



ネットワーク インターフェイスの設定

Cisco SD-WAN オーバーレイネットワークの設計では、インターフェイスは、VPN に関連付けられます。VPN に参加するインターフェイスは、その VPN で設定および有効化されます。各インターフェイスは、単一の VPN にのみ存在できます。

大まかに言うと、インターフェイスを動作可能にするには、インターフェイスの IP アドレスを設定し、動作可能 ([no shutdown]) としてマークする必要があります。実際には、インターフェイスごとに常に追加のパラメータを設定します。

Cisco IOS XE SD-WAN デバイスでは、最大 512 のインターフェイスを設定できます。この数には、物理インターフェイス、ループバックインターフェイス、およびサブインターフェイスが含まれます。



(注) Cisco vSmart コントローラ 間のロードバランシングの効率を最大化するには、ドメイン内の Cisco IOS XE SD-WAN デバイスにシステム IP アドレスを割り当てるときに連番を使用します。連番付与スキームの例は、172.16.1.1、172.16.1.2、172.16.1.3 などです。



(注) デバイスに構成されているネットワーク インターフェイスに一意の IP アドレスがあることを確認します。

- [VPN の設定 \(2 ページ\)](#)
- [WAN トランスポート VPN \(VPN 0\) でのインターフェイスの設定 \(7 ページ\)](#)
- [システムインターフェイスの設定 \(10 ページ\)](#)
- [コントロールプレーンの高可用性の設定 \(11 ページ\)](#)
- [その他のインターフェイスの設定 \(11 ページ\)](#)
- [インターフェイスプロパティの設定 \(21 ページ\)](#)
- [Cisco vManage を使用した DHCP サーバーの有効化 \(26 ページ\)](#)
- [PPPoE の設定 \(30 ページ\)](#)
- [PPPoE Over ATM の設定 \(35 ページ\)](#)
- [VRRP の設定 \(38 ページ\)](#)

- 動的インターフェイスの設定 (39 ページ)
- VPN イーサネット インターフェイスの設定 (42 ページ)
- VPN インターフェイスブリッジ (55 ページ)
- VPN インターフェイス DSL IPoE (62 ページ)
- VPN インターフェイス DSL PPPoA (74 ページ)
- VPN インターフェイス DSL PPPoE (84 ページ)
- VPN インターフェイス イーサネット PPPoE (97 ページ)
- Cisco VPN インターフェイス GRE (107 ページ)
- VPN インターフェイス IPsec (110 ページ)
- VPN インターフェイス マルチリンク (118 ページ)
- vManage を使用した VPN インターフェイス SVI の設定 (128 ページ)
- VPN インターフェイス T1/E1 (133 ページ)
- セルラーインターフェイス (144 ページ)

VPN の設定

VPN

Cisco SD-WAN ソフトウェアを実行しているすべての Cisco SD-WAN デバイスに VPN テンプレートを使用します。

Cisco vManage テンプレートを使用して VPN を設定するには、次の一般的なワークフローに従います。

1. VPN 機能テンプレートを作成して、VPN パラメータを設定します。VPN ごとに個別の VPN 機能テンプレートを作成します。たとえば、VPN 0 用に 1 つの機能テンプレート、VPN 1 用に 2 つ目、VPN 512 用に 3 つ目の機能テンプレートを作成します。

Cisco vManage ネットワーク管理システムおよび Cisco vSmart コントローラ の場合、VPN 0 および 512 のみを構成できます。VPN のデフォルト設定を変更する場合にのみ、これらの VPN のテンプレートを作成します。Cisco IOS XE SD-WAN デバイス の場合、これら 2 つの VPN のテンプレートと、サービス側のユーザーネットワークをセグメント化するための追加の VPN 機能テンプレートを作成できます。

- **VPN 0** : 設定された WAN トランスポート インターフェイスを介して制御トラフィックを伝送する **トランスポート VPN**。最初は、VPN 0 には管理インターフェイスを除くデバイスのすべてのインターフェイスが含まれていて、すべてのインターフェイスが無効になっています。
- **VPN 512** : オーバーレイネットワーク内の Cisco IOS XE SD-WAN デバイス 間でアウトオブバンド ネットワーク管理トラフィックを伝送する **管理 VPN**。管理トラフィックに使用されるインターフェイスは、VPN 512 に存在します。デフォルトでは、VPN 512 はすべての Cisco IOS XE SD-WAN デバイス で設定され、有効になっています。コントローラデバイスの場合、デフォルトでは、VPN 512 は設定されていません。

- **VPN 1 ~ 511、513 ~ 65530** : Cisco IOS XE SD-WAN デバイスのサービス側データトラフィック用のサービス VPN。

2. インターフェイス機能テンプレートを作成して、VPNのインターフェイスを設定します。

VPN テンプレートの作成



- (注) Cisco IOS XE SD-WAN デバイスは、セグメンテーションとネットワーク分離に VRF を使用します。ただし、Cisco vManage を介した Cisco IOS XE SD-WAN デバイスのセグメンテーションを設定する場合は、引き続き次の手順が適用されます。設定が完了すると、システムは VPN を Cisco IOS XE SD-WAN デバイスの VRF に自動的に変換します。



- (注) VPN テンプレートを使用して静的ルートを設定できます。

ステップ 1 Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。

ステップ 2 **[Device][Templates]** をクリックし、**[Create Template]** をクリックします。

- (注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Device Templates]** は **[Device]** と呼ばれます。

ステップ 3 **[Create Template]** ドロップダウンリストから、**[From Feature Template]** を選択します。

ステップ 4 **[Device Model]** ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。

ステップ 5 VPN 0 または VPN 512 のテンプレートを作成するには、次の手順を実行します。

1. **[Transport & Management VPN]** をクリックするか、**[Transport & Management VPN]** セクションまでスクロールします。
2. **[VPN 0]** または **[VPN 512]** ドロップダウンリストから、**[Create Template]** をクリックします。**[VPN]** テンプレートフォームが表示されます。

このフォームには、テンプレートに名前を付けるためのフィールドと、VPN パラメータを定義するためのフィールドが含まれています。

ステップ 6 VPN 1 ~ 511、および 513 ~ 65527 のテンプレートを作成するには :

1. **[Service VPN]** をクリックするか、**[Service VPN]** までスクロールします。
2. **[Service VPN]** ドロップダウンリストをクリックします。
3. **[VPN]** ドロップダウンリストから、**[Create Template]** をクリックします。**[VPN]** テンプレートフォームが表示されます。


パラメータ値の範囲を変更する

このフォームには、テンプレートに名前を付けるためのフィールドと、VPN パラメータを定義するためのフィールドが含まれています。


ステップ 7 [Template Name] に、テンプレートの名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。

ステップ 8 [Template Description] に、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。

パラメータ値の範囲を変更する

初めて機能テンプレートを開くと、デフォルト値を持つパラメータごとに、その範囲が [Default] () に設定され、デフォルト設定またはデフォルト値が表示されます。デフォルト値を変更するか、値を入力するには、[Scope] ドロップダウンリストをクリックし、次のいずれかを選択します。

パラメータ名	説明
 [Device Specific]	<p>デバイス固有の値がパラメータに使用されます。デバイス固有のパラメータの場合、機能テンプレートに値を入力できません。デバイスをデバイステンプレートに添付するときに、値を入力します。</p> <p>[Device Specific] をクリックすると、[Enter Key] ボックスが表示されます。このボックスには、作成する CSV ファイル内のパラメータを識別する一意の文字列であるキーが表示されます。このファイルは、キーごとに 1 つの列を含む Excel スプレッドシートです。ヘッダー行にはキー名（行ごとに 1 つのキー）が含まれます。その後の各行は、デバイスに対応し、そのデバイスのキーの値を定義します。デバイスをデバイステンプレートに添付するときに、この CSV ファイルをアップロードします。詳細については、「Create a Template Variables Spreadsheet」を参照してください</p> <p>デフォルトのキーを変更するには、新しい文字列を入力し、[Enter Key] ボックスの外にカーソルを移動します。</p> <p>デバイス固有のパラメータの例としては、システム IP アドレス、ホスト名、GPS ロケーション、サイト ID などがあります。</p>

パラメータ名	説明
 グローバル	パラメータの値を入力し、その値をすべてのデバイスに適用します。 デバイスのグループにグローバルに適用できるパラメータの例としては、DNS サーバー、Syslog サーバー、インターフェイス MTU などがあります。

テンプレートを作成して名前を付けたら、次の値を入力します。アスタリスクの付いたパラメータは必須です。

基本的な VPN パラメータの設定

基本的な VPN パラメータを設定するには、[Basic Configuration] を選択してから、次のパラメータを設定します。VPN を設定する場合、アスタリスクの付いたパラメータは必須です。

パラメータ名	説明
VPN	VPN の数値識別子を入力します。 Cisco IOS XE SD-WAN デバイスの範囲：0 ～ 65527 Cisco vSmart コントローラ および Cisco vManage のデバイスの値：0、512
名前	VPN の名前を入力します。 (注) Cisco IOS XE SD-WAN デバイスには、VPN のデバイス固有の名前を入力できません。
Enhance ECMP keying	[On] をクリックして、ECMP ハッシュキーとして、送信元と宛先の IP アドレスの組み合わせに加えて、レイヤ 4 の送信元ポートと宛先ポートの ECMP ハッシュキーでの使用を有効にします。 ECMP キーイングはデフォルトで [Off] です。



- (注) ルータでトランスポート VPN の設定を完了するには、VPN0 で少なくとも 1 つのインターフェイスを設定する必要があります。

機能テンプレートを保存するには、[Save] をクリックします。

CLI を使用する負荷分散アルゴリズムの設定



- (注) Cisco IOS XE リリース 17.8.1a 以降、IPv4 および IPv6 SD-WAN および非 SD-WAN トラフィックの **src-only** 負荷分散アルゴリズムを設定するには、CLI テンプレートが必要です。負荷分散アルゴリズム CLI の詳細については、「[IP Commands](#)」リストを参照してください。

これは、非 SD-WAN IPv4 および IPv6 トラフィックの Cisco Express Forwarding 負荷分散アルゴリズムを選択するための CLI 設定を提供します。ECMP キーイングを有効にして、IPv4 と IPv6 の両方の設定を送信できます。

```
Device# config-transaction
Device(config)# ip cef load-sharing algorithm {universal [id] | include-ports [ source
[id] | destination [id]] |
src-only [id]}
```

```
Device# config-transaction
Device(config)# ipv6 cef load-sharing algorithm {universal [id] | include-ports [ source
[id] | destination [id]] |
src-only [id]}
```

これは、SD-WAN IPv4 および IPv6 トラフィックのインターフェイスで負荷分散アルゴリズムを有効にするための CLI 設定を提供します。ECMP キーイングを有効にして、IPv4 と IPv6 の両方の設定を送信できます。

```
Device# config-transaction
Device(config)# sdwan
Device(config-sdwan)# ip load-sharing algorithm {ip-and-ports | src-dst-ip | src-ip-only}
```

```
Device# config-transaction
Device(config)# sdwan
Device(config-sdwan)# ipv6 load-sharing algorithm {ip-and-ports | src-dst-ip | src-ip-only}
```

ドメインネームシステム (DNS) および静的ホスト名マッピングの設定

DNS アドレスと静的ホスト名マッピングを設定するには、[DNS] をクリックして、次のパラメータを設定します。

パラメータ名	オプション	Description
Primary DNS Address	[IPv4] または [IPv6] をクリックし、この VPN のプライマリ DNS サーバーの IP アドレスを入力します。	

パラメータ名	オプション	Description
New DNS Address	[New DNS Address]	[New DNS Address] をクリックし、この VPN のセカンダリ DNS サーバーの IP アドレスを入力します。このフィールドは、プライマリ DNS アドレスを指定した場合にのみ表示されます。
	[Mark as Optional Row]	この設定をデバイス固有としてマークするには、[Mark as Optional Row] チェックボックスをオンにします。デバイスにこの設定を含めるには、デバイステンプレートをデバイスに添付するときに要求された変数値を入力するか、テンプレート変数スプレッドシートを作成して変数を適用します。
	Hostname	DNS サーバーのホスト名を入力します。名前には最大 128 文字を使用できます。
	List of IP Addresses	ホスト名に関連付ける IP アドレスを 8 つまで入力します。エントリをカンマで区切ります。
DNS サーバー設定を保存するには、[Add] をクリックします。		

機能テンプレートを保存するには、[Save] をクリックします。

ホスト名の IP アドレスへのマッピング

```
! IP DNS-based host name-to-address translation is enabled
ip domain lookup
! Specifies hosts 192.168.1.111 and 192.168.1.2 as name servers
ip name-server 192.168.1.111 192.168.1.2
! Defines cisco.com as the default domain name the device uses to complete
! Set the name for unqualified host names
ip domain name cisco.com
```

WAN トランスポート VPN (VPN 0) でのインターフェイスの設定

このトピックでは、WAN トランスポートとサービス側のネットワーク インターフェイスの一般的なプロパティを設定する方法について説明します。セルラーインターフェイス、DHCP、PPPoE、VRRP、WLAN インターフェイスなど、特定のインターフェイスタイプとプロパティを設定する方法に関する情報を提供します。

VPN 0 は WAN トランスポート VPN です。この VPN は、オーバーレイネットワークで OMP セッションを介して伝送されるすべてのコントロールプレーントラフィックを処理します。Cisco IOS XE SD-WAN デバイスがオーバーレイネットワークに参加するには、少なくとも 1 つのインターフェイスが VPN 0 で設定されている必要があります。少なくとも 1 つのインターフェイスが WAN トランスポートネットワーク（インターネット、MPLS、メトロイーサネットネットワークなど）に接続されている必要があります。この WAN トランスポートインターフェイスは、トンネルインターフェイスと呼ばれます。少なくとも、このインターフェ

イスでは、IPアドレスを設定し、インターフェイスを有効にして、トンネルインターフェイスとして設定する必要があります。

Cisco vSmart コントローラ または Cisco vManage NMS でトンネルインターフェイスを設定するには、VPN 0 にインターフェイスを作成した後、IP アドレスを割り当てるか、DHCP から IP アドレスを受信するようにインターフェイスを設定して、トンネルインターフェイスとしてマークします。IPアドレスは、IPv4またはIPv6アドレスのどちらにすることもできます。デュアルスタックを有効にするには、両方のアドレスタイプを設定します。オプションで、カラーをトンネルに関連付けることができます。



(注) IPv6 アドレスは、トランスポート インターフェイスでのみ、つまり VPN 0 でのみ設定できません。

Cisco IOS XE SD-WAN デバイスのトンネルインターフェイスには、IPアドレス、カラー、およびカプセル化タイプを設定する必要があります。IPアドレスは、IPv4またはIPv6アドレスのどちらにすることもできます。Cisco IOS XE リリース 17.3.2 より前のリリースでデュアルスタックを有効にするには、両方のアドレスタイプを設定します。

Cisco IOS XE リリース 17.3.2 の Cisco IOS XE SD-WAN デバイス でデュアルスタックを使用するには、すべてのコントローラに IPv4 アドレスと IPv6 アドレスの両方を設定します。さらに、IPv4 および IPv6 アドレスタイプを解決するように Cisco vBond オーケストレーション インターフェイス用のドメインネームシステム (DNS) を設定します。これにより、コントローラは、どちらの IP アドレスタイプを介しても Cisco vBond オーケストレーション に到達できます。



(注) Cisco vManage リリース 20.6.1 以降では、デュアルスタックを設定した際に、IPv4 アドレスや完全修飾ドメイン名 (FQDN) は使用できず、IPv6 アドレスは使用できる場合は、IPv6 アドレスを使用して Cisco vBond オーケストレーション に接続します。

トンネルインターフェイスの場合、固定 IPv4 または IPv6 アドレスを設定するか、DHCP サーバーからアドレスを受信するようにインターフェイスを設定できます。デュアルスタックを有効にするには、トンネルインターフェイスで IPv4 アドレスと IPv6 アドレスの両方を設定します。

Cisco IOS XE リリース 17.3.2 以降、Cisco IOS XE SD-WAN デバイス では同じ TLOC または インターフェイスでのデュアルスタックはサポートされません。TLOC または インターフェイスにプロビジョニングできるアドレスタイプは 1 つだけです。2 つ目のアドレスタイプを使用する場合、それをプロビジョニングできる 2 つ目の TLOC または インターフェイスが必要です。

Cisco vSmart コントローラ および Cisco vSmart コントローラ NMS では、*interface-name* は **eth number** または **loopback number** のいずれかになります。Cisco vSmart コントローラ と Cisco vSmart コントローラ NMS はオーバーレイネットワークのコントロールプレーンにのみ参加するため、これらのデバイスで設定できる VPN は VPN 0 と VPN 512 です。したがって、すべてのインターフェイスはこれらの VPN にのみ存在します。

インターフェイスを有効にするには、**no shutdown** コマンドを使用します。

カラーは、トランスポートトンネルを識別する Cisco SD-WAN ソフトウェア構造です。これは、**3g**、**biz-internet**、**blue**、**bronze**、**custom1**、**custom2**、**custom3**、**default**、**gold**、**green**、**lte**、**metro-ethernet**、**mpls**、**private1** ~ **private6**、**public-internet**、**red**、および **silver** のいずれかです。**metro-ethernet**、**mpls**、および **private1** ~ **private6** の各カラーは、プライベートアドレスを使用してプライベートネットワークのリモート側 Cisco IOS XE SD-WAN デバイスに接続するため、プライベートカラーと呼ばれます。ローカルとリモートの Cisco IOS XE SD-WAN デバイス 間に NAT デバイスがない場合は、パブリックネットワークでこれらのカラーを使用できます。

ローカル TLOC が BFD セッションを確立できるリモート TLOC を制限するには、[restrict] オプションで TLOC をマークします。TLOC が制限付きとしてマークされている場合、ローカルルータの TLOC は、リモート TLOC が同じカラーである場合にのみ、リモート TLOC とのトンネル接続を確立します。

Cisco vSmart コントローラ または Cisco vSmart コントローラ NMS では、1 つのトンネルインターフェイスを設定できます。Cisco IOS XE SD-WAN デバイス では、最大 8 つのトンネルインターフェイスを設定できます。

Cisco IOS XE SD-WAN デバイス では、トンネルのカプセル化を設定する必要があります。カプセル化は、IPsec または GRE のいずれかです。IPsec カプセル化の場合、デフォルトの MTU は 1442 バイトであり、GRE の場合は 1468 バイトです。これらの値は、すべての TLOC でデフォルトで有効になっている BFD パス MTU ディスカバリーに必要なオーバーヘッドに基づいて決定されます。(詳細については、「Configuring Control Plane and Data Plane High Availability Parameters」を参照してください。) 同じ **tunnel-interface** コマンドの下に 2 つの **encapsulation** コマンドを含めることにより、IPsec と GRE の両方のカプセル化を設定できます。リモート Cisco IOS XE SD-WAN デバイス では、2 つのルータがデータトラフィックを交換できるように、同じトンネルカプセル化タイプを設定する必要があります。IPsec トンネルから送信されたデータは IPsec トンネルでのみ受信でき、GRE トンネルで送信されたデータは GRE トンネルでのみ受信できます。Cisco SD-WAN ソフトウェアは、宛先 Cisco IOS XE SD-WAN デバイスの正しいトンネルを自動的に選択します。

トンネルインターフェイスでは、DTLS、TLS、および (Cisco IOS XE SD-WAN デバイスの場合) IPsec トラフィックのみがトンネルを通過できます。明示的なポリシーまたはアクセスリストを作成せずに追加のトラフィックが通過できるようにするには、サービスごとに 1 つの **allow-service** コマンドを追加することで有効にできます。**no allow-service** コマンドを追加することで、サービスを明示的に禁止することもできます。サービスは物理インターフェイスにのみ影響することに注意してください。トンネルインターフェイスで次のサービスを許可または禁止できます。

Service	Cisco vSmart コントローラ	Cisco vSmart コントローラ
all (個々のサービスを許可または禁止するコマンドをオーバーライドします)	X	X
bgp	—	—

Service	Cisco vSmart コントローラ	Cisco vSmart コントローラ
dhcp (DHCPv4 および DHCPv6 の場合)	—	—
dns	—	—
https	×	—
icmp	X	X
netconf	×	—
ntp	—	—
ospf	—	—
sshd	X	X
stun	X	X

allow-service stun コマンドを使用すると、Cisco IOS XE SD-WAN デバイスが汎用 STUN サーバーへの要求を生成することを許可または禁止して、このデバイスが NAT の背後にあるかどうかを判別し、NAT の背後にある場合は、NAT の種類とデバイスのパブリック IP アドレスとパブリックポート番号を判別できます。NAT の背後にある Cisco IOS XE SD-WAN デバイスでは、そのパブリック IP アドレスとポート番号を Cisco vBond オーケストレーション から検出するトンネルインターフェイスを設定することもできます。

この設定では、Cisco IOS XE SD-WAN デバイスは Cisco vBond オーケストレーション を STUN サーバーとして使用するため、ルータはそのパブリック IP アドレスとパブリックポート番号を判別できます。（この設定では、ルータは自身の前にある NAT の種類を学習できません。）オーバーレイネットワーク制御トラフィックは送信されず、Cisco vBond オーケストレーション に STUN サーバーとして設定されたトンネルインターフェイスを介してキーが交換されることもありません。ただし、BFD はトンネルで起動し、データトラフィックはトンネルで送信できます。Cisco vBond オーケストレーション を STUN サーバーとして使用するように設定されたトンネルインターフェイスを介して制御トラフィックは送信されないため、Cisco IOS XE SD-WAN デバイスで少なくとも1つの他のトンネルインターフェイスを設定して、Cisco vSmart コントローラ および Cisco vSmart コントローラ NMS と制御トラフィックを交換できるようにする必要があります。

allow-service コマンドで設定されたサービスと一致しないためにドロップされたすべてのパケットのヘッダーをログに記録できます。これらのログをセキュリティの目的で使用できます。たとえば、WAN インターフェイスに送信されるフローをモニタリングし、DDoS 攻撃の場合にブロックする IP アドレスを決定できます。

システムインターフェイスの設定

各 Cisco IOS XE SD-WAN デバイス に対し、`system system-ip` コマンドを使用してシステムインターフェイスを設定します。システムインターフェイスの IP アドレスは、Cisco IOS XE SD-WAN

デバイスを識別する永続的なアドレスです。これは通常のルータのルータ ID に似ていて、パケットの発信元のルータを識別するために使用されるアドレスです。

システムの IP アドレスを 10 進 4 部ドット表記の IPv4 アドレスとして指定します。アドレスだけを指定してください。プレフィックス長 (/32) は暗黙的です。

システム IP アドレスには、0.0.0.0/8、127.0.0.0/8、224.0.0.0/4、および 240.0.0.0/4 以降を除く任意の IPv4 アドレスを使用できます。オーバーレイネットワーク内の各デバイスには、一意のシステム IP アドレスが必要です。この同じアドレスを VPN 0 の別のインターフェイスに使用することはできません。

システムインターフェイスは、[system] という名前のループバック インターフェイスとして VPN 0 に配置されます。これは、インターフェイスに設定するループバックアドレスと同じではないことに注意してください。

システムインターフェイスに関する情報を表示するには、**show interface** コマンドを使用します。次に例を示します。

システム IP アドレスは、OMP TLOC の属性の 1 つとして使用されます。各 TLOC は、システム IP アドレス、色、およびカプセル化で構成される 3 つのタプルによって一意に識別されます。TLOC 情報を表示するには、**show omp tlocs** コマンドを使用します。

デバイス管理の目的で、ベストプラクティスとして、管理目的に適した VPN であるサービス側 VPN にあるループバック インターフェイスにも同じシステム IP アドレスを設定することをお勧めします。ループバック インターフェイスを使用する理由は、ルータが動作していて、オーバーレイネットワークが稼働しているときに常に到達できるためです。物理インターフェイスでシステム IP アドレスを設定する場合、ルータが到達可能であるためには、ルータとインターフェイスの両方が稼働する必要があります。データセンターから到達できるため、サービス側 VPN を使用します。サービス側 VPN は、VPN 0 (WAN トラnsポート VPN) および VPN 512 (管理 VPN) 以外の VPN であり、データトラフィックのルーティングに使用されます。

コントロールプレーンの高可用性の設定

可用性の高い Cisco SD-WAN ネットワークには、各ドメインに 2 つ以上の Cisco vSmart コントローラが含まれています。Cisco SD-WAN ドメインには、最大 8 つの Cisco vSmart コントローラを含めることができ、デフォルトでは、それぞれの Cisco IOS XE SD-WAN デバイスがそのうちの 2 つに接続します。この値は、トンネルごとに変更します。

その他のインターフェイスの設定

管理でのインターフェイスの構成 (VRF mgmt-intf)

すべての Cisco SD-WAN デバイスで、工場出荷時のデフォルト設定の一部として、デフォルトで VPN 512 が帯域外管理に使用されます。Cisco IOS XE SD-WAN デバイスでは、管理 VPN は VRF Mgmt-Intf に変換されます。

Cisco XE SD-WAN デバイスは、VPN の代わりに VRF を使用します。

デバイス# `show sdwan running-config | sec vrf definition Mgmt-intf`

```
vrf definition Mgmt-intf
  address-family ipv4
    exit-address-family
  !
  address-family ipv6
    exit-address-family
  !
=====
interface GigabitEthernet0
  no shutdown
  vrf forwarding Mgmt-intf
  negotiation auto
exit
=====
config-t
ip route vrf Mgmt-intf 10.0.0.1 10.0.0.1
```

設定された管理インターフェイスに関する情報を表示するには、`show interface` コマンドを使用します。次に例を示します。

```
デバイス# show interface gigabitEthernet0
GigabitEthernet0 is up, line protocol is up
  Hardware is RP management port, address is d478.9bfe.9f7f (bia d478.9bfe.9f7f)
  Internet address is 10.34.9.177/16
  MTU 1500 bytes, BW 1000000 Kbit/sec, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full Duplex, 1000Mbps, link type is auto, media type is RJ45
  output flow-control is unsupported, input flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:00, output 00:00:00, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 8000 bits/sec, 12 packets/sec
  5 minute output rate 1000 bits/sec, 2 packets/sec
    4839793 packets input, 415574814 bytes, 0 no buffer
    Received 3060073 broadcasts (0 IP multicasts)
    0 runs, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 watchdog, 0 multicast, 0 pause input
    82246 packets output, 41970224 bytes, 0 underruns
    Output 0 broadcasts (0 IP multicasts)
    0 output errors, 0 collisions, 0 interface resets
    0 unknown protocol drops
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier, 0 pause output
    0 output buffer failures, 0 output buffers swapped out
```



(注) VPN 512 はオーバーレイでアドバタイズされません。デバイスに対してローカルです。オーバーレイ経由で到達可能な管理 VPN が必要な場合は、512 以外の番号で VPN を作成します。

ループバック インターフェイスの設定

インターフェイス名形式 **loopback string** を使用します。string には任意の英数字を使用でき、下線 (_) とハイフン (-) を含めることができます。文字列「loopback」を含むインターフェイス名の合計の長さは、最長 16 文字です (CLI でのインターフェイスの命名の柔軟性のため、インターフェイス **lo0** と **loopback0** は異なる文字列として解析され、互換性がないことに注意してください。CLI がインターフェイスをループバック インターフェイスとして認識するためには、その名前が完全な文字列 **loopback** で始まる必要があります)。

ループバック インターフェイスの特別な用途の 1 つは、MPLS やメトロイーサネットネットワークなどのプライベート WAN でのデータトラフィック交換を設定することです。プライベートネットワークの背後にあるルータがプライベート WAN を介して他のエッジルータと直接通信できるようにするには、実際の物理 WAN インターフェイスではなく、トンネルインターフェイスとして設定されているループバック インターフェイスにデータトラフィックを送信します。

ループバック インターフェイスの暗黙的な ACL

表 1: 機能の履歴

機能名	リリース情報	説明
ループバック インターフェイスの暗黙的な ACL	Cisco IOS XE リリース 17.6.1a Cisco vManage リリース 20.6.1	<p>この機能により、ループバック TLOC インターフェイスで暗黙的な ACL を有効にできます。</p> <p>ループバック TLOC インターフェイスに独自の暗黙的な ACL がある場合、そのインターフェイス宛てのトラフィックに ACL ルールが適用されます。ループバック TLOC インターフェイスで暗黙的な ACL を有効にすると、制限されたサービスのみが許可されるため、ネットワークセキュリティが強化されます。</p> <p>ループバック TLOC インターフェイスが Cisco IOS XE SD-WAN デバイスの物理インターフェイスにバインドされている場合、物理インターフェイスは物理 TLOC インターフェイスのように扱われます。</p>

ループバック インターフェイスの暗黙的な ACL に関する情報

ローカライズされたデータポリシーを使用して設定するアクセスリストは、明示的な ACL と呼ばれます。ルータ トンネルインターフェイスには、サービスとも呼ばれる暗黙的な ACL もあります。これらの一部はデフォルトでトンネルインターフェイスに存在し、無効にするまで有効になっています。設定によって、その他の暗黙的な ACL を有効にすることもできます。Cisco IOS XE SD-WAN デバイスでは、DHCP、ドメインネームシステム (DNS)、および ICMP サービスがデフォルトで有効になっています。BGP、Netconf、NTP、OSPF、SSHD、および STUN のサービスを有効にすることもできます。

サービスを許可するには、**allow-service** コマンドを使用して暗黙的な ACL を設定および変更します。サービスを禁止するには、**no allow-service** コマンドを使用します。暗黙的な ACL と明示的な ACL の両方が設定されている場合、明示的な ACL は暗黙的な ACL よりも優先されます。

Cisco IOS XE SD-WAN デバイス ループバック インターフェイスにトランスポートロケーション (TLOC) が設定されている場合、暗黙的な ACL ルールが宛先へのトラフィックに適用されます。ループバック インターフェイスの暗黙的な ACL は、バインドモードとアンバインドモードの両方で適用されます。バインドモードは、ループバック インターフェイスが Cisco IOS XE SD-WAN デバイスの物理インターフェイスにバインドされてデータを送信するモードです。アンバインドモードでは、ループバック インターフェイスはどの物理インターフェイスにもバインドされません。

物理 WAN インターフェイスにバインドされたループバック TLOC インターフェイス

ループバック インターフェイスが TLOC であり、物理 WAN インターフェイスにバインドされている場合、トラフィックの宛先に基づいて、対応する暗黙的な ACL ルールが適用されます。

- ループバック TLOC インターフェイス宛てのトラフィックが物理 WAN インターフェイスで受信された場合、ループバック TLOC インターフェイスで設定された暗黙的な ACL ルールが適用されます。
- トラフィックの宛先がループバック TLOC インターフェイスではない場合、物理 WAN インターフェイスが TLOC 用に設定されているかどうかに応じて、次のルールが適用されます。
 - 物理 WAN インターフェイスに TLOC が設定されていない場合、ルーティングの決定が適用されます。

TLOC が設定されていない物理インターフェイスにバインドされたループバック TLOC インターフェイスは、物理インターフェイス自体に TLOC が設定されているかのように扱われます。違いは、トラフィックの宛先がデバイスのその他のインターフェイスである場合、そのようなトラフィックはループバックバインドモードで許可されることです。ただし、物理 TLOC の暗黙的な ACL ルールの対象となります。



- (注) 物理インターフェイスに TLOC が設定されておらず、ループバック TLOC インターフェイスにバインドされている場合、**implicit-acl-on-bind-intf** コマンドを使用して、物理インターフェイスでの暗黙的な ACL 保護を有効にします。

ループバック TLOC インターフェイスが物理 WAN インターフェイスにバインドされている場合、転送パケットまたはパススルーパケットはドロップされます。これは、物理インターフェイスが TLOC として設定されている場合と同じ動作です。したがって、パケットを転送するには、バインドされた物理インターフェイスで明示的な ACL を設定する必要があります。

次のサンプルシナリオでパススルーパケットを許可するには、明示的な ACL が必要です。

- **オンプレミスデータセンターでホストされているコントローラにアクセスするブランチエッジルータ**：このシナリオでは、物理 WAN インターフェイスにバインドされたループバック インターフェイスで設定されているデータセンターハブを介して、ブランチエッジルータがコントローラにアクセスすると想定しています。
 - **データセンターのインターネット回線を介してクラウドでホストされているコントローラにアクセスするブランチルータ**：このシナリオでは、ブランチルータが MPLS ネットワークを使用してデータセンターエッジに接続されていると想定しています。このようなブランチルータは、物理 WAN インターフェイスにバインドされたループバック インターフェイスで設定されたデータセンターエッジルータを介して、クラウドでホストされているコントローラにアクセスします。
-
- 物理 WAN インターフェイスに TLOC が設定されている場合、物理 TLOC インターフェイスの暗黙的な ACL ルールが適用されます。どちらのシナリオでも、パススルートラフィックを許可するには、バインドされた物理 WAN インターフェイスに明示的な ACL が必要です。

物理 WAN インターフェイスにバインドされていないループバック TLOC インターフェイス

ループバック インターフェイスが TLOC であり、物理 WAN インターフェイスにバインドされていない場合、トラフィックの宛先に基づいて、次のように暗黙的な ACL ルールが適用されます。

- ループバック TLOC インターフェイス宛でのトラフィックが物理 WAN インターフェイスで受信された場合、ループバック TLOC の暗黙的な ACL ルールが適用されます。

- トラフィックの宛先がループバック TLOC インターフェイスではない場合、入力物理 WAN インターフェイスが TLOC 用に設定されているかどうかに応じて、次のルールが適用されます。
 - 物理 WAN インターフェイスが TLOC 用に設定されていない場合、ルーティングの決定が適用されます。
 - 物理 WAN インターフェイスが TLOC 用に設定されている場合、設定された暗黙的な ACL ルールが適用されます。

ループバック TLOC のバインドモードとアンバインドモードの違いは、バインドモードでは、バインドされた物理インターフェイスがそれ自体で TLOC として扱われるため、パススルートラフィックがドロップされることです。アンバインドモードでは、パススルートラフィックは許可されます。

バインドモードとアンバインドモードの使用例

バインド モード (Bind Mode)

Cisco IOS XE SD-WAN デバイスには、TLOC として設定され、物理インターフェイス GigabitEthernet1 にバインドされた Loopback1 および Loopback2 があります。このデバイスには、TLOC として設定されていない別のインターフェイスである Loopback3 もあります。

物理インターフェイス GigabitEthernet1 は、着信 VPN 0 の TLOC インターフェイスとして扱われます。

着信 VPN 0 トラフィックの物理インターフェイス GigabitEthernet1 で暗黙的な ACL 保護を有効にするには、**implicit-acl-on-bind-intf** コマンドを使用します。

この例では、次のようになります。

- トラフィックの宛先が Loopback1 である場合、Loopback1 の暗黙の ACL ルールが適用されます。
- トラフィックの宛先が Loopback2 である場合、Loopback2 の暗黙の ACL ルールが適用されます。
- トラフィックの宛先が GigabitEthernet1 の Loopback3 である場合、トラフィックは許可されます。
- トラフィックの宛先が GigabitEthernet1 を通過する別のデバイスである場合、そのトラフィックはドロップされます。

バインドされたインターフェイスである GigabitEthernet1 も TLOC として設定されている場合、Loopback3 へのトラフィックは、GigabitEthernet1 の暗黙的な ACL ルールに従います。

アンバインドモード

Cisco IOS XE SD-WAN デバイスには、TLOC として設定された Loopback1 があり、アンバインドモードになっています。Loopback2 は TLOC として設定されていません。このデバイスには、TLOC として設定されている GigabitEthernet1 インターフェイスと、TLOC として設定されていない GigabitEthernet4 インターフェイスもあります。

この例では、次のようになります。

- Loopback1 宛でのトラフィックが GigabitEthernet1 に到着すると、Loopback1 の暗黙的な ACL ルールが適用されます。トラフィックの宛先が GigabitEthernet1 の場合、GigabitEthernet1 の暗黙的な ACL ルールが適用されます。
- Loopback1 宛でのトラフィックが GigabitEthernet4 に到着すると、Loopback1 の暗黙的な ACL ルールが適用されます。トラフィックの宛先が GigabitEthernet4 の場合、トラフィックは許可されます。
- Loopback2 宛でのトラフィックが GigabitEthernet1 に到着すると、GigabitEthernet1 の暗黙的な ACL ルールが適用されます。トラフィックの宛先が GigabitEthernet1 を通過する別のデバイスである場合、そのトラフィックはドロップされます。

トラフィックの宛先が GigabitEthernet4 を通過する別のデバイスである場合、トラフィックは転送されます。

ループバック インターフェイスの暗黙的な ACL の利点

ループバック TLOC インターフェイスの暗黙的な ACL は、限定されたサービスのみを許可することにより、サービス妨害 (DoS) 攻撃から保護します。これによって、ネットワークのセキュリティが強化されます。

ループバック インターフェイスでの暗黙的な ACL の設定

物理 WAN インターフェイスの設定と同様に、機能テンプレートまたは CLI アドオンテンプレートを Cisco vManage で使用して、ループバック インターフェイスに暗黙的な ACL を設定できます。

機能テンプレートを使用してループバック インターフェイスに暗黙的な ACL を設定する方法については、「[Configure VPN Ethernet Interface](#)」を参照してください。

CLI アドオンテンプレートの詳細については、「[Create a CLI Add-On Feature Template](#)」を参照してください。

CLI を使用したループバック インターフェイスでの暗黙的な ACL の設定

デフォルトでは、DNS、DHCP、ICMP、および HTTPS サービスは許可され、他のサービスは拒否されます。

すべてのサービスを許可するには、**allow-service all** コマンドを使用します。

特定のサービスを許可するには、**allow-service service name** コマンドを使用します。

サービスを拒否するには、**no allow-service service name** コマンドを使用します。

例

次に、ループバック インターフェイスに設定された暗黙の ACL の例を示します。

```
sdwan interface Loopback100
 tunnel-interface
```

```

no allow-service bgp
allow-service dhcp
allow-service dns
allow-service icmp
no allow-service sshd
no allow-service netconf
no allow-service ntp
no allow-service ospf
no allow-service stun
allow-service https
exit

```

TLOC が設定されたバインドモードのループバック インターフェイスに設定された暗黙的な ACL の設定例

次の例は、TLOC が設定されたバインドモードのループバック インターフェイスに設定された暗黙的な ACL を示しています。

```

Device(config)# sdwan interface Loopback1
Device (config-interface-Loopback1)# tunnel-interface
Device (config-tunnel-interface)# encap ipsec
Device (config-tunnel-interface)# color 3g
Device (config-tunnel-interface)# bind GigabitEthernet1
Device (config-tunnel-interface)# implicit-acl-on-bind-intf
Device (config-tunnel-interface)# no allow-service bgp
Device (config-tunnel-interface)# allow-service dhcp
Device (config-tunnel-interface)# allow-service dns
Device (config-tunnel-interface)# allow-service icmp
Device (config-tunnel-interface)# no allow-service sshd
Device (config-tunnel-interface)# no allow-service netconf
Device (config-tunnel-interface)# no allow-service ntp
Device (config-tunnel-interface)# no allow-service ospf
Device (config-tunnel-interface)# no allow-service stun
Device (config-tunnel-interface)# allow-service https
Device (config-tunnel-interface)# no allow-service snmp
Device (config-tunnel-interface)# no allow-service bfd
Device (config-tunnel-interface)# exit

```

TLOC が設定されたアンバインドモードのループバック インターフェイスに設定された暗黙的な ACL の設定例

次の例は、TLOC が設定されたアンバインドモードのループバック インターフェイスに設定された暗黙的な ACL を示しています。

```

Device(config)# sdwan interface Loopback1
Device (config-interface-Loopback1)# tunnel-interface
Device (config-tunnel-interface)# encap ipsec
Device (config-tunnel-interface)# color 3g
Device (config-tunnel-interface)# no allow-service bgp
Device (config-tunnel-interface)# allow-service dhcp
Device (config-tunnel-interface)# allow-service dns
Device (config-tunnel-interface)# allow-service icmp
Device (config-tunnel-interface)# no allow-service sshd
Device (config-tunnel-interface)# no allow-service netconf
Device (config-tunnel-interface)# no allow-service ntp
Device (config-tunnel-interface)# no allow-service ospf
Device (config-tunnel-interface)# no allow-service stun
Device (config-tunnel-interface)# allow-service https
Device (config-tunnel-interface)# no allow-service snmp

```

```
Device (config-tunnel-interface)# no allow-service bfd
Device (config-tunnel-interface)# exit
```

ループバック インターフェイスの暗黙的な ACL のモニタリング

show platform hardware qfp active statistics drop コマンドを使用して、ループバック インターフェイスの暗黙的な ACL 設定を監視します。

例

次に、**show platform hardware qfp active statistics drop** コマンドの出力例を示します。

```
Device# show platform hardware qfp active statistics drop
Last clearing of QFP drops statistics : never
```

```
-----
Global Drop Stats                Packets                Octets
-----
```

Global Drop Stats	Packets	Octets
Disabled	4	266
Ipv4EgressIntfEnforce	15	10968
Ipv6NoRoute	6	336
Nat64v6tov4	6	480
SVIInputInvalidMac	244	15886
SdwanImplicitAclDrop	160	27163
UnconfiguredIpv4Fia	942525	58524580
UnconfiguredIpv6Fia	77521	9587636

サブインターフェイスの設定

IP MTU 値を指定しないサブインターフェイスを作成すると、そのサブインターフェイスは親インターフェイスから IP MTU 値を継承します。サブインターフェイスに異なる IP MTU 値を設定する場合は、サブインターフェイスの設定で **ip mtu** コマンドを使用して、サブインターフェイスの IP MTU を設定します。

次に例を示します。

```
interface GigabitEthernet0/0/0
  mtu 1504
  no ip address
  !
interface GigabitEthernet0/0/0.9
  encapsulation dot1Q 9
  no shutdown
  ip address 192.168.9.32 255.255.255.0
  !
```

```
interface Tunnel9
  no shutdown
  ip unnumbered GigabitEthernet0/0/0.9
  no ip redirects
  ipv6 unnumbered GigabitEthernet0/0/0.9
  no ipv6 redirects
  tunnel source GigabitEthernet0/0/0.9
  tunnel mode sdwan
!
sdwan
interface GigabitEthernet0/0/0.9
  tunnel-interface
  encapsulation ipsec
  color private1
!
!
```

インターフェイスプロパティの設定

インターフェイス速度の設定

Cisco IOS XE SD-WAN デバイスが起動すると、Cisco SD-WAN ソフトウェアはルータに存在する SFP を自動検出し、それに応じてインターフェイス速度を設定します。次に、ソフトウェアは、接続のリモートエンドにあるデバイスとインターフェイス速度をネゴシエートして、インターフェイスの実際の速度を確立します。ルータに存在するハードウェアを表示するには、**show hardware inventory** コマンドを使用します。

各インターフェイスの実際の速度を表示するには、**show interface** コマンドを使用します。ここで、WAN クラウドに接続するインターフェイス [ge0/0] は 1000 Mbps (1Gbps、上記の出力で強調表示されている 1GE PIM) で実行されており、ローカルサイトのデバイスに接続するインターフェイス [ge0/1] は、100 Mbps の速度をネゴシエートしました。

システム IP アドレスやループバック インターフェイスなどの非物理インターフェイスの場合、インターフェイス速度はデフォルトで 10 Mbps に設定されます。

インターフェイス上の 2 つのデバイスによってネゴシエートされた速度を無効にするには、自動ネゴシエーションを無効にして、目的の速度を設定します。

Cisco vSmart コントローラ および Cisco vManage システムの場合、初期インターフェイス速度は 1000 Mbps であり、動作速度はインターフェイスのリモートエンドにあるデバイスとネゴシエートされます。コントローラ インターフェイスの速度は、仮想化プラットフォーム、使用される NIC、およびソフトウェアに存在するドライバによって異なる場合があります。

インターフェイス MTU の設定

デフォルトでは、すべてのインターフェイスの MTU は 1500 バイトです。これはインターフェイスで変更できます。

Cisco IOS XE リリース 17.4.1a より前のリリースでは、MTU の範囲は 576 ~ 2000 バイトです。

Cisco IOS XE リリース 17.4.1a 以降のリリースでは、MTU の範囲は 1 GE インターフェイスで 576 ～ 9216 バイトです。この MTU 範囲は、Cisco IOS XE リリース 17.5.1a 以降の 10 GE および 100 GE インターフェイスでもサポートされています。

インターフェイスの MTU を表示するには、**show interface** コマンドを入力します。

Cisco vBond オーケストレーション、Cisco vManage、および Cisco vSmart コントローラデバイスでは、ICMP を使用して Path MTU (PMTU) ディスカバリを実行するようにインターフェイスを設定できます。PMTU ディスカバリが有効になっている場合、デバイスは、パケットフラグメンテーションを排除または最小限に抑えるために、インターフェイスでサポートされる最大 MTU サイズを自動的にネゴシエートします。

Cisco IOS XE SD-WAN デバイス デバイスの Cisco SD-WAN BFD ソフトウェアは、各トランスポート接続（つまり、各 TLOC または色）で PMTU ディスカバリを自動的に実行します。BFD PMTU ディスカバリはデフォルトで有効になっていて、無効にせずを使用することをお勧めします。PMTU ディスカバリを実行するように BFD を明示的に設定するには、**bfd color pmtu-discovery** コンフィギュレーションコマンドを使用します。ただし、代わりに ICMP を使用して PMTU ディスカバリを実行することも選択できます。vEdge クラウドルータ

BFD はデータプレーンプロトコルであるため、Cisco vBond オーケストレーション、Cisco vManage、および Cisco vSmart コントローラデバイスでは実行されません。

TCP MSS と [Clear Dont Fragment] の設定

表 2: 機能の履歴

機能名	リリース情報	説明
TCP MSS の設定	Cisco IOS XE リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能により、Cisco SD-WAN トンネルインターフェイスの両方向で Cisco IOS XE SD-WAN デバイスの TCP MSS 調整サポートが追加されます。
[Clear Dont Fragment] オプションの設定	Cisco IOS XE リリース 17.5.1a Cisco vManage リリース 20.5.1	この機能は、Cisco SD-WAN トンネルで送信されるパケットの IPv4 パケットヘッダーの Don't Fragment ビットをクリアするオプションを提供します。[Don't Fragment] 設定をクリアすると、インターフェイス MTU より大きいパケットは送信前にフラグメント化されます。

TCP 最大セグメントサイズ (MSS) は、TCP ヘッダーまたは IP ヘッダーをカウントせずに、通信デバイスが単一の TCP セグメントで受信できるデータの最大量をバイト単位で指定する

パラメータです。MSS は、TCP ハンドシェイク中の TCP SYN パケットで最初に TCP MSS として指定されます。MSS 値が小さいと、IP フラグメンテーションが減少するかまたは排除され、オーバーヘッドが大きくなります。

デバイスを通る TCP SYN パケットの MSS を設定できます。デフォルトでは、MSS は、TCP SYN パケットが決してフラグメント化されないように、インターフェイスまたはトンネルの最大伝送ユニット (MTU) に基づいて動的に調整されます。インターフェイスを介して送信されるデータの場合、MSS は、インターフェイス MTU、IP ヘッダー長、および最大 TCP ヘッダー長を加算して計算されます。

制限事項

- TCP MSS 値は、Cisco SD-WAN トンネルインターフェイスに対してのみ調整できます。



(注) Cisco IOS XE リリース 17.9.1a および Cisco vManage リリース 20.9.1 以降、サービス VPN の場合、またはネットワークアドレス変換 (NAT) ダイレクトインターネットアクセス (DIA) を使用する場合に TCP MSS 値を調整できます。TCP MSS 値を調整すると、TCP セッションのドロップを防ぐことができます。

NAT DIA の詳細については、『[Cisco SD-WAN NAT Configuration Guide, Cisco IOS XE リリース 17.x](#)』を参照してください。

- [Clear Dont Fragment] オプションは、Cisco SD-WAN トンネルインターフェイスでのみ使用できます。

TCP MSS と [Clear Dont Fragment] の設定

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. **[Feature Templates]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Feature Templates]** のタイトルは **[Feature]** です。

3. 新しい CLI アドオン機能テンプレートを作成するか、次のいずれかのテンプレートを編集します。次の機能テンプレートのいずれかを使用して、TCP MSS を構成し、Dont Fragment をクリアできます。

- [VPN Ethernet インターフェイス](#)
- [VPN インターフェイス DSL IPoE](#)
- [VPN インターフェイス DSL PpPoA](#)
- [VPN インターフェイス DSL PPPoE](#)

- [VPN インターフェイス マルチリンク](#)
- [VPN インターフェイス T1/E1](#)
- [セルラーインターフェイス](#)

新しい CLI アドオン機能テンプレートの作成の詳細については、「[Create a CLI Add-on Feature Templates](#)」を参照してください。

4. [Tunnel] をクリックします。
5. TCP MSS を設定するには、[Tunnel TCP MSS] で、Cisco IOS XE SD-WAN デバイス を通過する TCP SYN パケットの MSS を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ~ 1460 バイト、デフォルト：なし

TCP MSS は、ルータを通過する最初の TCP ヘッダーを含むすべてのパケットに影響します。設定すると、TCP MSS は、スリーウェイハンドシェイクで交換される MSS に対して検査されます。構成された設定がヘッダーの MSS よりも低い場合、ヘッダーの MSS は低くなります。MSS ヘッダーの値がすでに TCP MSS よりも低い場合は、変更されずに通過します。トンネルの最後にあるホストは、2つのホストの低い方の設定を使用します。TCP MSS を設定する場合は、最小パス MTU より 40 バイト小さく設定する必要があります。

6. [Clear-Dont-Fragment] オプションをクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Dont Fragment ビットをクリアします。Dont Fragment ビットがクリアされると、そのインターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。



-
- (注) フラグメンテーションが必要で、Dont Fragment ビットが設定されている場合に、[Clear-Dont-Fragment] は Dont Fragment ビットをクリアします。フラグメンテーションを必要としないパケットの場合、Dont Fragment ビットは影響を受けません。
-

7. [Save] または [Update] をクリックします。

CLI を使用した TCP MSS の設定

次のコマンドを使用して、CLI で TCP MSS を構成します。

```
Device(config)#interface Tunnel 1
Device(config-if)#ip unnumbered GigabitEthernet1
Device(config-if)#ip tcp adjust-mss 1460
```

TCP MSS 構成の確認

次に、`show platform hardware qfp active feature sdwan datapath session summary` コマンドのサンプル出力を示します。

```
Device#show platform hardware qfp active feature sdwan datapath session summary
Src IP          Dst IP          Src Port Dst Port  Encap  Uidb      Bfd Discrim PMTU
```



```

-----
10.1.15.25      10.1.14.14      12347   12346   IPSEC   65526   10007   1446
10.1.15.25      10.0.5.21       12347   12357   IPSEC   65526   10009   1446
10.1.15.25      10.0.5.11       12347   12347   IPSEC   65526   10008   1446
10.1.15.25      10.1.16.16      12347   12366   IPSEC   65526   10006   1446

```

CLI での [Clear Dont Fragment] の設定

次のコマンドを使用して、CLI を使用して [Clear Dont Fragment] オプションを設定します。

```

Device(config)#interface Tunnel 1
Device(config-if)#ip unnumbered GigabitEthernet1
Device(config-if)#ip clear-dont-fragment

```

CLI での Dont Fragment 設定の確認

次に、[Clear-dont-fragment] が有効かどうかを確認する **show platform software interface rp active name Tunnell** コマンドの出力例を示します。

```

Device# show platform software interface rp active name Tunnell | include dont
IP Clear-dont-fragment: TRUE

```

次に、[Clear-dont-fragment] が有効な場合の実行コンフィギュレーションを表示する **show running-config interface Tunnell** コマンドの出力例を示します。

```

Device# show running-config interface Tunnell
Building configuration...

Current configuration : 132 bytes
!
interface Tunnell
ip unnumbered GigabitEthernet1
ip clear-dont-fragment
tunnel source GigabitEthernet1
tunnel mode sdwan
end

```

トランスポート回線の帯域幅のモニタリング

トランスポート回線の帯域幅使用量をモニタリングして、帯域幅使用量の傾向を判断できます。帯域幅使用量が最大値に近づき始めた場合、通知を送信するようにソフトウェアを設定できます。通知は、Cisco vManage NMS、SNMP トラップ、および syslog メッセージに送信される Netconf 通知として送信されます。回線のキャパシティプランを行うときや、帯域幅使用量に関する傾向情報を収集するときなど、帯域幅のモニタリングのためにこの機能を有効にすることができます。また、この機能を有効にして、帯域幅使用量に関するアラートを受信することもできます。たとえば、トランスポートインターフェイスがトラフィックで飽和状態になって顧客のトラフィックに影響を与える時期を判断する必要がある場合や、顧客が LTE トランスポートのケースのように従量課金プランを利用している場合などです。

インターフェイス帯域幅をモニタリングするには、トランスポート回線で送受信されるトラフィックの最大帯域幅を設定します。最大帯域幅は、通常、回線プロバイダーとネゴシエート

された帯域幅です。帯域幅使用量が受信または送信トラフィックの設定値の85%を超えると、SNMPトラップの形式で通知が生成されます。具体的には、インターフェイストラフィックは10秒ごとにサンプリングされます。受信または送信された帯域幅が、連続する5分間にサンプリングされた間隔の85%で設定値の85%を超えると、SNMPトラップが生成されます。最初のトラップが生成された後、サンプリングは同じ頻度で続行されますが、通知は1時間に1回に制限されます。次の1時間に10秒のサンプリング間隔の85%で帯域幅が値の85%を超えると、2つ目（およびそれ以降）のトラップが送信されます。1時間後にもう1つのトラップが送信されない場合、通知間隔は5分に戻ります。

Cisco IOS XE SD-WAN デバイスおよび Cisco vManage NMS でトランスポート回線の帯域幅をモニタリングできます。

物理インターフェイスで受信したトラフィックの帯域幅が特定の帯域幅の85%を超えたときに通知を生成するには、ダウンストリーム帯域幅を設定します。

物理インターフェイスで送信されるトラフィックの帯域幅が特定の帯域幅の85%を超えたときに通知を生成するには、アップストリーム帯域幅を設定します。

どちらの設定コマンドでも、帯域幅は1～2147483647 ($2^{32}/2$) - 1 kbps の範囲で指定できます。

設定された帯域幅を表示するには、**show interface detail** コマンドの出力で、**bandwidth-downstream** フィールドと **bandwidth-upstream** フィールドを確認します。このコマンドの **rx-kbps** および **tx-kbps** フィールドには、インターフェイスの現在の帯域幅使用量が表示されます。

Cisco vManage を使用した DHCP サーバーの有効化

表 3: 機能の履歴

機能名	リリース情報	機能説明
DHCP オプションのサポート	Cisco IOS XE SD-WAN リリース 16.12.1b	この機能により、DHCP サーバーオプション 43 および 191 は、クライアントとサーバーの交換でベンダー固有の情報を設定できます。

すべての Cisco SD-WAN に DHCP サーバーテンプレートを使用します。

Cisco SD-WAN デバイスインターフェイスで DHCP サーバー機能を有効にして、サービス側ネットワーク内のホストに IP アドレスを割り当てることができるようにします。

Cisco vManage テンプレートを使用して DHCP サーバーとして機能するように Cisco SD-WAN デバイスを設定するには、次の手順を実行します。

1. このトピックの説明に従って、DHCPサーバー機能テンプレートを作成し、DHCPサーバーパラメータを設定します。

- VPN-Interface-Ethernet および VPN-Interface-PPP-Ethernet のヘルプトピックの説明に従って、1 つ以上のインターフェイス機能テンプレートを作成します。
- VPN 機能テンプレートを作成して、VPN パラメータを設定します。VPN のヘルプトピックを参照してください。

Cisco IOS XE SD-WAN デバイスインターフェイスを DHCP ヘルパーとして設定して、DHCP サーバーから受信したブロードキャスト DHCP 要求を転送するには、該当するインターフェイステンプレートの [DHCP Helper] フィールドに、DHCP サーバーのアドレスを入力します。

[Template] 画面に移動し、テンプレートに命名する

- Cisco vManage メニューから、[Configuration] > [Templates] を選択します。
- [Device Templates] をクリックし、[Create Template] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

- [Create Template] ドロップダウンリストから、[From Feature Template] を選択します。
- [Device Model] ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。
- [Service VPN] をクリックするか、[Service VPN] セクションまでスクロールします。
- [Service VPN] ドロップダウンリストをクリックします。
- [Additional VPN Templates] から、[VPN Interface] をクリックします。
- [Sub-Templates] ドロップダウンリストから、[DHCP Server] を選択します。
- [DHCP Server] ドロップダウンリストから、[Create Template] をクリックします。
[DHCP-Server] テンプレートフォームが表示されます。

このフォームには、テンプレートに名前を付けるためのフィールドと、DHCP サーバーパラメータを定義するためのフィールドが含まれています。

- [Template Name] に、テンプレートの名前を入力します。
名前の最大長は 128 文字で、英数字のみを使用できます。
- [Template Description] に、テンプレートの説明を入力します。
説明の最大長は 2048 文字で、英数字のみを使用できます。

初めて機能テンプレートを開くと、デフォルト値を持つパラメータごとに、その範囲が [Default] に設定され (チェックマークで示される)、デフォルト設定またはデフォルト値が表示されま

す。デフォルト値を変更するか、値を入力するには、[Scope] ドロップダウンリストをクリックします。

DHCP サーバーの最小限の設定

DHCP サーバー機能を設定するには、[Basic Configuration] を選択して、次のパラメータを設定します。DHCP サーバーを設定する場合、アスタリスクの付いたパラメータは必須です。

表 4:

パラメータ名	説明
Address Pool*	ルータインターフェイスが DHCP サーバーとして機能するサービス側ネットワークのアドレスプールの IPv4 プレフィックス範囲を、 <i>prefix/length</i> の形式で入力します。
Exclude Addresses	DHCP アドレスプールから除外する 1 つ以上の IP アドレスを入力します。複数の個別のアドレスを指定するには、それらをカンマで区切ってリストします。アドレスの範囲を指定するには、ハイフンで区切ります。
Maximum Leases	このインターフェイスに割り当てることができる IP アドレスの数を指定します。範囲：0 ~ 4294967295
リース時間	DHCP によって割り当てられた IP アドレスが有効である時間を指定します。範囲：0 ~ 4294967295 秒
Offer Time	DHCP クライアントに提供された IP アドレスがそのクライアントのために予約される期間を指定します。デフォルトでは、提供された IP アドレスは、DHCP サーバーがアドレスを使い果たすまで無期限に予約されます。その時点で、アドレスは別のクライアントに提供されます。範囲：0 ~ 4294967295 秒、デフォルト：600 秒
管理ステータス	インターフェイスで DHCP 機能を有効にする場合は [Up]、無効にする場合は [Down] を選択します。デフォルトでは、DHCP サーバー機能はインターフェイスで無効になっています。

機能テンプレートを保存するには、[Save] をクリックします。

静的リースの設定

静的リースを設定し、サービス側ネットワーク上のクライアントデバイスに静的 IP アドレスを割り当てるには、[Static Lease] をクリックし、[Add New Static Lease] をクリックして、次のパラメータを設定します。

表 5:

パラメータ名	説明
MAC アドレス (MAC Address)	静的 IP アドレスが割り当てられるクライアントの MAC アドレスを入力します。
IP アドレス	クライアントに割り当てる静的 IP アドレスを入力します。
ホストネーム	クライアントデバイスのホスト名を入力します。

静的リースを編集するには、鉛筆アイコンをクリックします。

静的リースを削除するには、ごみ箱アイコンをクリックします。

機能テンプレートを保存するには、[Save] をクリックします。

詳細オプションの設定

DHCP サーバーの詳細オプションを設定するには、[Advanced] をクリックし、次のパラメータを設定します。

表 6:

パラメータ名	説明
インターフェイス MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。 範囲：68 ~ 65535 バイト
ドメイン名	DHCP クライアントがホスト名を解決するために使用するドメイン名を指定します。
デフォルト ゲートウェイ	サービス側ネットワークのデフォルトゲートウェイの IP アドレスを入力します。
DNS サーバー	サービス側ネットワークの DNS サーバーの IP アドレスを 1 つ以上入力します。複数のエントリがある場合は、カンマで区切ります。最大 8 つのアドレスを指定できます。
TFTP サーバ	サービス側ネットワークの TFTP サーバーの IP アドレスを入力します。1 つまたは 2 つのアドレスを指定できます。2 つの場合、アドレスはカンマで区切ってください

機能テンプレートを保存するには、[Save] をクリックします。

CLI を使用した DHCP サーバーの設定

```
Device# config-transaction
Device(dhcp-config)# ip dhcp pool DHCP-POOL
Device(dhcp-config)# network 10.1.1.1 255.255.255.0
Device(dhcp-config)# default-router 10.1.1.2
Device(dhcp-config)# dns-server 172.16.0.1
```

```
Device(dhcp-config)# domain-name DHCP-DOMAIN
Device(dhcp-config)# exit
Device(config)# ip dhcp excluded-address 10.1.1.2 10.1.1.10
Device(
```

リリース情報

リリース 15.2 の Cisco vManage で導入されました。

PPPoE の設定

Point-to-Point Protocol over Ethernet (PPPoE) は、一般的な顧客宅内機器を介して、イーサネットローカルエリアネットワーク経由で複数のユーザーをリモートサイトに接続します。PPPoE は一般的に、デジタル加入者線 (DSL) などのブロードバンドアグリゲーションで使用されます。PPPoE は、CHAP または PAP プロトコルによる認証を提供します。Cisco SD-WAN オーバーレイネットワークでは、Cisco SD-WAN デバイスが PPPoE クライアントを実行できます。PPPoE サーバーコンポーネントはサポートされていません。

Cisco SD-WAN デバイスで PPPoE クライアントを設定するには、PPP 論理インターフェイスを作成し、それを物理インターフェイスにリンクします。物理インターフェイスが起動すると、PPPoE 接続が起動します。PPP インターフェイスは Cisco SD-WAN デバイス上の 1 つの物理インターフェイスのみにリンクでき、物理インターフェイスは 1 つの PPP インターフェイスのみにリンクできます。Cisco SD-WAN デバイスで複数の PPPoE インターフェイスをイネーブルにするには、複数の PPP インターフェイスを設定します。

Quality of Service (QoS) とシェーピングレートは、PPP インターフェイスではなく、PPPoE 対応の物理インターフェイスで設定することをお勧めします。

PPPoE 対応の物理インターフェイスでは、以下はサポートされていません。

- 802.1Q
- サブインターフェイス
- NAT、PMTU、およびトンネルインターフェイス。これらは PPP インターフェイスで設定されているため、PPPoE 対応のインターフェイスでは使用できません。

PPPoE の Cisco SD-WAN 実装では、RFC 1962 で定義されている Compression Control Protocol (CCP) オプションはサポートされていません。

vManage テンプレートからの PPPoE の設定

vManage テンプレートを使用して Cisco IOS XE SD-WAN デバイスで PPPoE を設定するには、3 つの機能テンプレートと 1 つのデバイステンプレートを作成します。

- VPN-Interface-PPP 機能テンプレートを作成して、PPP 仮想インターフェイスの PPP パラメータを設定します。
- VPN-Interface-PPP-Ethernet 機能テンプレートを作成して、PPPoE 対応インターフェイスを設定します。

- 必要に応じて、VPN 機能テンプレートを作成して、VPN 0 の既定の構成を変更します。
- VPN-Interface-PPP、VPN-Interface-PPP-Ethernet、および VPN 機能テンプレートを組み込んだデバイステンプレートを作成します。

VPN-Interface-PPP 機能テンプレートを作成して、PPP 仮想インターフェイスの PPP パラメータを設定します。

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. **[機能テンプレート]** をクリックし、**[テンプレートの追加]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前では、**[Feature Templates]** のタイトルは **[Feature]** です。

3. Cisco IOS XE SD-WAN デバイスクラウドまたはルータモデルを選択します。
4. **[VPN-Interface-PPP]** テンプレートを選択します。
5. テンプレートで、次のパラメータを設定します。

表 7:

パラメータフィールド	手順
テンプレート名	テンプレートの名前を入力します。最大 128 文字の英数字を使用できます。
説明	テンプレートの説明を入力します。最大 2048 文字の英数字を使用できます。
シャットダウン	[No] をクリックして、PPP 仮想インターフェイスを有効にします。
Interface Name	PPP インターフェイスの番号を入力します。1～31 で指定できます。
説明 (Description) (任意)	PPP 仮想インターフェイスの説明を入力します。
認証プロトコル (Authentication Protocol)	CHAP または PAP のいずれかを選択して 1 つの認証プロトコルを設定するか、PAP と CHAP を選択して両方を設定します。CHAP の場合は、ISP から提供されたホスト名とパスワードを入力します。PAP の場合は、ISP から提供されたユーザー名とパスワードを入力します。PAP と CHAP の両方を設定する場合、両方に同じユーザー名とパスワードを使用するには、 [Same Credentials for PAP and CHAP] をクリックします。
AC Name (オプション)	[PPP] タブを選択し、 [AC Name] フィールドに、インターネットへの接続をルーティングするために PPPoE が使用するアクセスコンセントレータの名前を入力します。

パラメータフィールド	手順
IP MTU	[Advanced] をクリックし、[IP MTU] フィールドで、IP MTU が物理インターフェイスの MTU よりも少なくとも 8 バイト少ないことを確認します。PPP インターフェイスの最大 MTU は 1492 バイトです。PPPoE サーバーで Maximum Receive Unit (MRU) が指定されていない場合、PPP インターフェイスの MTU 値が MRU として使用されます。 Cisco vManage リリース 20.9.1 以降では、設定がデバイスにプッシュされるときに、指定された IPMTU 値に基づいて 8 バイトのオーバーヘッドが推定されます。
Save	機能テンプレートを保存するには、[Save] をクリックします。

VPN-Interface-PPP-Ethernet 機能テンプレートを作成して物理インターフェイスで PPPoE クライアントを有効にするには、次の手順を実行します。

1. Cisco vManage メニューから、[Configuration] > [Templates] を選択します。
2. [機能テンプレート] をクリックし、[テンプレートの追加] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前では、[Feature Templates] のタイトルは [Feature] です。

3. クラウドまたはルータモデルを選択します。
4. [VPN-Interface-PPP-Ethernet] テンプレートを選択します。
5. テンプレートで、次のパラメータを設定します。

パラメータフィールド	手順
テンプレート名	テンプレートの名前を入力します。最大 128 文字の英数字を使用できます。
説明	テンプレートの説明を入力します。最大 2048 文字の英数字を使用できます。
シャットダウン	[No] をクリックして、PPPoE 対応インターフェイスを有効にします。
Interface Name	PPP インターフェイスに関連付ける VPN 0 の物理インターフェイスの名前を入力します。
説明 (Description) (任意)	PPPoE 対応インターフェイスの説明を入力します。

パラメータフィールド	手順
IP Configuration	物理インターフェイスに IP アドレスを割り当てます。 <ul style="list-style-type: none"> • DHCP を使用するには、[Dynamic] を選択します。DHCP から学習したルートのデフォルトのアドミニストレティブ ディスタンスは 1 です。 • IP アドレスを直接設定するには、インターフェイスの IPv4 アドレスを入力します。
DHCP Helper (オプション)	ネットワーク内の DHCP サーバーの IP アドレスを 4 つまで入力します。
Save	機能テンプレートを保存するには、[Save] をクリックします。

VPN 機能テンプレートを作成して、VPN 0、トランスポート VPN で PPPoE 対応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。

1. Cisco vManage メニューから、[Configuration] > [Templates] を選択します。
2. [機能テンプレート] をクリックし、[テンプレートの追加] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前では、[Feature Templates] のタイトルは [Feature] です。

3. クラウドまたはルータモデルを選択します。
4. [VPN] テンプレートを選択します。
5. テンプレートで、次のパラメータを設定します。

パラメータフィールド	手順
テンプレート名	テンプレートの名前を入力します。最大 128 文字の英数字を使用できます。
説明	テンプレートの説明を入力します。最大 2048 文字の英数字を使用できます。
VPN 識別子	VPN 識別子 0 を入力します。
名前	VPN の名前を入力します。
Other interface parameters	必要なインターフェイスプロパティを設定します。
Save	機能テンプレートを保存するには、[Save] をクリックします。

VPN-Interface-PPP、VPN-Interface-PPP-Ethernet、および VPN 機能テンプレートを組み込んだデバイステンプレートを作成するには、次の手順を実行します。

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. **[Device Templates]** をクリックし、**[Create Template]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Device Templates]** のタイトルは **[Device]** です。

3. **[Create Template]** ドロップダウンリストから、**[From Feature Template]** を選択します。
4. **[Device Model]** ドロップダウンリストから、デバイステンプレートを作成するデバイスのタイプを選択します。

vManage NMS に、選択したデバイスタイプの機能テンプレートが表示されます。必須のテンプレートはアスタリスク (*) で示されます。
5. デバイステンプレートの名前と説明を入力します。これらのフィールドは必須です。テンプレート名には特殊文字は使用できません。
6. **[Transport & Management VPN]** の **[VPN 0]** で、使用可能なテンプレートのドロップダウンリストから、目的の機能テンプレートを選択します。使用可能なテンプレートのリストは、以前に作成したテンプレートです。
7. **[Additional VPN 0 Templates]** で、**[VPN Interface PPP]** の横にあるプラス記号 (+) をクリックします。
8. **[VPN-Interface-PPP]** および **[VPN-Interface-PPP-Ethernet]** フィールドから、使用する機能テンプレートを選択します。
9. VPN 0 で複数の PPPoE 対応インターフェイスを設定するには、**[Sub-Templates]** の横にあるプラス記号 (+) をクリックします。
10. デバイステンプレートに追加の機能テンプレートを含めるには、残りのセクションで機能テンプレートを順に選択し、使用可能なテンプレートのドロップダウンリストから目的のテンプレートを選択します。使用可能なテンプレートのリストは、以前に作成したテンプレートです。すべての必須機能テンプレート、および目的の任意の機能テンプレートのテンプレートを選択していることを確認してください。
11. デバイステンプレートを作成するには、**[Create]** をクリックします。

デバイステンプレートをデバイスにアタッチするには、次の手順を実行します。

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. **[Device Templates]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

3. テンプレートを選択します。
4. [...] をクリックして、[Attach Device] をクリックします。
5. デバイスを検索するか、左側の [Available Device(s)] 列からデバイスを選択します。
6. 右向き矢印をクリックして、デバイスを右側の [Selected Devices] 列に移動します。
7. [Attach] をクリックします。

PPPoE Over ATM の設定

表 8: 機能の履歴

機能名	リリース情報	説明
PPPoE over ATM の設定	Cisco IOS XE リリース 17.4.1a Cisco vManage リリース 20.4.1	この機能は、Cisco IOS XE SD-WAN デバイスでの PPPoEoA の設定をサポートします。PPPoEoA は AAL5MUX カプセル化を使用しており、他のカプセル化方法と比較して効率が優れています。

ADSL をサポートする Cisco IOS XE SD-WAN デバイスで PPPoE over ATM インターフェイス (PPPoEoA) を設定できます。PPPoEoA は、ATM Adaptation Layer 5 Multiplexed Encapsulation (AAL5MUX) カプセル化を使用して、ATM 相手先固定接続 (PVC) 上で PPPoE を伝送し、AAL5 LLC/SNAP カプセル化よりも効率が向上します。

PPPoEoA over AAL5MUX は、多重化 (MUX) カプセル化を使用して、音声パケットの伝送に必要なセルの数を減らすことにより、サブネットワークアクセスプロトコル (SNAP) カプセル化の帯域幅使用量を削減します。PPPoEoA over ATM AAL5MUX 機能を VoIP 環境に導入すると、スループットと帯域幅の使用率が向上します。

PPPoE Over ATM でサポートされるプラットフォーム

次のプラットフォームは、PPPoE over ATM をサポートしています。

- Cisco 1100 4G/6G シリーズ サービス統合型ルータ。
- Cisco 1100 シリーズ サービス統合型ルータ。

- Cisco 1109 シリーズ サービス統合型ルータ。
- Cisco111x シリーズ サービス統合型ルータ。
- Cisco1111x シリーズ サービス統合型ルータ。
- Cisco 1120 シリーズ サービス統合型ルータ。
- Cisco 1160 シリーズ サービス統合型ルータ。

Cisco vManage を使用した PPPoE Over ATM の設定

デバイス CLI テンプレートを使用して、Cisco vManage で PPPoE を設定できます。

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. **[Device Templates]** から、**[Create Template]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Device Templates]** のタイトルは **[Device]** です。

3. **[Create Template]** ドロップダウンリストから、**[CLI Template]** を選択します。
4. **[Device Model]** ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。
5. **[Template Name]** に、テンプレートの名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。
6. **[Template Description]** に、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。
7. **[Device configuration]** を選択します。このオプションを使用すると、`show sdwan running-config` コマンドの出力に表示される IOS-XE 設定コマンドを指定できます。
8. (オプション) 接続されたデバイスの実行構成をロードするには、**[Load Running config from reachable device]** リストからそのデバイスを選択し、**[Search]** をクリックします。
9. **[CLI Configuration]** で、手入力するか、カットアンドペーストするか、ファイルをアップロードして、設定を入力します。PPPoEoA の設定は、「[CLI での PPPoE Over ATM の設定](#)」セクションにあります。
10. 実際の設定値を変数に変換するには、値を選択して **[Create Variable]** をクリックします。変数名を入力し、**[Create Variable]** をクリックします。`{{variable-name}}` の形式で変数名を直接入力することもできます。たとえば、`{{hostname}}` です。
11. **[Add]** をクリックします。新しいデバイステンプレートが **[Device Template]** テーブルに表示されます。**[Type]** 列には、デバイステンプレートが CLI テキストから作成されたことを示す「CLI」が表示されます。

CLI での PPPoE Over ATM の設定

このセクションでは、CLI で PPPoE over ATM を設定するための CLI 設定例を示します。

```
Device(config)# interface atm number
Device(config)# no ip address
Device(config)# interface atm number point-to-point
Device(config)# no atm enable-ilmi-trap
Device(config)# encapsulation aal5mux pppoe-client
Device(config)# pppoe-client dial-pool-number number
Device(config)# interface Dialer dialer-rotary-group-number
Device(config)# mtu bytes
Device(config)# ip address negotiated
Device(config-if)# encapsulation encapsulation-type
Device(config)# load-interval seconds
Device(config)# dialer pool number
Device(config)# dialer-group group-number
Device(config)# ppp mtu adaptive
Device(config)# ppp chap hostname hostname
Device(config)# ppp chap password secret
Device(config)# ppp ipcp address required
Device(config)# ppp link reorders
```

PPPoE Over ATM インターフェイスの設定例

次に、ATM インターフェイスでの PPPoE の設定例を示します。

```
Device(config)# interface ATM0/1/0
Device(config)# no ip address
Device(config)# no atm enable-ilmi-trap
!
Device(config)# interface ATM0/1/0.10 point-to-point
Device(config)# no atm enable-ilmi-trap
Device(config)# cdp enable
Device(config)# pvc 22/62
Device(config)#ubr 1045
Device(config-if)# encapsulation aal5mux pppoe-client
Device(config)# pppoe-client dial-pool-number 120
!
!
Device(config)# interface Dialer 120
Device(config)# mtu 1492
Device(config)# ip address negotiated
Device(config)# ip nat outside
Device(config-if)# encapsulation ppp
Device(config)# load-interval 30
Device(config)# dialer pool 120
Device(config)# dialer-group 1
Device(config)# ppp mtu adaptive
Device(config)# ppp chap hostname test@cisco.com
Device(config)# ppp chap password 0 cisco
Device(config)# ppp ipcp address required
Device(config)# ppp link reorders
!
```

VRRP の設定



- (注) VRRP が機能するには、x710 NIC に `t->system-> vrrp-adv-t-with-phymac` コマンドが設定されている必要があります。

Virtual Router Redundancy Protocol (VRRP) は、スイッチおよび他の IP エンドステーションに冗長ゲートウェイサービスを提供する LAN 側のプロトコルです。Cisco SD-WAN ソフトウェアでは、VPN 内のインターフェイス（通常はサブインターフェイス）で VRRP を設定します。

VRRP はサービス側 VPN (VPN 0 および 512 が予約済み) でのみサポートされており、サブインターフェイスを使用する場合は、VPN 0 で VRRP 物理インターフェイスを設定する必要があります。

VRRP インターフェイス（またはサブインターフェイス）ごとに、IP アドレスを割り当て、そのインターフェイスを VRRP グループに配置します。

グループ番号は仮想ルータを識別します。ルータには最大 512 のグループを設定できます。一般的な VRRP トポロジでは、2 つの物理ルータが単一の仮想ルータとして機能するように構成するため、これら両方のルータのインターフェイスに同じグループ番号を設定します。

各仮想ルータ ID に対して 1 つの IP アドレスを設定する必要があります。

各 VRRP グループ内では、プライオリティ値の高いルータがプライマリ VRRP として選択されます。デフォルトでは、各仮想ルータの IP アドレスのデフォルトプライマリ選択プライオリティは 100 であるため、より高い IP アドレスのルータがプライマリとして選択されます。プライオリティ値は、1 ~ 254 の値に設定して変更できます。

プライマリ VRRP は、まだ動作していることを示すアドバタイズメントメッセージを定期的に送信します。バックアップルータが 3 つの連続した VRRP アドバタイズメントを失うと、プライマリ VRRP がダウンしていると見なされ、新しいプライマリ VRRP が選択されます。デフォルトでは、これらのメッセージは 1 秒ごとに送信されます。VRRP アドバタイズメントの時間は、1 ~ 3600 秒の値に変更できます。

デフォルトでは、VRRP は、どのルータがプライマリ仮想ルータであるかを判別するために、VRRP が実行されているインターフェイスの状態を使用します。このインターフェイスは、ルータのサービス (LAN) 側にあります。プライマリ VRRP のインターフェイスがダウンすると、VRRP プライオリティ値に基づいて新しいプライマリ VRRP 仮想ルータが選択されます。VRRP は LAN インターフェイスで実行されるため、ルータがすべての WAN 制御接続を失った場合、ルータが VRRP に機能的に参加できない場合でも、LAN インターフェイスは稼働の状態を示したままになります。VRRP の WAN 側の接続を考慮するには、次のいずれかを設定します。

- プライマリ VRRP 仮想ルータを決定するときに、WAN 接続で実行されているオーバーレイ管理プロトコル (OMP) セッションを追跡します。

プライマリ VRRP ルータですべての OMP セッションが失われた場合、VRRP は 1 つ以上のアクティブな OMP セッションを持つすべてのゲートウェイの中から新しいデフォルトゲートウェイを選択します。これは、選択されたゲートウェイの VRRP プライオリティが現在のプライマリ VRRP ルータよりも低い場合にも実行されます。このオプションでは、OMP 状態がアップからダウンに変化すると、VRRP フェールオーバーが発生します。この変化は、OMP ホールドタイマーが期限切れになったときに発生します（デフォルトの OMP ホールドタイマー間隔は 60 秒です）。ホールドタイマーが期限切れになり、新しいプライマリ VRRP が選択されるまでは、すべてのオーバーレイトラフィックがドロップされます。OMP セッションが回復すると、ローカル VRRP インターフェイスは、Cisco vSmart コントローラから OMP ルートを学習およびインストールする前でも、自身をプライマリ VRRP として主張します。ルータが学習されるまでは、トラフィックもドロップされます。

- OMP セッションとリモートプレフィックスのリストの両方を追跡します。

すべての OMP セッションが失われた場合、**track-omp** オプションで説明されているように、VRRP フェールオーバーが発生します。さらに、リスト内のすべてのプレフィックスへの到達可能性が失われた場合、VRRP フェールオーバーは、OMP ホールドタイマーが期限切れになるのを待たずにすぐに発生するため、ルータがプライマリ VRRP を決定する間にドロップされるオーバーレイトラフィックの量が最小限に抑えられます。

先ほど説明したように、IEEE 802.1Q プロトコルは各パケットの長さに 4 バイトを追加します。したがって、パケットを送信するには、VPN 0 の物理インターフェイスの MTU サイズを増やすか（デフォルトの MTU は 1500 バイトです）、VRRP インターフェイスの MTU サイズを減らします。

動的インターフェイスの設定

表 9: 機能の履歴

機能名	リリース情報	説明
動的インターフェイスの設定	Cisco IOS XE リリース 17.3.2 Cisco vManage リリース 20.3.2	この機能を使用すると、サポートされているデバイスの動的インターフェイスを設定できます。動的インターフェイスにより、デバイスはリアルタイムで最適なパスを選択できます。 この機能は、Cisco C8500-12X4QC ルータにのみ適用されます。

サポートされているデバイスの動的インターフェイスを設定できます。動的インターフェイスにより、デバイスはリアルタイムで最適なパスを選択できます。

動的インターフェイスの設定は、次の一般的な手順で構成されます。

1. 動的インターフェイスモード機能テンプレートを作成します。この手順の一部として、デバイスのベイのモードを定義します。
2. 制御接続のインターフェイスを設定します。
3. 動的インターフェイスモード機能テンプレートをデバイステンプレートに関連付けます。

動的インターフェイスモード機能テンプレートの作成

動的インターフェイスモード機能テンプレートを作成するときは、デバイスのベイのモードを定義するテンプレートを作成します。

ベイ 1、ベイ 2、またはその両方のモードを設定できます。

ベイ 0 のモードは自動的に設定され、変更できません。ベイ 1 のモードを 100G に設定すると、ベイ 0 の 10G インターフェイスは適用されないため、ベイ 0 は無効になります。

1. Cisco vManage メニューから、**[Configuration] > [Templates]** を選択します。
2. **[Device Templates]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Device Templates]** のタイトルは **[Device]** です。

3. **[Create Template]** ドロップダウンリストをクリックし、**[Feature Template]** を選択します。
4. **[Device Model]** ドロップダウンリストから、テンプレートを作成するデバイスを選択します。
5. **[Template Name]** に、テンプレートの名前を入力します。
このフィールドには、英大文字と小文字、0～9の数字、ハイフン (-)、下線 (_) を使用できます。
6. **[Description]** にテンプレートの説明を入力します。
このフィールドには任意の文字とスペースを使用できます。
7. **[Additional Templates]** から、**[Dynamic Interface Mode]** ドロップダウンリストを選択し、**[Create Template]** をクリックします。
8. **[Template Name]** に、テンプレートの名前を入力します。
このフィールドには、英大文字と小文字、0～9の数字、ハイフン (-)、下線 (_) を使用できます。
9. **[Description]** にテンプレートの説明を入力します。
このフィールドには任意の文字とスペースを使用できます。
10. **[Bay 1]**、**[Bay 2]**、または両方のフィールドで目的の値を選択して、ベイ 1、ベイ 2、または両方のベイのモードを設定します。

ベイ 0 のデフォルト値は変更できません。

11. **[Save]** をクリックします。

制御接続のインターフェイスを構成する

このセクションでは、「動的インターフェイスモード機能テンプレートの作成」で設定したベイで動作するように、既存の制御接続用の新しいVPN0インターフェイスを設定する方法について説明します。また、インターフェイスのIPv4ルートを設定する方法についても説明します。

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. **[Device Templates]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Device Templates]** のタイトルは **[Device]** です。

3. インターフェイスを設定するテンプレートの [...] をクリックし、**[Edit]** を選択します。
4. **[Transport & Management VPN]** をクリックし、次のアクションを実行してベイのインターフェイスを作成します。
 1. **[Additional VPN 0 Template]** で **[VPN Interface]** をクリックします。
 2. 表示される新しい **[VPN Interface Ethernet]** メニューを選択し、**[Create Template]** をクリックします。
 3. **[Template Name]** に、テンプレートの名前を入力します。

このフィールドには、英大文字と小文字、0~9の数字、ハイフン (-)、下線 (_) を使用できます。
 4. **[Description]** にテンプレートの説明を入力します。

このフィールドには任意の文字とスペースを使用できます。
 5. 「動的インターフェイスモード機能テンプレートの作成」の説明に従って、設定したベイに制御接続を追加します。
5. **[Basic Configuration]** を選択し、次のアクションを実行します。
 1. **[Interface Name]** にインターフェイスの名前を入力します。

この例に示す形式で名前を入力します。「FortyGigabitEthernet0/1/0」。
 2. 必要に応じてこのタブの他のオプションを設定します。
6. **[Tunnel]** から、**[Tunnel Interface]** を **[On]** に設定します。
7. **[Save]** をクリックします。

8. [IPv4 Route] を選択し、次のアクションを実行して、VPN0 テンプレートの IPv4 ルートを設定します。
 1. [New IPv4 Route] をクリックします。
 2. [Prefix] に、IPv4 ルートのプレフィックスを入力します。
 3. [Gateway] で、[Next Hop] を選択します。
 4. [Next Hop] で必要に応じて項目を構成し、[Add] をクリックします。
 5. [Save] をクリックします。
9. [更新 (Update)] をクリックします。

動的インターフェイスモード機能テンプレートとデバイステンプレートの関連付け

動的インターフェイスモード機能テンプレートを作成したら、それをデバイステンプレートに関連付け、デバイステンプレートをデバイスに接続します。手順については、「[機能テンプレートからのデバイステンプレートの作成](#)」を参照してください。

VPN イーサネット インターフェイスの設定

ステップ 1 Cisco vManage メニューから、[Configuration] > [Templates] を選択します。

ステップ 2 [Device Templates] をクリックし、[Create Template] をクリックします。

(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

ステップ 3 [Create Template] ドロップダウンリストから、[From Feature Template] を選択します。

ステップ 4 [Device Model] ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。

ステップ 5 VPN 0 または VPN 512 のテンプレートを作成するには、次の手順を実行します。

1. [Transport & Management VPN] をクリックするか、[Transport & Management VPN] セクションまでスクロールします。
2. [Additional VPN 0 Templates] で、[Cisco VPN Interface Ethernet] をクリックします。
3. From the **VPN Interface** drop-down list, click **Create Template**. [Cisco VPN Interface Ethernet] テンプレートフォームが表示されます。

このフォームには、テンプレートに名前を付けるためのフィールドと、VPN インターフェイスイーサネットパラメータを定義するためのフィールドが含まれています。

ステップ 6 [Template Name] に、テンプレートの名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。

ステップ7 [Template Description] に、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。

基本的なインターフェイス機能の設定

VPNで基本的なインターフェイス機能を設定するには、[Basic Configuration] を選択し、次のパラメータを設定します。



(注) インターフェイスを設定する場合、アスタリスクの付いたパラメータは必須です。

パラメータ名	IPv4 または IPv6	オプション	Description
[Shutdown] *			インターフェイスを有効にするには [No] をクリックします。
Interface name*			<p>インターフェイスの名前を入力します。</p> <p>Cisco IOS XE SD-WAN デバイス については、次のことを行う必要があります。</p> <ul style="list-style-type: none"> • インターフェイス名を完全にスペルアウトします (たとえば、GigabitEthernet0/0/0)。 • 使用していない場合でも、すべてのルータのインターフェイスを設定して、それらがシャットダウン状態で設定され、それらのすべてのデフォルト値が設定されるようにします。
Description			インターフェイスの説明を入力します。
[IPv4 / IPv6]			[IPv4] をクリックして、IPv4 VPN インターフェイスを設定します。[IPv6] をクリックして、IPv6 インターフェイスを設定します。

パラメータ名	IPv4 または IPv6	オプション	Description
Dynamic	インターフェイスを Dynamic Host Configuration Protocol (DHCP) クライアントとして設定し、インターフェイスが DHCP サーバーから IP アドレスを受信するようにするには、[Dynamic] を選択します。		
	両方	DHCP Distance	必要に応じて、DHCP サーバーから学習したルートのアドミニストレティブ ディスタンス値を入力します。デフォルトは 1 です。
	IPv6	DHCP Rapid Commit	必要に応じて、DHCP Rapid Commit をサポートするように DHCP IPv6 ローカルサーバーを設定して、ビジーな環境でクライアントの設定と確認を高速化できるようにします。 [On] をクリックして、DHCP 高速コミットを有効にします。 [Off] をクリックして、通常のコミットプロセスの使用を続行します。
[Static]	[Static] をクリックして、変更しない IP アドレスを入力します。		
	IPv4	IPv4 アドレス (IPv4 Address)	静的 IPv4 アドレスを入力します。
	IPv6	[IPv6 アドレス (IPv6 Address)]	静的 IPv6 アドレスを入力します。
Secondary IP Address	IPv4	[Add] をクリックして、サービス側インターフェイスのセカンダリ IPv4 アドレスを最大 4 つ入力します。	
[IPv6 アドレス (IPv6 Address)]	IPv6	[Add] をクリックして、サービス側インターフェイスのセカンダリ IPv6 アドレスを 2 つまで入力します。	
DHCP Helper	両方	インターフェイスをルータの DHCP ヘルパーとして指定するには、ネットワーク内の DHCP サーバーの IP アドレスをカンマで区切って 8 つまで入力します。DHCP ヘルパーインターフェイスは、指定された DHCP サーバーから受信した BootP (ブロードキャスト) DHCP 要求を転送します。	
Block Non-Source IP	Yes / No	[Yes] をクリックして、トラフィックのソース IP アドレスがインターフェイスの IP プレフィックス範囲と一致する場合にのみ、インターフェイスにトラフィックを転送させます。他のトラフィックを許可するには、[No] をクリックします。	

機能テンプレートを保存するには、[Save] をクリックします。

トンネルインターフェイスの作成

Cisco IOS XE SD-WAN デバイスでは、最大 8 つのトンネルインターフェイスを設定できます。つまり、各 Cisco IOS XE SD-WAN デバイス ルータに最大 8 つの TLOC を設定できます。Cisco vSmart コントローラ および Cisco vManage では、1 つのトンネルインターフェイスを設定できます。

オーバーレイネットワークが機能できるようにコントロールプレーンがそれ自体を確立するには、VPN 0 で WAN トランスポート インターフェイスを設定する必要があります。WAN インターフェイスは、オーバーレイへのトンネルトラフィックのフローを有効にします。WAN インターフェイスをトンネルインターフェイスとして設定しないと、次の表に示されている他のパラメータを追加できません。

トンネルインターフェイスを設定するには、[Interface Tunnel] を選択し、次のパラメータを設定します。

パラメータ名	説明
トンネルインターフェイス	[On] をクリックして、トンネルインターフェイスを作成します。
色	TLOC の色を選択します。
ポートホップ	<p>ポートホッピングを有効にするには [On] をクリックし、無効にするには [Off] をクリックします。ポートホッピングがグローバルに有効になっている場合は、個々の TLOC (トンネルインターフェイス) で無効にできます。ポートホッピングをグローバルレベルで制御するには、[System] 設定テンプレートを使用します。</p> <p>https://sdwan-docs.cisco.com/Product_Documentation/vManage_Help/Release_18.3/Configuration/Templates/System</p> <p>デフォルト：有効</p> <p>vManage NMS と Cisco vSmart コントローラ のデフォルト：無効</p>
TCP MSS	<p>TCP MSS は、ルータを通過する最初の TCP ヘッダーを含むすべてのパケットに影響します。設定すると、TCP MSS は 3 ウェイハンドシェイクで交換される MSS と比較されます。構成済みの TCP MSS 設定がヘッダーの MSS よりも小さい場合、ヘッダーの MSS の値が減少します。MSS ヘッダー値がすでに TCP MSS よりも小さい場合、パケットは変更されずに通過します。トンネルの終端にあるホストは、2 つのホストの小さい方の設定を使用します。TCP MSS を設定する場合は、最小パス MTU より 40 バイト小さく設定する必要があります。</p> <p>Cisco IOS XE SD-WAN デバイスを通過する TPC SYN パケットの MSS を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552～1460 バイト、デフォルト：なし</p>

パラメータ名	説明
Clear-Dont-Fragment	<p>Don't Fragment が設定されているインターフェイスに到着するパケットの [Clear-Dont-Fragment] を設定します。これらのパケットが MTU が許可するサイズより大きい場合、それらはドロップされます。Don't Fragment ビットをクリアすると、パケットはフラグメント化されて送信されます。</p> <p>[On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Dont Fragment ビットをクリアします。Dont Fragment ビットがクリアされると、インターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。</p> <p>(注) [Clear-Dont-Fragment] は Dont Fragment ビットをクリアし、Dont Fragment ビットが設定されます。フラグメンテーションを必要としないパケットの場合、Dont Fragment ビットは影響を受けません。</p>
サービスの許可	サービスごとに [On] または [Off] を選択して、インターフェイスでサービスを許可または禁止します。

追加のトンネルインターフェイスパラメータを設定するには、[Advanced Options] をクリックします。

パラメータ名	説明
通信事業者	<p>トンネルに関連付けるキャリア名またはプライベートネットワーク識別子を選択します。</p> <p>値 : carrier1、carrier2、carrier3、carrier4、carrier5、carrier6、carrier7、carrier8、default</p> <p>デフォルト : default</p>
NAT 更新間隔	<p>DTLS または TLS WAN トランスポート接続で送信される NAT リフレッシュパケットの間隔を入力します。</p> <p>範囲 : 1 ~ 60 秒</p> <p>デフォルト : 5 秒</p>
Hello 間隔 (Hello Interval)	<p>DTLS または TLS WAN トランスポート接続で送信される Hello パケットの間隔を入力します。</p> <p>範囲 : 100 ~ 10000 ミリ秒</p> <p>デフォルト : 1000 ミリ秒 (1 秒)</p>

パラメータ名	説明
Hello 許容度	<p>トランスポートトンネルのダウンを宣言する前に、DTLS または TLS WAN トランスポート接続で Hello パケットを待機する時間を入力します。</p> <p>範囲：12 ～ 60 秒</p> <p>デフォルト：12 秒</p>

キャリア名とトンネルインターフェイスの関連付け

キャリア名またはプライベートネットワーク識別子をトンネルインターフェイスに関連付けるには、**carrier** コマンドを使用します。*carrier-name* には **default** および、**carrier1** ～ **carrier8** を指定できます。

```
Device(config)# interface Tunnel 0
Device(config-if)# ip unnumbered GigabitEthernet1
Device(config-if)# ipv6 unnumbered GigabitEthernet2
Device(config-if)# tunnel source GigabitEthernet1
Device(config-if)# tunnel mode sdwan
Device(config-if)# exit
Device(config)# sdwan
Device(config-sdwan)# int GigabitEthernet1
Device(config-interface-GigabitEthernet1)# tunnel-interface
Device(config-tunnel-interface)# carrier default
```

トンネルグループの作成

デフォルトでは、WAN エッジルータは色に関係なく、ネットワーク内の他のすべての TLOC とのトンネルを構築しようとします。トンネル設定の下で色を指定して **restrict** オプションを使用すると、TLOC は同じ色の TLOC へのトンネルの構築のみに制限されます。**restrict** オプションの詳細については、「[Configure Interfaces in the WAN Transport VPN\(VPN0\)](#)」を参照してください。

トンネルグループ機能は **restrict** オプションに似ていますが、トンネルグループ ID がトンネルの下で割り当てられると、同じトンネルグループ ID を持つ TLOC のみが色に関係なく相互にトンネルを形成できるため、柔軟性が向上します。

TLOC がトンネルグループ ID に関連付けられている場合、トンネルグループ ID に関連付けられていないネットワーク内の他の TLOC とのトンネルを引き続き形成します。



- (注) **restrict** オプションは、この機能と組み合わせて使用できます。使用すると、インターフェイスで定義されたトンネルグループ ID と **restrict** オプションを持つインターフェイスは、同じトンネルグループ ID とカラーを持つ他のインターフェイスとだけトンネルを形成します。

CLI を使用した Cisco IOS XE SD-WAN デバイス でのトンネルグループの設定

Cisco IOS XE SD-WAN デバイスでトンネルグループを設定するには、次の手順を実行します。

```
Device(config)# sdwan
Device(config-sdwan)# interface GigabitEthernet2

Device(config-interface-GigabitEthernet2)# tunnel-interface
Device(config-tunnel-interface)#group Group ID
```

トンネルインターフェイスでのキープアライブトラフィックの制限

デフォルトでは、Cisco IOS XE SD-WAN デバイスは 1 秒に 1 回、Hello パケットを送信して、2 つのデバイス間のトンネルインターフェイスがまだ動作しているかどうかを判断し、トンネルを維持します。hello 間隔と hello 許容度の組み合わせによって、DTLS または TLS トンネルのダウンを宣言するまでの待機時間が決まります。デフォルトの hello 間隔は 1 秒で、デフォルトの許容値は 12 秒です。これらのデフォルト値では、Hello パケットが 11 秒以内に受信されない場合、トンネルは 12 秒時点でダウンが宣言されます。

DTLS または TLS トンネルの両端で hello 間隔、hello 許容度、またはその両方が異なる場合、トンネルは次のように間隔と許容度を選択します。

- 2 つのコントローラデバイス間のトンネル接続の場合、トンネルは 2 つのデバイス間の接続に対して、小さい方の hello 間隔と大きい方の許容間隔を使用します。（コントローラ デバイスは、vBond コントローラ、vManage NMS、および vSmart コントローラです。）この選択は、コントローラのいずれかに低速の WAN 接続がある場合に行われます。hello 間隔と許容時間は、コントローラデバイスのペアごとに個別に選択されます。
- Cisco IOS XE SD-WAN デバイスと任意のコントローラデバイス間のトンネル接続の場合、トンネルはルータに設定されている hello 間隔と許容時間を使用します。この選択は、トンネルを介して送信されるトラフィックの量を最小限に抑え、リンクのコストがリンクを通過するトラフィックの量の関数である状況を可能にするために行われます。hello 間隔と許容時間は、Cisco IOS XE SD-WAN デバイスとコントローラデバイス間のトンネルごとに個別に選択されます。

トンネルインターフェイスのキープアライブトラフィックの量を最小限に抑えるには、トンネルインターフェイスの Hello パケット間隔と許容度を増やします。

```
Device(config-tunnel-interface)# hello-interval milliseconds
Device(config-tunnel-interface)# hello-tolerance seconds
```

デフォルトの hello 間隔は 1000 ミリ秒で、100 ~ 600000 ミリ秒（10 分）の範囲の時間にすることができます。デフォルトの hello 許容度は 12 秒で、12 ~ 600 秒（10 分）の範囲の時間にすることができます。hello 許容間隔は、OMP ホールド時間の半分以下にする必要があります。デフォルトの OMP ホールド時間は 60 秒で、**omp timers holdtime** コマンドで設定します。

インターフェイスの NAT デバイスとしての設定

NAT の設定方法については、『[Cisco SD-WAN NAT Configuration Guide, Cisco IOS XE リリース 17.x](#)』を参照してください。

アクセスリストと QoS パラメータの適用

サービスの品質 (QoS) は、サービスの実行方法を決定するのに役立ちます。QoS を設定することにより、WAN 上のアプリケーションのパフォーマンスを向上させます。インターフェイスのシェーピングレートを設定し、QoS マップ、書き換えルール、アクセスリスト、およびポリサーをインターフェイスに適用するには、[ACL/QoS] をクリックして、次のパラメータを設定します。

パラメータ名	説明
成形率	インターフェイスの集約トラフィック転送速度を回線速度よりも低く設定します (キロビット/秒 (kbps) 単位)。
QoS マップ (QoS Map)	インターフェイスから送信されるパケットに適用する QoS マップの名前を指定します。
リライトルール	[On] をクリックし、インターフェイスに適用する書き換えルールの名前を指定します。
入力 ACL - IPv4	[On] をクリックして、インターフェイスで受信される IPv4 パケットに適用するアクセスリストの名前を指定します。
出力 ACL - IPv4	[On] をクリックし、インターフェイスで送信される IPv4 パケットに適用するアクセスリストの名前を指定します。
入力 ACL - IPv6	[オン] をクリックして、インターフェイスで受信される IPv6 パケットに適用するアクセスリストの名前を指定します。
出力 ACL - IPv6	[オン] をクリックし、インターフェイスで送信される IPv6 パケットに適用するアクセスリストの名前を指定します。
入力ポリサー	[On] をクリックして、インターフェイスで受信されるパケットに適用するポリサーの名前を指定します。
出力ポリサー	[オン] をクリックして、インターフェイスで送信されるパケットに適用するポリサーの名前を指定します。

機能テンプレートを保存するには、[Save] をクリックします。

ARP テーブルエントリの追加

アドレス解決プロトコル (ARP) は、リンク層アドレス (デバイスの MAC アドレスなど) を割り当てられたインターネット層アドレスに関連付けるのに役立ちます。動的マッピングが機能していない場合は、静的 ARP アドレスを設定します。インターフェイスで静的 ARP テーブルエントリを設定するには、ARP を選択します。次に、[Add New ARP] をクリックして、次のパラメータを設定します。

パラメータ名	Description
IP アドレス	ARP エントリの IP アドレスをドット付き 10 進表記または完全修飾ホスト名として入力します。

パラメータ名	Description
MAC アドレス	MAC アドレスをコロン区切りの 16 進表記で入力します。

ARP 設定を保存するには、[Add] をクリックします。

機能テンプレートを保存するには、[Save] をクリックします。

VRRP の設定

複数のルータがデフォルトゲートウェイの冗長性のために共通の仮想 IP アドレスを共有できるようにする Virtual Router Redundancy Protocol (VRRP) をインターフェイスで実行するには、[VRRP] タブを選択します。次に、[Add New VRRP] をクリックして、次のパラメータを設定します。

パラメータ名	説明
グループ ID (Group ID)	仮想ルータ ID を入力します。これは、仮想ルータの数値識別子です。最大 24 のグループを設定できます。 範囲：1 ~ 255
プライオリティ	ルータの優先度を入力します。最も優先順位が高いルータがプライマリ VRRP ルータとして選択されます。2 つのルータの優先順位が同じ場合、IP アドレスの高い方がプライマリ VRRP ルータとして選択されます。 範囲：1 ~ 254 デフォルト：100
Timer (ミリ秒)	プライマリ VRRP ルータが VRRP アドバタイズメント メッセージを送信する頻度を指定します。下位ルータが 3 回連続して VRRP アドバタイズメントに失敗すると、新しいプライマリ VRRP ルータが選択されます。 範囲：100 ~ 40950 ミリ秒 デフォルト：100 ミリ秒 (注) Cisco IOS XE SD-WAN デバイスの VRRP 機能テンプレートのタイマーが 100 ミリ秒の場合、LAN インターフェイスのトラフィックが多いと VRRP は失敗します。

パラメータ名	説明
Track OMP Track Prefix List	<p>デフォルトでは、VRRPは、どのルータがプライマリ仮想ルータであるかを判別するのに、実行されているサービス（LAN）インターフェイスの状態を使用します。ルータがすべてのWAN制御接続を失った場合、ルータがVRRPに機能的に参加できない場合でも、LANインターフェイスは稼働の状態を示したままになります。VRRPのWAN側の接続を考慮するには、次のいずれかを構成します。</p> <p>[Track OMP] : [On] をクリックすると、VRRPはWAN接続で実行されているオーバーレイ管理プロトコル（OMP）セッションをトラッキングします。プライマリVRRPルータがすべてのOMPセッションを失った場合、VRRPは、少なくとも1つのアクティブなOMPセッションを持つものから新しいデフォルトゲートウェイを選択します。</p> <p>[Track Prefix List] : OMPセッションと、ローカルルータで設定されたプレフィックスリストで定義されているリモートプレフィックスのリストの両方をトラッキングします。プライマリVRRPルータがすべてのOMPセッションを失った場合、[Track OMP] オプションで説明されているように、VRRPフェールオーバーが発生します。さらに、リスト内のすべてのプレフィックスへの到達可能性が失われた場合、VRRPフェールオーバーは、OMPホールドタイマーが期限切れになるのを待たずにすぐに発生するため、ルータがプライマリVRRPルータを決定する間にドロップされるオーバーレイトラフィックの量が最小限に抑えられます。</p>
IP アドレス	仮想ルータのIPアドレスを入力します。このアドレスは、ローカルルータとVRRPを実行しているピアの両方の構成済みインターフェイスIPアドレスとは異なる必要があります。

VRRP のプレフィックスリストを設定する

デバイスおよび機能テンプレートを使用して、VRRPのプレフィックスリストトラッキングを設定できます。プレフィックスリストを設定するには、次の手順を実行します。

1. Cisco vManage のメニューから、**[Configuration]** > **[Policy]** の順に選択します。
2. **[Localized Policy]** をクリックします。
3. **[Custom Options]** ドロップダウンリストから、**[Lists]** をクリックします。
4. 左ペインで **[Prefix]** をクリックし、**[New Prefix List]** をクリックします。
5. **[Prefix List Name]** に、プレフィックスリストの名前を入力します。
6. **[Internet Protocol]** として **[IPv4]** を選択します。
7. **[Add Prefix]** で、プレフィックスエントリをカンマで区切って入力します。
8. **[Add]** をクリックします。

9. [Next] をクリックし、[Forwarding Classes/QoS] を設定します。
10. [Next] をクリックし、[Access Control Lists] を設定します。
11. [Next] をクリックし、[Route Policy] ペインで、関連するルートポリシーを選択して [...] をクリックし、[Edit] をクリックして、新しく追加されたプレフィックスリストを追加します。
12. [Match] ペインで [AS Path List] をクリックし、[Address] で新しく追加されたプレフィックスリストを選択します。
13. [Save Match and Actions] をクリックします。
14. [Next] をクリックし、[Policy Overview] 画面で [Policy Name] と [Policy Description] を入力します。
15. [Save Policy] をクリックします。

デバイステンプレートでの VRRP のプレフィックスリストの設定

デバイステンプレートの VRRP およびローカライズされたポリシーにプレフィックスリストを設定するには、次の手順を実行します。

1. [Cisco vManage] メニューから、[Configuration] > [Templates] を選択します。
2. [Device Template] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

3. 関連するデバイステンプレートを選択して [...] をクリックし、[Edit] をクリックしてテンプレートの詳細を編集します。
4. [Policy] から、新しく追加されたプレフィックスリストを持つポリシーを選択します。
5. [更新 (Update)] をクリックします。
6. [Feature Templates] をクリックします。
7. 関連するデバイステンプレートを選択して [...] をクリックし、[Edit] をクリックしてテンプレートの詳細を編集します。
8. [VRRP] をクリックします。
9. 関連するグループ ID を選択し、ペンアイコンをクリックして、新しいプレフィックスリストを VRRP の詳細に関連付けます。
10. [Track Prefix List] ドロップダウンリストをクリックし、新しく追加されたプレフィックスリスト名を入力します。
11. [Save Changes] をクリックします。

12. [Update] をクリックして変更を保存します。
13. [Device Templates] をクリックし、新しく追加されたプレフィックスリストを持つポリシーを選択します。
14. [...] をクリックして、[Attach Devices] をクリックします。
15. [Available Devices] で、関連するデバイスをダブルクリックして [Selected Devices] に移動し、[Attach] をクリックします。

詳細プロパティの設定

他のインターフェイスプロパティを設定するには、[Advanced] タブを選択し、次のパラメータを設定します。

パラメータ名	説明
デュプレックス	[full] または [half] を選択して、インターフェイスが全二重または半二重のどちらのモードで動作するかを指定します。 デフォルト : full
MAC アドレス	インターフェイスに関連付ける MAC アドレスを、コロン区切りの 16 進表記で指定します。
IP MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。 範囲 : 576 ~ 1804 デフォルト : 1500 バイト
PMTU ディスカバリ	[On] をクリックして、インターフェイスで Path MTU Discovery を有効にします。PMTU は、パケットフラグメンテーションが発生しないように、インターフェイスがサポートする最大の MTU サイズを決定します。
Flow Control	インターフェイス上のデータの送信を一時的に停止するメカニズムである双方向フロー制御の設定を選択します。 値 : autonet、both、egress、ingress、none デフォルト : autoneg
TCP MSS	ルータを通過する TCP SYN パケットの最大セグメントサイズ (MSS) を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。 範囲 : 552 ~ 1460 バイト デフォルト : なし

パラメータ名	説明
速度	<p>接続のリモートエンドが自動ネゴシエーションをサポートしていない場合に使用する、インターフェイスの速度を指定します。</p> <p>値：10、100、1000、または 10000 Mbps</p>
Clear-Dont-Fragment	<p>[On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Don't Fragment (DF) ビットをクリアします。DF ビットがクリアされると、そのインターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。</p> <p>(注) フラグメンテーションが必要で、DF ビットが設定されている場合に、Clear-Dont-Fragment は DF ビットをクリアします。フラグメンテーションを必要としないパケットの場合、DF ビットは影響を受けません。</p>
自動ネゴシエーション	<p>(注) Cisco vManage リリース 20.6.1 より前のリリースでは、フィールドのデフォルト値は [On] です。自動ネゴシエーションをオフにするには、[Off] をクリックします。</p> <p>Cisco vManage リリース 20.6.1 以降、フィールドのデフォルトの動作は次のとおりです。</p> <ul style="list-style-type: none"> ギガビットイーサネット インターフェイス タイプの場合、[Autonegotiation] フィールドはデフォルトで空白になっています。ただし、フィールドが空白の場合、自動ネゴシエーションは [On] に設定されます。 10 ギガビットイーサネットや 100 ギガビットイーサネットなどの他のインターフェイス タイプの場合、[Autonegotiation] フィールドはデフォルトで空白になっています。自動ネゴシエーションをオンまたはオフにするには、それぞれ [On] または [Off] をクリックします。
TLOC Extension	<p>WAN トランスポートに接続する同じルータ上の物理インターフェイスの名前を入力します。次に、この構成により、このサービス側のインターフェイスが WAN トランスポートにバインドされます。それ自体は WAN に直接接続されておらず（通常、サイトには 1 つの WAN 接続しかないため）、同じサイトにあり、このサービス側インターフェイスに接続する 2 番目のルータには、WAN への接続が提供されます。</p> <p>L3 を介した TLOC 拡張は、Cisco IOS XE ルータでのみサポートされることに注意してください。Cisco IOS XE ルータに L3 を介した TLOC 拡張を設定する場合は、L3 インターフェイスの IP アドレスを入力します。</p>
GRE Tunnel Source IP	<p>拡張 WAN インターフェイスの IPv4 アドレスを入力します。</p>

パラメータ名	説明
Xconnect (IOS XE ルータ)	WAN トランスポートに接続する同じルータ上の物理インターフェイスの名前を入力します。

機能テンプレートを保存するには、[Save] をクリックします。

VPN インターフェイスブリッジ

すべての Cisco IOS XE SD-WAN デバイス クラウドおよび Cisco IOS XE SD-WAN デバイスに VPN インターフェイスブリッジテンプレートを使用します。

統合ルーティングおよびブリッジング (IRB) により、異なるブリッジドメイン内の Cisco IOS XE SD-WAN デバイスが相互に通信できます。IRB を有効にするには、ブリッジドメインを VPN に接続する論理 IRB インターフェイスを作成します。VPN は、異なる VLAN 間でトラフィックを交換できるようにするために必要なレイヤ3ルーティングサービスを提供します。各ブリッジドメインは1つの IRB インターフェイスを持つことができ、1つの VPN に接続できます。また、1つの VPN は、Cisco IOS XE SD-WAN デバイス上の複数のブリッジに接続できます。

Cisco vManage テンプレートを使用してブリッジインターフェイスを構成するには、次の手順を実行します。

1. この記事で説明されているように、論理 IRB インターフェイスのパラメータを構成する VPN インターフェイスブリッジ機能テンプレートを作成します。
2. ブリッジドメインのパラメータを設定するには、ブリッジドメインごとにブリッジ機能テンプレートを作成します。ブリッジのヘルプトピックを参照してください。

[Template] 画面に移動し、テンプレートに命名する

1. Cisco vManage メニューから、[Configuration] > [Templates] を選択します。
2. [Device Templates] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

3. [Create Template] ドロップダウンリストから、[From Feature Template] を選択します。
4. [Device Model] ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。
5. [Service VPN] をクリックするか、[Service VPN] セクションまでスクロールします。
6. [Service VPN] ドロップダウンリストをクリックします。

7. [Additional VPN Templates] から、[VPN Interface Bridge] をクリックします。
8. [VPN Interface Bridge] ドロップダウンリストから、[Create Template] をクリックします。
VPN インターフェイスブリッジテンプレートフォームが表示されます。フォームの上部にはテンプレートに名前を付けるためのフィールドがあり、下部には VPN インターフェイスブリッジパラメータを定義するためのフィールドがあります。
9. [Template Name] に、テンプレートの名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。
10. [Template Description] に、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。

初めて機能テンプレートを開くと、デフォルト値を持つパラメータごとに、その範囲が [Default] に設定され（チェックマークで示される）、デフォルト設定またはデフォルト値が表示されます。デフォルト値を変更するか、値を入力するには、パラメータフィールドの左側にある [Scope] ドロップダウンをクリックし、次のいずれかを選択します。

表 10:

パラメータの範囲	範囲の説明
デバイス固有（ホストのアイコンで示される）	<p>デバイス固有の値がパラメータに使用されます。デバイス固有のパラメータの場合、機能テンプレートに値を入力できません。Viptela デバイスをデバイステンプレートに添付するときに、値を入力します。</p> <p>[Device Specific] をクリックすると、[Enter Key] ボックスが表示されます。このボックスには、作成する CSV ファイル内のパラメータを識別する一意の文字列であるキーが表示されます。このファイルは、キーごとに 1 つの列を含む Excel スプレッドシートです。ヘッダー行にはキー名（行ごとに 1 つのキー）が含まれます。その後の各行は、デバイスに対応し、そのデバイスのキーの値を定義します。Viptela デバイスをデバイステンプレートに添付するときに、この CSV ファイルをアップロードします。詳細については、「Create a Template Variables Spreadsheet」を参照してください。</p> <p>デフォルトのキーを変更するには、新しい文字列を入力し、[Enter Key] ボックスの外にカーソルを移動します。</p> <p>デバイス固有のパラメータの例としては、システム IP アドレス、ホスト名、GPS ロケーション、サイト ID があります。</p>
グローバル（地球のアイコンで示される）	<p>パラメータの値を入力し、その値をすべてのデバイスに適用します。</p> <p>デバイスのグループにグローバルに適用できるパラメータの例としては、DNS サーバー、Syslog サーバー、インターフェイス MTU があります。</p>

リリース情報

リリース 15.3 の Cisco vManage NMS で導入されました。リリース 18.2 では、ICMP リダイレクト メッセージを無効にするためのサポートを追加します。

ブリッジング インターフェイスの作成

ブリッジサーバーに使用するインターフェイスを設定するには、[Basic Configuration] を選択し、次のパラメータを設定します。ブリッジを設定する場合、アスタリスクの付いたパラメータは必須です。

表 11:

パラメータ名	説明
Shutdown*	インターフェイスを有効にするには [No] をクリックします。
Interface name*	インターフェイスの名前を irb number の形式で入力します。IRB インターフェイス番号は 1～63 で、IRB が接続されているブリッジドメインのブリッジ機能テンプレートで設定された VPN 識別子と同じである必要があります。
説明	インターフェイスの説明を入力します。
IPv4 Address*	ルータの IPv4 アドレスを入力します。
DHCP ヘルパー	ネットワーク内の DHCP サーバーの IP アドレスをカンマで区切って 8 つまで入力して、インターフェイスを DHCP ヘルパーにします。DHCP ヘルパーインターフェイスは、指定された DHCP サーバーから受信した BOOTP (ブロードキャスト) DHCP 要求を転送します。
Block Non-Source IP	[Yes] をクリックして、トラフィックのソース IP アドレスがインターフェイスの IP プレフィックス範囲と一致する場合にのみ、インターフェイスにトラフィックを転送させます。
セカンダリ IP アドレス (Cisco IOS XE SD-WAN デバイス 上)	[Add] をクリックして、サービス側インターフェイスに最大 4 つのセカンダリ IPv4 アドレスを設定します。

テンプレートを保存するには、[Save] をクリックします。

アクセスリストの適用

アクセスリストの適用

アクセスリストを IRB インターフェイスに適用するには、[ACL] タブを選択し、次のパラメータを設定します。ACL フィルタは、ブリッジドメインの内外で何が許可されるかを決定します。

表 12:

パラメータ名	説明
入力 ACL-IPv4	[On] をクリックし、インターフェイスで受信されるパケットへの IPv4 アクセスリストの名前を指定します。
Egress ACL-IPv4	[On] をクリックして、インターフェイスで送信されるパケットへの IPv4 アクセスリストの名前を指定します。

機能テンプレートを保存するには、[Save] をクリックします。

VRRP の設定

複数のルータがデフォルトゲートウェイの冗長性のために共通の仮想 IP アドレスを共有できるようにする Virtual Router Redundancy Protocol (VRRP) をインターフェイスで実行するには、[VRRP] を選択します。次に、[Add New VRRP] をクリックして、次のパラメータを設定します。

表 13:

パラメータ名	説明
グループ ID (Group ID)	仮想ルータ ID を入力します。これは、仮想ルータの数値識別子です。最大 24 のグループを設定できます。範囲：1 ~ 255
プライオリティ	ルータの優先度を入力します。最も優先順位が高いルータがプライマリ VRRP ルータとして選択されます。2 つの Cisco IOS XE SD-WAN デバイスの優先順位が同じ場合、IP アドレスが大きい方がプライマリ VRRP ルータとして選択されます。範囲：1 ~ 254、デフォルト：100

パラメータ名	説明
Timer (ミリ秒)	<p>プライマリ VRRP ルータが VRRP アドバタイズメント メッセージを送信する頻度を指定します。下位ルータが3回連続して VRRP アドバタイズメントに失敗すると、新しいプライマリ VRRP ルータが選択されます。</p> <p>範囲：100 ～ 40950 ミリ秒</p> <p>デフォルト：100 ミリ秒</p> <p>(注) Cisco IOS XE SD-WAN デバイスの VRRP 機能テンプレートのタイマーが100ミリ秒の場合、LAN インターフェイスのトラフィックが多いと VRRP は失敗します。</p>
Track OMP Track Prefix List	<p>デフォルトでは、VRRP は、どの Cisco IOS XE SD-WAN デバイスがプライマリ仮想ルータであるかを判別するために、VRRP が実行されているサービス (LAN) インターフェイスの状態を使用します。Cisco IOS XE SD-WAN デバイスがすべての WAN 制御接続を失うと、ルータが VRRP に機能的に参加できない場合でも、LAN インターフェイスは稼働の状態を示したままになります。VRRP の WAN 側の接続を考慮するには、次のいずれかを設定します。</p> <p>Track OMP : [On] をクリックすると、VRRP は WAN 接続で実行されているオーバーレイ管理プロトコル (OMP) セッションをトラッキングします。プライマリ VRRP ルータがすべての OMP セッションを失った場合、VRRP は、少なくとも1つのアクティブな OMP セッションを持つものから新しいデフォルトゲートウェイを選択します。</p> <p>Track Prefix List : OMP セッションと、ローカルルータで設定されたプレフィックスリストで定義されているリモートプレフィックスのリストの両方をトラッキングします。プライマリ VRRP ルータがすべての OMP セッションを失った場合、[Track OMP] オプションで説明されているように、VRRP フェールオーバーが発生します。さらに、リスト内のすべてのプレフィックスへの到達可能性が失われた場合、VRRP フェールオーバーは、OMP ホールドタイマーが期限切れになるのを待たずにすぐに発生するため、Cisco IOS XE SD-WAN デバイスがプライマリ VRRP ルータを決定する間にドロップされるオーバーレイトラフィックの量が最小限に抑えられます。</p>
IP アドレス	<p>仮想ルータの IP アドレスを入力します。このアドレスは、ローカル Cisco IOS XE SD-WAN デバイスと VRRP を実行しているピアの両方の設定済みインターフェイス IP アドレスとは異なる必要があります。</p>

VRRP 設定を保存するには、[Add] をクリックします。

機能テンプレートを保存するには、[Save] をクリックします。

ARP テーブルエントリの追加

インターフェイスで静的アドレス解決プロトコル (ARP) テーブルエントリを構成するには、[ARP] を選択します。次に、[Add New ARP] をクリックして、次のパラメータを設定します。

表 14:

パラメータ名	Description
IPアドレス	ARP エントリの IP アドレスをドット付き 10 進表記または完全修飾ホスト名として入力します。
MAC アドレス	MAC アドレスをコロン区切りの 16 進表記で入力します。

ARP 設定を保存するには、[Add] をクリックします。

機能テンプレートを保存するには、[Save] をクリックします。

詳細プロパティの設定

他のインターフェイスプロパティを設定するには、[Advanced] をクリックし、次のパラメータを設定します。

表 15:

パラメータ名	説明
MAC アドレス (MAC Address)	MAC アドレスは、静的または動的に設定できます。静的 MAC アドレスは、ARP 要求を介して学習された動的 MAC アドレスとは対照的に、手動で構成されます。ルータのインターフェイスに静的 MAC を構成するか、ルータのインターフェイスを識別する静的 MAC を指定できます。 インターフェイスに関連付ける MAC アドレスを、コロンで区切った 16 進表記で指定します。
IP MTU	MTU と同様に、IP MTU は IP パケットにのみ影響します。IP パケットが IP MTU を超過すると、パケットはフラグメント化されます。 インターフェイス上のパケットの最大 MTU サイズを指定します。範囲：576 ~ 1804、デフォルト：1500 バイト

パラメータ名	説明
TCP MSS	<p>TCP MSS は、ルータを通過する最初の TCP ヘッダーを含むすべてのパケットに影響します。設定すると、TCPMSSは、スリーウェイハンドシェイクで交換される MSS に対して検査されます。構成された設定がヘッダーのMSSよりも低い場合、ヘッダーのMSSは低くなります。ヘッダー値がすでに低い場合は、変更されずにそのまま通過します。エンドホストは、2つのホストの低い方の設定を使用します。TCP MSS を構成する場合は、最小パス MTU より 40 バイト低く設定する必要があります。</p> <p>Cisco IOS XE SD-WAN デバイス を通過する TPC SYN パケットの最大セグメントサイズ (MSS) を指定します。デフォルトでは、MSSはインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ~ 1460 バイト、デフォルト：なし</p>
Clear-Dont-Fragment	<p>DF ビットが設定されたインターフェイスにパケットが到着する場合は、Clear-Dont-Fragment を設定します。これらのパケットが MTU が許可するサイズよりも大きい場合、それらはドロップされます。DF ビットをクリアすると、パケットはフラグメント化されて送信されます。</p> <p>[On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Don't Fragment (DF) ビットをクリアします。DF ビットがクリアされると、そのインターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。</p> <p>(注) フラグメンテーションが必要で、DF ビットが設定されている場合に、Clear-Dont-Fragment は DF ビットをクリアします。フラグメンテーションを必要としないパケットの場合、DF ビットは影響を受けません。</p>
ARP Timeout	<p>ARP タイムアウトは、ルータで ARP キャッシュを保持する期間を制御します。</p> <p>動的に学習された ARP エントリがタイムアウトするまでの時間を指定します。</p> <p>範囲：0 ~ 2678400 秒 (744 時間) デフォルト：1200 秒 (20 分)</p>
ICMP Redirect	<p>ICMP リダイレクトは、パケットが最適にルーティングされていないときに、ルータによって IP パケットの送信者に送信されます。</p> <p>ICMP リダイレクトは、送信側ホストに対し、後続のパケットを別のゲートウェイ経由で同じ宛先に転送するように通知します。</p> <p>インターフェイスで ICMP リダイレクトメッセージを無効にするには、[Disable] をクリックします。デフォルトでは、インターフェイスは ICMP リダイレクトメッセージを許可します。</p>

機能テンプレートを保存するには、[Save] をクリックします。

VPN インターフェイス DSL IPoE

Cisco IOS XE SD-WAN デバイスの IPoE テンプレートを使用します。

サービスプロバイダーのデジタル加入者線 (DSL) 機能をサポートするには、DSL インターフェイスを備えたルータに IPoE を設定します。

Cisco vManage テンプレートを使用して Cisco IOS XE SD-WAN デバイスに DSL 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。

1. この記事の説明に従って、IP-over-Ethernet インターフェイスのパラメータを設定する VPN インターフェイス DSL IPoE 機能テンプレートを作成します。
2. VPN 機能テンプレートを作成して、VPN パラメータを設定します。VPN のヘルプトピックを参照してください。

[Template] 画面に移動し、テンプレートに命名する

1. Cisco vManage メニューから、[Configuration] > [Templates] を選択します。
2. [Device Templates] をクリックし、[Create Template] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

3. [Create Template] ドロップダウンリストから、[From Feature Template] を選択します。
4. [Device Model] ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。
5. [Transport & Management VPN] をクリックするか、[Transport & Management VPN] セクションまでスクロールします。
6. [Additional VPN 0 Templates] で、[VPN Interface DSL IPoE] をクリックします。
7. [VPN Interface DSL IPoE] ドロップダウンリストから、[Create Template] を選択します。VPN インターフェイス DSL IPoE テンプレートフォームが表示されます。
このフォームには、テンプレートに名前を付けるためのフィールドと、IPoE インターフェイスのパラメータを定義するためのフィールドが含まれています。
8. [Template Name] に、テンプレートの名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。
9. [Template Description] に、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。

初めて機能テンプレートを開くと、デフォルト値を持つパラメータごとに、その範囲が [Default] に設定され (チェックマークで示される)、デフォルト設定またはデフォルト値が表示されます。デフォルト値を変更するか、値を入力するには、[Scope] ドロップダウンリストをクリックし、次のいずれかを選択します。

表 16:

パラメータの範囲	範囲の説明
デバイス固有 (ホストのアイコンで示される)	<p>デバイス固有の値がパラメータに使用されます。デバイス固有のパラメータの場合、機能テンプレートに値を入力できません。Viptela デバイスをデバイステンプレートに添付するときに、値を入力します。</p> <p>[Device Specific] をクリックすると、[Enter Key] ボックスが表示されます。このボックスには、作成する CSV ファイル内のパラメータを識別する一意の文字列であるキーが表示されます。このファイルは、キーごとに 1 つの列を含む Excel スプレッドシートです。ヘッダー行にはキー名 (行ごとに 1 つのキー) が含まれます。その後の各行は、デバイスに対応し、そのデバイスのキーの値を定義します。Viptela デバイスをデバイステンプレートに添付するときに、この CSV ファイルをアップロードします。詳細については、「Create a Template Variables Spreadsheet」を参照してください。</p> <p>デフォルトのキーを変更するには、新しい文字列を入力し、[Enter Key] ボックスの外にカーソルを移動します。</p> <p>デバイス固有のパラメータの例としては、システム IP アドレス、ホスト名、GPS ロケーション、サイト ID などがあります。</p>
グローバル (地球のアイコンで示される)	<p>パラメータの値を入力し、その値をすべてのデバイスに適用します。</p> <p>デバイスのグループにグローバルに適用できるパラメータの例としては、DNS サーバー、Syslog サーバー、インターフェイス MTU などがあります。</p>

IPoE 機能の設定

基本的な IPoE 機能を設定するには、[Basic Configuration] をクリックして、次のパラメータを設定します。必須パラメータはアスタリスクで示されています。

表 17:

パラメータ名	説明
Shutdown*	[No] をクリックして、VDSL コントローラ インターフェイスを有効にします。
Controller VDSL Slot*	コントローラ VDSL インターフェイスのスロット番号を、slot/subslot/port の形式で入力します (たとえば、0/2/0)。

パラメータ名	説明
Mode*	ドロップダウンから VDSL コントローラの動作モードを選択します。 <ul style="list-style-type: none"> • Auto : デフォルトのモード。 • ADSL1 : ITU G.992.1 Annex A フルレートモードを使用します。これは、1.3 Mbps のダウンストリームレートと 1.8 Mbps のアップストリームレートを提供します。 • ADSL2 : ITU G.992.3 Annex A、Annex L、および Annex M を使用します。これは、12 Mbps のダウンストリームレートと 1.3 Mbps のアップストリームレートを提供します。 • ADSL2+ : ITU G.992.5 Annex A および Annex M を使用します。これは、24 Mbps のダウンストリームレートと 3.3 Mbps のアップストリームレートを提供します。 • ANSI : ITU G.991.1、G.992.3、および G.992.5 (Annex A および Annex M) で定義されている ADSL2/2+ モード、および ITU-T G.993.2 で定義されている VDSL2 モードで動作します。 • VDSL2 : ITU-T G.993.2 で定義されている VDSL2 モードで動作します。これは、最大 30 MHz の周波数を使用して、200 Mbps のダウンストリームレートと 100 Mbps のアップストリームレートを提供します。
VDSL モデムの設定	NIM モジュールの DSL モデムに送信するコマンドを入力します。コマンドが有効な場合、コマンドが実行され、結果が Cisco vManage NMS に返されます。コマンドが有効でない場合、コマンドは実行されません。
SRA	[Yes] をクリックして、インターフェイスでのシームレスなレート調整を有効にします。SRA は、現在の回線状態に基づいて回線速度を調整します。

機能テンプレートを保存するには、[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

PPPoE を使用してイーサネット インターフェイスを設定すると、LAN 上の複数のユーザーをリモートサイトに接続できます。VDSL コントローラでイーサネット インターフェイスを設定するには、[Ethernet] をクリックして、次のパラメータを設定します。すべてのパラメータを設定する必要があります。

表 18:

パラメータ名	説明
Ethernet Interface Name	イーサネット インターフェイスの名前を <i>subslot/port</i> の形式で入力します (例: 2/0)。スロット番号は常に 0 であるため、入力する必要はありません。

パラメータ名	説明
VLAN ID	イーサネット インターフェイスの VLAN 識別子を入力します。
説明	インターフェイスの説明を入力します。
Dynamic/Static	動的または静的 IPv4 アドレスをイーサネット インターフェイスに割り当てます。
IPv4 Address	イーサネット インターフェイスの静的 IPv4 アドレスを入力します。
DHCP ヘルパー	ネットワーク内の DHCP サーバーの IP アドレスをカンマで区切って 8 つまで入力して、インターフェイスを DHCP ヘルパーにします。DHCP ヘルパーインターフェイスは、指定された DHCP サーバーから受信した BOOTP (ブロードキャスト) DHCP 要求を転送します。

機能テンプレートを保存するには、[Save] をクリックします。

トンネルインターフェイスの作成

IOS XE ルータでは、最大 4 つのトンネルインターフェイスを設定できます。つまり、各ルータに最大 4 つの TLOC を設定できます。

オーバーレイネットワークが機能できるようにコントロールプレーンがそれ自体を確立するには、VPN 0 で WAN トランスポート インターフェイスを設定する必要があります。

マルチリンク インターフェイスのトンネルインターフェイスを設定するには、[Tunnel Interface] タブを選択し、次のパラメータを設定します。

表 19:

パラメータ名	説明
トンネルインターフェイス	[On] をクリックして、トンネルインターフェイスを作成します。
色	TLOC の色を選択します。

パラメータ名	説明
制御接続	<p>デフォルトでは、制御接続は [On] に設定されており、TLOC の制御接続を確立します。ルータに複数の TLOC がある場合は、[No] をクリックして、トンネルが TLOC の制御接続を確立しないようにします。</p> <p>(注) 接続トラフィックでのデータ/パケットの損失を避けるために、デフォルトの 10 ミリ秒の hello-interval と 12 秒の hello-tolerance パラメータを設定して、650 ~ 700 Kbps 以上の帯域幅を設定することをお勧めします。</p> <p>BFD セッションごとに、175 バイトの追加の平均サイズ BFD パケットは、1.4 Kbps の帯域幅を消費します。</p> <p>双方向 BFD パケットフローに必要な帯域幅の計算例を以下に示します。</p> <ul style="list-style-type: none"> • 制御接続用にデバイスごとに 650 ~ 700 Kbps。 • デバイス上の BFD セッション (要求) ごとに 175 バイト (または 1.4 Kbps) • デバイス上の BFD セッション (応答) ごとに 175 バイト (または 1.4 Kbps) <p>パス MTU ディスカバリ (PMTUD) が有効になっている場合、30 秒ごと、トンネルごとに BFD パケットを送受信するための帯域幅：</p> <p>1500 バイトの BFD 要求パケットは、30 秒ごと、トンネルごとに送信されます。</p> <p>1500 バイト * 8 ビット/1 バイト * 1 パケット/30 秒 = 400 bps (要求)</p> <p>147 バイトの BFD パケットが応答として送信されます。</p> <p>147 バイト * 8 ビット/1 バイト * 1 パケット/30 秒 = 40 bps (応答)</p> <p>したがって、たとえば 775 BFD セッションを持つデバイスの場合、次の帯域幅が必要です。</p> <p>700k + (1.4k*775) + (400*775) + (1.4k*775) + (40*775) = ~ 3.5 MBps</p>
最大制御接続数	<p>WAN トンネルインターフェイスが接続できる Cisco vSmart コントローラの最大数を指定します。トンネルが制御接続を確立しないようにするには、この数値を 0 に設定します。</p> <p>範囲 : 0 ~ 8。デフォルト : 2</p>

パラメータ名	説明
Cisco vBond オーケストレーション As STUN Server	[On] をクリックして NAT (STUN) のセッション トラバーサル ユーティリティを有効にし、ルータが NAT の背後にある場合にトンネルインターフェイスがパブリック IP アドレスとポート番号を検出できるようにします。
コントローラグループリストの除外	トンネルインターフェイスの接続を許可しない Cisco vSmart コントローラを設定します。範囲：0 ～ 100
Cisco vManage Connection Preference	トンネルインターフェイスを使用して Cisco vManage NMS と制御トラフィックを交換するための優先順位を設定します。範囲：0 ～ 8。デフォルト：5
ポートホップ	ポートホッピングを有効にするには [On] をクリックし、無効にするには [Off] をクリックします。ルータが NAT の背後にある場合、ポートホッピングは、事前に選択された OMP ポート番号 (ベースポートと呼ばれる) のプールを循環して、接続の試行が失敗したときに他のルータとの DTLS 接続を確立します。デフォルトのベースポートは 12346、12366、12386、12406、および 12426 です。ベースポートを変更するには、ポートオフセット値を設定します。デフォルト：有効
低帯域幅リンク	トンネルインターフェイスの特性を低帯域幅リンクにする場合に選択します。
TCP MSS	<p>TCP MSS は、ルータを通過する最初の TCP ヘッダーを含むすべてのパケットに影響します。設定すると、TCP MSS は 3 ウェイハンドシェイクで交換される MSS と比較されます。構成済みの TCP MSS 設定がヘッダーの MSS よりも小さい場合、ヘッダーの MSS の値が減少します。MSS ヘッダー値がすでに TCP MSS よりも小さい場合、パケットは変更されずに通過します。トンネルの終端にあるホストは、2つのホストの小さい方の設定を使用します。TCP MSS を設定する場合は、最小パス MTU より 40 バイト小さく設定する必要があります。</p> <p>Cisco IOS XE SD-WAN デバイス を通過する TCP SYN パケットの MSS を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ～ 1460 バイト、デフォルト：なし</p>

パラメータ名	説明
Clear-Dont-Fragment	<p>Don't Fragment が設定されているインターフェイスに到着するパケットの [Clear-Dont-Fragment] を設定します。これらのパケットが MTU が許可するサイズより大きい場合、それらはドロップされます。Don't Fragment ビットをクリアすると、パケットはフラグメント化されて送信されます。</p> <p>[On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Dont Fragment ビットをクリアします。Dont Fragment ビットがクリアされると、インターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。</p> <p>(注) [Clear-Dont-Fragment] は Dont Fragment ビットをクリアし、Dont Fragment ビットが設定されます。フラグメンテーションを必要としないパケットの場合、Dont Fragment ビットは影響を受けません。</p>
サービスの許可	サービスごとに [On] または [Off] を選択して、インターフェイスでサービスを許可または禁止します。

追加のトンネルインターフェイスパラメータを設定するには、[Advanced Options] をクリックして、次のパラメータを設定します。

表 20:

パラメータ名	説明
GRE	<p>トンネルインターフェイスで GRE カプセル化を使用します。デフォルトでは、GRE は無効になっています。</p> <p>IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。</p>
IPSec	<p>トンネルインターフェイスで IPsec カプセル化を使用します。デフォルトでは、IPsec が有効になっています。</p> <p>IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。</p>
IPsec Preference	<p>トラフィックをトンネルに送信するための優先値を指定します。高い値が低い値に優先します。</p> <p>範囲：0 ~ 4294967295、デフォルト：0</p>

パラメータ名	説明
IPsec Weight	<p>複数の TLOC 間でトラフィックのバランスをとるために使用する重みを入力します。値が大きいほど、より多くのトラフィックがトンネルに送信されます。</p> <p>範囲：1 ～ 255、デフォルト：1</p>
通信事業者	<p>トンネルに関連付けるキャリア名またはプライベートネットワーク識別子を選択します。</p> <p>値：carrier1、carrier2、carrier3、carrier4、carrier5、carrier6、carrier7、carrier8、default、デフォルト：default</p>
ループバックトンネルのバインド	<p>ループバック インターフェイスにバインドする物理インターフェイスの名前を入力します。</p>
ラストリゾート回線	<p>トンネルインターフェイスをラストリゾート回線として使用する場合に選択します。</p> <p>(注) ラストリゾート回線として設定されたインターフェイスはダウン状態になるため、制御接続の数の計算中にスキップされ、セルラーモデムは休止状態になり、トラフィックはこの回線経由で送信されません。</p> <p>セルラーインターフェイスを備えたエッジデバイスで設定がアクティブ化されると、すべてのインターフェイスが制御および BFD 接続を確立するプロセスを開始します。1つまたは複数のプライマリインターフェイスが BFD 接続を確立すると、ラストリゾート回線は自動的にシャットダウンします。</p> <p>すべてのプライマリインターフェイスがリモートエッジへの接続を失った場合にのみ、ラストリゾート回線がアクティブになり、エッジデバイスで BFD TLOC ダウンアラームと制御 TLOC ダウンアラームがトリガーされます。ラストリゾートインターフェイスは、エッジデバイスのバックアップ回線として使用され、他のすべてのトランスポートリンク BFD セッションが失敗したときにアクティブ化されます。このモードでは、無線インターフェイスはオフになり、セルラーインターフェイスを介した制御またはデータ接続は存在しません。</p>
NAT 更新間隔	<p>DTLS または TLS WAN トランスポート接続で送信される NAT リフレッシュパケットの間隔を入力します。範囲：1 ～ 60 秒、デフォルト：5 秒</p>
Hello 間隔 (Hello Interval)	<p>DTLS または TLS WAN トランスポート接続で送信される Hello パケットの間隔を入力します。範囲：100 ～ 10000 ミリ秒、デフォルト：1000 ミリ秒 (1 秒)</p>

パラメータ名	説明
Hello 許容度	トランスポートトンネルのダウンを宣言する前に、DTLSまたはTLSWANトランスポート接続でHello パケットを待機する時間を入力します。 範囲：12 ～ 60 秒、デフォルト：12 秒

インターフェイスを NAT デバイスとして設定する

ポート転送などのアプリケーションの NAT デバイスとして機能するようにインターフェイスを設定するには、[NAT]をクリックし、[On]をクリックして、次のパラメータを設定します。

表 21:

パラメータ名	説明
NAT	[On] をクリックして、インターフェイスを NAT デバイスとして機能させます。
Refresh Mode	NAT マッピングを更新する方法（アウトバウンドまたは双方向（アウトバウンドとインバウンド）のいずれか）を選択します。デフォルト：アウトバウンド
[UDP Timeout]	UDP セッションを介した NAT 変換がいつタイムアウトするかを指定します。範囲：1 ～ 65536 分、デフォルト：1 分
[TCP Timeout]	TCP セッションを介した NAT 変換がいつタイムアウトするかを指定します。範囲：1 ～ 65536 分、デフォルト：60 分（1 時間）
Block ICMP	[On] を選択して、インバウンド ICMP エラーメッセージをブロックします。デフォルトでは、NAT デバイスとして機能するルータは、これらのエラーメッセージを受け取ります。デフォルト：Off
Respond to Ping	接続のパブリック側から受信した NAT インターフェイスの IP アドレスへの ping 要求にルータが応答するようにするには、[On] を選択します。

ポート転送ルールを作成するには、[Add New Port Forwarding Rule] をクリックし、次のパラメータを設定します。最大128のポート転送ルールを定義して、外部ネットワークからの要求が内部ネットワーク上のデバイスに到達できるようにすることができます。

表 22:

パラメータ名	説明
Port Start Range	ポート番号を入力して、ポートまたは対象の範囲の最初のポートを定義します。範囲：0 ～ 65535
Port End Range	同じポート番号を入力してポート転送を1つのポートに適用するか、より大きい番号を入力してポートの範囲に適用します。範囲：0 ～ 65535

パラメータ名	説明
プロトコル	ポート転送ルールを適用するプロトコル ([TCP] または [UDP]) を選択します。TCP トラフィックと UDP トラフィックの両方で同じポートを一致させるには、2つのルールを構成します。
VPN	内部サーバーが存在するプライベート VPN を指定します。この VPN は、オーバーレイネットワークの VPN 識別子の 1 つです。範囲：0 ～ 65530
プライベート IP	ポート転送ルールに一致するトラフィックの転送先となる内部サーバーの IP アドレスを指定します。

ポート転送ルールを保存するには、[Add] をクリックします。

機能テンプレートを保存するには、[Save] をクリックします。

アクセスリストの適用

ACL を設定して、どのトラフィックが QoS を利用するかを選択します。ルータインターフェイスに書き換えルール、アクセスリスト、およびポリサーを適用するには、[ACL] タブを選択し、次のパラメータを設定します。

表 23:

パラメータ名	説明
Shaping rate	インターフェイスの集約トラフィック転送速度を、回線速度よりも低く設定します (キロビット/秒 (kbps) 単位)。
QoS マップ	インターフェイスから送信されるパケットに適用する QoS マップの名前を指定します。
リライトルール	[On] をクリックし、インターフェイスに適用する書き換えルールの名前を指定します。
入力 ACL – IPv4	[On] をクリックして、インターフェイスで受信される IPv4 パケットに適用するアクセスリストの名前を指定します。
出力 ACL – IPv4	[On] をクリックし、インターフェイスで送信される IPv4 パケットに適用するアクセスリストの名前を指定します。
入力 ACL – IPv6	[On] をクリックして、インターフェイスで受信される IPv6 パケットに適用するアクセスリストの名前を指定します。
出力 ACL – IPv6	[On] をクリックし、インターフェイスで送信される IPv6 パケットに適用するアクセスリストの名前を指定します。
入力ポリサー	[On] をクリックして、インターフェイスで受信されるパケットに適用するポリサーの名前を指定します。

パラメータ名	説明
出力ポリサー	[On]をクリックして、インターフェイスで送信されるパケットに適用するポリサーの名前を指定します。

機能テンプレートを保存するには、[Save]をクリックします。

その他のインターフェイスプロパティの設定

他のインターフェイスプロパティを設定するには、[Advanced]タブを選択し、次のプロパティを設定します。

表 24:

パラメータ名	説明
Bandwidth Upstream	WAN トランスポート VPN (VPN 0) の物理インターフェイスで送信されるトラフィックの帯域幅が特定の制限を 85% 超えると (Cisco IOS XE SD-WAN デバイス および Cisco vManage NMS のみ)、Bandwidth Upstream により通知が発行されます 送信トラフィックについて、通知を生成する帯域幅を設定します。範囲：1 ~ $(2^{32}/2) - 1$ kbps
Bandwidth Downstream	WAN トランスポート VPN (VPN 0) の物理インターフェイスで受信されるトラフィックの帯域幅が特定の制限を 85% 超えると (Cisco IOS XE SD-WAN デバイス および Cisco vManage NMS のみ)、Bandwidth Downstream により通知が発行されます 受信トラフィックについて、通知を生成する帯域幅を設定します。範囲：1 ~ $(2^{32}/2) - 1$ kbps
IP MTU	IP MTU は IP パケットに影響します。IP パケットが IP MTU を超過すると、パケットはフラグメント化されます。 インターフェイス上のパケットの最大 MTU サイズを指定します。範囲：576 ~ 1804、デフォルト：1500 バイト
TCP MSS	単一の TCP/IPv4 データグラムでは、TCP の最大セグメントサイズ (MSS) は、ホストが受け入れる最大データを定義します。この TCP/IPv4 データグラムは、IPv4 レイヤでフラグメント化されている可能性があります。MSS 値は、TCP SYN セグメント内でのみ TCP ヘッダー オプションとして送信されます。 ルータを通過する TPC SYN パケットの最大セグメントサイズ (MSS) を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ~ 1460 バイト、デフォルト：なし

パラメータ名	説明
TLOC Extension	<p>TLOC 拡張機能を使用してインターフェイスをバインドし、同じ物理サイトにある別の Cisco IOS XE SD-WAN デバイスをローカルルータの WAN トランスポート インターフェイスに接続します (Cisco IOS XE SD-WAN デバイスのみ)。</p> <p>WAN トランスポート回線に接続する同じルータ上の物理インターフェイスの名前を入力します。次に、この構成により、このサービス側のインターフェイスが WAN トランスポートにバインドされます。それ自体は WAN に直接接続されておらず (通常、サイトには 1 つの WAN 接続しかないため)、同じサイトにあり、このサービス側インターフェイスに接続する 2 番目のルータには、WAN への接続が提供されます。</p>
Tracker	<p>インターフェイスステータスのトラッキングは、VPN 0 のトランスポート インターフェイスで NAT を有効にして、最初にデータセンターのルータにアクセスするのではなく、ルータからのデータトラフィックが直接インターネットに出られるようにする場合に役立ちます。この状況では、トランスポート インターフェイスで NAT を有効にすると、ローカルルータとデータセンター間の TLOC が 2 つに分割され、1 つはリモートルータに、もう 1 つはインターネットに送られます。</p> <p>トランスポート トンネルトラッキングを有効にすると、ソフトウェアはインターネットへのパスを定期的に調べて、インターネットが稼働しているかどうかを判断します。このパスがダウンしていることをソフトウェアが検出すると、インターネットの宛先へのルートが撤回され、インターネットに向かうトラフィックはデータセンターのルータを介してルーティングされます。インターネットへのパスが再び機能していることをソフトウェアが検出すると、インターネットへのルートが再インストールされます。</p> <p>インターネットに接続するトランスポート インターフェイスのステータスをトラッキングするトラッカーの名前を入力します。</p>

パラメータ名	説明
IP Directed-Broadcast	<p>IP ダイレクトブロードキャストは、宛先アドレスが何らかの IP サブネットの有効なブロードキャスト アドレスであるにもかかわらず、その宛先サブネットに含まれないノードから発信される IP パケットです。</p> <p>宛先サブネットに直接接続されていないデバイスは、そのサブネット上のホストを宛先とするユニキャスト IP パケットを転送する場合と同じ方法で IP ダイレクトブロードキャストを転送します。ダイレクトブロードキャストパケットが、宛先サブネットに直接接続されたデバイスに到着すると、そのパケットはその宛先サブネット上でブロードキャストされます。パケットの IP ヘッダー内の宛先アドレスはそのサブネットに設定された IP ブロードキャスト アドレスに書き換えられ、パケットはリンク層ブロードキャストとして送信されます。</p> <p>あるインターフェイスでダイレクトブロードキャストがイネーブルになっている場合、着信した IP パケットが、そのアドレスに基づいて、そのインターフェイスが接続されているサブネットを対象とするダイレクトブロードキャストとして識別されると、そのパケットはそのサブネット上でブロードキャストされます。</p>

機能テンプレートを保存するには、[Save] をクリックします。

リリース情報

リリース 18.4.1 の Cisco vManage NMS で導入されました。

VPN インターフェイス DSL PPPoA

サービスプロバイダーのデジタル加入者線 (DSL) 機能をサポートするには、DSL NIM モジュールを備えたルータに PPP-over-ATM インターフェイスを設定します。

Cisco IOS XE SD-WAN デバイスの VPN インターフェイス DSL PPPoA テンプレートを使用します。

サービスプロバイダーのデジタル加入者線 (DSL) 機能をサポートするには、DSL NIM モジュールを備えたルータに PPP-over-ATM インターフェイスを設定します。

Cisco vManage テンプレートを使用して Cisco ルータに DSL 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。

1. この記事の説明に従って、VPN インターフェイス DSL PPPoA 機能テンプレートを作成して、ATM インターフェイスパラメータを設定します。
2. VPN 機能テンプレートを作成して、VPN パラメータを設定します。VPN のヘルプトピックを参照してください。

[Template] 画面に移動し、テンプレートに命名する

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. **[Device Templates]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Device Templates]** のタイトルは **[Device]** です。

3. **[Create Template]** ドロップダウンリストから、**[From Feature Template]** を選択します。
4. **[Device Model]** ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。
5. **[Transport & Management VPN]** をクリックするか、**[Transport & Management VPN]** セクションまでスクロールします。
6. **[Additional VPN 0 Templates]** で、**[VPN Interface DSL PPPoA]** をクリックします。
7. **[VPN Interface DSL PPPoA]** ドロップダウンリストから、**[Create Template]** をクリックします。VPN インターフェイス DSL PPPoA テンプレートフォームが表示されます。このフォームには、テンプレートに名前を付けるためのフィールドと、VPN インターフェイス PPP のパラメータを定義するためのフィールドが含まれています。
8. **[Template Name]** に、テンプレートの名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。
9. **[Template Description]** に、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。

初めて機能テンプレートを開くと、デフォルト値を持つパラメータごとに、その範囲が **[Default]** に設定され (チェックマークで示される)、デフォルト設定またはデフォルト値が表示されます。デフォルト値を変更するか、値を入力するには、パラメータフィールドの左側にある **[Scope]** ドロップダウンをクリックし、次のいずれかを選択します。

表 25:

パラメータの範囲	範囲の説明
デバイス固有 (ホストのアイコンで示される)	<p>デバイス固有の値がパラメータに使用されます。デバイス固有のパラメータの場合、機能テンプレートに値を入力できません。Viptela デバイスをデバイステンプレートに添付するときに、値を入力します。</p> <p>[Device Specific] をクリックすると、[Enter Key] ボックスが表示されます。このボックスには、作成する CSV ファイル内のパラメータを識別する一意の文字列であるキーが表示されます。このファイルは、キーごとに1つの列を含む Excel スプレッドシートです。ヘッダー行にはキー名 (行ごとに1つのキー) が含まれます。その後の各行は、デバイスに対応し、そのデバイスのキーの値を定義します。Viptela デバイスをデバイステンプレートに添付するときに、この CSV ファイルをアップロードします。詳細については、「Create a Template Variables Spreadsheet」を参照してください。</p> <p>デフォルトのキーを変更するには、新しい文字列を入力し、[Enter Key] ボックスの外にカーソルを移動します。</p> <p>デバイス固有のパラメータの例としては、システム IP アドレス、ホスト名、GPS ロケーション、サイト ID があります。</p>
グローバル (地球のアイコンで示される)	<p>パラメータの値を入力し、その値をすべてのデバイスに適用します。</p> <p>デバイスのグループにグローバルに適用できるパラメータの例としては、DNS サーバー、Syslog サーバー、インターフェイス MTU があります。</p>

VDSL コントローラ機能の構成

VPN の基本的な VDSL コントローラ機能を設定するには、[Basic Configuration] を選択し、次のパラメータを設定します。必須パラメータはアスタリスクで示されています。

表 26:

パラメータ名	説明
Shutdown*	[No] をクリックして、VDSL コントローラ インターフェイスを有効にします。
Controller VDSL Slot*	コントローラ VDSL インターフェイスのスロット番号を、slot/subslot/port の形式で入力します (たとえば、0/2/0)。

パラメータ名	説明
Mode*	<p>ドロップダウンから VDSL コントローラの動作モードを選択します。</p> <ul style="list-style-type: none"> • [Auto] : デフォルトのモード。 • [ADSL1] : ITU G.992.1 Annex A フルレートモードを使用します。これは、1.3 Mbps のダウンストリームレートと 1.8 Mbps のアップストリームレートを提供します。 • [ADSL2] : ITU G.992.3 Annex A、Annex L、および Annex M を使用します。これは、12 Mbps のダウンストリームレートと 1.3 Mbps のアップストリームレートを提供します。 • [ADSL2+] : ITU G.992.5 Annex A および Annex M を使用します。これは、24 Mbps のダウンストリームレートと 3.3 Mbps のアップストリームレートを提供します。 • ANSI : ITU G.991.1、G.992.3、および G.992.5 (Annex A および Annex M) で定義されている ADSL2/2+ モード、および ITU-T G.993.2 で定義されている VDSL2 モードで動作します。 • VDSL2 : ITU-T G.993.2 で定義されている VDSL2 モードで動作します。これは、最大 30 MHz の周波数を使用して、200 Mbps のダウンストリームレートと 100 Mbps のアップストリームレートを提供します。
VDSL モデムの設定	NIM モジュールの DSL モデムに送信するコマンドを入力します。コマンドが有効な場合、コマンドが実行され、結果が Cisco vManage NMS に返されます。コマンドが有効でない場合、コマンドは実行されません。
SRA	デフォルトでは有効になっています。[No] をクリックして、インターフェイスでのシームレスなレート調整を無効にします。SRA は、現在の回線状態に基づいて回線速度を調整します。

機能テンプレートを保存するには、[Save] をクリックします。

ATM インターフェイスの設定

VDSL コントローラで ATM インターフェイスを設定するには、[ATM] を選択し、次のパラメータを設定します。すべてのパラメータを設定する必要があります。

表 27:

パラメータ名	説明
ATM Interface Name	ATM インターフェイスの名前を <i>subslot/port</i> の形式で入力します (例: 2/0)。スロット番号は常に 0 であるため、入力する必要はありません。
説明	インターフェイスの説明を入力します。

パラメータ名	説明
VPI and VCI	ATM 相手先固定接続 (PVC) を <i>vpi/vci</i> の形式で作成します。仮想パス識別子 (VPI) および仮想チャネル識別子 (VCI) の値を入力します。
カプセル化	ATM PVC で使用する ATM アダプテーション層 (AAL) およびカプセル化のタイプをドロップダウンから選択します。 <ul style="list-style-type: none"> • AAL5 MUX : PVC を単一のプロトコル専用にします。 • AAL5 NLPID : NLPID 多重化を使用します。 • AAL5 SNAP : 同じ PVC で 2 つ以上のプロトコルを多重化します。
Dialer Pool Member	インターフェイスが属するダイヤラプールの番号を入力します。1 ~ 255 の値を指定できます。
VBR-NRT	可変ビットレート非リアルタイムパラメータを設定します。 <ul style="list-style-type: none"> • Peak Cell Rate : 48 ~ 25000 Kbps の値を入力します。 • Sustainable Cell Rate : 持続可能なセルレートを Kbps で入力します。 • Maximum Burst Size : このサイズは 1 セルです。
VBR-RT	可変ビットレートリアルタイムパラメータを設定します。 <ul style="list-style-type: none"> • Peak Cell Rate : 48 ~ 25000 Kbps の値を入力します。 • Average Cell Rate : 平均セルレートを Kbps で入力します。 • Maximum Burst Size : このサイズは 1 セルです。

機能テンプレートを保存するには、[Save] をクリックします。

PPP 認証プロトコルの構成

PPP 認証プロトコルを構成するには、[PPP] を選択し、次のパラメータを設定します。

表 28:

パラメータ名	説明
認証プロトコル (Authentication Protocol)	MLP で使用される認証プロトコルを選択します。 <ul style="list-style-type: none"> • CHAP : インターネット サービス プロバイダー (ISP) から提供されたホスト名とパスワードを入力します。ホスト名は最大 255 文字です。 • PAP : ISP から提供されたユーザー名とパスワードを入力します。ユーザー名は最大 255 文字です。 • PAP および CHAP : 両方の認証プロトコルを設定します。それぞれのプロトコルのログイン情報を入力します。両方に同じユーザー名とパスワードを使用するには、[Same Credentials for PAP and CHAP] をクリックします。

機能テンプレートを保存するには、[Save] をクリックします。

トンネルインターフェイスの作成

Cisco IOS XE SD-WAN デバイスでは、最大 4 つのトンネルインターフェイスを設定できます。つまり、各 Cisco IOS XE SD-WAN デバイスに最大 4 つの TLOC を設定できます。

オーバーレイネットワークが機能できるようにコントロールプレーンがそれ自体を確立するには、VPN 0 で WAN トランスポートインターフェイスを設定する必要があります。

マルチリンク インターフェイスのトンネルインターフェイスを設定するには、[Tunnel Interface] を選択し、次のパラメータを設定します。

表 29:

パラメータ名	説明
トンネルインターフェイス	[On] をクリックして、トンネルインターフェイスを作成します。
色	TLOC の色を選択します。
制御接続	Cisco IOS XE SD-WAN デバイスに複数の TLOC がある場合は、[No] をクリックして、トンネルが TLOC を確立しないようにします。デフォルトは [On] で、TLOC の制御接続を確立します。 (注) データをドロップしない制御接続トラフィックの場合、hello-interval (10) および hello-tolerance (12) にデフォルトのパラメータを設定した、650 ~ 700 kbps 以上の帯域幅をお勧めします。

パラメータ名	説明
最大制御接続数	WAN トンネルインターフェイスが接続できる Cisco vSmart コントローラの最大数を指定します。トンネルが制御接続を確立しないようにするには、この数値を 0 に設定します。 範囲：0～8、デフォルト：2
Cisco vBond オーケストレーション As STUN Server	Session Traversal Utilities for NAT (STUN) を有効にし、Cisco IOS XE SD-WAN デバイスが NAT の背後にある場合に、トンネルインターフェイスでそのパブリック IP アドレスとポート番号を検出できるようにする場合は、[On] をクリックします。
コントローラグループリストの除外	トンネルインターフェイスの接続を許可しない Cisco vSmart コントローラを設定します。範囲：0～100
Cisco vManage Connection Preference	トンネルインターフェイスを使用して Cisco vManage NMS と制御トラフィックを交換するための優先順位を設定します。範囲：0～8、デフォルト：5
ポートホップ	ポートホッピングを有効にするには [On] をクリックし、無効にするには [Off] をクリックします。ルータが NAT の背後にある場合、ポートホッピングは、事前に選択された OMP ポート番号（ベースポートと呼ばれる）のプールを循環して、接続の試行が失敗したときに他のルータとの DTLS 接続を確立します。デフォルトのベースポートは 12346、12366、12386、12406、および 12426 です。ベースポートを変更するには、ポートオフセット値を設定します。デフォルト：有効
低帯域幅リンク	トンネルインターフェイスの特性を低帯域幅リンクにする場合に選択します。
トンネル TCP MSS	TCP MSS は、ルータを通過する最初の TCP ヘッダーを含むすべてのパケットに影響します。設定すると、TCP MSS は 3 ウェイハンドシェイクで交換される MSS と比較されます。構成済みの TCP MSS 設定がヘッダーの MSS よりも小さい場合、ヘッダーの MSS の値が減少します。MSS ヘッダー値がすでに TCP MSS よりも小さい場合、パケットは変更されずに通過します。トンネルの終端にあるホストは、2つのホストの小さい方の設定を使用します。TCP MSS を設定する場合は、最小パス MTU より 40 バイト小さく設定する必要があります。 Cisco IOS XE SD-WAN デバイスを通過する TCP SYN パケットの MSS を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552～1460 バイト、デフォルト：なし

パラメータ名	説明
Clear-Dont-Fragment	<p>Don't Fragment が設定されているインターフェイスに到着するパケットの [Clear-Dont-Fragment] を設定します。これらのパケットが MTU が許可するサイズより大きい場合、それらはドロップされます。Don't Fragment ビットをクリアすると、パケットはフラグメント化されて送信されます。</p> <p>[On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Dont Fragment ビットをクリアします。Dont Fragment ビットがクリアされると、インターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。</p> <p>(注) [Clear-Dont-Fragment] は Dont Fragment ビットをクリアし、Dont Fragment ビットが設定されます。フラグメンテーションを必要としないパケットの場合、Dont Fragment ビットは影響を受けません。</p>
サービスの許可	サービスごとに [On] または [Off] を選択して、インターフェイスでサービスを許可または禁止します。

追加のトンネルインターフェイスパラメータを設定するには、[Advanced Options] をクリックして、次のパラメータを設定します。

表 30:

パラメータ名	説明
GRE	<p>トンネルインターフェイスで GRE カプセル化を使用します。デフォルトでは、GRE は無効になっています。</p> <p>IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。</p>
IPSec	<p>トンネルインターフェイスで IPsec カプセル化を使用します。デフォルトでは、IPsec が有効になっています。</p> <p>IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。</p>
IPsec Preference	<p>トラフィックをトンネルに送信するための優先値を指定します。高い値が低い値に優先します。</p> <p>範囲：0 ~ 4294967295。デフォルト：0</p>

パラメータ名	説明
IPsec Weight	<p>複数の TLOC 間でトラフィックのバランスをとるために使用する重みを入力します。値が大きいほど、より多くのトラフィックがトンネルに送信されます。</p> <p>範囲：1～255。デフォルト：1</p>
通信事業者	<p>トンネルに関連付けるキャリア名またはプライベートネットワーク識別子を選択します。</p> <p>値：carrier1、carrier2、carrier3、carrier4、carrier5、carrier6、carrier7、carrier8、デフォルト。デフォルト：デフォルト</p>
ループバックトンネルのバインド	<p>ループバック インターフェイスにバインドする物理インターフェイスの名前を入力します。</p>
ラストリゾート回線	<p>トンネルインターフェイスをラストリゾート回線として使用する場合に選択します。</p> <p>(注) ラストリゾート回線として設定されたインターフェイスはダウン状態になるため、制御接続の数の計算中にスキップされ、セルラーモデムは休止状態になり、トラフィックはこの回線経由で送信されません。</p> <p>セルラーインターフェイスを備えたエッジデバイスで設定がアクティブ化されると、すべてのインターフェイスが制御および BFD 接続を確立するプロセスを開始します。1つまたは複数のプライマリインターフェイスが BFD 接続を確立すると、ラストリゾート回線は自動的にシャットダウンします。</p> <p>すべてのプライマリインターフェイスがリモートエッジへの接続を失った場合にのみ、ラストリゾート回線がアクティブになり、エッジデバイスで BFD TLOC ダウンアラームと制御 TLOC ダウンアラームがトリガーされます。ラストリゾートインターフェイスは、エッジデバイスのバックアップ回線として使用され、他のすべてのトランスポートリンク BFD セッションが失敗したときにアクティブ化されます。このモードでは、無線インターフェイスはオフになり、セルラーインターフェイスを介した制御またはデータ接続は存在しません。</p>
NAT 更新間隔	<p>DTLS または TLS WAN トランスポート接続で送信される NAT リフレッシュパケットの間隔を入力します。範囲：1～60 秒。デフォルト：5 秒。</p>
Hello 間隔 (Hello Interval)	<p>DTLS または TLS WAN トランスポート接続で送信される Hello パケットの間隔を入力します。範囲：100～10000 ミリ秒。デフォルト：1000 ミリ秒 (1 秒)</p>

パラメータ名	説明
Hello 許容度	トランスポートトンネルのダウンを宣言する前に、DTLSまたはTLS WAN トランスポート接続で Hello パケットを待機する時間を入力します。 範囲：12 ～ 60 秒。デフォルト：12 秒。

アクセスリストの適用

ルータインターフェイスに書き換えルール、アクセスリスト、およびポリサーを適用するには、[ACL] を選択し、次のパラメータを設定します。

表 31:

パラメータ名	説明
Shaping rate	インターフェイスの集約トラフィック転送速度を、回線速度よりも低く設定します（キロビット/秒 (kbps) 単位）。
QoS マップ	インターフェイスから送信されるパケットに適用する QoS マップの名前を指定します。
リライトルール	[On] をクリックし、インターフェイスに適用する書き換えルールの名前を指定します。
入力 ACL – IPv4	[On] をクリックして、インターフェイスで受信される IPv4 パケットに適用するアクセスリストの名前を指定します。
出力 ACL – IPv4	[On] をクリックし、インターフェイスで送信される IPv4 パケットに適用するアクセスリストの名前を指定します。
入力 ACL – IPv6	[On] をクリックして、インターフェイスで受信される IPv6 パケットに適用するアクセスリストの名前を指定します。
出力 ACL – IPv6	[On] をクリックし、インターフェイスで送信される IPv6 パケットに適用するアクセスリストの名前を指定します。
入力ポリサー	[On] をクリックして、インターフェイスで受信されるパケットに適用するポリサーの名前を指定します。
出力ポリサー	[On] をクリックして、インターフェイスで送信されるパケットに適用するポリサーの名前を指定します。

機能テンプレートを保存するには、[Save] をクリックします。

その他のインターフェイスプロパティの設定

他のインターフェイスプロパティを設定するには、[Advanced] を選択し、次のプロパティを設定します。

表 32:

パラメータ名	説明
PMTU ディスカバリ	[On] をクリックしてインターフェイスでパス MTU ディスカバリを有効にし、パケットのフラグメント化を必要とせずにサポートされる最大の MTU サイズをルータで判別できるようにします。
TCP MSS	Cisco IOS XE SD-WAN デバイス を通過する TCP SYN パケットの最大セグメントサイズ (MSS) を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552～1460 バイト。デフォルト：なし。
Dont Fragment のクリア	[On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Don't Fragment ビットをクリアします。DF ビットがクリアされると、そのインターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。
静的入力 QoS	着信トラフィックに使用するキュー番号を選択します。範囲：0～7
自動ネゴシエーション	[Off] をクリックして、自動ネゴシエーションをオフにします。デフォルトでは、インターフェイスは自動ネゴシエーションモードで実行されます。
TLOC Extension	WAN トランスポート回線に接続する同じルータ上の物理インターフェイスの名前を入力します。次に、この構成により、このサービス側のインターフェイスが WAN トランスポートにバインドされます。それ自体は WAN に直接接続されておらず（通常、サイトには 1 つの WAN 接続しかないため）、同じサイトにあり、このサービス側インターフェイスに接続する 2 番目の Cisco IOS XE SD-WAN デバイスには、WAN への接続が提供されます。

機能テンプレートを保存するには、[Save] をクリックします。

リリース情報

リリース 18.3 の Cisco vManage NMS で導入されました。

VPN インターフェイス DSL PPPoE

Cisco IOS XE SD-WAN デバイスの VPN インターフェイス DSL PPPoE テンプレートを使用します。

サービスプロバイダーのデジタル加入者線 (DSL) 機能をサポートするには、DSL NIM モジュールを備えたルータに PPP-over-Ethernet インターフェイスを構成します。

Cisco vManage テンプレートを使用して Cisco ルータに DSL 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。

1. この記事で説明されているように、PPP-over-Ethernet インターフェイスのパラメータを構成する VPN インターフェイス DSL PPPoE 機能テンプレートを作成します。
2. VPN 機能テンプレートを作成して、VPN パラメータを設定します。VPN のヘルプトピックを参照してください。

[Template] 画面に移動し、テンプレートに命名する

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. **[Device Templates]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Device Templates]** のタイトルは **[Device]** です。

3. **[Create Template]** ドロップダウンリストから、**[From Feature Template]** を選択します。
4. **[Device Model]** ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。
5. **[Transport & Management VPN]** をクリックするか、**[Transport & Management VPN]** セクションまでスクロールします。
6. **[Additional VPN 0 Templates]** で、**[VPN Interface DSL PPPoE]** をクリックします。
7. **[VPN Interface DSL PPPoE]** ドロップダウンリストから、**[Create Template]** をクリックします。VPN インターフェイス DSL PPPoE テンプレートフォームが表示されます。このフォームには、テンプレートに名前を付けるためのフィールドと、PPPoE インターフェイスのパラメータを定義するためのフィールドが含まれています。
8. **[Template Name]** に、テンプレートの名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。
9. **[Template Description]** に、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。

初めて機能テンプレートを開くと、デフォルト値を持つパラメータごとに、その範囲が **[Default]** に設定され (チェックマークで示される)、デフォルト設定またはデフォルト値が表示されます。デフォルト値を変更するか、値を入力するには、パラメータフィールドの左側にある **[Scope]** ドロップダウンをクリックし、次のいずれかを選択します。

表 33:

パラメータの範囲	範囲の説明
デバイス固有 (ホストのアイコンで示される)	<p>デバイス固有の値がパラメータに使用されます。デバイス固有のパラメータの場合、機能テンプレートに値を入力できません。Viptela デバイスをデバイステンプレートに添付するときに、値を入力します。</p> <p>[Device Specific] をクリックすると、[Enter Key] ボックスが表示されます。このボックスには、作成する CSV ファイル内のパラメータを識別する一意の文字列であるキーが表示されます。このファイルは、キーごとに1つの列を含む Excel スプレッドシートです。ヘッダー行にはキー名 (行ごとに1つのキー) が含まれます。その後の各行は、デバイスに対応し、そのデバイスのキーの値を定義します。Viptela デバイスをデバイステンプレートに添付するときに、この CSV ファイルをアップロードします。詳細については、「Create a Template Variables Spreadsheet」を参照してください。</p> <p>デフォルトのキーを変更するには、新しい文字列を入力し、[Enter Key] ボックスの外にカーソルを移動します。</p> <p>デバイス固有のパラメータの例としては、システム IP アドレス、ホスト名、GPS ロケーション、サイト ID があります。</p>
グローバル (地球のアイコンで示される)	<p>パラメータの値を入力し、その値をすべてのデバイスに適用します。</p> <p>デバイスのグループにグローバルに適用できるパラメータの例としては、DNS サーバー、Syslog サーバー、インターフェイス MTU があります。</p>

VDSL コントローラ機能の構成

VPN の基本的な VDSL コントローラ機能を設定するには、[Basic Configuration] を選択し、次のパラメータを設定します。必須パラメータはアスタリスクで示されています。



- (注) 展開に DSL を備えたデバイスが含まれている場合は、これらのテンプレートが使用されていない場合でも、DSL インターフェイス テンプレートを Cisco vManage に含める必要があります。

表 34:

パラメータ名	説明
Shutdown*	[No] をクリックして、VDSL コントローラ インターフェイスを有効にします。

パラメータ名	説明
Controller VDSL Slot*	コントローラ VDSL インターフェイスのスロット番号を、 <i>slot/subslot/port</i> の形式で入力します (たとえば、0/2/0)。
Mode*	ドロップダウンから VDSL コントローラの動作モードを選択します。 <ul style="list-style-type: none"> • [Auto] : デフォルトのモード。 • [ADSL1] : ITU G.992.1 Annex A フルレートモードを使用します。これは、1.3 Mbps のダウンストリームレートと 1.8 Mbps のアップストリームレートを提供します。 • [ADSL2] : ITU G.992.3 Annex A、Annex L、および Annex M を使用します。これは、12 Mbps のダウンストリームレートと 1.3 Mbps のアップストリームレートを提供します。 • [ADSL2+] : ITU G.992.5 Annex A および Annex M を使用します。これは、24 Mbps のダウンストリームレートと 3.3 Mbps のアップストリームレートを提供します。 • [ANSI] : ITU G.991.1、G.992.3、および G.992.5 (Annex A および Annex M) で定義されている ADSL2/2+ モード、および ITU-T G.993.2 で定義されている VDSL2 モードで動作します。 • [VDSL2] : ITU-T G.993.2 で定義されている VDSL2 モードで動作します。これは、最大 30 MHz の周波数を使用して、200 Mbps のダウンストリームレートと 100 Mbps のアップストリームレートを提供します。
VDSL Modem Configuration	NIM モジュールの DSL モデムに送信するコマンドを入力します。コマンドが有効な場合、コマンドが実行され、結果が Cisco vManage NMS に返されます。コマンドが有効でない場合、コマンドは実行されません。
SRA	[Yes] をクリックして、インターフェイスでのシームレスなレート調整を有効にします。SRA は、現在の回線状態に基づいて回線速度を調整します。

機能テンプレートを保存するには、[Save] をクリックします。

VDSL コントローラのイーサネット インターフェイスを設定する

VDSL コントローラでイーサネット インターフェイスを設定するには、[Ethernet] を選択し、次のパラメータを設定します。すべてのパラメータを設定する必要があります。

表 35: 機能の履歴

機能名	リリース情報	説明
DSL でのダイヤライ ンターフェイスの サポート	Cisco IOS XE リリー ス 17.3.2 Cisco vManage リ リース 20.3.1	この機能により、Cisco IOS XE SD-WAN デバイスのダイヤラインターフェイスを介した Point-to-Point Protocol (PPP) セッションの追跡が可能になります。 ダイヤラインターフェイスは、Point-to-Point Protocol over Ethernet (PPPoE)、Point-to-Point Protocol over Asynchronous Transfer Mode (PPPoA) の展開におけるデジタル加入者線 (DSL) で使用されます。ダイヤラインターフェイスは、PPP セッションのステータスに関係なく、常に稼働しています。これにより、ダイヤラインターフェイスの使用中に、IPSLA やルーティング フェールオーバーが機能するための追跡などの追加設定の必要性を回避できます。 次のコマンドを追加して、PPP セッションがダウンしたときにダイヤラインターフェイスをダウンさせる、 <code>dialer down-with-vInterface</code> を設定します。

表 36:

パラメータ名	説明
Ethernet Interface Name	イーサネット インターフェイスの名前を <code>subslot/port</code> の形式で入力します (例: 2/0)。スロット番号は常に 0 であるため、入力する必要はありません。
VLAN ID	イーサネット インターフェイスの VLAN 識別子を入力します。
説明	インターフェイスの説明を入力します。
Dialer Pool Member	インターフェイスが属するダイヤラプールの番号を入力します。1 ~ 255 の値を指定できます。
PPP Max Payload	PPP リンク制御プロトコル (LCP) ネゴシエーション中にネゴシエートされる最大受信ユニット (MRU) 値を入力します。範囲: 64 ~ 1792 バイト
Dialer IP	ダイヤラインターフェイスの IP プレフィックスを設定します。このプレフィックスは、インターフェイスが呼び出す宛先のノードのプレフィックスです。 • [Negotiated]: IPCP ネゴシエーション中に取得されたアドレスを使用します。

機能テンプレートを保存するには、[Save] をクリックします。

PPP 認証プロトコルの構成

PPP 認証プロトコルを構成するには、[PPP] を選択し、次のパラメータを設定します。

表 37:

パラメータ名	説明
認証プロトコル (Authentication Protocol)	MLP で使用される認証プロトコルを選択します。 <ul style="list-style-type: none"> • CHAP : インターネット サービス プロバイダー (ISP) から提供されたホスト名とパスワードを入力します。ホスト名は最大 255 文字です。 • [PAP] : ISP から提供されたユーザー名とパスワードを入力します。ユーザー名は最大 255 文字です。 • PAP および CHAP : 両方の認証プロトコルを設定します。それぞれのプロトコルのログイン情報を入力します。両方に同じユーザー名とパスワードを使用するには、[PAP と CHAP に同じ資格情報] をクリックします。

機能テンプレートを保存するには、[Save] をクリックします。

トンネルインターフェイスの作成

IOS XE ルータでは、最大 4 つのトンネルインターフェイスを設定できます。つまり、各ルータに最大 4 つの TLOC を設定できます。

オーバーレイネットワークが機能できるようにコントロールプレーンがそれ自体を確立するには、VPN 0 で WAN トランスポート インターフェイスを設定する必要があります。

マルチリンク インターフェイスのトンネルインターフェイスを設定するには、[Tunnel Interface] タブを選択し、次のパラメータを設定します。

表 38:

パラメータ名	説明
トンネルインターフェイス	[On] をクリックして、トンネルインターフェイスを作成します。
色	TLOC の色を選択します。

パラメータ名	説明
制御接続	<p>デフォルトでは、制御接続はオンに設定されており、TLOCの制御接続を確立します。ルータに複数のTLOCがある場合は、[いいえ]をクリックして、トンネルがTLOCの制御接続を確立しないようにします。</p> <p>(注) 接続トラフィックでのデータ/パケットの損失を避けるために、デフォルトの1秒のhelloインターバルと12秒のhelloトレランスパラメータを設定して、最低650～700Kbpsの帯域幅を設定することをお勧めします。</p> <p>BFDセッションごとに、175バイトの追加の平均サイズBFDパケットは、1.4Kbpsの帯域幅を消費します。</p> <p>双方向BFDパケットフローに必要な帯域幅の計算例を以下に示します。</p> <ul style="list-style-type: none"> • 制御接続用にデバイスごとに650～700Kbps。 • デバイス上のBFDセッション(要求)ごとに175バイト(または1.4Kbps) • デバイス上のBFDセッション(応答)ごとに175バイト(または1.4Kbps) <p>パスMTUディスカバリ(PMTUD)が有効になっている場合、30秒ごとにトンネルごとにBFDパケットを送受信するための帯域幅:</p> <p>1500バイトのBFD要求パケットは、トンネルごとに30秒ごとに送信されます。</p> <p>1500バイト * 8ビット / 1バイト * 1パケット / 30秒 = 400bps (リクエスト)</p> <p>147バイトのBFDパケットが応答として送信されます。</p> <p>147バイト * 8ビット / 1バイト * 1パケット / 30秒 = 40bps (レスポンス)</p> <p>したがって、たとえば775BFDセッションを持つデバイスの場合、次の帯域幅が必要です。</p> <p>$700k + (1.4k * 775) + (400 * 775) + (1.4k * 775) + (40 * 775) = \sim 3.5$ MBps</p>
最大制御接続数	<p>WANトンネルインターフェイスが接続できるの最大数を指定します。Cisco vSmartコントローラトンネルが制御接続を確立しないようにするには、この数値を0に設定します。</p> <p>範囲：0～8、デフォルト：2</p>

パラメータ名	説明
Cisco vBond オーケストレーション As STUN Server	[On] をクリックして NAT (STUN) のセッション トラバーサル ユーティリティを有効にし、ルータが NAT の背後にある場合にトンネルインターフェイスがパブリック IP アドレスとポート番号を検出できるようにします。
コントローラグループリストの除外	トンネル インターフェイスの接続を許可しない Cisco vSmart コントローラを設定します。 範囲：0 ～ 100
Cisco vManage Connection Preference	トンネルインターフェイスを使用して Cisco vManage NMS と制御トラフィックを交換するための優先順位を設定します。 範囲：0 ～ 8、デフォルト：5
ポートホップ	[On] をクリックしてポートホッピングを有効にするか、[Off] をクリックして無効にします。ルータが NAT の背後にある場合、ポートホッピングは、事前を選択された OMP ポート番号(ベースポートと呼ばれる)のプールを循環して、接続の試行が失敗したときに他のルータとの DTLS 接続を確立します。デフォルトのベースポートは 12346、12366、12386、12406、および 12426 です。ベースポートを変更するには、ポートオフセット値を設定します。デフォルト：有効
低帯域幅リンク	トンネルインターフェイスを低帯域幅リンクとして特徴付ける場合に選択します。
トンネル TCP MSS	<p>TCP MSS は、ルータを通過する最初の TCP ヘッダーを含むすべてのパケットに影響します。設定すると、TCP MSS は、スリーウェイハンドシェイクで交換される MSS に対して検査されます。構成された TCP MSS 設定がヘッダーの MSS よりも低い場合、ヘッダーの MSS は低くなります。MSS ヘッダー値がすでに TCP MSS よりも低い場合、パケットは変更されずに通過します。トンネルの最後にあるホストは、2つのホストの低い方の設定を使用します。TCP MSS を設定する場合は、最小パス MTU より 40 バイト小さく設定する必要があります。</p> <p>Cisco IOS XE SD-WAN デバイス を通過する TPC SYN パケットの MSS を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ～ 1460 バイト、デフォルト：なし</p>

パラメータ名	説明
Clear-Dont-Fragment	<p>Don't Fragment が設定されているインターフェイスに到着するパケットの [Clear-Dont-Fragment] を設定します。これらのパケットが MTU が許可するサイズより大きい場合、それらはドロップされます。Don't Fragment ビットをクリアすると、パケットはフラグメント化されて送信されます。</p> <p>[On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Dont Fragment ビットをクリアします。Dont Fragment ビットがクリアされると、インターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。</p> <p>(注) [Clear-Dont-Fragment] は Dont Fragment ビットをクリアし、Dont Fragment ビットが設定されます。フラグメンテーションを必要としないパケットの場合、Dont Fragment ビットは影響を受けません。</p>
サービスの許可	サービスごとに [On] または [Off] を選択して、インターフェイスでサービスを許可または禁止します。

追加のトンネルインターフェイスパラメータを設定するには、[Advanced Options] をクリックして、次のパラメータを設定します。

表 39:

パラメータ名	説明
GRE	<p>トンネルインターフェイスで GRE カプセル化を使用します。デフォルトでは、GRE は無効になっています。</p> <p>IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。</p>
IPSec	<p>トンネルインターフェイスで IPsec カプセル化を使用します。デフォルトでは、IPsec は有効になっています。</p> <p>IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。</p>
IPsec Preference	<p>トラフィックをトンネルに誘導するための優先値を指定します。高い値が低い値に優先します。</p> <p>範囲 : 0 ~ 4294967295、デフォルト : 0</p>

パラメータ名	説明
IPsec の重み	<p>複数の TLOC 間でトラフィックのバランスをとるために使用する重みを入力します。値が大きいほど、より多くのトラフィックがトンネルに送信されます。</p> <p>範囲：1 ～ 255、デフォルト：1</p>
通信事業者	<p>トンネルに関連付けるキャリア名またはプライベート ネットワーク 識別子を選択します。</p> <p>値：carrier1、carrier2、carrier3、carrier4、carrier5、carrier6、carrier7、carrier8、default、デフォルト：default</p>
ループバック トンネルのバインド	<p>ループバック インターフェイスにバインドする物理 インターフェイスの名前を入力します。</p>
ラストリゾート回線	<p>トンネル インターフェイスを最終手段の回線として使用する場合に選択します。</p> <p>(注) ラストリゾート回線として構成されたインターフェイスはダウンすると予想され、制御接続の数の計算中にスキップされ、セルラーモデムは休止状態になり、トラフィックは回線上で送信されません。</p> <p>セルラー インターフェイスを備えたエッジデバイスで設定がアクティブ化されると、すべてのインターフェイスが制御および BFD 接続を確立するプロセスを開始します。1 つ以上のプライマリ インターフェイスが BFD 接続を確立すると、最終手段の回線は自動的にシャットダウンします。</p> <p>すべてのプライマリ インターフェイスがリモートエッジへの接続を失った場合にのみ、ラストリゾート回線がアクティブになり、エッジデバイスで BFD TLOC ダウンアラームと制御 TLOC ダウンアラームがトリガーされます。ラストリゾート インターフェイスは、エッジデバイスのバックアップ回線として使用され、他のすべてのトランスポートリンク BFD セッションが失敗したときにアクティブ化されます。このモードでは、無線 インターフェイスはオフになり、セルラー インターフェイスを介した制御またはデータ接続は存在しません。</p>
NAT 更新間隔	<p>DTLS または TLS WAN トランスポート接続で送信される NAT リフレッシュ パケットの間隔を入力します。範囲：1 ～ 60 秒。デフォルト：5 秒。</p>
Hello 間隔 (Hello Interval)	<p>DTLS または TLS WAN トランスポート接続で送信される Hello パケットの間隔を入力します。範囲：100 ～ 10000 ミリ秒。デフォルト：1000 ミリ秒 (1 秒)</p>

パラメータ名	説明
Hello 許容度	トランスポートトンネルのダウンを宣言する前に、DTLSまたはTLSWANトランスポート接続で Hello パケットを待機する時間を入力します。 範囲：12 ～ 60 秒。デフォルト：12 秒。

インターフェイスを NAT デバイスとして設定する

ポート転送などのアプリケーションの NAT デバイスとして機能するようにインターフェイスを設定するには、[NAT] を選択し、[On] をクリックして、次のパラメータを設定します。

表 40:

パラメータ名	説明
NAT	[On] をクリックして、インターフェイスを NAT デバイスとして機能させます。
Refresh Mode	NAT マッピングを更新する方法（アウトバウンドまたは双方向（アウトバウンドとインバウンド）のいずれか）を選択します。デフォルト：アウトバウンド
[UDP Timeout]	UDP セッションを介した NAT 変換がいつタイムアウトするかを指定します。範囲：1 ～ 65536 分、デフォルト：1 分
[TCP Timeout]	TCP セッションを介した NAT 変換がいつタイムアウトするかを指定します。範囲：1 ～ 65536 分、デフォルト：60 分（1 時間）
Block ICMP	[On] を選択して、インバウンド ICMP エラーメッセージをブロックします。デフォルトでは、NAT デバイスとして機能するルータは、これらのエラーメッセージを受け取ります。デフォルト：Off
Respond to Ping	接続のパブリック側から受信した NAT インターフェイスの IP アドレスへの ping 要求にルータが応答するようにするには、[On] を選択します。

ポート転送ルールを作成するには、[Add New Port Forwarding Rule] をクリックし、次のパラメータを設定します。最大128のポート転送ルールを定義して、外部ネットワークからの要求が内部ネットワーク上のデバイスに到達できるようにすることができます。

表 41:

パラメータ名	説明
Port Start Range	ポート番号を入力して、ポートまたは対象の範囲の最初のポートを定義します。範囲：0 ～ 65535
Port End Range	同じポート番号を入力してポート転送を1つのポートに適用するか、より大きい番号を入力してポートの範囲に適用します。範囲：0 ～ 65535

パラメータ名	説明
プロトコル	ポート転送ルールを適用するプロトコル ([TCP] または [UDP]) を選択します。TCP トラフィックと UDP トラフィックの両方で同じポートを一致させるには、2つのルールを構成します。
VPN	内部サーバーが存在するプライベート VPN を指定します。この VPN は、オーバーレイネットワークの VPN 識別子の 1 つです。範囲：0 ~ 65530
プライベート IP	ポート転送ルールに一致するトラフィックを転送する内部サーバーの IP アドレスを指定します。

ポート転送ルールを保存するには、[Add] をクリックします。

機能テンプレートを保存するには、[Save] をクリックします。

アクセスリストの適用

ルータ インターフェイスに書き換えルール、アクセス リスト、およびポリサーを適用するには、ACL を選択し、次のパラメータを設定します。

表 42:

パラメータ名	説明
成形率	インターフェイスの集約トラフィック転送速度を、回線速度よりも低く設定します (キロビット/秒 (kbps) 単位)。
QoS マップ	インターフェイスから送信されるパケットに適用する QoS マップの名前を指定します。
リライトルール	[On] をクリックし、インターフェイスに適用する書き換えルールの名前を指定します。
入力 ACL - IPv4	[On] をクリックして、インターフェイスで受信される IPv4 パケットに適用するアクセスリストの名前を指定します。
出力 ACL - IPv4	[On] をクリックし、インターフェイスで送信される IPv4 パケットに適用するアクセスリストの名前を指定します。
入力 ACL - IPv6	[オン] をクリックして、インターフェイスで受信される IPv6 パケットに適用するアクセス リストの名前を指定します。
出力 ACL - IPv6	[オン] をクリックし、インターフェイスで送信される IPv6 パケットに適用するアクセス リストの名前を指定します。
入力ポリサー	[On] をクリックして、インターフェイスで受信されるパケットに適用するポリサーの名前を指定します。

パラメータ名	説明
出力ポリサー	[On]をクリックして、インターフェイスで送信されるパケットに適用するポリサーの名前を指定します。

機能テンプレートを保存するには、[Save]をクリックします。

その他のインターフェイスプロパティの設定

他のインターフェイスプロパティを設定するには、[Advanced]タブを選択し、次のプロパティを設定します。

表 43:

パラメータ名	説明
Bandwidth Upstream	送信トラフィックについて、通知を生成する帯域幅を設定します。範囲：1 ~ $(2^{32}/2) - 1$ kbps
Bandwidth Downstream	受信トラフィックについて、通知を生成する帯域幅を設定します。範囲：1 ~ $(2^{32}/2) - 1$ kbps
IP MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。範囲：576 ~ 1804。デフォルト：1500 バイト。
TCP MSS	ルータを通過する TCP SYN パケットの最大セグメントサイズ (MSS) を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ~ 1460 バイト。デフォルト：なし。
Dont Fragment のクリア	[オン]をクリックして、インターフェイスから送信されるパケットの IPv4 パケット ヘッダーの Don't Fragment ビットをクリアします。DF ビットがクリアされると、そのインターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。
TLOC Extension	WAN トランスポート回線に接続する同じルータ上の物理インターフェイスの名前を入力します。次に、この構成により、このサービス側のインターフェイスが WAN トランスポートにバインドされます。それ自体は WAN に直接接続されておらず（通常、サイトには 1 つの WAN 接続しかないため）、同じサイトにあり、このサービス側インターフェイスに接続する 2 番目のルータには、WAN への接続が提供されます。
トラッカー	インターネットに接続するトランスポート インターフェイスのステータスをトラッキングするトラッカーの名前を入力します。

機能テンプレートを保存するには、[Save]をクリックします。

リリース情報

リリース 18.3 の Cisco vManage NMS で導入されました。

VPN インターフェイス イーサネット PPPoE

Cisco IOS XE SD-WAN デバイスの PPPoE テンプレートを使用します。

Cisco IOS XE ルータで PPPoE over GigabitEthernet インターフェイスを設定して、PPPoE クライアントをサポートします。

Cisco vManage テンプレートを使用して Cisco ルータに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。

1. このセクションの説明に従って、VPN インターフェイス イーサネット PPPoE 機能テンプレートを作成して、イーサネット PPPoE インターフェイスパラメータを設定します。
2. VPN 機能テンプレートを作成して、VPN パラメータを設定します。VPN のヘルプトピックを参照してください。

[Template] 画面に移動し、テンプレートに命名する

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. **[Device Templates]** をクリックし、**[Create Template]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Device Templates]** のタイトルは **[Device]** です。

3. **[Create Template]** ドロップダウンリストから、**[From Feature Template]** を選択します。
4. **[Device Model]** ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。
5. **[Transport & Management VPN]** をクリックするか、**[Transport & Management VPN]** セクションまでスクロールします。
6. **[Additional VPN 0 Templates]** で、**[VPN Interface Ethernet PPPoE]** をクリックします。
7. **[VPN Interface Ethernet PPPoE]** ドロップダウンリストから、**[Create Template]** をクリックします。VPN インターフェイスイーサネット PPPoE テンプレートフォームが表示されます。

このフォームには、テンプレートに名前を付けるためのフィールドと、イーサネット PPPoE パラメータを定義するためのフィールドが含まれています。



8. **[Template Name]** に、テンプレートの名前を入力します。

名前の最大長は 128 文字で、英数字のみを使用できます。

9. [Template Description] に、テンプレートの説明を入力します。

説明の最大長は 2048 文字で、英数字のみを使用できます。

初めて機能テンプレートを開くと、デフォルト値を持つパラメータごとに、その範囲が [Default] に設定され（チェックマークで示される）、デフォルト設定またはデフォルト値が表示されます。デフォルト値を変更するか、値を入力するには、[Scope] ドロップダウンリストをクリックし、次のいずれかを選択します。

表 44:

パラメータの範囲	範囲の説明
デバイス固有（ホストのアイコンで示される）	<p>デバイス固有の値がパラメータに使用されます。デバイス固有のパラメータの場合、機能テンプレートに値を入力できません。Cisco SD-WAN デバイスをデバイステンプレートに添付するときに、値を入力します。</p> <p>[Device Specific] をクリックすると、[Enter Key] ボックスが表示されます。このボックスには、作成する CSV ファイル内のパラメータを識別する一意の文字列であるキーが表示されます。このファイルは、キーごとに 1 つの列を含む Excel スプレッドシートです。ヘッダー行にはキー名（行ごとに 1 つのキー）が含まれます。その後の各行は、デバイスに対応し、そのデバイスのキーの値を定義します。Cisco SD-WAN デバイスをデバイステンプレートに添付するときに、この CSV ファイルをアップロードします。詳細については、「Create a Template Variables Spreadsheet」を参照してください。</p> <p>デフォルトのキーを変更するには、新しい文字列を入力し、[Enter Key] ボックスの外にカーソルを移動します。</p> <p>デバイス固有のパラメータの例としては、システム IP アドレス、ホスト名、GPS ロケーション、サイト ID があります。</p>
グローバル（地球のアイコンで示される）	<p>パラメータの値を入力し、その値をすべてのデバイスに適用します。</p> <p>デバイスのグループにグローバルに適用できるパラメータの例としては、DNS サーバー、Syslog サーバー、インターフェイス MTU があります。</p>

PPPoE 機能の設定

基本的な PPPoE 機能を設定するには、[Basic Configuration] をクリックして、次のパラメータを設定します。必須パラメータはアスタリスクで示されています。

表 45:

パラメータ名	説明
Shutdown*	[No] をクリックして、GigabitEthernet インターフェイスを有効にします。
Ethernet Interface Name	GigabitEthernet インターフェイスの名前を入力します。 IOS XE ルータの場合、インターフェイス名を完全に入力する必要があります（たとえば、 GigabitEthernet0/0/0 ）。
VLAN ID	サブインターフェイスの VLAN タグ。
説明	Ethernet-PPPoE 対応インターフェイスの説明を入力します。
Dialer Pool Member	インターフェイスが属するダイヤラプールの番号を入力します。 範囲：100 ～ 255。
PPP Maximum Payload	PPP リンク制御プロトコル（LCP）ネゴシエーション中にネゴシエートされる最大受信ユニット（MRU）値を入力します。範囲：64 ～ 1792 バイト

機能テンプレートを保存するには、[Save] をクリックします。

PPP 認証プロトコルの設定

PPP 認証プロトコルを設定するには、[PPP] をクリックして、次のパラメータを設定します。必須パラメータはアスタリスクで示されています。

表 46:

パラメータ名	説明
PPP Authentication Protocol	MLP で使用される認証プロトコルを選択します。 <ul style="list-style-type: none"> • CHAP：インターネット サービス プロバイダー（ISP）から提供されたホスト名とパスワードを入力します。ホスト名は最大 255 文字です。 • PAP：ISP から提供されたユーザー名とパスワードを入力します。ユーザー名は最大 255 文字です。 • PAP および CHAP：両方の認証プロトコルを設定します。それぞれのプロトコルのログイン情報を入力します。両方に同じユーザー名とパスワードを使用するには、[Same Credentials for PAP and CHAP] をクリックします。

機能テンプレートを保存するには、[Save] をクリックします。

トンネルインターフェイスの作成

IOS XE ルータでは、最大 4 つのトンネルインターフェイスを設定できます。つまり、各ルータに最大 4 つの TLOC を設定できます。

オーバーレイネットワークが機能できるようにコントロールプレーンがそれ自体を確立するには、VPN 0 で WAN トランスポート インターフェイスを設定する必要があります。

マルチリンク インターフェイスのトンネルインターフェイスを設定するには、[Tunnel Interface] を選択し、次のパラメータを設定します。

表 47:

パラメータ名	説明
トンネルインターフェイス	[On] をクリックして、トンネルインターフェイスを作成します。
色	TLOC の色を選択します。

パラメータ名	説明
制御接続	<p>デフォルトでは、制御接続は [On] に設定されており、TLOC の制御接続を確立します。ルータに複数の TLOC がある場合は、[No] をクリックして、トンネルが TLOC の制御接続を確立しないようにします。</p> <p>(注) 接続トラフィックでのデータ/パケットの損失を避けるために、デフォルトの 1 秒の hello インターバルと 12 秒の hello トレランスパラメータを設定して、最低 650 ~ 700 Kbps の帯域幅を設定することをお勧めします。</p> <p>BFD セッションごとに、175 バイトの追加の平均サイズ BFD パケットは、1.4 Kbps の帯域幅を消費します。</p> <p>双方向 BFD パケットフローに必要な帯域幅の計算例を以下に示します。</p> <ul style="list-style-type: none"> • 制御接続用にデバイスごとに 650 ~ 700 Kbps。 • デバイス上の BFD セッション (要求) ごとに 175 バイト (または 1.4 Kbps) • デバイス上の BFD セッション (応答) ごとに 175 バイト (または 1.4 Kbps) <p>パス MTU ディスカバリ (PMTUD) が有効になっている場合、30 秒ごと、トンネルごとに BFD パケットを送受信するための帯域幅 :</p> <p>1500 バイトの BFD 要求パケットは、30 秒ごと、トンネルごとに送信されます。</p> <p>$1500 \text{ バイト} * 8 \text{ ビット} / 1 \text{ バイト} * 1 \text{ パケット} / 30 \text{ 秒} = 400 \text{ bps}$ (要求)</p> <p>147 バイトの BFD パケットが応答として送信されます。</p> <p>$147 \text{ バイト} * 8 \text{ ビット} / 1 \text{ バイト} * 1 \text{ パケット} / 30 \text{ 秒} = 40 \text{ bps}$ (応答)</p> <p>したがって、たとえば 775 BFD セッションを持つデバイスの場合、次の帯域幅が必要です。</p> <p>$700k + (1.4k * 775) + (400 * 775) + (1.4k * 775) + (40 * 775) = \sim 3.5 \text{ MBps}$</p>
最大制御接続数	<p>WAN トンネルインターフェイスが接続できる Cisco vSmart コントローラの最大数を指定します。トンネルが制御接続を確立しないようにするには、この数値を 0 に設定します。</p> <p>範囲 : 0 ~ 8、デフォルト : 2</p>

パラメータ名	説明
Cisco vBond オーケストレーション As STUN Server	[On] をクリックして NAT (STUN) のセッショントラバーサルユーティリティを有効にし、ルータが NAT の背後にある場合にトンネルインターフェイスがパブリック IP アドレスとポート番号を検出できるようにします。
コントローラグループリストの除外	トンネルインターフェイスの接続を許可しない Cisco vSmart コントローラを設定します。範囲：0～100
Cisco vManage Connection Preference	トンネルインターフェイスを使用して Cisco vManage NMS と制御トラフィックを交換するための優先順位を設定します。範囲：0～8、デフォルト：5
ポートホップ	ポートホッピングを有効にするには [On] をクリックし、無効にするには [Off] をクリックします。ルータが NAT の背後にある場合、ポートホッピングは、事前に選択された OMP ポート番号（ベースポートと呼ばれる）のプールを循環して、接続の試行が失敗したときに他のルータとの DTLS 接続を確立します。デフォルトのベースポートは 12346、12366、12386、12406、および 12426 です。ベースポートを変更するには、ポートオフセット値を設定します。デフォルト：有効
低帯域幅リンク	トンネルインターフェイスの特性を低帯域幅リンクにする場合に選択します。
サービスの許可	サービスごとに [On] または [Off] を選択して、インターフェイスでサービスを許可または禁止します。

追加のトンネルインターフェイスパラメータを設定するには、[Advanced Options] をクリックして、次のパラメータを設定します。

表 48:

パラメータ名	説明
GRE	トンネルインターフェイスで GRE カプセル化を使用します。デフォルトでは、GRE は無効になっています。 IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。
IPSec	トンネルインターフェイスで IPsec カプセル化を使用します。デフォルトでは、IPsec が有効になっています。 IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。

パラメータ名	説明
IPsec Preference	<p>トラフィックをトンネルに送信するための優先値を指定します。高い値が低い値に優先します。</p> <p>範囲：0 ～ 4294967295。デフォルト：0</p>
IPsec Weight	<p>複数の TLOC 間でトラフィックのバランスをとるために使用する重みを入力します。値が大きいほど、より多くのトラフィックがトンネルに送信されます。</p> <p>範囲：1 ～ 255。デフォルト：1</p>
通信事業者	<p>トンネルに関連付けるキャリア名またはプライベートネットワーク識別子を選択します。</p> <p>値：carrier1、carrier2、carrier3、carrier4、carrier5、carrier6、carrier7、carrier8、デフォルト。デフォルト：デフォルト</p>
ループバックトンネルのバインド	<p>ループバック インターフェイスにバインドする物理インターフェイスの名前を入力します。</p>
ラストリゾート回線	<p>トンネルインターフェイスをラストリゾート回線として使用する場合に選択します。</p> <p>(注) ラストリゾート回線として設定されたインターフェイスはダウン状態になるため、制御接続の数の計算中にスキップされ、セルラーモデムは休止状態になり、トラフィックはこの回線経由で送信されません。</p> <p>セルラーインターフェイスを備えたエッジデバイスで設定がアクティブ化されると、すべてのインターフェイスが制御および BFD 接続を確立するプロセスを開始します。1つまたは複数のプライマリインターフェイスが BFD 接続を確立すると、ラストリゾート回線は自動的にシャットダウンします。</p> <p>すべてのプライマリインターフェイスがリモートエッジへの接続を失った場合にのみ、ラストリゾート回線がアクティブになり、エッジデバイスで BFD TLOC ダウンアラームと制御 TLOC ダウンアラームがトリガーされます。ラストリゾートインターフェイスは、エッジデバイスのバックアップ回線として使用され、他のすべてのトランスポートリンク BFD セッションが失敗したときにアクティブ化されます。このモードでは、無線インターフェイスはオフになり、セルラーインターフェイスを介した制御またはデータ接続は存在しません。</p> <p>(注) プライマリ インターフェイス ルートでのアドミニストレーティブ ディスタンス値の設定はサポートされていません。</p>

パラメータ名	説明
NAT 更新間隔	DTLS または TLS WAN トランスポート接続で送信される NAT リフレッシュパケットの間隔を入力します。範囲：1 ～ 60 秒。デフォルト：5 秒
Hello 間隔 (Hello Interval)	DTLS または TLS WAN トランスポート接続で送信される Hello パケットの間隔を入力します。範囲：100 ～ 10000 ミリ秒。デフォルト：1000 ミリ秒 (1 秒)
Hello 許容度	トランスポートトンネルのダウンを宣言する前に、DTLS または TLS WAN トランスポート接続で Hello パケットを待機する時間を入力します。 範囲：12 ～ 60 秒。デフォルト：12 秒

インターフェイスを NAT デバイスとして設定する

ポート転送などのアプリケーションの NAT デバイスとして機能するようにインターフェイスを設定するには、[NAT] を選択し、[On] をクリックして、次のパラメータを設定します。

表 49:

パラメータ名	説明
NAT	[On] をクリックして、インターフェイスを NAT デバイスとして機能させます。
Refresh Mode	NAT マッピングを更新する方法 (アウトバウンドまたは双方向 (アウトバウンドとインバウンド) のいずれか) を選択します。デフォルト：アウトバウンド
[UDP Timeout]	UDP セッションを介した NAT 変換がいつタイムアウトするかを指定します。範囲：1 ～ 65536 分。デフォルト：1 分
[TCP Timeout]	TCP セッションを介した NAT 変換がいつタイムアウトするかを指定します。範囲：1 ～ 65536 分。デフォルト：60 分 (1 時間)
Block ICMP	[On] を選択して、インバウンド ICMP エラーメッセージをブロックします。デフォルトでは、NAT デバイスとして機能するルータは、これらのエラーメッセージを受け取ります。デフォルト：Off
Respond to Ping	接続のパブリック側から受信した NAT インターフェイスの IP アドレスへの ping 要求にルータが応答するようにするには、[On] を選択します。

ポート転送ルールを作成するには、[Add New Port Forwarding Rule] をクリックし、次のパラメータを設定します。最大 128 のポート転送ルールを定義して、外部ネットワークからの要求が内部ネットワーク上のデバイスに到達できるようにすることができます。

表 50:

パラメータ名	説明
Port Start Range	ポート番号を入力して、ポートまたは対象の範囲の最初のポートを定義します。範囲：0～65535
Port End Range	同じポート番号を入力してポート転送を1つのポートに適用するか、より大きい番号を入力してポートの範囲に適用します。範囲：0～65535
プロトコル	ポート転送ルールを適用するプロトコル（[TCP] または [UDP]）を選択します。TCP トラフィックと UDP トラフィックの両方で同じポートを一致させるには、2つのルールを構成します。
VPN	内部サーバーが存在するプライベート VPN を指定します。この VPN は、オーバーレイネットワークの VPN 識別子の1つです。範囲：0～65530
プライベート IP	ポート転送ルールに一致するトラフィックの転送先となる内部サーバーの IP アドレスを指定します。

ポート転送ルールを保存するには、[Add] をクリックします。

機能テンプレートを保存するには、[Save] をクリックします。

アクセスリストの適用

ルータインターフェイスに書き換えルール、アクセスリスト、およびポリサーを適用するには、[ACL] をクリックし、次のパラメータを設定します。

表 51:

パラメータ名	説明
Shaping rate	インターフェイスの集約トラフィック転送速度を、回線速度よりも低く設定します（キロビット/秒（kbps）単位）。
QoS マップ	インターフェイスから送信されるパケットに適用する QoS マップの名前を指定します。
リライトルール	[On] をクリックし、インターフェイスに適用する書き換えルールの名前を指定します。
入力 ACL – IPv4	[On] をクリックして、インターフェイスで受信される IPv4 パケットに適用するアクセスリストの名前を指定します。
出力 ACL – IPv4	[On] をクリックし、インターフェイスで送信される IPv4 パケットに適用するアクセスリストの名前を指定します。
入力 ACL – IPv6	[On] をクリックして、インターフェイスで受信される IPv6 パケットに適用するアクセスリストの名前を指定します。

パラメータ名	説明
出力 ACL – IPv6	[On] をクリックし、インターフェイスで送信される IPv6 パケットに適用するアクセスリストの名前を指定します。
入力ポリサー	[On] をクリックして、インターフェイスで受信されるパケットに適用するポリサーの名前を指定します。
出力ポリサー	[On] をクリックして、インターフェイスで送信されるパケットに適用するポリサーの名前を指定します。

機能テンプレートを保存するには、[Save] をクリックします。

その他のインターフェイスプロパティの設定

他のインターフェイスプロパティを設定するには、[Advanced] をクリックし、次のプロパティを設定します。

表 52:

パラメータ名	説明
Bandwidth Upstream	送信トラフィックについて、通知を生成する帯域幅を設定します。範囲：1 ~ $(2^{32}/2) - 1$ kbps
Bandwidth Downstream	受信トラフィックについて、通知を生成する帯域幅を設定します。範囲：1 ~ $(2^{32}/2) - 1$ kbps
IP MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。範囲：576 ~ 1804。デフォルト：1500 バイト
TCP MSS	ルータを通過する TCP SYN パケットの最大セグメントサイズ (MSS) を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ~ 1460 バイト。デフォルト：なし
TLOC Extension	WAN トランスポート回線に接続する同じルータ上の物理インターフェイスの名前を入力します。次に、この構成により、このサービス側のインターフェイスが WAN トランスポートにバインドされます。それ自体は WAN に直接接続されておらず（通常、サイトには 1 つの WAN 接続しかないため）、同じサイトにあり、このサービス側インターフェイスに接続する 2 番目のルータには、WAN への接続が提供されます。
Tracker	インターネットに接続するトランスポートインターフェイスのステータスをトラッキングするトラッカーの名前を入力します。

パラメータ名	説明
IP Directed-Broadcast	ダイレクトブロードキャストの物理ブロードキャストへの変換を有効にします。IP ダイレクトブロードキャストは、宛先アドレスが何らかの IP サブネットの有効なブロードキャストアドレスであるにもかかわらず、その宛先サブネットに含まれないノードから発信される IP パケットです。

機能テンプレートを保存するには、[Save] をクリックします。

リリース情報

リリース 18.4.1 の Cisco vManage NMS で導入されました。

Cisco VPN インターフェイス GRE

ファイアウォールなどのサービスが、GRE トンネルのみをサポートするデバイスで使用できる場合、論理 GRE インターフェイスを設定することにより、デバイスに GRE トンネルを設定して、リモートデバイスに接続できます。これにより、サービスが GRE トンネルを介して利用可能であることをアドバタイズし、適切なトラフィックをトンネルに送信するデータポリシーを作成できます。GRE インターフェイスは、設定されるとすぐに起動し、物理トンネルインターフェイスが起動している限り起動し続けます。

Cisco vManage テンプレートを使用して GRE 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。

1. Cisco VPN インターフェイス GRE 機能テンプレートを作成して、GRE インターフェイスを設定します。
2. GRE トンネル経由で到達可能なサービスをアドバタイズし、GRE 固有の静的ルートを設定し、他の VPN パラメータを設定する Cisco VPN 機能テンプレートを作成します。
3. **set-service service-name local** コマンドを含む、サービス VPN に適用されるデータポリシーを Cisco vSmart コントローラ で作成します。

[Template] 画面に移動し、テンプレートに命名する

1. Cisco vManage のメニューから、[Configuration] > [Templates] を選択します。
2. [Device Templates] をクリックし、[Create Template] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

3. [Create Template] ドロップダウンリストから、[From Feature Template] を選択します。

4. [Device Model] ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。
5. VPN 0 または VPN 512 のテンプレートを作成するには、次の手順を実行します。
 1. [Transport & Management VPN] をクリックするか、[Transport & Management VPN] セクションまでスクロールします。
 2. [Additional VPN 0 Templates] で、[VPN Interface GRE] をクリックします。
 3. [VPN Interface GRE] ドロップダウンリストから、[Create Template] をクリックします。VPN インターフェイス GRE テンプレートフォームが表示されます。
このフォームには、テンプレートに名前を付けるためのフィールドと、VPN インターフェイス GRE パラメータを定義するためのフィールドが含まれています。
6. [Template Name] に、テンプレートの名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。
7. [Template Description] に、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。

初めて機能テンプレートを開くと、デフォルト値を持つパラメータごとに、その範囲が [Default] に設定され（チェックマークで示される）、デフォルト設定またはデフォルト値が表示されます。デフォルト値を変更するか、値を入力するには、パラメータフィールドの左側にある [Scope] ドロップダウンをクリックし、パラメータ範囲を選択します。

基本的な GRE インターフェイスの設定

基本的な GRE インターフェイスを設定するには、[Basic Configuration] をクリックして、次のパラメータを設定します。GRE インターフェイスを設定する場合、アスタリスクの付いたパラメータは必須です。

表 53:

パラメータ名	説明
Shutdown*	インターフェイスを有効にするには [Off] をクリックします。
Interface Name*	GRE インターフェイスの名前を入力します。形式は gre number です。 <i>number</i> には 1 ~ 255 を指定できます。
説明	GRE インターフェイスの説明を入力します。

パラメータ名	説明
Source*	GRE インターフェイスの送信元を入力します。 <ul style="list-style-type: none"> • GRE Source IP Address : GRE トンネルインターフェイスの送信元 IP アドレスを入力します。このアドレスはローカルルータ上にあります。 • Tunnel Source Interface : GRE トンネルの送信元である物理インターフェイスを入力します。
Destination*	GRE トンネルインターフェイスの宛先 IP アドレスを入力します。このアドレスはリモートデバイス上にあります。
GRE Destination IP Address*	GRE トンネルインターフェイスの宛先 IP アドレスを入力します。このアドレスはリモートデバイス上にあります
IPv4 Address	GRE トンネルの IPv4 アドレスを入力します。
IP MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。範囲 : 576 ~ 1804、デフォルト : 1500 バイト
Clear-Dont-Fragment	[On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Don't Fragment ビットをクリアします。
TCP MSS	Cisco vEdge デバイス を通過する TCP SYN パケットの最大セグメントサイズ (MSS) を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲 : 552 ~ 1460 バイト、デフォルト : なし

機能テンプレートを保存するには、[Save] をクリックします。

インターフェイス アクセス リストの設定

GRE インターフェイスでアクセスリストを設定するには、[ACL] をクリックして、次のパラメータを設定します。

表 54:

パラメータ名	説明
リライトルール	[On] をクリックし、インターフェイスに適用する書き換えルールの名前を指定します。
入力 ACL - IPv4	[On] をクリックして、インターフェイスで受信される IPv4 パケットに適用するアクセスリストの名前を指定します。

パラメータ名	説明
出力 ACL – IPv4	[On] をクリックし、インターフェイスで送信される IPv4 パケットに適用するアクセスリストの名前を指定します。

トラッカーインターフェイスの設定

GRE インターフェイスのステータスをトラッキングするようにトラッカーインターフェイスを設定するには、[Advanced] を選択し、次のパラメータを設定します。

表 55:

パラメータ名	説明
Tracker	インターネットに接続する GRE インターフェイスのステータスをトラッキングするトラッカーの名前を入力します。

VPN インターフェイス IPsec

VPN インターフェイス IPsec 機能テンプレートを使用して、インターネット キー エクスチェンジ (IKE) セッションに使用されている Cisco IOS XE サービス VPN で IPsec トンネルを設定します。512 を除く、VPN 1 から 65530 までのトンネルで IPsec を構成できます。

Cisco Cisco IOS XE SD-WAN デバイスは、VPN の代わりに VRF を使用します。ただし、Cisco vManage を介した Cisco IOS XE SD-WAN デバイスの設定には引き続き次の手順が適用されます。Cisco vManage では、システムが VPN 設定を VRF 設定に自動的にマッピングします。

VPN IPsec インターフェイス テンプレートの作成

ステップ 1 Cisco vManage メニューから、[Configuration] > [Templates] を選択します。

ステップ 2 [Feature Templates] をクリックします。

(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

ステップ 3 [Add template] をクリックします。

ステップ 4 リストから Cisco IOS XE SD-WAN デバイス を選択します。

ステップ 5 [VPN] セクションで、[VPN Interface IPsec] をクリックします。Cisco VPN インターフェイス IPsec テンプレートが表示されます。

ステップ 6 [Template Name] に、テンプレートの名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。

ステップ7 [Template Description] に、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。

基本設定

基本的な IPsec トンネルインターフェイスを設定するには、[Basic Configuration] を選択し、次のパラメータを設定します。

パラメータ名	オプション/フォーマット	説明
Shutdown*	Yes / No	インターフェイスを有効にするには[No]をクリックし、無効にするには[Yes]をクリックします。
Interface Name*	ipsec number (1...255)	IPsec インターフェイスの名前を入力します。 Number は 1 ~ 255 を指定できます。
説明	IPsec インターフェイスの説明を入力します。	
IPv4 Address*	ipv4-prefix/length	IPsec インターフェイスの IPv4 アドレスを入力します。アドレスには /30 サブネットが必要です。
Source *	IKE キー交換に使用されている IPsec トンネルの送信元を設定します。	
	IP Address	クリックして、送信元トンネルインターフェイスである IPv4 アドレスを入力します。このアドレスは、VPN 0 で設定する必要があります。
	インターフェイス (Interface)	<p>クリックして、IPsec トンネルの送信元である物理インターフェイスの名前を入力します。このインターフェイスは、VPN 0 で設定する必要があります。</p> <ul style="list-style-type: none"> • [Source] にインターフェイスを選択した場合は、送信元インターフェイスの名前を入力します。ループバック インターフェイスを入力すると、[Tunnel Route-via Interface] フィールドが表示されます。ここには出力インターフェイスの名前を入力します。

パラメータ名	オプション/フォーマット	説明
Destination*		IKE キー交換に使用されている IPsec トンネルの宛先を設定します。
	IPsec Destination IP Address	宛先をポイントする IPv4 アドレスを入力します。
	TCP MSS	ルータを通過する TCP SYN パケットの最大セグメントサイズ (MSS) を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。 範囲：552 ～ 1960 バイト デフォルト：なし
	IP MTU	インターフェイス上のパケットの最大伝送ユニット (MTU) サイズを指定します。 範囲：576 ～ 2000 デフォルト：1500 バイト

CLI での同等コマンド

```
crypto
  interface tunnel ifnum
    no shutdown
    vrf forwarding vrf_id
    ip address ip_address[mask]
    tunnel source wanif_ip
    tunnel mode {ipsec ipv4 | gre ip}
    tunnel destination gateway_ip
    tunnel protection ipsec profile ipsec_profile_name
```

デッドピア検出の設定

インターネットキーエクスチェンジ (IKE) の Dead Peer Detection (DPD; デッドピア検出) を設定して、IKE ピアへの接続が機能していて到達可能かどうかを判別するには、[DPD] をクリックして、次のパラメータを設定します。

パラメータ名	説明
DPD Interval	IKE が接続で Hello パケットを送信する間隔を指定します。 範囲：10 ～ 3600 秒 デフォルト：無効

パラメータ名	説明
DPD Retries	IKE ピアがデッド状態であると宣言してピアへのトンネルを切断するまでに許容する、確認応答のないパケットの数を指定します。 範囲：2 ～ 60 デフォルト：3

機能テンプレートを保存するには、[Save] をクリックします。

CLI での同等コマンド

```
crypto
 ikev2
  profile ikev2_profile_name
    dpd 10-3600 2-60 {on-demand | periodic}
```

IKE の設定

表 56: 機能の履歴

機能名	リリース情報	説明
IPsec トンネルの SHA256 サポート	Cisco IOS XE リリース 17.2.1r	この機能により、セキュリティを強化するための HMAC_SHA256 アルゴリズムのサポートが追加されます。

IKE を設定するには、[IKE] をクリックして、次のパラメータを設定します。



- (注) Cisco IOS XE SD-WAN デバイスで IPsec トンネルを作成すると、トンネルインターフェイスで IKE バージョン 1 がデフォルトで有効になります。

IKE バージョン 1 および IKE バージョン 2

IKEv1 および IKEv2 トラフィックを伝送する IPsec トンネルを設定するには、[IPSEC] をクリックして、次のパラメータを設定します。

パラメータ名	オプション	Description
IKE Version	[1] IKEv1 [2] IKEv2	[1] を入力して IKEv1 を選択します。 [2] を入力して IKEv2 を選択します。 デフォルト：IKEv1

パラメータ名	オプション	Description
IKE Mode	Aggressive mode Main mode	<p>IKEv1 の場合のみ、次のいずれかのモードを指定します。</p> <ul style="list-style-type: none"> • [Aggressive mode] : ネゴシエーションが速くなり、イニシエータとレスポンドの ID が平文で渡されます。 • IPsec ネゴシエーションを開始する前に、IKE SA セッションを確立します。 <p>(注) IKEv2 の場合、モードはありません。</p> <p>(注) 事前共有キーを使用した IKE アグレッシブモードは、可能な限り避ける必要があります。それ以外の場合は、強力な事前共有キーを選択する必要があります。</p> <p>デフォルト : [Main mode]</p>
IPsec Rekey Interval	3600 ~ 1209600 秒	<p>IKE キーを更新する間隔を指定します。</p> <p>範囲 : 1 時間から 14 日</p> <p>デフォルト : 14400 秒 (4 時間)</p>
IKE Cipher Suite	3DES 192-AES 256-AES [AES] [DES]	<p>IKE キー交換中に使用する認証と暗号化のタイプを指定します。</p> <p>デフォルト : 256-AES</p>
IKE Diffie-Hellman Group	2 14 15 16	<p>IKEv1 または IKEv2 のいずれかで、IKE キー交換で使用する Diffie-Hellman グループを指定します。</p> <ul style="list-style-type: none"> • 1024 ビットの係数 • 2048 ビットの係数 • 3072 ビットの係数 • 4096 ビットの係数 <p>デフォルト : 4096 ビットの係数</p>

パラメータ名	オプション	Description
IKE 認証		IKE 認証を設定します。
	Preshared Key	事前共有キーで使用するパスワードを入力します。
	IKE ID for Local End Point	リモート IKE ピアがローカルエンドポイント識別子を必要とする場合は、それを指定します。 範囲：1～64 文字 デフォルト：トンネルのソース IP アドレス
	IKE ID for Remote End Point	リモート IKE ピアがリモートエンドポイント識別子を必要とする場合は、それを指定します。 範囲：1～64 文字 デフォルト：トンネルの宛先 IP アドレス

機能テンプレートを保存するには、[Save] をクリックします。

IKE バージョンを IKEv1 から IKEv2 に変更する

IKE バージョンを変更するには、次の手順を実行します。

1. Cisco vManage のメニューから、[Configuration] > [Templates] を選択します。
2. [Feature Templates] をクリックしてから、[Add Template] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] は [Feature] と呼ばれます。

3. テンプレートを作成するデバイスを選択します。
4. [Basic Configuration] をクリックします。
5. トンネルをシャットダウンするには、[shutdown] パラメータを [yes] オプション ([yes shutdown]) とともに使用します。
6. IPsec プロファイルから ISAKMP プロファイルを削除します。
7. IKEv2 プロファイルを IPsec プロファイルにアタッチします。



(注) IKEv2 プロファイルがすでにある場合は、この手順を実行します。それ以外の場合は、最初に IKEv2 プロファイルを作成します。

- トンネルを開始するには、[no] オプション ([no shutdown]) を指定して shutdown パラメータを使用します。



(注) [shutdown] 操作は、2 つの別個の操作で発行する必要があります。



(注) IKE バージョンを変更するための単一の CLI はありません。「IKE バージョンを IKEv1 から IKEv2 に変更する」セクションに記載されている一連の手順に従う必要があります。

IKEv1 の場合の CLI での 同等コマンド

IKEv1 の場合の ISAKMP CLI 設定

```
crypto
  isakmp
    keepalive 60-86400 2-60 {on-demand | periodic}
    policy policy_num
      encryption {AES128-CBC-SHA1 | AES256-CBC-SHA1}
      hash {sha384 | sha256 | sha}
      authentication pre-share
      group {2 | 14 | 16 | 19 | 20 | 21}
      lifetime 60-86400
    profile ikev1_profile_name
      match identity address ip_address [mask]
      keyring keyring_name
```

IKEv1 の場合の IPsec CLI 設定

```
profile ipsec_profile_name
  set transform-set transform_set_name
  set isakmp-profile ikev1_profile_name
  set security-association
    lifetime {kilobytes disable | seconds 120-2592000}
    replay {disable | window-size {64 | 128 | 256 | 512 | 1024}}
  set pfs group {14 | 16 | 19 | 20 | 21}
  keyring keyring_name
  pre-shared-key address ip_address [mask] key key_string
  ipsec transform-set transform_set_name {esp-gcm 256 | esp-aes 256 [esp-sha384-hmac |
  esp-sha256-hmac] mode tunnel
```

手順の概要

- enable
- configure terminal
- crypto isakmp policy *priority*
- encryption {des | 3des | aes | aes 192 | aes 256 }
- hash {sha | sha256 | sha384 | md5 }
- authentication {rsa-sig | rsa-encr | pre-share }

7. group {1 | 2 | 5 | 14 | 15 | 16 | 19 | 20 | 24 }
8. lifetime *seconds*
9. exit
10. exit

IKE2 の場合の CLI での同等コマンド

```
crypto
  ikev2
    proposal proposal_name
      encryption {3des | aes-cbc-128 | aes-cbc-192 | aes-cbc-256 | des}
      integrity {sha256 | sha384 | sha512}
      group {2 | 14 | 15 | 16}
    keyring idev2_keyring_name
    peer peer_name
      address tunnel_dest_ip [mask]
      pre-shared-key key_string
    profile ikev2_profile_name
      match identity remote address ip_address
      authentication {remote | local} pre-share
      keyring local ikev2_keyring_name
      lifetime 120-86400
```

IPsec トンネルパラメータの設定

IKE トラフィックを伝送する IPsec トンネルを設定するには、[IPSEC] をクリックして、次のパラメータを設定します。

パラメータ名	[オプション (Options)]	Description
IPsec Rekey Interval	3600 ~ 1209600 秒	IKE キーを更新する間隔を指定します。 範囲：1 時間から 14 日 デフォルト：3600 秒
IKE Replay Window	64、128、256、512、 1024、2048、4096、8192	IPsec トンネルのリプレイウィンドウサイズを指定します。 デフォルト：512
IPsec Cipher Suite	aes256-cbc-sha1 aes256-gcm null-sha1	IPsec トンネルで使用する認証と暗号化を指定します。 デフォルト：aes256-gcm

パラメータ名	[オプション (Options)]	Description
Perfect Forward Secrecy	2 1024 ビットの係数 14 2048 ビットの係数 15 3072 ビットの係数 16 4096 ビットの係数 none	IPsec トンネルで使用する PFS 設定を指定します。 次の Diffie-Hellman 素数係数グループのいずれかを選択します。 1024 ビット：グループ 2 2048 ビット：グループ 14 3072 ビット：グループ 15 4096 ビット：グループ 16 なし：PFS を無効にします。 デフォルト：グループ 16

機能テンプレートを保存するには、[Save] をクリックします。

CLI での同等コマンド

```
crypto
 ipsec
   profile ipsec_profile_name
     set ikev2-profile ikev2_profile_name
     set security-association
       lifetime {seconds 120-2592000 | kilobytes disable}
       replay {disable | window-size {64 | 128 | 256 | 512 | 1024 | 4096 | 8192}}
     set pfs group {2 | 14 | 15 | 16 | none}
     set transform-set transform_set_name
```

リリース情報

Cisco IOS XE SD-WAN リリース 16.11.x の Cisco vManage で導入されました。

VPN インターフェイス マルチリンク

Cisco SD-WAN ソフトウェアを実行している Cisco IOS XE SD-WAN デバイスには、VPN インターフェイス マルチリンク テンプレートを使用します。



- (注) Cisco IOS XE SD-WAN デバイスは、VPN の代わりに VRF を使用します。ただし、Cisco vManage を介した Cisco IOS XE SD-WAN デバイスの設定には引き続き次の手順が適用されます。設定を完了すると、VPN 設定が VRF 設定に自動的にマッピングされます。

マルチリンク ポイント ツー ポイント プロトコル (MLP) は、複数の物理リンクを、MLP バンドルと呼ばれる単一の論理接続に結合するために使用されます。

Cisco vManage テンプレートを使用して Cisco IOS XE SD-WAN デバイスでマルチリンクを構成するには、次の手順を実行します。

1. VPN インターフェイス マルチリンク 機能テンプレートを作成して、マルチリンク インターフェイスのプロパティを構成します。
2. 必要に応じて、VPN 機能テンプレートを作成して、VPN 0 の既定の構成を変更します。

[Template] 画面に移動し、テンプレートに命名する

1. Cisco vManage メニューから、[Configuration] > [Templates] を選択します。
2. [Device Templates] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

3. [Create Template] ドロップダウンリストから、[From Feature Template] を選択します。
4. [Device Model] ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。
5. トランスポート VPN (VPN0) でマルチリンク インターフェイスを構成している場合は、次の手順を実行します。
 1. [Transport & Management VPN] をクリックするか、[Transport & Management VPN] セクションまでスクロールします。
 2. 画面の右側にある [Additional VPN 0 Templates] の下で、[VPN Interface Multilink Controller] をクリックします。
6. サービス VPN (VPN 0 以外の VPN) でマルチリンク インターフェイスを構成している場合は、次の手順を実行します。
 1. [Service VPN] をクリックするか、[Service VPN] セクションまでスクロールします。
 2. [Service VPN] ドロップダウンリストで、サービス VPN の番号を入力します。
 3. 画面の右側にある [Additional VPN Templates] の下で、[VPN Interface Multilink Controller] をクリックします。
7. [VPN Interface Multilink Controller] ドロップダウンリストから、[Create Template] をクリックします。[VPN Multilink] テンプレートフォームが表示されます。このフォームには、テンプレートに名前を付けるためのフィールドと、マルチリンク インターフェイス パラメータを定義するためのフィールドが含まれています。
8. [Template Name] に、テンプレートの名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。

9. [Template Description] に、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。

初めて機能テンプレートを開くと、デフォルト値を持つパラメータごとに、その範囲が [Default] に設定され（チェックマークで示される）、デフォルト設定またはデフォルト値が表示されます。デフォルト値を変更するか、値を入力するには、パラメータフィールドの左側にある [Scope] ドロップダウンをクリックし、次のいずれかを選択します。

表 57:

パラメータの範囲	範囲の説明
デバイス固有（ホストのアイコンで示される）	<p>デバイス固有の値がパラメータに使用されます。デバイス固有のパラメータの場合、機能テンプレートに値を入力できません。Viptela デバイスをデバイステンプレートに添付するときに、値を入力します。</p> <p>[Device Specific] をクリックすると、[Enter Key] ボックスが表示されます。このボックスには、作成する CSV ファイル内のパラメータを識別する一意の文字列であるキーが表示されます。このファイルは、キーごとに 1 つの列を含む Excel スプレッドシートです。ヘッダー行にはキー名（行ごとに 1 つのキー）が含まれます。その後の各行は、デバイスに対応し、そのデバイスのキーの値を定義します。Viptela デバイスをデバイステンプレートに添付するときに、この CSV ファイルをアップロードします。詳細については、「Create a Template Variables Spreadsheet」を参照してください。</p> <p>デフォルトのキーを変更するには、新しい文字列を入力し、[Enter Key] ボックスの外にカーソルを移動します。</p> <p>デバイス固有のパラメータの例としては、システム IP アドレス、ホスト名、GPS ロケーション、サイト ID があります。</p>
グローバル（地球のアイコンで示される）	<p>パラメータの値を入力し、その値をすべてのデバイスに適用します。</p> <p>デバイスのグループにグローバルに適用できるパラメータの例としては、DNS サーバー、Syslog サーバー、インターフェイス MTU があります。</p>

マルチリンク インターフェイスの構成

マルチリンク インターフェイスを構成するには、[Basic Configuration] を選択し、次のパラメータを構成します。インターフェイスを設定する場合、アスタリスクの付いたパラメータは必須です。



- (注) VPN インターフェイス マルチリンク テンプレートを作成する場合は、T1/E1 コントローラ テンプレートまたは VPN インターフェイス T1/E1 テンプレートを作成する必要はありません。

表 58:

パラメータ名	説明
Shutdown*	[No] をクリックして、マルチリンク インターフェイスを有効にします。
Interface Name*	MLP インターフェイスの番号を入力します。1 から 65,535 までの数値を指定できます。
説明	マルチリンク インターフェイスの説明を入力します。
Multilink Group Number*	マルチリンクグループの番号を入力します。1 ~ 65,535 の数値を指定できますが、Multilink Interface Name パラメータに入力する数値と同じである必要があります。
IPv4 Address*	静的アドレスを構成するには、[Static] をクリックして、IPv4 アドレスを入力します。 インターフェイスを DHCP クライアントとして設定して、インターフェイスが DHCP サーバーから IP アドレスを受け取るようにするには、[Dynamic] をクリックします。オプションで、DHCP ディスタンスを設定して、DHCP サーバーから学習したルートのアドミニストレーティブディスタンスを指定できます。デフォルトの DHCP ディスタンスは 1 です。
IPv6 Address*	VPN 0 のインターフェイスに静的アドレスを設定するには、[Static] をクリックして、IPv6 アドレスを入力します。 インターフェイスを DHCP クライアントとして設定して、インターフェイスが DHCP サーバーから IP アドレスを受け取るようにするには、[Dynamic] をクリックします。オプションで、DHCP ディスタンスを設定して、DHCP サーバーから学習したルートのアドミニストレーティブディスタンスを指定できます。デフォルトの DHCP ディスタンスは 1 です。オプションで DHCP 高速コミットを有効にして、IP アドレスの割り当てを高速化できます。
Bandwidth Upstream	送信トラフィックについて、通知を生成する帯域幅を設定します。範囲：1 ~ $(2^{32}/2) - 1$ kbps
Bandwidth Downstream	受信トラフィックについて、通知を生成する帯域幅を設定します。範囲：1 ~ $(2^{32}/2) - 1$ kbps
IP MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。MLP のカプセル化は、アウトバウンドパケットのそれぞれに 6 バイト (4 バイトのヘッダーと 2 バイトのチェックサム) を追加します。これらのオーバーヘッドバイトは、実質的な接続の帯域幅を減少させます。そのため、MLP バンドルのスループットは、MLP を使用しない同等の帯域幅接続よりもわずかに少なくなっています。範囲：576 ~ 1804、デフォルト：1500 バイト

機能テンプレートを保存するには、[Save] をクリックします。

PPP 認証プロトコルの構成

PPP 認証プロトコルを構成するには、[PPP] を選択し、次のパラメータを設定します。

表 59:

パラメータ名	説明
認証プロトコル (Authentication Protocol)	MLP で使用される認証プロトコルを選択します。 <ul style="list-style-type: none"> • CHAP : インターネット サービス プロバイダー (ISP) から提供されたホスト名とパスワードを入力します。ホスト名は最大 255 文字です。 • PAP : ISP から提供されたユーザー名とパスワードを入力します。ユーザー名は最大 255 文字です。 • PAP および CHAP : 両方の認証プロトコルを設定します。それぞれのプロトコルのログイン情報を入力します。両方に同じユーザー名とパスワードを使用するには、[Same Credentials for PAP and CHAP] をクリックします。

機能テンプレートを保存するには、[Save] をクリックします。

トンネルインターフェイスの作成

最大4つのトンネルインターフェイスを設定できます。つまり、各デバイスに最大4つのTLOCを設定できます。

オーバーレイネットワークが機能できるようにコントロールプレーンがそれ自体を確立するには、VPN 0 で WAN トランスポート インターフェイスを設定する必要があります。

マルチリンク インターフェイスのトンネルインターフェイスを設定するには、[Tunnel Interface] タブを選択し、次のパラメータを設定します。

表 60:

パラメータ名	説明
トンネルインターフェイス	[On] をクリックして、トンネルインターフェイスを作成します。
色	TLOC の色を選択します。

パラメータ名	説明
制御接続	<p>デフォルトでは、制御接続は [On] に設定されており、TLOC の制御接続を確立します。ルータに複数の TLOC がある場合は、[No] をクリックして、トンネルが TLOC の制御接続を確立しないようにします。</p> <p>(注) 接続トラフィックでのデータ/パケットの損失を避けるために、デフォルトの 1 秒の hello インターバルと 12 秒の hello トレランスパラメータを設定して、最低 650 ~ 700 Kbps の帯域幅を設定することをお勧めします。</p> <p>BFD セッションごとに、175 バイトの追加の平均サイズ BFD パケットは、1.4 Kbps の帯域幅を消費します。</p> <p>双方向 BFD パケットフローに必要な帯域幅の計算例を以下に示します。</p> <ul style="list-style-type: none"> • 制御接続用にデバイスごとに 650 ~ 700 Kbps。 • デバイス上の BFD セッション (要求) ごとに 175 バイト (または 1.4 Kbps) • デバイス上の BFD セッション (応答) ごとに 175 バイト (または 1.4 Kbps) <p>パス MTU ディスカバリ (PMTUD) が有効になっている場合、30 秒ごと、トンネルごとに BFD パケットを送受信するための帯域幅 :</p> <p>1500 バイトの BFD 要求パケットは、30 秒ごと、トンネルごとに送信されます。</p> <p>$1500 \text{ バイト} * 8 \text{ ビット/1 バイト} * 1 \text{ パケット/30 秒} = 400 \text{ bps}$ (要求)</p> <p>147 バイトの BFD パケットが応答として送信されます。</p> <p>$147 \text{ バイト} * 8 \text{ ビット/1 バイト} * 1 \text{ パケット/30 秒} = 40 \text{ bps}$ (応答)</p> <p>したがって、たとえば 775 BFD セッションを持つデバイスの場合、次の帯域幅が必要です。</p> <p>$700k + (1.4k * 775) + (400 * 775) + (1.4k * 775) + (40 * 775)$ $= \sim 3.5 \text{ MBps}$</p>
最大制御接続数	<p>WAN トンネルインターフェイスが接続できる Cisco vSmart コントローラの最大数を指定します。トンネルが制御接続を確立しないようにするには、この数値を 0 に設定します。</p> <p>範囲 : 0 ~ 8、デフォルト : 2</p>

パラメータ名	説明
vBond As STUN Server	[On] をクリックして NAT (STUN) のセッショントラバーサルユーティリティを有効にし、デバイスが NAT の背後にある場合にトンネルインターフェイスがパブリック IP アドレスとポート番号を検出できるようにします。
コントローラグループリストの除外	トンネルインターフェイスが接続できない Cisco vSmart コントローラを設定します。範囲：0 ~ 100
vManage 接続設定	トンネルインターフェイスを使用して制御トラフィックを vManage NMS と交換するための優先順位を設定します。範囲：0 ~ 8、デフォルト：5
ポートホップ	ポートホッピングを有効にするには [On] をクリックし、無効にするには [Off] をクリックします。ルータが NAT の背後にある場合、ポートホッピングは、事前に選択された OMP ポート番号（ベースポートと呼ばれる）のプールを循環して、接続の試行が失敗したときに他のルータとの DTLS 接続を確立します。デフォルトのベースポートは 12346、12366、12386、12406、および 12426 です。ベースポートを変更するには、ポートオフセット値を設定します。デフォルト：有効
低帯域幅リンク	トンネルインターフェイスを低帯域幅リンクとして特徴付ける場合に選択します。
トンネル TCP MSS	<p>TCP MSS は、ルータを通過する最初の TCP ヘッダーを含むすべてのパケットに影響します。設定すると、TCP MSS は、スリーウェイハンドシェイクで交換される MSS に対して検査されます。構成済みの TCP MSS 設定がヘッダーの MSS よりも小さい場合、ヘッダーの MSS の値が減少します。MSS ヘッダー値がすでに TCP MSS よりも低い場合、パケットは変更されずに通過します。トンネルの最後にあるホストは、2つのホストの低い方の設定を使用します。TCP MSS を設定する場合は、最小パス MTU より 40 バイト小さく設定する必要があります。</p> <p>Cisco IOS XE SD-WAN デバイスを通過する TCP SYN パケットの MSS を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ~ 1460 バイト、デフォルト：なし</p>

パラメータ名	説明
Clear-Dont-Fragment	<p>Don't Fragment が設定されているインターフェイスに到着するパケットの [Clear-Dont-Fragment] を設定します。これらのパケットが MTU が許可するサイズより大きい場合、それらはドロップされます。Don't Fragment ビットをクリアすると、パケットはフラグメント化されて送信されます。</p> <p>[On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Dont Fragment ビットをクリアします。Dont Fragment ビットがクリアされると、インターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。</p> <p>(注) [Clear-Dont-Fragment] は Dont Fragment ビットをクリアし、Dont Fragment ビットが設定されます。フラグメンテーションを必要としないパケットの場合、Dont Fragment ビットは影響を受けません。</p>
サービスの許可	サービスごとに [On] または [Off] を選択して、インターフェイスでサービスを許可または禁止します。

追加のトンネルインターフェイスパラメータを設定するには、[Advanced Options] をクリックして、次のパラメータを設定します。

表 61:

パラメータ名	説明
GRE	<p>トンネルインターフェイスで GRE カプセル化を使用します。デフォルトでは、GRE は無効になっています。</p> <p>IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。</p>
IPSec	<p>トンネルインターフェイスで IPsec カプセル化を使用します。デフォルトでは、IPsec は有効になっています。</p> <p>IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。</p>
IPsec Preference	<p>トラフィックをトンネルに誘導するための優先値を指定します。高い値が低い値に優先します。</p> <p>範囲：0 ~ 4294967295。デフォルト：0</p>

パラメータ名	説明
IPsec の重み	<p>複数の TLOC 間でトラフィックのバランスをとるために使用する重みを入力します。値が大きいほど、より多くのトラフィックがトンネルに送信されます。</p> <p>範囲：1～255。デフォルト：1</p>
通信事業者	<p>トンネルに関連付けるキャリア名またはプライベートネットワーク識別子を選択します。</p> <p>値：carrier1、carrier2、carrier3、carrier4、carrier5、carrier6、carrier7、carrier8、デフォルト。デフォルト：デフォルト</p>
ループバックトンネルのバインド	<p>ループバック インターフェイスにバインドする物理インターフェイスの名前を入力します。</p>
ラストリゾート回線	<p>トンネルインターフェイスを最終手段の回線として使用する場合に選択します。</p> <p>(注) ラストリゾート回線として構成されたインターフェイスはダウンすると予想され、制御接続の数の計算中にスキップされ、セルラーモデムは休止状態になり、トラフィックは回線上で送信されません。</p> <p>セルラーインターフェイスを備えたエッジデバイスで設定がアクティブ化されると、すべてのインターフェイスが制御および BFD 接続を確立するプロセスを開始します。1つ以上のプライマリインターフェイスが BFD 接続を確立すると、最終手段の回線は自動的にシャットダウンします。</p> <p>すべてのプライマリインターフェイスがリモートエッジへの接続を失った場合にのみ、ラストリゾート回線がアクティブになり、エッジデバイスで BFD TLOC ダウンアラームと制御 TLOC ダウンアラームがトリガーされます。ラストリゾートインターフェイスは、エッジデバイスのバックアップ回線として使用され、他のすべてのトランスポートリンク BFD セッションが失敗したときにアクティブ化されます。このモードでは、無線インターフェイスはオフになり、セルラーインターフェイスを介した制御またはデータ接続は存在しません。</p>
NAT 更新間隔	<p>DTLS または TLS WAN トランスポート接続で送信される NAT リフレッシュパケットの間隔を入力します。範囲：1～60 秒。デフォルト：5 秒</p>
Hello 間隔 (Hello Interval)	<p>DTLS または TLS WAN トランスポート接続で送信される Hello パケットの間隔を入力します。範囲：100～10000 ミリ秒。デフォルト：1000 ミリ秒 (1 秒)</p>

パラメータ名	説明
Hello 許容度	トランスポートトンネルのダウンを宣言する前に、DTLSまたはTLS WAN トランスポート接続で Hello パケットを待機する時間を入力します。 範囲：12 ～ 60 秒。デフォルト：12 秒

アクセスリストの適用

ルータインターフェイスに書き換えルール、アクセスリスト、およびポリサーを適用するには、[ACL] を選択し、次のパラメータを設定します。

表 62:

パラメータ名	説明
成形率	インターフェイスの集約トラフィック転送速度を、回線速度よりも低く設定します（キロビット/秒 (kbps) 単位）。
QoS マップ	インターフェイスから送信されるパケットに適用する QoS マップの名前を指定します。
リライトルール	[On] をクリックし、インターフェイスに適用する書き換えルールの名前を指定します。
入力 ACL – IPv4	[On] をクリックして、インターフェイスで受信される IPv4 パケットに適用するアクセスリストの名前を指定します。
出力 ACL – IPv4	[On] をクリックし、インターフェイスで送信される IPv4 パケットに適用するアクセスリストの名前を指定します。
入力 ACL – IPv6	[On] をクリックして、インターフェイスで受信される IPv6 パケットに適用するアクセスリストの名前を指定します。
出力 ACL – IPv6	[On] をクリックし、インターフェイスで送信される IPv6 パケットに適用するアクセスリストの名前を指定します。
入力ポリサー	[On] をクリックして、インターフェイスで受信されるパケットに適用するポリサーの名前を指定します。
出力ポリサー	[On] をクリックして、インターフェイスで送信されるパケットに適用するポリサーの名前を指定します。

機能テンプレートを保存するには、[Save] をクリックします。

その他のインターフェイスプロパティの設定

他のインターフェイスプロパティを設定するには、[Advanced] タブを選択し、次のプロパティを設定します。

表 63:

パラメータ名	説明
PMTU ディスカバリ	[On] をクリックしてインターフェイスでパス MTU ディスカバリを有効にし、パケットのフラグメント化を必要とせずにサポートされる最大の MTU サイズをルータで判別できるようにします。
TCP MSS	Cisco SD-WAN デバイスを通過する TCP SYN パケットの最大セグメントサイズ (MSS) を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ~ 1460 バイト。デフォルト：なし
Dont Fragment のクリア	[On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Don't Fragment ビットをクリアします。DF ビットがクリアされると、そのインターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。
静的入力 QoS	着信トラフィックに使用するキュー番号を選択します。範囲：0 ~ 7
自動ネゴシエーション	[Off] をクリックして、自動ネゴシエーションをオフにします。デフォルトでは、インターフェイスは自動ネゴシエーションモードで実行されます。
TLOC Extension	WAN トランスポート回線に接続する同じルータ上の物理インターフェイスの名前を入力します。次に、この構成により、このサービス側のインターフェイスが WAN トランスポートにバインドされます。それ自体は WAN に直接接続されておらず (通常、サイトには 1 つの WAN 接続しかないため)、同じサイトにあり、このサービス側インターフェイスに接続する 2 番目の Cisco SD-WAN デバイスには、WAN への接続が提供されます。

機能テンプレートを保存するには、[Save] をクリックします。

リリース情報

リリース 18.3 で Cisco vManage に導入されました。

vManage を使用した VPN インターフェイス SVI の設定

Cisco IOS XE SD-WAN デバイスの SVI を設定するには、VPN インターフェイス SVI テンプレートを使用します。VLAN インターフェイスを設定するには、スイッチ仮想インターフェイス (SVI) を設定します。

Cisco vManage テンプレートを使用して Cisco ルータに DSL インターフェイスを設定するには、VPN インターフェイス SVI 機能テンプレートを作成して、VLAN インターフェイスパラメータを設定します。

VPN インターフェイス SVI テンプレートの作成

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. **[Device Templates]** で、**[Create Template]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Device Templates]** のタイトルは **[Device]** です。

3. **[Create Template]** ドロップダウンから、**[From Feature Template]** を選択します。
4. **[Device Model]** ドロップダウンから、テンプレートを作成するデバイスのタイプを選択します。
5. トランスポート VPN (VPN 0) で SVI を構成している場合は、次の手順を実行します。
 1. **[Transport & Management VPN]** をクリックするか、**[Transport & Management VPN]** セクションまでスクロールします。
 2. **[Additional VPN 0 Templates]** で、**[VPN Interface SVI]** をクリックします。
6. サービス VPN (VPN 0 以外の VPN) で SVI を構成している場合は、次の手順を実行します。
 1. **[Service VPN]** をクリックするか、**[Service VPN]** までスクロールします。
 2. **[Service VPN]** ドロップダウンリストで、サービス VPN の番号を入力します。
 3. **[Additional VPN Templates]** で、**[VPN Interface SVI]** をクリックします。
7. **[VPN Interface SVI]** ドロップダウンから、**[Create Template]** をクリックします。VPN インターフェイス SVI テンプレートフォームが表示されます。

このフォームには、テンプレートに名前を付けるためのフィールドと、VLAN インターフェイスパラメータを定義するためのフィールドが含まれています。
8. **[Template Name]** に、テンプレートの名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。
9. **[Template Description]** に、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。

初めて機能テンプレートを開くと、デフォルト値を持つパラメータごとに、その範囲が **[Default]** に設定され (チェックマークで示される)、デフォルト設定またはデフォルト値が表示されま

す。デフォルト値を変更するか、値を入力するには、パラメータフィールドの横にある [scope] ドロップダウンをクリックします。



(注) SVI インターフェイスを起動して機能させるには、適切な VLAN がスイッチポートアクセスまたはトランクインターフェイスで明示的に設定されていることを確認します。

基本的なインターフェイス機能の設定

表 64: 機能の履歴

機能名	リリース情報	説明
セカンダリ IP アドレスの構成のサポート	Cisco IOS XE リリース 17.2.1r	最大 4 つのセカンダリ IPv4 または IPv6 アドレス、および最大 4 つの DHCP ヘルパーを構成できます。セカンダリ IP アドレスは、異なるインターフェイス間で不均等なロードシェアリングを強制する場合、サブネットから使用できる IP がなくなったときに LAN 内の IP アドレスの数を増やす場合、および不連続なサブネットとクラスフルルーティングプロトコルに関する問題を解決する場合に役立ちます。

VPN で基本的な VLAN インターフェイス機能を設定するには、[Basic Configuration] を選択し、次のパラメータを設定します。インターフェイスを設定する場合、アスタリスクの付いたパラメータは必須です。

表 65:

パラメータ名	説明
Shutdown*	VLAN インターフェイスを有効にするには [No] をクリックします。
VLAN Interface Name*	インターフェイスの VLAN ID を入力します。範囲：1 ~ 1094。
説明	インターフェイスの説明を入力します。
IP MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。範囲：576 ~ 1500。デフォルト：2000 バイト

パラメータ名	説明
IPv4* or IPv6	クリックして、インターフェイスの IPv4 または IPv6 アドレスを 1 つ以上構成します。(Cisco IOS XE SD-WAN リリース 17.2 以降。)
IPv4 Address* IPv6 Address	インターフェイスの IPv4 アドレスを入力します。
Secondary IP Address	[Add] をクリックして、最大 4 つのセカンダリ IP アドレスを入力します。(Cisco IOS XE SD-WAN リリース 17.2 以降。)
DHCP Helper*	ネットワーク内の DHCP サーバーの IP アドレスを 8 つまで入力して、インターフェイスを DHCP ヘルパーにします。各アドレスはカンマで区切ります。DHCP ヘルパーインターフェイスは、指定された DHCP サーバーから受信した BOOTP (ブロードキャスト) DHCP 要求を転送します。 [Add] をクリックして、最大 4 つの DHCP ヘルパーを設定します。(IPv6 については、Cisco IOS XE SD-WAN リリース 17.2 以降。)

機能テンプレートを保存するには、[Save] をクリックします。

アクセスリストの適用

ルータインターフェイスに書き換えルール、アクセスリスト、およびポリサーを適用するには、[ACL] を選択し、次のパラメータを設定します。

表 66:

パラメータ名	説明
入力 ACL – IPv4	[On] をクリックして、インターフェイスで受信される IPv4 パケットに適用するアクセスリストの名前を指定します。
出力 ACL – IPv4	[On] をクリックして、インターフェイスで送信される IPv4 パケットに適用するアクセスリストの名前を指定します。
入力ポリサー	[On] をクリックして、インターフェイスで受信されるパケットに適用するポリサーの名前を指定します。
出力ポリサー	[On] をクリックして、インターフェイスで送信されるパケットに適用するポリサーの名前を指定します。

機能テンプレートを保存するには、[Save] をクリックします。

VRRP の設定

複数のルータがデフォルトゲートウェイの冗長性のために共通の仮想 IP アドレスを共有できるようにする Virtual Router Redundancy Protocol (VRRP) をインターフェイスで実行するには、

[VRRP] を選択します。次に、[Add New VRRP] をクリックして、次のパラメータを設定します。

表 67:

パラメータ名	説明
グループ ID (Group ID)	仮想ルータ ID を入力します。これは、仮想ルータの数値識別子です。最大 24 のグループを設定できます。範囲：1 ~ 255
プライオリ ティ	ルータの優先度を入力します。最も優先順位が高いルータがプライマリルータとして選択されます。2 つの Cisco IOS XE SD-WAN デバイスの優先順位が同じ場合、IP アドレスの高い方がプライマリとして選択されます。範囲：1 ~ 254、デフォルト：100
Timer	プライマリ VRRP ルータが VRRP アドバタイズメント メッセージを送信する頻度を指定します。下位ルータが 3 回連続して VRRP アドバタイズメントに失敗すると、新しいプライマリルータが選択されます。範囲：1 ~ 3600 秒、デフォルト：1 秒
Track OMP Track Prefix List	<p>デフォルトでは、VRRP は、どの Cisco IOS XE SD-WAN デバイスがプライマリ仮想ルータであるかを判別するために、VRRP が実行されているサービス (LAN) インターフェイスの状態を使用します。Cisco IOS XE SD-WAN デバイスがすべての WAN 制御接続を失うと、ルータが VRRP に機能的に参加できない場合でも、LAN インターフェイスは稼働の状態を示したままになります。VRRP の WAN 側の接続を考慮するには、次のいずれかを構成します。</p> <p>Track OMP : [On] をクリックすると、VRRP は WAN 接続で実行されているオーバーレイ管理プロトコル (OMP) セッションをトラッキングします。プライマリ VRRP ルータがすべての OMP セッションを失った場合、VRRP は、少なくとも 1 つのアクティブな OMP セッションを持つものから新しいデフォルトゲートウェイを選択します。</p> <p>Track Prefix List : OMP セッションと、ローカルルータで設定されたプレフィックスリストで定義されているリモートプレフィックスのリストの両方をトラッキングします。プライマリ VRRP ルータがすべての OMP セッションを失った場合、[Track OMP] オプションで説明されているように、VRRP フェールオーバーが発生します。さらに、リスト内のすべてのプレフィックスへの到達可能性が失われた場合、VRRP フェールオーバーは、OMP ホールドタイマーが期限切れになるのを待たずにすぐに発生するため、Cisco IOS XE SD-WAN デバイスがプライマリ VRRP ルータを決定する間にドロップされるオーバーレイトラフィックの量が最小限に抑えられます。</p>
IP アドレス	仮想ルータの IP アドレスを入力します。このアドレスは、ローカル Cisco IOS XE SD-WAN デバイスと VRRP を実行しているピアの両方の設定済みインターフェイス IP アドレスとは異なる必要があります。

ARP テーブルエントリの追加

インターフェイスで静的アドレス解決プロトコル（ARP）テーブルエントリを構成するには、[ARP] を選択します。次に、[Add New ARP] をクリックして、次のパラメータを設定します。

表 68:

パラメータ名	Description
IPアドレス	ARP エントリの IP アドレスをドット付き 10 進表記または完全修飾ホスト名として入力します。
MAC アドレス	MAC アドレスをコロン区切りの 16 進表記で入力します。

ARP 設定を保存するには、[Add] をクリックします。

機能テンプレートを保存するには、[Save] をクリックします。

その他のインターフェイスプロパティの設定

他のインターフェイスプロパティを設定するには、[Advanced] を選択し、次のプロパティを設定します。

表 69:

パラメータ名	説明
TCP MSS	Cisco IOS XE SD-WAN デバイス を通過する TCP SYN パケットの最大セグメントサイズ（MSS）を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ～ 1460 バイト、デフォルト：なし
ARP Timeout	動的に学習された ARP エントリがタイムアウトするまでの時間を指定します。範囲：0 ～ 2678400 秒（744 時間）デフォルト：1200（20 分）

機能テンプレートを保存するには、[Save] をクリックします。

VPN インターフェイス T1/E1

Cisco SD-WAN ソフトウェアを実行している Cisco SD-WAN には、VPN インターフェイス T1/E1 テンプレートを 사용합니다。

Cisco vManage テンプレートを使用して VPN の T1/E1 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。

1. この記事の説明に従って、VPN インターフェイス T1/E1 機能テンプレートを作成して、T1/E1 インターフェイスパラメータを設定します。

2. T1/E1 コントローラテンプレートを作成して、T1 または E1 ネットワーク インターフェイス モジュール (NIM) パラメータを設定します。
3. VPN 機能テンプレートを作成して、VPN パラメータを設定します。

[Template] 画面に移動し、テンプレートに命名する

1. Cisco vManage メニューから、[Configuration] > [Templates] を選択します。
2. [Device Templates] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

3. [Create Template] ドロップダウンリストから、[From Feature Template] を選択します。
4. [Device Model] ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。
5. VPN 0 または VPN 512 のテンプレートを作成するには、次の手順を実行します。



(注) 注 : Cisco IOS XE SD-WAN デバイスは、VPN の代わりに VRF を使用します。ただし、Cisco vManage を介した Cisco IOS XE SD-WAN デバイスの設定には引き続き次の手順が適用されます。設定を完了すると、VPN 設定が VRF 設定に自動的にマッピングされます。

1. [Transport & Management VPN] をクリックするか、[Transport & Management VPN] セクションまでスクロールします。
2. [Additional VPN 0 Templates] で、[VPN Interface T1/E1 Serial] をクリックします。
3. [VPN Interface T1/E1 Serial] ドロップダウンリストから、[Create Template] をクリックします。[VPN Interface T1/E1] テンプレートフォームが表示されます。このフォームには、テンプレートに名前を付けるためのフィールドと、VPN インターフェイスイーサネットパラメータを定義するためのフィールドが含まれています。
6. VPN 1 ~ 511 および 513 ~ 65530 のテンプレートを作成するには、次の手順を実行します。
 1. [Service VPN] をクリックするか、[Service VPN] セクションまでスクロールします。
 2. [Service VPN] ドロップダウンリストをクリックします。
 3. [Additional VPN] テンプレートで、[VPN Interface] をクリックします。
 4. [VPN Interface] ドロップダウンリストから、[Create Template] をクリックします。[VPN Interface Ethernet] テンプレートフォームが表示されます。このフォームには、テンプレ

レートに名前を付けるためのフィールドと、VPN インターフェイスイーサネットパラメータを定義するためのフィールドが含まれています。

7. [Template Name] に、テンプレートの名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。
8. [Template Description] に、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。

初めて機能テンプレートを開くと、デフォルト値を持つパラメータごとに、その範囲が [Default] に設定され (チェックマークで示される)、デフォルト設定またはデフォルト値が表示されます。デフォルト値を変更するか、値を入力するには、パラメータフィールドの左側にある [Scope] ドロップダウンをクリックします。

基本的なインターフェイス機能の設定

VPN で基本的なインターフェイス機能を設定するには、[Basic Configuration] を選択し、次のパラメータを設定します。インターフェイスを設定する場合、アスタリスクの付いたパラメータは必須です。

表 70:

パラメータ名	説明
Shutdown*	インターフェイスを有効にするには [No] をクリックします。
Interface name*	インターフェイスの名前を入力します。名前は、 serial slot / subslot / port : channel-group の形式にする必要があります。 また、T1/E1 コントローラ機能設定テンプレートでチャンネルグループの番号も設定する必要があります。
説明	インターフェイスの説明を入力します。
IPv4 Address*	IPv4 アドレスを入力します。
IPv6 Address*	IPv6 アドレスを入力します。
Bandwidth Upstream	送信トラフィックについて、通知を生成する帯域幅を設定します。範囲 : 1 ~ $(2^{32}/2) - 1$ kbps
Bandwidth Downstream	受信トラフィックについて、通知を生成する帯域幅を設定します。範囲 : 1 ~ $(2^{32}/2) - 1$ kbps
IP MTU	インターフェイス上のパケットの最大 MTU サイズを指定します。範囲 : 576 ~ 1804、デフォルト : 1500 バイト

トンネルインターフェイスの作成

Cisco IOS XE ルータでは、最大4つのトンネルインターフェイスを設定できます。つまり、各ルータに最大4つのTLOCを設定できます。

オーバーレイネットワークが機能できるようにコントロールプレーンがそれ自体を確立するには、VPN 0 で WAN トランスポート インターフェイスを設定する必要があります。

マルチリンク インターフェイスのトンネルインターフェイスを設定するには、[トンネルインターフェイス] を選択し、次のパラメータを設定します。

表 71:

パラメータ名	説明
トンネルインターフェイス	[オン] をクリックして、トンネルインターフェイスを作成します。
色	TLOC の色を選択します。

パラメータ名	説明
制御接続	<p>デフォルトでは、制御接続はオンに設定されており、TLOCの制御接続を確立します。ルータに複数の TLOC がある場合は、[いいえ] をクリックして、トンネルが TLOC の制御接続を確立しないようにします。</p> <p>(注) 接続トラフィックでのデータ/パケットの損失を避けるために、デフォルトの 1 秒の hello インターバルと 12 秒の hello トランスペアレンスパラメータを設定して、最低 650 ~ 700 Kbps の帯域幅を設定することをお勧めします。</p> <p>BFD セッションごとに、175 バイトの追加の平均サイズ BFD パケットは、1.4 Kbps の帯域幅を消費します。</p> <p>双方向 BFD パケット フローに必要な帯域幅の計算例を以下に示します。</p> <ul style="list-style-type: none"> • 制御接続用にデバイスごとに 650 ~ 700 Kbps。 • デバイス上の BFD セッション (要求) ごとに 175 バイト (または 1.4 Kbps) • デバイス上の BFD セッション (応答) ごとに 175 バイト (または 1.4 Kbps) <p>パス MTU ディスカバリ (PMTUD) が有効になっている場合、30 秒ごと、トンネルごとに BFD パケットを送受信するための帯域幅 :</p> <p>1500 バイトの BFD 要求パケットは、30 秒ごと、トンネルごとに送信されます。</p> <p>$1500 \text{ バイト} * 8 \text{ ビット/1 バイト} * 1 \text{ パケット/30 秒} = 400 \text{ bps}$ (リクエスト)</p> <p>147 バイトの BFD パケットが応答として送信されます。</p> <p>$147 \text{ バイト} * 8 \text{ ビット/1 バイト} * 1 \text{ パケット/30 秒} = 40 \text{ bps}$ (レスポンス)</p> <p>したがって、たとえば 775 BFD セッションを持つデバイスの場合、次の帯域幅が必要です。</p> <p>$700 \text{ k} + (1.4 \text{ k} * 775) + (400 * 775) + (1.4 \text{ k} * 775) + (40 * 775) = \sim 3.5 \text{ MBps}$</p>
最大制御接続数	<p>WAN トンネル インターフェイスが接続できる の最大数を指定します。Cisco vSmart コントローラ トンネルが制御接続を確立しないようにするには、この数値を 0 に設定します。</p> <p>範囲 : 0 ~ 8、デフォルト : 2</p>

パラメータ名	説明
Cisco vBond オーケストレーション As STUN Server	[オン] をクリックして NAT (STUN) のセッション トラバーサル ユーティリティを有効にし、ルータが NAT の背後にある場合にトンネルインターフェイスがパブリック IP アドレスとポート番号を検出できるようにします。
コントローラグループリストの除外	トンネルインターフェイスの接続を許可しない Cisco vSmart コントローラを設定します。範囲：0～100
Cisco vManage Connection Preference	トンネルインターフェイスを使用して Cisco vManage NMS と制御トラフィックを交換するための優先順位を設定します。範囲：0～8、デフォルト：5
ポートホップ	ポートホッピングを有効にするには [On] をクリックし、無効にするには [Off] をクリックします。ルータが NAT の背後にある場合、ポートホッピングは、事前に選択された OMP ポート番号(ベースポートと呼ばれる)のプールを循環して、接続の試行が失敗したときに他のルータとの DTLS 接続を確立します。デフォルトのベースポートは 12346、12366、12386、12406、および 12426 です。ベースポートを変更するには、ポートオフセット値を設定します。デフォルト：有効
低帯域幅リンク	トンネルインターフェイスを低帯域幅リンクとして特徴付ける場合に選択します。
トンネル TCP MSS	<p>TCP MSS は、ルータを通過する最初の TCP ヘッダーを含むすべてのパケットに影響します。設定すると、TCP MSS は、スリーウェイハンドシェイクで交換される MSS に対して検査されます。構成済みの TCP MSS 設定がヘッダーの MSS よりも小さい場合、ヘッダーの MSS の値が減少します。MSS ヘッダー値がすでに TCP MSS よりも低い場合、パケットは変更されずに通過します。トンネルの最後にあるホストは、2つのホストの低い方の設定を使用します。TCP MSS を設定する場合は、最小パス MTU より 40 バイト小さく設定する必要があります。</p> <p>を通過する TPC SYN パケットの MSS を指定します。Cisco IOS XE SD-WAN デバイスデフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552～1460 バイト、デフォルト：なし</p>

パラメータ名	説明
Clear-Dont-Fragment	<p>Dont Fragment が設定されているインターフェイスに到着するパケットの [Clear-Dont-Fragment] を設定します。これらのパケットが MTU が許可するサイズより大きい場合、それらはドロップされます。Don't Fragment ビットをクリアすると、パケットはフラグメント化されて送信されます。</p> <p>[On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Dont Fragment ビットをクリアします。Dont Fragment ビットがクリアされると、インターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。</p> <p>(注) [Clear-Dont-Fragment] は Dont Fragment ビットをクリアし、Dont Fragment ビットが設定されます。フラグメンテーションを必要としないパケットの場合、Dont Fragment ビットは影響を受けません。</p>
サービスの許可	サービスごとに [オン] または [オフ] を選択して、インターフェイスでサービスを許可または禁止します。

機能テンプレートを保存するには、[Save] をクリックします。

リリース情報

Cisco vManage リリース 18.2 で導入されました。

T1/E1 コントローラ

Cisco SD-WAN ソフトウェアを実行する Cisco IOS XE SD-WAN デバイスの場合、T1/E1 コントローラテンプレートを使用します。

Cisco vManage テンプレートを使用して VPN の T1/E1 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。

1. この記事の説明に従って、T1/E1 コントローラテンプレートを作成して、T1 または E1 ネットワーク インターフェイス モジュール (NIM) パラメータを設定します。
2. VPN インターフェイス T1/E1 機能テンプレートを作成して、T1/E1 インターフェイスパラメータを設定します。
3. VPN 機能テンプレートを作成して、VPN パラメータを設定します。

[Template] 画面に移動し、テンプレートに命名する

1. Cisco vManage メニューから、[Configuration] > [Templates] を選択します。
2. [Device Templates] をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

3. [Create Template] ドロップダウンリストから、[From Feature Template] を選択します。
4. [Device Model] ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。
5. VPN 0 または VPN 512 のテンプレートを作成するには、次の手順を実行します。
 1. [Transport & Management VPN] をクリックするか、[Transport & Management VPN] セクションまでスクロールします。
 2. [Additional VPN 0 Templates] で、[VPN Interface] をクリックします。
 3. [VPN Interface] ドロップダウンリストから、[Create Template] をクリックします。[VPN Interface T1/E1] テンプレートフォームが表示されます。このフォームには、テンプレートに名前を付けるためのフィールドと、VPN インターフェイスイーサネットパラメータを定義するためのフィールドが含まれています。
6. VPN 1 ~ 511 および 513 ~ 65530 のテンプレートを作成するには、次の手順を実行します。
 1. [Service VPN] をクリックするか、[Service VPN] セクションまでスクロールします。
 2. [Service VPN] ドロップダウンリストをクリックします。
 3. [Additional VPN] テンプレートで、[VPN Interface] をクリックします。
 4. [VPN Interface] ドロップダウンリストから、[Create Template] をクリックします。[VPN Interface Ethernet] テンプレートフォームが表示されます。This form contains fields for naming the template, and fields for defining VPN Interface Ethernet parameters.
7. [Template Name] に、テンプレートの名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。
8. [Template Description] に、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。

初めて機能テンプレートを開くと、デフォルト値を持つパラメータごとに、その範囲が [Default] に設定され (チェックマークで示される)、デフォルト設定またはデフォルト値が表示されます。デフォルト値を変更するか、値を入力するには、[Scope] ドロップダウンリストをクリックし、次のいずれかを選択します。

- デバイス固有 (ホストのアイコンで示される)
- グローバル (地球のアイコンで示される)

T1 コントローラの設定

T1 コントローラを設定するには、[T1] をクリックして、次のパラメータを設定します。インターフェイスを設定する場合、アスタリスクの付いたパラメータは必須です。

表 72:

パラメータ名	説明
Slot*	T1 NIM がインストールされているスロットの番号を、slot/subslot/port の形式で入力します。たとえば、0/1/0 と入力できます。
Framing*	T1 フレームタイプを入力します。 <ul style="list-style-type: none"> • [esf] : T1 フレームを拡張スーパーフレームとして送信します。これがデフォルトです。 • [sf] : T1 フレームをスーパーフレームとして送信します。スーパーフレームミングは、D4 フレームミングと呼ばれることもあります。
Line Code	T1 フレームの送信に使用する回線エンコーディングを選択します。 <ul style="list-style-type: none"> • [ami] : 回線コードとして Alternate Mark Inversion (AMI) を指定します。AMI シグナリングは、スーパーフレームにグループ化されたフレームを使用します。 • [b8zs] : 回線コードとして Bipolar 8-Zeros Substitution を使用します。これがデフォルトです。B8ZS は、拡張スーパーフレームにグループ化されたフレームを使用します
Clock Source	クロックソースを選択します。 <ul style="list-style-type: none"> • [internal] : コントローラフレームをプライマリクロックとして使用します。 • [line] : インターフェイスでフェーズロックループ (PLL) を使用します。これがデフォルトです。両方の T1 ポートが回線クロッキングを使用し、どちらのポートもプライマリとして設定されていない場合、デフォルトでは、ポート 0 がプライマリクロックソースで、ポート 1 がセカンダリクロックソースです。
Line Mode	回線クロックソースを選択した場合は、回線がプライマリまたはセカンダリ回線のどちらであるかを選択します。
説明	コントローラの説明を入力します。
Channel Group	チャンネルグループの番号を入力します。その場合は、[Time Slot] フィールドにタイムスロットを入力する必要があります。範囲 : 0 ~ 30

パラメータ名	説明
タイム スロット (Time Slot)	チャンネルグループの一部であるタイムスロットを入力します。範囲：1～24
ケーブル長	減衰を設定するケーブル長を選択します <ul style="list-style-type: none"> • [long]：パルスイコライゼーションと回線ビルドアウトを使用して、トランスミッタからのパルスを減衰させます。660 フィートを超えるケーブルには、長いケーブル長を設定できます。 • [short]：660 フィート以下のケーブルの伝送減衰を設定します。 デフォルトのケーブル長はありません。
長さ	[Cable Length Field] に値を指定する場合は、ケーブルの長さを入力します。短いケーブルの場合、長さの値は次のとおりです。 <ul style="list-style-type: none"> • [110]：0～110 フィートの長さ • [220]：111～220 フィートの長さ • [330]：221～330 フィートの長さ • [440]：331～440 フィートの長さ • [550]：441～550 フィートの長さ • [660]：551～660 フィートの長さ 長いケーブルの場合、長さの値は次のとおりです。 <ul style="list-style-type: none"> • 0 dB • -7.5 dB • -15 dB • -22.5 dB

機能テンプレートを保存するには、[Save] をクリックします。

E1 コントローラの設定

E1 コントローラを設定するには、[E1] をクリックして、次のパラメータを設定します。インターフェイスを設定する場合、アスタリスクの付いたパラメータは必須です。

表 73:

パラメータ名	説明
Slot*	E1 NIM がインストールされているスロットの番号を、slot/subslot/port の形式で入力します。たとえば、0/1/0 と入力できます。

パラメータ名	説明
Framing*	E1 フレームタイプを入力します。 <ul style="list-style-type: none"> • [crc4] : 巡回冗長検査 4 (CRC4) を使用します。これがデフォルトです。 • [no-crc4] : CRC4 を使用しません。
Line Code*	E1 フレームの送信に使用する回線エンコーディングを選択します。 <ul style="list-style-type: none"> • [ami] : 回線コードとして Alternate Mark Inversion (AMI) を指定します。 • [hdb3] : 回線コードとして High-Density Bipolar 3 を使用します。これがデフォルトです。
Clock Source	クロックソースを選択します。 <ul style="list-style-type: none"> • [internal] : コントローラフレームをプライマリクロックとして使用します。 • [line] : インターフェイスでフェーズロックループ (PLL) を使用します。これがデフォルトです。
Line Mode	回線クロックソースを選択した場合は、回線がプライマリまたはセカンダリ回線のどちらであるかを選択します。プライマリ回線とセカンダリ回線の両方を設定した場合、プライマリ回線に障害が発生すると、PLL は自動的にセカンダリ回線に切り替わります。プライマリ回線の PLL が再びアクティブになると、PLL は自動的にプライマリ回線に戻ります。
説明	コントローラの説明を入力します。
Channel Group	E1 インターフェイスでシリアル WAN を設定するには、チャンネルグループ番号を入力します。範囲 : 0 ~ 30
タイム スロット (Time Slot)	チャンネルグループの場合、タイムスロットを設定します。範囲 : 1 ~ 31

機能テンプレートを保存するには、[Save] をクリックします。

リリース情報

Cisco vManage リリース 18.1.1 で導入されました。

セルラーインターフェイス

LTE 接続を有効にするには、セルラーモジュールを備えたルータでセルラーインターフェイスを設定します。セルラーモジュールにより、サービスプロバイダーのセルラーネットワーク上でワイヤレス接続ができます。使用例の1つとしては、分散拠点にワイヤレス接続を提供することがあります。

セルラーネットワークは、ルータのすべての有線 WAN トンネルインターフェイスが使用できなくなった場合にネットワーク接続を提供するために、バックアップ WAN リンクとして一般的に使用されます。分散拠点内での使用パターンと、サービスプロバイダーのセルラーネットワークのコアによってサポートされるデータレートに応じて、セルラーネットワークを分散拠点のプライマリ WAN リンクとして使用することもできます。

デバイスでセルラーインターフェイスを設定すると、デバイスの電源ケーブルを差し込むことで、デバイスをインターネットまたは別の WAN に接続できます。これにより、Cisco vBond オーケストレーション、Cisco vSmart コントローラ、および Cisco vManage システムと接続して認証することで、デバイスはオーバーレイネットワークへの参加プロセスを自動的に開始します。

Cisco vManage を使用したセルラーインターフェイスの設定

Cisco vManage テンプレートを使用してセルラーインターフェイスを構成するには、次の手順を実行します。

1. このセクションの説明に従って、VPN インターフェイスセルラー機能テンプレートを作成して、セルラー モジュール パラメータを設定します。
2. セルラー プロファイル テンプレートを作成して、セルラーモデムが使用するプロファイルを構成します。
3. VPN 機能テンプレートを作成して、VPN パラメータを設定します。



(注) 展開にセルラーインターフェイスを備えたデバイスが含まれている場合は、これらのテンプレートが使用されていない場合でも、セルラーコントローラ テンプレートを Cisco vManage に含める必要があります。

デバイスに LTE またはセルラー コントローラ モジュールが構成されていて、セルラーコントローラ機能テンプレートが存在しない場合、デバイスはセルラー コントローラ テンプレートの削除を試みます。Cisco IOS XE リリース 17.4.2 より前のリリースでは、次のエラーメッセージが表示されます。

```
bad-cli - No controller Cellular 0/2/0, parser-context - No controller Cellular 0/2/0,
parser-response % Cannot remove controllers this way
```

Cisco IOS XE リリース 17.4.2 以降で実行されているデバイスの場合、デバイスは access-denied エラーメッセージを返します。

VPN インターフェイスセルラーの作成

1. Cisco vManage メニューから、**[Configuration]** > **[Templates]** を選択します。
2. **[Device Templates]** をクリックします。



(注) Cisco vManage リリース 20.7.x 以前のリリースでは、**[Device Templates]** のタイトルは **[Device]** です。

3. **[Create Template]** ドロップダウンリストから、**[From Feature Template]** を選択します。
4. **[Device Model]** ドロップダウンリストから、テンプレートを作成するデバイスのタイプを選択します。
5. **[Transport & Management VPN]** をクリックするか、**[Transport & Management VPN]** セクションまでスクロールします。
6. **[Additional Cisco VPN 0 Templates]** で、**[VPN Interface Cellular]** をクリックします。
7. **[VPN Interface Cellular]** ドロップダウンリストから、**[Create Template]** をクリックします。VPN インターフェイス セルラー テンプレート フォームが表示されます。
このフォームには、テンプレートに名前を付けるためのフィールドと、VPN インターフェイス セルラー パラメータを定義するためのフィールドが含まれています。
8. **[Template Name]** に、テンプレートの名前を入力します。名前の最大長は 128 文字で、英数字のみを使用できます。
9. **[Template Description]** に、テンプレートの説明を入力します。説明の最大長は 2048 文字で、英数字のみを使用できます。

初めて機能テンプレートを開くと、デフォルト値を持つパラメータごとに、その範囲が **[Default]** に設定され (チェックマークで示される)、デフォルト設定またはデフォルト値が表示されます。デフォルト値を変更するか、値を入力するには、**[scope]** ドロップダウンリストをクリックします。

基本的なセルラーインターフェイス機能の設定

基本的なセルラーインターフェイス機能を設定するには、**[Basic Configuration]** をクリックして、次のパラメータを構成します。Parameters marked with an asterisk are required to configure an interface. セルラーインターフェイスのトンネルインターフェイスも設定する必要があります。

表 74:

パラメータ名	説明
Shutdown*	インターフェイスを有効にするには [No] をクリックします。
Interface Name*	インターフェイスの名前を入力します。それは [cellular0] でなければなりません。

パラメータ名	説明
説明	セルラーインターフェイスの説明を入力します。
DHCP ヘルパー	ネットワーク内の DHCP サーバーの IP アドレスをカンマで区切って 4 つまで入力して、インターフェイスを DHCP ヘルパーにします。DHCP ヘルパーインターフェイスは、指定された DHCP サーバーから受信した BOOTP (ブロードキャスト) DHCP 要求を転送します。
Bandwidth Upstream	送信トラフィックについて、通知を生成する帯域幅を設定します。範囲：1 ~ $(2^{32}/2) - 1$ kbps
Bandwidth Downstream	受信トラフィックについて、通知を生成する帯域幅を設定します。範囲：1 ~ $(2^{32}/2) - 1$ kbps
IP MTU*	MTU サイズに 1428 と入力します (バイト単位)。この値は 1428 である必要があります。別の値を使用することはできません。

機能テンプレートを保存するには、[Save] をクリックします。

トンネルインターフェイスの作成

VPN 0 のインターフェイスを WAN トランスポート接続として構成するには、セルラーインターフェイスでトンネルインターフェイスを構成する必要があります。攻撃に対するセキュリティを提供するトンネルは、電話番号の送信に使用されます。前のセクションで説明したように、少なくとも、[On] を選択し、インターフェイスの色を選択します。通常、トンネルインターフェイス設定のリマインダについては、システムのデフォルトを受け入れることができます。

トンネルインターフェイスを構成するには、[Tunnel] をクリックし、次のパラメータを構成します。セルラーインターフェイスを設定する場合、アスタリスクの付いたパラメータは必須です。

パラメータ名	説明
Tunnel Interface*	ドロップダウンから、[Global] を選択します。[On] をクリックして、トンネルインターフェイスを作成します。
Per-tunnel QoS	ドロップダウンから、[Global] を選択します。[On] をクリックして、トンネルごとの QoS を作成します。 個々のトンネルにサービス品質 (QoS) ポリシーを適用でき、ハブツースポーク ネットワーク トポロジでのみサポートされます。

パラメータ名	説明
Per-tunnel QoS Aggregator	ドロップダウンから、[Global] を選択します。[On] をクリックして、トンネルごとの QoS を作成します。 (注) 「帯域幅ダウストリーム」は、トンネルごとの QoS 機能がスポークの役割として有効になるために必要です。
Color*	ドロップダウンから、[Global] を選択します。TLOC の色を選択します。セルラーインターフェイス トンネルに通常使用される色は [lte] です。
Groups	ドロップダウンから、[Global] を選択します。フィールドにグループのリストを入力します。
Border	ドロップダウンから、[Global] を選択します。[On] をクリックして、TLOC をボーダー TLOC として設定します。
最大制御接続数	WAN トンネルインターフェイスが接続できる vSmart コントローラの最大数を設定します。トンネルが制御接続を確立しないようにするには、この数値を 0 に設定します。範囲：0 ~ 8 デフォルト：2
vBond As STUN Server	[On] をクリックして NAT (STUN) のセッション トラバーサルユーティリティを有効にし、ルータが NAT の背後にある場合にトンネルインターフェイスがパブリック IP アドレスとポート番号を検出できるようにします。
コントロールグループリストの除外	このトンネルが制御接続の確立を許可しない 1 つ以上の vSmart コントローラグループの識別子を設定します。 範囲：0 ~ 100

パラメータ名	説明
vManage 接続設定	<p>トンネルを使用して制御トラフィックを Cisco vManage と交換するための優先順位を設定します。</p> <p>範囲：0～9</p> <p>デフォルト：5</p> <p>エッジデバイスに2つ以上のセルラーインターフェイスがある場合、Cisco vManage とセルラーインターフェイスの間のトラフィックの量を最小限に抑えるには、インターフェイスの1つを、Cisco vManage へのアップデートの送信時および Cisco vManage からの設定の受信時に使用する優先インターフェイスとして設定します。</p> <p>トンネルインターフェイスが Cisco vManage に接続されないようにするには、数を0に設定します。エッジデバイスの少なくとも1つのトンネルインターフェイスには、ゼロ以外の Cisco vManage 接続プリファレンスが必要です。</p>
ポートホップ	<p>ドロップダウンから、[Global] を選択します。[Control Group List] をクリックして、トンネルインターフェイスでのポートホッピングを許可します。</p> <p>デフォルト：[On]。トンネルインターフェイスでのポートホッピングを禁止します。</p>
低帯域幅リンク	<p>[On] をクリックして、トンネルインターフェイスを低帯域幅リンクとして設定します。</p> <p>デフォルトは Off です。</p>
トンネル TCP MSS	<p>TCP MSS は、ルータを通過する最初の TCP ヘッダーを含むすべてのパケットに影響します。設定すると、TCP MSS は、スリーウェイハンドシェイクで交換される MSS に対して検査されます。構成された TCP MSS 設定がヘッダーの MSS よりも低い場合、ヘッダーの MSS は低くなります。MSS ヘッダー値がすでに TCP MSS よりも低い場合、パケットは変更されずに通過します。トンネルの最後にあるホストは、2つのホストの低い方の設定を使用します。TCP MSS を設定する場合は、最小パス MTU より 40 バイト小さく設定する必要があります。</p> <p>Cisco IOS XE SD-WAN デバイスを通過する TCP SYN パケットの MSS を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552～1460 バイト。デフォルト：なし</p>

パラメータ名	説明
Clear-Dont-Fragment	<p>Don't Fragment が設定されているインターフェイスに到着するパケットの [Clear-Dont-Fragment] を設定します。これらのパケットが MTU が許可するサイズより大きい場合、それらはドロップされます。Don't Fragment ビットをクリアすると、パケットはフラグメント化されて送信されます。</p> <p>[On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Dont Fragment ビットをクリアします。Dont Fragment ビットがクリアされると、インターフェイスの MTU より大きいパケットは送信前にフラグメント化されません。</p> <p>(注) [Clear-Dont-Fragment] は Dont Fragment ビットをクリアし、Dont Fragment ビットが設定されます。フラグメンテーションを必要としないパケットの場合、Dont Fragment ビットは影響を受けません。</p>
Network Broadcast	<p>ドロップダウンから、[Global] を選択します。[On] をクリックして、ネットワークプレフィックス宛てのブロードキャストを受け入れて応答します。LAN インターフェイス機能テンプレートで [Directed Broadcast] が有効になっている場合にのみ、これを [On] にします。</p> <p>デフォルトは Off です。</p>
Allow Service	<p>サービスごとに [On] または [Off] をクリックして、セルラーインターフェイスでサービスを許可または禁止します。</p>

追加のトンネルインターフェイス パラメータを設定するには、[Advanced Options] をクリックして、次のパラメータを設定します。

表 75:

パラメータ名	説明
GRE	<p>ドロップダウンから、[Global] を選択します。[On] をクリックして、トンネルインターフェイスで GRE カプセル化を使用します。デフォルトでは、GRE は無効になっています。</p> <p>IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。</p>
GRE Preference	<p>ドロップダウンから、[Global] を選択します。値を入力して、TLOC の GRE プリファレンスを設定します。</p> <p>範囲 : 0 ~ 4294967295</p>

パラメータ名	説明
GRE Weight	ドロップダウンから、[Global] を選択します。値を入力して、TLOC の GRE 重み付けを設定します。 デフォルト : 1
IPSec	ドロップダウンから、[Global] を選択します。[On] をクリックして、トンネルインターフェイスでIPsecカプセル化を使用します。デフォルトでは、IPsec は有効になっています。 IPsec カプセル化と GRE カプセル化の両方を選択すると、トンネルインターフェイス用に同じ IP アドレスとカラーを持つ 2 つの TLOC が作成されますが、カプセル化が異なります。
IPsec Preference	ドロップダウンから、[Global] を選択します。トラフィックをトンネルに誘導するための優先順位を設定する値を入力します。高い値が低い値に優先します。 範囲 : 0 ~ 4294967295。デフォルト : 0
IPsec の重み	ドロップダウンから、[Global] を選択します。複数の TLOC 間でトラフィックのバランスをとるための重み付けを設定する値を入力します。値が大きいほど、より多くのトラフィックがトンネルに送信されます。 範囲 : 1 ~ 255。デフォルト : 1
通信事業者	ドロップダウンから、[Global] を選択します。[Carrier] ドロップダウンから、トンネルに関連付けるキャリア名またはプライベートネットワーク識別子を選択します。値 : carrier1、carrier2、carrier3、carrier4、carrier5、carrier6、carrier7、carrier8、デフォルト。デフォルト : デフォルト
ループバック トンネルのバ インド	ループバック インターフェイスにバインドする物理インターフェイスの名前を入力します。インターフェイス名の形式は、 ge slot/port です。

パラメータ名	説明
ラストリゾート回線	<p>ドロップダウンから、[Global] を選択します。[On] をクリックして、トンネルインターフェイスを最終手段の回線として使用します。デフォルトでは、無効になっています。</p> <p>(注) ラストリゾート回線として構成されたインターフェイスはダウンすると予想され、制御接続の数の計算中にスキップされ、セルラーモデムは休止状態になり、トラフィックは回線上で送信されません。</p> <p>セルラーインターフェイスを備えたエッジデバイスで設定がアクティブ化されると、すべてのインターフェイスが制御およびBFD接続を確立するプロセスを開始します。1 つ以上のプライマリインターフェイスが BFD 接続を確立すると、最終手段の回線は自動的にシャットダウンします。</p> <p>すべてのプライマリインターフェイスがリモートエッジへの接続を失った場合にのみ、ラストリゾート回線がアクティブになり、エッジデバイスで BFD TLOC ダウンアラームと制御 TLOC ダウンアラームがトリガーされます。ラストリゾートインターフェイスは、エッジデバイスのバックアップ回線として使用され、他のすべてのトランスポートリンク BFD セッションが失敗したときにアクティブ化されます。このモードでは、無線インターフェイスはオフになり、セルラーインターフェイスを介した制御またはデータ接続は存在しません。</p>
NAT 更新間隔	DTLS または TLS WAN トランスポート接続で送信される NAT リフレッシュパケットの間隔を設定します。範囲：1 ～ 60 秒。デフォルト：5 秒。
Hello 間隔 (Hello Interval)	DTLS または TLS WAN トランスポート接続で送信される Hello パケットの間隔を入力します。範囲：100 ～ 10000 ミリ秒。デフォルト：1000 ミリ秒 (1 秒)。

パラメータ名	説明
Hello 許容度	<p>トランスポートトンネルのダウンを宣言する前に、DTLS または TLS WAN トランスポート接続で Hello パケットを待機する時間を入力します。</p> <p>範囲：12 ～ 60 秒。デフォルト：12 秒。</p> <p>デフォルトの hello 間隔は 1000 ミリ秒で、100 ～ 600000 ミリ秒 (10 分) の範囲の時間にすることができます。デフォルトの hello トレランスは 12 秒で、12 ～ 600 秒 (10 分) の範囲の時間にすることができます。TLOC での発信制御パケットを減らすには、トンネルインターフェイスで hello インターフェイスを 60000 ミリ秒 (10 分) に設定し、hello 許容時間を 600 秒 (10 分) に設定し、エッジデバイスとコントローラ間の DTLS 接続の [no track-transport disable] 定期チェックを含めることをお勧めします。エッジデバイスと任意のコントローラデバイス間のトンネル接続の場合、トンネルはエッジデバイスで構成された hello 間隔と許容時間を使用します。この選択は、トンネルを介して送信されるトラフィックを最小限に抑え、リンクのコストがリンクを通過するトラフィックの量の関数である状況を可能にするために行われます。hello 間隔と許容時間は、エッジデバイスとコントローラデバイス間のトンネルごとに個別に選択されます。コントロールプレーントラフィックの量を最小限に抑えるために実行されるもう 1 つの手順は、他のインターフェイスが使用可能なときに、セルラーインターフェイスを介して OMP コントロールトラフィックを送受信しないようにすることです。この動作はソフトウェアに固有のものであり、構成することはできません。</p>

機能テンプレートを保存するには、[Save] をクリックします。

セルラーインターフェイスを NAT デバイスとして設定する

ポート転送などのアプリケーションの NAT デバイスとして機能するようにセルラーインターフェイスを設定するには、[NAT] をクリックして、次のパラメータを設定します。

表 76:

パラメータ名	説明
NAT	[On] をクリックして、インターフェイスを NAT デバイスとして機能させます。
Refresh Mode	NAT マッピングを更新する方法 (アウトバウンドまたは双方向 (アウトバウンドとインバウンド) のいずれか) を選択します。デフォルト：アウトバウンド
[UDP Timeout]	UDP セッションを介した NAT 変換がいつタイムアウトするかを指定します。範囲：1 ～ 65536 分。デフォルト：1 分
[TCP Timeout]	TCP セッションを介した NAT 変換がいつタイムアウトするかを指定します。範囲：1 ～ 65536 分。デフォルト：60 分 (1 時間)

パラメータ名	説明
Block ICMP	[On] を選択して、インバウンド ICMP エラーメッセージをブロックします。デフォルトでは、NAT デバイスとして機能するルータは、これらのエラーメッセージを受け取ります。デフォルト：[オフ (Off)]
Respond to Ping	接続のパブリック側から受信した NAT インターフェイスの IP アドレスへの ping 要求にルータが応答するようにするには、[On] を選択します。

ポート転送ルールを作成するには、[Add New Port Forwarding Rule] をクリックし、次のパラメータを設定します。最大 128 のポート転送ルールを定義して、外部ネットワークからの要求が内部ネットワーク上のデバイスに到達できるようにすることができます。

表 77:

パラメータ名	説明
Port Start Range	ポート番号を入力して、ポートまたは対象の範囲の最初のポートを定義します。範囲：0 ~ 65535
Port End Range	同じポート番号を入力してポート転送を 1 つのポートに適用するか、より大きい番号を入力してポートの範囲に適用します。範囲：0 ~ 65535
プロトコル	ポート転送ルールを適用するプロトコル ([TCP] または [UDP]) を選択します。TCP トラフィックと UDP トラフィックの両方で同じポートを一致させるには、2 つのルールを構成します。
VPN	内部サーバーが存在するプライベート VPN を指定します。この VPN は、オーバーレイネットワークの VPN 識別子の 1 つです。範囲：0 ~ 65530
プライベート IP	ポート転送ルールに一致するトラフィックを転送する内部サーバーの IP アドレスを指定します。

ポート転送ルールを保存するには、[Add] をクリックします。

機能テンプレートを保存するには、[Save] をクリックします。

アクセスリストの適用

セルラーインターフェイスのシェーピングレートを設定し、QoS マップ、書き換えルール、アクセスリスト、およびポリサーをルータインターフェイスに適用するには、[ACL/QoS] をクリックして、次のパラメータを設定します。

表 78: アクセスリストパラメータ

パラメータ名	説明
成形率	インターフェイスの集約トラフィック転送速度を、回線速度よりも低く設定します (キロビット/秒 (kbps) 単位)。

パラメータ名	説明
QoS マップ	インターフェイスから送信されるパケットに適用する QoS マップの名前を指定します。
書き換えルール	[On] をクリックし、インターフェイスに適用する書き換えルールの名前を指定します。
入力 ACL-IPv4	[On] をクリックし、インターフェイスで受信されるパケットへの IPv4 アクセスリストの名前を指定します。
Egress ACL-IPv4	[On] をクリックして、インターフェイスで送信されるパケットへの IPv4 アクセスリストの名前を指定します。
入力 ACL-IPv6	[On] をクリックし、インターフェイスで受信されるパケットへの IPv6 アクセスリストの名前を指定します。
Egress ACL-IPv6	[On] をクリックして、インターフェイスで送信されるパケットへの IPv6 アクセスリストの名前を指定します。
入力ポリサー	[On] をクリックして、インターフェイスで受信されるパケットに適用するポリサーの名前を指定します。
Egress policer	[On] をクリックして、インターフェイスで送信されるパケットに適用するポリサーの名前を指定します。

機能テンプレートを保存するには、[Save] をクリックします。

ARP テーブルエントリの追加

インターフェイスで静的アドレス解決プロトコル (ARP) テーブルエントリを構成するには、[ARP] をクリックします。Then click **Add New ARP** and configure the following parameters:

表 79:

パラメータ名	Description
IPアドレス	ARP エントリの IP アドレスをドット付き 10 進表記または完全修飾ホスト名として入力します。
MAC アドレス	MAC アドレスをコロン区切りの 16 進表記で入力します。

To save the ARP configuration, click **Add**.

機能テンプレートを保存するには、[Save] をクリックします。

その他のインターフェイスプロパティの設定

他のインターフェイスプロパティを設定するには、[Advanced] をクリックし、次のパラメータを設定します。

表 80: セルラーインターフェイスの高度なパラメータ

パラメータ名	説明
PMTU ディスカバリ	[On] をクリックしてインターフェイスでパス MTU ディスカバリを有効にし、パケットのフラグメント化を必要とせずにサポートされる最大の MTU サイズをルータで判別できるようにします。
TCP MSS	ルータを通過する TCP SYN パケットの最大セグメントサイズ (MSS) を指定します。デフォルトでは、MSS はインターフェイスまたはトンネル MTU に基づいて動的に調整され、TCP SYN パケットがフラグメント化されることはありません。範囲：552 ~ 1460 バイト。デフォルト：[None]。
Clear-Dont-Fragment	[On] をクリックして、インターフェイスから送信されるパケットの IPv4 パケットヘッダーの Don't Fragment (DF) ビットをクリアします。DF ビットがクリアされると、そのインターフェイスの MTU より大きいパケットは送信前にフラグメント化されます。
静的入力 QoS	着信トラフィックに使用するキュー番号を選択します。範囲：0 ~ 7
自動ネゴシエーション	[Off] をクリックして、自動ネゴシエーションをオフにします。デフォルトでは、インターフェイスは自動ネゴシエーションモードで実行されます。
TLOC Extension	WAN トランスポートに接続する同じルータ上の物理インターフェイスの名前を入力します。次に、この構成により、このサービス側のインターフェイスが WAN トランスポートにバインドされます。それ自体は WAN に直接接続されておらず（通常、サイトには 1 つの WAN 接続しかないため）、同じサイトにあり、このサービス側インターフェイスに接続する 2 番目のルータには、WAN への接続が提供されます。
トラッカー	インターネットに接続するトランスポート インターフェイスのステータスをトラッキングするトラッカーの名前を入力します。
IP Directed-Broadcast	ドロップダウンから、[Global] を選択します。IP directed-broadcast の場合、[On] をクリックします。 デフォルトは Off です。

機能テンプレートを保存するには、[Save] をクリックします。

CLI を使用したセルラーインターフェイスの設定

次の例では、セルラーインターフェイスを有効にします。

```
interface Cellular0/2/0
  description Cellular interface
  no shutdown
  ip address negotiated
  ip mtu 1428
  mtu 1500
  exit

controller Cellular 0/2/0
  lte sim max-retry 1
  lte failovertimer 7
  profile id 1 apn Broadband authentication none pdn-type ipv4
```

Data Profile

表 81: 機能の履歴

機能名	リリース情報	説明
シングルおよびデュアル SIM の実行設定で APN を設定する機能	Cisco IOS XE リリース 17.8.1a Cisco vManage リリース 20.8.1	この機能を使用すると、セルラーデバイスのデータプロファイルを作成できます。

セルラーデバイスのデータプロファイルでは、次のパラメータを定義します。デバイスでこれらのパラメータを使用して、サービスプロバイダーと通信します。セルラーコンフィギュレーションモードで **profile id** コマンドを使用して、次のパラメータを設定できます。次のパラメータの詳細については、[profile id](#) を参照してください。

- データプロファイルの識別番号
- サービスプロバイダーのアクセス ポイント ネットワーク名
- APN アクセスに使用される認証タイプ：認証なし、CHAP 認証のみ、PAP 認証のみ、または CHAP または PAP 認証のいずれか
- 認証が使用される場合、APN アクセス認証のためにサービスプロバイダーによって提供されるユーザー名とパスワード
- APN アクセスに使用されるパケットデータマッチングのタイプ：IPv4 タイプベアラー、IPv6 タイプベアラー、または IPv4v6 タイプベアラー
- 設定する SIM が挿入されている SIM スロット

セルラーインターフェイス設定のベストプラクティス

エッジデバイスのセルラーテクノロジーは、さまざまな方法で使用できます。

- **ラストリゾート回線**：ラストリゾート回線として設定されたインターフェイスはダウン状態になるため、制御接続の数の計算中にスキップされ、セルラーモデムは休止状態になり、トラフィックはこの回線経由で送信されません。

セルラー インターフェイスを備えたエッジデバイスで設定がアクティブ化されると、すべてのインターフェイスが制御およびBFD接続を確立するプロセスを開始します。1つ以上のプライマリ インターフェイスが BFD 接続を確立すると、最終手段の回線は自動的にシャットダウンします。

すべてのプライマリ インターフェイスがリモート エッジへの接続を失った場合にのみ、ラストリゾートサーキットがアクティブになり、エッジデバイスで BFD TLOC ダウンアラームと制御 TLOC ダウンアラームがトリガーされます。ラストリゾートインターフェイスは、エッジデバイスのバックアップ回線として使用され、他のすべてのトランスポートリンク BFD セッションが失敗したときにアクティブ化されます。このモードでは、無線インターフェイスはオフになり、セルラーインターフェイスを介した制御またはデータ接続は存在しません。

セルラーインターフェイスをラストリゾート回線として設定するには、**last-resort-circuit** コマンドを使用します。

- **アクティブ回線**：セルラーインターフェイスをアクティブ回線として使用することを選択できます。そうする理由は、おそらく、唯一のラストマイル回線であるためか、または回線のパフォーマンスを測定できるようにセルラーインターフェイスを常にアクティブにしておくためです。このシナリオでは、セルラーインターフェイスを介して制御接続とデータ接続を維持するために使用される帯域幅の量が問題になる可能性があります。セルラーインターフェイスを介した帯域幅の使用量を最小限に抑えるためのベストプラクティスを次に示します。
 - セルラーインターフェイスを備えたデバイスがスポークとして展開され、データトンネルがハブアンドスポーク方式で確立されている場合、セルラーインターフェイスを低帯域幅インターフェイスとして設定できます。これを行うには、セルラーインターフェイスのトンネルインターフェイスを設定するときに、**low-bandwidth-link** コマンドを含めます。セルラーインターフェイスが低帯域幅インターフェイスとして動作している場合、デバイススポークサイトはすべての発信制御パケットを同期できます。スポークサイトはまた、プロアクティブに、ルーティングアップデート以外の制御トラフィックがいずれかのリモートハブノードから生成されないようにすることもできます。ルーティングアップデートは重要なアップデートと見なされるため、引き続き送信されます。
 - 制御パケットタイマーを増やす。セルラーインターフェイスの制御トラフィックを最小限に抑えるために、インターフェイスでプロトコルアップデートメッセージが送信される頻度を減らすことができます。デフォルトでは、OMP はアップデートパケットを毎秒送信します。**omp timers advertisement-interval** 設定コマンドを含めることで、この間隔を最大 65535 秒（約 18 時間）に増やすことができます。デフォルトでは、BFD は Hello パケットを毎秒送信します。**bfd color hello-interval** 設定コマンドを含めることで、この間隔を最大 5 分（300000 ミリ秒）に増やすことができます（OMP アップデートパケットの間隔は秒単位で指定し、BFD Hello パケットの間隔はミリ秒単位で指定することに注意してください）。

- 非セルラーインターフェイスを介した Cisco vManage 制御トラフィックの優先順位付け：エッジデバイスにセルラー トランスポート インターフェイスと非セルラー トランスポート インターフェイスの両方がある場合、デフォルトでは、エッジデバイスはどちらかのインターフェイスを選択して、Cisco vManage と制御トラフィックを交換するために使用します。Cisco vManage とのトラフィック交換にセルラーインターフェイスを使用しないようにエッジデバイスを設定することも、このトラフィックにセルラーインターフェイスを使用するために低いプリファレンスを設定することもできます。トンネルインターフェイスを設定するときに **vmanage-connection-preference** コマンドを含めることで、プリファレンスを設定します。デフォルトでは、すべてのトンネルインターフェイスの Cisco vManage 接続プリファレンス値は 5 です。値の範囲は 0～8 で、値が大きいほど優先されます。プリファレンス値が 0 のトンネルは、Cisco vManage と制御トラフィックを交換することはできません。



(注) エッジデバイスの少なくとも 1 つのトンネルインターフェイスには、0 以外の Cisco vManage 接続プリファレンス値が必要です。そうでない場合、デバイスには制御接続がありません。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。