転送 (VRF)

PE では、仮想ルーティングおよび転送 (VRF) インスタンスが L3VPN サービスのトラフィック転送専用の仮想 IP ルータとして機能します。VRF は、マルチプロトコル ボーダー ゲートウェイ プロトコル (MP-BGP) を介して相互にルートを学習し、MPLS を使用してトラフィックを転送します。

VPN は少なくとも 1 つ、通常は複数の VRF で構成されます。Cisco EPN Manager は VPN ID を使用して、単一の VPN を一緒に形成する VRF を検出します。VPN ID がプロビジョニングされていない既存のネットワークを Cisco EPN Manager が検出すると、同じ名前のすべての VRF を取得し、それらを 1 つの VPN に関連付けます。バージョン番号プレフィックスと異なるサブプレフィックスによる命名規則を使用する Cisco PRIME プロビジョニングを使用して作成された VPN の場合、Cisco EPN Manager は異なる VRF を 1 つの VPN に属しているものとして認識します。

一般に、さまざまな命名規則を受け入れるように設定できる正規表現があります。

ルート ターゲット (RT)

VRF 間の接続は VRF によってインポートおよびエクスポートされるルートターゲット (RT) を使用して定義されます。Cisco EPN Manager は、フルメッシュ接続のセットアップを容易にし、使用するルートターゲットを自動的に割り当てます。ルートターゲットは、AS 番号または IPv4 アドレスのいずれかのプレフィックス (フルメッシュプレフィックス、100 [681682] など) で構成されます。プレフィックスは、ネットワーク内の既存の BGP 自律システム (AS) 番号から選択することも、手動で入力することもできます。プレフィックスに続く 2 番目の番号は Cisco EPN Manager によって自動的に割り当てられます。

あるいは、ルートターゲットを手動で選択することもでき、また、フルメッシュに加えてこれを行うこともできます。VPN の作成時に VPN 内で使用するルートターゲットを入力する初期画面が表示され、VRF ごとにインポートおよびエクスポートするルートターゲットを選択できます。また、ルートターゲットを使用するアドレスファミリ (IPv4 または IPv6) も指定します。これは、他の VPN で使用されるルートターゲットをインポートすることによって、エクストラネットを設定する場合などに使用できます。

ルートの再配布

PE と CE の間で交換されるルートは、リモートエンドポイントが各 VRF で到達できるプレフィックスがわかるように MP-BGP ルーティングプロトコルに再配布する必要があります。ルートの再配布を制御するため、Cisco EPN Manager では必要なプロトコル (OSPF、静的、接続済み、または RIP)、プロトコルのメトリック値、および必要に応じて適用可能なルートポリシーを定義できます。

エンドポイント

Cisco EPN Manager は、イーサネット サブインターフェイス上の IP エンドポイントの作成をサポートします。タグなしカプセル化の選択、あるいは 802.1q または 802.1ad のカプセル化を使用した、外部 VLAN と、必要に応じて内部 VLAN の指定をサポートします。エンドポイント上の IPv4 アドレスと IPv6 アドレスの両方を指定できます。また、BGP および OSPF ネイバーの詳細を指定して、CE と PE の間で BGP および OSPF ネイバーをプロビジョニングすることもできます。

Cisco EPN Manager を使用して L3VPN サービスをプロビジョニングする方法については、[L3VPN サービスのプロビジョニング \(69 ページ\)](#) を参照してください。

L3VPN プロビジョニングの機能と制限事項

Cisco EPN Manager は次の L3VPN 機能をサポートしています。

- VRF の作成。
- ルートターゲット ID の自動割り当て。
- ルート識別子の自動割り当て。
- 複数の条件 (VPN ID、共通名、およびプライム プロビジョニングの命名規則) に基づいて、複数の VRF で構成された VPN の検出。
- L3VPN プロビジョニング用のデバイスは、プロビジョニングをポイント アンド クリックの手法を使用して選択できます。
- VRF に付加された IP エンドポイントの定義。VRF とのイーサネット サブインターフェイスの関連付け。
- CE と PE 間での BGP または OSPF、あるいはその両方のネイバーのプロビジョニング。
- エンドポイント インターフェイスへの QoS プロファイルのアタッチ。
- 既存の VPN への新しい VRF の追加。
- Cisco EPN Manager を使用して作成し、展開された (または検出し、昇格させた) VPN と関連する VRF の変更。
- L3VPN サービスのネットワーク トポロジのオーバーレイ。
- デバイスから直接検出された L3VPN サービスの昇格。これは、検出されたサービスの変更と削除にさらに役立ちます。
- OSPF デュアル AS ルーティングによるルート ターゲットの使用。
- BDI/BVI インターフェイス (サブインターフェイス) を使用した L3VPN サービスをプロビジョニングするための、統合ルーティングとブリッジングの使用。
- IP サービス レベル契約 (SLA) および CLI テンプレートと L3VPN サービスとの関連付け。
- 接続されたルート、静的ルート、RIP ルート、または OSPF ルートを使用した PE-CE リンクと MP-BGP コア間でのルートの再配布。

- LAG インターフェイスを使用した L3VPN サービスのプロビジョニング。
- HSRP を使用している L3VPN サービスのプロビジョニング。

Cisco EPN Manager には、L3VPN に次の制限事項があります。

- VRF をサポートするデバイスのリストについては、[Cisco Evolved Programmable Network Manager のサポート対象デバイス](#)を参照してください。
- マルチキャスト VPN をプロビジョニングすることはできません。サポートされているのは、ユニキャスト VPN のみです。
- L3VPN サービスの作成中に、VPN に追加できる VRF は最大 5 つのみです。[VRF の変更 (Modify VRF)]オプションと [VRF の追加 (Add VRF)]オプションを使用して、後でより多くの VRF を VPN に追加できます。L3VPN サービスには、緑色のフィールドを使用してプロビジョニングされている場合、最大 15 個のエンドポイントを含めることができます。
- デバイスごとにサポートされているのは 1 つの VRF のみです。複数の VRF を作成できますが、異なるデバイス上で同じ VRF 名か、または異なる VRF 名を使用できます。
- ルート ポリシーは選択できますが、L3VPN サービス内で定義することはできません。
- PE-CE では、BGP、OSPF、および OSPFv3 ルーティング プロトコルのみがサポートされています。
- 複数の接続された PE はサポートされていないため、Site of Origin サポートもありません。
- L3VPN サービスを削除すると、サービスに関連付けられている IP SLA 操作がデバイスから削除されます。また、関連付された操作が削除されると、その操作はそれ以降は使用できなくなります。
- 統合ルーティングおよびブリッジング (IRB) は、Cisco Catalyst 6500 シリーズスイッチではサポートされていません。
- [Modify VRF] フローによるルート識別子の変更は、IOS XR デバイスでのみサポートされています。
- 最大 15 個のエンドポイントが、完全に検出された L3VPN サービスの昇格後の変更/削除でサポートされます。

L3VPN プロビジョニングの前提条件

L3VPN サービスのプロビジョニングを開始する前に、次の前提条件に従っていることを確認します。

L3VPN サービスをプロビジョニングするための前提条件は次のとおりです。

- BGP は、すべてのデバイス上に設定する必要があります。通常、すべてのデバイスは、ルート リフレクタのペアを介して相互に通信する必要があります。
- BGP のセットアップに必要な構成前の変更：

次の例に示すように、BGP ルータ ID を設定します。

```
router bgp 65300
  bgp router-id 1.1.1.1
```

次のコマンドを使用して、Vpn4 と Vpn6 を親アドレス ファミリとして設定します。

```
router bgp 100
  address-family vpnv4 unicast
  address-family vpnv6 unicast
```

- MPLS 到達可能性は、デバイス間で設定する必要があります。MPLS コア ネットワーク設定をセットアップする必要があります。
- L3VPN サービスがプロビジョニングされるデバイスのインベントリ収集ステータスが [完了済み (Completed)] である必要があります。デバイスのステータスを確認するには、[インベントリ (Inventory)] > [ネットワーク デバイス (Network Devices)] に移動し、[最新のインベントリ収集ステータス (Last Inventory Collection Status)] 列のステータスを確認します。
- XE デバイスで IPv6 アドレスファミリを使用して L3VPN サービスをプロビジョニングする前に、IPv6 ルーティングを有効にする必要があります。IPv6 ルーティングを有効にするには、次のコマンドを設定します。

```
ipv6 unicast-routing
```

- (オプション) L3VPN サービスのプロビジョニング時に L3VPN サービスを顧客に関連付けられるように、システム内に顧客を作成する必要があります。顧客を作成し、管理するには、[インベントリ Inventory] > [その他 (Other)] > [顧客 (Customers)] を選択します。

L3VPN サービスの検出

Cisco EPN Manager は、複数の条件を使用して複数の VRF を 1 つの VPN に関連付けます。

- VRF が VPN ID で設定されている場合：VPN サービスは VPN ID を使用して検出され、同じ VPN に属している VRF を識別します。検出する必要がある VPN があり、1 つの VPN 内で異なる VRF 名が使用されている場合、Cisco EPN Manager は VRF 名によって VRF を検出します。

デバイスごとに作成される VRF が 1 つのみの場合は、VPN 上のあらゆる場所で同じ VRF 名を使用するのが一般的です。Cisco EPN Manager が同じ名前でも VPN ID のない複数の VRF を確認した場合は、それらを単一の VPN と見なし、VPN 名は VRF の名前になります。

- 最初にプライム プロビジョニングを使用してプロビジョニングされた VPN の場合：Cisco EPN Manager はプライム プロビジョニング VRF 命名規則も認識します。プライム プロビジョニングで使用される命名規則は、次の形式です。

```
V<number>:<VPN name><optional suffix, one of -s -h -etc>
```

同じ名前と番号を持つ VRF は、同じ VPN に属しています。たとえば、「ABC」と呼ばれる VPN に属している VRF は次のとおりです。

V1:ABC、V2:ABC、V4:ABC-s、V22:ABC-h、V001:ABC など

- VRF に VPNID がなく、プライムプロビジョニング規則に従って他の名前と一致しない一意の名前を持つ場合は、単独で VPN に配置されます。VPN の名前は VRF の名前になります。

プライムプロビジョニング命名規則機能は、製品に埋め込まれた正規表現によって駆動されます。VPN の設定がオプションではなく、正規表現と一致する可能性がある命名規則がある場合は、その正規表現を変更できます。正規表現を変更するには、シスコアドバンスドサービス担当者にお問い合わせください。

新規 L3VPN サービスの作成およびプロビジョニング

ユニキャスト L3VPN の作成およびプロビジョニングプロセスには、次の作業が含まれます。

- (オプション) 顧客を VPN に関連付ける。
- L3VPN を経由してエンドポイントまで伝送されるトラフィックの処理方法に影響する属性の定義。
- L3VPN のエンドポイントおよびルート再配布値の指定。
- (オプション) IPv4 または IPv6 を使用するデバイス間のエンドツーエンド応答所要時間をモニタするための IP サービス レベル契約 (SLA) 動作を設定する。
- (オプション) ユーザ定義の CLI テンプレートを L3VPN サービスと関連付ける。

注：このリリースではユニキャスト L3VPN サービスのみがサポートされます。

新しい L3VPN サービスを作成するには、次の手順を実行します。

-
- ステップ 1** 左側のペインから、[マップ (Maps)] > [トポロジマップ (Topology Maps)] > [ネットワーク トポロジ (Network Topology)] を選択します。
- [ネットワーク トポロジ (Network Topology)] ウィンドウが開きます。
- ステップ 2** ツールバーで [デバイス グループ (Device Groups)] をクリックし、マップ上に表示するデバイスのグループを選択します。
- ステップ 3** [回線/VC (Circuits/VCs)] タブをクリックし、[回線/VC (Circuits/VCs)] ペインツールバーで [+] ([作成 (Create)]) アイコンをクリックします。
- マップの右側の新しいペインでプロビジョニングウィザードが開きます。あるいは、[設定 (Configuration)] > [ネットワーク (Network)] > [サービスのプロビジョニング (Service Provisioning)] を選択して L3VPN プロビジョニングウィザードにアクセスすることもできます。
- ステップ 4** [テクノロジー (Technology)] ドロップダウンリストから [L3VPN] を選択します。サポートされている L3VPN サービス タイプの一覧が表示されます。

- ステップ5** [サービス タイプ (Service Type)] セクションで、[ユニキャスト (Unicast)] を選択し、[次へ (Next)] をクリックして顧客とサービスの詳細を入力します。このリリースでサポートされているサービスタイプは、ユニキャスト L3VPN のみです。
- ステップ6** さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、[プロファイルの選択 (Select Profile)] ドロップダウンリストから必要なプロファイルを選択します。
- ステップ7** (オプション) VPNに関連付ける顧客を選択します。ドロップダウンリストに顧客が表示されていない場合は、[インベントリ (Inventory)] > [その他 (Other)] > [顧客 (Customers)] を選択して顧客を作成し、この手順に戻ります。
- ステップ8** 基本的な L3VPN パラメータを次のように指定します。
- [アクティブ化 (Activate)] チェックボックスを使用して、サービスをアクティブ状態にするか (チェックボックスがオン) 、それとも非アクティブにするか (チェックボックスがオフ) を指定します。アクティブ状態の場合、トラフィックが回線を通過できるようになり、関連付けられているすべての IP エンドポイントのサービス状態が自動的に True に設定されます。非アクティブ状態の場合は、IP エンドポイントのサービス状態を True または False に設定できます。
 - 一意のサービス名を指定し、オプションで説明を入力します。
 - サービスの一意の VPN ID を入力します。VPN ID は、OUI:VPN インデックス形式である必要があります。たとえば、36B:3 などです。ここでは、36B は組織固有識別子 (OUI) であり、3 は VPN インデックスです。
 - [IP MTU] フィールドに、値を 1522 (デフォルト) ~ 9216 の範囲で入力します。サービス MTU は、L3VPN 経由で非フラグメント化された状態で伝送できる最大 IP パケットサイズ (バイト数) です。これにはレイヤ 2 ヘッダーは含まれません。
設定されるインターフェイス MTU は、サービス MTU にすべてのレイヤ 2 ヘッダーのサイズを追加したものです。イーサネットの場合は、これによって 14 バイトおよび VLAN ヘッダーごとに 4 バイトが追加されます。
UNI MTU の値は、サービス MTU と外部および内部の VLAN 値によって異なります。
 - 外部および内部 VLAN の両方が存在する場合、UNI MTU 値はサービス MTU + 14 + (4*2) より大きくなります。
 - 外部 VLAN のみが存在する場合、UNI MTU 値はサービス MTU + 14 + (4*1) より大きくなります。
 - VLAN が存在しない場合、UNI MTU 値はサービス MTU + 14 より大きくなります。
- e) (オプション) このサービスのフルメッシュトポロジを作成するには、[フルメッシュの作成 (Create Full Mesh)] チェックボックスをオンにし、フルメッシュプレフィックスを [新規プレフィックス (New Prefix)] フィールドに手動で入力するか、[既存のプレフィックス (Existing Prefix)] ドロップダウンリストから値を選択します。使用可能なオプションは、選択されたデバイスから検出されたフルメッシュプレフィックス値によって異なります。
- f) アドレスファミリを [フルメッシュアドレスファミリ (Full Mesh Address Family)] ドロップダウンリストから [IPv4]、[IPv6]、または [両方 (Both)] として選択します。
- ステップ9** [ルート ターゲットの割り当て (Route Target Allocation)] セクションを使用して、ルート ターゲットアドレスファミリ ([IPv4]、[IPv6]、または [両方 (Both)]) および関連付けられているルートターゲット値を手動で指定します。1つの L3VPN サービスに複数のルートターゲットを作成できます。次の手順で

この L3VPN サービスに接続させる任意の VRF に、これらのルート ターゲットを関連付けることができます。

(注) また、VRF に関連付けられたルート ターゲットを、VRF が属する L3VPN にも関連付ける必要があります。

(注) 設定されたルートポリシーが、ルートポリシーの [エクスポート (Export)] ドロップダウンリストに表示されます。

ステップ 10 [展開アクション (Deployment Action)] ドロップダウン メニューで、サービス作成プロセスの完了時に実行する必要があるタスクを指定します。選択できるオプションは、次のとおりです。

- [プレビュー (Preview)] : デバイスに展開する前に、生成された設定を確認できます。
- [展開 (Deploy)] : 完了したらすぐに、該当するデバイスに設定を展開できます。

ステップ 11 [次へ (Next)] をクリックして、VRF を L3VPN サービスに関連付けます。

ステップ 12 [VRF (VRFs)] ドロップダウン リストから必要な VRF を選択するか、または以下の説明に従って新しい VRF を追加し、[次へ (Next)] をクリックします。L3VPN サービスの作成中に、最大 5 つの VRF を VPN に関連付けることができます。さらに多くの VRF を VPN に関連付けるには、[L3VPN サービスへの VRF の追加およびコピー \(95 ページ\)](#) を参照してください。新しい VRF を作成するには、次の手順を実行します。

1. [+] アイコンをクリックして、VRF の詳細を手動で追加します。VRF の詳細を自動入力するには、マップ上で該当するデバイスをクリックします。デバイスの詳細および VRF の新しい名前が自動的に [VRF の追加 (Add VRFs)] ページに入力されます。
2. 手動で VRF の詳細を指定するには、[デバイス (Device)] ドロップダウン リストから必要なデバイスを選択します。その後、VRF 名と説明を手動で入力し、[RD 自動] チェックボックスをオンにします。

(注) 同じデバイスに複数の VRF を作成する場合は、それらが同じ VPN に属さないようにするために、それぞれ異なる名前を付ける必要があります。同じデバイス上に同じ名前で複数の VRF を作成することはできません。

ステップ 13 IPv4 および IPv6 ルート ターゲットとルート配布詳細を次のように指定します。

1. ルート ターゲット : [ルート ターゲット (Route Target)] ドロップダウン メニューから、この VRF のルート ターゲットを選択します。このドロップダウン メニューに表示されるオプションは、ステップ 7 でこのサービスに関連付けられたルート ターゲットによって決まります。
2. ルートターゲットを適用する方向を選択します。選択したデバイスに応じて、[インポート (Import)]、[エクスポート (Export)]、[両方 (Both)]、または [なし (None)] を選択します。
選択したデバイスのタイプに従って方向を選択します。たとえば Cisco IOS-XR デバイスの場合は、ルート ターゲットの方向として [なし (None)] を選択できません。
3. [ルート ポリシー (Route Policy)] セクションで、ルート ターゲットのインポートおよびエクスポート ポリシーを指定します。

(注) オpaque拡張コミュニティ (Opaque Extended Community) が接続されている [ルートポリシー (Route Policy)] は、エクスポートにのみ適用されます。

4. [ルート配布 (Route Distribution)] セクションで、VRF に関連付ける必要があるプロトコル、プロトコルのメトリック値、ルーティングプロセスID、関連するルートポリシー、およびルート一致タイプを指定します。

- [プロトコル (Protocol)] : ルートの再配布元となる必要がある送信元プロトコルを選択します。選択できるオプションは、[静的 (Static)]、[接続 (Connected)]、[RIP]、および [OSPF] です。
- [メトリック (Metric)] : (オプション) 同じルータ上のルーティングプロセス間で再配布時に使用するメトリックの数値を入力します。
- [ルーティングプロセスID (Routing Process ID)] : (OSPF および RIP のみに適用可能) デバイス上のルーティングプロセスのインスタンスを識別する一意の数値を指定します。
- [ルートポリシー (Route Policy)] : (オプション) 選択したデバイス上に存在するいずれかのルートポリシーを選択します。Cisco EPN Manager を使用してルートポリシーを作成することはできません。

(注) オpaque拡張コミュニティ (Opaque Extended Community) が接続されている [ルートポリシー (Route Policy)] は、再配布では使用できません。

- [ルート一致タイプ (Route Match Type)] (OSPF にのみ適用可能) : 選択したルートポリシーに関連付けられている一致タイプをドロップダウンリストから指定します。

ステップ 14 IP エンドポイントおよび UNI の値を、次のように手動で指定します。

- エンドポイント インターフェイスがすでに UNI として設定されている場合は、[新規 UNI (New UNI)] チェックボックスをオフにし、[UNI名 (UNI Name)] ドロップダウンリストから必要なUNIを選択します。
- 新しい UNI を作成するには、次の手順を実行します。
 1. [新規 UNI (New UNI)] チェックボックスをオンにします。
 2. [UNI名 (UNI Name)] フィールドに、UNI の一意の名前を入力します。
 3. [デバイス (Device)] ドロップダウンで、デバイス、およびデバイスに必要なインターフェイスを選択して、UNI の説明を入力します。
 4. [サービス多重化 (Service Multiplexing)] チェックボックスをオンにして、複数の L3VPN またはキャリアイーサネットサービスを UNI でサポートできるようにします。
 5. UNI の IP 最大伝送ユニット (MTU) (UNI の速度とデュプレックスの設定) を指定します。
 6. [自動ネゴシエーション (Auto Negotiation)] チェックボックスをオンにして UNI の速度とデュプレックスの設定を自動的に調整するか、[自動ネゴシエーション (Auto Negotiation)] チェックボックスをオフにして速度とデュプレックスの設定を手動で指定します。

7. UNI での入力または出力トラフィック用の UNI QoS プロファイルを選択します。プロファイルの一覧には、デバイスで設定されシステムで検出されたポリシー マップと、ユーザ定義の QoS プロファイルが含まれます。UNI QoS プロファイルを選択した場合は、これ以降の手順でサービス エンドポイントに個別の QoS ポリシーを追加できません。エンドポイントに特定の QoS ポリシーを追加するには、[UNI 入力 QoS プロファイル (UNI Ingress QoS Profile)] および [UNI 出力 QoS プロファイル (Egress QoS Profile)] フィールドの両方を空のままにしてください。

(注) 入力および出力方向に対し、検出された 2 つの異なる QoS プロファイルを選択できますが、ユーザ定義 QoS プロファイルの場合は両方の方向に 1 つの QoS プロファイルだけを選択できます。

8. [リンク OAM の有効化 (Enable Link OAM)] を選択して IEEE 803.1ah リンクの動作およびメンテナンスを有効にします。リンク OAM が有効な場合、この UNI と顧客のアクセス スイッチの間のリンク状態に関連するイベントが表示されます。
9. [リンク管理の有効化 (Enable Link Management)] を選択すると、顧客のアクセス スイッチでこの UNI、VLAN ID、UNI 上のサービスなどの情報を取得できるようになります。

UNI テーブルのフィールドおよび属性の詳細については、[新規 UNI の詳細リファレンス \(23 ページ\)](#) を参照してください。

ステップ 15 次の詳細を設定することで L3VPN に関連付けるサービス エンドポイントを指定し、[次へ (Next)] をクリックします。

- [VRF 名 (VRF Name)]: この VPN に関連付けることができる VRF を 1 つ選択します。
- [IPv4 および IPv6 アドレス (IPv4 and IPv6 address)]: サービス エンドポイントの IP アドレスおよびネットワーク マスクを入力します。単にネットワーク マスクの長さを表す整数としてマスクを入力できます (または CIDR 形式も可能です)。
- [VLAN および内部 VLAN (VLAN and Inner VLANs)]: 1 ~ 4094 までの整数を使用して、内部および外部の VLAN の識別子を入力します。内部 VLAN は、VLAN タギングの第 2 レベルの識別子です。
- [QoS ポリシー (QoS Policy)]: (オプション) サービス エンドポイントに適用する必要がある QoS ポリシーを選択します。上記のステップで UNI 入力/出力 QoS プロファイルをサービスに関連付けた場合は、このフィールドが無効になります。QoS プロファイルの作成については、[Quality of Service \(QoS\) の設定](#) を参照してください。

(注) 入力および出力方向に対し、検出された 2 つの異なる QoS ポリシーを選択できますが、ユーザ定義の QoS ポリシーの場合は両方の方向に 1 つの QoS ポリシーだけを選択できません。

- [サービス状態 (Service State)]: 関連付けられた IP エンドポイントのサービス状態を True または False のいずれかに設定する必要があるかを指定します。L3VPN がアクティブ状態の場合 (上記のステップ 6 で指定)、このチェックボックスは無効になり、すべてのサービス状態値が自動的に True に設定されます。

- [統合ルーティングおよびブリッジングの使用 (Use Integrated Routing & Bridging)] : サブインターフェイスまたは BVI (仮想) インターフェイスで VRF および IP アドレスを設定する必要があるかどうかを指定します。
 - (注) このチェックボックスは、統合ルーティングおよびブリッジングをサポートするデバイス (Cisco ASR90XX デバイスなど) を選択している場合にのみ有効になります。Cisco ASR90x およびその他の IOS-XE デバイスでは、BDI インターフェイスによって設定が処理されるため、[Use Integrated Routing & Bridging] チェックボックスをオフにすることはできません。
- (オプション) HSRP の詳細を指定するには、[HSRP の有効化 (Enable HSRP)] チェックボックスをオンにします。 [HSRP の詳細のリファレンス \(83 ページ\)](#) を参照してください。

ステップ 16 [次へ (Next)] をクリックして、[PE-CE ルーティング (PE-CE Routing)] ページに移動します。

ステップ 17 [+] アイコンをクリックして、PE-CE ルーティングの詳細を追加します。 [PE-CE ルーティングの詳細のリファレンス \(85 ページ\)](#) を参照してください。

ステップ 18 (オプション) 一覧から既存の IP SLA パラメータを選択するか、以下の表で説明する IP SLA 動作パラメータを指定して、[次へ (Next)] をクリックします。

IP SLA 設定	IP SLA パラメータ	説明
動作設定	[名前 (Name)]	選択した L3VPN サービスに関する IP SLA 動作を識別する一意の名前を入力します。
	タイプ (Type)	この L3VPN サービスに参加するデバイス用に生成する必要がある IP SLA 動作のタイプを選択します。選択できるオプションは、次のとおりです。 <ul style="list-style-type: none"> • [UDP エコー (UDP Echo)] : 応答所要時間を測定し、シスコデバイスと IPv4 または IPv6 を使用するデバイス間のエンドツーエンド接続をテストするように、IP SLA の User Datagram Protocol (UDP) エコー動作を設定します。 • [ICMP エコー (ICMP Echo)] : シスコデバイスと、IPv4 または IPv6 を使用するその他のデバイス (後述する送信元/宛先値) との間のエンドツーエンドネットワーク応答所要時間を測定できるようにします。[ICMP エコー (ICMP Echo)] タイプの IP SLA 動作で、[接続損失 (Connection Loss)] アクション変数を関連付けることはできません。 • [UDP ジッター (UDP Jitter)] UDP ジッター動作を設定します。これにより、IPv4 または IPv6 ネットワークで UDP トラフィックを伝送するネットワークのラウンドトリップ遅延、一方向遅延、一方向ジッター、一方向パケット損失、および接続を分析できます。
	ソース (Source)	IP SLA 設定の生成の送信元ポイントとして機能するデバイスを指定します。IP SLA 応答は、この送信元デバイスと宛先デバイス間の接続に基づいて生成されます。この動作の VRF 値は、送信元の選択に応じて自動的に選択されます。
	送信元ポート (Source Port)	0 ~ 65535 の範囲の数値を 1 つ入力し、IP SLA 動作の設定対象となる送信元ポートの値を指定します。
	[接続先 (Destination)]	IP SLA 設定の生成の宛先ポイントとして機能するデバイスを指定します。IP SLA 応答は、送信元デバイスとこの宛先デバイス間の接続に基づいて生成されます。
	[宛先ポート (Destination Port)]	0 ~ 65535 の範囲の数値を 1 つ入力し、IP SLA 動作の生成対象となる宛先ポート値を指定します。
	VRF	VRF の詳細は、IP SLA 動作の送信元として指定したデバイスに基づいて自動的に選択されます。

IP SLA 設定	IP SLA パラメータ	説明
反応設定	アクション変数 (Action Variable)	<p>IP SLA 反応をトリガーする条件となる変数を選択します。たとえば、モニタリング対象の値が指定のレベルを超えるか下回った場合、またはタイムアウトや接続損失などのモニタリング対象のイベントが発生した場合です。</p> <ul style="list-style-type: none"> • [接続損失 (Connection Loss)] : 接続損失が発生した場合にイベントをトリガーする必要があることを指定します。動作のタイプとして [ICPM エコー (ICPM Echo)] を選択した場合、この値は表示されません。 • [ラウンドトリップ時間 (Round Trip Time)] : このアクション変数を選択した場合、[上限しきい値 (Upper Threshold Value)] および [下限しきい値 (Lower Threshold Value)] を入力する必要があります。これらは、モニタリング対象の値が特定の上限しきい値を超えるか下限を下回った場合に、イベントをトリガーする必要があることを示します。 • [タイムアウト (Time Out)] : 指定された一連のタイムアウトが連続して発生した場合に、イベントをトリガーする必要があることを示します。 • [エラーの確認 (Verify Error)] : VerifyError タイプのエラーが発生した場合に、イベントをトリガーする必要があることを示します。
	アクションタイプ	<p>[アクション変数 (Action Variable)] フィールドに設定された条件に基づいて実行する必要があるアクションを、次の中から 1 つ選択します。</p> <ul style="list-style-type: none"> • [なし (None)] : アクションは実行されません。 • [トラップおよびトリガー (Trap and Trigger)] : 違反条件に一致した場合に、以下の [トラップのみ (Trap Only)] および [トリガーのみ (Trigger Only)] オプションの定義に従って、両方の SNMP トラップをトリガーし、別の IP SLA 動作を開始します。 • [トラップのみ (Trap Only)] : モニタ対象の要素で特定の違反タイプが発生した場合に、SNMP ロギングトラップを送信します。 • [トリガーのみ (Trigger Only)] : 違反条件に一致した場合に、1 つ以上のターゲット動作の動作状態を [保留 (pending)] から [アクティブ (active)] に変更します。ターゲット動作は、ターゲット動作のライフタイム値の設定に従い、その存続期間が満了するまで続行されます。トリガーされたターゲット動作が再びトリガーされるには、その前に存続期間が終了している必要があります。

IP SLA 設定	IP SLA パラメータ	説明
	しきい値タイプ (Threshold Type)	<p>IP SLA イベントの生成条件とするしきい値タイプを選択します。</p> <ul style="list-style-type: none"> • [平均 (Average)]: このしきい値タイプを選択する場合は、[N 値 (N Value)]を入力します。これは、指定された上限しきい値を超えるか下限しきい値を下回り、N プローブの合計値の平均に達した場合に、イベントをトリガーする必要があることを示します。 • [連続 (Consecutive)]: このしきい値タイプを選択する場合は、反応設定の一部として [連続値 (Consecutive Values)]を入力してください。このしきい値タイプは、指定回数を超過して違反が連続発生した場合にのみ、イベントをトリガーします。たとえば連続値 5 を入力して連続違反タイプを使用した場合、タイムアウトが 5 回連続して発生した場合、またはラウンドトリップ時間が上限しきい値を 5 回連続して超えた場合にアクションが実行されます。 • [即時 (Immediate)]: 反応タイプ (応答所要時間など) の値が上限しきい値を超えるか下限しきい値を下回った場合、またはタイムアウト、接続の切断、エラーの確認イベントが発生した場合に、即座にイベントをトリガーします。 • [しない (Never)]: イベントをトリガーしません。 • [X/Y 回 (X out of Y occurrences)]: このしきい値タイプを選択した場合は、[X 値 (X Values)]および[Y 値 (Y Values)]を入力して、発生回数を指定します。これを選択すると、y 回のプローブ動作内に x 回の違反が発生した場合に (x 回/y 回)、イベントがトリガーされます。

IP SLA 設定	IP SLA パラメータ	説明
単純なスケジュール (Simple Schedule)	-	<p>次の値を入力して、個別の IP SLA 動作のスケジュールパラメータを入力します。</p> <ul style="list-style-type: none"> • [頻度 (Frequency)] : 経過時間を秒数で入力します。この時間内に動作が繰り返されます。 • [ライフタイム (Life Time)] : 動作がアクティブ状態に保たれる時間の合計を秒数で入力します。単一の動作は、その動作のライフタイム中に、指定された頻度で繰り返し実行されます。 • [エージアウトする (Age Out)] : 動作をアクティブ状態に保つ時間の長さを秒数で入力します。たとえば、エージアウトの値を 43200 に指定すると、非アクティブ状態が 12 時間続いた後で動作がエージアウトします。 • [今すぐ開始 (Start Now)] および [後で開始 (Start After)] : [今すぐ開始 (Start Now)] チェックボックスをオンにすると、保存後ただちに IP SLA 動作を実行するようにスケジュールされます。または [後で開始 (Start After)] フィールドを使用し、分数を指定すると、その経過後に動作が実行されます。

ステップ 19 (オプション) [サービス テンプレート (Service Template)] ページを使用すると、サービスに参加するデバイスに設定される追加の CLI コマンドを含むテンプレートを付加できます。詳細については、[テンプレートを使用した回線/VC の拡張 \(138 ページ\)](#) を参照してください。

ステップ 20 サービスに必要な情報をすべて入力したら、[送信 (Submit)] をクリックします。デバイスに展開される CLI のプレビューを表示することを選択した場合、プレビューがこの時点で表示され、[属性の編集 (Edit Attributes)] をクリックして L3VPN 属性を変更できます。そうでない場合は、設定が即座にデバイスに展開されます。

サービスに参加しているデバイスのうち 1 台でも展開に失敗した場合は、サービスに参加しているすべてのデバイスで設定がロールバックされます。サービスに関連付けられているエンドポイントを削除するには、[L3VPN サービス エンドポイントの削除](#) を参照してください。この L3VPN サービスにさらに VRF を追加するには、[L3VPN サービスへの VRF の追加およびコピー \(95 ページ\)](#) を参照してください。

HSRP の詳細のリファレンス

Hot Standby Router Protocol (HSRP) は、デフォルト ゲートウェイ IP アドレスが設定された IEEE 802 LAN 上の IP ホストにファースト ホップ冗長性を確保することでネットワークの可用性を高めるシスコの標準方式です。Hot Standby Router Protocol (HSRP) は、IP ネットワークに冗長性をもたらし、ユーザトラフィックが確実に最初のホップルータ障害から即座かつ透過的に回復できるようにします。HSRP を使用すると、1 つの LAN 上の複数のルータが、ホス

ト上のデフォルト ゲートウェイとして設定された仮想 IP と MAC アドレスを共有できます。HSRP グループで設定されたルータのグループから、アクティブルータとして選択された 1 台のルータと、スタンバイルータとして選択されたもう 1 台のルータがあります。アクティブルータは、仮想 IP アドレスに送信されるパケットを転送するロールを担います。アクティブルータで障害が発生すると、スタンバイルータが新しいアクティブルータのロールを引き継ぎます。Cisco EPN Manager では、IP ベースまたは IP サービスイメージを実行するスイッチでは IPv4 用の HSRP がサポートされており、IPv6 用の HSRP はユニキャストルーティングでサポートされています。HSRP は、アドレスファミリ IPv6 の IOS-XE デバイスではサポートされていません。次の表に、HSRP 属性のリストを示し、説明します。

表 12: HSRP 設定

属性	説明
グループ番号 (Group Number)	IOS-XE デバイスまたは IOS-XR デバイスのスタンバイ グループ番号を入力します。推奨される値の範囲は次のとおりです。 <ul style="list-style-type: none"> • IOS-XE : 値は 1 ~ 255 の間である必要があります。 • IOS-XR : 値は 1 ~ 4095 の間である必要があります。
仮想 IP (Virtual IP)	IPv4/IPv6 アドレスを入力します。仮想 IP アドレスと SEP アドレスが同じサブネット内に入力されていることを確認します。
プライオリティ (Priority)	優先度を入力して、プライマリルータにするルータを決定します。
Hello タイマー (Hello Timer)	hello パケット間の時間を秒単位で入力します。 (注) [Hello タイマー (Hello Timer)] と [最小遅延 (Minimum Delay)] の値を指定した IOS-XR デバイスでは、[ホールドタイマー (Hold Timer)] と [リロード遅延 (Reload Delay)] の値を入力する必要があります。
最小遅延 (Minimum Delay)	最小遅延時間を秒単位で入力します。
プリエンプト最小遅延 (Preempt Minimum Delay)	ルータのプリエンプト遅延を指定します。
認証キー (Authentication Key)	グループ番号が 1 ~ 255 の場合は、認証キーを入力します。これにより、認証メッセージを HSRP マルチキャストに含めることができます。これにより、承認されたルータのみが HSRP グループに確実に含まれます。
ホールドタイマー (Hold Timer)	保留時間を秒単位で入力します。 (注) 保留時間は、XE デバイスの hello タイマーよりも長くする必要があります。
リロード遅延 (Reload Delay)	リロードの遅延時間を入力します。

属性	説明
プリエンブトリロード遅延 (Preempt Reload Delay)	プリエンブト再読み込み遅延を入力します。 このフィールドは、IOS-XR デバイスではサポートされていません。

PE-CE ルーティングの詳細のリファレンス

次の表に、レイヤ 3 VPN サービスをプロビジョニングするための PE-CE を定義する属性のリストを示し、説明します。

表 13: PE-CE ルーティングのリファレンス

属性	説明
ルーティング プロトコル設定 (Routing Protocol Settings)	
PE デバイス (PE Device)	擬似回線デバイスの名前。
VRF	ウィザードの [VRF] ページで指定した VRF 名が読み込まれています。
ルーティングプロトコルタイプ (Routing Protocol Type)	[BGP]、[OSPF]、または [OSPFv3] をレイヤ 3 VPN サービスのルーティングプロトコルとして選択します。 (注) 選択したルーティングプロトコルに基づいて、[BGP ネイバー情報 (BGP Neighbor Information)] セクションまたは [OSPF プロセス情報 (OSPF Process Information)] セクションが表示されます。 XR デバイスおよび XE デバイスの場合、PE-CE 認証はルーティングプロトコルタイプと認証タイプの選択に基づきます。詳細については、「 PE-CE 認証 」テーブルを参照してください。
アドレスファミリ (Address Family)	アドレスファミリを IPv4 または IPv6 として選択します。 (注) IPv6 は OSPF ルーティングプロトコルではサポートされていません。
認証タイプ (Authentication Type)	認証タイプを選択します。MD5 認証タイプのみがサポートされます。 (注) [認証タイプ (Authentication Type)] フィールドは、ルーティングプロトコルとして OSPF または OSPFv3 を選択した場合にのみ使用できます。

属性	説明
BGP ネイバー情報 (BGP Neighbor information)	
(注) このセクションは、ルーティングプロトコルとして BGP を選択した場合にのみ使用できます。	
ネイバー アドレス (Neighbor Address)	ネイバーの IP アドレスを入力します。
ネイバー AS (Neighbor AS)	このネイバーの自律システム番号を入力します。これは、BGP ネイバーとのピアリングセッションを確立するために使用される固有識別子です。
入力ルート ポリシー (Ingress Route Policy)	このネイバーから受信した BGP ルートに適用されるルート ポリシーを入力します。
出力ルート ポリシー (Egress Route Policy)	このネイバーに送信されるルートに適用するルート ポリシーを入力します。
ローカル AS (Local AS)	BGP ネイバーとのピアリングセッションを確立するために使用される固有のローカル識別子を入力します。
AS アクション (AS Action)	ローカル自律システム (AS) 番号に関連付ける必要があるアクションタイプを、次の中から 1 つ選択します。 <ul style="list-style-type: none"> • [付加 (Prepend)] : このオプションを使用すると、ネイバーから受信するルートに AS 番号を付加するように BGP が設定されます。 • [付加しない (No Prepend)] : このオプションを使用すると、ネイバーから受信するルートに AS 番号を付加しないように BGP が設定されます。 • [付加しない (No Prepend)]、[AS を置換 (Replace AS)] : [AS を置換 (Replace AS)] を使用すると、(ip-address で設定された) ローカル AS 番号のみが AS_PATH 属性に付加されます。ローカル BGP ルーティングプロセスからの AS 番号は付加されません。 • [付加しない (No Prepend)]、[AS を置換 (Replace AS)]、[デュアル AS (Dual AS)] : [デュアル AS (Dual AS)] オプションを使用すると、ローカル BGP ルーティングプロセスから取得した AS 番号、または ip-address 引数 (local-as) で設定された AS 番号を使用してピアリングセッションを確立するように eBGP ネイバーが設定されます。

属性	説明
OSPF プロセス情報 (OSPF Process Information)	
(注) このセクションは、ルーティング プロトコルとして OSPF または OSPFv3 を選択した場合にのみ使用できます。	
ルータ ID (Router ID)	OSPF プロトコルの IPv4 アドレスを指定します。
エリア ID (Area ID)	OSPF プロトコルのエリアを定義します。有効範囲は 0 ~ 4294967295 です。
メトリック	OSPF プロトコルの数値を指定します。
ドメイン タイプ (Domain Type)	必要なドメイン タイプを選択します。
ドメイン値 (Domain Value)	6 オクテットの 16 進数形式でドメイン値を入力します。たとえば、00000000000F などです。
BFD 最小間隔 (BFD Min Interval)	制御パケットがネイバーに送信される最小間隔を入力します。範囲は 3 ~ 30000 ミリ秒です。 (注) このフィールドは、Cisco IOS-XR デバイスでのみ使用できます。
BFD の乗数 (BFD Multiplier)	この乗数は、BFD がネイバーのダウンを宣言するまでのパケットが失われる回数です。OSPF プロトコルの範囲は 2 ~ 50 です。 (注) このフィールドは、Cisco IOS-XR デバイスでのみ使用できます。
BFD 高速検出 (BFD Fast Detect)	隣接する転送エンジン間のパスで障害を迅速に検出するには、このチェックボックスをオンにします。 (注) このフィールドは、Cisco IOS-XR デバイスでのみ使用できます。



- (注) EPNM では、対象の L3VPN インスタンスの PE-CE ルーティング用に作成できる OSPF プロセスは 1 つだけです。XE プラットフォームの場合はこれで十分です。これは、単一の OSPFv3 プロセスで IPv4 と IPv6 の両方のアドレスファミリを管理できるためです。ただし、IOS-XR プラットフォームでは、OSPFv3 は IPv6 のみをサポートしており、IPv4 はサポートしていません。そのため、IPv4 と IPv6 の両方のアドレスファミリを使用する場合は、EPNM から OSPF と OSPFv3 の両方のプロセスを作成する必要があります。

PE-CE 認証

次の表に、XE デバイスと XR デバイスの選択に基づいた PE-CE 認証のルーティング プロトコルと認証タイプの関連する組み合わせのリストを示します。

表 14: PE-CE 認証のリファレンス

デバイス (Device)	ルーティング プロトコル (Routing Protocol)	認証タイプ (Authentication Type)	パスワードタイプ (Password Type)
XE	BGP	—	次のオプション ボタンのいずれかをクリックします。 <ul style="list-style-type: none"> • [プレーン テキスト (Plain Text)]: パスワードを入力できるようにします。 • [暗号化 (Encrypted)]: パスワードとして 16 進数値を入力できるようにします。
	OSPF	—	—
	OSPFv3	キーチェーン認証タイプのみが使用できます。 [キーチェーン (Key Chain)] ドロップダウンリストから、デバイス上に設定されている認証キーチェーンを選択します。	—

デバイス (Device)	ルーティングプロトコル (Routing Protocol)	認証タイプ (Authentication Type)	パスワードタイプ (Password Type)
XR	BGP	—	次のオプション ボタンのいずれかをクリックします。 <ul style="list-style-type: none"> • [プレーンテキスト (Plain Text)] : パスワードを入力できるようにします。 • [暗号化 (Encrypted)] : パスワードとして 16 進数値を入力できるようにします。
	OSPF	MD5 またはキーチェーンを選択します。	次のオプション ボタンのいずれかをクリックします。 <ul style="list-style-type: none"> • [プレーンテキスト (Plain Text)] : パスワードを入力できるようにします。 • [暗号化 (Encrypted)] : パスワードとして 16 進数値を入力できるようにします。
	OSPFv3	認証タイプとして、[IPSec-MD5] または [IPSec-SHA1] のいずれかを選択します。	次のオプション ボタンのいずれかをクリックします。 <ul style="list-style-type: none"> • [プレーンテキスト (Plain Text)] : パスワードを入力できるようにします。 • [暗号化 (Encrypted)] : パスワードとして 16 進数値を入力できるようにします。

設定例 : L3VPN サービスのプロビジョニング

次に、以下のパラメータを使用して Cisco ASR 9000 デバイスに展開する設定例を示します。

- BDI (仮想) インターフェイルでの VRF アドレスと IP アドレス (IPv4 と IPv6 の両方) の作成。
- OSPF プロトコルを BGP プロトコルの再配布。

例 : Cisco ASR 9000 デバイスの BVI 対応インターフェイス (サブインターフェイス) での L3VPN サービスのプロビジョニング。

```
vrf vrfrbvibdi9k
vpn id aaaaaa:21
address-family ipv4 unicast
    import route-target
        6:55
address-family ipv6 unicast
    import route-target
        6:55
    export route-target
        6:55
interface GigabitEthernet0/0/0/17
    no shutdown
    exit
interface GigabitEthernet0/0/0/17.1
    encapsulation dot1q 1198
    shutdown
interface BVI 1
    vrf vrfrbvibdi9k
    ipv4 address 88.7.6.4 255.224.0.0
l2vpn
    bridge group BDI1
        bridge-domain 1
            routed interface BVI 1
                interface GigabitEthernet0/0/0/17.1
router bgp 140
    vrf vrfrbvibdi9k
        rd auto
        address-family ipv6 unicast
        address-family ipv4 unicast
        exit
    exit
exit
```

例 : OSPF ルート配布を使用して L3VPN サービスをプロビジョニングするための BVI 対応インターフェイスの使用 (デュアル AS を使用) 。

```
vrf definition VRF2-2VRF-2UNI-BDI
vpn id AAAAAA:2
rd 532533:2
address-family ipv4
    route-target import 6:5
    route-target export 6:5
address-family ipv6
    route-target export 6:5
interface GigabitEthernet0/0/0
    duplex full
    service instance 2 ethernet
    encapsulation dot1q 761
    bridge-domain 14
    shutdown
    exit
interface BDI14
    vrf forwarding VRF2-2VRF-2UNI-BDI
    ip address 5.44.3.7 255.255.0.0
router bgp 120
    address-family ipv4 vrf VRF2-2VRF-2UNI-BDI
        neighbor 55.4.3.2 remote-as 71
        neighbor 55.4.3.2 activate
        redistribute rip metric 6
        neighbor 55.4.3.2 local-as 387
    address-family ipv6 vrf VRF2-2VRF-2UNI-BDI
```

```
neighbor c5::98 remote-as 50
neighbor c5::98 activate
redistribute ospf 65 match external metric 2
neighbor c5::98 local-as 324 no-prepend replace-as dual-as
exit
exit
```

L3VPN サービスの詳細表示

Cisco EPN Manager を使用すると、次の方法で L3VPN サービスに関する詳細情報を表示できます。

- [回線/VC 360 (Circuit/VC 360)]ビューの使用 : [回線/VC 360 (Circuit/VC 360)]ビューには、Cisco EPN Manager を使用して作成された特定の L3VPN に関する詳細情報が表示されます。「[View Circuit/VC Details](#)」を参照してください。L3VPN サービスに関連付けられているさまざまなパラメータは、[要約 (Summary)]、[VRF (VRFs)]、[サイトの詳細 (Site Details)]、[HSRP]、[PE-CE ルーティング (PE-CE Routing)]の 5 つのタブに表示されます。



(注) サービス検出時に HSRP のさらに詳しい説明を表示するには、[サイトの詳細 (Site Details)]タブをクリックし、IP エンドポイントから行を選択します。また、選択した OSPFv3 ルーティングプロトコルタイプと IPv6 アドレスファミリの 6VPE 認証プロパティを表示するには、[PE-CE ルーティング (PE-CE Routing)]タブをクリックします。

- [ネットワーク トポロジ (Network Topology)]と [サービスの詳細 (Service Details)]ビューの使用 : [ネットワーク トポロジ (Network Topology)]ウィンドウには、デバイスのグラフィカルなトポロジマップビュー、デバイス間のリンク、デバイスまたはリンクのアクティブアラームが示されます。また、表示されたトポロジマップ内で L3VPN を視覚化することもできます。
 - L3VPN とその詳細の完全なリストを表示するには、[トポロジ ウィンドウのデバイスグループの回線/VC リストの表示](#)を参照してください。[回線/VC 360 (Circuit/VC 360)]ビューを参照してください。
 - 特定のデバイスの L3VPN サービスの詳細を表示するには、「[View Circuits/VCS In Which a Specific Device Participates](#)」を参照してください。
- **アラーム テーブルの使用** : Cisco EPN Manager のアラーム テーブルには、L3VPN サービスに問題があるかどうかを一目で確認する方法がいくつかあります。「[Check Circuits/VCS for Faults](#)」を参照してください。

HSRP のより詳細な説明の表示

ホットスタンバイ ルーティング プロトコル (HSRP) の詳細を使用して L3VPN サービスを作成した後、[回線 360/拡張詳細 (Circuit 360/extended details)] ビューで HSRP プロパティを表示できます。

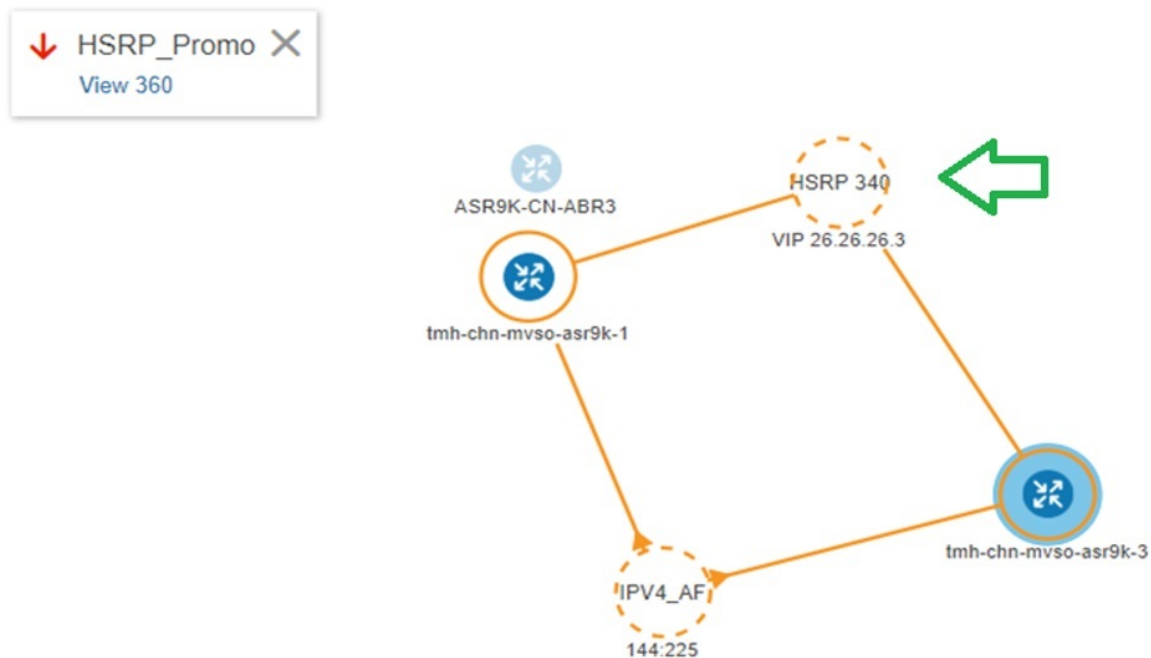
ステップ 1 左側のペインから、[マップ (Maps)] > [トポロジ マップ (Topology Maps)] > [ネットワーク トポロジ (Network Topology)] を選択します。

[ネットワーク トポロジ (Network Topology)] ウィンドウが開きます。

ステップ 2 ツールバーから [デバイス グループ (Device Groups)] をクリックした後、L3VPN サービスをフィルタ処理して表示します。

ステップ 3 図に示すように、L3VPN サービスを選択して HSRP のオーバーレイを表示します。

図 1: オーバーレイ : HSRP



ステップ 4 HSRP ノードまたはそれに接続されているリンクをクリックし、次に示す HSRP に関連する詳細を表示します。

図 2: HSRP の詳細

GigabitEthernet0/0/0/6.706

Device Name	VRF Name	Interface	IP Address
ASR9K-CN-ABR3	sd_l3vpn_6	GigabitEthernet0/0/...	77.6.0.1
ASR9K-CN-ABR4	sd_l3vpn_6	GigabitEthernet0/0/...	77.6.0.1

ステップ 5 HSRP のより詳しい説明を表示するには、次の手順を実行します。

- [360 度表示 (View 360)] ハイパーリンクをクリックします。[回線/VC 360* (Circuit/VC 360*)] ページが表示されます。
- [表示 (View)] > [詳細 (Details)] を選択します。
- [回線/VC の詳細 (Circuit-VC Details)] ウィンドウで、[サイトの詳細 (Site Details)] タブをクリックします。
- IP エンドポイントを選択した後、[HSRP] タブをクリックしてプロパティを表示します。

図 3: より詳細な説明 (*Extended Details*)

Circuit-VC Details - HSRP_Promo

Summary VRFs Site Details PE-CE Routing

IP Endpoints Select a row from the IP Endpoints list to view its details. Selected 1 / Total 2

Show Quick Filter

	UNI Name	Device Name	Interface	IP Address/Sub...	VRF
<input checked="" type="radio"/>	UNI- HSRP_Test-2	tmh-chn-mvso-asr9k-1.cis...	GigabitEthernet0/0/15.1	26.26.26.2/28	HSRP_Test
<input type="radio"/>	UNI- HSRP_Test-1	tmh-chn-mvso-asr9k-3.cis...	GigabitEthernet0/0/10.1	26.26.26.4/28	HSRP_Test

Site Details HSRP

Group Number 340
 Virtual Address 26.26.26.3
 Priority 30
 Hello Timer 100 Hold Timer 122
 Minimum Delay 455 Reload Delay 145
 Preempt Minimum Delay 500 Preempt Reload Delay No data available
 Authentication Key No data available

L3VPN および VRF の変更

Cisco EPN Manager を使用して作成されて展開された L3VPN サービスには変更を加えることができます。サービスに関連付けられているフルメッシュプレフィックス、QoS プロファイル、ルートターゲット値、OSPF 設定は変更できますが、サービスに関連付けられている顧客の詳細、VPN 名、サービス MTU 値などのパラメータを変更することはできません。これらのパラメータを変更するには、サービスを削除してから新しい値を設定してサービスを再作成する必要があります。また、L3VPN サービスに関連付けられている VRF を変更することもできます。

L3VPN サービスおよび VRF を変更するには、次の手順に従います。

始める前に

Cisco EPN Manager を使用して検出されてプロモートされた L3VPN サービスに変更を加えるには、L3VPN サービスのルート識別子が **rd device_ip:number** の形式で指定されていることを確認する必要があります。次に例を示します。

```
vrf definition vdvvgfr420
  rd 10.104.120.133:420
  vpn id 36B:420
  !
address-family...
```

ルート識別子が他の形式で指定されている場合、サービスを編集することはできません。

ステップ 1 [マップ (Maps)] > [ネットワーク トポロジ (Network Topology)] に移動します。

ステップ 2 [回線/VC (Circuits/VCS)] タブをクリックし、変更を加える L3VPN サービスを選択します。

ステップ 3 鉛筆 (変更) アイコンをクリックします。

ステップ 4 選択した L3VPN に変更を加えるには、[VPN の変更 (Modify VPN)] を選択し、[次へ (Next)] をクリックします。

[プロビジョニング (Provisioning)] ウィザードに、選択した L3VPN に関連付けられている VRF、エンドポイントおよびその他の詳細が表示されます。

ステップ 5 必要に応じて、[IP MTU] の値を変更できます。

ステップ 6 選択した L3VPN に関連付けられている VRF を変更するには、[VRF の変更 (Modify VRF)] を選択し、[次へ (Next)] をクリックします。

[プロビジョニング (Provisioning)] ウィザードに、選択した L3VPN に関連付けられている VRF、エンドポイントおよびその他の詳細が表示されます。既存の VRF パラメータを変更するだけでなく、新しいルートターゲット値を VRF に関連付けることもできます。

VRF を変更する際に、UNI に関連付けられている QoS プロファイルを変更することはできませんが、サービス エンドポイントに関連付けられている QoS ポリシーは変更できます。

(注) 選択した L3VPN に関連付けられている VRF 名とデバイスを変更することはできません。

ステップ 7 必要に応じて変更した後、[送信 (Submit)] をクリックしてデバイスに展開される設定をプレビューします。

(注) VPN を変更する際に、VPN に関連付けられている VRF を変更することはできません。VRF を変更する場合は、[L3VPN サービスへの VRF の追加およびコピー \(95 ページ\)](#) を参照してください。

ステップ 8 変更内容を確認してから [展開 (Deploy)] をクリックしてデバイスに変更を展開します。

サービスに参加しているデバイスのうち 1 台でも展開に失敗した場合は、サービスに参加しているすべてのデバイスで設定がロールバックされます。

ステップ 9 変更が保存されていることを確認するには、L3VPN サービスの詳細を表示します。[L3VPN サービスの詳細表示 \(91 ページ\)](#) を参照してください。

L3VPN サービスへの VRF の追加およびコピー

Cisco EPN Manager を使用して、新しい VRF を作成したり、それを既存の L3VPN サービスに関連付けたりすることができます。また、L3VPN サービス用に新しい VRF を作成するため、ルート ターゲットやその他の詳細を既存の VRF からコピーすることもできます。

新しい VRF を L3VPN サービスに関連付けるには、以下の手順を実行します。

ステップ1 [マップ (Maps)] > [ネットワーク トポロジ (Network Topology)] に移動します。

ステップ2 [回線/VC (Circuits/VCs)] タブをクリックして、新しいVRFに関連付けるL3VPNサービスを選択します。

また、[設定 (Configuration)] > [ネットワーク (Network)] > [サービス プロビジョニング (Service Provisioning)] の順に選択することによって、[L3VPN プロビジョニング (L3VPN Provisioning)] ウィザードにアクセスすることもできます。

ステップ3 鉛筆 (変更) アイコンをクリックします。

[L3VPN プロビジョニング (L3VPN Provisioning)] ウィザードが表示されます。

ステップ4 [VRF の追加 (Add VRF)] を選択して、[次へ (Next)] をクリックします。

ステップ5 [+] アイコンをクリックして、新しいVRFの詳細を手動で追加します。VRFの詳細を自動入力するには、マップでデバイスをクリックし、そのVRFを選択します。デバイスの詳細とVRFの新しい名前は、VRFのページに自動的に入力されます。

ステップ6 [コピー元 (Copy From)] ドロップダウンリストをクリックして必要なVRFを選択し、既存のVRFからVRFの詳細をコピーできます。

選択したL3VPNに関連付けられたそれらのVRFのみが、VRFルートターゲットおよびルート再配布の詳細とともに表示されます。

ステップ7 それ以外の場合は、選択したVPNサービスに追加するVRFの詳細を手動で指定します。さまざまなVRFパラメータの詳細については、「[新規L3VPNサービスの作成およびプロビジョニング](#)」を参照してください。

ステップ8 エンドポイントやBGPネイバーの詳細の追加など必要な変更を加え、[送信 (Submit)] をクリックします。

ステップ9 デバイスに導入する設定をプレビューし、必要な変更を加え、[導入 (Deploy)] をクリックしてデバイスへの変更を導入します。

導入された変更を確認するには、選択したL3VPNサービスの詳細を表示します。「[L3VPNサービスの詳細表示](#)」を参照してください。

L3VPNサービスの変更や削除の詳細については、[L3VPNサービスエンドポイントの削除およびL3VPNおよびVRFの変更 \(94 ページ\)](#) を参照してください。

回線エミュレーションサービスのプロビジョニング

- [Cisco EPN Manager CEM のプロビジョニング サポートの概要 \(97 ページ\)](#)
- [CEM プロビジョニングの前提条件 \(97 ページ\)](#)
- [新しいCEMサービスの作成とプロビジョニング \(97 ページ\)](#)
- [#unique_694](#)

Cisco EPN Manager CEM のプロビジョニング サポートの概要

Cisco EPN Manager は、回線エミュレーション (CEM) サービスのプロビジョニングをサポートします。CEM は、従来の TDM ネットワークとパケットスイッチドネットワーク (PSN) の間のブリッジを提供します。これは、TDM データをパケットにカプセル化し、適切なヘッダーを付与して、それらのパケットを PSN 経由で宛先ノードに送信します。詳細については、[サポートされる回線エミュレーション サービス](#)を参照してください。

さらに、MPLS TE トンネルを CEM サービスに割り当て、CEM サービスがネットワークを通過できるようにすることができます。プロビジョニング ウィザードの [優先パス (Preferred Path)] ドロップダウンリストを使用して、CEM サービスに MPLS TE トンネルを割り当てます。詳細については、[CEM サービスの詳細 \(99 ページ\)](#) を参照してください。



(注) 優先パスで選択されたトンネルに十分な帯域幅がない場合、CEM サービスのプロビジョニングは失敗します。

CEM プロビジョニングの前提条件

CEM サービスをプロビジョニングするには、次の前提条件を満たしている必要があります。

- CEM サービスの発信側と着信側のエンドポイントで、IP/MPLS 接続を有効にする必要があります。
- ループバック インターフェイスや ACR グループなどの CEM 設定を、CEM サービスで使用するデバイスで設定する必要があります。詳細については、[回線エミュレーションの設定](#)を参照してください。
- CEM サービスがプロビジョニングされるデバイスのインベントリ収集ステータスが、[完了済み (Completed)] である必要があります。これを確認するには、[インベントリ (Inventory)] > [デバイス管理 (Device Management)] > [ネットワーク デバイス (Network Devices)] を選択し、[最後のインベントリ収集ステータス (Last Inventory Collection Status)] 列でステータスを確認します。
- オプションで、顧客をシステムに作成して、サービスの作成中およびプロビジョニングプロセス中に CEM サービスを顧客に関連付けることができます。左のサイドバーから [インベントリ (Inventory)] > [その他 (Other)] > [顧客 (Customers)] を選択して、顧客を作成および管理します。

新しい CEM サービスの作成とプロビジョニング

Cisco EPN Manager で CEM サービスを作成してプロビジョニングするには、次の操作を行います。

- CEM サービスのエンドポイントの指定。
- CEM サービスとそのエンドポイントを介して配信されるトラフィックの処理方法に影響する属性の定義。

始める前に

CEM サービスをプロビジョニングする前に満たしている必要がある前提条件については、[CEM プロビジョニングの前提条件 \(97 ページ\)](#) を参照してください。

- ステップ 1** 左側のサイドバーのメニューから、**[マップ (Maps)] > [トポロジ マップ (Topology Maps)] > [ネットワーク トポロジ (Network Topology)]** の順に選択します。
- ステップ 2** **[デバイス グループ (Device Groups)]** をクリックして、CEM サービスを作成する場所を選択します。
- ステップ 3** **[デバイス グループ (Device Groups)]** ポップアップ ウィンドウを閉じます。
- ステップ 4** **[ネットワーク トポロジ (Network Topology)]** ウィンドウで **[回線/VC (Circuits/VCs)]** をクリックします。
- ステップ 5** **[+]** アイコンをクリックします。マップ右側の新しいペインにプロビジョニングウィザードが表示されません。
- プロビジョニングウィザードを表示するもう 1 つの方法として、**[設定 (Configuration)] > [ネットワーク (Network)] > [サービス プロビジョニング (Service Provisioning)]** の順に選択する方法があります。
- ステップ 6** **[テクノロジー (Technology)]** ドロップダウンリストから **[回線エミュレーション (Circuit Emulation)]** を選択します。
- ステップ 7** **[サービス タイプ (Service Type)]** ドロップダウンリストから、回線のデータ転送速度に基づいて必要な CEM サービス タイプを選択します。Cisco EPN Manager でサポートされている CEM サービス タイプのリストについては、[サポートされる回線エミュレーション サービス](#) を参照してください。
- ステップ 8** さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、**[プロファイルの選択 (Select Profile)]** ドロップダウンリストから必要なプロファイルを選択します。[回線/VC プロファイル \(134 ページ\)](#) を参照してください。
- ステップ 9** **[次へ (Next)]** をクリックして **[カスタマー サービスの詳細情報 (Customer Service Details)]** ページに移動します。
- ステップ 10** (オプション) EVC の作成対象顧客を選択します。リストに顧客が表示されない場合は、**Inventory > Other > Customers** に移動し、システムで顧客を作成し、プロビジョニング ウィザードに移動して CEM サービスのプロビジョニングを開始します。
- ステップ 11** **[アクティブ化 (Activate)]** チェックボックスをオンにし、プロビジョニングするサービスに関連付けられているインターフェイスをアクティブにします。
- ステップ 12** サービス名と説明を入力します。
- ステップ 13** **[展開アクション (Deployment Action)]** フィールドに、CEM サービス作成プロセス完了時のアクションを指定します。実際に展開する前に関連デバイスに展開される設定のプレビューを要求するか、または完了後すぐに設定を展開することができます。

[展開 (Deploy)] を選択した場合は、次の展開オプションのいずれかをクリックします。

- **[今すぐ展開 (Deploy Now)]** : プロビジョニング順序を直接展開します。
- **[後で展開 (Deploy Later)]** : 作成されたプロビジョニング順序を保存しておき、後で同じ順序を展開します。

- [展開のスケジュール (Schedule Deployment)] : プロビジョニングの順序をスケジュールし、スケジュールされた時刻に展開します。この [展開のスケジュール (Schedule Deployment)] オプションボタンをクリックした場合は、次を指定します。
 - [スケジュール時刻の展開 (Deploy Schedule Time)] : プロビジョニング順序の展開のスケジュール時刻を指定します。
 - [サーバ時刻 (Server Time)] : 現在のサーバ時刻を表示します。

ステップ 14 [次へ (Next)] をクリックし、[A エンド (A End)] 設定と [Z エンド (Z End)] 設定、および CEM サービスの転送設定を入力します。フィールドと属性の説明については、[CEM サービスの詳細 \(99 ページ\)](#) を参照してください。

ステップ 15 エンドポイントの 1 つが Cisco EPN Manager により管理されていないデバイス上のインターフェイスの場合は、[管理対象外デバイス (Unmanaged Device)] チェックボックスをオンにし、その管理対象外デバイスの情報を入力します。詳細については、[アンマネージドエンドポイントを使用した回線/VC のプロビジョニング \(137 ページ\)](#) を参照してください。

(注) [管理対象外デバイス (Unmanaged Device)] チェックボックスは、[Z エンド設定 (Z End Configurations)] ページだけで使用できます。

ステップ 16 (オプション) サービスに参加するデバイスで設定される追加の CLI コマンドがあるテンプレートを追加するには、[テンプレートの詳細 (Template Details)] ページで追加してください。詳細については、[テンプレートを使用した回線/VC の拡張 \(138 ページ\)](#) を参照してください。

ステップ 17 サービスに必要な情報をすべて入力したら、[送信 (Submit)] をクリックします。デバイスに展開される CLI のプレビューを表示することを選択した場合は、プレビューが表示されます。この場合、属性の編集 (Edit Attributes)] をクリックすることで、属性を変更できます。そうでない場合は、すぐに設定がデバイスに展開されます。

CEM サービスを [ネットワーク トポロジ (Network Topology)] ウィンドウの [回線/VC (Circuits/VCS)] ペインのリストに追加する必要があります。プロビジョニング状態を確認するには、回線/VC 名の横の [i] アイコンをクリックします。[回線/VC 360 (Circuit/VC 360)] ビューが表示されます。また、保存されたプロビジョニング ジョブは、[管理 (Administration)] > [ダッシュボード (Dashboards)] > [ジョブ ダッシュボード (Job Dashboard)] > [プロビジョニング (Provisioning)] から [計画済み回線/VC (Planned Circuits/VCS)] タブに表示できます。

CEM サービスの詳細

次の表では、CEM サービスのタイプを定義する属性をリストし、説明しています。

表 15: 回線セクションのリファレンス - CEM サービス タイプ

属性	説明
[A エンド (A End)] と [Z エンドの設定 (Z End Configurations)]	
Device	CEM サービスの送信元と宛先のデバイスの名前。

属性	説明
作業パスと保護パス	
ポート名またはインターフェイス名 (Port Name or Interface Name)	<p>CEMサービスにおける送信元と宛先デバイスのインターフェイス名。ポート名またはポート グループを選択できます。</p> <p>[保護パス (Protecting Path)] エリアの下にあるポート名を選択すると、単方向パス スイッチ型リング (UPSR) 保護メカニズムが有効になります。</p> <p>[保護パス (Protecting Path)] エリアの下にあるポート グループを選択すると、自動保護スイッチング (APS) の保護メカニズムが有効になります。保護グループの設定方法の詳細については、APS または MSP および UPSR または SNCP 保護グループの設定を参照してください。</p>
高次パス	<p>SONET/SDH 回線がチャネライズされると、高次パス (HOP) および低次パス (LOP) と呼ばれる、より小さな帯域幅のチャンネルに論理的に分割されます。HOP または同期転送信号 (STS) パスは、より高い帯域幅の TDM データを伝送するために使用されます。HOP は、その中に LOP を含むこともできます。</p> <p>CEM サービスで使用可能なパスとパスモードを選択します。</p>
低次パス	<p>LOP またはバーチャルトリビュタリ (VT) パスは、より低い帯域幅の TDM データを伝送するために使用されます。</p>
DS0 タイムスロット (DS0 Time Slot)	<p>DS0 グループで使用できる1つ以上のタイムスロットを選択します。</p> <p>(注) このフィールドは、[サービスタイプ (Service Type)] フィールドの [DS0] を選択するときのみ使用できます。</p>
<p>クロッキング</p> <p>ネットワーク内のノードは、クロックレートが異なる可能性があります。ノードでのタイミングの違いによって、受信ノードは、送信された情報をドロップしたり、再読み取りしたりする可能性があります。すべてのノードを同じクロックレートに同期させるには、クロッキングが必要です。クロッキングの詳細については、CEMのクロッキングの設定を参照してください。</p>	

属性	説明
Clock Source	<p>すべてのノードを同じクロック レートで同期できるように、単一の送信元からクロック レートを回復できるようにします。値は次のとおりです。</p> <ul style="list-style-type: none"> • [内部 (Internal)] : ホストから回復されるクロック レート。 • [回線 (Line)] : SONET/SDH 回線から回復されるクロック レート。 • [適応クロック回復 (Adaptive Clock Recovery)] : デジッタ バッファ フル レベルに基づいてクロック レートが回復されます。遅延変動により、デジッタ バッファ フル レベルは常に変動します。TDM サービス クロックは、変動をフィルタリングした後に回復されます。復元クロックの精度は遅延変動によって異なります。 • [差分クロックリカバリ (Differential Clock Recovery)] : クロック レートは Sync-E を使用してプライマリクロックから回復されます。ネットワークのプライマリクロックを設定する方法の詳細については、Sync-E、BITS、および PTP を使用したクロックの同期 を参照してください。

QoS

選択可能なプロファイルのリストには、デバイスで設定され、システムによって検出されたポリシーマップ、およびユーザ定義の QoS プロファイルが含まれます。QoS プロファイルの作成方法の詳細は、[QoS プロファイルの作成 \(135 ページ\)](#) を参照してください。

入力 QoS プロファイル (Ingress QoS Profile)	A エンド デバイスと Z エンド デバイスで設定されている入力 QoS ポリシーを選択します。
-------------------------------------	--

管理されていないデバイス詳細

(注) 次のフィールドは Z エンドの設定でのみ使用できます。

管理対象外デバイス (Unmanaged Device)	Cisco EPN Manager で管理されていないデバイスを含めて、部分的サービスを作成する場合に、このチェックボックスをオンにします。
新規デバイス (New Device)	新しい管理対象外デバイスを作成する場合に、このチェックボックスをオンにします。
Device	<p>ドロップダウンリストから管理対象外デバイスを選択します。</p> <p>(注) このフィールドは、[新規デバイス (New Device)] チェックボックスがオフになっている場合にだけ使用できます。</p>

属性	説明
デバイス名 (Device Name)	作成する新しい管理対象外デバイスの一意の名前を入力します。 (注) このフィールドは、[新規デバイス (New Device)] チェックボックスがオンになっている場合にだけ使用できます。[新規デバイス (New Device)] チェックボックスがオフの場合、[デバイス (Device)] ドロップダウンリストで選択した管理対象外デバイスの名前がこのフィールドに入力されます。
デバイス IP (Device IP)	作成する新しい管理対象外デバイスの IP アドレスを入力します。 (注) このフィールドは、[新規デバイス (New Device)] チェックボックスがオンになっている場合にだけ使用できます。[新規デバイス (New Device)] チェックボックスがオフの場合、[デバイス (Device)] ドロップダウンリストで選択した管理対象外デバイスの IP アドレスがこのフィールドに入力されます。
LDP IP	管理対象外デバイスの有効な LDP IP を入力します。
VC ID	管理対象外デバイスの仮想回線 (VC) の固有 ID を入力します。
転送設定	
フレーム タイプ (Frame Type)	このフィールドは表示専用で、CEM サービスの作成時に選択した CEM サービスタイプに基づいて自動入力されます。値は [CESoPSN]、[SAToP]、[FRAMED_SAToP]、および [CEP] です。 サービスタイプが [T1]、[T3]、[E1]、および [E3 CEM] の場合は、フレームタイプを [SAToP] または [FRAMED_SAToP] として選択します。 E3 コントローラ上のサービスタイプ E3 のフレームタイプ CEP を選択できます。 (注) CEM サービスの展開後、SDH を持つ SONET フレームモードを介した T1/T3 サービスと E1/E3 サービスの CLI 変更を [デバイスプレビューの設定 (Device Preview Config)] に表示します。FRAMED-SAToP フレームタイプは、NCS42xx デバイスまたは ASR9xx デバイスでサポートされています。
ペイロード サイズ (Payload Size)	各 IP パケットに入れられるバイト数。有効な範囲は 64 ~ 1312 です。範囲は、デバイスの機能、サポートレベル、および設定されたデジタバッファサイズの値に応じて異なります。

属性	説明
デジッタ バッファ サイズ (Dejitter Buffer Size)	ネットワーク ジッターを許容するエミュレートされた回路の能力を決定します。有効な範囲は 1 ~ 32 です。範囲は、デバイスの機能、サポートのレベル、および設定されたペイロードサイズの値によって異なります。
アイドル パターン (Idle pattern)	サービスがダウンしたときにデータを送信するアイドル パターン。有効範囲は 0x00 ~ 0xFF です。
ダミー モード (Dummy Mode)	損失フレームまたは破損フレームの穴埋め用ビット パターンを設定できます。値はラスト フレームとユーザ定義です。
ダミー パターン (Dummy Pattern)	損失フレームまたは破損フレームの穴埋め用ビット パターン。有効範囲は 0x00 ~ 0xFF です。デフォルトは 0xFF です。 (注) このフィールドは、ユーザ定義としてダミーモードを選択した場合にのみ有効になります。
RTP ヘッダー対応 (RTP Header Enabled)	CEM サービスの Real-Time Transport Protocol (RTP) ヘッダーを有効にするには、このチェックボックスをオンにします。
RTP 圧縮対応 (RTP Compression Enabled)	パケットが送信される前にパケットの IP ヘッダーを圧縮するには、このチェックボックスをオンにします。ネットワークのオーバーヘッドを削減し、RTP の伝送を高速化します。
疑似回線の設定	
優先パス タイプ (Preferred Path Type)	優先パスタイプを双方向または単方向として選択します。
優先経路 (Preferred Path)	CEM サービスを通過させる MPLS 双方向 TE トンネルを選択します。 (注) このフィールドは、優先パス タイプに [双方向 (Bidirectional)] を選択したときにのみ使用できます。
優先パス (A~Z) (Preferred Path (A-Z))	A エンドポイントから Z エンドポイントまで CEM サービスを移動させるために必要な単方向トンネルを選択します。 (注) このフィールドは、優先パス タイプに [単方向 (Unidirectional)] を選択したときにのみ使用できます。
優先パス (Z~A) (Preferred Path (Z-A))	Z エンドポイントから A エンドポイントに CEM サービスを移動させるために必要な単方向トンネルを選択します。 (注) このフィールドは、優先パス タイプに [単方向 (Unidirectional)] を選択したときにのみ使用できます。

属性	説明
LDP へのフォールバックを許可 (Allow Fallback to LDP)	<p>選択した優先パスがダウンした時に、CEM サービスがデフォルトの MPLS Label Distribution Protocol (LDP) にフォールバックされるようにするには、このチェックボックスをオンにします。</p> <p>(注) このチェックボックスは、[優先パス (Preferred Path)] フィールドで有効な MPLS TE トンネルを選択した場合にのみ使用できます。</p>
送信コントロールワード (Send Control Word)	接続の両側で疑似回線ペイロードを特定するためにコントロールワードを使用する場合は、このチェックボックスをオンにします。
[インターネットワーキング (Internetworking)] のオプション	EVC のエンドポイントのいずれかが管理対象外デバイスの場合、オプションを選択します。
帯域幅 (kbps) (Bandwidth (kbps))	疑似回線に必要な帯域幅を入力します。
PWID	疑似回線識別子を入力します。この ID は、ポイントツーポイントサービスの [疑似線設定 (Pseudowire Settings)] に表示されます。

CEM サービスの変更

Cisco EPN Manager を使用して作成および展開された CEM サービスを変更できます。

始める前に

-
- ステップ 1 左側のサイドバーから、[マップ (Maps)] > [トポロジマップ (Topology Maps)] > [ネットワークトポロジ (Network Topology)] の順に選択します。
 - ステップ 2 [Device Groups] をクリックして、変更する CEM サービスがある場所を選択します。
 - ステップ 3 [デバイス グループ (Device Groups)] ポップアップ ウィンドウを閉じます。
 - ステップ 4 [Network Topology] ウィンドウで、[Circuits/VCs] タブをクリックし、変更する CEM サービスを選択します。
 - ステップ 5 鉛筆 (変更) アイコンをクリックします。
[Modify CEM] ウィンドウが表示されます。[Z Endpoint] の詳細のみを変更できます。
 - ステップ 6 [Device] を変更するには、[Device] ドロップダウンリストからデバイスを選択します。
 - ステップ 7 [Working Path] を変更するには、ドロップダウンリストから [Interface Name] を選択します。
 - ステップ 8 [Higher Order Path] を変更するには、ドロップダウンリストから [Available Paths] と [Path Mode] を選択します。

- ステップ 9** [Lower Order Path] を変更するには、ドロップダウンリストから [Available Paths] を選択します。
- ステップ 10** 必要に応じて変更したら、[送信 (Submit)] をクリックしてデバイスに展開される設定をプレビューします。
- ステップ 11** 変更内容を確認してから [展開 (Deploy)] をクリックしてデバイスに変更を展開します。

プロビジョニング順序の保存とスケジュール

回線/VC、MPLS トンネル、または L3VPN サービステクノロジーなどのプロビジョニングサービスを作成、変更、または削除すると、サービスをプレビューまたは展開できます。プロビジョニング順序を保存またはスケジュールする前に、[今すぐ展開 (Deploy Now)]、[後で展開 (Deploy Later)]、[展開のスケジュール (Schedule Deployment)] などの展開オプションを選択できます。

[計画回線/VC (Planned Circuits/VCs)] タブに保存されたプロビジョニング順序を表示し、必要に応じて計画サービスを変更するか、後続サービスを作成することができます。次に、制限事項の一部を示します。

- 計画バージョンが存在する場合は、ライブ回線の変更および削除操作はすべて無効になります。また、[インベントリ (Inventory)] > [回線/VC およびネットワーク インターフェイス (Circuits/VCs & Network Interfaces)] で計画順序のサービスを修正することはできません。詳細については、「次の作業」の項を参照してください。
- [計画回線 (Planned Circuits)] から順序を編集する場合、Cisco EPNM では計画に変更を加えることができます。
- [計画回線 (Planned Circuits)] からの削除アクションは、最後に試行されたプロビジョニングされたバージョンに戻される計画サービスを削除します。スケジュール順序の場合、ジョブダッシュボードから時刻が更新されると、同じ時刻が [計画回線 (Planned Circuits)] に反映されません。

展開を保存してスケジュールするには、次の手順を実行します。

- ステップ 1** 次のパスのいずれかを使用して計画プロビジョニングの順序を作成するには、次の手順を実行します。
- [マップ (Maps)] > [トポロジ マップ (Topology Maps)] > [ネットワーク トポロジ (Network Topology)] を選択します。
- または
- [インベントリ (Inventory)] > [回線/VCs およびネットワーク インターフェイス (Circuits/VCs&Network Interfaces)] を選択します。
- ステップ 2** 「での回線/VC のプロビジョニング Cisco EPN Manager」というトピックのステップ 2 ~ 12 を繰り返します。
- ステップ 3** 展開を保存してスケジュールするには、次の手順を実行します。

- a) [展開 (Deploy)] 領域で、[後で展開 (Deploy Later)] オプション ボタンをクリックして、プロビジョニング順序を保存します。
- b) [展開 (Deploy)] 領域で、[展開のスケジュール (Schedule Deployment)] オプション ボタンをクリックし、指定した時刻に今後の展開の順序を保存します。次の値を指定します。
 - [スケジュール時刻の展開 (Deploy Schedule Time)] : プロビジョニング順序の展開のスケジュール時刻を指定します。
 - [サーバ時刻 (Server Time)] : 現在のサーバ時刻を表示します。
- c) [次へ (Next)] をクリックしてエンドポイントを選択し、選択したテクノロジーに基づいて属性を定義します。
- d) [送信 (Submit)] をクリックします。選択した展開アクションに応じて、関連するアクションが実行されます。つまり、設定のプレビューを選択した場合は、設定を表示できるプレビュー ページが表示され、その後に [展開 (Deploy)] をクリックします。展開を選択した場合、設定は関連するデバイスに直接展開されます。展開の保存/スケジュールが成功したことを示すメッセージを受け取ったら、[閉じる (Close)] をクリックします。

ステップ 4 左側のペインで、[回線/VC (Circuit/VCS)] ハイパーリンクをクリックします。[場所/すべての場所/未割り当て (Locations/All Locations/Unassigned)] 拡張ビュー ウィンドウが表示されます。

ステップ 5 [計画回線 VC (Planned Circuits VC)] タブをクリックし、新しく作成されたプロビジョニング サービスの詳細を表示します。新しく作成されたプロビジョニング サービスのステータスは、[計画済みの作成 (Create Planned)] として表示されます。展開スケジュールの時刻、プロビジョニングするサービスのタイプおよび名前、顧客名、および最終変更日時を表示します。必要に応じて、サービスは再度変更することができます。計画されたサービスの場合、展開するまでは何度でも修正できます。ステータスは [計画済みの変更 (Modify Planned)] として表示されます。

(注) [計画回線/VC (Planned Circuits/VCS)] タブは、[マップ (Maps)] > [トポロジ (Topology)] > [ネットワーク トポロジ (Network Topology)] から [回線/VC (Circuit/VCS)] をクリックした場合にのみ使用できます。[後で展開 (Deploy Later)] オプションの場合は、展開スケジュール時刻が表示されません。

何度かの修正の間に最新バージョンがキャプチャされます。スケジュールされた順序があり、最新バージョンが [後で展開 (Deploy Later)] に設定されている場合は、そのうちに以前にスケジュールされたすべての順序が [ジョブ (Job)] ダッシュボードから削除されます。

ステップ 6 計画順序の作成をクリックした後、[アクション (Actions)] > [展開 (Deploy)] を選択してサービスを直接展開します。

ステップ 7 (オプション) 必要に応じて他のアクションを実行できます。

- a) 新しいプロビジョニング ワークフローを作成するには、[+] アイコンをクリックします。
- b) 計画したサービスを削除するには、[X] アイコンをクリックします。サービスが削除されると、ウィンドウの右下隅に成功か失敗かのメッセージが表示されます。
- c) [後でデプロイ (Deploy Later)] サービスは、[X] をクリックすると削除され、計画されていたデプロイ サービスに関するトレースは EPNM に保存されません。
- d) デプロイされたスケジュール済みのサービスが削除されると、対応するジョブとサービスがクリアされます。

ステップ 8 スケジュールしたプロビジョニング ジョブを表示するには、[管理 (Administration)] > [ダッシュボード (Dashboard)] > [ジョブ ダッシュボード (Job Dashboard)] を選択します。ステータスは [スケジュール済み (Scheduled)] として表示され、次回の展開の開始時刻などを表示できます。

- a) (オプション) [スケジュールの編集 (Edit Schedule)] をクリックして、スケジュールの順序を編集します。
- [スケジュール (Schedule)] ウィンドウで、必要に応じてスケジュール時刻やその他の詳細を変更します。
 - [保存 (Save)] をクリックして [ジョブダッシュボード (Job Dashboard)] ウィンドウに戻ります。
- b) (オプション) ジョブを削除するには、[X] アイコンをクリックします。

ジョブが正常にデプロイされると、エントリのリストがジョブダッシュボードに表示されます。[後で展開 (Deploy Later)] オプションでは、時刻が定義されていないため、ジョブは作成されません。

次のタスク

[インベントリ (Inventory)] > [回線/VC およびネットワーク インターフェイス (Circuits/VCS&Network インターフェイス)] を選択して計画回線/VC を表示します。新しいプロビジョニングワークフローの作成、既存のサービスの展開、または特定のプロビジョニング順序のサービスの修正を行えます。正常に展開されると、プロビジョニング順序のエントリが [計画回線/VC (Planned Circuits)] タブからクリアされます。



- (注) [回線/VC (Circuit/VCS)] タブに展開した回線/VC を、[計画回線/VC (Planned Circuits/VCS)] タブに計画回線を表示します。

回線/VC の変更または削除操作は実行できません。これは、展開したバージョンにさらに修正を加える前に、まず計画したバージョンをクリアする必要があるためです。[計画回線/VC (Planned Circuits/VCS)] をクリックして、選択した回線/VC に修正を加えるか、または計画したバージョンを展開します。

削除操作

計画したバージョンを削除すると、ウィンドウの右下隅に成功または失敗を示すメッセージが表示されます。[回線/VC (Circuits/VCS)] タブでサービスを削除すると、[計画の変更がキャンセルされました (Modify Plan Canceled)] と [計画の削除がキャンセルされました (Delete Plan Canceled)] というステータスが表示されます。

[計画回線/VC (Planned Circuit/VCS)] タブからサービスを削除すると、関連付けられた UNI も [ネットワークインターフェイス (Network Interface)] タブから削除されます。削除された UNI は再利用可能になります。

設定のプレビュー

新しいプロビジョニング回線/VC の作成時に [展開アクション (Deployment Action)] が [プレビュー (Preview)] として選択されている場合は、[展開 (Deploy)] ページに [今すぐ展開

[Deploy Now] または [後で展開 (Deploy Later)] あるいは [展開のスケジュール (Schedule Deployment)] のいずれかを選択するオプションが表示されます。

ネットワーク インターフェイスの表示

[回線/VC (Circuits/VCs)] タブで [ネットワーク インターフェイス (Network Interfaces)] をクリックして、サービスをプロビジョニングするためのネットワーク インターフェイスの詳細を表示します。ウィザードを使用してインターフェイスを変更または削除できます。

MPLS トラフィック エンジニアリング サービスのプロビジョニング

- [Cisco EPN Manager MPLS TE のプロビジョニング サポートの概要 \(108 ページ\)](#)
- [MPLS TE サービスのプロビジョニング機能 \(108 ページ\)](#)
- [MPLS TE サービスのプロビジョニングの前提条件 \(117 ページ\)](#)
- [MPLS TE トンネルの作成とプロビジョニング \(118 ページ\)](#)
- [MPLS TE レイヤ 3 リンクの作成とプロビジョニング \(109 ページ\)](#)

Cisco EPN Manager MPLS TE のプロビジョニング サポートの概要

Cisco EPN Manager は、MPLS トラフィック エンジニアリング サービスのプロビジョニングをサポートしています。MPLS TE を使用すると、MPLS バックボーンはレイヤ 2 の TE 機能をレイヤ 3 上に復元し、拡張できます。MPLS TE は、バックボーン全体でラベルスイッチドパス (LSP) を確立および維持するために、Resource Reservation Protocol (RSVP) を使用します。詳細については、[サポートされている MPLS トラフィック エンジニアリング サービス](#)を参照してください。

MPLS TE サービスのプロビジョニング機能

Cisco EPN Manager は次の MPLS TE 機能をサポートしています。

- 明示的なルーティング、制約ベースのルーティング、およびトランク アドミッション コントロールのサポート。
- リンク障害とノード障害に対するパス保護メカニズムのプロビジョニング。
- ラベル交換パス (LSP) を確立し、維持するための Resource Reservation Protocol (RSVP) の使用。
- OSPF と ISIS を使用して TE リンクをアドバタイズする機能。

Cisco EPN Manager の MPLS TE 制限事項を次に示します。

- MPLS TE トンネルは、NCS 4206、4216 デバイス、NCS4K、NCS 5500、ASR9k、および ASR9XX でのみサポートされています。ただし、インベントリ サポートは NCS 4201 と NCS 4202 に対して提供されます。
- OSPF および ISIS は、MPLS TE を実装するための IGP としてサポートされています。
- NCS5500 デバイスでは、ラップ保護、BFD、および障害 OAM はサポートされていません。
- MPLS TE 属性は、属性が Cisco EPN Manager Web インターフェイスを介してプロビジョニングされている場合にのみ使用でき、データベースに入力されます。



(注) MPLS TE トンネルのプロビジョニングをサポートするデバイスのリストについては、次を参照してください。 [Cisco Evolved Programmable Network Manager のサポート対象デバイス](#)

MPLS TE レイヤ 3 リンクの作成とプロビジョニング

MPLS TE レイヤ 3 リンクをプロビジョニングするには、次の手順を実行します。

始める前に

MPLS TE レイヤ 3 リンクをプロビジョニングする前に満たす必要がある前提条件については、「[MPLS TE サービスのプロビジョニングの前提条件 \(117 ページ\)](#)」を参照してください。

- ステップ 1 左側のサイドバーから、[マップ (Maps)] > [トポロジマップ (Topology Maps)] > [ネットワーク トポロジ (Network Topology)] を選択します。
- ステップ 2 [Device Groups] をクリックして、MPLS TE レイヤ 3 リンクを作成する場所を選択します。
- ステップ 3 [デバイス グループ (Device Groups)] ポップアップ ウィンドウを閉じます。
- ステップ 4 [ネットワーク トポロジ (Network Topology)] ウィンドウで [回線/VC (Circuits/VCs)] をクリックします。
- ステップ 5 [+] アイコンをクリックします。マップ右側の新しいペインにプロビジョニング ウィザードが表示されます。
- ステップ 6 [テクノロジー (Technology)] ドロップダウンリストから [MPLS TE] を選択します。Cisco EPN Manager は、関連するサービス タイプのリストを [サービス タイプ (Service Type)] 領域に表示します。
- ステップ 7 [サービス タイプ (Service Type)] 領域で、[レイヤ 3 リンク (Layer 3 Link)] を選択します。
- ステップ 8 さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、[プロファイルの選択 (Select Profile)] ドロップダウン リストから必要なプロファイルを選択します。 [回線/VC プロファイル \(134 ページ\)](#) を参照してください。
- ステップ 9 [次へ (Next)] をクリックして [リンク設定 (Link Settings)] ページに移動します。
- ステップ 10 レイヤ 3 リンクの名前と説明を入力します。

ステップ 11 次のいずれかの方法で、[A エンドデバイス (A End Device)]、[A エンドインターフェイス (A End Interface)]、[Z エンドデバイス (Z End Device)]、および[Z エンドインターフェイス (Z End Interface)] フィールドを選択します。

- マップ上のリンクをクリックすると、[A エンドデバイス (A End Device)]、[A エンドインターフェイス (A End Interface)]、[Z エンドデバイス (Z End Device)]、および[Z エンドインターフェイス (Z End Interface)] の各フィールドが自動的に設定されます。
- マップ上のデバイス ノードをクリックすると、[A エンドデバイス (A End Device)] フィールドが自動的に設定されます。A エンドデバイスが 1 つのデバイスのみ接続されている場合は、[Z エンドデバイス (Z End Device)] フィールドが自動的に設定されます。[A エンドデバイス (A End Device)] が複数のデバイスに接続されている場合は、[Z エンドデバイス (Z End Device)] を手動で選択する必要があります。

ステップ 12 A エンドデバイスと Z エンドデバイスの IP アドレスとマスクを入力します。

ステップ 13 次のオプションから L2 検出プロトコルを選択します。

- [なし (NONE)] : レイヤ 3 リンクに対して有効にする L2 Discovery Protocol がありません。
- [CDP] : ネットワークに接続されているシスコ デバイス間での通信を容易にするために レイヤ 3 リンクに対して有効にする Cisco Discovery Protocol。
- [LLDP] : シスコ以外のデバイスをサポートし、IEEE 802.1AB LLDP をサポートする他のデバイス間の相互運用を可能にするために、レイヤ 3 リンクに対して有効にする Link Layer Discovery Protocol。
- [ALL] : レイヤ 3 リンクに対して有効にする CDP と LLDP の両方。

ステップ 14 レイヤ 3 リンクに必要なルーティングプロトコルを選択します。値は[BGP]、[ISIS]、および[OSPF]です。ルーティングプロトコルの設定方法については、次を参照してください。[ルーティングプロトコルとセキュリティの設定](#)

ステップ 15 (オプション) レイヤ 3 リンクのリンク VLAN ID を入力します。

ステップ 16 (オプション) プロビジョニングするレイヤ 3 リンクで MPLS TE をサポートするには、[MPLS TE の有効化 (Enable MPLS TE)] チェックボックスをオンにします。

(注) このチェックボックスは、ルーティングプロトコルとして OSPF または ISIS を選択した場合にのみ使用できます。

ステップ 17 [次へ (Next)] をクリックし、[A エンド (A End)] と [Z エンド (Z End)] の詳細を入力します。フィールドと属性の説明については、[MPLS TE レイヤ 3 リンクの A エンドの詳細と Z エンドの詳細に関するフィールド参照 \(111 ページ\)](#) を参照してください。

ステップ 18 [展開アクション (Deployment Action)] フィールドに、MPLS レイヤ 3 リンクの作成プロセス完了時のアクションを指定します。実際に展開する前に、該当するデバイスに展開される設定のプレビューを表示するように指定することも、完了時にすぐに設定を展開するように指定することもできます。

ステップ 19 [送信 (Submit)] をクリックします。デバイスに展開される CLI のプレビューを表示することを選択した場合は、プレビューが表示されます。この場合、属性の編集 (Edit Attributes)] をクリックすることで、属性を変更できます。そうでない場合は、すぐに設定がデバイスに展開されます。

サービスが [ネットワーク トポロジ (Network Topology)] ウィンドウの [回線/VC (Circuits/VCs)] タブのリストに追加されます。プロビジョニング状態を確認するには、回線/VC 名の横にある [i] アイコンをクリックし、[回線/VC 360 (Circuit/VC 360)] ビューを表示します。

MPLS TE レイヤ 3 リンクの A エンドの詳細と Z エンドの詳細に関するフィールド参照

次の表に、MPLS TE レイヤ 3 リンクを定義する属性のリストを示し、説明します。

表 16: MPLS TE レイヤ 3 リンクの A エンドの詳細と Z エンドの詳細に関するフィールド参照

属性	説明	ルーティング プロトコルが次の場合に使用できます。
A エンドと同じ (Same as A End)	A エンドデバイスと Z エンドデバイスの両方に同じルーティングおよび MPLS-TE 設定を使用する場合は、このチェックボックスをオンにします。 (注) このチェックボックスは、プロビジョニングウィザードの [Z エンドの詳細 (Z End Details)] ページでのみ使用できます。	BGP、ISIS、および OSPF
BGP AS 番号 (BGP AS Number)	ネットワークに割り当てられている固有の BGP 自律システム番号を選択します。	BGP
ルート ポリシー (ルート ポリシー)	BGP が格納するルートとルーティングテーブルから取得するルートを制御するには、ルーティング ポリシーを選択します。	BGP
ルート リフレクタ クライアント (Route Reflector Client)	ローカルルートのリフレクタのルート リフレクタ クライアントとして BGP ネイバーを設定して使用可能なルートをアドバタイズするには、このチェックボックスをオンにします。	BGP
AIGP の使用 (Use AIGP)	レイヤ 3 リンクに Accumulated Interior Gateway Protocol (AIGP) メトリック属性を使用するには、このチェックボックスをオンにします。AIGP は、ネットワーク内のパスの累積エンドツーエンドメトリックを伝送する BGP 属性です。	BGP

属性	説明	ルーティング プロトコルが次の場合に使用できます。
更新の送信元 (Update Source)	<p>必要な送信元インターフェイスを選択します。</p> <p>(注) このフィールドは、[AIGP の使用 (Use AIGP)] チェックボックスがオフになっている場合にのみ使用できます。</p>	BGP
ISIS プロセス ID (ISIS Process ID)	<p>A エンド デバイスと Z エンド デバイスの両方で使用できる ISIS ルーティング プロセス ID を選択します。ISIS プロセスを設定する方法については、IS-IS の設定を参照してください。</p>	ISIS
ネットワーク (Network)	<p>選択した ISIS プロセス ID に基づいて、ネットワーク ID が自動的に設定されます。</p>	ISIS
回線タイプ (Circuit Type)	<p>次のオプションから、レイヤ3リンクに必要な隣接関係のタイプを選択します。</p> <ul style="list-style-type: none"> • [なし (NONE)] : 隣接関係は確立されません。 • [レベル 1 (Level-1)] : 選択したデバイスとそのネイバー間に共通するエリアアドレスが1つ以上ある場合は、レベル 1 隣接関係を確立します。 • [レベル 2 のみ (Level-2-only)] : 回線上にレベル 2 の隣接関係を確立します。隣接デバイスがレベル 1 のみのデバイスの場合、隣接関係は確立されません。 • [レベル 1-2 (Level-1-2)] : ネイバーもレベル 1-2 デバイスとして設定されており、共通するエリアが1つ以上ある場合、レベル 1 と 2 の隣接関係を確立します。共通のエリアがない場合は、レベル 2 の隣接関係が確立されません。 	ISIS

属性	説明	ルーティング プロトコルが次の場合に使用できます。
レベル1メトリック (Level 1 Metric)	レベル 1 (エリア内) ルーティングの SPF 計算で使用する必要があるメトリックを入力します。 (注) このフィールドは、[回線タイプ (Circuit Type)] を [レベル 1 (Level-1)] または [レベル 1-2 (Level-1-2)] として選択した場合にのみ使用できます。	ISIS
レベル2メトリック (Level 2 Metric)	レベル 2 (エリア間) ルーティングの SPF 計算で使用する必要があるメトリックを入力します。 (注) このフィールドは、[回線タイプ (Circuit Type)] を [レベル 2 (Level-2)] または [レベル 1-2 (Level-1-2)] として選択した場合にのみ使用できます。	ISIS
OSPF プロセス ID (OSPF Process ID)	OSPF ルーティング プロセス ID を選択します。OSPF プロセスを設定する方法については、 OSPF の設定 を参照してください。 (注) Z エンド デバイスの OSPF ルーティング プロセスは変更できません。	OSPF
OSPF Area	OSPF ルーティング プロセスを展開するエリアを入力します。	OSPF
メトリック (Metric)	OSPF ルーティング プロセスで使用されるルーティング メトリックを入力します。	OSPF

属性	説明	ルーティング プロトコルが次の場合に使用できます。
BFD テンプレート (BFD Template)	<p>レイヤ3 リンクの BFD テンプレートを選択します。BFD テンプレートは、BFD セッションで使用される設定可能パラメータのセットを定義します。これには、BFD 制御およびエコー パケットに使用される送受信タイマー、セッションが CV 関数を提供するとき使用される送信タイマー間隔、乗数値、およびエコー受信間隔が含まれます。</p> <p>(注) BFD テンプレートは、IOS-XE デバイスに適用できます。</p>	ISIS および OSPF
BFD 最小間隔 (BFD Min Interval)	<p>対応する BFD 設定範囲の BFD セッションの最小制御パケット間隔を入力します。</p> <p>(注) このフィールドは、[BFD テンプレート (BFD Template)] を選択していない場合にのみ使用できます。</p>	BGP、ISIS、および OSPF
BFD の乗数 (BFD Multiplier)	<p>BFD 乗数を入力します。この値は BFD 最小間隔とともに使用して、バンドルメンバリンクの非同期モードでの制御パケットとエコーパケットの両方の間隔と障害検出時間を決定します。</p> <p>(注) このフィールドは、[BFD テンプレート (BFD Template)] を選択していない場合にのみ使用できます。</p>	BGP、ISIS、および OSPF
BFD 高速検出 (BFD Fast Detect)	<p>隣接する転送エンジン間のパスで障害を迅速に検出するには、このチェックボックスをオンにします。</p> <p>(注) これは、Cisco IOS-XR デバイスにのみ適用されます。</p>	BGP、ISIS、および OSPF

属性	説明	ルーティング プロトコルが次の場合に使用できます。
認証モード (Authentication Mode)	ISIS パケットの送受信に必要な認証モードを選択します。 (注) 認証フィールドは、Cisco IOS XE デバイスを選択した場合にのみ使用できます。使用可能なオプションは、[なし (NONE)]、[HMAC_MD5]、および [テキスト (TEXT)] です。デフォルトでは、[なし (NONE)] が選択されます。	ISIS
認証キーチェーン (Authentication Key Chain)	認証キー チェーンを選択します。これにより、ルーティング プロトコルの認証が有効になり、認証キーのグループを識別します。	ISIS
送信専用の認証 (Authentication for Send Only)	送信される ISIS パケットに対してのみ認証を実行するには、このチェックボックスをオンにします。 (注) これは、IOS-XE デバイスにのみ適用されます。	ISIS
パスワードタイプ (Password Type)	パスワードタイプを [暗号化 (Encrypted)] または [プレーンテキスト (Plain Text)] として選択します。	BGP
パスワード (Password)	目的のパスワードを入力します。2つのピア間の接続を確立するには、パスワードが必要です。	BGP
MPLS-TE		
ループバック インターフェイス	レイヤ 3 リンクのループバック インターフェイス アドレスを選択します。ループバック インターフェイスを設定する方法については、「ループバック インターフェイスの設定」を参照してください。	ISIS および OSPF
Administrative Weight	MPLS TE トンネル メトリックを絶対モードで入力します。	ISIS および OSPF

属性	説明	ルーティング プロトコルが次の場合に使用できます。
TE 属性 (TE Attributes)	パス選択時にトンネルのアフィニティビットと比較する MPLS TE リンク属性を入力します。	ISIS および OSPF
パーセンテージを使用 (Is Percentage)	レイヤ3 リンクの帯域幅をパーセンテージで割り当てるには、このチェックボックスをオンにします。	ISIS および OSPF
グローバル帯域幅 (Global Bandwidth)	<p>CBR のレイヤ3 リンク用に予約される通常の TE トンネル帯域幅を入力します。</p> <p>たとえば、レイヤ3 リンクのグローバル帯域幅として 10% を割り当てる場合は、[パーセンテージを使用 (Is Percentage)] チェックボックスをオンにし、[グローバル帯域幅 (Global Bandwidth)] フィールドに値 10 を入力します。一方で、グローバル帯域幅として 50 Kbps を割り当てる場合は、[パーセンテージを使用 (Is Percentage)] チェックボックスをオフにし、[帯域幅の単位 (Bandwidth Unit)] ドロップダウンリストから [Kbps] を選択し、[グローバル帯域幅 (Global Bandwidth)] フィールドに値 50 を入力します。</p>	ISIS および OSPF
サブプール帯域幅 (Subpool Bandwidth)	<p>グローバル プール帯域幅から予約されているサブプール帯域幅を入力します。</p> <p>たとえば、レイヤ3 リンクのサブプール帯域幅として 10% を割り当てる場合は、[パーセンテージを使用 (Is Percentage)] チェックボックスをオンにし、[サブプール帯域幅 (Subpool Bandwidth)] フィールドに値 10 を入力します。一方で、サブプール帯域幅として 50 Kbps を割り当てる場合は、[パーセンテージを使用 (Is Percentage)] チェックボックスをオフにし、[帯域幅の単位 (Bandwidth Unit)] ドロップダウンリストから [Kbps] を選択し、[サブプール帯域幅 (Subpool Bandwidth)] フィールドに値 50 を入力します。</p>	ISIS および OSPF

属性	説明	ルーティング プロトコルが次の場合に使用できます。
自動トンネルバックアップ (Auto Tunnel Backup)	このチェックボックスをオンにして、ルータが MPLS TE トンネルを使用して設定されたインターフェイスでバックアップトンネルが動的に構築できるようにします。	ISIS および OSPF
バックアップトンネルでの SLRG の除外 (Exclude SLRG for Backup Tunnel)	このチェックボックスをオンにして、特定のインターフェイスに関連付けられた自動トンネルバックアップの特定のリンク上で、SRLG 値の除外を有効にできるようにします。	ISIS および OSPF
BFD 高速検出 (BFD Fast Detect)	隣接する転送エンジン間のパスで障害を迅速に検出するには、このチェックボックスをオンにします。	ISIS および OSPF
QoS		
Ingress Policy	A エンドデバイスと Z エンドデバイスで設定されている入力 QoS ポリシーを選択します。	BGP、ISIS、および OSPF
出力ポリシー (Egress Policy)	A エンドデバイスと Z エンドデバイスで設定されている出力 QoS ポリシーを選択します。	BGP、ISIS、および OSPF
追加設定 (Additional Settings)		
Enable MPLS TE	プロビジョニングするレイヤ 3 リンクで MPLS をサポートするには、このチェックボックスをオンにします。	ISIS および OSPF
SyncE の有効化 (Enable SyncE)	レイヤ 3 リンクのインターフェイス レベルで同期イーサネットを有効にするには、このチェックボックスをオンにします。 (注) これは、IOS-XE デバイスにのみ適用されます。	BGP、ISIS、および OSPF

MPLS TE サービスのプロビジョニングの前提条件

MPLS TE サービスをプロビジョニングするには、次の前提条件を満たす必要があります。

- OSPF または IS-IS は、MPLS TE サービスに参加するデバイスで設定する必要があります。

- MPLS TE L3 リンクをプロビジョニングする前に、LLDP/CDP を有効にする必要があります。
- MPLS TE サービス プロビジョニングに使用されるすべてのリンクは TE に対応している必要があります。
- TE に対応しているリンクは、運用上、稼働している必要があります。
- トンネルの送信元ノードと宛先ノードに到達可能である必要があります。
- WAE パラメータ REST コールは EPN Manager から自動的にセットアップできます。
- MPLS 到達可能性は、デバイス間で設定する必要があります。MPLS コア ネットワーク設定をセットアップする必要があります。
- MPLS TE サービスがプロビジョニングされるデバイスのインベントリ収集ステータスが、[完了済み (Completed)] である必要があります。これを確認するには、[インベントリ (Inventory)] > [デバイス管理 (Device Management)] > [ネットワーク デバイス (Network Devices)] に移動し、[最後のインベントリ収集ステータス (Last Inventory Collection Status)] 列でステータスを確認します。
- 必要に応じて、顧客をシステムに作成して、サービスの作成中およびプロビジョニングプロセス中に MPLS TE サービスを顧客に関連付けることができます。左のサイドバーから [インベントリ (Inventory)] > [その他 (Other)] > [顧客 (Customers)] を選択して、顧客を作成および管理します。

MPLS TE トンネルの作成とプロビジョニング

MPLS TE トンネルをプロビジョニングするには、次の手順を実行します。

始める前に

MPLS TE トンネルをプロビジョニングする前に満たす必要がある前提条件については、次を参照してください。 [MPLS TE サービスのプロビジョニングの前提条件 \(117 ページ\)](#)

-
- ステップ 1** 左側のサイドバーから、[マップ (Maps)] > [トポロジ マップ (Topology Maps)] > [ネットワーク トポロジ (Network Topology)] の順に選択します。
 - ステップ 2** [デバイス グループ (Device Groups)] をクリックして、MPLS TE トンネルを作成する場所を選択します。
 - ステップ 3** [デバイス グループ (Device Groups)] ポップアップ ウィンドウを閉じます。
 - ステップ 4** [ネットワーク トポロジ (Network Topology)] ウィンドウで [回線/VC (Circuits/VCs)] をクリックします。
 - ステップ 5** [+] アイコンをクリックします。マップ右側の新しいペインにプロビジョニングウィザードが表示されません。
 - ステップ 6** [テクノロジー (Technology)] ドロップダウンリストから [MPLS TE] を選択します。Cisco EPN Manager は、関連するサービス タイプのリストを [サービス タイプ (Service Type)] 領域に表示します。

- ステップ 7** [サービス タイプ (Service Type)] 領域で、[単方向 TE トンネル (Unidirectional TE Tunnel)] または [双方向 TE トンネル (Bidirectional TE Tunnel)] を選択します。
- ステップ 8** さまざまなサービスの属性を設定するためにプロファイルを定義している場合は、[プロファイルの選択 (Select Profile)] ドロップダウン リストから必要なプロファイルを選択します。 [回線/VC プロファイル \(134 ページ\)](#) を参照してください。
- ステップ 9** [次へ (Next)] をクリックして [カスタマー サービスの詳細情報 (Customer Service Details)] ページに移動します。
- ステップ 10** (オプション) サービスをプロビジョニングする対象としての顧客を選択します。リストに顧客が表示されない場合は、[インベントリ (Inventory)] > [その他 (Other)] > [顧客 (Customers)] の順に移動し、システムで顧客を作成してから、プロビジョニング ウィザードを再起動します。
- ステップ 11** サービス名とその説明を入力した後、サービスの詳細を入力します。 [サービスの詳細に関するフィールド参照 : MPLS TE トンネル \(119 ページ\)](#) を参照してください。
- (注)
- サービス名を指定しない場合、Cisco EPN Manager は次の形式でサービス名を割り当てます。
 - 送信元デバイスと宛先デバイスに共通のトンネル ID がある場合、サービス名は <SourceDeviceName>_<TunnelId>_<DestinationDeviceName> 形式で割り当てられます。
 - 送信元デバイスと宛先デバイスに固有のトンネル ID がある場合、サービス名は <SourceDeviceName>_<ATunnelId>_<ZTunnelId>_<DestinationDeviceName> 形式で割り当てられます。
 - トンネルのシグナル名は、システム内のデバイス間で一意である必要があります。
- ステップ 12** [次へ (Next)] をクリックした後、トンネル作成パラメータを入力します。フィールドと属性の説明については、 [トンネルの作成に関するフィールド参照 : MPLS TE トンネル \(121 ページ\)](#) を参照してください。
- ステップ 13** [次へ (Next)] をクリックした後、パスの制約の詳細を入力します。フィールドと属性の説明については、 [パスの制約の詳細に関するフィールド参照 : MPLS TE トンネル \(130 ページ\)](#) を参照してください。
- ステップ 14** [送信 (Submit)] をクリックします。デバイスに展開される CLI のプレビューを表示することを選択した場合は、プレビューが表示されます。この場合、属性の編集 (Edit Attributes)] をクリックすることで、属性を変更できます。そうでない場合は、すぐに設定がデバイスに展開されます。

[ネットワーク トポロジ (Network Topology)] ウィンドウの [回線/VC (Circuits/VCs)] ペインのリストにサービスが追加されます。プロビジョニング状態を確認するには、回線/VC名の横にある [i] アイコンをクリックし、[回線/VC 360 (Circuit/VC 360)] ビューを表示します。

サービスの詳細に関するフィールド参照 : MPLS TE トンネル

次の表に、MPLS TE トンネルを作成するためのサービスの詳細を定義する属性のリストを示し、説明します。

表 17: [サービスの詳細 (Service Details)]セクションのリファレンス : MPLS TE トンネル

属性	説明
FRR の有効化 (Enable FRR)	このチェックボックスをオンにすると、MPLS TE トンネルのリンクとノード保護を提供する高速再ルーティング機能が有効になります。 (注) このチェックボックスは、単方向TEトンネルを作成する場合にのみ使用できます。
自動帯域幅の有効化 (Enable Auto Bandwidth)	トラフィックに基づいて TE トンネルに最大帯域幅と最小帯域幅を自動的に割り当てるには、このチェックボックスをオンにします。
ラップ保護 (Wrap Protection)	中間リンクの障害シナリオを検出するには、このチェックボックスをオンにします。 (注) このチェックボックスは、双方向TEトンネルを作成する場合にのみ使用できます。
障害 OAM の有効化 (Enable Fault OAM)	MPLS TE トンネルのプロビジョニングとメンテナンスをサポートする障害 OAM プロトコルとメッセージを有効にするには、このチェックボックスをオンにします。 (注) このチェックボックスは、双方向TEトンネルを作成する場合にのみ使用できます。
自動ルートの有効化 (Enable Autoroute)	トンネルの自動ルートを有効にするには、このチェックボックスをオンにします。
BFD 設定の有効化 (Enable BFD Settings)	Bidirectional Forwarding Detection (BFD) プロトコルを有効にするには、このチェックボックスをオンにします。BFDは、高速転送パスの障害検出時刻と、一貫した障害検出方式を提供します。

属性	説明
保護タイプ (Protection Type)	<p>TE トンネルには、次のいずれかの保護メカニズムを選択します。</p> <ul style="list-style-type: none"> • [動作中 (Working)] : トンネルには動作中のパスのみが存在します。 • [動作中+保護 (Working+Protected)] : トンネルには動作中のパスと保護されたパスがあり、動作中のパスに障害が発生した場合、トラフィック フローは、リンクがダウンすることなく、保護されたパスに自動的にルーティングされます。 • [動作中+復元 (Working+Restore)] : トンネルには動作中のパスと復元パスがあり、動作中のパスに障害が発生するとリンクがダウンし、トラフィック フローが復元パスにルーティングされます。 • [動作中+保護+復元 (Working+Protected+Restore)] : トンネルには動作中のパス、保護パス、および復元パスがあり、動作中のパスに障害が発生した場合、トラフィック フローは保護されたパスにルーティングされます。また、保護されたパスにも障害が発生すると、リンクがダウンし、トラフィック フローが復元パスにルーティングされます。
展開アクション (Deployment Action)	<p>MPLS TE トンネル作成プロセスが完了したときに実行する操作を指定するには、次のいずれかのオプションを選択します。</p> <ul style="list-style-type: none"> • [プレビュー (Preview)] : 実際の展開前に、関連するデバイスに展開される設定をプレビューします。 • [展開 (Deploy)] : 完了直後に設定を展開します。

トンネルの作成に関するフィールド参照：MPLS TE トンネル

次の表に、MPLS TE トンネルの作成を定義する属性のリストを示し、説明します。

表 18:[トンネル作成 (Tunnel Creation)]セクションのリファレンス：MPLS TE トンネル

属性	説明
トンネルの作成 (Create Tunnel)	
送信元 (Source)	トンネルの送信元または A エンドポイント。
送信元ルーティングプロセス (Source routing Process)	TE が有効で、選択した送信元エンドポイントで設定されている OSPF または ISIS ルーティングプロセス。OSPF または ISIS ルーティングプロセスに基づいて、送信元エンドポイントで設定されたルータ ID とループバック アドレスを決定できます。

属性	説明
接続先 (Destination)	トンネルの宛先または Z エンドポイント。
宛先ルーティングプロセス (Destination Routing Process)	TE が有効になっており、選択した宛先エンドポイントで設定されている OSPF または ISIS ルーティングプロセス。OSPF または ISIS ルーティングプロセスに基づいて、宛先エンドポイントで設定されたルータ ID とループバック アドレスを決定できます。
トンネル設定 (Tunnel Setting)	
グローバル ID (Global ID)	送信元と宛先の両方のエンドポイントに割り当てられているグローバル ID。この ID は、2 つの単方向トンネルを 1 つの双方向 TE トンネルにバインドする ID と同じである必要があります。デフォルト値は 0 です。 (注) この属性は、双方向 TE トンネルを作成する場合にのみ使用できます。EPNM は、1 ~ 2147483647 の範囲内でのみグローバル ID をサポートします。
アフィニティビット (Affinity Bits)	アフィニティビットは、動的バックアップパスの設定時に双方向 TE トンネルが使用するリンク属性を決定します。
アフィニティ マスク (Affinity Mask)	アフィニティ マスクは、ルータが確認する必要があるリンク属性を決定します。 アフィニティビットとアフィニティマスクを使用して、動的バックアップパスを構成するときにリンク属性を含めるか除外することができます。マスクのビットが 0 の場合、そのビットに関連付けられているリンク属性の値とは無関係です。この場合、動的バックアップパスを設定する際に、リンク属性は除外されます。マスクのビットが 1 の場合、関連付けられているリンク属性の値は、そのビットのトンネルのアフィニティと一致する必要があります。この場合、動的バックアップパスを設定するときに link 属性が含まれます。
セットアップ優先度 (Setup Priority)	単方向または双方向の TE トンネルの LSP に割り当てられているセットアップ優先度。この優先度に基づいて、LSP は、ブロックする既存のトンネルか、または優先度の低い LSP を決定できます。 有効な値の範囲は 0 ~ 7 です。値が小さいほど、プライオリティが高いことを示します。たとえば、セットアップ優先順位が 0 の LSP は、セットアップ優先順位が 1 ~ 7 の任意の LSP をブロックできます。 (注) セットアップ優先度を保留優先度より高くすることはできません。

属性	説明
保留優先度 (Hold Priority)	<p>単方向または双方向の TE トンネルの LSP に割り当てられている保留優先度この優先度に基づいて、LSP はセットアップ優先度の高い別のシグナリング LSP によってブロックする必要があるかどうかを決定できます。</p> <p>有効な値の範囲は 0～7 です。値が小さいほど、プライオリティが高いことを示します。たとえば、保留優先度が 0 の LSP は、別の LSP によってブロックすることはできません。</p>
帯域幅プール タイプ (Bandwidth Pool Type)	<p>MPLS TE の制約ベースルーティング (CBR) の各リンクの予約可能帯域幅を管理するために使用される帯域幅プール。値は次のとおりです。</p> <ul style="list-style-type: none"> • [グローバル (Global)] : 通常の TE トンネル帯域幅。 • [サブプール (Subpool)] : グローバル プールの一部。サブプール帯域幅は、使用中以外はグローバルプールから予約されません。サブプールトンネルには、グローバルプールトンネルよりも高い優先度が必要です。 <p>(注) このフィールドは、[自動帯域幅の有効化 (Enable Auto Bandwidth)] チェックボックスがオフになっている場合にのみ使用できます。</p>
帯域幅 (Bandwidth)	<p>双方向 TE トンネルの帯域幅。値は Kbps 単位で指定する必要があります。</p> <p>たとえば、トンネルに 1000000 Kbps の帯域幅を割り当てる場合は、値を 1000000 Gbps と入力します。</p> <p>(注) このフィールドは、[自動帯域幅の有効化 (Enable Auto Bandwidth)] チェックボックスがオフになっている場合にのみ使用できます。</p>
自動最大帯域幅 (Auto Bandwidth Max)	<p>Cisco EPN Manager は、トラフィックに基づいて TE トンネルの最大帯域幅を自動的に割り当てます。ただし、必要に応じて帯域幅を変更できます。</p> <p>(注) このフィールドは、[顧客サービスの詳細 (Customer Service Detail)] 画面の [自動帯域幅の有効化 (Enable Auto Bandwidth)] チェックボックスをオンにした場合にのみ使用できます。</p>

属性	説明
自動最小帯域幅 (Auto Bandwidth Min)	<p>Cisco EPN Manager は、トラフィックに基づいて TE トンネルの最小帯域幅を自動的に割り当てます。ただし、必要に応じて帯域幅を変更できます。</p> <p>(注) このフィールドは、[顧客サービスの詳細 (Customer Service Detail)] 画面の [自動帯域幅の有効化 (Enable Auto Bandwidth)] チェックボックスをオンにした場合にのみ使用できます。</p>
帯域幅変更頻度 (秒) (Bandwidth Change Frequency (Sec))	<p>帯域幅変更頻度を秒単位で入力します。有効な範囲は 300 ~ 604800 です。</p> <p>(注) このフィールドは、トンネルの作成時に [顧客サービスの詳細 (Customer Service Detail)] ページの [自動帯域幅の有効化 (Enable Auto Bandwidth)] チェックボックスをオンにした場合にのみ使用できます。</p>
調整しきい値 (Adjustment Threshold)	<p>最大のサンプルパーセンテージが現在の帯域幅よりも大きいか、または小さい場合に、調整をトリガーする帯域幅調整しきい値をパーセンテージ単位で入力します。調整しきい値は、現在のトンネル帯域幅と絶対 (最小) 帯域幅のパーセンテージです。トンネルに再度シグナリングするには、自動帯域幅の両方のしきい値を満たす必要があります。トンネル帯域幅は、最大のサンプル出力レートと現在のトンネル帯域幅の差分が調整しきい値よりも大きい場合にのみ調整されます。</p> <p>Cisco IOS-XR デバイスを接続するトンネルの有効な範囲は 1 ~ 100 で、Cisco IOS-XE デバイスを接続するトンネルの範囲は 1 ~ 99 です。</p> <p>(注) このフィールドは、トンネルの作成時に [顧客サービスの詳細 (Customer Service Detail)] ページの [自動帯域幅の有効化 (Enable Auto Bandwidth)] チェックボックスをオンにした場合にのみ使用できます。</p>

属性	説明
オーバーフローしきい値 (Overflow Threshold)	<p>オーバーフロー検出をトリガーするには、オーバーフローしきい値をパーセンテージで入力します。これは、実際にシグナリングされたトンネル帯域幅のパーセンテージです。測定された帯域幅と実際の帯域幅の差分が、(オーバーフロー制限として定義された)連続して N 回のオーバーフローしきい値のパーセンテージよりも大きい場合、オーバーフロー検出がトリガーされます。</p> <p>Cisco IOS-XR デバイスを接続するトンネルの有効な範囲は 1 ~ 100 で、Cisco IOS-XE デバイスを接続するトンネルの範囲は 1 ~ 99 です。</p> <p>(注) このフィールドは、トンネルの作成時に [顧客サービスの詳細 (Customer Service Detail)] ページの [自動帯域幅の有効化 (Enable Auto Bandwidth)] チェックボックスをオンにした場合にのみ使用できます。</p>
オーバーフロー制限 (Overflow Limit)	<p>測定された帯域幅と実際のトンネルの帯域幅のちがいがトンネル用に定義されているオーバーフローしきい値を超える場合がある連続的な収集期間の数を入力します。</p> <p>有効な範囲は 1 ~ 10 です。</p> <p>(注) このフィールドは、トンネルの作成時に [顧客サービスの詳細 (Customer Service Detail)] ページの [自動帯域幅の有効化 (Enable Auto Bandwidth)] チェックボックスをオンにした場合にのみ使用できます。</p>
収集帯域幅 (Collect Bandwidth)	<p>トンネルの帯域幅情報を収集するには、このチェックボックスをオンにします。</p> <p>(注) このフィールドは、トンネルの作成時に [顧客サービスの詳細 (Customer Service Detail)] ページの [自動帯域幅の有効化 (Enable Auto Bandwidth)] チェックボックスをオンにした場合にのみ使用できます。</p>
BFD 設定 (BFD Settings)	
新規 BFD (New BFD)	<p>デフォルトでは、[BFD 設定の有効化 (Enable BFD Settings)] チェックボックスをオンにすると、このチェックボックスはオンになります。プロビジョニング中に双方向 (Flex LSP) と単方向のトンネルの両方に対して新しい BFD テンプレートを作成できます。</p>
BFD テンプレート名 (BFD Template Name)	<p>新しい BFD テンプレートの名前を入力します。</p>

属性	説明
BFD テンプレート (BFD Template)	<p>デバイス名を連結して、選択した BFD テンプレート名を表示します。たとえば、A エンド デバイスや Z エンド デバイスから連結します。既存のテンプレート名から既存のテンプレートを選択すると、関連する [最小間隔 (Min Interval)] と [乗数 (Multiplier)] の範囲値がデフォルトで表示されます。</p> <p>アルファベット、数字、および特殊文字の _ (アンダースコア)、- (ハイフン)、. (ドット) を使用することができ、BFD テンプレート名の長さは 32 文字未満である必要があります。</p> <p>BFD テンプレート名には. (ドット) または数字または数字と. (ドット) の組み合わせは使用できません。</p> <p>(注) このフィールドは、[新規 BFD (New BFD)] チェックボックスをオフにした場合にのみ使用できます。</p>
最小間隔 (Min Interval)	<p>BFD は、間隔と乗数を使用して、非同期モードで制御およびエコーパケットが送信される期間と、それらに対応する障害検出を指定します。障害検出タイマーは ($I \times M$) に基づいて起動します。この場合、I は最小間隔、M は乗数です。</p> <p>(注) これらのフィールドは、[BFD 設定の有効化 (Enable BFD Settings)] チェックボックスと [新規 BFD (New BFD)] チェックボックスがオンになっている場合にのみ使用できます。</p> <p>[最小間隔 (Min Interval)] と [乗数 (Multiplier)] の値が新しい BFD と既存の BFD の両方に表示されます。既存の BFD の場合は、値を編集することはできません。</p>
Multipplier (乗数)	

BFD テンプレートの使用に関するロジック

XE デバイスの単方向および FLEX の LSP トンネルに BFD テンプレート設定を使用します。XR デバイスの単方向および FLEX の LSP トンネルには、インライン設定を使用します。EPNM には、新しい BFD テンプレートを作成するか、または次のロジックに基づいて既存の BFD テンプレートを再利用するオプションが用意されています。



(注) FLEX LSP トンネルは双方向トンネルと呼ばれています。

次の表に、BFD テンプレートを使用するためのロジックを示します。

表 19: BFD テンプレートのロジック: MPLS TE トンネル

単一方向 (Unidirectional)

デバイス名の組み合わせ	設定ロジックの説明
XE-XE XE-XR	<p>XE デバイスを送信元と宛先（または XR デバイスを宛先）として選択した場合、ロジックは BFD テンプレート設定として動作します。</p> <p>新しい BFD テンプレートを作成するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. EPNM は、デフォルトで選択された [新規 BFD (New BFD)] チェックボックスを表示します。 2. BFD テンプレートの名前を入力します。 3. [最小間隔 (Min Interval)] に 4 ~ 1000 の範囲値を入力します。 4. [乗数 (Multiplier)] に 3 ~ 50 の範囲値を入力します。 <p>既存の BFD テンプレートを再利用するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. [新規 BFD (New BFD)] チェックボックスをオフにします。 2. [BFD テンプレート (BFD Template)] ドロップダウンリストから、既存の BFD テンプレートを選択します。A エンドデバイスの既存の BFD テンプレート名すべてのリストが表示されます。 3. [最小間隔 (Min Interval)] と [乗数 (Multiplier)] の範囲値が表示されます。 4. [送信 (Submit)] をクリックします。
XR-XR XR-XE	<p>XR デバイスを送信元と宛先（または XE デバイスを宛先）として選択した場合、ロジックはインライン設定として動作します。EPNM は、[最小間隔 (Min Interval)] フィールドと [乗数 (Multiplier)] フィールドのみを表示します。</p>
双方向	

XE-XE	<p>XE デバイスを送信元と宛先として選択した場合、ロジックは BFD テンプレート設定として動作します。</p> <p>BFD テンプレートを作成するには、次の手順を実行します。</p> <ol style="list-style-type: none">1. EPNM は、デフォルトで選択された [新規 BFD (New BFD)] チェックボックスを表示します。2. BFD テンプレートの名前を入力します。3. [最小間隔 (Min Interval)] に 4 ~ 1000 の範囲値を入力します。4. [乗数 (Multiplier)] に 3 ~ 50 の範囲値を入力します。 <p>既存の BFD テンプレートを再利用するには、次の手順を実行します。</p> <ol style="list-style-type: none">1. [新規 BFD (New BFD)] チェックボックスをオフにします。2. [BFD テンプレート (BFD Template)] ドロップダウンリストから、既存の BFD テンプレートを選択します。A エンド デバイスと Z エンド デバイスの既存の BFD テンプレート名すべてのリストが表示されます。3. [最小間隔 (Min Interval)] と [乗数 (Multiplier)] の範囲値が表示されます。4. [送信 (Submit)] をクリックします。
-------	---

XE-XR	<p>XE デバイスを送信元、XR デバイスを宛先として選択した場合、ロジックは BFD テンプレート設定として動作します。</p> <p>新しい BFD テンプレートを作成するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. EPNM は、デフォルトで選択された [新規 BFD (New BFD)] チェックボックスを表示します。 2. BFD テンプレート名を入力します。 3. [最小間隔 (Min Interval)] に 4 ~ 1000 の範囲値を入力します。 4. [乗数 (Multiplier)] に 3 ~ 10 の範囲値を入力します。 <p>既存の BFD テンプレートを再利用するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. [新規 BFD (New BFD)] チェックボックスをオフにします。 2. [BFD テンプレート (BFD Template)] ドロップダウンリストから、既存の BFD テンプレートを選択します。これにより、A エンドデバイスの既存のすべての BFD テンプレート名のリストが表示されます。 3. [最小間隔 (Min Interval)] と [乗数 (Multiplier)] の範囲値が表示されます。 4. [送信 (Submit)] をクリックします。
XR-XR	<p>XR デバイスを送信元と宛先として選択した場合、ロジックはインライン設定として動作します。EPNM は、[最小間隔 (Min Interval)] フィールドと [乗数 (Multiplier)] フィールドのみを表示します。</p>

XR-XE	<p>XR デバイスを送信元、XE デバイスを宛先として選択した場合、ロジックは BFD テンプレート設定として動作します。</p> <p>新しい BFD テンプレートを作成するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. EPNM は、デフォルトで選択された [新規 BFD (New BFD)] チェックボックスを表示します。 2. BFD テンプレートの名前を入力します。 3. [最小間隔 (Min Interval)] に 4 ~ 1000 の範囲値を入力します。 4. [乗数 (Multiplier)] に 3 ~ 10 の範囲値を入力します。 <p>既存のテンプレートを再利用するには、次の手順を実行します。</p> <ol style="list-style-type: none"> 1. [新規 BFD (New BFD)] チェックボックスをオフにします。 2. [BFD テンプレート (BFD Template)] ドロップダウンリストから、既存の BFD テンプレートを選択します。Z エンド デバイスの既存の BFD テンプレート名がすべて一覧表示されます。 3. [最小間隔 (Min Interval)] と [乗数 (Multiplier)] の範囲値が表示されます。 4. [送信 (Submit)] をクリックします。
-------	--

パスの制約の詳細に関するフィールド参照 : MPLS TE トンネル

次の表に、MPLS TE トンネルを作成するためのパスの制約の詳細を定義する属性のリストを示し、説明します。

表 20: パスの制約の詳細に関するセクションのリファレンス : MPLS TE トンネル

属性	説明
Path Type	TE トンネルに必要なパスを選択します。値は、[動作中 (Working)]、[保護 (Protected)]、および [復元 (Restore)] です。[パスタイプ (Path Type)] フィールドで選択した値に基づいて、[ワーキングパス (Working Path)]、[プロテクションパス (Protection Path)]、および [リストアパス (Restore Path)] フィールドグループを使用できます。
ロックダウンの有効化 (Enable Lock Down)	動作中の LSP を再最適化しない場合は、このチェックボックスをオンにします。
Enable SRLG	SRLG を有効にする場合は、このチェックボックスをオンにします。 (注) これは、保護パスでのみ設定できます。

属性	説明
スティッキの有効化 (Enable Sticky)	トンネルパスが変更された場合に新しい LSP に切り替えないようにするには、このチェックボックスをオンにします。 (注) ロックダウンが有効になっている場合にのみ、ワーキングパス用に設定できます。
非リバーティブの有効化 (Enable Non-Revertive)	動作中のパスが復元された場合でも、プロテクションパスから最初のワーキングパスに戻さない場合は、このチェックボックスをオンにします。 (注) これは、保護パスでのみ設定できます。
タイプ (Type)	トンネルに動作中のパスまたは保護パスのタイプを選択します。値は [動的 (Dynamic)] および [明示的 (Explicit)] です。
新規パス (New Path)	トンネルに新たに動作中のパス、保護パス、または復元パスを作成する場合にこのチェックボックスをオンにします。 (注) 以下のすべてのフィールドは、[タイプ (Type)] フィールドで [明示的 (Explicit)] を選択した場合にのみ使用できます。
既存のパスの選択 (Select Existing Path)	トンネルに既存の明示的な動作中のパス、保護パス、または復元パスを選択します。 (注) このフィールドは、[新規パス (New Path)] チェックボックスをオフにした場合にのみ使用できます。
WAE サーバからのパスの選択 (Choose path from WAE server)	WAE ネットワークとパスを指定するには、このチェックボックスをオンにします。 (注) このフィールドは、[新規パス (New Path)] チェックボックスをオンにした場合にのみ使用できます。 [動的 (Dynamic)] タイプと [パス (Path)] タイプを [動作中 (Working)] に選択した場合は、このチェックボックスをオンまたはオフにすることができます。明示的なパスを WAE サーバから直接読み取り、手動で設定しない場合は、このチェックボックスをオンにすることを推奨します。
WAE ネットワークの選択 (Select WAE Network)	下向き矢印をクリックして、ダイアログボックスから WAE ネットワークを選択します。 (注) このフィールドは、[WAE サーバからのパスの選択 (Choose path from WAE server)] チェックボックスをオンにした場合にのみ使用できます。

属性	説明
WAE パスの選択 (Select the WAE Path)	<p>下向きの矢印をクリックして、明示的なパスを選択します。</p> <p>(注) このフィールドは、[WAE サーバからのパスの選択 (Choose path from WAE server)] チェックボックスをオンにした場合にのみ使用できます。</p>
パス名 (Path Name)	<p>作成する明示的なパスの名前を入力します。[動作中のパス (Working Path)] テーブル、[保護パス (Protection Path)] テーブル、または [復元パス (Restore Path)] テーブルで、[+] ボタンをクリックしてテーブルに新しい行を追加した後、MPLS 対応デバイス、デバイスのインターフェイスとして明示的なパス コントローラ、およびパスの制約タイプを選択します。</p> <p>パス テーブルでは、送信元デバイスと宛先デバイスを除く MPLS 対応デバイスを選択できます。Cisco EPN Manager は厳密なパス制約タイプのみをサポートしています。</p> <p>(注) このフィールドは、[新規 (New)] チェックボックスをオンにした場合にのみ使用できます。</p>
	<p>[動作中のパス LSP 属性リスト (Working Path LSP Attribute List)]、[保護パス LSP 属性リスト (Protection Path LSP Attribute List)]、および [復元パス LSP 属性リスト (Restore Path LSP Attribute List)]</p> <p>[パス タイプ (Path Type)] フィールドで選択した値に基づいて、それぞれのフィールドグループを使用できます。</p> <p>ここで定義する LSP 属性は、[パス タイプ (Path Type)] フィールドで選択したパス オプションに関連付けられており、これらの属性は送信元デバイスと宛先デバイスに適用できます。</p> <p>(注) 特定のパス オプションに定義されている値は、インターフェイス トンネル レベルで指定された値をオーバーライドします。たとえば、動作中のパスの LSP 属性を定義した場合、これらの値はインターフェイス トンネル レベルの [トンネル設定 (Tunnel Settings)] セクションで定義した値をオーバーライドします。これは、すべてのパス オプションに共通しています。</p> <p>双方向トンネルでは、[ロックダウンの有効化 (Enable Lock Down)] チェックボックスをオフにした場合にのみ、[ワーキングパス (Working Path)] LSP 属性リストを設定できます。</p>
新しい LSP 属性リスト (New LSP Attribute List)	<p>選択したパス タイプに新しい LSP 属性リストを作成するには、このチェックボックスをオンにします。</p>

属性	説明
既存の LSP 属性リスト (Existing LSP Attribute List)	<p>選択したパス タイプの既存の LSP 属性リストを選択します。</p> <p>(注) このフィールドは、[新規 LSP 属性リスト (New LSP Attribute List)] チェックボックスをオフにした場合にのみ使用できます。</p>
LSP 属性リスト名 (LSP Adjustment Threshold Name)	<p>作成する LSP 属性リストの名前を入力します。</p> <p>(注) このフィールドを含む以下のすべてのフィールドは、[新しい LSP 属性リスト (New LSP Attribute List)] チェックボックスがオフの場合、読み取り専用として表示されます。</p>
LSP アフィニティビット (LSP Affinity Bits)	<p>バックアップ パス (動作中、保護、または復元) の設定時に双方向 TE トンネルが使用するリンク属性を決定する LSP アフィニティビットを入力します。</p>
LSP アフィニティマスク (LSP Affinity Mask)	<p>バックアップ パスの設定時にルータが確認する必要があるリンク属性を決定する LSP アフィニティ マスクを入力します。</p>
LSP セットアップ優先度 (LSP Setup Priority)	<p>選択したパス タイプの LSP に割り当てられているセットアップ優先度を入力します。この優先度に基づいて、LSP は、ブロックする既存のトンネルか、または優先度の低い LSP を決定できます。</p> <p>有効な値の範囲は 0 ~ 7 です。値が小さいほど、プライオリティが高いことを示します。たとえば、セットアップ優先順位が 0 の LSP は、セットアップ優先順位が 1 ~ 7 の任意の LSP をブロックできます。</p> <p>(注) LSP セットアップ優先度を LSP 保留優先度より高くすることはできません。</p> <p>(注) Cisco IOS-XR デバイスの場合、[LSP セットアップ優先度 (LSP Setup Priority)] フィールドと [LSP 保留優先度 (LSP Hold Priority)] フィールドは適用されません。</p>

属性	説明
LSP 保留優先度 (LSP Hold Priority)	<p>選択したパスタイプの LSP に割り当てられている保留優先度を入力します。この優先度に基づいて、LSP はセットアップ優先度の高い別のシグナリング LSP によってブロックする必要があるかどうかを決定できます。</p> <p>有効な値の範囲は 0～7 です。値が小さいほど、プライオリティが高いことを示します。たとえば、保留優先度が 0 の LSP は、別の LSP によってブロックすることはできません。</p> <p>(注) Cisco IOS デバイスの場合、LSP 保持優先度を指定しない場合は、Cisco EPN Manager は [LSP セットアップ優先度 (LSP Setup Priority)] フィールドで指定された値を取得します。</p> <p>(注) Cisco IOS-XR デバイスの場合、[LSP セットアップ優先度 (LSP Setup Priority)] フィールドと [LSP 保留優先度 (LSP Hold Priority)] フィールドは適用されません。</p>
LSP レコードルート (LSP Record Route)	チェックボックスをオンにして、LSP が使用するルートを記録します。

回線/VC プロファイル

プロファイルには、各種回線/VC固有の一連の属性が含まれています。作成したプロファイルは、回線/VCの作成時にすべてのユーザに対して選択可能になります。プロファイルを選択すると、プロビジョニングウィザードにプロファイル属性が読み込まれます。ユーザが行う必要がある操作はサービスのエンドポイントの定義だけです。また必要に応じて、回線/VCのプロビジョニング前に多少変更を行います。

作成できるプロファイルのタイプは、プロビジョニング可能な回線/VCのタイプを反映しています。

各プロファイルには一意の名前が指定されるので、回線/VCタイプごとに、必要に応じて複数のプロファイルを作成できます。

プロファイルを作成するには、次の手順に従います。

-
- ステップ 1** 左側のナビゲーションペインで **Inventory > Other > Profiles** を選択します。[プロファイル (Profiles)] ウィンドウが開き、既存のプロファイルの表が表示されます (存在する場合)。表でプロファイルを選択して、そのプロファイルを編集または削除できます。
- ステップ 2** **Create Profile** をクリックします。
- ステップ 3** プロファイル作成ウィザードで、プロファイルに一意の名前を指定し、説明を入力します。
- ステップ 4** [テクノロジー (Technology)] リストから、[Carrier Ethernet]、[Optical]、または [L3VPN] を選択します。選択したテクノロジーに関連するサービスタイプが表示されます。

ステップ5 必要なサービス タイプを選択します。

L3VPN のサービスの場合、ほとんどの L3VPN サービス作成フィールドに値を事前に読み込むことができるプロファイルを作成するには、[ユニキャスト (Unicast)] を選択します。L3VPN サービスの IP SLA 固有のオプションを使用してプロファイルを作成するには、[IPSLA 操作 (IPSLA Operations)] を選択します。

ステップ6 **Next** をクリックし、属性定義ページに移動して、選択したサービスタイプの属性を定義します。プロファイルの属性は、プロビジョニング ウィザードの属性と同じであり、次に示す関連セクションで説明しています。

イーサネット VC 属性の詳細については、次のトピックで説明します。

- サービス自体に関連する属性については、次を参照してください：[サービス詳細の参考資料 \(22 ページ\)](#)
- UNI 固有の属性については、次を参照してください：[新規 UNI の詳細リファレンス \(23 ページ\)](#)
- サービス内で機能する UNI に関連する属性については、[UNI サービス詳細の参照 \(24 ページ\)](#) を参照してください。
- QoS プロファイルの属性については、次を参照してください：[QoS プロファイルの作成 \(135 ページ\)](#)
- UNI 属性については、次を参照してください。[UNI としてのデバイスおよびインターフェイスの設定 \(28 ページ\)](#)
- ENNI 属性については、次を参照してください：[デバイスとインターフェイスを ENNI として設定する \(29 ページ\)](#)

OCH 属性と OTN 属性については、[OCH 回線タイプの \[回線 \(Circuit\)\] セクションリファレンス \(42 ページ\)](#) と [OTN 回線タイプの回線セクション参照 \(61 ページ\)](#) で説明します。

L3VPN 属性については、[新規 L3VPN サービスの作成およびプロビジョニング \(74 ページ\)](#) と [L3VPN サービスの詳細表示 \(91 ページ\)](#) で説明します。

ステップ7 属性の定義が完了したら、**Create Profile** をクリックします。[プロファイル (Profiles)] ウィンドウの表にプロファイルが追加されます。

QoS プロファイルの作成

EVC を作成およびプロビジョニングする際に選択可能にする QoS プロファイルのライブラリを作成できます。選択する QoS プロファイルによって、UNI または EVC レベルでのさまざまなクラスのトラフィックの帯域幅プロファイルが決まり、クラス分けされたトラフィックの処理方法が定義されます。

QoS プロファイルでは最大4つのレベル（超高、高、中、低）の帯域幅プロファイルを定義できます。各帯域幅プロファイルでは、トラフィックの一致基準を指定します。その一致基準を満たすトラフィックは、その帯域幅プロファイルに属するものとして分類されます。

QoS プロファイルを作成するには、次の手順に従います。

- ステップ 1** 新規キャリアイーサネット EVC の作成およびプロビジョニング (13 ページ) の手順に従って、プロビジョニング ウィザードにアクセスします。
- ステップ 2** [テクノロジー (Technology)] ドロップダウン リストから [キャリアイーサネット (Carrier Ethernet)] を選択します。
- ステップ 3** [サービス タイプ (Service Type)] ドロップダウン リストから **QoS Profile** を選択します。
- ステップ 4** **Next** をクリックして QoS プロファイルの定義ページに移動します。
- ステップ 5** QoS プロファイルの一意の名前と説明を入力します。
- ステップ 6** QoS プロファイルを選択可能にする場所 (QoS プロファイルのドロップダウン リストに表示する場所) を定義するために、必要なチェックボックスをオンにします。
- [インターフェイスに適用 (Applicable for Interfaces)] : UNI または ENNI をプロビジョニングする際に QoS プロファイルが選択可能になります。
 - [仮想サービスに適用 (Applicable for Virtual Services)] : VLAN ベースのサービス (EVPL、EV-LAN など) を作成する際に、QoS プロファイルが UNI サービス属性として選択可能になります。
 - [プライベート サービスに適用 (Applicable for Private Services)] : プライベート VC (EPL、EP-LAN など) を作成する際に、QoS プロファイルが UNI サービス属性として選択可能になります。
- ステップ 7** [分類 (Classification)] フィールドに、トラフィックを識別して分類するために使用する方法を指定し、必要な帯域幅プロファイルの [一致基準 (Match Criteria)] フィールドに該当する値を入力します。
- [DSCP] : DiffServ コードポイント (DSCP) 値を使用してトラフィックを分類します。有効な値は 0 ~ 63 です。最大 8 つのカンマ区切り値を入力できます。
 - [COS] : PCP とも呼ばれます。COS は、FCoe やその他のトランキング デバイスをサポートするホストからのレイヤ 2 フレームのヘッダーに含まれる IEEE 802.1Q ビットです。有効な値は 0 ~ 7 です。複数のカンマ区切り値またはハイフンで表記された値の範囲 (たとえば、0-2) を入力できます。
- ステップ 8** サービスに適用する 1 つ以上のサービス クラスを選択します。
- ステップ 9** 選択するサービス クラスごとに、一致基準および基準と一致するトラフィックの処理方法を指定する帯域幅プロファイルを定義します。上記の **ステップ 7** で説明したように帯域幅プロファイルごとに一致基準を入力します。
- ステップ 10** 帯域幅プロファイルごとに、一致するトラフィックの処理方法を指定するルールを作成します。入力トラフィックと出力トラフィックに別々のルールを作成することも、トラフィックの両方向で適用するルールを作成することもできます。各ルールでは、以下の項目を指定します。
- [設定情報レート (CIR) (Committed Information Rate (CIR))] : 1 秒あたりのビット数 (bps) で指定される、長期的な平均転送速度。
 - [認定バースト サイズ (CBS) (Committed Burst Size (CBS))] : トラフィック バーストの最大許容サイズ (バイト数)。この値を超えると、トラフィックは CIR を超過したとみなされます。
 - [超過情報レート (EIR) (Excess Information Rate (EIR))] : パケットに許容される最大平均レート。EIR には、CIR の値と同じか、それより大きい値を指定します。通常、CIR を超過したパケットは廃棄されます。
 - [超過バースト サイズ (EBS) (Excess Burst Size (EBS))] : トラフィック バーストの最大許容サイズ (バイト数)。この値を超えると、トラフィックは EIR を超過したとみなされます。

- [カラー モード (Color Mode)] : トラフィックの色分けを適用するかどうかを指定します。

ステップ 11 必要なすべての帯域幅プロファイルを定義したら、**Submit** をクリックします。QoS プロファイルが作成され、VC を作成する際に選択可能になります。

顧客の作成

回線/VC プロビジョニングプロセス中に選択に使用できるように、システムに顧客を作成する必要があります。

顧客を作成するには、次の手順を実行します。

ステップ 1 左側のサイドバーから **Inventory > Other > Customers** を選択します。

ステップ 2 **Create Customer** をクリックします。

ステップ 3 顧客の名前と (必要に応じて) 説明を入力します。

ステップ 4 **OK** をクリックします。これで、顧客が顧客のテーブルに追加されます。編集または削除する顧客を選択できます。

アンマネージド エンドポイントを使用した回線/VC のプロビジョニング

1つ以上のエンドポイントが Cisco EPN Manager で管理されないデバイスであっても、回線/VC を作成してプロビジョニングすることができます。[プロビジョニングウィザード (Provisioning Wizard)]を使用することで、エンドポイント デバイスを「アンマネージド」として識別したり、システムが回線/VCを作成できるようにアンマネージドデバイスに関する情報を指定したりできます。アンマネージドデバイスを識別すると、そのデバイスはシステムのアンマネージドデバイス グループ内で有効になり、他のサービスに使用できるようになります。

ステップ 1 [回線/VC のプロビジョニング \(1 ページ\)](#) の説明に従って、対象のテクノロジーに応じた回線/VC 作成プロセスを開始します。

ステップ 2 ポイントツーポイント EVC および CEM サービスの場合 :

- a) Z エンドポイントを定義する際に、[アンマネージドデバイス (Unmanaged Device)] チェックボックスをオンにします。[アンマネージドデバイスの詳細 (Unmanaged Device Details)] パネルが開きます。
- b) システム内ですでに識別されているアンマネージド デバイスの場合、[新規デバイス (New Device)] チェックボックスをオフにして、リストから必要なデバイスを選択します。新しいアンマネージド デバイスを識別する場合は、デバイス名、IP アドレス、および LDP IP を入力します。LDP IP は、管理対象デバイス上の疑似回線のネイバー アドレスとして使用されます。

- ステップ3** ポイントツーマルチポイントまたはマルチポイントツーマルチポイントEVCの場合、[アンマネージドUNI (Unmanaged UNI)] ページでテーブル内のプラス アイコンをクリックして行を追加し、選択した行に対するアンマネージドデバイスの詳細とサービスエンドポイントの詳細を定義します。
- ステップ4** [回線/VCのプロビジョニング \(1 ページ\)](#) の説明に従って、対象テクノロジーの回線/VCの作成およびプロビジョニングプロセスを完了します。

テンプレートを使用した回線/VCの拡張

回線/VCを作成してプロビジョニングすると、Cisco EPN Managerは参加デバイスに一連のCLIコマンドを設定します。同じデバイスに追加のコマンドを設定する必要がある場合は、それらのコマンドを含むテンプレートを作成して、回線/VCの作成プロセス中にそのテンプレートを含めることができます。こうすることで、Cisco EPN Managerによる設定内容を超えて、回線/VCを効果的に拡張できます。この機能はプロビジョニングウィザードで使用できますが、回線/VCの作成前または変更前に作成されるテンプレートに依存しています。

CLIテンプレートを使用した回線/VCの拡張には、次の手順が含まれます。

1. 空白のテンプレートまたは既存のテンプレートを使用して、CLIテンプレートを作成します。空白テンプレートを使用した新しいCLI設定テンプレートの作成および既存のテンプレートを使用した新規CLI設定テンプレートの作成を参照してください。
2. 回線/VCを作成または変更し、CLIテンプレートを付加します。回線/VCのプロビジョニング (1 ページ) を参照してください。

ステップ1 CLIテンプレートを作成します。

- a) 左のサイドバーで、[設定 (Configuration)] > [テンプレート (Templates)] > [機能およびテクノロジー (Features & Technologies)] を選択します。
- b) [テンプレート (Templates)] パネルで、[CLIテンプレート (CLI Templates)] > [CLI] を選択します。
- c) CLI、グローバル変数、および/またはテンプレート変数を使用して、新しい回線の識別情報を指定し、テンプレートの内容を定義します。「CLIテンプレートの作成」およびテンプレートでのグローバル変数の使用を参照してください。
- d) [新しいテンプレートとして保存 (Save as New Template)] をクリックします。
- e) [マイテンプレート (My Templates)] > [CLIテンプレート (ユーザ定義) (CLI Templates (User Defined))] の下に、新しいCLIテンプレートが保存されます。

ステップ2 作成したテンプレート（または該当する場合には異なるテンプレート）を含むサービスを作成または変更します。

- a) 左側のサイドバーから、[マップ (Maps)] > [トポロジマップ (Topology Maps)] > [ネットワークトポロジ (Network Topology)] を選択します。
[ネットワークトポロジ (Network Topology)] ウィンドウが開きます。
- b) [回線/VC (Circuits/VCS)] タブをクリックします。

- c) [回線/VC (Circuits/VCS)] ペイン ツールバーから、[+] ([作成 (Create)]) アイコンをクリックするか、回線を選択してから鉛筆 ([変更 (Modify)]) アイコンをクリックします。
マップの右側の新しいペインでプロビジョニング ウィザードが開きます。
- d) 必要な回線または VC の作成または変更を開始します。 [回線/VC のプロビジョニング \(1 ページ\)](#) および [回線/VC の変更](#) を参照してください。
- e) [サービス テンプレート (Service Template)] ページで、テンプレートをサービス設定のプレフィックスにする場合は [事前設定 (Pre-Configuration)] セクションを使用し、テンプレートをサービス設定のサフィックスにする場合は [事後設定 (Post-Configuration)] セクションを使用します。
- f) [テンプレート (Template)] ドロップダウンメニューで、必要な CLI テンプレートを選択します。
事前設定オプションと事後設定オプションの両方に同じ CLI テンプレートを選択することはできません。
- g) [テンプレートの使用 (Template Usage)] ドロップダウンメニューで、デバイスに CLI テンプレートを設定する条件を示すオプションを選択します。たとえば [サービス作成のみ (Service Create Only)] を選択した場合、サービスの作成時にのみ、テンプレート CLI がデバイスに設定されます。サービスの変更時には設定されません。
- h) テンプレート パラメータの値を入力します。ここに示すパラメータは、テンプレートに定義された変数によって異なります。
- i) [送信 (Submit)] をクリックします。
(注) デフォルトでは、サービスに参加するすべてのデバイスに、選択された CLI テンプレートが関連付けられます。CLI テンプレートに関連付ける特定のデバイスを選択することはできません。

ステップ 3 設定したテンプレート用のロールバックテンプレートを設定できます。 [設定例：ロールバックテンプレート \(144 ページ\)](#) を参照してください。

ステップ 4 インタラクティブ テンプレートを設定することもできます。 [設定例：インタラクティブ テンプレート \(146 ページ\)](#) を参照してください。

設定例：CLI テンプレートを使用した回線/VC の拡張

設定例 1：グローバルおよびテンプレート (ローカル) 変数を持つ CLI テンプレートを使用した Cisco ASR 903 デバイスでの L3VPN サービスの拡張：

```
vrf definition Testdoc1
exit
vrf Testdoc1
  vpn id 36B:3
  address-family ipv4 unicast
    import route-target
      65:1
    export route-target
      65:1
  address-family ipv6 unicast
    import route-target
      65:1
```

```

export route-target
  65:1
interface GigabitEthernet0/0/0/11.2
  vrf Testdoc1
  ipv4 address 4.5.7.8 255.255.255.0
  mtu 1522
router bgp 140
  vrf Testdoc1
  rd auto
  address-family ipv6 unicast
  address-family ipv4 unicast
  redistribute static metric 54
  neighbor 3.4.6.8
  remote-as 21
  address-family ipv4 unicast
  exit
  exit
  exit
exit
interface GigabitEthernet0/0/6
desc postconfig
delay 5988
mtu 436
exit

```

設定例 2 : グローバル変数とテンプレート (ローカル) 変数を持つ CLI テンプレートを使用した CEM サービスの拡張 :

```

#set($interfaceNameList = $gv.service-cem-cemInterfaceNameList.split(","))
#set($cemGroupNumberList = $gv.service-cem-cemGroupNumberList.split(","))
#set($count = 0)
#foreach($interfaceName in $interfaceNameList)
  interface $interfaceName
    service-policy input MainInterfacePolicy
    #if($count == 0)
      cem $cemGroupNumberList[0]
    #else
      cem $cemGroupNumberList[1]
    #end
    service-policy input servicePolicy
    #set($count = $count+1)
#end

```

設定例 3 : QoS over CEM を設定する CEM サービスの拡張 :

```

#set($count = 0)
#foreach($interfaceName in $gv.service-cem-cemInterfaceNameList)
  interface $interfaceName
  service-policy input MainInterfacePolicy
  #if($count == 0)
  cem $gv.service-cem-cemGroupNumberList[0]
  #else
  cem $gv.service-cem-cemGroupNumberList[1]
  #end
  service-policy input servicePolicy
  #set($count = $count+1)
#end
exit

```

設定例 4 : Cisco ME3800 デバイス上でのグローバル変数とテンプレート変数を持つ CLI テンプレートを使用した CE サービスの拡張 : 強調表示されたテキストは、CE サービスのプロビジョニング設定の前後に追加される設定前と設定後の変更を表します。

```

pseudowire-class PWClass_51_192-168-12-29
protocol ldp
exit
ethernet cfm domain EVC level 4
  service evplextnpseudowireclass_ evc evplextnpseudowireclass_
    continuity-check
    continuity-check interval 1s
ethernet evc evplextnpseudowireclass
interface GigabitEthernet0/11
  no shutdown
  no spanning-tree portfast
  mtu 1522
  ethernet uni id 3800x
  service instance 1 ethernet evplextnpseudowireclass
    encapsulation dot1q 88
    xconnect 192.168.12.29 51 encapsulation mpls pw-class PWClass_51_192-168-12-29
    mtu 1508
  service instance 1 ethernet evplextnpseudowireclass_
    cfm mep domain EVC mpid 2
    ethernet lmi ce-vlan map 88
ip sla 17
  ethernet y1731 loss SLM domain EVC evc evplextnpseudowireclass_ mpid 1 cos 5 source
mpid 2
  history interval 5
  aggregate interval 60
ip sla schedule 17 life forever start-time after 00:02:00
interface GigabitEthernet0/11
desc postconfig
exit

```

設定例 5 : グローバル変数とテンプレート (ローカル) 変数を持つ CLI テンプレートを使用したレイヤ 3 リンク サービスの拡張 :

```

##CREATE AND MODIFY CASE
#if($gv.service-serviceOperationType == "CREATE" || $gv.service-serviceOperationType ==
"MODIFY")
##XE DEVICE
#if($variant=="IOS-XE")
#if($gv.service-l3Link-routingProtocolName=="BGP")
  router bgp $gv.service-l3Link-routerProcessId
    address-family ipv4
      neighbor $gv.service-l3Link-bgpNeighborName next-hop-self all
    ##assume A End as remote building
    #if($gv.service-l3Link-isRouteReflectorClient=="TRUE" && $prefixListName!="")
&& $gv.service-l3Link-endPointDesignation=="AEND")
      neighbor $gv.service-l3Link-bgpNeighborName capability orf prefix-list send
      neighbor $gv.service-l3Link-bgpNeighborName prefix-list $prefixListName
in
      #elseif($gv.service-l3Link-isRouteReflectorClient=="TRUE" &&
$prefixListName!="") && $gv.service-l3Link-endPointDesignation=="ZEND")
      neighbor $gv.service-l3Link-bgpNeighborName capability orf prefix-list receive
    #end
  exit
  exit
#end

#if($xeMTU!="" || $xeClnsMTU!="")
interface $gv.service-l3Link-interfaceName
  #if($xeMTU!="")
    mtu $xeMTU
  #end
  #if($xeClnsMTU!="")
    clns mtu $xeClnsMTU
  #end

```

```

        exit
    #end

    #if($gv.service-l3Link-routingProtocolName=="BGP")
    #if($addressFamily != "" && $addressFamily=="vpn4")
        router bgp $gv.service-l3Link-routerProcessId
        address-family $addressFamily
            neighbor $gv.service-l3Link-bgpNeighborName activate
        neighbor $gv.service-l3Link-bgpNeighborName send-community both
    #if($gv.service-l3Link-isRouteReflectorClient=="TRUE")
        neighbor $gv.service-l3Link-bgpNeighborName route-reflector-client
    #end
        bgp additional-paths install
        neighbor $gv.service-l3Link-bgpNeighborName next-hop-self all
        exit
    #end
#end
#end
##XR DEVICE
#else

    #if($xrMTU!="")
    #if($gv.service-l3Link-subInterfaceName!="")
        interface $gv.service-l3Link-subInterfaceName
            mtu $xrMTU
        #end
    #else
        interface $gv.service-l3Link-interfaceName
            mtu $xrMTU
        #end
    #end
#end

    #if($gv.service-l3Link-routingProtocolName=="BGP")
    #if($addressFamily != "" && $addressFamily=="vpn4")
        router bgp $gv.service-l3Link-routerProcessId
        address-family $addressFamily unicast
        additional-paths receive
        #end
        neighbor $gv.service-l3Link-bgpNeighborName
        address-family $addressFamily unicast
            #if($gv.service-l3Link-isRouteReflectorClient=="TRUE")
                route-reflector-client
            #end
        #end
        aigp
            #if( $routePolicyName!="")
                route-policy $routePolicyName in
            #end
        #end
        #end
    #end
#end

#end

##DELETE USE CASE
#elseif($gv.service-serviceOperationType == "DELETE")
##XE DEVICE
#if($variant=="IOS-XE")

    #if($xeMTU!="" || $xeClnsMTU!="")
        interface $gv.service-l3Link-interfaceName
    
```

```

        #if($xeMTU!="")
            no mtu $xeMTU
        #end
        #if($xeClnsMTU!="")
            no clns mtu $xeClnsMTU
        #end
        exit
    #end

    #if($gv.service-l3Link-routingProtocolName=="BGP")
    #if($addressFamily != "" && $addressFamily=="vpnv4")
        router bgp $gv.service-l3Link-routerProcessId
        no address-family $addressFamily
        exit
    #end
    #end

##XR DEVICE
#else
    #if($xrMTU!="")
        #if($gv.service-l3Link-subInterfaceName=="")
            interface $gv.service-l3Link-interfaceName
            no mtu $xrMTU
            exit
        #end
        #end

        #if($gv.service-l3Link-routingProtocolName=="BGP")
        #if($addressFamily != "" && $addressFamily=="vpnv4")
            router bgp $gv.service-l3Link-routerProcessId
            address-family $addressFamily unicast
            no additional-paths receive
            exit
            neighbor $gv.service-l3Link-bgpNeighborName
            no address-family $addressFamily unicast
            exit
        #end
        #end

#end

#end

```

設定例 6 : グローバル変数とテンプレート (ローカル) 変数を持つ CLI テンプレートを使用した双方向 TE トンネルの拡張 :

```

##CREATE AND MODIFY CASE
#if($gv.service-serviceOperationType == "CREATE" || $gv.service-serviceOperationType ==
"MODIFY")
    #if($variant && $variant=="IOS-XE")
        #if($gv.service-teTunnel-tunnelId && $gv.service-teTunnel-tunnelId!="")
            #if($xeBandWidth && $xeBandWidth != "")
                interface Tunnel$gv.service-teTunnel-tunnelId
                bandwidth $xeMaxBandWidth
                tunnel mpls traffic-eng auto-bw frequency $xeBandWidth max-bw
                $xeMaxBandWidth min-bw $xeMinBandWidth
                exit
            #end
        #end
    #end
#else
    #if($gv.service-teTunnel-tunnelId && $gv.service-teTunnel-tunnelId!="")

```

```

    #if($xrBandWidth && $xrBandWidth!="")
        interface tunnel-te$gv.service-teTunnel-tunnelId
            bandwidth $xrMaxBandWidth
            auto-bw
            bw-limit min $xrMinBandWidth max $xrMaxBandWidth
            application $xrBandWidth
        exit
    exit
#end
#end
#end
#elseif($gv.service-serviceOperationType == "DELETE")
    #if($variant && $variant=="IOS-XE")
        #if($gv.service-teTunnel-tunnelId && $gv.service-teTunnel-tunnelId!="")
            #if($xeBandWidth && $xeBandWidth!="")
                interface Tunnel$gv.service-teTunnel-tunnelId
                    no bandwidth
                    no tunnel mpls traffic-eng auto-bw
                exit
            #end
        #end
    #end
#else
    #if($gv.service-teTunnel-tunnelId && $gv.service-teTunnel-tunnelId!="")
        #if($xrBandWidth && $xrBandWidth!="")
            interface tunnel-te$gv.service-teTunnel-tunnelId
                no bandwidth
                no auto-bw
            exit
        #end
    #end
#end
#end
#end

```

設定例：ロールバックテンプレート

ロールバックテンプレートを作成して、展開に失敗した場合に使用することができます。
 [Configuration] > [Templates] > [Features and Technologies] の順に移動し、[CLI Templates] を選択してカスタムロールバックテンプレートを設定します。テンプレートを設定する際は、ロールバックのフラグとして #ROLLBACK_CONFIG_START と #ROLLBACK_CONFIG_END を使用する必要があります。これらのフラグの間で、CLI がロールバックする必要があるものを指定する必要があります。これは、サービス前とサービス後の両方の設定に使用できます。



(注) これらのロールバックテンプレートは、光サービスには適用されません。

サンプルテンプレート形式

```

#ROLLBACK_CONFIG_START
interface GigabitEthernet0/0/20
mtu 1555
#ROLLBACK_CONFIG_END

```

設定例 1：パラメータのない設定前 CLI のロールバック：

CLI の例：


```
snmp-server enable traps
FAIL here
vrf definition PreConfigTest
  vpn id 12:566
  rd 23.23.23.23:2
  address-family ipv4
    route-target import 32:1
    route-target export 32:1
interface GigabitEthernet0/10
  service instance 3 ethernet
  encapsulation dot1q 521
  rewrite ingress tag pop 1 symmetric
  bridge-domain 8
exit
interface Vlan8
  no shutdown
  mtu 1522
  vrf forwarding PreConfigTest
  ip address 33.44.24.55 255.255.255.0
router bgp 100
  address-family ipv4 vrf PreConfigTest
  exit
```

設定例 2: パラメータのない設定後 CLI のロールバック：

CLI の例：

```
snmp-server enable traps
vrf definition PreConfigTest
  vpn id 12:566
  rd 23.23.23.23:3
  address-family ipv4
    route-target import 24:1
    route-target export 24:1
interface GigabitEthernet0/10
  service instance 4 ethernet
  encapsulation dot1q 685
  rewrite ingress tag pop 1 symmetric
  bridge-domain 9
exit
interface Vlan9
  no shutdown
  mtu 1522
  vrf forwarding PostConfigTest
  ip address 23.44.55.56 255.255.255.0
router bgp 100
  address-family ipv4 vrf PostConfigTest
  exit
exit
snmp-server enable traps
FAIL here
```

設定例 3： 設定前有効テンプレート、設定後無効テンプレート、展開失敗、およびロールバック CLI

CLI の例：

```
snmp-server enable traps
vrf definition PrePostConfig
  vpn id 34:55
  rd 23.23.23.23:4
  address-family ipv4
    route-target import 234:1
    route-target export 234:1
```

```

interface GigabitEthernet0/10
 service instance 5 ethernet
  encapsulation dot1q 664
  rewrite ingress tag pop 1 symmetric
  bridge-domain 11
 exit
interface Vlan11
 no shutdown
 mtu 1522
 vrf forwarding PrePostConfig
 ip address 44.55.22.55 255.255.255.0
 router bgp 100
 address-family ipv4 vrf PrePostConfig
  exit
 exit
 snmp-server enable traps
 FAIL here

```

設定例：インタラクティブテンプレート

設定例 1：単一のプロンプトを含むコマンドのインタラクティブテンプレート：

テンプレートの形式：

```

#INTERACTIVE
no username test<IQ>confirm<R>y
#ENDS_INTERACTIVE

```

CLI の例（サービス前設定として設定されたテンプレート）：

```

no username test
bridge-domain 8
ethernet cfm domain EVC level 4
  service b_evplan_4Mar evc b_evplan_4Mar vlan 8
  continuity-check
  continuity-check interval 1s
ethernet evc b_evplan_4Mar
  oam protocol cfm domain EVC
interface GigabitEthernet0/0/1
  ethernet uni id UniName3
  service instance 2 ethernet b_evplan_4Mar
  encapsulation dot1q 22
  bridge-domain 8
  cfm mep domain EVC mpid 1
  ethernet lmi ce-vlan map 22
  snmp trap link-status
  exit
exit

```

設定例 2：複数のプロンプトを含むコマンドのインタラクティブテンプレート：

テンプレートの形式：

```

#INTERACTIVE
crypto key generate rsa<IQ>% Do you really want to replace them? [yes/no]:<EM><R>yes<IQ>How
many bits in the modulus [512]:<EM><R>512
#ENDS_INTERACTIVE

```

CLI の例（サービス後設定として設定されたテンプレート）：

```

bridge-domain 8
ethernet cfm domain EVC level 4
  service b_evplan_4Mar evc b_evplan_4Mar vlan 8

```

```
continuity-check
continuity-check interval 1s
ethernet evc b_evplan_4Mar
oam protocol cfm domain EVC
interface GigabitEthernet0/0/0
ethernet uni id UniName4
ethernet lmi interface
service instance 1 ethernet b_evplan_4Mar
encapsulation dot1q 345
bridge-domain 8
cfm mep domain EVC mpid 1
ethernet lmi ce-vlan map 345
snmp trap link-status
exit
exit
crypto key generate rsa
```

プロビジョニング障害の syslog

サービスプロビジョニングの障害が発生すると、EPNMはsyslogを生成し、EPNMで設定された受信者に送信します。このsyslogは、作成、変更、削除、および昇格操作のために生成されます。

受信者は、EPNMサーバにログインすることによってCLIで設定できます。[CLI経由の接続](#)を参照してください。**conf**モードで**logging security <syslog receiver ip>**を実行します。

syslogの視覚的な表現は、受信側のマシン/サーバで使用されているソフトウェアによって異なります。

