ルーティング プロトコルのサポート

この章は、次の内容で構成されています。

ルーティング プロトコルのサポートについて

Cisco ACIファブリック内のルーティングは、BGP（BFDサポート）およびOSPFまたはEIGRPルーティング プロトコルを使用して実装されます。

IP 送信元ルーティングは ACI ファブリックではサポートされません。

Cisco ACI の等コスト マルチパス ルーティングについて

Cisco Application Centric Infrastructure（ACI）では、境界リーフ スイッチに接続されているすべてのネクストホップは、ハードウェアで転送されるときに、1つの等コストマルチパス（ECMP）ルーティングパスと見なされます。Cisco ACI は、直接接続されたネクストホップの場合は ECMP パスを BGP に再配布しませんが、再帰的なネクストホップの場合は再配布します。

次の例では、ボーダー リーフ スイッチ1および2が、ネクストホップ伝播を使用して10.1.1.0/24ルートをアドバタイズし、接続されたホスト機能を再配布します。

```
10.1.1.0/24
    through 192.168.1.1 (border leaf switch 1) -> ECMP path 1
    through 192.168.1.2 (border leaf switch 1) -> ECMP path 1
    through 192.168.1.3 (border leaf switch 1) -> ECMP path 1
    through 192.168.1.4 (border leaf switch 2) -> ECMP path 2
```

- ECMP パス 1：50%（ネクストホップ 192.168.1.1、192.168.1.2、192.168.1.3）
- ECMP パス 2：50%（ネクストホップ 192.168.1.4）

（注） 各ネクストホップのトラフィック ハッシュのパーセンテージは概算値です。実際のパーセンテージは異なります。

非境界リーフ スイッチのこのルート エントリは、非境界リーフから各境界リーフ スイッチへの 2 つの ECMP パスになります。これにより、ルートをアドバタイズするボーダー リーフ スイッチ間でネクストホップが均等に分散されていない場合、ボーダー リーフ スイッチへのロード バランシングが不均衡になる可能性があります。

Cisco ACI リリース 6.0(2) 以降では、ネクストホップ伝播および接続ホスト機能の再配布を使用して、Cisco ACI ファブリック内の最適でないルーティングを回避できます。これらの機能が有効になっている場合、非境界リーフ スイッチからのパケット フローは、ネクストホップ アドレスに接続されているリーフ スイッチに直接転送されます。すべてのネクストホップがハードウェアからの ECMP 転送に使用されるようになりました。さらに、Cisco ACI は、直接接続されたネクストホップと再帰ネクストホップの両方の ECMP パスを BGP に再配布するようになりました。

次の例では、リーフ スイッチ 1 と 2 がネクストホップで 10.1.1.0/24 ルートをアドバタイズし、接続されたホスト機能を再配布します。

```
10.1.1.0/24
    through 192.168.1.1 (border leaf switch 1) -> ECMP path 1
    through 192.168.1.2 (border leaf switch 1) -> ECMP path 2
    through 192.168.1.3 (border leaf switch 1) -> ECMP path 3
    through 192.168.1.4 (border leaf switch 2) -> ECMP path 4
```

- ECMP パス 1：25%（ネクストホップ 192.168.1.1）
- ECMP パス 2：25%（ネクストホップ 192.168.1.2）
- ECMP パス 3：25%（ネクストホップ 192.168.1.3）
- ECMP パス 4：25%（ネクストホップ 192.168.1.4）

BGP 外部ルーテッド ネットワークと BFD のサポート

ここでは、BFD をサポートする BGP 外部ルーテッド ネットワークの詳細について説明します。

BGP レイヤ 3 外部ネットワーク接続設定のガイドライン

BGP外部ルーテッドネットワークを設定するときは、以下のガイドラインに従ってください。

- BGP 直接ルート エクスポートの動作は、リリース 3.2(1) 以降に変更されました。この場合 ACI は、エクスポート ルート マップ節を照合するときに、発信元ルート タイプ（スタティック、ダイレクトなど）を評価しません。その結果、アウトバウンド ネイバー ルート マップに常に含まれる「match direct」deny 節は、直接ルートと一致しなくなり、ユー

ザ定義のルートマップ節が一致するかどうかに基づいて直接ルートがアドバタイズされるようになりました。

したがって、直接ルートはルートマップを介して明示的にアドバタイズする必要があります。そうしないと、アドバタイズされている直接ルートが暗黙的に拒否されます。

- L3Out の BGP ピア接続プロファイルの [BGP 制御（BGP Controls）] フィールドの [AS オーバーライド（AS override）] オプションは、リリース 3.1(2) で導入されました。これにより、Cisco Application Centric Infrastructure（ACI）は AS_PATH 内のリモート AS を ACI BGP AS で上書きできます。Cisco ACI において、これは通常、eBGP L3Out から同じ AS 番号を持つ別の eBGP L3Out への中継ルーティングを実行するときに使用されます。

  ただし、eBGP ネイバーの AS 番号が異なる場合に [AS オーバーライド（AS override）] オプションを有効にすると、問題が発生します。この状況では、ピアに反映するときに AS_PATH から peer-as を削除します。

- BGP ピア接続プロファイルの **[ローカル AS 番号（Local-AS Number）]**オプションは、eBGP ピアリングでのみサポートされます。これにより、Cisco ACI ボーダー リーフ スイッチは、ファブリック MP-BGP ルート リフレクタ ポリシーに割り当てられた実際の AS に加えて、別の AS のメンバーであるように見えます。そのため、ローカル AS 番号は Cisco ACI ファブリックの実際の AS 番号とは異なる必要があります。この機能が構成されている場合、Cisco ACI ボーダー リーフ スイッチは、ローカル AS 番号を着信更新の AS_PATH に付加し、同じ番号を発信更新の AS_PATH に付加します。**[ローカル AS 番号構成（Local-AS Number Config）]** の **no-prepend** 設定によって、ローカル AS 番号の着信更新への付加を無効にできます。**no-prepend + replace-as** 設定を使用すると、ローカル AS 番号が発信更新に付加されるのを防ぐことができます。

- ルーティング プロトコルの L3Out のルーター ID は、ルーテッド インターフェイス、サブインターフェイス、SVI などの L3Out インターフェイスと同じ IP アドレスまたは同じサブネットにすることはできません。ただし、必要に応じて、ルータ ID を L3Out ループバック IP アドレスの 1 つと同じにすることができます。

- 同じ VRF インスタンスの同じリーフ スイッチに同じルーティング プロトコルの複数の L3Out がある場合、それらのルータ ID は同じである必要があります。ルータ ID と同じ IP アドレスを持つループバックが必要な場合は、それらの L3Out の 1 つだけにループバックを構成できます。

- L3Out の BGP ピアを定義するには、次の 2 つの方法があります。

  - ループバック IP アドレスに BGP ピアを関連付ける論理ノード プロファイル レベル（l3extLNodeP）のBGPピア接続プロファイル（bgpPeerP）を介した方法。BGP ピアがこのレベルで設定されている場合は、BGP 接続にループバック アドレスが想定されます。そのため、ループバック アドレス設定が欠落していると、障害が発生します。

  - BGP ピアをそれぞれのインターフェイスまたはサブインターフェイスに関連付け、論理インターフェイス プロファイル レベル（l3extRsPathL3OutAtt）で BGP ピア接続プロファイル（bgpPeerP）を介した方法。

- IPv6 を使用したループバックを介したピアリングを有効にするには、ユーザーが IPv6 アドレスを構成する必要があります。
- BGP `l3extOut` 接続のテナント ネットワーキング プロトコル ポリシーは、最大プレフィックス制限を使用して構成できます。これにより、ピアから受信するルートプレフィックスの数をモニタし、制限することができます。最大プレフィックス制限を超えると、ログエントリの記録、それ以降のプレフィックスの拒否、固定期間中にカウントがしきい値未満になった場合の接続の再起動、または接続のシャットダウンを行うことができます。一度に 1 つのオプションだけを使用できます。デフォルト設定では 20,000 プレフィックスに制限され、その後は新しいプレフィックスは拒否されます。拒否オプションを展開すると、BGP は設定されている制限よりも 1 つ多くプレフィックスを受け入れるようになり、Cisco Application Policy Infrastructure Controller（APIC）はエラーを発生させます。

（注） Cisco ACI は IP フラグメンテーションをサポートしていません。したがって、外部ルータへのレイヤ 3 Outside（L3Out）接続、または Inter-Pod Network（IPN）を介した マルチポッド 接続を設定する場合は、インターフェイス MTU がリンクの両端で適切に設定されていることが推奨されます。Cisco ACI、 Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定可能な MTU 値はイーサネット ヘッダー (一致する IP MTU、14-18 イーサネット ヘッダー サイズを除く) を考慮していません。また、IOS XR などの他のプラットフォームには、設定された MTU 値にイーサネットヘッダーが含まれています。設定された値が 9000 の場合、Cisco ACI、Cisco NX-OS Cisco IOS の最大 IP パケット サイズは 9000 バイトになりますが、IOS-XR のタグなしインターフェイスの最大 IP パケットサイズは 8986 バイトになります。

各プラットフォームの適切な MTU 値については、それぞれの設定ガイドを参照してください。

CLI ベースのコマンドを使用して MTU をテストすることを強く推奨します。たとえば、Cisco NX-OS CLI で `ping 1.1.1.1 df-bit packet-size 9000 source-interface ethernet 1/1` などのコマンドを使用します。

BGP の接続タイプとループバックのガイドライン

ACI では次の BGP 接続の種類をサポートし、それらのループバックのガイドラインをまとめています。

BGP 接続タイプ	ループバックが必要	ルータ ID と同じループバック	スタティック ルートまたは OSPF ルートが必要
直接 iBGP	非対応	N/A	非対応

BGP 接続タイプ	ループバックが必要	ルータ ID と同じループバック	スタティック ルートまたは OSPF ルートが必要
iBGP ループバック ピアリング	はい（L3Out ごとに個別のループバック）	いいえ（同じノードに複数のレイヤ 3 Out がある場合）	はい
直接 eBGP	非対応	N/A	非対応
eBGP ループバック ピアリング（マルチホップ）	はい（L3Out ごとに個別のループバック）	いいえ（同じノードに複数のレイヤ 3 Out がある場合）	はい

外部 BGP スピーカーに対する BGP プロトコル ピアリング

ACI は、iBGP と eBGP を使用して境界リーフと外部 BGP スピーカーの間のピアリングをサポートします。ACI は、BGP ピアリングで以下の接続をサポートします。

- OSPF 上の iBGP ピアリング
- OSPF 上の eBGP ピアリング
- 直接接続上の iBGP ピアリング
- 直接接続上の eBGP ピアリング
- スタティック ルート上の iBGP ピアリング

（注） BGP ピアリングで OSPF が使用される場合、OSPF は BGP ピアリング アドレスへのルートの学習とアドバタイズのみに使用されます。レイヤ 3 Outside ネットワーク（EPG）に適用されるすべてのルート制御が BGP プロトコル レベルで適用されます。

ACI は、外部ピアへの iBGP および eBGP 接続用に多数の機能をサポートします。BGP 機能は、[BGP Peer Connectivity Profile] で設定されます。

BGP ピアの接続プロファイル機能について、次の表で説明します。

（注） ACI は、次の BGP 機能をサポートしています。以下にリストされていない NX-OS BGP 機能は、現在 ACI ではサポートされていません。

表 *1: BGP* ピアの接続プロファイル機能

BGP 機能	機能の説明	NX-OS での同等のコマンド
Allow Self-AS	Allowed AS Number Count 設定と併用されます。	**allowas-in**
Disable peer AS check	アドバタイズ時のピア AS 番号のチェックを無効にします。	**disable-peer-as-check**
Next-hop self	常にローカル ピア アドレスにネクスト ホップ属性を設定します。	**next-hop-self**
Send community	ネイバーにコミュニティ属性を送信します。	**send-community**
Send community extended	ネイバーに拡張コミュニティ属性を送信します。	**send-community extended**
Password	BGP MD5 認証。	**password**
Allowed AS Number Count	Allow Self-AS 機能と併用されます。	**allowas-in**
Disable connected check	直接接続された EBGP ネイバーの接続チェックを無効にします（EBGP ネイバーがループバックからピアリングすることを許可）。	
TTL	EBGP マルチホップ接続の TTL 値を設定します。これは EBGP でのみ有効です。	**ebgp-multihop <TTL>**
Autonomous System Number	ピアのリモート自律システム番号。	**neighbor <x.x.x.x> remote-as**
Local Autonomous System Number Configuration	ローカル AS 機能を使用するときのオプション（No Prepend+replace-AS+dual-AS など）。	

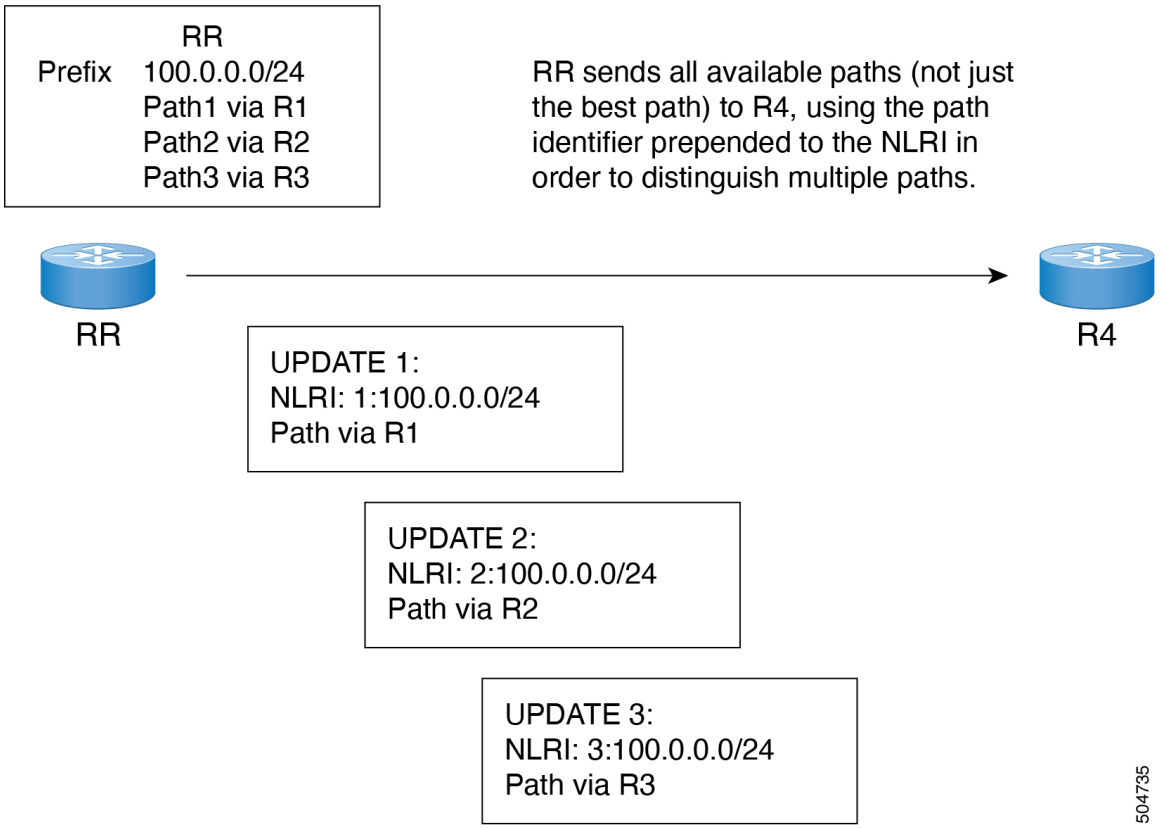
BGP 機能	機能の説明	NX-OS での同等のコマンド
Local Autonomous System Number	ファブリック MP-BGP ルート リフレクタ プロファイルに割り当てられている AS とは異なる AS 番号をアドバタイズするために使用されるローカル AS 機能。これは EBGP ネイバーの場合にのみサポートされ、ローカル AS 番号がルート リフレクタ ポリシー AS と異なっている必要があります。	**local-as xxx <no-prepend> <replace-as> <dual-as>**
Site of Origin	site-of-origin（SoO）は、ルーティング ループを防ぐためにルートを学習するサイトを一意に識別するために使用される BGP 拡張コミュニティ属性です。	**soo<value>**

BGP 付加パス

Cisco Application Policy Infrastructure Controller（APIC）6.0(2) リリース以降、BGP は、以前のパスに代わる新しいパスなしで、BGP スピーカが同じプレフィックスに対して複数のパスを伝播し、受け入れることを可能にする追加のパス機能をサポートします。この機能は、BGP スピーカのピアが、プレフィックスごとの複数パスのアドバタイズおよび受信をサポートし、また、そのパスのアドバタイズをサポートするかどうかネゴシエートすることを可能にします。特別な 4 バイトのパス ID は、ピア セッションを介して送信される同じプレフィックスに対して複数のパスを区別するため、ネットワーク層到達可能性情報（NLRI）に追加されます。

次の図に、追加の BGP 追加パス受信機能を示します。

図 *1:* 追加パスの機能を持つ *BGP* ルート アドバタイズメント



次の制限が適用されます。

- Cisco APIC は受信機能のみをサポートします。
- セッションの確立後に BGP 追加パス受信機能を設定すると、その設定は次のセッション フラップで有効になります。

追加パス受信機能が導入される前は、BGP は 1 つのパスだけをアドバタイズし、BGP スピーカは特定ピアからの特定プレフィックスの1パスだけを受け入れました。BGPスピーカが同じセッション内で同じプレフィックスの複数のパスを受信した場合、最新のアドバタイズメントが使用されました。

BGP 外部ルーテッド ネットワークの設定

BGP 外部ルーテッド ネットワークを設定するには、次の項の手順を使用します。

GUI を使用した BGP L3Out の設定

始める前に

BGP L3Out を設定するテナント、VRF、およびブリッジ ドメインはすでに作成されており、VRF の作成時に [BGP ポリシーの設定（Configure BGP Policies）] オプションを選択しました。

手順

ステップ 1 **[メニュー（Menu）]** バーで、**[テナント（Tenants）]** > **[すべてのテナント（All Tenants）]**を選択します。

ステップ 2 作業ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 [**ナビゲーション（Navigation**）] ペインで、**[*Tenant_name*]** > **[ネットワーキング（Networking）]** > **[L3Outs]** の順に展開します。

ステップ 4 [L3Outs] を右クリックし、[L3Out の作成（Create L3Out）] を選択します。

[**L3Out の作成（Create L3Out**）] ウィザードが表示されます。

ステップ 5 **[L3Out の作成（Create L3Out）]** ウィザードの **[識別（Identity）]** ページに必要な情報を入力します。

a) [名前（Name）]、[VRF]、および [L3 ドメイン（L3 Domain）] フィールドに必要な情報を入力します。

b) ルーティング プロトコルのチェック ボックスがある領域で、[BGP] を選択します。

c) [**次（Next**）] をクリックして [**ノードとインターフェイス（Nodes and Interfaces**）] ウィンドウに移動します。

ステップ 6 **[L3Out の作成（Create L3Out）]** ウィザードの **[ノードとインターフェイス（Nodes and Interfaces）]** ページに必要な情報を入力します。

a) [レイヤ 3（Layer 3）] 領域で、[ルーテッド（Routed）] を選択します。

b) [**ノード ID（Node ID**）] フィールドのドロップダウン メニューで、L3Out のノードを選択します。

これらの例のトポロジでは、ノード `103` を使用します。

c) [Router ID] フィールドに、ルータ ID を入力します。

d) （任意） 必要に応じて、ループバック アドレスに別の IP アドレスを設定できます。

[ルータ ID（Router ID）] フィールドに入力したエントリと同じ内容が [ループバック アドレス（Loopback Address）] フィールドに自動で入力されます。これは以前のビルドでの [ループバック アドレスのルータ ID の使用（Use Router ID for Loopback Address）] と同等です。ループバック アドレスにルータ ID を使用しない場合は、ループバック アドレスに別の IP アドレスを入力します。または、ループバック アドレスにルータ ID を使用しない場合は、このフィールドを空のままにします。

e) **[ノードとインターフェイス（Nodes and Interfaces）]** ページに追加の必要な情報を入力します。

このページに表示されるフィールドは、**[レイヤ 3（Layer 3）]** および **[レイヤ 2（Layer 2）]** 領域で選択したオプションによって異なります。

f) **[ノードとインターフェイス（Nodes and Interfaces）]** ページで残りの追加の情報を入力したら、**[次へ（Next）]** をクリックします。

[プロトコル（Protocol）] ページが表示されます。

ステップ 7 **[L3Out の作成（Create L3Out）]** ウィザードの **[プロトコル（Protocols）]** ページに必要な情報を入力します。

a) [BGP ループバック ポリシー（BGP Loopback Policies）] および [BGP インターフェイス ポリシー（BGP Interface Policies）] 領域で、次の情報を入力します。

- **ピア アドレス（Peer Address）**：ピア IP アドレスを入力します
- **EBGP Multihop TTL（EBGP マルチホップ TTL）**：接続の存続可能時間（TTL）を入力します。範囲は 1 ー 255 ホップです。ゼロの場合、TTL は指定されません。デフォルトは 1 です。
- **リモート ASN（Remote ASN）**：ネイバー自律システムを固有に識別する番号を入力します。自律システム番号は、1 ー 4294967295 のプレーン形式で 4 バイトにすることができます。

（注） ACI は asdot または asdot + 形式の AS 番号をサポートしていません。

b) **[次へ（Next）]** をクリックします。

[外部タスク（External Tasks）] ページが表示されます。

ステップ 8 **[L3Out の作成（Create L3Out）]** ウィザードで **[外部 EPG（External EPG）]** ページに必要な情報を入力します。

a) **Name** フィールドに、外部ネットワークの名前を入力します。
b) **[提供済みコントラクト（Provided Contract）]** フィールドで、提供済みコントラクトの名前を入力します。
c) **[消費済みコントラクト（Consumed Contract）]** フィールドで、消費済みコントラクトの名前を入力します。
d) [すべての外部ネットワークのデフォルト EPG（Default EPG for all external network）] フィールドで、この L3Out 接続からのすべての中継ルートをアドバタイズしない場合はオフにします。

このボックスをオフにすると、[Subnets] 領域が表示されます。次の手順に従って、必要なサブネットとコントロールを指定します。

e) [+] アイコンをクリックして [サブネット（Subnet）] を展開し、[サブネットの作成（Create Subnet）] ダイアログ ボックスで次の操作を実行します。
f) **IP address** フィールドに、外部ネットワークの IP アドレスとサブネット マスクを入力します。

（注） 前のステップで入力した内容に応じて、IPv4 または IPv6 のアドレスを入力します。

外部サブネットを作成するときに、プレフィックス EPG の BGP ループバックの両方を設定するか、またはどちらも設定しない必要があります。BGP ループバックを 1 つのみ設定すると、BGP ネイバーシップは確立されません。

g) [**名前（Name**）] フィールドに、サブネットの名前を入力します。

h) [Scope] フィールドで、[Export Route Control Subnet] 、[Import Route Control Subnet] 、および [Security Import Subnet] のチェックボックスをオンにします。[OK] をクリックします。

（注） BGP でインポート制御を適用する場合は、[Import Route Control Subnet] チェックボックスをオンにします。

i) [サブネットの作成（Create Subnet）] ウィンドウで必要な設定が完了したら、[OK] をクリックします。

j) [完了（Finish）] をクリックして、[L3Out の作成（Create L3Out）] ウィザードに必要な設定の入力を完了させます。

ステップ 9 （任意） 必要に応じて、[BGP ピア接続プロファイル（BGP Peer Connectivity Profile）] ウィンドウに移動して、BGP 外部ルーテッドネットワークの追加設定を行います。

[テナント（Tenants）] > [*tenant_name*] > [ネットワーキング（Networking）] > [L3Outs] > [*L3Out_name*] > [論理ノード プロファイル（Logical Node Profiles）] > [*log_node_prof_name*] > [BGP ピア（BGP Peer）*] <address>*

この L3Out の **[BGP ピア接続プロファイル（BGP Peer Connectivity Profile）]** ページが表示されます。

a) [BGP Controls] フィールドで、目的の制御をオンにします。

ピアは、ピアに送信される境界ゲートウェイ プロトコル（BGP）属性を指定します。ピア制御オプションは次のとおりです。

- **[自身の AS を許可（Allow Self AS）]**：自律番号チェックを自身で有効にします。これにより、同じ AS 番号が使用されている場合に BGP ピアが更新を挿入できます。
- **[AS オーバーライド（AS override）]**：BGP AS オーバーライド機能を有効にして、デフォルト設定をオーバーライドします。AS オーバーライド機能では、発信元のルータからの AS 番号を、アウトバウンド ルートの AS パスの BGP ルータ送信の AS 番号に置き換えます。アドレス ファミリごとにこの機能を有効にできます（IPv4 または IPv6）。

  AS オーバーライド機能を有効にするには、[ピア AS チェックを無効化（Disable Peer AS Check）] チェックボックスもオンにする必要があります。

- **[ピア AS チェックを無効化（Disable Peer AS Check）]**：ピア自律番号チェックを無効にします。このチェックボックスをオンにすると、アドバタイジング ルータが

AS パスでレシーバの AS 番号を見つけた場合、そのルータはレシーバにルートを送信しません。

AS オーバーライド機能を有効にするには、[ピア AS チェックを無効化（Disable Peer AS Check）] チェックボックスをオンにする必要があります。

- **[自身にネクスト ホップを送信（Next-hop Self）]**：BGP ネクスト ホップ属性を自身に送信します。
- **[コミュニティの送信（Send Community）]**：ピアに BGP コミュニティ属性を送信します。
- **[拡張コミュニティの送信（Send Extended Community）]**：ピアに BGP 拡張コミュニティ属性を送信します。
- **[ドメイン パスの送信（Send Domain Path）]**：BGP ドメイン パスをピアに送信します。

b) **[追加パスの受信（Receive Additional Paths）]** チェックボックスをオンにして、この eBGP L3Out ピアが他の eBGP ピアからプレフィックスごとに追加のパスを受信できるようにします。

[追加パスの受信（Receive Additional Paths）] 機能がない場合、eBGP では、リーフ スイッチがプレフィックスのピアからネクスト ホップを 1 つだけ受信できます。

または、他の eBGP ピアからプレフィックスごとに追加のパスを受信するように、テナントの VRF インスタンス内のすべての eBGP ピアを設定できます。詳細については、GUI を使用した BGP Max Path の設定 （16 ページ）を参照してください。

c) [パスワード（Password）] フィールドと [パスワードの確認（Confirm Password）] フィールドに、管理パスワードを入力します。

d) [自身の AS 番号カウントを許可（Allow Self AS Number Count）] フィールドで、ローカル自律システム番号（ASN）の許可される発生回数を選択します。

値の範囲は 1 ～ 10 です。デフォルトは 3 です。

e) [ピア制御（Peer Controls）] フィールドに、ネイバー チェック パラメータを入力します。

次のオプションがあります。

- **[双方向フォワーディングの検出（Bidirectional Forwarding Detection）]**：ピアの BFD を有効にします。
- **[接続チェックの無効化（Disable Connected Check）]**：ピア接続のチェックを無効にします。

f) [アドレス タイプ制御（Address Type Controls）] フィールドで、必要に応じて BGP IPv4/IPv6 アドレスファミリ機能を設定します。

- [AF Mcast]：マルチキャスト アドレスファミリ機能を有効にする場合にオンにします。

- [AF Ucast]：ユニキャストアドレスファミリ機能が有効にする場合にオンにします。

g) 必要に応じて、[ルーティング ドメイン ID（Routing Domain ID）] のエントリをメモします。

[ルーティング ドメイン ID（Routing Domain ID）] フィールドの値は、[BGP ルート リフレクタ ポリシー（BGP Route Reflector Policy）] ページに入力されたグローバル ドメイン ID ベース値を反映します。詳細については、「ループ防止のための BGP ドメインパス機能について」を参照してください。

h) [EBGP マルチホップ TTL（EBGP Multihop TTL）] フィールドに、接続存続可能時間（TTL）を入力します。

範囲は 1 ー 255 ホップです。ゼロの場合、TTL は指定されません。デフォルトは 1 です。

i) [このネイバーからのルートの重み付け（Weight for routes from this neighbor）] フィールドで、ピアからのルートに許可される重みを選択します。

ルータにローカルに割り当てられた重みが、最適パスの選択に使用されます。範囲は 0 ～ 65535 です。

j) [プライベート AS 制御（Private AS Control）] フィールドで、プライベート AS 制御を設定します。

これらのオプションは、ACI BGP AS がパブリック AS 番号である場合、または [no-Prepend+replace-as] オプションを指定した [Local-AS 番号設定（Local-AS Number Config）] が、指定された BGP ピア接続プロファイル（BGP ネイバー コンフィギュレーション）。[プライベート AS 制御（Private AS Control）] 機能は自身のローカル プライベート AS を削除しないため、[replace-as] オプションを使用して、実際のローカル プライベート AS を AS_PATH から削除します。

次のオプションがあります。

- **[すべてのプライベート AS の削除（Remove all private AS）]**：発信 eBGP ルート更新ではこのネイバーを更新する際に、AS_PATH からすべてのプライベート AS 番号を削除します。eBGP ルートにプライベート AS 番号とパブリック AS 番号がある場合は、このオプションを使用します。パブリック AS 番号は保持されます。

  ネイバーのリモート AS が AS_PATH にある場合、このオプションは適用されません。

  このオプションを有効にするには、[プライベート AS の削除（Remove private AS）] を有効にする必要があります。

- **[プライベート AS の削除（Remove private AS）]**：このネイバーへの発信 eBGP ルート更新では、AS_PATH にプライベート AS 番号しかない場合、このオプションはすべてのプライベート AS 番号を削除します。eBGP ルートにプライベート AS 番号のみがある場合は、このオプションを使用します。

  ネイバーのリモート AS が AS_PATH にある場合、このオプションは適用されません。

- **[プライベート AS をローカル AS と置換（Replace private AS with local AS）]**：このネイバーへの発信 eBGP ルート更新では、このオプションは、パブリック AS またはネイバー リモート AS が AS_PATH に含まれているかどうかに関係なく、AS_PATH 内のすべてのプライベート AS 番号を ACI ローカル AS に置き換えます。

  このオプションを有効にするには、[すべてのプライベート AS を削除（Remove all private AS）] を有効にする必要があります。

k) [BGP ピア プレフィックス ポリシー（BGP Peer Prefix Policy）] フィールドで、既存のピア プレフィックス ポリシーを選択するか、新しいポリシーを作成します。

ピア プレフィックス ポリシーは、ネイバーから受信できるプレフィックスの数と、許可されるプレフィックスの数を超えた場合に実行するアクションを定義します。この機能は、外部 BGP ピアで一般的に使用されますが、内部 BGP ピアにも適用できます。

l) [Site of Origin] フィールドに、このピアを識別するための拡張コミュニティ値を入力します。

Site-of-Origin（SoO）拡張コミュニティは、サイトを発信元とするルートを識別し、そのプレフィックスの再アドバタイズメントが送信元のサイトに戻されることを防ぐために使用される BGP 拡張コミュニティ属性です。この SoO 拡張コミュニティは、ルータがルートを学んだサイトを一意に識別します。BGP は、ルートに関連付けられた SoO 値を使用し、ルーティング ループを防止できます。

有効な形式：

- extended:as2-nn2:<2-byte number>:<2-byte number>

  例：`extended:as2-nn2:1000:65534`

- extended:as2-nn4:<2-byte number>:<4-byte number>

  例： `extended:as2-nn4:1000:6554387`

- extended:as4-nn2:<4-byte number>:<2-byte number>

  例：`extended:as4-nn2:1000:65504`

- extended:ipv4-nn2:<IPv4 address>:<2-byte number>

  例： `extended:ipv4-nn2:1.2.3.4:65515`

（注） ユーザ テナント L3Out の SoO を設定する場合は、ACI ファブリック内で設定されたグローバル ファブリック、ポッド、またはマルチ サイト SoO と同じ SoO 値を設定しないようにしてください。スイッチで次のコマンドを実行すると、ファブリック内に設定されたファブリック、ポッド、およびマルチサイト SoO の値を表示できます。

```
show bgp process vrf overlay-1 | grep SOO
```

m) [リモート自律システム番号（Remote Autonomous System Number）] フィールドで、ネイバー自律システムを一意に識別する番号を選択します。

自律システム番号は、1 ー 4294967295 のプレーン形式で 4 バイトにすることができます。

（注） ACI は asdot または asdot + 形式の AS 番号をサポートしていません。

n) [ローカル AS 番号設定（Local-AS Number Config）] フィールドで、ローカル自律システム番号（ASN）設定を選択します。

グローバル AS ではなくローカル AS 番号を使用すると、関連付けられたネットワーク内のルーティング デバイスが以前の AS に属しているように見えます。設定は次のとおりです。

- **[no-Prepend+replace-as+dual-as]**：ローカル AS での先頭付加を許可せず、両方の AS 番号で置き換えます。

  AS パスの先頭に 1 つ以上の自律システム（AS）番号を付加できます。AS 番号は、ルートの発信元である実際の AS 番号がパスに追加された後に、パスの先頭に追加されます。AS パスの前に付加すると、AS パスが短く見えるため、BGP よりも優先度が低くなります。

- **[no-prepend]**：ローカル AS でのプリペンドを許可しません。
- **[no options]**：ローカル AS の変更を許可しません。
- **[no-Prepend+replace-as]**：ローカル AS での先頭追加を許可せず、AS 番号を置き換えます。

o) [ローカル AS 番号（Local-AS Number）] フィールドで、目的の値を選択します。

eBGP ピアのローカル自律システム機能の場合にオプションで必要です。ローカル自律システム番号は、1 ー 4294967295 のプレーン形式で 4 バイトにすることができます。ACI は asdot または asdot + 形式の AS 番号をサポートしていません。

p) [管理状態（Admin State）] フィールドで、[無効化（Disabled）] または [有効化（Enabled）] を選択します。

[管理状態（Admin State）] フィールドでは、対応する BGP ネイバーをシャットダウンできます。この機能を使用すると、BGP ピア設定を削除せずに BGP セッションがシャットダウンされます。

次のオプションがあります。

- 無効化：BGP ネイバーの管理状態を無効にします。
- 有効化：BGP ネイバーの管理状態を有効にします。

q) [ルート制御プロファイル（Route Control Profile）]フィールドで、BGP ピアごとにルート制御ポリシーを設定します。

[+] をクリックして、次を設定します。

- [名前（Name）]：ルート制御プロファイル名を選択します。
- [**方向（Direction**）]：次のいずれかのオプションを選択します。

- ルートインポートポリシー
- ルートエクスポートポリシー

r) **[送信（Submit）]** をクリックします。`

ステップ 10 **[テナント（Tenants）]** > **[*tenant_name*]** > **[ネットワーキング（Networking）]** > **[L3Outs]** > **[*L3Out_name*]** に移動します。

ステップ 11 [ポリシー/メイン（Policy/Main）] タブをクリックし、次の操作を実行します。

a) （任意） [Route Control Enforcement] フィールドで、[mport] チェックボックスをオンにします。

（注） BGP でインポート制御を適用する場合は、このチェックボックスをオンにします。

b) [Route Control for Dampening] フィールドを展開し、目的のアドレス ファミリ タイプとルート ダンプニング ポリシーを選択します。[Update] をクリックします。

このステップでは、ポリシーはステップ 4 で作成することができます。または、ポリシー名が選択されているドロップダウン リストで **[ルート プロファイルの作成（Create route profile）]** をするオプションがあります。

ステップ 12 **[テナント（Tenants）]** > **[*tenant_name*]** > **[ネットワーキング（Networking）]** > **[L3Outs]** > **[*L3Out_name*]** に移動します。

ステップ 13 **[ルート制御のインポートおよびエクスポートのルート マップ（Route Map for import and export rout control）]** を右クリックし、**[ルート制御のインポートおよびエクスポートのルート マップの作成（Create Route Map for import and export rout control）]** を選択します。

ステップ 14 このウィンドウに必要な情報を入力し、[コンテキスト（Context）] 領域で [+] をクリックして [ルート制御コンテキストの作成（Create Route Control Context）] ウィンドウを表示します。

a) **[名前（Name）]**フィールドに、ルート制御 VRF の名前を入力します。

b) [Set Attribute] ドロップダウン リストから、[Create Action Rule Profile] を選択します。

アクション ルールを作成するときに、必要に応じてルート ダンプニング属性を設定します。

BGP Max Path の設定

次の機能を使用すると、等コスト マルチパスのロード バランシングを有効にするルート テーブルへのパスの最大数を追加できます。

GUI を使用した BGP Max Path の設定

始める前に

適切なテナントと BGP 外部ルーティング ネットワークが作成され、使用可能になります。

手順

ステップ 1 **[メニュー（Menu）]** バーで、**[テナント（Tenants）]** > **[すべてのテナント（All Tenants）]** を選択します。

ステップ 2 作業ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 **[ナビゲーション（Navigation）]** ペインで、***[*** **テナント名（*Tenant_name*）** ***]*** > **[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[BGP]** > **[BGP アドレス ファミリ コンテキスト（BGP Address Family Context）]** を展開します。

ステップ 4 **[BGP アドレス ファミリ コンテキスト（BGP Address Family Context）]** を右クリックし、**[BGP アドレス ファミリ コンテキスト ポリシーの作成（Create BGP Address Family Context Policy）]** を選択します。

ステップ 5 **[Create BGP Address Family Context Policy]** ダイアログ ボックスで、次のタスクを実行します。

次のフィールドの許容値については、Cisco APICドキュメンテーションページの *Cisco APIC* 検証済みスケーラビリティ ガイドを参照してください。

a) [Name] フィールドにポリシーの名前を入力します。
b) **[eBGP 距離（eBGP Distance）]** フィールドに、eBGP ルートの [管理距離（Administrative Distance）] の値を入力します。
c) **[iBGP 距離（iBGP Distance）]** フィールドに、iBGP ルートの [管理距離（Administrative Distance）] の値を入力します。
d) [ローカル距離（Local Distance）] フィールドに、ローカル距離の値を入力します。
e) [eBGP 最大 ECMP（eBGP Max ECMP）] フィールドに、eBGP ロード シェアリングの等コスト パスの最大数の値を入力します。
f) [iBGP 最大 ECMP（iBGP Max ECMP）] フィールドに、iBGP ロード シェアリングの等コスト パスの最大数の値を入力します。
g) DCIG への EVPN タイプ 2（MAC/IP）ホスト ルートの配布を有効にする場合には、**[ホスト ルート リークの有効化（Enable Host Route Leak）]** チェックボックスをオンにします。
h) エントリを更新した後、**[Submit]** をクリックします。

ステップ 6 **[テナント（Tenants）]** > ***[tenant_name]*** > **[ネットワーキング（Networking）]** > **[VRFs]** > ***[vrf_name]*** の順にクリックします。

ステップ 7 対象の VRF の設定の詳細を確認します。

ステップ 8 [アドレス ファミリごとの BGP コンテキスト（BGP Context Per Address Family）] フィールドを見つけ、[BGP アドレス ファミリ タイプ（BGP Address Family Type）] 領域で、IPv4 unicast address family または IPv6 unicast address family を選択します。

ステップ 9 **[BGP Address Family Context]** ドロップダウン リストで作成した [BGP Address Family Context] にアクセスし、それをサブジェクト VRF に関連付けます。

ステップ 10 [送信（Submit）] をクリックします。

AS パス プリペンドの設定

次の項の手順を使用して、AS パスのプリペンドを設定します。

AS パス プリペンドの設定

BGP ピアは、AS パス アトリビュートの長さを増やすことで、リモート ピアでベスト パス選択の影響を与えることができます。番号として指定桁の前に付加してASパス アトリビュートの長さを向上するために使用するメカニズムを提供する AS パス Prepend。

ASパス前に付加は、ルートマップを使用してアウトバウンド方向にのみ適用できます。パスとして前に付加が機能しない iBGP セッションで。

AS パス Prepend 機能は、次のように変更を有効に。

プリペンド	ルート マップと一致するルートの AS パスに、指定した AS 番号を付加します。 （注） • 1 個以上の AS 番号を設定できます。 • 4 バイト番号がサポートされています。 • 合計を prepend は 32 の AS 番号。AS 番号は、AS パス アトリビュートに挿入されます順序を指定する必要があります。
Prepend-最後-として	最後の前に付加 AS パス 1 から 10 までの範囲に番号として。

次の表では、AS パス Prepend の実装の選択基準について説明します。

プリペンド	1	指定された AS 番号を追加します。
Prepend-最後-として	2	最後のAS番号をASパスに付加します。
デフォルト	Prepend(1)	指定された AS 番号を追加します。

設定の AS パス Prepend GUI を使用して

始める前に

構成済みのテナント

手順

ステップ 1 APIC GUI にログインしメニュー バーで、**[テナント（Tenants）]** > **[*tenant_name*]** > **[ポリシー（Policies）** > **[プロトコル（Protocol）]** > **[設定ルール（Set Rules）]**の順にクリックし、**[ルート マップの設定ルールの作成（Create Set Rules for a Route Map）]** を右クリックします。

[**ルート マップの設定ルールの作成（Create Set Rules For A Route Map**）] ウィンドウが表示されます。

ステップ 2 **設定ルールの A ルート マップの作成** ダイアログボックス、次のタスクを実行します。

a) [Name] フィールドに、名前を入力します

b) [AS パスの設定（Set AS Path）] チェックボックスをオンにし、[次へ（Next）] をクリックします。

c) [**AS パス（AS Path**）] ウィンドウで [+] をクリックして [**AS パスの設定を作成（Create Set AS Path**）] ダイアログ ボックスを開きます。

ステップ 3 基準に [**AS 番号の付加（Prepend AS**）] を選択し、**[+]** をクリックして AS 番号を先頭に付加します。

ステップ 4 AS 番号とその順序を入力し、クリックして **更新** 。[+] をクリックして複数の AS 番号の先頭を追加する必要があるかどうかを繰り返します。

ステップ 5 AS 番号の先頭を追加する設定が完了したら、基準 [**AS 番号の末尾を追加（Prepend Last-AS**）] を選択し、指定された回数の数を AS 番号の末尾に付加します。

ステップ 6 **[カウント]**(1-10) を入力します。

ステップ 7 **[OK]** をクリックします。

ステップ 8 [ルート マップの設定ルールを作成（Create Set Rules For A Rout Map）] ウィンドウで AS パスに基づく設定ルールの基準を確認し、[完了（Finish）] をクリックします。

ステップ 9 APIC GUI メニューバーで、[テナント（Tenants）] [tenant_name] [ポリシー（Policies）] [プロトコル（Protocol）] [設定ルール（Set Rules）] の順にクリックし、プロファイルを右クリックします。 > > > >

ステップ 10 確認、 **AS パスの設定** 画面の下部の値します。

AS オーバーライドの BGP 外部ルーテッド ネットワーク

AS オーバーライドを使用して BGB 外部ルーテッド ネットワークを設定するには、次の項の手順を使用します。

BGP 自律システムのオーバーライドについて

BGP のループ防止は、自律システム パスの自律システム番号を確認することで行われます。受信側のルータが受信した BGP パケットの自律システム パスで独自の自律システム番号が表示される場合、パケットは廃棄されます。受信側のルータでは、パケットが独自の自律システムから発信され、最初に発信元から同じ場所に達したことが想定されます。この設定では、ルーティング ループが発生しないようにするためのデフォルトです。

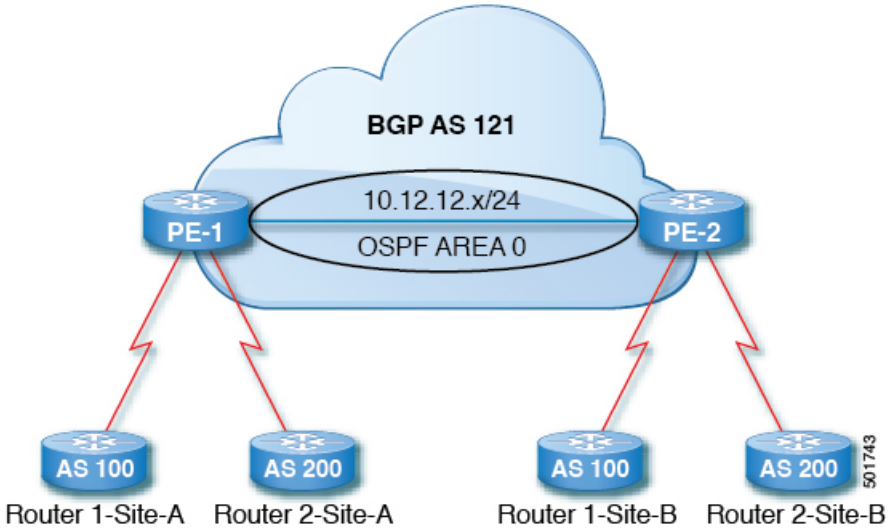
別の自立システム番号によりリンクする同一の自律システム番号を持つさまざまなサイトや禁止ユーザーのサイトを使用する場合、デフォルトルートのループが発生しないようにする設定によって問題が発生する可能性があります。このようなシナリオでは、その他のサイトが受信した場合 1 つのサイトからのルーティング更新は廃棄されます。

このような状況の発生を防ぐため、Cisco APIC リリース 3.1(2m) 以降、BGP 自律システムのオーバーライド機能を有効にして、デフォルトの設定をオーバーライドすることができます。同時に、ピア AS チェックの無効化も有効にする必要があります。

自律システム オーバライド機能では、発信元のルータからの自律システム番号を、アウトバウンド ルートの AS パスの BGP ルータ送信の自律システム番号に置き換えます。アドレス ファミリごとにこの機能を有効にできます（IPv4 または IPv6）。

自律システム オーバライド機能は、GOLF レイヤ 3 設定および非 GOLF レイヤ 3 の設定でサポートされています。

図 *2:* 自律システム オーバライド機能を説明するトポロジ例



ルータ 1 およびルータ 2 は、複数のサイトを持つ 2 つの顧客です（サイト A とサイト B）。顧客ルータ 1 は AS 100 で動作し、顧客ルータ 2 は AS 200 で動作します。

上の図は、次のような自律システム（AS）オーバーライド プロセスを示しています。

1. ルータ A サイト 1 では、AS100 でルート 10.3.3.3 をアドバタイズします。
2. ルータ PE-1 は、AS100 として PE2 へ内部ルートとして反映します。
3. ルータ PE-2 は AS121 で 10.3.3.3 をプリペンドし（AS パスの 100 を 121 に置き換えます）、プレフィックスをプロパゲートします。
4. ルータ 2 サイト B は 10.3.3.3 更新プログラムを承認します。

GUI を使用して、BGP 外部ルーテッド ネットワークと有効になっている自律システム オーバーライドを設定する

始める前に

- テナント、VRF、およびブリッジ ドメインが作成されています。

- 非 GOLF 設定の外部ルーテッド ネットワーク、論理ノード プロファイル、および BGP ピア接続プロファイルが作成されています。

手順

ステップ 1 メニューバーで、**[テナント（Tenants）]** > **[*Tenant_name*]** > **[ネットワーキング（Networking）]** > **[L3Outs]** > **[*Non-GOLF Layer 3 Out_name*]** > **[論理ノード プロファイル（Logical Node Profiles）]** を選択します。

ステップ 2 **Navigation** ウィンドウで、適切な **BGP Peer Connectivity Profile** を選択します。

ステップ 3 [作業（Work）] ペインで、[BGP ピア接続プロファイル（BGP Peer Connectivity Profile）] の [プロパティ（Properties）] 下の [BGP 制御（BGP Controls）] フィールドで、次の手順を実行します:

a) **AS override** フィールドのチェック ボックスをオンにして、**Autonomous System override** 機能を有効にします。

b) **Disable Peer AS Check** フィールドのチェック ボックスをオンにします。

（注） AS オーバーライド機能を有効にするには、 **AS override** および **Disable Peer AS Check** チェック ボックスをオンにする必要があります。

c) 必要に応じてその他のフィールドを選択します。

ステップ 4 [Submit] をクリックします。

BGP ネイバー シャットダウンおよびソフト リセット

BGB ネイバーのシャットダウンとソフト リセットを設定するには、次の項の手順を使用します。

BGP ネイバー シャットダウンとソフト リセットについて

リリース 4.2(1) 以降、次の機能がサポートされるようになりました。

- BGP ネイバー シャットダウン （21 ページ）
- BGP ネイバー ソフト リセット （22 ページ）

BGP ネイバー シャットダウン

BGP ネイバー シャットダウン機能は、NX-OS の neighbor shutdown コマンドに似ており、対応する BGP ネイバーをシャットダウンします。このポリシーを使用して、BGP ネイバーの管理状態を無効または有効にします。この機能を使用すると、BGP ピア設定を削除せずに BGP セッションがシャットダウンされます。

BGP ネイバー ソフト リセット

BGP ネイバー ソフト リセット機能は、BGP ルート リフレッシュ機能を使用して、保存されているルーティング テーブル アップデート情報に依存しない着信および発信 BGP ルーティング テーブル アップデートのダイナミック ソフト リセットを自動的にサポートします。ソフト ダイナミック インバウンド リセットとソフト アウトバウンド リセットを有効にするには、このポリシーを使用します。

GUI を使用した BGP ネイバー シャットダウンの設定

次の手順では、GUI を使用して BGP ネイバー シャットダウン機能を使用する方法について説明します。

始める前に

L3Out を設定する前に、次のような標準的な前提条件を満たします。

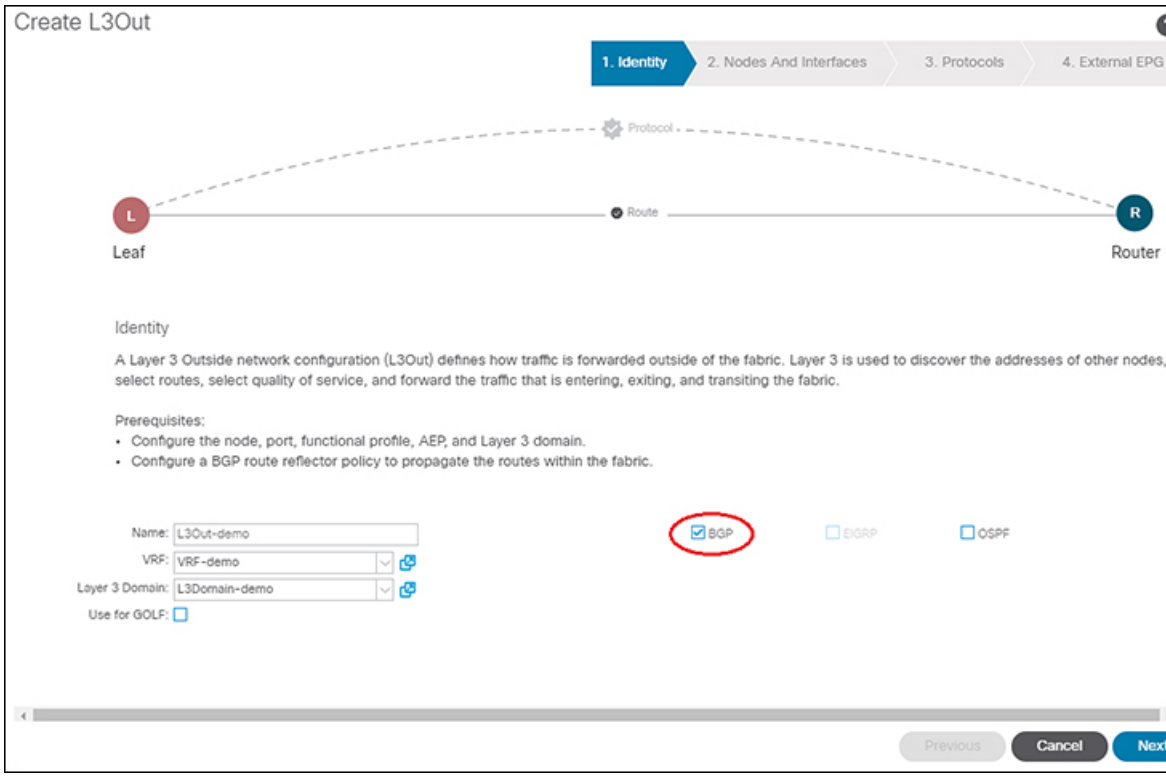
- ノード、ポート、AEP、機能プロファイル、レイヤ 3 ドメインを設定します。
- ファブリック内でルートを伝播させるための、BGP ルート リフレクタ ポリシーを設定します。

手順

ステップ 1 L3Out を作成し、L3Out の BGP を設定します。

a) [**ナビゲーション**（**Navigation**）] ペインで [**テナント**（**Tenant**）] および [**ネットワーキング**（**Networking**）] を展開します。
b) [L3Outs] を右クリックし、[L3Out の作成（Create L3Out）] を選択します。
c) L3Out の BGP を設定するために必要な情報を入力します。

この L3Out の BGP プロトコルを設定するには、L3Out 作成ウィザードの [識別（Identity）] ページで [BGP] を選択します。



d) 残りのページを続けて行い（[**ノードとインターフェイス（Nodes and Interfaces）**]、[**プロトコル（Protocols）**]、および [**外部 EPG（External EPG）**]）、L3Out の設定を完了します。

ステップ 2 L3Out の設定が完了したら、BGP ネイバーのシャットダウンを設定します。

a) BGP ピア接続プロファイル画面に移動します。

[テナント（Tenants）] > [テナント（*tenant*）] > [ネットワーキング（Networking）] > [L3Outs] > [*L3out-name*] > [論理ノード プロファイル（Logical Node Profiles）] > [*logical-node-profile-name*] > [論理インターフェイス プロファイル（Logical Interface Profiles）] > [*logical-interface-profile-name*] > [BGP ピア接続プロファイル（BGP Peer Connectivity Profile） *] [IP-address*]

b) [管理状態（Admin State）] フィールドまでスクロールし、このフィールドで適切な選択を行います。

- 無効化：BGP ネイバーの管理状態を無効にします。
- 有効化：BGP ネイバーの管理状態を有効にします。

GUI を使用した BGP ネイバー ソフト リセットの設定

次の手順では、GUI を使用して BGP ネイバー ソフト リセット機能を使用する方法について説明します。

始める前に

L3Out を設定する前に、次のような標準的な前提条件を満たします。

- ノード、ポート、AEP、機能プロファイル、レイヤ 3 ドメインを設定します。
- ファブリック内でルートを伝播させるための、BGP ルート リフレクタ ポリシーを設定します。

手順

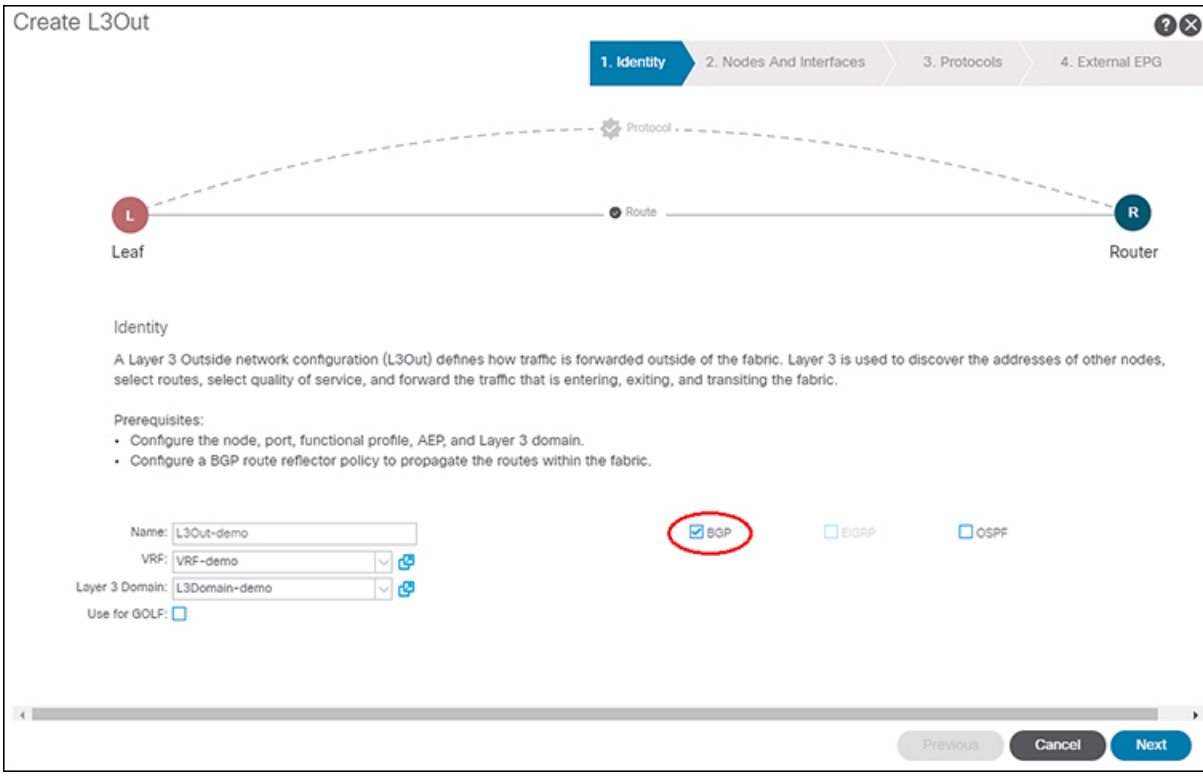
ステップ 1 L3Out を作成し、L3Out の BGP を設定します。

a) [**ナビゲーション（Navigation）**] ペインで [**テナント（Tenant）**] および [**ネットワーキング（Networking）**] を展開します。

b) [L3Outs] を右クリックし、[L3Out の作成（Create L3Out）] を選択します。

c) L3Out の BGP を設定するために必要な情報を入力します。

この L3Out の BGP プロトコルを設定するには、L3Out 作成ウィザードの [識別（Identity）] ページで [BGP] を選択します。



d) 残りのページを続けて行い（[**ノードとインターフェイス（Nodes and Interfaces）**]、[**プロトコル（Protocols）**]、および [**外部 EPG（External EPG）**]）、L3Out の設定を完了します。

ステップ 2 L3Out の設定が完了したら、BGP ネイバーのソフト リセットを設定します。

a) [BGP ピア エントリ（BGP Peer Entry）] 画面に移動します。

[テナント（Tenants）] > [テナント（*tenant*）] > [ネットワーキング（Networking）] > [L3Outs] > [*L3out-name*] > [論理ノード プロファイル（Logical Node Profiles）] > [*logical-node-profile-name*] > [設定済みノード（Configured Nodes）] > [ノード（*node*）] > [BGP for VRF-*vrf-name*] > [ネイバー（Neighbors）]

b) 適切なネイバー エントリを右クリックし、[BGP ピアのクリア（Clear BGP Peer）] を選択します。

[BGP をクリア（Clear BGP）] ページが表示されます。

c) [モード（Mode）] フィールドで、[ソフト（Soft）] を選択します。

[方向（Direction）] フィールドが表示されます。

d) [方向（Direction）] フィールドで適切な値を選択します。

- Incoming：ソフト ダイナミック インバウンド リセットを有効にします。
- Outgoing：ソフト アウトバウンド リセットを有効にします。

VRF ごと、ノード BGP ごとのタイマーの値の設定

ノードごとの BGP タイマー値を設定するには、次の項の手順を使用します。

ノード BGP タイマー値ごとの各 VRF

この機能を紹介する前に、特定の VRF について、すべてのノードには同じ BGP タイマーの値が使用されます。

ノード BGP タイマー値ごとの各 VRF 機能の導入により、BGP タイマーを定義し、各ノードベースの VRF ごとに関連付けることが可能です。ノードでは複数の VRF を所持することが可能で、それぞれ、`fvCtx` に対応しています。ノード設定（`l3extLNodeP`）には、BGP プロトコル プロファイル（`bgpProtP`）の設定が含まれており、希望の BGP コンテキスト ポリシーを参照します（`bgpCtxPol`）。これにより、同じ VRF 内のさまざまなノードが異なる BGP タイマーの値を含めることが可能になります。

各 VRF ではノードに `bgpDom` の具体的な MO を含みます。その名前（プライマリ キー）は、VRF `<fvTenant>:<fvCtx>` です。属性として BGP タイマーの値が含まれています（例：`holdIntvl`、`kaIntvl`、`maxAsLimit`）。

有効なレイヤ 3 アウト設定を作成するために必要なすべての手順は、ノード BPG タイマーごとの各 VRF に正常に適用する必要があります。たとえば、次のような MO は必須です：`fvTenant`、`fvCtx`、`l3extOut`、`l3extInstP`、`LNodeP`、`bgpRR`。

ノードでは、BGP タイマー ポリシーは次のアルゴリズムに基づいて選択されます。

- `BgpProtP` が指定されると、`bgpProtP` の下で参照される `bgpCtxPol` を使用します。
- それ以外の場合、指定されると対応する `fvCtx` の下で参照される `bgpCtxPol` を使用します。

- それ以外の場合、指定されるとテナントでデフォルト ポリシーを使用します。例：`uni/tn-<tenant>/bgpCtxP-default`。
- それ以外の場合、テナント `common` の下の `default` ポリシーを使用します。例：`uni/tn-common/bgpCtxP-default`。これはプログラム済みです。

設定の高度な GUI を使用して BGP タイマーのノードごとの VRF あたり

BGP タイマーが特定のノードに設定されているときに、ノードで BGP タイマー ポリシーを使用し、VRF に関連付けられている BGP ポリシー タイマーはすべて無視されます。

始める前に

テナントと VRF はすでに設定されています。

手順

ステップ 1 メニュー バーで、**[テナント（Tenant）** > **[*Tenant_name*]** > **[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[BGP]** > **[BGP タイマー（BGP Timers）]** を選択し、[**BGP タイマー ポリシーの作成（Create BGP Timers Policy**）] を右クリックします。

ステップ 2 [**BGP タイマー ポリシーの作成（Create BGP Timers Policy**）] ダイアログ ボックスで、次の操作を実行します:

a) **Name** フィールドに、BGP タイマー ポリシーの名前を入力します。
b) 使用可能なフィールドには、必要に応じて、適切な値を選択します。[Submit] をクリックします。`

BGP タイマー ポリシーが作成されます。

ステップ 3 **[テナント（Tenant）]** > **[*Tenant_name*]** > **[ネットワーキング（Networking）]** > **[L3Outs]**に移動し、[**L3Out の作成（Create L3Out**）] を右クリックします。

Create L3Out ウィザードが表示されます。次の操作を実行して、BGP を有効にした L3Out を作成します。

ステップ 4 [L3Out の作成（Create L3Out）] ウィザードの [識別（Identity）] ウィンドウに必要な情報を入力します。

a) **Name** フィールドに L3Out の名前を入力します。
b) **VRF** ドロップダウンリストから VRF を選択します。
c) [**L3 ドメイン（L3 Domain**）]ドロップダウン リストから、適切なドメインを選択します。
d) ルーティング プロトコルのチェック ボックスがある領域で、[**BGP**] を選択します。
e) **Next** をクリックして **Nodes and Interfaces** ウィンドウに移動します。
f) [**L3Out の作成（Create L3Out**）] ウィザードの残りのウィンドウに進み、L3Out の作成プロセスを完了します。

ステップ 5 L3Out を作成したら、作成した L3Out の論理ノード プロファイル（[テナント（Tenant）] [Tenant_name] [ネットワーキング（Networking）] [L3Outs] [L3Out_name] [論理ノード プロファイル（Logical Node Profiles）] [LogicalNodeProfile-name]）に移動します。> > > > > >

ステップ 6 [論理ノード プロファイル（Logical Node Profile）] ウィンドウで、[BGP プロトコル プロファイルの作成（Create BGP Protocol Profile）] の横にあるチェックボックスをオンにします。

[ノード指定 BGP プロトコル プロファイルの作成（Create Node Specific BGP Protocol Profile）] ウィンドウが表示されます。

ステップ 7 **BGP タイマー**] フィールドに、ドロップダウンリストから、この特定のノードに関連付ける BGP タイマー ポリシー選択します。**[送信（Submit）]** をクリックします。`

特定の BGP タイマー ポリシーは、ノードに適用されます。

（注） BGP タイマー ポリシーと、既存のノードのプロファイルを関連付ける、ノードのプロファイルを右クリックし、タイマー ポリシーを関連付けます。

タイマー ポリシーが具体的に選択していない場合、 **BGP タイマー** されたノードのプロファイルが存在する自動的に VRF に関連付けられている BGP タイマー ポリシーは、このノードに適用を取得し、ノードのフィールドします。

ステップ 8 設定を確認するには、**Navigation** ウィンドウで、次の手順を実行します:

a) **[テナント（Tenants）]** > **[*Tenant_name*]** > **[ネットワーキング（Networking）]** > **[L3Outs]** > **[*L3Out_name*]** > **[論理ノード プロファイル（Logical Node Profiles）]** > **[*LogicalNodeProfile-name*]** > **[プロトコル プロファイル（Protocol Profiles）]**の順に移動します。

b) **作業**] ペインで、ノードのプロファイルに関連付けられている BGP プロトコル プロファイルが表示されます。

不整合や障害のトラブルシューティング

特定の状況下では、次のような不整合や障害が発生する可能性があります:

異なるレイヤ 3 Out (`l3Out`) が同じ VRF (`fvCtx`) に関連付けられているか、同じノードで `bgpProtP` が異なるポリシー (`bgpCtxPol`) に関連付けられていると、障害が発生します。次の例では、同じ Layer 3 Out (`out1` と `out2`) が同じ VRF (`ctx1`) に関連付けられています。`out1` の下では、`node1` は BGP タイマー プロトコル `pol1` に関連付けられており、`out2` の下では、`node1` は別の BGP タイマー プロトコル `pol2` に関連付けられています。。この場合、障害が発生します。

```
tn1
  ctx1
  out1
    ctx1
    node1
      protp pol1

  out2
    ctx1
    node1
      protp pol2
```

このような障害が発生した場合は、設定を変更して、BGP タイマー ポリシー間の競合を削除してください。

BFD サポートの設定

BFD サポートを設定するには、次の項の手順を使用します。

双方向フォワーディング検出

双方向フォワーディング検出（BFD）を使用して、ピアリングルータの接続をサポートするように設定された ACI ファブリック境界リーフ スイッチ間の転送パスのサブセカンド障害検出時間を提供します。

BFD は、次のような場合に特に役立ちます。

- ルータ同士の間に直接的な接続がない場合に、レイヤ 2 デバイスまたはレイヤ 2 クラウド経由でピアリング ルータが接続されているとき。転送パスに障害があっても、ピア ルータにはそれがわからない可能性があります。プロトコルの制御に利用できるメカニズムは hello タイムアウトだけですが、タイムアウトまでには数十秒、さらには数分の時間がかかる場合があります。BFD では、障害を 1 秒未満で検出することが可能です。
- 信頼できる障害検出に非対応の物理メディア（共有イーサネットなど）経由でピアリング ルータが接続されているとき。この場合も、ルーティング プロトコルは、時間のかかる hello タイマーに頼るしかありません。
- 1 組のルータの間で多くのプロトコルが実行されているとき、各プロトコルは、独自のタイムアウトでリンク障害を検出する独自の hello メカニズムを持っています。BFD は、すべてのプロトコルに均一のタイムアウトを指定し、それによってコンバージェンス時間の一貫性を保ち、予測可能にします。

次に示す BFD の設定のガイドラインおよび制限事項に従ってください。

- APIC リリース 3.1 (1) 以降、リーフおよびスパイン スイッチ間の BFD は IS-IS のファブリック インターフェイスでサポートされています。さらに、スパイン スイッチの BFD 機能は、OSPF ルートとスタティック ルートでサポートされます。
- Cisco APIC リリース 5.2(4) 以降、BFD 機能は、ルーテッド インターフェイスで設定されているセカンダリ IPv4/IPv6 サブネットを使用して到達可能なスタティック ルートでサポートされています。サブネットに複数のアドレスが設定されている場合、スタティック BFD セッションは L3Out インターフェイスのセカンダリ サブネットから発信できません。共有サブネット アドレス (vPC シナリオに使用) と浮動 L3Out に使用される浮動 IP アドレスは、サブネットの追加アドレスとして許可され、自動的にスキップされ、静的 BFD セッションの発信元には使用されません。

（注） セッションのソースに使用されているセカンダリ アドレスを変更するには、同じサブネットに新しいアドレスを追加し、後で以前のアドレスを削除します。

- BFD は -EX および -FX ライン カード（または新しいバージョン）のモジュラ スパイン スイッチでサポートされ、また BFD は Nexus 9364C 非モジュラ スパイン スイッチ（または新しいバージョン）でサポートされます。
- VPC ピア間の BFD はサポートされません。
- APIC リリース 5.0(1) 以降、BFD マルチホップはリーフ スイッチでサポートされます。BFD マルチホップ セッションが合計に含まれるようになったため、BFD セッションの最大数は変更されません。
- APIC リリース 5.0(1) 以降、ACI は C ビット対応 BFD をサポートしています。BFD がコントロール プレーンに依存しているかいないかは、受信する BFD パケットの C ビットによって判別されます。
- ループバック アドレス ピアでの iBGP 上の BFD はサポートされません。
- インターフェイス ポリシーで BFD サブインターフェイス最適化を有効化できます。このフラグを 1 つのサブインターフェイスに立てることにより、その物理インターフェイス上のすべてのサブインターフェイスの最適化が有効になります。
- BGP プレフィクス ピアの BFD はサポートされません。

（注） Cisco ACI は IP フラグメンテーションをサポートしていません。したがって、外部ルータへのレイヤ 3 Outside（L3Out）接続、または Inter-Pod Network（IPN）を介した マルチポッド 接続を設定する場合は、インターフェイス MTU がリンクの両端で適切に設定されていることが推奨されます。Cisco ACI、 Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定可能な MTU 値はイーサネット ヘッダー (一致する IP MTU、14-18 イーサネット ヘッダー サイズを除く) を考慮していません。また、IOS XR などの他のプラットフォームには、設定された MTU 値にイーサネット ヘッダーが含まれています。設定された値が 9000 の場合、Cisco ACI、Cisco NX-OS Cisco IOS の最大 IP パケット サイズは 9000 バイトになりますが、IOS-XR のタグなしインターフェイスの最大 IP パケットサイズは 8986 バイトになります。

各プラットフォームの適切な MTU 値については、それぞれの設定ガイドを参照してください。

CLI ベースのコマンドを使用して MTU をテストすることを強く推奨します。たとえば、Cisco NX-OS CLI で `ping 1.1.1.1 df-bit packet-size 9000 source-interface ethernet 1/1` などのコマンドを使用します。

サブインターフェイスの BFD の最適化

サブインターフェイスの BFD は最適化できます。BFD により、設定されているすべてのサブインターフェイスのセッションが作成されます。BFD により、設定されている最小の VLAN ID を持つサブインターフェイスがマスター サブインターフェイスとして設定され、そのサブインターフェイスは親インターフェイスの BFD セッション パラメータを使用します。残りのサブインターフェイスは slow timer を使用します。

最適化サブインターフェイス セッションでエラーが検出されると、BFD により、その物理インターフェイスのすべてのサブインターフェイスがダウンとマークされます。

BFD モニタ対象リンクの一端または両端で BFD エコー機能を設定できます。エコー機能は設定された slow timer に基づいて必要最小受信間隔を遅くします。*[RequiredMinEchoRx]* BFD セッション パラメータは、エコー機能がディセーブルの場合、ゼロに設定されます。slow timer は、エコー機能がイネーブルの場合、必要最小受信間隔になります。

（注） サブインターフェイスの 1 つがフラップすると、その物理インターフェイスのサブインターフェイスが影響を受け、1 秒間ダウンします。

GUI を使用したセカンダリ IP アドレスでの双方向フォワーディング検出の構成

この手順では、GUI を使用して、セカンダリ IP アドレスで双方向フォワーディング検出（BFD）を構成します。

手順

ステップ 1 メニュー バーで、[テナント（Tenants）] > [すべてのテナント（ALL Tenants）] の順に選択します。 >

ステップ 2 作業ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーション ペインから、***[tenant_name]*** > **[ネットワーキング（Networking）]** > **[L3Outs]** > ***[l3Out_name]*** > **[論理ノード プロファイル（Logical Node Profiles）]** > ***[node_profile_name]*** > **[論理インターフェイス プロファイル（Logical Interface Profiles）]** > ***[interface_profile_name***] の順に移動します。

ステップ 4 [Work] ペインで、必要に応じて **[Policy（ポリシー）]** > **[ルーテッド サブインターフェイス（Routed Sub-interfaces）]**、**[Policy（ポリシー）]** > **Routed Interfaces**または **[Policy（ポリシー）]** > **[SVI]**を選択します。

ステップ 5 インターフェイスをダブルクリックして、そのプロパティを編集します。

ステップ 6 インターフェイスのタイプに応じて、次のサブステップのいずれかを実行します。

a) インターフェイスがルーテッド サブインターフェイスまたはルーテッド インターフェイス、または**[パス タイプ（Path Type）]**が**[ポート（Port）]**または**[ダイレクト ポート チャネル（Direct Port Channel）]**に設定されたスイッチ仮想インターフェイス (SVI) である場合は、**[IPv4 セカンダリ/IPv6 追加アドレス（IPv4 secondary/IPv6 Additional Addresses）]** テーブルで、**+** をクリックし、IP を入力します。アドレスとサブネットを選択し、**[送信（Submit）]** をクリックします。

b) インターフェイスがスイッチ仮想インターフェイス (SVI) で、パス タイプが仮想ポート チャネルに設定されている場合は、サイド B の IPv4 セカンダリ/IPv6 追加アドレス テーブルで、+ をクリックし、IP アドレスとサブネットを入力して、[OK] をクリックします。

ステップ 7 [ナビゲーション] ペインで、***[tenant_name]*** > **[ネットワーキング（Networking）]** > **[L3Outs]** > ***[l3out_name]*** > **[論理ノード プロファイル（Logical Node Profiles）]** > ***[node_profile_name]*** > **[構成済みノード（Configured Nodes）]** > ***[node_name]***を選択します。

ステップ 8 **[静的ルート（Static Routes）]** テーブルで、**[+]** をクリックして、次のサブステップを実行します。

a) **[プレフィックス（Prefix）]** フィールドに、外部ネットワークに割り当てられている静的ルートの IP アドレスとマスクを入力します。

b) **[BFD]** チェックボックスをオンにします。

c) **[次のホップ アドレス（Next Hop Addresses）]** テーブルで、**[+]** をクリックし、**[次のホップ アドレス（Next Hop Addresses）]** フィールドに、インターフェイスに指定したセカンダリ IP アドレスから到達可能な IP アドレスを入力します。

d) 必要に応じて、残りのフィールドに入力します。

e) [OK] をクリックします。

ステップ 9 必要に応じて、残りのフィールドに入力します。

ステップ 10 [Submit] をクリックします。

GUI を使用してリーフ スイッチの BFD をグローバルに設定する

手順

ステップ 1 メニュー バーで、**[Fabric]** > **[Access Policies]** の順に選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシー（Policies）]** > **[スイッチ（Switch）]** > **[BFD]**の順に展開します。
設定を双方向フォワーディング検出 (BFD) には、使用可能な 2 つの種類があります:

- BFD IPV4
- BFD IPV6

これらのBFD設定ごとに、デフォルトポリシーを使用するか、特定のスイッチ(またはスイッチのセット) 用に新しいポリシーを作成できます。

（注） デフォルトでは、APIC コントローラはシステムの起動時にデフォルトのポリシーを作成します。これらのデフォルトポリシーはグローバルなもので、双方向転送検出 (BFD) の設定ポリシーです。デフォルト グローバルポリシー内の属性は、**作業**ウィンドウで設定できます。または、これらデフォルトのポリシーの値を変更することもできます。ただし、いったんデフォルトのグローバルポリシーを変更すると、システム全体(すべてのスイッチ)に影響することに注意してください。デフォルトではありませんが、特定のスイッチ(またはスイッチの設定)の特定の設定を使用する場合は、次の手順の説明に従って、スイッチのプロファイルを作成します。

ステップ 3 特定のグローバル BFD ポリシー（デフォルトではないもの）向けにスパイン スイッチ プロファイルを作成するには、[**ナビゲーション**（**Navigation**）] ペインで、**[スイッチ（Switches）]** > **[リーフ スイッチ（Leaf Switches）]** > **[プロファイル（Profiles）]**の順に展開します。
リーフ スイッチ - プロファイル（Leaf Switches - Profiles） 画面が [**作業**（**Work**）] ペインに表示されます。

ステップ 4 [**作業**（**Work**）] ペインの右側、アクション アイコンの下で、**リーフ プロファイルの作成（Create Leaf Profile）** を選択します。
[Create Leaf Profile] ダイアログボックスが表示されます。

ステップ 5 **Create Leaf Profile** ダイアログボックスで、次の操作を実行します:

a) **Name** フィールドに、リーフ スイッチ プロファイルの名前を入力します
b) （任意）[**説明**（**Description**）] フィールドに、プロファイルの説明を入力します。
c) （任意）[**リーフ セレクタ**（**Leaf Selectors**）] ツールバーで、[+] をクリックします。
d) [**名前**（**Name**）]（スイッチに名前を付けます）、[**ブロック**（**Blocks**）]（スイッチを選択します）、および [**ポリシー グループ**（**Policy Group**）]（[**アクセス スイッチ ポリシー グループの作成**（**Create Access Switch Policy Group**）]）に適切な値を入力します。
Create Access Switch Policy Group ダイアログボックスが表示されます。ここでは、ポリシー グループの識別プロパティを指定できます。

ステップ 6 (リーフセレクタを設定する場合）[**アクセス スイッチ ポリシー グループの作成**（**Create Access Switch Policy Group**）] ダイアログ ボックスで次のアクションを実行します。

a) [Name] フィールドにポリシー グループの名前を入力します。
b) （任意）[**説明**（**Description**）] フィールドで、ポリシー グループの説明を入力します。
c) BFD ポリシー タイプ (**BFD IPV4 Policy** または **BFD IPV6 Policy**) を選択し、値 (**default** または **Create BFD Global Ipv4 Policy**) を特定のスイッチまたはスイッチのセットに対して選択します。
d) [更新（Update）] をクリックします。

ステップ 7 [**次へ**（**Next**）] をクリックして [**関連付け**（**Associations**）] へ進みます。

（任意）[関連付け（Associations）] メニューで、リーフ プロファイルをリーフ インターフェイス プロファイルおよびアクセス モジュール プロファイルに関連付けることができます。

ステップ 8 [完了（Finish）] をクリックします。

BFD グローバルポリシーを作成するもう 1 つの方法は、**BFD IPV4** または **BFD IPV6** のいずれかを右クリックします (**Navigation** ウィンドウにあります)。

ステップ 9 作成した BFD グローバル コンフィギュレーションを確認するには、[**ナビゲーション**（**Navigation**）] ペインで、**[ポリシー（Policies）]** > **[スイッチ（Switch）]** > **[BFD]** の順に展開します。

GUI を使用してスパイン スイッチで BFD のグローバル設定

手順

ステップ 1 メニュー バーで、**[Fabric]** > **[Access Policies]** の順に選択します。

ステップ 2 [**ナビゲーション**（**Navigation**）] ペインで、**[ポリシー**（**Policies**）**]** > **[スイッチ**（**Switch**）**]** > **[BFD]** の順に展開します。
設定を双方向フォワーディング検出 (BFD) には、使用可能な 2 つの種類があります:

- BFD IPV4
- BFD IPV6

これらのBFD設定ごとに、デフォルトポリシーを使用するか、特定のスイッチ(またはスイッチのセット) 用に新しいポリシーを作成できます。

（注） デフォルトでは、APIC コントローラはシステムの起動時にデフォルトのポリシーを作成します。これらのデフォルトポリシーはグローバルなもので、双方向転送検出 (BFD) の設定ポリシーです。デフォルト グローバルポリシー内の属性は、**作業** ウィンドウで設定できます。または、これらデフォルトのポリシーの値を変更することもできます。ただし、いったんデフォルトのグローバルポリシーを変更すると、システム全体(すべてのスイッチ) に影響することに注意してください。デフォルトではありませんが、特定のスイッチ(またはスイッチの設定) の特定の設定を使用する場合は、次の手順の説明に従って、スイッチのプロファイルを作成します。

ステップ 3 特定のグローバル BFD ポリシー（デフォルトではないもの）向けにスパイン スイッチ プロファイルを作成するには、[**ナビゲーション**（**Navigation**）]ペインで、**[スイッチ**（**Switches**）**]**> **[スパイン スイッチ**（**Spine Switches**）**]** > **[プロファイル**（**Profiles**）**]**の順に展開します。
スパイン スイッチ：**プロファイル** 画面が [**作業**（**Work**）] ペインに表示されます。

ステップ 4 [**作業**（**Work**）] ペインの右側、アクション アイコンの下で、[**スパイン プロファイルの作成**（**Create Spine Profile**）] を選択します。
Create Spine Profile ダイアログボックスが表示されます。

ステップ 5 **Create Spine Profile** ダイアログボックスで、次の操作を実行します:

a) **Name** フィールドに、スイッチ プロファイルの名前を入力します。
b) **Description** フィールドの隣にに、プロファイルの説明を入力します。（この手順は任意です）。
c) （任意）[スパイン セレクタ（Spine Selectors）] ツールバーで、[+] をクリックします。
d) [**名前**（**Name**）]（スイッチに名前を付けます）、[**ブロック**（**Blocks**）]（スイッチを選択します）、および [**ポリシー グループ**（**Policy Group**）]（[**スパイン スイッチ ポリシー グループの作成**（**Create Spine Switch Policy Group**）]）に適切な値を入力します。
スパイン スイッチ ポリシー グループの作成 ダイアログボックスはポリシー グループ id のプロパティを指定できますが表示されます。

ステップ 6 (スパイン セレクタを設定する場合）[**スパイン スイッチ ポリシー グループの作成**（**Create Spine Switch Policy Group**）] ダイアログ ボックスで次のアクションを実行します。

a) [Name] フィールドにポリシー グループの名前を入力します。
b) （任意）[**説明（Description**）] フィールドで、ポリシー グループの説明を入力します。
c) BFD ポリシー タイプ (**BFD IPV4 Policy** または **BFD IPV6 Policy**) を選択し、値 (**default** または **Create BFD Global Ipv4 Policy**) を特定のスイッチまたはスイッチのセットに対して選択します。
d) [更新（Update）] をクリックします。

ステップ 7 [**次へ（Next**）] をクリックして [**関連付け（Associations**）] へ進みます。

（任意）[関連付け（Associations）] メニューで、スパイン プロファイルをスパイン インターフェイス プロファイルに関連付けることができます。

ステップ 8 [完了（Finish）] をクリックします。

BFD グローバルポリシーを作成するもう 1 つの方法は、**BFD IPV4** または **BFD IPV6** のいずれかを右クリックします (**Navigation** ウィンドウにあります)。

ステップ 9 作成した BFD グローバル コンフィギュレーションを確認するには、[**ナビゲーション（Navigation**）] ペインで、**[ポリシー（Policies**）] > **[スイッチ（Switch**）] > **[BFD]** の順に展開します。

GUI を使用した BFD インターフェイスのオーバーライドの設定

明示的な双方向フォワーディング検出 (BFD) を設定できる、3 つのサポート対象のインターフェイス（ルーテッド レイヤ インターフェイス、外部インターフェイス SVI とルーテッド サブインターフェイス）があります。グローバル コンフィギュレーションを使用しないで、さらに特定のインターフェイスの明示的な設定をしたい場合、特定のスイッチまたは一連のすべてのインターフェイスに適用される独自のグローバル コンフィギュレーションを作成できます。特定のインターフェイス上の特定のスイッチの粒度がさらに必要な場合、このインターフェイス オーバーライド設定を使用する必要があります。

（注） BFD インターフェイス ポリシーが親ルーテッド インターフェイスに設定されている場合、デフォルトでは、親インターフェイスと同じアドレス ファミリを持つすべてのルーテッド サブインターフェイスがこのポリシーを継承します。継承された設定のいずれかを上書きする必要がある場合は、サブインターフェイスで明示的な BFD インターフェイス ポリシーを設定します。ただし、親インターフェイスで **Admin State** または **Echo Admin State** が無効になっている場合、サブインターフェイスでプロパティをオーバーライドすることはできません。

始める前に

テナントはすでに作成されています。

手順

ステップ 1 メニュー バーで、 **Tenant** を選択します。

ステップ 2 [**ナビゲーション（Navigation）**] ペイン (クイック スタートの下)、作成したテナント **[*Tenant_name*] > [ネットワー キング（Networking）] > [L3Outs]**を展開します。

ステップ 3 [**L3Outs**] を右クリックし、[**L3Out の作成（Create L3Out）**] を選択します。
[**L3Out の作成（Create L3Out）**] ウィザードが表示されます。

ステップ 4 [L3Out の作成（Create L3Out）] ウィザードの [識別（Identity）] ウィンドウに必要な情報を入力します。

a) [名前（Name）]、[VRF]、および [L3 ドメイン（L3 Domain）] フィールドに必要な情報を入力します。
b) ルーティング プロトコルのチェック ボックスがある領域で、[BGP] を選択します。
c) [**次（Next）**] をクリックして [**ノードとインターフェイス（Nodes and Interfaces）**] ウィンドウに移動します。

ステップ 5 [L3Out の作成（Create L3Out）] ウィザードの [ノードとインターフェイス（Nodes and Interfaces）] ウィンドウに必要な情報を入力します。

a) [レイヤ 3（Layer 3）] 領域で、[ルーテッド（Routed）] を選択します。
b) [**ノード ID（Node ID）**] フィールドのドロップダウン メニューで、L3Out のノードを選択します。

これらの例のトポロジでは、ノード `103` を使用します。

c) [Router ID] フィールドに、ルータ ID を入力します。
d) （任意） 必要に応じて、ループバック アドレスに別の IP アドレスを設定できます。

[ルータ ID（Router ID）] フィールドに入力したエントリと同じ内容が [ループバック アドレス（Loopback Address）] フィールドに自動で入力されます。これは以前のビルドでの [ループバック アドレスのルータ ID の使用（Use Router ID for Loopback Address）] と同等です。ループバック アドレスにルータ ID を使用しない場合は、ループバック アドレスに別の IP アドレスを入力します。または、ループバック アドレスにルータ ID を使用しない場合は、このフィールドを空のままにします。

e) [ノードとインターフェイス（Nodes and Interfaces）] ウィンドウに追加の必要な情報を入力します。

このウィンドウに表示されるフィールドは、[レイヤ 3（Layer 3）] および [レイヤ 2（Layer 2）] 領域で選択したオプションによって異なります。

f) [ノードとインターフェイス（Nodes and Interfaces）] ウィンドウで残りの追加の情報を入力したら、[次（Next）] をクリックします。

[**プロトコル（Protocols**）] ウィンドウが表示されます。

ステップ 6 [L3Out の作成（Create L3Out）] ウィザードの [プロトコル（Protocols）] ウィンドウに必要な情報を入力します。

a) [BGP ループバック ポリシー（BGP Loopback Policies）] および [BGP インターフェイス ポリシー（BGP Interface Policies）] 領域で、次の情報を入力します。

- **ピア アドレス（Peer Address）**：ピア IP アドレスを入力します
- **EBGP Multihop TTL（EBGP マルチホップ TTL）**：接続の存続可能時間（TTL）を入力します。範囲は 1 ー 255 ホップです。ゼロの場合、TTL は指定されません。デフォルトは 0 です。
- **リモート ASN（Remote ASN）**：ネイバー自律システムを固有に識別する番号を入力します。自律システム番号は、1 ー 4294967295 のプレーン形式で 4 バイトにすることができます。

（注） ACI は asdot または asdot + 形式の AS 番号をサポートしていません。

b) [**OSPF**] 領域で、デフォルト OSPF ポリシー、以前に作成した OSPF ポリシー、または [**OSPF インターフェイス ポリシーの作成（Create OSPF Interface Policy**）] を選択します。

c) **[次へ（Next）]** をクリックします。

[**外部 EPG（External EPG**）] ウィンドウが表示されます。

ステップ 7 [L3Out の作成（Create L3Out）] ウィザードで [外部 EPG（External EPG）] ウィンドウに必要な情報を入力します。

a) **Name** フィールドに、外部ネットワークの名前を入力します。

b) [**提供済みコントラクト（Provided Contract**）] フィールドで、提供済みコントラクトの名前を入力します。

c) [**消費済みコントラクト（Consumed Contract**）] フィールドで、消費済みコントラクトの名前を入力します。

d) [すべての外部ネットワークのデフォルト EPG（Default EPG for all external network）] フィールドで、この L3Out 接続からのすべての中継ルートをアドバタイズしない場合はオフにします。

このボックスをオフにすると、[Subnets] 領域が表示されます。次の手順に従って、必要なサブネットとコントロールを指定します。

e) [完了（Finish）] をクリックして、[L3Out の作成（Create L3Out）] ウィザードに必要な設定の入力を完了させます。

ステップ 8 **[テナント（Tenants）]** > **[*tenant_name*]** > **[ネットワーキング（Networking）]** > **[L3Outs]** > **[*L3Out_name*]** > **[論理ノード プロファイル（Logical Node Profiles）]** > **[*logical_node_profile_name*]** > **[論理インターフェイス プロファイル（Logical Interface Profiles）]** > **[*logical_interface_profile_name*]** の順に移動します。

ステップ 9 [論理インターフェイス プロファイル（Logical Interface Profile）] ウィンドウで、[BFD インターフェイス プロファイルの作成（Create BFD Interface Profile）] フィールドまで下にスクロールし、このフィールドの横にあるボックスをオンにします。

ステップ 10 [**BFD インターフェイス プロファイルの作成（Create BFD Interface Profile**）] ウィンドウで、BFD の詳細を入力します。

- **認証タイプ** フィールドで、選択 **No authentication** または **キー SHA1** 。

  認証 (SHA1 のキーを選択) により、入力を選択すると、 **認証キー ID** を入力してください、 **の認証キーを** (パスワード)、再次を入力して、パスワードを確認 **キーの確認** 。

- [**BFD インターフェイス ポリシー（BFD Interface Policy**）] フィールドで、[**一般的な/デフォルト（common/default**）] 設定（デフォルト BFD ポリシー）のいずれかを選択、または、[**BFD インターフェイス ポリシーの作成（Create BFD Interface Policy**）] を選択することによって自分の BFD ポリシーを作成します。

  選択した場合 **BFD インターフェイス ポリシーの作成** 、 **BFD インターフェイス ポリシーの作成** BFD インターフェイス ポリシーの値を定義するダイアログボックスが表示されます。

ステップ 11 [Submit] をクリックします。

ステップ 12 設定したインターフェイス レベルの BFD ポリシーを確認するには、**[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[BFD]** に移動します。

GUI を使用して BFD コンシューマ プロトコルを設定する

この手順では、BFD機能の消費者であるコンシューマプロトコル(OSPF、BGP、EIGRP、スタティック ルート、および IS-IS) での双方向フォワーディング検出 (BFD) を有効にする方法を説明します。これらのプロトコルで BFD を使用するには、それらのフラグを有効にする必要があります。

（注） これらの 4 つのコンシューマ プロトコルは、左側のナビゲーション ペインの **[テナント（Tenant）]** > **[ポリシー（Policies）]** > **[プロトコル（Protocol）]** の下にあります。

始める前に

テナントはすでに作成されています。

手順

ステップ 1 [L3Out の作成（Create L3Out）] ウィザードを使用して L3Out を作成します。

ステップ 2 メニュー バーで、**[テナント（Tenant）]**を選択します。

ステップ 3 BGP プロトコルの BFD を設定するには、[**ナビゲーション（Navigation**）] ペイン（Quick Start の下）で、作成したテナント、**[*Tenant_name*]** > **[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[BGP]** > **[BGP ピア プレフィックス（BGP Peer Prefix）]** を展開します。

ステップ 4 **Work** ウィンドウの右側の **[ACTIONS]** の下で、**[Create BGP Peer Prefix Policy]** を選択します。**[Create BGP Peer Prefix Policy]** ダイアログボックスが表示されます。

（注） 左のナビゲーション ウィンドウで **[BGP Peer Prefix]** を右クリックして **[Create BGP Peer Prefix]** を選択し、ポリシーを作成することもできます。

ステップ 5 **[Name]** フィールドに名前を入力し、残りのフィールドに値を入力して BGP ピア プレフィックス ポリシーを定義します。

ステップ 6 **[送信（Submit）]** をクリックします。`
作成した BGP ピア プレフィックス ポリシーは、左のナビゲーション ウィンドウの **[BGP Peer Prefix]** の下に表示されます。

ステップ 7 **[テナント（Tenants）]** > **[*tenant_name*]** > **[ネットワーキング（Networking）]** > **[L3Outs]** > **[*L3Out_name*]** > **[論理ノード プロファイル（Logical Node Profiles）]** > **[*logical_node_profile_name*]** > **[論理インターフェイス プロファイル（Logical Interface Profiles）]** > **[*logical_interface_profile_name*]** > **[BGP ピア接続プロファイル（BGP Peer Connectivity Profile）]** の順に移動します。

ステップ 8 [BGP ピア接続プロファイル（BGP Peer Connectivity Profile）] ウィンドウで、[BGP ピア プレフィックス ポリシー（BGP Peer Prefix Policy）] フィールドまでスクロールし、作成した BGP ピア プレフィックス ポリシーを選択します。

ステップ 9 [**ピア制御（Peer Controls**）] フィールドで、[**双方向フォワーディング検出（Bidirectional Forwarding Detection**）] を選択して BGP コンシューマ プロトコルの BFD を有効にします（またはオフにして BFD を無効にします）。

ステップ 10 OSPF プロトコルの BFD を設定するには、[**ナビゲーション（Navigation**）] ペインで、**[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[OSPF]** > **[OSPF インターフェイス（OSPF Interface）]** に移動します。

ステップ 11 **Work** ウィンドウの右側の、**[ACTIONS]** の下で、**[Create OSPF Interface Policy]** を選択します。
[Create OSPF Interface Policy] ダイアログボックスが表示されます。

（注） 左のナビゲーション ウィンドウで **[OSPF Interface]** を右クリックして **[Create OSPF Interface Policy]** を選択し、ポリシーを作成することもできます。

ステップ 12 **[Name]** フィールドに名前を入力し、残りのフィールドに値を入力して OSPF インターフェイス ポリシーを定義します。

ステップ 13 このダイアログボックスの **[Interface Controls]** セクションでは、BFD の有効と無効を切り替えることができます。有効にするには、図のように、**[BFD]** の隣のボックスをオンにして OSPF コンシューマ プロトコルにフラグを追加します (またはボックスをオフにして BFD を無効にします)。

ステップ 14 **[送信（Submit）]** をクリックします。`

ステップ 15 EIGRP プロトコルの BFD を設定するには、[**ナビゲーション（Navigation**）] ペインで、**[*tenant_name*]** > **[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[EIGRP]** > **[EIGRP インターフェイス（EIGRP Interface）]** に移動します。

ステップ 16 **Work** ウィンドウの右側の、**[ACTIONS]** の下で、**[Create EIGRP Interface Policy]** を選択します。
[Create EIGRP Interface Policy] ダイアログボックスが表示されます。

（注） 左のナビゲーション ウィンドウで **[EIGRP Interface]** を右クリックして **[Create EIGRP Interface Policy]** を選択し、ポリシーを作成することもできます。

ステップ 17 **[Name]** フィールドに名前を入力し、残りのフィールドに値を入力して OSPF インターフェイス ポリシーを定義します。

ステップ 18 このダイアログボックスの **[Control State]** セクションでは、BFD の有効と無効を切り替えることができます。有効にするには、図のように、**[BFD]** の隣のボックスをオンにして EIGRP コンシューマ プロトコルにフラグを追加します (またはボックスをオフにして BFD を無効にします)。

ステップ 19 **[送信（Submit）]** をクリックします。`

ステップ 20 スタティック ルート プロトコルで BFD を設定するには、**[ナビゲーション（Navigation）]** ペインで **[ネットワーキング（Networking）] > [L3Outs] > [*L3Out_name*] > [設定済みのノード（Configured Nodes）]** に戻り、設定済みのノードをクリックして **[ノード関連付け（Node Association）]** ウィンドウを表示します。

ステップ 21 **[Static Routes]** セクションで、[+] (展開) ボタンをクリックします。
[Create Static Route] ダイアログボックスが表示されます。このセクションで、必要なフィールドの値を入力します。

ステップ 22 **[Route Control]** の隣で、**[BFD]** の隣のボックスをオンにして有効にします (または、無効にする場合にはオフにします)。

ステップ 23 **[送信（Submit）]** をクリックします。`

ステップ 24 IS-IS プロトコルの BFD を設定するには、**[ナビゲーション（Navigation）]** ペインで **[ファブリック（Fabric）] > [ファブリック ポリシー（Fabric Policies）] > [ポリシー（Policies）] > [インターフェイス（Interface）] > [L3 インターフェイス（L3 Interface）]** に移動します。

ステップ 25 **Work** ウィンドウの右側の、**[ACTIONS]** の下で、**[Create L3 Interface Policy]** を選択します。
[Create L3 Interface Policy] ダイアログボックスが表示されます。

（注） 左のナビゲーション ウィンドウで **[L3 Interface]** を右クリックして **[Create EIGRP Interface Policy]** を選択し、ポリシーを作成することもできます。

ステップ 26 **[Name]** フィールドに名前を入力し、残りのフィールドに値を入力して L3 インターフェイス ポリシーを定義します。

ステップ 27 BFD ISIS ポリシーを有効にするには、[BFD ISIS ポリシー設定（BFD ISIS Policy Configuration）] フィールドで **[有効化（enabled）]** をクリックします。

ステップ 28 [Submit] をクリックします。

BFD マルチホップ

BFD マルチホップでは、複数ホップ（最大 255 ホップ）の宛先に対する 1 秒未満の転送障害検出が可能になります。リリース 5.0(1) 以降、APIC は IPv4 の BFD マルチホップおよび IPv6 の BFD マルチホップを、RFC5883 に準拠してサポートします。BFD マルチホップ セッションは、固有のソースと宛先アドレス ペア間で設定されます。BFD マルチホップ セッションは、

シングルホップ BFD セッションの場合、インターフェイスではなく、送信元と宛先の間で作成されます。

BFD マルチホップは TTL フィールドを BGP によってサポートされる最大制限に設定し、受信時に値のチェックを行いません。ACI リーフは、BFD マルチホップ パケットが通過できるホップ数には影響しませんが、ホップ数は 255 に制限されます。

BFD マルチホップの注意事項と制約事項

- BFDマルチホップのデフォルトおよび最小送信/受信インターバル タイマーは 250 ミリ秒です。
- デフォルトの最小検出乗数は 3 です。
- エコー モードは BFD マルチホップではサポートされません。

BFD マルチホップ ポリシーの設定

ポリシーの目的に応じて、GUI の複数の場所で BFD マルチホップ ポリシーを設定できます。

- **グローバル ポリシー**：デフォルトでは、APIC コントローラはシステムの起動時にデフォルトのポリシーを作成します。これらのデフォルト ポリシーは、グローバル BFD マルチホップ設定ポリシーです。デフォルト グローバル ポリシー内の属性は、[作業（Work）] ペインで設定できます。または、これらデフォルトのポリシーの値を変更することもできます。ただし、いったんデフォルトのグローバル ポリシーを変更すると、システム全体(すべてのスイッチ)に影響が及びます。デフォルトではありませんが、特定のスイッチまたはスイッチのセットの特定の設定を使用する場合は、スイッチ プロファイルを作成し、そのスイッチ プロファイル内で BFD マルチホップの値を変更します。

  次の GUI の場所で、IPv4 または IPv6 のグローバル BFD マルチホップ設定ポリシーを作成または変更できます。

  - [ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）] > [ポリシー（Policies）] > [スイッチ（Switch）] > [BFD マルチホップ（BFD Multihop）] > [BFD マルチホップ IPv4（BFD Multihop IPv4)] : [BFD グローバル IPv4 MH ポリシーの作成（Create BFD Global IPv4 MH Policy）] を右クリックして選択します。
  - [ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）] > [ポリシー（Policies）] > [スイッチ（Switch）] > [BFD マルチホップ（BFD Multihop）] > [BFD マルチホップ IPv6（BFD Multihop IPv6)] : [BFD グローバル IPv6 MH ポリシーの作成（Create BFD Global IPv6 MH Policy）] を右クリックして選択します。

- ノード ポリシー：BFD マルチホップ ノード ポリシーは、ノード プロファイルの下のインターフェイスに適用されます。

  この GUI の場所で BFD マルチホップ ノード ポリシーを作成または変更できます。

  - [テナント（Tenants）] > [テナント（tenant）] > [ポリシー（Policies）] > [プロトコル（Protocol）] > [BFD マルチホップ（BFD Multihop）] > [ノード ポリシー（Node

Policies）]：[BFD マルチホップ ノード ポリシーの作成（Create BFD Multihop Node Policy）] を右クリックして選択します。

- インターフェイス ポリシー：BFD マルチホップ インターフェイス ポリシーは、インターフェイス プロファイルの下のインターフェイスに適用されます。

  この GUI の場所で BFD マルチホップ インターフェイス ポリシーを作成または変更できます。

  - [テナント（Tenants）] > [テナント（tenant）] > [ポリシー（Policies）] > [プロトコル（Protocol）] > [BFD マルチホップ（BFD Multihop）] > [インターフェイス ポリシー（Interface Policies）]：[BFD マルチホップ インターフェイス ポリシーの作成（Create BFD Multihop Interface Policy）] を右クリックして選択します。

- グローバル ポリシーの上書き：デフォルトのグローバル設定を使用せず、特定のインターフェイスで明示的な設定を行う場合は、独自のグローバル設定を作成できます。この設定は、特定のスイッチまたはスイッチセットのすべてのインターフェイスに適用されます。特定のインターフェイス上の特定のスイッチの粒度がさらに必要な場合、このインターフェイス オーバーライド設定を使用する必要があります。

  次の GUI ロケーションで、ノード プロファイルまたはインターフェイス プロファイルの BFD マルチホップ オーバーライド ポリシーを作成または変更できます。

  - [テナント（Tenants）] > [テナント（tenant）] > [ネットワーキング（Networking）] > [L3Outs] > [l3out] > [論理ノード プロファイル（Logical Node Profiles）] > [logical_node_profile]：[BFD インターフェイス プロトコル プロファイルの作成（Create BFD Interface Protocol Profile）] を右クリックして選択し、BFD マルチホップ ノード ポリシーを指定します。

  - [テナント（Tenants）] > [テナント（tenant）] > [ネットワーキング（Networking）] > [L3Outs] > [l3out] > [論理ノード プロファイル（Logical Node Profiles）] > [logical_node_profile] > [論理インターフェイス プロファイル（Logical Interface Profiles）] > [logical_interface_profile]：[MH-BFD インターフェイス プロトコル プロファイルの作成（Create MH-BFD Interface Protocol Profile）] を右クリックして選択し、BFD マルチホップ インターフェイス ポリシーを指定します。

  - [テナント（Tenants）] > [インフラ（infra）] > [ネットワーキング（Networking）] > [SR-MPLS Infra L3Outs] > [l3out] > [論理ノード プロファイル（Logical Node Profiles）] > [logical_node_profile] > [論理インターフェイス プロファイル（Logical Interface Profiles）] > [logical_interface_profile]：[MH-BFD インターフェイス プロトコル プロファイルの作成（Create MH-BFD Interface Protocol Profile）] を右クリックして選択し、BFD マルチホップ インターフェイス ポリシーを指定します。

手順

ステップ 1 BFD マルチホップ ポリシーを作成または設定する GUI の場所に移動します。

ステップ 2 既存のプロファイルまたはポリシーを編集するか、ダイアログボックスを起動して新しいプロファイルを作成します。

ステップ 3 プロファイルで、BFD マルチホップ セッションの [認証タイプ（Authentication Type）] を選択します。

認証なしまたは SHA-1 認証を要求するように選択できます。

ステップ 4 新しいポリシーを作成する場合は、ダイアログ ボックスで設定を行います。

a) ポリシーの [**名前（Name）**] を入力します。

b) [管理状態（Admin State）] を [有効（Enabled）] に設定します。

c) [検出乗数（Detection Multiplier）] の値を設定します。

セッションがダウンしたと BFD が宣言する前に失われた可能性のある連続するパケットの最小数を指定します。範囲は 1 ～ 50 パケットです。デフォルトは 3 です。

d) [最小送信間隔（Minimum Transit Interval）] の値を設定します。

送信されるパケットの最小間隔時間。指定できる範囲は 250 ～ 999 ミリ秒です。デフォルトは 250 です。

e) [最大受信間隔（Maximum Receive Interval）] の値を設定します。

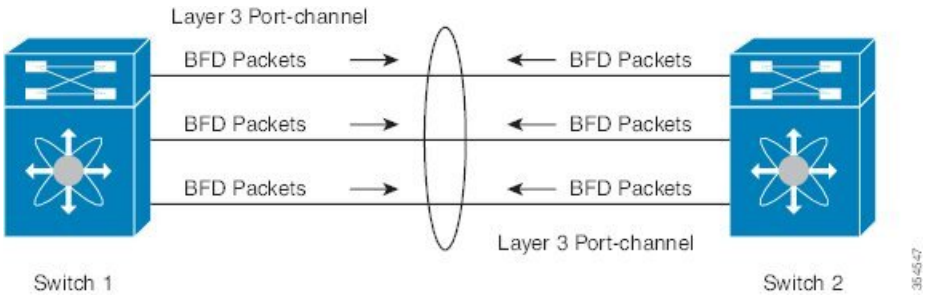
受信されたパケットの最大インターバル時間。指定できる範囲は 250 ～ 999 ミリ秒です。デフォルトは 250 です。

f) [Submit] をクリックします。

マイクロ BFD

Cisco APIC リリース 5.2(3) 以降、IETF RFC 7130 で定義されているように、APIC は マイクロ BFD をサポートします。Bidirectional Forwarding Detection（BFD）がポート チャネルで設定されている場合、キープアライブ パケットは使用可能なメンバー リンクで送信されます。キープアライブ パケットは残りのリンクを通過するだけであるため、単一のメンバー リンクの障害は検出されない場合があります。マイクロ BFD は、次の図に示すように、ポート チャネルの各メンバー リンクで個別の BFD セッションを確立する BFD の拡張機能です。

図 *3:* マイクロ *BFD* ポート チャネルでのセッション



リンク単位の BFD セッションがメンバー リンクで障害を検知すると、障害が発生したリンクは転送テーブルから削除されます。このメカニズムは、障害検出を高速化し、ポートチャネルで障害が発生したリンクを特定します。

に関する注意事項と制限事項 マイクロ BFD

- マイクロ BFD は、LACP ポートチャネルと非 LACP ポートチャネルの両方でサポートされます。
- マイクロ BFD は、同じポート チャネルでマルチホップ BFD と同時に実行できますが、シングルホップ BFD では実行できません。
- マイクロ BFD は、シングルホップ BFD 実装です。スイッチのメイン ポート チャネルとスイッチのピアの間にレイヤ 2 スイッチが存在する場合は機能しません。
- マイクロ BFD は、第 1 世代のリーフ スイッチではサポートされていません。第 1 世代のスイッチは、PID（製品識別子）に -EX や -FX などのサフィックスが含まれていないスイッチです。
- マイクロ BFD は、ポート チャネル上のルーテッド インターフェイスでのみサポートされます。
- クライアント プロトコルは、マイクロ BFD が有効になっている同じポート チャネル上のサブインターフェイスで実行できます。
- マイクロ BFD は、FEX ポートまたはファブリック ポートではサポートされません。
- BFD エコーは、マイクロ BFD セッションではサポートされません。
- マイクロ BFD が有効になっているデュアル IP スタック ポート チャネル（IPv4 および IPv6）では、IPv4 アドレスまたは IPv6 アドレスのいずれかを使用して マイクロ BFD を設定する必要がありますが、両方は必須ではありません。IPv4 と IPv6 の両方の マイクロ BFD セッションを設定することはできません。
- Cisco APIC リリース 5.2(3) 以降、Cisco APIC では、L3 ポート チャネルのメイン インターフェイスと同じ L3 ポート チャネル上のサブインターフェイスを使用できます。ただし、L3 ポート チャネルのメイン インターフェイスを作成または削除すると、ポート チャネルの物理メンバー ポートがフラップします。これにより、ポート チャネル サブインターフェイスがすでにアクティブな場合、トラフィックが失われます。

ポート チャネルでの マイクロ BFD の設定

この手順では、L3Outポートチャネルインターフェイスを有効に変更します。ポートチャネルの各メンバーリンクで個別のBFDセッションを確立します。マイクロ BFD マイクロ BFD

始める前に

- ダイレクト ポート チャネルが L3Out インターフェイスに設定されています。

手順

ステップ 1 **[テナント（Tenants）]** > **[*tenant_name*]** > **[ネットワーキング（Networking）]** > **[L3Outs]** > **[*L3Out_name*]** > **[論理ノード プロファイル（Logical Node Profiles）]** > **[*logical_node_profile_name*]** > **[論理インターフェイス プロファイル（Logical Interface Profiles）]**の順に移動します。

ステップ 2 変更する [論理インターフェイス プロファイル（Logical Interface Profile）] を選択します。

ステップ 3 [ルーテッド インターフェイス（Routed Interfaces）] タブを選択します。

マイクロ BFD は、ポート チャネル上のルーテッド インターフェイスでのみサポートされます。

ステップ 4 [ルーテッドインターフェイス（Routed Interfaces）]セクションで、既存のインターフェイスをダブル クリックして変更するか、[+] アイコンをクリックして新しいインターフェイスを論理インターフェイス プロファイルに追加します。

この手順の残りの手順では、既存の論理インターフェイスでのイネーブル化についてのみ説明します。マイクロ BFD 論理インターフェイス プロファイルに新しいインターフェイスを追加する場合は、GUI を使用した L3Out のインターフェイスの変更 を参照してください。

ステップ 5 選択したインターフェイスの設定済みプロパティで、選択した [パス タイプ（Path Type）] が [ダイレクト ポート チャネル（Direct Port Channel）] であることを確認します。

マイクロ BFD は、ポート チャネルでのみ適用できます。

ステップ 6 [Micro BFD の有効化（Enable Micro BFD）] チェックボックスをオンにします。

ステップ 7 [Micro BFD 宛先アドレス（Micro BFD Destination Address）] にポート チャネルの宛先 IP アドレスを入力します。

ステップ 8 [Micro BFD 開始タイマー（秒）（Micro BFD Start Timer（sec））]に 60 ー 3600 秒の値を入力します。

開始タイマーは、BFD セッションの確立を可能にするためにメンバー リンクでの BFD モニタリングのアクティブ化を遅延させます。タイマーはオプションです。タイマーが設定されていない場合、アクティベーションは遅延しません。

ステップ 9 **[送信（Submit）]** をクリックします。`

次のタスク

次の例に示すように、CLI を使用して マイクロ BFD セッションを確認できます。

```
leaf4# show port-channel database interface port-channel 3
port-channel3
Last membership update is successful
4 ports in total, 4 ports up
First operational port is Ethernet1/44
Age of the port-channel is 0d:22h:46m:03s
Time since last bundle is 0d:22h:42m:43s
Last bundled member is Ethernet1/44
Ports: Ethernet1/41 [on] [up]
```

```
Ethernet1/42 [on] [up]
Ethernet1/43 [on] [up]
Ethernet1/44 [on] [up] *

leaf4# show bfd neighbors vrf tenant1:vrf1

OurAddr NeighAddr
LD/RD RH/RS Holdown(mult) State Int Vrf Type

2003:190:190:1::1 2003:190:190:1::2
1090519041/0 Up 6000(3) Up Po3 tenant1:vrf1 singlehop

2003:190:190:1::1 2003:190:190:1::2
1090519042/2148074790 Up 180(3) Up Eth1/44 tenant1:vrf1 singlehop

2003:190:190:1::1 2003:190:190:1::2
1090519043/2148074787 Up 180(3) Up Eth1/41 tenant1:vrf1 singlehop

2003:190:190:1::1 2003:190:190:1::2
1090519044/2148074789 Up 180(3) Up Eth1/43 tenant1:vrf1 singlehop

2003:190:190:1::1 2003:190:190:1::2
1090519045/2148074788 Up 180(3) Up Eth1/42 tenant1:vrf1 singlehop
```

OSPF 外部ルーテッド ネットワーク

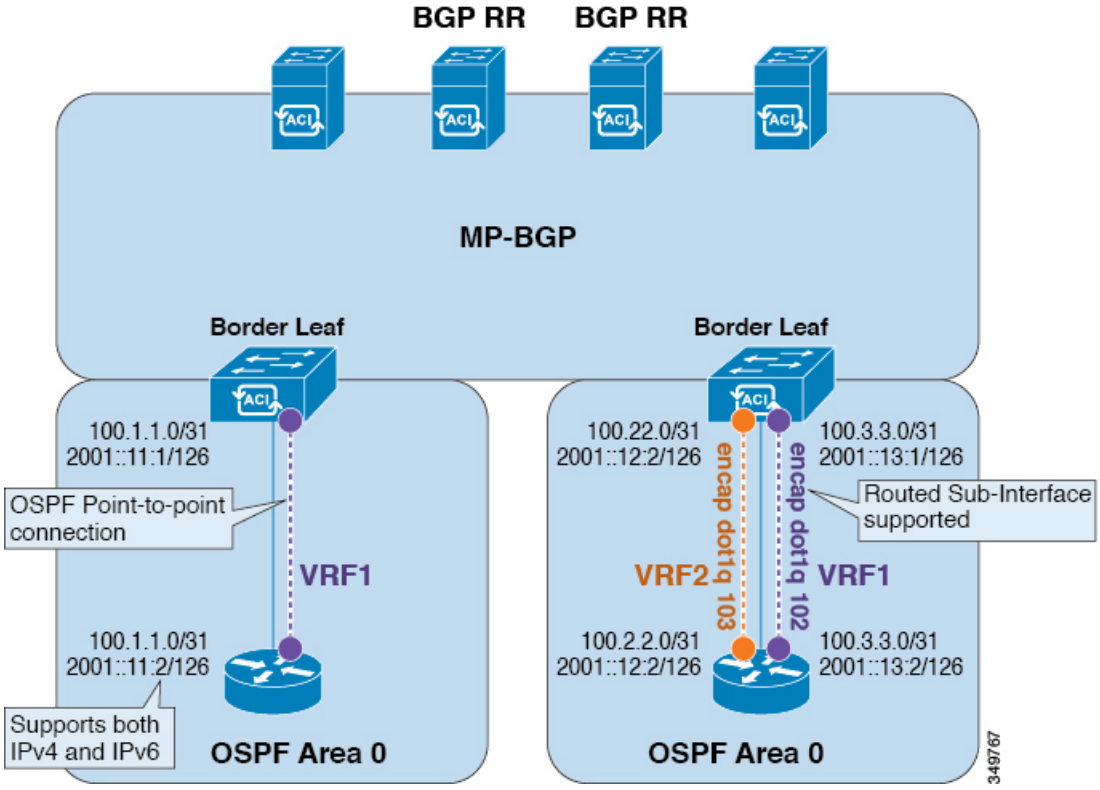
OSPF 外部ルーテッド ネットワークを設定するには、次の項の手順を使用します。

OSPF レイヤ 3 Outside 接続

OSPF レイヤ 3 Outside 接続は、標準または NSSA エリアです。バックボーン（エリア 0）エリアも、OSPF レイヤ 3 Outside 接続エリアとしてサポートされます。ACI は、IPv4 の OSPFv2 と IPv6 の OSPFv3 の両方をサポートします。OSPF レイヤ 3 Outside を作成するときに、OSPF バージョンを設定する必要はありません。インターフェイス プロファイル設定（IPv4 または IPv6 アドレッシング）に基づいて、正しい OSPF プロセスが自動的に作成されます。IPv4 と IPv6 の両方のプロトコルが同じインターフェイス（デュアル スタック）でサポートされますが、2 つの個別インターフェイス プロファイルを作成する必要があります。

レイヤ 3 Outside 接続は、ルーテッド インターフェイス、ルーテッド サブインターフェイス、および SVI でサポートされます。SVI は、レイヤ 2 とレイヤ 3 両方のトラフィックで物理接続を共有する必要がある場合に使用されます。SVI は、物理ポート、ポート チャネル、および仮想ポート チャネル（vPC）でサポートされています。

図 *4 : OSPF* レイヤ *3 Out* 接続



SVI がレイヤ 3 Outside 接続に使用されると、外部ブリッジ ドメインが境界リーフ スイッチに作成されます。外部ブリッジ ドメインは、ACI ファブリック上の 2 つの VPC スイッチ間の接続を可能にします。これにより、両方の VPC スイッチが、相互の、および外部 OSPF デバイスとの OSPF 隣接関係を確立できます。

ブロードキャスト ネットワークで OSPF を実行する場合、障害が発生したネイバーを検出する時間は dead 間隔（デフォルトは 40 秒）です。障害が発生した後でネイバー隣接関係を再確立する場合にも、代表ルータ（DR）の選定が原因で時間がかかる可能性があります。

（注）

- 1 つの vPC ノードへのリンクまたはポート チャネルに障害が発生しても、OSPF 隣接関係がダウンすることはありません。OSPF 隣接関係は、その他の vPC ノードを介してアクセスできる外部ブリッジ ドメインによりアップ状態を維持することができます。
- OSPF 時間ポリシーまたはBGP、OSPF、またはEIGRPアドレス ファミリ ポリシーがL3Outに適用されると、次の動作を観察できます。
  - L3Out とポリシーが同じテナントで定義されている場合、動作に変更はありません。
  - 共通テナント以外のユーザー テナントで L3Out が設定されている場合、L3Out VRF インスタンスは共通テナントに解決され、ポリシーが共通テナントで定義されている場合、デフォルト値のみが適用されます。ポリシーの変更は有効になりません。
- 境界リーフ スイッチが 2 つの外部スイッチと OSPF 隣接関係を形成し、2 つのスイッチの 1 つでルート損失が発生し、隣接スイッチでは発生しない場合、Cisco ACI 境界リーフ スイッチは両方のネイバーのルートを再コンバージェンスします。

GUI を使用した管理テナントの OSPF L3Out の作成

- ルータ ID と論理インターフェイス プロファイルの IP アドレスが異なっていて重複していないことを確認します。
- 次の手順は、管理テナントの OSPF L3Out を作成するためのものです。テナントの OSPF L3Out を作成するには、テナントを選択し、テナント用の VRF を作成する必要があります。
- 詳細については、『*Cisco APIC and Transit Routing*』を参照してください。

手順

ステップ 1 メニュー バーで、**[Tenants]** > **[mgmt]** の順に選択します。

ステップ 2 [**ナビゲーション**（**Navigation**）] ペインで、**[ネットワーキング**（**Networking**）**]** > **[L3Outs]** を展開します。

ステップ 3 [L3Outs] を右クリックし、[L3Out の作成（Create L3Out）] をクリックします。

[**L3Out の作成**（**Create L3Out**）] ウィザードが表示されます。

ステップ 4 [L3Out の作成（Create L3Out）] ウィザードの [識別（Identity）] ウィンドウで、次の操作を実行します。

a) [Name] フィールドに、名前（RtdOut）を入力します。

b) [VRF] フィールドのドロップダウン リストから、VRF（inb）を選択します。

（注） このステップでは、ルーテッド Outside をインバンド VRF に関連付けます。

c) [L3 ドメイン（L3 Domain）] ドロップダウン リストから、適切なドメインを選択します。
d) [OSPF] チェックボックスをオンにします。
e) [OSPF Area ID] フィールドに、エリア ID を入力します。
f) [OSPF Area Control] フィールドで、適切なチェックボックスをオンにします。
g) [OSPF Area Type] フィールドで、適切なエリア タイプを選択します。
h) [OSPF Area Cost] フィールドで、適切な値を選択します。
i) **[次へ（Next）]** をクリックします。

[**ノードとインターフェイス（Nodes and Interfaces**）] ウィンドウが表示されます。

ステップ 5 [ノードとインターフェイス（Nodes and Interfaces）] ウィンドウで、次の操作を実行します。

a) [デフォルトを使用（Use Defaults）] ボックスをオフにします。

これにより、[ノードプロファイル名（Node Profile Name）] フィールドを編集できます。

b) [**ノード プロファイル名（Node Profile Name**）] フィールドに、ノードプロファイルの名前を入力します（borderLeaf）。
c) [Node ID] フィールドで、ドロップダウン リストから、最初のノードを選択します（leaf1）。
d) [Router ID] フィールドに、一意のルータ ID を入力します。
e) ループバック アドレスにルータ ID を使用しない場合は、[ループバック アドレス（Loopback Address）] フィールドで別の IP アドレスを使用するか、空のままにします。

（注） [ルータ ID（Router ID）] フィールドに入力したエントリと同じ内容が [ループバック アドレス（Loopback Address）] フィールドに自動で入力されます。これは以前のビルドでの [ループバック アドレスのルータ ID の使用（Use Router ID for Loopback Address）] と同等です。ループバック アドレスにルータ ID を使用しない場合は、別の IP アドレスを使用するか、このフィールドを空のままにします。

f) 必要に応じて、このノードの [インターフェイス（Interface）]、[IP アドレス（IP Address）]、[インターフェイス プロファイル名（Interface Profile Name）]、および [MTU] フィールドに適切な情報を入力します。
g) [ノード（Nodes）] フィールドで、[+] アイコンをクリックして、別のノードの 2 番目のフィールド セットを追加します。

（注） 2 つ目のノード ID を追加します。

h) [Node ID] フィールドで、ドロップダウン リストから、最初のノードを選択します（leaf1）。
i) [Router ID] フィールドに、一意のルータ ID を入力します。
j) ループバック アドレスにルータ ID を使用しない場合は、[ループバック アドレス（Loopback Address）] フィールドで別の IP アドレスを使用するか、空のままにします。

（注） [ルータ ID（Router ID）] フィールドに入力したエントリと同じ内容が [ループバック アドレス（Loopback Address）] フィールドに自動で入力されます。これは以前のビルドでの [ループバック アドレスのルータ ID の使用（Use Router ID for Loopback Address）] と同等です。ループバック アドレスにルータ ID を使用しない場合は、別の IP アドレスを使用するか、このフィールドを空のままにします。

k) 必要に応じて、このノードの [インターフェイス（Interface）]、[IP アドレス（IP Address）]、[インターフェイス プロファイル名（Interface Profile Name）]、および [MTU] フィールドに適切な情報を入力します。

l) **[次へ（Next）]** をクリックします。

[**プロトコル（Protocols**）] ウィンドウが表示されます。

ステップ 6 [プロトコル（Protocols）] ウィンドウの [ポリシー（Policy）] 領域で、[デフォルト（default）] をクリックし、[次（Next）] をクリックします。

[**外部 EPG（External EPG**）] ウィンドウが表示されます。

ステップ 7 [外部 EPG（External EPG）] ウィンドウで次のアクションを実行します。

a) [Name] フィールドに、外部ネットワークの名前（extMgmt）を入力します。

b) [すべての外部ネットワークのデフォルト EPG（Default EPG for all external network）]フィールドをオフにします。

[サブネット（Subnets）] 領域が表示されます。

c) [+] をクリックして [サブネットの作成（Create Subnet）] ダイアログ ボックスにアクセスします。

d) [サブネットの作成（Create Subnet）] ダイアログ ボックスで、[IP アドレス（IP address）] フィールドに、サブネットの IP アドレスとマスクを入力します。

e) [Scope] フィールドで、目的のチェックボックスをオンにします。[OK] をクリックします。

f) [外部 EPG（External EPG）] ダイアログ ボックスで、[完了（Finish）]をクリックします。

（注） [作業（Work）] ペインの [L3Outs] 領域に、[L3Out] アイコン（RtdOut）が表示されます。

EIGRP 外部ルーテッド ネットワーク

EIGRP 外部ルーテッド ネットワークを設定するには、次の項の手順を使用します。

EIGRP レイヤ 3 Outside 接続について

この例は、Cisco APIC を使用して、拡張内部ゲートウェイ ルーティング プロトコル（EIGRP）を設定する方法を示しています。次の情報は、EIGRP を設定するときに適用されます:

- テナント、VRF、およびブリッジ ドメインがすでに作成されている必要があります。
- レイヤ 3 外部テナント ネットワークがすでに設定されている必要があります。
- 外部ルーテッドのルート制御プロファイルがすでに設定されている必要があります。
- EIGRP VRF ポリシーは EIGRP ファミリ コンテキスト ポリシーと同じです。
- EIGRP はエクスポート ルート制御プロファイルをサポートしています。ルート制御に関する設定はすべてのプロトコルで共通です。

サブネット ルートをネットワーク レベルのルートへ自動的に要約するよう（ルート要約）、EIGRP を設定できます。たとえば、192.31.7.0 のサブネットが設定されているインターフェイス上で、サブネット 131.108.1.0 が 131.108.0.0 としてアドバタイズされるように設定することができます。自動集約は、EIGRP プロセスに設定されているネットワーク ルータ設定コマンドが2つまたはそれ以上ある場合に実行されます。デフォルトでは、この機能は有効です。詳細については、「*Route Summarization*」を参照してください。

EIGRP プロトコルのサポート

EIGRP プロトコルは、Cisco Application Centric Infrastructure（ACI）ファブリック内の他のルーティング プロトコルと同様にモデル化されています。

サポートされる機能

サポートされる機能は次のとおりです。

- IPv4 および IPv6 ルーティング
- 各アドレス ファミリの仮想ルーティングおよび転送（VRF）とインターフェイスの制御
- ノード間の OSPF による再配布
- VRF ごとのデフォルト ルート リーク ポリシー
- パッシブ インターフェイスおよびスプリット ホライズンのサポート
- エクスポートされたルートにタグを設定するためのルート マップ制御
- EIGRP インターフェイス ポリシーの帯域幅および遅延設定オプション
- 認証サポート

サポートされない機能

次の機能はサポートされていません。

- スタブ ルーティング
- BGP 接続に使用される EIGRP
- 同じノード上の複数の EIGRP `L3extOut`

- インターフェイスごとの集約（EIGRP サマリー ポリシーは、L3Out で設定されたすべてのインターフェイスに適用されます）
- インターフェイスごとのインポートおよびエクスポート用配布リスト

EIGRP 機能のカテゴリ

EIGRP の機能は、次のように大きく分類できます。

- プロトコル ポリシー
- `L3extOut` の設定
- インターフェイス設定
- ルート マップ サポート
- デフォルト ルート サポート
- 中継サポート

EIGRP をサポートしているプライマリ管理対象オブジェクト

次のプライマリ管理対象オブジェクトは、EIGRP サポートを提供します。

- **EIGRP アドレス ファミリ コンテキスト ポリシー** `eigrpCtxAfPol`：`fvTenant`（テナント/プロトコル）で設定されているアドレス ファミリ コンテキスト ポリシー
- `fvRsCtxToEigrpCtxAfPol`：所定のアドレス ファミリ（IPv4 または Ipv6）についての VRF から `eigrpCtxAfPol` への関係。関係は、アドレス ファミリごとに 1 つのみ存在できます。
- `eigrpIfPol`：`fvTenant` で設定される EIGRP インターフェイス ポリシー。
- `eigrpExtP`：`L3extOut` 上で EIGRP のフラグを有効にします。
- `eigrpIfP`：`l3extLIfP` に接続された EIGRP インターフェイス プロファイル。
- `eigrpRsIfPol`：EIGRP インターフェイス プロファイルから `eigrpIfPol` への関係。
- `Defrtleak`：`l3extOut` 下のデフォルト ルート リーク ポリシー。

テナントでサポートされる EIGRP プロトコル ポリシー

テナント下では次の EIGRP プロトコル ポリシーがサポートされます。

- **EIGRP インターフェイス ポリシー（`eigrpIfPol`）**：インターフェイス上の所定のアドレス ファミリに適用される設定が含まれます。インターフェイス ポリシーでは次の設定が可能です。
  - 秒単位の *hello* 間隔
  - 分単位の *hold* 間隔
  - 次のインターフェイス制御フラグのうち 1 つ以上。

- スプリット ホライズン
- パッシブ
- ネクスト ホップ セルフ

- **EIGRP アドレス ファミリ コンテキスト ポリシー（`eigrpCtxAfPol`）**：所定の VRF 内の所定のアドレス ファミリの設定が含まれます。`eigrpCtxAfPol` は、テナント プロトコル ポリシー下で設定され、テナント下の 1 つ以上の VRF に適用できます。`eigrpCtxAfPol` は、VRF-per-address ファミリの関係を通して VRF で有効にできます。所定のアドレス ファミリに関係がない場合、あるいは関係に記述されている `eigrpCtxAfPol` が存在しない場合は、`[共通]` テナント下に作成されたデフォルトの VRF ポリシーがそのアドレス ファミリに使用されます。

  次の設定では、`eigrpCtxAfPol` で許可されます。

  - 内部ルートのアドミニストレーティブ ディスタンス
  - 外部ルートのアドミニストレーティブ ディスタンス
  - 最大許容 ECMP パス数
  - アクティブ タイマー間隔
  - メトリック バージョン（32 ビット/64 ビット メトリック）

ガイドラインと EIGRP を設定するときの制限事項

EIGRP を設定する場合は、次の注意事項に従ってください。

- 外部同じレイヤ 3 の EIGRP および BGP を設定することはサポートされていません。
- 外部同じレイヤ 3 の EIGRP や OSPF を設定することはサポートされていません。
- 1 つ EIGRP レイヤ 3 Out VRF あたりノードごとできますがあります。ノードで複数の Vrf を導入している場合、自身レイヤ 3 Out 各 VRF ことができます。
- 複数の EIGRP ピア、1 つレイヤ 3 Out からがサポートされます。これにより、1 つレイヤ 3 Out と同じノードから複数の EIGRP デバイスに接続できます。

次の設定では、EIGRP ネイバーがフラップします。

- VRF の EIGRP アドレス ファミリ コンテキストによるアドミニストレーティブ ディスタンスまたはメトリック スタイル（ワイド/ナロー）の変更
- 内部で使用されるテーブルマップを更新する次の設定を設定します。
  - VRF のルート タグの変更
  - EIGRP L3Out と同じ境界リーフ スイッチ上の同じ VRF 内の OSPF L3Out のインポート方向ルート制御の設定の設定（たとえば、ルート制御適用「インポート」オプションの有効化または無効化、インポート方向）。この機能は EIGRP ではサポートされ

ていないため、このような設定はEIGRP L3Out自体では許可されないことに注意してください。ただし、OSPF L3Out の設定は、同じ VRF とリーフ スイッチの EIGRP L3Out に影響を与えます。これは、OSPF のインポート ルート制御が、同じ境界リーフ スイッチ上の同じ VRF の EIGRP と他の目的で共有されるテーブル マップを使用するためです。

GUI を使用したEIGRPの設定

手順

ステップ 1 メニュー バーで、**[Tenants]** > **[All Tenants]** の順に選択します。

ステップ 2 **Work** ウィンドウで、テナントをダブルクリックします。

ステップ 3 [**ナビゲーション**（**Navigation**）] ペインで、**[*Tenant_name*]** > **[ポリシー**（**Policies**）**]** > **[プロトコル**（**Protocol**）**]** > **[EIGRP]** を展開します。

ステップ 4 右クリックして **EIGRP アドレス ファミリ コンテキスト**] を選択します **EIGRP アドレス ファミリ コンテキストのポリシーを作成** します。

ステップ 5 **Create EIGRP Address Family Context Policy** ダイアログボックスで、以下の操作を実行します:

a) **Name** フィールドに、コンテキスト ポリシーの名前を入力します。

b) **アクティブ間隔 (分)** フィールドで、インターバル タイマーを選択します。

c) **外部距離** 、および **内部距離** フィールドで、適切な値を選択します。

d) **パスの上限** フィールドで、[インターフェイス (ノードごと/リーフ スイッチごと) 間の値を適切なロード バランシングを選択します。

e) **メトリック スタイル** フィールドで、適切なメトリック スタイルを選択します。[Submit] をクリックします。`

Work ウィンドウに、コンテキスト ポリシーの詳細が表示されます。

ステップ 6 VRF のコンテキスト ポリシーを適用する、 **ナビゲーション**] ペインで、[展開 **ネットワー キング** > **Vrf** 。

ステップ 7 適切な VRF を選択し、[**作業**（**Work**）] ペインの [**ポリシー**（**Policy**）] タブで [**アドレス ファミリごとの EIGRP コンテキスト**（**EIGRP Context Per Address Family**）] を展開します。

ステップ 8 **EIGRP アドレス ファミリ タイプ** ドロップダウンリスト、IP バージョンを選択します。

ステップ 9 **EIGRP アドレス ファミリ コンテキスト** ドロップダウンリスト、コンテキスト ポリシーを選択します。**Update** をクリックし、**Submit** をクリックします。

ステップ 10 レイヤ 3 Out 内の EIGRP を有効にするには、[**ナビゲーション**（**Navigation**）] ペインで、**[ネットワーキング**（**Networking**）**]** > **[L3Out]**をクリックして目的のレイヤ 3 外部ネットワークをクリックします。

ステップ 11 [**作業**（**Work**）] ペインの [**ポリシー**（**Policy**）] タブで [**EIGRP**] のチェックボックスをオンにして EIGRP 自律システム番号を入力します。**[送信**（**Submit**）**]** をクリックします。`

ステップ 12 EIGRPインターフェイスポリシーを作成するには、[**ナビゲーション（Navigation**）ペインで、**[*Tenant_name*] > [ポリシー（Policies**）**] > [プロトコル（Protocol**）**] > [EIGRP]** をクリックして次のアクションを実行します。

a) 右クリックして **EIGRP インターフェイス** 、をクリックし、 **EIGRP インターフェイス ポリシーの作成** します。

b) **Create EIGRP Interface Policy** ダイアログボックスで、**Name** フィールドにポリシーの名前を入力します。

c) **制御状態** フィールドは、1 つまたは複数の制御を有効にする目的のチェック ボックスをチェックします。

d) **Helloインターバル (秒)** フィールドで、目的の間隔を選択します。

e) **保留間隔 (秒)** フィールドで、目的の間隔を選択します。[Submit] をクリックします。`

f) **Bandwidth** フィールドで、目的の帯域幅を選択します。

g) **遅延** フィールドで、10 マイクロ秒またはピコセル秒で、目的の遅延を選択します。

作業] ペインで、EIGRP インターフェイス ポリシーの詳細が表示されます。

ステップ 13 **ナビゲーション**] ペインで、適切な外部ルーテッド ネットワークの EIGRP が有効になってクリック展開 **論理ノード プロファイル** および次の操作の実行します。

a) 適切なノードとそのノードの下にインターフェイスを展開します。

b) インターフェイスを右クリックし、をクリックして **EIGRP インターフェイス プロファイルの作成** します。

c) **EIGRP インターフェイス プロファイルの作成** ダイアログボックスで、 **EIGRP ポリシー** フィールドで、目的のEIGRPインターフェイスポリシーを選択します。[Submit]をクリックします。`

（注） EIGRP の VRF ポリシーおよび EIGRP インターフェイス ポリシーは、EIGRP が有効になっているときに使用するプロパティを定義します。EIGRP の VRF ポリシーおよび EIGRP インターフェイス ポリシーは、新しいポリシーを作成しない場合にもデフォルトポリシーとして利用できます。したがって、ポリシーのいずれかを明示的に選択しない場合は、EIGRPが有効になっているとき、デフォルトのポリシーが自動的に利用されます。

これで EIGRP の設定は完了です。

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。