



# デバイスの設定

---

この章では、次のトピックについて説明します。

- [Cisco Evolved Programmable Network Manager](#) を使用してデバイスを設定する方法, [on page 2](#)
- どのデバイスが設定操作をサポートしているか。 (3 ページ)
- CLI 設定テンプレートで使用されているコマンドの特定, [on page 3](#)
- デバイスのクレデンシャルとプロトコル設定の変更 (3 ページ)
- 基本的なデバイス プロパティの変更, [on page 4](#)
- インターフェ이스の有効化と無効化 (6 ページ)
- デバイス インターフェ이스の物理属性の設定 (6 ページ)
- 回線エミュレーションの設定 (12 ページ)
- Sync-E、BITS、および PTP を使用したクロックの同期 (36 ページ)
- IP SLA の設定 (TWAMP レスポンダ/TWAMP ライトレスポンダ) (45 ページ)
- インターフェ이스の設定 (48 ページ)
- シャーシビューを使用したデバイスの設定 (84 ページ)
- 光カードの設定 (101 ページ)
- MPLS LDP および MPLS-TE リンクの検出と設定 (119 ページ)
- SPAN と RSPAN を使用したポートの分析 (123 ページ)
- イーサネット Link Aggregation Group の設定と表示 (126 ページ)
- ルーティング プロトコルとセキュリティの設定 (129 ページ)
- セグメントルーティングの設定 (140 ページ)
- EOAM の障害とパフォーマンスのモニターリングを設定する, [on page 151](#)
- Quality of Service (QoS) の設定, [on page 159](#)
- デバイスの変更内容の保存 (175 ページ)
- Cisco NCS および Cisco ONS デバイスを管理するための Cisco Transport Controller の起動, [on page 177](#)

# Cisco Evolved Programmable Network Manager を使用してデバイスを設定する方法

Cisco EPN Manager には、ネットワークの物理デバイスを変更する方法として次の2つが用意されています。実行できるアクションは、ユーザーアカウント権限とネットワーク内のデバイスのタイプによって異なります。

デバイスを設定するための出発点	この方法の使用目的：
左側のナビゲーションメニューの [設定 (Configuration)] メニュー	デバイス名をクリックし、[設定 (Configuration)] タブをクリックします。選択したデバイスでデバイス機能を設定できます。また、デバイスに展開された適用済みおよびスケジュール済みの機能テンプレートのリストを表示できます。
設定テンプレートの作成と展開	システムテンプレートを使用して1つ以上のデバイスに対して一般的なネットワーク管理タスクを実行します。たとえば、ホスト名の追加やルーティングプロトコルの設定などです。導入のニーズに合わせて独自のテンプレートを作成することもできます。これらは複数のデバイスに適用できるため、通常、テンプレートは特定のデバイス オペレーティング システムやデバイス タイプに適用されます。構成テンプレートを使用すると、Cisco EPN Manager は、テンプレート基準を満たすデバイスのみを表示します。



**Note** また、デバイスを選択し、[編集 (Edit)] をクリックして、[ネットワーク デバイス (Network Devices)] 表 ([設定 (Configuration)] > [ネットワーク (Network)] > [ネットワーク デバイス (Network Devices)]) からデバイスのプロパティを編集することもできます。これにより、デバイスの編集ウィザードが起動されます。ただし、ウィザードを使用して行う変更は、デバイス クレデンシャルに限定されており、行った変更は物理デバイスに影響しません。データベースに保存されているデバイス情報を更新するのみです。

光デバイスの場合は、Cisco EPN Manager から起動できる Cisco Transport Controller を使用してデバイスを設定することもできます。[Cisco NCS および Cisco ONS デバイスを管理するための Cisco Transport Controller の起動, on page 177](#)を参照してください

変更を行った後、データベースに変更を保存し、必要に応じてデバイスの物理および論理インベントリを収集します。詳細については、[デバイスのインベントリの即時収集 \(同期\), on page 175](#)を参照してください。

## どのデバイスが設定操作をサポートしているか。

次の場合、デバイスで設定操作がサポートされています。

- Cisco EPN Manager では、デバイス モデルがサポートされています。
- Cisco EPN Manager では、デバイスのオペレーティングシステムがサポートされています。
- Cisco EPN Manager では適用可能なテクノロジーまたはサービスがサポートされており、それらはデバイスで有効になっています。

何がサポートされているかについては、[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。

## CLI 設定テンプレートで使用されているコマンドの特定

この手順を使用して、[CLI テンプレート (CLI Templates)] ドロワから起動するコマンドで使用されるコマンドそのものを表示します。

**ステップ 1** [設定 (Configuration)] > [テンプレート (Templates)] > [機能およびテクノロジー (Features and Technologies)] を選択し、[CLI テンプレート (CLI Templates)] を選択します。次に例を示します。

- 設定済みのテンプレートは、[システム テンプレート (System Template)] の [CLI] の下にあります。
- カスタマイズされたテンプレートは、[マイ テンプレート (My Templates)] の下にあります。

**ステップ 2** 左側のサイドバーにある [テンプレート (Templates)] メニューのテンプレートをダブルクリックします。

**ステップ 3** [テンプレートの詳細 (Template Detail)] 領域で、[CLI コンテンツ (CLI Content)] タブを選択します。コマンドがそのタブに表示されます。

## デバイスのクレデンシャルとプロトコル設定の変更

デバイスのクレデンシャルとプロトコル設定を更新するには、次の手順に従います。設定をデータベースに保存するときにインベントリの収集を実行し、毎日インベントリの収集を待機するのではなく、すべての物理デバイスと論理デバイスの変更を収集して、それらの変更をデータベースに保存することもできます。

**ステップ 1** [インベントリ (Inventory)] > [ネットワーク デバイス (Network Devices)] を選択します。

**ステップ 2** 編集するデバイスを選択して、[編集 (Edit)] をクリックします。複数のデバイスを選択して、一括で変更することもできます。

**ステップ3** 変更するパラメータをダブルクリックします。デバイス タイプに応じて、次を編集できます。

- デバイスで使用されているクレデンシャル プロファイル
- デバイスが属するグループ
- SNMP ポート、再試行、タイムアウト、クレデンシャル、および SNMPv3 認証情報
- Telnet/SSH2 のクレデンシャルとタイムアウト
- HTTP/HTTPS のクレデンシャル、ポート、タイムアウト
- TL1 のクレデンシャルとプロキシ IP アドレス (GNE/ENE の場合)
- シビック ロケーション (Civic Location)

**ステップ4** [クレデンシャルの確認 (Verify Credentials)] をクリックして、新しいクレデンシャルが物理デバイス上のクレデンシャルと同じであることを確認します。

**ステップ5** 次のように変更を保存します。

- [更新 (Update)] は、変更をデータベースに保存します。
- [更新して同期 (Update and Sync)] は、変更をデータベースに保存し、デバイスの物理インベントリと論理インベントリも収集して、すべての変更をデータベースに保存します。

---

## 基本的なデバイス プロパティの変更

Cisco EPN Manager は、物理デバイスで基本的なプロパティを変更するために使用できるコマンドテンプレートを提供します。これらのテンプレートを使用するには、[設定 (Configuration)] > [テンプレート (Templates)] > [機能およびテクノロジー (Features & Technologies)] の順に選択し、左側の [テンプレート (Templates)] ペインから [CLI テンプレート (CLI Templates)] > [システム テンプレート - CLI (System Templates - CLI)] を選択します。



**Note** ここで実行する操作は、[編集 (Edit)] ウィザード (ネットワーク デバイス テーブルから起動できる) で実行する操作とは異なります。[編集 (Edit)] ウィザードでは、データベースに保存されたデバイス情報のプロパティを変更します。この操作では、物理デバイスのプロパティは変更されません。

---

CLI 設定テンプレート名	次の場合に使用します。	必要な入力値	
Add-Host-Name-IOS および -IOS-XR	クライアントホスト名を設定します	ホスト名	
Remove-Host-Name-IOS および -IOS-XR			
Syslog-Host-Logging-IOS および -IOS-XR	特定のレベルのメッセージを記録するホストを指定します	ホスト名	
Add-Tacacs-Server-IOS および -IOS-XR	認証に使用する TACACS または TACACS+ サーバーを設定します	ホストアドレス、キー値、認証リスト名、グループ名	
Remove-Tacacs-Server-IOS およ び -IOS-XR			
Add-Tacacs-Plus-Server-IOS およ び -IOS-XR			
Remove-Tacacs-Plus-Server-IOS および -IOS-XR			
Add-SNMP-Configuration-IOS お よび -IOS-XR	SNMP バージョン、パスワード、パスワードの暗号化、サーバーおよびグループ設定、UDP ポートなどを設定します	ホスト名、コミュニティ名、システム所有者	
Remove-SNMP-Configuration-IOS および -IOS-XR			
Enable-Traps-ASR903	Cisco ASR 903 でトラップの有効/無効を切り替えます	トラップ名 (リストが提供されます)	
Disable-Traps-ASR903			
Enable-Traps-IOS および -IOS-XR	Cisco IOS および Cisco IOS XR のデバイスでトラップの有効/無効を切り替えます		
Disable-Traps-IOS および -IOS-XR			
Enable-Traps-ME3600 および -ME3800	Cisco ME3600 および ME3800 でトラップの有効/無効を切り替えます		
Disable-Traps-ME3600 および -ME3800			
Enable-Trap-Host-IOS および IOS-XR	SNMP トラップのターゲットホストを設定します		ホスト IP アドレス、コミュニティストリング
Show-Users-on-Device-IOS およ び -IOS-XR	Cisco IOS および Cisco IOS XR のデバイスのユーザーセッション情報を表示します		(選択したデバイスから実行されます。必要な入力はありません)

## インターフェイスの有効化と無効化

インターフェイス 360 ビューを使用して、インターフェイスをすばやく有効または無効にします。[デバイスの詳細 (Device Details)] ページからこれらと同じアクションを実行できますが、インターフェイス 360 ビューを使用するほうがより効率的な場合があります (アラームに反応する場合など)。インターフェイス 360 ビューの右上には、有効化と無効化のオプションが表示された [アクション (Actions)] メニューがあります。

インターフェイス 360 ビューを起動するには、[デバイス インターフェイスの概要](#) : [インターフェイス 360 (Interface 360)] ビューを参照してください。

デバイスの [デバイスの詳細 (Device Details)] ページからインターフェイスを有効または無効にするには、インターフェイスの設定のトピック (イーサネット、ループバック、シリアル、トンネルなど) を参照してください。

## デバイス インターフェイスの物理属性の設定

Cisco EPN Manager を使用すると、デバイスのインターフェイスの物理属性を設定できます。カードの操作モード、スロットごとの帯域幅割り当て、スロット接続可能タイプ (VCoP など) の属性と AINS 設定は設定可能です。

インターフェイスの物理属性を設定するには、次の手順を実行します。

- 
- ステップ 1 [設定 (Configuration)] > [ネットワーク デバイス (Network Devices)] を選択します。
  - ステップ 2 デバイス名のハイパーリンクをクリックして、設定するデバイスを選択します。
  - ステップ 3 [論理ビュー (Logical View)] タブをクリックします。
  - ステップ 4 インターフェイスを設定するには、次の表に示すパスに移動します。
  - ステップ 5 変更を加えるには、コントローラ/カード名のハイパーリンクをクリックし、ページの右上隅にある [編集 (Edit)] アイコンをクリックします。変更を加えて、[保存 (Save)] をクリックします。

表 1: インターフェイスの物理属性の設定

物理インターフェイスの設定	ナビゲーション	コメント/説明	サポートされるスロット/コントローラ
5G または 10G としてカードタイプの設定。	【物理 (Physical) ]> [カードモード (Card Mode) ]	<p>設定を 10G から 5G に変更することはできますが、5G から 10G への変更はサポートされていません。選択したデバイスによって、デフォルトのカードモードは 5G または 10G に設定されます。サポートされるカードモードの詳細については、<a href="#">Cisco EPN Manager でサポートされるデバイス</a>を参照してください。</p> <p>(注) アクティブ回線の一部となっているスロットでカードモードを設定することはできません。</p>	<p>デバイスのスロットとサポートされているカードモードのタイプの詳細については、次の表（「デバイスのスロットとサポートされるカードモードのタイプ」）を参照してください。</p>
T1 または E1 としてのカードモードの設定。	【物理 (Physical) ]> [カードモード (Card Mode) ]	<p>選択するデバイスとカードに応じて、設定を T1 から E1 に変更することも、その逆に変更することもできます。</p> <p>T1 モードと E1 モードは、カードで使用されるチャネルモードのタイプを表します。</p> <p>(注) アクティブ回線の一部となっているスロットでカードモードを設定することはできません。</p>	-
OC3 または OC12 としてのカードモードの設定。	【物理 (Physical) ]> [カードモード (Card Mode) ]	<p>(Cisco ASR 903 ルータの) A900-IMA4OS カードのカードモードを OC3 または OC12 として設定できます。</p> <p>OC3 モードと OC12 モードは、異なる光伝送回線のデータ伝送速度を表します。</p>	-

物理インターフェイスの設定	ナビゲーション	コメント/説明	サポートされるスロット/コントローラ
カード保護の設定	[物理 (Physical) ]> [カード保護 (Card Protection) ]	<p>カードをプライマリ メンバーまたはバックアップメンバー (インターフェイス) として機能するように設定します。プライマリ インターフェイスとそのバックアップ インターフェイスは、保護グループを構成します (一意の整数で示されます)。カードをバックアップメンバーに関連付けると、プライマリ インターフェイスに障害が発生した場合、保護インターフェイスはプライマリ インターフェイスからのトラフィック負荷を迅速に想定できるようになります。アクティブメンバーとして表示されるカードは、サービスの保護メンバーとして機能するカードです。</p> <p>プライマリ メンバーとバックアップメンバーが同じタイプであることを確認します。たとえば、プライマリ メンバーとして T1 インターフェイスを選択した場合、バックアップメンバーも T1 インターフェイスである必要があります。</p> <p>ホールドオフタイマーは、1+1 カードプロテクション (IOS XE バージョン 16.10.1 以降を搭載した NCS42XX デバイス) で使用できます。これは、ネットワークの不整合が発生した場合に連続してスイッチングが行われないようにするために使用されます。有効な範囲は 0 ~ 10 秒です。デフォルト値は 5 です。</p> <p>保護グループの管理モードは、[ロックアウト (Lockout) ]&gt; [強制切り替え (Force Switch) ]&gt; [手動スイッチ (Manual Switch) ]&gt; [なし (None) ] の順序で設定されます。これらのモードと元に戻すタイマーの詳細については、<a href="#">APS または MSP および UPSR または SNCP 保護グループの設定 (20 ページ)</a> の説明を参照してください。</p>	-
NCS42xx デバイス上に NCS4200-1T16G-PS カードを設定します。	[物理 (Physical) ]> [カード モード (Card Mode) ]	<p>スロット番号に関係なく、NCS4200-1T16G-PS カードのすべてのカード モードを表示できます。</p> <p>(注) NCS42xx デバイスの一部のスロットで NCS4200-1T16G-PS カードを設定すると、それらのスロットの設定はデフォルト値にリセットされます。</p>	-



物理インターフェイスの設定	ナビゲーション	コメント/説明	サポートされるスロット/コントローラ
ASR9xx デバイス上で A900-IMA8CT1Z-M カードと A900-IMA8CS1Z-M カードを設定します。	[物理 (Physical) ]> [カードモード (Card Mode) ]	A900-IMA8CT1Z-M カードと A900-IMA8CS1Z-M カードのカードモードを表示および設定できます。	-

物理インターフェイスの設定	ナビゲーション	コメント/説明	サポートされるスロット/コントローラ
<p>自動インサースervice (AINS) のインターフェイスモジュールのタイプを設定します。</p>	<p>[物理 (Physical) ] &gt; [自動インサースervice (AINS) (Automatic In-Service (AINS))]</p>	<p>[カード (Cards) ] タブを使用して、AINS に適切なコントローラタイプを設定します。カードを手動で挿入および取り出す場合、AINS 値は 20 分遅れて取り込まれます。</p> <p>[ポート/コントローラ (Ports/Controllers) ] タブには、AINS 対応のすべてのポートとコントローラのリストが表示されます。サポートされているポートとコントローラは、Ethernet、E1、E3、T1、T3、および SONET と SDH です。[編集 (Edit) ] アイコンを使用して、[セカンダリ管理状態 (Secondary Admin State) ] の値と [Soak タイマー (Soak Timer) ] の値 (時間単位または分単位) を設定できます。</p> <p>注：ポートまたはコントローラでの AINS の有効化は、デバイス上で手動で実行する操作です。</p> <p>次に、設定可能な [セカンダリ管理状態 (Secondary Admin State) ] の値を示します。</p> <ul style="list-style-type: none"> <li>• [IS_AINS] : デバイスが [自動インサースervice (Automatic In-Service) ] 状態であることを示します。</li> <li>• [IS] : デバイスが [インサースervice (In-Service) ] 状態であることを示します。</li> <li>• [OOS_MT] : デバイスが [インメンテナンス (In-Maintenance) ] 状態であることを示します。</li> </ul> <p>Soak タイマーを時間単位で設定するには、[Soak タイマー (時間) (Soak Timer Hours) ] フィールドを使用します。有効な範囲は 0 ~ 48 時間です。Soak タイマーを分単位で設定するには、[Soak タイマー (分) (Soak Timer Minutes) ] ドロップダウンリストを使用します。使用可能な値は、15 分、30 分、および 45 分です。デフォルト値は 15 分です。</p>	<p>-</p>

物理インターフェイスの設定	ナビゲーション	コメント/説明	サポートされるスロット/コントローラ
選択したデバイススロット用に予約する必要がある帯域幅を設定します。	[物理 (Physical) ]> [帯域幅 (Bandwidth) ]	指定した帯域幅は、選択したスロット用に予約され、スロットが動作しているかどうかにかかわらず、スロットで使用できるようになります。選択したスロット/カードがダウンし、しばらくしてからオンラインに戻った場合は、このフィールドで指定された値に基づいて設定された帯域幅が使用できるようになります。	NCS4200-1T16G-PS カードでは、事前設定された帯域幅値 80 Gbps または 100 Gbps を NCS4216 デバイスで予約できます。
Virtual Container over Packet (VCoP) のインターフェイスプラグブルタイプを設定します。	[物理 (Physical) ]> [接続可能 (Pluggable) ]	このメニューを使用して、VCoP 対応インターフェイスに適切なポートタイプを選択します。たとえば、ポートタイプは OC3、OC12、DS3 のいずれかに設定できます。  (注) VCoP スマート SFP は、パケットネットワーク全体で透過的に SONET 信号を転送する機能を提供します。VCoP スマート SFP は特殊なタイプの光トランシーバであり、STS1、STS-3c、または STS-12c レベルで SONET ビットストリームをパケット形式にカプセル化します。	-

条件と制限事項：次に、Cisco ASR 920、Cisco NCS4202、および Cisco NCS 4206 のデバイスでサポートされている Cisco ASR 900 シリーズルートスイッチプロセッサ 2 (RSP2A) モジュール (A900-RSP2A-128) でコントローラ モードを設定するための条件と制限を示します。

- 設定できる最大帯域幅は OC-48 です。モジュール上には最大 20 個のポートを設定できます。
  - ポート 0 ~ 11 は T1 ポートです。
  - ポート 12 ~ 15 は T3/E3 ポートです。
  - ポート 16 ~ 19 は OC3/OC12 ポートです。
- (注) 特定のポートが OC48 として設定されている場合、設定可能な最大帯域幅が OC48 であるため、設定できるのはそれらの特定のポートの 1 つのみです。
- Cisco A900-RSP2A-128 モジュールの設定制限：
  - SDH/E3/E1/DS0 コントローラ モードは設定できません。
  - イーサネットはコントローラ モードとして設定できません。
  - 保護タイプ UPSR は設定できません。
  - コントローラ モード設定をデバイスに展開すると、Cisco EPN Manager を使用して設定を元に戻すことはできません。

表 2: デバイスのスロットとサポートされるカードモードのタイプ

Cisco NCS 4206 デバイス	Cisco NCS 4216 デバイス	Cisco ASR903 デバイス	Cisco ASR907 デバイス
<ul style="list-style-type: none"> <li>スロット 0、1 : 非サポート</li> <li>スロット 2、3、4、5 : デフォルト モード 10G</li> </ul>	<ul style="list-style-type: none"> <li>スロット 0、1 : 非サポート</li> <li>スロット 3、4、7、8、11、12 : デフォルト モード 10G</li> <li>スロット 2、5、6、9、10、13、14、15 : デフォルト モード 5G</li> </ul>	<ul style="list-style-type: none"> <li>スロット 0、1 : 非サポート</li> <li>スロット 2、3、4、5 : デフォルト モード 10G</li> </ul>	<ul style="list-style-type: none"> <li>スロット 0、1 : 非サポート</li> <li>スロット 3、4、7、8、11、12 : デフォルト モード 10G</li> <li>スロット 2、5、6、9、10、13、14、15 : デフォルト モード 5G</li> </ul>

表 3: コントローラ モードおよびサポートされるポートタイプ

SONET (0 ~ 3)	SONET (4 ~ 7)
<ul style="list-style-type: none"> <li>最大 2.5G</li> <li>OC48/OC12/OC3 をサポートできますが、合計 2.5G に制限されます。</li> <li>たとえば、ポート 0 に OC48 が設定されている場合、ポート 1/2/3 は使用できません。</li> </ul>	<ul style="list-style-type: none"> <li>最大 2.5G</li> <li>ポート グループに OC12/OC3/1G が設定されている場合、OC48 は許可されません。</li> </ul>

## 回線エミュレーションの設定

Cisco EPN Manager 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) 間にブリッジを提供する回線エミュレーション (CEM) のプロビジョニングをサポートします。CEM は、パケットスイッチドネットワーク上で TDM (または PDH) 回線を伝送する方法です。回線エミュレーション (CEM) は物理接続の模倣です。この機能によって、既存の IP ネットワークを使用して専用回線エミュレーションサービスを提供できるようになります。また、他のマルチサービスプラットフォームインターフェイスの形式の要件を満たさないデータストリームやプロトコルを伝送できるようになります。

Cisco EPN Manager は次の CEM モードをサポートしています。

- Structure-Agnostic time-division multiplexing (TDM) over Packet (SAToP) : これは、着信 TDM データが任意のビットストリームと見なされる非構造化モードです。ビットストリームに適用される可能性がある構造は無視されます。SAToP では、TDM ビットストリームが PSN 経由の疑似回線 (PW) としてカプセル化されます。

- **Circuit Emulation over Packet (CEP)** : このモードは、MPLS プロバイダを介して同期光ネットワーク/同期デジタル階層 (SONET/SDH) 回線とサービスをエミュレートするために使用されます。パケット指向ネットワークで SONET/SDH 回線を伝送するために、同期ペイロードエンベロープ (SPE) またはバーチャルトリビュタリ (VT) はフラグメントに分割されます。CEP ヘッダーと必要に応じて RTP ヘッダーが各フラグメントの前に付加されます。

Cisco EPN Manager での CEP の詳細については、[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。

回線がチャンネル化される場合、回線は論理的に、高順位のパス (HOP) と低順位のパス (LOP) と呼ばれる小さい帯域幅チャンネルに分割されます。これらのパスが SONET ペイロードを伝送します。回線がチャンネル化されない場合、回線の全帯域幅がブロードバンドサービスを伝送する単一のチャンネル専用となります。Cisco EPN Manager では、T3 または E3 チャンネルを T1 にチャンネル化し、T1 をさらに DS0 タイム スロットにチャンネル化できます。Cisco EPN Manager を使用して CEM サービスをプロビジョニングする前に、まず、CEM インターフェイスを設定して、HOP および LOP のパラメータを設定する必要があります。

チャンネル化された SONET インターフェイスは、複数の STS ストリームを複合したものであり、固有のペイロードポインタを持つ独立したフレームとして維持されます。フレームは、転送される前に多重化されます。SONET では同期転送信号 (STS) フレーミングが使用され、SDH では同期トランスポートモード (STM) フレーミングが使用されます。STS はオプティカルキャリア 1 (OC-1) の電氣的等価であり、STM-1 は 3 オプティカルキャリア 1 (OC-1) の電氣的等価です。

ここでは、Cisco EPN Manager を使用して最初に CEM のインターフェイスを設定する方法について説明します。次に、適切なコントローラモードと保護グループが設定されたこれらのインターフェイスを使用して、CEM サービスをプロビジョニングすることができます。

## CEM サービスを設定するための前提条件

CEM サービスのプロビジョニング ([回線エミュレーションサービスのプロビジョニング](#)を参照) 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。

- デバイスの CEM に必要なループバックを設定します。[ループバック インターフェイスの設定 \(51 ページ\)](#) を参照してください。
- SONET、SDH、PDH、HOP、および HOP コントローラに必要な CEM パラメータを設定します。[CEM のインターフェイスの設定 \(15 ページ\)](#) を参照してください。
- APS 保護を提供するように、現用インターフェイス グループとバックアップ用インターフェイス グループを構成します。[APS または MSP および UPSR または SNCP 保護グループの設定 \(20 ページ\)](#) を参照してください。

## SONET モードの設定例

次に、STS-1 モードを設定する設定コマンドと例を示します。

### STS-1 モードの設定

STS-1 モードを設定するには、次のコマンドを使用します。

```
enable
configure terminal
controller sonet 0/5/0
sts-1 1
mode vt-15
end
```



- (注) デフォルトのモードはありません。modes vt-15、mode ct3、mode t3、mode unframed、mode vt-2 がサポートされています。システムをデフォルトの状態に戻すには、このコマンドの **no** 形式を使用します。

### STS-1 の DS1/T1 CT3 モードの設定 :

STS-1 の DS1/T1 CT3 モードを設定するには、次の手順を使用して T1 リンクを設定します。

```
enable
configure terminal
controller sonet 0/5/0
sts-1 1
mode ct3
t1 1 clock source internal
t1 1 framing unframed
end
```



- (注) システムをデフォルトの状態に戻すには、このコマンドの **no** 形式を使用します。

### STS-Nc の設定 : 連続連結

STS-Nc の連続連結を設定するには、次のコマンドを使用します。

```
enable
configure terminal
controller sonet 0/5/0
sts-1 1-3 mode sts-3c
end
```



- (注) システムをデフォルトの状態に戻すには、このコマンドの **no** 形式を使用します。また、STS-3c または STS-12c を設定するには、それぞれ 3 または 12 の倍数の数値を使用します。

#### CESoPSNでの SONET モード VT1.5-T1 のCEMグループの設定

CESoPSN の STS-1 の VT 1.5 モードで CEM グループを設定するには、次のコマンドを使用します。

```
enable
configure terminal
controller sonet 0/5/0
sts-1 2
mode vt-15
vtg 1 t1 1 cem-group 56 timeslots 1 - 8
end
```

#### CESoPSN における SONET モード CT3-T1 の CEM グループの設定

CESoPSN の STS-1 の CT3 モードで CEM グループを設定するには、次のコマンドを使用します。

```
enable
configure terminal
controller sonet 0/5/0
sts-1 1
mode ct3
t1 3 cem-group 28 timeslots 1 - 7
end
```

## CEM のインターフェイスの設定

Cisco EPN Manager を使用して、回線エミュレーション (CEM) にインターフェイスを設定できます。これを行うには、適切なコントローラ モードをインターフェイスに設定してから、CEM の PDH (E1、T1、E3、T3)、SONET、および SDH コントローラを設定します。CEM で設定したインターフェイスは、CEM サービスをプロビジョニングする際に使用できます。[回線エミュレーションサービスのプロビジョニング](#)を参照してください。

CEM のインターフェイスを設定するには、次の手順に従います。

- ステップ 1** [設定 (Configuration)] > [ネットワーク デバイス (Network Devices)] を選択します。
- ステップ 2** デバイス名のハイパーリンクをクリックして、設定するデバイスを選択します。
- ステップ 3** [論理ビュー (Logical View)] タブをクリックします。
- ステップ 4** CEM のパラメータを設定するには、次の表で説明する設定オプションに移動します。
- ステップ 5** 変更を加えるには、コントローラ/カード名のハイパーリンクをクリックし、ページの右上隅にある [編集 (Edit)] アイコンをクリックします。変更を加えて、[保存 (Save)] をクリックします。

例

表 4: CEM インターフェイスの設定オプション

CEM インターフェイスの設定	ナビゲーション	コメント/説明	サポートされるスロット/コントローラ
SONET、SDH、イーサネット、T3、あるいは E1、E3、または STS1E としてコントローラモードを設定します。	[回線エミュレーション (Circuit Emulation)] > [コントローラモード (Controller Mode)]	選択のために表示されるコントローラモードオプションは、選択したメディアタイプに基づいています。詳細については、「コントローラモードおよびサポートされるポートタイプ」を参照してください。	-
PDH (E1、T1、E3 および T3) コントローラを設定します。	[回線エミュレーション (Circuit Emulation)] > [PDH]	各種の PDH パラメータについては、次を参照してください。 CEM インターフェイス (PDH、SONET、および SDH) のフィールドの説明 (25 ページ)	-



CEM インターフェイスの設定	ナビゲーション	コメント/説明	サポートされるスロット/コントローラ
CEM の SONET および SDH コントローラを設定します。	[回線エミュレーション (Circuit Emulation)] > [SONET および SDH (SONET and SDH)]	各種の SONET および SDH パラメータについては、次を参照してください。 CEM インターフェイス (PDH、SONET、および SDH) のフィールドの説明 (25 ページ)	デバイスのポートとサポートされているコントローラのタイプの詳細については、次の表 (「コントローラモードおよびサポートされるポートタイプ」) を参照してください。
CEM プロビジョニングの現用メンバーインターフェイスと保護メンバーインターフェイスを設定します。	[回線エミュレーション (Circuit Emulation)] > [保護グループ (Protection Group)]	APS または MSP および UPSR または SNCP 保護グループの設定 (20 ページ) を参照してください	-

コントローラ モードおよびサポートされるポート タイプ

- EOWYNIM にはペアワイズ制限があります。有効なペアは (0,1) (2,3) (4,5) (6,7) です。



**注** ペアごとに最大 2.5Gbps (OC48) の帯域幅 (両方のポートを組み合わせる) を設定できます。

- レート OC3/OC12/OC48 はポート 0 ~ 7 についてのみ設定でき、ポート 8 では OC192 レートのみを設定できます。

表 5:異なるレート  $OCN \rightarrow n * 51.84 \text{ Mbit/s}$  で使用される帯域幅

レート設定	帯域幅
OC1	51.84 Mb/s
OC3	155.52 Mb/s
OC12	622.08 Mb/s
OC48	2488.32 Mb/s $\sim$ = 2.5 Gb/s
OC192	9953.28 Mb/s $\sim$ = 10 Gb/s

### MediaType コントローラの設定

MediaType コントローラを設定するには、次のコマンドを使用します。

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
end
```

### SONET ポートの設定

SONET ポートを設定するには、次のコマンドを使用します。

```
enable
configure terminal
controller MediaType 0/5/0
mode sonet
controller sonet 0/5/0
rate OC12
end
```

上記の例には、OC-12 モードで SONET ポートを設定する方法が示されています。

### STS1E ポートの設定

STS1E ポートを設定するには、次のコマンドを使用します。

```
NCS4200-120.33#sh run | sec 0/4/0
controller MediaType 0/4/0
mode sts1e
controller STS1E 0/4/0
no snmp trap link-status
no ais-shut
alarm-report all
secondary-admin-state auto-in-service
clock source internal
cablelength short
overhead j0 tx length 64-byte
overhead j0 expected length 64-byte
!
sts-1 1
```

### CEM インターフェイスの設定例 :

- 次の例は、CEM フレーミングのタイプが「unframed」、モードが「c-11」、クロックソースのタイプが「internet」、保護グループに関連付けられた ACR 値が「acr

255」に設定されたデバイスに挿入する CEM インターフェイス設定を示しています。

```
NCS4206-120.32#show running-config | section 0/4/0
controller MediaType 0/4/0
  mode sonet
controller SONET 0/4/0
  rate OC3
  no ais-shut
  framing sonet
  clock source line
  loopback network
  !
sts-1 1
  clock source internal
  mode unframed
  cem-group 1 cep
  !
sts-1 2
  clock source internal
  loopback network
  mode unframed
  cem-group 2 cep
  !
sts-1 3
  clock source internal
  mode vt-15
  vtg 1 vt 1 protection-group 15 working
  vtg 1 vt 3 protection-group 16 working
  vtg 1 vt 4 protection-group 17 working
  !
aps group acr 255
aps protect 1 6.6.6.6 / aps working 1
!
interface CEM0/4/0
  no ip address
  cem 1
  !
  cem 2
  !
connect sam CEM0/4/0 1 CEM0/4/0 2
!
NCS4206-120.32#
```

- 次に、STS1E を使用した CEM インターフェイスの設定例を示します。

```
controller STS1E 0/4/1
  sts-1 1
    mode vt-15
    vtg 1 t1 1 cem-group 0 cep
interface CEM0/4/1
  no ip address
  cem 0
  !
```

```
controller STS1E 0/4/0
  sts-1 1
    clock source internal
    mode unframed
    cem-group 0 cep
```

```
interface CEM0/4/0
  no ip address
  cem 0
  !
```

## APS または MSP および UPSR または SNCP 保護グループの設定

CEMの保護グループを表示すると、デバイスに対して有効な自動保護スイッチング（APS）、単方向パススイッチングリング（UPSR）、多重サービス保護（MSP）、サブネットワーク接続保護（SNCP）インターフェイスを理解するのに役立ちます。APSとUPSRは、SONETネットワーク内の保護インターフェイスを動作中インターフェイスのバックアップとして使用するメカニズムです。インターフェイスをAPSまたはUPSRの保護グループに関連付けると、動作中インターフェイスで障害が発生した場合に、保護インターフェイスにそのトラフィック負荷が迅速に引き継がれます。現用インターフェイスとその保護インターフェイスが保護グループを構成します。SONET保護グループは、SONET回線層でファイバ（外部）障害または機器（インターフェイスおよび内部）障害からの回復機能を提供します。Cisco EPN Managerを使用すると、CEM回線のメイン動作コントローラとして機能するSONETコントローラの現用メンバーを表示できます。保護メンバーは、メインの現用コントローラのバックアップとして機能します。これらの詳細を表示するには、[CEMのインターフェイスの設定（15ページ）](#)の説明に従ってインターフェイスが必要なコントローラモードに設定されていることを確認してください。

MSPとSNCPとは、SDHネットワーク内の保護インターフェイスを動作中インターフェイスのバックアップとして使用するメカニズムです。インターフェイスをMSPまたはSNCPの保護グループに関連付けると、動作中インターフェイスで障害が発生した場合に、そのトラフィック負荷が保護インターフェイスに迅速に引き継がれます。動作中インターフェイスとそれらの保護インターフェイスとで保護グループを構成します。

MSPは、1+1保護メカニズムを提供するポートレベル保護のためのSDHの保護メカニズムです。ネットワークトポロジマップでは、復帰モード、単方向モード、双方向モード、およびacr/dcrモードなど、すべてのモードがサポートされています。SDHのMSPはSONETのAPSに似ています。たとえば、NCS4206デバイスには動作モードと保護モードの両方があります。

SDH-MSP機能は、インターフェイスモジュール（IM）全体のSDHコントローラのポートレベルの冗長性を提供します。異なるIMのポートは、動作モードの1つのポートと保護モードの他のポートを設定できます。

SNCPはSDHネットワークの保護メカニズムで、回線障害が発生したときにSDH接続を別のSDH回線に切り替えることができます。保護インターフェイスは、現用インターフェイスのバックアップインターフェイスとして機能します。動作中インターフェイスに障害が発生すると、保護インターフェイスはそのトラフィック負荷を迅速に引き継ぎます。保護パスへの切り替えは、非リバーティブモードで行われます。トランスミッション障害が原因で保護が保護パスに切り替えられた場合、障害が修正されると、元のパスへの自動スイッチバックは行われません。SONETでのSNCPと同等な機能はUPSRと呼ばれています。プロビジョニングウィザードまたはCLIを使用して、CEMサービスとSNCPをプロビジョニングできます。サポートされているモードは、VC4\_16C、VC4\_4C、VC4、AU4\_VC12、AU4-VC11、AU3-VC12、AU3-VC11です。



(注) ミックスモードのサポートは利用できません。

次に制限事項の一部を示します。

- SNCP を使用して SDH でサポートされているモードは STM64 ポートではサポートされていません。
- ループバックおよびビット エラー レート テスト (BERT) は、物理メンバー コントローラでのみ設定できます。
- サポートされている拡張性は 336 回路に制限されています

保護グループを変更する前に、コントローラ/インターフェイスを保護に必ず追加してください。

APS/MSP 保護グループを設定し、UPSR/SNCP インターフェイスを表示するには、次の手順を実行します。

- ステップ 1** [設定 (Configuration)] > [ネットワーク デバイス (Network Devices)] を選択します。
- ステップ 2** 保護グループで設定されたデバイスを選択するため、そのデバイス名のハイパーリンクをクリックします。
- ステップ 3** [論理ビュー (Logical View)] タブをクリックします。
- ステップ 4** [回線エミュレーション (Circuit Emulation)] > [保護グループ (Protection Group)] を選択します。
- ステップ 5** APS/MSP パラメータを設定するには、[APS/MSP] タブをクリックし、変更するグループの [保護グループ (Protection)] ハイパーリンクをクリックし、ページの右上隅にある [編集 (Edit)] アイコンをクリックします。
- ステップ 6** 表示および設定できるフィールドは次のとおりです。
  - [動作中メンバー (Working Member)] には、回線のメインの動作コントローラとして機能する SONET/SDH コントローラが表示されます。
  - [保護メンバー (Protecting Member)] には、回線の動作中メンバーへのバックアップとして機能する SONET/SDH コントローラが表示されます。
  - [保護ステータス (Protection Status)] には、グループが回線のアクティブメンバーか非アクティブメンバーかが示されます。
  - [Hello 時間 (Hello Time)] フィールドと [保留時間 (Hold Time)] フィールドは、保護メンバーと現用メンバーの時間範囲を表示します。hello タイマーは、hello パケット間の時間を定義します。保留タイマーは、保護インターフェイスプロセスが現用インターフェイスのルータのダウンを宣言するまでの時間を設定します。デフォルトでは、保留時間は hello 時間の 3 倍以上となります。
  - [ループバック IP (Loopback IP)] は、現用インターフェイスを持つルータの IP アドレス (通常はループバック アドレス) を含む保護インターフェイスの設定を決定します。

- [復帰時間 (Revertive Time)] (分単位) は、動作中インターフェイスが利用可能になった後に、設定されている時間に基づいて保護インターフェイスから動作中インターフェイスへの自動スイッチオーバーを有効にできます。リバーティブ時間がゼロの場合、保護は非リバーティブになります。
- [方向 (Directional)] ドロップダウンメニューには、バックアップ保護を有効にする必要がある方向が表示されます。
  - 双方向モードでは、動作中メンバーの障害によって動作中メンバーから保護メンバーへの APS/MSP スwitchオーバーがトリガーされます。この場合、受信チャネルと送信チャネルはペアとして切り替わります。
  - 単方向モードでは、動作中メンバーの障害によって障害が発生したメンバーから保護インターフェイスの対応する回線のみへの APS/MSP スwitchオーバーがトリガーされます。
- [ADM] チェックボックスが有効になっている場合は、アド/ドロップマルチプレクサ (ADM) と保護メンバーが関連付けられます。
- [APS 要求 (APS Request)] ドロップダウンメニューを使用すると次の値を設定できます。値は [ロックアウト (Lockout)] > [強制切り替え (Force Switch)] > [手動切り替え (Manual Switch)] > [モードなし (No Mode)] の順序に設定できます。たとえば、[強制切り替え (Force Switch)] がデバイスに現在設定されている場合は、[手動スイッチ (Manual Switch)] または [モードなし (No Mode)] の値のみを設定できます。[強制切り替え (Force Switch)] の設定時にロックアウトは設定できません。
  - [ロックアウト (Lockout)] : 動作中インターフェイスが保護インターフェイスに切り替わるのを防ぎます。たとえば、保護インターフェイスが回線 1 として設定されている場合、ロックアウトオプションを使用すると、保護インターフェイスがアクティブになるのを防ぎます。
  - [手動切り替え (Manual Switch)] : 同等かより高いプライオリティを持つ要求が実行されている場合を除いて、回線を保護インターフェイスに手動で切り替えます。
  - [強制切り替え (Force Switch)] : 同等かより高いプライオリティを持つ要求が実行されている場合を除いて、回線を保護インターフェイスに手動で切り替えます。たとえば、保護インターフェイスが特定の回線として設定されている場合、force コマンドは保護インターフェイスをアクティブに設定します。
  - [モードなし (No Mode)] : デバイスの保護グループから現在の APS/MSP 要求設定を削除します。

(注) SONET または SDH の保護グループをクリアするには、SONET または SDH いずれかの保護グループ ID を選択し、[削除 (Delete)] (X) アイコンをクリックします。

**ステップ 7** UPSR/SNCP インターフェイスに関連付けられている類似パラメータを表示するには、[UPSR/SNCP] タブをクリックします。

保護グループ番号、デバイスで構成されている現用メンバーと保護メンバー、グループのアクティブパス、現在の保護ステータスなどの情報を表示できます。この情報は変更できません。

(注) 設定された SDH を超える UPSR/SNCP を持つ IM のシャットダウンまたは削除中に、UI の変更を検証し、各インターフェイスモジュールの活性挿抜 (OIR) を確認できます。 **show protection-group** コマンドを使用します。

- 次のステータスの変更を表示するには、次の手順を実行します。
  - [手動 (Manual) ] : SNCP 保護グループを手動で設定すると、ステータスが表示されます。
  - [クリア (Clear) ] : 以前に設定された外部コマンドをクリアします。
  - [自動 (Auto) ] : SNCP 保護グループを最初に設定したときにステータスが表示されます。
  - [強制 (Force) ] : 手動で切り替えるときにステータスが表示されます。
  - [Fail (失敗) ] : 保護された現用パスがダウンしているときにステータスが表示されます。
  - [信号障害 (Signal Failure) ] : リンク障害が発生しているときにステータスが SF に送信されます。
  - [信号の劣化 (Signal Degrade) ] : 現用パスがダウンしているときにステータスが表示されます。
  - [ロックアウト (Lockout) ] : 動作中インターフェイスが保護インターフェイスに切り替わるのを防ぎます。

**ステップ 8** [回線エミュレーション (Circuit Emulation) ]>[SONET および SDH (SONET and SDH) ]を選択します。

**ステップ 9** ACR コントローラ、上位パス、下位パスのパラメータを表示または設定するには、関連するタブをクリックします。変更する SONET または SDH ハイパーリンクをクリックし、ページの右上隅にある [編集 (Edit) ] アイコンをクリックします。SDH の設定の詳細については、 [EPNM での SDH のモード設定 \(33 ページ\)](#)、[SDH パラメータの設定 \(31 ページ\)](#)、および [SDH 回線およびセクションパラメータの設定 \(34 ページ\)](#) [SAToP の SDH VC 設定パラメータ \(36 ページ\)](#) [SDH T1/E1 設定パラメータ \(35 ページ\)](#) [SDH T3/E3 設定パラメータ \(35 ページ\)](#) を参照してください。

[ACR コントローラ] タブを使用して、SONET/SDH 保護グループの仮想 SONET アクセス回線冗長性 (ACR) /SDH アクセス回線冗長性 (ACR) の詳細を表示します。

## CEM のクロッキングの設定

クロッキングモードは、CEM 回線の送信側と受信側で同じクロックを達成するための複数の方法を定義します。Cisco EPN Manager を使用すると、次の方法でクロックの復元と配信を設定できます。

- 同期クロッキング : 同期クロッキングによって、送信元と宛先の PDH (TDM) 回線が同じクロックに合わせて同期化されます。このクロックは、何らかの物理的クロック配信手

段で配信されたものです (SONET、SDH など)。特定の TDM 回線のクロックは、次のものから渡すことができます。

- 回線：送信クロックは、同じ物理回線の受信者からのものです。
- 内部：コントローラは、内部クロックを使用して送信データをクロッキングします。
- フリーランニング：送信クロックはラインカードから取得され、内部のフリーランニングオシレータから導出できます。
- 回復：送信クロックは、CEM インターフェイスでインバンド擬似回線ベースのアクティブクロック回復から導出されます。

Cisco EPN Manager でこれらのクロッキング値を設定するには、「CEM インターフェイスの設定」を参照してください。

- 適応クロッキング：適応クロッキングは、ルータに共通クロックソースがない場合に使用されます。クロックは、デジッタバッファ占有レベルに基づくパケット到達率に基づいて、導出されます。Cisco EPN Manager では、CEM サービスのプロビジョニングの際に、デジッタバッファのサイズ (1 ~ 32) を設定できます。デジッタバッファのサイズにより、回線がどれほどネットワークジッターを許容できる決定します。
- 差分クロッキング：差分クロッキングが使用されるのは、セルサイトと集約ルータに共通のクロックソースがあるが、TDM 回線のクロッキングに別のソースが使用されている場合です。TDM のクロックは、共通のクロックを基準とする、パケットの RTP ヘッダーの差分情報から導出されます。差分クロック回復の基になるのは、RTP ヘッダーで受信したタイムスタンプです。

CEM のクロック復元を設定するには、次の手順を実行します。

- 
- ステップ 1** [設定 (Configuration)] タブをクリックし、左側の [論理ビュー (Logical View)] タブをクリックします。
- ステップ 2** [クロック (Clock)] > [復元クロック (Recovered Clock)] を選択します。
- ステップ 3** クロックソースの導出元の新しいインターフェイスを追加するには、追加アイコン ([+]) をクリックします。
- ステップ 4** 既存の復元クロック設定を編集するには、[復元インターフェイス (Recovering Interface)] ハイパーリンクをクリックし、ページ右上にある [編集 (Edit)] アイコンをクリックします。
- ステップ 5** 次の復元クロック値を指定します。
1. 復元されたクロック設定を容易に識別できるように、[復元されたクロック ID (Recovered Clock ID)] に固有の数値を入力します。この ID を使用して、CEM インターフェイスをこの復元クロック設定に直接関連付けることができます。
  2. [復元モード (Recover Mode)] ドロップダウンリストから、次のいずれかを選択します。
    - [適応 (Adaptive)]：デバイス間に共通のクロックソースがない場合、関連付けられている保護グループの保護メンバーとして選択されたコントローラでのパケット到着率から、復元クロックが導出されます。



- [差分 (Differential) ] : エッジデバイス間に共通のクロックソースがある場合、パケットのタイミング情報と、共通クロックの関連する差分から、復元クロックが導出されます。
3. **CEM グループ番号**を容易に識別できるように、固有の数値を入力します。これにより、クロックに関連付けられている CEM が識別されます。
  4. [復元インターフェイス (Recovering Interface) ] ドロップダウンリストから、必要なコントローラを選択します。クロックに関連付けられているこのコントローラは仮想 CEM インターフェイスであり、バックアップクロック ソースが必要な場合にはこのインターフェイスからクロックが導出されます。

ステップ 6 [保存 (Save) ] をクリックします。

変更が保存され、デバイスに展開されます。

---

## CEM インターフェイス (PDH、SONET、および SDH) のフィールドの説明

次の表に示された CEM パラメータを設定するには、次の手順を実行します。

- ステップ 1 SONET、PDH、HOP、および HOP コントローラで必須の CEM パラメータを設定します。[CEM のインターフェイスの設定 \(15 ページ\)](#) を参照してください。
- ステップ 2 CEM のクロックのディストリビューションとリカバリを設定します。[CEM のクロッキングの設定 \(23 ページ\)](#) を参照してください。

表 6: CEM インターフェイス (SONET、SDH、および PDH) フィールドの説明

フィールド	説明	値	説明	適切なコントローラモード
利率	データが転送されるレートを識別します。SFP (Small Form-factor Pluggable) によって異なります。	LR_DSR_OC1_STM0	STM レベル 0 のチャネライズド OC-1 回線でサポートされるレイヤレートを示します。OC-1 は、転送データ レートが最大 51.84 Mbit/s の光キャリア ネットワーク回線です。	STS1E
		LR_DSR_OC3_STM1	STM レベル 1 のチャネライズド OC-3 回線でサポートされるレイヤレートを示します。OC-3 は、転送データ レートが最大 155.52 Mbit/s のオプティカル キャリア ネットワーク回線です。	SONET/SDH
		LR_DSR_OC12_STM4	STM レベル 4 のチャネライズド OC-12 回線でサポートされるレイヤレートを示します。  OC-12 は、転送データ レートが最大 622.08 Mbit/s のオプティカル キャリア ネットワーク回線です。	SONET/SDH
		LR_DSR_OC48_STM16	STM レベル 16 のチャネライズド OC-48 回線でサポートされるレイヤレートを示します。OC-48 は、転送データ レートが最大 2.4Gbps のオプティカル キャリア ネットワーク回線です。	SONET/SDH
		LR_DSR_OC192_STM64	STM レベル 64 のチャネライズド OC-192 回線でサポートされるレイヤレートを示します。  STM レベル 64 のチャネライズド OC-192 回線。OC-192 は、転送データ レートが最大 9.6Gbps のオプティカル キャリア ネットワーク回線です。	SONET/SDH

フィールド	説明	値	説明	適切なコントローラモード
[モード (Mode) ]	高次および低次パスのチャネル化のタイプ (レベル n の同期転送信号 (STS-n) など) を示します。	<p>高次パス値 :</p> <p>STS3C、STS12C、STS48C、STS192C、T3、UNFRAMED、VT15、VT2、および CT3。</p> <p>下位パス値 :</p> <p>VT15、T1、および E1。</p> <p>(注) STS1E でサポートされているモード :</p> <p>上位パス値 : T3 と UNFRAMED</p> <p>下位パス値 : CT3 と VT15</p>	<ul style="list-style-type: none"> <li>• STS-n : レベル n の同期転送信号 (STS) のチャネル化を伴うモード。</li> <li>• T1、E1、T3、および E3 : コントローラで使用されるチャネル化モードを示します。T1 または E1 回路の伝送データ レートは最大 1.544 Mbps です。T3 または E3 回路の伝送データ レートは最大 44.736 Mbit/s です。</li> <li>• VT 1.5 : コントローラが最大 1.728 Mbit/s の転送データ レートのパケットトリビュタリネットワーク回線であることを示します。</li> <li>• VT 2 : コントローラが最大 2.304 Mbit/s の転送データ レートのパケットトリビュタリネットワーク回線であることを示します。</li> <li>• Unframed : 1 つの CEM チャンネルがすべての T1/E1 タイムスロットに使用されることを示します。</li> </ul>	HOP と LOP
		VC4_16C、VC4_4C、VC4、AU4_VC12、AU4-VC11、AU3-VC12、AU3-VC11、T3、E3、VC1X、TUG3	サポートされている SDH モード	HOP と LOP

フィールド	説明	値	説明	適切なコントローラモード
クロック送信元 (Clock Source)	SONET ポートまたは SDH ポートで送信されたクロック信号の送信元を特定します。	回線 (Line)	コントローラは、回線の受信データストリームから回復されたクロックを使用して送信データのログを記録します。	すべて (All)
		内線	送信クロックはラインカードから取得され、内部の物理回線から派生させることができます。	すべて (All)
		回復	送信クロックを駆動するために使用される CEM インターフェイス上のインバウンド疑似回線ベースのアクティブクロック回復。	SONET、SDH、HOP、および LOP。
フレーミング (Framing)	CEM チャンネルに使用するフレーミングモード。	CRC と NO_CRC。	CRC : 巡回冗長検査でフレーミングタイプを表します。	SONET/SDH
		Unframed、DSX1_ESF、DSX1_SF、Auto Detect、C_BIT、および M13。	<ul style="list-style-type: none"> <li>• Unframed : 1つの CEM チャンネルがすべてのタイムスロットに使用されることを示します。</li> <li>• DSX1_SF : インターフェイスの DS1 タイプがスーパーフレームとしてフレーミングタイプを持つことを示します。SF は、インバウンドシグナリング抽出に 1つのスーパーフレームあたり 12のフレームを使用します。</li> <li>• DSX1_ESF : DS1 タイプのインターフェイスが拡張スーパーフレームとしてフレーミングタイプを持つことを示します。ESF は 1つの ESF あたり 24のフレームを使用します。</li> </ul>	PDH、HOP、LOP、および STS1E。

フィールド	説明	値	説明	適切なコントローラモード
ループバック	CEM インターフェイスに関連付けられたループバック値を指定します。	ローカル、ネットワーク回線、リモート、リモート回線、ネットワークペイロード、および不明。	様々なループバック値に関する詳細な説明については、最新の IOS コマンドリファレンスを参照してください。	すべて (All)
		Diag、ローカルペイロード、リモート ESF ペイロード、リモート ESF 回線、リモート ESF 回線 CSU、リモート ESF 回線 NIU、リモート Iboc、リモート Iboc CSU、リモート Iboc FAC1、リモート Iboc、および FAC2。	—	PDH
保護権限	復元クロックを取得する優先順位を指定します。	現用 (WORKING!!)	復元クロックは、優先順位の最も高いクロックから取得されます。	SONET/SDH
		保護 (PROTECT)	復元クロックはプライマリクロックより優先順位の低いクロックから取得されます。	SONET/SDH
ケーブル長 (Cable Length)	ケーブルの長さに応じて伝送減衰を設定します。たとえば、短い 115 を選択した場合、ケーブル長は 0 ~ 115 フィートです。ケーブル長さが 110 ~ 220 フィートなどの場合は、[ショート 220 (Short 220)] を選択します。値は [ショート 110 (Short 110)] から [ショート 550 (Short 550)]、[ショート LT 225 (Short LT 225)]、[ロング GT 225 (Long GT 225)] の間になります。			PDH
回線コーディング (Line Coding)	コントローラの回線エンコーディング方式は次のとおりです。 <ul style="list-style-type: none"> <li>• E1 の場合、オプションは交互マーク反転 (AMI) です。</li> <li>• T1 の場合、選択可能なオプションは AMI と Bipolar with 8 Zero Substitution (B8ZS) です。</li> </ul>			PDH
チャンネル化モード (Channelization Mode)	コントローラで使用する必要があるチャンネル化モードを示します。T1 または E1 の回線の伝送データレートは最大 1.544 Mbps です。値は [T1]、[E1]、および [非チャンネル化 (Unchannelized)] です。 <p>(注) T3 コントローラの場合はチャンネル化された T1/E1 プロパティを表示または変更し、E3 コントローラの場合はチャンネル化された T1/E1 プロパティを表示または変更します。</p>			PDH

フィールド	説明	値	説明	適切なコントローラモード
保護グループ番号 (Protection Group Number)	保護番号または ACR グループを識別します。			SONET/SDH
保護ループバック名 (Protection Loopback Name)	デバイス上のループバック インターフェイスの名前を識別します。			SONET/SDH
保護ループバック IP (Protection Loopback IP)	デバイス上のループバック インターフェイスの IP アドレスを識別します。			SONET/SDH
保護復帰時間 (Protection Revertive Time) 保護非復帰時間 (Protection Non-Revertive Time)	<p>現用回線で障害が発生した場合、ソフトウェアは保護回線に切り替え、現用回線が回復した場合は復帰タイマーに基づいて待機し、現用回線をアクティブリンクに戻します。</p> <p>信号に障害が発生した場合、ソフトウェアは保護回線に切り替えますが、現用回線への自動復帰は行いません。これがデフォルトのオプションです。</p>			SONET/SDH
動作ステータス	CEM インターフェイスの動作ステータス。このフィールドは編集できません。	Up、Down、および Not-Applicable。	<ul style="list-style-type: none"> <li>• Down : インターフェイスがダウンしています。</li> <li>• Not-Applicable : インターフェイスの動作ステータスが不明です。</li> <li>• Up : インターフェイスが機能しています。</li> </ul>	SONET、SDH、HOP、LOP、および STS1E。

フィールド	説明	値	説明	適切なコントローラモード
管理ステータス	CEM インターフェイスの管理ステータス。	Up、Down、および Not-Applicable。	<ul style="list-style-type: none"> <li>• Up : CEM インターフェイスは機能しています。</li> <li>• Down : CEM インターフェイスはダウンしています。</li> <li>• Not-Applicable : 管理ステータスは不明です。</li> </ul>	SONET、SDH、HOP、LOP、および STS1E。
復元クロック ID	CEM インターフェイスに関連付けられたクロック設定の一意の識別子。復元クロック ID を設定するには、CEM のクロック設定を参照してください。			PDH、ホップ、および LOP。
AUG タイプ (AUG Type)	管理ユニットグループ (AUG) は、STM レベルにおいて定義された位置を占めている 1 台以上の管理ユニットから構成されます。AUG-3 グループ化と AUG-4 グループ化はサポートされている AUG タイプです。			SDH

## SDH パラメータの設定

SDH CEM チャンネル化モードを設定するには、次の表を参照してください。

表 7: コントローラ モードおよびサポートされるポート タイプ

SDH モード	CEM	ポート	適切なコントローラモード
VC4_16c	CEP	STM16	HOP
VC4_4c	CEP	STM4、STM16	HOP
VC4	CEP	OC3/STM1、OC12/STM4、OC48/STM16	HOP
VC1X	CEP	OC3/STM1、OC12/STM4、OC48/STM16	HOP
TUG3-E3	SATop	OC3/STM1、OC12/STM4、OC48/STM16	HOP

SDH モード	CEM	ポート	適切なコントローラモード
TUG-3-T3	SATop	OC3/STM1、 OC12/STM4、 OC48/STM16	HOP
VC11_T1	SATop	OC3/STM1、 OC12/STM4、 OC48/STM16	LOP
VC12_E1	SATop	STM1、STM4、STM16	LOP
VC11	CEP	OC3/STM1、 OC12/STM4、 OC48/STM16	LOP
VC12	CEP	OC3/STM1、 OC12/STM4、 OC48/STM16	LOP

#### メディアタイプコントローラの設定

各 SFP ポート（16～19）は、STM1、STM4、STM16 として設定できます。設定するメディアタイプコントローラを選択し、コントローラ設定モードを開始する必要があります。コントローラを SDH ポートとして設定する必要があります。

```
To configure MediaType Controller:
enable
configure terminal controller
MediaType 0/0/16
mode sdh
end
```

#### SDH ポートでのレートの設定

```
To configure rate on SDH ports:
enable
configure terminal
controller MediaType 0/0/16
mode sdh
end
```



(注) コマンドの **no** 形式の設定はサポートされていません。デフォルトの状態に戻すには、そのポートの下にあるすべての設定を削除した後、メディアタイプコントローラの下で **no mode sdh** コマンドを使用します。



## EPNM での SDH のモード設定

同期転送モジュール (STM) 信号は、SONET の STS の同期デジタル階層 (SDH) 版に相当します。このドキュメントでは、STM という用語はパス幅と光回線レートの両方を表します。STM 信号内のパスは、管理ユニット (AU) と呼ばれます。AU は、より上位のパス層と多重化セクション層間の適合を可能にする情報構造です。AU は、情報ペイロード (より上位の VC) と AU ポインタで構成されます。AU ポインタは、ペイロードフレームの開始のオフセットを多重化セクションフレームの開始と相対的に示します。AU-3 ポインタは 3 バイトで構成され、AU-4 ポインタは 9 バイトで構成されます。STM-1 フレームのペイロードは、1 つの AU-4 ユニットまたは 3 つの AU-3 ユニットで構成されています。管理ユニットグループ (AUG) の拡張マッピングは、STM ペイロードにおいて固定の定義された位置を占める 1 つまたは複数の管理ユニットで構成されます。拡張マッピングは STM1 レベルでサポートされています。

次のタイプの拡張マッピングがサポートされています。

- 拡張マッピング AU-4



これはデフォルトの拡張マッピングモードです

- 拡張マッピング AU-3

SDH では次のモードがサポートされています。

- AU-4\_16c (VC4-16c)
- AU-4\_4c (VC4-4c)
- AU-4 (VC4)
- AU-4 — TUG-3 — DS3
- AU-4 — TUG-3 — T3
- AU-4 — TUG-3 — E3
- AU-4 — TUG-3 — TUG-2 — VC-11 — T1
- AU-4 — TUG-3 — TUG-2 — VC-12 — E1
- AU-4 — TUG-3 — TUG-2 — VC-11
- AU-4 — TUG-3 — TUG-2 — VC-12
- AU-3: T3
- AU-3 — TUG-2 — VC-11—T1
- AU-3 — TUG-2 — VC-12—E1
- AU-3 — TUG-2 — VC-11
- AU-3 — TUG-2 — VC-12
- AU-3 — E3

管理ユニットグループ (AUG) マッピングを構成するには、たとえば、AU-3 または AU-4 マッピングの設定に次の設定コマンドを使用します。

```
configure terminal
  aug mapping [au-3 | au-4]
end
```



(注) **aug mapping** コマンドは、SDH フレーミングが設定されているときにのみ使用できます。AUG モードはデフォルトでは AUG-4 であり、STM-1 レベルでサポートされています。

## SDH 回線およびセクションパラメータの設定

次のパラメータは、回線レベルとセクションレベルでの SDH 設定に影響します。

### ループバック (Loopback)

SDH ポートをテストするループバックを設定します。

- **local** : Tx から Rx パスに信号をループします。アラーム表示信号 (AIS) をネットワークに送信します。
- **network** : Rx から Tx パスに信号をループします。

### 回線ループバックの設定

```
To configure loopback:
enable
configure terminal
controller sdh 0/0/16
loopback [local | network]
end
```



(注) システムをデフォルトの状態に戻すには、このコマンドの **no** 形式を使用します。

### クロック送信元 (Clock Source)

次の場合にクロックソースを指定します。

- **line** : リンクは回線から回復したクロックを使用します。
- **internal** : リンクは内部クロックソースを使用します。これがデフォルトの設定です。

```
To configure clock, use the following commands:
enable
configure terminal
controller sdh 0/0/16
clock source [line | internal]
end
```



- (注) デフォルトは **internal** です。システムをデフォルトの状態に戻すには、このコマンドの **no** 形式を使用します。

### ネットワーククロック SDH の設定

To configure network-clock SDH, use the following commands:

```
enable
configure terminal
controller sdh 0/0/16
clock source line
end
enable
configure terminal
network-clock input-source 1 controller sdh 0/0/16
end
```

## SDH T1/E1 設定パラメータ

次のパラメータは、SDH T1/E1 の設定に影響します。

- クロック : T1 インターフェイスまたは E1 インターフェイスのクロック ソースを指定します。
- 説明 : コントローラの説明を指定します。
- ループバック : ループバック モードでの T1 インターフェイスまたは E1 インターフェイスを設定します。

### SDH T1/E1 パラメータの設定

```
To configure T1/E1 parameters:
enable
configure terminal
controller sdh 0/0/16
rate stm4
au-3 1
mode vc1x
tug-2 1 payload vc11
t1 1 loopback [local | network line]
t1 1 clock source [line | internal | recovered]
end
```

## SDH T3/E3 設定パラメータ

次のパラメータは、SDH T3/E3 の設定に影響します。

- クロック : T3 リンクまたは E3 リンクのクロック ソースを指定します。
- ループバック : ループバック モードでの T3 リンクまたは E3 リンクを設定します。

### SDH T3/E3 パラメータの設定

```
To configure SDH T3/E3 parameters configuration:
enable
```

```

configure terminal
controller sdh 0/0/16
rate stm4
au-4 1
mode tug 3
tug-3 1
mode e3
e3 1 clock source [line | internal | recovered]
e3 framing [m13 | c-bit ] (applicable to for mode e3)
e3 1 loopback [local | network line]
e3 bert pattern 0s interval 2
tug-3 2
mode t3
t3 1 clock source [line | internal | recovered]
t3 framing [m13 | c-bit ] (applicable to for mode t3)
t3 1 loopback [local | network line]
end

```



(注) これは、AUG マッピング AU-4 モード T3 および AU-3 モード T3 に適用されます。

## SAToP の SDH VC 設定パラメータ

次のパラメータは、SDH VC 設定に影響します。

- クロック : VC のクロック ソースを指定します。
- ループバック : ループバック モードでの VC を設定します。

### VC パラメータの設定

```

To configure VC parameters:
enable
configure terminal
controller sdh 0/0/16
rate stm4
au-3 1
mode vclx
tug-2 1 payload vcl1
vc 1 loopback [local | network]
vc 1 clock source internal
end

```

## Sync-E、BITS、および PTP を使用したクロックの同期

### 同期イーサネット (Sync-E) :

Cisco EPN Manager を使用すると、周波数同期を有効にして、イーサネット インターフェイス上で高品質のビットクロック同期を実現できます。同期イーサネット (Sync-E) により、必要な同期が物理レベルで実現します。

これには、ルータがネットワーク内のクロックを最優先で識別できるように Sync-E を設定する必要があります。このクロックは「プライマリクロック」とも呼ばれます。ネットワーク上の他のデバイス (メンバー) は、すべてプライマリクロックの設定に基づいてクロックをリ

セットします。プライマリクロックとそのメンバー間で常にメッセージが交換され、ネットワーク内のすべてのクロックが効率的かつ継続的に同期されます。Cisco EPN Manager を使用すると、このプライマリクロックを指定でき、また、Sync-Eパラメータをグローバルレベルとインターフェイスレベルで設定できます。Sync-E プロパティを設定すると、ネットワークトポロジ オーバーレイ上のデバイス間の論理階層とトポロジを表示できます。



(注) Sync-E 構成は、イーサネット インターフェイスでのみサポートされています。

#### **Building Integrated Timing Supply (BITS) :**

BITS では、Building Integrated Timing Supply (BITS) ポートクロックによってクロッキング情報が提供されます。Sync-Eを使用するイーサネットリンクは、SONET/SDHと同じ方法で、つまり高品質なストラタム1追跡可能クロック信号とビットクロックのタイミングを取ることで同期されます。SSMやESMCなどの処理メッセージは、Sync-Eリンクを維持し、ノードが最も信頼性に優れた送信元から常にタイミングを得られるようにします。

#### **Precision Time Protocol (PTP) :**

TDMを使用するネットワークでデータストリームを正確にリアセンブルするには、受信デバイスが正しいチャンネルを認識できるように、デバイスクロックを定期的に同期する必要があります。Precision Time Protocol (PTP) 標準 :

- この同期を可能にするクロック同期プロトコルを指定します。
- ネットワーク経由で通信する1つ以上のノードから構成される分散システムに適用されます。

PTPは、プライマリと従属のデバイスの概念を使用して、正確なクロック同期を実現します。Cisco EPN Managerを使用することで、PTPにより、従属デバイスと定期的にメッセージを交換するプライマリデバイスを設定できます。各従属デバイスは、メッセージの送受信時刻を通知した後、そのシステム時刻とプライマリデバイスのシステム時刻の差を計算します。従属デバイスは、プライマリデバイスと同期されるようにクロックを調整します。プライマリデバイスが次のメッセージ交換を開始すると、従属デバイスは再び時刻の差を計算し、クロックを調整します。このように同期が繰り返されることによって、デバイスクロックが調整され、データストリームが正確にリアセンブルされます。個々のインターフェイス上の PTP を変更するには、PTPクロックポートコマンドを使用します。PTPプロパティを設定すると、ネットワークトポロジ オーバーレイ上のデバイス間の論理階層とトポロジを表示できます。



(注) デバイスには制限があるため、インターフェイスモジュールには最大4つ（インターフェイスモジュールごとに最大2つ）のクロックソースを設定できます。この制限は、Sync-EとTDMの両方のインターフェイスに適用されます。

Sync-E、BITS、および PTP を設定するには :

**ステップ 1** [設定 (Configuration)] > [ネットワーク デバイス (Network Devices)] を選択します。

**ステップ 2** デバイス名のハイパーリンクをクリックして、設定するデバイスを選択します。

**ステップ 3** グローバル Sync-E プロパティを設定します。

- a) [論理ビュー (Logical View)] タブをクリックします。
- b) [クロック (Clock)] > [Sync-E] をクリックします。利用可能なすべての Sync-E グローバル設定が一覧表示されます。
- c) 新しいグローバル Sync-E プロパティのセットを作成するには、[+] アイコンをクリックします。Sync-E グローバルパラメータのセットは、1 つのみ作成できます。
- d) Sync-E のグローバルパラメータを指定します。これらのパラメータの詳細な説明については、次の表を参照してください。
- e) [保存 (Save)] をクリックします。  
変更が保存され、グローバル Sync-E の構成がデバイスに展開されます。これで、この構成に関連付けるインターフェイスを指定できます。

**ステップ 4** 関連付けられたインターフェイスと、インターフェイス固有の Sync-E パラメータを指定します。

- a) [クロック (Clock)] > [Sync-E] をクリックし、上記の手順で作成した Sync-E グローバル構成を選択します。
- b) [インターフェイス入力ソース (Interface Input Source)] タブをクリックします。
- c) [+] をクリックして、必要なインターフェイスを指定します。  
同期タイプごとに 1 つのインターフェイスのみを設定できます。
- d) [インターフェイス名 (Interface Name)] ドロップダウンメニューを使用して、必要なインターフェイスを選択します。
- e) インターフェイスレベルの Sync-E パラメータを指定します。これらのパラメータの詳細については、下記の表を参照してください。
- f) [保存 (Save)] をクリックします。

**ステップ 5** BITS の周波数設定を指定します (XE デバイス場合)。

- a) [論理ビュー (Logical View)] タブをクリックします。
- b) [クロック (Clock)] > [BITS 周波数 (BITS-Frequency)] をクリックします。
- c) 次の BITS の値を指定します。
  - [送信元スロット (Source Slot)] : 値は RO と R1 です。
  - [プライオリティ (Priority)] : 1 ~ 250 の範囲の数値。
  - [クロックタイプ (Clock Type)] : 値は 2.048 MHz および 10 MHz です。
- d) [保存 (Save)] をクリックします。

**ステップ 6** BITS のインターフェイスを設定します。

- a) [論理ビュー (Logical View)] タブをクリックします。
- b) [クロック (Clock)] > [BITS インターフェイス (BITS-Interface)] をクリックします。
- c) 次の BITS の値を指定します。

**XE デバイスの場合：**

- [送信元スロット (Source Slot) ]：オプションは RO と R1 です。
- [プライオリティ (Priority) ]：1 ～ 250 の範囲の数値。
- [クロックタイプ (Clock Type) ]：オプションは E1 と T1 です。

(注) BITS インターフェイスを T1 として設定するには、SSM オプションは OPTION2\_GEN1 または OPTION2\_GEN2 である必要があります。

**XR デバイスの場合：**

- [クロックインターフェイス (Clock Interface) ]：オプションは BITS0\_IN、BITS0\_OUT、BITS1\_IN、および BITS1\_OUT です。
- [クロックタイプ (Clock Type) ]：オプションは E1、T1、J1、\_2M、および \_64K です。

d) [保存 (Save) ] をクリックします。

e) インターフェイスの BITS クロックを設定します。

1. [クロック (Clock) ] > [BITS インターフェイス (BITS-Interface) ] に移動し、上記のステップで作成した BITS インターフェイス設定の送信元スロットをクリックします。
2. [BITS クロックの設定 (Bits Clock Settings) ] タブをクリックし、下記の表の説明に従ってクロックを設定します。
3. [保存 (Save) ] をクリックします。

**ステップ 7 PTP クロックを設定します。**

- a) [論理ビュー (Logical View) ] タブをクリックします。
- b) [クロック (Clock) ] > [PTP] をクリックします。
- c) [+] をクリックして、新しい PTP 値のセットを指定するか、[クロック モード (Clock Mode) ] ハイパーリンクをクリックし、ページの右上にある [編集 (Edit) ] アイコンをクリックします。
- d) 次の共通の PTP パラメータを指定し、[保存 (Save) ] をクリックします。
  - [クロック モード (Clock Mode) ]：PTP 操作のモードを選択します。オプションは [通常 (Ordinary) ]、[境界 (Boundary) ]、および [E2E トランスペアレント (E2E Transparent) ] です。E2E は、エンドツーエンド トランスペアレント クロック モードを表します。
  - [ドメイン番号 (Domain No) ]：PTP トラフィックに使用されるドメインの番号を入力します。1 つのネットワークに複数のドメインを含めることができます。範囲は 1 ～ 127 です。
  - [ハイブリッドクロック (Hybrid Clock) ]：ハイブリッドクラウドを有効または無効にします。
- e) [クロック モード (Clock Mode) ] ハイパーリンクをクリックし、[ポート (Port) ] タブをクリックして、共通のプロパティに関連付ける必要があるポートの詳細を指定します。
- f) 次のポートの詳細を指定し、[保存 (Save) ] をクリックします。
  - [ポート名 (Port Name) ]：PTP ポート クロックの名前を入力します。

- [ポートモード (Port Mode)] : プライマリまたは従属のクロックの PTP 権限を選択します。
  - [ループバック インターフェイス番号 (Loopback Interface Number)] : デバイス インターフェイスから取得したクロック識別子を入力します。
  - [アナウンス タイムアウト (Announce Timeout)] : セッションがタイムアウトするまでの PTP アナウンス間隔の数を入力します。範囲は 1 ~ 10 です。
  - [遅延要求間隔 (Delay Request Interval)] : インターフェイスを PTP プライマリモードで動作させる時間を選択します。選択した間隔は、遅延要求メッセージのメンバーデバイスに適用されます。間隔には、基数 2 の値が使用されます。
  - [同期間隔 (Sync Interval)] : PTP 同期メッセージを送信する時間間隔を選択します。
  - [アナウンス間隔 (Announce Interval)] : PTP アナウンス パケットを送信する時間間隔を選択します。
- g) [ポート名 (Port Name)] ハイパーリンクをクリックし、[クロック ソース (Clock Source)] タブをクリックします。
- h) [+] をクリックして新しいインターフェイスを追加するか、発信元アドレスのハイパーリンクをクリックし、ページの右上にある [編集 (Edit)] をクリックします。
- i) クロックの [発信元アドレス (Source Address)] と [プライオリティ (Priority)] を指定します。
- [プライオリティなし (No Priority)] : 優先順位値として 0 を割り当てます。
  - [プライオリティ 1 (Priority 1)] : クロック選択の最初の値を確認します。優先順位が最も低いクロックが優先され、値 1 が割り当てられます。
  - [プライオリティ 2 (Priority 2)] : [プライオリティ 1 (Priority 1)] フィールドで複数のクロックの値が同じである場合、このフィールドの値がクロック選択に使用されます。これにより、優先順位値として 2 が割り当てられます。
- j) [保存 (Save)] をクリックして、変更内容をデバイスに展開します。

すべての Sync-E グローバルおよびインターフェイス レベルのパラメータの詳細については、次の表を参照してください。

フィールド	説明
<b>[クロック (Clock)] &gt; [Sync-E 共通プロパティ (Sync-E Common Properties)] (グローバル レベル)</b>	
自動選択プロセス	<p>クロックの同期に使用されるメソッドのタイプを示します。値は[自動 (Automatic)]、[強制 (Forced)]、[手動 (Manual)]、および [Cisco] です。</p> <p>注：各同期タイプでは、1つのインターフェイスのみを設定できません。</p>



フィールド	説明
[クロック タイプ (Clock Type) ]	<p>使用されるイーサネット機器クロック (EEC) オプションを示します。</p> <p>[オプション 1 (Option 1) ] : 欧州のタイム ゾーンの EEC オプション I を表します。</p> <p>[オプション 2 (Option 2) ] : 北米のタイム ゾーンの EEC オプション II を表します。</p>
[QL モードの有効化 (QL Mode Enabled) ]	<p>クロックを品質レベル (QL) 機能で使用するかどうかを示します。値は [有効 (Enabled) ] または [無効 (Disabled) ] です。</p>
[ESMC の有効化 (ESMC Enabled) ]	<p>イーサネット同期メッセージング チャネル (ESMC) のステータスを示します。値は [有効 (Enabled) ] または [無効 (Disabled) ] です。</p>
[SSM オプション (SSM Option) ]	<p>同期ステータス メッセージ (SSM) オプションが使用されていることを示します。</p> <p>[オプション 1 (Option 1) ] : ITU-T オプション I を表します。</p> <p>[オプション 2- GEN1 (Option 2-GEN1) ] : ITU-T オプション II 第 1 世代を表します。</p> <p>[オプション 2- GEN2 (Option 2-GEN2) ] : ITU-T オプション II 第 2 世代を表します。</p>
[ホールド オフ時間 (Hold Off Time) ] (グローバル レベル)	<p>障害イベントに対して保護応答を発行するまでデバイスが待機する時間の長さ (ミリ秒単位) を示します。</p> <p>有効範囲は 300 ~ 1800 ミリ秒です。</p>
[復元待ち時間 (Wait To Restore Time) ] (グローバル レベル)	<p>障害が修正された後、スパンが元の状態に戻るまで待機する時間の長さ (秒単位) を示します。</p> <p>有効な範囲は 0 ~ 86400 秒です。</p>
[復帰の有効化 (Revert Enabled) ]	<p>ネットワーククロックがリバーティブモードを使用するかどうかを指定します。値は [有効 (Enabled) ] または [無効 (Disabled) ] です。</p>
<b>[Sync-E]&gt;[インターフェイス入力ソース (インターフェイスレベル) プロパティ (Interface Input Source (Interface Level) Properties) ]</b>	
[インターフェイス名 (Interface Name) ]	<p>Sync-E に関連付けられたギガビットまたは 10 ギガビット インターフェイスの名前とハイパーリンク。</p>
[アクティブ クロック (Active Clock) ]	<p>インターフェイスがアクティブ クロックとして現在選択されているかどうかを示します。このインターフェイスはプライマリ インターフェイスにもセカンダリ インターフェイスにもなりますが、Sync-E に現在有効になっているインターフェイスはアクティブなインターフェイスと見なされます。</p>

フィールド	説明
[プライオリティ (Priority) ]	複数のインターフェイスが設定されている場合、クロッキング用の Sync-E インターフェイスを選択するために使用される値を示します。値は 1 ~ 250 で、優先順位が最も高いのは 1 です。 優先順位が最も高いクロックは、プライマリクロックです。
[ホールド オフ時間 (Hold Off Time) ] (インターフェイス レベル)	クロック ソースがダウンした後、ソースを削除するまでに待機する時間の長さ (ミリ秒単位) を示します。 有効な値の範囲は 300 ~ 1800 ミリ秒です。
[復元待ち時間 (Wait To Restore Time) ] (インターフェイス レベル)	障害が修正された後、インターフェイスが元の状態に戻るまで待機する時間の長さ (秒単位) を示します。 有効な値の範囲は 0 ~ 86400 秒です。
[Rx Exact/QL Use]	クロックを使用する必要がある QL 受信機能を示します。
[Tx Exact/QL Send]	クロックを使用する必要がある QL 送信機能を示します。
<b>[クロック (Clock) ] &gt; [BITS 周波数と BITS インターフェイスのプロパティ (BITS-Frequency and BITS-Interface Properties) ]</b>	
[送信元スロット (Source Slot) ]	クロックソースが R0 か R1 かを示します (XE デバイスの場合)。
クロックインターフェイス	クロックソースが BITS0_IN、BITS0_OUT、BITS1_IN、または BITS1_OUT かどうかを示します (XR デバイスの場合)。
[プライオリティ (Priority) ]	複数のインターフェイスが設定されている場合、クロッキング用の BITS インターフェイスを選択するために使用される値を示します。値は 1 ~ 250 で、優先順位が最も高いのは 1 です。 優先順位が最も高いクロックは、プライマリクロックです。

フィールド	説明
[クロック タイプ (Clock Type) ]	<p>使用する必要のあるクロックタイプが E1 回線と T1 回線のどちらであるかを示します (XE デバイスの場合)。XR デバイスの場合、回線は E1、T1、J1、2M、または 64K のいずれかです。</p> <p>BITS インターフェイスのパラメータの場合、[クロックタイプ (Clock Type) ]は、クロックに関連付ける必要のある周波数の値を示します。</p> <p>XE デバイスでサポートされているクロックタイプは次のとおりです。</p> <ul style="list-style-type: none"> <li>• [BITS 周波数 (BITS Frequency) ] : サポートされているオプションは 2.048_MHz と 10_MHz です。</li> <li>• [BITS インターフェイス (BITS Interface) ] : サポートされているオプションは T1 と E1 です。</li> </ul> <p>XR デバイスでサポートされているクロックタイプは次のとおりです。</p> <ul style="list-style-type: none"> <li>• [BITS インターフェイス (BITS Interface) ] : サポートされているオプションは T1、E1、J1、2M、および 64K です。</li> </ul>
[BITS フレーミング (Bits Framing) ]	<p>BITS 構成に関連付ける必要のあるフレーミング値 (CAS など)。</p> <ul style="list-style-type: none"> <li>• XE デバイスのサポートされているビットフレーミング値 : E1_CAS_CRC4、E1_CAS、E1_CRC4、E1_FAS、T1_D4、T1_ESF、および T1_SF</li> <li>• XR デバイスのサポートされているビットフレーミング値 : E1_CRC4、E1_FAS、J1_D4、J1_ESF、T1_D4、および T1_ESF</li> </ul>
[インピーダンス (Impedance) ]	<p>OHMS 形式のクロックに関連付けられているインピーダンス値。サポートされているインピーダンス値は 75 オームおよび 120 オームです。</p>
[BITS サブフレーミング (Bits Sub Framing) ]	<p>E1 クロックタイプの XR デバイスでサポートされているビットサブフレーミング値は、SA4、SA5、SA6、SA7、および SA8 です。</p>

フィールド	説明
Line Code	<p>BITS インターフェイスに関連付ける必要がある回線コードの値。 XE デバイスでサポートされている回線コードの値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• E1 インターフェイスの場合：値は AMI と HDB3 です。</li> <li>• T1 インターフェイスの場合：値は AMI と B8ZS です。</li> </ul> <p>XR デバイスでサポートされている回線コードの値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• E1 インターフェイスの場合：値は AMI と HDB3 です。</li> <li>• J1 インターフェイスの場合：値は AMI と B8ZS です。</li> <li>• T1 インターフェイスの場合：値は AMI と B8ZS です。</li> </ul>
Line Build Out (LBO)	<p>BITS インターフェイスに関連付ける必要がある Line Build Out の値。 このフィールドは、T1 インターフェイスでのみサポートされています。</p> <p>XE デバイスでサポートされている Line Build Out の値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• T1 インターフェイスの場合：値は 0 ~ 133ft、133 ~ 266ft、266 ~ 399ft、399 ~ 533ft、および 533 ~ 655ft です。</li> </ul> <p>XR デバイスのサポートされている Line Build Out の値は次のとおりです。</p> <ul style="list-style-type: none"> <li>• T1 BITS0_OUT インターフェイスの場合：値は 0、1、2、3、および 4 です。</li> <li>• T1 BITS1_OUT インターフェイスの場合：値は 0、1、2、3、および 4 です。</li> </ul>

### 次のタスク

(オプション) ネットワーク トポロジ オーバーレイでは、Sync-E および PTP デバイスのプロパティを表示できます。「[ネットワーク トポロジ マップでのクロック同期ネットワークの表示](#)」を参照してください。

- [Sync-E オーバーレイ (Sync-E overlay) ] : Sync-E ネットワークのトポロジと階層が表示されます。各デバイスのプライマリおよびセカンダリ クロック入力が表示されます。

- [PTPオーバーレイ (PTP overlay)] : クロック同期ツリートポロジ、Precision Time Protocol の階層、およびツリー内の各デバイスのクロックロール (プライマリ、境界、従属、またはトランスペアレント) が表示されます。

## IP SLA の設定 (TWAMP レスポンダ/TWAMP ライトレスポンダ)

IETF Two-Way Active Measurement Protocol (TWAMP) は、TWAMP をサポートする 2 台のデバイス間でのラウンドトリップ IP パフォーマンスの測定に関する規格を定めたものです。TWAMP 制御プロトコルは、パフォーマンス測定プローブを送受信することで、パフォーマンス測定セッションを設定するために使用されます。セッションが作成されると、TWAMP テストパケットが送信され、パケット損失、遅延などのパフォーマンス統計情報の計算を支援します。TWAMP ライトは、テストセッションの確立に使用される制御プロトコルをシンプル化するという点で標準の TWAMP とは異なります。

TWAMP レスポンダは、Cisco IOS XE (NCS 42xx) と Cisco IOS XR (ASR 9000、NCS 540、NCS 560、NCS 5500) デバイスの両方でサポートされています。TWAMP ライトレスポンダは、Cisco IOS XR (ASR 9000、NCS 540、NCS 560、NCS 5500) デバイスのみでサポートされています。TWAMP ライトは IPv4 アドレスと IPv6 アドレスをサポートしていますが、標準 TWAMP は IPv4 アドレスのみをサポートしています。

TWAMP インターフェイスの設定の詳細については、次を参照してください。

- [TWAMP レスポンダの設定 \(45 ページ\)](#)
- [TWAMP ライト レスポンダの設定 \(46 ページ\)](#)

## TWAMP レスポンダの設定

Cisco EPN Manager を使用して TWAMP を設定すると、選択したデバイスは TWAMP サーバーとして設定されます。TWAMP サーバーは、指定されたポートで接続要求と制御要求をリッスンします。指定した非アクティビティ値は、TWAMP 制御セッションの非アクティビティタイマー (秒単位) として構成されます。

TWAMP のエントリを追加または編集するには、次の手順を使用します。

**ステップ 1** 移行方法 **Configuration > Network Devices**.

**ステップ 2** 設定するデバイスのハイパーリンクをクリックしてデバイスを選択し、[デバイスの詳細 (Device Details)] ページを起動します。

**ステップ 3** [論理ビュー (Logical View)] タブをクリックします。

**ステップ 4** TWAMP レスポンダ設定を追加または編集するには、[IP SLA]>[TWAMP レスポンダ (TWAMP Responder)] を選択します。

**ステップ 5** 選択したデバイスに TWAMP パラメータを追加するには、[+] アイコンをクリックします。既存のパラメータを編集するには、[ポート名 (Port Name)] ハイパーリンクをクリックし、ページの右上隅にある [編集 (Edit)] アイコンをクリックします。デバイスごとに追加できる TWAMP パラメータのセットは 1 つだけです。

**ステップ 6** 必要に応じて、次のパラメータを編集します。すべてのパラメータは必須です。

- [ポート (Port)]: 1 ~ 65535 の数値を使用して、接続要求と制御要求をリッスンするように TWAMP サーバーに設定する必要があるポートを指定します。デフォルト値は 862 です。
- [非アクティビティタイムアウト (Inactivity Timeout)]: 1 ~ 604800 の数値を使用して、TWAMP レスポンドテストセッションの非アクティビティ時間 (秒単位) として設定する必要がある時間を指定します。デフォルト値は 900 秒です。
- [サーバーアイドル時間タイムアウト (Server Inactivity Timeout)]: 1 ~ 6000 の数値を使用して、TWAMP 制御セッションの TWAMP サーバーアイドル時間 (秒単位) として設定する必要がある時間を指定します。デフォルト値は 900 秒です。

**ステップ 7** [保存 (Save)] をクリックして、デバイスに変更を展開します。

---

## TWAMP ライトレスポンドの設定

TWAMP ライトレスポンドのインターフェイスを管理するには、次の手順を使用します。

- [TWAMP ライトレスポンドの追加 \(46 ページ\)](#)
- [TWAMP ライトレスポンドの設定の編集 \(47 ページ\)](#)
- [TWAMP ライトレスポンド設定の削除 \(47 ページ\)](#)
- [TWAMP ライトセッションの詳細を表示するコマンド \(48 ページ\)](#)

### TWAMP ライトレスポンドの追加

TWAMP ライトレスポンドのエントリを追加するには、次の手順を使用します。

**ステップ 1** [Configuration] > [Network Devices] を選択します。

**ステップ 2** 設定するデバイスのハイパーリンクをクリックしてデバイスを選択し、[デバイスの詳細 (Device Details)] ページを起動します。

**ステップ 3** 左側のタブで、[Logical View] をクリックします。

**ステップ 4** [IP SLA] > [Twamp Light Responder] を選択します。

**ステップ 5** [TWAMP Light Responder] ページで [+] アイコンをクリックします。

**ステップ 6** 表示されたフィールドに適切な値を入力します。特定のフィールドの横にあるツールチップにマウスを合わせると、許容値の範囲に関する情報が表示されます。

- a) Session ID: セッション ID を指定します。最大 65535 個のテストセッションを設定できます。

- b) Timeout : (任意) TWAMP ライトレスポンドのテストセッションの非アクティブ時間を 60 ~ 86400 (秒単位) の範囲で指定します。デフォルトは、タイムアウトなしです。
- c) Local IP address : IPv4 アドレスまたは IPv6 アドレスを指定します。
- d) Local Port : 1 ~ 65535 の範囲の数値を使用して、セッション用に設定するポートを指定します。
- e) Remote IP address : IPv4 アドレスまたは IPv6 アドレスを指定します。

(注) 指定された [Local IP address] が IPv4 アドレスである場合、[Remote IP address] は IPv4 アドレスである必要があります。同様に、指定された [Local IP address] が IPv6 アドレスである場合、[Remote IP address] も IPv6 アドレスである必要があります。

- f) Remote Port : 1 ~ 65535 の範囲の数値を使用して、セッション用に設定するポートを指定します。
- g) VRF Name : ドロップダウンリストから任意の VRF 名を選択します。

**ステップ 7** [保存 (Save)] をクリックして、デバイスに変更を展開します。

---

## TWAMP ライトレスポンドの設定の編集

既存の TWAMP ライトレスポンド設定を編集するには、次の手順を実行します。

**ステップ 1** [Configuration] > [Network Devices] を選択します。

**ステップ 2** 設定するデバイスのハイパーリンクをクリックしてデバイスを選択し、[デバイスの詳細 (Device Details)] ページを起動します。

**ステップ 3** 左側のタブで、[Logical View] をクリックします。

**ステップ 4** [IP SLA] > [Twamp Light Responder] を選択します。

**ステップ 5** [Session ID] をクリックして、選択したセッションのパラメータを編集します。

(注) [Timeout] のみを変更できます。

**ステップ 6** [保存 (Save)] をクリックして、デバイスに変更を展開します。

---

## TWAMP ライトレスポンド設定の削除

既存の TWAMP ライトレスポンド設定を削除するには、次の手順を実行します。

**ステップ 1** [Configuration] > [Network Devices] を選択します。

**ステップ 2** 設定するデバイスのハイパーリンクをクリックしてデバイスを選択し、[デバイスの詳細 (Device Details)] ページを起動します。

**ステップ 3** 左側のタブで、[Logical View] をクリックします。

**ステップ 4** [IP SLA] > [Twamp Light Responder] を選択します。

**ステップ 5** 削除する [Session ID] の隣にあるチェックボックスをオンにします。

ステップ 6 [X] をクリックし、続いて [Delete] をクリックして、選択した設定の削除を確認してから削除します。

## TWAMP ライトセッションの詳細を表示するコマンド

デバイスでのセッションの詳細を表示するには、次のコマンドを使用します。

コマンド	使用法
<code>show ipsla twamp session</code>	有効になっているすべての TWAMP ライトセッションを一覧表示します。
<code>show running-config ipsla responder twamp-light test-session &lt;test session ID&gt;</code>	特定の TWAMP ライトセッションの詳細を表示します。

## インターフェイスの設定

Cisco EPN Manager を使用すると、次の設定オプションを使用して CE インターフェイスおよび光インターフェイスを設定できます。

インターフェイスを設定する前に、デバイスのインベントリ収集ステータスが [完了 (Completed) ] であることを確認します。

- [イーサネット インターフェイスとサブインターフェイスの設定 \(49 ページ\)](#)
- [ループバック インターフェイスの設定 \(51 ページ\)](#)
- [トンネル インターフェイスの有効化または無効化 \(53 ページ\)](#)
- [スイッチ ポート インターフェイスの設定 \(54 ページ\)](#)
- [イーサネット インターフェイスの設定 \(54 ページ\)](#)
- [仮想テンプレートのインターフェイスの表示 \(55 ページ\)](#)
- [VLAN のインターフェイスの表示 \(56 ページ\)](#)
- [ネットワークチーム \(リンク集約\) の設定](#)
- [ネットワークトラフィックをフィルタ処理するための IP アクセスリストの作成または変更](#)
- [保護プロファイルの設定 \(74 ページ\)](#)
  - [光インターフェイスでのループバック設定の変更 \(57 ページ\)](#)
  - [接続ステータスの継続的な確認 \(58 ページ\)](#)
  - [ODU コントローラ上の PRBS の設定 \(60 ページ\)](#)
  - [OSC の有効化および無効化 \(62 ページ\)](#)



- [光インターフェイスのプロビジョニング \(63 ページ\)](#)
  - [光インターフェイスの管理ステータスの変更 \(72 ページ\)](#)
  - [保護プロファイルの設定 \(74 ページ\)](#)
  - [TCM パラメータと TTI パラメータの設定 \(75 ページ\)](#)
  - [ポートモード/ペイロード設定とブレークアウト設定の変更 \(78 ページ\)](#)
  - [OTN インターフェイスの設定 \(79 ページ\)](#)
  - [GCC 接続の有効化および無効化 \(80 ページ\)](#)
  - [スケルチ モードの設定 \(81 ページ\)](#)
  - [NCS 1004 インターフェイスのスケルチモードとホールドオフタイマーの設定 \(82 ページ\)](#)
- [例：Cisco NCS 2006 インターフェイスの管理ステータスの変更 \(82 ページ\)](#)

## イーサネット インターフェイスとサブインターフェイスの設定

[デバイスの詳細 (Device Details)] ページの [設定 (Configuration)] タブには、デバイスでの現在のインターフェイス設定のリストが表示されます。デバイス設定とユーザーアカウントの権限に応じて、これらのインターフェイスを作成、編集、削除、有効化、無効化できます。

**ステップ 1** 選択項目 **Configuration > Network Devices**.

**ステップ 2** デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details)] ページを起動します。

**ステップ 3** [論理ビュー (Logical View)] タブをクリックします。

**ステップ 4** **Interfaces > Ethernet** を選択します。

**ステップ 5** イーサネット サブインターフェイスを追加するには、次の手順を実行します。

- a) イーサネット インターフェイスを選択し、**Add Subinterface** をクリックします。

**Note** このボタンは、選択するデバイスに応じて有効になります。たとえば Cisco ASR903 デバイスの場合、このボタンは無効です。

- a) [基本設定 (Basic Configuration)] エリアでは、少なくとも [インターフェイス番号 (Interface Number)] に番号を入力し (事前に番号が入力されていない場合)、オプションでサブインターフェイスの説明を入力します。
- b) [VLAN 番号 (VLAN Number)] フィールドに、このサブインターフェイスの VLAN ID を表すのに使用できる数値を入力します。802.1Q タイプのカプセル化だけがサポートされている点に注意してください。
- c) ネイティブ VLAN ID と同じ VLAN 番号を使用するには、[ネイティブ VLAN (Native VLAN)] チェックボックスをオンにします。

- d) [データプレーンループバック (Dataplane Loopback)] ドロップダウンメニューで、ループバック値として設定する必要がある値を選択します。オプションは、[空白 (Blank)] (設定を変更しない)、[なし (None)] (インターフェイスからイーサネットループバックを削除する)、[内部 (Internal)]、および [外部 (External)] です。デバイスですでに設定されている値は、太字で強調表示されます。
- e) IPv4 サブインターフェイスを作成する場合は、[IPv4 インターフェイス (IPv4 Interface)] エリアで [IP タイプ (IP Type)] を選択します。選択できるオプションは、次のとおりです。

- なし
- [スタティック IP (Static IP)] : IP アドレスおよびサブネット マスクを入力します。
- [DHCP IP] : プール名を入力します。
- [DHCP ネゴシエーション (DHCP Negotiated)] : ホスト名およびクライアント ID を入力します ([なし (None)]、[インターフェイス (Interface)]、[ポート チャネル (Port Channel)] )。

また、セカンダリ IP アドレスとマスクを入力できます。

- f) [IPv6 アドレス (IPv6 Address)] エリアで IPv6 サブインターフェイスを追加するには、[追加 (Add)] ドロップダウンリストからタイプを選択します。オプションは [グローバル (Global)]、[アンナンバード (Unnumbered)]、[リンク ローカル (Link Local)]、[自動設定 (Auto Configuration)]、[DHCP] です。

- [グローバル (Global)] : IP アドレスとサブネットマスク、およびタイプ ([一般 (General)]、[EUI-64]、[エニーキャスト (Anycast)]、[CGA]) を入力します。
- [アンナンバード (Unnumbered)] : [アンナンバード インターフェイス (Interface Unnumbered To)] テキストボックスにテキストを入力します。
- [リンク ローカル (Link Local)] : 自動設定または手動設定 (IPv6 アドレスが必要です)。
- [自動設定 (Autoconfiguration)]。
- [DHCP] : アドレスの割り当てのための 2 メッセージ交換を有効にするオプション。

既存のインターフェイスまたはサブインターフェイスを編集する場合は、[インターフェイス番号 (Interface Number)] の値以外のすべての値を変更できます。

**Note** 異常な動作を避けるため、[説明 (Description)] フィールドに \$ 文字を使用しないでください。

- g) [保存 (Save)] をクリックして、デバイスの選択したインターフェイスにサブインターフェイスを追加します。

**ステップ 6** インターフェイスとサブインターフェイスを有効、無効、または削除するには、インターフェイスを選択して該当するボタンをクリックします。

[サブインターフェイスの削除 (Delete Subinterface)] ボタンは、サポートされている一部のデバイス (Cisco ASR903 デバイスなど) でのみ有効になります。

**ステップ 7** [保存 (Save)] をクリックして、デバイスに変更を展開します。

## ループバック インターフェイスの設定

インターフェイスのループバック状態を変更して、光ネットワークのパフォーマンスをテストできます。ループバック設定を変更する前に、デバイスが管理状態であるか、または理想的には完了状態であることを確認してください。

インターフェイスのループバック設定を変更するには、次の手順を実行します。

**ステップ 1** 移行方法 **Configuration > Network Devices**.

**ステップ 2** 設定するデバイスのハイパーリンクをクリックしてデバイスを選択し、[デバイスの詳細 (Device Details)] ページを起動します。

**ステップ 3** [論理ビュー (Logical View)] タブをクリックします。

**ステップ 4** **Interfaces > Loopback** を選択します。

**ステップ 5** 新しいループバック インターフェイスを指定するには、**Add** をクリックします。

- a) [基本設定 (Basic Configuration)] タブで、[ループバック インターフェイス番号 (Loopback Interface Number)] を指定します (事前に入力されていない場合)。
- b) IPv4 ループバック インターフェイスを作成する場合は、[IP タイプ (IP Type)] を指定します。
  - なし。
  - [静的 (Static)]: 静的 IP アドレスと静的 IP アドレスのサブネット マスクを入力します。
  - [DHCP IP]: DHCP プール名を入力します。

また、バックアップループバック インターフェイスとして使用できるように、マスクを使用してセカンダリ IP アドレスを入力することもできます。

- c) IPv6 ループバック インターフェイスを追加する場合は、[IPv6 アドレス (IPv6 Address)] 領域で [追加 (Add)] ドロップダウンリストから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。
  - [グローバル (Global)]: IP アドレス、サブネット マスク、およびタイプ ([一般 (General)], [EUI-64], [エニーキャスト (Anycast)], [CGA]) を指定する必要があります。
  - [アンナンバード (Unnumbered)]: [アンナンバード インターフェイスの宛先 (Interface Unnumbered To)] テキストボックスにテキストを入力する必要があります。
  - [リンク ローカル (Link Local)]: 自動設定または手動設定のいずれかであり、IPv6 アドレスが必要です。
  - Autoconfiguration
  - [DHCP]: アドレスの自動割り当てのための 2 メッセージ交換を有効にするオプションも設定できます。

**ステップ 6** 既存のループバック インターフェイスを編集するには、インターフェイスを選択し、[編集 (Edit)] ボタンをクリックして、速度、デュプレックス、およびその他の設定のみを変更します。インターフェイス番号は編集できません。

**ステップ 7** インターフェイスで上記のループバック設定を有効にするには、必要なループバック プロセスを選択し、[有効にする] をクリックします。

ステップ 8 **Save** をクリックし、これらの変更をデバイス上に展開します。

## IOT インターフェイスの有効化または無効化

[デバイスの詳細 (Device Details)] ページの [設定 (Configuration)] タブには、デバイスでの現在のインターフェイス設定のリストが表示されます。デバイス設定とユーザーアカウントの権限に応じて、IOT インターフェイスを有効または無効にすることができます。これは、EM、C3794、X.21、およびシリアルインターフェイス (RS232、RS485、および RS422) に適用されます。インターフェイスを有効または無効にすると、上記技術に対応するすべてのコントローラのリストが表示されます。



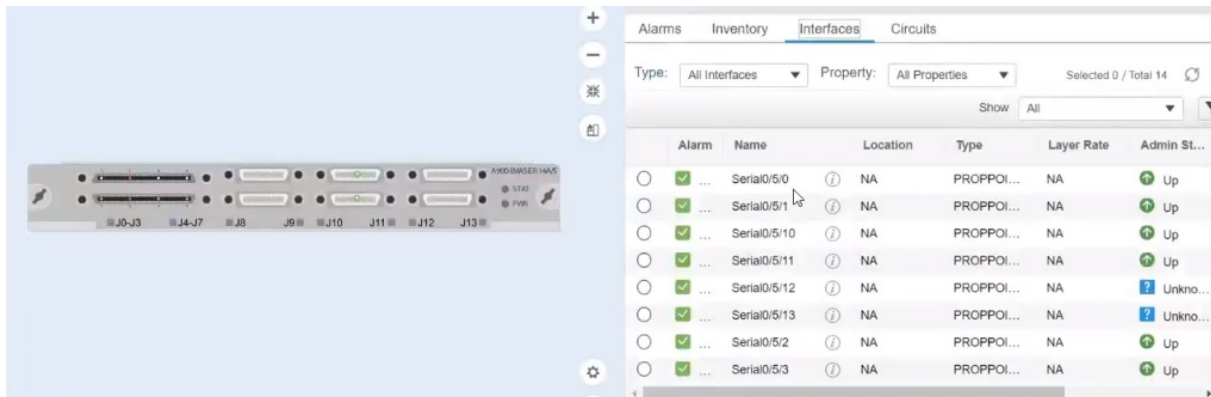
(注) インターフェイスが存在しない場合は、インターフェイスの有効化または無効化のコマンドはデバイスに送信されません。

ステップ 1 選択項目 **Configuration > Network Devices**.

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details)] ページを起動します。

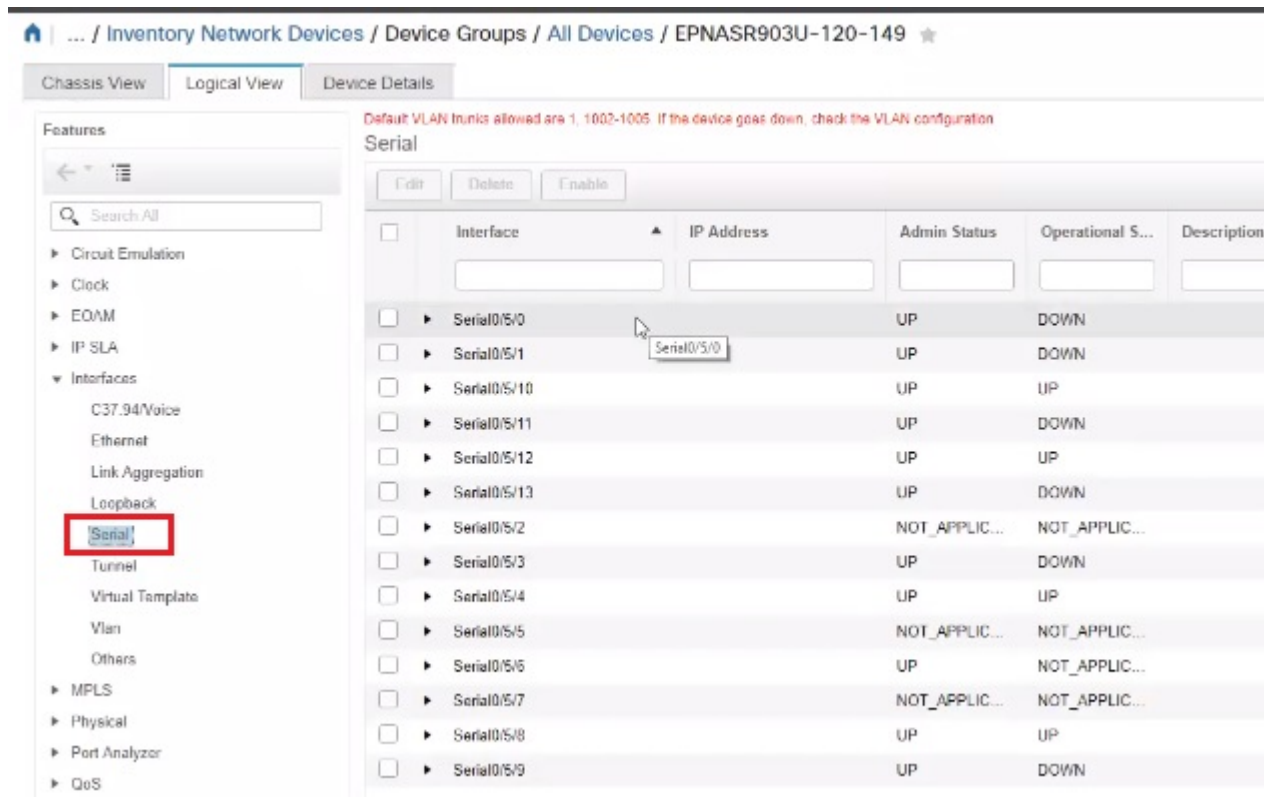
ステップ 3 [シャーシビュー (Chassis View)] タブで、設定されている CEM またはチャンネルグループにリストされているすべてのシリアルコントローラを表示します。

図 1: シャーシビュー (Chassis View)



ステップ 4 [論理ビュー (Logical View)] タブで、すべてのシリアルインターフェイスと、さらに X.21 インターフェイスも表示するか、あるいは有効または無効にします。

図 2: シリアル



ステップ 5 **Interfaces > Serial** を選択します。

ステップ 6 右側のペインで、EPNM でサポートされているシリアルコントローラのすべてのリストを表示し、一度に 1 つのコントローラを確認にして有効にするか、または無効にします。

ステップ 7 **Save** をクリックします。

## トンネル インターフェイスの有効化または無効化

[デバイスの詳細 (Device Details)] ページの [設定 (Configuration)] タブには、デバイスでの現在のインターフェイス設定のリストが表示されます。デバイス設定とユーザーアカウントの権限に応じて、これらのインターフェイスを有効または無効にすることができます。

ステップ 1 選択項目 **Configuration > Network Devices**.

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details)] ページを起動します。

ステップ 3 [論理ビュー (Logical View)] タブをクリックし、左側のメニューから **Interfaces > Tunnel** を選択します。

ステップ 4 トンネル インターフェイスを有効または無効にするには、インターフェイスを選択し、[有効にする (Enable)] または [無効にする (Disable)] ボタンをクリックします。

**Note** MPLSTE トンネルインターフェイスは、ここで有効または無効にすることができます。MPLSTE トンネルの作成または編集については、[MPLS TE トンネルの作成とプロビジョニング](#)を参照してください。

## スイッチポートインターフェイスの設定

[デバイスの詳細 (Device Details)] ページの [設定 (Configuration)] タブには、デバイスでの現在のインターフェイス設定のリストが表示されます。デバイス設定とユーザーアカウントの権限に応じて、これらのインターフェイスを編集、削除、有効化、無効化できます。

**ステップ 1** 選択項目 **Configuration > Network Devices**.

**ステップ 2** デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details)] ページを起動します。

**ステップ 3** [論理ビュー (Logical View)] タブをクリックします。

**Note** [Configuration] タブは、サポートされるデバイスに対してのみ表示されます。

**ステップ 4** **Interfaces > Switch Port** を選択します。

**ステップ 5** インターフェイスを編集するには、インターフェイスを選択し、**Edit** をクリックします。

- 管理モードの選択: [静的 (Static)]、[トンネル 802.1Q]、または [ルーテッド (Routed)]
- ポートの高速設定を有効または無効にし、必要に応じて速度とデュプレックスを調整します。

**ステップ 6** **Save** をクリックします。

## イーサネットインターフェイスの設定

[デバイスの詳細 (Device Details)] ページの [設定 (Configuration)] タブには、デバイスでの現在のインターフェイス設定のリストが表示されます。デバイス設定とユーザーアカウントの権限に応じて、イーサネットインターフェイスを編集、削除、有効化、無効化できます。

### 制限事項

- NCS 4202 および ASR 901 では、メディアタイプ RJ45 ギガビットイーサネットで速度とデュプレックスがサポートされます。
- メディアタイプが設定されていない場合、速度とデュプレックスのドロップダウンは無効になります。
- 他の IOS/XE デバイスタイプの場合、ドロップダウンは無効になり、EPNM から速度とデュプレックスの値を設定することはできません。

- NCS 4202 では、速度が 1 Gig に設定されている場合は全二重オプションのみがサポートされ、10 および 100 Mbps の場合は半二重と全二重の両方がサポートされます。
- ASR 901 では、10、100、1000 Mbps のすべての速度で、半二重および全二重がサポートされます。
- 速度ドロップダウンで [自動 (Auto) ] オプションを選択すると、速度とデュプレックスの両方のドロップダウンに [自動 (Auto) ] が反映され、この場合、ユーザーはネゴシエーションモードを [自動 (Auto) ] に設定できます。
- ドロップダウンから速度とデュプレックスを手動で選択すると、「no negotiation auto」コマンドが適切な速度とデュプレックスの値でデバイスに送信されます。

---

**ステップ 1** 選択項目 **Configuration > Network Devices**.

**ステップ 2** デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details) ] ページを起動します。

**ステップ 3** [論理ビュー (Logical View) ] タブをクリックします。

(注) [Configuration] タブは、サポートされるデバイスに対してのみ表示されます。

**ステップ 4** **Interfaces > Ethernet** を選択します。

**ステップ 5** インターフェイスを編集するには、インターフェイスを選択し、**Edit** をクリックします。

これで、必要な詳細を変更できます。

**ステップ 6** **Save** をクリックします。

---

## 仮想テンプレートのインターフェイスの表示

[デバイスの詳細 (Device Details) ] ページの [設定 (Configuration) ] タブには、デバイスでの現在のインターフェイス設定のリストが表示されます。このページからは、仮想テンプレートのインターフェイスのみを表示できます。インターフェイスを追加、編集、有効化、または無効化することはできません。

---

**ステップ 1** [設定 (Configuration) ] > [ネットワークデバイス (Network Devices) ] を選択します。

**ステップ 2** デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details) ] ページを起動します。

**ステップ 3** [論理ビュー (Logical View) ] タブをクリックします。

**ステップ 4** [インターフェイス (Interfaces) ] > [仮想テンプレート (Virtual Template) ] を選択します。

---

## VLAN のインターフェイスの表示

[デバイスの詳細 (Device Details)] ページの [設定 (Configuration)] タブには、デバイスでの現在のインターフェイス設定のリストが表示されます。このページからは、VLAN のインターフェイスのみを表示できます。インターフェイスを追加、編集、有効化、または無効化することはできません。

**ステップ 1** [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] を選択します。

**ステップ 2** デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details)] ページを起動します。

**ステップ 3** [論理ビュー (Logical View)] タブをクリックします。

**ステップ 4** [インターフェイス (Interfaces)] > [VLAN] を選択します。

## 光インターフェイスの設定

EPN Manager を使用すると、光インターフェイスを設定して、管理設定を変更し、標準的な FEC モードをインターフェイス上で有効にし、ペイロード設定を変更し、ループバック設定を変更できます。これを行うには、デバイスの現在のインターフェイス設定のリストを表示する [デバイスの詳細 (Device Details)] ページの [設定 (Configuration)] タブを使用します。デバイス設定とユーザーアカウントの権限に応じて、これらのインターフェイスを作成、編集、削除、有効化、無効化できます。

光インターフェイスは、次の方法で設定できます。

- [光インターフェイスでのループバック設定の変更 \(57 ページ\)](#)
- [接続ステータスの継続的な確認 \(58 ページ\)](#)
- [ODU コントローラ上の PRBS の設定 \(60 ページ\)](#)
- [OSC の有効化および無効化 \(62 ページ\)](#)
- [未確認アラームの表示および確認応答 \(63 ページ\)](#)
- [光インターフェイスのプロビジョニング \(63 ページ\)](#)
  - [光インターフェイスの管理ステータスの変更 \(72 ページ\)](#)
  - [保護プロファイルの設定 \(74 ページ\)](#)
  - [TCM パラメータと TTI パラメータの設定 \(75 ページ\)](#)
  - [ポートモード/ペイロード設定とブレイクアウト設定の変更 \(78 ページ\)](#)
  - [OTN インターフェイスの設定 \(79 ページ\)](#)
  - [GCC 接続の有効化および無効化 \(80 ページ\)](#)



- スケルチ モードの設定 (81 ページ)
- NCS 1004 インターフェイスのスケルチモードとホールドオフタイマーの設定 (82 ページ)
- 例 : Cisco NCS 2006 インターフェイスの管理ステータスの変更 (82 ページ)

## 光インターフェイスでのループバック設定の変更

インターフェイスのループバック状態を変更して、光ネットワークのパフォーマンスをテストできます。ループバック設定を変更する前に、デバイスが管理状態であるか、または理想的には完了状態であることを確認してください。変更するインターフェイスは、メンテナンス (OOS、MT) 管理状態である必要があります。EPN マネージャでは、SONET、SDH、イーサネット、FC/FICON、および OTN インターフェイス タイプでのみループバック設定を編集できます。

インターフェイスのループバック設定を変更するには、次の手順を実行します。

- ステップ 1** [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] を選択します。
- ステップ 2** デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details)] ページを起動します。
- ステップ 3** [設定 (Configuration)] タブをクリックします。  
Cisco NCS 2000 と Cisco ONS のデバイスでは、この選択は、[デバイスの詳細 (Device Details)] ページの上部にある [論理ビュー (Logical View)] タブの下にあります。
- ステップ 4** [光インターフェイス (Optical Interfaces)] > [メンテナンス (Maintenance)] > [ループバック (Loopback)] を選択します。  
選択したデバイスのインターフェイスがループバック設定と共に表示されます。サポートされていないインターフェイス (データストレージ、OTS、ビデオなど) は表示されません。
- ステップ 5** ループバック設定を編集するには、インターフェイス名 (ハイパーリンク) を選択し、[編集 (Edit)] をクリックして変更を加えます。デバイスが [管理対象 (Managed)] または [完全 (Complete)] の状態で、インターフェイスが [メンテナンス (OOS、MT) (Maintenance (OOS, MT))] 管理状態であることを確認します。
  - [内部 (Internal)] : これは、ターミナルループバックで適用されるのと同じ設定を適用します。
  - [回線 (Line)] : これは、ファシリティループバックで適用されるのと同じ設定を適用します。
  - [ループバックなし (No\_Loopback)] : このオプションを選択すると、ループバックの値がインターフェイスに設定されません。

ループバック状態を変更する前に、まずドロップダウンメニューから [ループバックなし (No\_loopback)] オプションを使用して現在のループバック設定をクリアしてから、選択した設定を再適用してください。
- ステップ 6** [保存 (Save)] をクリックして編集内容を保存します。  
ポップアップ通知によって変更のステータスが通知されます。

- (注) 編集タスクが失敗した場合は、デバイスが[管理 (Managed)]または[完了 (Completed)]の状態にあることを確認し、Cisco EPN Managerがデバイス設定と同期していることを確認します。そうでない場合は、デバイスを Cisco EPN Manager と再同期します。[デバイスのインベントリの即時収集 \(同期\) \(175 ページ\)](#) を参照してください。

## 接続ステータスの継続的な確認

接続確認機能を使用すると、光インターフェイスの電力レベルを表示し、インターフェイスでの接続と挿入損失を確認できます。接続の確認ではケーブルが接続状態にあるかどうかを示され、挿入損失の確認ではケーブル損失が予想値内にあるかどうかを示されます。挿入損失のパラメータは、発生する可能性がある障害を予測するために、ネットワーク要素内の考えられるすべての光パスで収集されます。

Cisco EPN Manager を使用すると、接続確認パラメータを表示することができ、インターフェイスでの接続確認を有効または無効にすることができます。関連付けられているアラームの応答確認の値を設定することもできます。

光インターフェイスの接続ステータスを確認するには、次の手順を実行します。

- ステップ 1** [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] の順に選択します。
- ステップ 2** デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details)] ページを起動します。
- ステップ 3** [設定 (Configuration)] タブをクリックします。  
Cisco NCS 2000 と Cisco ONS のデバイスでは、この選択は、[デバイスの詳細 (Device Details)] ページの上部にある [論理ビュー (Logical View)] タブの下にあります。
- ステップ 4** 接続確認機能を有効または無効にし、共通しきい値を設定するには、[光インターフェイス (Optical Interfaces)] > [プロビジョニング (Provisioning)] > [接続確認 (Connection Verification)] をクリックします。
- ステップ 5** ページの右上隅にある [編集 (Edit)] アイコンをクリックし、共通のパラメータを編集します。
- ステップ 6** 選択したデバイスの次のしきい値パラメータを入力し、[保存 (Save)] をクリックします。
- [接続確認の有効化 (Connection Verification Enabled)] : [はい (True)] または [いいえ (False)] に設定し、選択したデバイス上でこの機能を有効または無効にします。
  - [失敗 IL しきい値 (dB) (Fail IL Threshold (dB))] : 0 ~ 20 の範囲の数値を入力します。このしきい値を超えると、アラームが生成されます。
  - [等級の IL しきい値 (db) (Degree IL Threshold (dB))] : 失敗した IL しきい値より小さい値を入力します。
- ステップ 7** [光インターフェイス (Optical Interfaces)] > [メンテナンス (Maintenance)] > [接続確認エントリ (Connection Verification Entry)] をクリックします。

Cisco NCS 2000 と Cisco ONS のデバイスでは、この選択は、[デバイスの詳細 (Device Details)] ページの上部にある [論理ビュー (Logical View)] タブの下にあります。

**ステップ 8** [A 側 (A Side)] ハイパーリンクをクリックすると、接続の次の値が表示されます。

- [A 側 (A Side)] : 接続確認の開始スロットを表示します。
- [Z 側 (Z Side)] : 接続確認の宛先スロットを表示します。
- [最終更新 (Last Refresh)] : 接続確認と挿入損失の確認が前回実行された日時を表示します。
- [最後の接続変更 (Connectivity Last Change)] : 接続情報が前回変更された日時を表示します。
- [接続確認 (Connectivity Verification)] : 接続のステータスを表示します。
  - [接続済み (Connected)] : ケーブルまたはパッチ コードが接続されています。
  - [切断済み (Disconnected)] : ケーブルまたはパッチ コードは切断されています。
  - [無効 (無効)] : ケーブルまたはパッチ コードは接続確認から除外されています。
  - [未測定 (Not Measurable)] : 電源を検出できません。接続確認でケーブルまたはパッチ コードをテストできません。
  - [未確認 (Not Verified)] : 接続確認でケーブルまたはパッチ コードがテストされていません。
- [過剰な挿入損失 (dB) (Excess Insertion Loss (dB))] : 設定しきい値を超える過剰な挿入損失を表示します。
- [挿入損失の最終変更 (Insertion Loss Last Change)] : 挿入損失の確認情報が前回変更された日時を表示します。
- [表示名 : A と Z 側、A と Z 側モジュール (Display names for- A and Z side, A and Z Side Modules)] : A と Z 側、および A と Z 側モジュールの接続の識別名。
- [Insertion Loss Verification] : 次のいずれかの挿入損失の確認ステータスを表示します。
  - [Not Verified] : ケーブルまたはパッチコードに対して挿入損失の確認がテストされていません (これは最初のブート時のデフォルトステータスです)。
  - [Not Measurable] : 電源を検出できません。ケーブルまたはパッチコードに対して挿入損失をテストできません。
  - [Loss OK] : ケーブルまたはパッチコードの挿入損失は予測値の範囲内です。
  - [Degrade] : ケーブルまたはパッチコードの挿入損失が劣化しています。  
挿入損失が挿入損失の劣化しきい値を超え、挿入損失の障害しきい値よりも小さい場合、パッチコードの挿入損失の確認は [Degrade] になります。[Connection Verification] ペインのパッチコードの対応する行が黄色で強調表示されます。
  - [Fail] : ケーブルまたはパッチコードの挿入損失が不合格しきい値を超えました。この状態が発生すると、GUI でパッチコードが強調表示され、障害状態を示します。

挿入損失が挿入損失の障害しきい値を超えた場合、パッチコードの挿入損失の確認は [Fail] になります。[Connection Verification] ペインのパッチコードの対応する行がオレンジ色で強調表示されます。

- [Disabled] : ケーブルまたはパッチコードは接続確認から除外されています。
- [Acknowledgement] : 関連付けられたアラームの設定値が表示されます。値は True または False に設定できます。

**ステップ 9** [接続確認アクション (Connection Verification Action) ] ドロップダウン メニューで、設定したしきい値に到達したときに実行する必要があるアクションを選択し、[保存 (Save) ] をクリックします。オプションは、[損失と接続の確認 (Verify loss and connectivity) ]、[確認を無効にする (Disable verification) ]、および [損失アラームへの確認応答 (Acknowledge loss alarm) ] です。

**ステップ 10** (オプション) 接続確認パラメータについてアラームの生成方法を指定するには、次のいずれかの値を選択します。

- [損失アラームへの確認応答 (Acknowledge Loss Alarm) ] : アラームを発生させずに、インターフェイスが [失敗 IL しきい値 (Fail IL Threshold) ] のしきい値を超えて動作できるようにします。失敗 IL しきい値がさらに増加する場合は、アラームが再発生します。
- [確認応答のクリア (Clear Acknowledge) ] : [失敗 IL しきい値 (Fail IL Threshold) ] のしきい値がデフォルトに設定され、アラームが再評価されていることを示します。しきい値を超えると、アラームが発生します。

## ODU コントローラ上の PRBS の設定

疑似ランダム バイナリ シーケンス (PRBS) は、選択したオーバーヘッド バイトを使用してヘッダーとトレーラデータを安全に転送できることを確認するためのテストメカニズムです。送信側ノードと受信側ノードの両方が、PRBS テストが行われていることを認識する必要があります。それには Cisco EPN Manager を使用して、これらのノード上で適切な PRBS モードを有効にします。Cisco EPN Manager を使用して PRBS を設定できるのは、光デバイスの非チャネライズド ODU コントローラのみです。

PRBS は PRBS\_31 パターンを生成し、PRBS\_11、PRBS\_23、および PRBS\_31 パターンを検出するために、トランク ポートも有効にします。

**ステップ 1** [設定 (Configuration) ] > [ネットワークデバイス (Network Devices) ] の順に選択します。

**ステップ 2** デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details) ] ページを起動します。

**ステップ 3** [設定 (Configuration) ] タブに移動します。

- NCS 1004 デバイスの場合、このオプションは [シャーシビュー (Chassis View) ] > [設定 (Configuration) ] > [PRBS の設定 (PRBS Configuration) ] で使用できます。ステップ 5 に進みます。

- NCS 4000 デバイスの場合、このオプションは [デバイスの詳細 (Device Details)] ページの左上にある [論理ビュー (Logical View)] タブにあります

**ステップ 4** [光インターフェイス (Optical Interfaces)] > [メンテナンス (Maintenance)] > [PRBS の設定 (PRBS Configuration)] の順に選択します。すべての ODU コントローラとそれらのコントローラの現在の PRBS パラメータが表示されます。コントローラがリストされない場合は、上述の前提条件が満たされていることを確認してください。

**ステップ 5** PRBS を設定するには、コントローラ名のハイパーリンクをクリックし、ページの右上隅にある [編集 (Edit)] アイコンをクリックします。

**ステップ 6** 次のパラメータに変更を加えます。

- [管理状態 (Admin State)] ドロップダウンリストから、ODU コントローラの有効な管理状態を選択します。[00S-MT] (メンテナンス)、[OOS-DSBLD] (無効)、および [IS] (インサービス) の中から選択できます。

PRBS パラメータを編集できるのは、[管理状態 (Admin State)] を [00S-MT] (メンテナンス) 状態に設定した場合のみです。

コントローラの管理状態だけを編集する場合は、PRBS モードを [無効 (Disabled)] に設定し、目的の管理状態を選択します。

- [PRBS テスト (PRBS Test)] の値として [有効 (Enabled)] または [無効 (Disabled)] を選択します。
- コントローラの PRBS モードを選択します。表の 1 列目の値 (以下を参照) を最初のコントローラに設定したら、2 列目で示されている対応する値を 2 番目のコントローラ (ノード 2) に設定します。

コントローラ 1 のモード (ノード 1)	コントローラ 2 のモード (ノード 2)
ソース (Source)	シンク
シンク	ソース (Source)
送信元シンク	Loopback
Loopback	送信元シンク

- [パターン (Pattern)] ドロップダウンリストから、次のいずれかの PRBS パターンを選択します。選択したパターンがラインカードで生成または検出されます。

- NONE
- PN11
- PN23
- PN31
- INVERTEDPN11
- INVERTEDPN31

**ステップ 7** [保存 (Save)] をクリックして、更新後の設定をデバイスに展開します。

**ステップ 8** (オプション) 設定を確認するには、選択したコントローラの [設定 (Configuration) ] タブで [光インターフェイス (Optical Interfaces) ] > [プロビジョニング (Provisioning) ] > [PRBS] を選択して更新後の PRBS パラメータを表示します。ODU UNI 回線に対して PRBS テストを実行するには、[回線 \(ODU UNI\) での PRBS テストの実行](#)を参照してください。

## OSCの有効化および無効化

Cisco EPN Manager を使用して、光デバイスのインターフェイス上で光サービスチャンネル (OSC) の終端を有効または無効にします。OSC は OC3 回線と、次のカードの FastEthernet (FSTE) インターフェイスおよび GigabitEthernet (GigE) インターフェイス上で設定できます。

- 伝送ネットワーク制御システム (TNCS)
- 転送ノード コントローラ : 拡張 (TNCE)
- 転送ノード コントローラ (TNC)

ONS15454NE の場合、サポートされているインターフェイスは次のカードの OC3 インターフェイスです。

- 光サービス チャンネル モデム (OSCM)
- 光サービス チャンネルおよびコンバイナ/セパレータ モジュール (OSC-CSM)

光デバイスで OSC を設定するには、次の手順を実行します。

- ステップ 1** [設定 (Configuration) ] > [ネットワークデバイス (Network Devices) ] の順に選択します。
- ステップ 2** デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details) ] ページを起動します。
- ステップ 3** [設定 (Configuration) ] タブをクリックします。  
Cisco NCS 2000 と Cisco ONS のデバイスでは、この選択は、[デバイスの詳細 (Device Details) ] ページの上部にある [論理ビュー (Logical View) ] タブの下にあります。
- ステップ 4** [光インターフェイス (Optical Interfaces) ] > [通信チャンネル (Comm Channel) ] を選択します。  
選択したデバイスの設定可能なすべての G709 対応インターフェイスが表示されます。
- ステップ 5** [OSC] タブをクリックします。
- ステップ 6** 通信チャンネルの名前のハイパーリンクをクリックして、設定する通信チャンネルを選択します。  
通信チャンネル名と現在の OSC 設定が表示されます。
- ステップ 7** ページの右上にある [編集 (Edit) ] アイコンをクリックします。
- ステップ 8** [OSC] チェックボックスを使用して、選択した通信チャンネルで [OSC] を有効または無効にします。
- ステップ 9** [保存 (Save) ] をクリックします。

変更が保存され、更新された設定がデバイスに展開されます。確認するには、[光インターフェイス (Optical Interfaces)] > [プロビジョニング (Provisioning)] > [通信チャネル (Comm Channel)] の下に選択した通信チャネルの OSC 設定を表示します。

## 未確認アラームの表示および確認応答

デバイスで生成されたアラームに基づいて、未確認ステータスのアラームの詳細を表示し、デバイス上で未読アラーム通知として表示されなくなるように [確認応答済み (Acknowledged)] としてマークできます。手順は次のとおりです。

- ステップ 1** [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] の順に選択します。
- ステップ 2** デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details)] ページを起動します。
- ステップ 3** [設定 (Configuration)] タブをクリックします。  
Cisco NCS 2000 と Cisco ONS のデバイスでは、この選択は、[デバイスの詳細 (Device Details)] ページの上部にある [論理ビュー (Logical View)] タブの下にあります。
- ステップ 4** [光インターフェイス (Optical Interfaces)] > [メンテナンス (Maintenance)] > [未確認アラーム (Unverified Alarms)] を選択して、[未確認 (Unverified)] ステータスのアラームを表示します。
- ステップ 5** アラームを確認し、必要なアクションを実行したら、アラームを選択し、[確認応答済み (Acknowledged)] ボタンをクリックして、これらのアラームを直接デバイス上で [確認済み (Verified)] とマークします。

## 光インターフェイスのプロビジョニング

Cisco EPN Manager を使用して次の設定オプションを光デバイスで有効にすることができます。



- (注) 選択したデバイスに応じて、次の設定オプションが有効または無効になります。デバイスがこれらのオプションをサポートしているかどうかを確認するには、「[Cisco EPN マネージャ用のサポートされているデバイス](#)」を参照してください。

### • イーサネット MTU

Cisco EPN Manager を使用すると、光デバイスのイーサネットインターフェイス上に MTU 値を設定できます。MTU は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) です。Cisco EPN Manager を使用して、TNC モジュールと ECU モジュールのギガビットイーサネットインターフェイスと高速イーサネットインターフェイスを除くすべてのイーサネットインターフェイスの MTU 値を変更できます。

新しいイーサネット MTU 値がデバイスに設定されていることを確認するには、デバイスの [デバイスの詳細 (Device Details)] ページに移動し、[イーサネットインターフェイス (Ethernet Interface)] タブをクリックします。

## • GMPLS

Generalized Multi-Protocol Label Switching (GMPLS) を使用すると、GMPLS 回線の作成時に使用される光ファイバと異種波長パラメータを定義および表示できます。これは、MPLS プロトコル上のパケットベースのデータを網羅し、ネットワーク間でのチャンネルの作成と保守を可能にします。非パケットスイッチングデバイスがサポートされています。つまり、GMPLS はパケットベースの MPLS プロトコルを拡張して、非パケットスイッチングデバイスで構成されるネットワーク間でトンネルの作成と保守を可能にします。GMPLS トンネルは、時分割多重 (TDM) インターフェイスとスイッチングタイプを横断できます。

GMPLS を設定するには、Cisco EPN Manager の [設定 (Configuration) ] タブを使用します。このタブでは、すべての LMP 対応光コントローラで GMPLS を設定できます。GMPLS 設定の前提条件である LMP の有効化も同じ [設定 (Configuration) ] タブを使用して実行できます。



**注** アクティブな光回線の一部である LMP 対応コントローラでは、GMPLS を無効にすることはできません。

## • パケット終端

Cisco EPN Manager を使用すると、光デバイスの ODU コントローラでパケット終端を設定できます。これを行うには、イーサネットパケットのデバイスでパケット終端が事前に設定されていることを確認します。その後、デバイスで既に作成され、Cisco EPN Manager によって検出された設定を編集できます。

パケット終端を設定するには、[終端モード (Termination Mode) ] と [マッピングモード (Mapping Mode) ] の両方の値を指定する必要があります。

## • LMP

リンク管理プロトコル (LMP) は、ルーティング、シグナリング、およびリンク管理を行うために、ノード間で必要なチャンネルとリンクを管理するのに役立ちます。また、LMP は、トラフィックエンジニアリング (TE) リンクの管理にも使用されます。これにより、ノードのペア間で実行する単一のトラフィック エンジニアリング (TE) リンクに複数のデータ リンクを使用できます。

Cisco EPN Manager を使用して LMP ネイバーを作成するには、ネイバーの名前、リンク ID、ルータ ID、およびインターフェイス ID と、共通リンクおよびインターフェイス ID を指定する必要があります。光デバイスにコントローラごとに追加できる LMP リンクは 1 つだけです。

LMP が効果的に動作できるように Cisco EPN Manager を使用して単一のデバイスに LMP 設定を正常に展開できますが、リンクに参加している両方のデバイスセットで LMP を設定する必要があります。これにより、LMP リンクがアクティブになります。

制限事項：



- LMP リンクの作成後は [番号 (Numbering)] の値を編集することはできません。[番号 (Numbering)] の値を編集するには、LMP リンクを削除してから、新しい [番号 (Numbering)] の値で再作成します。
- 2つの LMP ネイバー間でネイバー ルータの ID を重複させることはできません。
- LMP リンクを追加する場合は、コントローラが別の LMP リンクにまだ関連付けられていないことを確認します。関連付けられていると、展開が失敗する原因となります。

#### • OTN トポロジ

[設定 (Configuration)] タブを使用して、光 OTN コントローラに関連付けられているトポロジインスタンスとエリア ID を追加または変更できます。コントローラに事前に構成されたトポロジインスタンスとエリア ID がない場合、Cisco EPN Manager はトポロジインスタンスを OTN に、エリア ID を 0 に設定します。

Cisco EPN Manager では、他のコントローラで事前に設定されているのと同じトポロジインスタンスとエリア ID を使用できません。デバイスに事前に設定されているトポロジインスタンスとエリア ID を知るには、[マップ (Maps)] > [ネットワーク トポロジ (Network Topology)] をクリックします。

#### • NNI

光インターフェイスは、ネットワーク ノード インターフェイス (NNI) として機能するように設定できます。NNI は、インターフェイスが他のネットワーク ノードに接続していることを示します。Cisco EPN Manager を使用すると、光デバイスの OTU コントローラで NNI を設定できます。これらのインターフェイスはさらに、送信元ポートと宛先ポートとして機能するように設定できます。

デバイスがトポロジに含まれていない場合、その NNI コントローラを設定すると、エリア ID 0 を持つそのコントローラの OTN トポロジインスタンスが作成されます。

デバイスに存在するすべてのコントローラに対して、コントローラごとに作成できる NNI 設定は 1 つのみです。

注：トポロジインスタンスで事前に設定されている NNI コントローラは削除できません。

#### • ブレークアウト (Breakout)

光デバイスでのブレークアウトを有効にすると、光ファイバとケーブルのマルチレーンアーキテクチャを使用して、単一の高密度ポートを複数の低密度ポートに分割できます。たとえば、100G ポートは 10 個の異なる 10G ポートとして動作するように設定できます。また、単一の 40G ポートは 4 つの異なる 10G ポートとして機能します。Cisco EPN Manager を使用してブレークアウトを設定するには、次の表を参照してください。

前提条件：

インターフェイスの [ポート モード (Port Mode)] の値を [ブレークアウト (Breakout)] に変更して、インターフェイスにブレークアウトを事前に設定してください。[ポートモード/ペイロード設定とブレークアウト設定の変更 \(78 ページ\)](#) を参照してください。これにより、そのインターフェイスの他のすべてのポートモードパラメータが [なし (None)]

に変更されてポート上でのブレイクアウトが可能になり、レーンを設定できるようになります。インターフェイスごとに最大 10 個のレーンを追加できます。

制限事項：

- 特定のインターフェイスに属するすべてのレーンは、同じマッピングタイプである必要があります。
- OTU2 コントローラと OTU2e コントローラは、パケット終端モードの場合にのみサポートされます。
- Cisco NCS 5.2.4x デバイスでは、ブレイクアウトレーンはポートモードがイーサネットタイプの場合にのみ作成できます。
- OPU2e フレーミングタイプにマップされている 10G クライアントはサポートされていません。
- SONET コントローラと SDH コントローラでは、ブレイクアウトは設定できません。

設定例：

コントローラ オプティクス 0/0/0/0 を選択し、マッピングモードとして GFPF でブレイクアウトを有効にし、フレーム値が OPU2 の場合、デバイスにプッシュされる設定は次のようになります。

```
controller optics 0/0/0/0 breakout-mode 1 ethernet framing opu2 mapping gFpF
```

#### • パフォーマンス モニターリング

パフォーマンスのモニターリング (PM) は、システムの保守とトラブルシューティングのためのパフォーマンスカウンタを収集するのに役立ちます。現在の PM カウンタと履歴 PM カウンタの両方を定期的に取得できます。光デバイスの OTU コントローラと ODU コントローラでパフォーマンスのモニターリングを有効または無効にできます。

TCM コントローラ レベルでパフォーマンスのモニターリングを設定するには、OTN インターフェイスとそれらに関連する TCM パフォーマンスカウンタを設定する必要があります。

- [参考：OTN-FEC インターフェイス用のパフォーマンスカウンタ](#)
- [参考：OTN-ODU インターフェイスのパフォーマンスカウンタ](#)
- [参考：OTN-OTU インターフェイスのパフォーマンスカウンタ](#)

#### • ODU (LO) コントローラのチャネル化：

ODU コントローラを複数の下位 ODU サブコントローラに関連付け、それらの ODU サブコントローラの支流ポート番号 (TPN) と支流スロット (TS) を設定します。TPN の有効な範囲は 1 ~ 80 です。コロン (:) を使用して TS 文字列が区切られている場合、これは個々の支流スロットであることを示します。TS 文字列が半角ダッシュ (-) を使用して区切られている場合、これは支流スロットの範囲を示します。

サブコントローラの ODU レベルを選択する場合は、サブコントローラの ODU レベルが、関連付けるメインコントローラの ODU レベルよりも低くなるようにしてください。たと

例えば、サブコントローラを ODU3 レベルの ODU コントローラと関連付ける場合は、サブコントローラ キャブはレベル ODU2、ODU1、または ODU1 になります。

#### • OTDR の設定 :

この機能を使用すると、修復されたファイバスペンまたは OSC チャンネルの起動時に OTDR スキャンを自動的に開始するように設定できます。これを行うには、[LOS 上の自動スキャン (Auto Scan on LOS)] パラメータが有効になっていることを確認します。ファイバ上の LOS がクリアされ、次の基準に基づいてアラームが発生すると、ファイバは修復するものと見なされます。

- [絶対しきい値を有効にする (Enable Absolute Threshold)] チェックボックスをオンにすると、OTDR スキャンで測定された挿入損失が設定されている [絶対イベント損失しきい値 (db) (Absolute Event Loss Threshold (dB))] の値より大きい場合は「OTDR-LOSS-THR-EXCEEDED」アラームが発生します。
- OTDR スキャンの合計背面反射が指定した [合計背面反射 (db) (Total Back Reflection (dB))] の値より小さい場合。
- [絶対合否基準 (Absolute Pass Fail Criteria)] が無効になっている場合は、前回のリリースの基準からの [損失 (Loss)] と [背面反射 (Back Reflection)] の値がしきい値と見なされます。このシナリオでは、OTDR-LOSS-THR-EXCEEDED アラームが発生します。

自動スキャンをトリガーする方法に応じて、次のパラメータを設定できます。

- [スパン損失増加時の自動スキャン (Auto Scan on Span Loss Increase)] : ファイバ上で測定されたスパン損失が設定されたしきい値より大きい場合、ファイバ上で OTDR スキャンが自動的に開始されます。デフォルトのしきい値は 2 です。
- [Rx 方向での OLR 連続測定を有効にする (Enable OLR continuous measurement on RX direction)] : 設定されたしきい値に応じてカードの LINE-RX ポート (入力) のスパン損失を測定します。
- [WSON プロビジョニングから WDM 側を有効にする (Enable WDM Side from WSON Provisioning)] : OTDR スキャン中に [損失 (Loss)] と [背面反射 (Back Reflection)] のしきい値が交差すると、回線の作成が阻止されます。

ファイバの合計スパン損失が許可されている範囲内に [イベント損失しきい値 (Event Loss Threshold)] の値を設定できます。ファイバ上で測定されたスパン損失がイベント損失しきい値より大きい場合、OTDR スキャンはファイバ上でトリガーされます。

#### • 自動レーザー遮断 (ALS) の設定

自動レーザー遮断 (ALS) は、ファイバの切断などの問題が発生した場合にトランスミッタの出力電力を自動的にシャットダウンするために使用される技術です。ALS がファイバペアの両端にプロビジョニングされていれば、破損したファイバから危険なレベルのレーザー光が漏れるのを防ぐ安全機能になります。インターフェイスがシャットダウンされたら、ALS モードを次のように設定し、インターフェイスを再起動するために実行する必要があります。アクションを設定できます。

- [無効モード (Disabled mode)] : モードが無効になっている場合は、ALS が無効になります。信号消失 (LOS) はレーザーのシャットダウンを引き起こしません。
- [手動再起動モード (Manual restart mode)] : ALS エージェントが 500 ミリ秒にわたる LOS を検出するとレーザーがオフになります。ALS を連動させると、手動コマンドが発行されてパルス幅の期間はレーザーがオンになります。LOS が 100 ms 間解除されていた場合、レーザーがオンになります。
- [自動再起動モード (Automatic restart mode)] : ALS エージェントが 500 ミリ秒にわたる LOS を検出すると、レーザーはパルス間隔の間はシャットダウンされます。その後、選択したパルス幅の期間はレーザーが自動的にオンになります。LOS が依然として存在する場合、レーザーは再びシャットダウンされます。LOS が 100 ms 間解除されるまでこのパターンは継続し、100 ms 間解除されると、レーザーがオンのままになります。

Cisco EPN Manager を使用すると、ALS モード、ALS リカバリ間隔 (秒単位)、およびリカバリパルス幅 (秒単位) を設定できます。インターフェイスの ALS モードが [手動再起動 (Manual Restart)] に設定されている場合は、インターフェイスを手動で再起動する必要があります。これを行うには、デバイスの [デバイスの詳細 (Device Details)] ページに移動し、[光 (Optical)] > [自動レーザー シャットダウン (Automatic Laser Shutdown)] を選択し、[手動再起動 ALS モード (Manual Restart ALS mode)] に設定されたインターフェイスを見つけて、[再起動 (Restart)] ボタンをクリックします。

#### • SNTP サーバーを使用した日付と時刻の設定 :

シンプルネットワークタイムプロトコル (SNTP) は、コンピュータのクロックを基準時刻に同期するために使用されるインターネットプロトコルです。SNTP サーバーを使用すると、すべての NE で同じ日付と時刻の基準が使用されます。サーバーにより、停電やソフトウェアのアップグレード後にノードの時刻が同期されます。

SNTP サーバーを使用して日付と時刻を設定するには、まず現在の時刻とタイムゾーン値を指定してから、日付と時刻の基準ポイントとして使用できるプライマリサーバーとバックアップサーバーを設定する必要があります。タイムゾーン値を設定する前に、SNTP サーバー値が設定されていないことを確認してください。SNTP サーバーを削除する場合は、最初に必ずバックアップサーバーを削除した後でプライマリサーバーを削除します。プライマリサーバーのみを削除することはできません。

#### • 波長の設定 :

Cisco EPN Manager を使用すると、光学コントローラの波長周波数をプロビジョニングできます。光学コントローラで設定された現在の波長を表示した後、選択したカードのタイプに応じて波長周波数を変更できます。

波長は、DWDM 光学ポートとして設定されている場合にも、光学コントローラで設定できます。波長を変更するときは、光ポートを [In Service] 状態にすることはできません。

#### 表 : 光インターフェイスのプロビジョニング

上記の機能を使用して光デバイスを設定するには、次の手順を実行します。

- ステップ 1** [設定 (Configuration) ]>[ネットワークデバイス (Network Devices) ]を選択します。
- ステップ 2** デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details) ] ページを起動します。
- ステップ 3** [設定 (Configuration) ] タブをクリックします。  
Cisco NCS 2000 と Cisco ONS のデバイスでは、この選択は、[デバイスの詳細 (Device Details) ] ページの上部にある [論理ビュー (Logical View) ] タブの下にあります。
- ステップ 4** 次の表に示すように、必要な設定メニューに移動し、必要な値を指定します。

表 8: 表 : 光インターフェイスの設定

タスク	サポートされているインターフェイス/コントローラ	ナビゲーション	注記
イーサネット MTU の設定	TNC モジュールと ECU モジュール上のギガビット/高速イーサネットインターフェイスを除くすべてのイーサネットインターフェイス。	[光インターフェイス (Optical Interfaces) ]> [プロビジョニング (Provisioning) ]> [イーサネット MTU (Ethernet MTU) ]	-
GMPLS の設定	LMP 対応の光コントローラ。	[光インターフェイス (Optical Interfaces) ]> [プロビジョニング (Provisioning) ]> [GMPLS]	-
パケット終端の設定	パケット終端で事前に設定された ODU コントローラ。	[光インターフェイス (Optical Interfaces) ]> [プロビジョニング (Provisioning) ]> [OTN] > [パケット終端 (Packet Termination) ]	イーサネットパケットにのみ適用されます。
LMP ネイバーの設定	すべての光コントローラ。	[光インターフェイス (Optical Interfaces) ]> [プロビジョニング (Provisioning) ]> [LMP]	ネイバー ルータ ID をネイバー間で重複させることはできません
OTN トポロジの設定	すべての光 OTN コントローラ。	[光インターフェイス (Optical Interfaces) ]> [プロビジョニング (Provisioning) ]> [OTN] > [トポロジ (Topology) ]	-

NNI の設定	すべての OTU コントローラ。	[光インターフェイス (Optical Interfaces) ]> [プロビジョニング (Provisioning) ]> [OTN] > [NNI]	-
ブレイクアウトの設定	ポート モードの値を持つすべての光コントローラが「ブレイクアウト」に設定されています。	光インターフェイス>プロビジョニング>ポートモード>ブレイクアウトタブ	-
パフォーマンスモニタリングの設定	すべての OTU および ODU コントローラ。	[光インターフェイス (Optical Interfaces) ]> [プロビジョニング (Provisioning) ]> [パフォーマンスモニタリング (Performance Monitoring) ]	-
ODU (LO) コントローラのチャンネル化	すべての ODU コントローラ。	[光インターフェイス (Optical Interfaces) ]> [プロビジョニング (Provisioning) ]> [ODU チャンネル化 (ODU Channelization) ]> [サブコントローラ (Sub-Controllers) ] タブ	-
OTDR の設定	-	[光インターフェイス (Optical Interfaces) ]> [プロビジョニング (Provisioning) ]> [OTDR 設定 (OTDR Settings) ]	-
ALS の設定	すべての ALS サポート対象インターフェイス	[光インターフェイス (Optical Interfaces) ]> [プロビジョニング (Provisioning) ]> [自動レーザーシャットダウン (Automatic Laser Shutdown) ]	-

<p>SNTP を使用した日付と時刻の設定</p>	<p>-</p>	<ul style="list-style-type: none"> <li>• SNTP のプライマリサーバーとバックアップサーバーを指定するには、次の手順を実行します。</li> </ul> <p>[光インターフェイス (Optical Interfaces) ] &gt; [プロビジョニング (Provisioning) ] &gt; [NTP 設定 (NTP Settings) ] を選択します。</p> <ul style="list-style-type: none"> <li>• SNTP で使用できる現在の時刻とタイムゾーンを指定するには、次の手順を実行します。</li> </ul> <p>[光インターフェイス (Optical Interfaces) ] &gt; [プロビジョニング (Provisioning) ] &gt; [タイムゾーン設定 (Time Zone Settings) ] を選択します。</p>	<p>-</p>
<p>波長の設定</p>	<p>すべての光学コントローラ</p>	<p>[光インターフェイス (Optical Interfaces) ] &gt; [プロビジョニング (Provisioning) ] &gt; [波長 (Wavelength) ]</p>	<p>-</p>
<p>TCM と TTI の設定</p>	<p>-</p>	<p><a href="#">TCMパラメータとTTIパラメータの設定 (75ページ)</a> を参照してください</p>	<p>-</p>
<p>保護プロファイルの設定</p>	<p>-</p>	<p><a href="#">保護プロファイルの設定 (74ページ)</a> を参照してください</p>	<p>-</p>
<p>ペイロードとブレイクアウトの設定</p>	<p>-</p>	<p><a href="#">ポートモード/ペイロード設定とブレイクアウト設定の変更 (78ページ)</a> を参照してください</p>	<p>-</p>

管理ステータスの設定	-	光インターフェイスの管理ステータスの変更 (72 ページ) を参照してください	-
FEC モードの設定	-	OTN インターフェイスの設定 (79 ページ) を参照してください	-
GCC の有効化と無効化	-	参照 GCC 接続の有効化および無効化 (80 ページ)	-
スケルチモードの設定	-	参照 スケルチモードの設定 (81 ページ)	-

### 光インターフェイスの管理ステータスの変更

Cisco EPN Manager を使用すると、インターフェイスの管理状態を変更して、光ネットワークのパフォーマンステスト能力を向上させることができます。インターフェイスの管理ステータスは、インターフェイスが Cisco EPN Manager によって管理されているか、ダウンしているか、またはメンテナンスモードになっているかを定義します。インターフェイスの管理ステータスがダウンの場合は、そのインターフェイスが到達不能状態であるか、またはデバイスが Cisco EPN Manager でサポートされていないことを示します。管理ステータスを [動作中 (Up)] に変更すると、Cisco EPN Manager でインターフェイスを管理できるため、より優れた監視機能が提供されます。インターフェイスの管理状態を変更するには、次の手順を実行します。

**ステップ 1** [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] を選択します。

**ステップ 2** デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details)] ページを起動します。

**ステップ 3** [設定 (Configuration)] タブをクリックします。

Cisco NCS 2000 と Cisco ONS のデバイスでは、この選択は、[デバイスの詳細 (Device Details)] ページの上部にある [論理ビュー (Logical View)] タブの下にあります。

**ステップ 4** [光インターフェイス (Optical Interfaces)] > [プロビジョニング (Provisioning)] > [管理ステータス (Admin Status)] を選択します。

選択したデバイスのインターフェイスが、管理状態の設定と共に表示されます。管理状態を変更できないインターフェイス (PCHAN インターフェイスや PLINE インターフェイスなど) は表示されません。

**ステップ 5** [光コントローラ (Optical Controllers)] タブまたは [イーサネット コントローラ (Ethernet Controllers)] タブをクリックして、必要なコントローラを編集します。

**ステップ 6** 管理ステータスを編集するには、インターフェイスの名前ハイパーリンクをクリックしてインターフェイスを選択し、ページの右上隅にある [編集 (Edit)] アイコンをクリックします。デバイスのインベントリ収集ステータスが [管理 (Managed)] か [完了 (Completed)] であることを確認します。



次の値のいずれかを選択します。

- a) [ダウン (DOWN) ]: インターフェイスが管理上はダウンすることを意味します。
- b) [動作中 (UP) ]: インターフェイスが管理上は動作していることを意味します。
- c) [テスト中 (TESTING) ]: インターフェイスはメンテナンス状態であり、管理者がインターフェイスを使用してテストを実行していることを意味します。

**ステップ 7** [保存 (Save) ] をクリックして保存して、変更をデバイスに展開します。

ポップアップ通知によって変更のステータスが通知されます。Cisco NCS2K デバイス上で変更される管理ステータスの例を確認するには、例: [Cisco NCS 2006 インターフェイスの管理ステータスの変更 \(82 ページ\)](#) を参照してください。

(注) 編集タスクが失敗した場合は、デバイスが [管理 (Managed) ] または [完了 (Completed) ] の状態にあることを確認し、Cisco EPN Manager がデバイス設定と同期していることを確認します。そうでない場合は、[デバイスのインベントリの即時収集 \(同期\) \(175 ページ\)](#) の説明に従って、デバイスを Cisco EPN Manager と再同期します。

## シャーシビューでの光インターフェイスの管理ステータスの変更

Cisco EPN Manager を使用すると、インターフェイスの管理状態を変更して、光ネットワークのパフォーマンステスト能力を向上させることができます。インターフェイスの管理ステータスは、インターフェイスが Cisco EPN Manager によって管理されているか、ダウンしているか、またはメンテナンスモードになっているかを定義します。インターフェイスの管理ステータスがダウンの場合は、そのインターフェイスが到達不能状態であるか、またはデバイスが Cisco EPN Manager でサポートされていないことを示します。管理ステータスを [動作中 (Up) ] に変更すると、Cisco EPN Manager でインターフェイスを管理できるため、より優れた監視機能が提供されます。インターフェイスの管理状態を変更するには、次の手順を実行します。

### 始める前に

**ステップ 1** [設定 (Configuration) ] > [ネットワークデバイス (Network Devices) ] を選択します。

**ステップ 2** デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details) ] ページを起動します。

**ステップ 3** [シャーシビュー (Chassis View) ] ウィンドウで、[設定 (Configuration) ] タブをクリックし、[回線 (Line) ] をクリックします。

Cisco NCS 2000 と Cisco ONS のデバイスでは、この選択は、[デバイスの詳細 (Device Details) ] ページの上部にある [論理ビュー (Logical View) ] タブの下にあります。

**ステップ 4** 管理ステータスを編集するには、インターフェイスの名前ハイパーリンクをクリックしてインターフェイスを選択し、ページの右上隅にある [編集 (Edit) ] アイコンをクリックします。デバイスのインベントリ収集ステータスが [管理 (Managed) ] か [完了 (Completed) ] であることを確認します。

次の値のいずれかを選択します。

- a) [ダウン (DOWN) ]: インターフェイスが管理上はダウンすることを意味します。

- b) [動作中 (UP) ]: インターフェイスが管理上は動作していることを意味します。
- c) [テスト中 (TESTING) ]: インターフェイスはメンテナンス状態であり、管理者がインターフェイスを使用してテストを実行していることを意味します。
- d) [動作および使用中 (UP AINS) ]: インターフェイスが管理上は動作し、使用中であることを意味します。

(注) [動作および使用中 (UP AINS) ]ステータスは、シャーシビューにのみ表示されます。

**ステップ 5** [保存 (Save) ]をクリックして保存して、変更をデバイスに展開します。

ポップアップ通知によって変更のステータスが通知されます。

(注) 編集タスクが失敗した場合は、デバイスが[管理 (Managed) ]または[完了 (Completed) ]の状態にあることを確認し、Cisco EPN Managerがデバイス設定と同期していることを確認します。そうでない場合は、[デバイスのインベントリの即時収集 \(同期\) \(175 ページ\)](#) の説明に従って、デバイスを Cisco EPN Manager と再同期します。

## 保護プロファイルの設定

Cisco EPN Manager を使用すると、光デバイスに異なる保護プロファイル (またはグループ) をプロビジョニングできます。これにより、これらのデバイスの可用性が確保され、信頼性が向上します。保護プロファイルは、カードで自動保護スイッチング (APS) を有効にする必要があるかどうかを定義し、また、障害発生時のトラフィックフローの方向も設定します。デバイス上のカードは、設定の単方向の再生成をサポートするように設定することも、送信チャネルと受信チャネルのいずれかに障害が発生した場合に、両方のチャネルが切り替わるように設定することもできます。

**ステップ 1** [設定 (Configuration) ]>[ネットワークデバイス (Network Devices) ]を選択します。

**ステップ 2** デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details) ] ページを起動します。

**ステップ 3** [デバイスの詳細 (Device Details) ] ページの上部にある [論理ビュー (Logical View) ] タブをクリックします。

**ステップ 4** [光インターフェイス (Optical Interfaces) ]>[プロビジョニング (Provisioning) ]>[保護プロファイル (Protection Profile) ] を選択します。

**ステップ 5** 保護プロファイルを追加するには、[+] 記号をクリックします。

**ステップ 6** 保護プロファイルに一意の名前を指定します。この名前は必須フィールドであり、最大 32 文字で、スペースを含めることはできません。

**ステップ 7** 保護プロファイルに必要な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。

- [1 + 1 BDIR APS (One plus one BDIR APS) ]: 1 + 1 の自動保護切り替え (APS) を有効にし、カードを双方向に設定します。
- [1 + 1 UNIDIR APS (One plus one UNIDIR APS) ]: 1 + 1 の自動保護切り替え (APS) を有効にし、カードを単方向に設定します。

- [1 + 1 UNIDIR NO APS (One plus one UNIDIR NO APS) ] : APS なしに 1 + 1 を有効にし、カードを単方向に設定します。
- [1 + 1 PLUS R BIDIR APS (One plus one PLUS R BIDIR APS) ] : 1 + 1 + R の APS を有効にし、カードを双方向に設定します。

- (注)
- BDIR (双方向) は、送信チャネルと受信チャネルのどちらかに障害が発生した場合に、その両方が切り替わることを意味します。
  - UNIDIR (単方向) は、カードが単方向の設定の再生成をサポートしていることを意味します。したがって、ポートが送信ポートである場合はリンクの送信元として、受信ポートである場合はリンクの宛先としてのみポートを使用できます。

**ステップ 8** プロファイルの保護モードを[元に戻す]または[非リバーティブ]として選択します。リバースモードは、[復元の待機時間 (Wait to Restore Time) ]として指定した (ステップ 9) 時間が経過した後、障害状態をポストした現用ポートに対してノードがトラフィックを戻すようにします。

**ステップ 9** サブネットワークの接続モードを [SNC\_N] (デフォルト) 、[SNC\_I]、または [SNC\_S] として選択します。

**ステップ 10** サブネットワークの接続モードを [SNC\_S] として選択すると、TCM ドロップダウンリストから TCM-ID 値を選択できます。デフォルトでは、サブネットワーク接続モードとして [SNC\_S] を選択すると、TCM-4 が選択されます。[TCM-ID] 列値は、SNC\_S の場合、[TCM4] から [TCM1] ~ [TCM6] に変更できます。

- (注) [SNC\_I] と [SNC\_N] の場合、[TCM-ID] 値を変更することはできません。[なし (None) ] に設定する必要があります。

**ステップ 11** 0 ~ 720 の数値を使用して、[復元の待機時間 (Wait to Restore Time) ] を秒単位で入力します。0 より大きい値の場合、値は 300 より大きく、30 秒間隔で指定してください。復元の待機時間は、回線が復元されるまで待機する必要がある時間を定義します。保護モードに[元に戻す (Revertive) ]を選択した場合、デフォルトの復元の待機時間は 300 で、それ以外は 0 です。

**ステップ 12** [保留時間 (Hold Off Time) ] の値をミリ秒単位で入力します。この値は、システムが代替パスに切り替えるまで待機する時間を定義します。有効な範囲は 100 ~ 10000 秒です。デフォルト値は 0 です。

**ステップ 13** [保存 (Save) ] をクリックして、更新後の変更内容をデバイスに展開します。

**ステップ 14** (オプション) 設定を確認するには、選択したコントローラの [設定 (Configuration) ] タブで [光インターフェイス (Optical Interfaces) ] > [プロビジョニング (Provisioning) ] > [保護プロファイル (Protection Profile) ] を選択して更新後の保護プロファイルパラメータを表示します。

- (注) 上記の手順は、NCS2K デバイスには適用されません。

## TCM パラメータと TTI パラメータの設定

Cisco EPN Manager を使用すると、ODU トンネル 回線の ODU コントローラでタンデム接続モニタリング (TCM) とトレイルトレース識別子 (TTI) を設定できます。これにより、これらのコントローラでのパフォーマンス監視機能を有効または無効にすることができます。

これらのODUコントローラのTCM接続に信号障害と信号劣化のしきい値を設定することで、デバイスの機能をさらに監視できます。また、送信元および宛先のアクセスポイント識別子を変更することもできます。これを行うには、次の前提条件が満たされていることを確認してください。

始める前に

- デバイスのインベントリ収集ステータスが [完了 (Completed) ]であることを確認します。
- コントローラがループバック用に設定されていることを確認します。そうでない場合は、**[光インターフェイス (Optical Interfaces) ]>[メンテナンス (Maintenance) ]>[ループバック (Loopback) ]**でコントローラのループバック設定を変更します。[ループバックインターフェイスの設定 \(51 ページ\)](#) を参照してください。



(注) ODU UNI 回線のエンドポイントでは、TCM は OTUx-ODUx コントローラでのみサポートされています。

- ステップ 1** [設定 (Configuration) ]>[ネットワークデバイス (Network Devices) ]を選択します。
- ステップ 2** デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details) ] ページを起動します。
- ステップ 3** [設定 (Configuration) ] タブをクリックします。  
Cisco NCS 2000 と Cisco ONS のデバイスでは、この選択は、[デバイスの詳細 (Device Details) ] ページの上部にある [論理ビュー (Logical View) ] タブの下にあります。
- ステップ 4** TCM/TTI パラメータを設定するには、**[光インターフェイス (Optical Interfaces) ]>[プロビジョニング (Provisioning) ]>[TCM の設定 (TCM Configuration) ]** を選択します。  
または、デバイスの [シャーシビュー (Chassis View) ] タブに移動し、シャーシエクスプローラからカードを選択して [設定 (Configuration) ] タブをクリックし、[OTN]>[トレース識別子 (Trail Trace Identifier) ] を選択します。  
(注) NCS2K デバイスの TCM パラメータを設定するには、デバイスの [シャーシビュー (Chassis View) ] タブに移動し、シャーシエクスプローラからカードを選択して [設定 (Configuration) ] タブをクリックし、[OTN]>[トレールトレース識別子 (Trail Trace Identifier) ] を選択します。
- ステップ 5** リストに表示されているコントローラのいずれかの TCM パラメータを表示または編集するには、そのコントローラの [TCM ID] ハイパーリンクをクリックします。
- ステップ 6** これらのパラメータを編集するには、ページの右上隅にある [編集 (Edit) ] アイコンをクリックします。
- ステップ 7** 次の TCM パラメータに変更を加えます。

編集可能な TCM パラメータ	説明
状態 (State)	デバイス上の TCM プロパティの状態を有効または無効に設定します。

編集可能な TCM パラメータ	説明
信号障害のしきい値 (Signal Failure Threshold)	ODUk コントローラの信号障害のしきい値を設定します。値は E6、E7、E8、および E9 です。
送信済み API (Sent API)	TTI の送信元アクセス ポイント識別子を設定します。 最大 14 バイト長の値を入力します。
送信済み DAPI (Sent DAPI)	TTI の宛先アクセス ポイント識別子を設定します。最大 14 バイト長の値を入力します。
送信済み演算子固有文字列型 (Sent Operator Specific String Type)	TTI の演算子固有文字列の型を 16 進数または ASCII 型として設定します。
送信済み演算子固有文字列 (Sent Operator Specific String)	TTI の演算子固有文字列を設定します。 最大 32 文字の長さの値を入力します。
パフォーマンス モニター (Performance Monitor)	ODUk コントローラのパフォーマンス監視を有効または無効にします。
信号劣化のしきい値	信号劣化のしきい値を設定します。 値は E6、E7、E8、および E9 です。
予測 SAPI (Expected SAPI)	TTI の現在の送信元アクセス ポイント識別子を設定します。 最大 14 バイト長の値を入力します。
予測 DAPI (Expected DAPI)	TTI の現在の宛先アクセス ポイント識別子を設定します。 最大 14 バイト長の値を入力します。
予測演算子固有文字列型 (Expected Operator Specific String Type)	TTI の演算子固有文字列の型を 16 進数または ASCII 型として設定します。
予測演算子固有文字列 (Expected Operator Specific String)	TTI の演算子固有文字列を設定します。 最大 32 文字の長さの値を入力します。

**ステップ 8** [保存 (Save)] をクリックして、更新後の設定をデバイスに展開します。

**ステップ 9** (オプション) 設定を確認するには、[設定 (Configuration)] タブで [光インターフェイス (Optical Interfaces)] > [プロビジョニング (Provisioning)] > [TCM の設定 (TCM Configuration)] を選択し、選択したデバイスの TCM パラメータを表示します。

**ステップ 10** (オプション) これらの更新後の TCM パラメータと TTI パラメータは、選択したデバイスの [デバイスの詳細 (Device Details)] とポート 360 ビューで表示できます。 [デバイスの詳細の表示](#) および [特定のデバイスのインターフェイスを表示する : \[デバイス 360 \(Device 360\)\] ビュー](#) を参照してください。

**ステップ 11** (オプション) TCM パラメータは、ネットワーク トポロジ オーバーレイにも表されます。これらのパラメータを表示するには、[マップ (Map)] > [ネットワーク トポロジ] に移動し、関連付けられたこれらの TCM パラメータを持つ光回線を選択します。

## ポートモード/ペイロード設定とブレイクアウト設定の変更

[デバイスの設定 (Device Configuration)] タブを使用すると、SONET インターフェイスと SDH インターフェイス上のパケットのペイロードのタイプを表示および変更して、それらのブレイクアウトを有効にすることができます。ペイロード設定を変更する前に、デバイスが Cisco EPN Manager と同期していることを確認します。光デバイスでのブレイクアウトを有効にすると、光ファイバとケーブルのマルチレーンアーキテクチャを使用して、単一の高密度ポートを複数の高密度ポートに分割できます。たとえば、100G ポートは 10 個の異なる 10G ポートとして動作するように設定できます。また、単一の 40G ポートは 4 つの異なる 10G ポートとして機能します。

インターフェイス上のペイロードとブレイクアウト設定を変更するには、次の手順を実行します。

- 
- ステップ 1 [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] を選択します。
  - ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details)] ページを起動します。
  - ステップ 3 [デバイスの詳細 (Device Details)] ページの上部にある [論理ビュー (Logical View)] タブをクリックします。
  - ステップ 4 [光インターフェイス (Optical Interfaces)] > [プロビジョニング (Provisioning)] を選択します。
  - ステップ 5 選択したデバイスのタイプに応じて、[ペイロードタイプ (Payload Type)] または [ポートモード (Port Mode)] を選択します。
  - ステップ 6 変更するインターフェイスの名前 (ハイパーリンク) をクリックします。  
名前やそのペイロードタイプなどのインターフェイスの共通プロパティが表示されます。
  - ステップ 7 変更する OTN インターフェイスの名前 (ハイパーリンク) をクリックし、[編集 (Edit)] アイコンをクリックします。
  - ステップ 8 [ポートモード (Port Mode)]、[フレーミング (Framing)]、[マッピングタイプ (Mapping Type)]、[レート (Rate)]、および [ビットレート (Bit Rate)] の値を変更します。これらの値がカードの帯域幅制限を超えないようにしてください。
  - ステップ 9 このインターフェイス上のイーサネットパケットと OTN パケットのブレイクアウトレーンを関連付けるには、[ブレイクアウト (Breakout)] タブをクリックします。このタブは、デバイスにブレイクアウトが事前に設定されている場合にのみ表示されます。
    - a) [+] アイコンをクリックして新しいレーンを追加します。コントローラあたり最大 10 レーンを追加できます。既存のレーンを変更するには、[レーン (Lane)] ハイパーリンクをクリックします。
    - b) ブレイクアウトレーンのレーン番号、ポートモード、マッピングタイプ、所有ポート番号、フレーミング値などのブレイクアウトパラメータを指定します。
  - ステップ 10 [保存 (Save)] をクリックして、変更内容をデバイスに展開します。  
ポップアップ通知によって変更のステータスが通知されます。

(注) 編集タスクが失敗した場合は、インターフェイスが [管理 (Managed)] であることを確認し、Cisco EPN Manager がデバイス設定と同期していることを確認します。そうでない場合は、デバイスを Cisco EPN Manager と再同期します。 [デバイスの変更内容の保存 \(175 ページ\)](#) を参照してください。また、ペイロードがカードの帯域幅制限を超えていないことを確認します。

(注) 手順 6 – 10 は、NCS2K デバイスには適用されません。

## OTN インターフェイスの設定

FEC モードは、OTN 回線の転送エラー修正 (FEC) メカニズムを定義します。転送エラー修正 (FEC) メカニズムはマージンの改善と光リーチの拡張のためにパフォーマンスを向上させます。FEC モード設定を [標準 (Standard)] に変更するには、[デバイスの設定 (Device Configuration)] タブを使用する必要があります。

FEC モード設定を変更する前に、変更しようとしているインターフェイスの管理状態が [ダウン (故障中) (Down (out of service))] で、G709 の設定が有効になっていることを確認してください。G709 の設定を有効にするには、シャーシビューで OTN 回線の設定を使用します。

インターフェイスの FEC モードを変更するには、次の手順を実行します。

- ステップ 1 [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] を選択します。
- ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details)] ページを起動します。
- ステップ 3 [設定 (Configuration)] タブをクリックします。  
Cisco NCS 2000 と Cisco ONS のデバイスでは、この選択は、[デバイスの詳細 (Device Details)] ページの上部にある [論理ビュー (Logical View)] タブの下にあります。
- ステップ 4 [光インターフェイス (Optical Interfaces)] > [プロビジョニング (Provisioning)] を選択します。
- ステップ 5 FEC を [ダウン (Down)] に変更する必要がある OTN インターフェイスの管理状態を変更します。 [光インターフェイスの管理ステータスの変更 \(72 ページ\)](#) を参照してください。
- ステップ 6 デバイス タイプに応じて次のいずれかを選択し、変更するインターフェイスを選択します。

- [OTN 回線 (OTN Lines)] > [OTNFEC]
- [OTN] > [FEC]

選択したデバイスの設定可能なすべての G709 対応インターフェイスが表示されます。

または、デバイスの [シャーシビュー (Chassis View)] タブに移動し、シャーシエクスプローラからカードを選択して [設定 (Configuration)] タブをクリックし、[OTN] > [OTN 回線 (OTN Lines)] を選択します。このオプションを使用すると、同期メッセージの有効化、管理者 SSM の選択、同期提供パラメータの有効化、G709 値の true または false への設定など、追加パラメータを設定できます。

- ステップ 7 編集するインターフェイスを選択し、ウィンドウの右上にある [編集 (Edit)] アイコンをクリックします。



## GCC 接続の有効化および無効化

- ステップ 8** 必要な FEC モードを選択します。デフォルトは [なし (None) ] です。
- ステップ 9** (Cisco NCS 2000 デバイスのみ) 必要な **SDBER** 値を選択します。信号劣化ビットエラーレート (SDBER) の条件は、設定したしきい値に基づき、回線劣化に対して信号劣化アラームが発生することを示します。
- ステップ 10** [保存 (Save) ] をクリックして変更を保存します。
- ポップアップ通知によって変更のステータスが通知されます。
- (注) 編集タスクが失敗した場合は、インターフェイスが [管理 (Managed) ] または [完了 (Completed) ] であることを確認し、Cisco EPN Manager がデバイス設定と同期していることを確認します。また、デバイスで G709 の設定が有効になっていることを確認する必要があります。インターフェイスの管理状態を変更するには、[光インターフェイスの管理ステータスの変更 \(72 ページ\)](#) を参照してください。

## GCC 接続の有効化および無効化

Cisco EPN Manager は、光デバイスのインターフェイス上での汎用通信チャネル (GCC) 接続のプロビジョニングをサポートしています。GCC は、TXP カードまたは MXP カードのトランクポートと OTN、OTU、および ODU コントローラで設定できます。GCC の設定は、インターフェイスで設定された FEC モードと管理ステータスに関係なく変更できます。

光デバイスで GCC を設定するには、次の手順を実行します。

- ステップ 1** [設定 (Configuration) ] > [ネットワークデバイス (Network Devices) ] の順に選択します。すべての Cisco EPN Manager デバイスが表示されます。
- ステップ 2** デバイス名のハイパーリンクをクリックして、設定する光デバイスを選択します。
- ステップ 3** [設定 (Configuration) ] タブをクリックし、[光インターフェイス (Optical Interfaces) ] > [プロビジョニング (Provisioning) ] を選択します。
- ステップ 4** デバイス タイプに応じて次のいずれかを選択します。
- [通信チャネル (Comm Channels) ] > [GCC]
  - [OTN] > [GCC]
- 選択したデバイスの設定可能なすべての G709 対応インターフェイスが表示されます。
- ステップ 5** 編集するコントローラのタイプに基づいて、[OTU コントローラ (OTU Controllers) ] タブまたは [ODU コントローラ (ODU Controllers) ] タブをクリックします。
- ステップ 6** リストに表示されているコントローラのいずれかの GCC の設定を編集するには、コントローラの名前ハイパーリンクをクリックします。
- ステップ 7** ページの右上にある [編集 (Edit) ] アイコンをクリックします。
- ステップ 8** [GCC] チェックボックスを使用し、選択したコントローラの GCC を有効または無効にします。ODU コントローラで設定される値は GCC1 で、OTU コントローラで設定される値は GCC0 です。
- ステップ 9** [保存 (Save) ] をクリックします。変更が保存され、更新された設定がデバイスに展開されます。



設定を確認するには、[光インターフェイス (Optical Interfaces)] > [プロビジョニング (Provisioning)] で、選択したコントローラの GCC パラメータを表示します。

400G-XC トランク ポートを搭載した Cisco NCS デバイス上で GCC を有効にすると、Cisco EPN Manager はトランク ポート間の OUT リンクを検出します。

## スケルチモードの設定

Cisco EPN Manager を使用すると、光デバイスのインターフェイス上に異なるスケルチモードを設定できます。スケルチモードは特定の障害に反応して遠端レーザーをシャットダウンするのに役立ちます。スケルチモードは、OCH、OTN、SONET または SDH、FC または FICON、イーサネット、ビデオ、および光デバイスのデータ ストレージインターフェイスで設定できます。

**ステップ 1** [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] を選択します。

**ステップ 2** デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details)] ページを起動します。

**ステップ 3** [設定 (Configuration)] タブをクリックします。

Cisco NCS 2000 と Cisco ONS のデバイスでは、この選択は、[デバイスの詳細 (Device Details)] ページの上部にある [論理ビュー (Logical View)] タブの下にあります。

**ステップ 4** [光インターフェイス (Optical Interfaces)] > [プロビジョニング (Provisioning)] > [スケルチモード (Squelch Mode)] を選択します。

**ステップ 5** インターフェイスの名前ハイパーリンクをクリックして、設定するインターフェイスを選択します。

インターフェイスの名前と現在のスケルチモード設定が表示されます。

**ステップ 6** ページの右上隅にある [編集 (Edit)] アイコンをクリックします。

**ステップ 7** インターフェイスに必要なスケルチモードを選択します。選択できるオプションは、次のとおりです。

- [無効 (DISABLE)] : スケルチが無効になっています。
- [AIS] : アラーム表示信号 (AIS) が有効になっています。
- [なし (NONE)] : 透過モードが有効になっています。
- [スケルチ (SQUELCH)] : スケルチが有効になっています。
- [ODU\_AIS]
- [G\_AIS] : Generis AIS が有効になっています。
- [NOS] : FC ペイロードでスケルチが無効になっています。
- [LF]

**ステップ 8** [保存 (Save)] をクリックします。

変更が保存され、更新された設定がデバイスに展開されます。確認するには、[光インターフェイス]>[スケルチモード]の下に、選択したインターフェイスのスケルチモードパラメータを表示します。

---

### NCS 1004 インターフェイスのスケルチモードとホールドオフタイマーの設定

スケルチモードは特定の障害に応答して遠端レーザーをシャットダウンするのに役立ちます。NCS 1004 インターフェイスのスケルチモードとホールドオフタイマーを設定するには、次の手順を実行します。

**ステップ 1** [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] を選択します。

**ステップ 2** デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details)] ページを起動します。

**ステップ 3** [Configuration] タブをクリックして [Ethernet] タブを選択します。

**ステップ 4** 編集するインターフェイスを選択して編集アイコンをクリックします。

[Edit Ethernet Controller] ウィンドウが表示されます。

**ステップ 5** ドロップダウンリストから [Squelch Mode] を選択します。

**ステップ 6** [Hold Off Timer] に値を入力します。

ホールドオフ時間の範囲は、0 ~ 3000 ミリ秒です。

**ステップ 7** [Apply] をクリックします。

---

### 例 : Cisco NCS 2006 インターフェイスの管理ステータスの変更

この例では、Cisco NCS 2006 VLINE インターフェイスの管理ステータスを変更する方法を示します。この例では、設定の変更は [デバイスの詳細 (Device Details)] ページから開始されますが、[論理ビュー (Logical View)] タブの下にあります (その他のデバイスでは、[設定 (Configuration)] タブで設定の変更が実行されます)。

**ステップ 1** [論理ビュー (Logical View)] タブの [デバイスの詳細 (Device Details)] ページで、編集するインターフェイスのハイパーリンクをクリックします。

Home | ... / Device Management / Network Devices / Device Group / All Devices ★

Chassis View Logical View **Device Details**

**Features**

Search All

- Optical Interfaces
  - Maintenance
  - Provisioning
    - OTN Lines
      - Adminstatus**
      - Automatic Laser Shutdown
      - Comm Channels
      - Ethernet MTU
      - NTP Settings
      - OTDR Autoscan
      - Payload

**Admin Status**

Optical Controllers Ethernet Controllers

Name	Display Name	Admin Status
<input type="text" value="VLINE"/>	<input type="text"/>	<input type="text"/>
<input type="checkbox"/> VLINE-5-7-1-1-10	VLINE-5-7-1-1-10	UP
<input type="checkbox"/> VLINE-5-7-1-1-11	VLINE-5-7-1-1-11	UP
<input type="checkbox"/> VLINE-5-7-1-1-2	VLINE-5-7-1-1-2	UP
<input type="checkbox"/> VLINE-5-7-1-1-3	VLINE-5-7-1-1-3	UP
<input type="checkbox"/> VLINE-5-7-1-1-6	VLINE-5-7-1-1-6	UP
<input type="checkbox"/> VLINE-5-7-1-1-7	VLINE-5-7-1-1-7	UP

**ステップ2** インターフェイスの [共通プロパティ (Common Properties)] ウィンドウで、ウィンドウの右上隅にある [編集 (Edit)] アイコンをクリックします。

Home | ... / Device Management / Network Devices / Device Group / All Devices ★

Chassis View Logical View **Device Details**

**Features**

Search All

- Optical Interfaces
  - Maintenance
  - Provisioning
    - OTN Lines
      - Adminstatus**
      - Automatic Laser Shutdown
      - Comm Channels

**VLINE-5-7-1-1-10**

Admin Status

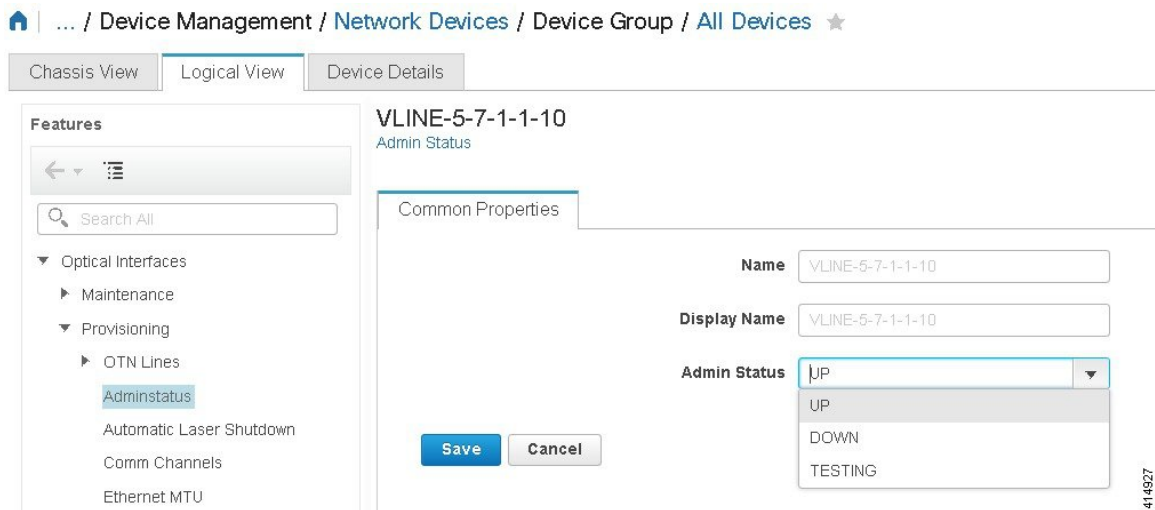
Common Properties

**Name** VLINE-5-7-1-1-10

**Display Name** VLINE-5-7-1-1-10

**Admin Status** UP

**ステップ3** [管理ステータス (Admin Status)] ドロップダウン リストから新しい設定を選択し、[保存 (Save)] をクリックします。

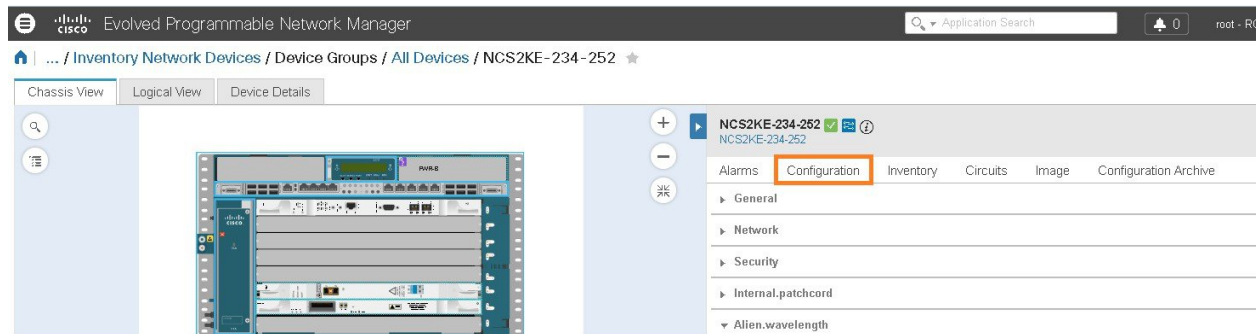


## シャーシビューを使用したデバイスの設定

デバイスのシャーシビューからデバイスとカードを設定できます。これは、シャーシビューの [設定 (Configuration)] サブタブからのみ実行できます。サブタブは、[ネットワーク デバイス (Network Devices)] ページで選択したデバイスのタイプに応じて表示されます。



(注) この機能は Cisco NCS 2000 と Cisco ONS のデバイスでのみ使用できます。



- ステップ 1 左側のサイドバーから、[設定 (Configuration)] > [ネットワークデバイス (Network Devices)] を選択します。
- ステップ 2 デバイス名のハイパーリンクをクリックして、設定するデバイスを選択します。デバイスの [シャーシビュー (Chassis View)] タブが表示されます。
- ステップ 3 右側のペインで、[設定 (Configuration)] サブタブをクリックします。

- ステップ 4** [全般 (General)] 領域を展開した後、ノード名、ノードエイリアスなどのデバイスの詳細を入力し、デバイスをプロビジョニングする場所を選択します。
- ステップ 5** デバイスが関連付けられているコントローラと同期するためのデバイスの同期時間を設定します。NTP/SNTP サーバーの時刻を使用するか、または同期用に手動の日付と時刻を設定できます。
- ステップ 6** デバイスの冷却プロファイルを手動で変更するには、[手動冷却を有効にする (Enable Manual Cooling)] チェック ボックスをオンにします。冷却プロファイルを使用すると、デバイスのシェルフのファンの速度を制御できます。
- ステップ 7** [適用 (Apply)] をクリックします。設定の変更が更新されます。
- ステップ 8** [ネットワーク (Network)] を展開し、変更するネットワーク設定を選択し、[ネットワーク (Network)] 領域の左上にある [編集 (Edit)] アイコンをクリックします。[ネットワークの全般設定の編集 (Edit Network General Settings)] ウィンドウが表示されます。
- ステップ 9** 必要な設定を変更し、[適用 (Apply)] をクリックします。
- (注) デバイスのノードアドレス、ネット/サブネットマスクの長さ、マスク、および MAC アドレスは変更できません。
- ステップ 10** デバイスのセキュリティを設定します。 [デバイスのユーザーおよびユーザー ログインの作成と管理 \(85 ページ\)](#) を参照してください。
- ステップ 11** デバイスの送信側 (TX) と受信側 (RX) のパッチコードを設定します。 [デバイスのパッチコードの設定 \(86 ページ\)](#) を参照してください。
- ステップ 12** デバイスの異種波長を設定します。 [GMPLS および WSON のプロパティの構成 \(98 ページ\)](#) を参照してください。

## デバイスのユーザーおよびユーザー ログインの作成と管理

この手順を使用してユーザーを作成し、デバイスを管理するロールを割り当てます。また、一度にデバイスにアクセスしているユーザーのリストを表示することもできます。

- ステップ 1** 左側のサイドバーから、[設定 (Configuration)] > [ネットワークデバイス (Network Devices)] を選択します。
- ステップ 2** デバイス名のハイパーリンクをクリックして、設定するデバイスを選択します。デバイスの [シャーシビュー (Chassis View)] タブが表示されます。
- ステップ 3** 右側のペインで、[設定 (Configuration)] サブタブをクリックし、[セキュリティ (Security)] 領域を展開します。
- ステップ 4** [ユーザー (User)] タブで、[+] アイコンをクリックしてユーザーを追加します。
- ステップ 5** ユーザー名を入力します。
- ステップ 6** [セキュリティ レベル (Security Level)] ドロップダウン リストから、次のオプションのいずれかを選択します。
- [レトリバー (Retriever)] : このセキュリティ レベルのユーザーは、デバイスから情報を表示および取得できますが、設定を変更することはできません。

- [メンテナンス (Maintenance)] : このセキュリティ レベルを持つユーザーはデバイスから情報を取得して、カードのリセット、相互接続または保護グループ内での手動/強制/ロックアウト、BLSR メンテナンスなどの限られた保守操作を実行できます。
- [プロビジョニング (Provisioning)] : このセキュリティ レベルを持つユーザーは、スーパーユーザーに制限されている操作を除き、すべての保守操作およびプロビジョニングアクションを実行できます。
- [スーパーユーザー (Super User)] : このセキュリティ レベルを持つユーザーは、すべてのプロビジョニングユーザーのアクションに加え、ユーザーセキュリティプロファイルの作成と削除、時刻、日付、ノード名、IP アドレスなどの基本的なシステムパラメータの設定、ならびにデータベースのバックアップと復元を実行できます。

**ステップ 7** パスワードを入力し、[保存 (Save)] をクリックします。ユーザーが [ユーザー (Users)] テーブルに追加されます。

ユーザーを編集または削除するユーザーを選択できます。ただし、ユーザー名は編集できません。また、Cisco EPN Manager にデバイスを追加したユーザーを削除することはできません。

[セキュリティ (Security)] 領域で [ActiveLogins] タブをクリックし、CTC、TL1 セッション、または Cisco EPN Manager を使用してデバイスにログインしたユーザーのリストを表示します。デバイスの最大ログインセッション数に到達すると、1人のユーザーまたは複数のユーザーをログアウトさせることができます。

## デバイスのパッチコードの設定

クライアントカードトランクポートと DWDM フィルタポートは、異なるノードまたは同じ単一シェルフノードまたはマルチシェルフノードに配置できます。クライアントカードトランクポートと DWDM フィルタポートの間には、仮想リンクが必要です。内部パッチコードは、単一シェルフノードまたはマルチシェルフノードのいずれかで、DWDM シェルフの2つの側面の間に仮想リンクを提供します。ただし、パッチコードには双方向性があり、それぞれの方向が別々のパッチコードとして管理されます。

この機能は Cisco NCS 2000 と Cisco ONS のデバイスでのみサポートされています。

この手順では、WDM (波長分割多重化) に ANS (自動ノード設定) を使用して、シャーシビューで内部パッチコードを設定する方法を説明します。シャーシビューを使用して、これらの内部パッチコードを作成および削除できます。デバイスの送信側 (TX) と受信側 (RX) のパッチコードを設定するには、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、[設定 (Configuration)] > [ネットワークデバイス (Network Devices)] を選択します。

**ステップ 2** デバイス名のハイパーリンクをクリックして、設定するデバイスを選択します。デバイスの [シャーシビュー (Chassis View)] タブが表示されます。

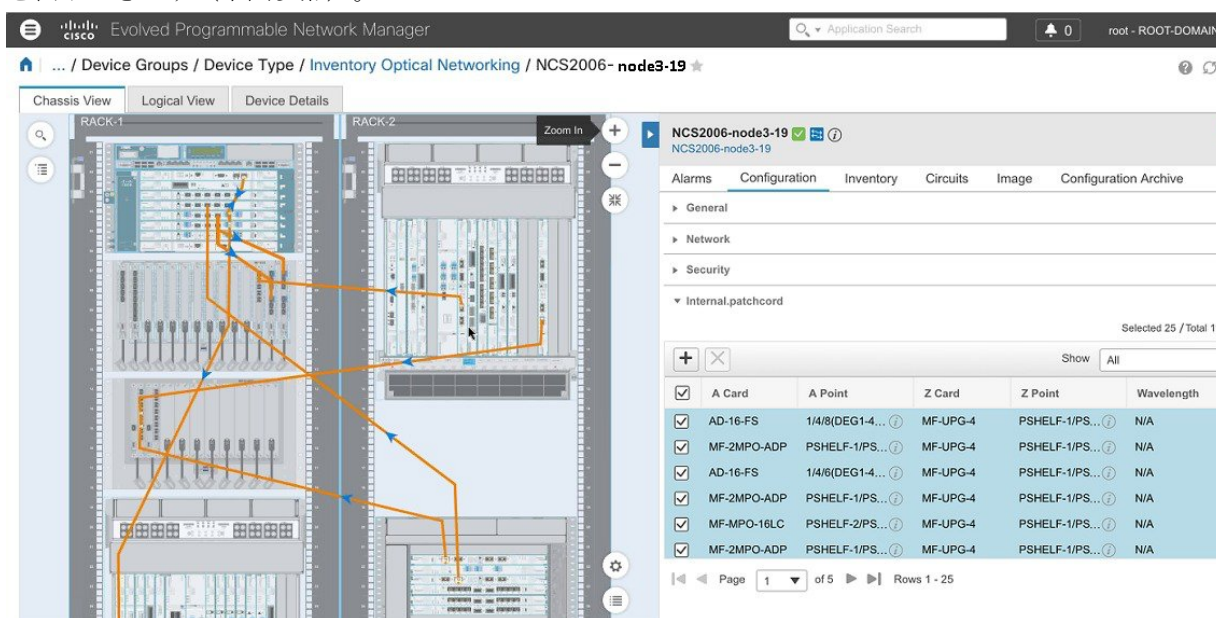
**ステップ 3** 右側のペインで、[設定 (Configuration)] サブタブをクリックし、[Internal.patchcord] 領域を展開します。

- ステップ 4** [+]アイコンをクリックした後、デバイスに必要な送信側（TX）と受信側（RX）のパッチコードを選択します。
- ステップ 5** [終了（Finish）]をクリックします。パッチコードが[内部パッチコード（Internal Patchcords）]テーブルに追加されます。



(注) パッチコードはいったん作成したら、変更することはできません。ただし、削除できます。

[内部パッチコード（Internal Patchcords）]テーブルで1つのパッチコードまたは複数のパッチコードを選択し、左側のペインに表示されるデバイスのシャーシビューにパッチコードの方向を表示できます（下図参照）。



## デバイス内のシェルフに対する保護グループの設定

デバイス内のシェルフの保護グループを作成するには、次の手順を実行します。



(注) ラックの保護グループは設定できません。

### 始める前に

次に、シェルフの保護グループを作成するときの前提条件を示します。

- Yケーブル保護グループを作成するには、クライアントポートで設定されている同じタイプの2枚のカードが同じシェルフに接続されていることを確認します。

- スプリッタ保護グループを作成するには、トランク ポート 3-1 とトランク 4-1 で構成されている少なくとも1枚のOTU2XPカードがシェルフに接続されていることを確認します。

- 
- ステップ 1** 左側のサイドバーから、[設定 (Configuration)] > [ネットワークデバイス (Network Devices)] を選択します。
- ステップ 2** デバイス名のハイパーリンクをクリックして、設定するデバイスを選択します。デバイスの [シャーシビュー (Chassis View)] タブが表示されます。
- ステップ 3** シャーシビュー エクスプローラを展開した後、保護グループを設定するシェルフを選択します。
- ステップ 4** 右側のペインで、[設定 (Configuration)] サブタブをクリックした後、[保護 (Protection)] 領域を展開します。
- ステップ 5** [+] アイコンをクリックして、[保護グループの作成 (Create Protection Group)] ウィンドウを開きます。
- ステップ 6** [タイプ (Type)] ドロップダウンリストから、次のいずれかの保護タイプを選択します。
- [スプリッタ (Splitter)] : この保護タイプは、MXPP/TXPP カードを使用する場合にのみ適用されます。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。
  - [Y ケーブル (Y Cable)] : この保護タイプは、クライアント ポートで構成されている 2 つのトランスポンダまたは 2 つのマックスポンダカードがデバイス内の同じシェルフに接続されている場合にのみ適用されます。
- ステップ 7** シェルフの保護ポートと現用ポートを選択します。
- (注) これらのポートは、この手順の冒頭に記載されている前提条件を満たしている場合にのみ選択できます。
- ステップ 8** 保護タイプに単方向か、双方向かのいずれかを選択します。双方向モードでは、アクティブインターフェイスで障害が発生すると、アクティブ インターフェイスから保護/バックアップ インターフェイスへのトラフィックの切り替えがトリガーされます。
- ステップ 9** [元に戻す (Revertive)] トグル オプション ボタンをクリックして、障害が修正された後にシェルフを保護ポートから元のポートに戻します。
- ステップ 10** ミリ秒単位で [保留時間 (Hold Off Time)] を選択します。保留時間は、障害が修正された後に元のポートに切り替えられるまで、保護ポートのシェルフが待機する必要がある時間です。保留時間が経過すると、シェルフは元のポートに戻ることができます。保留時間の最小値は 0.5 である必要があります。
- ステップ 11** [適用 (Apply)] をクリックします。保護グループが [保護 (Protection)] テーブルに追加されます。
- 

## ラインカードの動作モードの設定

NCS 1004 デバイスの NCS1K4-OTN-XP カードの動作モードを設定し、ラインカードをアクティブまたは非アクティブにするには、次の手順を実行します。



- ステップ1 **シャーシビューを開く**の説明に従って、シャーシビューを起動します。
- ステップ2 右側に表示されるウィンドウで [設定 (Configuration) ] タブをクリックします。
- ステップ3 [ラインカードの動作モード (Line Card Operating Mode) ] サブタブを展開します。
- ステップ4 ラインカードの動作モードを編集するには、カードの動作モードを選択して [編集 (Edit) ] をクリックします。
- ステップ5 ドロップダウンリストから [カード動作モード (Card Operating Mode) ] を選択し、[アクション (Action) ] ドロップダウンリストから目的のアクションを割り当てます。
- ステップ6 [適用 (Apply) ] をクリックして変更内容を展開します。

## スライスの設定

Cisco EPN Manager を使用すると、クライアントポートとトランクポートのビットレートを制御し、各スライスの FEC と暗号化のタイプを設定することでスライスを設定できます。

スライスの5つのクライアントポートを同じビットレートで設定する必要があります。また、トランクポートは両方とも常に同じ FEC モードに設定してください。



(注) スライスの設定は現在、Cisco NCS 1002 および NCS 1004 デバイスでのみサポートされています。

### NCS 1002 デバイスのスライスの設定

Cisco NCS 1002 デバイスのスライスを設定するには、次の手順を実行します。

- ステップ1 **シャーシビューを開く**の説明に従って、シャーシビューを起動します。
- ステップ2 右側に表示されるウィンドウで [設定 (Configuration) ] タブをクリックします。
- ステップ3 [スライスの設定 (Slice Configuration) ] サブタブを展開します。
- ステップ4 新しいスライスを設定を追加するには、[+] (追加) ボタンをクリックし、次の詳細を指定します。

スライス設定パラメータ	説明
スライス番号	スライス ID を表す数値。スライスごとに作成できる設定セットは1つのみです。
クライアントビットレート	スライスのクライアントポートで設定するビット/秒 (ギガビット/秒単位) の合計数。
トランクビットレート	スライスのトランクポートで設定するビット/秒 (ギガビット/秒単位) の合計数。
FEC	トランクポートに設定する FEC 値。

スライス設定パラメータ	説明
	FECモード設定を変更する前に、変更しようとしているインターフェイスの管理状態が [ダウン (故障中) (Down (out of service))] で、G709 の設定が有効になっていることを確認してください。
暗号化 (Encryption)	暗号化されたトラフィックまたは暗号化されていないトラフィックで機能するようにスライスを設定します。

**ステップ 5** [適用 (Apply)] をクリックして、変更をすぐにデバイスに展開します。

スライスごとに追加できるパラメータのセットは1つだけで、一度保存するとすべてのパラメータが編集できなくなります。パラメータを編集するには、スライスの設定を削除してからもう一度追加します。

(注) 管理状態が [動作中 (UP)] の場合、スライス設定は削除できません。

## NCS 1004 デバイスのスライスの設定

NCS1004 デバイスのスライスを設定するには、次の手順を実行します。

**ステップ 1** [シャーシビューを開く](#)の説明に従って、[シャーシビュー](#)を起動します。

**ステップ 2** [シャーシエクスプローラ (Chassis Explorer)] から、設定するスロットを選択します。

**ステップ 3** 右側に表示されるウィンドウで [設定 (Configuration)] タブをクリックします。

**ステップ 4** [スライスの設定 (Slice Configuration)] サブタブを展開します。

**ステップ 5** [カードモード (Card Mode)] ドロップダウンリストから、適切なオプションを選択します。

使用可能なオプションは、[Slice Mode]、[Muxponder Mode]、および [Regen Mode] です。

**ステップ 6** 新しいスライスの設定を追加するには、[+] (追加) ボタンをクリックし、次の詳細を指定します。

スライス設定パラメータ	説明
スライス番号	スライス ID を表す数値。この値は、NCS 1004 デバイスでは変更できません。
クライアント ビットレート	スライスのクライアントポートで設定するビット/秒 (ギガビット/秒単位) の合計数。選択可能なオプションは、[100GE] および [OTU4] です。[100GE] は、[スライスモード (Slice Mode)] と [マックスポンダモード (Muxponder Mode)] の両方に適用されます。[OTU4] は [マックスポンダモード (Muxponder Mode)] にのみ適用されます。
トランク ビットレート	スライスのトランクポートで設定するビット/秒 (ギガビット/秒単位) の合計数。 (注) [Regen Mode] の場合、[Trunk Bitrate] は設定にのみ適用されます。

**ステップ7** [適用 (Apply) ] をクリックして、変更をすぐにデバイスに展開します。

スライスごとに追加できるパラメータのセットは1つだけで、一度保存するとすべてのパラメータが編集できなくなります。パラメータを編集するには、スライスの設定を削除してからもう一度追加します。

(注) 管理状態が [動作中 (UP) ] の場合、スライス設定は削除できません。

---

## [デバイスの詳細 (Device Details) ] ページからのインターフェイスの設定

[デバイスの詳細 (Device Details) ] ページからインターフェイスを設定するには、次の手順を実行します。

**ステップ1** デバイスのシャーシビューを開いて、[設定の起動 (Launch Configuration) ] リンクをクリックします。

[デバイスの詳細 (Device Details) ] ページが開きます。

**ステップ2** [論理ビュー (Logical View) ] タブをクリックします。

**ステップ3** [機能 (Features) ] ウィンドウで、[インターフェイス (Interfaces) ] > 設定するインターフェイスのタイプを選択します。

**ステップ4** 選択したインターフェイスタイプに固有の手順を実行してインターフェイスを追加または編集します ([インターフェイスの設定 \(48 ページ\)](#) を参照)。

---

## Cisco NCS 1000 インターフェイス設定の更新

Cisco NCS 1000 シリーズ デバイスに設定されてインターフェイスの [管理ステータス (Admin Status) ]、[波長 (nm) (Wavelength (nm)) ]、および [ループバック (Loopback) ] の設定は [デバイスの詳細 (Device Details) ] ページからすばやく更新できます。これを行うには、次の手順を実行します。

**ステップ1** [完全なデバイス情報の取得 : \[デバイスの詳細 \(Device Details\) \] ページ](#)の説明に従って、Cisco NCS 1000 シリーズ デバイスの [デバイスの詳細 (Device Details) ] ページを開きます。

**ステップ2** [設定 (Configuration) ] タブをクリックします。

ページが更新され、3つのサブタブ ([光学 (Optics) ]、[イーサネット (Ethernet) ]、および [コヒーレント DSP (Coherent DSP) ]) が表示されます。

**ステップ3** 更新するインターフェイスのタイプのサブタブをクリックします。

**ステップ4** 必要な変更を加えます。

### 方法1

1. [インターフェイス (Interfaces) ] テーブルで、更新するインターフェイスを見つけます。

2. 変更するパラメータをクリックして、ドロップダウンリストを開きます。
3. 設定する値を選択し、[保存 (Save)] をクリックします。

## 方法 2

1. 更新するインターフェイスのオプション ボタンをクリックし、鉛筆 ([編集 (Edit)]) アイコンをクリックします。  
[インターフェイス タイプの編集 (Edit Interface Type)] ダイアログボックスが開きます。
2. 使用可能なドロップダウンリストから設定する値を選択し、[適用 (Apply)] をクリックします。
3. [OK] をクリックして、変更内容を確定します。

次の点に注意してください。

- 光学インターフェイスの場合：
  - [管理ステータス (Admin Status)] と [波長 (nm) (Wavelength (nm))] パラメータを更新できません。
  - 新しい波長値を設定できるのは、[光学タイプ (Optics Type)] パラメータが [DWDM] に設定されている場合のみです。
- コヒーレント DSP およびイーサネット インターフェイスの場合：
  - [管理ステータス (Admin Status)] と [ループバック (Loopback)] パラメータを更新できます。
  - 新しいループバック値を設定できるのは、[管理者ステータス (Admin Status)] パラメータが [テスト中 (Testing)] に設定されている場合のみです。
  - [ループバック (Loopback)] パラメータを [回線 (Line)] に設定すると、Cisco EPN Manager はファシリテーループバックに適用されるのと同じ設定を適用します。ファシリテーループバックは、カードの回線インターフェイスユニット (LIU)、電気インターフェイスアセンブリ (EIA)、および関連するケーブル配線をテストします。
  - [ループバック (Loopback)] パラメータを [内部 (Internal)] に設定した場合、Cisco EPN Manager は端末ループバックに適用されるのと同じ設定を適用します。

## コントローラ（光学、OTS、OCH、DSP、およびDWDM）の設定

Cisco EPN Manager を使用すると、波長、FEC、SD、SF BER のレポートとしきい値などの光デバイス コントローラのパラメータを、OTS、OTS OCH、DWDM などのタイプのコントローラに設定できます。

光トランスポート セクション (OTS) コントローラは、OTS 光インターフェイスのすべての光パラメータを保持します。光インターフェイスは、VOA や増幅器などのハードウェア コンポーネントに応じて異なる機能を備えています。したがって、OTS コントローラで有効または

無効にするパラメータは、特定の光インターフェイスの実際のハードウェア機能によって異なります。OTS コントローラの増幅器のゲイン範囲、増幅器チルト、OSRI などのパラメータを設定できます。

光トランスポートセクション OCH (OTS OCH) コントローラは、OTS 光インターフェイスで使用可能な OCM デバイスを表します。このコントローラは、OTS インターフェイス上のチャネルの粒度を持ちます。OTS OCH コントローラには波長情報が含まれています。OTS OCH コントローラの管理ステータスのみを設定できます。

コントローラを設定する前にスライス設定の完了を確認するには、[NCS 1002 デバイスのスライスの設定 \(89 ページ\)](#) を参照してください。

光コントローラのパラメータを設定するには、次の手順を実行します。

- ステップ 1** [シャーシ ビューを開く](#)の説明に従って、[シャーシ ビュー](#)を起動します。
  - ステップ 2** 右側に表示されるウィンドウで [設定 (Configuration) ] タブをクリックします。
  - ステップ 3** [コントローラ (Controllers) ] サブタブを展開します。デバイスの選択に応じて、サポートされているタブが表示されます。
  - ステップ 4** 光コントローラの設定を編集するには、[光学 (Optics) ] をクリックし、必要な設定を選択して [変更 (Modify) ] アイコンをクリックし、変更を加えます。
  - ステップ 5** OTS コントローラの設定を編集するには、[OTS] をクリックし、必要な設定を選択して [変更 (Modify) ] アイコンをクリックし、変更を加えます。
  - ステップ 6** OTS-OCH コントローラの設定を編集するには、[OTS-OCH] をクリックし、必要な設定を選択して [変更 (Modify) ] アイコンをクリックし、変更を加えます。
  - ステップ 7** コヒーレント DSP の設定を編集するには、[コヒーレント DSP (Coherent DSP) ] をクリックし、必要な設定を選択して [変更 (Modify) ] アイコンをクリックし、変更を加えます。
- トランスポート管理ステータスが IS に設定されている場合は、パラメータを編集できないことに注意してください。
- ステップ 8** DWDM コントローラの設定を編集するには、[DWDM] をクリックし、必要な設定を選択して [変更 (Modify) ] アイコンをクリックし、変更を加えます。

カテゴリ	パラメータ	説明
一般的な光学、OTS-OCH、DSP、および DWDM のコントローラパラメータ	<ul style="list-style-type: none"> <li>• 名前 (Name)</li> <li>• 管理者ステータス (Admin Status)</li> <li>• 動作ステータス (Operational Status)</li> <li>• トランスポート管理ステータス</li> </ul>	<p>[名前 (Name) ] : (表示のみ) ポート番号を表示します。</p> <p>[管理者ステータス (Admin Status) ] : インターフェイスが管理対象 (動作中) かダウンか、またはメンテナンス モードかを定義します。インターフェイスのステータスが [動作中 (Up) ] の場合、コントローラのプロパティは変更できません。</p> <p>[動作ステータス (Operational Status) ] : インターフェイスが動作可能で、プロビジョニング済みとして実行されているかどうかを定義します。</p> <p>[トランスポート管理ステータス (Transport Admin Status) ] : コントローラのトランスポート管理状態を定義します。</p>

カテゴリ	パラメータ	説明
	(Transport Admin Status)	
一般的な光学およびDWDMのパラメータ	実波長 (nm) (Actual Wavelength (nm))	チャンネルで使用する実際の波長を表示します。
-	波長 (nm) (Wavelength (nm))	チャンネルで設定された波長値を表示します。デバイスインベントリ収集ステータスが [完了 (Completed)] になると、[実波長 (Actual Wavelength)] と [波長 (Wavelength)] の値が一致します。
-	FEC モード (FEC Mode)	コントローラで設定する FEC 値。  FEC モード設定を変更する前に、変更しようとしているインターフェイスの管理状態が [ダウン (故障中) (Down (out of service))] で、G709 の設定が有効になっていることを確認してください。
光パラメータ	速度 (Speed)	コントローラが動作する必要がある速度値 (ギガビット/秒) を設定します。
-	DAC レート	ドロップダウンリストから DAC レートを選択します。
-	最小波長分散	最小波長分散値を入力します。
-	最大波長分散	最大波長分散値を入力します。
-	設定される送信電力	送信電力を入力します。
-	変調タイプ	ドロップダウンリストから変調タイプを設定します。
-	差分変調 (Differential Modulation)	設定された速度値に基づいて、差分エンコーディング (DE) を有効または無効にします。
-	ループバック (Loopback)	ループバックを次のように設定します。  <ul style="list-style-type: none"> <li>• [内部 (Internal)] : すべてのパケットがルータの内部でループバックされてから外部インターフェイスに到達します。内部 Rx から Tx へのパスをテストし、物理ポートから出力するトラフィックを停止します。</li> <li>• [回線 (Line)] : 着信ネットワークパケットが外部インターフェイスを通じてループバックされます。</li> </ul>
-	SD BER	信号劣化ビット エラー レートを設定します。オプションは、E-5、E-6、E-7、E-8、または E-9 です。
-	SF BER	信号障害ビット エラー レートを設定します。オプションは E-3、E-4、または E-5 です。

カテゴリ	パラメータ	説明
DWDM パラメータ	ループバック (Loopback)	ループバックを次のように設定します。 <ul style="list-style-type: none"> <li>• [内部 (Internal)] : すべてのパケットがルータの内部でループバックされてから外部インターフェイスに到達します。内部 Rx から Tx へのパスをテストし、物理ポートから出力するトラフィックを停止します。</li> <li>• [回線 (Line)] : 着信ネットワークパケットが外部インターフェイスを通じてループバックされます。</li> </ul>
-	<ul style="list-style-type: none"> <li>• OTU-SD</li> <li>• OTU-SF</li> <li>• ODU-SD</li> <li>• ODU-SF</li> </ul>	SF (信号障害) と SD (信号劣化) の BER レポートとしきい値の設定 アラームが OTU アラームか ODU アラームかに応じて、アラームは SM BER が SD BER しきい値または SF BER しきい値に基づいて超過していることを表します。
OTS パラメータ	ポートロール (Port Role)	ポートの現在の動作状態。 保護スイッチの場合、通信の作業ロールが表示されますが、増幅器モジュールの場合は [通信回線/OSC (Com Line/Osc)] ロールまたは [通信確認 (Com Check)] ロールが表示されます。
-	Rx/Tx 下限しきい値 (dBm) (Rx/Tx Low Threshold (dBm))	受信者/トランスポンダの下限受信電力しきい値を設定します。有効な範囲は -500 ~ 300 です。
-	増幅器チャンネル電力 (dBm) (Amplifier Channel Power (dBm))	チャンネル電力設定ポイントごとに増幅器を設定します。有効な範囲は -500 ~ 300 です。デフォルト値は 0.0 です。
-	チャンネル電力最大デルタ (dBm) (Channel Power Max Delta (dBm))	測定されたすべてのチャンネル電力間の最大差異を設定します。有効値は 0 ~ 200 です。
-	増幅器ゲインと増幅器ゲインの範囲 (Amplifier Gain and Amplifier Gain Range)	増幅器ゲイン設定ポイントを設定します。この範囲の有効モードは [通常 (Normal)] または [拡張 (Extended)] です。 注: 増幅器ゲインの範囲は、コントローラがシャットダウン状態にある場合にのみ設定できます。
-	増幅器安全性コントローラモード (Amplifier Safety Controller Mode)	安全制御モードを [自動 (Auto)] または [無効 (Disabled)] に設定します。

カテゴリ	パラメータ	説明
-	OSRI	光安全性リモート インターロックを [オン (On) ] または [オフ (Off) ] に設定します。
-	増幅器チルト (Ampli Tilt)	-50 ~ +50 の数値を使用して増幅器チルトを設定します。

(注) IOS-XR (RON) 光コントローラの編集画面に表示される値は、デバイスの実行コンフィギュレーションです。

光コントローラの [DAC レート (DAC Rate) ]、[FEC]、および [変調方式 (Modulation Type) ] 属性に対して [設定しない (Not Set) ] が選択されている場合、EPNM はデバイスから既存の構成を削除し、GI が完了するとそれらの属性の動作値をユーザーインターフェイスに表示します。

**ステップ 9** [適用 (Apply) ] をクリックして、変更内容をデバイスにすぐに展開します。

**ステップ 10** (オプション) DWDM グリッド値の単位を波長または周波数に変更するには、[管理者 (Administrator) ] > [設定 (Settings) ] > [システム設定 (System Settings) ] > [回線/VC 表示 (Circuits/VCs Display) ] に移動し、[DWDM グリッド単位 (DWDM Grid Unit) ] 領域で [波長 (ナノメートル (nm) ) (Wavelength (Nanometer (nm) ) ] または [周波数 (テラヘルツ派 (THz) ) (Frequency (Tetraherxtx (THz))) ] のいずれかを選択します。

## パッシブユニットの設定

パッシブユニットは、光デバイス用に Cisco EPN Manager を使用してプロビジョニングされたパッシブカードです。Cisco EPN Manager はこれらのパッシブユニットをデータベースに保持し、デバイスには展開しません。設定が完了したら、これらのパッシブユニットを [デバイスの詳細 (Device Details) ] ページと [インベントリ (Inventory) ] ページで表示し、それらを使用してネットワーク トポロジで管理対象リンクを作成できます。



(注) パッシブユニットの設定は現在、Cisco NCS 1001 デバイスでのみサポートされています。

パッシブユニットを追加または削除するには、次の手順を実行します。

### 始める前に

このタスクを実行する前に、「管理者」または「設定マネージャ」のユーザー権限があることを確認します。

**ステップ 1** [シャーシビューを開く](#)の説明に従って、シャーシビューを起動します。

**ステップ 2** 右側に表示されるウィンドウで [設定 (Configuration) ] タブをクリックします。



**ステップ3** [パッシブユニット (Passive Units) ]サブタブを展開します。

**ステップ4** パッシブユニットを追加するには、[追加 (Add) ] (+) アイコンをクリックし、次の詳細を指定します。

- 機器 ID : パッシブユニットの一意的識別子を選択します。デバイスごとに最大9つのパッシブユニットを追加できます。
- 機器のタイプ : スロットが48チャンネルマックスポンダ/でマックスポンダとしてプロビジョニングされるか、ODD/EVENユニットとしてプロビジョニングされるかを決定する機器のタイプを選択します。オプションは[CME]、[ODDE]、および[EVENE]です。
- (オプション) シリアル番号 : 各パッシブユニットに固有のシリアル番号。Cisco EPN Managerは、この構成をデバイスに展開せず、データベースにのみ保持します。

**ステップ5** [適用 (Apply) ]をクリックして変更内容をデバイスに展開します。

**ステップ6** (オプション) パッシブユニットが正常に作成されたことを確認するには、[インターフェイス (Interfaces) ]タブまたは[デバイスの詳細 (Device Details) ]タブに移動し、[インターフェイス名 (Interface Name) ]フィルタを使用してパッシブユニットを見つけます。

パッシブユニットに使用される命名規則は次のとおりです。

*PUnit<number of the card> <equipment ID of the passive unit>*

たとえば、*PUnit/1/16* などです。

**ステップ7** パッシブユニットの設定を編集するには、それらの設定を削除し、同じ機器 ID を使用して詳細を再度設定します。

**ステップ8** パッシブユニットを削除するには、必要なパッシブユニットを選択し、[削除 (Delete) ] (X) アイコンをクリックします。リンクに関連付けられているパッシブユニットも削除できます。これにより、リンクが[部分的 (Partial) ]状態に切り替わります。

**ステップ9** (オプション) 同じ値を持つ複数のパッシブユニットを照合するには、必要なパッシブユニットを選択し、[照合 (Match) ]をクリックします。ドロップダウンリストからシミュレートされたパッシブユニット番号を選択し、[適用 (Apply) ]をクリックします。

**ステップ10** (オプション) これらのパッシブポートを使用して手動リンクを設定するには、ネットワークトポロジに移動し、[トポロジマップへのリンクの手動による追加](#)に従って、リンクを作成します。

## 光ケーブルでの増幅器モジュール設定の編集

グリッドモード、ノードタイプ、およびUDC VLANの設定を変更することで、デバイスの光スロットに挿入されている増幅器モジュールの設定を変更できます。

増幅器モジュール設定を編集するには、次の手順を実行します。

### 始める前に

このタスクを実行する前に、「管理者」または「設定マネージャ」のユーザー権限があることを確認します。

**ステップ 1** **シャーシビューを開く**の説明に従って、シャーシビューを起動します。

**ステップ 2** 右側に表示されるウィンドウで [設定 (Configuration)] タブをクリックします。

**ステップ 3** [増幅器モジュール設定 (Amplifier Module Settings)] サブタブを展開します。

**ステップ 4** 編集する設定を選択し、[編集 (Edit)] アイコンをクリックして次のパラメータを指定します。

- [グリッドモード (Grid Mode)] : 増幅器モジュールのインターフェイス上の光スペクトルを定義します。
- [ノードタイプ (Node Type)] : 増幅器が動作するように設定するノードのタイプを定義します。オプションは、[端末 (Terminal)]、[回線 (Line)]、および [設定なし (Not Set)] です。
- [UDC VLAN] : 選択したスロットとその UDC ポートに関連付けられている VLAN を定義します。

(注) 指定した UDC VLAN がデバイス上で一意であることを確認します。重複する値はサポートされていません。

**ステップ 5** [適用 (Apply)] をクリックして変更内容をデバイスに展開します。

**ステップ 6** (オプション) イーサネットコントローラを設定するには、[イーサネット (Ethernet)] サブタブを展開します。編集するコントローラを選択し、[編集 (Edit)] アイコンをクリックし、必要な変更を加えます。[適用 (Apply)] をクリックして、変更内容をデバイスに保存します。

## GMPLS および WSON のプロパティの構成

### GMPLS UNI :

Generalized Multiprotocol Label Switching (GMPLS) ユーザー ネットワーク インターフェイス (UNI) は、光ネットワーク内の 2 台のクライアント (UNI-C) 間の回線接続を作成します。この接続は、UNI-C ノードがルータ ノードであり、UNI-N ノードが光ノードである、UNI クライアント (UNI-C) と UNI ネットワーク (UNI-N) ノード間のシグナリング交換によって実行されます。

GMPLS UNI は、Cisco NCS 1002 ノードの 100G および 200G トランク ポートでのみサポートされています。OCH トレイル回路の前提条件は、NCS 2000 シリーズ ノードの光チャネルアド/ドロップ NCS 2000 シリーズ インターフェイスと NCS 1002 ノードの NCS 1002 インターフェイス間にリンク管理プロトコル (LMP) リンクを作成することです。

UNI はクライアント (UNI-C) とネットワーク (UNI-N) のロールに分割されます。UNI-C ネットワーク要素は、回路プロビジョニング情報を要求して受け入れます。UNI-N ネットワーク要素は、UNI-C ノードに隣接するノードであり、コア ネットワーク全体の回路プロビジョニング情報を受け入れ、転送します。

UNI 回線プロビジョニングの場合、ネットワークは次の要件を満たしている必要があります。

- NE は UNI-C として設定され、UNI-N NE に接続されている必要があります。
- NE は UNI-N として設定され、UNI-C NE に接続されている必要があります。

**静的 UNI :**

リンク管理プロトコル (LMP) は、トンネルの送信元ノードと宛先ノードのトランク光コントローラ上に作成される論理リンクです。2つの異なるデバイスのポート間に静的 LMP リンク (静的 UNI) を作成できます。たとえば、Cisco NCS 2000 シリーズ ノードと Cisco NCS 1002 ノードの間などです。これは、GMPLS UNI トンネルの LMP ネイバーの設定に役立ちます。

Cisco EPN Manager を使用して静的 UNI を設定し、選択した RX ポートと TX ポートで UNI に参加するカード、シェルフ、またはスロットを識別します。RX ポートは UNI の送信元を表し、TX ポートは宛先を表します。

[リモート デバイス (Remote Device) ] フィールドを使用して、選択したノードの管理 IP アドレスを指定します。[リモートクライアントインターフェイス (Remote Client Interface) ] フィールドを使用して、光学コントローラの LMP リンク IP アドレスを選択します。

**異種波長 :**

[異種波長 (Alien Wavelength) ] タブを使用して、異種波長のポートと波長パラメータを表示および設定します。また、必要な異種波長タイプ、トランク モード、および転送エラー補正 (FEC) モードを指定することもできます。

**光ファイバ属性 :**

GMPLS UNI の作成時に使用するパラメータを光ファイバのタイプ (分散シフト (DS) 、 True-Wave Classic (TWC) 、またはその他の値を選択) などの値を設定することで設定できます。また、光ファイバの長さを指定し、偏光モード分散ファイバ係数を指定することもできます。

[減衰器入力 (Attenuator In) ] の値は、ノード出力ポート (LINE-TX ポートなど) と光ファイバの入力パラメータ間での入力光減衰 (dB 単位) を識別します。同様に、[減衰器出力 (Attenuator Out) ] の値は、ノード入力ポート (LINE-RX ポートなど) と光ファイバの出力パラメータ間での入力光減衰 (dB 単位) を識別します。

光グリッド内の2つの隣接チャンネル間の最小周波数間隔を設定するチャンネル間隔値を選択できます。スパンで予測される最大チャンネル数を指定するには、[チャンネル番号 (Channel Number) ] フィールドを指定します。チャンネル番号とチャンネル間隔の値が一貫していることを確認します。たとえば、100 GHz 間隔を持つ 80 個のチャンネルは存在できません。

**仮想トランク :**

[仮想トランク (Virtual Trunk) ] タブを使用して、デバイスの [ドロップポート (Drop Port) ]、[説明設定 (Description Configuration) ]、および [異種波長タイプ (Alien Wavelength Type) ] を指定できます。

**LMP の終了 :**

[LMP の終了 (LMP Termination) ] タブを使用して、デバイスの [仮想トランク (Virtual Trunk) ]、[LMP タイプ (LMP Type) ]、[リモートデバイス (Remote Device) ]、[リモートインターフェイス (Remote Interface) ]、および [ピアリング (Peering) ] を指定できます。また、[LMP の終了 (LMP Termination) ] タブで既存の LMP の終了を編集することもできます。

GMPLS/WSON パラメータを設定するには、次の手順を実行します。

ステップ1 シャーシビューを開くの説明に従って、シャーシビューを起動します。

ステップ2 右側に表示されるウィンドウで [設定 (Configuration)] タブをクリックします。

ステップ3 これらのパラメータを設定するには、次の表に示すパスに移動します。

タスク	ナビゲーション	説明
ファイバ属性の設定	[GMPLS/WSON] サブタブ > [ファイバ属性 (Fiber Attributes)]	ファイバ側、タイプ、長さ、検証、チャンネル間隔、チャンネル番号、およびドメインの値を指定します。必要に応じて、減衰器 (入力と出力) の値を指定することもできます。
静的 UNI の作成と編集	[GMPLS/WSON] サブタブ > [静的 UNI (Static UNI)]	<ul style="list-style-type: none"> <li>UNI に参加する必要がある RX ポートと TX ポートのリモートコントローラを追加します。</li> <li>[リモートデバイス (Remote Device)] フィールドは、ノードの管理 IP アドレスを指定します。</li> <li>[リモートクライアントインターフェイス (Remote Client Interface)] フィールドは、コントローラのリンク IP アドレスを指定します。</li> </ul> <p>(注) 上記の設定を使用して、リモート TXP ノードを設定できます。</p>
GMPLS UNI の作成と編集	[GMPLS/WSON] サブタブ > [GMPLS UNI (GMPLS UNIs)]	<ul style="list-style-type: none"> <li>GMPLS UNI の入力ポートと出力ポートを指定し、UNI のタイプが番号付けされているか、番号なしかを選択します。UNI が UNI-C タイプか UNI-N タイプかを必ず指定してください。</li> <li>トランク値は、GMPLS UNI の設定に応じて、それぞれの異種波長値に自動的に設定されます。設定された異種波長が両方のトランクポートでサポートされている場合は、トランクポートの1つに設定すると、両方のトランクポート上に同じ異種波長が自動的に設定されます。</li> <li>Cisco NCS 2000 デバイスの場合、GMPLS UNI トランク値はデフォルトに設定できます。</li> <li>ローカルおよびリモートシステムの IP と、リモートシステムの IP およびコントローラを指定します。これらの値を指定すると、UNI のリモートシステム接続が有効になります。</li> </ul> <p>(注) Cisco EPN Manager で管理されるデバイスのリモートシステム IP のみを指定できます。</p>
異種波長パラメータの設定:	[GMPLS/WSON] サブタブ > [異種波長 (Alien Wavelength)]	必要な異種波長のタイプ、トランクモード、および FEC モードを指定します。

タスク	ナビゲーション	説明
仮想トランクの設定	[GMPLS/WSON] サブタブ > [仮想トランク (Virtual Trunk) ]	[ドロップポート (Drop Port) ]、[説明設定 (Description Configuration) ]、および[異種波長タイプ (Alien Wavelength Type) ]を指定します。
LMP の終了の設定と編集	[GMPLS/WSON] サブタブ > [LMP の終了 (LMP Termination) ]	[仮想トランク (Virtual Trunk) ]、[LMP タイプ (LMP Type) ]、[リモートデバイス (Remote Device) ]、[リモートインターフェイス (Remote Interface) ]、および[ピアリング (Peering) ]を指定します。

(注) 信号未送信 LMP の場合、コマンドはローカルデバイスにのみプッシュされます。手動で、または設定テンプレートを使用して、リモートデバイスに設定をプッシュする必要があります。

**ステップ 4** 変更を加えて、[保存 (Save) ] をクリックします。

**ステップ 5** 設定後に値を編集するには、値を選択し、ツールバーの [編集 (Edit) ] アイコンをクリックします。変更を加えて、[保存 (Save) ] をクリックします。

LMP リンクの作成については、[光チャネル \(OCH\) トレールのユーザー/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。

## OTS ポートでの OSRI の有効化または無効化

OTS インターフェイスで設定されたポートの OSRI ステータスを変更できます。

OSRI を有効または無効にするには、次の手順を実行します。

### 始める前に

このタスクを実行する前に、「管理者」または「設定マネージャ」のユーザー権限があることを確認します。

**ステップ 1** [シャーシビューを開く](#)の説明に従って、[シャーシビュー](#)を起動します。

**ステップ 2** 右側に表示されるウィンドウで [設定 (Configuration) ] タブをクリックします。

**ステップ 3** [Maintenance] タブを展開し、[OSRI] サブタブをクリックします。

**ステップ 4** OSRI を有効または無効にするポートを選択します。

**ステップ 5** ドロップダウンリストから、[Enable] または [Disable] を選択して OSRI を有効または無効にします。

## 光カードの設定

- [シャーシビューからカードを設定する \(102 ページ\)](#)

- [カードのリセット \(103 ページ\)](#)
- [カードの削除 \(103 ページ\)](#)
- [カードの設定 : 400G-XP-LC、100G-CK-C、100ME-CK-C、200G-CK-LC、100GS-CK-C、100G-LC-C、100G-ME-C、および 10x10G-LC \(106 ページ\)](#)
- [カードの設定 : OTU2-XP、MR-MXP、WSE、AR-XPE、AR-XP、AR-MXP、40E-MXP-C、および 40ME-MXP-C \(104 ページ\)](#)
- [SONET および Flex の回線カードの設定 \(109 ページ\)](#)
- [着脱可能ポート モジュールおよびカード モード設定の編集と削除 \(113 ページ\)](#)
- [Cisco NCS 2000 デバイス用のカードとサポートされる設定 \(114 ページ\)](#)

## シャーシビューからカードを設定する

この手順では、シャーシビューを使用して、Cisco EPN Manager にカードを追加します。カードを追加したら、そのカードタイプの関連トピック内の手順に従って、それを設定できます。通常は、カードを物理的にスロットに挿入する前に行います。

### 始める前に

この機能は Cisco NCS 2000 と Cisco ONS のデバイスでのみサポートされています。

**ステップ 1** [シャーシビューを開く](#)の説明に従って、シャーシビューを起動します。

**ステップ 2** 次のいずれかの操作を実行して、カードを追加するスロットを選択します。

- 物理シャーシビューで空のスロットを選択してから、スロットポップアップウィンドウで [カードの追加 (Add Card) ] リンクをクリックします。
- シャーシビューエクスプローラを使用して空のスロットに移動し、そのスロットの横にある [i] アイコンの上にマウスカーソルを移動してから、情報ポップアップウィンドウで [カードの追加 (Add Card) ] ハイパーリンクをクリックします。

Cisco EPN Manager では、物理シャーシビューでスロット強調表示され（それが事前にプロビジョニングされていることを示す）、そのデバイスタイプでサポートされているすべてのカードの一覧が表示されません。

(注) 選択したカードが物理スロットタイプに適切であることを確認します。

**ステップ 3** 追加するカードを見つけて、[追加 (Add) ] をクリックします。カードが追加された後に Cisco EPN Manager によってステータスメッセージが表示されます。

**ステップ 4** カードをすぐに設定するには、ステータスポップアップメッセージ内の [今すぐ設定 (Configure Now) ] をクリックします。そうでない場合は、[無視 (Ignore) ] をクリックします。

## カードの削除

カードを削除すると、Cisco EPN Manager はカードに関連付けられている動作モードの設定を含め、カードに関するすべての情報を削除します。削除したカードを後になって再び追加する際に、この情報は復元されません。

この機能は Cisco NCS 2000 と Cisco ONS のデバイスでのみサポートされています。

カードを Cisco EPN Manager から削除するには、次の手順に従います。

### 始める前に

カードを削除する前に、以下の点を確認してください。

- 関連付けられているペイロード値とカードの動作モードが削除されていること。
- カード上で実行されるアクティブな設定がないこと（カードを再び追加する際に、設定を復元することはできません）。

---

**ステップ 1** 「[シャーシビューを開く](#)」の説明に従って、シャーシビューを起動します。

**ステップ 2** 次のいずれかの方法で、削除するカードのロットを選択します。

- 物理シャーシビューでロット内のカードを選択し、表示されるポップアップウィンドウ内で[カードの削除 (Delete Card)] リンクをクリックします。
- シャーシビューエクスプローラを使用してカードに移動し、カードの横にある「i」アイコンの上にマウスのカーソルを重ね、表示されるポップアップウィンドウで[カードの削除 (Delete Card)] ハイパーリンクをクリックします。

Cisco EPN Manager の物理シャーシビューでは、ロットが強調表示され（プロビジョニング済みであることを意味する）、ロット内のすべてのカードを削除すると、そのロットはシャーシビューで空の状態になります。

カードを削除した後、Cisco EPN Manager によってノードのインベントリ収集が行われます。

---

## カードのリセット

カードをリセットすると、同期操作の実行と同じようにシャーシ内にカードが再配置されます。Cisco EPN Manager は設定の変更を修正せず、その代わりに設定を保存してインベントリ収集をトリガーします。

この機能は Cisco NCS 2000 と Cisco ONS のデバイスでのみサポートされています。

設定済みのカードをリセットするには：

---

**ステップ 1** 「[シャーシビューを開く](#)」の説明に従って、シャーシビューを起動します。



**ステップ 2** 次のいずれかの方法で、削除するカードのスロットを選択します。

- スロット内のカードを物理シャーシビューから選択し、ポップアップ ウィンドウの [カードのリセット (Reset Card) ] リンクをクリックします。
- シャーシビュー エクスプローラを使用してカードに移動し、マウス カーソルをカードの横の [i] アイコンの上に置き、ポップアップ ウィンドウの [カードのリセット (Reset Card) ] ハイパーリンクをクリックします。

Cisco EPN Manager では、物理シャーシビューでスロットが強調表示されます (プロビジョニング済みであることを示します)。カードをリセットすると、同期が実行され、インベントリ収集がトリガーされます。

#### 次のタスク

「カードの設定 : 400G-XP-LC、100G-CK-C、100ME-CK-C、200G-CK-LC、100GS-CK-C、100G-LC-C、100G-ME-C、および 10x10G-LC (106 ページ) 」の説明に従って、カードのプロパティを設定します。

## カードの設定 : OTU2-XP、MR-MXP、WSE、AR-XPE、AR-XP、AR-MXP、40E-MXP-C、および 40ME-MXP-C

カードの動作モードと接続可能ポートモジュール (PPM) を設定するには、次の手順を実行します。

#### 始める前に

OTU2-XP カードと 40E-MXP-Cカードは、カード動作モードを設定することなく、PPMで直接設定できます。ただし、他のカードのカード動作モードを設定する場合は、シスコ トランスポート コントローラを介して直接この設定を実行できます。

- デバイス同期が完了しており、デバイスのインベントリ収集ステータスが「管理 (Managed) 」または「完了 (Completed) 」であることを確認してください。
- PPMを追加または削除するたびに、事後対応型インベントリ収集がトリガーされ、デバイスは同期プロセスを開始します。デバイスにさらに設定変更を展開する前に、事後対応型インベントリの収集が完了するまで待機してください。デバイスの同期が進行中である場合は、PPM 設定変更のデバイスへの展開が失敗します。
- カードの動作モードが設定されたら、デバイスの同期が完了していることを確認します。慰安両していない場合は、Cisco EPN Manager は選択したカードの適切なペイロード値を表示できません。
- カードで設定変更を行う前に、すべてのカードできめ細かなインベントリが使用可能であることを確認してください。



- 40E-MXP-C、40ME-MXP-C、および OTU2-XP カードを除くすべてのサポート対象カードでは、まずシスコトランスポートコントローラを使用してカードの動作モードを設定してから Cisco EPN Manager に戻り、次の手順に進む必要があります。

- ステップ 1** [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] を選択します。
- ステップ 2** 設定するデバイス名のハイパーリンクをクリックしてデバイスを選択し、そのデバイスの [シャーシ (Chassis)] ビューを起動します。この機能は、Cisco NCS 2000 デバイスのみでサポートされています。
- ステップ 3** [シャーシエクスプローラ (Chassis Explorer)] を使用して、設定するカードを選択します。
- ステップ 4** 右側に表示されるウィンドウで [設定 (Configuration)] サブタブをクリックします。
- ステップ 5** CTC ツールに移動し、カードの動作モードを設定します。カードモードの設定は、OTU2-XP、MR-MXP、WSE、AR-XPE、AR-XP、および AR-MXP カードではサポートされていません。Cisco NCS 2000 デバイス上の他のすべてのカードについては、[カードの設定 : 400G-XP-LC、100G-CK-C、100ME-CK-C、200G-CK-LC、100GS-CK-C、100G-LC-C、100G-ME-C、および 10x10G-LC \(106 ページ\)](#) の説明に従って、カードの動作モードを設定します。
- ステップ 6** [接続可能ポート モジュール (Pluggable Port Modules)] セクションを展開し、ポート モジュールとそれぞれの適切なペイロード値を設定します。
- ステップ 7** [ポート モジュール (Port Modules)] セクションの [+] (追加) アイコンをクリックし、ポート モジュール (PPM) を作成します。
- ステップ 8** **PPM 番号** を選択し、[保存 (Save)] をクリックします。[PPM ポート (PPM Port)] はデフォルトで [PPM (1 ポート) (PPM (1 port))] に設定されており、変更できません。
- (注) 選択されているカードの最大数の PPM が作成されている場合、+ (追加) アイコンは無効になります。次の手順に進むには、使用可能なすべてのポートを作成する必要があります。
- ステップ 9** [接続可能ポート モジュール (Pluggable Port Modules)] セクションの [+] (追加) アイコンをクリックします。
- (注) 一部の PPM では、該当するペイロード値が有効ではないことがあります。有効にするには、上記のステップ 5 で説明したカードモードの設定を行い、ペイロード値をもう一度設定してみます。
- ステップ 10** 選択した PPM に関連付ける必要がある **ポート番号**、**ポートタイプ**、および **レーン数** を選択します。[ポートタイプ (ペイロード) (Port Type (payload))] には、以下の表 2 で説明するサポートされているクライアント信号のいずれかを設定できます。
- (注) 指定されたポートタイプ (ペイロード) が、選択されているカードの動作モードまたは PPM でサポートされていない場合は、デバイスへの変更の展開が失敗します。指定するペイロード値が、選択したカードでサポートされていることを確認します。参考までに、次の表 2 を参照してください。
- ステップ 11** [終了 (Finish)] をクリックして、デバイスに変更を展開します。

**ステップ 12** (オプション) Cisco EPN Manager で変更が表示されない場合、これは複数のユーザーが同じカードモード設定を操作しているために、変更が動的に反映されていないことが原因で発生している可能性があります。最新の変更を表示するには、各セクションの [更新 (Refresh)] アイコンをクリックします。

展開が失敗する場合は、エラー ログ フォルダ (`/opt/CSCOLumos/logs/config.log`) に移動して、エラーの原因の詳細を確認してください。

## カードの設定 : 400G-XP-LC、100G-CK-C、100ME-CK-C、200G-CK-LC、100GS-CK-C、100G-LC-C、100G-ME-C、および 10x10G-LC

カード動作モードと PPM を設定するには、次の手順に従います。

### 始める前に

- デバイス同期が完了しており、デバイスのインベントリ収集ステータスが「完了 (Completed)」であることを確認してください。デバイス同期が実行中の場合、PPM 設定変更の展開が失敗します。
- カードモードの設定は、OTU2-XP、MR-MXP、WSE、AR-XPE、AR-XP、および AR-MXP カードではサポートされていません。これらのカードのカード動作モードを設定するには、Cisco Transport Controller ツールを使用します。
- デバイス同期が完了しており、デバイスのインベントリ収集ステータスが「管理 (Managed)」または「完了 (Completed)」であることを確認してください。
- カードで設定変更を行う前に、すべてのカードできめ細かなインベントリが使用可能であることを確認してください。
- デフォルトでは、デバイススロットリングは無効です。デバイススロットリングを有効にするには、`cd /opt/CSCOLumos/xmp_inventory/xde-home/inventoryDefaults` に移動し、`vi onsTL1.def` を実行して次の xml タグを追加します。

```
<default attribute="DEVICE_THROTTLING">noOfconnections</default>
```

ここで、`noOfconnections` は EPNM への最大 TL1 セッションの番号です。

次に例を示します。<default attribute="DEVICE\_THROTTLING">6</default>

**ステップ 1** [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] を選択します。

**ステップ 2** 設定するデバイス名のハイパーリンクをクリックしてデバイスを選択し、そのデバイスの [シャーシ (Chassis)] ビューを起動します。

**ステップ 3** [シャーシエクスプローラ (Chassis Explorer)] を使用して、設定するカードを選択します。

**ステップ 4** 右側に表示されるウィンドウで [設定 (Configuration)] サブタブをクリックします。

**ステップ 5** [接続可能ポート モジュール (Pluggable Port Modules)] セクションを展開し、ポート モジュールとそれぞれの適切なペイロード値を設定します。

**ステップ 6** [ポート モジュール (Port Modules) ] セクションの [+] (追加) アイコンをクリックし、ポート モジュール (PPM) を作成します。PPM 番号を選択し、[保存 (Save) ] をクリックします。[PPM ポート (PPM Port) ] の値はデフォルトで [PPM (1 ポート) (PPM (1 port)) ] に設定されており、変更できません。

- (注)
- 選択されているカードに適用可能な最大数の PPM が作成されている場合、[+] (追加) アイコンは無効になります。次のステップに進む前に、選択されたカードに必要な数の PPM を作成する必要があります。100G-CK-C カードの場合、次の手順に進む前に、少なくとも 1 つの PPM を作成する必要があります。
  - 400G-XP-LC カードでは、次のステップで説明するカード動作モードの設定の前に、PPM 11 と 12 が作成されていることを確認してください (ただし、カードモードはいずれかのトランク ポートで作成されます)。PPM 11 と 12 がない場合、デバイスに展開される設定変更は失敗します。
  - このステップは、100G-LC-C、100G-ME-C、100G-CK-C、100ME-CK-C、200G-CK-LC、および 100GS-CK-C カードではオプションです。

**ステップ 7** [カード動作モード (Card Operating Modes) ] セクションを展開し、選択したカードの動作モードを設定します。

**ステップ 8** [+] (追加) アイコンをクリックしてサポートされているカード動作モードのリストを表示するか、または編集アイコンをクリックして既存のカード動作モードを変更します。10x10G-LC カードの場合、最大 5 つのカード動作モード (クライアントまたはトランク ポートのセットとして動作可能な 10 ポート) を追加できますが、その他のすべてのカードでは、設定できるカード動作モードは 1 つだけです。カード動作モードを設定すると、「+」 (追加) アイコンは無効になります。

**ステップ 9** 左側のパネルから動作モードを選択してパラメータを変更します。

- (注)
- カードのピア構成に基づいて、一部のカード動作モードが無効になります。動作モードの横にある [i] アイコンをクリックして、動作モードを有効にする方法を確認します。動作モードを有効にするために必要なピアカード構成については、以下の「表 1」を参照してください。
  - MXP カードの場合、トランクカード、ピアカード、およびピアスキップカード構成が、以下に説明する順序になっていることを確認してください。

カード動作モード	トランクカード	ピアカード	ピアスキップカード
MXP_200G	スロット 2	スロット 3	スロット 4
ONS 15454 M6 デバイスの MXP_200G	スロット 2 または 7 の 100GS-CK-LC または 200G-CK-LC カード。	スロット 3、4 または 5、6。	スロット 3、4 または 5、6。
Cisco NCS 2015 デバイスの MXP_200G	スロット 2、7、8、13 または 14 の 100GS-CK-LC または 200G-CK-LC カード。	隣接スロットの MR-MXP カード。	隣接スロットの MR-MXP カード。
MXP_10x10G_100G	スロット 7	スロット 6	スロット 5
ONS 15454 M6 デバイスの MXP_10x10G_100G	スロット 2 または 7 の 100GS-CK-LC または 200G-CK-LC カード	隣接スロット 3、4 または 5、6 の MR-MXP カード。	隣接スロット 3、4 または 5、6 の MR-MXP カード。
Cisco NCS 2015 デバイスの MXP_10x10G_100G	スロット 2、7、8、13 または 14 の 100GS-CK-LC または 200G-CK-LC カード。	隣接スロットの MR-MXP カード。	隣接スロットの MR-MXP カード。
ONS 15454 M6 デバイスの MXP_CK_100G	100GS-CK-LC または 200G-CK-LC カードとピア MR-MXP カードを隣接スロット 2-3、4-5、6-7 に装着する必要があります。		
Cisco NCS 2015 デバイスの MXP_CK_100G	100GS-CK-LC または 200G-CK-LC カードとピア MR-MXP カードを隣接スロット 2-3、4-5、6-7、8-9、10-11、12-13、14-15 に装着する必要があります。		

400G-XP-LC カードの場合は、M-100G/M-200G のトランク動作モードで OTNXC カードの動作モードを設定できます。トランク動作モードに基づいてサポートされるスライス設定（それぞれ「スライス 1 とスライス 4」またはスライス 1、2、3、4）は OPM-100G と OPM-10x10G です。

トランク 11 で設定されているトランク動作モードは、トランク 12 に自動的に反映されます。たとえば、トランク 11 で M-200G を設定すると、トランク 12 のトランク動作モードはグレー表示されます。ただし、M-200G はトランク 12 に自動的に設定されます。OPM\_100G スライスと OPM\_10x10G スライスを混在させることができ、スライスそれぞれは互いの影響を受けません。

**ステップ 10** [保存 (Save)] をクリックして、デバイスに変更を展開します。

**ステップ 11** [接続可能ポート モジュール (Pluggable Port Modules)] セクションを展開して、各 PPM のペイロード値を設定します。

**ステップ 12** [接続可能ポート モジュール (Pluggable Port Modules)] セクションの [+] (追加) アイコンをクリックします。

(注) 一部の PPM では、該当するペイロード値が有効ではないことがあります。有効にするには、上記のステップ 9 で説明したカードモードの設定を行い、ペイロード値をもう一度設定してみます。

**ステップ 13** 選択した PPM に関連付ける必要があるポート番号、ポートタイプ、およびレーン数を選択します。[ポートタイプ (ペイロード) (Port Type (payload))] には、以下の「表 1」で説明するサポートされているクライアント信号のいずれかを設定できます。

- (注)
- 指定されたポートタイプ (ペイロード) が、選択されているカードモードまたは PPM でサポートされていない場合は、デバイスへの変更の展開が失敗します。指定するペイロード値が、選択したカードでサポートされていることを確認します。参考のために「表 1」を参照してください。
  - レーン数は、ペイロード値の分割が可能なカードでのみ設定できます。その他のすべてのカードでは、[レーン数 (Number of Lanes)] フィールドは無効になっています。

**ステップ 14** [終了 (Finish)] をクリックして、デバイスに変更を展開します。

**ステップ 15** (オプション) Cisco EPN Manager で変更が表示されない場合、これは複数のユーザーが同じカードモード設定を操作しているために、変更が動的に反映されていないことが原因で発生している可能性があります。最新の変更を表示するには、各セクションの [更新 (Refresh)] アイコンをクリックします。

展開が失敗する場合は、エラー ログ フォルダ (/opt/CSCOlumos/logs/config.log) に移動して、エラーの原因の詳細を確認してください。

## SONET および Flex の回線カードの設定

この手順では、Cisco EPN Manager を使用して 10X10G-LC SONET カードと 400G-XP、200G-CK-LC、および 100GS-CK-LC Flex カードの回線カードの設定を変更する方法について説明します。

この機能は Cisco NCS 2000 と Cisco ONS のデバイスでのみサポートされています。

SONET または Flex 回線カードを設定するには、次の手順を実行します。

#### 始める前に

- SONET 回線カードを設定するには、動作モード MXP10X10G および OC192 のペイロード値を持つカードを選択してください。
- SONET または Flex の回線カード設定を削除するには、選択したカードに関連付けられているペイロード値を削除する必要があるだけです。これにより、SONET または Flex の設定がデバイスから自動的に削除されます。ペイロード値を削除するには、[設定 (Configuration)] サブタブの下にある [接続可能なポートモード (Pluggable Port Mode)] 領域を使用します。
- SONET または Flex の回線カードの設定中に、回線カードのタイプを SONET から SDH に変更する場合、またはその他の同様の変更を行う場合は、まずデバイスの管理状態が [OOS 無効 (OOS-Disabled)] に設定されていることを確認する必要があります。デバイスの状態が [OOS 無効 (OOS-Disabled)] でない場合、デバイスに展開された回線設定の変更は失敗します。
- Flex 回線カードを設定するには、カードのカード動作モードが以前に設定済みであることを確認します。カードの設定：400G-XP-LC、100G-CK-C、100ME-CK-C、200G-CK-LC、100GS-CK-C、100G-LC-C、100G-ME-C、および 10x10G-LC (106 ページ) を参照してください。

**ステップ 1** [シャーシビューを開く](#)の説明に従って、シャーシビューを起動します。

**ステップ 2** 次のいずれかの方法で、設定するカードのスロットを選択します。

- ズームインとズームアウトのオプションを使用して、物理 [シャーシビュー (Chassis View)] からスロット内のカードを選択します。
- [シャーシエクスプローラ (Chassis Explorer)] ビューを使用し、カードに移動して選択します。

**ステップ 3** 右側に表示されるウィンドウで [設定 (Configuration)] サブタブをクリックします。

**ステップ 4** [ライン (Line)] セクションを展開し、[SONET] または [Flex] サブタブを選択します。

SONET の設定でサポートされているカードは 10x10G-LC カードのみです。Flex カードの場合は、400G-XP、200G-CK-LC、および 100GS-CK-LC カードです。

**ステップ 5** 設定を編集するには、次のいずれかの方法を選択します。

- 編集する設定の [SONET] タブまたは [Flex] タブを選択し、[編集] アイコンをクリックします。
- 編集するインラインパラメータを、テーブルの行内で 1 つずつクリックします。

**ステップ 6** 次の表に示すパラメータに必要な変更を加え、[保存 (Save)] をクリックしてデバイスに変更を展開します。

SONET パラメータの設定時：

- [タイプ (Type) ] を [SDH] に設定すると、[メッセージの同期 (Sync Messages) ] チェックボックスが自動的に無効になり、設定できません。
- [メッセージの同期 (Sync Messages) ] チェックボックスを有効にすると、[管理者SSM (AdminSSM) ] オプションが無効になり、null に設定されます。

Flex パラメータの設定時：

- 400G-XP-LC カードの場合、Flex ラインカードはトランク ポート 11/12 に対してのみ設定できます。
- 100GS-CK-LC カードの場合、Flex ラインカードはトランク ポート 2 に対してのみ設定できます。

表 9: SONET および Flex ラインの設定パラメータと説明

ラインカードのタイプ	ラインカードの設定パラメータ	説明
SONET	ポート番号 (Port Number)	設定する SONET インターフェイスのポート番号。
	ポート名 (Port Name)	SONET 光ポートの名前を追加できます。
	SD BER	信号劣化ビット エラー レートを設定します。
	SF BER	信号障害ビット エラー レートを設定します。
	タイプ (Type)	ポートを SONET または SDH として定義します。
	同期を提供 (Provides Sync)	オンにすると、カードは NE のタイミング基準としてプロビジョニングされます。
	メッセージングの同期 (Sync Messaging)	同期ステータスメッセージ (S1 バイト) をイネーブルにします。これにより、ノードで最適なタイミングソースを選択できるようになります。
管理 SSM 入力 (Admin SSM In)	<p>ノードが SSM 信号を受信しない場合、デフォルトで STU (Synchronization Traceability Unknown) になります。管理者 SSM を使用すると、STU 値を次のいずれかでオーバーライドできます。</p> <ul style="list-style-type: none"> <li>• PRS : プライマリ基準ソース (Stratum 1)</li> <li>• STS2 : Stratum 2</li> <li>• TNC - トランジット ノードクロック</li> <li>• STS3E : Stratum 3E</li> <li>• STS3 : Stratum 3</li> <li>• SMC : SONET 最小クロック</li> <li>• ST4 : Stratum 4</li> </ul>	



ラインカードのタイプ	ラインカードの設定パラメータ	説明
Flex	ポート (Port)	設定する Flex インターフェイスのポート番号。
	グリッドレス (Gridless)	<p>選択したカードのグリッドレス調整機能を有効または無効にします。この機能を有効にすると、カードの周波数値を設定できます。選択できるオプションは、次のとおりです。</p> <ul style="list-style-type: none"> <li>• 有効：選択すると、Flex の周波数パラメータを編集できます。</li> <li>• 無効：選択すると、Flex の周波数パラメータが無効になります。</li> </ul>
	周波数 (Frequency)	400G-XP、200G-CK-LC、および 100GS-CK-LC カードのポートの周波数を、191350 ～ 196100 の範囲で指定します。

## 着脱可能ポート モジュールおよびカード モード設定の編集と削除

始める前に

**PPM を削除するための前提条件：**

- PPM がアクティブ回線またはプロビジョニング回線の一部となっていないことを確認します。
- PPM とそのそれぞれのペイロード値を、以下の手順で説明している順序でのみ削除する必要があります。先にクライアント ポート 1 ～ 10 を手動で削除してから、関連付けられた PPM を削除します。
- デバイス同期が完了しており、デバイスのインベントリ収集ステータスが「完了 (Completed)」または「管理 (Managed)」であることを確認します。

**カード動作モードを削除するための前提条件：**

- カードがアクティブ回線またはプロビジョニング回線の一部となっていないことを確認します。
- 400G-XP カードの場合、PPM 11 および 12 は削除できません。これらの PPM は、関連付けられたカード動作モードが削除されると自動的に削除されます。
- ピアカードまたはスキップカードがアクティブ状態でない必要があります。CTC を使用してピアカードまたはスキップカードの関連付けを削除してから、Cisco EPN Manager を使用して再びカード動作モードの削除を試すことができます。Cisco EPN Manager から直接、カードの削除を試みることもできます。詳細については、[カードの削除 \(103ページ\)](#) を参照してください。

- ステップ1 [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] を選択します。
- ステップ2 設定するデバイス名のハイパーリンクをクリックしてデバイスを選択し、そのデバイスの [シャーシ (Chassis)] ビューを起動します。
- ステップ3 [シャーシエクスプローラ (Chassis Explorer)] を使用して、設定を削除するカードを選択します。
- ステップ4 右側に表示されるウィンドウで [設定 (Configuration)] サブタブをクリックします。
- ステップ5 着脱式ポート モジュール (PPM) を削除するには、[着脱式ポートモジュール (Pluggable Port Modules)] セクションを展開します。
- [着脱式ポートモジュール (Pluggable Port Modules)] サブセクションで、削除対象の関連付けられたペイロード値を選択し、[X] (削除) アイコンをクリックします。
  - [OK] をクリックして確定します。変更がデバイスに展開されます。
  - [ポートモジュール (Port Modules)] サブセクションで、削除する PPM を選択し、[X] (削除) アイコンをクリックします。
  - [OK] をクリックして確定します。変更がデバイスに展開されます。
- (注) PPM を削除する前に、対象の PPM に関連付けられているすべてのペイロード値を削除する必要があります。
- ステップ6 [カード動作モード (Card Operating Modes)] セクションを展開し、カードの設定を削除します。
- カードモードの設定を編集するには、必ず 400G-XP カードのみを選択し、編集アイコンをクリックして変更を加えます。他のカードの設定を編集する場合はすべて、カードモードの設定を削除してから、新しい値で再作成する必要があります。
  - カードモードの設定を削除するには、削除が必要なカードモードの設定を選択し、[X] (削除) アイコンをクリックします。
  - [OK] をクリックして確定します。変更がデバイスに展開されます。

## Cisco NCS 2000 デバイス用のカードとサポートされる設定

表 10: 100GS-CK-LC および 200G-CK-LC カード: サポートされる構成

カード動作モード	トランク カード	ピア カード	ピア スキップカード	サポートされるペイロードタイプ

MXP_200G	スロット 2、7、8、13 または 14 の 100GS-CK-LC または 200G-CK-LC カード。	スロット 3、6、9、12、または 15 の MR-MXP カード。	スロット 4、5、10、11 または 16 の MR-MXP カード。	100GE と OTU4 OTU4 は 200G-CK-LC カードでのみサポートされています。任意の 100 G 構成の再生成 10GE 10GE 100GE
MXP_10x10G_100G	スロット 2、7、8、13 または 14 の 100GS-CK-LC または 200G-CK-LC カード。	スロット 3、6、9、12、または 15 の 10x10G-LC カード。	スロット 4、5、10、11 または 16 の MR-MXP カード。	100GE と OTU4 OTU4 は 200G-CK-LC カードでのみサポートされています。任意の 100 G 構成の再生成 10GE 10GE 100GE
MXP_CK_100G	100GS-CK-LC または 200G-CK-LC カードとピア MR-MXP カードを隣接スロット 2-3、4-5、6-7、8-9、10-11、12-13、14-15 に装着する必要があります。	該当なし	該当なし	100GE と OTU4 OTU4 は 200G-CK-LC カードでのみサポートされています。任意の 100 G 構成の再生成 10GE 10GE 100GE
RGN-100G	100GS-CK-LC または 200G-CK-LC カードとピアカード 100GS-CK-LC または 200G-CK-LC を隣接スロット 2-3、4-5、6-7、8-9、10-11、12-13、14-15 に装着する必要があります。	該当なし	該当なし	100GE と OTU4 OTU4 は 200G-CK-LC カードでのみサポートされています。任意の 100 G 構成の再生成 10GE 10GE 100GE

TXP-100G	100GS-CK-LC または 200G-CK-LC	該当なし	該当なし	該当なし
----------	----------------------------	------	------	------

表 11: 100G-CK-C および 100ME-CKC カード : サポートされる構成

カード動作モード	トランク カード	ピア カード	スキップ カード	サポートされるペイロードタイプ
TXP-100G	100G-CK-C/ 100ME-CKC	該当なし	該当なし	100GE、OTU4 : 任意の 100 G 構成の再生成 40GE
RGN-100G	100G-CK-C/ 100ME-CKC カードとピアカード  100G-LC-C/ 100G-ME-C/ 100G-CK-C/ 100ME-CKC を隣接スロット 2-3、 4-5、6-7、8-9、10-11、12-13、14-15 に装着する必要がある。	該当なし	該当なし	100GE、OTU4 : 任意の 100 G 構成の再生成 40GE
MXP-2x40G	100G-CK-C/ 100ME-CKC	該当なし	該当なし	100GE、OTU4 : 任意の 100 G 構成の再生成 40GE

表 12: 100G-LC-C および 100G-ME-C カード : サポートされる構成

カード動作モード	トランク カード	ピア カード	スキップ カード	サポートされるペイロードタイプ
TXP-100G	100G-LC-C/ 100G-ME-C	該当なし	該当なし	100GE、OTU4 : 任意の 100 G 構成の再生成 40GE
RGN-100G	100G-LC-C/ 100G-ME-C カードとピアカード 100G-LC-C/ 100G-ME-C/ 100G-CK-C/ 100ME-CKC を隣接スロット 2-3、 4-5、6-7、8-9、10-11、 12-13、14-15 に装着する必要がある。	該当なし	該当なし	100GE、OTU4 : 任意の 100 G 構成の再生成 40GE

表 13: 10X10G-LC カード : サポートされる構成

カード動作モード	トランク カード	ピアカード	スキップカード	サポートされるペイロードタイプ
TXPP-10G	10x10G-LC	該当なし	該当なし	<p>OC192/STM-64、10GE-LAN Phy、10GE-WANPhy (OC192を使用)、OTU2、OTU2e、8G FC、10G FC、FICON</p> <p>10x10G-LC カードを 100GS-CK-LC カードに接続すると、OC192/STM64 および 10GE のみがサポートされます。</p> <p>10x10G-LC カードを 200G-CK-LC カードに接続すると、OC192/STM64、10GE、および OTU2 のみがサポートされます。</p> <p>10GE-LAN Phy、OTU2</p> <p>10GE-LAN Phy、OTU2e、OTU2、OC192/STM-64、8G FC、10G FC、IB_5G</p> <p>10GE、10G FC</p> <p>10GE</p> <p>10GE、OTU2e</p>
TXP-10G	10x10G-LC	該当なし	該当なし	<p>OC192/STM-64、10GE-LAN Phy、10GE-WANPhy (OC192を使用)、OTU2、OTU2e、8G FC、10G FC、FICON</p> <p>10x10G-LC カードを 100GS-CK-LC カードに接続すると、OC192/STM64 および 10GE のみがサポートされます。</p> <p>10x10G-LC カードを 200G-CK-LC カードに接続すると、OC192/STM64、10GE、および OTU2 のみがサポートされます。</p> <p>10GE-LAN Phy、OTU2</p> <p>10GE-LAN Phy、OTU2e、OTU2、OC192/STM-64、8G FC、10G FC、IB_5G</p> <p>10GE、10G FC</p> <p>10GE</p> <p>10GE、OTU2e</p>

MXP-10x10G	10x10G-L カードと ピア 100G-LC-C、 100G-ME-C、 100G-CK-C、 100ME-CKC、 100GS-CK-LC また は200G-CK-LC カー ドを隣接スロット 2-3、4-5、6-7、 8-9、10-11、12-13、 14-15 に装着する必 要がある。	該 当 な し	該 当 な し	<p>OC192/STM-64、10GE-LAN Phy、 10GE-WAN Phy (OC192を使用)、OTU2、 OTU2e、8G FC、10G FC、FICON</p> <p>10x10G-LC カードを 100GS-CK-LC カード に接続すると、OC192/STM64 および 10GE のみがサポートされます。</p> <p>10x10G-LC カードを 200G-CK-LC カード に接続すると、OC192/STM64、10GE、お よび OTU2 のみがサポートされます。</p> <p>10GE-LAN Phy、OTU2</p> <p>10GE-LAN Phy、OTU2e、OTU2、 OC192/STM-64、8G FC、10G FC、IB_5G</p> <p>10GE、10G FC</p> <p>10GE</p> <p>10GE、OTU2e</p>
RGN-10G	10x10G-LC	該 当 な し	該 当 な し	<p>OC192/STM-64、10GE-LAN Phy、 10GE-WAN Phy (OC192を使用)、OTU2、 OTU2e、8G FC、10G FC、FICON</p> <p>10x10G-LC カードを 100GS-CK-LC カード に接続すると、OC192/STM64 および 10GE のみがサポートされます。</p> <p>10x10G-LC カードを 200G-CK-LC カード に接続すると、OC192/STM64、10GE、お よび OTU2 のみがサポートされます。</p> <p>10GE-LAN Phy、OTU2</p> <p>10GE-LAN Phy、OTU2e、OTU2、 OC192/STM-64、8G FC、10G FC、IB_5G</p> <p>10GE、10G FC</p> <p>10GE</p> <p>10GE、OTU2e</p>
低遅延	10x10G-LC	該 当 な し	該 当 な し	該 当 な し

ファンアウト - 10X10G	10x10G-LC	該当なし	該当なし	<p>OC192/STM-64、10GE-LAN Phy、10GE-WAN Phy (OC192を使用)、OTU2、OTU2e、8G FC、10G FC、FICON</p> <p>10x10G-LCカードを100GS-CK-LCカードに接続すると、OC192/STM64および10GEのみがサポートされます。</p> <p>10x10G-LCカードを200G-CK-LCカードに接続すると、OC192/STM64、10GE、およびOTU2のみがサポートされます。</p> <p>10GE-LAN Phy、OTU2</p> <p>10GE-LAN Phy、OTU2e、OTU2、OC192/STM-64、8G FC、10G FC、IB_5G</p> <p>10GE、10G FC</p> <p>10GE</p> <p>10GE、OTU2e</p>
-----------------	-----------	------	------	--

Cisco NCS 2000 デバイスの 400G-XP-LC カードおよび MR-MXP カードは、次のカード動作モードとペイロード値で設定できます。

- ペイロードタイプ OTU2/OC192 は MR-MXP カードでサポートされます。
- ペイロードタイプ 16G-FC/OTU2 は 400G-XP-LC カードでサポートされます。
- スライス動作モード OPM\_6x16G\_LC は 400G-XP-LC カードでサポートされます。

## MPLS LDP および MPLS-TE リンクの検出と設定

Cisco EPN Manager を使用して、MPLS ネットワークでラベル配布プロトコル (LDP) および MPLS-TE リンクを設定できます。

### MPLS LDP

LDP は、基になる IGP ルーティング プロトコルによって選択されたルートにラベルを割り当てることにより、MPLS ネットワークにおけるホップバイホップ (つまりダイナミック ラベル) 配布の標準の方式を提供します。この結果得られるラベル付きパスはラベルスイッチドパス (LSP) と呼ばれ、これによりラベル付きトラフィックが MPLS バックボーン全体に転送されます。Cisco EPN Manager を使用すると、潜在的なピアを設定し、それらのピアとの LDP セッションを確立して情報を交換できます。

Cisco EPN Manager を使用して LDP を設定するには、LDP リンクの設定を必要とするデバイスのネットワーク アドレスとインターフェイス、および設定する IP アドレスのサブネットマスクを知る必要があります。



(注) MPLS LDP を設定する前に、LDP ID がデバイスで事前に設定されていることを確認してください。

### MPLS-TE

Cisco EPN Manager は、MPLS トラフィック エンジニアリング (MPLS-TE) 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 により、MPLS バックボーンにおいてレイヤ 2 の TE 機能をレイヤ 3 経由でレプリケートして拡張できます。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。

LDP パラメータと MPLS-TE パラメータを設定する手順は次のとおりです。

**ステップ 1** [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] の順に選択します。

**ステップ 2** 設定するデバイスのハイパーリンクをクリックしてデバイスを選択し、[デバイスの詳細 (Device Details)] ページを起動します。

**ステップ 3** [論理ビュー (Logical View)] タブをクリックします。

(注) デバイスに提供されている EPNM サポートのレベルに応じて、[Logical View] タブが表示される場合があります。

**ステップ 4** LDP リンクを設定する手順は次のとおりです。

a) [MPLS] > [LDP] を選択し、[共通プロパティ (Common Properties)] タブをクリックし、[+] をクリックして新しい LDP パラメータを指定します。既存のパラメータを編集するには、[LDP アドレス (LDP Address)] ハイパーリンクをクリックし、ページの右上隅にある [編集 (Edit)] アイコンをクリックします。

(注) デバイスごとに 1 セットの LDP 設定のみ追加できます。

b) [共通プロパティ (Common Properties)] タブで、次の表に示す LDP パラメータを指定します。

MPLS LDP のフィールド	フィールドの説明
LDP インターフェイス (LDP Interface)	デバイス上の LDP セッションのソース ループバック インターフェイスとなる LDP インターフェイスを選択します。
LDP アドレス (LDP Address)	LDP インターフェイスの IP アドレスを指定します。いったん設定した LDP アドレスは編集できません。LDP アドレスを変更するには、LDP セッションを削除し、新しい LDP アドレスを使用して新しいセッションを作成します。
セッション保留時間 (Session Hold Time)	(任意) 保留タイマーが期限切れになった後に hello を受信しなかった場合に LDP セッションがダウンする時間 (秒単位) を入力します。範囲は 15 ~ 65535 です。



MPLS LDP のフィールド	フィールドの説明
NSR の有効化 (NSR Enabled)	true または false を選択して、LDP ノンストップルーティング (NSR) を有効または無効にします。NSR を有効にすると、ラベル配布プロトコル (LDP) がピアセッションを失うことなく動作を継続できます。
検出保留時間 (Discovery Hold time) と検出ターゲット保留時間 (Discovery Target Hold time)	(任意) LDP ソースと検出された LDP ネイバーから LDP hello メッセージを受信しなくてもそのネイバーを記憶しておく時間 (秒単位) を入力します。範囲は 1 ~ 65535 です。
検出保留間隔 (Discovery Hold Interval) と検出ターゲット保留間隔 (Discovery Target Hold Interval)	(任意) LDP ソースと検出された LDP ネイバーを記憶しておく時間間隔 (秒単位) を入力します。範囲は 1 ~ 65535 です。
ダウンストリーム最小ラベル (DownStream Min Label) とダウンストリーム最大ラベル (DownStream Max Label)	(任意) LSP で許可され、ダウンストリーム オン デマンド方式のラベル配布により確立される最小および最大ホップ数を入力します。ISO XE の場合は 16 ~ 32767、ISO XR デバイスの場合は 16000 ~ 1048575 の範囲で指定します。
ダウンストリーム最大ホップ数 (DownStream Max Hop Count)	(任意) LSP で許可され、ダウンストリーム オン デマンド方式のラベル配布により確立されるホップ数を入力します。範囲は 1 ~ 255 です。
IGP ホールド ダウン時間 (IGP Hold Down Time)	(任意) リンクアップ時のセッション確立後に LDP 同期ステータスの宣言が遅延される時間 (秒単位) を入力して指定します。ISO XE の場合は 1 ~ 2147483647 ミリ秒、ISO XR デバイスの場合は 5 ~ 300 ミリ秒の範囲で指定します。
エントロピーの有効化 (Entropy Enabled)	true または false を選択して、MPLS LDP エントロピー ラベル サポート機能を有効または無効にします。この機能は、エントロピーラベルを使用して MPLS ネットワーク間の負荷分散を改善するのに役立ちます。
明示的ヌルの有効化 (Explicit Null Enabled)	(任意) 直接接続されたルートの明示的 null ラベルをアドバタイズするには、この値を有効にします。値は Yes (有効) または No (無効) です。
初期バックオフ (Initial Back Off) と最大バックオフ (Max Back Off)	(任意) 初期バックオフ遅延値と最大バックオフ遅延値 (秒単位) を入力します。範囲は 5 ~ 2147483 です。

- c) [保存 (Save)] をクリックして、変更内容をデバイスに展開します。
- d) [インターフェイス (Interfaces)] をクリックし、[+] をクリックしてインターフェイスパラメータを指定します。

MPLS LDP のフィールド	フィールドの説明
インターフェイス名 (Interface Name)	LDP セッションに参加するインターフェイスの名前を指定します。
ラベル配布方法 (Label Distribution Method)	ラベル配布方法として「LDP」を指定します。
Hello 間隔 (Hello Interval)	(任意) hello メッセージが送信される時間間隔 (秒単位) を入力します。範囲は 1 ~ 65535 です。

- e) [保存 (Save)] をクリックして、変更内容をデバイスに展開します。同じプロパティがピア デバイスで構成されます。ネイバー デバイスが形成されると、[ネイバー (Neighbors)] タブに詳細が設定されます。

**ステップ 5** MPLS-TE リンクを設定する手順は次のとおりです。

- a) [MPLS] > [MPLS-TE] を選択します。  
 b) [MPLS-TE FRR] 領域で、[MPLS TE Tunnel Enabled] チェックボックスをオンにします。MPLS-TE パラメータのデフォルト値は、次の表に示すように表示されます。

MPLS TE トンネルのフィールド	フィールドの説明
MPLS TE トンネルの有効化 (MPLS TE Tunnel Enabled)	自動帯域幅対応トンネルのリストの表示を有効にし、トンネルの現在の信号送信帯域幅が、自動帯域幅によって適用される帯域幅と同じかどうかを示します。
自動帯域幅タイマー周波数 (秒) (Auto Bandwidth Timer Frequency (Sec))	トンネル インターフェイスの自動帯域幅がトリガーされる間隔 (秒単位) を設定します。
タイマー周波数の再最適化 (秒) (Reoptimize Timer Frequency (Sec))	すべての TE トンネルの再最適化間隔をトリガーする値 (秒単位) を設定します。
自動バックアップトンネルの有効化 (Auto Backup Tunnel Enabled)	自動的に構築される MPLS-TE バックアップ トンネルに関する情報を表示します。
バックアップ トンネル最小範囲 (Backup Tunnel Min. Range) とバックアップ トンネル最大範囲 (Backup Tunnel Max. Range)	指定した最小値と最大値の間でバックアップ自動トンネル番号の範囲を設定します。バックアップ トンネルの最小範囲は最大範囲よりも小さくしてください。
SRLG を除く (SRLG Exclude)	除外の目的で SRLG 値を取得する IP アドレスを指定します。必要に応じて、次のいずれかのオプションを選択します。 <ul style="list-style-type: none"> <li>• 優先 (Preferred)</li> <li>• 強制 (Forced)</li> <li>• なし (None)</li> </ul> (注) [SRLG を除く (SRLG Exclude)] オプションは IOS-XE でのみ使用できます。

MPLS TE トンネルのフィールド	フィールドの説明
番号付けされていないインターフェイス (Un-numbered Interface)	明示的なアドレスを使用せずに、指定したインターフェイスでの IP 処理を有効にします。

ステップ 6 [保存 (Save)] をクリックして、変更内容をデバイスに展開します。

### 次のタスク

ネットワーク トポロジ上で LDP リンクを監視します。

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。
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。
3. トポロジツールバーで [表示 (Show)] をクリックし、[リンク (Links)] を選択します。
4. [コントロールプレーン (Control Plane)] の [LDP] チェックボックスをオンにすると、マップ上に LDP リンクが表示されます。
5. LDP リンクをクリックすると、リンクの詳細が表示されます。

MPLS-TE サービスをプロビジョニングする方法については、[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](#)を参照してください。

## SPAN と RSPAN を使用したポートの分析

Cisco EPN Manager を使用すると、SPAN または RSPAN を使用して、スイッチ上の別のポートまたはモニター デバイスにトラフィックのコピーを送信することで、ポートまたは VLAN を通過するネットワーク トラフィックを解析できます。SPAN では、送信元ポート上または送信元 VLAN 上で受信、送信、または送受信されたトラフィックが宛先ポートにコピー (ミラーリング) されて解析されます。送信元ポートに出入りするトラフィックや、送信元 VLAN に出入りするトラフィックが監視されます。

着信トラフィックを監視するように SPAN を設定した場合、別の VLAN から送信元 VLAN にルーティングされるトラフィックは監視できません。ただし、送信元 VLAN で受信され、別の VLAN にルーティングされるトラフィックは監視できます。

Cisco EPN Manager では、デバイスごとに 1 つのローカル SPAN セッションのみを設定できます。ローカル SPAN セッションでは、1 つ以上の送信元ポートからのトラフィックが宛先ポートにコピーされて解析されます。

リモート SPAN を使用すると、異なるスイッチ上の送信元ポート、送信元 VLAN、および宛先ポートを設定でき、ネットワーク上にある複数のスイッチのリモートモニターリングが可能になります。各 RSPAN セッションのトラフィックは、ユーザーが指定した RSPAN VLAN 上で

伝送されます。この RSPAN VLAN は、参加しているすべてのスイッチで RSPAN セッション専用です。送信元ポートまたは VLAN からの RSPAN トラフィックは RSPAN VLAN にコピーされ、RSPAN VLAN を伝送するトランクポートを介して、RSPAN VLAN を監視する宛先セッションに転送されます。



(注) ポートを監視するには、ポートを1つ以上の VLAN（送信元または宛先）に関連付ける必要があります。

ポートの監視（またはミラーリング）を有効にする手順は次のとおりです。

**ステップ 1** [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] の順に選択します。

**ステップ 2** 設定するデバイスのハイパーリンクをクリックしてデバイスを選択し、[デバイスの詳細 (Device Details)] ページを起動します。

**ステップ 3** [論理ビュー (Logical View)] タブをクリックします。

**ステップ 4** RSPAN セッションを設定します。

- a) [ポートアナライザ (Port Analyzer)] > [RSPAN] > [宛先ノード (Destination Node)] の順に選択し、RSPAN の宛先ノードを設定します。
- b) [+] をクリックして RSPAN セッション ID を指定します。既存の設定を編集するには、セッション ID のハイパーリンクをクリックし、ページの右上隅にある [編集 (Edit)] アイコンをクリックします。  
最大 14 個の RSPAN セッションと SPAN セッションを追加できます。
- c) セッション ID を選択し、[保存 (Save)] をクリックします。  
セッションタイプのリモート宛先 (リモート RSPAN) はデフォルトで設定されており、編集できません。
- d) セッション ID のハイパーリンクをクリックし、宛先ノードの送信元設定と宛先設定を指定します。
- e) [送信元設定 (Source Settings)] タブをクリックし、有効な VLAN ID (選択したデバイスで設定された VLAN に基づいて自動設定) を選択して、[保存 (Save)] をクリックします。  
宛先ノードの送信元として追加できる VLAN は 1 つだけです。VLAN を設定していない場合は、設定してからこの手順に戻る必要があります。[VLAN のインターフェイスの表示 \(56 ページ\)](#) を参照してください。
- f) [宛先設定 (Destination Settings)] タブをクリックし、RSPAN の宛先ノードとして機能させるインターフェイスを選択して、[保存 (Save)] をクリックします。
- a) 機能パネルから、[ポートアナライザ (Port Analyzer)] > [RSPAN] > [送信元ノード (Source Node)] の順に選択し、RSPAN の送信元ノードを設定します。
- b) [+] をクリックし、共通の RSPAN 送信元ノード設定を指定します。既存の設定を編集するには、セッション ID のハイパーリンクをクリックし、ページの右上隅にある [編集 (Edit)] アイコンをクリックします。
- c) セッション ID を選択し、[保存 (Save)] をクリックします。  
セッションタイプ [リモート送信元 (リモート RSPAN)] はデフォルトで設定されており、編集できません。

- d) セッションIDのハイパーリンクをクリックし、送信元ノードの送信元設定と宛先設定を指定します。
- e) [送信元設定 (Source Settings)] タブをクリックし、次の値を指定して、[保存 (Save)] をクリックします。
  - i) [インターフェイス (Interface)] ドロップダウンメニューで、RSPAN 送信元ノードの送信元インターフェイスとして機能するインターフェイスを選択します。

RSPAN の送信元ノードとして指定したインターフェイスは、SPAN の送信元/宛先ノードとしても使用できます。

- ii) [方向 (Direction)] ドロップダウンメニューで、インターフェイスを RSPAN 送信元ノードに適用する際の必要な方向を選択します。選択できるオプションは、次のとおりです。

- [送信 (Transmit)] : スイッチによる変更および処理がすべて完了した後に、送信元インターフェイスが送信したすべてのパケットをモニターします。送信元が送信した各パケットのコピーが、そのセッションに対応する宛先ポートに送られます。コピーはパケットの変更後に用意されます。
- [受信 (Receive)] : スイッチが変更または処理を行う前に、送信元インターフェイスまたはVLANが受信したすべてのパケットをモニターします。送信元が受信した各パケットのコピーが、そのセッションに対応する宛先ポートに送られます。
- [両方 (Both)] : (デフォルト値) 受信パケットと送信パケットの両方についてポートまたはVLANをモニターします。

RSPANの送信元ノードに複数のインターフェイスを追加し、それらのインターフェイスに単一のVLAN ID を関連付けることができます。

- f) [宛先設定 (Destination Settings)] タブをクリックし、有効な VLAN ID (選択したデバイスで設定された VLAN に基づいて自動設定) を選択して、[保存 (Save)] をクリックします。

#### ステップ5 SPAN セッションを設定します。

- a) [ポートアナライザ (Port Analyzer)] > [SPAN] をクリックします。
- b) [+] をクリックし、共通の SPAN 送信元ノード設定を指定します。既存の設定を編集するには、セッションIDのハイパーリンクをクリックし、ページの右上隅にある [編集 (Edit)] アイコンをクリックします。

RSPAN の送信元ノードおよび宛先ノードとして設定したインターフェイスは、SPAN 用には使用できません。

- c) セッションIDを選択し、[保存 (Save)] をクリックします。  
セッションタイプ[ローカル (ローカルRSPAN)] はデフォルトで設定されており、編集できません。
- d) セッションIDのハイパーリンクをクリックし、SPAN の送信元設定と宛先設定を指定します。
- e) [送信元設定 (Source Settings)] タブをクリックし、インターフェイスと、インターフェイスを SPAN に適用する際の必要な方向を選択し、[保存 (Save)] をクリックします。詳細については、ステップ4を参照してください。

RSPAN の送信元ノードとして指定したインターフェイスは、SPAN の送信元/宛先ノードとしても使用できます。

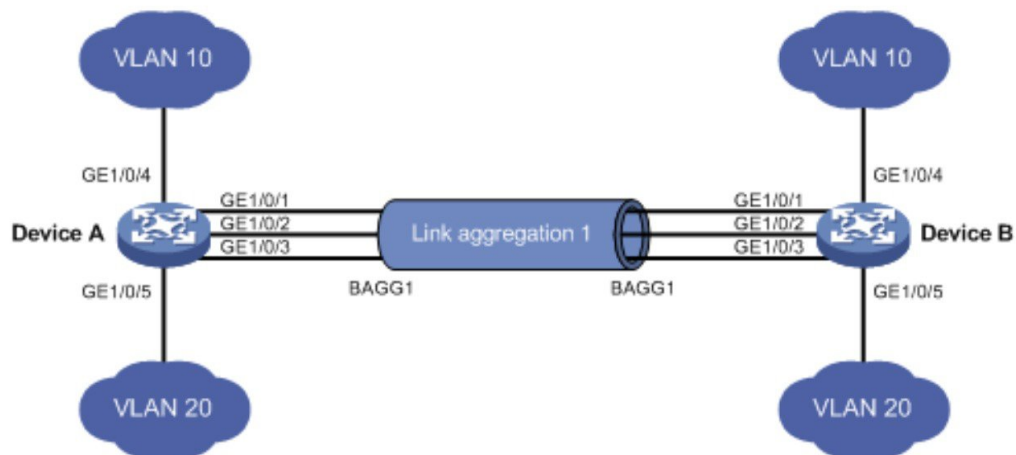
- f) [宛先設定 (Destination Settings)] タブをクリックし、有効な VLAN ID (選択したデバイスで設定された VLAN に基づいて自動設定) を選択して、[保存 (Save)] をクリックします。
- g) (任意) 変更が正しく構成されたことを確認するには、デバイス CLI で次のコマンドを使用します。

```
show monitor session all
```

## イーサネット Link Aggregation Group の設定と表示

イーサネット Link Aggregation Group (LAG) は、1つ以上のポートを集約したグループで、単一のリンクとして扱われます。各バンドルには、1つの MAC、1つの IP アドレス、1つの設定セット (ACL など) があります。LAG により、複数のスイッチポートを1つのスイッチポートとして扱うことができます。ポートグループは、2つのネットワーク要素間で高帯域接続を行う単一の論理ポートとして動作します。単一の LAGI により、トラフィックの負荷がチャンネルのリンク全体にわたって分散します。LAG は、2つのリンクを使用してサービスをプロビジョニングするのに役立ちます。リンクの一方で障害が発生すると、トラフィックが他方のリンクに移動します。

次の図は、デバイス A とデバイス B の2つのデバイス間で作成された LAG を示しています。



Cisco EPN Manager では次の方法で LAG を表示および管理できます。

- 複数のインターフェイスを使用した Link Aggregation Group (LAG) の作成 (127 ページ)
- イーサネット LAG プロパティの表示 (128 ページ)

## 複数のインターフェイスを使用した Link Aggregation Group (LAG) の作成

Cisco EPN Manager を使用すると、複数の物理スイッチポートを単一の論理スイッチポートとして扱う機能を提供する LAG を作成できます。

### 始める前に

- まだ既存の LAG の一部となっていないインターフェイスのみを選択できます。1つのインターフェイスを複数の LAG の一部にすることはできません。
- 選択したインターフェイスのグループはすべて同じ帯域幅タイプで構成されている必要があります。
- LAG に参加するデバイスのインベントリ収集ステータスは「完了 (Completed) 」となっている必要があります。

LAG を作成する手順は次のとおりです。

- 
- ステップ 1** [設定 (Configuration) ] > [ネットワークデバイス (Network Devices) ] を選択します。
  - ステップ 2** デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details) ] ページを起動します。
  - ステップ 3** [論理ビュー (Logical View) ] タブをクリックします。
  - ステップ 4** [インターフェイス (Interfaces) ] > [リンクの集約 (Link Aggregation) ] を選択します。
  - ステップ 5** 使用する制御方法の種類に応じて [PAgP] タブまたは [LACP] タブをクリックします。
  - ステップ 6** 追加 (+) 記号をクリックして新しい LAG を作成します。
  - ステップ 7** LAG の一意の名前を入力します。指定するチャンネルグループ ID が LAG 名の一部となるようにします。たとえば、チャンネルグループ ID が 10 の場合、LAG 名は次のようになります。
    - 「Bundle-Ether10」 (Cisco IOS-XR デバイスの場合)。
    - 「Port-channel10」 (Cisco IOS、Cisco ME3600、および Cisco ME3800 デバイスの場合)。
  - ステップ 8** チャンネルグループ ID を指定するには、1 ~ 16 の数値を入力します。各種デバイスのチャンネルグループ ID の範囲は、Cisco ASR 90X デバイスでは 1 ~ 8、Cisco ASR 920X デバイスでは 1 ~ 64、Cisco ME3x00 デバイスでは 1 ~ 26、Cisco NCS42xx デバイスでは 1 ~ 48、Cisco ASR9000 デバイスでは 1 ~ 65535 です。
  - ステップ 9** [メンバーポート設定 (Member Port Settings) ] タブをクリックし、メンバーポートの値を指定します。
    - LACP モード (LACP Modes) : LACP は次のモードに設定できます。
      - アクティブ (Active) : このモードでは、ポートから LACP パケットが定期的にパートナーポートに送信されます。
      - パッシブ (Passive) : このモードでは、パートナーポートから LACP パケットが送信されるまで、ポートから LACP パケットが送信されません。パートナーポートから LACP パケットを受信した後で、ポートは LACP パケットをパートナーポートに送信します。

- **PAgP モード (PAgP Modes)** : PAgP モードは、AUTO、DESIRABLE、または ON に設定できます。ASR9K デバイスでは、ON の PAgP モードのみ有効です。ON は、モードが PAgP - 手動に設定されたことを意味します。

**ステップ 10** [保存 (Save) ] をクリックします。

変更内容が保存され、作成された LAG にインターフェイスを追加できるようになりました。

**ステップ 11** 作成された LAG にインターフェイスを追加するには、[リンク集約 (Link Aggregation) ] テーブルから必要なチャンネル グループを選択し、[編集] アイコンをクリックします。

**ステップ 12** LAG の作成に使用するインターフェイスを選択します。

**ステップ 13** [保存 (Save) ] をクリックします。

選択したインターフェイスを使用して LAG が作成されます。

---

## イーサネット LAG プロパティの表示

イーサネット LAG のプロパティは次の方法で表示できます。

- デバイスの [設定 (Configuration) ] タブを使用する :

1. [ネットワークデバイス (Network Devices) ] > [デバイスのプロパティ (Device Properties) ] > [設定 (Configuration) ] タブに移動します。
2. デバイス名のハイパーリンクをクリックして、LAG を設定するデバイスを選択します。
3. [論理ビュー (Logical View) ] タブをクリックします。
4. [機能 (Features) ] パネルで、[インターフェイス (Interfaces) ] > [リンク集約 (Link Aggregation) ] をクリックします。

- [デバイスの詳細 (Device Details) ] タブを使用する :

1. [ネットワークデバイス (Network Devices) ] > [デバイスのプロパティ (Device Properties) ] に移動します。
2. デバイス名のハイパーリンクをクリックして、LAG を設定するデバイスを選択します。
3. [デバイスの詳細 (Device Details) ] タブをクリックします。
4. [機能 (Features) ] パネルで、[インターフェイス (Interfaces) ] > [イーサネットチャンネル (Ether Channel) ] をクリックします。



# ルーティングプロトコルとセキュリティの設定

Cisco EPN Manager を使用して、CE および光デバイス用に次のルーティングプロトコルを設定できます。ACL を使用してデバイスのセキュリティを設定することもできます。

ルーティングプロトコルやACLを設定する場合は、事前にデバイスのインベントリ収集ステータスが [完了 (Completed) ] であることを確認してください。

デバイスのルーティングテーブルを表示するには、[デバイス 360 (Device 360) ] ビューを開き、[操作 (Actions) ] > [ルーティングテーブル情報 (Routing Table Info) ] > [すべて (All) ] を選択します。

- [BGP の設定 \(129 ページ\)](#)
- [IS-IS の設定 \(134 ページ\)](#)
- [OSPF の設定 \(136 ページ\)](#)
- [スタティック ルーティングの設定 \(138 ページ\)](#)
- [ACL の設定 \(139 ページ\)](#)

## BGP の設定

ボーダーゲートウェイプロトコル (BGP) は、ネットワーク内の自律システム (AS) 間でルーティング情報と到達可能性情報を交換することを目的とした、標準化された外部ゲートウェイプロトコルです。BGP を設定することにより、デバイスでは、ネットワーク管理者が設定したパス、ネットワークポリシー、またはルールセットに基づいてルーティングを決定できます。

Cisco EPN Manager を使用すると、AS 番号とルータ ID を指定して、BGP ルーティングを設定し、BGP ルーティングプロセスを確立できます。そして、BGP ネイバーを作成できます。これにより、ルータが BGP ルーティングのためにネイバー コンフィギュレーションモードになり、ネイバーの IP アドレスが BGP ピアとして設定されます。BGP ネイバーを設定するには、ネイバーの IPv4 アドレスとそのピア AS 番号を指定する必要があります。BGP ネイバーは BGP ルーティングの一部として設定してください。BGP ルーティングを有効にするには、1 つ以上のネイバーと 1 つ以上のアドレス ファミリーを事前に設定しておく必要があります。

デバイスの BGP と BGP ネイバー ルーティングテーブルを表示するには、[デバイス 360 (Device 360) ] ビューを開き、[操作 (Actions) ] > [ルーティングテーブル情報 (Routing Table Info) ] を選択します。

デバイスで BGP ルーティング プロトコルを設定する手順は次のとおりです。

- ステップ 1 [設定 (Configuration) ] > [ネットワークデバイス (Network Devices) ] を選択します。
- ステップ 2 デバイス名のハイパーリンクをクリックして、必要なデバイスを選択します。
- ステップ 3 [論理ビュー (Logical View) ] タブをクリックします。
- ステップ 4 [ルーティング (Routing) ] > [BGP] を選択します。

(注) クアッドスーパーバイザ仮想スイッチングシステム (VSS) を備えた Cisco Catalyst 6500 シリーズ デバイスの設定変更は、このページには動的に反映されません。これらの変更を表示するには、24 時間の定期的なデバイス同期が完了していることを確認してください。または、Cisco EPN Manager でこれらのデバイスを手動で同期することもできます。

- ステップ 5 BGP ルーティング プロセスを設定するには、[+] アイコンをクリックします。または、BGP が既に設定されている場合は、AS 番号のハイパーリンクをクリックし、[編集 (Edit)] アイコンをクリックして、次の表に示す BGP プロセスの詳細を入力します。
- ステップ 6 [保存 (Save)] をクリックしてデバイスに変更を展開し、[BGP アドレスファミリー (BGP Address Family)] タブと [BGP ネイバー (BGP Neighbor)] タブを有効にします。
- ステップ 7 BGP アドレス ファミリの詳細を設定するには、[BGP アドレスファミリー (BGP Address Family)] タブをクリックし、次の表に示すアドレス ファミリの詳細を選択して、[保存 (Save)] をクリックします。
- ステップ 8 BGP ネイバーを設定するには、[BGP ネイバー (BGP Neighbor)] タブをクリックし、リストからデバイスの IP アドレスを選択してネイバー デバイスを選択します。
- ステップ 9 新しい BGP ネイバーを作成するには、[追加 (Add)] アイコン ([+]) をクリックし、次の表に示す詳細を指定します。
- ステップ 10 [保存 (Save)] をクリックします。更新された BGP ルーティングプロセス値が保存され、選択したデバイスに展開されます。

変更内容が保存されたことを確認するには、[設定 (Configuration)] > [ネットワークデバイス (Network Devices)] に移動し、[デバイスの詳細 (Device Details)] ページを起動し、[論理ビュー (Logical View)] タブをクリックします。[ルーティング (Routing)] > [BGP] を選択します。ネイバーアドレス (Neighbor Address)、リモート AS (Remote AS)、アドレスファミリータイプ (Address Family Type) とモディファイヤ (Modifier)、アドバタイズ間隔時間 (Advertise Interval Time) など、デバイスで設定されている BGP 設定の詳細を表示できます。

フィールド	サブフィールド	説明
共通の BGP プロセス フィールド	AS 番号 (AS Number)	1 から 4294967295 までの数値を使用して AS 番号を入力します。
	ルータ ID (Router ID)	<ul style="list-style-type: none"> <li>• ルータ ID を入力します。値には、IPv4 アドレスを次の形式で指定できます。</li> <li>• A.B.C.D (IPv4 アドレスの場合)。A、B、C、および D は 0～255 の整数です。</li> </ul>
	ネイバーの変更を記録 (Log Neighbor Changes)	ネイバー ルータの変更を追跡する場合に選択します。

フィールド	サブフィールド	説明
BGP アドレス ファミリ フィールド	BGP グローバル AF (BGP Global AF)	<ul style="list-style-type: none"> <li>• アドレス ファミリ (Address Family) : ルーティング プロセスの BGP アドレス ファミリ プレフィックスを入力します。IPv4 と IPv6 (ユニキャスト、マルチキャスト、および MVPN の場合)、VPNv4 と VPNv6 (ユニキャストの場合)、IPv4 (MDT の場合)、および L2VPN_EVPN_AF (EVPN ベースのサービスの場合) を選択できます。</li> <li>• ラベルの割り当て (Allocate Label) : ラベル付きユニキャスト アドレス プレフィックスを選択します。</li> <li>• ラベルの割り当てのカスタム ポリシー名 (Allocate Label Custom Policy Name) : ルーティング プロセスに関連付けるカスタム ポリシーを選択します。</li> </ul> <p>(注) [Allocate Label] および [Allocate Label Custom Policy Name] フィールドは、IOS デバイスタイプにのみ適用されます。</p>
	BGP の追加パス (BGP Additional Paths)	<p>パスの詳細を指定します。これらのパスにより、暗黙的に以前のパスから新しいパスに代わることなく、同じピアセッションを介して同じプレフィックスのマルチパスをアドバタイズできます。</p> <ul style="list-style-type: none"> <li>• 追加パス (Additional Paths) : デバイスが追加パスを送信、受信、または送受信する必要があるかどうかを選択します。これらはアドレスファミリ レベルまたはネイバー レベルで行われます。セッションの確立中に、指定した BGP ネイバーが追加パス機能 (送信または受信のどちらか (あるいは両方) を実行できるか) についてネゴシエートします。</li> </ul> <p>(注) Cisco CAT65000 デバイスの設定時には、追加パスの値として [インストール (Install) ] のみ設定できます。</p> <ul style="list-style-type: none"> <li>• 最適値 (Best Value) : このフィールドは、選択した [追加パス (Additional Paths) ] の値が [最適値 (Best Value) ] フィールドの設定をサポートしている場合にのみ有効になります。</li> </ul>
	BGP ネイバー AF (BGP Neighbor AF)	<p>指定した BGP ネイバーが属するアドレス ファミリの詳細を指定します。</p> <ul style="list-style-type: none"> <li>• ネイバー アドレス (Neighbor Address) : 隣接ルータのルータ ID を選択します。これらの値は [ネイバー (Neighbor) ] タブで作成した BGP ネイバーに基づいて設定されます。値には、IPv4 または IPv6 のアドレスを次の形式で指定できます。 <ul style="list-style-type: none"> <li>• A.B.C.D (IPv4 アドレスの場合)。A、B、C、および D は 0 ~ 255 の整数です。</li> <li>• xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (IPv6 アドレスの場合)。x は 16 進数の値であり、アドレスではコロン (:) で区切られた 4</li> </ul> </li> </ul>

フィールド	サブフィールド	説明
		<p>つの 16 進数アドレスの 8 セット (セットごとに 16 ビット) を使用します。</p> <ul style="list-style-type: none"> <li>• ラベルの送信 (Send Label) : ネイバーに関連付ける必要があるラベルのタイプを選択します。</li> <li>• リフレクタクライアントのルーティング (Route Reflector Client) : このフィールドでは、ルータを BGP ルートリフレクタとして設定し、指定したネイバーをそのクライアントとして設定できます。</li> <li>• AIGP : Accumulated Interior Gateway Protocol (AIGP) のパス属性を有効にする場合に選択します。</li> <li>• コミュニティの送信 (Send Community) : コミュニティ属性を外部ボーダーゲートウェイプロトコル (eBGP) ネイバーに送信する際に従う送信方法を選択します。</li> <li>• ネクストホップセルフ (Next Hop Self) : ピアリングセッションを通じてアドバタイズされるルートの BGP ネクストホップ属性を、セッションのローカル発信元アドレスに設定する場合に選択します。</li> <li>• 着信および発信ルートマップ名 (Incoming and Outgoing Route Map Name) : ルートポリシーをネイバーからの着信更新または送信更新に適用する必要があるかどうかを指定する場合に選択します。</li> </ul>
	BGP ネットワークマスク (BGP Network Mask)	<ul style="list-style-type: none"> <li>• ネットワークアドレス (Network Address) とネットワークマスク (Network Mask) : 指定した IP アドレスのネットワーク IP アドレスとネットワークマスクを指定します。</li> <li>• バックドアルート (Back Door Route) : 外部ボーダーゲートウェイプロトコル (eBGP) のアドミニストレーティブディスタンスに、ローカル発信元の BGP ルートのアドミニストレーティブディスタンスを設定し、Interior Gateway Protocol (IGP) ルートよりも推奨度を低くすることができます。</li> <li>• ネットワークルートポリシー名 (Network Route Policy Name) : ラベル割り当てのプレフィックスの選択に使用するルートポリシーを選択します。これにより、BGP において、すべてのグローバルルートセットまたはフィルター処理されたグローバルルートセットにラベルを割り当てることができます (ルートポリシーにより指定)。</li> </ul>
[BGP ネイバー (BGP Neighbor) ]	-	<p>次の値を指定します。</p> <ul style="list-style-type: none"> <li>• ピア AS 番号 (Peer AS Number) : 1 ~ 4294967295 の整数を使用して自律システム番号の値を入力します。</li> </ul>

フィールド	サブフィールド	説明
タブのフィールド		<ul style="list-style-type: none"> <li>• ネイバー アドレス (Neighbor Address) : 設定する BGP ネイバーの IP アドレスを入力します。値には、IPv4 または IPv6 のアドレスを次の形式で指定できます。 <ul style="list-style-type: none"> <li>• A.B.C.D (IPv4 アドレスの場合)。A、B、C、および D は 0～255 の整数です。</li> <li>• xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx (IPv6 アドレスの場合)。x は 16 進数の値であり、アドレスではコロン (:) で区切られた 4 つの 16 進数アドレスの 8 セット (セットごとに 16 ビット) を使用します。</li> </ul> </li> <li>• ローカル AS 番号 (Local AS Number) とアクション (Action) : AS_PATH 属性の先頭に付ける自律システム番号を指定します。値の範囲は、1～65535 の有効な自律システム番号です。</li> <li>• 更新元 (Update Source) : このオプションを使用して、ピア ルータに最も近いインターフェイスを使用する代わりにループバック インターフェイスを使用してピアの関係 (TCP 接続) を確立します。</li> <li>• フォールオーバー (Fall-over) : 値を選択すると、BGP 高速ピアリングセッションの無効化が有効になり、指定した BGP ネイバーの隣接の変更についてコンバージェンスと応答時間が向上します。</li> <li>• パスワードの暗号化 (Password Encryption) とパスワード (Password) : パスワードの暗号化を有効にするかどうかを指定し、有効にした場合はパスワードの値を指定します。</li> <li>• (表示のみ) ネイバー状態 (Neighbor State) : BGP ルーティングプロセスに参加しているネイバーデバイスの接続ステータスを表示します。ステータスは、アイドル (Idle)、接続 (Connect)、アクティブ (Active)、オープン送信 (Opensent)、オープン確認 (Openconfirm)、および確立済み (Established) です。                      ネイバーデバイスは、接続ステータスが確立済み (Established) の場合にのみイベントを生成します。デバイスからの更新が生じている場合は、接続状態を頻繁に確認してください。</li> </ul> <p>(注) インベントリが詳細に同期されている間は、ネイバー状態の値は更新されません。更新値を表示するには、同期が正常に終了するまで待ってください。</p>

## IS-IS の設定

Intermediate System-to-Intermediate System (IS-IS) プロトコルは、2 レベルの階層を使用して大規模なルーティングドメイン（管理の目的でエリアに分割される）をサポートする、ドメイン内 OSI 動的ルーティングプロトコルです。1つのエリア内のルーティングのことと、レベル1ルーティングと呼びます。エリア間のルーティングのことを、レベル2ルーティングと呼びます。シスコルータで IP の IS-IS を有効にし、他の IS-IS 対応ルータとルーティング情報を交換するには、次のタスクを実行する必要があります。

- デバイスで IS-IS ルーティング プロセスを有効にし、エリアを割り当てます。
- 必要なインターフェイスで IS-IS IP ルーティングを有効にします。

有効な IP アドレスを持つインターフェイスは、レベル1（エリア内）ルータ、レベル1\_2（レベル1ルータとレベル2の両方）ルータ、または特定の IS-IS インスタンスのレベル2（エリア間のみ）ルーティングインターフェイスとして機能するように指定できます。指定したインターフェイス間のルータ間で IS-IS ルーティングの動作が開始されると、IS-IS ネイバーフッドが自動的に生成されます。



- (注) IS-IS ルーティングを有効にするには、デフォルトで少なくとも1つのアドレスファミリを設定する必要があります。このリリースでは、Cisco EPN Manager を使用したアドレスファミリの設定はできません。

デバイスで IS-IS プロセスを設定する手順は次のとおりです。

- ステップ1** [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] を選択します。
- ステップ2** デバイス名のハイパーリンクをクリックして、IS-IS ルーティングプロトコルを設定するデバイスを選択します。
- ステップ3** [論理ビュー (Logical View)] タブをクリックします。
- ステップ4** [ルーティング (Routing)] > [IS-IS] を選択します。
- ステップ5** 新しい IS-IS プロセスを設定するには、[+] アイコンをクリックし、次のパラメータを入力します。
- 英数字のみを使用して [IS-IS プロセス ID (S-IS Process ID)] を指定します。スペースや特殊文字は使用できません。
  - [NET ID] を NSAP 形式で指定します。たとえば、49.0001.0000.0001.0010.00 などと指定できます。
    - 49 : AFI (権限および形式インジケータ) を表すエリア ID の 1 番目の部分を表します。
    - 0001 : エリア ID の 2 番目の部分を表します。
    - 0000.0001.0010 : システム ID を表します。
    - 00 : N セレクタを表します。常に 0 です。

- [IS-IS タイプ (IS-IS Type)] フィールドで IS-IS ルーティングプロトコルのタイプを指定します。[レベル 1 (Level 1)]、[レベル 2 (Level 2)]、[レベル 1\_2 (Level 1\_2)] を選択できます。

**ステップ 6** [保存 (Save)] をクリックします。

**ステップ 7** 選択したデバイスのインターフェイスでこのルーティングプロセスを設定する手順は次のとおりです。

- a) [ルーティング (Routing)] > [IS-IS] のリストから、上記の手順で作成した IS-IS プロトコルプロセスを選択します。
- b) IS-IS プロセス ID のハイパーリンクをクリックします。
- c) [IS-IS インターフェイス (IS-IS Interfaces)] タブを使用して、選択した IS-IS 設定を適用するデバイスのインターフェイスを指定します。

- [+] アイコンをクリックして、インターフェイスの詳細を入力します。

- [回路タイプ (Circuit Type)] ドロップダウンメニューから、この設定を適用する回路のタイプを選択します。[レベル 1 (Level 1)]、[レベル 2 (Level 2)]、[レベル 1\_2 (Level 1\_2)] を選択できます。

- [インターフェイス (Interface)] ドロップダウンメニューで、必要なインターフェイスを選択します。

- (任意) レベル1とレベル2のメトリックと優先度の値を指定します。[優先度 (Priority)] フィールドでは、1 ~ 127 の値を入力します。[メトリック (Metric)] では、1 ~ 16777214 の値を入力します。

- ポイントツーポイント接続を有効にする場合は、[ポイントツーポイント (Point-to-Point)] チェックボックスをオンにします。

- [保存 (Save)] をクリックして、選択したインターフェイスに設定を展開します。

**ステップ 8** [保存 (Save)] をクリックします。選択した IS-IS プロセスが、デバイス上の指定したインターフェイスで設定されます。

**ステップ 9** (任意) 選択したデバイスに関連付けられている IS-IS ネイバーを表示するには、IS-IS のハイパーリンクをクリックし、[IS-IS ネイバー (IS-IS Neighbors)] タブをクリックします。設定されたネイバーのホスト名、IP アドレス、システム ID、IS-IS タイプ、接続状態、設定済みのホールドダウン時間値、およびローカルインターフェイス名を表示できます。

(注) IS-IS ネイバーのホスト名が 15 の一意の文字を超える場合は、ホスト名が Cisco EPN Manager に表示されません。ホスト名は必ず一意の 15 文字以下にしてください。

**ステップ 10** (任意) Cisco EPN Manager を使用して設定した IS-IS ルーティングプロセスを削除する手順は次のとおりです。

- a) [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] に移動し、[デバイスの詳細 (Device Details)] ページを起動し、[ルーティング (Routing)] > [IS-IS] を選択します。
- b) リストから必要な IS-IS プロセスを選択します。
- c) 削除のための [x] アイコンをクリックし、[OK] をクリックして削除操作を確定します。

## OSPF の設定

Open Shortest Path First (OSPF) は各種の標準規格に準拠したルーティングプロトコルであり、最短パス優先 (SPF) アルゴリズムを使用して宛先への最適なルートを決めます。OSPF は、同じ設定済みエリア内のすべてのルータにリンク ステート アドバタイズメント (LSA) を送信します。OSPF は、ルーティングテーブル内の変更に関するルーティングアップデートだけを送信します。ルーティング テーブル全体を定期的には送信することはありません。

Cisco EPN Manager を使用して、IPv4 および IPv6 アドレスの OSPF を設定できます。そのためには、ルータ ID、ルータで設定するアドミニストレーティブ ディスタンス、および設定する最大パス値がわかっていることが必要です。

OSPF ルーティング プロセスを設定する手順は次のとおりです。

**ステップ 1** [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] を選択します。

**ステップ 2** デバイス名のハイパーリンクをクリックして、OSPF を有効にするデバイスを選択します。IOS-XR デバイスのみを選択します。

**ステップ 3** [論理ビュー (Logical View)] タブをクリックします。

**ステップ 4** [ルーティング (Routing)] > [OSPF] を選択します。

**Note** クラウド スーパーバイザ仮想スイッチング システム (VSS) を備えた Cisco Catalyst 6500 シリーズ デバイスの設定変更は、このページには動的に反映されません。これらの変更を表示するには、24 時間の定期的なデバイス同期が完了していることを確認してください。または、Cisco EPN Manager でこれらのデバイスを手動で同期することもできます。

**ステップ 5** 新しい OSPF プロセスを追加するには、[+] 記号をクリックします。既存の OSPF プロセスを変更するには、プロセス ID のハイパーリンクをクリックして必要なプロセスを選択し、ページの右上隅にある [編集 (Edit)] アイコンをクリックします。

**ステップ 6** 次の表に示すように、共通の OSPF パラメータを指定します。

**ステップ 7** [保存 (Save)] をクリックします。設定の変更が保存されます。確認するには、[設定 (Configuration)] タブをクリックし、[ルーティング (Routing)] > [OSPF] を選択して、表示される詳細を確認します。

**ステップ 8** [OSPF インターフェイス (OSPF Interfaces)] の設定を指定します。

基本的なプロパティで OSPF プロセスを設定したら、その設定をネットワーク全体または OSPF エリアに直接展開できます。それには、OSPF エリア ID、デバイスのインターフェイスの詳細、ネットワーク タイプなどを指定する必要があります。OSPF インターフェイスの設定を変更する手順は次のとおりです。

- a) [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] を選択します。
- b) デバイス名のハイパーリンクをクリックして、設定を変更するデバイスを選択します。
- c) [設定 (Configuration)] タブをクリックし、[ルーティング (Routing)] > [OSPF] を選択します。
- d) プロセス ID のハイパーリンクをクリックして、必要なプロセスを選択します。
- e) [OSPF インターフェイス (OSPF Interfaces)] タブをクリックします。
- f) [追加 (Add)] アイコン ([+]) をクリックして、選択したデバイスの OSPF プロセスに関連付けられたインターフェイスに新しい設定を追加します。既存の値を編集するには、インターフェイス名のハイパーリンクをクリックし、ページの右上にある [編集 (Edit)] アイコンをクリックします。



- g) 次の表に示すように、パラメータを指定します。  
 h) [保存 (Save) ] をクリックして、変更内容をデバイスに展開します。

Option	Description
<b>OSPF の共通のプロパティ</b>	<b>説明</b>
プロセス ID (Process ID)	選択した OSPF プロセスを識別する 1 ~ 65535 の一意の数値。
ルータ ID (Router ID)	エリア 0 ルータのルータ ID。
コスト (Cost)	ネットワーク全体のパケット送信コストを設定します。この値は、OSPF ルータによる最短パスの計算に使用されます。これは Cisco IOS-XE デバイスでは有効になりません。  1 ~ 65535 の数値を入力します。
トポロジーの優先順位 (Topology Priority)	サブネット用に指定されたルータを表示します。1 ~ 255 の数値を入力します。
ルートあたりの最大パス数 (Maximum number of paths per route)	ルータがルートごとの負荷分散に使用できるパスの最大数を定義します。デフォルト値は 4 です。1 ~ 64 の数値を設定できます。
アドミニストレーティブ ディスタンス (Administrative Distance)	パスの選択に設定する距離を指定します。デフォルト値は 110 で、使用可能な値は 1 ~ 255 です。
外部エリア ディスタンス (External Area Distance)	外部タイプ 5 およびタイプ 7 のルートの距離を指定します。1 ~ 255 の数値を選択できます。
エリア間ディスタンス (Inter Area Distance)	1 ~ 255 の値を使用して、エリア間ルートのエリア間距離を指定します。
エリア内ディスタンス (Intra Area Distance)	1 ~ 255 の値を使用して、エリア内ルートのエリア内距離を指定します。
<b>ルーティング (Routing) &gt; OSPF &gt; OSPF インターフェイス (OSPF Interface) / PEP プロパティ (PEP Properties)</b>	<b>説明</b>
エリア ID (Area ID)	0 ~ 4294967295 の整数を使用して、NE の OSPF エリア ID を指定します。  ID を 0.0.0.0 にすることはできません。
インターフェイス名 (Interface Name)	指定した OSPF インターフェイス/PEP 設定を関連付ける必要があるデバイスのインターフェイス。
インターフェイスコスト (Interface cost)	ネットワーク全体のパケット送信のコスト。このコストは、OSPF ルータによる最短パスの計算に使用されます。
インターフェイス プライオリティ (Interface Priority)	サブネット用に指定されたルータ。

Option	Description
ネットワーク タイプ (Network Type)	OSPF プロセスに関連付けられたネットワークのタイプ。ブロードキャスト (Broadcast)、NBMA、ポイントツーポイント (Point to Point)、およびポイントツーマルチポイント (Point to Multipoint) を選択できます。
dead 間隔 (Dead Interval)	OSPF ルータの packets が表示されなくなってから、ネイバー ルータがそのルータのダウンを宣言するまでの秒数。シスコのデフォルトは 40 秒です。
Hello 間隔 (Hello Interval)	OSPF ルータが送信する OSPF hello パケット アドバタイズメントの間隔の秒数。シスコのデフォルトは 10 秒です。
再送信間隔 (Retransmit Interval)	パケットが再送信される前に経過する時間。シスコのデフォルトは 5 秒です。
送信遅延 (Transmit Delay)	サービス速度。シスコのデフォルトは 1 秒です。

## スタティックルーティングの設定

スタティックルーティングは最も単純な形式のルーティングで、ネットワーク管理者が手動でルーティングテーブルにルートを入力します。ルートは、ネットワーク管理者が変更しない限り変わりません。スタティックルーティングは通常、設定するデバイスが非常に少なく、ルートが変わらないことを管理者が確信している場合に使用します。スタティックルーティングの主な欠点は、接続が切断されるたびに、手動で設定したルートを更新して修正する必要があるため、ネットワークトポロジの変更または外部ネットワークの障害に対処できないことです。

**ステップ 1** 選択項目 **Configuration > Network Devices**.

**ステップ 2** デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details)] ページを起動します。

**ステップ 3** [論理ビュー (Logical View)] タブをクリックします。

**ステップ 4** **Routing > Static** を選択します。

**ステップ 5** スタティックルーティングを設定するには、**Add** をクリックします。

- a) IPv4 スタティックルートを追加する場合は、[IPv4 スタティックルート (IPv4 Static route)] 領域で、[追加 (+) (Add (+))] アイコンをクリックします。次のフィールドに必要な詳細情報を入力します。

[宛先ネットワーク (Destination Network)]、[ネットワークマスク (Network Mask)]、[ネクストホップ IP (Next Hop IP)]、[発信インターフェイス (Outgoing Interface)]、[永続的ルート (Permanent Route)]、または [アドミニストレーティブディスタンス (Administrative Distance)]。

- b) IPv6 スタティックルートを追加する場合は、[IPv6 スタティックルート (IPv6 Static route)] 領域で、[追加 (+) (Add (+))] アイコンをクリックします。次のフィールドに必要な詳細情報を入力します。

[宛先 IPv6 プレフィックス (Destination IPv6 Prefix)]、[プレフィックス長 (Prefix Length)]、[ネクストホップ IPv6 アドレス (Next Hop IPv6 Address)]、[発信インターフェイス (Outgoing interface)]、[アドミニストレーティブ ディスタンス (Administrative Distance)]、[キャストタイプ (Cast Type)]、または [タグ値 (Tag Value)]。

ステップ 6 **Save** をクリックします。

## ACL の設定

[デバイスの詳細 (Device Details)] ページの [設定 (Configuration)] タブには、デバイスでの現在の CFM 設定のリストが表示されます。デバイス設定とユーザー アカウントの権限に応じて、デバイスで ACL を設定できます。

ACL を設定する手順は次のとおりです。

ステップ 1 選択項目 **Configuration > Network Devices**.

ステップ 2 デバイスのハイパーリンクをクリックして、そのデバイスの [デバイスの詳細 (Device Details)] ページを起動します。

ステップ 3 [論理ビュー (Logical View)] タブをクリックします。

ステップ 4 **Security > ACL** を選択します。

ステップ 5 ACL に次のパラメータを指定します。

- 名前 (Name) /番号 (Number) : ACL の一意の識別子を指定します。英数字、ハイフン、および下線を使用できます。
- タイプ (Type) : ACL のタイプが標準か拡張かを指定します。選択したデバイスのタイプによってはこのドロップダウンメニューが非表示になります。たとえば、Cisco IOS-XR デバイスではこのドロップダウンメニューは非表示になります。
- (任意) 説明 (Description) : ACL に関する参照用の説明を入力します。

ステップ 6 **Save** をクリックして値を Cisco EPN Manager に保存します。この操作ではデバイスに変更が展開されません。

ステップ 7 上記の手順で作成した ACL の横にあるドロップダウンアイコンをクリックし、次の ACE 値を指定します。

- [行の追加 (Add Row)] をクリックして新しい ACE を追加します。または、既存の ACE を選択し、[編集 (Edit)] をクリックして、[アクション] ([許可 (Permit)] または [拒否 (Deny)])、[ソース IP (Source IP)]、[宛先 IP (Destination IP)] を指定し、必要に応じて、ACE に関連付ける必要があるフィールドカードソース、ポート情報、および説明を指定します。
- [保存 (Save)] をクリックして、ACE に関連付けられた値を保存します。

- c) 上下矢印（ボタン）を使用して、選択した ACL についてデバイスに ACE を適用する順序を指定します。

**ステップ 8** 上記の手順で作成した ACL を選択し、[インターフェイスに適用（Apply to Interface）] をクリックして、この ACL を適用する必要があるインターフェイスを指定します。

**ステップ 9** [OK] をクリックして、デバイスの選択したインターフェイスに、指定した ACL 値を展開します。

## 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）では、送信元ルーティングの概念を使用します。送信元ルーティングでは、送信元が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が組み合わせることができるサブパスです。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。

Cisco EPN Manager GUI では、次のセグメントルーティングサブメニュー オプションを使用して、デバイスのセグメントルーティングパラメータを設定できます。また、CLI から設定されたセグメントルーティング設定を表示または編集することもできます。

- [セグメント設定の構成](#)
- [ルーティングプロセスの設定](#)
- [PCE サーバーの設定](#)
- [パス計算クライアント（PCC）の設定](#)
- [アフィニティの設定](#)
- [オンデマンドポリシーの設定](#)

次の表に、UI からセグメントルーティングパラメータを設定できるデバイス、およびサポートされているソフトウェアバージョンを示します。

デバイスシリーズおよびタイプ	ソフトウェアバージョン
NCS 540	6.5.3、6.6.1、7.0.1、7.1.1
NCS 560	6.5.3、6.6.1、7.0.1、7.1.1
NCS 5500	6.5.3、6.6.1、7.0.1、7.1.1
ASR 9000	6.5.3、6.6.1、7.0.1、7.1.1

## セグメント設定の構成

選択したデバイスのセグメントルーティングのグローバル設定を構成するには、次の手順を実行します。

- ステップ 1 [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] を選択します。
- ステップ 2 デバイス名のハイパーリンクをクリックして、セグメントルーティングを設定するデバイスを選択します。
- ステップ 3 左側のタブで、[Logical View] をクリックします。
- ステップ 4 [Segment Routing] > [Segment Settings] を選択します。
- ステップ 5 [General] タブで、[+] アイコンをクリックして必要な値を入力し、[Save] をクリックします。既存の設定を編集するには、対応するハイパーリンクをクリックします。

属性	説明
Global Block Min	セグメントルーティンググローバルブロック (SRGB) は、ラベルスイッチデータベースでセグメントルーティング用に保存されているラベル値の範囲です。SRGB ラベル値は SR 対応ノードにプレフィックスセグメント識別子 (SID) として割り当てられ、ドメイン全体で有効です。  16000 ~ 1048575 の範囲で値を入力します。
Global Block Max	
Local Block Min	セグメントルーティングローカルブロック (SRLB) は、隣接関係セグメント識別子 (adj-SID) の手動割り当てのために保存されているラベル値の範囲です。これらのラベルはローカルで重要であり、ラベルを割り当てるノードでのみ有効です。  15000 ~ 1048575 の範囲で値を入力します。
Local Block Max	
Binding SID	ドロップダウンリストから値を選択します。
最大 SID 深度	ノードまたはノード上のリンクによってサポートされている SID の数。1 ~ 255 の範囲で値を入力します。

(注) 次のコマンドを実行して、SRGB または SRLB の変更が有効になるように、ラベルの不一致をクリアします。

```
#clear segment-routing local-block discrepancy all
```

- ステップ 6 [Mapping Server] タブで、[+] をクリックして必要な値を入力し、[Save] をクリックします。[OK] をクリックして、変更をデバイスにプッシュすることを確認します。既存の設定を削除するには、対応するチェックボックスをオンにして [X] をクリックします。

属性	説明
IP Address Prefix	IPv4 アドレスを入力します。
Mask	サブネットマスクの詳細を入力します
アドレス ファミリ (Address Family)	アドレスファミリを IPv4 として選択します。
Start of SID Range	0 ~ 1048575 の範囲で値を入力します。
Number of Allocated SIDs	0 ~ 1048575 の範囲で値を入力します。デフォルト値は 1 です。

**ステップ 7** [Adjacency SID Mapping] タブで、[+] をクリックして必要な値を入力し、[Save] をクリックします。[OK] をクリックして、変更をデバイスにプッシュすることを確認します。既存の設定を削除するには、対応するチェックボックスをオンにして [X] をクリックします。

属性	説明
インターフェイス (Interface)	ループバックインターフェイスをドロップダウンリストから選択します。
アドレス ファミリ (Address Family)	アドレスファミリを IPv4 として選択します。
ネクスト ホップ アドレス	ネクストホップの IPv4 アドレスを入力します。
SID Mapping Type	マッピングタイプとして、[Absolute] または [Index] のいずれかを選択します。
SID Value	SID 値の有効範囲は SID マッピングタイプによって異なります。 <ul style="list-style-type: none"> <li>• [Index] タイプの場合 : 0 ~ 1048575</li> <li>• [Absolute] タイプの場合 : 15000 ~ 1048575</li> </ul>

## ルーティングプロセスの設定

選択したデバイスのセグメントルーティングのルーティング プロセス パラメータを設定するには、次の手順を実行します。

### 始める前に

ルーティング プロセス パラメータを設定する前に、**[論理的ビュー (Logical View)] > [ルーティング (Routing)]** ページで、デバイスに対して OSPF および ISIS ルーティングプロセスを設定したことを確認します。詳細については、「[ルーティングプロトコルとセキュリティの設定 \(129 ページ\)](#)」を参照してください。



(注) Cisco EPN Manager は、セグメントルーティングで OSPFV3 プロトコルをサポートしていません。

- ステップ 1 [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] を選択します。
- ステップ 2 デバイス名のハイパーリンクをクリックして、パラメータを設定するデバイスを選択します。
- ステップ 3 左側のタブで、[Logical View] をクリックします。
- ステップ 4 [Segment Routing] > [Routing Process] をクリックします。
- ステップ 5 対応するハイパーリンクをクリックし、[Save] をクリックして、各タブで必要に応じて属性の値を入力します。

タブ	属性	説明
プロパティ (Properties)	プロセス ID (Process ID)	このフィールドには、デバイスに対して設定されているプロセス ID が自動的に入力されます。
	Process Type	このフィールドは、デバイスの設定に基づいて ISIS または OSPF として自動的に入力されます。
	Global Block Min	デフォルトの SRGB の範囲は 16000 ~ 23999 です。ここで入力した値は、[Segment Settings] で設定されたグローバル値を上書きします。
	Global Block Max	
	Advertise Local Prefix SID Mapping	このフィールドは、デフォルトで有効になっています。
	Override LDP Labels	LDP ラベルを上書きするには、このチェックボックスをオンにします。
	Receive Remote Prefix SID Mapping	リモートプレフィックス SID マッピングを受信するには、このチェックボックスをオンにします。
	Avoid Microloop	マイクロループを回避するには、このチェックボックスをオンにします。

タブ	属性	説明
Connected Prefix SID Mapping	Ip Address Prefix	IPv4 アドレスを入力します
	Mask	サブネットマスクの詳細を入力します
	SID Mapping Type	ドロップダウンリストから、 <b>[Absolute]</b> または <b>[Index]</b> マッピングタイプのいずれかを選択します。
	SID Value	SID 値の有効範囲は SID マッピングタイプによって異なります。 <ul style="list-style-type: none"> <li>• <b>[Index]</b> タイプの場合 : 0 ~ 1048575</li> <li>• <b>[Absolute]</b> タイプの場合 : 16000 ~ 1048575</li> </ul>
	Flex Algorithm	128 ~ 255 の範囲の Flex アルゴリズム値を入力します。 <b>[Strict SPF]</b> が有効になっている場合、このフィールドはグレー表示されます。
	Strict SPF	必要に応じてチェックボックスをオンにします。
	Replace Prefix SID with Explicit Null	必要に応じてチェックボックスをオンにします。



タブ	属性	説明
Interface Prefix SID Mapping	SID Mapping Type	ドロップダウンリストから、 [Absolute] または [Index] マッピング タイプの内いずれかを選択しま す。
	SID Value	SID 値の有効範囲は SID マッピン グタイプによって異なります。  <ul style="list-style-type: none"> <li>• [Index] タイプの場合 : 0 ~ 1048575</li> <li>• [Absolute] タイプの場合 : 16000 ~ 1048575</li> </ul>
	Strict SPF	必要に応じてチェックボックスを オンにします。
	Replace Prefix SID with Explicit Null	必要に応じてチェックボックスを オンにします。

- (注)
- ISIS ルーティングプロセスの場合は、接続されたプレフィックスまたはローカルプレフィックスの内いずれかを設定できます。OSPF ルーティングプロセスの場合は、ローカルプレフィックス SID 設定のみがサポートされます。
  - ローカルプレフィックス SID を設定する場合、IP が設定されているループバック インターフェイスのみが [ルーティングプロセス (Routing Process)] でモデル化されます。
  - ローカルプレフィックス SID の場合、デバイスは次の設定をサポートしています。
    - prefix-sid index/absolute 100 explicit-null (algorithm/strict-spf が無い prefix-sid)
    - prefix-sid algorithm 128 index /absolute 16000 (algorithm がある prefix-sid)
    - prefix-sid strict-spf index/absolute 200 explicit-null (strict-spf がある prefix-sid)

## パス計算クライアント (PCC) の設定

選択したデバイスの PCC クライアントパラメータを設定するには、次の手順を実行します。

### 始める前に

- PCC は、EPNM で表示および変更するために事前に検出する必要があるワントタイム設定です。

### 設定例

`segment-routing`

`traffic-eng`

`pcc`

- PCC ピアイベントを受信するには、`segment-routing traffic-eng logging` の下で、`pcep peer-status logging` を使用してデバイスを有効にする必要があります。

ステップ 1 [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] を選択します。

ステップ 2 デバイス名のハイパーリンクをクリックして、パラメータを設定するデバイスを選択します。

ステップ 3 左側のタブで、[Logical View] をクリックします。

ステップ 4 [Segment Routing] > [PCC] をクリックします。

ステップ 5 対応するハイパーリンクをクリックし、[Save] をクリックして、各タブで必要に応じて属性の値を入力します。[Ok] をクリックして、変更をデバイスにプッシュすることを確認します。

タブ	属性	説明
PCC	Source Address	IPv4 アドレスを入力します。
	Report All	この値を True に設定するには、このチェックボックスをオンにします。
	PCC Centric Model	この値を True に設定するには、このチェックボックスをオンにします。
	Session Dead time	単位は秒です。 0 ~ 255 の範囲の値を入力します。
	Session Keepalive Time	単位は秒です。 0 ~ 255 の範囲の値を入力します。 このパラメータを無効にする場合は、0 を入力します。
	Delegated Policy Up Time	単位は秒です。 0 ~ 3600 の値を入力します。このパラメータを無効にする場合は、0 を入力します。
	PCE Initiated Orphan State Time	15 ~ 14400 の範囲の値を入力します。
	PCE Initiated Policy Delegation Time	10 ~ 180 秒の範囲の値を入力します。

タブ	属性	説明
PCC's Peer Database	PCE Address	IPv4 アドレスを入力します。
	Precedence	0 ~ 255 の範囲の値を入力して優先度を設定します。0 が最も優先度が高く、255 が最も優先度が低くなります。
	[Password]	クライアント/サーバー認証のパスワード (クリアテキストパスワード) とキーチェーンの詳細を入力します。
	Keychain	

## PCE サーバーの設定

選択したデバイスを PCE サーバーとして設定するには、次の手順を実行します。

- ステップ 1 [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] を選択します。
- ステップ 2 デバイス名のハイパーリンクをクリックして、パラメータを設定するデバイスを選択します。
- ステップ 3 左側のタブで、[Logical View] をクリックします。
- ステップ 4 [Segment Routing] > [PCE Server] をクリックします。
- ステップ 5 [+] をクリックして必要な値を入力し、[Save] をクリックします。[Ok] をクリックして、変更をデバイスにプッシュすることを確認します。

タブ	属性	説明
PCE Sever	IPアドレス	IPv4 アドレスを入力します。
	State Sync Address	複数のIPv4アドレスをカンマで区切って入力します。
	Keepalive Time	単位は秒です。 0～255の範囲の値を入力します。デフォルト値は30です。このパラメータを無効にする場合は、0を入力します。
	[Password]	クライアント/サーバーの詳細を認証するためのパスワード（クリアテキスト）を入力します。
	Minimum Peer Keepalive Interval	単位は秒です。 0～255の範囲の数値を入力します。デフォルト値は20です。このパラメータを無効にする場合は、0を入力します。
	Strict SIDs Only	このオプションを有効にするには、チェックボックスをオンにします。このオプションは、デフォルトで無効になっています。
	Topology Reoptimization Interval	単位は秒です。 600～86400の範囲の値を入力します。デフォルト値は1800です。



(注) デバイスとネットワークの制限により、一度設定した PCE サーバーは削除できません。

## アフィニティの設定

選択したデバイスのセグメントルーティングのアフィニティパラメータを設定するには、次の手順を実行します。

ステップ1 [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] を選択します。

**ステップ2** デバイス名のハイパーリンクをクリックして、パラメータを設定するデバイスを選択します。

**ステップ3** 左側のタブで、[Logical View] をクリックします。

**ステップ4** [Segment Routing] > [Affinity] を選択します。

**ステップ5** [+]アイコンをクリックして必要な値を入力し、[Save] をクリックします。[OK] をクリックして、変更をデバイスにプッシュすることを確認します。編集するには、対応するハイパーリンクをクリックします。既存の設定を削除するには、対応するチェックボックスをオンにして [X] をクリックします。

タブ	属性	説明
アフィニティ	Affinity Name	アフィニティ属性の名前を入力します。
	ビット位置	0～255の範囲の値を入力します。
Affinity Mapping	Interface Name	ドロップダウンリストからループバックインターフェイスを選択して、インターフェイスをアフィニティに関連付けます。少なくとも1つのアフィニティをインターフェイスに関連付ける必要があります。
	Affinity Name	インターフェイスに関連付けるアフィニティをドロップダウンリストから選択します。  1つのインターフェイスに複数のアフィニティを関連付けることができます。
	Metric value	0～2147485647の範囲の値を入力します

## オンデマンドポリシーの設定

選択したデバイスのセグメントルーティングのオンデマンドポリシーパラメータを設定するには、次の手順を実行します。

**ステップ1** [設定 (Configuration)] > [ネットワークデバイス (Network Devices)] を選択します。

**ステップ2** デバイス名のハイパーリンクをクリックして、パラメータを設定するデバイスを選択します。

**ステップ3** 左側のタブで、[Logical View] をクリックします。

**ステップ4** [Segment Routing] > [On-Demand Policy] をクリックします。

**ステップ 5** [+]アイコンをクリックして必要な値を入力し、[Save]をクリックします。[OK]をクリックして、変更をデバイスにプッシュすることを確認します。編集するには、対応するハイパーリンクをクリックします。既存の設定を削除するには、対応するチェックボックスをオンにして [X] をクリックします。

タブ	属性	説明
オンデマンドポリシーテンプレート	カラー	1 ~ 4294901295 の範囲で値を入力します。
	Bandwidth	1 ~ 4294967295 (kbps) の範囲で値を入力します。
	Path type	ドロップダウンリストから値を選択します。
	SID の上限 (Max SID Limit)	1 ~ 255 の範囲で値を入力します。
	Metric Margin Mode	ドロップダウンリストから値を選択します。
	メトリック タイプ	ドロップダウンリストからメトリックタイプを選択します。
	メトリックマージン値 (Metric Margin Value)	0 ~ 2147483647 の範囲の値を入力します。
Flex Algorithm	カラー	このフィールドには、[On-Demand Policy Template] タブに入力した値が自動的に入力されます。
	Flex Algorithm	128 ~ 255 の範囲でプレフィックス SID アルゴリズム値を入力します。
Disjoint Path	カラー	このフィールドには、[On-Demand Policy Template] タブに入力した値が自動的に入力されます。
	Group Id	1 ~ 65535 の値を入力します。
	Disjointness Type	ドロップダウンリストを使用して値を選択します。
	Sub Group Id	1 ~ 65535 の値を入力します。

セグメントルーティングポリシーを設定するには、「[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](#)」を参照してください。

# EOAM の障害とパフォーマンスのモニターリングを設定する

Cisco EPN Manager を使用すれば、キャリアイーサネットサービスのモニターリングとトラブルシューティングに EOAM (Ethernet Operations, Administration and Management) プロトコルを使用するようにネットワーク内のデバイスを設定することができます。また、Cisco EPN Manager 内の事前定義のテンプレートとして使用可能な CLI コマンドのセットを使用して、イーサネットサービスに対して接続テストとパフォーマンステストを実行することができます。

## CFM の設定

CFM 設定では、EOAM プロトコルを使用してキャリアイーサネットサービスのモニターリングとトラブルシューティングを行うためのステージを設定します。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で説明しているように、EVC を作成およびプロビジョニングするときに CFM を EVC レベルで設定することもできます。

CFM を設定すると、個々のデバイスについて CFM の設定をすばやく簡単に表示できるようになります。

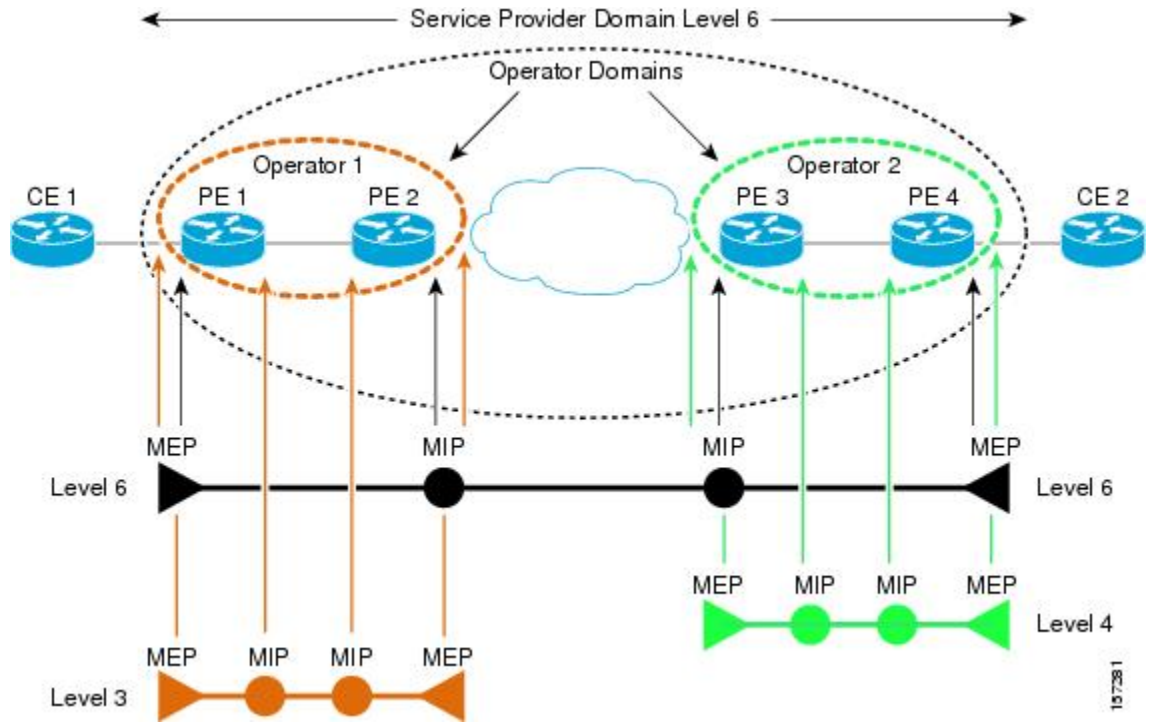
## CFM の概要

IEEE 接続障害管理 (CFM) は、サービスごとのエンドツーエンドイーサネットレイヤの運用、管理、保守 (OAM) プロトコルです。CFM には、大規模イーサネットメトロポリタンエリア ネットワーク (MAN) および WAN の予防的な接続モニターリング、障害検証、および障害分離の機能が含まれています。

CFM は、サービス VLAN 単位 (または EVC 単位) で動作します。EVC に障害が発生したかどうかを知ることができ、発生した障害を迅速に切り分けるツールが用意されています。

CFM 対応ネットワークは、以下で説明するように、メンテナンスドメイン、CFM サービス、およびメンテナンスポイントで構成されます。

Figure 3: CFM メンテナンス ドメイン



### メンテナンス ドメイン

イーサネットCFMは、任意のサービスプロバイダネットワーク内にあり、階層型メンテナンスドメインで構成される機能モデルに依存しています。メンテナンスドメインは、シングルエンティティにより所有および運用が行われ、一連の内部境界ポートにより定義される、ネットワーク上の管理空間です。ドメインは一意的メンテナンスレベルに割り当てられ、これによりドメインの階層関係が定義されます。複数のメンテナンスドメインのネストまたは接触は許されますが、交差はできません。2つのドメインがネストする場合、外側のドメインはそれに含まれるドメインより上位のメンテナンスレベルでなければなりません。1台のデバイスが複数のメンテナンスドメインに参加する場合があります。

### CFM サービス

CFM サービス（メンテナンスの関連付け）により、ネットワーク内の接続に応じてCFMメンテナンスドメインを分割することが可能になります。たとえば、ネットワークがいくつかの仮想LAN（VLAN）に分割されている場合、CFMサービスはそれぞれに作成されます。CFMは、各サービスに個別に実行できます。CFMサービスは、常にメンテナンスドメインに関連付けられ、そのメンテナンスドメイン内で動作するため、そのドメインのメンテナンスレベルに関連付けられます。サービス関連のCFMフレームはすべて、関連付けられたメンテナンスドメインのメンテナンスレベルを伝送します。ドメイン内には多数のCFMサービスが存在する可能性があります。MEPを設定するには、あらかじめCFMサービスをドメインで設定しておく必要があります。



## メンテナンス ポイント

メンテナンス ポイントは、CFM メンテナンス ドメインに参加するインターフェイスの境界を定めるものです。メンテナンス ポイントは、特定のインターフェイス上の特定の CFM サービスのインスタンスになります。CFM は、インターフェイスに CFM メンテナンス ポイントが存在する場合にのみ、そのインターフェイス上で動作します。メンテナンス ポイントは、特定の CFM サービスに常に関連付けられるため、特定のレベルの特定のメンテナンス ドメインに関連付けられます。メンテナンス ポイントは、関連するメンテナンス ドメインと同じレベルの CFM フレームを一般的に処理するだけです。下位メンテナンス レベルのフレームは通常ドロップされますが、上位のメンテナンス レベルのフレームは常に透過的に転送されます。これはメンテナンス ドメイン階層の適用に役立ち、特定のドメインの CFM フレームがドメインの境界を越えてリークできないようになります。メンテナンス ポイントには次の 2 種類があります。

- **メンテナンス エンド ポイント (MEP)** : ドメインのエッジに作成されます。CFM メッセージをドメイン内に制限する役割があります。メンテナンス エンド ポイント (MEP) は、ドメイン内の特定のサービスのメンバで、CFM フレームを送信および受信する役割があります。これらは定期的に連続性チェック メッセージを送信し、ドメイン内の他の MEP から同様のメッセージを受信します。また、管理者の要求に応じて traceroute メッセージやループバック メッセージも送信します。
- **メンテナンス 中間ポイント (MIP)** : ドメイン内部のポイントです。MIP は CFM パケットを転送しますが、MEP は CFM パケットをドメイン内に保持する必要があるため、CFM パケットを転送しません。MEP とは異なり、MIP はインターフェイスごとに明示的に設定されません。MIP は、CFM 802.1ag 規格で指定されたアルゴリズムに従って自動的に作成されます。

## CFM メンテナンスドメインとメンテナンスの関連付け（サービス）の表示

デバイスの CFM 設定を表示するには、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 > Network Devices** を選択します。

**ステップ 2** デバイスのリストで必要なデバイスを見つけ、デバイス名のハイパーリンクをクリックしてデバイスの詳細ウィンドウを開きます。

**ステップ 3** [論理ビュー (Logical View)] タブをクリックします。

**ステップ 4** **EOAM > CFM** を選択します。

## EOAM の接続チェックとパフォーマンス チェックの実行

Cisco EPN Manager では、EOAM 関連の定義済みの設定テンプレートが提供されています。これらを使用して、キャリアイーサネットネットワーク内の仮想接続 (VC) について接続とパフォーマンスをモニターリングできます。

これらのテンプレートを使用するには、左側のサイドバーから [設定 (Configuration)] > [テンプレート (Templates)] > [機能およびテクノロジー (Features & Technologies)] の順に選

択し、[CLI テンプレート (CLI Templates)] > [システム テンプレート - CLI (System Templates - CLI)] を選択します。

次の表に、使用可能な EOAM 設定テンプレートと、その目的、および指定する必要がある必須入力パラメータを示します。



**Note** テンプレートの展開の結果や出力を確認するには、変更の展開時に表示されるジョブの詳細を確認します。

Table 14: EOAM テンプレート

テンプレート名	用途	必須入力値	その他の情報
EOAM-CCDB-Content- IOS	CFM の動作を確認するため、またはネットワークでの EOAM の設定状況を確認するために、メンテナンス中間ポイント (MIP) の連続性チェック データベース (CCDB) の内容を表示します。	どのフィールドも必須ではありません。 <b>Domain ID:</b> メンテナンス ドメインを識別する方法を選択し、対応するフィールドに値を入力します。 <b>Service:</b> ICC MEG 識別子、VLAN ID、または VPN ID に基づいて、ドメイン内のメンテナンス アソシエーションを指定します。	
EOAM-CCDB-Content- IOS-XR	CFM の動作を確認するため、またはネットワークでの EOAM の設定状況を確認するために、メンテナンス中間ポイント (MIP) の連続性チェック データベース (CCDB) の内容を表示します。	どのフィールドも必須ではありません。 <b>Node ID:</b> ラック/スロット/モジュールの表記に 入力された、指定されたノードの CFM CCM 学習データベース。	
EOAM-CFM-Ping-IOS および EOAM-CFM-Ping- IOS-XR	CFM ループバック メッセージを使用して、宛先 MIP または MEP への接続を確認します。	<b>Ping Destination Type:</b> 宛先 MEP を MAC アドレスまたは MEP ID で識別します。宛先 MEP が複数ある場合は、[マルチキャスト (Multicast)] を選択します。  宛先 MEP のメンテナンス ドメイン名 (Maintenance domain name for destination MEP) : 宛先 MEP が存在するドメインの名前。	

テンプレート名	用途	必須入力値	その他の情報
EOAM-CFM-Traceroute- IOS	IOS デバイス (IOS devices) : 宛先 MEP までルートをトレースし、ホップの数とホップ間の接続を確認します。	<p><b>Destination Type:</b> MAC アドレス、MEP ID、または explore のオプションで宛先 MEP を識別します。</p> <p><b>Maintenance domain name for destination MEP:</b> 宛先 MEP が存在するドメインの名前。</p> <p><b>Service Type:</b> ドメイン内のメンテナンス アソシエーション (MA) を名前、ITU キャリアコード (ICC)、MA 番号、VLAN ID、または VPN ID のいずれかで識別します。</p>	
EOAM-CFM-Traceroute- IOS-XR	IOS-XR デバイス (IOS-XR devices) : 宛先 MEP までルートをトレースし、ホップの数とホップ間の接続を確認します。	<p><b>Maintenance domain name for destination MEP:</b> 宛先 MEP が存在するドメインの名前。</p> <p><b>Service Name:</b> 指定されたメンテナンス ドメイン内のメンテナンス アソシエーション (MA) によってモニターリングされるサービス インスタンスの名前。</p> <p><b>Destination Type:</b> MAC アドレス、MEP ID、または explore のオプションのいずれかで宛先 MEP を識別します。</p> <p><b>Source MEP ID:</b> ドメイン内のメンテナンス アソシエーション (MA) を名前、ITU キャリアコード (ICC)、MA 番号、VLAN ID、または VPN ID のいずれかで識別します。</p> <p><b>Source Interface Type:</b> ローカルに定義された CFM MEP のソース インターフェイス タイプ。</p> <p><b>Interface Path ID:</b> 物理または仮想 インターフェイス名。</p>	

テンプレート名	用途	必須入力値	その他の情報
EOAM-Configure-Y-1731-PM-On-Demand-Operation-CFM-Loopback-IOS-XR	CFM ループバックのオンデマンドイーサネット SLA 動作を設定します。デフォルトでは、双方向の遅延とジッタを測定します。	<p><b>Probe Domain:</b> プローブを有効にする場合にチェックボックスをオンにします。</p> <p><b>Domain Name:</b> ローカルに定義された CFM MEP のメンテナンス ドメインの名前。</p> <p><b>Domain Interface Type:</b> ローカルに定義された CFM MEP のソースインターフェイスタイプ。</p> <p><b>Domain Interface Path ID:</b> 物理または仮想インターフェイス名。</p> <p><b>Domain MAC Address or MEP-ID:</b> ドメインを MAC アドレスで識別するか MEP ID で識別するかを選択し、以下の関連するフィールドに必要な情報を入力します。MEP ID の場合は、1 から 8191 までの ID を入力します。</p>	必要に応じて、測定する統計のタイプ、集計タイプにビンを使用するか、プローブの頻度と期間の値などを指定できます。指定した値によってデフォルトのアクションがオーバーライドされます。
EOAM-Configure-Y-1731-PM-On-Demand-Operation-CFM-Synthetic-Loss-Measurement-IOS-XR	CFM の合成損失測定のオンデマンドイーサネット SLA 動作を設定します。デフォルトでは、両方の方向について一方向フレーム損失率 (FLR) を測定します。	<p><b>Probe Domain:</b> プローブを有効にする場合にチェックボックスをオンにします。</p> <p><b>Domain Name:</b> ローカルに定義された CFM MEP のメンテナンス ドメインの名前。</p> <p><b>Domain Interface Type:</b> ローカルに定義された CFM MEP のソースインターフェイスタイプ。</p> <p><b>Domain Interface Path ID:</b> 物理または仮想インターフェイス名。</p> <p><b>Domain MAC Address or MEP-ID:</b> ドメインを MAC アドレスで識別するか MEP ID で識別するかを選択し、以下の関連するフィールドに必要な情報を入力します。MEP ID の場合は、1 から 8191 までの ID を入力します。</p>	必要に応じて、測定する統計のタイプ、集計タイプにビンを使用するか、プローブの頻度と期間の値などを指定できます。指定した値によってデフォルトのアクションがオーバーライドされます。

テンプレート名	用途	必須入力値	その他の情報
EOAM-Configure-Y-1731-PM-On-Demand-Operation-CFM-Delay-Measurement-IOS-XR	CFMの遅延測定のアナライザネットワーク SLA動作を設定します。デフォルトでは、両方の方向について一方向の遅延とジッタ、および双方向の遅延とジッタを測定します。	<p><b>Probe Domain:</b> プロブを有効にする場合にチェックボックスをオンにします。</p> <p><b>Domain Name:</b> ローカルに定義された CFM MEP のメンテナンス ドメインの名前。</p> <p><b>Domain Interface Type:</b> ローカルに定義された CFM MEP のソースインターフェイスタイプ。</p> <p><b>Domain Interface Path ID:</b> 物理または仮想インターフェイス名。</p> <p><b>Domain MAC Address or MEP-ID:</b> ドメインを MAC アドレスで識別するか MEP ID で識別するかを選択し、以下の関連するフィールドに必要な情報を入力します。MEP ID の場合は、1 から 8191 までの ID を入力します。</p>	必要に応じて、測定する統計のタイプ、集計タイプにビンを使用するかどうか、プロブの頻度と期間の値などを指定できます。指定した値によってデフォルトのアクションがオーバーライドされます。

テンプレート名	用途	必須入力値	その他の情報
EOAM-Configure-Y-1731-PM-Direct-On-Demand-IOS	イーサネット サービスのリアルタイム トラブルシューティングをダイレクト モードで実行します。ダイレクト モードでは、動作が作成されて直ちに実行されます。	<p>フレームタイプ (Frame Type) : DMMv1 (フレーム遅延) または SLM (フレーム損失) のいずれかのフレーム タイプ。</p> <p>ドメイン名 (Domain Name) : ローカルに定義された CFM MEP のメンテナンス ドメインの名前。</p> <p>EVC または VLAN : テストを実行する EVC または VLAN を識別します。VLAN ID には 1 ~ 4096 を指定できます。</p> <p>ターゲット MPID (Target MPID) または MAC アドレス (MAC Address) : 宛先の MEP を、MPID (1 ~ 8191) または MAC アドレスのいずれかで識別します。</p> <p>CoS 値 (CoS Value) : 指定した MEP の CFM メッセージに適用されるサービスクラスレベル (0 ~ 7)。</p> <p>ローカル MPID (Local MPID) または MAC アドレス (MAC Address) : ソースの MEP を、MPID (1 ~ 8191) または MAC アドレスのいずれかで識別します。</p> <p>バースト (Burst) または連続 (Continuous) : オンデマンド動作中にフレームの連続ストリームを送信するかフレームのバーストを送信するかを指定します。</p> <p>集計期間 (Aggregation Period) : パフォーマンス測定が実行される時間の長さを秒単位で指定します (1 ~ 900)。この時間の経過後に統計が生成されます。</p>	
EOAM-Configure-Y-1731-PM-Referenced-On-Demand-IOS	イーサネット サービスのリアルタイム トラブルシューティングを参照モードで実行します。参照モードでは、以前に設定した動作が開始され実行されます。	<p>フレームタイプ (Frame Type) : プローブのタイプ (DMMv1 または SLM)。</p> <p>動作番号 (Operation Number) : 参照される動作の番号。</p>	
Remove-CFM-MEP-IOS	デバイスから MEP 設定を削除します。	インターフェイス名 (Interface Name)、サービスインスタンス番号 (Service Instance Number)、EVC 名 (EVC Name)。	

テンプレート名	用途	必須入力値	その他の情報
Remove-CFM-MEP- IOSXR	デバイスから MEP 設定を削除します。	インターフェイス名 (Interface Name)、ドメイン名 (Domain Name)。	
Remove-CFM- Service- IOS	CFM サービスを削除します。	インターフェイス名 (Interface Name)、サービス インスタンス番号 (Service Instance Number)、EVC 名 (EVC Name)、ドメイン名 (Domain Name)、レベル (Level)、サービス名 (Service Name)。	

## Quality of Service (QoS) の設定

Quality of Service (QoS) は、ネットワーク トラフィックの差別化サービスを配信できるようにするための機能のセットです。QoS 機能は、次の機能によって、より優れた予測可能性の高いネットワーク サービスを提供します。

- さまざまなネットワーク トラフィック クラスへの優先的な処理の提供。
- 重要なユーザーおよびアプリケーションの専用帯域幅のサポート。
- ジッターおよび遅延の制御 (リアルタイム トラフィックに必要)。
- ネットワークの輻輳の回避と管理。
- トラフィック フローをスムーズにするネットワーク トラフィックのシェーピング。
- ネットワーク全体でのトラフィックの優先順位の設定。

Cisco EPN Manager を使用して、キャリアイーサネットインターフェイスでの QoS を設定できます。適切な QoS アクションを適用する前に、分類プロファイル (またはクラス マップ) を作成することによって、関連するトラフィックを差別化する必要があります。デバイスに着信したパケットは、分類プロファイルの一致基準と照らし合わせて検査され、パケットがそのクラスに属しているかどうかを判定されます。一致するトラフィックは、アクションプロファイル (またはポリシー マップ) で定義されたアクションの対象となります。

分類プロファイルとアクションプロファイルを設定するには、左側のサイドバーから **Configuration > QoS > Profiles** を選択します。

このセクションは、次のトピックで構成されています。

- [QoS 分類プロファイルの作成, on page 160](#)
- [QoS アクションプロファイルの作成, on page 163](#)
- [デバイスで設定されている QoS プロファイルの確認, on page 169](#)
- [インターフェイスへの QoS アクションプロファイルの適用, on page 170](#)
- [デバイスから検出された QoS プロファイルのインポート, on page 171](#)

- 複数のインターフェイスからの QoS アクションプロファイルの関連付け解除, on page 172
- デバイスからの QoS 分類およびアクションプロファイルの削除, on page 173

## QoS 分類プロファイルの作成

トラフィックをクラス別に分類して、各クラスの分類基準と一致するトラフィックに特定のアクションが適用されるようにするには、分類プロファイル（クラス マップ）を作成します。

分類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** 左側のサイドバーで [設定 (Configuration)] > [QoS] > [プロファイル (Profiles)] の順に選択します。
- ステップ 2** [グローバル QoS 分類プロファイル (Global QoS Classification Profiles)] ページの上部にある追加アイコン ([+]) をクリックします。
- ステップ 3** 分類プロファイルの一意の名前を入力します。プロファイルを識別しやすくするために、プロファイルで定義された分類基準を反映した名前にしてください。さらに識別しやすくするには、説明を追加できます。
- ステップ 4** プロファイルでの一致基準を定義します。
- [すべてと一致 (Match All)] : トラフィックがすべてのクラス分類基準と一致すると、このクラスに分類されます。
  - [いずれかと一致 (Match Any)] : トラフィックがいずれかのクラス分類基準と一致すると、このクラスに分類されます。
- ステップ 5** 分類プロファイルの分類基準を定義するために、[QoS 分類 (QoS Classifications)] の下にあるプラスアイコンをクリックします。
- ステップ 6** トラフィックの分類基準とするアクションを選択してから、[値 (Value)] 列をクリックして関連する値を入力します。

アクション	説明	値
ACL	指定のアクセス コントロール リスト (ACL) でパケットを許可する必要があります。	ACL 名。最大 32 文字の英数字。
MPLS : インポジション	パケットに設定されたラベルエントリの Experimental (EXP) ビットの値が、ユーザーが指定した MPLSEXP 値と一致する必要があります。MPLS インポジションまたは MPLS Topmost を一致基準として使用します。MPLS 基準のいずれかを使用すると、他の基準は使用できなくなります。	0 ~ 7 の数値。最大 8 つのカンマ区切り値を入力できます。
MPLS : Topmost	topmost ラベルの Experimental (EXP) ビットの値が、ユーザーが指定した MPLSEXP 値と一致する必要があります。	0 ~ 7 の数値。最大 8 つのカンマ区切り値を入力できます。



アクション	説明	値
重ねて表示	このアクションは、クラスマップを別のクラスマップにカスケードするために使用します。既存のクラスマップと同様の分類ポリシーを使用する新しいクラスマップを作成する場合は、このアクションを使用できます。	子クラス マップを参照します。
QoS 分類 : COS	パケットのレイヤ 2 サービス クラス (CoS) ビットの値が、指定された CoS 値と一致する必要があります。	0～7の数値。最大 8 つのカンマ区切り値を入力できます。
QoS 分類 : COS : 内部	指定された値が、パケットのレイヤ 2 サービス クラス (CoS) マーキングの QinQ パケットの内部 CoS 値と一致する必要があります。	0～7の数値。最大 8 つのカンマ区切り値を入力できます。
QoS 分類 : DSCP	パケットの IP DiffServ コードポイント (DSCP) の値が、指定された値の 1 つ以上と一致する必要があります。	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。
QoS 分類 : DSCP : IPv4 のみ	IPv4 パケットの DSCP 値と照合します。	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。
QoS 分類 : 優先順位	パケットの IP プレシデンス値が、1 つ以上のプレシデンス値と一致する必要があります。	0～7の数値。最大 8 つのカンマ区切り値を入力できます。
QoS 分類 : 優先順位 : IPv4 のみ	IPv4 パケットのプレシデンス値と照合します。	0～7の数値。最大 8 つのカンマ区切り値を入力できます。
QoS 分類 : DEI	Drop Eligible Indicator (DEI) を使用して、輻輳発生時にドロップする対象フレームを示します。パケットが指定された DEI 値と一致する必要があります。	0 または 1。
QoS グループ	選択された QoS グループに応じてパケットを許可する必要があります。	選択されたデバイスに応じて、0～55、0～99、または 0～511 の範囲内にある最大 8 つのカンマ区切り値を入力できます。入力する値がデバイスでサポートされることを確認してください。

アクション	説明	値
QoS 分類：サービスインスタンス	<p>プロバイダ エッジ (PE) ルータでのサービスプロバイダ設定には、さまざまなサービスインスタンスがあります。QoS ポリシーマップは、これらのサービスインスタンスまたはサービスインスタンス グループに適用されます。</p> <p><b>Note</b> この基準が適用されるのは Cisco ASR 903 のみです。</p>	1 ~ 8000 の範囲にある任意の数のカンマ区切り値、またはそれぞれ 1 ~ 8000 の範囲にある、ハイフンでつながれた値を入力できます。
QoS 分類：VLAN	<p>仮想ローカルエリアネットワーク (VLAN) の識別番号を基本にしてトラフィックの照合と分類を行います。</p> <p><b>Note</b> [+] アイコンをクリックして、複数の QoS 分類：VLAN を追加し、値を指定します。</p>	1 ~ 4095 の範囲にある任意の数のカンマ区切り値、またはそれぞれ 1 ~ 4095 の範囲にある、ハイフンでつながれた値を入力できます。
QoS 分類：VLAN：内部	<p>内部仮想ローカルエリア ネットワーク (VLAN) の識別番号を基本にしてトラフィックの照合と分類を行います。</p> <p><b>Note</b> [+] アイコンをクリックして、複数の QoS 分類：VLAN：内部行を追加し、値を指定します。</p>	1 ~ 4095 の範囲にある任意の数のカンマ区切り値、またはそれぞれ 1 ~ 4095 の範囲にある、ハイフンでつながれた値を入力できます。
QoS 分類：廃棄クラス	<p>選択された破棄クラスに応じて、パケットを許可/破棄する必要があることを意味します。</p>	0 ~ 7 の任意の数値を入力できます。
QoS 分類：トラフィック クラス	<p>QoS 設定のトラフィック クラス。</p>	0 ~ 7 の任意の数値を入力できます。

- ステップ 7** 必要に応じて、追加の QoS 分類を定義します。
- ステップ 8** ウィンドウ下部で [保存 (Save)] をクリックし、プロファイルを保存します。右下隅に、プロファイルが保存されたことを示す通知が表示され、左側のプロファイル リストにプロファイルが表示されます。
- ステップ 9** リストからプロファイルを選択し、**Deploy** ボタンをクリックしてデバイスへのプロファイルの展開を開始します。
- ステップ 10** 既存の分類プロファイルの詳細を使用して新しいプロファイルを作成する場合は、**Clone** ボタンをクリックします。このプロファイルには、複製元の分類プロファイルの名前の末尾にサフィックス **-clone** が追加された名前が付けられます。複製したプロファイルの名前、一致基準、その他の詳細は編集できます。
- ステップ 11** 選択したプロファイルで、デバイス上の既存のクラスマップをオーバーライドするには、**Override existing configuration** チェックボックスをオンにします。このチェックボックスをオンにしないと、プロファイルはデバイス上の設定とマージされます。
- ステップ 12** QoS 分類プロファイルを展開するデバイスを選択します。
- ステップ 13** 必要に応じて、展開をスケジュールします。

**ステップ 14** [送信 (Submit)] をクリックします。右下隅に、プロファイルが展開されたことを示す通知が表示されます。展開ジョブのステータスを確認するには、左側のサイドバーから **Administration > Job Dashboard** を選択します。該当するジョブを選択します。ウィンドウの下部セクションにジョブの詳細情報と履歴が表示されます。詳細については、[情報 (Information)] アイコンをクリックしてください。

## QoS アクション プロファイルの作成

特定のトラフィッククラスに属しているトラフィックに適用するアクションを指定するには、アクションプロファイル (ポリシーマップ) を作成します。

アクション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** 左側のサイドバーで [設定 (Configuration)] > [QoS] > [プロファイル (Profiles)] を選択します。
- ステップ 2** 左側の [QoS プロファイル (QoS Profiles)] ペインで [ユーザー定義のグローバル QoS プロファイル (User Defined Global QoS Profiles)] > [アクションプロファイル (Action Profiles)] を選択します。
- ステップ 3** [アクションプロファイルの作成 (Create Action Profile)] ペイン上部にある追加 ([+]) アイコンをクリックします。
- ステップ 4** アクションプロファイルに一意の名前を指定し、必要に応じて説明を入力します。
- ステップ 5** アクションを割り当てる分類プロファイルを選択します。[分類プロファイル (Classification Profiles)] でプラス記号のアイコンをクリックし、リストから必要なプロファイルを選択し、**OK** をクリックします。
- ステップ 6** 分類プロファイル (クラス マップ) を選択し、トラフィックがプロファイルに一致する場合に適用するアクションを定義します。ポリシング、マーキング、キューイング、シェーピング、および RED の各アクションと、サービス ポリシー (H-QoS) を定義できます。各アクションタイプとその説明が表示される次のようなタブがあります。

- [ポリサーアクション (Policer Action)] : トラフィック ポリシングは、トークンバケットアルゴリズムによりインターフェイスで許容されるトラフィックの最大レートを管理します。トラフィック ポリシングでは、CIR のバーストサイズ (Bc) を設定できるので、ある程度の帯域幅管理も行えます。最大情報レート (PIR) がサポートされている場合は 2 番目のトークンバケットが強制的に適用されます。この 2 レート ポリサーは 2 つの独立レート (設定情報レート (CIR) と最大情報レート (PIR)) でトラフィックを計測できます。認定トークンバケットは、オーバーフローするまで最大で認定バースト (Bc) のサイズのバイト数を保持でき、パケットが CIR に準拠しているか、CIR を超えているかを判別します。ピークトークンバケットは、オーバーフローするまで最大でピークバースト (Be) のサイズのバイト数を保持でき、パケットが PIR に違反しているかどうかを判別します。パケットが CIR/PIR に準拠している場合、超えている場合、違反している場合それぞれに異なるアクションを実行できます。たとえば、準拠するパケットが送信されるように設定し、超過するパケットは優先順位を低くして送信し、違反するパケットはドロップされるように設定できます。

[ポリサーアクション (Policer Action)] タブでは、次の項目を指定します。

- [設定情報レート (CIR) (Committed Information Rate (CIR))] : 長期平均転送速度。これは 1 秒あたりのビット数 (bps) または使用可能/未使用帯域幅に対する割合として指定できます。このレートを下回るトラフィックは、常に適用されます。入力する CIR 値がデバイスでサポートさ

れていることを確認し、正しいCIR単位値 (bps、kbps、mbps、gpbs、パーセント) を選択します。

- [バースト (Bc) (Burst (Bc))] : トラフィック バーストの最大サイズ (バイト単位) 。これを超えると、一部のトラフィックは CIR を超えます。
- [最大情報レート (PIR) (Peak Information Rate (PIR))] : 一部のトラフィックが CIR に関連付けられた PIR 値を超えるまでの許容トラフィック バースト量。入力する PIR 値がデバイスでサポートされていることを確認し、CIR で選択したものと同一単位値 (bps、kbps、mbps、gpbs、パーセント) を選択します。
- [超過バースト (Be) (Excess Burst (Be))] : トラフィック バーストの最大サイズ (バイト単位) 。これを超えると、トラフィックは PIR を超えます。
- [トラフィックの色分け動作 (Traffic Coloring Behavior)] で、トラフィックがレート制限に準拠している場合、超えた場合、または違反した場合に実行するアクションを選択します。必要に応じて値を指定します。カラーアウェアトラフィック ポリシングを有効にするには、[適合カラー (Conform Color)] と [超過カラー (Exceed Color)] の値をそれぞれのクラスプロファイルに関連付けて指定します。カラーアウェアポリシングでは、CIR、PIR、適合アクション、超過アクション、および違反アクションに基づいて、次のような結果になります。
  - 測定レートが CIR 以下で、指定されたクラス (適合カラー) に属するパケットは、レートに適合しているものとしてポリシングされます。これらのパケットは、指定された適合アクションに従ってもポリシングされます。この場合、パケットは送信されます。
  - 測定レートが CIR と PIR の間にあり、適合カラークラスまたは超過カラークラスのいずれかに属するパケットは、CIR を超えているものとしてポリシングされます。これらのパケットは、指定された超過アクションに従ってもポリシングされます。この場合、パケットの優先順位値が設定されて、パケットが送信されます。
  - 測定レートが PIR より高いパケット、または適合カラークラスにも超過カラークラスにも属さないパケットは、レートに違反しているものとしてポリシングされます。これらのパケットは、指定された違反アクションに従ってもポリシングされます。この場合、パケットは廃棄されます。
- [マーカーアクション (Marker Action)] : パケットマーキングを利用すれば、ネットワークを複数の優先度レベルまたはサービスクラスに分割できます。トラフィックフローのマーキングは、次により実行されます。
  - タイプオブサービス (ToS) バイトに IP precedence ビットまたは DSCP ビットを設定する。
  - レイヤ2ヘッダー内の CoS ビットを設定する。
  - インポーズされた、または最上位のマルチプロトコルラベルスイッチング (MPLS) ラベル内に EXP ビットを設定する。
  - qos-group ビット、traffic-clas ビット、および discard-class ビットを設定する。

[マーカーアクション (Marker Action)] タブでは、次の項目を指定します。

- [マーキング機能とマーキング値 (Marking Feature and Marking Value) ]: トラフィックのマーキング方法と必須値。
- [キューイングアクション (Queueing Action) ]: キューイングは、トラフィック輻輳管理に使用されます。輻輳管理では、キューを作成し、そのキューにパケットの分類に基づいてパケットを割り当て、キューにあるパケットの送信をスケジューリングする必要があります。

[キューイングアクション (Queueing Action) ]タブで、トラフィックのキューイング方法 ([帯域幅 (Bandwidth) ] または [プライオリティ (Priority) ]) を選択し、次の項目を指定します。

- [帯域幅 (Bandwidth) ]: トラフィッククラスに割り当てられる帯域幅の量を、キロビット/秒または絶対保証帯域幅に対するパーセンテージのいずれかで指定します。帯域幅に基づいてキューイングすることを選択した場合は、残り帯域幅のパーセンテージとして帯域幅を割り当てることもできます。
- [キュー制限 (Queue Limit) ]: このクラスに関連付けられているすべての個別キューのパケット/バイト/ミリ秒の最大数。キューのサイズがこの値を超えると、パケットがドロップされます。

[帯域幅 (Bandwidth) ] を選択した場合は、次の項目を指定します。

- [均等化キューを有効にする (Enable Fair Queue) ]: 重み付け均等化キューイングを有効にするには、このチェックボックスをオンにします。
- [個別キュー サイズ (Individual Queue Size) ]: 均等化キューが有効な場合に使用します。輻輳期間に各クラス別キューで許容する最大パケット数を指定します。

[プライオリティ (Priority) ] を選択した場合は、次の項目を指定します。

- [キューバーストサイズ (バイト数) (Queue Burst Size (bytes)) ]: バーストサイズにより、ネットワークが一時的なトラフィックのバーストに対応できるように設定されます。範囲は 18 ~ 2000000 バイトです。デフォルトは、設定された帯域幅レートで 200 ミリ秒のトラフィックです。
- [プライオリティ レベル (Priority Level) ]: ポリシーマップのクラスに、異なる優先順位 (プライオリティ キュー レベル 1 ~ 3) を設定できます。これらのキューのパケットは、他のキューと比較して低遅延になります。同じポリシー マップ内の異なる 2 つのクラスに同じ優先度レベルを指定することはできません。
- [シェーピングアクション (Shaping Action) ]: トラフィックシェーピングでは、指定されたレートにトラフィックをシェーピングすることでトラフィックが調整されます。

[シェーピングアクション (Shaping Action) ]タブでは、次の項目を指定します。

- [平均またはピーク レートトラフィックシェーピングの選択 (Select Average or Peak rate traffic shaping) ]: 平均レートシェーピングでは、転送速度が CIR に制限されます。ピークレートシェーピングでは、CIRを超えるトラフィックを送信するようルータを設定します。ピークレートを判別するため、ルータでは「ピークレート=CIR(1+Be/Bc)」という公式が使用されます。ここで Be は超過バーストサイズ、Bc は認定バーストサイズです。

- ピーク レート トラフィック シェーピングを選択する場合は、バースト サイズと超過バースト サイズをバイト単位で指定します。
- 必要に応じて、FECN 適応型シェーピングを有効にします。適応型シェーピングでは、逆方向明示的輻輳通知 (BECN) 信号を受信すると使用可能な帯域幅が推定されます。FECN 適応型シェーピングにより、ルータは順方向明示的輻輳通知 (FECN) 信号を BECN 信号として反映します。
- FECN 適応型シェーピングが有効な場合は、適応レート (トラフィックシェーピングの最小ビット レート) を指定します。

• [RED アクション (RED Action) ] : 重み付けランダム早期検出 (WRED) は、キューがその制限に達する前に輻輳を制御する、プロアクティブなキューイング戦略を採用した輻輳回避手法です。WRED は、ランダム早期検出 (RED) メカニズムと IP プレシデンス、DiffServ コードポイント (DSCP) 、および discard-class の機能を組み合わせて、優先順位が高いパケットから処理します。インターフェイスで輻輳が発生し始めると、WRED は優先順位の低いトラフィックを高い確率で破棄します。WRED は、レイヤ 3 キューの平均の深さを制御します。

[RED アクション (RED Action) ] タブで、次の項目を指定します。

- [分類メカニズム (Classification Mechanism) ] : WRED ドロップ ポリシーを定義するための基準を選択します。WRED では、次のように特定の packets 分類に基づいてドロップポリシーを定義します。

[CLP] : セル損失率優先度 (CLP) 値に基づいて WRED のドロップ ポリシーを設定します。有効な値は、0 または 1 です。

[CoS] : パケットに関連付けられている指定されたサービス クラス (CoS) ビットに基づいて WRED のドロップ ポリシーを設定します。有効な値は 0 ~ 7 です。

[破棄クラス (Discard Class) ] : discard-class の値に基づいて WRED のドロップ ポリシーを設定します。有効な値は 0 ~ 7 です。discard-class の値により、トラフィック ドロップの Per-Hop Behavior (PHB) が設定されます。discard-class に基づく WRED は出力機能です。

[DSCP] : DSCP 値に基づいて WRED のドロップ ポリシーを設定します。設定されている場合、ルータは設定した WRED しきい値に従い、指定された DSCP 値を持つパケットをランダムにドロップします。

[プレシデンス (Precedence) ] : IP プレシデンス レベルに基づいて WRED のドロップ ポリシーを設定します。有効な値は 0 ~ 7 です。通常、0 はアグレッシブに管理可能な (ドロップ可能な) 優先順位が低いトラフィックを表し、7 は優先順位が高いトラフィックを表します。プレシデンス レベルが低いトラフィックは通常、廃棄確率が高くなります。WRED によりパケットがドロップされると、TCP を使用している送信元ホストはこのドロップ操作を検知し、パケットの送信速度を低下させます。

[DEI] : フレーム リレーフレームのアドレス フィールドの廃棄条件 (DE) ビットを使用して、輻輳が発生しているフレーム リレー ネットワークでのフレームの廃棄を優先します。フレーム リレー DE ビットは 1 ビットしかないため、設定は 2 つ (0 または 1) しかありません。フレーム リレー ネットワークで輻輳が発生した場合、DE ビットが 0 に設定されているフレームよりも前に、DE ビットが 1 に設定されているフレームが廃棄されます。

[RED デフォルト (RED Default)] : WRED プロファイルのクラスの最小しきい値、最大しきい値、およびマーク確率デノミネータ (MPD) の設定値のデフォルトセットです。

- 必要に応じて ECN を有効にします。ECN (明示的輻輳通知) は、平均キュー長が特定のしきい値を超えた場合、ECN は、それらをドロップする代わりにパケットをマーキングします。ルータとエンドホストは、このマーキングをネットワークの輻輳とパケットの送信速度の低下を示す警告として使用します。
- 選択した分類メカニズムの有効な値ごとに、しきい値とマーク確率を定義します。たとえば、プレシデンスを使用する場合には 7 つの有効な値それぞれにしきい値を定義できます。最小しきい値は、キューで許容する最小パケット数です。平均キューの長さが最小しきい値に達すると、WRED では、指定された DSCP、IP プレシデンス、discard-class、または atm-clp の値で、「一部の」パケットがランダムにドロップされます。有効な最小しきい値は 1 ~ 16,384 です。最大しきい値は、キューで許容する最大パケット数です。平均キューの長さが最大しきい値を超えると、WRED では、指定された DSCP、IP プレシデンス、discard-class、または atm-clp の値のすべてのパケットがドロップされます。有効な最大しきい値は、最小しきい値 ~ 16,384 です。

• [サービス ポリシー (Service Policy)] :

[サービス ポリシー (Service Policy)] タブでは、階層型 QoS (H-QoS) を設定できます。H-QoS により、階層の複数レベルで QoS 動作を指定できます。H-QoS を使用して、複数のキューを一括でシェーピングするため複数のポリシーマップを指定できます。すべての階層型ポリシータイプは、最上位の親ポリシーと 1 つ以上の子ポリシーで構成されます。service-policy コマンドは、ポリシーを異なるポリシーに適用する場合、およびポリシーをインターフェイスに適用する場合に使用します。

H-QoS を設定するには、[サービス ポリシー (Service Policy)] タブに移動し、[有効化 (Enable)] チェックボックスをオンにし、[サービス ポリシー (Service Policy)] ドロップダウンメニューから子サービスポリシーを選択します。選択した子サービスポリシーは、このアクションプロファイルが属する親ポリシーマップに関連付けられます。子サービスポリシーは、同じポリシーマップの親ポリシーとして機能できない点に注意してください。たとえば、子サービスポリシー「X」が親ポリシーマップ「Y」に属している場合、子ポリシー「X」にサービスポリシーマップ「Y」を含めることはできません。

H-QoS の制約事項 : Cisco IOS-XE デバイス (Cisco ASR903、Cisco ASR907、Cisco ASR920、Cisco NCS42XX など) には、次に示す H-QoS の制約事項が適用されます。

- 親ポリシーマップの制約事項 :
  - 親ポリシーマップを作成するときには、「class-default」クラスだけを使用できます。
  - 親ポリシーマップには、EFP (サービス インスタンス) などの一致条件が設定されているクラスが含まれている必要があります。
  - 親ポリシーマップには、VLAN などの一致条件が設定されているクラスが含まれている必要があります。
- 子ポリシーマップの制約事項 :

- EFP（サービスインスタンス）と VLAN を一致タイプとして使用して子ポリシーマップを作成することはできません。

- ステップ 7** ウィンドウ下部で [保存 (Save)] をクリックし、プロファイルを保存します。右下隅に、プロファイルが保存されたことを示す通知が表示され、左側のプロファイルリストにプロファイルが表示されます。
- ステップ 8** [グローバル QoS アクション プロファイル (Global QoS Action Profiles)] ペインでプロファイルを選択し、[展開 (Deploy)] ボタンをクリックし、デバイスへのプロファイルの展開を開始します。
- ステップ 9** 既存のアクションプロファイルの詳細情報を使用して新しいプロファイルを作成するには、[複製 (Clone)] ボタンをクリックします。このプロファイルの名前は、複製元のアクションプロファイルの名前にサフィックス **-clone** が付いたものになります。複製したプロファイルでは、名前やアクションなどの詳細情報を編集できます。
- ステップ 10** 選択したプロファイルで、デバイス上の既存のポリシーマップをオーバーライドするには、[既存の設定の上書き (Override existing configuration)] チェックボックスをオンにします。このチェックボックスをオンにしないと、プロファイルにデバイスの設定がマージされます。
- ステップ 11** QoS アクションプロファイルを展開するデバイスを選択します。
- ステップ 12** 必要に応じて、展開をスケジュールします。
- ステップ 13** [送信 (Submit)] をクリックします。右下隅に、プロファイルが展開されたことを示す通知が表示されます。展開ジョブのステータスを確認するには、左側のサイドバーから **Administration > Job Dashboard** を選択します。該当するジョブを選択します。ウィンドウの下部セクションにジョブの詳細情報と履歴が表示されます。詳細については、[情報 (Information)] アイコンをクリックしてください。

## QoS サブアクション プロファイルの作成

アクションプロファイル（ポリシーマップ）は、特定のトラフィック クラスに属しているトラフィックに適用するアクションを指定します。これらは、トラフィックがプロファイルに一致する場合に適用するアクションを定義する、複数の分類プロファイルに関連付けられます。ポリシング、マーキング、キューイング、シェーピング、および RED の各アクションと、サービスポリシー（H-QoS）を定義できます。

サブアクションプロファイルは、単一の分類プロファイルにのみ関連付けられているアクションプロファイルです。回線/VC のプロビジョニング中にサブアクションプロファイルを使用して、単一のアクションに基づくアクションプロファイルを回線/VCに関連付けることができます。

サブアクションプロファイルを作成する手順は次のとおりです。

- ステップ 1** 左側のサイドバーで [設定 (Configuration)] > [QoS] > [プロファイル (Profiles)] を選択します。
- ステップ 2** 左側の [QoS プロファイル (QoS Profiles)] ペインで [ユーザー定義のグローバル QoS プロファイル (User Defined Global QoS Profiles)] > [サブアクションプロファイル (Sub-Action Profiles)] を選択します。
- ステップ 3** [サブアクションプロファイルの作成 (Create Sub-Action Profile)] ペイン上部にある追加 ([+]) アイコンをクリックします。



- ステップ4** サブアクションプロファイルに一意の名前を指定します。説明を入力することもできます。
- ステップ5** アクションを割り当てる分類プロファイルを選択します。[分類プロファイル (Classification Profiles)] でプラス記号のアイコンをクリックし、リストから必要なプロファイルを選択し、**OK** をクリックします。
- サブアクションプロファイルに追加できる分類プロファイルは1つだけです。複数の分類プロファイルに関連付けるには、アクションプロファイルを作成する必要があります。
- ステップ6** トラフィックが分類プロファイルで指定された条件と一致する場合に実行する必要があるアクションを指定します。各種のオプションの説明については、[QoS アクションプロファイルの作成 \(163 ページ\)](#) を参照してください。

---

## QoS アクションおよびサブアクション プロファイルのインポートとエクスポート

---

- ステップ1** 左側のサイドバーで [設定 (Configuration)] > [QoS] > [プロファイル (Profiles)] を選択します。
- ステップ2** アクションプロファイルをエクスポートするには、左側のペインで [ユーザー定義のグローバル QoS プロファイル (User Defined Global QoS Profiles)] > [アクションプロファイル (Action Profiles)] を選択します。
- ステップ3** サブアクションプロファイルをエクスポートするには、左側のペインで [ユーザー定義のグローバル QoS プロファイル (User Defined Global QoS Profiles)] > [サブアクションプロファイル (Sub-Action Profiles)] を選択します。
- ステップ4** プロファイルのエクスポートするには、エクスポートするプロファイルを選択し、[エクスポート (Export)] をクリックします。指定した場所にファイルが保存されます。
- ステップ5** プロファイルをインポートするには、[インポート (Import)] をクリックし、インポートする XML ファイル (アクションまたはサブアクションプロファイルに関する情報を含む) を選択し、[OK] をクリックします。インポートされたプロファイルはそれぞれ、[アクションプロファイル (Action Profiles)] ページまたは [サブアクションプロファイル (Sub-Action Profiles)] ページに表示されます。

以下の点に注意してください。

- 1つのインスタンスでインポートできるプロファイルの数に制限はありませんが、最適なパフォーマンスを確保するため、選択するプロファイルは10個までにすることをお勧めします。
- インポートするファイルのサイズは20 MB 未満にしてください。
- XML 形式のみのファイルをインポートできます。

---

## デバイスで設定されている QoS プロファイルの確認

特定のデバイスに展開された QoS プロファイルを確認するには、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 > Network Devices** を選択します。

- ステップ 2** 必要なデバイスを見つけ、デバイス名のハイパーリンクをクリックします。デバイスの詳細が表示されず。
- ステップ 3** [論理ビュー (Logical View)] タブをクリックします。
- ステップ 4** 左側のペインで QoS の横の矢印をクリックし、[アクション プロファイル (Action Profiles)] または [分類 プロファイル (Classification Profiles)] を選択します。選択したデバイスに展開されているプロファイルを示すテーブルが表示されます。プロファイル名 (青色のハイパーリンク) をクリックして、プロファイルの詳細を表示します。

## インターフェイスへの QoS アクション プロファイルの適用

デバイスに導入されたアクション プロファイルを選択し、そのデバイス上の複数のインターフェイスにアクション プロファイルを適用できます。アクション プロファイルにより、特定のトラフィッククラスに属するトラフィックに適用するアクションを指定できます。既存のプロファイルをインターフェイスに適用する前に、プロファイルに変更を加えたり、そのプロファイルを使用して新しいプロファイルを作成したりできます。すでにアクション プロファイルが適用されているインターフェイスを選択すると、Cisco EPN Manager はその旨を通知し、ユーザーに既存のプロファイルをオーバーライドするオプションを提示します。インターフェイスにアクション プロファイルを適用するには、その前に、必要なプロファイルがデバイスに導入されている状態にしなければなりません。これを行うには、[QoS アクション プロファイルの作成 \(163 ページ\)](#) を参照してください。

アクション プロファイルをインターフェイスに適用するには、次の手順に従います。

- ステップ 1** 左側のサイドバーで、[構成 (Configuration)] > [QoS] > [インターフェイス (Interfaces)] の順に選択します。

Cisco EPN Manager インターフェイスが [イーサネット CSMA/CD、IEEE8023 ADLAG (Ethernet CSMA/CD、IEEE8023 ADLAG)]、[ギガビットイーサネット (Gigabit Ethernet)]、および [L2 VLAN] カテゴリに表示されます。その他すべてのポートは、[ユーザー定義 (User Defined)] カテゴリに表示されます。

- ステップ 2** アクション プロファイルに関連付けるインターフェイスを選択します。

- ステップ 3** [アクション プロファイルの関連付け (Associate Action Profile)] をクリックし、アクション プロファイルを選択して、そのプロファイルを適用する方向を設定します。使用可能なアクション プロファイルのリストと、それらのプロファイルを適用できるインターフェイスがリストされます。インターフェイスごとに、その名前、適用方向、およびそのインターフェイスにすでに存在するアクション プロファイルがリストされます。

(注) QoS スケーリング プロファイルの設定は、バンドルイーサネットインターフェイスとサブインターフェイスのアクション プロファイルを関連付けるための前提条件になります。設定例：

```
hw-module profile qos bundle <high-scale|medium-scale|low-scale> location <card>
```

- ステップ 4** [アクション プロファイル (Action Profiles)] ドロップダウンリストから必要なアクション プロファイルを選択します。メニューが空の場合は、アクション プロファイルを作成してから、それらのアクション プロ

ファイルをデバイスに関連付ける必要があります。[QoS アクションプロファイルの作成 \(163 ページ\)](#) を参照してください。

**ステップ 5** **インターフェイス (Interfaces)** ]セクションで、プロファイルを適用する方向を指定します。プロファイルをサブインターフェイスに適用する場合は、メインインターフェイスの方向と逆の方向で適用するようにしてください。適用する方向を変更するには、ダイアログの左上隅にある **[編集 (Edit)]** アイコンを使用します。

(注) キューイングアクションが含まれるポリシーマップを入力方向でインターフェイスに適用することはできません。

**ステップ 6** (任意) 選択したアクションプロファイルを将来の日時に適用するようにスケジュールすることもできます。それには、**[スケジュール (Schedule)]**セクションを展開し、プロファイルを適用する日時と頻度を指定します。必要に応じて、このタスクは**[ジョブ (Jobs)]**ページでさらに編集できます。

**ステップ 7** **[OK]** をクリックしてアクションプロファイルを選択したデバイスに適用します。ダイアログの右下隅に表示される通知で、プロファイルが正常に適用されたか、またはジョブが失敗したかを確認できます。詳細情報を確認するには、**[詳細の表示 (Show Details)]** リンクをクリックします。

アクションプロファイルとそのプロファイルが適用されるインターフェイスとの関連付けを解除するには、次を参照してください。[複数のインターフェイスからの QoS アクションプロファイルの関連付け解除 \(172 ページ\)](#)

---

## デバイスから検出された QoS プロファイルのインポート

デバイスから検出された QoS プロファイルを Cisco EPN Manager に直接インポートできます。インポートした QoS プロファイルを、Cisco EPN Manager を使って編集したり、デバイス上でさらに詳細に設定したりできます。Cisco EPN Manager にすでに存在する他のプロファイルと同じプロファイル名を持つ、デバイスから検出されたプロファイルは、グローバルプロファイルとして表されます。これは、**[グローバルプロファイル (Global Profiles)]** ページの **[グローバル (Global)]** ]列に示されます。複数のグローバルプロファイルの名前が同じでも、QoS 設定が異なる場合があることに注意してください。グローバルプロファイルのインポート時には、検出されたプロファイルによって (同じ名前の) 既存のプロファイルを上書きするか、それともインポート前にプロファイルの名前を変更するかを選択できます。

デバイスから検出された QoS プロファイルをインポートするには、次の手順を実行します。

### 始める前に

デバイスのインベントリ収集ステータスが **[完了 (Completed)]** であることを確認します。これにより、デバイスの QoS プロファイルが Cisco EPN Manager によって検出されることを確認できます。

---

**ステップ 1** 左側のサイドバーから **[設定 (Configuration)]** ]>**[QoS]** >**[プロファイル (Profiles)]** ]を選択し、すべての Cisco EPN Manager QoS プロファイルを表示します。

- ステップ 2** アクションプロファイルをインポートするには、左側の [QoS プロファイル (QoS Profiles) ] ペインから、**[検出されたプロファイル (Discovered Profiles) ] > [アクション プロファイル (Action Profiles) ]** を選択します。
- ステップ 3** 分類プロファイルをインポートするには、左側の [QoS プロファイル (QoS Profiles) ] ペインから、**[検出されたプロファイル (Discovered Profiles) ] > [分類プロファイル (Classification Profiles) ]** を選択します。
- ステップ 4** 最初にデバイスを選択した後で、そのデバイスで検出されたプロファイルを選択するには、次の手順を実行します。
- [設定 (Configuration) ] > [ネットワーク デバイス (Network Devices) ] を選択し、デバイス名のハイパーリンクをクリックして、デバイスを選択します。
  - [論理ビュー (Logical View) ] タブをクリックします。
  - [QoS] を展開します。
  - デバイスからインポートするプロファイルのタイプに応じて、[アクション プロファイル (Action Profiles) ] または [分類プロファイル (Classification Profiles) ] を選択します。
  - (オプション) プロファイルを表示した後、Cisco EPN Manager によって検出されたすべての QoS プロファイルを一覧しているページからそれらのプロファイルを直接インポートするには、[グローバル プロファイル ページ (Global Profile Page) ] ハイパーリンクをクリックし、ステップ 5 に進みます。
  - プロファイルを選択し、[グローバルにする (Make Global) ] をクリックします。
  - ステップ 6 に進みます。
- ステップ 5** インポートするプロファイルを選択して、[インポート (Import) ] をクリックします。まだデバイスに存在しないプロファイルのみを確実にインポートするには、([グローバル (Global) ] 列に [いいえ (No) ] とマークされている) グローバルでないプロファイルを選択します。
- ステップ 6** Cisco EPN Manager に重複プロファイルがある場合は、プロファイルの名前を変更して新しい名前と同じ QoS 設定のプロファイルを作成するか、それとも既存のプロファイルを上書きするかを選択するように求められます。必要な変更を加えます。
- ステップ 7** 既存の QoS プロファイルの詳細を使用して新しいプロファイルを作成するには、[複製 (Clone) ] ボタンをクリックします。このプロファイルは、複製元の QoS プロファイルの名前にサフィックス **-clone** が付いた名前になります。この複製されたプロファイルの詳細を任意に編集できます。
- ステップ 8** [保存 (Save) ] をクリックして、選択した QoS プロファイルをインポートします。  
インポートしたプロファイルを特定のデバイスのインターフェイスに適用するには、[インターフェイスへの QoS アクション プロファイルの適用 \(170 ページ\)](#) を参照してください。

## 複数のインターフェイスからの QoS アクション プロファイルの関連付け解除

アクションプロファイルにより、特定のトラフィック クラスに属するトラフィックに適用するアクションを指定できます。デバイスに導入されたアクションプロファイルを選択し、そのデバイス上の複数のインターフェイスにアクションプロファイルを適用できます。プロファイルをインターフェイスに適用した後、必要に応じてプロファイルとインターフェイスの関連付けを解除することができます。アクションプロファイルとインターフェイスの関連付けを解除するには、その前に、対象のプロファイルがデバイスに適用されていることを確認する必要があります。

あります。 [インターフェイスへの QoS アクションプロファイルの適用 \(170ページ\)](#) を参照してください。

アクションプロファイルをインターフェイスに適用するには、次の手順に従います。

**ステップ 1** 左側のサイドバーで、[構成 (Configuration)] > [QoS] > [インターフェイス (Interfaces)] の順に選択します。

あるいは、[構成 (Configuration)] > [QoS] > [プロファイル (Profiles)] に移動してプロファイルを選択した後、そのプロファイルが適用されているインターフェイスからプロファイルの関連付けを解除することもできます。

Cisco EPN Manager インターフェイスが [イーサネット CSMA/CD、IEEE8023 ADLAG (Ethernet CSMA/CD、IEEE8023 ADLAG)] および [L2 VLAN] カテゴリの下に表示されます。その他すべてのポートは、[ユーザー定義 (User Defined)] カテゴリの下に表示されます。

**ステップ 2** アクションプロファイルの関連付けを解除するインターフェイスを選択します。

**ステップ 3** [アクションプロファイルの関連付け解除 (De-associate Action Profile)] をクリックします。

**ステップ 4** (任意) 選択したアクションプロファイルを将来の日時に関連付け解除するようにスケジュールすることもできます。それには、[スケジュール (Schedule)] セクションを展開し、関連付けを解除する必要があるプロファイルに応じて日時と頻度を指定します。

**ステップ 5** [OK] をクリックして確認します。選択したインターフェイスからアクションプロファイルの関連付けが解除されます。ウィンドウの右下隅に表示される通知で、プロファイルが正常に関連付け解除されたか、またはジョブが失敗したかを確認できます。詳細情報を確認するには、[詳細の表示 (Show Details)] リンクをクリックします。

## デバイスからの QoS 分類およびアクション プロファイルの削除

デバイスに展開されている QoS 分類およびアクション プロファイルを削除するには、次の表に示すパスに移動します。



(注) デバイスから直接検出された QoS アクションおよび分類プロファイルは削除できません。Cisco EPN Manager を使用して作成した (およびそれにインポートした) プロファイルのみを削除できます。

参照プロファイルの削除を避けるため、削除操作は次のシナリオではサポートされていません。

- 他の分類プロファイルに関連付けられた QoS 分類プロファイルは削除できません。たとえば、分類プロファイルで [カスケード (Cascade)] オプションを使用して選択した分類プロファイルを参照する場合、選択したプロファイルの削除操作は失敗します。
- アクションプロファイルによって参照される QoS 分類プロファイルは削除できません。

- デバイス インターフェイスに正常に適用されたアクション プロファイルは削除できません。
- アクション プロファイルは、別のアクション プロファイルによって参照されている場合は削除できません。たとえば、アクション プロファイルが参照ポリシーを使用して他のアクション プロファイルに関連付けられている場合、そのアクション プロファイルの削除操作は失敗します。

表 15: QoS アクションおよび分類プロファイルを削除するためのナビゲーションパス

タスク	GUI での手順
ユーザー定義の分類プロファイルの削除	<ol style="list-style-type: none"> <li>1. [構成 (Configuration) ] &gt; [QoS] &gt; [分類プロファイル (Classification Profiles) ] を選択します。</li> <li>2. デバイスや Cisco EPN Manager から削除する分類プロファイルを選択します。</li> <li>3. タスク バーで [X] (削除) アイコンをクリックします。</li> <li>4. または、デバイスのハイパーリンクをクリックして、選択した分類プロファイルを削除するデバイスを選択することもできます。</li> <li>5. [送信 (Submit) ] をクリックします。[ジョブの詳細 (Job Details) ] ポップアップウィンドウをクリックして、削除操作のステータスを確認できます。</li> </ol>
ユーザー定義のアクションプロファイルの削除	<ol style="list-style-type: none"> <li>1. [構成 (Configuration) ] &gt; [QoS] &gt; [アクションプロファイル (Action Profiles) ] を選択します。</li> <li>2. デバイスや Cisco EPN Manager から削除するアクションプロファイルを選択します。</li> <li>3. タスク バーで [X] (削除) アイコンをクリックします。</li> <li>4. または、デバイスのハイパーリンクをクリックして、選択したアクションプロファイルを削除するデバイスを選択することもできます。</li> <li>5. [送信 (Submit) ] をクリックします。[ジョブの詳細 (Job Details) ] ポップアップウィンドウをクリックして、削除操作のステータスを確認できます。</li> </ol>



## デバイスの変更内容の保存

デバイスに変更を加えた後、データベースに変更を保存し、必要に応じてデバイスの物理および論理インベントリを収集します。詳細については、次のトピックを参照してください。

- [データベースへのデバイス設定変更の保存（更新）（175 ページ）](#)
- [デバイスのインベントリの即時収集（同期）（175 ページ）](#)

### データベースへのデバイス設定変更の保存（更新）

デバイスに変更を加えた後は、構成ウィンドウの[更新 (Update)] をクリックして変更内容をデータベースに保存してください。[更新 (Update)] ボタンが表示されていない場合は、手動による同期を実行して、変更を保存するだけでなく、デバイスの物理および論理インベントリを収集してデータベースに保存してください。参照先 [デバイスのインベントリの即時収集（同期）（175 ページ）](#)

### デバイスのインベントリの即時収集（同期）

同期操作は、デバイスの即時インベントリ収集を実行します。同期の実行時に、Cisco EPN Manager は選択されているデバイスの物理インベントリと論理インベントリを収集し、データベースを存在するすべての更新で同期します。デバイスの変更後に同期操作を実行しない場合は、日次インベントリ収集まで変更内容がデータベースに保存されません。



- (注) 同期操作は、更新操作とは異なります。更新操作では、設定の変更内容が保存されますが、インベントリ収集は実行されません。同期の代わりに更新を使用する場合は、[データベースへのデバイス設定変更の保存（更新）（175 ページ）](#) を参照してください。



- (注) この同期操作は、同期されていないデバイス コンフィギュレーション ファイルを使用した作業とは異なります。同期されていないデバイスとは、スタートアップコンフィギュレーション ファイルが実行コンフィギュレーションファイルと異なるデバイスです。詳細については、[実行デバイス コンフィギュレーションとスタートアップ デバイス コンフィギュレーションの同期](#) を参照してください。



手動での同期を実行するには、次のいずれかの方法を使用します。

インベントリ収集対象：	次の手順を実行します。
単一デバイス	<ul style="list-style-type: none"> <li>• デバイスの [デバイス 360 (Device 360)] ビューで [アクション (Actions)] &gt; [今すぐ同期する (Sync Now)] を選択します。</li> <li>(注) デバイスでの同期操作のステータスを表示できます。詳細については、<a href="#">デバイス同期状態 (176 ページ)</a> を参照してください。</li> <li>• [ネットワークデバイス (Network Devices)] テーブルでデバイスのチェックボックスをオンにし、[同期 (Sync)] をクリックします。</li> </ul>
複数のデバイス	[ネットワーク デバイス (Network Devices)] テーブルでデバイスを選択し (デバイスのチェックボックスをオンにし)、[同期 (Sync)] をクリックします。


## デバイス同期状態

[デバイスの同期状態 (Device Sync State)] : デバイスで実行された同期操作のステータスを示します。

表 16: デバイス同期状態

アイコン	デバイス同期状態	説明
	同期中	デバイスの同期を実行中です。
	完了	デバイスの同期が正常に完了しました。



	エラー/警告 (Error/Warning)	以下の一覧に示すエラーまたは警告 : <ul style="list-style-type: none"> <li>• 追加開始 (Add Initiated)</li> <li>• 収集の失敗 (Collection Failure)</li> <li>• 警告付き完了 (Completed with Warning)</li> <li>• 削除処理中 (Delete In Progress)</li> <li>• サービス中 (In Service)</li> <li>• サービスメンテナンス中 (In Service Maintenance)</li> <li>• ライセンスなし</li> <li>• 収集一部失敗 (Partial Collection Failure)</li> <li>• SNMP 接続失敗 (SNMP Connectivity Failed)</li> <li>• SNMP ユーザー認証失敗 (SNMP User Authentication Failed)</li> <li>• スイッチ ポート トレース (Switch Port Trace)</li> <li>• 誤った CLI クレデンシャル (Wrong CLI Credentials)</li> </ul>
---	---------------------------	---



(注) サービスメンテナンスフィルタは、最後のインベントリ収集ステータスには使用できません。

## Cisco NCS および Cisco ONS デバイスを管理するための Cisco Transport Controller の起動

Cisco Transport Controller (CTC) は、Cisco ONS および Cisco NCS デバイスのサブセットに使用されるソフトウェア インターフェイスです。CTC はコントロールカード上で Java アプリケーションとして実行されます。CTC を使用して、これらのデバイスをプロビジョニングおよび管理します。

CTC は Cisco EPN Manager から起動できます。選択した NE リリースに関わらず、最新の CTC リリースだけが起動されます。他の CTC リリースを使用する必要がある場合は、Web ブラウザから CTC を起動し、該当する CTC リリースを使用している NE に直接接続してください。

CTC を起動するには、次の手順に従います。

### Before you begin

CTCを起動するようにデバイスが正しく設定されていることを確認します。[デバイスをモデル化してモニターできるように設定する](#)を参照してください。

- 
- ステップ 1** 左側のサイドバーで、[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)] を選択します。
- ステップ 2** Cisco ONS または Cisco NCS デバイスの IP アドレスの横にある「i」アイコンをクリックし、デバイスの 360 度ビューを起動します。
- ステップ 3** デバイスの 360 度ビューで、[アクション (Actions)] > [CTC の起動 (Launch CTC)] の順に選択します。CTC ランチャアプリケーションがコンピュータにダウンロードされます。選択したデバイスタイプで CTC の起動がサポートされていない場合、このアクションは無効になります。
- ステップ 4** [CTC ランチャ (CTC Launcher)] ウィンドウで、次のいずれかの接続モードを選択します。
- [IP を使用 (Use IP)] : デバイスの IP アドレスを使用してデバイスへの接続が確立されます (デフォルト オプション)。
  - [TL1 トンネルを使用 (Use TL1 Tunnel)] : TL1 セッションを使用してデバイスへの接続が確立されます。TL1 セッションは、CTC から開始することも、TL1 端末を使用して開始することもできます。注 : サードパーティの OSI ベースの GNE の背後にあるデバイスには、このオプションを使用して接続してください。CTC ランチャにより、OSI ベースの GNE 経由で TCP トラフィックを転送するための TL1 トンネルが作成され、CTC でプロビジョニングが行われます。
- ステップ 5** CTC のバージョンを選択し、**Launch CTC** をクリックします。
- ステップ 6** CTC クレデンシャルを入力します。
-