



ダイナミック オンデマンド トンネル

表 1: 機能の履歴

機能名	リリース情報	説明
ダイナミック オンデマンド トンネル	Cisco IOS XE リリース 17.3.1a Cisco vManage リリース 20.3.1	この機能を使用すると、エッジデバイス間のトンネルに非アクティブ状態を設定できるため、デバイスのパフォーマンスの要求を減らし、ネットワークトラフィックを削減できます。

Cisco SD-WAN は、任意の 2 つの Cisco SD-WAN スポークデバイス間の動的オンデマンドトンネルをサポートします。これらのトンネルは、2 つのデバイス間にトラフィックがある場合のみ設定されるようにトリガーされます。デバイス間のトラフィックのフローが停止すると、ユーザーが設定可能な非アクティブタイマーが開始され、設定された時間が経過すると、デバイス間のトンネルが削除されます。その後、2 つのデバイス間のオンデマンドリンクは、非アクティブであると見なされます。この非アクティブ状態では、ネットワーク帯域幅を使用せず、デバイスのパフォーマンスに影響しません。

ルートのバックアップとトンネルの再アクティブ化

2 つのスポークデバイスピアがオンデマンドトンネルを使用できるようにするには、ハブを経由する代替ルート（バックアップルート）が必要です。バックアップルートを使用すると、どちらのスポークデバイスも 2 つのスポーク間のトラフィックフローを再開できます。これにより、トンネルが再アクティブ化され、ピアからピアへのトラフィックが直接処理されます。

利点

オンデマンドトンネルには、次の利点があります。

- 特に、フルメッシュネットワークで動作するあまり強力ではないプラットフォームのパフォーマンスが向上。

- スポーク間でオンデマンドトンネルが使用されている場合にハブアンドスポーク展開の遅延が改善。
- 非アクティブ状態のトンネルは **Bidirectional Forwarding Detection (BFD)** プローブを必要としないため、ネットワークで使用される帯域幅が削減され、ネットワークで生成される BFD トラフィックが少ない。
- CPU とメモリの使用量を最適化しながら、スポーク間の直接トンネル。
- [オンデマンドトンネルメカニズムの詳細 \(2 ページ\)](#)
- [注意事項と制限事項 \(4 ページ\)](#)
- [オンデマンドトンネルの設定 \(5 ページ\)](#)

オンデマンドトンネルメカニズムの詳細

ダイナミックトンネルを使用するようにサイトを設定すると、オンデマンド機能が有効になります。この動作モードでは、Cisco SD-WAN エッジルータは、オンデマンド機能も有効になっている他のサイトへの直接トンネルを起動しません。

Cisco SD-WAN はバックアップ転送ノードとして機能する 1 つ以上のエッジルータ（通常は中央に配置されたルータ）を選択し、2 つのノード間のトラフィックにセカンダリパスを提供します。バックアップノードはオンデマンドで有効になっていません。すべてのオンデマンドサイトは、バックアップノードと静的トンネルを形成します。バックアップノードは、オンデマンドが有効になっている 2 つのノード間のトラフィックに静的バックアップルートを提供します。

2 つのノード間のトラフィックの最初のパケットは、静的バックアップパスを介してルーティングされ、サイト間でオンデマンドトンネルがアクティブになるようにトリガーします。バックアップパスは、直接パスがアクティブになるまでトラフィックを転送し続けます。

すべてのオンデマンドサイトは、他のすべてのオンデマンドリモートサイトの TLOC とプレフィックスを学習します。プレフィックスには、Cisco vSmart コントローラ制御ポリシーによって設定されたバックアップパスもあります。したがって、コントロールプレーンでは、オンデマンドトンネルネットワークは、バックアップパスを含むフルメッシュトンネルネットワークと同じ状態になります。コントロールプレーンはデータプレーンにダウンロードし、バックアップパスと、2 つのサイト間の潜在的な直接パスを表すリモート TLOC を使用してルーティングしますが、リモート TLOC への直接パストンネルは設定しません。

オンデマンドトンネルのいずれかの端からのトラフィックは、トンネルの設定をトリガーします。これにより、オンデマンドトンネルがネットワークアドレス変換 (NAT) トラバーサルに対応することができます。

オンデマンドトンネル機能により、オンデマンドブランチサイトには 2 つの状態が導入されます。

- **非アクティブ**：リモートサイトとのオンデマンドトンネルは設定されていません。リモートサイトとの間でアクティブなトラフィックはありません。リモートサイトの TLOC は非アクティブです。Bidirectional Forwarding Detection (BFD) は設定されず、プレフィックス

には非アクティブパスがインストールされ、バックアップパスがトラフィックを転送するパスとして設定されます。非アクティブパスはフローを検出し、直接のサイト間トンネルの設定をトリガーします。

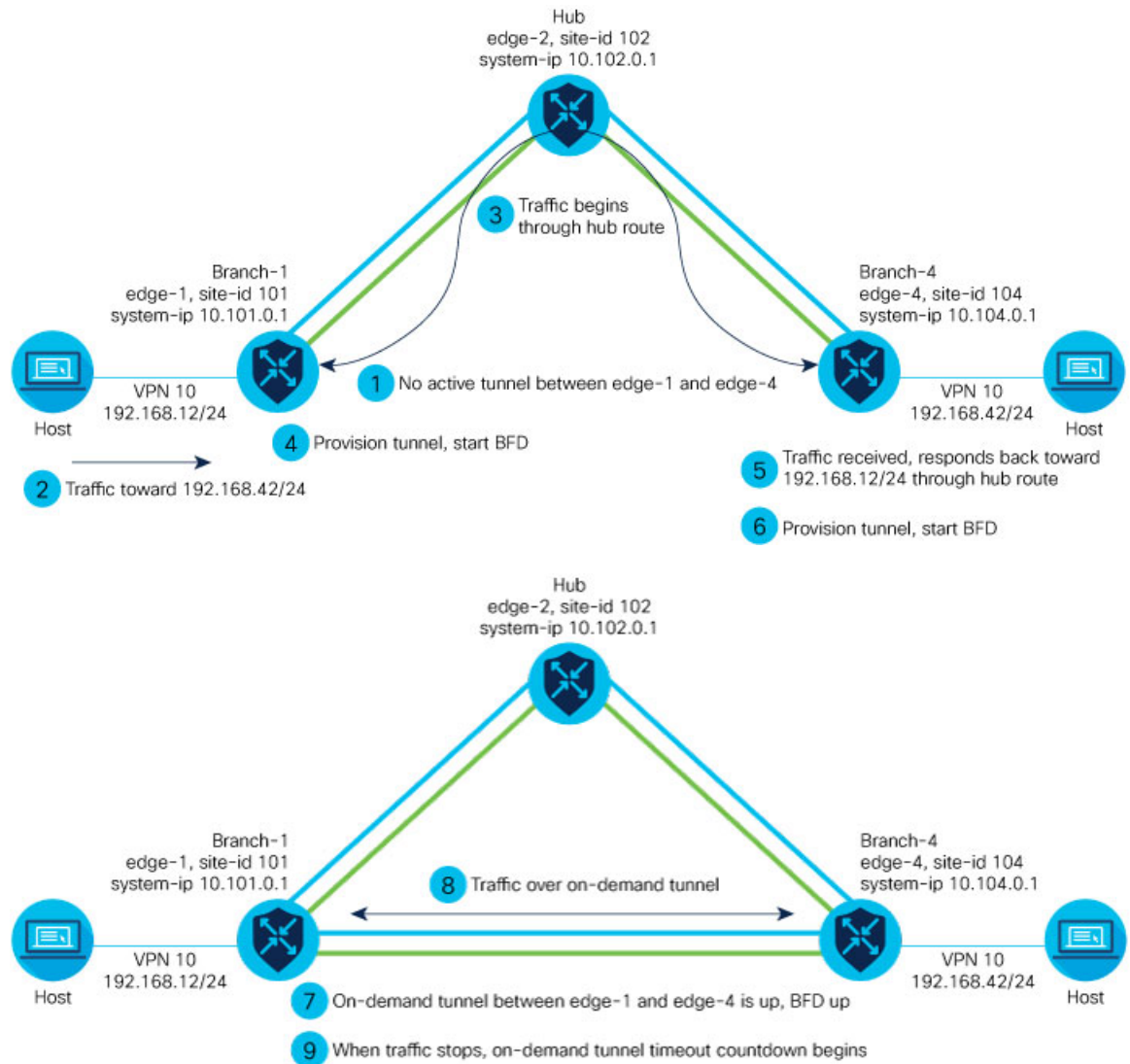
- **アクティブ**：オンデマンドの直接のサイト間トンネルがリモートサイトに設定されています。リモートサイトとの間にはアクティブなトラフィックがあります。この状態は一般的なトンネルの場合と同じであり、リモート TLOC に BFD が設定され、プレフィックスには直接パストンネルがインストールされます。この状態で、トンネルアクティビティが追跡されます。「アイドル時間」の期間（デフォルトは10分）にトラフィックがない場合、直接のサイト間トンネルは削除され、状態は非アクティブに変わります。

図の手順

次の図は、オンデマンドトンネルが設定された2つのエッジルータ間で行われる次の手順を示しています。

1. 2つのエッジルータ間にアクティブなトンネルはありません。edge-1 と edge-4 は非アクティブ状態です。
2. edge-1 の背後にあるホストは、edge-4 の背後にあるホストへのトラフィックを開始します。
3. edge-1 は、ハブまたはバックアップノードを使用してバックアップパス経由でトラフィックを edge-4 に転送します。
4. edge-1 はオンデマンドトンネルをプロビジョニングし、Bidirectional Forwarding Detection (BFD) を開始します。edge-4 は、edge-1 でアクティブ状態になります。
5. edge-4 は、edge-1 の背後にあるホストへのリターントラフィックを受信すると、ハブまたはバックアップノードを使用してバックアップパス経由でトラフィックを edge-1 に転送します。
6. edge-4 はオンデマンドトンネルをプロビジョニングし、BFD を開始します。edge-1 は、edge-4 でアクティブ状態になります。
7. この時点で、edge-1 と edge-4 の間のオンデマンドトンネルが稼働していて、BFD が稼働しています。
8. 2つのエッジデバイス間のトラフィックは、オンデマンドトンネルを経由する直接ルートを使用します。
9. edge-1 と edge-4 の両方が、オンデマンドトンネルのトラフィックアクティビティを双方向に追跡します。

アイドルタイムアウト期間中にトラフィックがない場合、オンデマンドトンネルは削除され、edge-1 および edge-4 デバイスは非アクティブ状態に戻ります。



520715

520716

注意事項と制限事項

- オンデマンドトンネルの Performance Routing (PfR) 統計の収集は、オンデマンドトンネルがセットアップされるたびに新たに開始されます。アイドルタイムアウト後、削除されたオンデマンドトンネルの PFR 統計はキャッシュされません。
- トラフィックがバックアップパスから直接オンデマンドトンネルに移動すると、Out Of Order (OOO) パケットが発生することがあります。パケットは、受信時に Cisco SD-WAN ルータによって転送されます。
- 単方向のフローは、オンデマンドのトンネルセットアップをトリガーしません。バックアップパスを引き続き使用します。

- マルチキャストトラフィックは、オンデマンドのトンネルセットアップをトリガーしません。バックアップパスを引き続き使用します。
- オンデマンドサイト TLOC に **set tloc-list** アクションを適用するデータポリシーは設定しないでください。設定されている場合、トラフィックはドロップされます。
- ペアワイズキー (PWK) IPSEC 機能が有効になっている場合、オンデマンドトンネルはサポートされません。
- **on-demand enable** または **no on-demand enable** が実行されると、システム内のすべての TLOC がリセット (無効化および有効化) されます。
- エッジデバイスがオンデマンドトンネルをプロビジョニングすると、リモートサイトのすべての TLOC にプロビジョニングされます。
- マルチホームサイトをオンデマンドモードにするには、サイトのすべてのシステムで **on-demand enable** を設定する必要があります。
- いずれかの方向のオンデマンドトンネルにサービスまたはユーザートラフィックがある場合、オンデマンドトンネルを使用するすべてのエッジデバイスはアクティブなままです。
- オンデマンドトンネルは、両方のサイトがオンデマンドモードで有効になっている場合のみ、2つのサイト間で有効にできます。
- リモートサイトの背後にあるホストへの最初のパケットは、そのリモートサイトへのオンデマンドトンネルセットアップをトリガーします。そのホストからのリターントラフィックは、反対方向のトンネルセットアップをトリガーします。
- オンデマンドリモートサイトからのすべてのプレフィックスにも、バックアップパスが設定されている必要があります。設定されていない場合、サイトはオンデマンドトンネルをセットアップできません。バックアップパスは静的トンネルであり、常に稼働している必要があります。
- オンデマンドトンネルのセットアップまたは削除は、Cisco vSmart コントローラによるオーバーレイルート (OMP) アップデート、またはサービス/LAN 側のルートアップデート (例: OSPF または BGP) には影響しません。
- ローカルサイトまたはリモートサイトのいずれかがオンデマンドモードでない場合、サイト間には静的トンネルがセットアップされます。

オンデマンドトンネルの設定

オンデマンドトンネルの前提条件

オンデマンドトンネルを使用するには、いくつかの前提条件があります。

- [前提条件 : Cisco vSmart コントローラ 集中管理ポリシー \(6 ページ\)](#)
- [前提条件 : OMP 設定 \(7 ページ\)](#)

- [前提条件 : ハブデバイス \(8 ページ\)](#)
- [前提条件 : スポークデバイス \(8 ページ\)](#)

前提条件 : Cisco vSmart コントローラ 集中管理ポリシー

1. Cisco vSmart コントローラ 集中管理ポリシーには、**tloc-action backup** アクションを含める必要があります。

説明 : これにより、すべてのスポークデバイス間の通信のためにハブを介したバックアップパスが確保されます。
2. Cisco vSmart コントローラ 集中管理ポリシーは、すべてのスポーク プレフィックスルートを受け入れる必要があります。
3. Cisco vSmart コントローラ 集中管理ポリシーは、すべてのスポークの TLOC を受け入れる必要があります。

Cisco vSmart コントローラの集中管理ポリシーの設定については、『[Cisco SD-WAN Configuration Guides](#)』のポリシー設定ガイドを参照してください。

CLI の例 (集中管理ポリシーアドレッシングの前提条件)

```
viptela-policy:policy
control-policy Dynamic-Tunnel-Control-Policy
sequence 100
match route
site-list Branches
!
action accept
set
tloc-action backup
tloc-list Hub-TLOCs
!
!
sequence 200
match tloc
!
action accept
!
default-action accept
!
lists
site-list Branches
site-id 200
site-id 300
!
tloc-list Hub-TLOCs
tloc 10.0.0.1 color mpls encap ipsec
tloc 10.0.0.1 color public-internet encap ipsec
!
!
apply-policy
site-list Branches
control-policy Dynamic-Tunnel-Control-Policy out
!
!
```

Cisco vManage の手順

1. Cisco vManage のメニューから [Configuration] > [Policies] を選択します。
2. [Centralized Policy] を選択します。
3. [Add Topology] をクリックし、[Custom Control (Route & TLOC)] を選択します。
4. [Match Conditions] の [Site] で、1つまたは複数のサイトリストを選択し、[Accept] をクリックします。
5. [Actions] の [TLOC Action] で、[Backup] アクションを選択します。
6. [TLOC List] から、既存の TLOC リストを選択するか、新しいリストを作成します。

前提条件 : OMP 設定

1. Cisco vSmart コントローラ の send-path-limit は、デフォルトの 4 より大きい必要があります。推奨 : 16

説明 : オンデマンドトンネルが有効になっている場合、スポークはハブ経由のバックアップパスを使用するため、より高いパス制限が必要です。これに対応するには、使用可能なすべてのパスをアダプタイズするように Cisco vSmart コントローラ の send-path-limit を増やします。

vSmart の **send-path-limit** の設定については、[Cisco SD-WAN の『Configuration Guides』ページのルーティング設定ガイド](#)を参照してください。

CLI の例

```
omp
no shutdown
send-path-limit 16
graceful-restart
```

Cisco vManage の手順

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. [Add template] をクリックします。
4. デバイスを選択し、[Cisco OMP] をクリックします。
5. [Basic Configuration] で、[Number of Paths Advertised per Prefix] を 16 (推奨) に設定します。

前提条件：ハブデバイス

1. ハブデバイスで、トラフィック エンジニアリング サービス（サービス TE）を有効にする必要があります。

説明：これにより、スポークデバイスの Cisco SD-WAN オーバーレイ管理プロトコル（OMP）が、2つのスポークデバイス間の中間パスとして追加されるハブを経由するバックアップパスを受け入れるようになります。これがないと、ハブを経由するバックアップパスは無効と見なされ、スポークデバイスによって解決されません。

CLI の例（Cisco vEdge デバイス）

```
vpn 0
  service TE
exit
```

CLI の例（Cisco IOS XE SD-WAN デバイス）

```
sdwan
  service TE vrf global
exit
```

Cisco vManage の手順

1. Cisco vManage で、[Configuration] > [Templates] を開きます。
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. [Add template] をクリックします。
4. プラットフォームを選択します。
5. [VPN] から [VPN] を選択します。
6. [Basic Configuration] で、[VPN] フィールドが 0 に設定されていることを確認します。
7. [Service] から、[New Service] をクリックし、[TE] を選択します。
8. [Add] をクリックしてから、[Update] をクリックします。サービスのテーブルに TE サービスが表示されます。
9. VPN-0 テンプレートをハブに適用します。

前提条件：スポークデバイス

1. スポークデバイスでは、ecmp-limit をデフォルトの 4 より大きくする必要があります。推奨：16

説明：オンデマンドトンネルが有効になっている場合、スポークデバイスはダイレクトパスとバックアップパスの両方を作成します。より多いパスのニーズに対応するため、ecmp-limit を増やします。

CLI の例

```
omp
no shutdown
ecmp-limit          16
```



(注) **show running-config omp** コマンドを使用して、現在の ecmp-limit を表示できます。

Cisco vManage の手順

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. [Add template] をクリックします。
4. デバイスを選択し、[Cisco OMP] をクリックします。
5. [Basic Configuration] で、[ECMP Limit] フィールドを 16（推奨）に設定します。

Cisco vManage を使用したオンデマンドトンネルの設定



- (注)
- 「[オンデマンドトンネルの前提条件](#)」を参照してください。
 - ハブデバイスでオンデマンドを有効にしないでください。

スポークデバイスで、すべての VPN-0 トランспорт インターフェイスのシステムレベルでオンデマンドを有効にします。マルチホームサイトの場合は、サイト内のすべてのシステムでオンデマンドを有効にします。

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. [Add template] をクリックします。
4. デバイスを選択します。
5. [Basic Information] から、[Cisco System] を選択します。
6. [詳細設定 (Advanced)] をクリックします。
7. [On-demand Tunnel] を有効にします。
8. (オプション) [On-demand Tunnel Idle Timeout] 時間を設定します。デフォルトのアイドルタイムアウト値は 10 分です。範囲 : 1 ~ 65535 分
9. システム機能テンプレートをスポークデバイスのデバイステンプレートにアタッチします。

CLI を使用したオンデマンドトンネルの設定



- (注)
- [オンデマンドトンネルの前提条件 \(5 ページ\)](#) を参照してください。
 - ハブデバイスでオンデマンドを有効にしないでください

1. スポークデバイスで、システムレベルでのオンデマンドトンネルを有効にします。マルチホームサイトの場合は、サイト内のすべてのシステムでオンデマンドを有効にします。
デフォルトのアイドルタイムアウト値は 10 分です。範囲 : 1 ~ 65535 分

例

```
system
  on-demand enable
  on-demand idle-timeout 10
```

Cisco vManage でオンデマンドトンネルの現在のステータスを表示

1. Cisco vManage のメニューから [Monitor] > [Devices] を選択します。
Cisco vManage リリース 20.6.x 以前のリリース : Cisco vManage のメニューから [Monitor] > [Network] を選択します。
2. デバイスを選択します。
3. [リアルタイム (Real Time)] を選択します。

4. [Device Options] で、次のいずれかを選択します。
 - **On Demand Local** : 指定したデバイスのオンデマンドトンネルのステータスを表示します。
 - **On Demand Remote** : 指定したデバイスおよび接続されているすべてのデバイスのオンデマンドトンネルのステータスを表示します。

出力は、`show [sdwan] system on-demand [remote-system] [system-ip ip-address]` CLI コマンドを実行した場合と同等です。オンデマンドトンネルのステータスを表示します。

Cisco vManageでオンデマンドトンネルのステータスの経時的なチャートを表示

1. Cisco vManage のメニューから [Monitor] > [Devices] を選択します。
Cisco vManage リリース 20.6.x 以前のリリース : Cisco vManage のメニューから [Monitor] > [Network] を選択します。
2. デバイスを選択します。
3. [WAN] から、[Tunnel] を選択します。
4. [Chart Options] ドロップダウンリストから、[On-Demand Tunnel Status] を選択します。チャートには、トンネルのステータスが [ACTIVE] または [INACTIVE] として表示されます。[INACTIVE] は、オンデマンドトンネルが非アクティブモードであることを示します。

詳細については、「[Cisco SD-WAN Configuration Guides](#)」ページのモニタリングおよびメンテナンスガイドを参照してください。

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。