Cisco APIC Layer 3 ネットワーキング設定ガイド

初版：2017 年 9 月 22 日

最終更新：2018 年 6 月 18 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次

はじめに

この前書きは、次の項で構成されています。

対象読者

このガイドは、次の1つ以上に責任を持つ、専門知識を備えたデータセンター管理者を主な対象にしています。

- 仮想マシンのインストールと管理
- サーバ管理
- スイッチおよびネットワークの管理

新機能および変更された機能に関する情報

次の表は、現行リリースに至るまでにガイドの編成と特徴に加えられた主な変更点の概要を示しています。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

表 *1 : Cisco APIC Release 3.2(1)* の新機能と変更された動作

機能または変更	説明	参照先
孤立した ポートのサポート	vPC ドメインで、リモート リーフ スイッチの孤立したポート チャネルまたは物理ポートに対するサポートが利用できるようになりました。	次の章を参照してください: リモート リーフ スイッチ （295 ページ）
L3Outs のための QoS の章	L3Outs のための QoSは、個別の章に移動されました。	次の章を参照してください: L3Outs の QoS （67 ページ）
レイヤ 3 ルーティングとサブインターフェイス ポート チャネル	レイヤ 3 ポート チャネル へのサポーが追加されました。	次の項を参照してください。レイヤ 3 ルーティングおよびサブ インターフェイス ポート チャネル （47 ページ）
リモートのリーフ スイッチの強化	新しい機能とオプションがサポートされました。	次の章を参照してください: リモート リーフ スイッチ （295 ページ）
トランジット ルーティングの強化	APIC GUI、NX-OS スタイル CLI、または REST API を使用してトランジット ルーティングを構成する方法についての情報が追加されました。	次の章を参照してください: トランジットルーティング （313 ページ）

表 *2 : Cisco APIC Release 2.2(4)* の新機能と変更された動作

機能または変更	説明	参照先
ネイバー探索重複アドレス検出（DAD）	ネイバー探索重複アドレス検出 (DAD) を無効にするためのサポートが追加されました。	次の章を参照してください: IPv6 ネイバー探索 （195 ページ）

表 *3 : Cisco APIC Release 3.1(2m)* の新機能と変更された動作

機能または変更	説明	参照先
L3Outs のための QoS	このリリースでは、L3Out 入力トラフィックでの QoSポリシーの適用が強化されました。	L3Outs の QoS （67 ページ） を参照してください。

機能または変更	説明	参照先
最大 MTU の増加	9216 までの外部ネットワークと通信するために使用される MTU の設定を有効にするために、最大 MTU が 9000 から 9216 バイトに増加されました。	次の章を参照してください: 外部ネットワークへのルーテッド接続 （23 ページ）
Out レイヤ 3 でネイバー探索ルータ アドバタイズメント	RS/RA パケットは、自動設定は使用されは、ルーテッド インターフェイス、レイヤ 3 サブインターフェイス、SVI などのレイヤ 3 インターフェイスで設定できます。	次の章を参照してください: IPv6 ネイバー探索 （195 ページ）
BGP 外部ルーテッド ネットワークと自律システムのオーバーライド	AS オーバーライド機能が、アウトバウンド ルートの AS パスで送信 BGP ルータの AS 番号を持つ発信元ルータからの AS 番号を置き換えます。	次の章を参照してください: ルーティング プロトコル サポート （71 ページ）

表 *4 : Cisco APIC Release 3.1(1i)* の新機能と変更された動作

機能または変更	説明	参照先
FEX でのレイヤ 3 マルチキャストのサポート	FEX ポートに接続されているマルチキャストの送信元または受信先がサポートされています。	次の章を参照してください: IP Multicast：IP マルチキャスト （209 ページ）
スイッチ仮想インターフェイス （SVI） 自動状態	SVI 自動状態操作を有効にできます。これにより、VLAN 内のすべてのポートがダウンすると SVI 状態をダウン状態にできます。 この機能は、APIC リリース 2.2(3x) リリースおよび APIC リリース 3.1 (1) で使用できます。APIC リリース 3.0(x) ではサポートされていません。	次の章を参照してください: スイッチ仮想インターフェイス （165 ページ）

機能または変更	説明	参照先
リモート リーフ スイッチ	ACI ファブリックを導入すると、ACI サービスと APIC 管理を、ローカル スパイン スイッチまたは APIC が接続されていない Cisco ACI リーフ スイッチのあるリモート データ センターに拡張できます。	次の章を参照してください: リモート リーフ スイッチ （295 ページ）
Multipod しの新しいハードウェア サポート	マルチポッドおよび GOLF は、すべての Cisco Nexus 9300 プラットフォーム ACI モード スイッチと、Cisco Nexus 9500 プラットフォーム ACI モード スイッチ ライン カードとファブリック モジュールによりサポートされています。Cisco APIC、リリース 3.1(x) 以降では、これに N9K-C9364C スイッチも含まれます。	Cisco ACI GOLF （257 ページ）と マルチポッドの章を参照してください。
Multi-Site サイト間の共有 GOLF 接続を使用する	拡大 Vrf ゴルフ接続を共有する場合、複数のサイト トポロジでは、APIC サイトの VRF 間のトラフィックの問題を回避するガイドラインが追加されました。	次の章を参照してください: Cisco ACI GOLF （257 ページ）
スパイン スイッチの BFD サポート	スパイン スイッチ上で Bidirectional Forwarding Detection（BFD）のサポートが追加されます。	次の章を参照してください: ルーティング プロトコル サポート （71 ページ）
L3Out 構成の新しい例	新しい GUI、NX-OS スタイル CLI、および REST API の例は、明確で一貫したものになりました。	次の章を参照してください: 外部ネットワークへのルーテッド接続 （23 ページ）
トランジット ルーティングの設定	ナレッジ ベースの記事、「*Cisco APIC* とトランジット ルーティング」がこのガイドに組み込まれました。APIC GUI、NX-OS スタイル CLI、および REST API の新しい構成例が含まれています。	次の章を参照してください: トランジット ルーティング （313 ページ）

機能または変更	説明	参照先
再編成された章	このガイドの章は、より論理的な順番になるように再編成されました。次の章名が変更されています: • 「テナント外部のネットワーク」が「外部ネットワークへのルーティング接続」に • 「ルート プロファイル、ルート マップ、および *IP* プレフィックス リスト」が「ルート制御」に • 「共有レイヤ *3* 外部接続」が「共有サービス」に • 「*SVI* 外部カプセル化スコープ が「スイッチ仮想インターフェイス」に	--

表 *5 : Cisco APIC Release 3.0(2h)* の新機能と変更された動作

機能または変更	説明	参照先
BD のスタティック ルート：	パーベイシブ ブリッジ ドメイン (BD) からファイアウォールの背後にある仮想サービスへのルートを有効にする、スタティック ルートの構成へのサポートが追加されました。 この機能は、通常の EPG を使用して、パーベイシブ BD には直接接続されていないサブネットやホストへのエンドポイント (EP) の到達可能性を有効にします。	次の章を参照してください: スタティック ルート ブリッジ ドメイン （155 ページ）

注: APIC Release 2.2(3x) の機能は、この特定のリリースでのみ使用可能です。APIC Release 3.0(x) または 3.1(x) ではサポートされていません。

表 *6 : Cisco APIC Release 2.2(3x)* に関連した *Cisco APIC* の新機能と変更された動作

機能または変更	説明	参照先
スイッチ仮想インターフェイス（SVI）自動状態	SVI 自動状態操作を有効にできます。これにより、VLAN 内のすべてのポートがダウンすると、SVI 状態もダウン状態になります。 （注） この機能は APIC Release 2.2(3x) リリースで利用可能です。APIC Release 3.0(x) ではサポートされていません。	次の章を参照してください: スイッチ仮想インターフェイス （165 ページ）

表 *7 : Cisco APIC Release 3.0(1k)* に関連した *Cisco APIC* の新機能と変更された動作

機能または変更	説明	参照先
AS パスのプリペンド	リモート ピアによる最適なパス選択の呼び出しのため、BGP ルートの自律システム パスの長さを変更できます	次の章を参照してください: ルーティング プロトコル サポート （71 ページ）
BGP 最大パス	等コストマルチパス ロードバランシングを呼び出すために、BGP がルート テーブルに追加するパスの最大数を構成できるようになりました。	次の章を参照してください: ルーティング プロトコル サポート （71 ページ）

表 *8 : Cisco APIC Release 2.3(1e)* に関連した *Cisco APIC* の新機能と変更された動作

機能または変更	説明	参照先
レイヤ 3 外部ネットワーク経由での SVI のカプセル化の範囲	このリリースでは、レイヤ 3 ネットワーク経由での SVI のカプセル化の範囲を構成できます。	次の章を参照してください: スイッチ仮想インターフェイス （165 ページ）
Denyプレフィックスのサポート	特定のルートのコンテキスト ルールを拒否することがサポートされるようになりました。	次の章を参照してください: ルート制御 （133 ページ）

表 *9 : Cisco APIC Release 2.2(2e)* および *2.2(2f)* に関連した *Cisco APIC* の新機能と変更された動作

機能または変更	説明	参照先
ノード BGP タイマー値ごとの各 VRF	このリリースでは、ノードあたりの各 VRF で BPG タイマーを定義および関連付けることができます。	次の章を参照してください: ルーティング プロトコル サポート （71 ページ）
レイヤ 3 をインター VRF 漏出 Out Out 3 をレイヤします。	このリリースでは、異なる Vrf に、共有のレイヤ 3 が記録されるコントラクトを使用して相互に通信できます。	次の章を参照してください: 共有サービス （175 ページ）
ルート プレフィックスごとに割り当てられた複数の BGP コミュニティ	このリリースでは、複数の BGP コミュニティは、ルートプレフィックスの BGP プロトコルを使用してごとここで割り当てられます。	See chapter 外部ネットワークへのルーテッド接続 （23 ページ） and ルート制御 （133 ページ）
EIGRP から BGP へのトランジット ルーティングが利用可能になりました。	サポート トランジット コンビネーション マトリクスでのサポートが追加されました。	次の章を参照してください: トランジット ルーティング （313 ページ）
異なる VRF の共有 L3Outs 間の通信	範囲とサブネットの集約コントロールでのステートメントへのサポートが追加されました。	次の章を参照してください: トランジット ルーティング （313 ページ）

表 *10 :* このドキュメントの新機能と変更された情報

機能または変更	説明	参照先
ドキュメントの再編成	このガイドのトピックは、『*Cisco APIC* ベーシック コンフィギュレーション ガイド リリース *2.x*』、『*Cisco ACI* および *Cisco ACI* でのレイヤ *3* マルチキャスト』、および次の知識ベースの記事から取られています: • *Cisco APIC* と外部ルートの *Interleak* • *Cisco APIC* と明示的なプレフィックス リストを使用するルート マップ • *Cisco APIC* の *IP*エージング ポリシー • テナント ネットワークのための *Cisco APIC Layer 3 Outside* • *Cisco APIC* テナント、*VRF*、および *IPv6* ネイバー探索でのブリッジ ドメインの作成 • *Cisco APIC* と共通パーベイシブ ゲートウェイ • *Cisco APIC* と *HSRP* • *Cisco APIC* と *IGMP* スヌープ レイヤ *2* マルチキャスト構成 • Cisco APIC とインポートおよびエクスポート制御を使用するルート制御プロトコル • *Cisco APIC* と *BGP* 外部ルーティング ネットワークと *BFD* • *Cisco APIC* と *EIGRP*	*Cisco APIC* レイヤ *3* 構成ガイド (本書)

機能または変更	説明	参照先
名称変更	「ファブリック WAN のためのレイヤ 3 EVPN サービス」の名前が「Cisco ACI GOLF」に変更されました	Cisco ACI GOLF （257ページ）と マルチポッドの章を参照してください。

表 *11 : Cisco APIC Release 2.2(1n)* に関連して本書に記されている新機能および変更点に関する情報

機能または変更	説明	参照先
HSRP	このリリースでは、HSRPを有効にできます。これはファーストホップ冗長プロトコル（FHRP）であり、ファーストホップ IP ルータの透過的なフェールオーバーを可能にします。HSRP は、デフォルトルータの IP アドレスを指定して設定された、イーサネットネットワーク上の IP ホストにファーストホップ ルーティングの冗長性を提供します。ルータ グループでは HSRP を使用して、アクティブ ルータおよびスタンバイ ルータを選択します。ルータ グループでは、アクティブ ルータはパケットをルーティングするルータであり、スタンバイ ルータはアクティブ ルータに障害が発生したときや、プリセット条件に達したときに使用されるルータです。	次の章を参照してください: HSRP （243 ページ）

表 *12 : Cisco APIC Release 2.1(1h)* に関連した *Cisco APIC* の新機能と変更された動作

機能または変更	説明	参照先
EVPN タイプ 2 ホスト ルートの配布	EVPN トポロジの最適なトラフィック転送へのサポートが追加されました。これを実現するため、ファブリックのスパインが BGP EVPN タイプ 5（IP プレフィックス）ルートの形式のパブリック BD サブネットとともに、EVPN タイプ 2（MAC-IP）ルートを使用するホスト ルートを DCIG にアドバタイズするように設定できます。	次の章を参照してください: Cisco ACI GOLF （257 ページ）
明示的なプレフィクス リストを使用するルート マップ	パブリックなブリッジ ドメイン(BD)サブネットと外部トランジット ネットワークのための明示的なプレフィックス リストは、インバウンドとアウトバウンドのルート制御を可能にします。レイヤ 3 アウトのインバウンドおよびアウトバウンドルート コントロールは、ルートマップ/プロファイル（rtctrlProfile）によって管理されます。ルートマップ/プロファイル ポリシーは、Cisco ACI ファブリックでレイヤ 3 アウトを完全に管理するプレフィックス リストをサポートしています。	次の章を参照してください: ルート制御 （133 ページ）

機能または変更	説明	参照先
IP エージング ポリシー	このリリースでは、エンドポイントでの IP のための新しいエージング ポリシーを有効にできます。IP エージング ポリシーは、エンドポイント上の使用されていない IP を追跡し、その寿命を管理します。追跡は、ローカルのエンドポイント エージング間隔の 75% で、IPv4 の場合には ARP リクエスト、IPv6 の場合にはネイバー誘導を送信する、BD 用に設定されたエンドポイント保持ポリシーを使用して実行されます。IP から応答を受信しなかった場合、その IP の寿命は切れます。	次の章を参照してください: IP エージング （191 ページ）
IGMP スヌープ アクセス グループのサポートおよびIGMP スヌープ スタティック グループのサポート	Internet Group Management Protocol（IGMP） ネットワーク トラフィックをリッスンするプロセスである IGMP スヌーピングのサポートが追加されました。この機能は、ネットワーク スイッチがホストとルータの間の対話をリッスンし、必要のないマルチキャスト リンクはフィルタして、どのポートが特定のマルチキャスト トラフィックを受信するかを制御できるようにします。	次の章を参照してください: IGMP スヌーピング （223 ページ）
multipod でのマルチキャストのサポート	multipod トポロジで IP マルチキャストのサポートが追加されました	次の章を参照してください: IP Multicast：IP マルチキャスト （209 ページ）

表 *13 : Cisco APICCisco APIC* リリース *2.0(1m)* の新機能と変更された動作

機能または変更	説明	参照先
OSPF インバウンド フィルタリングでのインポート制御ポリシーのサポート	BGP の場合と同様に、OSPF を使用したインポートおよびエクスポート制御へのサポートが追加されました。	See chapters 外部ネットワークへのルーテッド接続 （23 ページ） and ルート制御 （133 ページ）
GOLF (ファブリック WAN 経由のレイヤ 3 EVPN サービス)	GOLF が導入されました。	次の章を参照してください: Cisco ACI GOLF （257 ページ）
トランジット ルーティングで GOLF がサポートされました。	GOLF L3Outs と境界リーフ BGP/OSPF L3Outs がサポートされました。	次の章を参照してください: トランジット ルーティング （313 ページ）
EIGRP インターフェイス ポリシーの強化	帯域幅と遅延などの EIGRP のプロパティのサポートが追加されました。	次の章を参照してください: ルーティング プロトコル サポート （71 ページ）
レイヤ 3 マルチキャスト	レイヤ 3 マルチキャスト が導入されました。	次の章を参照してください: IP Multicast : IP マルチキャスト （209 ページ）
トランジット ルーティングのサブネットの集約コントロールのサポート	サブネットの範囲と集約コントロールについての新しいセクションを追加されました。	次の章を参照してください: トランジット ルーティング （313 ページ）
Ethertype、プロトコル、L4 ポート、および TCP フラグ フィルタのサポート	Ethertype、プロトコル、L4 ポート、および TCP フラグ フィルタのサポートが使用可能になり、トランジット ルーティング制御に使用できるようになりました。	次の章を参照してください: トランジット ルーティング （313 ページ）

表 *14 : Cisco APICCisco APIC* リリース *1.3(1g)* の新機能と変更された動作

機能または変更	説明	参照先
ルート集約	オブジェクト モデル CLI の手順が削除されました。 GUI と NX-OS CLI インターフェイスの追加ルート集約手順が追加されました。	次の章を参照してください: ルーティング プロトコル サポート （71 ページ）

機能または変更	説明	参照先
-	オブジェクト モデル CLI の手順が削除され、NX-OS スタイル CLI の手順が追加されました。	• この章の NX-OS スタイル CLI のトピック 次の章を参照してください: トランジット ルーティング （313 ページ） *IPv6* とネイバー探索 • ルート コントロールでの NX-OS スタイル CLI のトピック • *BFD* での *BGP* 外部ルーテッドネットワーク (ルーティング プロトコルのサポート) でのNX-OS スタイル CLIの トピック • 次の章を参照してください: ルーティング プロトコル サポート （71 ページ）

表 *15 : Cisco APIC Release 1.2(x)* に関連した *Cisco APIC* の新機能と変更された動作

機能または変更	説明	参照先
OSPF から受信し、再分配したすべてのルートへの属性設定	コミュニティ、ローカル プレフィックス、MED など、受信したすべてのルートの属性設定のサポートが追加されました。タグ、ローカル プレフィックス、コミュニティなど、再分配したすべてのルートの属性を設定します。	次の章を参照してください: ルーティング プロトコル サポート （71 ページ）

機能または変更	説明	参照先
OSPF、BGP、およびEIGRPのルート集約	ルート集約では、ルート テーブルで多数の固有アドレスを1つのアドレスに置き換えること可能にします。たとえば、10.1.1.0/24、10.1.2.0/24、10.1.3.0/24は10.1.0.0/16に置き換えられます。ルート集約ポリシーにより、ボーダー リーフ スイッチとそのネイバー リーフ スイッチの間でルートを効率的に共有することができます。BGP、OSPF、あるいはEIGRPのルート集約ポリシーは、ブリッジ ドメインまたは中継サブネットに適用されます。OSPFでは、エリア間ルート集約と外部ルート集約がサポートされます。	次の章を参照してください: ルーティング プロトコル サポート （71 ページ）
共通パーベイシブ ゲートウェイ	ブリッジ-ドメインごとにIPv4共通ゲートウェイを使用して2つのACIファブリックを設定できます。これにより、1つ以上の仮想マシン（VM）または従来のホストを、ホストがそのIPアドレスを保持したままファブリック間で移動できます。ファブリック間のVMとホストの移動は、VMハイパーバイザによって自動的に行うことができます。ACIファブリックは、同じ場所に配置することも、複数のサイト間でプロビジョニングすることもできます。ACIファブリック間のレイヤ2接続は、ローカル リンクか、ブリッジ型ネットワークにわたるものになります。	次の章を参照してください: 共通パーベイシブ ゲートウェイ （149 ページ）

機能または変更	説明	参照先
着信コミュニティに基づくルートの BGP 属性の設定	BGP 属性の設定は、コミュニティ、ローカル環境設定、MED などの着信のコミュニティに基づくルートに対して有効です。	次の章を参照してください: ルーティング プロトコル サポート （71 ページ）
Bidirectional Forwarding Detection（BFD）： GUI、NX-OS CLI および REST API のグローバル構成 GUI、NX-OS CLI および REST API のインターフェイス構成 GUI、NX-OS CLI および REST API コンシューマ プロトコルの構成	BFD のサポートが導入されました。これにより、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。	次の章を参照してください: ルーティング プロトコル サポート （71 ページ）
最大プレフィックスの制限	BGP 最大プレフィックスの制限のサポートが追加されました。	次の章を参照してください: ルーティング プロトコル サポート （71 ページ）
アクション ルール プロファイルとピア接続プロファイルの属性設定のための BGP の強化	BGP 属性のダイナミック ネイバー、ルート ダンプニング、ウェイト属性と remove-private-as へのサポートの追加。	次の章を参照してください: ルーティング プロトコル サポート （71 ページ）
IPv6 のサポートとインターフェイス ポリシーの強化	IPv6 は EIGRP でサポートされます。 インターフェイス ポリシーが強化されました。既存のインターフェイス ポリシー パラメータだけでなく、帯域幅と遅延も、eigrpIfPol 属性によってインターフェイス上で制御できます。。 NX OS スタイル CLI の手順が追加されました。	次の章を参照してください: ルーティング プロトコル サポート （71 ページ）

機能または変更	説明	参照先
外部ルータのインターリーク	OSPF から BGP へのルートのインターリークを有効にするため、属性(コミュニティ、設定、またはメトリック)を設定するためのサポートが追加されました。	次の章を参照してください:外部ルートのインターリーク （187 ページ）
トランジット ルーティングのサポート	ファブリックでの中継ルーティングのサポートが追加されました。	次の章を参照してください:トランジットルーティング （313 ページ）

表 *16 : Cisco APIC* 、リリース *1.1(x)* の新機能と変更された動作

機能または変更	説明	参照先
IPv6 のサポート、直接 BGP のサポートおよびeBGP のサポート	IPv6 のサポート、直接 BGP のサポートおよびeBGP のサポートが導入されました。	次の章を参照してください:ルーティング プロトコル サポート （71 ページ）
テナント レイヤ 3 外部ネットワーク	テナント レイヤ 3 外部ネットワークに付いての記述が追加されました。	次の章を参照してください:外部ネットワークへのルーテッド接続 （23 ページ）

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	省略可能な要素（キーワードまたは引数）は、角かっこで囲んで示しています。
[x | y]	いずれか1つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか1つを選択しなければならない必須キーワードや引数は、波かっこで囲み、縦棒で区切って示しています。

表記法	説明
[x {y | z}]	角かっこまたは波かっこが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角かっこ内の波かっこと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
`variable`	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

例では、次の表記法を使用しています。

表記法	説明
`screen フォント`	スイッチが表示する端末セッションおよび情報は、スクリーンフォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字のスクリーンフォントで示しています。
イタリック体の *screen* フォント	ユーザが値を指定する引数は、イタリック体のスクリーンフォントで示しています。
<>	パスワードのように出力されない文字は、山カッコ（<>）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

このマニュアルでは、次の表記法を使用しています。

（注） 「注釈」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

注意 「要注意」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

警告 安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

これらの注意事項を保存しておいてください

関連資料

Application Policy Infrastructure Controller（APIC）のマニュアル

次のガイドでは、APIC のドキュメントを提供します。

- 『*Cisco APIC Getting Started Guide*』
- 『*Cisco APIC Basic Configuration Guide*』
- *Cisco ACI* の基礎
- *Cisco APIC* レイヤ *2* ネットワーク設定ガイド
- *Cisco APIC Layer 3* ネットワーキング設定ガイド
- 『*Cisco APIC NX-OS Style Command-Line Interface Configuration Guide*』
- *Cisco APIC REST API* 設定ガイド
- 『*Cisco APIC* レイヤ *4* ～ レイヤ *7* サービス導入ガイド』
- 『*Cisco ACI Virtualization Guide*』
- *Cisco* アプリケーション セントリック インフラストラクチャ：ベスト プラクティス ガイド

これらすべてのドキュメントは、次の URL で入手できます。 http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

シスコ アプリケーション セントリック インフラストラクチャ（ACI）のマニュアル

ACI の各種マニュアルは、次の URL から入手できます。http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

シスコ アプリケーション セントリック インフラストラクチャ（ACI）シミュレータのマニュアル

Cisco ACI Simulator のマニュアルは、次の URL から入手できます：http://www.cisco.com/c/en/us/support/cloud-systems-management/application-centric-infrastructure-simulator/tsd-products-support-series-home.html

Cisco Nexus 9000 シリーズ スイッチのマニュアル

Cisco Nexus 9000 シリーズ スイッチのマニュアルは、次の URL で入手できます。
http://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/tsd-products-support-series-home.html

Cisco Application Virtual Switch のマニュアル

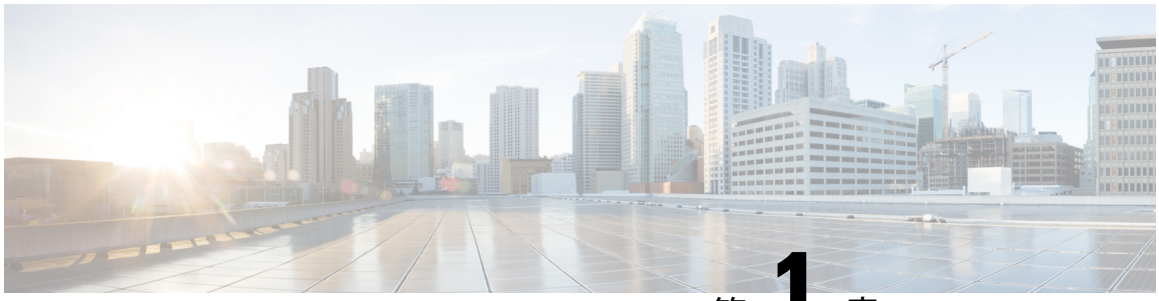
Cisco Application Virtual Switch（AVS）のマニュアルは、次の URL で入手できます。
http://www.cisco.com/c/en/us/support/switches/application-virtual-switch/tsd-products-support-series-home.html

シスコ アプリケーション セントリック インフラストラクチャ（ACI）と OpenStack の統合に関するマニュアル

Cisco ACI と OpenStack の統合に関するマニュアルは、次の URL から入手できます。
http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載もれなどお気づきの点がございましたら、apic-docfeedback@cisco.com までご連絡ください。ご協力をよろしくお願いいたします。



第 1 章

Cisco ACI 転送

この章の内容は、次のとおりです。

ファブリック内での転送

ACI ファブリックは現代のデータ センター トラフィック フローを最適化する

Cisco ACI アーキテクチャは、従来のデータセンター設計から来る制限を解放して、最新のデータセンターで増大する East-West トラフィックの需要に対応します。

今日のアプリケーション設計は、データセンターのアクセス レイヤを通る、サーバ間の East-West トラフィックを増大させています。このシフトを促進しているアプリケーションには、Hadoop のようなビッグデータの分散処理の設計 、VMware vMotion のようなライブの仮想マシンまたはワークロードの移行、サーバのクラスタ リング、および多層アプリケーションなどが含まれます。

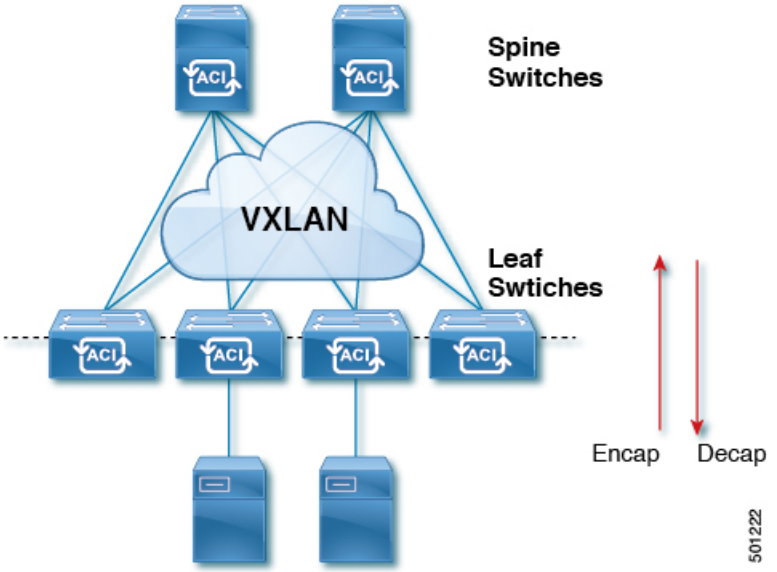
North-South トラフィックは、コア、集約、およびアクセス レイヤ、またはコラプスト コアとアクセス レイヤが重要となる、従来型のデータセンター設計を推進します。クライアントデータはWAN またはインターネットで受信され、サーバの処理を受けた後、データセンターを出ます。このような方式のため、WAN またはインターネットの帯域幅の制限により、データセンターのハードウェアは過剰設備になりがちです。ただし、スパニング ツリー プロトコルが、ループをブロックするために要求されます。これは、ブロックされたリンクにより利用可能な帯域幅を制限し、トラフィックが準最適なパスを通るように強制する可能性があります。

従来のデータセンター設計においては、、IEEE 802.1Q VLAN がレイヤ 2 境界の論理セグメンテーションまたはまたはブロードキャスト ドメインを提供します。ただし、ネットワーク リンクの VLAN の使用は効率的ではありません。データセンター ネットワークでデバイスの配置要件は柔軟性に欠け、VLAN の最大値である 4094 の VLAN が制限となり得ます。IT 部門と

クラウドプロバイダが大規模なマルチテナントデータセンターを構築するようになるにつれ、VLAN の制限は問題となりつつあります。

スパイン リーフ アーキテクチャは、これらの制限に対処します。ACI ファブリックは、外界からは、ブリッジングとルーティングが可能な単一のスイッチに見えます。レイヤ 3 のルーティングをアクセス レイヤに移動すると、最新のアプリケーションが必要としている、レイヤ 2 の到達可能性が制限されます。仮想マシン ワークロード モビリティや一部のクラスタ リングのソフトウェアのようなアプリケーションは、送信元と宛先のサーバ間がレイヤ 2 で隣接していることを必要とします。アクセス レイヤでルーティングを行えば、トランク ダウンされた同じ VLAN の同じアクセス スイッチに接続したサーバだけが、レイヤ 2 で隣接します。ACI では、VXLAN が、基盤となるレイヤ 3 ネットワーク インフラストラクチャからレイヤ 2 のドメインを切り離すことにより、このジレンマを解決します。

図 *1: ACI* ファブリック



トラフィックがファブリックに入ると、ACIがカプセル化してポリシーを適用し、必要に応じてスパイン スイッチ (最大 2 ホップ) によってファブリックを通過させ、ファブリックを出るときにカプセル化を解除します。ファブリック内では、ACIはエンドポイント間通信でのすべての転送について、Intermediate System-to-Intermediate System プロトコル (IS-IS) および Council of Oracle Protocol (COOP) を使用します。これにより、すべての ACI リンクがアクティブで、ファブリック内での等コストマルチパス (ECMP) 転送と高速再コンバージョンが可能になります。ファブリック内と、ファブリックの外部のルータ内でのソフトウェア定義ネットワーク間のルーティング情報を伝播するために、 ACI はマルチプロトコル Border Gateway Protocol (MP-BGP) を使用します。

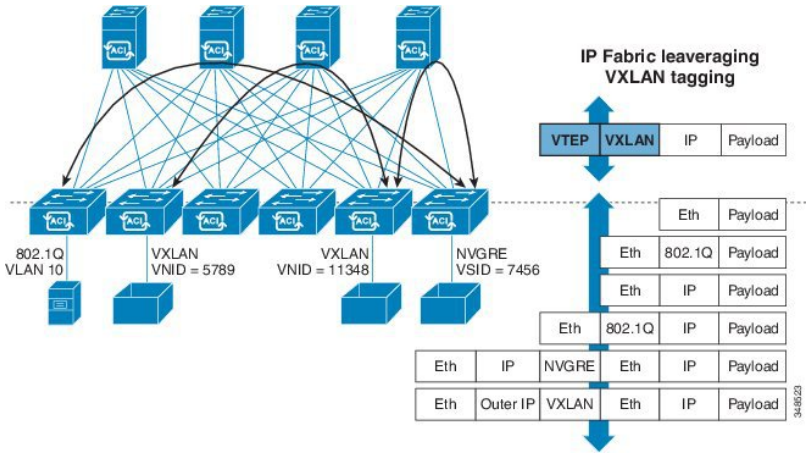
ACI で VXLAN

VXLAN は、レイヤ 2 オーバーレイの論理ネットワークを構築するレイヤ 3 のインフラストラクチャ上でレイヤ 2 のセグメントを拡張する業界標準プロトコルです。ACIインフラストラクチャ レイヤ 2 ドメインが隔離ブロードキャストと障害ブリッジ ドメインをオーバーレイ内に

存在します。このアプローチは大きすぎる、障害ドメインの作成のリスクなしで大きくなるデータセンター ネットワークを使用できます。

すべてのトラフィック、ACIファブリックはVXLANパケットとして正規化されます。入力でACI VXLANパケットで外部VLAN、VXLAN、およびNVGREパケットをカプセル化します。次の図は、ACIカプセル化の正規化を示します。

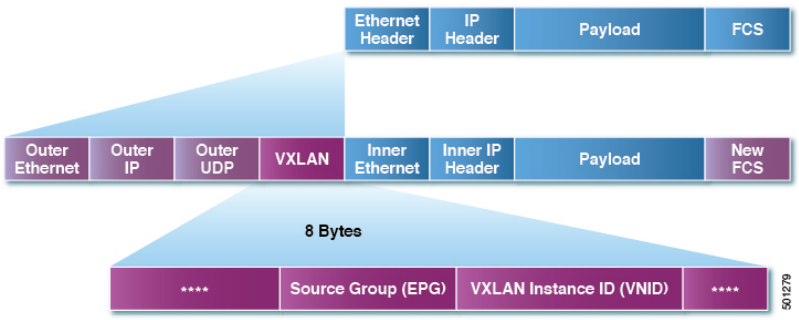
図 *2 : ACI* カプセル化の正規化



ACI ファブリックでの転送は、カプセル化のタイプまたはカプセル化のオーバーレイ ネットワークによって制限または制約されません。ACI ブリッジ ドメインのフォワーディング ポリシーは、必要な場合に標準の VLAN 動作を提供するために定義できます。

ファブリック内のすべてのパケットにACIポリシー属性が含まれているため、ACIは完全に分散された方法でポリシーを一貫して適用できます。ACIにより、アプリケーション ポリシーのEPG IDが転送から分離されます。次の図に示すように、ACI VXLANヘッダーは、ファブリック内のアプリケーション ポリシーを特定します。

図 *3 : ACI VXLAN* のパケット形式



ACIVXLAN パケットには、レイヤ 2 の MAC アドレスとレイヤ 3 IP アドレスの送信元と宛先フィールド、ファブリック内の効率的なと拡張性の転送を有効にします。ACIVXLAN パケット ヘッダーの送信元グループ フィールドは、パケットが属するアプリケーション ポリシー エンドポイント グループ (EPG) を特定します。VXLAN インスタンス ID (VNID) は、テナントの仮想ルーティングおよび転送 (VRF) ドメイン ファブリック内で、パケットの転送を有効にします。VXLAN ヘッダーで 24 ビット VNID フィールドでは、同じネットワークで一意レイヤ 2

のセグメントを最大 16 個の拡張アドレス空間を提供します。この拡張アドレス空間は、大規模なマルチテナント データセンターを構築する柔軟性 IT 部門とクラウド プロバイダーを提供します。

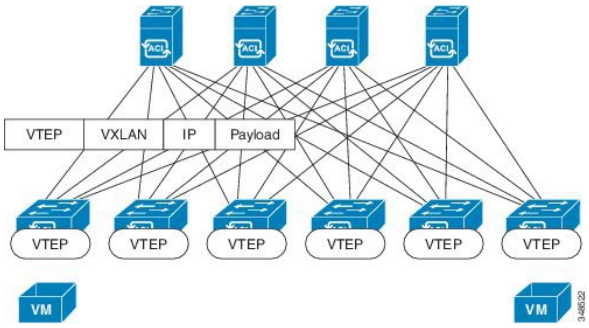
VXLAN を有効に ACI ファブリック全体にわたってスケールでの仮想ネットワーク インフラストラクチャのレイヤ 3 のアンダーレイ レイヤ 2 を展開します。アプリケーション エンドポイント ホスト柔軟に配置できます、アンダーレイ インフラストラクチャのレイヤ 3 バウンダリのリスクなしでデータセンター ネットワーク間をオーバーレイ ネットワーク、VXLAN でレイヤ 2 の隣接関係を維持します。

サブネット間のテナント トラフィックの転送を促進するレイヤ3VNID

ACI ファブリックは、ACI ファブリック VXLAN ネットワーク間のルーティングを実行するテナントのデフォルト ゲートウェイ機能を備えています。各テナントに対して、ファブリックはテナントに割り当てられたすべてのリーフ スイッチにまたがる仮想デフォルト ゲートウェイを提供します。これは、エンドポイントに接続された最初のリーフ スイッチの入力インターフェイスで提供されます。各入力インターフェイスはデフォルト ゲートウェイ インターフェイスをサポートします。ファブリック全体のすべての入力インターフェイスは、特定のテナント サブネットに対して同一のルータの IP アドレスと MAC アドレスを共有します。

ACI ファブリックは、エンドポイントのロケータまたは VXLAN トンネル エンドポイント (VTEP) アドレスで定義された場所から、テナント エンドポイント アドレスとその識別子を切り離します。ファブリック内の転送は VTEP 間で行われます。次の図は、ACI で切り離された ID と場所を示します。

図 *4: ACI* によって切り離された *ID* と場所



VXLAN は VTEP デバイスを使用してテナントのエンド デバイスを VXLAN セグメントにマッピングし、VXLAN のカプセル化およびカプセル化解除を実行します。各 VTEP 機能には、次の 2 つのインターフェイスがあります。

- ブリッジングを介したローカル エンドポイント通信をサポートするローカル LAN セグメントのスイッチ インターフェイス
- 転送 IP ネットワークへの IP インターフェイス

IP インターフェイスには一意の IP アドレスがあります。これは、インフラストラクチャ VLAN として知られる、転送 IP ネットワーク上の VTEP を識別します。VTEP デバイスはこの IP ア

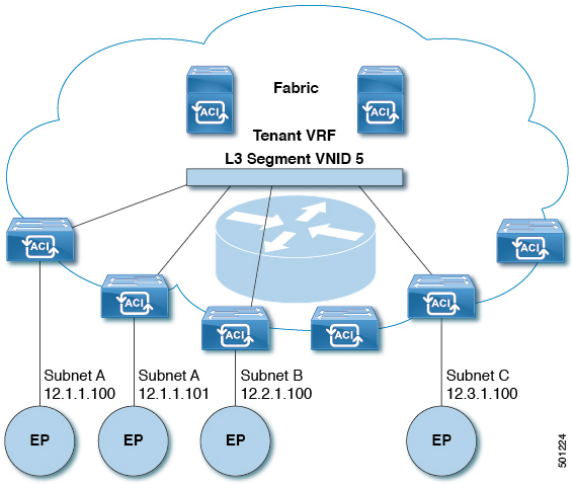
ドレスを使用してイーサネット フレームをカプセル化し、カプセル化されたパケットを、IP インターフェイスを介して転送ネットワークへ送信します。また、VTEP デバイスはリモート VTEP で VXLAN セグメントを検出し、IP インターフェイスを介してリモートの MAC Address-to-VTEP マッピングについて学習します。

ACI の VTEP は分散マッピング データベースを使用して、内部テナントの MAC アドレスまたはIPアドレスを特定の場所にマッピングします。VTEPはルックアップの完了後に、宛先リーフ スイッチ上の VTEP を宛先アドレスとして、VXLAN 内でカプセル化された元のデータ パケットを送信します。宛先リーフ スイッチはパケットをカプセル化解除して受信ホストに送信します。このモデルにより、ACI はスパニングツリー プロトコルを使用することなく、フル メッシュでシングル ホップのループフリー トポロジを使用してループを回避します。

VXLAN セグメントは基盤となるネットワーク トポロジに依存しません。逆に、VTEP 間の基盤となる IP ネットワークは、VXLAN オーバーレイに依存しません。これは発信元 IP アドレスとして開始 VTEP を持ち、宛先 IP アドレスとして終端 VTEP を持っており、外部 IP アドレス ヘッダーに基づいてパケットをカプセル化します。

次の図は、テナント内のルーティングがどのように行われるかを示します。

図 *5 : ACI* のサブネット間のテナント トラフィックを転送するレイヤ *3 VNID*



ACI はファブリックの各テナント VRF に単一の L3 VNID を割り当てます。ACI は、L3 VNID に従ってファブリック全体にトラフィックを転送します。出力リーフ スイッチでは、ACI によって L3 VNID からのパケットが出力サブネットの VNID にルーティングされます。

ACI のファブリック デフォルト ゲートウェイに送信されてファブリック入力に到達したトラフィックは、レイヤ 3 VNID にルーティングされます。これにより、テナント内でルーティングされるトラフィックはファブリックで非常に効率的に転送されます。このモデルを使用すると、たとえば同じ物理ホスト上の同じテナントに属し、サブネットが異なる 2 つの VM 間では、トラフィックが (最小パス コストを使用して) 正しい宛先にルーティングされる際に経由する必要があるは入力スイッチ インターフェイスのみです。

ACIルート リフレクタは、ファブリック内での外部ルートの配布にマルチプロトコル BGP（MP-BGP）を使用します。ファブリック管理者は自律システム (AS) 番号を提供し、ルート リフレクタにするスパイン スイッチを指定します。

WAN およびその他の外部ネットワーク

ネットワーク ドメイン

ファブリック管理者は、ポート、プロトコル、VLANプール、およびカプセル化を設定するドメインポリシーを作成します。これらのポリシーは、単一テナント専用にすることも、共有することもできます。ファブリック管理者がACIファブリック内にドメインを設定すると、テナント管理者はテナント エンドポイント グループ（EPG）をドメインに関連付けることができます。

以下のネットワーク ドメイン プロファイルを設定できます。

- VMM ドメイン プロファイル（vmmDomP）は、仮想マシンのハイパーバイザ統合のために必要です。
- 物理ドメイン プロファイル（physDomP）は、ベア メタル サーバ接続と管理アクセスに使用します。
- ブリッジド外部ネットワーク ドメイン プロファイル（l2extDomP）は通常、ACI ファブリックのリーフ スイッチにブリッジド外部ネットワーク トランク スイッチを接続するために使用されます。
- ルーテッド外部ネットワーク ドメイン プロファイル（l3extDomP）は、ACI ファブリックのリーフ スイッチにルータを接続するために使用されます。
- ファイバチャネル ドメインプロファイル(fcDomP)は、ファイバチャネルのVLANとVSANを接続するために使用されます。

ドメインはVLANプールに関連付けられるように設定されます。その後、EPGは、ドメインに関連付けられているVLANを使用するように設定されます。

（注） EPGポートとVLANの設定は、EPGが関連付けられているドメイン インフラストラクチャ設定で指定されている設定に一致する必要があります。一致しない場合、APIC でエラーが発生します。そのようなエラーが発生した場合は、ドメインインフラストラクチャ設定がEPGポートとVLANの設定に一致していることを確認してください。

ルート リフレクタの設定

ACIファブリックのルートリフレクタは、マルチプロトコルBGP（MP-BGP）を使用してファブリック内に外部ルートを配布します。ACIファブリックでルートリフレクタをイネーブルにするには、ファブリックの管理者がルート リフレクタになるスパイン スイッチを選択して、自律システム（AS）番号を提供する必要があります。ルート リフレクタがACI ファブリック

でイネーブルになると、管理者は次の項で説明するように、外部ネットワークへの接続を設定できます。

ACI ファブリックに外部ルータを接続するには、ファブリック インフラストラクチャの管理者がボーダー ゲートウェイ プロトコル（BGP）のルート リフレクタとしてスパイン ノードを設定します。冗長性のために、複数のスパインがルータ リフレクタ ノードとして設定されます（1 台のプライマリ リフレクタと 1 台のセカンダリ リフレクタ）。

テナントが ACI ファブリックに WAN ルータを接続する必要がある場合は、インフラストラクチャの管理者が WAN ルータが WAN のトップ オブ ラック（ToR）として接続されるリーフ ノードを（以下の通りに）設定し、この WAN ToR を BGP ピアとしてルート リフレクタ ノードの 1 つと組み合わせます。ルート リフレクタが WAN ToR に設定されていると、ファブリックにテナント ルートをアドバタイズできます。

各リーフ ノードには最大 4000 のルートを保存できます。WAN ルータが 4000 を超えるルートをアドバタイズしなければならない場合、複数のリーフ ノードとピアリングする必要があります。インフラストラクチャの管理者は、ペアになったリーフ ノードそれぞれをアドバタイズできるルート（またはルート プレフィクス）で設定します。

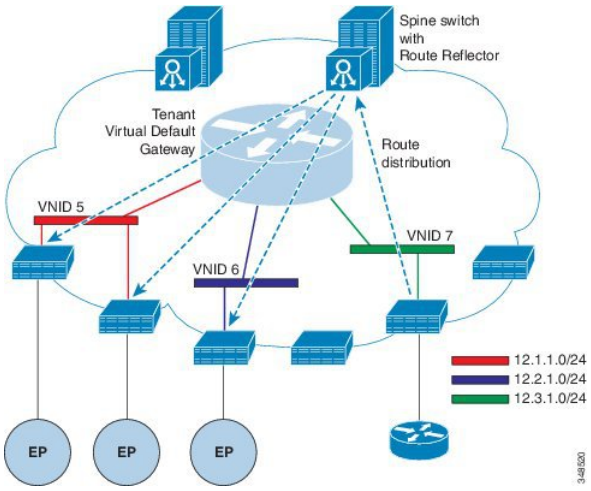
インフラストラクチャの管理者は、次のようにファブリックに接続されている外部 WAN ルータを設定する必要があります。

1. ルート リフレクタとして最大 2 つのスパイン ノードを設定します。冗長性のために、プライマリおよびセカンダリ ルート リフレクタを設定します。
2. WAN ToR で、プライマリおよびセカンダリ ルート リフレクタのノードを設定します。
3. WAN ToR で、ToR がアドバタイズを担当するルートを設定します。これは任意で、テナント ルータが 4000 を超えるルートをアドバタイズすることがわかっている場合にのみ行う必要があります。

ルータ ピアリングおよびルート配布

次の図に示すように、ルーティング ピア モデルを使用すると、リーフ スイッチ インターフェイスが外部ルータのルーティング プロトコルとピアリングするように静的に設定されます。

図 *6:* ルータのピアリング



ピアリングによって学習されるルートは、スパイン スイッチに送信されます。スパイン スイッチはルート リフレクタとして動作し、外部ルートを同じテナントに属するインターフェイスを持つすべてのリーフ スイッチに配布します。これらのルートは、最長プレフィクス照合 (LPM) により集約されたアドレスで、外部ルータが接続されているリモートのリーフ スイッチの VTEP IP アドレスが含まれるリーフ スイッチの転送テーブルに配置されます。WAN ルートには転送プロキシはありません。WAN ルートがリーフ スイッチの転送テーブルに適合しない場合、トラフィックはドロップされます。外部ルータがデフォルト ゲートウェイではないため、テナントのエンドポイント (EP) からのパケットは ACI ファブリックのデフォルト ゲートウェイに送信されます。

ルートのインポートとエクスポート、ルート集約、ルート コミュニティの一致

サブネット ルートのエクスポートまたはインポート設定オプションは、次に説明するスコープおよび集約オプションに従って指定できます。

ルーティング対象サブネットについては、以下のスコープ オプションが使用可能です。

- エクスポート ルート制御サブネット：エクスポート ルート方向を制御します。
- インポート ルート制御サブネット：インポート ルート方向を制御します。

（注） インポート ルート コントロールは、BGP と、OSPF が EIGRP ではなく、サポートされています。

- 外部 EPG (セキュリティ インポート サブネット) の外部サブネット: 指定する外部サブネットが外部ネットワークの特定のインスタンスのプロファイルの一部として適用される契約を保持 (`l3extInstP`)。[サブネットの `l3extInstP` 外部 EPG として分類、サブネット上の範囲を「インポートセキュリティ」に設定する必要があります。この範囲のサブネット

を決定する IP アドレスが関連付けられています、 `l3extInstP` 。これが決定されると、契約は、他のどのEpgでその外部のサブネットが通信を許可を決定します。たとえば、トラフィックが入力した場合、ACIスイッチはレイヤ3外部の外部ネットワークに(`L3extOut`) に関連付けられている送信元IPアドレスを判断する場合は、参照、 `l3extInstP` 。このアクションより一般的なサブネット上で複数の特定のサブネットが優先されるようにで最長プレフィックス一致 (ほか) に基づいて行われます。

- 共有ルート制御サブネット — 共有サービス設定においては、この特性が有効になっているサブネットだけが、コンシューマ EPG の Virtual Routing and Forwarding （VRF）にインポートされます。これは VRF 間の共有サービスのルート方向を制御します。
- 共有セキュリティ インポート サブネット：インポート対象サブネットに共有コントラクトを適用します。デフォルトの仕様では、外部 EPG 用外部サブネットが設定されています。

ルート対象サブネットを集約することができます。集約が設定されていない場合は、サブネットが正確に照合されます。たとえば、サブネットが 11.1.0.0/16 の場合、11.1.1.0/24 ルートにはポリシーが適用されず、ルートが11.1.0.0/16である場合のみ適用されます。すべてのサブネットを1つずつ定義する作業は面倒でエラーが発生しやすいので、それを回避するために、サブネットのセットを1つのエクスポート、インポートまたは共有ルートポリシーに集約することができます。現時点では、0/0サブネットのみ集約可能です。0/0に集約を指定すると、次の選択オプションに基づき、すべてのルートがインポート、エクスポートされ、異なる VRF と共有されます:

- 集約エクスポート — VRF (サブネット 0/0) のすべての中継ルートをエクスポートします。
- 集約インポート — 所定の L3 ピア (サブネット 0/0) のすべて着信ルートをインポートします。

（注） BGP、OSPF が EIGRP の集約インポート ルート制御はサポートされます。

- 集約共有ルート — 1 つの VRF で学習されているルートを別の VRF にアドバタイズする必要がある場合、サブネットとの正確な一致、またはサブネットマスクに従った方法で共有できます。集約共有ルートでは、複数のサブネットマスクを使用して、どの特定のルートグループを VRF 間で共有するかを決定できます。たとえば、10.1.0.0/16 と 12.1.0.0/16 を指定してこれらのサブネットを集約することができます。あるいは、0/0 を使用すると、複数の VRF のすべてのサブネット ルートを共有できます。

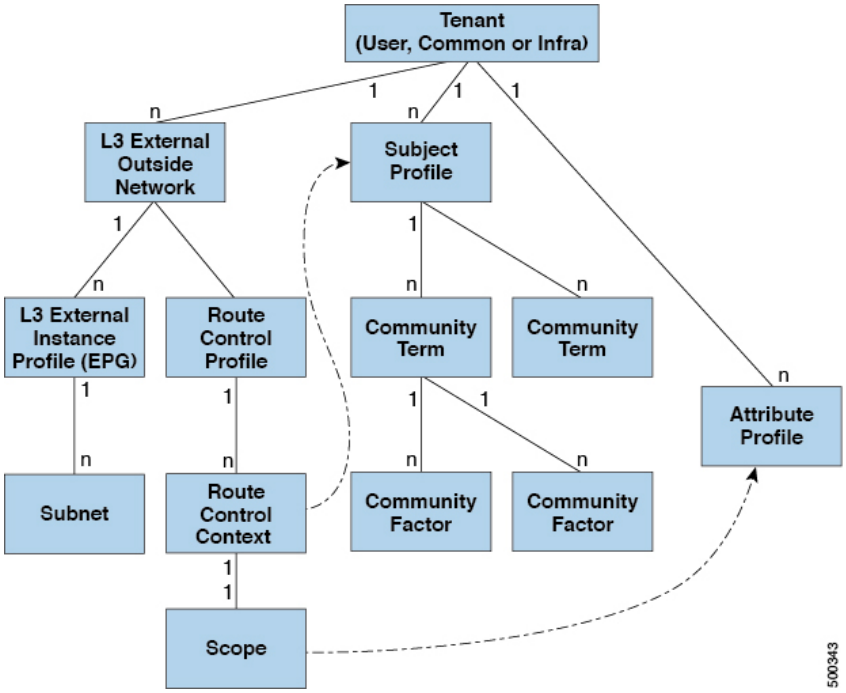
（注） 第 2 世代のスイッチの VRF 機能間で正常にルートが共有されます（N9K-93108TC-EX など、スイッチ モデル名の最後やその後に「EX」や「FX」がつく Cisco Nexus N9K）。第 1 世代のスイッチですが、ルートを保存する物理的な 3 進コンテンツ対応メモリ（TCAM）にルートの解析を完全にサポートするだけの容量がないため、この設定のパケットは失敗する可能性があります。

ルート集約では、多数の具体的なアドレスを1つのアドレスに置き換えることで、ルートテーブルが簡素化します。たとえば、10.1.1.0/24、10.1.2.0/24、10.1.3.0/24 は 10.1.0.0/16 に置き換えられます。ルート集約ポリシーにより、ボーダー リーフ スイッチとそのネイバー リーフ スイッチの間でルートを効率的に共有することができます。BGP、OSPF、あるいはEIGRPのルート集約ポリシーは、ブリッジ ドメインまたは中継サブネットに適用されます。OSPF では、エリア間ルート集約と外部ルート集約がサポートされます。集約ルートはエクスポートされます。ファブリック内でのアドバタイズは行われません。上記の例では、ルート集約ポリシーが適用され、EPG が 10.1.0.0/16 サブネットを使用している場合、10.1.0.0/16 の範囲全体がすべての隣接リーフ スイッチと共有されます。

（注） 同じリーフ スイッチで 2 つの `L3extOut` ポリシーに OSPF を設定している場合（1 つはレギュラーで、もう 1 つはバックボーン）には、VRF内の全エリアに集約が適用されるため、一方の `L3extOut` で設定されているルート集約ポリシーが両方の L3extOut ポリシーに適用されます。

次の図に示すように、ルート制御プロファイルは、プレフィックス ベースおよびコミュニティ ベースの一致に基づいて、ルート マップを取得します。

図 *7:* ルート コミュニティ マッチング



ルート制御プロファイル（`rtctrtlProfile`）は、許可される対象を指定します。ルート制御コンテキストは一致対象を指定し、スコープは設定すべき対象を指定します。サブジェクトプロファイルには、コミュニティ マッチの仕様が含まれます。これは複数の `l3extOut`で使用できます。サブジェクト プロファイル（`SubjP`）には、それぞれ 1 つまたは複数のコミュニティ ファクタ（コミュニティ）を含む複数のコミュニティ タームを含めることができます。これにより、次のブール演算を指定することができます。

- 複数コミュニティ ターム間の論理的 OR
- 複数コミュニティ ターム間の論理的 AND

たとえば、北東と呼ばれるコミュニティタームに、それぞれ多くのルートを含む複数のコミュニティが含まれているとします。また、南東という別のコミュニティタームにも、さまざまなルートが多数含まれているとします。管理者は、そのどちらかあるいは両方を一致させることを選択できます。コミュニティファクタタイプには、レギュラーまたは拡張を使用できます。拡張タイプのコミュニティファクタを使用する際には、仕様間の重複がないよう注意することが必要です。

ルート制御プロファイルのスコープ部分は、属性プロファイル（rtctrlAttrP）を参照して、適用すべき設定-アクション（プリファレンス、ネクスト ホップ、コミュニティなど）を指定します。ルートを l3extOut から学習した場合は、ルートの属性を変更できます。

上の図は、l3extOut に rtctrtlProfile が含まれているケースを示しています。rtctrtlProfile はテナントの下にも配置できます。この例では、l3extOut に、自身をテナント下の rtctrtlProfile と関連付ける相互リーク関係ポリシー（L3extRsInterleakPol）が設定されています。この設定により、再利用、 rtctrtlProfile 複数の l3extOut 接続します。BGP 属性 (BGP は、ファブリック内で使用される) は、それを OSPF からは、ファブリックを学習ルートの追跡することもできます。L3extOut 下で定義された rtctrtlProfile の優先順位は、テナント下で定義されたものよりも高くなります。

rtctrtlProfile には、組み合わせ可能およびグローバルという 2 つのモードがあります。デフォルトの組み合わせ可能モードでは、パーベイシブ サブネット（fvSubnet）および外部サブネット（l3extSubnet）に一致/設定メカニズムを組み合わせてルート マップをレンダリングします。グローバルモードはテナント内のすべてのサブネットに適用され、そのほかのポリシー属性の設定が無効になります。グローバル rtctrtlProfile では、明示的な（0/0）サブネットを定義しなくても、すべての動作が許可されます。グローバル rtctrtlProfile は、コミュニティやネクストホップといった異なるサブネット属性を使用してマッチングが行われる非プレフィックス ベースの一致ルールと一緒に使用されます。1 つのテナント下で複数の rtctrtlProfile ポリシーを設定できます。

rtctrtlProfile ポリシーによって、デフォルト インポートおよびデフォルト エクスポートのルート制御の拡張が可能になります。集約インポートあるいはエクスポートルートを伴う Layer 3 Outside ネットワークには、サポート対象デフォルト エクスポート/デフォルト インポートおよびサポート対象 0/0 集約ポリシーを指定するインポート/エクスポート ポリシーを設定できます。すべてのルート（着信または発信）に rtctrtlProfile ポリシーを適用するには、一致ルールのないグローバル デフォルト rtctrtlProfile を定義します。

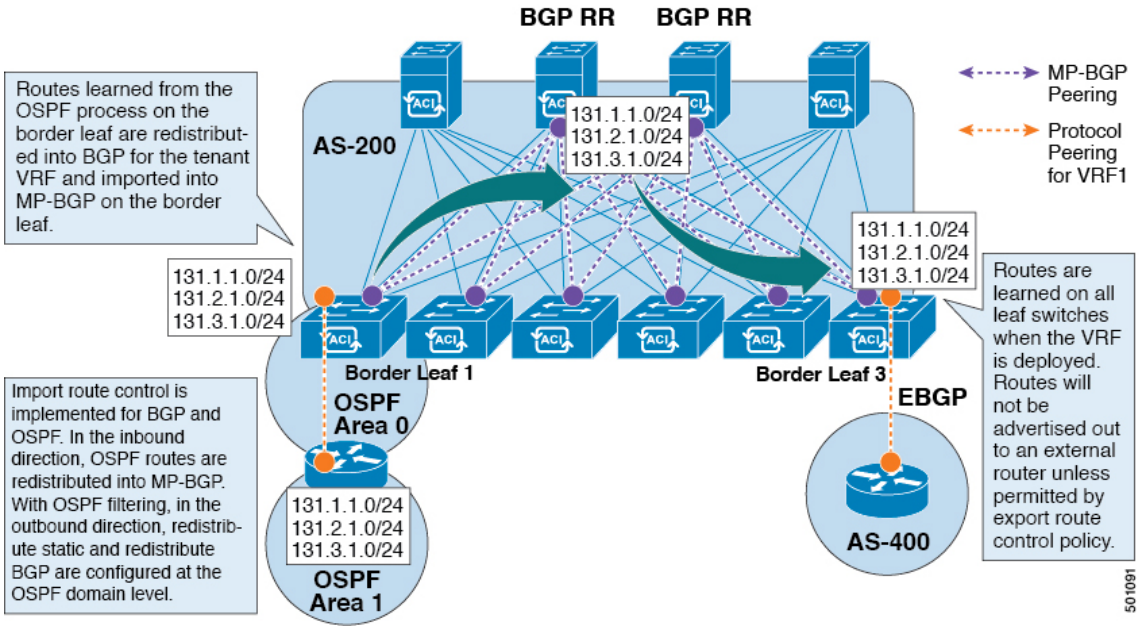
（注） 1 つのスイッチ上で複数の l3extOut 接続を設定することは可能ですが、スイッチは 1 つのルートマップしか持つことができないため、スイッチで設定されているすべてのレイヤ 3 外側ネットワークが同じ rtctrtlProfile を使用する必要があります。

プロトコル相互リークと再配布ポリシーは、ACI ファブリック BGP ルートで共有される外部学習ルートを制御します。設定属性はサポートされています。これらのポリシーは L3extOut

単位、ノード単位、VRF 単位でサポートされます。相互リークポリシーは、`L3extOut` 内のルーティングプロトコルによって学習されたルートに適用されます。現在のところ、相互リークと再配布ポリシーは、OSPF v2 および v3 でサポートされています。ルート制御ポリシー `rtctrtlProfile` は、相互リーク ポリシーによって消費される場合、グローバルとして定義する必要があります。

ACI のルート再配布

図 *8 : ACI* のルート再配布



- 境界リーフの OSPF プロセスで学習されたルートは、テナント VRF 用に BGP に再配布され、それらは境界リーフの MP-BGP にインポートされます。
- インポート ルート制御は、BGP および OSPF ではサポートされていますが、EIGRP ではサポートされていません。
- エクスポート ルート制御は、OSPF、BGP、および EIGRP でサポートされています。
- ルートは、VRF が導入されている境界リーフで学習されます。ルートは、エクスポートルート制御で許可されていない限り、外部レイヤ 3 Outside 接続にアドバタイズされません。

（注） ブリッジ ドメイン/EPG のサブネットが [Advertise Externally] に設定されている場合、サブネットは境界リーフの静的ルートとしてプログラムされます。スタティック ルートがアドバタイズされると、ルーティング プロトコルに直接注入されない外部ネットワークとして EPG のレイヤ 3 ネットワーク ルーティング プロトコルに再配布されます。

ACI ファブリック内のルート配布

ACI は以下のルーティング メカニズムをサポートします。

- スタティック ルート
- OSPFv2（IPv4）
- OSPFv3（IPv6）
- iBGP
- eBGP（IPv4 および IPv6）
- EIGRP (IPv4 および IPv6) プロトコル

ACI は、外部ルータに接続する際に VRF-Lite の実装をサポートします。サブインターフェイスを使用して、境界リーフは 1 つの物理インターフェイスを持つ複数のテナントへのレイヤ 3 Outside 接続を提供できます。VRF-Lite の実装では、テナントごとに 1 つのプロトコル セッションが必要です。

ACI ファブリック内の外部ルートを伝播するために、ACI ファブリック内のリーフ スイッチとスパイン スイッチの間に Multiprotocol BGP（MP-BGP）が実装されています。単一ファブリック内で多数のリーフ スイッチをサポートするために、BGP ルート リフレクタ テクノロジーが導入されています。リーフ スイッチとスパイン スイッチはすべて 1 つの BGP 自律システム（AS）内にあります。境界リーフが外部ルートを学習すると、MP-BGP アドレス ファミリ VPN バージョン 4 または VPN バージョン 6 に特定の VRF の外部ルートを再配布できます。アドレス ファミリ VPN バージョン 4 を使用して、MP-BGP は VRF ごとに別の BGP ルーティング テーブルを維持します。MP-BGP 内で、境界リーフは BGP ルート リフレクタであるスパイン スイッチにルートをアドバタイズします。その後、ルートは VRF（APIC GUI の用語ではプライベート ネットワーク）がインスタンス化されているすべてのリーフに伝播されます。

外部レイヤ 3 Outside 接続タイプ

ACI は、以下の外部レイヤ 3 Outside 接続オプションをサポートします。

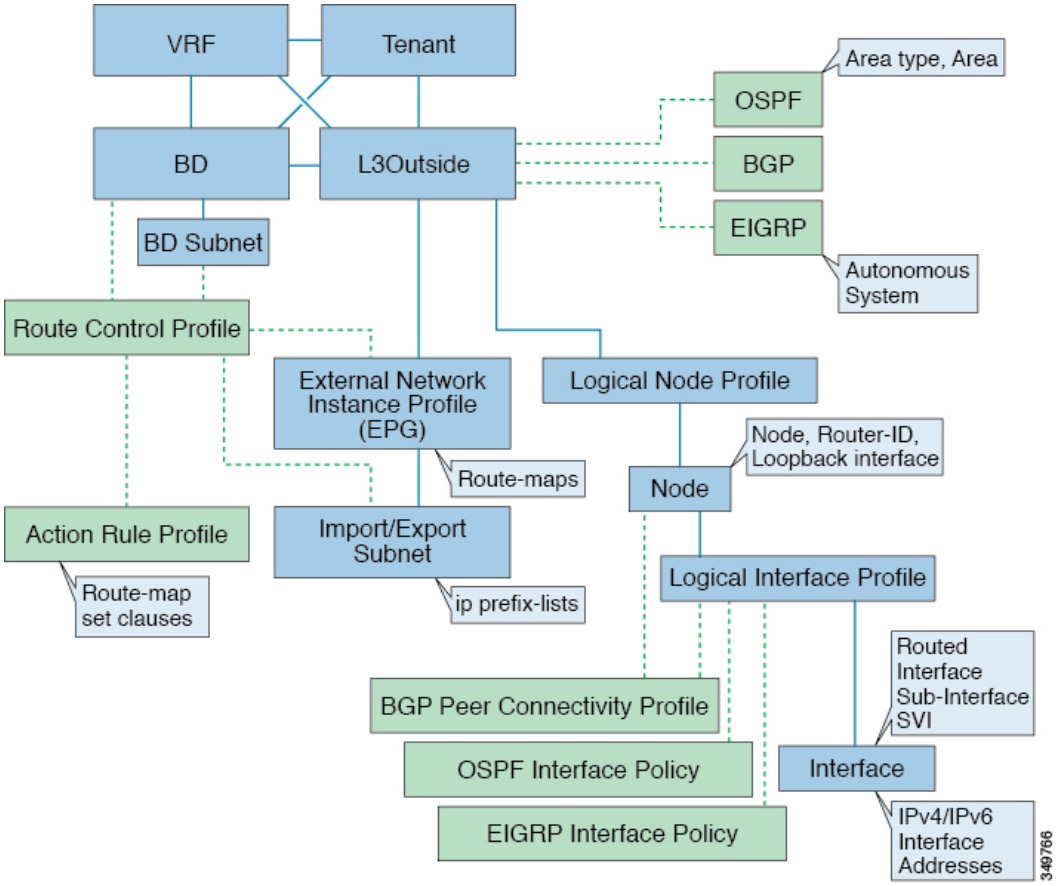
- スタティック ルーティング（IPv4 および IPv6 でサポート）
- 標準および NSSA エリアの OSPFv2（IPv4）
- 標準および NSSA エリアの OSPFv3（IPv6）
- iBGP（IPv4 および IPv6）
- eBGP（IPv4 および IPv6）
- BGP（IPv4 および IPv6）

外部レイヤ 3 Outside 接続は、以下のインターフェイスでサポートされます。

- レイヤ 3 ルーテッド インターフェイス

- 802.1Q タギング対応のサブインターフェイス：サブインターフェイスを使用すると、複数のプライベート ネットワークに対するレイヤ 2 外部接続を提供できます。
- スイッチ仮想インターフェイス（SVI）：SVI インターフェイスを使用すると、レイヤ 2 とレイヤ 3 をサポートする同じ物理インターフェイスをレイヤ 2 外部接続とレイヤ 3 外部接続に使用できます。

図 *9: ACI* レイヤ *3* 管理対象オブジェクト



L3Outside 接続に使用される管理対象オブジェクトは、次のとおりです。

- 外部レイヤ 3 Outside（L3ext）：ルーティング プロトコル オプション（OSPF エリア タイプ、エリア、EIGRP AS、BGP）、プライベート ネットワーク、外部物理ドメイン。
- 論理ノード プロファイル：外部レイヤ 3 Outside 接続に対して 1 つ以上のノードが定義されたプロファイル。ルータ ID とループバック インターフェイス設定はプロファイルで定義されます。

（注） 複数の外部レイヤ 3 Outside 接続間の同じノードには同じルータ ID を使用してください。

（注） 単一の L3Out 内では、ノードは、1 つの論理ノード プロファイルの一部でのみあり得ます。単一の L3Out 内に複数の論理ノード プロファイルの一部であるノードを構成すると、1 つの論理ノード プロファイルからループバック アドレスがプッシュされるものの、他方からはそうならないなど、予測できない動作が生じる可能性があります。既存の論理インターフェイス プロファイルの下の追加パスのバインディングを使用します。または、既存の論理ノードのプロファイルの下に新しい論理インターフェイス プロファイルを作成してください。

- 論理インターフェイス プロファイル：IPv4 および IPv6 インターフェイスの IP インターフェイス設定。これは、ルート 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、物理ポート、ポート チャネルまたは VPC で設定できます。
- OSPF インターフェイス ポリシー：OSPF のネットワーク タイプ、優先順位などの詳細が含まれています。
- EIGRP インターフェイス ポリシー：タイマー、スプリット ホライズン タイマーなどの詳細が含まれています。
- BGP ピア接続プロファイル：ほとんどの BGP ピア設定、リモート AS、ローカル AS、および BGP ピア接続オプションが設定されるプロファイル。BGP ピア接続プロファイルは、ノード プロファイルの下の論理インターフェイス プロファイルまたはループバック インターフェイスに関連付けることができます。これは、BGP ピアリング セッションの update-source 設定を決定します。
- 外部ネットワーク インスタンス プロファイル（EPG）（l3extInstP）：外部 EPG はプレフィックス ベースの EPG または InstP とも呼ばれます。インポートおよびエクスポートのルート制御ポリシー、セキュリティ インポート ポリシー、およびコントラクトの関連付けは、このプロファイルで定義されます。単一 L3Out に複数の外部 EPG を設定できます。単一外部レイヤ 3 Outside 接続で別のルートまたはセキュリティ ポリシーが定義されている場合、複数の外部 EPG を使用できます。1 つの外部 EPG または複数の外部 EGP がルート マップにまとめられます。外部 EPG で定義されるインポート/エクスポート サブネットは、ルート マップの IP プレフィックス リストの match 句と関連しています。外部 EPG は、インポート セキュリティ サブネットとコントラクトが関連付けられる場所でもあります。これは、この L3out のトラフィックの許可またはドロップに使用されます。
- アクション ルール プロファイル：アクション ルール プロファイルは、L3Out のルート マップの set 句を定義するために使用されます。サポートされる set 句は、BGP communities（standard および extended）、Tags、Preference、Metric、および Metric type です。
- ルート制御プロファイル：ルート制御プロファイルは、アクション ルール プロファイルを参照するために使用されます。これは、アクション ルール プロファイルの順序付きプロファイルにすることができます。ルート制御プロファイルは、テナント BD、BD サブネット、外部 EPG、または外部 EPG サブネットで参照できます。

BGP、OSPF、およびEIGRP L3Out用の追加のプロトコル設定が存在します。これらの設定は、GUI の [ACI Protocol Policies] セクションでテナントごとに設定されます。

（注） 外部 EPG (中継ルーティング ケース) の間でポリシーの適用を設定する際には、エクスポートルート制御、集約エクスポート、および外部のセキュリティのために、デフォルトプレフィックスである 0/0 で 2 番目の外部 EPG (InstP) を設定する必要があります。さらに、優先グループを除外し、中継 InstPs 間では任意の契約 (または適切な契約) を使用する必要があります。

レイヤ 3 外部接続の設定のモードについて

APIC は設定のための複数のユーザ インターフェイス (UI) をサポートしているので、1 つの UI を使用して設定を作成し、その後、別の UI を使用して設定を変更する場合は、予期しないインタラクションが潜んでいます。ここでは、さらに他の APIC のユーザ インターフェイスを使用した可能性がある場合、APIC NX-OS スタイルの CLI を使用してレイヤ 3 外部接続を設定するための考慮事項を説明します。

APIC NX-OS スタイルの CLI を使用してレイヤ 3 外部接続を設定する場合、次の 2 つのモードを選択することができます。

- よりシンプルな暗黙 モードは、APIC GUI または REST API と互換性がありません。
- 名前付き（または明示) モードは、APIC GUI および REST API と互換性があります。

いずれの場合も、設定は互換性がない UI では読み取り専用であると考えてください。

モードの違いについて

どちらのモードでも、構成設定は API の **l3extOut** クラスのインスタンスである内部コンテナ オブジェクト「L3 Outside」（または「L3Out」）内で定義されます。2 つのモード間の主な違いは、このコンテナ オブジェクト インスタンスの命名にあります。

- 暗黙モード：コンテナのネーミングは潜在的であり、CLI コマンドには表示されません。CLI は、これらのオブジェクトを内部的に作成し保持します。
- 名前付きモード：名前はユーザーが決定します。名前付きモードの CLI コマンドには、追加の **l3Out** フィールドがあります。名前付き L3Out がを正常に設定され障害を回避するためには、ユーザーが外部レイヤ 3 用の API オブジェクト モデルを理解する必要があります。

（注） 「名前付きモードセクションを使用したレイヤ *3* 外部接続の設定」セクションの手順を除き、このガイドでは、暗黙モードの手順を説明します。

注意事項および制約事項

- 同じ APIC インターフェイスでは、両方のモードを、次の制限でレイヤ 3 外部接続を設定するために一緒に使用することができます。テナント VRF、およびリーフの特定の組み合わせのレイヤ 3 外部接続設定は、1 つのモードを介してのみ実行できます。
- 特定のテナント VRF の場合、外部 L3 EPG を配置できるポリシー ドメインは、名前付きモードまたは暗黙モードのいずれかになります。推奨する設定方式は、特定のテナント VRF が、レイヤ 3 外部接続用に展開されたすべてのノード全体で、特定のテナント VRF の組み合わせに対して 1 つのモードだけを使用することです。モードは、異なるテナントまたは異なる VRF 全体で変えることができ、制限は適用されません。
- 一部のケースで、ACI クラスタの着信設定が整合性を検証されます。次に例を示します。
- 外部レイヤ 3 機能は、次の例外を除いて、両方の設定モードでサポートされます
  - L4 ～ L7 サービス アプライアンスを使用したルーティング ピアリングとルート ヘルス インジェクション (RHI) は、名前付きモードでのみをサポートされます。名前付きモードは、ルーティング ピアリングが含まれるテナント VRF のすべての境界リーフ スイッチ全体で使用する必要があります。
- 暗黙モード CLI 手順を使用して作成されたレイヤ 3 外部ネットワーク オブジェクト（l3extOut）は、「__ui_」で始まる名前で識別され、GUI で読み取り専用としてマークされます。CLI は、インターフェイス、プロトコル、ルートマップ、EPG などの機能で、これらの外部 L3 ネットワークを分割します。REST API を介して実行される設定変更は、この構造を破棄することができ、CLI を介してさらなる変更を防ぐことができます。

このようなオブジェクトを削除する手順については、『*APIC Troubleshooting Guide*』の「*Troubleshooting Unwanted _ui_ Objects*」を参照してください。

L3Out ネットワーク インスタンス プロファイルで設定されているサブネットで有効な制御

L3Out ネットワーク インスタンス プロファイルで設定されているサブネットに対して以下の制御を有効にすることができます。

表 *17:* ルート制御オプション

ルート制御設定	使用目的	オプション
エクスポート ルート制御	ルートマップと IP プレフィクスリストを使用して、どの外部ネットワークがファブリックからアドバタイズされるかを制御します。IP プレフィックスリストは、定義されているサブネットごとに BL スイッチに作成されます。エクスポート制御ポリシーは、デフォルトで有効になっており、BGP、EIGRP、および OSPF でサポートされています。	特定の一致(プレフィックスとプレフィックス長)。
インポート ルート制御	ファブリックに許可されているサブネットを制御します。ルールを設定してルートをフィルタリングすることができます。BGP および OSPF ではサポートされますが、EIGRP ではサポートされません。サポートされていないプロトコルのインポート制御ポリシーを有効にすると、自動的に無視されます。インポート制御ポリシーは、デフォルトでは有効になっていませんが、**[Create Routed Outside]** パネルで有効にすることができます。**[Identity]** タブで、**[Route Control Enforcement: Import]** を有効にします。	特定の一致(プレフィックスとプレフィックス長)。
セキュリティ インポート サブネット	2 つのプレフィックス ベースの EPG 間をパケットが流れるようにするために使用されます。ACL で実装されます。	ACL のプレフィックスまたはワイルドカードによる一致ルールを使用します。
集約エクスポート	すべてのプレフィックスを外部ピアにアドバタイズできるようにするために使用されます。0.0.0.0/ le 32 IP プレフィックス リストで実装されます。	0.0.0.0/0 サブネット (すべてのプレフィックス) の場合にのみサポートされます。

ルート制御設定	使用目的	オプション
集約インポート	外部 BGP ピアからの着信であるすべてのプレフィックスを許可するために使用されます。0.0.0.0/0 le 32 IP プレフィックス リストで実装されます。	0.0.0.0/0 サブネット (すべてのプレフィックス) の場合にのみサポートされます。

L3Out接続からすべての中継ルートをアドバタイズすることをお勧めします。この場合、プレフィックス0.0.0.0/0の集約エクスポートオプションを使用します。この集約エクスポートオプションを使用すると、APIC システムがエクスポート ルート マップのマッチ句として使用する IP プレフィクス リスト エントリ (permit 0.0.0.0/0 le 30) が作成されます。出力を表示するには、**show route-map <outbound route-map>** および **show ip prefix-list <match-clause>** コマンドを使用します。

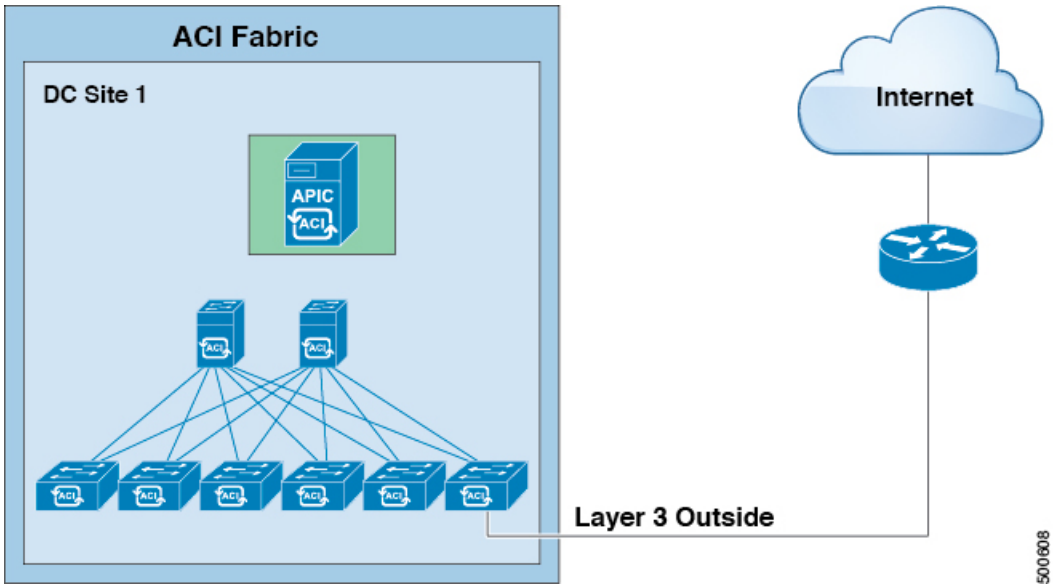
集約共有ルートを有効にすると、ある VRF で学習されたルートを別の VRF にアドバタイズする必要がある場合、サブネットを正確に一致させることでルートを共有するか、集約サブネットマスクを使用してルートを共有できます。複数のサブネットマスクを使用して、特定のルート グループを VRF 間で共有するかどうかを判断できます。たとえば、10.1.0.0/16 と 12.1.0.0/16 を指定してこれらのサブネットを集約することができます。あるいは、0/0 を使用すると、複数の VRF のすべてのサブネット ルートを共有できます。

（注） 第 2 世代のスイッチの VRF 機能間で正常にルートが共有されます（N9K-93108TC-EX など、スイッチ モデル名の最後やその後に「EX」や「FX」がつく Cisco Nexus N9K）。第 1 世代のスイッチですが、ルートを保存する物理的な 3 進コンテンツ対応メモリ（TCAM）にルートの解析を完全にサポートするだけの容量がないため、この設定のパケットは失敗する可能性があります。

ACI レイヤ 3 Outside ネットワークのワークフロー

このワークフローでは、レイヤ 3 Outside (L3Out) ネットワーク接続を設定するために必要なステップの概要を示します。

図 *10 :* レイヤ *3 Outside* ネットワーク接続



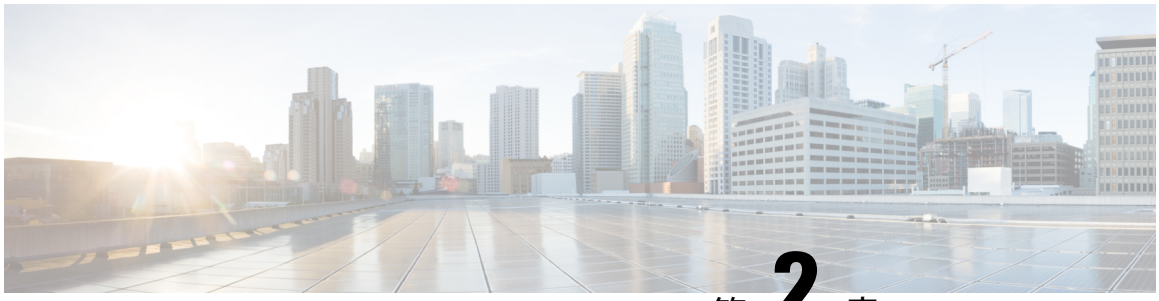
1. 前提条件

- インフラ セキュリティ ドメインに読み取り/書き込みアクセス権限があることを確認します。
- 必要なインターフェイスを持つターゲット リーフ スイッチが使用できることを確認します。

レイヤ 3 Outside ネットワークの設定

次の L3Outl シナリオのいずれかを選択します。

- 単一のテナント内で消費される L3Out について、BGP または OSPF の設定の指示に従います。
- 複数のテナント間で消費 (共有) される L3Out について、「共有レイヤ 3 Out」のガイドラインに従います。
- L3Out の中継ルーティング使用例については、ACI 中継ルーティング手順に従ってください。



第 2 章

レイヤ 3 ネットワーク設定の前提条件

この章の内容は、次のとおりです。

レイヤ 3 前提条件

このガイドのタスクを開始する前に、次のことを行ってください。

- ACI ファブリックと APIC コントローラがオンラインであり、APIC クラスタが形成され健全であることを確認します— 詳細については、*Cisco APIC Getting Started Guide, Release 2.x* を参照してください。
- レイヤ 3 ネットワークを構成する管理者のファブリック管理者アカウントが使用可能であることを確認します— 詳細については、*Cisco APIC Basic Configuration Guide* の *User Access, Authentication, and Accounting* および *Management* の章を参照してください。
- 目的のリーフ スイッチとスパイン スイッチ (必要なインターフェイスを使用可能) が使用可能であることを確認します— 詳細については、*Cisco APIC Getting Started Guide, Release 2.x* を参照してください。

  仮想スイッチのインストールと登録の詳細については、*Cisco ACI Virtualization Guide* を参照してください。
- レイヤ 3 ネットワークを消費するテナント、ブリッジドメイン、VRF、および EPG (アプリケーションプロファイルとコントラクトを含む) を設定します— 詳細については、*Cisco APIC Basic Configuration Guide* の *Basic User Tenant Configuration* の章を参照してください。
- NTP、DNS サービス、および DHCP リレー ポリシーを設定します— 詳細については、*Cisco APIC Basic Configuration Guide, Release 2.x* の *Provisioning Core ACI Fabric Services* の章を参照してください。

⚠

注意 ファブリックのリーフ スイッチとスパイン スイッチの間に 1 ギガビット イーサネット (GE) または 10GE リンクを設置すると、帯域幅が不十分なために、パケットが転送されずにドロップされる可能性があります。これを避けるためには、リーフ スイッチとスパイン スイッチの間で 40GE または 100GE リンクを使用してください。

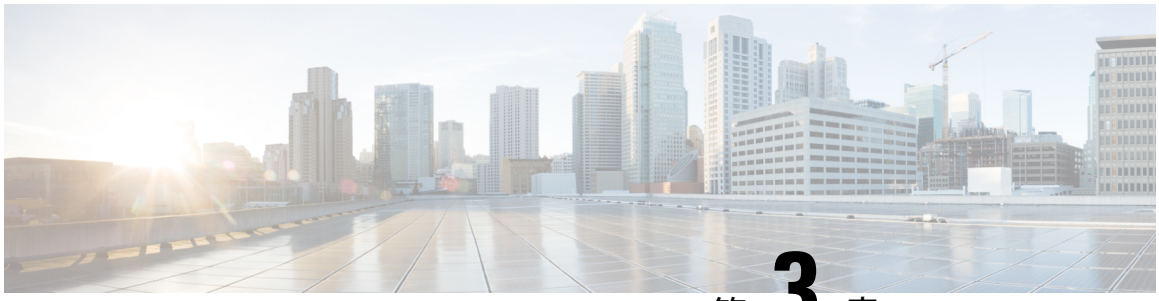
ブリッジ ドメインの設定

レイヤ 3 の設定 ブリッジ ドメイン ()] パネルのタブには次のパラメータを設定するには、管理者が使用できます。

- **ユニキャスト ルーティング** : この設定が有効になっているサブネット アドレスが設定されている場合は、ファブリックはデフォルト ゲートウェイの機能を提供して、トラフィックをルーティングします。ユニキャストルーティングもの有効化するように指示マッピング データベースをこのブリッジ ドメインのエンドポイントの IP-VTEP にマッピングを参照してください。IP ラーニングはブリッジ ドメインで設定されているサブネットを含むに依存ではありません。
- **サブネット アドレス** : このオプションは、ブリッジ ドメインの SVI IP アドレス (デフォルト ゲートウェイ) を設定します。
- **制限のサブネット IP ラーニング** : このオプションは、ユニキャスト リバース転送パス チェックに似ています。このオプションを選択すると、ファブリックはブリッジ ドメインに設定されている 1 以外のサブネットから IP アドレスを学習されません。

⚠

注意 有効化 **サブネットに制限 IP ラーニング** がブリッジ ドメイン内のトラフィックを停止します。



第 3 章

外部ネットワークへのルーテッド接続

この章の内容は、次のとおりです。

外部ネットワークへルートされた接続について

ネットワーク構成 (L3Out) 外部レイヤ 3 では、ファブリック以外のトラフィックを転送する方法を定義します。レイヤ 3 はし、他のノードのアドレスを見つける、ルートを選択して、サービスの品質を選択して、入力して、終了、およびファブリックを移動する際は、トラフィックを転送に使用されます。

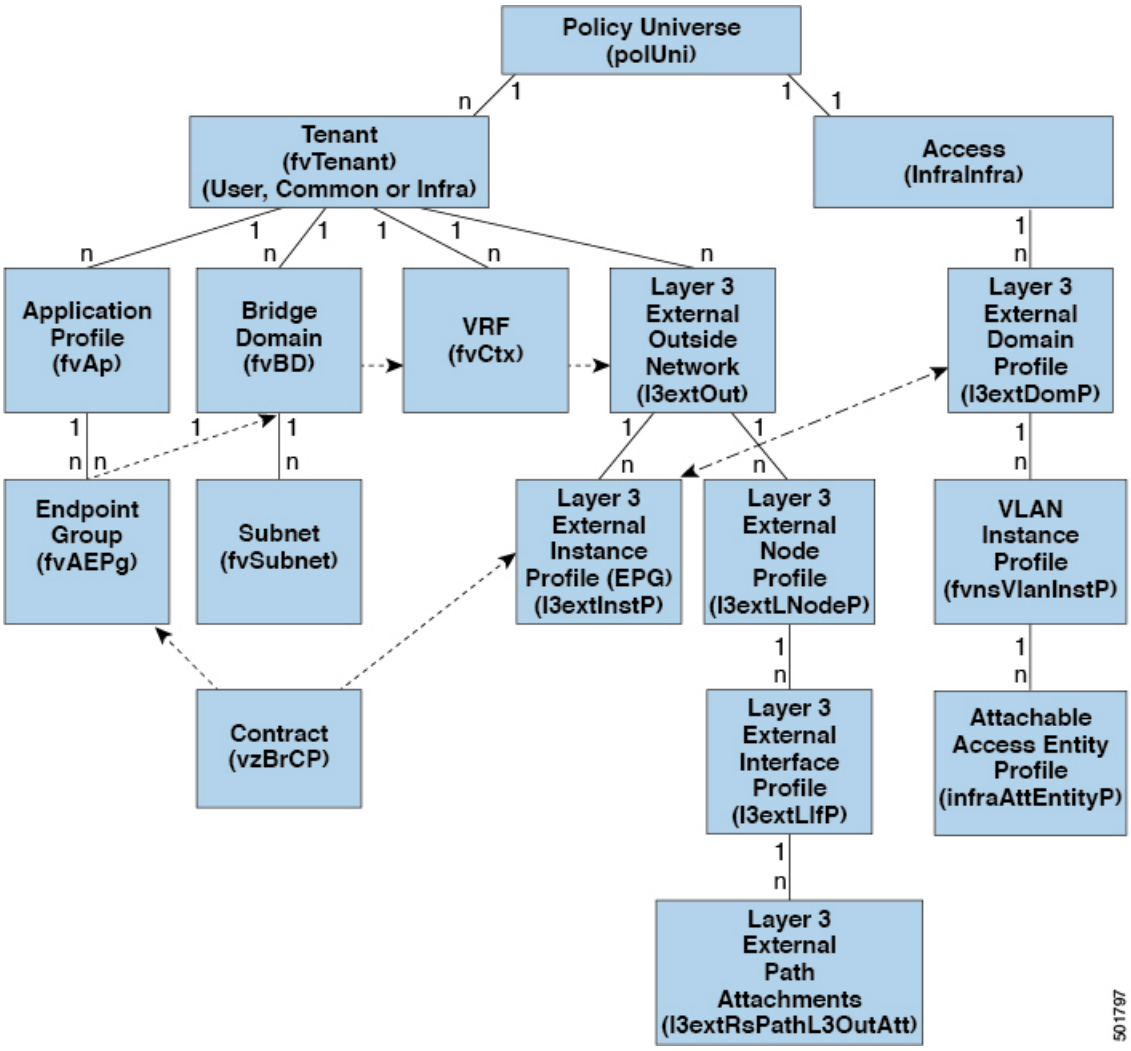
（注） ガイドラインとの設定と接続の外部レイヤ 3 を維持するための注意事項は、次を参照してください。 外部ネットワークへの接続をルーティングするための注意事項 （25 ページ） 。

L3Outs の種類についての詳細は、外部レイヤ 3 Outside 接続タイプ （13 ページ） を参照してください。

外部ネットワークへのルーテッド接続のためのレイヤ 3 Out

外部ネットワークへのルーテッド接続は、次の図の階層で示すようにファブリック アクセス（infraInfra）外部ルーテッド ドメイン（l3extDomP）をレイヤ 3 外部外側ネットワーク（l3extOut）のテナント レイヤ 3 外部インスタンス プロファイル（l3extInstP または外部 EPG）に関連付けることによって有効になります。

図 *11 :* レイヤ *3* 外部接続のポリシー モデル



レイヤ 3 外部アウトサイドネットワーク（`l3extOut` オブジェクト）には、ルーティング プロトコルのオプション（BGP、OSPF、または EIGRP またはサポートされている組み合わせ）およびスイッチとインターフェイス固有の設定が含まれています。`l3extOut` にルーティング プロトコル（たとえば、関連する仮想ルーティングおよび転送（VRF）およびエリア ID を含む OSPF）が含まれる一方で、レイヤ 3 外部インターフェイスのプロファイルには必要な OSPF インターフェイスの詳細が含まれます。いずれも OSPF のイネーブル化に必要です。

`l3extInstP` EPG は、コントラクトを通してテナント EPG に外部ネットワークを公開します。たとえば、Web サーバのグループを含むテナント EPG は、`l3extOut` に含まれるネットワーク設定に応じてコントラクトを介して `l3extInstP` EPG と通信できます。外部ネットワーク設定は、ノードを L3 外部ノード プロファイルに関連付けることで複数のノードに容易に再利用できます。同じプロファイルを使用する複数のノードをフェールオーバーやロードバランシングのために設定できます。ノードを複数の l3extOuts に追加することで、l3extOuts に関連付けられている VRF がノードでも展開されます。拡張性に関する情報については、現行の「*Verified Scalability Guide for Cisco ACI*」を参照してください。

外部ネットワークへの接続をルーティングするための注意事項

レイヤ 3 外部接続を作成し、維持する際には、次のガイドラインを使用してください。

トピック	注意またはガイドライン
入力ベース ポリシーの適用	Cisco APIC リリース 1.2(1) 以降、入力ベース ポリシーの適用により、出入力両方向でレイヤ3アウトサイド（L3Out）トラフィックにポリシー適用を定義できます。デフォルトでは入力になっています。リリース 1.2(1) 以降にアップグレード中、既存の L3Out 設定が出力に設定され、動作が既存の設定と一致します。特別なアップグレードのシーケンスは必要ありません。アップグレード後、グローバルプロパティ値を入力に変更します。変更されると、システムがルールとプレフィックス エントリを再プログラミングします。規則は出力リーフから削除され、入力リーフ上に既存の規則がない場合は、入力リーフ上にインストールされます。既存の設定がない場合、`Actrl` プレフィックス エントリが入力リーフ上にインストールされます。ダイレクト サーバ リターン（DSR）および属性 EPG には入力ベースのポリシー適用が必要です。vzAny と禁止コントラクトは、入力ベースのポリシー適用を契約無視します。入力には中継規則が適用されます。
L3Outs によるブリッジ ドメイン	テナントのブリッジ ドメインには、共通テナントでプロビジョニングされている `l3extOut` によってアドバタイズされたパブリック サブネットを含めることができます。
BGP 最大プレフィックス制限	Cisco APICリリース 1.2（1x）以降、BGP `l3extOut` 接続のテナント ポリシーは、最大プレフィックス制限を使用して設定できます。これにより、ピアから受信されるルート 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 エントリが記録され、さらにプレフィックスが拒否されます。カウントが一定の間隔でしきい値を下回る場合、接続を再起動することができますが、そうしない場合接続がシャットダウンします。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。拒否オプションが導入されると、APIC でエラーが発生する前に 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ます。

トピック	注意またはガイドライン
MTU	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 multipod 接続を設定する場合は、MTU が両側で適切に設定されていることが重要です。ACI、Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定された MTU 値は IP ヘッダーを考慮に入れています（結果として、最大パケット サイズは、ACI で 9216 バイト、NX-OS および IOS で 9000 バイトに設定されます）。ただし、IOS XR などの他のプラットフォームは、パケット ヘッダーのを除く MTU 値を設定します（結果として最大パケット 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。
レイヤ 4 から 7	マルチノード サービス グラフを使用する際、異なる VRF で 2 つの EPG が必須です。これらの機能では、システムはレイヤ 3 検索を実行する必要があるため、EPG が異なる VRF を分離する必要があります。この制限は、レイヤ 2 およびレイヤ 3 の検索に基づいてレガシ サービスの挿入に続きます。
L3Outs の QoS	L3Out 用の QoS ポリシーを設定し、L3Out が存在する BL スイッチで適用されるポリシーを有効にするには、次の注意事項に従ってください。 • VRF ポリシー制御の適用方向を **出力** に設定する必要があります。 • VRF ポリシー制御適用の優先度設定を **有効** に設定する必要があります。 • L3Out を使用して EPG 間の通信を制御するコントラクトを設定する際に、コントラクトまたはコントラクトの件名に QoS クラスまたはターゲット DSCP を含めます。

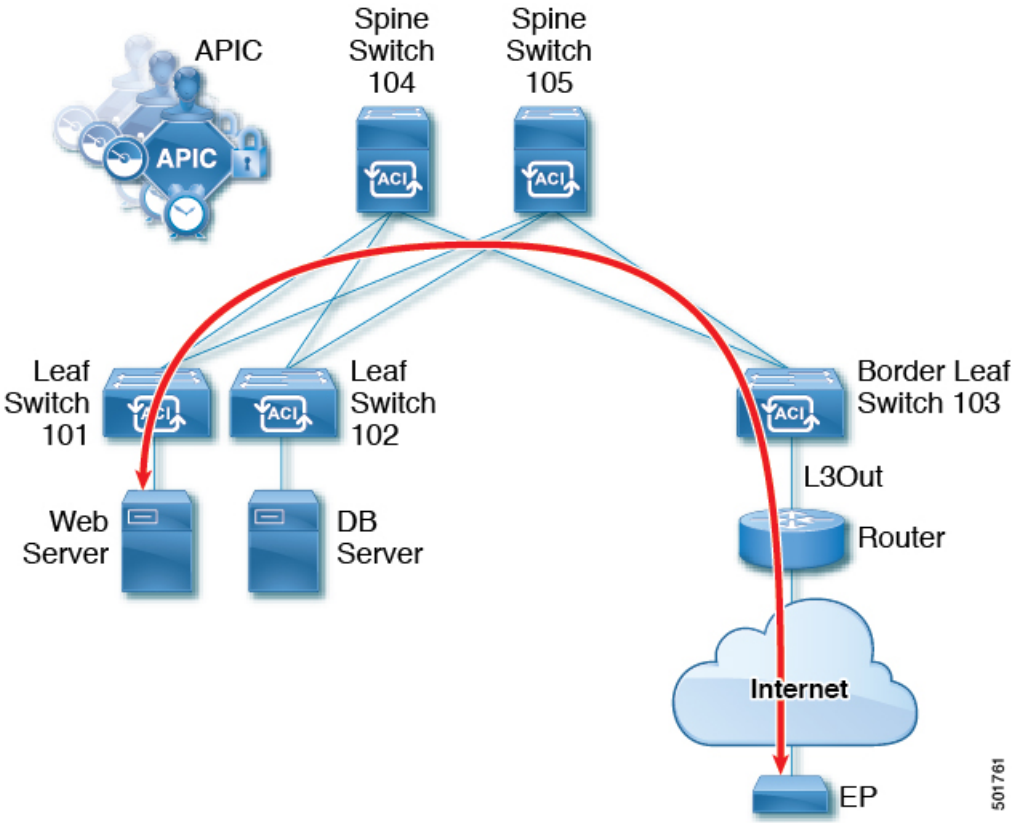
テナント ネットワークのためのレイヤ 3 Outside の設定

テナントのレイヤ 3 Outside ネットワーク接続の設定の概要

このトピックでは、Cisco APIC 使用時にテナント ネットワークに対してレイヤ 3 Outside を設定する方法の典型的な例を示します。

この章の例では、次のトポロジを使用しています。

図 *12 :* レイヤ *3* 外部接続トポロジ



この例では、Cisco ACI ファブリックは、3 つのリーフ スイッチと、APIC クラスタによって制御される 2 つのスパイン スイッチをいます。非境界リーフ スイッチ（101 および 102）は、Web サーバとデータベース サーバに接続されます。境界リーフ スイッチ（103）には、ルータへの接続とインターネットへの接続を提供する L3Out があります。この例の目標は、インターネット上のエンドポイント（EP）に対して、境界のリーフ スイッチの L3Out 経由で通信する Web サーバを有効にすることです。

この例では、L3Out に関連付けられているテナントは `t1` で、VRF `v1` および L3Out 外部 EPG `extnw1` を有します。

L3Out を設定する前に、ノード、ポート、機能プロファイル、AEP、レイヤ 3 ドメインを設定します。BGP ルート リフレクタとしてスパイン スイッチ 104 および 105 を設定する必要があります。

L3Out の設定には、次のコンポーネントの定義が含まれます。

1. テナントおよび VRF
2. リーフ 103 上のノードおよびインターフェイス
3. プライマリ ルーティング プロトコル（この例では BGP など境界リーフ スイッチと外部ルータ間のルートを交換するために使用）
4. 接続のルーティング プロトコル（この例では、OSPF などプライマリ プロトコルの到達可能性情報を提供します)
5. 外部 EPG
6. ルート マップ
7. ブリッジ ドメイン
8. ノード 101 に少なくとも 1 個のアプリケーション EPG
9. フィルタとコントラクト
10. コントラクトを EPG に関連付ける

次の表では、この章で使用される名前を一覧にしています。

プロパティ	ノード 103（境界リーフ）	ノード 101（非境界リーフ）
テナント	`t1`	`t1`
VRF	`v1`	`v1`
レイヤ 3 アウトサイド	`l3out1`	--
ブリッジ ドメイン	--	サブネット 44.44.44.1/24 で `bd1`
ノード	ルータ ID 11.11.11.103 およびパス スルー 12.12.12.3/24 を持つプロファイル `nodep1` のノード 103	ノード 101
インターフェイス	IP アドレス 11.11.11.1/24 を持つ eth/1/3 の OSPF インターフェイス `ifp1`	--
BGP の詳細	ピア アドレス 15.15.15.2/24 および ASN 100	--

プロパティ	ノード 103（境界リーフ）	ノード 101（非境界リーフ）
OSPF の詳細	OSPF エリア 0.0.0.0 と正規の種類	--
EPG	20.20.20.0/24 の外部 EPG `extnw1`	`App1`、`epg1`、`bd1` を持つアプリケーション
ルート制御プロファイル	ルート制御コンテキスト `ctxp1` を持つ `rp1`	--
ルート マップ	ルート宛先 200.3.2.0/24 を持つルール `match-rule1` による `map1`	--
フィルタ	`http-filter`	`http-filter`
コントラクト	Extnw1 により提供される `httpCtrct`	Epg1 により提供される `httpCtrct`

REST API を使用したテナント ネットワークのレイヤ 3 Outside の設定

例で設定されている外部ルーテッド ネットワークは、IPv4 および Ipv6 の両方をサポートするように拡張可能です。IPv4 と IPv6 両方のルートを外部ルーテッド ネットワークにアドバタイズし、外部ルーテッド ネットワークから学習することができます。テナント ネットワークの L3Out を設定するには、例のように XML で post を送信します。

この例は、わかりやすくするための手順に分割されます。マージされた例については、REST API の例：L3Out （33 ページ） を参照してください。

始める前に

- 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。
- 外部ルーテッド ドメインを作成し、L3Out のインターフェイスに関連付けます。
- ファブリック内でルートを伝播させるために、BGP ルート リフレクタ ポリシーを設定します。

これらの前提条件の XML の例については、REST API の例: L3Out の前提条件 （32 ページ） を参照してください。

手順

ステップ 1 テナント 、VRF、ブリッジ ドメインを設定します。

この例では VRF `v1` を持つテナント `t1` およびブリッジ ドメイン `bd1` を設定します。テナント、VRF、および BD はまだ展開されていません。

例：

```
<fvTenant  name="t1">
    <fvCtx name="v1"/>
    <fvBD name="bd1">
        <fvRsCtx tnFvCtxName="v1"/>
        <fvSubnet ip="44.44.44.1/24" scope="public"/>
        <fvRsBDToOut tnL3extOutName="l3out1"/>
    </fvBD>/>
</fvTenant>
```

ステップ 2 アプリケーション プロファイルおよびアプリケーション EPG を設定します。

この例では、アプリケーション プロファイル `app1`（ノード 101 上）、EPG `epg1` を設定し、コンシューマとして `bd1` を持つ EPG とコントラクト `httpCtrct` を関連付けます。

例：

```
<fvAp name="app1">
    <fvAEPg name="epg1">
        <fvRsDomAtt instrImedcy="immediate" tDn="uni/phys-dom1"/>
        <fvRsBd tnFvBDName="bd1" />
        <fvRsPathAtt encap="vlan-2011" instrImedcy="immediate" mode="regular"
tDn="topology/pod-1/paths-101/pathep-[eth1/3]"/>
        <fvRsCons tnVzBrCPName="httpCtrct"/>
    </fvAEPg>
</fvAp>
```

ステップ 3 ノードおよびインターフェイスを設定します。

この例では、ノード プロファイル、`nodep1`、ルータ ID `11.11.11.103` を持つノード 103（境界リーフ スイッチ）上で、VRF `v1` を設定します。. また、IP アドレス `12.12.12.1/24` およびレイヤ 3 ドメイン `dom1` で、ルーテッド インターフェイス（レイヤ 3 ポート）としてインターフェイス `eth1/3` を設定します。

例：

```
<l3extOut name="l3out1">
    <l3extRsEctx tnFvCtxName="v1"/>
    <l3extLNodeP name="nodep1">
        <l3extRsNodeL3OutAtt rtrId="11.11.11.103" tDn="topology/pod-1/node-103"/>
        <l3extLIfP name="ifp1"/>
         <l3extRsPathL3OutAtt addr="12.12.12.3/24" ifInstT="l3-port"
tDn="topology/pod-1/paths-103/pathep-[eth1/3]"/>
        </l3extLIfP>
    </l3extLNodeP>
    <l3extRsL3DomAtt tDn="uni/l3dom-dom1"/>
</l3extOut>
```

ステップ 4 ルーティング プロトコルを設定します。

この例では、IP アドレス、`15.15.15.2`、ASN 100 を持つ BGP ピアで、プライマリ ルーティング プロトコルとして BGP を設定します。

例：

```
<l3extOut name="l3out1">
    <l3extLNodeP name="nodep1">
        <bgpPeerP addr="15.15.15.2">
            <bgpAsP asn="100"/>
        </bgpPeerP>
    </l3extLNodeP>
```

```
    <bgpExtP/>
</l3extOut>
```

ステップ 5 接続ルーティング プロトコルを設定します。

この例では、定期的なエリア ID `0.0.0.0` で に対して通信プロトコルとして OSPF を設定します。

例：

```
<l3extOut name="l3out1">
    <ospfExtP areaId="0.0.0.0" areaType="regular"/>
    <l3extLNodeP name="nodep1">
        <l3extLIfP name="ifp1">
            <ospfIfP/>
        <l3extIfP>
    <l3extLNodeP>
</l3extOut>
```

ステップ 6 外部 EPG を設定します。

この例では、外部ネットワーク `extnw1` としてネットワーク `20.20.20.0/24` を設定します。プロバイダとして、`extnw1` とルート制御プロファイル `rp1` およびコントラクト `httpCtrct` を関連付けます。

例：

```
<l3extOut name="l3out1">
    <l3extInstP name="extnw1">
        <l3extSubnet ip="20.20.20.0/24" scope="import-security"/>
        <fvRsProv tnVzBrCPName="httpCtrct"/>
    </l3extInstP>
</l3extOut>
```

ステップ 7 オプション。ルート マップを設定します。

この例では、アウトバウンド方向に BGP ピアのルート マップを設定します。ルート マップがルートの宛先に一致するのに適用される `200.3.2.0/24` 。また、正常な一致で (ルートには、この範囲が一致する) ルート AS パス アトリビュートが更新され、 `200` および `100` 。

例：

```
<fvTenant name="t1">
    <rtctrlSubjP name="match-rule1">
         <rtctrlMatchRtDest ip="200.3.2.0/24"/>
    </rtctrlSubjP>
    <l3extOut name="l3out1">
        <rtctrlProfile name="rp1">
            <rtctrlCtxP name="ctxp1" action="permit" order="0">
                <rtctrlScope>
                    <rtctrlRsScopeToAttrP tnRtctrlAttrPName="attrp1"/>
                </rtctrlScope>
                <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule1"/>
            </rtctrlCtxP>
        </rtctrlProfile>
        <l3extInstP name="extnw1">
            <l3extSubnet ip="20.20.20.0/24" scope="import-security"/>
            <l3extRsInstPToProfile direction='export' tnRtctrlProfileName="rp1"/>
            <fvRsProv tnVzBrCPName="httpCtrct"/>
        </l3extInstP>
    </l3extOut>
</fvTenant>
```

ステップ 8 この例では、フィルタおよびコントラクトを作成し、EPG の通信を可能にします。外部 EPG およびアプリケーション EPG は、プロバイダおよびコンシューマとして個別にコントラクト `httpCtrct` にすでに関連付けられています。コントラクトの範囲（適用される範囲）はアプリケーション、テナント、VRF 内か、グローバルを選択できます（ファブリック全体）。この例では、範囲は VRF（`context`）です。

例：

```
<vzFilter name="http-filter">
    <vzEntry  name="http-e" etherT="ip" prot="tcp"/>
</vzFilter>
<vzBrCP name="httpCtrct" scope="context">
    <vzSubj name="subj1">
        <vzRsSubjFiltAtt tnVzFilterName="http-filter"/>
    </vzSubj>
</vzBrCP>
```

REST API の例: L3Out の前提条件

この例では、ノード、ポート、AEP、レイヤ 3 ドメインを設定します。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/policymgr/mo/.xml -->
<polUni>
    <infraInfra>
        <!-- Node profile -->
        <infraNodeP name="nodeP1">
            <infraLeafS name="leafS1" type="range">
                <infraNodeBlk name="NodeBlk1" from_="101" to_="103" />
            </infraLeafS>
            <infraRsAccPortP tDn="uni/infra/accportprof-PortP1" />
        </infraNodeP>
        <!-- Port profile -->
        <infraAccPortP name="PortP1">
            <!-- 12 regular ports -->
            <infraHPortS name="PortS1" type="range">
                <infraPortBlk name="portBlk1" fromCard="1" toCard="1" fromPort="3"
toPort="32"/>
                <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-default" />
            </infraHPortS>
        </infraAccPortP>
        <!-- Functional profile -->
        <infraFuncP>
            <!-- Regular port group -->
            <infraAccPortGrp name="default">
                <infraRsAttEntP tDn="uni/infra/attentp-aeP1" />
            </infraAccPortGrp>
        </infraFuncP>
        <infraAttEntityP name="aeP1">
            <infraRsDomP tDn="uni/phys-dom1"/>
            <infraRsDomP tDn="uni/l3dom-dom1/>
        </infraAttEntityP>
        <fvnsVlanInstP name="vlan-1024-2048" allocMode="static">
           <fvnsEncapBlk name="encap" from="vlan-1024" to="vlan-2048" status="created"/>

        </fvnsVlanInstP>
    </infraInfra>
    <physDomP dn="uni/phys-dom1" name="dom1">
         <infraRsVlanNs tDn="uni/infra/vlanns-[vlan-1024-2048]-static"/>
```

```
    </physDomP>
    <l3extDomP name="dom1">
        <infraRsVlanNs tDn="uni/infra/vlanns-[vlan-1024-2048]-static" />
    </l3extDomP>
</polUni>
```

次の例では、必要な BGP ルート リフレクタを設定します。

```
 <!-- Spine switches 104 and 105 are configured as route reflectors -->
<?xml version="1.0" encoding="UTF8"?>
<!-- api/policymgr/mo/.xml -->
<polUni>
    <bgpInstPol name="default">
        <bgpAsP asn="100"/>
        <bgpRRP>
            <bgpRRNodePEp id="104"/>
            <bgpRRNodePEp id="105"/>
        </bgpRRP>
    </bgpInstPol>
    <fabricFuncP>
        <fabricPodPGrp name="bgpRRPodGrp1">
            <fabricRsPodPGrpBGPRRP tnBgpInstPolName="default"/>
        </fabricPodPGrp>
    </fabricFuncP>
    <fabricPodP name="default">
        <fabricPodS name="default" type="ALL">
            <fabricRsPodPGrp tDn="uni/fabric/funcprof/podpgrp-bgpRRPodGrp1"/>
        </fabricPodS>
    </fabricPodP>
</polUni>
```

REST API の例：L3Out

次の例は、REST API を使用した L3Out を設定する手順のマージ バージョンです。

```
<?xml version="1.0" encoding="UTF8"?>
<!-- api/policymgr/mo/.xml -->
<polUni>
   <fvTenant name="t1">
       <fvCtx name="v1"/>
       <fvBD name="bd1">
           <fvRsCtx tnFvCtxName="v1"/>
           <fvSubnet ip="44.44.44.1/24" scope="public"/>
           <fvRsBDToOut tnL3extOutName="l3out1"/>
       </fvBD>
       <fvAp name="app1">
           <fvAEPg name="epg1">
               <fvRsDomAtt instrImedcy="immediate" tDn="uni/phys-dom1"/>
               <fvRsBd tnFvBDName="bd1" />
               <fvRsPathAtt encap="vlan-2011" instrImedcy="immediate" mode="regular"
tDn="topology/pod-1/paths-101/pathep-[eth1/3]"/>
               <fvRsCons tnVzBrCPName="httpCtrct"/>
           </fvAEPg>
       </fvAp>
       <l3extOut name="l3out1">
           <l3extRsEctx tnFvCtxName="v1"/>
           <l3extLNodeP name="nodep1">
              <l3extRsNodeL3OutAtt rtrId="11.11.11.103" tDn="topology/pod-1/node-103"/>

               <l3extLIfP name="ifp1">
                   <l3extRsPathL3OutAtt addr="12.12.12.3/24" ifInstT="l3-port"
tDn="topology/pod-1/paths-103/pathep-[eth1/3]"/>
               </l3extLIfP>
               <bgpPeerP addr="15.15.15.2">
```

```
                    <bgpAsP asn="100"/>
                </bgpPeerP>
            </l3extLNodeP>
            <l3extRsL3DomAtt tDn="uni/l3dom-dom1"/>
            <bgpExtP/>
            <ospfExtP areaId="0.0.0.0" areaType="regular"/>
            <l3extInstP name="extnw1" >
                <l3extSubnet ip="20.20.20.0/24" scope="import-security"/>
                <l3extRsInstPToProfile direction="export" tnRtctrlProfileName="rp1"/>
                <fvRsProv tnVzBrCPName="httpCtrct"/>
            </l3extInstP>
            <rtctrlProfile name="rp1">
                <rtctrlCtxP name="ctxp1" action="permit" order="0">
                    <rtctrlScope>
                        <rtctrlRsScopeToAttrP tnRtctrlAttrPName="attrp1"/>
                    </rtctrlScope>
                    <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule1"/>
                </rtctrlCtxP>
            </rtctrlProfile>
        </l3extOut>
        <rtctrlSubjP name="match-rule1">
            <rtctrlMatchRtDest ip="200.3.2.0/24"/>
        </rtctrlSubjP>
        <rtctrlAttrP name="attrp1">
            <rtctrlSetASPath criteria="prepend">
                <rtctrlSetASPathASN asn="100" order="2"/>
                <rtctrlSetASPathASN asn="200" order="1"/>
            </rtctrlSetASPath>
        </rtctrlAttrP>
        <vzFilter name='http-filter'>
            <vzEntry name="http-e" etherT="ip" prot="tcp"/>
        </vzFilter>
        <vzBrCP name="httpCtrct" scope="context">
            <vzSubj name="subj1">
                <vzRsSubjFiltAtt tnVzFilterName="http-filter"/>
            </vzSubj>
        </vzBrCP>
    </fvTenant>
</polUni>
```

NX-OS スタイルの CLI を使用したテナント ネットワークのレイヤ 3 Outside の設定

次の手順では、テナント ネットワークのネットワークの外部レイヤ 3 を設定する方法について説明します。次に、NX-OS CLI を使用してテナント VRF 外部 L3 接続にノードと L3 ポートを配備する例を示します。

この例は、わかりやすくするための手順に分割されます。マージされた例については、NX-OS スタイル CLI の例：L3Out （38 ページ） を参照してください。

始める前に

- ノード、ポート、機能プロファイル、AEP、レイヤ 3 ドメインを設定します。
- 使用して VLAN ドメイン設定、 **vlan ドメイン** ドメイン および **vlan** *vlan* 範囲 コマンド。
- BGP ルート リフレクタ ポリシーを設定し、ファブリック内でルーテッドを伝達します。

コマンドを使用して、これらの前提条件の例を参照してください。NX-OS スタイル CLI の例: L3Out の前提条件 （38 ページ） 。

手順

ステップ 1 テナントおよび VRF を設定します。

この例では VRF `v1` でテナント `t1` を設定します。これらはまだ展開されていません。

例：

```
apic1# configure
apic1(config)# tenant t1
apic1(config-tenant)# vrf context v1
apic1(config-tenant-vrf)# exit
apic1(congig-tenant)# exit
apic1(config)#
```

ステップ 2 L3Out のノードとインターフェイスを設定します。

この例では設定 VRF `v1` ノード 103 (border リーフ スイッチ) と呼ばれるで `node1` 、ルータ ID を `11.11.11.103` 。インターフェイスの設定も `eth1/3` ルーテッド インターフェイス (レイヤ 3 のポート)、IP アドレスとして `12.12.12.3/24` とレイヤ 3 ドメイン `dom1` 。

例：

```
apic1(config)# leaf 103
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# router-id 11.11.11.103
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# interface ethernet 1/3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vrf member tenant t1 vrf v1
apic1(config-leaf-if)# ip address 12.12.12.3/24
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

ステップ 3 ルーティング プロトコルを設定します。

この例では、BGP ピアのアドレスを使用して、プライマリのルーティング プロトコルとして BGP を設定 `15.15.15.2` ASN 100 ドルとします。

例：

```
apic1(config)# leaf 103
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 15.15.15.2
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# exit
```

ステップ 4 オプション。接続ルーティング プロトコルを設定します。

この例では、定期的なエリア ID と、通信プロトコルとして OSPF を設定 `0.0.0.0` 、ループバック アドレスと `30.30.30.0` 。

例：

```
apic1(config)# leaf 103
apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant t1 vrf v1
apic1(config-leaf-ospf-vrf)# area 0.0.0.0 loopback 30.30.30.0
apic1(config-leaf-ospf-vrf)# exit
apic1(config-leaf-ospf)# exit
apic1(config-leaf)# exit
```

ステップ 5 ノード 103 上に外部 EPG を設定します。

この例では、ネットワークで `20.20.20.0/24` 外部ネットワークとして設定されている `extnw1` 。

例：

```
apic1(config)# tenant t1
apic1(config-tenant)# external-l3 epg extnw1
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# match ip 20.20.20.0/24
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# exit
apic1(config)# leaf 103
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# external-l3 epg extnw1
apic1(config-leaf-vrf)# exit
```

ステップ 6 オプション。ルート マップを設定します。

この例では、ルート マップ設定 `rp1` アウト バウンド方向に BGP ピアの。ルート マップがルートの宛先に一致するのに適用される `200.3.2.0/24` 。また、正常な一致で (ルートには、この範囲が一致する) ルート AS パス アトリビュートが更新され、 `200` および `100` 。

例：

```
apic1(config-leaf)# template route group match-rule1 tenant t1
apic1(config-route-group)# ip prefix permit 200.3.2.0/24
apic1(config-route-group)# exit
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# route-map rp1
apic1(config-leaf-vrf-route-map)# match route group match-rule1 order 0
apic1(config-leaf-vrf-route-map-match)# exit
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf)# exit
apic1(config)# leaf 103
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 15.15.15.2
apic1(config-leaf-bgp-vrf-neighbor)# route-map rp1 in
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)#exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# exit
```

ステップ 7 ブリッジ ドメインを追加します。

例：

```
apic1(config)# tenant t1
apic1(config-tenant)# bridge-domain bd1
apic1(config-tenant-bd)# vrf member v1
apic1(config-tenant-bd)# exit
```

```
apic1(config-tenant)# interface bridge-domain bd1
apic1(config-tenant-interface)# ip address 44.44.44.1/24 scope public
apic1(config-tenant-interface)# exit
apic1(config-tenant)# exit
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# route-map rp1
apic1(config-leaf-vrf-route-map)# match bridge-domain bd1 tenant t1
apic1(config-leaf-vrf-route-map-match)# exit
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# exit
```

ステップ 8 ノード 101 で EPG アプリケーションを作成します。

例：

```
apic1(config)# tenant t1
apic1(config-tenant)# application app1
apic1(config-tenant-app)# epg epg1
apic1(config-tenant-app-epg)# bridge-domain member bd1
apic1(config-tenant-app-epg)# exit
apic1(config-tenant-app)# exit
apic1(config-tenant)# exit
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# switchport trunk allowed vlan 2011 tenant t1 application app1 epg
 epg1
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config)#
```

ステップ 9 フィルタ (アクセス リスト) と契約を作成します。

例：

```
apic1(config)# tenant t1
apic1(config-tenant)# access-list http-filter
apic1(config-tenant-acl)# match ip
apic1(config-tenant-acl)# match tcp dest 80
apic1(config-tenant-acl)# exit
apic1(config-tenant)# contract httpCtrct
apic1(config-tenant-contract)# scope vrf
apic1(config-tenant-contract)# subject subj1
apic1(config-tenant-contract-subj)# access-group http-filter both
apic1(config-tenant-contract-subj)# exit
apic1(config-tenant-contract)# exit
```

ステップ 10 契約を設定し、Epg に関連付けます。

例：

```
apic1(config-tenant)# external-l3 epg extnw1
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# contract provider httpCtrct
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# application app1
apic1(config-tenant-app)# epg epg1
apic1(config-tenant-app-epg)# contract consumer httpCtrct
apic1(config-tenant-app-epg)# exit
apic1(config-tenant-app)# exit
```

```
apic1(config-tenant)# exit
apic1(config)#
```

NX-OS スタイル CLI の例: L3Out の前提条件

L3Out を設定する前に、次の手順を実行します。

1. VLAN ドメインを設定します。

```
apic1# configure
apic1(config)# vlan-domain dom1
apic1(config-vlan)# vlan 1024-2048
apic1(config-vlan)# exit
```

2. BGP ルート リフレクタを設定します:

```
apic1(config)# bgp-fabric
apic1(config-bgp-fabric)# asn 100
apic1(config-bgp-fabric)# route-reflector spine 104,105
```

NX-OS スタイル CLI の例：L3Out

次の例は、L3Out を設定する手順のマージ バージョン NX-OS スタイル CLI を使用します。L3Out を設定する前に、次の前提条件を設定します。

```
apic1# configure
apic1(config)# tenant t1
apic1(config-tenant)# vrf context v1
apic1(config-tenant-vrf)# exit
apic1(config-tenant)# exit
apic1(config)# leaf 103
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# router-id 11.11.11.103
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# interface ethernet 1/3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vrf member tenant t1 vrf v1
apic1(config-leaf-if)# ip address 12.12.12.3/24
apic1(config-leaf-if)# exit
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 15.15.15.2
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant t1 vrf v1
apic1(config-leaf-ospf-vrf)# area 0.0.0.0 loopback 30.30.30.0
apic1(config-leaf-ospf-vrf)# exit
apic1(config-leaf-ospf)# exit
apic1(config-leaf)# exit
apic1(config)# tenant t1
apic1(config-tenant)# external-l3 epg extnw1
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# match ip 20.20.20.0/24
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# exit
```

```
apic1(config)# leaf 103
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# external-l3 epg extnw1
apic(config-leaf-vrf)# exit
apic1(config-leaf)# template route group match-rule1 tenant t1
apic1(config-route-group)# ip prefix permit 200.3.2.0/24
apic1(config-route-group)# exit
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# route-map rp1
apic1(config-leaf-vrf-route-map)# match route group match-rule1 order 0
apic1(config-leaf-vrf-route-map-match)# exit
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 15.15.15.2
apic1(config-leaf-bgp-vrf-neighbor)# route-map rp1 in
apic1(config-leaf-bgp-vrf-neighbor)#exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# exit
apic1(config)# tenant t1
apic1(config-tenant)# bridge-domain bd1
apic1(config-tenant-bd)# vrf member v1
apic1(config-tenant-bd)# exit
apic1(config-tenant)# interface bridge-domain bd1
apic1(config-tenant-interface)# ip address 44.44.44.1/24 scope public
apic1(config-tenant-interface)# exit
apic1(config-tenant)# exit
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# route-map map1
apic1(config-leaf-vrf-route-map)# match bridge-domain bd1 tenant t1
apic1(config-leaf-vrf-route-map-match)# exit
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# exit
apic1(config)# tenant t1
apic1(config-tenant)# application app1
apic1(config-tenant-app)# epg epg1
apic1(config-tenant-app-epg)# bridge-domain member bd1
apic1(config-tenant-app-epg)# exit
apic1(config-tenant-app)# exit
apic1(config-tenant)# exit
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# switchport trunk allowed vlan 2011 tenant t1 application app1 epg
 epg1
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config)# tenant t1
apic1(config-tenant)# access-list http-filter
apic1(config-tenant-acl)# match ip
apic1(config-tenant-acl)# match tcp dest 80
apic1(config-tenant-acl)# exit
apic1(config-tenant)# contract httpCtrct
apic1(config-tenant-contract)# scope vrf
apic1(config-tenant-contract)# subject subj1
apic1(config-tenant-contract-subj)# access-group http-filter both
apic1(config-tenant-contract-subj)# exit
apic1(config-tenant-contract)# exit
apic1(config-tenant)# external-l3 epg extnw1
apic1(config-tenant-l3ext-epg)# vrf member v1
```

```
apic1(config-tenant-l3ext-epg)# contract provider httpCtrct
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# application app1
apic1(config-tenant-app)# epg epg1
apic1(config-tenant-app-epg)# contract consumer httpCtrct
apic1(config-tenant-app-epg)# exit
apic1(config-tenant-app)# exit
apic1(config-tenant)# exit
apic1(config)#
```

GUI を使用したテナント ネットワークのレイヤ 3 Outside の設定

ファブリックの外部レイヤ 3 (L3Out) 接続を設定するには、次の手順を実行します。

始める前に

- 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。
- 外部ルーテッド ドメインを作成し、L3Out のインターフェイスに関連付けます。
- 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 テナントと VRF を作成するには、メニュー バーで、**Tenants** > **Add Tenant** を選択し、**Create Tenant** ダイアログボックスで、次のタスクを実行します:

a) **Name** フィールドに、テナント名を入力します。
b) In the **VRF Name** フィールドに、VRF 名を入力します。
c) **Submit** をクリックします。

ステップ 2 ブリッジ ドメインを作成するには、**Navigation** ウィンドウで **Tenant** および **Networking** を展開し、次の手順を実行します:

a) **Bridge Domains** を右クリックして、**Create Bridge Domain** を選択します。
b) **Name** フィールドに、ブリッジ ドメイン (BD) の名前を入力します。
c) **VRF** フィールドのドロップダウンリストから、作成した VRF を選択します (この例では v1)。
d) **Next** をクリックします。
e) + アイコンを **Subnets** でクリックします。
f) **Gateway IP** フィールドに、BD のサブネットを入力します。
g) **Scope** フィールドで、**Advertised Externally** を選択します。

後ほど作成した後に、**L3 Out for Route Profile** を追加します。

h) **OK** をクリックします。
i) **Next** をクリックし、 **Finish** をクリックします。

ステップ 3 アプリケーション EPG を作成するには、次の手順を実行します:

a) **Application Profiles** を右クリックし、**Create Application Profile** を選択します。
b) アプリケーションの名前を入力します。
c) EPG の + アイコンをクリックします。
d) EPG の名前を入力します。
e) BD ドロップダウンリストで、以前に作成したブリッジ ドメインを選択します。
f) **Update** をクリックします。
g) [Submit] をクリックします。`

ステップ 4 L3Out の作成を開始するには、**Navigation** ウィンドウで **Tenant** および **Networking** を展開し、次の手順に従います:

a) **External Routed Networks** を右クリックして、**Create Routed Outside** を選択します。
b) **Name** フィールドに、L3Out の名前を入力します。
c) **VRF** ドロップダウンリストから VRF を選択します。
d) **External Routed Domain** ドロップダウンリストで、先ほど作成した、外部ルーテッド ドメインを選択します。
e) ルーテッド プロトコルのチェックボックスがある領域で、目的のプロトコル (BGP、OSPF、または EIGRP) をオンにします。

この章の例では、**BGP** および **OSPF** を選択します。

選択するプロトコルに応じて、設定する必要のあるプロパティに入力します。

f) OSPF を有効にした場合は、OSPF の詳細を入力します。

この章の例では、OSPF エリア **0** を使用し、**Regular area** に入力します。

g) [+] をクリックして **Nodes and Interfaces Protocol Profiles** を展開します。
h) **Name** フィールドに、名前を入力します
i) [+] をクリックして **Nodes** を展開します。
j) **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。

k) **Router ID** フィールドで、ルータ ID (L3Out に接続されているルータの IPv4 または IPv6 アドレス) を入力します。
l) （任意） ループバック アドレスに別の IP アドレスを設定することができます。**Use Router ID as Loopback Address** をオフにし、**Loopback Addresses** を展開し、IP アドレスを入力し、**Update** をクリックします。
m) **Select Node** ダイアログボックスで、**OK** をクリックします。

ステップ 5 BGP を有効にしている場合には、+ アイコンをクリックして **BGP Peer Connectivity Profiles** を展開し、次の手順を実行します:

a) **Peer Address** フィールドに、BGP ピアのアドレスを入力します。
b) **Local-AS Number** フィールドに、BGP AS 番号を入力します。

この章の例では、BGP ピア アドレス **15.15.15.2** および ASN 番号 **100** を使用します。

c) **OK** をクリックします。

ステップ 6 [+] をクリックして **Interface Profiles** (OSPF を有効にする場合は **OSPF Interface Profiles**) を展開し、次の操作を実行します:

a) **Name** フィールドに、インターフェイス プロファイルの名前を入力します。
b) **Next** をクリックします。
c) **Protocol Profiles** ダイアログボックスの **OSPF Policy** フィールドで、OSPF ポリシーを選択します。
d) **Next** をクリックします。
e) + アイコンをクリックして **Routed Interfaces** を展開します。
f) **Select Routed Interface** ダイアログボックスで、**Node** ドロップダウンリストからノードを選択します。
g) **Path** ドロップダウンリストから、インターフェイスのパスを選択します。
h) **IPv4 Primary/IPv6 Preferred Address** フィールドに、インターフェイスの IP アドレスとネットワーク マスクを入力します。

（注） IPv6 を設定するには、**Link-local Address** フィールドにリンクローカル アドレスを入力します。

i) **OK (Select Routed Interface** ダイアログボックス) をクリックします。
j) **OK (Create Interface Profile** ダイアログボックス) をクリックします。

ステップ 7 [Create Node Profile] ダイアログボックスで、[OK] をクリックします。

ステップ 8 [Create Routed Outside] ダイアログボックスで、[Next] をクリックします。

ステップ 9 **External EPG Networks** タブで、**Create Route Profiles** をクリックします。

ステップ 10 + アイコンをクリックして **Route Profiles** を展開し、次のアクションを実行します:

a) **Name** フィールドに、ルート マップ名を入力します。
b) **Type** を選択します。

この例では、デフォルトの **Match Prefix AND Routing Policy** のままにします。

c) + アイコンをクリックして **Contexts** を展開し、ルート マップのルート コンテキストを作成します。
d) プロファイル コンテキストの順序と名前を入力します。
e) このコンテキストで実行するアクションとして **Deny** または **Permit** を選択します。
f) （任意） **Set Rule** フィールドで、**Create Set Rules for a Route Map** を選択します。

セット ルールのための名前を入力し、ルールで使用するオブジェクトをクリックし、**Finish** をクリックします。

g) **Associated Matched Rules** フィールドで、[+] をクリックしてルート マップの一致ルールを作成します。
h) 一致ルールの名前を入力し、ルールで一致させる対象として **Match Regex Community Terms**、**Match Community Terms**、または **Match Prefix** を入力します。
i) ルール名をクリックして、**Update** をクリックします。
j) **Create Match Rule** ダイアログボックスで、**Submit** をクリックし、**Update** をクリックします。

k) **Create Route Control Context** ダイアログボックスで、**OK** をクリックします。
l) **Create Route Map** ダイアログボックスで、**OK** をクリックします。

ステップ 11 + アイコンをクリックして、**External EPG Networks** を展開します。

ステップ 12 **Name** フィールドに、外部ネットワークの名前を入力します。

ステップ 13 + アイコンをクリックして、**Subnet** を展開します。

ステップ 14 **Create Subnet** ダイアログボックスで、次の操作を実行します。

a) **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。
b) **Scope** フィールドで、L3Out のプレフィックスのエクスポートとインポートを制御するための適切なチェック ボックスをオンにします。

（注） 範囲のオプションの詳細については、この **Create Subnet** パネルのオンライン ヘルプを参照してください。

c) （任意） **Route Summarization Policy** フィールドでは、ドロップダウンリストから既存のルート集約ポリシーを選択するか、必要に応じて新しいユーザを作成します。また、**Export Route Control Subnet** のチェック ボックスもオンにします。

ルート集約ポリシーのタイプは、L3Out に対して有効になっているルーティング プロトコルに依存します。

d) + アイコンをクリックして **Route Control Profile** を展開します。
e) **Name** フィールドのドロップダウン リストから、前に作成したルート制御プロファイルを選択します。
f) **Direction** フィールドで、**Route Export Policy** を選択します。
g) **Update** をクリックします。
h) **Create Subnet** ダイアログボックスで、**OK** をクリックします。
i) （任意） より多くのサブネットを追加するにはこれを繰り返します。
j) **[Create External Network]** ダイアログボックスで、**[OK]** をクリックします。

ステップ 15 **[Create Routed Outside]** ダイアログボックスで、**[Finish]** をクリックします。

ステップ 16 **Navigation** ウィンドウの、***Tenant_name*** > **Networking** の下で **Bridge Domains** を展開します。

（注） L3Out がスタティックである場合は、BD 設定を選択する必要はありません。

ステップ 17 作成した BD を選択します。

a) **Work** ウィンドウで、**Policy** と **L3 Configurations** をクリックします。
b) + アイコンをクリックして **Associated L3 Outs** フィールドを展開し、前に設定した L3Out を選択し、**Update** をクリックします。
c) **L3Out for Route Profile** フィールドで、もう一度 L3Out を選択します。
d) **Next** と **Finish** をクリックします。

ステップ 18 **Navigation** ウィンドウの **External Routed Networks** の下で、前に作成した L3Out を展開し、**Route Maps/Profiles** を右クリックします。

（注） 受信ルートについてBGP、OSPF、またはEIGRPの属性を設定するには、default-importルート制御プロファイルを作成し、適切な set アクションと、 no match のアクションを作成します。

ステップ 19 **Create Route Map/Profile** を選択し**Create Route Map/Profile** ダイアログボックスで、次の手順を実行します:

a) **Name** フィールドのドロップダウンリストから、**default-import** を選択します。
b) **Type** フィールドでは、**Match Routing Policy Only** をクリックする必要があります。**Submit** をクリックします。

ステップ 20 （任意） 次の手順を使用して、BGP を使用する追加のコミュニティを有効にします:

a) **Set Rules for Route Maps** を右クリックして、**Create Set Rules for a Route Map** をクリックします。
b) **Create Set Rules for a Route Map** ダイアログボックスで、**Add Communities** フィールドをクリックし、次の手順を実行して、ルートプレフィックスごとに複数のBGPコミュニティを割り当てます。

ステップ 21 L3Outを使用していたEPG間の通信を有効にするには、次の手順を使用して、少なくとも1つのフィルタと契約を作成します:

a) ナビゲーション ウィンドウのL3Outを使用するテナントの下で、**Contracts** を展開します。
b) **Filters** を右クリックして **Create Filter** を選択します。
c) **Name** フィールドに、フィルタのの名前を入力します。

フィルタは基本的にはアクセス コントロール リスト (ACL) です。

d) + アイコンをクリックして **Entries** を展開し、フィルタ エントリを追加します。
e) エントリ の詳細を追加します。。

たとえば、単純な Web フィルタの場合には、次のような条件を設定します:

- **EtherType—IP**
- **IP Protocol—tcp**
- **Destination Port Range From—Unspecified**
- **Destination Port Range To** to **https**

f) **Update** をクリックします。
g) **Create Filter** ダイアログボックスで、**Submit** をクリックします。

ステップ 22 契約を追加するには、次の手順を実行します:

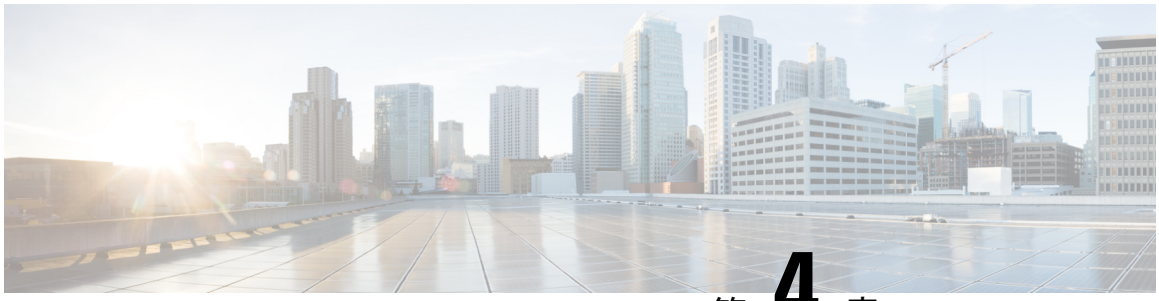
a) **Contracts** の下で、**Standard** を右クリックして、**Create Contract** を選択します。
b) 契約の名前を入力します。
c) + アイコンをクリックして **Subjects** を展開し、情報カテゴリを契約に追加します。
d) 情報カテゴリの名前を入力します。
e) + アイコンをクリックして **Filters** を展開し、ドロップダウンリストから、前に作成したフィルタを選択します。

f) **Update** をクリックします。
g) **Create Contract Subject** ダイアログボックスで、**OK** をクリックします。
h) **Create Contract** ダイアログボックスで、**Submit**をクリックします。

ステップ 23 次の手順で、L3Out の EPGを契約に関連付けます:

この例では、L3 外部 EPG (`extnw1`) がプロバイダで、アプリケーション EPG (`epg1`) がコンシューマです。

a) 契約をプロバイダーとしての L3 外部 EPG に関連付けるには、テナントの下で **Networking** をクリックし、**External Routed Networks** をクリックし、L3Out を展開します。
b) **Networks** を展開し、L3 外部 EPG をクリックし、**Contracts** をクリックします。
c) + アイコンをクリックして **Provided Contracts** を展開します。
d) **Name** フィールドで、前に作成した契約をリストから選択します。
e) **Update** をクリックします。
f) 契約をコンシューマとしてのアプリケーション EPG に関連付けるには、テナントの下で **Application Profiles** > ***app-prof-name*** > **Application EPGs** > に移動し、*app-epg-name* を展開します。
g) **Contracts** を右クリックして **Add Consumed Contract** を選択します。
h) **Contract** フィールドで、前に作成した契約を選択します。
i) [送信（Submit）] をクリックします。



第 4 章

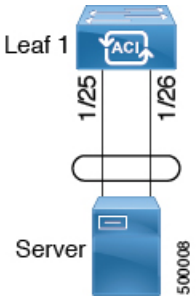
レイヤ3ルーティングおよびサブインターフェイス ポート チャネル

これらのセクションでは、GUI、NX-OS CLI および REST API を使用して、レイヤ 3 ルーティングおよびサブ インターフェイス ポート チャネルを設定する方法について説明します:

レイヤ 3 ポート チャネルについて

以前、Cisco APIC ではレイヤ 2 ポート チャネルのみサポートしていました。リリース 3.2(1) より、Cisco APIC ではレイヤ 3 ポート チャネルもサポートしています。

図 *13 :* スイッチ ポート チャネル設定



GUI を使用したポート チャネル の設定

後の手順で GUI を使用してポート チャネルへのレイヤ 3 ルートを設定する前に、まずこれらの手順でポート チャネルを設定する必要があります。

次の手順では、クイック スタート ウィザードを使用します。

始める前に

（注） このセクションで説明する手順は、レイヤ 3 ルーテッドまたはサブインターフェイス ポート チャネルを設定するための手順に対する前提条件として、特にポートチャネルを設定することを意図しています。一般的なリーフ スイッチ ポート チャネルの設定手順については、『*Cisco APIC Basic Configuration Guide*』を参照してください。

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチが ACI ファブリックに登録され、使用可能であること。

手順

ステップ 1 APIC メニュー バーで、**Fabric** > **External Access Policies** > **Quick Start** に移動し、*Configure Interface, PC, and VPC* をクリックします。

ステップ 2 **Configure Interface, PC, and VPC** 作業エリアで、大きな + をクリックして、設定するスイッチを選択します。

ステップ 3 *Switches* セクションで、利用可能なスイッチ ID のドロップダウンリストからスイッチ ID を選択します。

ステップ 4 大きい [+] をクリックして、スイッチ インターフェイスを設定します。

ステップ 5 **Interface Type** フィールドで、使用するインターフェイスのタイプとして *PC* を指定します。

ステップ 6 **Interfaces** フィールドで、使用するインターフェイス IDを指定します。

ステップ 7 (オプション) 必要であれば、**Interface Selector Name** フィールドで、一意のインターフェイス セレクタ名を入力します。

ステップ 8 [Interface Policy Group] エリアで、使用するインターフェイス ポリシーを指定します。たとえば、**Port Channel Policy** ドロップダウン矢印をクリックして、既存のポート チャネル ポリシーから選択するか、新しいポート チャネル ポリシーを作成します。

（注）
- ポートチャネル ポリシーを作成することを選択すると、**[Create Port Channel Policy]** ダイアログ ボックスが表示され、ポリシーの詳細を指定したり、対称ハッシュなどの機能を有効にしたりできます。**[Symmetric hashing]** オプションを選択すると、ハッシュ タプルを設定できる **[Load Balance Hashing]** フィールドが表示されます。ただし、1 つのみのカスタマイズされたハッシュ オプションを同じリーフ スイッチに適用することはできません。
- 対称ハッシュは、次のスイッチではサポートされていません。
  - Cisco Nexus 93128TX
  - Cisco Nexus 9372PX
  - Cisco Nexus 9372PX-E
  - Cisco Nexus 9372TX
  - Cisco Nexus 9372TX-E
  - Cisco Nexus 9396PX
  - Cisco Nexus 9396TX

ステップ 9 **Attached Device Type** フィールドで、**`External Routed Devices`** オプションを選択します。

ステップ 10 **Domain** フィールドで、インターフェイスに割り当てるドメインを作成するか、選択します。

ステップ 11 ドメインの作成を選択した場合には、**VLAN** フィールドで、既存の VLAN プールから選択するか、新しい VLAN 範囲を作成して、インターフェイスに割り当てます。

ステップ 12 **[Save]** をクリックしてポリシーの詳細を更新し、**[Submit]** をクリックしてスイッチプロファイルを APIC に送信します。
APIC が、インターフェイス、セレクタ、および接続デバイス タイプの各ポリシーとともに、スイッチ プロファイルを作成します。

次のタスク

GUI を使用して、レイヤ 3 ルーテッドポート チャネルまたはレイヤ 3 サブインターフェイス ポート チャネルを設定します。

GUI を使用してレイヤ 3 ルーテッド ポート チャネルを設定する

この手順では、以前に作成したポート チャネルへのレイヤ 3 ルートを設定します。

始める前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチが ACI ファブリックに登録され、使用可能であること。
- ポート チャネルは、「GUI を使用したポート チャネルの設定」の手順を使用して設定します。

手順

ステップ 1 APIC メニュー バーで、**Tenants** > **Tenant** > **Networking** > **External Routed Networks** > ***L3Out*** > **Logical Node Profiles** > ***node*** > **Logical Interface Profiles** に移動します。

ステップ 2 設定するインターフェイスを選択します。そのインターフェースの **Logical Interface Profile** ページが表示されます。

ステップ 3 *[ルーテッド インターフェイス]* をクリックします。[Properties] ページが開きます。

ステップ 4 作成 (+) ボタンをクリックして、レイヤ 3 ルーテッド ポート チャネルを設定します。**[ルーテッド インターフェイスの選択]** ページが表示されます。

ステップ 5 **Path Type** フィールドで、**`Direct Port Channel`** を選択します。

ステップ 6 **[パス]** フィールドで、ドロップダウン リストから以前に作成したポート チャネルを選択します。これは、インターフェイス プロファイルのポート チャネル エンド ポイントへのパスです。

ステップ 7 **Description** フィールドに、ルーテッド インターフェイスの説明を入力します。

ステップ 8 **IPv4 Primary / IPv6 Preferred Address** フィールドに、レイヤ 3 外側プロファイルにアタッチされているパスのプライマリ IP アドレスを入力します。

ステップ 9 **[IPv6 DAD]** フィールドで、**[無効]** または **[有効]** を選択します。

このフィールドの詳細については、「IPv6 ネイバー探索重複アドレス検出の設定」を参照してください。

ステップ 10 **[IPv4 セカンダリ/IPv6 追加アドレス]** フィールドに、レイヤ 3 外側プロファイルにアタッチされているパスのセカンダリ IP アドレスを入力します。

[セカンダリ IP アドレスの追加] 画面の [IPv6 DAD] フィールドの詳細については、「IPv6 ネイバー探索重複アドレス検出の設定」を参照してください。

ステップ 11 インターフェイスに対し、ネイバー探索ルータ アドバタイズメント プレフィックスを有効にする場合には、**[ND RA プレフィックス]** ボックスをオンにします。ND RA プレフィックス ポリシーのオプションが表示されます。

これを有効にすると、自動設定でルーテッドインターフェイスを使用できるようになり、プレフィックスは自動設定のためにホストに送信されます。

ND RA インターフェイス ポリシーは BD や レイヤ 3 Out に導入されるのに対し、ND プレフィックス ポリシーは個々のサブネットに導入されます。ND プレフィックス ポリシーはサブネット レベルにあります。

ND RA プレフィックスは、IPv6 アドレスにのみ適用されます。

ステップ 12 **[ND RA プレフィックス]** ボックスをオンにした場合、使用する ND RA プレフィックス ポリシーを選択します。デフォルト ポリシーを選択することもできますし、独自の ND RA プレフィックス ポリシーを作成することもできます。独自のポリシーを作成する場合は、[Create ND RA Prefix Policy] 画面が表示されます。

a) **Name** フィールドに、プレフィックス ポリシーのルータ アドバタイズメント (RA) 名を入力します。
b) **Description** フィールドに、プレフィックスポリシーの説明を入力します。
c) **[コントローラ状態]** フィールドで、コントローラの管理状態に適したチェック ボックスをオンにします。複数のボックスをオンにできます。デフォルトは **[自動設定]** および **[オンリンク]** です。
d) **Valid Prefix Lifetime** フィールドで、プレフィックスを有効にする期間について適切な値を選択します。有効な範囲は 0 ～ 4294967295 ミリ秒です。デフォルト値は 2592000 です。
e) **[優先プレフィックス ライフタイム]** フィールドで、プレフィックスの優先有効期間について適切な値を選択します。有効な範囲は 0 ～ 4294967295 ミリ秒です。デフォルト値は 604800 です。
f) **Submit** をクリックします。

ステップ 13 **[MAC アドレス]** フィールドに、レイヤ 3 外側プロファイルにアタッチされているパスの MAC アドレスを入力します。

ステップ 14 **[MTU（バイト）]** フィールドで、外部ネットワークの最大転送単位を設定します。指定できる範囲は 576 ～ 9216 です。値を継承するには、*inherit* フィールドに入力します。

ステップ 15 **[ターゲット DSCP]** フィールドで、ドロップダウンリストからレイヤ 3 アウトサイド プロファイルに接続されているパスのターゲット Differentiated Services Code Point（DSCP）を選択します。

ステップ 16 **Link-local Address** フィールドに、 IPv6 リンクローカル アドレスを入力します。これは、システムによって生成された IPv6 リンクローカル アドレスをオーバーライドします。

ステップ 17 [Submit] をクリックします。`

ステップ 18 このポート チャネルのレイヤ 3 のマルチキャストを設定するかどうかを判断します。

このポート チャネルのレイヤ 3 のマルチキャストを設定するには：

a) APIC メニュー バーで、このポート チャネルに線t亡くしたレイヤ 3 アウトに移動します（**[テナント]** > **[テナント]** > **[ネットワー キング]** > **[外部ルーテッド ネットワーク]** > ***[L3Out]***）。
b) [ポリシー] タブをクリックして、レイヤ 3 アウトの [プロパティ] 画面にアクセスします。
c) レイヤ 3 アウトの [プロパティ] 画面で、PIM フィールドまでスクロールし、フィールドの隣にあるチェック ボックスをチェックして、PIM を有効にします。

   これで、このポート チャネルを含む レイヤ 3 アウトの下で、すべてのインターフェイスの PIM を有効にします。

d) 外部ルータで PIM を設定します。

   外部 ルータからポート チャネルまで PIM セッションを継続する必要があります。外部ルータで PIM の設定を行う方法については、外部ルータで受信したドキュメントを参照してください。

e) ポート チャネル L3 アウトをマルチキャストが有効な VRF にマップします。

   手順については、「IP Multicast：IP マルチキャスト （209 ページ）」を参照してください。次の点に注意してください。

   - VRF のマッピング プロセスに対して、このポート チャネル L3 の一部としてマルチキャストを有効にした状態で、特定の VRF を選択します。VRF のマルチキャストの画面で、インターフェイス エリアの L3 アウトを選択するときにこのポート チャネルに L3 アウトが表示されない場合、このポート チャネルの L3 アウトに戻り、[ポリシー] タブに移動して、適切な VRF を選択してから、[送信] と [変更の送信] をクリックします。このポート チャネルの L3 アウトは、その VRF のマルチキャスト画面で使用できます。
   - ファブリックに対して外部にあたる IP アドレスであるマルチキャストに、Rendezvous Point（RP）を設定する必要があります。スタティック RP、自動 RP、RP のブートストラップのルータを指定できます。たとえば、スタティック RP を選択すると、IP アドレスが外部ルータに存在することになり、APIC は L3 アウトを介してこの IP アドレスを学習します。詳細については、「IP Multicast：IP マルチキャスト （209 ページ）」を参照してください。

GUIを使用したレイヤ3サブインターフェイスポートチャネルの設定

この手順では、以前に作成したポート チャネルへのレイヤ 3 サブインターフェイス ルートを設定します。

始める前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチが ACI ファブリックに登録され、使用可能であること。
- ポート チャネルは、「GUI を使用したポート チャネルの設定」の手順を使用して設定します。

手順

ステップ 1 APIC メニュー バーで、**Tenants** > **Tenant** > **Networking** > **External Routed Networks** > ***L3Out*** > **Logical Node Profiles** > ***node*** > **Logical Interface Profiles** に移動します。

ステップ 2 設定するインターフェイスを選択します。そのインターフェースの **Logical Interface Profile** ページが表示されます。

ステップ 3 *Routed Sub-interfaces* をクリックします。[Properties] ページが開きます。

ステップ 4 作成 (+) ボタンをクリックして、レイヤ 3 ルーテッド サブインターフェイス ポートチャネルを設定します。**Select Routed Sub-Interface** ページが表示されます。

ステップ 5 **Path Type** フィールドで、**`Direct Port Channel`** を選択します。

ステップ 6 **[パス]** フィールドで、ドロップダウンリストから以前に作成したポート チャネルを選択します。これは、インターフェイス プロファイルのポート チャネル エンド ポイントへのパスです。

ステップ 7 **Description** フィールドに、ルーテッド インターフェイスの説明を入力します。

ステップ 8 **Encap** フィールドで、ドロップダウン メニューから **`VLAN`** を選択します。これは、レイヤ 3 外側プロファイルにアタッチされているパスのカプセル化です。このエントリの整数値を入力します。

ステップ 9 **IPv4 Primary / IPv6 Preferred Address** フィールドに、レイヤ 3 外側プロファイルにアタッチされているパスのプライマリ IP アドレスを入力します。

ステップ 10 **[IPv6 DAD]** フィールドで、**[無効]** または **[有効]** を選択します。

このフィールドの詳細については、「IPv6 ネイバー探索重複アドレス検出の設定」を参照してください。

ステップ 11 **[IPv4 セカンダリ/IPv6 追加アドレス]** フィールドに、レイヤ 3 外側プロファイルにアタッチされているパスのセカンダリ IP アドレスを入力します。

[セカンダリ IP アドレスの追加] 画面の [IPv6 DAD] フィールドの詳細については、「IPv6 ネイバー探索重複アドレス検出の設定」を参照してください。

ステップ 12 インターフェイスに対し、ネイバー探索ルータ アドバタイズメント プレフィックスを有効にする場合には、**[ND RA プレフィックス]** ボックスをオンにします。ND RA プレフィックス ポリシーのオプションが表示されます。

これを有効にすると、自動設定でルーテッドインターフェイスを使用できるようになり、プレフィックスは自動設定のためにホストに送信されます。

ND RA インターフェイス ポリシーは BD やレイヤ 3 Out に導入されるのに対し、ND プレフィックスポリシーは個々のサブネットに導入されます。ND プレフィックスポリシーはサブネットレベルにあります。

ND RA プレフィックスは、IPv6 アドレスにのみ適用されます。

ステップ 13 **[ND RA プレフィックス]** ボックスをオンにした場合、使用する ND RA プレフィックス ポリシーを選択します。デフォルト ポリシーを選択することもできますし、独自の ND RA プレフィックス ポリシーを作成することもできます。独自のポリシーを作成する場合は、[Create ND RA Prefix Policy] 画面が表示されます。

a) **Name** フィールドに、プレフィックス ポリシーのルータ アドバタイズメント (RA) 名を入力します。
b) **Description** フィールドに、プレフィックスポリシーの説明を入力します。
c) **[コントローラ状態]** フィールドで、コントローラの管理状態に適したチェック ボックスをオンにします。複数のボックスをオンにできます。デフォルトは **[自動設定]** および **[オンリンク]** です。
d) **Valid Prefix Lifetime** フィールドで、プレフィックスを有効にする期間について適切な値を選択します。有効な範囲は 0 ～ 4294967295 ミリ秒です。デフォルト値は 2592000 です。
e) **[優先プレフィックス ライフタイム]** フィールドで、プレフィックスの優先有効期間について適切な値を選択します。有効な範囲は 0 ～ 4294967295 ミリ秒です。デフォルト値は 604800 です。
f) **Submit** をクリックします。

ステップ 14 **[MAC アドレス]** フィールドに、レイヤ 3 外側プロファイルにアタッチされているパスの MAC アドレスを入力します。

ステップ 15 **[MTU（バイト）]** フィールドで、外部ネットワークの最大転送単位を設定します。指定できる範囲は 576 ～ 9216 です。値を継承するには、*inherit* フィールドに入力します。

ステップ 16 **Link-local Address** フィールドに、IPv6 リンクローカル アドレスを入力します。これは、システムによって生成された IPv6 リンクローカル アドレスをオーバーライドします。

確認：vpc が適切に設定されていることを確認するには、外部スイッチがアタッチされているリーフ スイッチ上で、CLI コマンド **show int** を使用します。

ステップ 17 [送信（Submit）] をクリックします。

ポート チャネルの NX-OS は、CLI を使用してをルーテッド レイヤ 3 の設定

この手順では、レイヤ 3 ルーテッドポート チャネルを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**leaf** *node-id* 例： `apic1(config)# leaf 101`	リーフ スイッチまたはリーフ スイッチの設定を指定します。*Node-id* は形式 *node-id1-node-id2* の単一ノード ID またはID の範囲となる可能性があり、設定が適用されます。
ステップ 3	**interface port-channel** *channel-name* 例： `apic1(config-leaf)# interface port-channel po1`	指定したポート チャネルのインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**no switchport** 例： `apic1(config-leaf-if)# no switchport`	レイヤ 3 インターフェイスを可能になります。
ステップ 5	**vrf member** *vrf-name* **tenant** *tenant-name* 例： `apic1(config-leaf-if)# vrf member v1 tenant t1`	この仮想ルーティングおよび転送(VRF)インスタンスと L3 ポリシー、外部には、このポートチャネルを関連付けます場所。 • *Vrf-name* は VRF 名です。32 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。 • テナント名 は、テナント名です。32 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。

	コマンドまたはアクション	目的
ステップ 6	**vlan-domain member** *vlan-domain-name* 例： `apic1(config-leaf-if)# vlan-domain member dom1`	以前に設定された VLAN ドメインには、ポートチャネルのテンプレートを関連付けます。
ステップ 7	**ip address** *ip-address* / *subnet-mask* 例： `apic1(config-leaf-if)# ip address 10.1.1.1/24`	指定した インターフェイスの IP アドレスとサブネット マスクを設定します。
ステップ 8	**ipv6 address** *sub-bits*/*prefix-length* **preferred** 例： `apic1(config-leaf-if)# ipv6 address 2001::1/64 preferred`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。場所： • *sub-bits* i引数は、prefix-name 引数で指定された一般的なプレフィックスによって提供されるプレフィックスに連結する、アドレスのサブプレフィックス ビットおよびホスト ビットです。sub-bits 引数は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16進数値を 16 ビット単位でコロンで区切って指定します。 • *Prefix-length* は IPv6 プレフィックスの長さです。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
ステップ 9	**ipv6 link-local** *ipv6-link-local-address* 例： `apic1(config-leaf-if)# ipv6 link-local fe80::1`	インターフェイスに IPv6 リンクローカル アドレスを設定します。
ステップ 10	**mac-address** *mac-address* 例： `apic1(config-leaf-if)# mac-address 00:44:55:66:55::01`	インターフェイス MAC アドレスを手動で設定します。

	コマンドまたはアクション	目的
ステップ 11	**mtu** *mtu-value* 例： `apic1(config-leaf-if)# mtu 1500`	このサービス クラスの MTU を設定します

例

この例では、基本レイヤ 3 ポート チャネルを設定する方法を示します。

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface port-channel po1
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vrf member v1 tenant t1
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# ip address 10.1.1.1/24
apic1(config-leaf-if)# ipv6 address 2001::1/64 preferred
apic1(config-leaf-if)# ipv6 link-local fe80::1
apic1(config-leaf-if)# mac-address 00:44:55:66:55::01
apic1(config-leaf-if)# mtu 1500
```

NX-OS CLI を使用したレイヤ 3 サブインターフェイス ポート チャネルの設定

この手順では、レイヤ 3 サブインターフェイス ポート チャネルを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**leaf** *node-id* 例： `apic1(config)# leaf 101`	リーフ スイッチまたはリーフ スイッチの設定を指定します。*Node-id* は形式 *node-id1-node-id2* の単一ノード ID または ID の範囲となる可能性があり、設定が適用されます。
ステップ 3	**vrf member** *vrf-name* **tenant** *tenant-name* 例：	この仮想ルーティングおよび転送(VRF)インスタンスと L3 アウトサイド ポリ

	コマンドまたはアクション	目的
	`apic1(config-leaf-if)# vrf member v1 tenant t1`	シーにポート チャネルを関連付けます。場所： • *Vrf-name* は VRF 名です。32 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。 • テナント名 は、テナント名です。32 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。
ステップ 4	**vlan-domain member** *vlan-domain-name* 例： `apic1(config-leaf-if)# vlan-domain member dom1`	以前に設定された VLAN ドメインには、ポートチャネルのテンプレートを関連付けます。
ステップ 5	**ip address** *ip-address* / *subnet-mask* 例： `apic1(config-leaf-if)# ip address 10.1.1.1/24`	指定した インターフェイスの IP アドレスとサブネット マスクを設定します。
ステップ 6	**ipv6 address** *sub-bits*/*prefix-length* **preferred** 例： `apic1(config-leaf-if)# ipv6 address 2001::1/64 preferred`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。場所： • *sub-bits* i引数は、prefix-name 引数で指定された一般的なプレフィックスによって提供されるプレフィックスに連結する、アドレスのサブプレフィックス ビットおよびホスト ビットです。sub-bits 引数は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16進数値を 16 ビット単位でコロンで区切って指定します。 • *Prefix-length* は IPv6 プレフィックスの長さです。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10

	コマンドまたはアクション	目的
		進数値の前にスラッシュ記号が必要です。
ステップ 7	**ipv6 link-local** *ipv6-link-local-address* 例： `apic1(config-leaf-if)# ipv6 link-local fe80::1`	インターフェイスにIPv6リンクローカル アドレスを設定します。
ステップ 8	**mac-address** *mac-address* 例： `apic1(config-leaf-if)# mac-address 00:44:55:66:55::01`	インターフェイス MAC アドレスを手動で設定します。
ステップ 9	**mtu** *mtu-value* 例： `apic1(config-leaf-if)# mtu 1500`	このサービス クラスの MTU を設定します
ステップ 10	exit 例： `apic1(config-leaf-if)# exit`	設定モードに戻ります。
ステップ 11	**interface port-channel** *channel-name* 例： `apic1(config-leaf)# interface port-channel po1`	指定したポート チャネルのインターフェイス コンフィギュレーション モードを開始します。
ステップ 12	**vlan-domain member** *vlan-domain-name* 例： `apic1(config-leaf-if)# vlan-domain member dom1`	以前に設定された VLAN ドメインには、ポートチャネルのテンプレートを関連付けます。
ステップ 13	exit 例： `apic1(config-leaf-if)# exit`	設定モードに戻ります。
ステップ 14	**interface port-channel** *channel-name.number* 例： `apic1(config-leaf)# interface port-channel po1.2001`	指定したサブインターフェイス ポート チャネルのインターフェイス設定モードを開始します。
ステップ 15	**vrf member** *vrf-name* **tenant** *tenant-name* 例： `apic1(config-leaf-if)# vrf member v1 tenant t1`	この仮想ルーティングおよび転送(VRF)インスタンスと L3 アウトサイド ポリシーにポート チャネルを関連付けます。場所：

	コマンドまたはアクション	目的
		• *Vrf-name* は VRF 名です。32 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。 • テナント名 は、テナント名です。32 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。
ステップ 16	exit 例： `apic1(config-leaf-if)# exit`	設定モードに戻ります。

例

この例では、基本的なレイヤ 3 サブインターフェイス ポートチャネルを設定する方法を示します。

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface vlan 2001
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vrf member v1 tenant t1
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# ip address 10.1.1.1/24
apic1(config-leaf-if)# ipv6 address 2001::1/64 preferred
apic1(config-leaf-if)# ipv6 link-local fe80::1
apic1(config-leaf-if)# mac-address 00:44:55:66:55::01
apic1(config-leaf-if)# mtu 1500
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface port-channel po1
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface port-channel po1.2001
apic1(config-leaf-if)# vrf member v1 tenant t1
apic1(config-leaf-if)# exit
```

NX-OS CLI を使用したレイヤ 3 ポート チャネルにポートを追加する

この手順では、以前に設定したレイヤ 3 ポート チャネルにポートを追加します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**leaf** *node-id* 例： `apic1(config)# leaf 101`	リーフ スイッチまたはリーフ スイッチの設定を指定します。*Node-id* は形式 *node-id1-node-id2* の単一ノード ID または ID の範囲となる可能性があり、設定が適用されます。
ステップ 3	**interface Ethernet** *slot/port* 例： `apic1(config-leaf)# interface Ethernet 1/1-2`	設定するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**channel-group** チャネル名 例： `apic1(config-leaf-if)# channel-group p01`	チャネル グループでポートを設定します。

例

この例では、ポートをレイヤ 3 にポートチャネルを追加する方法を示します。

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface Ethernet 1/1-2
apic1(config-leaf-if)# channel-group p01
```

REST API を使用したポート チャネルの設定

始める前に

（注） このセクションで説明する手順は、レイヤ 3 ルーテッドまたはサブインターフェイス ポート チャネルを設定するための手順に対する前提条件として、特にポート チャネルを設定することを意図しています。一般的なリーフ スイッチの設定手順については、「*Cisco APIC* 基本設定ガイド」または「*Cisco APIC* レイヤ *2* ネットワー キング設定ガイド」を参照してください。

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチが ACI ファブリックに登録され、使用可能であること。

（注） 次の REST API 例では、長い 1 行のテキストは \ で分けて読みやすくします。

手順

REST API を使用してポート チャネルを設定するには、次ののように XML で POST 送信します。

例：

```
<polUni>
<infraInfra dn="uni/infra">
        <infraNodeP name="test1">
             <infraLeafS name="leafs" type="range">
                  <infraNodeBlk name="nblk" from_="101" to_="101"/>
             </infraLeafS>
             <infraRsAccPortP tDn="uni/infra/accportprof-test1"/>
       </infraNodeP>
        <infraAccPortP name="test1">
             <infraHPortS name="pselc" type="range">
                   <infraPortBlk name="blk1" fromCard="1" toCard="1" fromPort="18" \
                    toPort="19"/>
                   <infraRsAccBaseGrp tDn="uni/infra/funcprof/accbundle-po17_PolGrp"/>
             </infraHPortS>
        </infraAccPortP>

        <infraFuncP>
             <infraAccBndlGrp name="po17_PolGrp" lagT="link">
                  <infraRsHIfPol  tnFabricHIfPolName="default"/>
                  <infraRsCdpIfPol tnCdpIfPolName="default"/>
                  <infraRsLacpPol tnLacpLagPolName="default"/>
             </infraAccBndlGrp>
        </infraFuncP>

</infraInfra>
</polUni>
```

次のタスク

REST API を使用してレイヤ 3 ルーテッドポート チャネルまたはサブインターフェイス ポート チャネルを設定します。

REST API を使用したレイヤ 3 ルーテッド ポート チャネルの設定

始める前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチが ACI ファブリックに登録され、使用可能であること。
- ポート チャネルは、「REST API を使用したポート チャネルの設定」の手順を使用して設定されます。

（注） 次の REST API 例では、1 つ以上の行のテキストはで区分するが、\ 読みやすさを改善する文字。

手順

REST API を使用して以前作成したポート チャネルにレイヤ 3 ルートを設定するには、次のように XML で post を送信します。

例：

```
<polUni>
<fvTenant name=pep9>
    <l3extOut descr="" dn="uni/tn-pep9/out-routAccounting" enforceRtctrl="export" \
     name="routAccounting" nameAlias="" ownerKey="" ownerTag="" \
     targetDscp="unspecified">
        <l3extRsL3DomAtt tDn="uni/l3dom-Dom1"/>
        <l3extRsEctx tnFvCtxName="ctx9"/>
        <l3extLNodeP configIssues="" descr="" name="node101" nameAlias="" ownerKey="" \
         ownerTag="" tag="yellow-green" targetDscp="unspecified">
            <l3extRsNodeL3OutAtt rtrId="10.1.0.101" rtrIdLoopBack="yes" \
             tDn="topology/pod-1/node-101">
                <l3extInfraNodeP descr="" fabricExtCtrlPeering="no" \
                 fabricExtIntersiteCtrlPeering="no" name="" nameAlias="" spineRole=""/>
            </l3extRsNodeL3OutAtt>
            <l3extLIfP descr="" name="lifp17" nameAlias="" ownerKey="" ownerTag="" \
             tag="yellow-green">
                <ospfIfP authKeyId="1" authType="none" descr="" name="" nameAlias="">
                    <ospfRsIfPol tnOspfIfPolName=""/>
                </ospfIfP>
                <l3extRsPathL3OutAtt addr="10.1.5.3/24" autostate="disabled" descr="" \
                 encap="unknown" encapScope="local" ifInstT="l3-port" llAddr="::" \
                 mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit" \
                 tDn="topology/pod-1/paths-101/pathep-[po17_PolGrp]" \
```

```
                 targetDscp="unspecified"/>
                <l3extRsNdIfPol tnNdIfPolName=""/>
                <l3extRsIngressQosDppPol tnQosDppPolName=""/>
                <l3extRsEgressQosDppPol tnQosDppPolName=""/>
            </l3extLIfP>
        </l3extLNodeP>
        <l3extInstP descr="" floodOnEncap="disabled" matchT="AtleastOne" \
         name="accountingInst" nameAlias="" prefGrMemb="exclude" prio="unspecified" \
         targetDscp="unspecified">
            <fvRsProv matchT="AtleastOne" prio="unspecified" tnVzBrCPName="webCtrct"/>
           <l3extSubnet aggregate="export-rtctrl,import-rtctrl" descr="" ip="0.0.0.0/0"
 \
             name="" nameAlias="" scope="export-rtctrl,import-rtctrl,import-security"/>
            <l3extSubnet aggregate="export-rtctrl,import-rtctrl" descr="" ip="::/0" \
             name="" nameAlias="" scope="export-rtctrl,import-rtctrl,import-security"/>
            <fvRsCustQosPol tnQosCustomPolName=""/>
        </l3extInstP>
        <l3extConsLbl descr="" name="golf" nameAlias="" owner="infra" ownerKey="" \
         ownerTag="" tag="yellow-green"/>
    </l3extOut>
</fvTenant>
</polUni>
```

REST API を使用して、レイヤ 3 サブインターフェイス ポート チャネルの設定

始める前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチが ACI ファブリックに登録され、使用可能であること。
- ポート チャネルは、「REST API を使用したポート チャネルの設定」の手順を使用して設定されます。

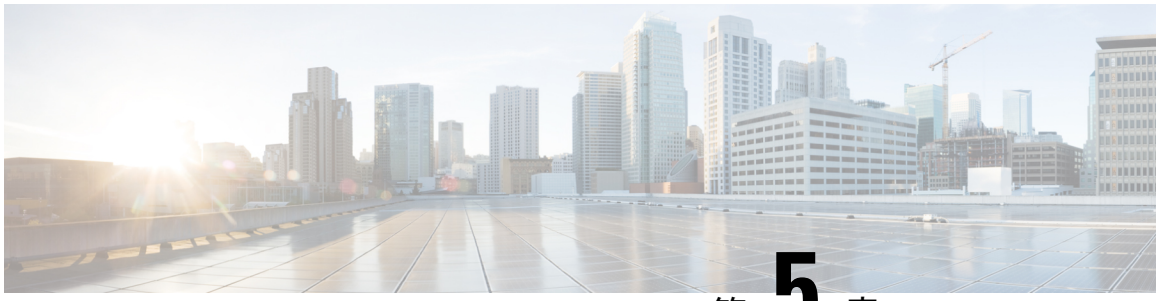
（注） 次の REST API 例では、1 つ以上の行のテキストはで区分するが、\ 読みやすさを改善する文字。

手順

REST API を使用して、以前に作成したポート チャネルをレイヤ 3 サブインターフェイス ルートを設定するには、次のようには、XML で post を送信します。

例：

```
<polUni>
<fvTenant name=pep9>
    <l3extOut descr="" dn="uni/tn-pep9/out-routAccounting" enforceRtctrl="export" \
     name="routAccounting" nameAlias="" ownerKey="" ownerTag="" targetDscp="unspecified">

        <l3extRsL3DomAtt tDn="uni/l3dom-Dom1"/>
        <l3extRsEctx tnFvCtxName="ctx9"/>
        <l3extLNodeP configIssues="" descr="" name="node101" nameAlias="" ownerKey="" \
         ownerTag="" tag="yellow-green" targetDscp="unspecified">
            <l3extRsNodeL3OutAtt rtrId="10.1.0.101" rtrIdLoopBack="yes" \
             tDn="topology/pod-1/node-101">
                <l3extInfraNodeP descr="" fabricExtCtrlPeering="no" \
                 fabricExtIntersiteCtrlPeering="no" name="" nameAlias="" spineRole=""/>
            </l3extRsNodeL3OutAtt>
            <l3extLIfP descr="" name="lifp27" nameAlias="" ownerKey="" ownerTag="" \
             tag="yellow-green">
                <ospfIfP authKeyId="1" authType="none" descr="" name="" nameAlias="">
                    <ospfRsIfPol tnOspfIfPolName=""/>
                </ospfIfP>
                <l3extRsPathL3OutAtt addr="11.1.5.3/24" autostate="disabled" descr="" \
                 encap="vlan-2001" encapScope="local" ifInstT="sub-interface" \
                 llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit" \
                 tDn="topology/pod-1/paths-101/pathep-[po27_PolGrp]" \
                 targetDscp="unspecified"/>
                <l3extRsNdIfPol tnNdIfPolName=""/>
                <l3extRsIngressQosDppPol tnQosDppPolName=""/>
                <l3extRsEgressQosDppPol tnQosDppPolName=""/>
            </l3extLIfP>
        </l3extLNodeP>
        <l3extInstP descr="" floodOnEncap="disabled" matchT="AtleastOne" \
         name="accountingInst" nameAlias="" prefGrMemb="exclude" prio="unspecified" \
         targetDscp="unspecified">
            <fvRsProv matchT="AtleastOne" prio="unspecified" tnVzBrCPName="webCtrct"/>
           <l3extSubnet aggregate="export-rtctrl,import-rtctrl" descr="" ip="0.0.0.0/0"
 \
             name="" nameAlias="" scope="export-rtctrl,import-rtctrl,import-security"/>
            <l3extSubnet aggregate="export-rtctrl,import-rtctrl" descr="" ip="::/0" \
             name="" nameAlias="" scope="export-rtctrl,import-rtctrl,import-security"/>
            <fvRsCustQosPol tnQosCustomPolName=""/>
        </l3extInstP>
        <l3extConsLbl descr="" name="golf" nameAlias="" owner="infra" ownerKey="" \
         ownerTag="" tag="yellow-green"/>
    </l3extOut>
</fvTenant>
</polUni>
```



第 5 章

L3Outs の QoS

この章の内容は、次のとおりです。

L3Outs の QoS

L3Out の QoS ポリシーを設定するには、次のガイドラインを使用します。

- L3Outがある障壁リーフに適用するQoSポリシーを設定するには、VRFが出力モード（ポリシー制御適用方向は「出力」にする必要があります）である必要があります。
- 適用するQoSポリシーを有効にするには、VRFポリシー制御適用設定を「適用」にする必要があります。
- L3Outとその他のEPG間の通信を制御する契約を設定する際に、契約またはサブジェクトのQoSクラスまたはターゲットDSCPを含めます。

（注） 外部 EPG ではなく、契約の QoS クラスまたはターゲット DSCP のみ設定します（`l3extInstP`）。

REST API を使用した L3Outs の QoS の設定

L3Out の QoS は、L3Out 設定の一部として設定されます。

手順

ステップ 1 テナント、VRF、ブリッジ ドメインを設定する場合、ポリシー適用が有効になっている状態で、出力モードに VRF を設定します（`pcEnfDir="egress"`）。次の例のように XML で post を送信します。

例：

```
<fvTenant  name="t1">
      <fvCtx name="v1" pcEnfPref="enforced" pcEnfDir="egress"/>
        <fvBD name="bd1">
            <fvRsCtx tnFvCtxName="v1"/>
            <fvSubnet ip="44.44.44.1/24" scope="public"/>
            <fvRsBDToOut tnL3extOutName="l3out1"/>
        </fvBD>"/>
</fvTenant>
```

ステップ 2 通信のため L3Out に参加して EPG を有効にする契約を作成するときは、優先順位の QoS を設定します。

この例のコントラクトには、L3Out で出力されるトラフィックの `level1` の QoS 優先順位を含みますまたは、ターゲットの DSCP 値を定義する可能性があります。QoS ポリシーは、契約またはサブジェクトのいずれかでサポートされます。

フィルタに matchDscp =「Ef」条件があるため、このタグを持つトラフィックがコントラクト件名で指定されたキューを通して L3out プロセスにより受信できます。

例：

```
<vzFilter name="http-filter">
     <vzEntry  name="http-e" etherT="ip" prot="tcp" matchDscp="EF"/>
</vzFilter>
<vzBrCP name="httpCtrct" prio="level1" scope="context">
     <vzSubj name="subj1">
          <vzRsSubjFiltAtt tnVzFilterName="http-filter"/>
     </vzSubj>
</vzBrCP>
```

NX-OS スタイルの CLI を使用した L3Outs の QoS の設定

L3Out の QoS は、L3Out 設定の一部として設定されます。

手順

ステップ 1 L3Out で QoS 優先順位の適用をサポートするには、テナントと、VRF を設定するときに出力モードの VRF を設定し、次のコマンドを使用して、ポリシーの適用を有効に。

例：

```
apic1# configure
apic1(config)# tenant t1
apic1(config-tenant)# vrf context v1
```

```
apic1(config-tenant-vrf)# contract enforce egress
apic1(config-tenant-vrf)# exit
apic1(congig-tenant)# exit
apic1(config)#
```

ステップ 2 フィルタ (アクセス リスト) を作成するときに含める、 **dscp を一致** コマンドで、ターゲット DSCP では、この例ではレベル EF。契約を設定するときなど、QoS クラスを含める レベル 1 、L3Out でトラフィック ingressing の。または、ターゲットの DSCP 値を定義する可能性があります。QoS ポリシーは、契約またはサブジェクトのいずれかでサポートされます。

例：

```
apic1(config)# tenant t1
apic1(config-tenant)# access-list http-filter
apic1(config-tenant-acl)# match ip
apic1(config-tenant-acl)# match tcp dest 80
apic1(config-tenant-acl)# match dscp EF
apic1(config-tenant-acl)# exit
apic1(config-tenant)# contract httpCtrct
apic1(config-tenant-contract)# scope vrf
apic1(config-tenant-contract)# qos-class level1
apic1(config-tenant-contract)# subject http-subject
apic1(config-tenant-contract-subj)# access-group http-filter both
apic1(config-tenant-contract-subj)# exit
apic1(config-tenant-contract)# exit
```

GUI を使用した L3Out の QoS の設定

L3Out の QoS は、L3Out 設定の一部として設定されます。

手順

ステップ 1 L3Out により使用される境界リーフに適用されるQoS をサポートするために、 L3Out を利用していたテナントの VRF を設定します。

a) メニュー バーで、**Tenants** > ***tenant-name*** を選択します。
b) **Navigation** ウィンドウで、**Networking** を展開し、**VRFs** を右クリックし、 **Create VRF** を選択します。
c) VRF の名前を入力します。
d) **Policy Control Enforcement Preference** フィールドで、**Enforced** を選択します。
e) **Policy Control Enforcement Dirction** で、**Egress** を選択します。
f) L3Out の要件に従って VRF を設定します。

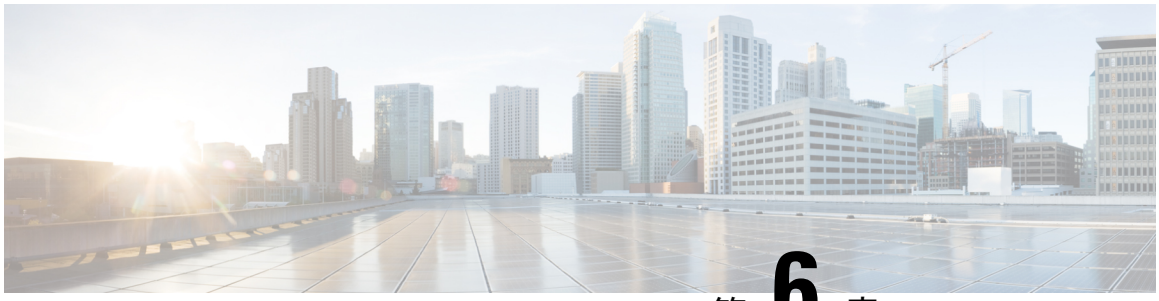
ステップ 2 L3Out を使用する EPG の間の通信を可能にするためにフィルタを設定するときには、QoS クラスまたはターゲット DSCP を含めて、L3Out を通して入力されるトラフィックにおける QoS の優先順位を適用します。

a) [Navigation] ウィンドウの L3Out を使用するテナントで、**Contracts** を展開し、**Filters** を右クリックし、**Create Filter** を選択します。

b) **Name** フィールドに、ファイルの名前を入力します。
c) **Entries** フィールドで、[+] をクリックしてフィルタ エントリを追加します。
d) エントリの詳細を追加し、**Update** をクリックし、**Submit** をクリックします。
e) 以前に作成したフィルタを展開し、フィルタ エントリをクリックします。
f) **Match DSCP** フィールドを、そのエントリで必要な DSCP レベルに設定します。たとえば **EF** にします。

ステップ 3 契約を追加するには、次の手順を実行します:

a) **Contracts** の下で、**Standard** を右クリックして、**Create Contract** を選択します。
b) 契約の名前を入力します。
c) **QoS Class** フィールドで、この契約で管理されるトラフィックの QoS 優先順位を選択します。または、**Target DSCP** の値を選択することもできます。
d) **Subjects** の [+] アイコンをクリックして、情報カテゴリを契約に追加します。
e) 情報カテゴリの名前を入力します。
f) **Filter Chain** の下で、**Filters** の [+] アイコンをクリックし、先ほど作成したフィルタをドロップダウンリストから選択します。
g) **Update** をクリックします。
h) **Create Contract Subject** ダイアログボックスで、**OK** をクリックします。



第 6 章

ルーティング プロトコル サポート

この章の内容は、次のとおりです。

概要

ルーティング プロトコル サポート

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。

BGP 外部ルーテッド ネットワークと BFD のサポート

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。

- リーフ スイッチにルータ ID を作成すると、必ず内部ループバック アドレスが作成されます。リーフ スイッチに BGP 接続をセットアップする場合、ルート ID をインターフェイスの IP アドレスと同じにすることはできません。これは、その設定が ACI リーフ スイッチではサポートされていないためです。ルータ ID は、別のサブネット内の別のアドレスである必要があります。外部レイヤ 3 デバイスでは、ルータ ID はループバック アドレスまたはインターフェイス アドレスです。スタティック ルートまたは OSPF 設定のいずれかを使用して、レイヤ 3 デバイスのルーティング テーブルにリーフ ルータ ID へのルートが存在することを確認してください。また、レイヤ 3 デバイスに BGP ネイバーをセットアッ

プする場合、使用するピア IP アドレスはリーフ スイッチのルータ ID である必要があります。

- BGP を使用する 2 つの外部レイヤ 3 ネットワークを同じノードに設定する際、ループバック アドレスを明示的に定義する必要があります。このガイドラインに従わないと、BGP を確立できない可能性があります。
- 定義上、ルータ ID はループバック インターフェイスです。ルータ ID を変更してループバックに別のアドレスを割り当てるには、ループバック インターフェイス ポリシーを作成する必要があります（ループバック ポリシーは、アドレス ファミリ、IPv4、および IPv6 ごとに 1 つずつ設定できます）。ループバック ポリシーを作成しない場合は、ルータ ID ループバック（デフォルトで有効）を有効にすることができます。ルータ ID ループバックが無効である場合、導入先の特定のレイヤ 3 Outside に対するループバックは作成されません。
- この設定作業は iBGP および eBGP に適用されます。BGP 設定がループバック アドレスに対するものである場合、iBGP セッションまたはマルチホップ eBGP セッションです。ピア IP アドレスが BGP ピアが定義されている物理インターフェイスに対するものである場合、物理インターフェイスが使用されます。
- 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、ユーザが IPv6 アドレスを設定する必要があります。
- 自律システム機能は eBGP ピアでしか使用できません。この機能では、ルータが実際の AS に加えて、2 番めの自律システム（AS）のメンバであるように見せることができます。ローカル AS を使用すると、ピアリングの調整を変更せずに 2 つの ISP をマージできます。マージされた ISP 内のルータは、新しい自律システムのメンバになりますが、使用者に対しては古い自律システム番号を使用し続けます。
- リリース 1.2（1x）以降、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設定できます。これにより、ピアから受信されるルート 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。拒否オプションが導入されると、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、APIC でエラーが発生します。

（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 multipod 接続を設定する場合は、MTU が両側で適切に設定されていることが重要です。ACI、Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定された MTU 値は IP ヘッダーを考慮に入れています（結果として、最大パケット サイズは、ACI で 9216 バイト、NX-OS および IOS で 9000 バイトに設定されます）。ただし、IOS XR などの他のプラットフォームは、パケット ヘッダーのを除く MTU 値を設定します（結果として最大パケット 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	いいえ（No）	該当なし	いいえ
iBGP ループバック ピアリング	はい（BGP ピア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	いいえ（No）	該当なし	いいえ
eBGP ループバック ピアリング（マルチホップ）	はい（BGP ピア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）	○

BGP 外部ルーテッド ネットワークの設定

GUI を使用した BGP 外部ルーテッド ネットワークの設定

始める前に

外部ルーテッド ネットワークを設定するテナント、VRF、およびブリッジ ドメインがすでに作成されていること。

手順

ステップ 1 [Navigation] ペインで、**[Tenant_name]** > **[Networking]** > **[External Routed Networks]** を展開します。

ステップ 2 右クリックし、[Create Routed Outside] をクリックします。

ステップ 3 [Create Routed Outside] 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、外部ルーテッド ネットワーク ポリシーの名前を入力します。

b) [BGP] チェックボックスをクリックします。

（注） 次の 2 つの方法のいずれかで、BGP ピアの到達可能性を使用できるようになっている必要があります。スタティック ルートを設定するか、または OSPF を有効にする必要があります。

c) （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。

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

e) [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 プロファイルを作成するオプションがあります。

f) [Nodes and Interfaces Protocol Policies] を展開します。

g) [Create Node Profile] ダイアログボックスに、ノード プロファイルの名前を入力します。

h) [Nodes] を展開します。

i) [Select Node] ダイアログボックスの [Node ID] フィールドのドロップダウン リストから、ノードを選択します。

j) [Router ID] フィールドに、ルータ ID を入力します。

k) [Loopback Address] を展開し、[IP] フィールドに IP アドレスを入力します。[Update] をクリックします。

（注） IPv6 アドレスを入力します。前のステップでルータ ID を追加しなかった場合は、[IP] フィールドに IPv4 アドレスを追加できます。

l) [OK] をクリックします。

ステップ 4 [Navigation] ペインで、**[Tenant_name]** > **[Networking]** > **[Route Profiles]** の順に展開します。[Route Profiles] を右クリックし、[Create Route Profile] をクリックします。[Create Route 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、ルート制御 VRF の名前を入力します。
b) [Create Route Control Context] ダイアログボックスを展開します。
c) [Name] フィールドに、ルート制御 VRF の名前を入力します。
d) [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。

ステップ 5 [Create Interface Profiles] 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、インターフェイス プロファイル名を入力します。
b) [Interfaces] 領域で、目的のインターフェイス タブを選択し、インターフェイスを展開します。

ステップ 6 [Select Routed Interface] ダイアログボックスで、次の操作を実行します。

a) [Path] ドロップダウン リストから、ノードおよびインターフェイスを選択します。
b) [IP Address] フィールドに、IP アドレスを入力します。

（注） 必要に応じて、IPv6 アドレスまたは IPv4 アドレスを追加できます。

c) （任意） 前のステップで IPv6 アドレスを入力した場合は、[Link-local Address] フィールドに IPv6 アドレスを入力します。
d) [BGP Peer Connectivity Profile] フィールドを展開します。

ステップ 7 [Create Peer Connectivity Profile] ダイアログボックスで、次の操作を実行します。

a) [Peer Address] フィールドでは、ダイナミック ネイバー機能を使用できます。必要に応じて、指定されたサブネット内のすべてのピアが BGP と通信またはルートを交換できます。

手順内の前のステップで入力した IPv4 または IPv6 のアドレスに対応する IPv4 または IPv6 のアドレスを入力します。

b) [BGP Controls] フィールドで、目的の制御をオンにします。
c) [Autonomous System Number] フィールドで、目的の値を選択します。
d) （任意） [Weight for routes from this neighbor] フィールドで、目的の値を選択します。
e) （任意） [Private AS Control] フィールドで、[Remove AS] のチェックボックスをオンにします。
f) （任意） [Local Autonomous System Number Config] 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。

g) （任意） [Local Autonomous System 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。

（注） このフィールドの値は、[Autonomous System Number] フィールドの値と同じであってはなりません。

h) [OK] をクリックします。

ステップ 8 次のアクションを実行します。

a) [Select Routed Interface] ダイアログボックスで、[OK] をクリックします。
b) [Create Interface Profile] ダイアログボックスで、[OK] をクリックします。
c) [Create Node Profile] ダイアログボックスで、[OK] をクリックします。
[External EPG Networks] 領域が表示されます。
d) [Create Routed Outside] ダイアログボックスで、前に作成したノード プロファイルを選択し、[Next] をクリックします。

ステップ 9 [External EPG Networks] を展開し、[Create External Network] 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、外部ネットワークの名前を入力します。
b) [Subnet] を展開します。
c) [Create Subnet] ダイアログボックスの [IP address] フィールドに、必要に応じてサブネットアドレスを入力します。

（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。

d) [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。

ステップ 10 **[Create External Network]** ダイアログボックスで、**[OK]** をクリックします。

ステップ 11 **[Create Routed Outside]** ダイアログボックスで、**[Finish]** をクリックします。
eBGP は外部接続用に設定されています。

NX-OS スタイルの CLI を使用した BGP 外部ルーテッド ネットワークの設定

手順

ここでは、NX-OS CLI を使用して BGP 外部ルーテッド ネットワークを設定する方法を示します。

例：

```
apic1(config-leaf)#template route-profile damp_rp tenant t1
This template will be available on all leaves where tenant t1 has a VRF deployment
apic1(config-leaf-template-route-profile)#set dampening 15 750 2000 60
apic1(config-leaf-template-route-profile)#exit
apic1(config-leaf)#
apic1(config-leaf)#router bgp 100
apic1(config-bgp)#vrf member tenant t1 vrf ctx3
apic1(config-leaf-bgp-vrf)# neighbor 32.0.1.0/24 l3out l3out-bgp
apic1(config-leaf-bgp-vrf-neighbor)#update-source ethernet 1/16.401
apic1(config-leaf-bgp-vrf-neighbor)#address-family ipv4 unicast
apic1(config-leaf-bgp-vrf-neighbor-af)#weight 400
apic1(config-leaf-bgp-vrf-neighbor-af)#exit
apic1(config-leaf-bgp-vrf-neighbor)#remote-as 65001
apic1(config-leaf-bgp-vrf-neighbor)#private-as-control remove-exclusive
apic1(config-leaf-bgp-vrf-neighbor)#private-as-control remove-exclusive-all
apic1(config-leaf-bgp-vrf-neighbor)#private-as-control remove-exclusive-all-replace-as
apic1(config-leaf-bgp-vrf-neighbor)#exit
apic1(config-leaf-bgp-vrf)# address-family ipv4 unicast
apic1(config-leaf-bgp-vrf-af)#inherit bgp dampening damp_rp
This template will be inherited on all leaves where VRF ctx3 has been deployed
apic1(config-leaf-bgp-vrf-af)#exit
apic1(config-leaf-bgp-vrf)# address-family ipv6 unicast
apic1(config-leaf-bgp-vrf-af)#inherit bgp dampening damp_rp
This template will be inherited on all leaves where VRF ctx3 has been deployed
apic1(config-leaf-bgp-vrf-af)#exit
```

REST API を使用した BGP 外部ルーテッド ネットワークの設定

始める前に

外部ルーテッド ネットワークを設定するテナントがすでに作成されていること。

ここでは、REST API を使用して BGP 外部ルーテッド ネットワークを設定する方法を示します。

例：

手順

例：

```
<l3extOut descr="" dn="uni/tn-t1/out-l3out-bgp" enforceRtctrl="export" name="l3out-bgp"
 ownerKey="" ownerTag="" targetDscp="unspecified">
<l3extRsEctx tnFvCtxName="ctx3"/>
<l3extLNodeP configIssues="" descr="" name="l3extLNodeP_1" ownerKey="" ownerTag=""
tag="yellow-green" targetDscp="unspecified">
<l3extRsNodeL3OutAtt rtrId="1.1.1.1" rtrIdLoopBack="no" tDn="topology/pod-1/node-101"/>
<l3extLIfP descr="" name="l3extLIfP_2" ownerKey="" ownerTag="" tag="yellow-green">
<l3extRsNdIfPol tnNdIfPolName=""/>
<l3extRsIngressQosDppPol tnQosDppPolName=""/>
<l3extRsEgressQosDppPol tnQosDppPolName=""/>
<l3extRsPathL3OutAtt addr="3001::31:0:1:2/120" descr="" encap="vlan-3001"
```

```
encapScope="local" ifInstT="sub-interface" llAddr="::" mac="00:22:BD:F8:19:FF"
mode="regular" mtu="inherit" tDn="topology/pod-1/paths-101/pathep-[eth1/8]"
targetDscp="unspecified">
<bgpPeerP addr="3001::31:0:1:0/120" allowedSelfAsCnt="3" ctrl="send-com,send-ext-com"
descr="" name="" peerCtrl="bfd" privateASctrl="remove-all,remove-exclusive,replace-as"
ttl="1" weight="1000">
<bgpRsPeerPfxPol tnBgpPeerPfxPolName=""/>
<bgpAsP asn="3001" descr="" name=""/>
</bgpPeerP>
</l3extRsPathL3OutAtt>
</l3extLIfP>
<l3extLIfP descr="" name="l3extLIfP_1" ownerKey="" ownerTag="" tag="yellow-green">
<l3extRsNdIfPol tnNdIfPolName=""/>
<l3extRsIngressQosDppPol tnQosDppPolName=""/>
<l3extRsEgressQosDppPol tnQosDppPolName=""/>
<l3extRsPathL3OutAtt addr="31.0.1.2/24" descr="" encap="vlan-3001" encapScope="local"
ifInstT="sub-interface" llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
 tDn="topology/pod-1/paths-101/pathep-[eth1/8]" targetDscp="unspecified">
<bgpPeerP addr="31.0.1.0/24" allowedSelfAsCnt="3" ctrl="send-com,send-ext-com" descr=""
 name="" peerCtrl="" privateASctrl="remove-all,remove-exclusive,replace-as" ttl="1"
weight="100">
<bgpRsPeerPfxPol tnBgpPeerPfxPolName=""/>
<bgpLocalAsnP asnPropagate="none" descr="" localAsn="200" name=""/>
<bgpAsP asn="3001" descr="" name=""/>
</bgpPeerP>
</l3extRsPathL3OutAtt>
</l3extLIfP>
</l3extLNodeP>
<l3extRsL3DomAtt tDn="uni/l3dom-l3-dom"/>
<l3extRsDampeningPol af="ipv6-ucast" tnRtctrlProfileName="damp_rp"/>
<l3extRsDampeningPol af="ipv4-ucast" tnRtctrlProfileName="damp_rp"/>
<l3extInstP descr="" matchT="AtleastOne" name="l3extInstP_1" prio="unspecified"
targetDscp="unspecified">
<l3extSubnet aggregate="" descr="" ip="130.130.130.0/24" name="" scope="import-rtctrl">
</l3extSubnet>
<l3extSubnet aggregate="" descr="" ip="130.130.131.0/24" name="" scope="import-rtctrl"/>
<l3extSubnet aggregate="" descr="" ip="120.120.120.120/32" name=""
scope="export-rtctrl,import-security"/>
<l3extSubnet aggregate="" descr="" ip="3001::130:130:130:100/120" name=""
scope="import-rtctrl"/>
</l3extInstP>
<bgpExtP descr=""/>
</l3extOut>
<rtctrlProfile descr="" dn="uni/tn-t1/prof-damp_rp" name="damp_rp" ownerKey="" ownerTag=""
 type="combinable">
 <rtctrlCtxP descr="" name="ipv4_rpc" order="0">
  <rtctrlScope descr="" name="">
   <rtctrlRsScopeToAttrP tnRtctrlAttrPName="act_rule"/>
  </rtctrlScope>
 </rtctrlCtxP>
</rtctrlProfile>
<rtctrlAttrP descr="" dn="uni/tn-t1/attr-act_rule" name="act_rule">
  <rtctrlSetDamp descr="" halfLife="15" maxSuppressTime="60" name="" reuse="750"
suppress="2000" type="dampening-pol"/>
</rtctrlAttrP>
```

BGP 最大パスの設定

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 APIC GUI にログインし、**[Tenants]** > **<Your_Tenant>** > **[Networking]** > **[Protocol Policies]** > **[BGP]** > **[BGP Address Family Context]** をクリックし、**[Create BGP Address Family Context Policy]** を右クリックします。

ステップ 2 **[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。

a) **[Name]** フィールドにポリシーの名前を入力します。
b) **[eBGP Distance]** フィールドをクリックして、実装の値を確認します。
c) **[iBGP Distance]** フィールドをクリックして、実装の値を確認します。
d) **[Local Distance]** フィールドをクリックして、実装の値を確認します。
e) **[eBGP Max ECMP]** フィールドをクリックして、実装の値を確認します。
f) **[iBGP Max ECMP]** フィールドをクリックして、実装の値を確認します。
g) エントリを更新した後、**[Submit]** をクリックします。

ステップ 3 **[Tenants]** > **<Your_Tenant>** > **[Networking]** > **[VRFs]** > **<your_VRF>** をクリックします。

ステップ 4 対象の VRF の設定の詳細を確認します。

ステップ 5 **[BGP Context Per Address Family]** フィールドにアクセスし、[Address Family] ドロップダウン リストで [Ipv6] を選択します。

ステップ 6 **[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 7 [送信（Submit）] をクリックします。

NX-OS スタイルの CLI を使用した BGP 最大パスの設定

始める前に

適切なテナントと BGP 外部ルーテッド ネットワークが作成され、使用可能になっています。

さらに多くのパスを設定できるようにする 2 つのプロパティは、bgpCtxAfPol オブジェクトの maxEcmp と maxEcmpIbgp です。これら 2 つのプロパティを設定した後、実装の残り部分に反映されます。

BGP にログインして、次のコマンドを使用します:

```
maximum-paths [ibgp]
```

```
no maximum-paths [ibgp]
```

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# template bgp address-family newAf tenant t1
This template will be available on all nodes where tenant t1 has a VRF deployment
apic1(config-bgp-af)# maximum-paths ?
<1-16>  Maximum number of equal-cost paths for load sharing. The default is 16.
ibgp  Configure multipath for IBGP paths
apic1(config-bgp-af)# maximum-paths 10
apic1(config-bgp-af)# maximum-paths ibpg 8
apic1(config-bgp-af)# end
apic1#
no maximum-paths [ibgp]
```

REST API を使用した BGP パスの設定

次の例では、REST API を使用して BGP 最長パス機能を設定する方法の情報を提供します。

```
<fvTenant descr="" dn="uni/tn-t1" name="t1">
    <fvCtx name="v1">
        <fvRsCtxToBgpCtxAfPol af="ipv4-ucast" tnBgpCtxAfPolName="bgpCtxPol1"/>
    </fvCtx>
    <bgpCtxAfPol name="bgpCtxPol1" maxEcmp="8" maxEcmpIbgp="4"/>
</fvTenant>
```

AS パスのプリペンドの設定

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 ログインし、APIC GUI に、メニュー バーで、をクリックして **テナント** > **<Your_Tenant>** > **ネットワー キング** > **外部ルーテッド ネットワーク** > **ルート マップの設定のルール** を右クリックし、 **設定ルールの A ルート マップの作成** .</Your_Tenant>

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) をクリックして、 **AS パスの設定** を開くにアイコン、 **設定 AS パスの作成** ダイアログボックス。

ステップ 3 条件を選択 **Prepend AS** に番号に付加します。

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** 。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 条件を選択 **Prepend 最後 AS** に指定された回数を番号と最後を付加します。

ステップ 6 **[カウント]**(1-10) を入力します。

ステップ 7 **設定ルールの A ルート マップの作成** 表示、AS パスに基づいて、ルールにリストされている条件を確認し、をクリックして **終了します。**

ステップ 8 APIC GUI メニュー バーで、をクリックして **テナント** > **<Your_Tenant>** > **ネットワー キング** > **外部ルーテッド ネットワーク** > **ルート マップのルールの設定** し、お客様のプロファイルを右クリックします</Your_Tenant>。

ステップ 9 確認、 **AS パスの設定** 画面の下部の値します。

NX-OS スタイルの CLI を使用した AS パスのプリペンド

このセクションでは、NX-OS スタイル コマンドライン インターフェイス (CLI) を使用して、AS パスのプリペンド機能を実現する方法について説明します。

始める前に

構成済みのテナント

手順

境界ゲートウェイ プロトコル (BGP) ルートの自動システムパス (AS パス) を変更するには、`set as-path` コマンドを使用します。set as-path コマンドは、`apic1(config-leaf-vrf-template-route-profile)# set as-path {'prepend as-num [ ,... as-num ] | prepend-last-as num}` の形式で実行します。

例：

```
apic1(config)# leaf 103
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# template route-profile rp1
apic1(config-leaf-vrf-template-route-profile)# set as-path ?
prepend Prepend to the AS-Path
prepend-last-as Prepend last AS to the as-path
apic1(config-leaf-vrf-template-route-profile)# set as-path prepend 100, 101, 102, 103
apic1(config-leaf-vrf-template-route-profile)# set as-path prepend-last-as 8
apic1(config-leaf-vrf-template-route-profile)# exit
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# exit
```

次のタスク

AS パスのプリペンドを無効にするには、示されているコマンドの no 形式を使用します:

```
apic1(config-leaf-vrf-template-route-profile)# [no] set
as-path { prepend as-num [ ,... as-num ] | prepend-last-as num}
```

REST API を使用した AS パス プリペンドの設定

次の例では、REST API を使用した AS パス プリペンド機能を設定する方法の情報を提供します。

```
<?xml version="1.0" encoding="UTF-8"?>
<fvTenant name="coke">
    <rtctrlAttrP name="attrp1">
        <rtctrlSetASPath criteria="prepend">
            <rtctrlSetASPathASN asn="100" order="1"/>
            <rtctrlSetASPathASN asn="200" order="10"/>
            <rtctrlSetASPathASN asn="300" order="5"/>
        <rtctrlSetASPath/>
        <rtctrlSetASPath criteria="prepend-last-as" lastnum=”9" />
    </rtctrlAttrP>

    <l3extOut name="out1">
        <rtctrlProfile name="rp1">
            <rtctrlCtxP name="ctxp1" order="1">
                <rtctrlScope>
                    <rtctrlRsScopeToAttrP tnRtctrlAttrPName="attrp1"/>
                </rtctrlScope>
            </rtctrlCtxP>
        </rtctrlProfile>
    </l3extOut>
</fvTenant>
```

BGP 外部ルーテッド ネットワークと AS オーバーライド

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。

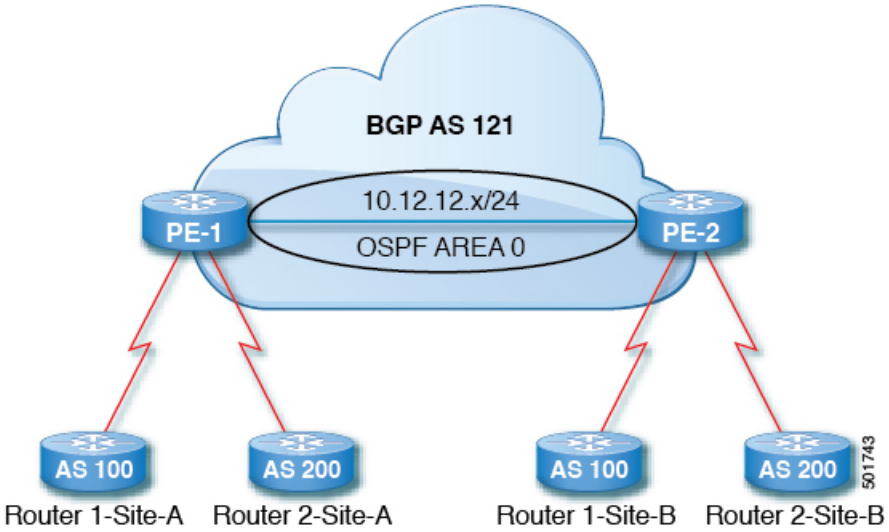
別の自立システム番号によりリンクする同一の自律システム番号を持つさまざまなサイトや禁止ユーザーのサイトを使用する場合、デフォルトルートのループが発生しないようにする設定によって問題が発生する可能性があります。このようなシナリオでは、その他のサイトが受信した場合 1 つのサイトからのルーティング更新は廃棄されます。

そのような状況が発生しないようにするには、BGP 自律システム オーバーライド機能を有効にしてデフォルト設定を上書きします。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 *14 :* 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、 **Tenants** > ***Tenant_name*** > **Networking** > **External Routed Network** > ***Non-GOLF Layer 3 Out_name*** > **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 **Work** ウィンドウの **Properties (BGP Peer Connectivity Profile** のもの) の下、**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 [送信（Submit）] をクリックします。

REST API を使用した自律システム オーバーライド対応のネットワークのルーティング BGP 外部の設定

手順

自律型オーバーライドを有効にして、BGP 外部ルーテッド ネットワークを設定します。

例：

```
<fvTenant name="coke">

   <fvCtx name="coke" status="">
       <bgpRtTargetP af="ipv4-ucast">
           <bgpRtTarget type="import" rt="route-target:as4-nn2:1234:1300" />
           <bgpRtTarget type="export" rt="route-target:as4-nn2:1234:1300" />
       </bgpRtTargetP>
       <bgpRtTargetP af="ipv6-ucast">
           <bgpRtTarget type="import" rt="route-target:as4-nn2:1234:1300" />
           <bgpRtTarget type="export" rt="route-target:as4-nn2:1234:1300" />
       </bgpRtTargetP>
   </fvCtx>

   <fvBD name="cokeBD">
       <!-- Association from Bridge Doamin to Private Network -->
       <fvRsCtx tnFvCtxName="coke" />
       <fvRsBDToOut tnL3extOutName="routAccounting" />
       <!-- Subnet behind the bridge domain-->
       <fvSubnet ip="20.1.1.1/16" scope="public"/>
       <fvSubnet ip="2000:1::1/64" scope="public"/>
   </fvBD>
   <fvBD name="cokeBD2">
       <!-- Association from Bridge Doamin to Private Network -->
       <fvRsCtx tnFvCtxName="coke" />
       <fvRsBDToOut tnL3extOutName="routAccounting" />
       <!-- Subnet behind the bridge domain-->
       <fvSubnet ip="30.1.1.1/16" scope="public"/>

   </fvBD>
   <vzBrCP name="webCtrct" scope="global">
```

```
        <vzSubj name="http">
            <vzRsSubjFiltAtt tnVzFilterName="default"/>
        </vzSubj>
    </vzBrCP>

    <!-- GOLF L3Out -->
    <l3extOut name="routAccounting">
       <l3extConsLbl name="golf_transit" owner="infra" status=""/>
       <bgpExtP/>
       <l3extInstP name="accountingInst">
           <!--
           <l3extSubnet ip="192.2.2.0/24" scope="import-security,import-rtctrl" />
           <l3extSubnet ip="192.3.2.0/24" scope="export-rtctrl"/>
           <l3extSubnet ip="192.5.2.0/24" scope="export-rtctrl"/>
           <l3extSubnet ip="64:ff9b::c007:200/120" scope="export-rtctrl" />
           -->
           <l3extSubnet ip="0.0.0.0/0"
                                scope="export-rtctrl,import-security"
                                aggregate="export-rtctrl"

           />
           <fvRsProv tnVzBrCPName="webCtrct"/>
       </l3extInstP>

       <l3extRsEctx tnFvCtxName="coke"/>
    </l3extOut>

     <fvAp name="cokeAp">
       <fvAEPg name="cokeEPg" >
           <fvRsBd tnFvBDName="cokeBD" />
           <fvRsPathAtt tDn="topology/pod-1/paths-103/pathep-[eth1/20]" encap="vlan-100"
 instrImedcy="immediate" mode="regular"/>
            <fvRsCons tnVzBrCPName="webCtrct"/>
       </fvAEPg>
       <fvAEPg name="cokeEPg2" >
           <fvRsBd tnFvBDName="cokeBD2" />
           <fvRsPathAtt tDn="topology/pod-1/paths-103/pathep-[eth1/20]" encap="vlan-110"
 instrImedcy="immediate" mode="regular"/>
            <fvRsCons tnVzBrCPName="webCtrct"/>
       </fvAEPg>
     </fvAp>

     <!-- Non GOLF L3Out-->
     <l3extOut name="NonGolfOut">
        <bgpExtP/>
        <l3extLNodeP name="bLeaf">
           <!--
           <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="20.1.13.1"/>
           -->
           <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="20.1.13.1">
           <l3extLoopBackIfP addr="1.1.1.1"/>

           <ipRouteP ip="2.2.2.2/32"  >
             <ipNexthopP nhAddr="20.1.12.3"/>
       </ipRouteP>


        </l3extRsNodeL3OutAtt>
           <l3extLIfP name='portIfV4'>
               <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/17]"
encap='vlan-1010' ifInstT='sub-interface' addr="20.1.12.2/24">

               </l3extRsPathL3OutAtt>
           </l3extLIfP>
```

```
            <l3extLIfP name='portIfV6'>
                <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/17]"
encap='vlan-1010' ifInstT='sub-interface' addr="64:ff9b::1401:302/120">
                    <bgpPeerP addr="64:ff9b::1401:d03" ctrl="send-com,send-ext-com" />
                </l3extRsPathL3OutAtt>
            </l3extLIfP>
            <bgpPeerP addr="2.2.2.2" ctrl="as-override,disable-peer-as-check,
send-com,send-ext-com" status=""/>
        </l3extLNodeP>
        <!--
         <bgpPeerP addr="2.2.2.2" ctrl="send-com,send-ext-com" status=""/>
         -->
        <l3extInstP name="accountingInst">
            <l3extSubnet ip="192.10.0.0/16" scope="import-security,import-rtctrl" />
            <l3extSubnet ip="192.3.3.0/24" scope="import-security,import-rtctrl" />
            <l3extSubnet ip="192.4.2.0/24" scope="import-security,import-rtctrl" />
           <l3extSubnet ip="64:ff9b::c007:200/120" scope="import-security,import-rtctrl"
 />
            <l3extSubnet ip="192.2.2.0/24" scope="export-rtctrl" />
            <l3extSubnet ip="0.0.0.0/0"
                                scope="export-rtctrl,import-rtctrl,import-security"
                                aggregate="export-rtctrl,import-rtctrl"

          />
        </l3extInstP>
       <l3extRsEctx tnFvCtxName="coke"/>
    </l3extOut>

</fvTenant>
```

（注） 太字の例では、コードの行に設定の BGP AS オーバーライド部分が表示されます。

VRF ごと、ノード BGP ごとのタイマーの値の設定

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、次のように選択します。 **テナント** > ***Tenant_name*** > **ネットワー キング** > **プロトコル ポリシー** 。**ナビゲーション**] ペインで、[展開 **ネットワー キング** > **プロトコル ポリシー** > **BGP** > **BGP タイマー** 。

ステップ 2 **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 移動し、 **外部ルーテッド ネットワーク** 、し、次のアクションを実行して有効になっている BGP を使用したレイヤ 3 Out 作成します。

a) [Create Routed Outside] を右クリックします。
b) **Create Routed Outside** ダイアログボックスで、Layer 3 Out の名前を指定します。
c) チェック ボックスをオンにして、**BGP** を有効にします。
d) [Nodes and Interfaces Protocol Policies] を展開します。

ステップ 4 新しいノードを作成するには、**Create Node 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、ノード プロファイルの名前を入力します

b) **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。[Finish] 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 5 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) 展開 **レイヤ 3 Out** > **外部ルーテッド** *Network_name* > **論理ノード プロファイル** > **論理ノード** *Profiles_name* > **BGP プロトコル プロファイル。**>

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。

REST API を使用した VRF ごと、ノード BGP ごとのタイマーの設定

次の例では、ノード内の VRF ごと、ノード BGP ごとのタイマーの設定方法を示します。`bgpProtP` (`l3extLNodeP` の下) を設定します。`bgpProtP` の下で、目的とする関係 (`bgpRsBgpNodeCtxPol`) を設定します。これは、BGP コンテキスト ポリシー (`bgpCtxPol`) に対するものです。

手順

`node1` でノード固有の BGP タイマー ポリシーを設定し、`node2` を、ノード固有ではない BGP タイマー ポリシーで設定します。

例：

```
POST https://apic-ip-address/mo.xml

<fvTenant name="tn1" >
    <bgpCtxPol name="pol1" staleIntvl="25" />
    <bgpCtxPol name="pol2" staleIntvl="35" />
    <fvCtx name="ctx1" >
      <fvRsBgpCtxPol tnBgpCtxPolName="pol1"/>
    </fvCtx>
     <l3extout name="out1" >
      <l3extRsEctx toFvCtxName="ctx1" />
      <l3extLNodeP name="node1" >
        <bgpProtP name="protp1" >
            <bgpRsBgpNodeCtxPol tnBgpCtxPolName="pol2" />
        </bgpProtP>
      </l3extLNodeP>
      <l3extLNodeP name="node2" >
      </l3extLNodeP>
```

この例では、node1 は BGP タイマー値をポリシー pol2 から取得し、node2 は BGP タイマー値を pol1 から取得します。タイマー値は bgpDom に適用されますが、これは VRF tn1:ctx1 に対応しています。これは、「*VRF* ごと、ノード *BGP* ごとのタイマーの値」のセクションで説明したアルゴリズムに従って選択された、BGP タイマー ポリシーに基づきます。

削除するノード BGP タイマーが REST API を使用してごとの VRF あたり

次の例では、ノード内で既存の VRF ごとの各ノード BGP タイマーを削除する方法を示します。

手順

node1 で特定の BGP タイマー ポリシーのノードを削除します。

例：

```
POST https://apic-ip-address/mo.xml

<fvTenant name="tn1" >
    <bgpCtxPol name="pol1" staleIntvl="25" />
    <bgpCtxPol name="pol2" staleIntvl="35" />
    <fvCtx name="ctx1" >
      <fvRsBgpCtxPol tnBgpCtxPolName="pol1"/>
    </fvCtx>
     <l3extout name="out1" >
      <l3extRsEctx toFvCtxName="ctx1" />
      <l3extLNodeP name="node1" >
        <bgpProtP name="protp1" status="deleted" >
            <bgpRsBgpNodeCtxPol tnBgpCtxPolName="pol2" />
        </bgpProtP>
      </l3extLNodeP>
      <l3extLNodeP name="node2" >
      </l3extLNodeP>
```

上の例のコード フレーズ <bgpProtP name="protp1" status="deleted" > は、BGP タイマー ポリシーを削除します。削除後、node1 が node1 が関連付けられている VRF の BGP タイマー ポリシーのデフォルト設定になります。上の例では pol1 です。

NX-OS スタイル CLI を使用してノード BGP タイマー ポリシーあたりの VRF あたりを設定する

手順

	コマンドまたはアクション	目的

ステップ 1	タイマーポリシーを作成する前に、BGP ASN およびルート リフレクタを設定します。
	例：
	`apic1(config)#`
	`apic1(config)# bgp-fabric`
	`apic1(config-bgp-fabric)#`
	`route-reflector spine 102`
	`apic1(config-bgp-fabric)# asn 42`
	`apic1(config-bgp-fabric)# exit`
	`apic1(config)# exit`
	`apic1#`	

ステップ 2	タイマー ポリシーを作成します。
	例：
	`apic1# config`
	`apic1(config)# leaf 101`
	`apic1(config-leaf)# template bgp timers pol7 tenant tn1`
	`This template will be available on all nodes where tenant tn1 has a VRF deployment`
	`apic1(config-bgp-timers)# timers bgp 120 240`
	`apic1(config-bgp-timers)# graceful-restart stalepath-time 500`
	`apic1(config-bgp-timers)# maxas-limit 300`
	`apic1(config-bgp-timers)# exit`
	`apic1(config-leaf)# exit`
	`apic1(config)# exit`
	`apic1#`
		特定の値は、例としてのみ提供されます。

ステップ 3	設定された BGP ポリシーを表示します。
	例：
	`apic1# show run leaf 101 template bgp timers pol7`
	`# Command: show running-config leaf 101 template bgp timers pol7`
	`leaf 101`
	`template bgp timers pol7 tenant tn1`
	`timers bgp 120 240`
	`graceful-restart stalepath-time 500`	

	コマンドまたはアクション	目的
	maxas-limit 300 exit exit	
ステップ 4	ノードで特定のポリシーを参照します。 **例：** apic1# **config** apic1(config)# **leaf 101** apic1(config-leaf)# **router bgp 42** apic1(config-leaf-bgp)# **vrf member tenant tn1 vrf ctx1** apic1(config-leaf-bgp-vrf)# **inherit node-only bgp timer pol7** apic1(config-leaf-bgp-vrf)# **exit** apic1(config-leaf-bgp)# **exit** apic1(config-leaf)# **exit** apic1(config)# **exit** apic1#	
ステップ 5	特定の BGP のタイマー ポリシーのノードが表示されます。 **例：** apic1# **show run leaf 101 router bgp 42 vrf member tenant tn1 vrf ctx1** # Command: show running-config leaf 101 router bgp 42 vrf member tenant tn1 vrf ctx1 leaf 101 router bgp 42 vrf member tenant tn1 vrf ctx1 inherit node-only bgp timer pol7 exit exit exit apic1#	

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

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。
- 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。
- マルチホップ BFD はサポートされません。
- 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 multipod 接続を設定する場合は、MTU が両側で適切に設定されていることが重要です。ACI、Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定された MTU 値は IP ヘッダーを考慮に入れています（結果として、最大パケット サイズは、ACI で 9216 バイト、NX-OS および IOS で 9000 バイトに設定されます）。ただし、IOS XR などの他のプラットフォームは、パケット ヘッダーのを除く MTU 値を設定します（結果として最大パケット 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。

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 **Navigation** うぃんどうで、 **Switch Policies** > **Policies** > **BFD** を展開します。
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 デフォルトではない特定のBFDポリシーのスイッチプロファイルを作成するには、**Navigation** ウィンドウで、 **Switch Policies** > **Profiles** > **Leaf Profiles** を選択します
Work ウィンドウに **[Profiles - Leaf Profiles]** 画面が表示されます。

ステップ 4 **Work** ウィンドウの右側の、**[ACTIONS]** の下で、**[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) **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) **Switch Selectors** フィールドで、**[Name]** (スイッチの名前)、**[Blocks]** (スイッチの選択)、および **[Policy Group]** (**[Create Access Switch Policy Group]** の選択) 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 **Create Access Switch Policy Group** ダイアログボックスで、次の操作を実行します:

a) [Name] フィールドにポリシー グループの名前を入力します。

b) **Description** フィールドに、ポリシーの説明を入力します。（この手順はオプションです）。

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。

ステップ 7 **Submit** 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 8 作成した BFD グローバル設定を表示するには、**Navigation** ウィンドウで、 **Switch Policies** > **Policies** > **BFD** を展開します。

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 **Navigation** うぃんどうで、 **Switch Policies** > **Policies** > **BFD** を展開します。
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 特定グローバル BFD ポリシー(これは、デフォルトではありません) でのスパイン スイッチ プロファイルを作成する、 **ナビゲーション**] ペインで、展開、 **スイッチ ポリシー** > **プロファイル** > **スパイン プロファイル** 。
Profiles- Spine Profiles 画面が **Work** ウィンドウに表示されます。

ステップ 4 右側にある、 **作業** ()] ペインで、 **アクション** 、select **スパイン プロファイルの作成** 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) **スパイン セレクタ** フィールドで、適切な値を入力 **名** (スイッチの名前)、 **ブロック** (スイッチを選択し、) および **ポリシー グループ** (選択 **スパイン スイッチ ポリシー グループの作成**)。
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 **Create スパイン スイッチ Policy Group** ダイアログボックスで、次の操作を実行します:

a) [Name] フィールドにポリシー グループの名前を入力します。
b) **Description** フィールドに、ポリシーの説明を入力します。（この手順はオプションです）。
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。

ステップ 7 **Submit** 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 8 作成した BFD グローバル設定を表示するには、**Navigation** ウィンドウで、 **Switch Policies** > **Policies** > **BFD** を展開します。

NX-OS スタイル CLI を使用したリーフ スイッチでの BFD のグローバルな設定

手順

ステップ 1 NX-OS CLI を使用して BFD IPV4 グローバル設定（bfdIpv4InstPol）を設定するには：

例：

```
apic1# configure
apic1(config)# template bfd ip bfd_ipv4_global_policy
apic1(config-bfd)# [no] echo-address 1.2.3.4
apic1(config-bfd)# [no] slow-timer 2500
apic1(config-bfd)# [no] min-tx 100
apic1(config-bfd)# [no] min-rx 70
apic1(config-bfd)# [no] multiplier 3
apic1(config-bfd)# [no] echo-rx-interval 500
apic1(config-bfd)# exit
```

ステップ 2 NX-OS CLI を使用して BFD IPV6 グローバル設定（bfdIpv6InstPol）を設定するには：

例：

```
apic1# configure
apic1(config)# template bfd ipv6 bfd_ipv6_global_policy
apic1(config-bfd)# [no] echo-address 34::1/64
apic1(config-bfd)# [no] slow-timer 2500
apic1(config-bfd)# [no] min-tx 100
apic1(config-bfd)# [no] min-rx 70
apic1(config-bfd)# [no] multiplier 3
apic1(config-bfd)# [no] echo-rx-interval 500
apic1(config-bfd)# exit
```

ステップ 3 NX-OS CLI を使用してアクセス リーフ ポリシー グループ (infraAccNodePGrp) を設定し、以前に作成した BFD グローバル ポリシーを継承するには:

例：

```
apic1# configure
apic1(config)# template leaf-policy-group test_leaf_policy_group
apic1(config-leaf-policy-group)# [no] inherit bfd ip bfd_ipv4_global_policy
apic1(config-leaf-policy-group)# [no] inherit bfd ipv6 bfd_ipv6_global_policy
apic1(config-leaf-policy-group)# exit
```

ステップ 4 NX-OS CLI を使用して以前に作成したリーフ ポリシー グループを リーフに関連付けるには:

例：

```
apic1(config)# leaf-profile test_leaf_profile
apic1(config-leaf-profile)# leaf-group test_leaf_group
apic1(config-leaf-group)# leaf-policy-group test_leaf_policy_group
apic1(config-leaf-group)# leaf 101-102
apic1(config-leaf-group)# exit
```

NX-OS スタイル CLI を使用したスパイン スイッチ上の BFD のグローバル設定

次の手順を使用して、NX-OS スタイル CLI を使用してスパイン スイッチの BFD をグローバルに設定します。

手順

ステップ 1 NX-OS CLI を使用して BFD IPV4 グローバル設定（bfdIpv4InstPol）を設定するには：

例：

```
apic1# configure
apic1(config)# template bfd ip bfd_ipv4_global_policy
apic1(config-bfd)# [no] echo-address 1.2.3.4
apic1(config-bfd)# [no] slow-timer 2500
apic1(config-bfd)# [no] min-tx 100
apic1(config-bfd)# [no] min-rx 70
apic1(config-bfd)# [no] multiplier 3
apic1(config-bfd)# [no] echo-rx-interval 500
apic1(config-bfd)# exit
```

ステップ 2 NX-OS CLI を使用して BFD IPV6 グローバル設定（bfdIpv6InstPol）を設定するには：

例：

```
apic1# configure
apic1(config)# template bfd ipv6 bfd_ipv6_global_policy
apic1(config-bfd)# [no] echo-address 34::1/64
apic1(config-bfd)# [no] slow-timer 2500
apic1(config-bfd)# [no] min-tx 100
apic1(config-bfd)# [no] min-rx 70
apic1(config-bfd)# [no] multiplier 3
apic1(config-bfd)# [no] echo-rx-interval 500
apic1(config-bfd)# exit
```

ステップ 3 NX-OS CLI を使用してスパイン ポリシー グループを設定し以前作成した BFD グローバル ポリシーを継承するには：

例：

```
apic1# configure
apic1(config)# template spine-policy-group test_spine_policy_group
apic1(config-spine-policy-group)# [no] inherit bfd ip bfd_ipv4_global_policy
apic1(config-spine-policy-group)# [no] inherit bfd ipv6 bfd_ipv6_global_policy
apic1(config-spine-policy-group)# exit
```

ステップ 4 NX-OS を使用して以前作成したスパイン ポリシー グループをスパイン スイッチに関連付けるには；

例：

```
apic1# configure
apic1(config)# spine-profile test_spine_profile
apic1(config-spine-profile)# spine-group test_spine_group
apic1(config-spine-group)# spine-policy-group test_spine_policy_group
```

```
apic1(config-spine-group)# spine 103-104
apic1(config-leaf-group)# exit
```

グローバル REST API を使用して BFD の設定

手順

次の REST API は、(BFD) を双方向フォワーディング検出のグローバル コンフィギュレーションを示します。

例：

```
<polUni>
 <infraInfra>
    <bfdIpv4InstPol name="default" echoSrcAddr="1.2.3.4" slowIntvl="1000" minTxIntvl="150"
 minRxIntvl="250" detectMult="5" echoRxIntvl="200"/>
    <bfdIpv6InstPol name="default" echoSrcAddr="34::1/64" slowIntvl="1000" minTxIntvl="150"
 minRxIntvl="250" detectMult="5" echoRxIntvl="200"/>
 </infraInfra>
</polUni>
```

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 L3 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。

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** ウィンドウ ([クイック スタート)、作成したテナントの展開 ***Tenant_name*** > **ネットワー キング** > **外部ルーテッド ネットワーク** 。

ステップ 3 **External Routed Networks** を右クリックし、**Create Routed Outside** を選択します。
[Create Routed Outside] ダイアログボックスが表示されます。

ステップ 4 **外部ルーティング作成** ダイアログボックス未満で **ルーティング外部定義** 、既存の設定はすでにセットアップする必要があります。それ以外の場合は、外部ルーティングの設定のアイデンティティを定義する値を入力します。

ステップ 5 [**ノードとインターフェイスのプロトコル プロファイル** の下部にある、 **外部ルーティングの作成** ダイアログボックス] をクリックして、「 + 」(expand)] ボタン。
Create Node Profile ダイアログボックスが表示されます。

ステップ 6 **ノードのプロファイルを指定** 、ノードのプロファイルの名前を入力、 **名** フィールド。

ステップ 7 をクリックして、「 + 」(expand) の右側にあるボタン、 **ノード** フィールド。
Select Node ダイアログボックスが表示されます。

ステップ 8 **ノードとスタティック ルートの設定を選択** でノードを選択、 **ノード ID** フィールド。

ステップ 9 **Router ID** フィールドにルータ ID を入力します。

ステップ 10 [OK] をクリックします。
Create Node Profile ダイアログボックスが表示されます。

ステップ 11 をクリックします」 + 」(expand) の右側にあるボタン、 **インターフェイス プロファイル** フィールド。
Create Interface Profile ダイアログボックスが表示されます。

ステップ 12 インターフェイスプロファイル名を **Name** フィールドに入力します。

ステップ 13 インターフェイスのタブのいずれかをクリックして、以前に作成したノードの目的のユーザインターフェイスを選択します。

- **ルーテッド インターフェイス**
- **SVI**
- **Routed Sub-Interfaces**

ステップ 14 **BFD インターフェイス プロファイル** フィールドで、BDF 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** 。

ステップ 15 BFD インターフェイス ポリシー] フィールドのいずれかを選択、 **一般的な/デフォルト** 設定 (デフォルト BFD policy) を選択して、自分 BFD ポリシーの作成または **BFD インターフェイス ポリシーの作成** 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 16 [Submit] をクリックします。

ステップ 17 BFD ポリシーのレベルに移動して、設定されているインターフェイスを表示する **ネットワーキング** > **プロトコル ポリシー** > **BFD** 。

NX-OS スタイルの CLI を使用して BFD インターフェイスのオーバーライドを設定する

手順

ステップ 1 NX-OS CLI を使用して BFD インターフェイス ポリシー (bfdIfPol) を設定するには:

例：

```
apic1# configure
apic1(config)# tenant t0
apic1(config-tenant)# vrf context v0
apic1(config-tenant-vrf)# exit
apic1(config-tenant)# exit
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant t0 vrf v0
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# interface Ethernet 1/18
apic1(config-leaf-if)# vrf  member tenant t0 vrf v0
apic1(config-leaf-if)# exit
apic1(config-leaf)# template bfd bfdIfPol1 tenant t0
apic1(config-template-bfd-pol)# [no] echo-mode enable
apic1(config-template-bfd-pol)# [no] echo-rx-interval 500
apic1(config-template-bfd-pol)# [no] min-rx 70
apic1(config-template-bfd-pol)# [no] min-tx 100
apic1(config-template-bfd-pol)# [no] multiplier 5
apic1(config-template-bfd-pol)# [no] optimize subinterface
apic1(config-template-bfd-pol)# exit
```

ステップ 2 NX-OS CLI を使用して、以前に作成した BFD インターフェイス ポリシーを、IPv4 アドレスを持つ L3 インターフェイスに継承させるには:

例：

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface Ethernet 1/15
apic1(config-leaf-if)# bfd ip tenant mode
apic1(config-leaf-if)# bfd ip inherit interface-policy bfdPol1
apic1(config-leaf-if)# bfd ip authentication keyed-sha1 key 10 key password
```

ステップ 3 NX-OS CLI を使用して、以前に作成した BFD インターフェイス ポリシーを、IPv6 アドレスを持つ L3 インターフェイスに継承させるには:

例：

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface Ethernet 1/15
apic1(config-leaf-if)# ipv6 address 2001::10:1/64 preferred
apic1(config-leaf-if)# bfd ipv6 tenant mode
apic1(config-leaf-if)# bfd ipv6 inherit interface-policy bfdPol1
apic1(config-leaf-if)# bfd ipv6 authentication keyed-sha1 key 10 key password
```

ステップ 4 NX-OS CLI を使用して、IPv4 アドレスを持つ VLAN インターフェイス上の BFD を設定するには:

例：

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface vlan 15
apic1(config-leaf-if)# vrf member tenant t0 vrf v0
apic1(config-leaf-if)# bfd ip tenant mode
apic1(config-leaf-if)# bfd ip inherit interface-policy bfdPol1
apic1(config-leaf-if)# bfd ip authentication keyed-sha1 key 10 key password
```

ステップ 5 NX-OS CLI を使用して、IPv6 アドレスを持つ VLAN インターフェイス上の BFD を設定するには:

例：

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface vlan 15
apic1(config-leaf-if)# ipv6 address 2001::10:1/64 preferred
apic1(config-leaf-if)# vrf member tenant t0 vrf v0
apic1(config-leaf-if)# bfd ipv6 tenant mode
apic1(config-leaf-if)# bfd ipv6 inherit interface-policy bfdPol1
apic1(config-leaf-if)# bfd ipv6 authentication keyed-sha1 key 10 key password
```

REST API 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

手順

次の REST API は、(BFD) を双方向フォワーディング検出のインターフェイスのオーバーライド コンフィギュレーションを示します。

例：

```
<fvTenant name="ExampleCorp">
  <bfdIfPol name="bfdIfPol" minTxIntvl="400" minRxIntvl="400" detectMult="5"
echoRxIntvl="400" echoAdminSt="disabled"/>
    <l3extOut name="l3-out">
        <l3extLNodeP name="leaf1">
            <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="2.2.2.2"/>

            <l3extLIfP name='portIpv4'>
                <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/11]"
ifInstT='l3-port' addr="10.0.0.1/24" mtu="1500"/>
                <bfdIfP type="sha1" key="password">
                    <bfdRsIfPol tnBfdIfPolName='bfdIfPol'/>
                </bfdIfP>
            </l3extLIfP>


        </l3extLNodeP>
    </l3extOut>
</fvTenant>
```

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 ウィンドウの **Tenant** > **Networking** > **Protocol Policies** 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 メニュー バーで、 **Tenant** を選択します。

ステップ 2 BGP プロトコルの BFD を設定するには、**Navigation** ウインドウ (クイック スタートの下) で、作成したテナント、 ***Tenant_name*** > **Networking** > **Protocol Policies** > **BGP** > **BGP Peer Prefix** を展開します。

ステップ 3 **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 4 **[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 5 **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 6 **Navigation** ウィンドウで、 **Networking** > **External Routed Networks** に戻ります。

ステップ 7 **External Routed Networks** を右クリックし、**Create Routed Outside** を選択します。
[Create Routed Outside] ダイアログボックスが表示されます。

ステップ 8 **Create Routed Outside** ダイアログボックスで、**[Name]** フィールドに名前を入力します。**[Name]** フィールドの右側で、**[BGP]** プロトコルを選択します。

ステップ 9 **[Nodes and Interfaces Protocol Profiles]** セクションで、[+] (展開) ボタンをクリックします。
[Create Node Profile] ダイアログボックスが表示されます。

ステップ 10 **BGP ピア接続** セクションで、をクリックします」 ＋ 」(expand)] ボタン。
[Create BGP Peer Connectivity Profile] ダイアログボックスが表示されます。

ステップ 11 **[Create BGP Peer Connectivity Profile]** ダイアログボックスの **[Peer Controls]** の隣で、**[Bidirectional Forwarding Detection]** を選択して BGP コンシューマ プロトコルの BFD を、次のように有効にします (またはオフにして BFD を無効にします)。

ステップ 12 OSPF プロトコルの BFD を設定するには、**Navigation** ウィンドウで、 **Networking** > **Protocol Policies** > **OSPF** > **OSPF Interface** に移動します。

ステップ 13 **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 14 **[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 15 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 16 **Submit** をクリックします。

ステップ 17 EIGRP プロトコルの BFD を設定するには、**Navigation** ウィンドウで、 **Networking** > **Protocol Policies** > **EIGRP** > **EIGRP Interface** に移動します。

ステップ 18 **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 19 **[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 20 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 21 **Submit** をクリックします。

ステップ 22 スタティック ルート プロトコルで BFD を設定するには、**Navigation** ウィンドウで、**Networking** > **External Routed Networks** > に戻ります。

ステップ 23 **External Routed Networks** を右クリックし、**Create Routed Outside** を選択します。
[Create Routed Outside] ダイアログボックスが表示されます。

ステップ 24 **[Define the Routed Outside]** セクションで、すべての必須フィールドに値を入力します。

ステップ 25 **[Nodes and Interfaces Protocol Profiles]** セクションで、[+] (展開) ボタンをクリックします。
[Create Node Profile] ダイアログボックスが表示されます。

ステップ 26 **[Nodes]** セクションで、[+] (展開) ボタンをクリックします。

[Select Node] ダイアログボックスが表示されます。

ステップ 27 **[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 28 **[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 29 **[OK]** をクリックします。

ステップ 30 IS-IS プロトコルの BFD を設定するには、**Navigation** ペインで **Fabric** > **Fabric Policies** > **Interface Policies** > **Policies** > **L3 Interface** に移動します。

ステップ 31 **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 32 **[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 33 BFD ISIS ポリシーを有効にするには、 **Enable** をクリックします。

ステップ 34 [SUBMIT] をクリックします。

NX-OS スタイルの CLI を使用した BFD コンシューマ プロトコルの設定

手順

ステップ 1 NX-OS は、CLI を使用して、BGP コンシューマ プロトコルを BFD をイネーブルにします。

例：

```
apic1# configure
apic1(config)# bgp-fabric
apic1(config-bgp-fabric)# asn 200
apic1(config-bgp-fabric)# exit
apic1(config)# leaf 101
apic1(config-leaf)# router bgp 200
apic1(config-bgp)# vrf member tenant t0 vrf v0
apic1(config-leaf-bgp-vrf)# neighbor 1.2.3.4
apic1(config-leaf-bgp-vrf-neighbor)# [no] bfd enable
```

ステップ 2 NX-OS は、CLI を使用して、EIGRP コンシューマ プロトコルを BFD をイネーブルにします。

例：

```
apic1(config-leaf-if)# [no] ip bfd eigrp enable
```

ステップ 3 NX-OS は、CLI を使用して、OSPF コンシューマ プロトコルを BFD をイネーブルにします。

例：

```
apic1(config-leaf-if)# [no] ip ospf bfd enable


apic1# configure
apic1(config)# spine 103
apic1(config-spine)# interface ethernet 5/3.4
apic1(config-spine-if)# [no] ip ospf bfd enable
```

ステップ 4 NX-OS は、CLI を使用して、スタティック ルート コンシューマ プロトコルを BFD をイネーブルにします。

例：

```
apic1(config-leaf-vrf)# [no] ip route 10.0.0.1/16 10.0.0.5 bfd


apic1(config)# spine 103
apic1(config-spine)# vrf context tenant infra vrf overlay-1
apic1(config-spine-vrf)# [no] ip route 21.1.1.1/32 32.1.1.1 bfd
```

ステップ 5 NX-OS は、CLI を使用して、IS-IS コンシューマ プロトコルを BFD をイネーブルにします。

例：

```
apic1(config)# leaf 101
apic1(config-spine)# interface ethernet 1/49
apic1(config-spine-if)# isis bfd enabled
apic1(config-spine-if)# exit
apic1(config-spine)# exit


apic1(config)# spine 103
apic1(config-spine)# interface ethernet 5/2
apic1(config-spine-if)# isis bfd enabled
apic1(config-spine-if)# exit
apic1(config-spine)# exit
```

REST API を使用した BFD コンシューマ プロトコルの設定

手順

ステップ 1 次の例では、双方向の転送検出（BFD）のインターフェイス設定を示します。

例：

```
<fvTenant name="ExampleCorp">
  <bfdIfPol name="bfdIfPol" minTxIntvl="400" minRxIntvl="400" detectMult="5"
echoRxIntvl="400" echoAdminSt="disabled"/>
    <l3extOut name="l3-out">
        <l3extLNodeP name="leaf1">
            <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="2.2.2.2"/>

            <l3extLIfP name='portIpv4'>
                <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/11]"
ifInstT='l3-port' addr="10.0.0.1/24" mtu="1500"/>
```

```
                <bfdIfP type="sha1" key="password">
                    <bfdRsIfPol tnBfdIfPolName='bfdIfPol'/>
                </bfdIfP>
            </l3extLIfP>


        </l3extLNodeP>
    </l3extOut>
</fvTenant>
```

ステップ 2 次の例では、OSPF および EIGRP で BFD を有効にするためのインターフェイス設定を示します。

例：

リーフ スイッチ上の BFD

```
<fvTenant name="ExampleCorp">
      <ospfIfPol  name="ospf_intf_pol" cost="10" ctrl="bfd"/>
      <eigrpIfPol ctrl="nh-self,split-horizon,bfd"
dn="uni/tn-Coke/eigrpIfPol-eigrp_if_default"
</fvTenant>
```

例：

スパイン スイッチ上の BFD

```
<l3extLNodeP name="bSpine">

             <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-103" rtrId="192.3.1.8">
                 <l3extLoopBackIfP addr="10.10.3.1" />
                 <l3extInfraNodeP fabricExtCtrlPeering="false" />
             </l3extRsNodeL3OutAtt>

             <l3extLIfP name='portIf'>
                 <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-103/pathep-[eth5/10]"
encap='vlan-4' ifInstT='sub-interface' addr="20.3.10.1/24"/>
                 <ospfIfP>
                     <ospfRsIfPol tnOspfIfPolName='ospf_intf_pol'/>
                 </ospfIfP>
                 <bfdIfP name="test" type="sha1" key="hello" status="created,modified">
                    <bfdRsIfPol tnBfdIfPolName='default' status="created,modified"/>
                </bfdIfP>
             </l3extLIfP>

         </l3extLNodeP>
```

ステップ 3 次の例では、BGP 上の BFD を有効にするためのインターフェイス設定を示します。

例：

```
<fvTenant name="ExampleCorp">
    <l3extOut name="l3-out">
        <l3extLNodeP name="leaf1">
            <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="2.2.2.2"/>

            <l3extLIfP name='portIpv4'>
                <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/11]"
ifInstT='l3-port' addr="10.0.0.1/24" mtu="1500">
                 <bgpPeerP addr="4.4.4.4/24" allowedSelfAsCnt="3" ctrl="bfd" descr=""
name="" peerCtrl="" ttl="1">
                    <bgpRsPeerPfxPol tnBgpPeerPfxPolName=""/>
```

```
                        <bgpAsP asn="3" descr="" name=""/>
                    </bgpPeerP>
                </l3extRsPathL3OutAtt>
            </l3extLIfP>


        </l3extLNodeP>
    </l3extOut>
</fvTenant>
```

ステップ 4 次の例では、スタティック ルートで BFD を有効にするためのインターフェイス設定を示します。

例：

リーフ スイッチ上の BFD

```
<fvTenant name="ExampleCorp">
    <l3extOut name="l3-out">
        <l3extLNodeP name="leaf1">
            <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="2.2.2.2">
              <ipRouteP ip="192.168.3.4" rtCtrl="bfd">
                <ipNexthopP nhAddr="192.168.62.2"/>
              </ipRouteP>
            </l3extRsNodeL3OutAtt>
            <l3extLIfP name='portIpv4'>
                <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/3]"
ifInstT='l3-port' addr="10.10.10.2/24" mtu="1500" status="created,modified" />

            </l3extLIfP>

        </l3extLNodeP>

    </l3extOut>
</fvTenant>
```

例：

スパイン スイッチ上の BFD

```
<l3extLNodeP name="bSpine">

             <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-103" rtrId="192.3.1.8">
              <ipRouteP ip="0.0.0.0" rtCtrl="bfd">
                <ipNexthopP nhAddr="192.168.62.2"/>
              </ipRouteP>
             </l3extRsNodeL3OutAtt>

             <l3extLIfP name='portIf'>
                 <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-103/pathep-[eth5/10]"
encap='vlan-4' ifInstT='sub-interface' addr="20.3.10.1/24"/>

                <bfdIfP name="test" type="sha1" key="hello" status="created,modified">
                   <bfdRsIfPol tnBfdIfPolName='default' status="created,modified"/>
                </bfdIfP>
             </l3extLIfP>

         </l3extLNodeP>
```

ステップ 5 次の例では、IS-IS で BFD を有効にするためのインターフェイス設定を示します。

例：

```
<fabricInst>
          <l3IfPol name="testL3IfPol" bfdIsis="enabled"/>
              <fabricLeafP name="LeNode" >
  <fabricRsLePortP tDn="uni/fabric/leportp-leaf_profile" />
 <fabricLeafS name="spsw" type="range">
 <fabricNodeBlk name="node101" to_="102" from_="101" />
 </fabricLeafS>
            </fabricLeafP>

           <fabricSpineP name="SpNode" >
 <fabricRsSpPortP tDn="uni/fabric/spportp-spine_profile" />
 <fabricSpineS name="spsw" type="range">
     <fabricNodeBlk name="node103" to_="103" from_="103" />
 </fabricSpineS>
         </fabricSpineP>

          <fabricLePortP name="leaf_profile">
 <fabricLFPortS name="leafIf" type="range">
<fabricPortBlk name="spBlk" fromCard="1" fromPort="49" toCard="1" toPort="49" />
       <fabricRsLePortPGrp tDn="uni/fabric/funcprof/leportgrp-LeTestPGrp" />
 </fabricLFPortS>
        </fabricLePortP>

       <fabricSpPortP name="spine_profile">
 <fabricSFPortS name="spineIf" type="range">
      <fabricPortBlk name="spBlk" fromCard="5" fromPort="1" toCard="5" toPort="2" />
      <fabricRsSpPortPGrp tDn="uni/fabric/funcprof/spportgrp-SpTestPGrp" />
 </fabricSFPortS>
     </fabricSpPortP>

 <fabricFuncP>
               <fabricLePortPGrp name = "LeTestPGrp">
 <fabricRsL3IfPol tnL3IfPolName="testL3IfPol"/>
              </fabricLePortPGrp>

            <fabricSpPortPGrp name = "SpTestPGrp">
 <fabricRsL3IfPol tnL3IfPolName="testL3IfPol"/>
           </fabricSpPortPGrp>

</fabricFuncP>

</fabricInst>
```

OSPF 外部ルーテッド ネットワーク

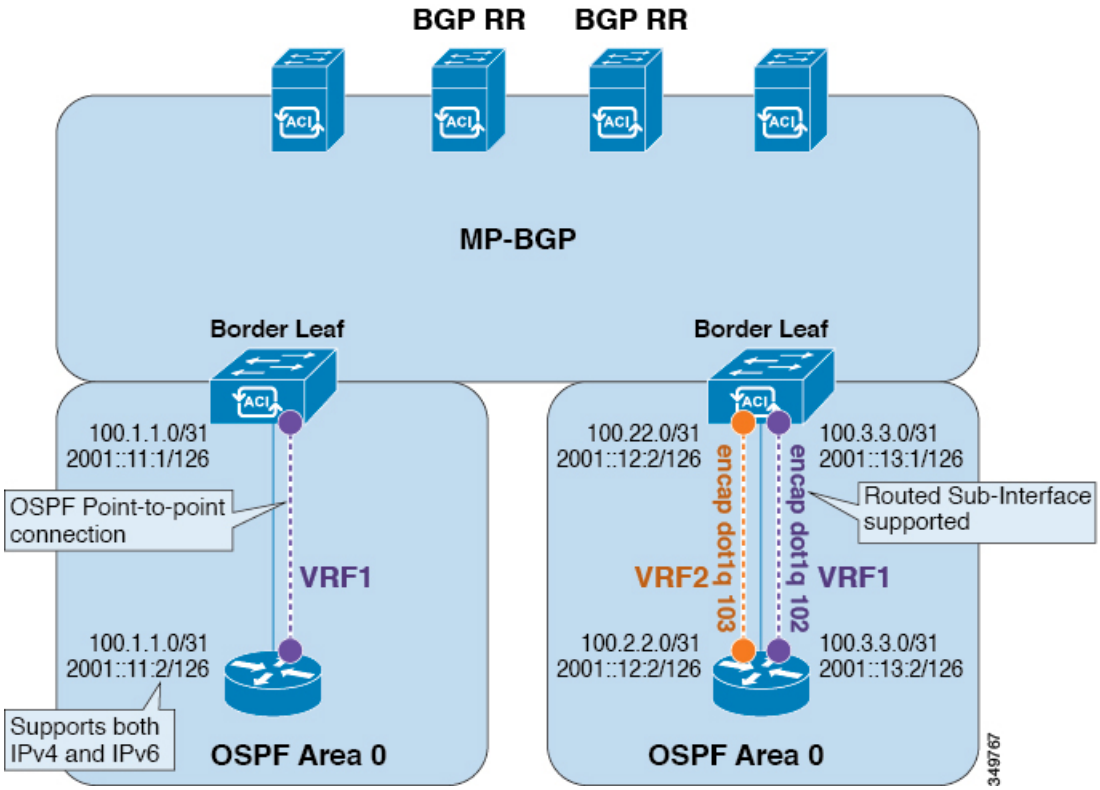
OSPF レイヤ 3 Outside 接続

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、L2 と L3 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、ポート、ポート チャネル、VPC ポート チャネルでサポートされます。

図 *15 : 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 BD によりアップ状態を維持することができます。

GUI を使用した管理テナントの OSPF 外部ルーテッド ネットワークの作成

- 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 外部ルーテッド ネットワークを作成するためのものです。テナントの OSPF 外部ルーテッド ネットワークを作成するには、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]** を選択します。

ステップ 2 [Navigation] ペインで、**[Networking]** > **[External Routed Networks]** を展開します。

ステップ 3 [External Routed Networks] を右クリックし、[Create Routed Outside] をクリックします。

ステップ 4 [Create Routed Outside] 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、名前（RtdOut）を入力します。
b) [OSPF] チェックボックスをオンにします。
c) [OSPF Area ID] フィールドに、エリア ID を入力します。
d) [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。
e) [OSPF Area Type] フィールドで、適切なエリア タイプを選択します。
f) [OSPF Area Cost] フィールドで、適切な値を選択します。
g) [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。

h) [External Routed 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。
i) [Nodes and Interfaces Protocol Profiles] 領域の [+] アイコンをクリックします。

ステップ 5 [Create Node 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、ノード プロファイルの名前を入力します（borderLeaf）。
b) [Nodes] フィールドで、[+] アイコンをクリックして [Select Node] ダイアログボックスを表示します。
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) [Use Router ID as Loopback Address] フィールドをオフにします。

（注） デフォルトでは、ルータ ID がループバック アドレスとして使用されます。これらが異なるようにする場合は、[Use Router ID as Loopback Address] チェックボックスをオフにします。

f) [Loopback Addresses] を展開し、[IP] フィールドに IP アドレスを入力します。[Update] をクリックし、[OK] をクリックします。

希望する IPv4 または IPv6 の IP アドレスを入力します。

g) [Nodes] フィールドで、[+] アイコンを展開して [Select Node] ダイアログボックスを表示します。

（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、次のノードを選択します（leaf2）。

i) [Router ID] フィールドに、一意のルータ ID を入力します。

j) [Use Router ID as Loopback Address] フィールドをオフにします。

（注） デフォルトでは、ルータ ID がループバック アドレスとして使用されます。これらが異なるようにする場合は、[Use Router ID as Loopback Address] チェックボックスをオフにします。

k) [Loopback Addresses] を展開し、[IP] フィールドに IP アドレスを入力します。[Update] をクリックし、[OK] をクリックします。[OK] をクリックします。

希望する IPv4 または IPv6 の IP アドレスを入力します。

ステップ 6 [Create Node Profile] ダイアログボックスで、[OSPF Interface Profiles] 領域の [+] アイコンをクリックします。

ステップ 7 [Create Interface Profile] ダイアログボックスで、次のタスクを実行します。

a) [Name] フィールドに、プロファイルの名前（portProf）を入力します。

b) [Interfaces] 領域で、[Routed Interfaces] タブをクリックし、[+] アイコンをクリックします。

c) [Select Routed Interfaces] ダイアログボックスの [Path] フィールドで、ドロップダウン リストから、最初のポート（leaf1、ポート 1/40）を選択します。

d) [IP Address] フィールドに、IP アドレスとマスクを入力します。[OK] をクリックします。

e) [Interfaces] 領域で、[Routed Interfaces] タブをクリックし、[+] アイコンをクリックします。

f) [Select Routed Interfaces] ダイアログボックスの [Path] フィールドで、ドロップダウン リストから、2 つ目のポート（leaf2、ポート 1/40）を選択します。

g) [IP Address] フィールドに、IP アドレスとマスクを入力します。[OK] をクリックします。

（注） この IP アドレスは、前に leaf1 に入力した IP アドレスと異なっている必要があります。

h) [Create Interface Profile] ダイアログボックスで、[OK] をクリックします。

インターフェイスが OSPF インターフェイスとともに設定されます。

ステップ 8 [Create Node Profile] ダイアログボックスで、[OK] をクリックします。

ステップ 9 [Create Routed Outside] ダイアログボックスで、[Next] をクリックします。
[Step 2 External EPG Networks] 領域が表示されます。

ステップ 10 [External EPG Networks] 領域で、[+] アイコンをクリックします。

ステップ 11 [Create External Network] 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、外部ネットワークの名前（extMgmt）を入力します。
b) [Subnet] を展開し、[Create Subnet] ダイアログボックスの [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。
c) [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。
d) **[Create External Network]** ダイアログボックスで、**[OK]** をクリックします。
e) **[Create Routed Outside]** ダイアログボックスで、**[Finish]** をクリックします。

（注） [Work] ペインで、[External Routed Networks] 領域に、外部ルーテッド ネットワークのアイコン（RtdOut）が表示されるようになりました。

NX-OS CLI を使用したテナントの OSPF 外部ルーテッド ネットワークの作成

外部ルーテッド ネットワーク接続の設定には、次のステップがあります。

1. テナントの下に VRF を作成します。
2. 外部ルーテッド ネットワークに接続された境界リーフ スイッチの VRF の L3 ネットワーキング構成を設定します。この設定には、インターフェイス、ルーティング プロトコル (BGP、OSPF、EIGRP) 、プロトコル パラメータ、ルートマップが含まれています。
3. テナントの下に外部 L3 EPG を作成してポリシーを設定し、これらの EPG を境界リーフ スイッチに導入します。ACI ファブリック内で同じポリシーを共有する VRF の外部ルーテッド サブネットが、1 つの「外部 L3 EPG」または 1 つの「プレフィクス EPG」を形成します。

設定は、2 つのモードで実現されます。

- テナント モード：VRF の作成および外部 L3 EPG 設定
- リーフ モード：L3 ネットワーキング構成と外部 L3 EPG の導入

次の手順は、テナントの OSPF 外部ルーテッド ネットワークを作成するためのものです。テナントの OSPF 外部ルーテッド ネットワークを作成するには、テナントを選択してからテナント用の VRF を作成する必要があります。

（注） この項の例では、テナント「exampleCorp」の「OnlineStore」アプリケーションの「web」epg に外部ルーテッド接続を提供する方法について説明します。

手順

ステップ 1 VLAN ドメインを設定します。

例：

```
apic1(config)# vlan-domain dom_exampleCorp
apic1(config-vlan)# vlan 5-1000
apic1(config-vlan)# exit
```

ステップ 2 テナント VRF を設定し、VRF のポリシーの適用を有効にします。

例：

```
apic1(config)# tenant exampleCorp
apic1(config-tenant)# vrf context
 exampleCorp_v1
apic1(config-tenant-vrf)# contract enforce
apic1(config-tenant-vrf)# exit
```

ステップ 3 テナント BD を設定し、ゲートウェイ IP を「public」としてマークします。エントリ「scope public」は、このゲートウェイ アドレスを外部 L3 ネットワークのルーティング プロトコルによるアドバタイズに使用できるようにします。

例：

```
apic1(config-tenant)# bridge-domain exampleCorp_b1
apic1(config-tenant-bd)# vrf member exampleCorp_v1
apic1(config-tenant-bd)# exit
apic1(config-tenant)# interface bridge-domain exampleCorp_b1
apic1(config-tenant-interface)# ip address 172.1.1.1/24 scope public
apic1(config-tenant-interface)# exit
```

ステップ 4 リーフの VRF を設定します。

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant exampleCorp vrf exampleCorp_v1
```

ステップ 5 OSPF エリアを設定し、ルート マップを追加します。

例：

```
apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant exampleCorp vrf exampleCorp_v1
apic1(config-leaf-ospf-vrf)# area 0.0.0.1 route-map map100 out
apic1(config-leaf-ospf-vrf)# exit
apic1(config-leaf-ospf)# exit
```

ステップ 6 VRF をインターフェイス (この例ではサブインターフェイス) に割り当て、OSPF エリアを有効にします。

例：

（注） サブインターフェイスの構成では、メイン インターフェイス (この例では、ethernet 1/11) は、「no switchport」によって L3 ポートに変換し、サブインターフェイスが使用するカプセル化 VLAN を含む vlan ドメイン (この例では dom_exampleCorp) を割り当てる必要があります。サブインターフェイス ethernet1/11.500 で、500 はカプセル化 VLAN です。

```
apic1(config-leaf)# interface ethernet 1/11
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vlan-domain member dom_exampleCorp
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface ethernet 1/11.500
apic1(config-leaf-if)# vrf member tenant exampleCorp vrf exampleCorp_v1
apic1(config-leaf-if)# ip address 157.10.1.1/24
apic1(config-leaf-if)# ip router ospf default area 0.0.0.1
```

ステップ 7 外部 L3 EPG ポリシーを設定します。これは、外部サブネットを特定し、epg「web」と接続する契約を消費するために一致させるサブネットが含まれます。

例：

```
apic1(config)# tenant t100
apic1(config-tenant)# external-l3 epg  l3epg100
apic1(config-tenant-l3ext-epg)# vrf member v100
apic1(config-tenant-l3ext-epg)# match ip 145.10.1.0/24
apic1(config-tenant-l3ext-epg)# contract consumer web
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)#exit
```

ステップ 8 リーフ スイッチの外部 L3 EPG を導入します。

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant t100 vrf v100
apic1(config-leaf-vrf)# external-l3 epg l3epg100
```

REST API を使用した管理テナントの OSPF 外部ルーテッド ネットワークの作成

- 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 外部ルーテッド ネットワークを作成するためのものです。テナントの OSPF 外部ルーテッド ネットワークを作成するには、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

管理テナントの OSPF 外部ルーテッド ネットワークを作成します。

例：

```
POST: https://apic-ip-address/api/mo/uni/tn-mgmt.xml

<fvTenant name="mgmt">
```

```
   <fvBD name="bd1">
      <fvRsBDToOut tnL3extOutName="RtdOut" />
      <fvSubnet ip="1.1.1.1/16" />
      <fvSubnet ip="1.2.1.1/16" />
      <fvSubnet ip="40.1.1.1/24" scope="public" />
      <fvRsCtx tnFvCtxName="inb" />
   </fvBD>
   <fvCtx name="inb" />

   <l3extOut name="RtdOut">
      <l3extRsL3DomAtt tDn="uni/l3dom-extdom"/>
      <l3extInstP name="extMgmt">
      </l3extInstP>
      <l3extLNodeP name="borderLeaf">
         <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="10.10.10.10"/>

         <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-102" rtrId="10.10.10.11"/>

         <l3extLIfP name='portProfile'>
           <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/40]"
ifInstT='l3-port' addr="192.168.62.1/24"/>
           <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-102/pathep-[eth1/40]"
ifInstT='l3-port' addr="192.168.62.5/24"/>
            <ospfIfP/>
                                  </l3extLIfP>
      </l3extLNodeP>
      <l3extRsEctx tnFvCtxName="inb"/>
      <ospfExtP areaId="57" />
   </l3extOut>
</fvTenant>
```

EIGRP 外部ルーテッド ネットワーク

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

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`
- 認証サポート
- サマリー プレフィックス
- 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。

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 **Navigation** ウィンドウで、***Tenant_name*** > **Networking** > **Protocol Policies** > **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** ペインの [**プロパティ** 、展開 **アドレス ファミリごとの EIGRP コンテキスト** 。

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、 **ナビゲーション**] ペインで、をクリックして **ネットワー キング** > **外部ルーテッド ネットワーク** 、目的のレイヤ 3 ネットワークの外部] をクリックします。

ステップ 11 **作業** ペインの [**プロパティ** 、チェック ボックスをオンに **EIGRP** 、EIGRP 自律システム番号を入力します。[Submit] をクリックします。`

ステップ 12 EIGRP インターフェイス ポリシーの作成、 **ナビゲーション**] ペインで、をクリックして **ネットワー キング** > **プロトコル ポリシー** > **EIGRP インターフェイス** し、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、ユーザが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、ユーザには、ポリシーのいずれかの選択に明示的には、デフォルトのポリシーは EIGRP が有効になっているときに利用自動的にします。

これで EIGRP の設定は完了です。

NX-OS スタイルの CLI を使用したEIGRPの設定

手順

ステップ 1 ファブリックの Application Policy Infrastructure Controller (APIC) に SSH 接続します。

例：

```
# ssh admin@node_name
```

ステップ 2 設定モードを開始します。

例：

```
apic1# configure
```

ステップ 3 テナントの設定モードを入力します。

例：

```
apic1(config)# tenant tenant1
```

ステップ 4 テナントでレイヤ 3 Outside を設定します:

例：

```
apic1(config-tenant)# show run
# Command: show running-config tenant tenant1
# Time: Tue Feb 16 09:44:09 2016
  tenant tenant1
    vrf context l3out
      exit
    l3out l3out-L1
      vrf member l3out
      exit
    l3out l3out-L3
      vrf member l3out
      exit
    external-l3 epg tenant1 l3out l3out-L3
      vrf member l3out
      match ip 0.0.0.0/0
      match ip 3.100.0.0/16
      match ipv6 43:101::/48
      contract consumer default
      exit
    external-l3 epg tenant1 l3out l3out-L1
      vrf member l3out
      match ipv6 23:101::/48
      match ipv6 13:101::/48
      contract provider default
      exit
    exit
```

ステップ 5 リーフで EIGRP の VRF を設定します:

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant tenant1 vrf l3out l3out l3out-L1
apic1(config-leaf-vrf)# show run
# Command: show running-config leaf 101 vrf context tenant tenant1 vrf l3out l3out
l3out-L1
# Time: Tue Feb 16 09:44:45 2016
  leaf 101
    vrf context tenant tenant1 vrf l3out l3out l3out-L1
      router-id 3.1.1.1
      route-map l3out-L1_in
        scope global
        ip prefix-list tenant1 permit 1:102::/48
        match prefix-list tenant1
          exit
        exit
      route-map l3out-L1_out
        scope global
        ip prefix-list tenant1 permit 3.102.10.0/23
        ip prefix-list tenant1 permit 3.102.100.0/31
        ip prefix-list tenant1 permit 3.102.20.0/24
        ip prefix-list tenant1 permit 3.102.30.0/25
        ip prefix-list tenant1 permit 3.102.40.0/26
        ip prefix-list tenant1 permit 3.102.50.0/27
        ip prefix-list tenant1 permit 3.102.60.0/28
        ip prefix-list tenant1 permit 3.102.70.0/29
        ip prefix-list tenant1 permit 3.102.80.0/30
        ip prefix-list tenant1 permit 3.102.90.0/32
        <OUTPUT TRUNCATED>
        ip prefix-list tenant1 permit ::/0
        match prefix-list tenant1
          exit
        exit
      route-map l3out-L1_shared
        scope global
        exit
      exit
    exit
```

ステップ 6 EIGRP インターフェイス ポリシーを設定します:

例：

```
apic1(config-leaf)# template eigrp interface-policy tenant1 tenant tenant1
This template will be available on all leaves where tenant tenant1 has a VRF deployment
apic1(config-template-eigrp-if-pol)# show run
# Command: show running-config leaf 101 template eigrp interface-policy tenant1 tenant
tenant1
# Time: Tue Feb 16 09:45:50 2016
  leaf 101
    template eigrp interface-policy tenant1 tenant tenant1
      ip hello-interval eigrp default 10
      ip hold-interval eigrp default 30
      ip throughput-delay eigrp default 20 tens-of-micro
      ip bandwidth eigrp default 20
      exit
    exit
```

ステップ 7 EIGRP の VRF ポリシーを設定します:

例：

```
apic1(config-leaf)# template eigrp vrf-policy tenant1 tenant tenant1
This template will be available on all leaves where tenant tenant1 has a VRF deployment
apic1(config-template-eigrp-vrf-pol)# show run
```

```
# Command: show running-config leaf 101 template eigrp vrf-policy tenant1 tenant tenant1
# Time: Tue Feb 16 09:46:31 2016
  leaf 101
    template eigrp vrf-policy tenant1 tenant tenant1
      metric version 64bit
      exit
    exit
```

ステップ 8 EIGRP VLAN インターフェイスを設定し、インターフェイスで EIGRP を有効にします:

例：

```
apic1(config-leaf)# interface vlan 1013
apic1(config-leaf-if)# show run
# Command: show running-config leaf 101 interface vlan 1013
# Time: Tue Feb 16 09:46:59 2016
  leaf 101
    interface vlan 1013
      vrf member tenant tenant1 vrf l3out
      ip address 101.13.1.2/24
      ip router eigrp default
      ipv6 address 101:13::1:2/112 preferred
      ipv6 router eigrp default
      ipv6 link-local fe80::101:13:1:2
      inherit eigrp ip interface-policy tenant1
      inherit eigrp ipv6 interface-policy tenant1
      exit
    exit
apic1(config-leaf-if)# ip summary-address ?
 eigrp  Configure route summarization for EIGRP
apic1(config-leaf-if)# ip summary-address eigrp default 11.11.0.0/16 ?
 <CR>
apic1(config-leaf-if)# ip summary-address eigrp default 11.11.0.0/16
apic1(config-leaf-if)# ip summary-address eigrp default 11:11:1::/48
apic1(config-leaf-if)# show run
# Command: show running-config leaf 101 interface vlan 1013
# Time: Tue Feb 16 09:47:34 2016
  leaf 101
    interface vlan 1013
      vrf member tenant tenant1 vrf l3out
      ip address 101.13.1.2/24
      ip router eigrp default
      ip summary-address eigrp default 11.11.0.0/16
      ip summary-address eigrp default 11:11:1::/48
      ipv6 address 101:13::1:2/112 preferred
      ipv6 router eigrp default
      ipv6 link-local fe80::101:13:1:2
      inherit eigrp ip interface-policy tenant1
      inherit eigrp ipv6 interface-policy tenant1
      exit
    exit
```

ステップ 9 物理インターフェイスに VLAN を適用します:

例：

```
apic1(config-leaf)# interface ethernet 1/5
apic1(config-leaf-if)# show run
# Command: show running-config leaf 101 interface ethernet 1 / 5
# Time: Tue Feb 16 09:48:05 2016
  leaf 101
    interface ethernet 1/5
      vlan-domain member cli
      switchport trunk allowed vlan 1213 tenant tenant13 external-svi l3out l3out-L1
```

```
      switchport trunk allowed vlan 1613 tenant tenant17 external-svi l3out l3out-L1
      switchport trunk allowed vlan 1013 tenant tenant1 external-svi l3out l3out-L1
     switchport trunk allowed vlan 666 tenant ten_v6_cli external-svi l3out l3out_cli_L1

      switchport trunk allowed vlan 1513 tenant tenant16 external-svi l3out l3out-L1
      switchport trunk allowed vlan 1313 tenant tenant14 external-svi l3out l3out-L1
      switchport trunk allowed vlan 1413 tenant tenant15 external-svi l3out l3out-L1
      switchport trunk allowed vlan 1113 tenant tenant12 external-svi l3out l3out-L1
      switchport trunk allowed vlan 712 tenant mgmt external-svi l3out inband_l1
      switchport trunk allowed vlan 1913 tenant tenant10 external-svi l3out l3out-L1
      switchport trunk allowed vlan 300 tenant tenant1 external-svi l3out l3out-L1
      exit
    exit
```

ステップ 10 ルータ EIGRP を有効にします:

例：

```
apic1(config-eigrp-vrf)# show run
# Command: show running-config leaf 101 router eigrp default vrf member tenant tenant1
vrf l3out
# Time: Tue Feb 16 09:49:05 2016
  leaf 101
    router eigrp default
      exit
    router eigrp default
      exit
    router eigrp default
      exit
    router eigrp default
      vrf member tenant tenant1 vrf l3out
        autonomous-system 1001 l3out l3out-L1
        address-family ipv6 unicast
          inherit eigrp vrf-policy tenant1
          exit
        address-family ipv4 unicast
          inherit eigrp vrf-policy tenant1
          exit
        exit
      exit
```

REST API を使用した EIGRP の設定

手順

ステップ 1 EIGRP コンテキスト ポリシーを設定します。

例：

```
<polUni>
    <fvTenant name="cisco_6">
        <eigrpCtxAfPol actIntvl="3" descr=""
dn="uni/tn-cisco_6/eigrpCtxAfP-eigrp_default_pol" extDist="170"
          intDist="90" maxPaths="8" metricStyle="narrow" name="eigrp_default_pol"
ownerKey="" ownerTag=""/>
    </fvTenant>
</polUni>
```

ステップ 2 EIGRP インターフェイス ポリシーを設定します。

例：

```
<polUni>
    <fvTenant name="cisco_6">
        <eigrpIfPol bw="10" ctrl="nh-self,split-horizon" delay="10"
delayUnit="tens-of-micro" descr="" dn="uni/tn-cisco_6/eigrpIfPol-eigrp_if_default"
         helloIntvl="5" holdIntvl="15" name="eigrp_if_default" ownerKey="" ownerTag=""/>

    </fvTenant>
</polUni>
```

ステップ 3 EIGRP VRF.を設定します。

例：

IPv4：

```
<polUni>
    <fvTenant name="cisco_6">
        <fvCtx name="dev">
          <fvRsCtxToEigrpCtxAfPol tnEigrpCtxAfPolName="eigrp_ctx_pol_v4" af="1"/>
        </fvCtx>
    </fvTenant>
</polUni>
```

IPv6：

```
<polUni>
    <fvTenant name="cisco_6">
        <fvCtx name="dev">
         <fvRsCtxToEigrpCtxAfPol tnEigrpCtxAfPolName="eigrp_ctx_pol_v6" af="ipv6-ucast"/>

        </fvCtx>
    </fvTenant>
</polUni>
```

ステップ 4 外部の EIGRP Layer3 を設定します。

例：

IPv4

```
<polUni>
    <fvTenant name="cisco_6">
        <l3extOut name="ext">
            <eigrpExtP asn="4001"/>
            <l3extLNodeP name="node1">
                <l3extLIfP name="intf_v4">
                    <l3extRsPathL3OutAtt addr="201.1.1.1/24" ifInstT="l3-port"
                      tDn="topology/pod-1/paths-101/pathep-[eth1/4]"/>
                    <eigrpIfP name="eigrp_ifp_v4">
                        <eigrpRsIfPol tnEigrpIfPolName="eigrp_if_pol_v4"/>
                    </eigrpIfP>
                </l3extLIfP>
            </l3extLNodeP>
        </l3extOut>
    </fvTenant>
</polUni>
```

IPv6

```
<polUni>
    <fvTenant name="cisco_6">
        <l3extOut name="ext">
```

```
            <eigrpExtP asn="4001"/>
            <l3extLNodeP name="node1">
                <l3extLIfP name="intf_v6">
                    <l3extRsPathL3OutAtt addr="2001::1/64" ifInstT="l3-port"
                      tDn="topology/pod-1/paths-101/pathep-[eth1/4]"/>
                    <eigrpIfP name="eigrp_ifp_v6">
                        <eigrpRsIfPol tnEigrpIfPolName="eigrp_if_pol_v6"/>
                    </eigrpIfP>
                </l3extLIfP>
            </l3extLNodeP>
        </l3extOut>
    </fvTenant>
</polUni>
```

IPv4 および IPv6

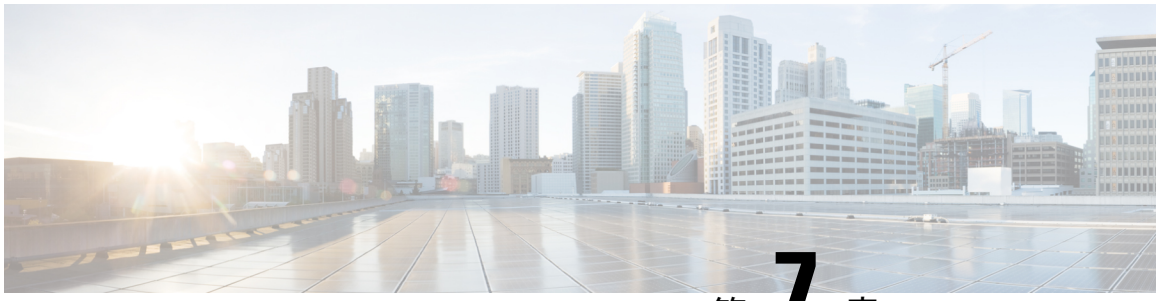
```
<polUni>
    <fvTenant name="cisco_6">
        <l3extOut name="ext">
            <eigrpExtP asn="4001"/>
            <l3extLNodeP name="node1">
                <l3extLIfP name="intf_v4">
                    <l3extRsPathL3OutAtt addr="201.1.1.1/24" ifInstT="l3-port"
                      tDn="topology/pod-1/paths-101/pathep-[eth1/4]"/>
                    <eigrpIfP name="eigrp_ifp_v4">
                        <eigrpRsIfPol tnEigrpIfPolName="eigrp_if_pol_v4"/>
                    </eigrpIfP>
                </l3extLIfP>

                <l3extLIfP name="intf_v6">
                    <l3extRsPathL3OutAtt addr="2001::1/64" ifInstT="l3-port"
                      tDn="topology/pod-1/paths-101/pathep-[eth1/4]"/>
                    <eigrpIfP name="eigrp_ifp_v6">
                        <eigrpRsIfPol tnEigrpIfPolName="eigrp_if_pol_v6"/>
                    </eigrpIfP>
                </l3extLIfP>
            </l3extLNodeP>
        </l3extOut>
    </fvTenant>
</polUni>
```

ステップ 5 （任意） インターフェイス ポリシー ノブを設定します。

例：

```
<polUni>
    <fvTenant name="cisco_6">
        <eigrpIfPol bw="1000000" ctrl="nh-self,split-horizon" delay="10"
          delayUnit="tens-of-micro" helloIntvl="5" holdIntvl="15" name="default"/>
    </fvTenant>
</polUni>
```

`Bandwidth（bw）属性は`（bw）属性は kbps で定義されています。`DelayUnit` 属性は、「1 万マイクロ」または「ピコ」です。



第 7 章

ルート集約

この章の内容は、次のとおりです。

ルート集約

ルート集約では、多数の具体的なアドレスを 1 つのアドレスに置き換えることで、ルートテーブルが簡素化します。たとえば、10.1.1.0/24、10.1.2.0/24、10.1.3.0/24 は 10.1.0.0/16 で置き換えることができます。ルート集約ポリシーにより、ボーダーリーフスイッチとそのネイバーリーフ スイッチの間でルートを効率的に共有することができます。BGP、OSPF、あるいは EIGRP のルート集約ポリシーは、ブリッジ ドメインまたは中継サブネットに適用されます。OSPF では、エリア間ルート集約と外部ルート集約がサポートされます。集約ルートはエクスポートされます。ファブリック内でのアドバタイズは行われません。

BGP、OSPF、および REST API を使用して EIGRP のルート集約の設定

手順

ステップ 1 次のように、REST API を使用して BGP ルート集約を設定します。

例：

```
<fvTenant name="common">
           <fvCtx name="vrf1"/>
   <bgpRtSummPol name="bgp_rt_summ" cntrl='as-set'/>
```

```
   <l3extOut name="l3_ext_pol" >
             <l3extLNodeP name="bLeaf">
                <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="20.10.1.1"/>
              <l3extLIfP name='portIf'>
              <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/31]"
ifInstT='l3-port' addr="10.20.1.3/24/>
              </l3extLIfP>
            </l3extLNodeP>
          <bgpExtP />
            <l3extInstP name="InstP" >
          <l3extSubnet ip="10.0.0.0/8" scope="export-rtctrl">
            <l3extRsSubnetToRtSumm tDn="uni/tn-common/bgprtsum-bgp_rt_summ"/>
            <l3extRsSubnetToProfile tnRtctrlProfileName="rtprof"/>
          </l3extSubnet>
        </l3extInstP>
        <l3extRsEctx tnFvCtxName="vrf1"/>
   </l3extOut>
</fvTenant>
```

ステップ 2 次の REST API を使用して、OSPF のエリア間および外部の集約を設定します。

例：

```
<?xml version="1.0" encoding="utf-8"?>
<fvTenant name="t20">
  <!--Ospf Inter External route summarization Policy-->
  <ospfRtSummPol cost="unspecified" interAreaEnabled="no" name="ospfext"/>
  <!--Ospf Inter Area route summarization Policy-->
  <ospfRtSummPol cost="16777215" interAreaEnabled="yes" name="interArea"/>
  <fvCtx name="ctx0" pcEnfDir="ingress" pcEnfPref="enforced"/>
  <!-- L3OUT backbone Area-->
  <l3extOut enforceRtctrl="export" name="l3_1" ownerKey="" ownerTag=""
targetDscp="unspecified">
    <l3extRsEctx tnFvCtxName="ctx0"/>
    <l3extLNodeP name="node-101">
      <l3extRsNodeL3OutAtt rtrId="20.1.3.2" rtrIdLoopBack="no"
tDn="topology/pod-1/node-101"/>
      <l3extLIfP name="intf-1">
       <l3extRsPathL3OutAtt addr="20.1.5.2/24" encap="vlan-1001" ifInstT="sub-interface"
 tDn="topology/pod-1/paths-101/pathep-[eth1/33]"/>
      </l3extLIfP>
    </l3extLNodeP>
    <l3extInstP name="l3InstP1">
      <fvRsProv tnVzBrCPName="default"/>
      <!--Ospf External Area route summarization-->
      <l3extSubnet aggregate="" ip="193.0.0.0/8" name="" scope="export-rtctrl">
        <l3extRsSubnetToRtSumm tDn="uni/tn-t20/ospfrtsumm-ospfext"/>
      </l3extSubnet>
    </l3extInstP>
    <ospfExtP areaCost="1" areaCtrl="redistribute,summary" areaId="backbone"
areaType="regular"/>
  </l3extOut>
  <!-- L3OUT Regular Area-->
  <l3extOut enforceRtctrl="export" name="l3_2">
    <l3extRsEctx tnFvCtxName="ctx0"/>
    <l3extLNodeP name="node-101">
      <l3extRsNodeL3OutAtt rtrId="20.1.3.2" rtrIdLoopBack="no"
tDn="topology/pod-1/node-101"/>
      <l3extLIfP name="intf-2">
       <l3extRsPathL3OutAtt addr="20.1.2.2/24" encap="vlan-1014" ifInstT="sub-interface"
 tDn="topology/pod-1/paths-101/pathep-[eth1/11]"/>
      </l3extLIfP>
```

```
    </l3extLNodeP>
    <l3extInstP matchT="AtleastOne" name="l3InstP2">
      <fvRsCons tnVzBrCPName="default"/>
      <!--Ospf Inter Area route summarization-->
      <l3extSubnet aggregate="" ip="197.0.0.0/8" name="" scope="export-rtctrl">
        <l3extRsSubnetToRtSumm tDn="uni/tn-t20/ospfrtsumm-interArea"/>
      </l3extSubnet>
    </l3extInstP>
    <ospfExtP areaCost="1" areaCtrl="redistribute,summary" areaId="0.0.0.57"
areaType="regular"/>
  </l3extOut>
</fvTenant>
```

ステップ 3 次の REST API を使用して EIGRP の集約を設定します。

例：

```
<fvTenant name="exampleCorp">
  <l3extOut name="out1">
    <l3extInstP  name="eigrpSummInstp" >
     <l3extSubnet aggregate="" descr="" ip="197.0.0.0/8" name="" scope="export-rtctrl">

       <l3extRsSubnetToRtSumm/>
      </l3extSubnet>
    </l3extInstP>
  </l3extOut>
  <eigrpRtSummPol name="pol1" />
```

（注） EIGRP を設定するルート集約ポリシーはありません。EIGRP の集約を有効にするために必要なだけの設定では、サマリー サブネット、InstP でです。

NX-OS スタイル CLI を使用した BGP、OSPF、および EIGRP のルート集約の設定

手順

ステップ 1 NX-OS CLI を使用して次のように BGP ルート集約を設定します:

a) 次のように BGP を有効にします:

例：

```
apic1(config)# pod 1
apic1(config-pod)# bgp fabric
apic1(config-pod-bgp)# asn 10
apic1(config-pod)# exit
apic1(config)# leaf 101
apic1(config-leaf)# router bgp 10
```

b) 次のように 要約ルートを設定します:

例：

```
apic1(config-bgp)# vrf member tenant common vrf vrf1
apic1(config-leaf-bgp-vrf)# aggregate-address 10.0.0.0/8
```

ステップ 2 NX-OS CLI を使用して次のように OSPF 外部集約を設定します。

例：

```
apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant common vrf vrf1
apic1(config-leaf-ospf-vrf)# summary-address 10.0.0.0/8
```

ステップ 3 NX-OS CLI を使用して次のように OSPF エリア間集約を設定します。

```
apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant common vrf vrf1
apic1(config-leaf-ospf-vrf)# area 0.0.0.2 range 10.0.0.0/8 cost 20
```

ステップ 4 NX-OS CLI を使用して次のように EIGRP 集約を設定します。

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/31 (Or interface vlan <vlan-id>)
apic1(config-leaf-if)# ip summary-address eigrp default 10.0.0.0/8
```

（注） EIGRP を設定するルート集約ポリシーはありません。EIGRP の集約を有効にするために必要なだけの設定では、サマリー サブネット、InstP でです。

GUI を使用した BGP、OSPF、および EIGRP のルート集約の設定

始める前に

次の設定のそれぞれに対して、L3 Out がすでに作成されていること。L3 Out については、外部ルーテッド ネットワーク、サブネット、およびルート集約ポリシーを作成することができます。

手順

ステップ 1 次のように、GUI を使用して BGP ルート集約を設定します:

a) メニュー バーで、**Tenants > common** を選択します。
b) ナビゲーション ウィンドウで、**Networking.> External Routed Networks** を選択します。
c) **External Routed Networks** を右クリックし、**Create Routed Outside** を選択します。

Create Routed Outside ダイアログボックスが表示されます。

d) 作業ウィンドウで、**BGP** の隣のチェック ボックスをオンにします。

e) **Name** フィールドに名前を入力し、**NEXT** をクリックします。
External EPG Networks ダイアログボックスが表示されます。

f) 作業ウィンドウで、+ 記号をクリックします。
Define an External Network ダイアログボックスが表示されます。

g) **Name** フィールドに名前を入力し、+ 記号 (**Route Summarization Policy** の上のもの) をクリックします。
Create Subnet ダイアログボックスが表示されます。

h) **Specify the Subnet** ダイアログボックスでは、次の方法で、ルート集約ポリシーをサブネットに関連付けることができます。

例：

- IP アドレスを **IP Address** フィールドに入力します。
- **Export Route Control Subnet** の隣のチェック ボックスをオンにします。
- **External Subnets for the External EPG** の隣のチェック ボックスをオンにします。
- **BGP Route Summarization Policy** ドロップダウンメニューで、既存の (デフォルトの) ポリシーを選択する場合には **default** を、新しいポリシーを作成する場合には **Create BGP route summarization policy** を選択します。
- **Create BGP route summarization policy** を選択した場合には、**Create BGP Route Summarization Policy** ダイアログボックスが表示されます。**Name** フィールドに名前を入力し、**Control State** チェック ボックスをオンにし **(Generate AS-SET information)**、**SUBMIT** をクリックし、**OK** をクリックし、**OK** をクリックし、**FINISH** をクリックします。

ステップ 2 GUI を使用して、次のように OSPF のエリア間および外部の集約を設定します。

a) メニュー バーで、**Tenants > common** を選択します。

b) ナビゲーション ウィンドウで、**Networking > External Routed Networks > Networks** を選択します。

c) 作業ウィンドウで、+ 記号 **(Route Summarization Policy** の上) をクリックします。
Create Subnet ダイアログボックスが表示されます。

d) **Specify the Subnet** ダイアログボックスでは、次の方法で、ルート集約ポリシーをサブネットに関連付けることができます。

例：

- IP アドレスを **IP Address** フィールドに入力します。
- **Export Route Control Subnet** の隣のチェック ボックスをオンにします。
- **External Subnets for the External EPG** の隣のチェック ボックスをオンにします。
- **OSPF Route Summarization Policy** ドロップダウンメニューで、既存の (デフォルトの) ポリシーを選択する場合には **default** を、新しいポリシーを作成する場合には **Create OSPF route summarization policy** を選択します。

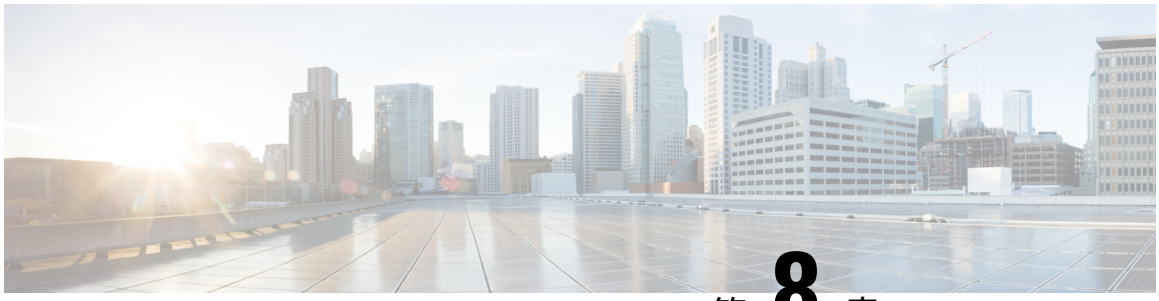
- **Create OSPF route summarization policy** を選択した場合には、**Create OSPF Route Summarization Policy** ダイアログボックスが表示されます。名前を **Name** フィールドに入力し、**Inter-Area Enabled** の隣のチェック ボックスをオンにし、**Cost** の隣に値を入力し、**SUBMIT** をクリックします。

ステップ 3 次のように、GUI を使用して EIGRP の集約を設定します。

a) メニュー バーで、**Tenants > common** を選択します。
b) ナビゲーション ウィンドウで、**Networking.> External Routed Networks** を展開します。
c) **External Routed Networks** を右クリックし、**Create Routed Outside** を選択します。
Create Routed Outside ダイアログボックスが表示されます。
d) 作業ウィンドウで、**EIGRP** の隣のチェック ボックスをオンにします。
e) **Name** フィールドに名前を入力し、**NEXT** をクリックします。
External EPG Networks ダイアログボックスが表示されます。
f) 作業ウィンドウで、**+** 記号をクリックします。
Define an External Network ダイアログボックスが表示されます。
g) **Name** フィールドに名前を入力し、**+** 記号 **(Route Summarization Policy** の上のもの) をクリックします。
Create Subnet ダイアログボックスが表示されます。
h) **Specify the Subnet** ダイアログボックスでは、次の方法で、ルート集約ポリシーをサブネットに関連付けることができます。

例：

- IP アドレスを **IP Address** フィールドに入力します。
- **Export Route Control Subnet** の隣のチェック ボックスをオンにします。
- **External Subnets for the External EPG** の隣のチェック ボックスをオンにします。
- **EIGRP Route Summarization** の隣のチェック ボックスをオンにし、**OK** をクリックし、**OK** をクリックし、 **FINISH** をクリックします。



第 8 章

ルート制御

この章の内容は、次のとおりです。

明示的なプレフィクス リストでルート マップ/プロファイル

ルート マップ/プロファイルについて

ルートプロファイルは、関連付けられているセットアクションルールと一致する論理アクション ルールの順序付きのセット (rtctrlCtxP) を定義する論理ポリシーです。ルート プロファイルでは、ルート マップの論理抽象です。複数のルート プロファイルは、1 個のルート マップにマージすることができます。ルートプロファイルには、以下のいずれかのタイプを指定できます。

- プレフィックスとルーティング ポリシーと一致: 普及サブネット (fvSubnet) と外部のサブネット (l3extSubnet) がルート プロファイルと組み合わせるし、マージされ、1 つのルート マップ (またはルート マップ エントリ) になります。一致するプレフィックスとルーティング ポリシーは、デフォルト値です。
- 一致ルーティング ポリシーのみ: は、ルート プロファイルは、ルート マップを生成する情報の唯一のソースと、その他のポリシー属性が上書きされます。

（注） 明示的なプレフィクス リストを使用すると、「ルーティング ポリシーのみを一致」にルートプロファイルのタイプを設定する必要があります。

一致後の設定プロファイルが定義されていると、レイヤ 3 Out でルート マップを作成する必要があります。ルート マップは以下のいずれかの方法で作成できます。

- エクスポート ルート コントロールでは、「デフォルト エクスポート」ルート マップとインポート ルート制御の「デフォルト インポート」ルート マップを作成します。
- (デフォルトエクスポートまたはデフォルトインポートしないという名前)他のルートマップを作成し、l3extInstPs またはサブネット、l3extInstP の下の 1 つまたは複数の関係を設定します。
- いずれにしても、ルートマップ内で rtctrlSubjP を指しているによって明示的なプレフィックス リストでルート マップに一致します。

エクスポートとインポート ルート マップの設定と一致ルールはグループ化されている相対的なシーケンスとともにグループ (rtctrlCtxP) 間で)。一致の各グループの下でさらに、いずれかに関係ステートメント (rtctrlCtxP) を設定し、または一致プロファイルの詳細については、使用可能な (rtctrlSubjP)。

(たとえばBGPプロトコル)は、アウトのレイヤ3で有効になっているすべてのプロトコルは、エクスポートを使用し、ルート フィルタ リングのマップをインポート ルート。

ルートマップ/プロファイルの明示的なプレフィックスリストのサポートについて

Cisco APIC では、公開ブリッジ ドメイン（BD）サブネットと外部の中継ネットワークのインバウンドおよびアウトバウンド ルート コントロールは、明示的なプレフィックス リストを通して提供されます。レイヤ 3 アウトのインバウンドおよびアウトバウンド ルート コントロールは、ルート マップ/プロファイル（rtctrlProfile）によって管理されます。ルート マップ/プロファイル ポリシーは、Cisco ACI ファブリックでレイヤ 3 アウトを完全に管理するプレフィックス リストをサポートしています。

プレフィックス リストのサブネットは、ブリッジ ドメイン公開サブネットまたは外部のネットワークを表すことがあります。明示的なプレフィックス リストは別の方法を示し、次の代わりに使用できます。

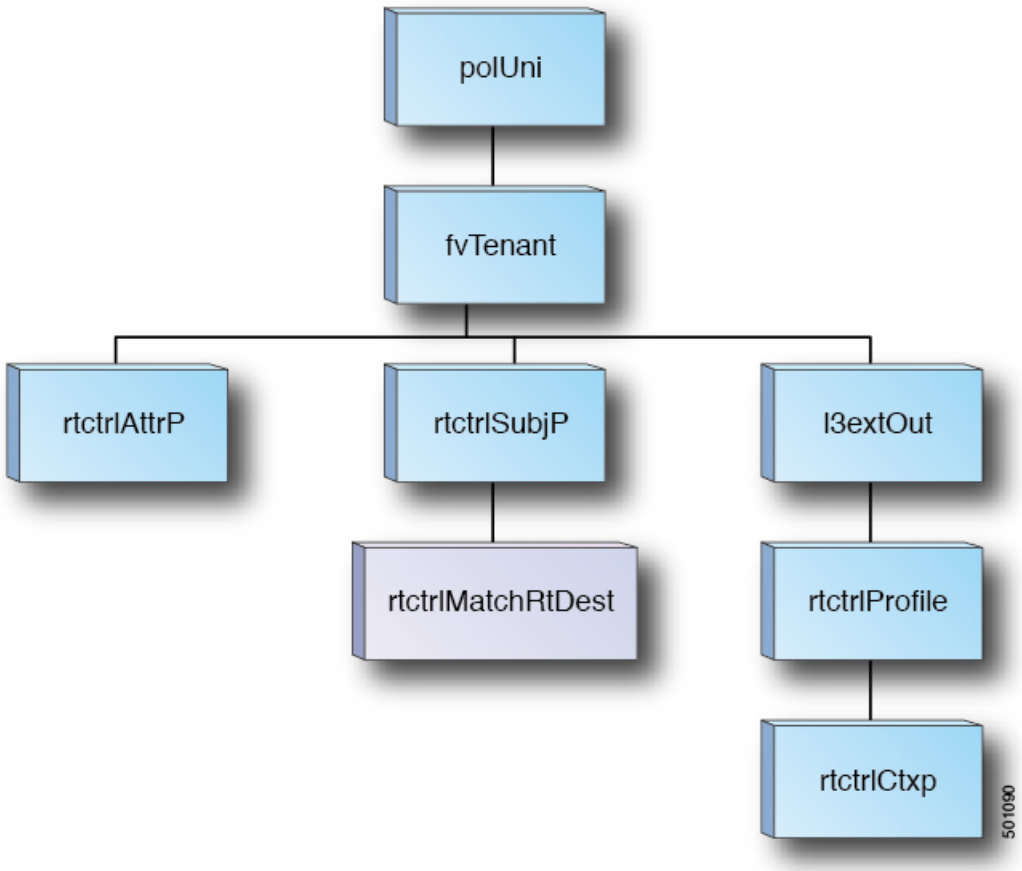
- BD を介して BD サブネットをレイヤ 3 アウト関係にアドバタイズします。

（注） BD のサブネットは、アドバタイズされるサブネットに公開としてマークする必要があります。

- 中継トラフィックと外部ネットワークをアドバタイジングするため、エクスポート/インポート ルート コントロールにより l3extInstP でサブネットを指定します。

明示的なプレフィックス リストは一致ルートの宛先（rtctrlMatchRtDest）と呼ばれる新しい一致タイプで定義されます。使用例は次の API の例で説明します。

図 *16 : API* の外部ポリシー モデル



明示的なプレフィクス リストを使用する場合の一致ルール、ルール設定に関する追加情報は次の通りです。

一致ルール

- テナント（fvTenant）で、ルートマップ フィルタ リングの一致プロファイル（rtctrlSubjP）を作成できます。各一致プロファイルは 1 個以上の一致ルールを含めることができます。一致ルールでは、複数の一致タイプをサポートしています。Cisco APIC リリース 2.1(x) 以前、サポートされていた一致タイプは明示的なプレフィックス リストおよびコミュニティ リストでした。

  Cisco APIC リリース 2.1(x) より、明示的なプレフィック一致または一致ルートの宛先（rtctrlMatchRtDest）がサポートされています。

  一致プレフィックス リスト（rtctrlMatchRtDest）は、オプションの集約フラグで 1 つまたは複数のサブネットがサポートされています。集約フラグは、設定で言及されているマスクから始めて、プレフィックスのアドレスファミリで許可されている最大数のマスクに達するまで、プレフィックスが複数のマスクと一致できるようにするために使用されます。これは、NX-OS ソフトウェアのプレフィックス リストの「le」オプションに相当します (たとえば 10.0.0.0/8 le 32)。

プレフィクス リストは、次のケースに対応するために使用できます。

- すべてを許可する（0.0.0.0/0 集約フラグ。「0.0.0.0/0 le 32」と同等）
- 1 つ以上の特定のプレフィクス (たとえば 10.1.1.0/24)
- 1 つ以上の集約フラグを伴うプレフィックス (たとえば 10.1.1.0/24 le 32 と同等)。

- 明示的なプレフィックス一致ルールには、1 個以上のサブネットを含むことが可能で、これらのサブネットはブリッジ ドメインの公開サブネットまたは外部ネットワークに指定できます。またサブネットは、最大サブネットマスクまで集約することもできます (IPv4 では /32、IPv6 では /128)。
- さまざまなタイプの複数の一致ルールが存在する場合 (一致コミュニティや明示的なプレフィックスの一致など)、一致ルールは、個々の一致タイプすべての一致ステートメントが一致する場合だけを許可します。これは AND フィルタと等価です。明示的なプレフィクス一致はサブジェクト プロファイル (rtctrlSubjP) に含められ、サブジェクト プロファイル下に他の一致ルールが存在する場合には論理 AND を形成します。
- 特定の一致タイプ (一致プレフィックス リスト) 内では、少なくとも 1 つの一致ルール ステートメントが一致する必要があります。複数の明示的なプレフィックス一致 (rtctrlMatchRtDest) は、論理 OR を形成する同じサブジェクト プロファイル (rtctrlSubjP) 下で定義することができます。

設定ルール

- 設定ポリシ - は、設定コミュニティ、設定タグなど明示的なプレフィックスで実施される設定ルールを定義するために作成する必要があります。

明示プレフィックス リストの集約サポート

一致するプレフィックス リストの各プレフィックス（rtctrlMatchRtDest）は、1 つのプレフィックス リスト エントリに一致する複数のサブネットをサポートするように集約できます。

集約されたプレフィックスと BD プライベート サブネット：集約または完全一致を使用して明示プレフィクス一致リスト内のサブネットが BD プライベート サブネットと一致していても、明示プレフィックス リストを使用してルーティング プロトコルからプライベート サブネットはアドバタイズされません。BD サブネットの範囲は、BD サブネットをアドバタイズするため明示プレフィックス リスト機能に対して「public」に設定する必要があります。

注意事項と制約事項

- 次の 2 つの方法のいずれかを選択し、ルートマップの設定を行う必要があります。両方の方法を使用する場合は、二重エントリになり定義されていないルートマップになります。
  - レイヤ 3 アウトサイド関係にブリッジ ドメイン（BD）でルートを追加し、BD を設定します。
  - rtctrlSubjP マッチ プロファイルで、マッチ プレフィックスを構成します。

- 2.3(x) 以降、**[deny-static]** 暗黙エントリはエクスポート ルート マップから削除されています。ユーザ-は、静的ルートのエクスポートを制御するために必要な許可と拒否を暗黙で設定する必要があります。

GUI を使用した、明示的なプレフィックス リストでルート マップ/プロファイルの設定

始める前に

- テナントと VRF を設定する必要があります。
- リーフ スイッチで VRF をイネーブルにする必要があります。

手順

ステップ 1 メニューバーで、**Tenant** をクリックし、**Navigation** ウィンドウで **Tenant_name** > **Networking** > **External Routed Networks** > **Match Rules for Route Maps** を展開します。

ステップ 2 **Match Rules for Route Maps** を右クリックし、**Create Match Rule for a Route Map** をクリックします。

ステップ 3 **Create Match Rule for a Route Map** ダイアログボックスで、ルールの名前を入力し、必要なコミュニティ条件を選択します。

ステップ 4 **Create Match Rule** ダイアログボックスで、**Match Prefix** を展開し、次の手順を実行します:

a) **IP** フィールドで、明示的プレフィックス リストを入力します。

明示的プレフィックスは、BD サブネットまたは外部ネットワークを表記できます。

b) **Route Type** フィールドで、**Route Destination** を選択します。

c) **Aggregate** チェック ボックスは、集約プレフィックスが必要な場合にのみオンにします。**Update** をクリックし、**Submit** をクリックします。

一致ルールは、1 つ以上の一致宛先ルールと、1 つ以上の一致コミュニティ条件を持つことができます。一致の種類では AND フィルタがサポートされています。これを利用すると、受け入れられるためには、一致ルール内のすべて条件がルート一致ルールと一致することが必要になります。**Match Destination Rules** に複数の一致プレフィックスがある場合には、OR フィルタがサポートされます。これを利用すると、任意の一致プレフィックスがルート タイプとして受け入れられます。

ステップ 5 **External Routed Networks** の下で、利用可能なデフォルト レイヤ 3 Out をクリックして選択します。

別のレイヤ 3 Out が必要な場合には、代わりにそれを選択することができます。

ステップ 6 **Route Maps/Profiles** を右クリックし、**Create Route Map/Profile** をクリックします。

ステップ 7 **Create Route Map** ダイアログボックスで、デフォルトのルート マップを使用するか、使用するルート マップの名前を入力します。

この例では、**default_export** ルート マップを使用します。

ステップ 8 **Type** フィールドで、**Match Routing Policy Only** を選択します。

一致ルーティング ポリシーは、グローバルな RPC 一致宛先ルートです。このフィールドで使用できる他のオプションとしては、一致プレフィックスおよびルーティング ポリシーで、RPC ルーティング ポリシーの宛先ルートと組み合わせることができます。

ステップ 9 + アイコンを展開して **Create Route Control Context** ダイアログボックスを表示します。

ステップ 10 ルート制御のコンテキストの名前を入力し、各フィールドで必要なオプションを選択します。一致ルール (**手順11**) で定義した基準に一致するルートを拒否するには、**deny** を選択します。デフォルトのアクションは **permit** です。

ステップ 11 **Match Rule** フィールドで、前に作成したルールを選択します。

ステップ 12 **Set Rule** フィールドで、**Create Set Rules for a Route Map** を選択します。

通常は、ルート マップ/プロファイルで一致させることにより、プレフィックス リストに入出力を許可しますが、それに加えて何らかの属性をこれらのルートに設定し、その属性を持つルートをさらに一致させることもできます。

ステップ 13 **Create Set Rules for a Route Map** ダイアログボックスで、アクション ルールの名前を入力し、必要なチェック ボックスをオンにします。**Submit** をクリックします。

ステップ 14 **Create Route Control Context** ダイアログボックスで、**OK** をクリックします。そして、**Create Route Map/Profile** ダイアログボックスで **Submit** をクリックします。

これで、ルート マップ/プロファイルの作成は完了です。ルート マップは、一致アクション ルールと設定アクション ルールの組み合わせです。ルートマップは、ユーザの必要に応じて、エクスポート プロファイルまたはインポート プロファイルまたは再配布可能プロファイルに関連付けられます。ルート マップのプロトコルを有効にすることができます。

NX-OS スタイルの CLI を使用した明示的なプレフィックス リストによるルートマップ/プロファイルの設定

始める前に

- テナントと VRF を設定する必要があります。
- リーフ スイッチで VRF をイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	コンフィギュレーション モードに入ります。
ステップ 2	**leaf** *node-id* 例： `apic1(config)# leaf 101`	設定するリーフを指定します。
ステップ 3	**template route group** *group-name* **tenant** *tenant-name* 例： `apic1(config-leaf)# template route group g1 tenant exampleCorp`	ルート グループ テンプレートを作成します。 （注） ルート グループ (マッチ ルール) は、1 つ以上の IP プレフィックスと 1 つ以上のマッチ コミュニティ タームを持つことができます。マッチ タイプ全体では、AND フィルタがサポートされているため、ルート マッチ ルールが受け入れられるようにするために、ルート グループ内のすべての条件がマッチしている必要があります。ルート グループに複数の IP プレフィックスがある場合は、OR フィルタがサポートされます。マッチする場合は、いずれかのプレフィックスがルート タイプとして受け入れられます。
ステップ 4	**ip prefix permit** *prefix/masklen* [**le**{**32** | **128** }] 例： `apic1(config-route-group)# ip prefix permit 15.15.15.0/24`	ルート グループに IP プレフィックスを追加します。 （注） IP プレフィックスは、BD サブネットまたは外部ネットワークを示すことができます。集約プレフィックスが必要な場合は、IPv4 にはオプションの le 32 を、IPv6 には le 128 を使用してください。

	コマンドまたはアクション	目的
ステップ 5	**community-list** [**standard** | **expanded**] *expression* 例： `apic1(config-route-group)# community-list standard 65535:20`	コミュニティーもIPプレフィックスと照合する必要がある場合は、コミュニティのマッチ基準を追加します。
ステップ 6	**vrf context tenant** *tenant-name* **vrf** *vrf-name* 例： `apic1(config-leaf)# vrf context tenant exampleCorp vrf v1`	ノードのテナントVRFモードを開始します。
ステップ 7	**template route-profile** *profile-name* 例： `apic1(config-leaf-vrf)# template route-profile rp1`	マッチするルートに適用する必要のあるセットアクションを含むテンプレートを作成します。
ステップ 8	**set metric** *value* 例： `apic1(config-leaf-vrf-template-route-profile)# set metric 128`	必要な属性 (アクションの設定) をテンプレートに追加します。
ステップ 9	**exit** 例： `apic1(config-leaf-vrf-template-route-profile)# exit`	テンプレート モードを終了します。
ステップ 10	**route-map** *map-name* 例： `apic1(config-leaf-vrf)# route-map bgpMap`	ルートマップを作成し、ルートマップコンフィギュレーションモードを開始します。
ステップ 11	**match route group** *group-name* [**order** *number*] [**deny**] 例： `apic1(config-leaf-vrf-route-map)# match route group g1 order 1`	すでに作成されているルートグループとマッチし、マッチモードを開始してルートプロファイルを設定します。さらに、ルートグループで定義されているマッチ基準にマッチするルートを拒否する必要がある場合は、キーワード **[Deny]**を選択します。デフォルトの設定は **[Permit]** です。
ステップ 12	**inherit route-profile** *profile-name* [**order** *number*] 例：	ルート プロファイルを継承します (アクションを設定します)。

	コマンドまたはアクション	目的
	`apic1(config-leaf-vrf-route-map-match)# inherit route-profile rp1`	（注） これらのアクションは、マッチしたルートに適用されます。または、ルートプロファイルを継承する代わりに、インラインで設定されたアクションを設定することもできます。
ステップ 13	**[no]bridge-domain-match** 例： `apic1(config-leaf-vrf)# no bridge-domain-match`	これは任意のコマンドです。**no bridge-domain-match** コマンドを設定すると、**match bridge-domain** コマンドは有効になりません。 （注） これは、テナント共通が外部レイヤ 3 出力構成を持ち、複数のテナントが使用する次のシナリオで役立ちます。テナント共通管理者は、個々のテナント管理者が BD パブリック サブネットのエクスポートを制御できないようにすることができます (NX-OSスタイルCLIでは、**match bridge-domain**コマンドと一致します)。代わりに、テナント共通は、BD サブネットを明示的プレフィックス リスト マッチ ステートメントに追加して、同じ結果を達成することができます。これにより、複数のテナントが同じテナント共通レイヤ 3 出力/VRF を使用している場合に、サブネット構成エラーを防止できます。
ステップ 14	**route-map** *map-name* {**in** | **out** } 例： `apic1(config-leaf-bgp-vrf-neighbor)# route-map bgpMap out`	BGP ネイバのルート マップを設定します。

REST API を使用して、明示的なプレフィックス リストでルート マップ/プロファイルの設定

始める前に

- テナントと VRF を設定する必要があります。

手順

明示的なプレフィックス リストを使用してルート マップ/プロファイルを設定します。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<fvTenant name="PM" status="">
   <rtctrlAttrP name="set_dest">
      <rtctrlSetComm community="regular:as2-nn2:5:24" />
   </rtctrlAttrP>
   <rtctrlSubjP name="allow_dest">
      <rtctrlMatchRtDest ip="192.169.0.0/24" />
      <rtctrlMatchCommTerm name="term1">
         <rtctrlMatchCommFactor community="regular:as2-nn2:5:24" status="" />
         <rtctrlMatchCommFactor community="regular:as2-nn2:5:25" status="" />
      </rtctrlMatchCommTerm>
      <rtctrlMatchCommRegexTerm commType="regular" regex="200:*" status="" />
   </rtctrlSubjP>
   <rtctrlSubjP name="deny_dest">
      <rtctrlMatchRtDest ip="192.168.0.0/24" />
   </rtctrlSubjP>
   <fvCtx name="ctx" />
   <l3extOut name="L3Out_1" enforceRtctrl="import,export" status="">
      <l3extRsEctx tnFvCtxName="ctx" />
      <l3extLNodeP name="bLeaf">
         <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="1.2.3.4" />
         <l3extLIfP name="portIf">
            <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/25]"
ifInstT="sub-interface" encap="vlan-1503" addr="10.11.12.11/24" />
            <ospfIfP />
         </l3extLIfP>
         <bgpPeerP addr="5.16.57.18/32" ctrl="send-com" />
         <bgpPeerP addr="6.16.57.18/32" ctrl="send-com" />
      </l3extLNodeP>
      <bgpExtP />
      <ospfExtP areaId="0.0.0.59" areaType="nssa" status="" />
      <l3extInstP name="l3extInstP_1" status="">
         <l3extSubnet ip="17.11.1.11/24" scope="import-security" />
      </l3extInstP>
      <rtctrlProfile name="default-export" type="global" status="">
         <rtctrlCtxP name="ctx_deny" action="deny" order="1">
            <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="deny_dest" status="" />
         </rtctrlCtxP>
         <rtctrlCtxP name="ctx_allow" order="2">
            <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="allow_dest" status="" />
         </rtctrlCtxP>
         <rtctrlScope name="scope" status="">
            <rtctrlRsScopeToAttrP tnRtctrlAttrPName="set_dest" status="" />
         </rtctrlScope>
      </rtctrlProfile>
```

```
   </l3extOut>
   <fvBD name="testBD">
      <fvRsBDToOut tnL3extOutName="L3Out_1" />
      <fvRsCtx tnFvCtxName="ctx" />
      <fvSubnet ip="40.1.1.12/24" scope="public" />
      <fvSubnet ip="40.1.1.2/24" scope="private" />
      <fvSubnet ip="2003::4/64" scope="public" />
   </fvBD>
</fvTenant>
```

ルート制御プロトコル

インポート制御とエクスポート制御を使用するルーティング制御プロトコルの設定について

このトピックでは、インポート制御とエクスポート制御を使用するルーティング制御プロトコルを設定する方法の典型的な例を示します。これは、外部 BGP を使用したネットワーク接続のレイヤ 3 が設定されていると仮定します。OSPF で設定されたネットワークの外部レイヤ 3 の次のタスクを実行することもできます。

（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 multipod 接続を設定する場合は、MTU が両側で適切に設定されていることが重要です。ACI、Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定された MTU 値は IP ヘッダーを考慮に入れています（結果として、最大パケット サイズは、ACI で 9216 バイト、NX-OS および IOS で 9000 バイトに設定されます）。ただし、IOS XR などの他のプラットフォームは、パケット ヘッダーのを除く MTU 値を設定します（結果として最大パケット 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。

GUI を使用した、インポート制御とエクスポート制御を使用するルート制御プロトコルの設定

この例では、レイヤ 3 Outside ネットワーク接続を BGP を使用するように設定していることを前提としています。OSPF を使用するように設定されたネットワークに対してもこれらのタスクを実行することができます。

このタスクでは、インポートポリシーとエクスポートポリシーの作成手順を示します。デフォルトでは、インポート制御は適用されていないため、インポート制御を手動で割り当てる必要があります。

始める前に

- テナント、プライベートネットワーク、およびブリッジドメインが作成されていること。
- テナント ネットワークのレイヤ 3 Outside が作成されていること。

手順

ステップ 1 メニュー バーで、**[TENANTS]** > ***[Tenant_name]*** > **[Networking]** > **[External Routed Networks]** > ***[Layer3_Outside_name]*** の順にクリックします。

ステップ 2 *Layer3_Outside_name* を右クリックして、**Create Route Map** をクリックします。

ステップ 3 **Create Route Map** ダイアログボックスで、次の操作を実行します:

a) [Name] フィールドのドロップダウン リストから、適切なルート プロファイルを選択します。
選択内容に応じて、特定の Outside でアドバタイズされている内容が自動的に使用されます。

b) **Type** フィールドで、**Match Prefix AND Routing Policy** を選択します。

c) [Order] を展開します。

ステップ 4 [Create Route Control Context] ダイアログボックスで、次の操作を実行します。

a) [Order] フィールドで、目的の順序の番号を選択します。

b) [Name] フィールドに、ルート制御プライベート ネットワークの名前を入力します。

c) **Match Rule** フィールドのドロップダウンリストで、**Create Match Rule For a Route Map** をクリックします。

d) **Create Match Rule** ダイアログボックスの **Name** フィールドに、一致ルールの名前を入力します。[Submit] をクリックします。`

必要に応じて、正規表現による一致コミュニティ条件および一致コミュニティ条件を指定します。一致コミュニティファクタでは、名前、コミュニティ、およびスコープを指定する必要があります。

e) **Set Attribute** ドロップダウンリストから、**Create Set Rules For a Route Map** を選択します。

f) **Create Set Rules For a Route Map** ダイアログボックスの **Name** フィールドに、ルールの名前を入力します。

g) 設定するルールのチェックボックスをオンにし、選択肢として表示されている適切な値を選択します。**Submit** をクリックします。
ポリシーが作成され、アクション ルールに関連付けられました。

h) **OK** をクリックします。

i) **Create Route Map** ダイアログボックスで、**Submit** をクリックします。

ステップ 5 [Navigation] ペインで、**[Route Profile]** > ***[route_profile_name]*** > ***[route_control_private_network_name]*** の順に選択します。
[Work] ペインの [Properties] に、ルート プロファイル ポリシーと関連アクション ルール名が表示されます。

ステップ 6 [Navigation] ペインで、[Layer3_Outside_name] をクリックします。
Work ウィンドウに、**Properties** が表示されます。

ステップ 7 （任意） **Route Control Enforcement** フィールドをクリックし、**Import** チェック ボックスをオンにして、インポート ポリシーを有効にします。

インポート制御ポリシーはデフォルトで有効になっていませんが、ユーザが有効にすることができます。インポート制御ポリシーは BGP と OSPF でサポートされていますが、EIGRP ではサポートされていません。ユーザがサポートされていないプロトコルのインポート制御ポリシーを有効にしても、自動的に無視されます。エクスポート制御ポリシーは、BGP、EIGRP、および OSPF でサポートされます。

（注） BGP が OSPF 上で確立されると、インポート制御ポリシーは BGP にのみ適用され、OSPF は無視されます。

ステップ 8 カスタマイズされたエクスポート ポリシーを作成するには、**Route Map/Profiles** を右クリックし、**Create Route Map** をクリックし、次の操作を行います:

a) **Create Route Map** ダイアログボックスで、**Name** フィールドのドロップダウンリストから、エクスポート ポリシーを選択するか、名前を入力します。
b) ダイアログ ボックスの [+] 記号を展開します。
c) [Create Route Control Context] ダイアログボックスの [Order] フィールドで、値を選択します。
d) [Name] フィールドに、ルート制御プライベート ネットワークの名前を入力します。
e) （任意） **Match Rule** フィールドのドロップダウンリストから **Create Match Rule For a Route Map** を選択し、必要に応じて一致ルール ポリシーを作成して、アタッチします。
f) **Set Attribute** フィールドのドロップダウンリストから、**Create Set Rules For a Route Map** を選択して、**OK** をクリックします。
   または、必要に応じて既存の set アクションを選択し、**OK** をクリックします。
g) **Create Set Rules For A Route Map** ダイアログボックスの **Name** フィールドに名前を入力します。
h) 設定するルールのチェックボックスをオンにし、選択肢として表示されている適切な値を選択します。**Submit** をクリックします。
   [Create Route Control Context] ダイアログ ボックスでは、ポリシーが作成されてアクション ルールに関連付けられています。
i) **OK** をクリックします。
j) **Create Route Map** ダイアログボックスで、**Submit** をクリックします。

[Work] ペインに、エクスポート ポリシーが表示されます。

（注） エクスポートポリシーを有効にするには、最初に適用する必要があります。この例では、このポリシーはネットワークのすべてのサブネットに適用されます。

ステップ 9 [Navigation] ペインで、**[External Routed Networks]** > ***[External_Routed_Network_name]*** > **[Networks]** > ***[Network_name]*** の順に展開し、次の操作を実行します。

a) **Route Control Profile** を展開します。
b) **Name** フィールドのドロップダウン リストから、前に作成したポリシーを選択します。
c) **Direction** フィールドのドロップダウン リストから、**Route Control Profile** を選択します。**Update** をクリックします。

NX-OS スタイルの CLI を使用した、インポート制御とエクスポート制御を使用するルート制御プロトコルの設定

この例では、ネットワーク接続 BGP を使用して外部レイヤ 3 が設定されていることを前提としています。OSPF を使用するように設定されたネットワークに対してもこれらのタスクを実行することができます。

ここでは、NX-OS CLI を使用してルート マップを作成する方法を説明します。

始める前に

- テナント、プライベート ネットワーク、およびブリッジ ドメインが作成されていること。
- レイヤ 3 Outside テナント ネットワークが設定されていること。

手順

ステップ 1 一致コミュニティ、一致プレフィックス リストを使用したインポート ルート制御

例：

```
apic1# configure
apic1(config)# leaf 101
    # Create community-list
apic1(config-leaf)# template community-list standard CL_1 65536:20 tenant exampleCorp
apic1(config-leaf)# vrf context tenant exampleCorp vrf v1

     #Create Route-map and use it for BGP import control.
apic1(config-leaf-vrf)# route-map bgpMap
    # Match prefix-list and set route-profile actions for the match.
apic1(config-leaf-vrf-route-map)# ip prefix-list list1 permit 13.13.13.0/24
apic1(config-leaf-vrf-route-map)# ip prefix-list list1 permit 14.14.14.0/24
apic1(config-leaf-vrf-route-map)# match prefix-list list1
apic1(config-leaf-vrf-route-map-match)# set tag 200
apic1(config-leaf-vrf-route-map-match)# set local-preference 64

apic1(config-leaf)# router bgp 100
apic1(config-bgp)# vrf member tenant exampleCorp vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 3.3.3.3
apic1(config-leaf-bgp-vrf-neighbor)# route-map bgpMap in
```

ステップ 2 一致 BD、デフォルトのエクスポート ルート プロファイルを使用したエクスポート ルート制御

例：

```
# Create custom and "default-export" route-profiles
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant exampleCorp vrf v1
apic1(config-leaf-vrf)# template route-profile default-export
apic1(config-leaf-vrf-template-route-profile)# set metric 256
apic1(config-leaf-vrf)# template route-profile bd-rtctrl
apic1(config-leaf-vrf-template-route-profile)# set metric 128

#Create a Route-map and match on BD, prefix-list
apic1(config-leaf-vrf)# route-map bgpMap
apic1(config-leaf-vrf-route-map)# match bridge-domain bd1
apic1(config-leaf-vrf-route-map-match)#exit
apic1(config-leaf-vrf-route-map)# match prefix-list p1
apic1(config-leaf-vrf-route-map-match)#exit
apic1(config-leaf-vrf-route-map)# match bridge-domain bd2
apic1(config-leaf-vrf-route-map-match)# inherit route-profile bd-rtctrl
```

（注） この場合、bd1 のパブリック サブネットとプレフィックスリスト p1 を照合するプレフィックスが、ルート プロファイルの「default-export」を使用してエクスポートされ、bd2 のパブリック サブネットはルート プロファイルの「bd-rtctrl」を使用してエクスポートされます。

REST API を使用した、インポート制御とエクスポート制御によるルーティング制御プロトコルの設定

この例では、ネットワーク接続 BGP を使用して外部レイヤ 3 が設定されていることを前提としています。OSPF を使用してネットワークを次のタスクを実行することもできます。

始める前に

- テナント、プライベート ネットワーク、およびブリッジ ドメインが作成されていること。
- レイヤ 3 Outside テナント ネットワークが設定されていること。

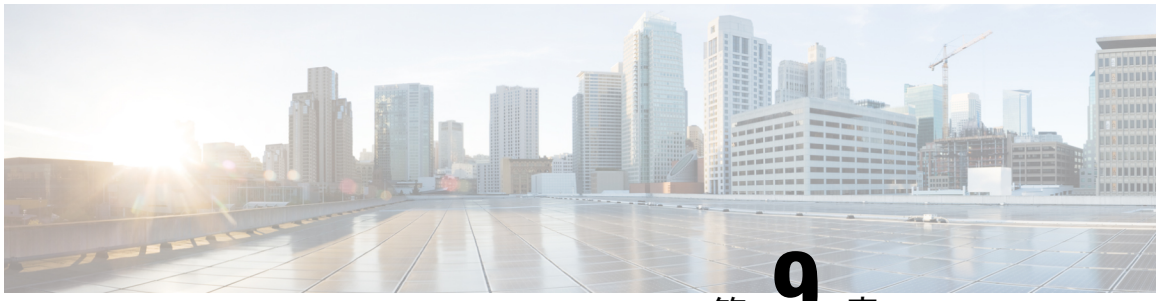
手順

インポート制御とエクスポート制御を使用するルート制御プロトコルを設定します。

例：

```
<l3extOut descr="" dn="uni/tn-Ten_ND/out-L3Out1" enforceRtctrl="export" name="L3Out1"
ownerKey="" ownerTag="" targetDscp="unspecified">
        <l3extLNodeP descr="" name="LNodeP1" ownerKey="" ownerTag="" tag="yellow-green"
```

```
 targetDscp="unspecified">
            <l3extRsNodeL3OutAtt rtrId="1.2.3.4" rtrIdLoopBack="yes"
tDn="topology/pod-1/node-101">
                <l3extLoopBackIfP addr="2000::3" descr="" name=""/>
            </l3extRsNodeL3OutAtt>
            <l3extLIfP descr="" name="IFP1" ownerKey="" ownerTag="" tag="yellow-green">
                <ospfIfP authKeyId="1" authType="none" descr="" name="">
                    <ospfRsIfPol tnOspfIfPolName=""/>
                </ospfIfP>
                <l3extRsNdIfPol tnNdIfPolName=""/>
                <l3extRsPathL3OutAtt addr="10.11.12.10/24" descr="" encap="unknown"
ifInstT="l3-port"
llAddr="::" mac="00:22:BD:F8:19:FF" mtu="1500"
tDn="topology/pod-1/paths-101/pathep-[eth1/17]" targetDscp="unspecified"/>
            </l3extLIfP>
        </l3extLNodeP>
        <l3extRsEctx tnFvCtxName="PVN1"/>
        <l3extInstP descr="" matchT="AtleastOne" name="InstP1" prio="unspecified"
targetDscp="unspecified">
            <fvRsCustQosPol tnQosCustomPolName=""/>
            <l3extSubnet aggregate="" descr="" ip="192.168.1.0/24" name="" scope=""/>
        </l3extInstP>
        <ospfExtP areaCost="1" areaCtrl="redistribute,summary" areaId="0.0.0.1"
areaType="nssa" descr=""/>
        <rtctrlProfile descr="" name="default-export" ownerKey="" ownerTag="">
            <rtctrlCtxP descr="" name="routecontrolpvtnw" order="3">
                <rtctrlScope descr="" name="">
                    <rtctrlRsScopeToAttrP tnRtctrlAttrPName="actionruleprofile2"/>
                </rtctrlScope>
            </rtctrlCtxP>
        </rtctrlProfile>
    </l3extOut>
```



第 9 章

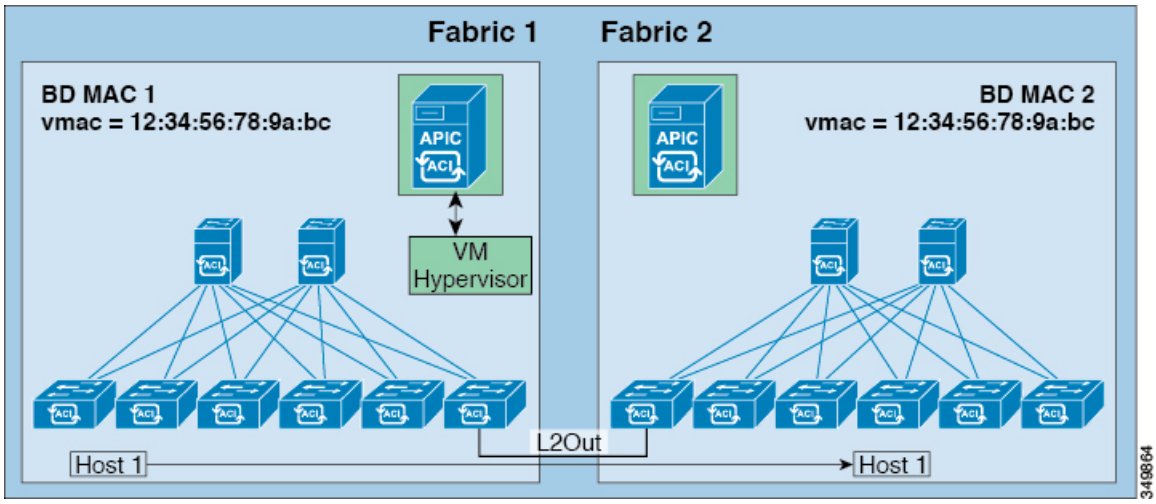
共通パーベイシブ ゲートウェイ

この章の内容は、次のとおりです。

概要

この例は、Cisco APIC を使用して、IPv4 共通パーベイシブ ゲートウェイを設定する方法について示しています。

ブリッジ ドメインごとに IPv4 共通ゲートウェイを使用して 2 つの ACI ファブリックを設定できます。これにより、1 つ以上の仮想マシン（VM）または従来型のホストを、ホストの IP アドレスを保持したまま、ファブリック間で移動できます。ファブリック間の VM ホストの移動は、VM ハイパーバイザによって自動的に行うことができます。ACI ファブリックは、同じ場所に配置することも、複数のサイト間でプロビジョニングすることもできます。ACI ファブリック間のレイヤ 2 接続は、ローカル リンクか、ブリッジ型ネットワークにわたるものになります。次の図は、基本的な共通パーベイシブ ゲートウェイ トポロジを示しています。



（注） 2 つの Cisco ACI ファブリックを相互接続するために用いられるトポロジによっては、相互接続するデバイスが、ゲートウェイ スイッチの仮想インターフェイス (SVI) の仮想 MAC アドレスを持つトラフィックの送信元を除外することが必要となります。

GUI を使用した共通パーベイシブ ゲートウェイの設定

始める前に

- テナントおよび VRF が作成されていること。
- ブリッジ ドメインの仮想 MAC アドレスとサブネットの仮想 IP アドレスは、ブリッジ ドメインのすべての ACI ファブリックで同じにする必要があります。複数のブリッジ ドメインを、接続されている ACI ファブリック間で通信するように設定できます。仮想 MAC アドレスと仮想 IP アドレスは、ブリッジ ドメイン間で共有できます。
- ACI ファブリック間で通信するように設定されているブリッジ ドメインは、**フラッド** モードである必要があります。
- ブリッジ ドメインの 1 つの EPG のみを (BD に複数の EPG がある場合) 、2 つ目のファブリックに接続されているポートの境界リーフ上に設定する必要があります。
- 2 つの ACI ファブリック間のパーベイシブ共通ゲートウェイを有効にする相互接続されたレイヤ 2 ネットワークには、ホストを直接接続しないでください。

手順

ステップ 1 メニュー バーで、**[TENANTS]** をクリックします。

ステップ 2 **[Navigation]** ペインで、***[Tenant_name]*** > **[Networking]** > **[Bridge Domains]** の順に展開します。

ステップ 3 **[Bridge Domains]** を右クリックし、**[Create Bridge Domain]** をクリックします。

ステップ 4 **[Create Bridge Domain]** ダイアログ ボックスで、必要な操作を実行し、適切な属性を選択します。

a) **[Main]** タブで、**[Name]** フィールドにブリッジ ドメインの名前を入力し、残りのフィールドに必要な値を選択します。

b) **[L3 configurations]** タブで **[Subnets]** を展開し、**[Create Subnets]** ダイアログボックスの **[Gateway IP]** フィールドに IP アドレスを入力します。

c) **[Treat as virtual IP address]** フィールドで、チェックボックスをオンにします。**[Ok]** をクリックし、**[Finish]** をクリックします。

d) **[Make this IP address primary]** フィールドで、DHCP リレーにこの IP アドレスを指定するチェックボックスをオンにします。

このチェック ボックスをオンにすると、DHCP リレーにのみ影響します。

e) **[Ok]** をクリックし、**[Finish]** をクリックします。

f) もう一度 **[Subnets]** を展開し、仮想 IP アドレスとして設定されているものと同じサブネットを使用して、**[Create Subnets]** ダイアログボックスの **[Gateway IP]** フィールドで物理 IP アドレスを作成します。

（注） 物理 IP アドレスは ACI ファブリック全体で一意である必要があります

ステップ 5 適切な手順を完了し、完了をクリックして完了します。

ステップ 6 **[Work]** ペインで作成した**Bridge Domain** をダブルクリックし、次の操作を実行します。

a) [L3 Configurations] タブで、**[Virtual MAC Address]** フィールドをクリックし、**[not-applicable]** を適切な値に変更します。**[Submit]** をクリックします。

（注） デフォルト BD の MAC アドレス値はすべての ACI ファブリックで同じです。この設定では、ブリッジ ドメイン MAC 値が各 ACI ファブリックで一意である必要があります。

各ファブリックのブリッジ ドメイン MAC (pmac) 値が一意であることを確認してください。

ステップ 7 BD を別のファブリックに拡張するために L2Out EPG を作成するには、ナビゲーションペインで **[External Bridged Networks]** を右クリックし、**[Create Bridged Outside]** ダイアログボックスを開き、次の操作を実行します。

a) **[Name]** フィールドに、ブリッジされる Outside の名前を入力します。

b) **[Bridge Domain]** フィールドで、すでに作成されているブリッジ ドメインを選択します。

c) **[Encap]** フィールドに、その他のファブリック l2out カプセル化に一致する VLAN カプセル化を入力します。

d) **[Path Type]** フィールドで、**[Port]**、**[PC]**、または **[VPC]** を選択して EPG を導入し、**[Next]** をクリックします。

e) 外部 EPG ネットワークを作成するには、**[Name]** フィールドをクリックしてネットワークの名前を入力し (QoS クラスの指定も可能) 、**[Finish]** をクリックして共通パーベイシブ設定を完了します。

NX-OS スタイルの CLI を使用した共通パーベイシブ ゲートウェイの設定

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ること。

手順

共通パーベイシブ ゲートウェイを設定します。

例：

```
apic1#configure
apic1(config)#tenant demo
apic1(config-tenant)#bridge-domain test
apic1(config-tenant-bd)#l2-unknown-unicast flood
apic1(config-tenant-bd)#arp flooding
apic1(config-tenant-bd)#exit

apic1(config-tenant)#interface bridge-domain test
apic1(config-tenant-interface)#multi-site-mac-address 12:34:56:78:9a:bc
apic1(config-tenant-interface)#mac-address 00:CC:CC:CC:C1:01 (Should be unique for each
 ACI fabric)
apic1(config-tenant-interface)#ip address 192.168.10.1/24 multi-site
apic1(config-tenant-interface)#ip address 192.168.10.254/24 (Should be unique for each
ACI fabric)
```

REST API を使用した共通パーベイシブ ゲートウェイの設定

始める前に

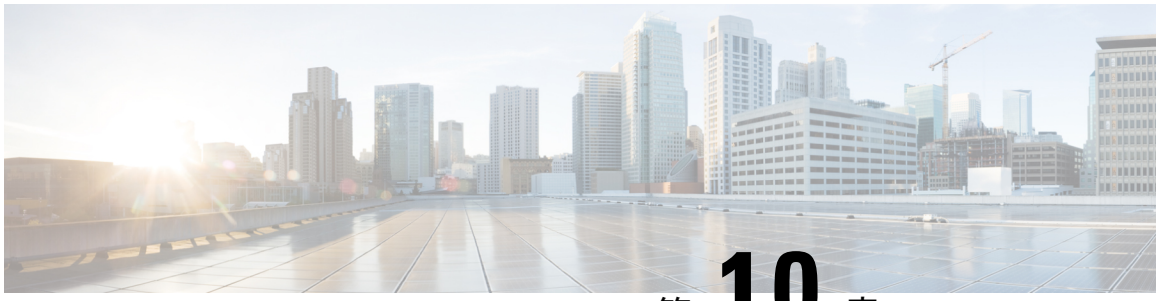
- テナント、VRF、およびブリッジ ドメインが作成されていること。

手順

共通パーベイシブ ゲートウェイを設定します。

例：

```
<!-Things that are bolded only matters-->
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/policymgr/mo/.xml -->
<polUni>
  <fvTenant name="test">
    <fvCtx name="test"/>

    <fvBD name="test" vmac="12:34:56:78:9a:bc">
      <fvRsCtx tnFvCtxName="test"/>
      <!-- Primary address -->
      <fvSubnet ip="192.168.15.254/24" preferred="yes"/>
      <!-- Virtual address -->
      <fvSubnet ip="192.168.15.1/24" virtual="yes"/>
    </fvBD>

    <fvAp name="test">
      <fvAEPg name="web">
        <fvRsBd tnFvBDName="test"/>
        <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/3]" encap="vlan-1002"/>
      </fvAEPg>
    </fvAp>
  </fvTenant>
</polUni>
```



第 10 章

スタティック ルート ブリッジ ドメイン

この章の内容は、次のとおりです。

スタティック ルート ブリッジ ドメインについて

Cisco APIC リリース 3.x では、ファイアウォールの背後にある仮想サービスへのルーティングを可能にする、パーベイシブ ブリッジ ドメイン (BD) でのスタティック ルート設定へのサポートが追加されました。

この機能は、通常の EPG の使用を通して、エンドポイント (EP) がパーベイシブ BD に直接には接続されていない IP アドレスへ到達することを可能にします。

スタティック ルートを設定すると、APIC は、それを BD を使用しているすべてのリーフ スイッチ、およびその BD に関連付けられた契約を有しているすべてのリーフ スイッチに展開します。

サブネット マスクは、1 つの IP アドレスまたは 1 つのエンドポイントをポイントしている /32 (IPv6 の場合は /128) である必要があります。これは、パーベイシブ BD に関連付けられている EPG に含まれます。

この機能は、名前の末尾が EX である Cisco Nexus 9000 シリーズ スイッチとそれ以降の機種によりサポートされています (たとえば N9K-C93180LC-EX)。

EP の到達可能性は、APIC GUI、NX-OS スタイル CLI および REST API を使用して設定できます。

GUI を使用してブリッジ ドメインでのスタティック ルートを設定する

- スタティック ルートのサブネットを作成するには、epg (fvAEPg で fvSubnet オブジェクト)、普及 BD (fvBD) 自体 BD しないに関連付けられているように構成されます。
- サブネットマスクが/32 にする必要があります (128/for IPv6) 1 つの IP アドレスまたは 1 つのエンドポイントをポイントします。これは、EPG に関連付けられている普及 BD で含まれています。

始める前に

テナント、VRF、BD、および EPG が作成されます。

手順

ステップ 1 メニュー バーで、**Tenants** > ***tenant-name*** の順にクリックします。
ステップ 2 ナビゲーション ウィンドウで **Application Profiles** を展開し、アプリケーション プロファイル名をクリックします。
ステップ 3 **Application EPGs** をクリックして、スタティック ルートの EPG を展開します。
ステップ 4 **Subnets** を展開して、スタティック ルートのサブネットを右クリックし、**Create Endpoints Behind EPG Subnet** を選択します。
ステップ 5 エンドポイントの **NextHop IP Address** を入力して、**Update** をクリックします。
ステップ 6 [送信（Submit）] をクリックします。

NX-OS スタイル CLI を使用したブリッジ ドメイン上のスタティック ルートの設定

パーベイシブ ブリッジ ドメイン (BD) でスタティック ルートを設定するには、NX-OS スタイルの次の CLI コマンドを使用します:

始める前に

テナント、VRF、BD および EPG が設定されています。

- スタティック ルートのサブネットを作成するには、epg (fvAEPg で fvSubnet オブジェクト)、普及 BD (fvBD) 自体 BD しないに関連付けられているように構成されます。

- サブネットマスクが/32 にする必要があります (128/for IPv6) 1 つの IP アドレスまたは 1 つのエンドポイントをポイントします。これは、EPG に関連付けられている普及 BD で含まれています。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	コンフィギュレーション モードに入ります。
ステップ 2	**tenant** *tenant-name* 例： `apic1(config)# tenant t1`	テナントを作成するか、テナント設定モードに入ります。
ステップ 3	**application** *ap-name* 例： `apic1(config-tenant)# application ap1`	アプリケーション プロファイルを作成するか、アプリケーション プロファイル モードに入ります。
ステップ 4	**epg** *epg-name* 例： `apic1(config-tenant-app)# epg ep1` <> <A.B.C.D> [scope <scope>]	EPG を作成するか、EPG 設定モードに入ります。
ステップ 5	**endpoint ip***A.B.C.D/LEN* **next-hop** *A.B.C.D* [scope *scope*] 例： `apic1(config-tenant-app-epg)# endpoint ip 125.12.1.1/32 next-hop 26.0.14.101`	EPG の背後にエンドポイントを作成します。サブネットマスクは /32 で (IPv6 の場合は /128)、1 つの IP アドレスまたは1つのエンドポイントをポイントしている必要があります。

例

次の例は、EPG の背後にあるエンドポイントを設定するコマンドを示しています。

```
apic1# config
      apic1(config)# tenant t1
      apic1(config-tenant)# application ap1
      apic1(config-tenant-app)# epg ep1
      apic1(config-tenant-app-epg)# endpoint ip 125.12.1.1/32 next-hop 26.0.14.101
```

REST API を使用してブリッジ ドメインでのスタティック ルートの設定

- スタティック ルートのサブネットを作成するには、epg (fvAEPg で fvSubnet オブジェクト)、普及 BD (fvBD) 自体 BD しないに関連付けられているように構成されます。
- サブネットマスクが/32 にする必要があります (128/for IPv6) 1 つの IP アドレスまたは 1 つのエンドポイントをポイントします。これは、EPG に関連付けられている普及 BD で含まれています。

始める前に

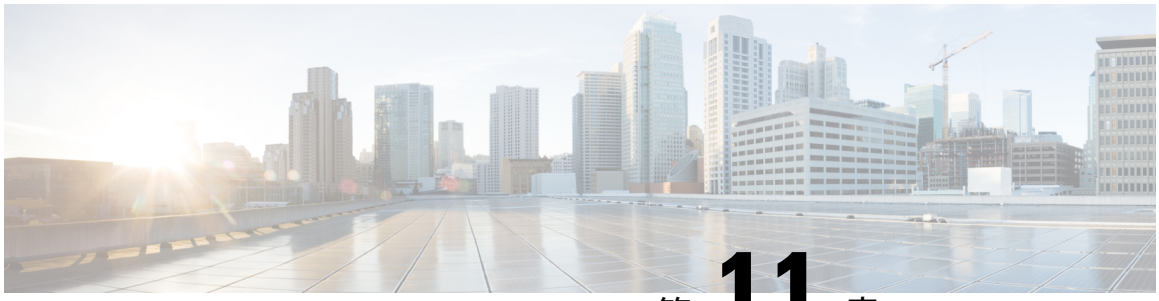
テナント、VRF、BD、および EPG が作成されています。

手順

普及ゲートウェイで使用される BD のスタティック ルートを設定するには、次の例など post を入力します。

例：

```
       <fvAEPg name="ep1">
    <fvRsBd tnFvBDName="bd1"/>
          <fvSubnet ip="2002:0db8:85a3:0000:0000:8a2e:0370:7344/128"
ctrl="no-default-gateway"   >
              <fvEpReachability>
                  <ipNexthopEpP  nhAddr="2001:0db8:85a3:0000:0000:8a2e:0370:7343/128"
/>
              </fvEpReachability>
          </fvSubnet>
       </fvAEPg>
```



第 11 章

MP-BGP ルート リフレクタ

この章の内容は、次のとおりです。

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。

表 *18 : 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>**

GUI を使用した MP-BGP ルート リフレクタの設定

手順

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

ステップ 2 **Navigation** ウィンドウで、**BGP Route Reflector** を右クリックして、**Create Route Reflector Node Policy EP** をクリックします。

ステップ 3 [Create Route Reflector Node Policy EP] ダイアログボックスで、[Spine Node] ドロップダウン リストから、適切なスパイン ノードを選択します。**Submit** をクリックします。

（注） 必要に応じてスパイン ノードを追加するには、上記の手順を繰り返してください。

スパイン スイッチがルート リフレクタ ノードとしてマークされます。

ステップ 4 **BGP Route Reflector** プロパティ エリアの **Autonomous System Number** フィールドで、適切な番号を選択します。**Submit** をクリックします。

（注） 自律システム番号は、Border Gateway Protocol（BGP）がルータに設定されている場合は、リーフが接続されたルータ設定に一致する必要があります。スタティックまたは Open Shortest Path First（OSPF）を使用して学習されたルートを使用している場合は、自律システム番号値を任意の有効な値にできます。

ステップ 5 メニュー バーで、**Fabric** > **Fabric Policies** > **POD Policies** をクリックします。

ステップ 6 [Navigation] ペインで、[Policy Groups] を展開して右クリックし、[Create POD Policy Group] をクリックします。

ステップ 7 [Create POD Policy Group] ダイアログボックスで、[Name] フィールドに、ポッド ポリシー グループの名前を入力します。

ステップ 8 [BGP Route Reflector Policy] ドロップダウン リストで、適切なポリシー（デフォルト）を選択します。[Submit] をクリックします。`
BGP ルート リフレクタのポリシーは、ルート リフレクタのポッド ポリシー グループに関連付けられ、BGP プロセスはリーフ スイッチでイネーブルになります。

ステップ 9 [Navigation] ペインで、**[Pod Policies]** > **[Profiles]** > **[default]** の順に選択します。[Work] ペインで、[Fabric Policy Group] ドロップダウン リストから、前に作成されたポッド ポリシーを選択します。[Submit] をクリックします。`
ポッド ポリシー グループが、ファブリック ポリシー グループに適用されました。

ACI ファブリックの MP-BGP ルート リフレクタの設定

ACI ファブリック内のルートを配布するために、MP-BGP プロセスを最初に実行し、スパイン スイッチを BGP ルート リフレクタとして設定する必要があります。

次に、MP-BGP ルート リフレクタの設定例を示します。

（注） この例では、BGP ファブリック ASN は 100 です。スパイン スイッチ 104 と 105 が MP-BGP ルート リフレクタとして選択されます。

```
apic1(config)# bgp-fabric
apic1(config-bgp-fabric)# asn 100
apic1(config-bgp-fabric)# route-reflector spine 104,105
```

REST API を使用した MP-BGP ルート リフレクタの設定

手順

ステップ 1 スパイン スイッチをルート リフレクタとしてマークします。

例：

```
POST https://apic-ip-address/api/policymgr/mo/uni/fabric.xml

<bgpInstPol name="default">
  <bgpAsP asn="1" />
  <bgpRRP>
     <bgpRRNodePEp id="<spine_id1>"/>
     <bgpRRNodePEp id="<spine_id2>"/>
  </bgpRRP>
</bgpInstPol>
```

ステップ 2 次のポストを使用してポッド セレクタをセットアップします。

例：

FuncP セットアップの場合：

```
POST https://apic-ip-address/api/policymgr/mo/uni.xml

<fabricFuncP>
  <fabricPodPGrp name="bgpRRPodGrp”>
    <fabricRsPodPGrpBGPRRP tnBgpInstPolName="default" />
  </fabricPodPGrp>
</fabricFuncP>
```

例：

PodP セットアップの場合：

```
POST https://apic-ip-address/api/policymgr/mo/uni.xml

<fabricPodP name="default">
  <fabricPodS name="default" type="ALL">
    <fabricRsPodPGrp tDn="uni/fabric/funcprof/podpgrp-bgpRRPodGrp"/>
  </fabricPodS>
</fabricPodP>
```

MP-BGP ルート リフレクタ設定の確認

手順

ステップ 1 次の操作を実行して、設定を確認します。

a) セキュア シェル（SSH）を使用して、必要に応じて各リーフ スイッチへの管理者としてログインします。

b) show processes | grep bgp コマンドを入力して、状態が S であることを確認します。

状態が NR（実行していない）である場合は、設定が正常に行われませんでした。

ステップ 2 次の操作を実行して、自律システム番号がスパイン スイッチで設定されていることを確認します。

a) SSH を使用して、必要に応じて各スパイン スイッチへの管理者としてログインします。

b) シェル ウィンドウから次のコマンドを実行します。

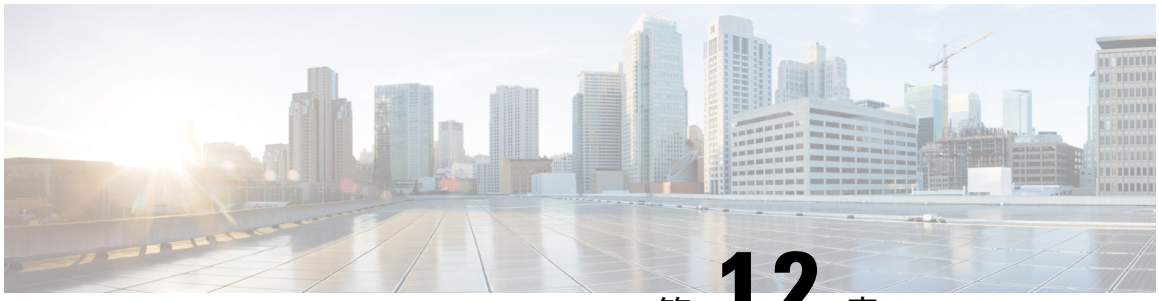
例：

cd /mit/sys/bgp/inst

例：

grep asn summary

設定した自律システム番号が表示される必要があります。自律システム番号の値が 0 と表示される場合は、設定が正常に行われませんでした。



第 12 章

スイッチ仮想インターフェイス

この章の内容は、次のとおりです。

SVI 外部カプセル化の範囲

SVI 外部カプセル化の範囲について

レイヤ 3 アウト設定のコンテキストでは、スイッチ仮想インターフェイス（SVI）は ACI リーフ スイッチとルータ間に接続性を提供するように設定されます。

デフォルトで単一のレイヤ 3 アウトが SVI インターフェイスで設定されている場合、VLAN のカプセル化はファブリック内の複数のノードに範囲が及びます。これは、図で示されるように SVI インターフェイスが同じ外部カプセル化（SVI）を使用する限り、レイヤ 3 アウト SVI が展開されているファブリックで、ACI ファブリックがすべてのノード上に同じブリッジ ドメイン（VXLAN VN）を設定するため発生します。

ただし、異なるレイヤ 3 アウトが展開されている場合、同じ外部カプセル化 (SVI) を使用している場合でも ACI ファブリックは異なるブリッジ ドメインを使用します。

図 *17 :* ローカル範囲のカプセル化と *1* 個のレイヤ *3* アウト

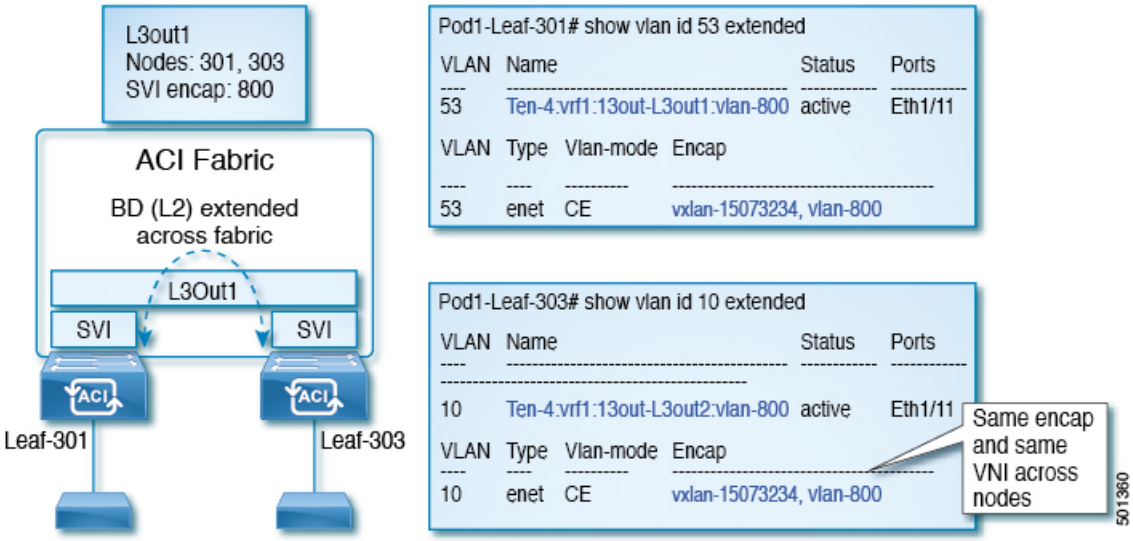
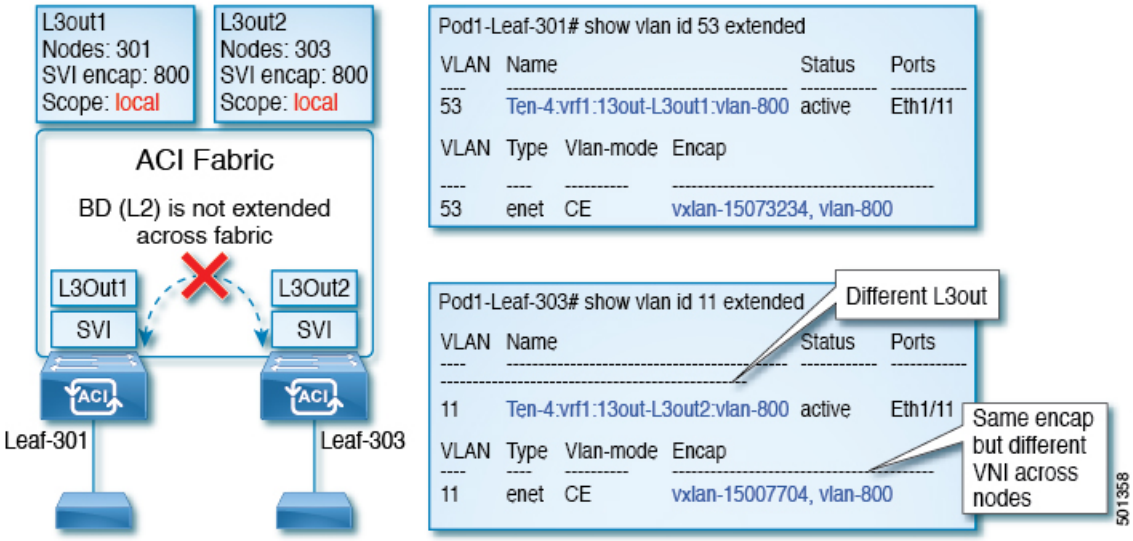


図 *18 :* ローカル範囲のカプセル化と *2* 個のレイヤ *3* アウト

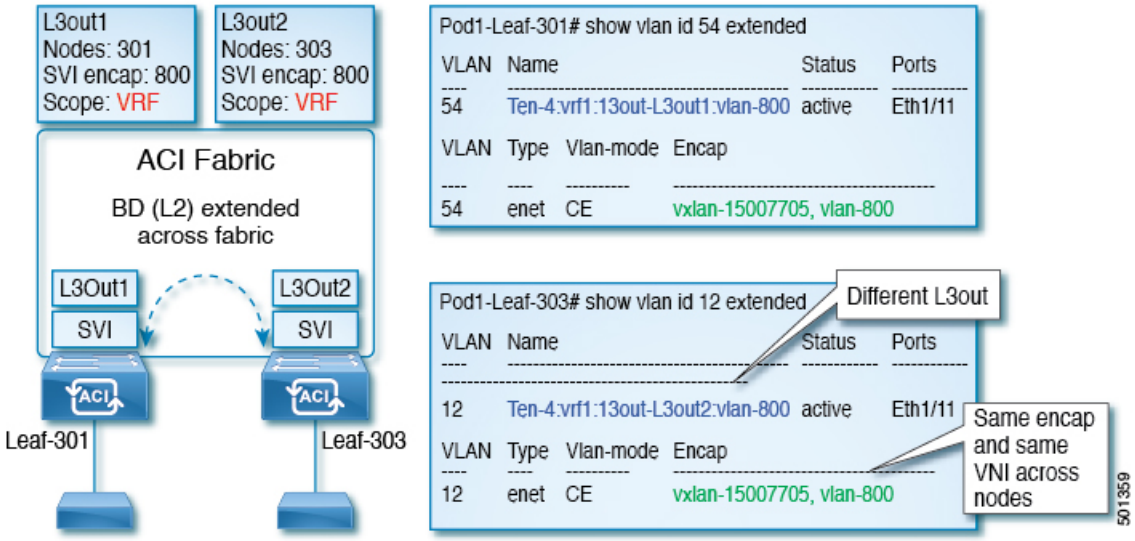


Cisco APIC リリース 2.3 以降、同じ外部カプセル化（SVI）を使用して、2 個以上のレイヤ 3 アウトを展開する場合の動作を選択できるようになりました。

カプセル化の範囲は、ローカルまたは VRF として設定できます。

- ローカル範囲（デフォルト）：例の動作が「ローカル範囲のカプセル化および *2* 個のレイヤ *3* アウト」というタイトルの図に表示されます。
- VRF 範囲：ACI ファブリックが、同じ外部カプセル化（SVI）が展開されているすべてのノードとレイヤ 3 アウト上で同じブリッジドメイン（VXLAN VNI）を設定します。「*VRF* 範囲のカプセル化および *2* 個のレイヤ *3* アウト」というタイトルの図の例を参照してください。

図 *19 : VRF* 範囲のカプセル化および *2* 個のレイヤ *3* アウト



カプセル化スコープ構文

レイヤ 3 Out プロファイルで使用されるカプセル化の範囲を設定するためのオプションは次のとおりです。

- **Ctx**]: 特定の VLAN のカプセル化の同じ VRF に、すべてのレイヤ 3 が記録されるで同じ外部 SVI。これはグローバル値です。
- **ローカル** : レイヤ 3 Out ごとの一意の外部 SVI。これはデフォルト値です。

CLI、API、および GUI 構文間のマッピングは次のとおりです。

表 *19 :* カプセル化スコープ構文

CLI	API	GUI
l3out	local	local
vrf	ctx	VRF

（注） カプセル化の範囲を設定する CLI コマンドでは、名前付きのレイヤ 3 アウト設定、VRF が設定されている場合にのみサポートされます。

SVI 外部カプセル化の範囲のガイドライン

SVI 外部カプセル化の範囲を使用する際には、次のガイドラインに従ってください:

- 同じノード上にレイヤ 3 Out を設定するためには、両方のレイヤ 3 Out の OSPF エリアが異なっている必要があります。
- 同じノード上にレイヤ 3 Out を設定するためには、両方のレイヤ 3 Out の BGP ピア設定が異なる必要があります。

GUI を使用して SVI 外部カプセル化の範囲の設定

始める前に

- テナントと VRF が設定されています。
- レイヤ 3 アウトが設定されているし、レイヤ 3 Out で論理ノードプロファイルが設定されています。

手順

ステップ 1 メニュー バーで、 > **Tenants** > **Tenant_name** をクリックします。**Navigation** ペインで、**Networking** > **External Routed Networks** > **External Routed Network_name** > **Logical Node Profiles** > **Logical Interface Profile** をクリックします。

ステップ 2 **Navigation** ウィンドウで、**Logical Interface Profile** を右クリックし、**Create Interface Profile** をクリックします。

ステップ 3 [Create Interface Profile] ダイアログボックスで、次の操作を実行します。

a) **Step 1 Identity** 画面の **Name** フィールドで、インターフェイス プロファイルの名前を入力します。

b) 残りのフィールドに、適切なオプションを選択し] をクリックして **次** 。

c) **ステップ 2 プロトコル プロファイル** 画面、目的のプロトコルを選択するには、プロファイルの詳細、および] をクリックして **次** 。

d) **ステップ 3 インターフェイス** 画面で、をクリックして、 **SVI**] タブをクリックして、 + を開くにアイコン、 **選択 SVI** ダイアログボックス。

e) **インターフェイスの指定**] 領域で、目的、さまざまなフィールド値を選択します。

f) **Encap スコープ** フィールドで、目的のカプセル化範囲の値を選択します。[OK] をクリックします。

デフォルト値は **Local** です。

SVI 外部のカプセル化の範囲は、指定されたインターフェイスで設定されます。

NX-OS スタイル CLI を使用して、SVI インターフェイスのカプセル化スコープの設定

SVIインターフェイス カプセル化のスコープ設定を次の例表示する手順では、名前付きのレイヤ 3 アウト設定です。

手順

	コマンドまたはアクション	目的
ステップ 1	コンフィギュレーション モードを開始します。 **例：** `apic1# configure`	コンフィギュレーション モードを開始します。
ステップ 2	スイッチ モードを開始します。 **例：** `apic1(config)# leaf 104`	スイッチ モードを開始します。
ステップ 3	VLANインターフェイスを作成します。 **例：** `apic1(config-leaf)# interface vlan 2001`	VLANインターフェイスを作成します。VLAN の範囲は 1 ～ 4094 です。
ステップ 4	カプセル化の範囲を指定します。 **例：** `apic1(config-leaf-if)# encap scope vrf context`	カプセル化の範囲を指定します。
ステップ 5	インターフェイスモードを終了します。 **例：** `apic1(config-leaf-if)# exit`	インターフェイスモードを終了します。

REST API を使用して、SVI インターフェイスのカプセル化スコープの設定

始める前に

インターフェイス セレクタが設定されます。

手順

SVI インターフェイスのカプセル化の範囲を設定します。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- /api/node/mo/.xml -->
<polUni>
 <fvTenant name="coke">
  <l3extOut descr="" dn="uni/tn-coke/out-l3out1" enforceRtctrl="export" name="l3out1"
nameAlias="" ownerKey="" ownerTag="" targetDscp="unspecified">
   <l3extRsL3DomAtt tDn="uni/l3dom-Dom1"/>
   <l3extRsEctx tnFvCtxName="vrf0"/>
   <l3extLNodeP configIssues="" descr="" name="__ui_node_101" nameAlias="" ownerKey=""
ownerTag="" tag="yellow-green" targetDscp="unspecified">
    <l3extRsNodeL3OutAtt rtrId="1.1.1.1" rtrIdLoopBack="no" tDn="topology/pod-1/node-101"/>

    <l3extLIfP descr="" name="int1_11" nameAlias="" ownerKey="" ownerTag=""
tag="yellow-green">
     <l3extRsPathL3OutAtt addr="1.2.3.4/24" descr="" encap="vlan-2001" encapScope="ctx"
 ifInstT="ext-svi" llAddr="0.0.0.0" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
 tDn="topology/pod-1/paths-101/pathep-[eth1/5]" targetDscp="unspecified"/>
     <l3extRsNdIfPol tnNdIfPolName=""/>
     <l3extRsIngressQosDppPol tnQosDppPolName=""/>
     <l3extRsEgressQosDppPol tnQosDppPolName=""/>
    </l3extLIfP>
   </l3extLNodeP>
  <l3extInstP descr="" matchT="AtleastOne" name="epg1" nameAlias="" prefGrMemb="exclude"
 prio="unspecified" targetDscp="unspecified">
    <l3extSubnet aggregate="" descr="" ip="101.10.10.1/24" name="" nameAlias=""
scope="import-security"/>
    <fvRsCustQosPol tnQosCustomPolName=""/>
   </l3extInstP>
  </l3extOut>
 </fvTenant>
</polUni>
```

SVI 自動状態

SVI 自動状態について

（注） この機能は、APIC リリース 2.2(3x) リリースおよび APIC リリース 3.1 (1) で使用できます。APIC リリース 3.0(x) ではサポートされていません。

スイッチ仮想インターフェイス（SVI）は、デバイスの VLAN のブリッジング機能とルーティング機能間の論理インターフェイスを表します。SVIは、物理ポート、直接ポートチャネル、仮想ポートチャネルのメンバーを有することができます。SVI論理インターフェイスはVLANに関連付けられ、VLAN ポート メンバーシップを有します。

SVI の状態はメンバーに依存しません。Cisco APIC の SVI のデフォルトの自動状態動作は、自動状態の値が無効になっているときに最新の状態になっていることを意味します。これは、イ

ンターフェイスが対応するVLANで動作していない場合、SVIがアクティブであることを意味します。

SVI 自動状態の値を有効に変更する場合、関連する VLAN のポート メンバーに依存します。VLANインターフェイスがVLANで複数のポートを有する場合、SVIはVLANのすべてのポートがダウンするとダウン状態になります。

表 *20 : SVI* 自動状態

SVI 自動状態	SVI 状態の説明
ディセーブル	インターフェイスが対応する VLAN で動作していない場合、SVI がアップ状態であることを意味します。 無効がデフォルトの SVI 自動状態の値です。
イネーブル	SVI は、関連付けられている VLAN のポート メンバによって異なります。VLAN インターフェイスに複数のポートを含む場合、SVIはVLANのすべてのポートがダウンするとダウン状態になります。

SVI 自動状態の動作のガイドラインと制限事項

次のガイドラインをお読みください。

- SVI の自動状態の動作を有効化または無効化にすると、SVI あたりの自動状態の動作を設定します。これらはグローバル コマンドではありません。

GUI を使用した SVI 自動状態の設定

始める前に

- テナントと VRF が設定されています。
- レイヤ3アウトが設定されており、レイヤ3アウトの論理ノードプロファイルと論理インターフェイス プロファイルが設定されています。

手順

ステップ 1 メニュー バーで、 > **Tenants** > **Tenant_name** をクリックします。**Navigation** ペインで、**Networking** > **External Routed Networks** > **External Routed Network_name** > **Logical Node Profiles** > **Logical Interface Profile** をクリックします。

ステップ 2 **Navigation** ウィンドウで、**Logical Interface Profile** を展開し、適切な論理インターフェイス プロファイルをクリックします。

ステップ 3 作業ウィンドウで、+ 記号をクリックして **SVI** ダイアログボックスを表示します。

ステップ 4 付加的な SVI を追加するには、 **SVI** ダイアログボックスで、以下の手順を実行します:

a) **Path Type** フィールドで、適切なパス タイプを選択します。
b) **Path** フィールドで、ドロップダウンリストから適切な物理インターフェイスを選択します。
c) **Encap** フィールドで、適切な値を選択します。
d) **Auto State** フィールド **(Work** ウィンドウ**)** で SVI を選択し、自動状態を表示または変更します。

デフォルト値は **Disabled** です。

（注） 既存 SVI の自動状態の値を確認または変更するには、適切な SVI を選択して、値を確認または変更します。

NX-OS スタイル CLI を使用した SVI 自動状態の設定

始める前に

- テナントおよび VRF が設定されています。
- レイヤ 3 アウトが設定されており、レイヤ 3 アウトの論理ノードプロファイルと論理インターフェイス プロファイルが設定されています。

手順

	コマンドまたはアクション	目的
ステップ 1	コンフィギュレーション モードを開始します。 **例：** `apic1# configure`	コンフィギュレーション モードを開始します。
ステップ 2	スイッチ モードを開始します。 **例：** `apic1(config)# leaf 104`	スイッチ モードを開始します。
ステップ 3	VLANインターフェイスを作成します。 **例：** `apic1(config-leaf)# interface vlan 2001`	VLANインターフェイスを作成します。VLAN の範囲は 1 ～ 4094 です。
ステップ 4	SVI 自動状態を有効にします。 **例：** `apic1(config-leaf-if)# autostate`	SVI 自動状態を有効にします。 デフォルトで、SVI 自動状態の値は有効ではありません。

	コマンドまたはアクション	目的
ステップ 5	インターフェイスモードを終了します。 例： `apic1(config-leaf-if)# exit`	インターフェイスモードを終了します。

REST API を使用した SVI 自動状態の設定

始める前に

- テナントと VRF が設定されています。
- レイヤ 3 アウトが設定されており、レイヤ 3 アウトの論理ノードプロファイルと論理インターフェイス プロファイルが設定されています。

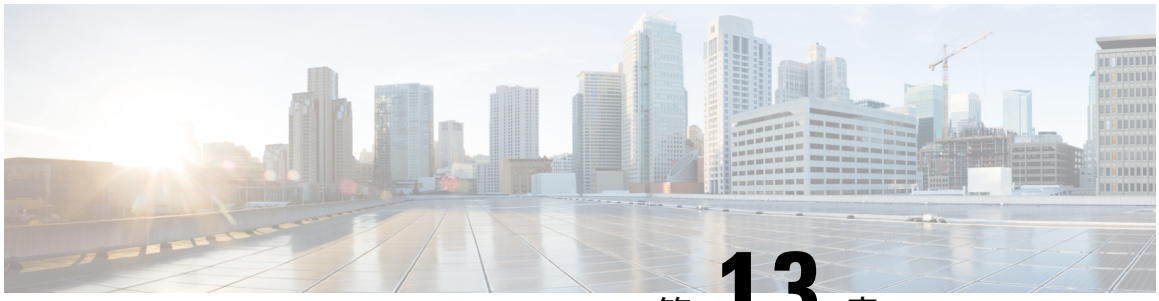
手順

SVI の自動状態の値を有効にします。

例：

```
<fvTenant name="t1" >
   <l3extOut name="out1">
      <l3extLNodeP name="__ui_node_101" >
         <l3extLIfP descr="" name="__ui_eth1_10_vlan_99_af_ipv4" >
            <l3extRsPathL3OutAtt addr="19.1.1.1/24" autostate="enabled" descr=""
encap="vlan-100" encapScope="local" ifInstT="ext-svi" llAddr="::" mac="00:22:BD:F8:19:FF"
 mode="regular" mtu="inherit" tDn="topology/pod-1/paths-101/pathep-[eth1/10]"
targetDscp="unspecified" />
         </l3extLIfP>
      </l3extLNodeP>
   </l3extOut>
</fvTenant>
```

自動状態を無効にするには、上記の例では無効に値を変更する必要があります。例：`autostate="disabled"`。



第 13 章

共有サービス

この章の内容は、次のとおりです。

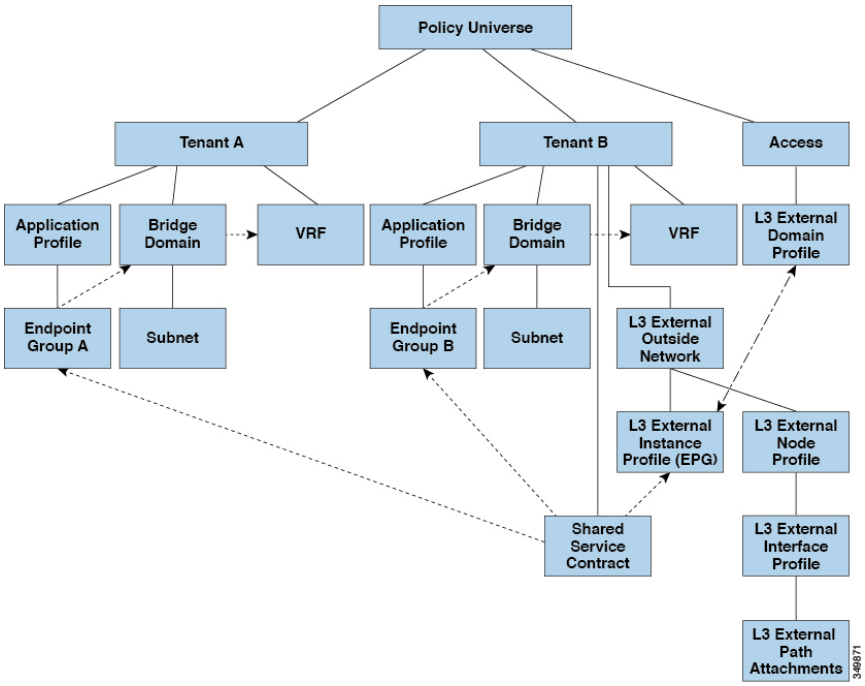
共有レイヤ 3 Out

共有レイヤ 3 アウトサイド ネットワーク(L3extOut)は、外部ネットワークへのルーテッド接続を共有サービスとして提供します。L3extOut プロファイル（l3extInstP)）EPG は、外部ネットワークへのルーテッド接続を提供します。これは、任意のテナント（*user*、common、infra、mgmt.）の共有サービスとしてプロビジョニングできます。リリース 1.2(1x) より前では、この設定は *user* テナントと common テナントでのみサポートされていました。任意のテナントの EPG が、l3extInstP EPG がファブリック内のどこにプロビジョニングされているかには関係なく、共有サービス コントラクトを使用してその l3extInstP EPG に接続できます。これにより、外部ネットワークへのルーテッド接続のプロビジョニングが簡単になります。複数のテナントが、外部ネットワークへのルーテッド接続用に単一の l3extInstP EPG を共有できます。l3extInstP EPG を共有すると、単一の共有 l3extInstP EPG を使用する EPG の数には関係なくスイッチ上で使用されるセッションは 1 つのみであるため、より効率的になります。

（注） l3extInstP EPG 共有サービス コントラクトを使用するすべてのスイッチは、APIC 1.2（1x）およびスイッチ 11.2（1x）の各リリース以降で使用可能なハードウェアおよびソフトウェアのサポートを必要とします。詳細については、「*Cisco APIC Management, Installation, Upgrade, and Downgrade Guide*」 とリリース ノート ドキュメントを参照してください。

次の図は、共有 l3extInstP EPG 用に設定された主なポリシー モデル オブジェクトを示しています。

図 *20 :* 共有レイヤ *3 Out* ポリシー モデル



共有レイヤ3アウトサイドネットワーク設定については、以下の注意事項と制限事項に注意してください。

- テナント制限なし：テナント A と B は、任意の種類のテナント（*user*、`common`、`infra`、`mgmt`）です。共有 `l3extInstP` EPG が `common` テナントにある必要はありません。
- EPG の柔軟な配置：上の図の EPG A と EPG B は異なるテナントにあります。EPG A と EPG B で同じブリッジ ドメインと VRF を使用することはできますが、それは必須ではありません。EPG A と EPG B は異なるブリッジ ドメインおよび異なる VRF にありますが、同じ `l3extInstP` EPG を共有しています。
- サブネットは、*private*、*public*、または *shared* です。`L3extOut` のコンシューマまたはプロバイダ EPG にアドバタイズされるサブネットは、*shared* に設定されている必要があります。`L3extOut` にエクスポートされるサブネットは *public* に設定される必要があります。
- 共有サービス コントラクトは、共有レイヤ 3 アウトサイド ネットワーク サービスを提供する `l3extInstP` EPG が含まれているテナントからエクスポートされます。共有サービス コントラクトは、共有サービスを使用する EPG が含まれているテナントにインポートされます。
- 共有 L3 Out では禁止コントラクトを使用しないでください。この設定はサポートされません。
- `l3extInstP` は共有サービス プロバイダとしてサポートされますが、l3extInstP 以外のコンシューマのみに限定されます（`L3extOut` EPG = `l3extInstP` である場合）。

- トラフィック中断（フラップ）：l3instP EPG が、l3instP サブセットのスコープ プロパティを共有ルート制御（*shared-rctrl*）または共有セキュリティ（*shared-security*）に設定して外部サブネット 0.0.0.0/0 を使用して設定されると、VRF はグローバル pcTag を使用して再配置されます。これにより、その VRF 内のすべての外部トラフィックが中断されます（VRF がグローバル pcTag を使用して再配置されるため）。

- 共有レイヤ L3extOut のプレフィックスは一意である必要があります。同じコンテキスト（VRF）の同じプレフィックスを使用した、複数の共有 L3extOut 設定は動作しません。VRF にアドバタイズする外部サブネット（外部プレフィックス）が一意であることを確認してください（同じ外部サブネットが複数の l3instP に属することはできません）。プレフィックス prefix1 を使用した L3extOut 設定（たとえば、L3Out1）と、同様にプレフィックス prefix1 を使用した 2 番目のレイヤ 3 アウトサイド設定（たとえば、L3Out2）が同じ VRF に属すると、動作しません（導入される pcTag は 1 つのみであるため）。L3extOut のさまざまな動作は、同じ VRF の同じリーフ スイッチに設定されている可能性があります。考えられるシナリオは次の 2 つです。

  - シナリオ 1 には、SVI インターフェイスおよび 2 個のサブネット（10.10.10.0/24 および 0.0.0.0/0）が定義された.L3extOut があります。レイヤ 3 アウトサイド ネットワークの入力トラフィックに一致するプレフィックス 10.10.10.0/24 がある場合、入力トラフィックは外部 EPG pcTag を使用します。レイヤ 3 アウトサイド ネットワーク上の入力トラフィックに一致するデフォルト プレフィックス 0.0.0.0/0 がある場合、入力トラフィックは外部ブリッジ pcTag を使用します。

  - シナリオ 2 には、2 個のサブネット（10.10.10.0/24 および 0.0.0.0/0）が定義されたルーテッドまたは routed-sub-interface を使用する L3extOut があります。レイヤ 3 アウトサイド ネットワークの入力トラフィックに一致するプレフィックス 10.10.10.0/24 がある場合、入力トラフィックは外部 EPG pcTag を使用します。レイヤ 3 アウトサイド ネットワーク上の入力トラフィックに一致するデフォルト プレフィックス 0.0.0.0/0 がある場合、入力トラフィックは VRF pcTag を使用します。

  - これらの説明した動作の結果として、SVI インターフェイスを使用して L3extOut-A および L3extOut-B で同じ VRF および同じリーフ スイッチが設定されている場合、次のユース ケースが考えられます。

    ケース 1 は L3extOut -A 用です。この外部ネットワーク EPG には 2 個のサブネットが定義されています。 10.10.10.0/24 & 0.0.0.0/1。L3extOut-A の入力トラフィックに一致するプレフィックス 10.10.10.0/24 がある場合、L3extOut-A に関連付けられている外部 EPG pcTag & コントラクトを使用します。L3extOut-A の出力トラフィックに特定の一致がなく、最大のプレフィックス一致が 0.0.0.0/1 の場合、外部ブリッジ ドメイン（BD）pcTag & コントラクト-A を使用します。

    ケース 2 は L3extOut-B です。 この外部ネットワーク EPG には定義された 1 個のサブネット: 0.0.0.0/0 があります。L3extOut-B の入力トラフィックに一致するプレフィックス 10.10.10.0/24 (L3extOut-A で定義）がある場合、L3extOut-A に関連付けられている L3extOut-A およびコントラクト A の外部 EPG pcTag を使用します。L3extOut-B に関連付けられているコントラクト-B は使用しません。

- 許可されないトラフィック：無効な設定で、共有ルート制御（shared-rtctrl）に対する外部サブネットのスコープが、共有セキュリティ（shared-security）に設定されているサブネットのサブセットとして設定されている場合、トラフィックは許可されません。たとえば、以下の設定は許可されません。
  - *shared rtctrl*：10.1.1.0/24, 10.1.2.0/24
  - *shared security*：10.1.0.0/16

  この場合、10.1.1.0/24 および 10.1.2.0/24 の各プレフィックスがドロップ ルールを使用してインストールされているため、宛先 IP 10.1.1.1 を使用して非境界リーフの入力トラフィックはドロップされます。トラフィックは許可されません。そのようなトラフィックは、`shared-rtctrl` プレフィックスを shared-security プレフィックスとしても使用するように設定を修正することで、有効にすることができます。
- 不注意によるトラフィック フロー：次の設定シナリオを避けることで、不注意によるトラフィック フローを予防します。
  - **ケース 1** 設定の詳細：
    - VRF1 を持つレイヤ 3 アウトサイド ネットワーク設定（たとえば、名前付き `L3extOut` -1）は provider1 と呼ばれます。
    - VRF2 を持つ二番目のレイヤ 3 アウトサイド ネットワーク設定（たとえば、名前付き `L3extOut`-2）は provider2 と呼ばれます。
    - `L3extOut` -1 VRF1 は、インターネット 0.0.0.0/0 にデフォルト ルートをアドバタイズし、これは *shared-rtctrl* および *shared-security* の両方を有効にします。
    - `L3extOut`-2 VRF2 は特定のサブネットを DNS および NTP 192.0.0.0/8 にアドバタイズし、*shared-rtctrl* を有効にします。
    - `L3extOut`-2 VRF2 に特定の 192.1.0.0/16 があり、*shared-security* を有効にします。
    - **バリエーション A**：EPG トラフィックが複数の VRF に向かいます。
      - EPG1 と `L3extOut`-1 の間の通信は *allow_all* コントラクトによって制御されます。
      - EPG1 と `L3extOut`-2 の間の通信は *allow_all* コントラクトによって制御されます。

        結果：EPG1 から `L3extOut`-2 へのトラフィックも 192.2.x.x に向かいます。
    - **バリエーション B**：EPG は 2 番目の共有レイヤ 3 アウトサイド ネットワーク の *allow_all* コントラクトに従います。
      - EPG1 と `L3extOut`-1 の間の通信は *allow_all* コントラクトによって制御されます。
      - EPG1 と `L3extOut`-2 の間の通信は *allow_icmp* コントラクトによって制御されます。

結果：EPG1 ～ `L3extOut`-2 から 192.2.x.x へのトラフィックは *allow_all* コントラクトに従います。

- **ケース 2** 設定の詳細：
  - `L3extOut` プロファイル（l3instP）は、1 つの共有プレフィックスとその他の非共有プレフィックスを持っています。
  - `src = non-shared` で到達するトラフィックは、EPG に向かうことが許可されます。
    - **バリエーション A**：意図しないトラフィックが EPG を通過します。

      `L3extOut`（l3instP）EPG のトラフィックがこれらのプレフィックスを持つ `L3extOut` に向かいます。

      - `192.0.0.0/8 = import-security, shared-rtctrl`

      - `192.1.0.0/16 = shared-security`

      - EPG には `1.1.0.0/16 = shared` があります

      結果：192.2.x.x からのトラフィックも EPG に向かいます。
    - **バリエーション B**：意図しないトラフィックが EPG を通過します。共有 `L3extOut` に到達したトラフィックは EPG を通過できます。

      -共有 `L3extOut` VRF には、`pcTag = prov vrf` を持つ EPG と *allow_all* に設定されているコントラクトがあります。

      - EPG は `<subnet> = shared` となっています。

      結果：レイヤ 3 Out に到達するトラフィックは EPG を通過することができます。

レイヤ 3 アウトからレイヤ 3 アウト内部 VRF への漏洩

Cisco APIC リリース 2.2(2e) から、2 つの異なる VRF に 2 個のレイヤ 3 アウトがある場合、VRF 内部の漏洩がサポートされています。

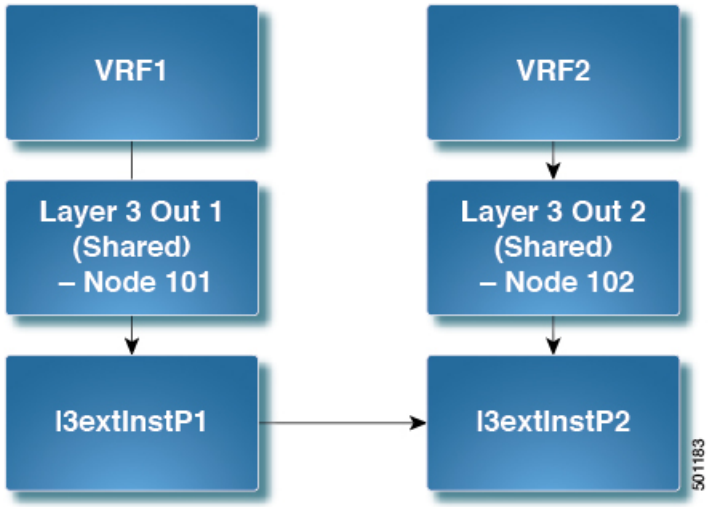
この機能を稼働するには、次の条件を満たす必要があります。

- 2 個のレイヤ 3 アウト間にはコントラクトが必要です。
- レイヤ 3 アウトの接続したり移行したりするサブネットのルートは、コントラクトを適用し（L3Out-L3Out および L3Out-EPG）、VRF 間の動的または静的ルートを漏洩させることなく漏洩します。
- 動的または静的ルートは、コントラクトを適用し（L3Out-L3Out および L3Out-EPG）、VRF 間で直接接続したり移行したりするルートをアドバタイズすることなく漏洩します。

- 異なる VRF の共有のレイヤ 3 アウトは相互に通信できます。
- 2 個のレイヤ 3 アウトは異なる 2 個の VRF に存在し、正常にルートを交換できます。
- この強化は、アプリケーション EPG およびレイヤ 3 アウト内部 VRF 間の通信と同じです。唯一の違いは、アプリケーション EPG ではなく別のレイヤ 3 アウトが存在します。したがってこの状況では、コントラクトは 2 個のレイヤ 3 アウト間で記録されます。

次の図では、共有サブネットによる 2 個のレイヤ 3 アウトが存在します。両方の VRF でレイヤ 3 外部インスタンス プロファイル（l3extInstP）間のコントラクトがあります。この場合、VRF 1 の共有レイヤ 3 アウト は VRF 2 の共有レイヤ 3 と通信できます。

図 *21 : 2* 個の *VRF* 間で通信する共有レイヤ *3* アウト



共有設定の 2 つのレイヤ REST API を使用して 2 つの Vrf に 3 が記録されます。

2 つの方法が表示されますが、2 つの Vrf にレイヤ 3 が記録されるを共有する次の REST API の設定例は次の通信します。

手順

ステップ 1 プロバイダー レイヤ 3 を設定します。

例：

```
<tenant name="t1_provider">
<fvCtx name="VRF1">
<l3extOut name="T0-o1-L3OUT-1">
                <l3extRsEctx tnFvCtxName="o1"/>
                <ospfExtP areaId='60'/>
                <l3extInstP name="l3extInstP-1">
                <fvRsProv tnVzBrCPName="vzBrCP-1">
                </fvRsProv>
```

```
                <l3extSubnet ip="192.168.2.0/24" scope="shared-rtctrl, shared-security"
 aggregate=""/>
                </l3extInstP>
</l3extOut>
</tenant>
```

ステップ 2 レイヤ 3 Out コンシューマを設定します。

例：

```
<tenant name="t1_consumer">
<fvCtx name="VRF2">
<l3extOut name="T0-o1-L3OUT-1">
                <l3extRsEctx tnFvCtxName="o1"/>
                <ospfExtP areaId='70'/>
                <l3extInstP name="l3extInstP-2">
                <fvRsCons tnVzBrCPName="vzBrCP-1">
                </fvRsCons>
                <l3extSubnet ip="199.16.2.0/24" scope="shared-rtctrl, shared-security"
         aggregate=""/>
                </l3extInstP>
</l3extOut>
</tenant>
```

NX-OS スタイル CLI を使用して共有 レイヤ 3 VRF 内リークを設定する - 名前が付けられた例

手順

	コマンドまたはアクション	目的
ステップ 1	コンフィギュレーション モードを開始します。 **例：** `apic1# configure`	

ステップ 2	プロバイダー レイヤ 3 を設定します。
	例：
	`apic1(config)# tenant t1_provider`
	`apic1(config-tenant)# external-l3 epg l3extInstP-1 l3out T0-o1-L3OUT-1`
	`apic1(config-tenant-l3ext-epg)# vrf member VRF1`
	`apic1(config-tenant-l3ext-epg)# match ip 192.168.2.0/24 shared`
	`apic1(config-tenant-l3ext-epg)# contract provider vzBrCP-1`
	`apic1(config-tenant-l3ext-epg)# exit`
	`apic1(config-tenant)# exit`
	`apic1(config)# leaf 101`
	`apic1(config-leaf)# vrf context tenant t1_provider vrf VRF1 l3out T0-o1-L3OUT-1`	

	コマンドまたはアクション	目的
	apic1(config-leaf-vrf)# **route-map T0-o1-L3OUT-1_shared** apic1(config-leaf-vrf-route-map)# **ip prefix-list l3extInstP-1 permit 192.168.2.0/24** apic1(config-leaf-vrf-route-map)# **match prefix-list l3extInstP-1** apic1(config-leaf-vrf-route-map-match)# **exit** apic1(config-leaf-vrf-route-map)# **exit** apic1(config-leaf-vrf)# **exit** apic1(config-leaf)# **exit**	
ステップ 3	レイヤ 3 Out コンシューマを設定します。 例： apic1(config)# **tenant t1_consumer** apic1(config-tenant)# **external-l3 epg l3extInstP-2 l3out T0-o1-L3OUT-1** apic1(config-tenant-l3ext-epg)# **vrf member VRF2** apic1(config-tenant-l3ext-epg)# **match ip 199.16.2.0/24 shared** apic1(config-tenant-l3ext-epg)# **contract consumer vzBrCP-1 imported** apic1(config-tenant-l3ext-epg)# **exit** apic1(config-tenant)# **exit** apic1(config)# **leaf 101** apic1(config-leaf)# **vrf context tenant t1_consumer vrf VRF2 l3out T0-o1-L3OUT-1** apic1(config-leaf-vrf)# **route-map T0-o1-L3OUT-1_shared** apic1(config-leaf-vrf-route-map)# **ip prefix-list l3extInstP-2 permit 199.16.2.0/24** apic1(config-leaf-vrf-route-map)# **match prefix-list l3extInstP-2** apic1(config-leaf-vrf-route-map-match)# **exit** apic1(config-leaf-vrf-route-map)# **exit** apic1(config-leaf-vrf)# **exit** apic1(config-leaf)# **exit** apic1(config)#	

NX-OS Style CLI を使用した共有レイヤ 3 VRF 間リークの設定：名前を付けた例

手順

	コマンドまたはアクション	目的
ステップ 1	コンフィギュレーション モードを開始します。 例： `apic1# configure`	

ステップ 2	プロバイダ テナントおよび VRF の設定
	例：
	`apic1(config)# tenant t1_provider`
	`apic1(config-tenant)# vrf context VRF1`
	`apic1(config-tenant-vrf)# exit`
	`apic1(config-tenant)# exit`	

ステップ 3	コンシューマ テナントおよび VRF の設定
	例：
	`apic1(config)# tenant t1_consumer`
	`apic1(config-tenant)# vrf context VRF2`
	`apic1(config-tenant-vrf)# exit`
	`apic1(config-tenant)# exit`	

ステップ 4	コントラクトの設定
	例：
	`apic1(config)# tenant t1_provider`
	`apic1(config-tenant)# contract vzBrCP-1 type permit`
	`apic1(config-tenant-contract)# scope exportable`
	`apic1(config-tenant-contract)# export to tenant t1_consumer`
	`apic1(config-tenant-contract)# exit`	

ステップ 5	プロバイダ外部レイヤ 3 EPG の設定
	例：
	`apic1(config-tenant)# external-l3 epg l3extInstP-1`
	`apic1(config-tenant-l3ext-epg)# vrf member VRF1`
	`apic1(config-tenant-l3ext-epg)# match ip 192.168.2.0/24 shared`
	`apic1(config-tenant-l3ext-epg)# contract provider vzBrCP-1`
	`apic1(config-tenant-l3ext-epg)# exit`
	`apic1(config-tenant)# exit`	

	コマンドまたはアクション	目的

ステップ 6	プロバイダ エクスポート マップの設定
	例：
	`apic1(config)# leaf 101`
	`apic1(config-leaf)# vrf context tenant t1_provider vrf VRF1`
	`apic1(config-leaf-vrf)# route-map map1`
	`apic1(config-leaf-vrf-route-map)# ip prefix-list p1 permit 192.168.2.0/24`
	`apic1(config-leaf-vrf-route-map)# match prefix-list p1`
	`apic1(config-leaf-vrf-route-map-match)# exit`
	`apic1(config-leaf-vrf-route-map)# exit`
	`apic1(config-leaf-vrf)# export map map1`
	`apic1(config-leaf-vrf)# exit`
	`apic1(config-leaf)# exit`	

ステップ 7	コンシューマ外部レイヤ 3 EPG の設定
	例：
	`apic1(config)# tenant t1_consumer`
	`apic1(config-tenant)# external-l3 epg l3extInstP-2`
	`apic1(config-tenant-l3ext-epg)# vrf member VRF2`
	`apic1(config-tenant-l3ext-epg)# match ip 199.16.2.0/24 shared`
	`apic1(config-tenant-l3ext-epg)# contract consumer vzBrCP-1 imported`
	`apic1(config-tenant-l3ext-epg)# exit`
	`apic1(config-tenant)# exit`	

ステップ 8	コンシューマ エクスポート マップの設定
	例：
	`apic1(config)# leaf 101`
	`apic1(config-leaf)# vrf context tenant t1_consumer vrf VRF2`
	`apic1(config-leaf-vrf)# route-map map2`
	`apic1(config-leaf-vrf-route-map)# ip prefix-list p2 permit 199.16.2.0/24`
	`apic1(config-leaf-vrf-route-map)# match prefix-list p2`
	`apic1(config-leaf-vrf-route-map-match)# exit`
	`apic1(config-leaf-vrf-route-map)# exit`
	`apic1(config-leaf-vrf)# export map map2`
	`apic1(config-leaf-vrf)# exit`
	`apic1(config-leaf)# exit`
	`apic1(config)#`	

拡張 GUI を使用した共有レイヤ 3 Out VRF 間リーキングの設定

始める前に

コンシューマとプロバイダーによって使用される契約ラベルが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 **Tenants** > **Add Tenant** を選択します。

ステップ 2 **Create Tenant** ダイアログボックスに、プロバイダーのテナント名を入力します。

ステップ 3 **VRF Name** フィールドに、プロバイダーの VRF 名を入力します。

ステップ 4 **Navigation** ウィンドウの新しいテナント名の下で、**External Routed Networks** に移動します。

ステップ 5 **Work** ウィンドウの Canvas で、**L3 Out** のアイコンをドラッグし、作成した新しい VRF にドロップして関連付けます。

ステップ 6 **Create Routed Outside** 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、Layer 3 Routed Outside の名前を入力します。
b) **Next** をクリックして、 **Step 2 > External EPG Networks** ダイアログボックスに移動します。
c) **External EPG networks** を展開します。

ステップ 7 **Create External Network** 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、外部ネットワーク名を入力します。
b) **Subnet** を展開し、**Create Subnet** ダイアログボックスの **IP Address** フィールドに、マッチングを行う IP アドレスを入力します。**OK** をクリックします。

ステップ 8 **Navigation** ウィンドウで、作成した **Layer 3 Outside_name** > **Networks** > **External_network_name** に移動します。

ステップ 9 **Work** ウィンドウの、外部ネットワークの **Properties** の下で、**Resolved VRF** フィールドに解決された VRF が表示されていることを確認します。

ステップ 10 外部サブネットの **Configured Subnet IP** アドレスをクリックして、**Subnet** ダイアログボックスを開きます。

ステップ 11 **Scope** フィールドで、必要なチェック ボックスをオンにして、**Submit** をクリックします。

このシナリオでは、**Shared Route Control Subnet** と **Shared Security Import Subnet** のチェックボックスをオンにします。

ステップ 12 以前に作成した **Layer 3 Outside** に移動します。

ステップ 13 **Provider Label** フィールドに、このタスクを開始するための前提条件として作成したプロバイダー名を入力します。**Submit** をクリックします。

ステップ 14 メニュー バーで、 **Tenants** > **Add Tenant** をクリックします。

ステップ 15 **Create Tenant** ダイアログボックスで、Layer 3 Outside コンシューマのためのテナント名を入力します。

ステップ 16 **VRF Name** フィールドに、コンシューマの VRF 名を入力します。

ステップ 17 **Navigation** ウィンドウの新しいテナント名の下で、コンシューマの **External Routed Networks** に移動します。

ステップ 18 **Work** ウィンドウの Canvas で、**L3 Out** のアイコンをドラッグし、作成した新しい VRF にドロップして関連付けます。

ステップ 19 **Create Routed Outside** ダイアログボックスで、次の操作を実行します:

a) **Name** フィールドで、ドロップダウン メニューから、コンシューマのために作成された VRF を選択します。

b) **Consumer Label** フィールドに、コンシューマ ラベルの名前を入力します。

c) **Next** をクリックして、 **Step 2 > External EPG Networks** ダイアログボックスに移動します。

ステップ 20 **EPG networks** を展開し、**Create External Network** 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、外部ネットワークの名前を入力します。

b) **Subnet** を展開し、**Create Subnet** ダイアログボックスの **IP Address** フィールドに、マッチングを行う IP アドレスを入力します。**OK** をクリックします。

c) **Scope** フィールドで、必要なチェック ボックスをオンにして、**OK** をクリックします。

このシナリオでは、**Shared Route Control Subnet** と **Shared Security Import Subnet** のチェック ボックスをオンにします。

ステップ 21 **[Create External Network]** ダイアログボックスで、**[OK]** をクリックします。**[Create Routed Outside]** ダイアログボックスで、**[Finish]** をクリックします。

これで、共有レイヤ 3 Out VRF 間リーキングの設定は完了です。

第 14 章

外部ルートのインターリーク

この章は、次の項で構成されています。

概要

このトピックでは、Cisco APIC を使用する場合、OSPF など外部ルートの内部リークを設定する方法の一般的な例を説明します。

OSPF からの内部リークは、以前のリリースで使用できるようになりました。この機能により、OSFP から BGP へルートをリーキングするコミュニティ、基本設定、メトリックなどユーザーが属性を設定できるようになりました。

GUI を使用して外部ルートの Interleak の設定

この例で設定されている外部ルーテッド ネットワークを、IPv4 をサポートするように拡張することもできます。IPv4 と IPv6 両方のルートを外部ルーテッド ネットワークにアドバタイズし、外部ルーテッド ネットワークから学習することができます。

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ること。
- 外部ルーテッド ドメインが作成されていること。

手順

ステップ 1 メニュー バーで、[TENANTS] をクリックします。

ステップ 2 **[Navigation]** ペインで、***[Tenant_name]*** > **[Networking]** > **[External Routed Networks]** の順に展開し、次の操作を実行します。

a) **[External Routed Networks]** を右クリックし、**[Create Routed Outside]** をクリックします。
b) **[Create Routed Outside]** ダイアログボックスの **[Name]** フィールドに、ルーテッド Outside の名前を入力します。
c) **[VRF]** フィールドのドロップダウン リストから、適切な VRF を選択します。
d) **[External Routed Domain]** ドロップダウン リストから、適切な外部ルーテッド ドメインを選択します。
e) 目的のプロトコルのチェックボックスをオンにします。

このタスクの目的で、オプションでは、OSPF です。

f) **Interleak のルート プロファイル** フィールドで、をクリックして **ルート プロファイルの作成** します。

ステップ 3 **[Create Route Profile]** ダイアログ ボックスで、**[Name]** フィールドに、ルート プロファイル名を入力します。

ステップ 4 **[Type]** フィールドで、 **[Match Routing Policy Only]** を選択する必要があります。

ステップ 5 をクリックして、 + を開くにサインイン、 **ルート制御コンテキストの作成** ダイアログボックスし、次のアクションを実行します。

a) **順序と名前を入力** 必要に応じてフィールドします。
b) **[Set Attribute]** フィールドで、**[Create Action Rule Profile]** をクリックします。
c) **[Create Action Rule Profile]** ダイアログ ボックスの **[Name]** フィールドに、アクション ルール プロファイルの名前を入力します。
d) 目的の属性および関連するコミュニティ、条件、タグ、および設定 (preferences) を選択します。[OK] をクリックします。
e) **[Create Route Profile]** ダイアログボックスで、**[Submit]** をクリックします。

ステップ 6 **外部ルーティング作成** ダイアログボックス、展開、 **ノードとインターフェイス プロトコル プロファイル** エリア。

ステップ 7 **[Create Node Profile]** ダイアログ ボックスで、ノード プロファイルを指定します。[OK] をクリックします。

ステップ 8 **[Create Routed Outside]** ダイアログボックスで、**[Next]** をクリックします。

ステップ 9 [External EPG Networks] 領域で、[External EPG Networks] を展開します。

ステップ 10 **[Create External Network]** ダイアログ ボックスの **[Name]** フィールドに名前を入力します。

ステップ 11 **[Subnet]** を展開し、[Create **Subnet]** ダイアログボックスの **[IP address]** フィールドに IP アドレスを入力します。[OK] をクリックします。

ステップ 12 **[Create External Network]** ダイアログボックスで、**[OK]** をクリックします。

ステップ 13 **[Create Routed Outside]** ダイアログボックスで、**[Finish]** をクリックします。
Interleak のルート プロファイルが作成され、外部 L3 に関連付けられています。

NX-OSスタイルのCLIを使用したインターリーク外部ルートの設定

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ること。
- 外部ルーテッド ドメインが作成されていること。

手順

NX-OS は、CLI を使用して、ルート再配布ルート ポリシーを設定します:

a) テナントを範囲とするルート プロファイルを作成します:

例：

```
apic1(config-leaf)# template route-profile map_ospf tenant ExampleCorp
apic1(config-leaf-template-route-profile)# set tag 100
apic1(config-leaf-template-route-profile)# exit
```

b) 前のステップで作成したルートプロファイルのいずれかを使用してOSPFのBGPの下で、再配布ルート プロファイルを設定します。

例：

```
apic1(config-leaf)# router bgp 100
apic1(config-bgp)# vrf member tenant ExampleCorp vrf v1
apic1(config-leaf-bgp-vrf)# redistribute ospf route-map map_ospf
```

（注） 再配布ルート マップはすべてのルートを許可しており、ルート プロファイルをルート コントロール アクションに適用することに注意してください。例では、すべての OSPF 学習ルートが、タグ 100 の BGP に再配布されます。

REST API を使用した外部ルートの内部リークの設定

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ること。
- 外部ルーテッド ドメインが作成されていること。

手順

外部ルートのインターリークを設定します。

例：

```
<l3extOut descr="" enforceRtctrl="export" name="out1" ownerKey="" ownerTag=""
targetDscp="unspecified">
      <l3extLNodeP configIssues="" descr="" name="Lnodep1" ownerKey="" ownerTag=""
tag="yellow-green" targetDscp="unspecified">
        <l3extRsNodeL3OutAtt rtrId="1.2.3.4" rtrIdLoopBack="yes"
tDn="topology/pod-1/node-101"/>
        <l3extLIfP descr="" name="lifp1" ownerKey="" ownerTag="" tag="yellow-green">
          <ospfIfP authKeyId="1" authType="none" descr="" name="">
            <ospfRsIfPol tnOspfIfPolName=""/>
          </ospfIfP>
          <l3extRsNdIfPol tnNdIfPolName=""/>
          <l3extRsIngressQosDppPol tnQosDppPolName=""/>
          <l3extRsEgressQosDppPol tnQosDppPolName=""/>
          <l3extRsPathL3OutAtt addr="12.12.7.16/24" descr="" encap="unknown"
encapScope="local" ifInstT="l3-port" llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular"
 mtu="inherit" tDn="topology/pod-1/paths-101/pathep-[eth1/11]" targetDscp="unspecified"/>

        </l3extLIfP>
      </l3extLNodeP>
      <l3extRsEctx tnFvCtxName="ctx1"/>
      <l3extRsInterleakPol tnRtctrlProfileName="interleak"/>
      <l3extRsL3DomAtt tDn="uni/l3dom-Domain"/>
      <l3extInstP descr="" matchT="AtleastOne" name="InstP1" prio="unspecified"
targetDscp="unspecified">
        <fvRsCustQosPol tnQosCustomPolName=""/>
        <l3extSubnet aggregate="" descr="" ip="14.15.16.0/24" name=""
scope="export-rtctrl,import-security"/>
      </l3extInstP>
      <ospfExtP areaCost="1" areaCtrl="redistribute,summary" areaId="0.0.0.1"
areaType="nssa" descr=""/>
    </l3extOut>
```

第 15 章

IP エージング

この章の内容は、次のとおりです。

概要

IP エージング ポリシーは、エンドポイントの未使用の IP アドレスを追跡しエージングが行われます。トラッキングはブリッジドメインに設定されたエンドポイント保持ポリシーを使用して実行され、ローカル エンドポイント エージング間隔の 75% で、ARP 要求（IPv4）やネイバー要請（IPv6）を送信します。IP アドレスから応答を受信しなかった場合、その IP アドレスはエージング アウトします。

このドキュメントでは、IP エージング ポリシーを設定する方法について説明します。

GUI を使用した IP エージングポリシーの設定

このセクションでは、IP エージング ポリシーの有効と無効を切り替える方法について説明します。

手順

ステップ 1 メニュー バーで、**System** タブをクリックします。

ステップ 2 サブメニュー バーで、**System Settings** をクリックします。

ステップ 3 ナビゲーション ウィンドウで、**Endpoint Controls** をクリックします。

ステップ 4 作業ウィンドウで、**Ip Aging** をクリックします。
IP Aging Policy が、**Administrative State** の **Disabled** ボタンが選択された状態で表示されます。

ステップ 5 **Administrative State** で、次のオプションのいずれかをクリックします:

- **Enabled**— IP エージングを有効にします。
- **Disabled**— IP エージングを無効にします。

次のタスク

エンドポイントの IP アドレスを追跡するために使用される間隔を指定するには、エンド ポイント保持ポリシーを作成します。**Tenants** > ***tenant-name*** > **Policies** > **Protocol** に移動し、**End Point Retention** を右クリックし、**Create End Point Retention Policy** を選択します。

NX-OS スタイル CLI を使用した IP エージング ポリシーの設定

このセクションでは、CLI を使用した IP エージング ポリシーを有効および無効にする方法を説明します。

手順

ステップ 1 IP エージング ポリシーを有効にするには：

例：

```
ifc1(config)# endpoint ip aging
```

ステップ 2 IP エージング ポリシーを無効にするには：

例：

```
ifav9-ifc1(config)# no endpoint ip aging
```

次のタスク

エンドポイントの IP アドレスをトラッキングするために使用される間隔を指定するには、エンドポイント保持ポリシーを作成します。

REST API を使用した IP エージングの設定

このセクションでは、REST API を使用した IP エージング ポリシーを有効および無効にする方法を説明します。

手順

ステップ 1 IP エージング ポリシーを有効にするには：

例：

```
<epIpAgingP adminSt="enabled" descr="" dn="uni/infra/ipAgingP-default" name="default"
ownerKey="" ownerTag=""/>
```

ステップ 2 IP エージング ポリシーを無効にするには：

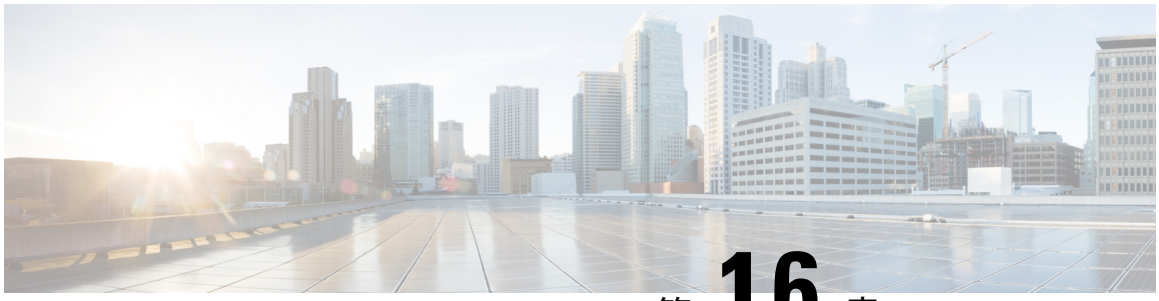
例：

```
<epIpAgingP adminSt="disabled" descr="" dn="uni/infra/ipAgingP-default" name="default"
ownerKey="" ownerTag=""/>
```

次のタスク

エンドポイントの IP アドレスをトラッキングするために使用される間隔を指定するには、次の例のように XML で post を送信することによって、エンドポイント保持ポリシーを作成します。

```
<fvEpRetPol bounceAgeIntvl="630" bounceTrig="protocol"
holdIntvl="350" lcOwn="local" localEpAgeIntvl="900" moveFreq="256"
name="EndpointPol1" remoteEpAgeIntvl="350"/>
```



第 16 章

IPv6 ネイバー探索

この章の内容は、次のとおりです。

ネイバー探索

IPv6 ネイバー探索（ND）は、ノードのアドレスの自動設定、リンク上の他のノードの探索、他のノードのリンク層アドレスの判別、重複アドレスの検出、使用可能なルータと DNS サーバの検出、アドレス プレフィックスの探索、および他のアクティブなネイバー ノードへのパスに関する到達可能性情報の維持を担当します。

ND 固有のネイバー要求/ネイバー アドバタイズメント（NS/NA）およびルータ要求/ルータ アドバタイズメント（RS/RA）パケット タイプは、物理、層3 サブ インターフェイス、および SVI（外部およびパーベイシブ）を含むすべての ACI ファブリックのレイヤ 3 インターフェイスでサポートされます。APIC リリース 3.1(1x) まで、RS/RA パケットはすべてのレイヤ 3 インターフェイスの自動設定のために使用されますが、拡散型 SVI の設定のみ可能です。

APIC リリース 3.1(2x) より、RS/RA パケットは自動設定のため使用され、ルーテッド インターフェイス、レイヤ 3 サブ インターフェイス、SVI（外部および拡散）を含むレイヤ 3 インターフェイスで設定できます。

ACI のブリッジ ドメイン ND は常にフラッド モードで動作します。ユニキャスト モードはサポートされません。

ACI ファブリック ND サポートに含まれるもの：

- インターフェイス ポリシー（`nd:IfPol`）は、NS/NA メッセージに関する ND タイマーと動作を制御します。
- ND プレフィックス ポリシー（`nd:PfxPol`）コントロール RA メッセージ。
- ND の IPv6 サブネット（fv:Subnet）の設定。

- 外部ネットワークの ND インターフェイス ポリシー。
- 外部ネットワークの設定可能 ND サブネットおよびパーベイシブ ブリッジ ドメインの任意サブネット設定はサポートされません。

設定可能なオプションは次のとおりです。

- 隣接関係
  - 設定可能な静的 Adjacencies：（<vrf、L3Iface < ipv6 address> --> mac address）
  - 動的 Adjacencies：NS/NA パケットの交換経由で学習
- インターフェイス単位
  - ND パケットの制御（NS/NA）
    - ネイバー要求間隔
    - ネイバー要求再試行回数
  - RA パケットの制御
    - RA の抑制
    - RA MTU の抑制
    - RA 間隔、RA 最小間隔、再送信時間
- プレフィックス単位（RA でアドバタイズ）の制御
  - ライフタイム、優先ライフタイム
  - プレフィックス コントロール（自動設定、リンク上）
- ネイバー検索重複アドレスの検出（DAD）

ブリッジ ドメインでの IPv6 ネイバー探索の設定

REST API を使用したブリッジ ドメインの IPv6 ネイバー探索対応のテナント、VRF、およびブリッジ ドメインの作成

手順

ネイバー探索インターフェイス ポリシーとネイバー探索プレフィックス ポリシーが適用された、テナント、VRF、ブリッジ ドメインを作成します。

例：

```
<fvTenant descr="" dn="uni/tn-ExampleCorp" name="ExampleCorp" ownerKey="" ownerTag="">
    <ndIfPol name="NDPol001" ctrl="managed-cfg”  descr="" hopLimit="64" mtu="1500"
nsIntvl="1000" nsRetries="3" ownerKey="" ownerTag="" raIntvl="600" raLifetime="1800"
reachableTime="0" retransTimer="0"/>
    <fvCtx descr="" knwMcastAct="permit" name="pvn1" ownerKey="" ownerTag=""
pcEnfPref="enforced">
    </fvCtx>
    <fvBD arpFlood="no" descr="" mac="00:22:BD:F8:19:FF" multiDstPktAct="bd-flood"
name="bd1" ownerKey="" ownerTag="" unicastRoute="yes" unkMacUcastAct="proxy"
unkMcastAct="flood">
        <fvRsBDToNdP tnNdIfPolName="NDPol001"/>
        <fvRsCtx tnFvCtxName="pvn1"/>
       <fvSubnet ctrl="nd" descr="" ip="34::1/64" name="" preferred="no" scope="private">

            <fvRsNdPfxPol tnNdPfxPolName="NDPfxPol001"/>
        </fvSubnet>
       <fvSubnet ctrl="nd" descr="" ip="33::1/64" name="" preferred="no" scope="private">

            <fvRsNdPfxPol tnNdPfxPolName="NDPfxPol002"/>
        </fvSubnet>
    </fvBD>
    <ndPfxPol ctrl="auto-cfg,on-link" descr="" lifetime="1000" name="NDPfxPol001"
ownerKey="" ownerTag="" prefLifetime="1000"/>
    <ndPfxPol ctrl="auto-cfg,on-link" descr="" lifetime="4294967295" name="NDPfxPol002"
 ownerKey="" ownerTag="" prefLifetime="4294967295"/>
</fvTenant>
```

（注） 外部ルーテッドを設定するときにパブリック サブネットがある場合は、ブリッジ ドメインを外部設定と関連付ける必要があります。

NX-OS スタイル CLI を使用したブリッジ ドメイン上の IPv6 ネイバー検索によるテナント、VRF、ブリッジ ドメインの設定

手順

ステップ 1 IPv6 ネイバー検索インターフェイス ポリシーを設定し、ブリッジ ドメインに割り当てます。

a) IPv6 ネイバー検索インターフェイス ポリシーを作成します。

例：

```
apic1(config)# tenant ExampleCorp
apic1(config-tenant)# template ipv6 nd policy NDPol001
apic1(config-tenant-template-ipv6-nd)# ipv6 nd mtu 1500
```

b) VRF およびブリッジ ドメインを作成します:

例：

```
apic1(config-tenant)# vrf context pvn1
apic1(config-tenant-vrf)# exit
```

```
apic1(config-tenant)# bridge-domain bd1
apic1(config-tenant-bd)# vrf member pvn1
apic1(config-tenant-bd)# exit
```

c) IPv6 ネイバー検索ポリシーをブリッジ ドメインに割り当てます。

例：

```
apic1(config-tenant)# interface bridge-domain bd1
apic1(config-tenant-interface)# ipv6 nd policy NDPol001
apic1(config-tenant-interface)#exit
```

ステップ 2 サブネット上で IPV6 ブリッジ ドメイン サブネットおよびネイバー検索プレフィックス ポリシーを作成します。

例：

```
apic1(config-tenant)# interface bridge-domain bd1
apic1(config-tenant-interface)# ipv6 address 34::1/64
apic1(config-tenant-interface)# ipv6 address 33::1/64
apic1(config-tenant-interface)# ipv6 nd prefix 34::1/64 1000 1000
apic1(config-tenant-interface)# ipv6 nd prefix 33::1/64 4294967295 4294967295
```

GUI を使用して、ブリッジ ドメイン上に IPv6 ネイバー探索対応のテナント、VRF、およびブリッジ ドメインを作成する

このタスクでは、テナント、VRF、およびブリッジ ドメイン（BD）を作成し、それらの中に 2 つの異なるタイプのネイバー探索（ND）ポリシーを作成する方法を示します。これらは ND インターフェイス ポリシーと ND プレフィックス ポリシーです。ND インターフェイス ポリシーは BD に導入されますが、ND プレフィックス ポリシーは個々のサブネットに導入されます。各 BD に独自の ND インターフェイス ポリシーを適用することができます。ND インターフェイス ポリシーは、デフォルトですべての IPv6 インターフェイスに導入されます。Cisco APIC には、使用可能なデフォルトの ND インターフェイス ポリシーがすでに存在します。必要に応じて、代わりに使用するカスタム ND インターフェイス ポリシーを作成できます。ND プレフィックス ポリシーはサブネット レベルにあります。すべての BD が複数のサブネットを持つことができ、各サブネットが異なる ND プレフィックスを持つことができます。

手順

ステップ 1 メニュー バーで、**[TENANT]** > **[Add Tenant]** の順にクリックします。

ステップ 2 [Create Tenant] ダイアログボックスで、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) [Security Domains +] アイコンをクリックして [Create Security Domain] ダイアログボックスを開きます。

c) [Name] フィールドに、セキュリティ ドメインの名前を入力します。**Submit** をクリックします。

d) [Create Tenant] ダイアログボックスで、作成したセキュリティ ドメインのチェックボックスをオンにし、[Submit] をクリックします。

ステップ 3 [Navigation] ペインで、**[Tenant-name]** > **[Networking]** の順に展開します。[Work] ペインで、[VRF] アイコンをキャンバスにドラッグして [Create VRF] ダイアログボックスを開き、次の操作を実行します。

a) [Name] フィールドに、名前を入力します。
b) [Submit] をクリックして VRF の設定を完了します。

ステップ 4 [Networking] 領域で、[BD] アイコンを [VRF] アイコンにつなげながらキャンバスにドラッグします。[Create Bridge Domain] ダイアログボックスが表示されたら、次の操作を実行します。

a) [Name] フィールドに、名前を入力します。
b) [L3 Configurations] タブをクリックし、[Subnets] を展開して [Create Subnet] ダイアログボックスを開き、[Gateway IP] フィールドにサブネット マスクを入力します。

ステップ 5 [Subnet Control] フィールドで、[ND RA Prefix] チェックボックスがオンになっていることを確認します。

ステップ 6 [ND Prefix policy] フィールドのドロップダウン リストで、[Create ND RA Prefix Policy] をクリックします。

（注） すべての IPv6 インターフェイスに導入される使用可能なデフォルト ポリシーがすでに存在しています。または、この例で示されているように、使用する ND プレフィックス ポリシーを作成できます。デフォルトでは、IPv6 ゲートウェイのサブネットは ND RA メッセージの ND プレフィックスとしてアドバタイズされます。ユーザは、[ND RA prefix] チェックボックスをオフにして、ND RA メッセージでサブネットをアドバタイズしないことを選択できます。

ステップ 7 [Create ND RA Prefix Policy] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドにプレフィックス ポリシーの名前を入力します。

（注） 特定のサブネットに対して存在できるプレフィックス ポリシーは 1 つのみです。サブネットは共通プレフィックス ポリシーを使用できますが、各サブネットに異なるプレフィックス ポリシーを適用することが可能です。

b) [Controller State] フィールドで、目的のチェックボックスをオンにします。
c) [Valid Prefix Lifetime] フィールドで、プレフィックスを有効にする期間について目的の値を選択します。
d) [Preferred Prefix Lifetime] フィールドで、目的の値を選択します。[OK] をクリックします。

（注） ND プレフィックス ポリシーが作成され、特定のサブネットに接続されます。

ステップ 8 [ND policy] フィールドのドロップダウン リストで、[Create ND Interface Policy] をクリックし、次のタスクを実行します。

a) [Name] フィールドにポリシーの名前を入力します。
b) [Submit] をクリックします。`

ステップ 9 [OK] をクリックしてブリッジ ドメインの設定を完了します。

同様に、さまざまなプレフィックス ポリシーが適用された追加のサブネットを必要に応じて作成できます。

IPv6 アドレスのサブネットが BD に作成され、ND プレフィックス ポリシーが関連付けられています。

レイヤ 3 インターフェイス上での IPv6 ネイバー探索の設定

注意事項と制約事項

次のガイドラインと制限事項に適用ネイバー探索ルータ アドバタイズメント (ND RA) のプレフィックスのレイヤ 3 インターフェイス。

- ND RA 設定は、IPv6 プレフィクスにのみ適用されます。IPv4 プレフィクスで ND ポリシーを設定しようとするは適用に失敗します。

GUI を使用して、レイヤ 3 インターフェイス上の RA の IPv6 ネイバー探索インターフェイス ポリシーの設定

（注） 次の手順では、レイヤ 3 インターフェイスで IPv6 ネイバー探索インターフェイス ポリシーを関連付ける方法を表示します。この特定の例は、非 VPC インターフェイスを使用して設定する方法を示しています。

始める前に

- テナント、VRF、BD が作成されていること。
- 外部ルーテッド ネットワークで、L3Out が作成されます。

手順

ステップ 1 **ナビゲーション**] ペインで、適切なテナントで、適切な外部ルーテッド ネットワークに移動します。

ステップ 2 **外部ルーテッド ネットワーク** 、展開 > **論理ノード プロファイル** > **論理ノード生成** > **論理インターフェイス プロファイル** 。

ステップ 3 適切なをダブルクリック **論理インターフェイス プロファイル** 、し、[、 **作業**] ペインで、をクリックして **ポリシー** > **ルーテッド インターフェイス** > 。

（注） 作成論理インターフェイスプロファイルを持っていない場合は、ここにプロファイルを作成することができます。

ステップ 4 **Routed Interface** ダイアログボックスで、次の操作を実行します:

a) **ND RA プレフィックス** フィールドで、インターフェイスの ND RA プレフィックスを有効にするチェック ボックスをチェックします。

有効にすると、ルーテッド インターフェイスは自動設定使用できます。

また、 **ND RA プレフィックス ポリシー** フィールドが表示されます。

b) **ND RA Prefix Policy** フィールドで、ドロップダウンリストから、適切なポリシーを選択します。

c) 必要に応じて、画面上の他の値を選択します。[Submit] をクリックします。`

（注） **VPC インターフェイスを使用してを設定する際に、VPC の設定内のメンバは、その両方としてに、サイド A とサイド B の両方の ND RA プレフィックスが有効にする必要があります** 。**作業** ()] ペインで、 **論理インターフェイス プロファイル** 画面で、をクリックします **SVI** ()] タブ。**プロパティ** 、有効にするチェック ボックスをオン、**ND RA プレフィックス** サイド A とサイド B の両方を選択、同一の **ND RA プレフィックス ポリシー** サイド A とサイド B の

REST API を使用したレイヤ 3 インターフェイス上の RA による IPv6 ネイバー探索インターフェイス ポリシーの設定

手順

IPv6 ネイバー検索インターフェイス ポリシーを設定し、レイヤ 3 インターフェイスに関連付けます。

次の例では、非 VPC セットアップの設定が表示されます。

例：

```
<fvTenant dn="uni/tn-ExampleCorp" name="ExampleCorp">
  <ndIfPol name="NDPol001" ctrl="managed-cfg" hopLimit="64" mtu="1500" nsIntvl="1000"
nsRetries="3" raIntvl="600" raLifetime="1800" reachableTime="0" retransTimer="0"/>
  <fvCtx name="pvn1" pcEnfPref="enforced">
                    </fvCtx>
  <l3extOut enforceRtctrl="export" name="l3extOut001">
    <l3extRsEctx tnFvCtxName="pvn1"/>
    <l3extLNodeP name="lnodeP001">
      <l3extRsNodeL3OutAtt rtrId="11.11.205.1" rtrIdLoopBack="yes"
tDn="topology/pod-2/node-2011"/>
```

```
      <l3extLIfP name="lifP001">
        <l3extRsPathL3OutAtt addr="2001:20:21:22::2/64" ifInstT="l3-port" llAddr="::"
mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
tDn="topology/pod-2/paths-2011/pathep-[eth1/1]">
          <ndPfxP>
            <ndRsPfxPToNdPfxPol tnNdPfxPolName="NDPfxPol001"/>
          </ndPfxP>
        </l3extRsPathL3OutAtt>
        <l3extRsNdIfPol tnNdIfPolName="NDPol001"/>
      </l3extLIfP>
    </l3extLNodeP>
    <l3extInstP name="instp"/>
  </l3extOut>
  <ndPfxPol ctrl="auto-cfg,on-link" descr="" lifetime="1000" name="NDPfxPol001" ownerKey=""
 ownerTag="" prefLifetime="1000"/>
</fvTenant>
```

（注） VPC ポートについては、ndPfxP が l3extRsNodeL3OutAtt ではなく l3extMember の子である必要があります。次のコード スニペットは、VPC のセットアップでの設定を示します。

```
<l3extLNodeP name="lnodeP001">
<l3extRsNodeL3OutAtt rtrId="11.11.205.1" rtrIdLoopBack="yes"
tDn="topology/pod-2/node-2011"/>
<l3extRsNodeL3OutAtt rtrId="12.12.205.1" rtrIdLoopBack="yes"
tDn="topology/pod-2/node-2012"/>
  <l3extLIfP name="lifP002">
    <l3extRsPathL3OutAtt addr="0.0.0.0" encap="vlan-205" ifInstT="ext-svi"
llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
tDn="topology/pod-2/protpaths-2011-2012/pathep-[vpc7]" >
      <l3extMember addr="2001:20:25:1::1/64" descr="" llAddr="::" name=""
nameAlias="" side="A">
        <ndPfxP >
          <ndRsPfxPToNdPfxPol tnNdPfxPolName="NDPfxPol001"/>
        </ndPfxP>
      </l3extMember>
      <l3extMember addr="2001:20:25:1::2/64" descr="" llAddr="::" name=""
nameAlias="" side="B">
        <ndPfxP >
          <ndRsPfxPToNdPfxPol tnNdPfxPolName="NDPfxPol001"/>
        </ndPfxP>
      </l3extMember>
    </l3extRsPathL3OutAtt>
    <l3extRsNdIfPol tnNdIfPolName="NDPol001"/>    </l3extLIfP>
   </l3extLNodeP>
```

NX-OS スタイル CLI を使用したレイヤ 3 インターフェイス上の RA による IPv6 ネイバー探索インターフェイス ポリシーの設定

この例では、IPv6 ネイバー検索インターフェイス ポリシーを設定し、レイヤ 3 インターフェイスに割り当てます。次に、IPv6 レイヤ 3 アウトインターフェイス、ネイバー検索プレフィックス ポリシーを設定し、インターフェイスにネイバー検索ポリシーを関連付けます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	コンフィギュレーションモードに入ります。

ステップ 2	**tenant** *tenant_name*
	例：
	`apic1(config)# tenant ExampleCorp`
	`apic1(config-tenant)#`
		テナントを作成し、テナントモードを開始します。

ステップ 3	**template ipv6 nd policy** *policy_name* 例： `apic1(config-tenant)# template ipv6 nd policy NDPol001`	IPv6 ND ポリシーを作成します。

ステップ 4	**ipv6 nd mtu** *mtu value*
	例：
	`apic1(config-tenant-template-ipv6-nd)# ipv6 nd mtu 1500`
	`apic1(config-tenant-template-ipv6)# exit`
	`apic1(config-tenant-template)# exit`
	`apic1(config-tenant)#`
		IPv6 ND ポリシーに MTU 値を割り当てます。

ステップ 5	**vrf context** *VRF_name*
	例：
	`apic1(config-tenant)# vrf context pvn1`
	`apic1(config-tenant-vrf)# exit`
		VRF を作成します。

ステップ 6	**l3out** *VRF_name* 例： `apic1(config-tenant)# l3out l3extOut001`	レイヤ 3 アウト を作成します。
ステップ 7	**vrf member** *VRF_name* 例： `apic1(config-tenant-l3out)# vrf member`	VRF をレイヤ 3 アウトインターフェイスに関連付けます。

	コマンドまたはアクション	目的
	pvn1 apic1(config-tenant-l3out)# **exit**	
ステップ 8	**external-l3 epg instp l3out** *l3extOut001* 例： apic1(config-tenant)# **external-l3 epg instp l3out l3extOut001** apic1(config-tenant-l3ext-epg)# **vrf member pvn1** apic1(config-tenant-l3ext-epg)# **exit**	レイヤ 3 アウトおよび VRF をレイヤ 3 インターフェイスに割り当てます。
ステップ 9	**leaf** *2011* 例： apic1(config)# **leaf 2011**	リーフ スイッチ モードを開始します。
ステップ 10	**vrf context tenant** *ExampleCorp* **vrf** *pvn1* **l3out** *l3extOut001* 例： apic1(config-leaf)# **vrf context tenant ExampleCorp vrf pvn1 l3out l3extOut001** apic1(config-leaf-vrf)# **exit**	VRF をリーフ スイッチに関連付けます。
ステップ 11	**int** *eth 1/1* 例： apic1(config-leaf)# **int eth 1/1** apic1(config-leaf-if)#	インターフェイス モードに入ります。
ステップ 12	**vrf member tenant** *ExampleCorp* **vrf** *pvn1* **l3out** *l3extOut001* 例： apic1(config-leaf-if)# **vrf member tenant ExampleCorp vrf pvn1 l3out l3extOut001**	インターフェイスで関連付けられているテナント、VRF、レイヤ 3 Out を指定します。
ステップ 13	**ipv6 address** *2001:20:21:22::2/64* **preferred** 例：	プライマリまたは優先 Ipv6 アドレスを指定します。

	コマンドまたはアクション	目的
	apic1(config-leaf-if)# **ipv6 address 2001:20:21:22::2/64 preferred**	
ステップ 14	**ipv6 nd prefix** *2001:20:21:22::2/64 1000 1000* 例： apic1(config-leaf-if)# **ipv6 nd prefix 2001:20:21:22::2/64 1000 1000**	レイヤ 3 インターフェイス下で IPv6 ND プレフィックス ポリシーを設定します。
ステップ 15	**inherit ipv6 nd** *NDPol001* 例： apic1(config-leaf-if)# **inherit ipv6 nd NDPol001** apic1(config-leaf-if)# **exit** apic1(config-leaf)# **exit**	レイヤ 3 インターフェイス下で ND ポリシーを設定します。

設定が完了します。

IPv6 ネイバー探索重複アドレス検出の設定

ネイバー探索重複アドレス検出について

重複アドレス検出 (DAD) は、ネットワーク内で重複アドレスを検出するためにネイバー探索が使用するプロセスです。デフォルトでは、ACI ファブリック リーフ レイヤ 3 インターフェイスで使用されているリンクローカル アドレスとグローバルサブネット IPv6 アドレスの DAD が有効になっています。オプションとして、REST API (**ipv6Dad="disabled"** 設定を使用)または GUI を通してノブを構成することにより、IPv6 グローバルサブネットの DAD プロセスを無効にすることができます。外部接続されたデバイスに境界リーフ冗長性を提供するため、異なる境界リーフ スイッチ上の L3Outs にわたって同じ共有セカンダリ アドレスが必要な場合には、このノブを構成します。このような場合、DAD プロセスを無効にすれば、DAD が複数の境界リーフ スイッチ上の同じ共有セカンダリ アドレスを重複と見なすことを避けられます。このような場合には DAD プロセスを無効にしないと、共有セカンダリ アドレスが DUPLICATE DAD 状態に入り、使用できなくなることがあります。

REST API を使用したネイバー探索重複アドレス検出の設定

手順

ステップ 1 サブネットの ipv6Dad エントリの値を **disabled** に変更することによって、サブネットのネイバー探索重複アドレス検出プロセスを無効にします。

次の例は、2001:DB8:A::11/64 サブネットのネイバー探索重複アドレス検出エントリを **disabled** に設定する方法を示しています:

（注） 次の REST API の例では、読みやすくなるように、長い行を\文字で分割しています。

例：

```
                <l3extRsPathL3OutAtt addr="2001:DB8:A::2/64" autostate="enabled" \
                 childAction="" descr="" encap="vlan-1035" encapScope="local" \
                 ifInstT="ext-svi" ipv6Dad="enabled" llAddr=": :" \
                 mac="00:22:BD:F8:19:DD"  mtu="inherit"  \
                 rn="rspathL3OutAtt-[topology/pod-1/paths-105/pathep-[eth1/1]]"  \
                 status=""  tDn="topology/pod-1/paths-105/pathep-[eth1/1]"  >
                    <l3extIp addr="2001:DB8:A::11/64" childAction="" descr="" \
                     ipv6Dad="disabled"  name="" nameAlias="" \
                     rn="addr-[2001:DB8:A::11/64]" status=""/>

                </l3extRsPathL3OutAtt>
            </l3extLIfP>
        </l3extLNodeP>
```

ステップ 2 リーフ スイッチで **show ipv6 int** コマンドを入力して、設定がリーフ スイッチに正しくプッシュされたか確認してください。次に例を示します。

```
swtb23-leaf5# show ipv6 int vrf icmpv6:v1
IPv6 Interface Status for VRF "icmpv6:v1"(9)

vlan2, Interface status: protocol-up/link-up/admin-up, iod: 73
if_mode: ext
  IPv6 address:
    2001:DB8:A::2/64 [VALID] [PREFERRED]
    2001:DB8:A::11/64 [VALID] [dad-disabled]
  IPv6 subnet:  2001:DB8:A::/64
  IPv6 link-local address: fe80::863d:c6ff:fe9f:eb8b/10 (Default) [VALID]
```

GUI を使用したネイバー探索重複アドレス検出の設定

サブネットのネイバー探索重複アドレス検出プロセスを無効にするには、このセクションの手順に従ってください。

手順

ステップ 1 適切なページに移動して、そのインターフェイスの DAD フィールドにアクセスします。次に例を示します。

a) **Tenants** > **Tenant** > **Networking** > **External Routed Networks** > ***L3Out*** > **Logical Node Profiles** > ***node*** > **Logical Interface Profiles** に移動し、設定するインターフェイスを選択します。

b) *Routed Sub-interfaces* または *SVI* をクリックし、作成 (+) ボタンをクリックしてインターフェイスを設定します。

ステップ 2 このインターフェイスで、DAD エントリを次のように設定します:

- プライマリ アドレスでは、DAD エントリの値を **enabled** に設定します。
- 共有セカンダリ アドレスでは、DAD エントリの値を **disabled** に設定します。セカンダリ アドレスが境界リーフ スイッチ間で共有されていない場合には、そのアドレスの DAD を無効にする必要がないことに注意してください。

例：

たとえば、SVI インターフェイスのこの設定を構成する場合には、次のようになります:

- サイド A の IPv6 DAD を **enabled** に設定します。
- サイド B の IPv6 DAD を **disabled** に設定します。

例：

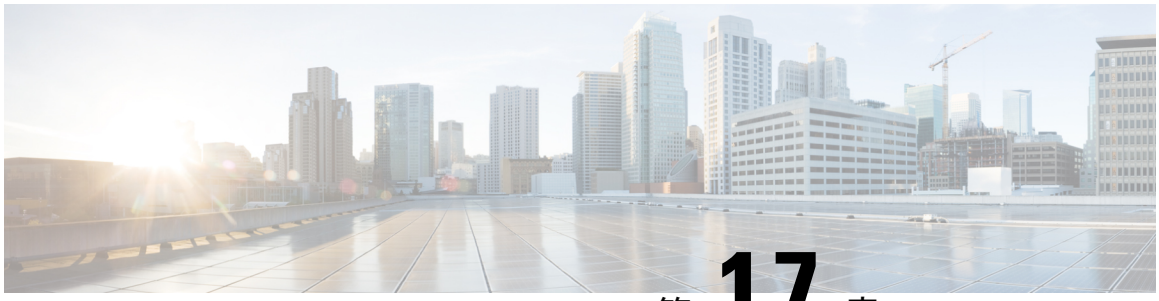
別の例として、ルーテッドサブインターフェイスの設定を構成する場合には、次のようになります:

- メインの [Select Routed Sub-Interface] ページで、ルーテッド サブインターフェイスの IPv6 DAD を **enabled** に設定します。
- [IPv4 Secondary/IPv6 Additional Addresses] エリアで作成 (+) ボタンをクリックして [Create Secondary IP Address] ページにアクセスし、IPv6 DAD の値を **disabled** に設定します。[OK] ボタンをクリックして、この画面での変更点を適用します。

ステップ 3 [Submit] ボタンをクリックして、変更を適用します。

ステップ 4 リーフ スイッチで **show ipv6 int** コマンドを入力して、設定がリーフ スイッチに正しくプッシュされたか確認してください。次に例を示します。

```
swtb23-leaf5# show ipv6 int vrf icmpv6:v1
IPv6 Interface Status for VRF "icmpv6:v1"(9)

vlan2, Interface status: protocol-up/link-up/admin-up, iod: 73
if_mode: ext
  IPv6 address:
    2001:DB8:A::2/64 [VALID] [PREFERRED]
    2001:DB8:A::11/64 [VALID] [dad-disabled]
  IPv6 subnet:  2001:DB8:A::/64
  IPv6 link-local address: fe80::863d:c6ff:fe9f:eb8b/10 (Default) [VALID]
```



第 17 章

IP Multicast：IP マルチキャスト

この章の内容は、次のとおりです。

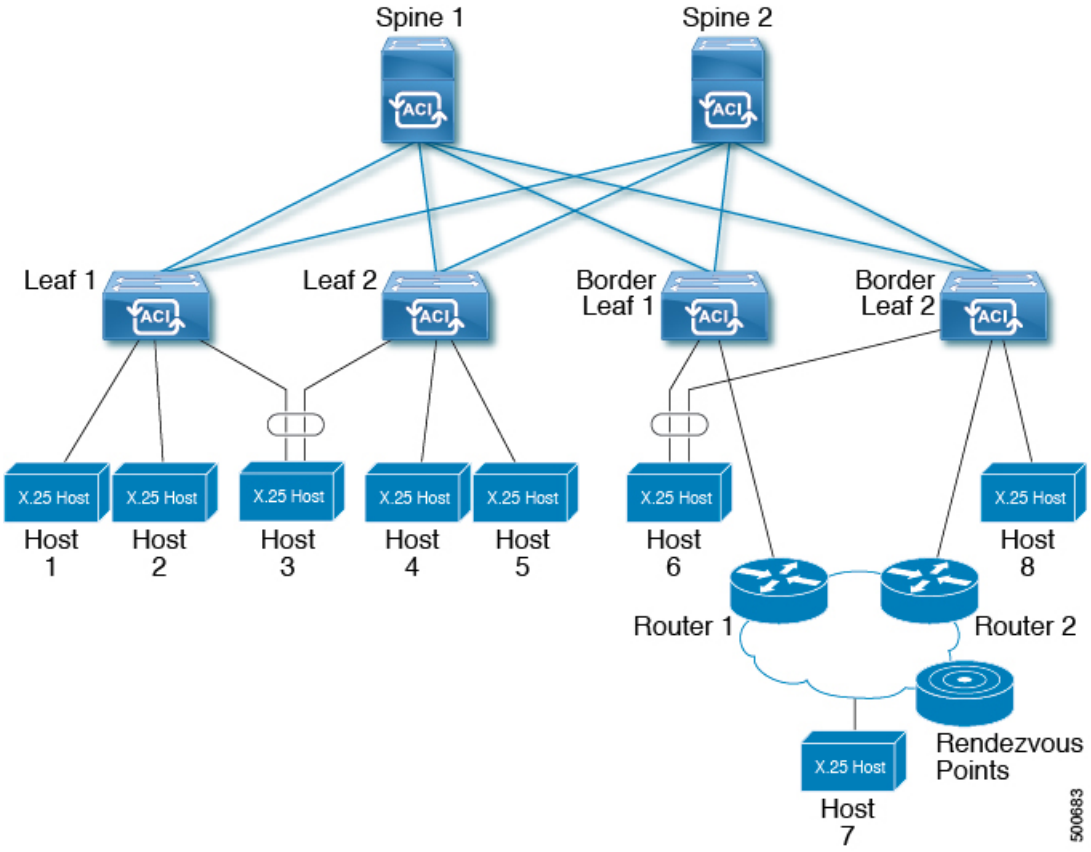
レイヤ 3 マルチキャスト

ACI ファブリックでは、ほとんどのユニキャストとマルチキャスト ルーティングが同じ境界リーフ スイッチで稼働しており、ユニキャスト ルーティング プロトコル上でマルチキャスト プロトコルが稼働しています。

このアーキテクチャでは、ボーダー リーフ スイッチのみが完全な Protocol Independent Multicast（PIM）プロトコルを実行します。非ボーダー リーフ スイッチは、インターフェイス上でパッシブ モードの PIM を実行します。これらは、その他の PIM ルータとピアリングしません。ボーダー リーフ スイッチは、L3 Out を介してそれらの接続された他の PIM ルータとピアリングし、またそれら相互にもピアリングします。

次の図に、マルチキャスト クラウド内のルータ（R1 と R2）に接続しているボーダー リーフ（BL）スイッチを示します。マルチキャスト ルーティングを必要とするファブリック内の各 Virtual Routing and Forwarding（VRF）は、それぞれ別に外部マルチキャスト ルータとピアリングします。

図 *22*：マルチキャスト クラウドの概要



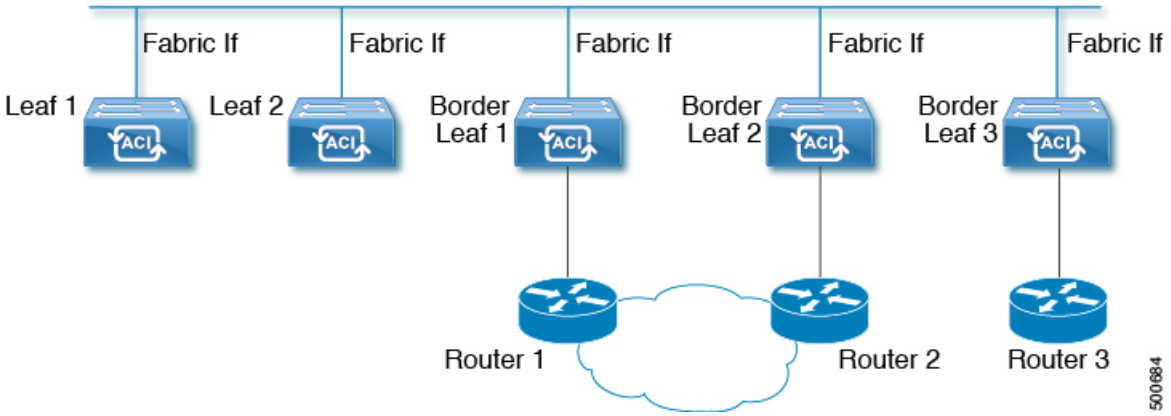
ファブリック インターフェイスについて

ファブリック インターフェイスはソフトウェア モジュール間の仮想インターフェイスであり、マルチキャスト ルーティングのファブリックを表します。インターフェイスは、宛先が VRF GIPo (グループ IP 外部アドレス) であるトンネル インターフェイスの形式を取ります。たとえば、境界リーフがグループのトラフィックの転送を担当する指定フォワーダの場合、ファブリック インターフェイスはグループの発信インターフェイス (OIF) となります。ハードウェアのインターフェイスに相当するものはありません。ファブリック インターフェイスの動作状態は、intermediate system-to-intermediate system（IS-IS）によって公開される、**aggFabState** に従ったものとなります。

（注） ユーザは、マルチキャスト ルーティングを有効にする VRF ごとの境界リーフごとに、一意のループバック アドレスを設定する必要があります。

ユニキャスト ルーティング用に設定された任意のループバックは再利用できます。このループバック アドレスは、外部ネットワークからルーティングする必要があり、VRF のファブリック MPBGP (マルチプロトコル境界ゲートウェイ プロトコル) ルートに挿入されます。ファブリック インターフェイスの送信元 IP は、このループバックに、ループバック インターフェイスとして設定されます。次の図は、マルチキャスト ルーティング用のファブリックを示しています。

図 *23 :* マルチキャスト ルーティング用のファブリック



マルチキャスト ルーティングの有効化

マルチキャストはVRF、L3アウト、ブリッジドメイン（BD）の3つのレベルで有効または無効です。上位レベルで、マルチキャスト ルーティングはマルチキャストが有効な BD を持つ VRF で有効にする必要があります。マルチキャストが有効な VRF では、マルチキャスト ルーティングが有効な BD およびマルチキャストが無効な BD の組み合わせにすることができます。マルチキャスト ルーティングが無効な BD は、VRF マルチキャスト パネルでは表示されません。マルチキャスト ルーティングが有効な L3 アウトはパネル上でも表示されますが、マルチキャスト ルーティングが有効な BD は常にマルチキャスト ルーティングが有効な VRF の一部になります。

Cisco Nexus 93128TX、9396PX、9396TX などのリーフ スイッチでは、マルチキャスト ルーティングはサポートされていません。すべてのマルチキャスト ルーティングとマルチキャストが有効な VRF は、製品 ID に Cisco Nexus 93108TC-EX および 93180YC-EX などの -EX という名前を持つスイッチでのみ展開される必要があります。

（注） レイヤ3ポートとサブインターフェイスはサポートされていますが、外部SVIはサポートされていません。外部 SVI がサポートされていないため、PIM を L3-VPC で有効にできません。

VRF GIPo の割り当て

VRF GIPo は、構成に基づいて暗黙的に割り当てられます。VRF に対して 1 つの GIPoが、そしてその VRF の下の各 BD に対して 1 つの GIPo があります。さらに、任意の GIPo は、複数の BD または複数の VRF の間で共有される可能性がありますが、しかし、VRF と BD の組み合わせで共有されることはありません。APIC は、この点を確認する必要があります。すでに処理され、VRF GIPo ツリーが構築された BD GIPo に加えて VRF GIPo を処理する場合には、IS-IS が変更されます。

すべてのマルチキャスト ルーティングのトラフィックは、VRF GIPo を使用して、ファブリックに転送されます。マルチキャストルーティングが有効なBD上のブロードキャストまたはユニキャスト フフラッド トラフィックは、引き続き BD GIPo を使用します。ルーティングされたがマルチキャスト トラフィックだけが VRF GIPo を使用します。

表 *21 : GIPo* の使用方法

トラフィック	非 MC ルーティングが有効な BD	MC ルーティングが有効な BD
ブロードキャスト	BD GIPo	BD GIPo
不明なユニキャスト フラッディング	BD GIPo	BD GIPo
マルチキャスト	BD GIPo	VRF GIPo

指定されたフォワーダとしての複数の境界リーフスイッチ

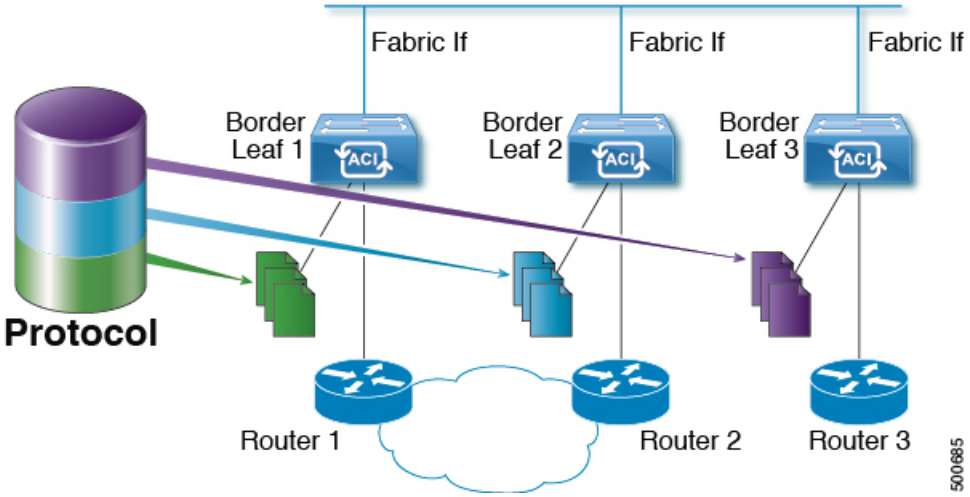
ファブリック内に、マルチキャストルーティングを行う複数の境界スイッチ(BL)がある場合、境界リーフのうちの1台だけが、外部マルチキャストネットワークからのトラフィックを集めてファブリックに転送する、指定されたフォワーダとなる必要があります。。これによってトラフィックの複数のコピーが発生することを防ぎ、複数の BL スイッチの間でバランスが取れるようにします。

このことは利用可能な BL スイッチにわたる、これはグループ アドレスと VRF ネットワーク ID(VNID)としてのグループの所有権を、ストライピングすることによって行われます。グルー

プの責任を担う BL は、PIM の参加を処理して、ファブリックのレシーバの代わりにファブリックへのトラフィックを集めます。

ファブリックの各 BL は、その VRF の他のすべてのアクティブな BL スイッチのビューを持ちます。それでそれぞれの BL スイッチは、独立に矛盾なく、グループのストライピングを行えます。各 BL は、アクティブな BL スイッチのリストを取得するために、ファブリック インターフェイス上の PIM ネイバーの関係をモニタします。BL スイッチが削除または検出されたときには、その時点でのアクティブな BL スイッチ間で、グループの再ストライピングが行われます。ストライピングは、マルチポッド環境で GIPos を外部リンクにハッシュするために用いられる方法に似ています。それで、グループから BL へのマッピングは持続性があり、アップ時やダウン時の変化が少なくてすみます。

図 *24 :* 指定されたフォワーダとしての複数の境界リーフのモデル



PIM 代表ルータの選定

ACI ファブリックのレイヤ 3 マルチキャストでは、異なるインターフェイス タイプの PIM DR（代表ルータ）メカニズムは次の通りです。

- [PIM が有効な L3 アウト インターフェイス]：これらのインターフェイス タイプの標準の PIM DR メカニズムに従います。
- [ファブリック インターフェイス]：このインターフェイスの DR 選定は、ストライピングにより決定される DR 機能ほど重要ではありません。PIM DR の選定は、引き続きこのインターフェイスに残ります。
- [マルチキャスト ルーティングが有効な普及 BD]：マルチキャスト ルーティングで接続されている限り、ファブリックの普及 BD はすべてのスタブです。そのため、すべてのリーフ スイッチで、vPC を含む普及 BD の SVI インターフェイスがセグメントの DR と見なされます。

非境界リーフ スイッチの動作

非境界リーフ スイッチ上の PIM は、ファブリック インターフェイスとパーベイシブ BD SVI では、パッシブ モードで動作します。PIM は新しいパッシブ プローブ モードになっており、*hellos* だけを送信します。これらのパーベイシブ BD SVI では、PIM ネイバーは想定されていません。PIM がパーベイシブ BD から *hello* を受信した場合には、障害が発生するのが望ましい動作です。非境界リーフ スイッチ上の PIM は、パーベイシブ BD上の *hellos* と、ファブリック インターフェイス上のソース登録パケットを除き、PIM プロトコルパケットを送信しません。

同時に、PIM はファブリック インターフェイス上の次の PIM パケットを受信して処理します:

- **PIM Hellos**: これはファブリック インターフェイス上でアクティブな BL リストを追跡するために使用されます。パーベイシブ BD上では、フォールトを発生するために使用されます。
- **PIM BSR、自動 RP アドバタイズメント**: これはファブリック インターフェイスで受信され、RP からグループ範囲へのマッピングを収集するために処理されます。

アクティブな境界リーフ スイッチ リスト

すべてのリーフ スイッチで、PIM はストライピングとその他の目的に使用されるアクティブな境界リーフスイッチのリストを保持しています。境界リーフスイッチ自体で、このアクティブな境界リーフ リストはアクティブな PIM のネイバー関係から導出されます。非境界リーフスイッチで、リストファブリックインターフェイス上のモニタ対象の *Hello* メッセージを使用して PIM によりリストが生成されます。*Hello* メッセージの送信元 IP は、各境界リーフ スイッチに割り当てられたループバック IP です。

ブートアップ時の過負荷の動作

境界リーフスイッチが起動後、または接続を失った後に初めてファブリックへの接続を得たとき、境界リーフスイッチが **COOP** リポジトリ情報をプルする機会を得て、サウスバウンド プロトコルの隣接関係を実際に利用するようになるまでは、境界リーフ スイッチがアクティブな境界リーフ スイッチのリストに加えられるのは望ましいことではありません。これは、PIM の *hello* メッセージの伝送を、設定されていない期間だけ遅らせることで実現できます。

ファーストホップの機能

リーフへの直接接続は、PIMサブネットマネージャ（PIM）に必要なファーストホップ機能を処理します。

ラストホップ

ラストホップ ルータは受信側に接続されるもので、PIM の any-source マルチキャスト (ASM) が発生した場合、最短パスツリー (SPT) スイッチオーバーを実行する責任を負います。境界リーフ スイッチはこの機能を処理します。境界非リーフ スイッチはこの機能には参加しません。

高速コンバージェンス モード

ファブリックはすべての境界リーフ スイッチがルートへの接続性の外部で設定可能な高速コンバージェンス モードをサポートしています (の *RP (*、G)* の送信元と *(S, G)*)、外部ネットワークからのトラフィックを停止します。重複を防ぐためには、1 人だけ、BL スイッチ転送トラフィック、ファブリックにします。ファブリックに、グループのトラフィックを転送する BL グループの代表フォワーダ (DF) と呼びます。グループのストライプ受賞は、DF を決定します。ストライプ受賞にルートに到達可能性がある場合は、[ストライプ受賞 DF もです。ストライプで優先されるデータが、ルートを外部の接続を持っていない場合、その BL は、ファブリック インターフェイス経由で PIM join を送信することによって、DF を選択し、します。PIM はトラフィックをひく点ですが、続行すると、ルートの RPF インターフェイスとして、ファブリック インターフェイスにアウト ルートの送信を外部の到達可能性をすべて非ストライプ受賞 BL スイッチ。これは、結果、トラフィックをドロップされたが、外部のリンク上で BL スイッチに到達します。

高速コンバージェンス モードの利点はプログラミング右のリバース パス フォワーディング（RPF） インターフェイスの新しいストライプ受賞 BL スイッチのみに必要なアクションになどの損失のためのストライプ所有者変更がある場合にです。新しいストライプ受賞から PIM ツリーに参加によって発生する遅延はありません。これは、非ストライプ受賞の外部リンクで追加帯域幅の使用増やしますが機能します。

（注） 追加の帯域幅のコストが保存コンバージェンス時間を上回る導入では、高速コンバージェンス モードを無効にできます。

レイヤ 3 マルチキャストの設定に関するガイドライン

次のガイドラインを参照してください。

- レイヤ 3 マルチキャストの設定は VRF レベルで実行されます。そのため、VRF 内とマルチキャスト内のプロトコル機能が VRF で有効になり、各マルチキャスト VRF を個別にオンまたはオフにすることができます。

- マルチキャストで VRF が有効になると、有効になった VRF の個別のブリッジ ドメイン (BD) と L3 Out を有効にしてマルチキャストを設定できます。デフォルトでは、マルチキャストはすべての BD およびレイヤ 3 Out で無効になっています。
- 現時点では、レイヤ 3 マルチキャストは、共有 L3 Out で設定された VRF ではサポートされていません。
- Any Source Multicast (ASM) と Source-Specific Multicast (SSM) はサポートされています。
- 現時点では、双方向 PIM、ACI ファブリック内のランデブー ポイント (RP) 、および PIM IPv6 はサポートされていません。
- IGMP スヌーピングは、マルチキャスト ルーティングが有効になっているパーベイシブ ブリッジ ドメインでは無効にできません。
- マルチキャスト ルータは、パーベイシブ ブリッジ ドメインではサポートされていません。
- 次の -EX でレイヤ 3 のマルチキャスト機能がサポートされているリーフ スイッチのモデルします。
  - N9K-93180YC-EX
  - N9K-93108TC-EX
  - N9K-93180LC-EX
- レイヤ 3 ポートとサブインターフェイスはサポートされていますが、外部 SVI はサポートされていません。外部 SVI がサポートされていないため、PIM を L3-VPC で有効にできません。
- マルチポッドのレイヤ 3 マルチキャスト サポートについて、イングレス リーフ スイッチはマルチキャスト ルーティングに対応しているブリッジ ドメインに接続されたソースからパケットを受信するとき、イングレス リーフ スイッチはファブリックにルート済み VRF コピーのみ送信します（ルート済みとは TTL が 1 に減少し、source-mac が拡散型サブネット MAC に再度書き込みされます）。また、出力リーフ スイッチも、関連するすべてのブリッジ ドメイン内の受信者へパケットをルーティングします。そのため、受信者のブリッジ ドメインが送信元と同じで、リーフ スイッチが送信元とは異なる場合、その受信者は同じブリッジ ドメイン内であっても、ルーティングされたコピーを受け取り続けます。

  詳細については、次のリンクで、既存のレイヤ 2 設計を活用する multipod サポート レイヤ 3 マルチキャストに関する詳細情報を参照してください。 追加ポッド 。
- リリース 3.1(1x) で始まる、FEX にマルチキャストのレイヤ 3 はサポートされています。マルチキャストのソースまたは FEX ポートに接続されているレシーバがサポートされます。詳細については、テスト環境で FEX を追加する方法について、設定、次の URL をアプリケーション セントリック インフラストラクチャとファブリック エクステンダを参照してください: https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/application-policy-infrastructure-controller-apic/200529-Configure-a-Fabric-Extender-with-Applica.html 。リリース 3.1(1x) 以降のレイヤ 3 マルチキャストでは FEX がサポートされていません。マルチキャストのソースまたは FEX ポートに接続されているレシーバはサポートされていません。

（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 multipod 接続を設定する場合は、MTU が両側で適切に設定されていることが重要です。ACI、Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定された MTU 値は IP ヘッダーを考慮に入れています（結果として、最大パケット サイズは、ACI で 9216 バイト、NX-OS および IOS で 9000 バイトに設定されます）。ただし、IOS XR などの他のプラットフォームは、パケット ヘッダーのを除く MTU 値を設定します（結果として最大パケット 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。

GUI を使用したレイヤ 3 マルチキャストの設定

始める前に

- 目的の VRF、ブリッジ ドメイン、IP アドレスを持つレイヤ 3 Out インターフェイス は、PIM および IGMP が有効になるように設定する必要があります。
- 基本的なユニキャスト ネットワークを設定する必要があります。

手順

ステップ 1 **Tenants** > ***Tenant_name*** > **Networking** > **VRFs** > ***VRF_name*** > **Multicast** に移動します。
[Work] ペインに、**PIM is not enabled on this VRF. Would you like to enable PIM?** というメッセージが表示されます。

ステップ 2 **YES, ENABLE MULTICAST** をクリックします。

ステップ 3 **Work** ウィンドウで、**Interfaces** タブをクリックします。

ステップ 4 **Bridge Domain** エリアで、次の操作を実行します:

a) **BD** ドロップダウン リストから、適切な BD を選択します。
b) **IGMP Policy** ドロップダウンリストで、目的の IGMP ポリシーを選択します。

Create IGMP Policy を選択して、新しい IGMP ポリシーを作成することができます。または、デフォルトのポリシーを使用することもできます。

ステップ 5 **Interfaces** エリアで、次の操作を実行します:

a) **Interfaces** を展開し、**Select and L3 Out** ダイアログボックスで、 **L3 Out** ドロップダウンリストから、適切な L3 Out を選択します。

b) **Select** をクリックします。

ステップ 6 **Rendezvous Points** タブをクリックします。

ステップ 7 使用可能なオプションから適切なランデブー ポイント (RP) を選択します。スタティック RP、自動 RP、またはブートス トラップ ルータを選択できます。または必要な RP を組み合わせて設定することもできます。

ステップ 8 （任意） **Static RP** を展開し、**RouteMap** ドロップダウンリストで、**Create RouteMap Policy** をクリックし、次の手順を実行します:

これは、マルチキャスト用に設定された特定のルート マップです。必要なルート マップがすでに存在する場合には、新しいルート マップを作成する代わりにそれを選択します。

a) **Name** フィールドにルート マップ ポリシ - の名前を入力します。
b) Enter the values in the fields for **Order**, **Source IP** , **Group IP**, **RP IP** for that entry.
c) **Action** フィールドで、必要なアクションに対して許可または拒否を選択します。**OK** をクリックします。
d) **Submit** をクリックして、**RouteMaps** の下にエントリを表示します。

ステップ 9 **[Work]** ウィンドウで、**Pattern Policy** タブをクリックします。

ステップ 10 **Pattern Policy** をクリックして、必要なマルチキャスト オプションを選択します。

ポリシーごとに、**Multicast Route Map** を選択します。

ステップ 11 **PIM Settings** タブをクリックして、必要な **PIM Setting** および**Resource Policy** の値を設定します。

ステップ 12 **IGMP Setting** タブをクリックします。

a) **[Group Prefix]** および **[Source Address]** フィールドに、それぞれの適切な値を入力します。
b) **Update** をクリックして、そのブリッジ ドメインの IGMP 設定を完了します。

ステップ 13 設定を確認するには次のアクションを実行します:

a) **Work** ウィンドウで、**Interfaces** をクリックして、関連付けられた **Bridge Domains** を表示します。
b) **Interfaces** をクリックして、関連付けられた **L3 Out** インターフェイスを表示します。
c) **Navigation** ウィンドウで、**BD** に移動します。
d) **Work** ウィンドウに、設定された IGMP ポリシーと PIM の機能が、先ほど設定されたように表示されます。
e) **Navigation** ウィンドウに、L3 Out インターフェイスが表示されます。
f) **Work** ウィンドウに、PIM の機能が先ほど設定されたように表示されます。
g) **Work** ウィンドウで、**Fabric** > **Inventory** > **Protocols** > **IGMP** に移動して、設定した IGMP インターフェイスの動作状態を表示します。
h) **Work** ウィンドウで、**Fabric** > **Inventory** > ***Pod name*** > ***Leaf_Node*** > **Protocols** > **IGMP** > **IGMP Domains** に移動して、マルチキャストが有効化/無効化されたノードのドメイン情報を表示します。

NX-OS スタイルの CLI を使用したレイヤ 3 マルチキャストの設定

手順

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# configure
```

ステップ 2 テナントの設定モード、VRF の設定モードは、および PIM オプションの設定モードに入ります。

例：

```
apic1(config)# tenant tenant1
apic1(config-tenant)# vrf context tenant1_vrf
apic1(config-tenant-vrf)# ip pim
apic1(config-tenant-vrf)# ip pim fast-convergence
apic1(config-tenant-vrf)# ip pim bsr forward
```

ステップ 3 IGMP を設定し、VRF に適切な IGMP オプションを設定します。

例：

```
apic1(config-tenant-vrf)# ip igmp
apic1(config-tenant-vrf)# exit
apic1(config-tenant)# interface bridge-domain tenant1_bd
apic1(config-tenant-interface)# ip multicast
apic1(config-tenant-interface)# ip igmp allow-v3-asm
apic1(config-tenant-interface)# ip igmp fast-leave
apic1(config-tenant-interface)# ip igmp inherit interface-policy igmp_intpol1
apic1(config-tenant-interface)# exit
```

ステップ 4 テナントの L3 Out モードに入り、PIM を有効にし、リーフ インターフェイス モードに入ります。このインターフェイスの PIM を設定します。

例：

```
apic1(config-tenant)# l3out tenant1_l3out
apic1(config-tenant-l3out)# ip pim
apic1(config-tenant-l3out)# exit
apic1(config-tenant)# exit
apic1(config)#
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/125
apic1(config-leaf-if) ip pim inherit interface-policy pim_intpol1
```

ステップ 5 IGMP コマンドを使用して、インターフェイスの IGMP を設定します。

例：

```
apic1(config-leaf-if)# ip igmp fast-leave
apic1(config-leaf-if)# ip igmp inherit interface-policy igmp_intpol1
```

これにより、APIC のレイヤ 3 マルチキャストの設定を完了します。

REST API を使用したレイヤ 3 マルチキャストの設定

手順

ステップ 1 テナント、VRF を設定し、VRF のマルチキャストを有効にします。

例：

```
<fvTenant dn="uni/tn-PIM_Tenant" name="PIM_Tenant">
   <fvCtx knwMcastAct="permit" name="ctx1">
       <pimCtxP mtu="1500">
       </pimCtxP>
   </fvCtx>
  </fvTenant>
```

ステップ 2 L3 アウト設定し、L3 アウト上のマルチキャスト (PIM、IGMP) を有効にします。

例：

```
<l3extOut enforceRtctrl="export" name="l3out-pim_l3out1">
       <l3extRsEctx tnFvCtxName="ctx1"/>
       <l3extLNodeP configIssues="" name="bLeaf-CTX1-101">
         <l3extRsNodeL3OutAtt rtrId="200.0.0.1" rtrIdLoopBack="yes"
tDn="topology/pod-1/node-101"/>
         <l3extLIfP name="if-PIM_Tenant-CTX1" tag="yellow-green">
           <igmpIfP/>
           <pimIfP>
             <pimRsIfPol tDn="uni/tn-PIM_Tenant/pimifpol-pim_pol1"/>
           </pimIfP>
           <l3extRsPathL3OutAtt addr="131.1.1.1/24" ifInstT="l3-port" mode="regular"
mtu="1500" tDn="topology/pod-1/paths-101/pathep-[eth1/46]"/>
         </l3extLIfP>
       </l3extLNodeP>
       <l3extRsL3DomAtt tDn="uni/l3dom-l3outDom"/>
       <l3extInstP name="l3out-PIM_Tenant-CTX1-1topo" >
       </l3extInstP>
       <pimExtP enabledAf="ipv4-mcast" name="pim"/>
     </l3extOut>
```

ステップ 3 テナントと enable マルチキャストおよび IGMP BD で BD を設定します。

例：

```
<fvTenant dn="uni/tn-PIM_Tenant" name="PIM_Tenant">
   <fvBD arpFlood="yes" mcastAllow="yes" multiDstPktAct="bd-flood" name="bd2"
type="regular" unicastRoute="yes" unkMacUcastAct="flood" unkMcastAct="flood">
       <igmpIfP/>
       <fvRsBDToOut tnL3extOutName="l3out-pim_l3out1"/>
       <fvRsCtx tnFvCtxName="ctx1"/>
       <fvRsIgmpsn/>
      <fvSubnet ctrl="" ip="41.1.1.254/24" preferred="no" scope="private" virtual="no"/>

     </fvBD>
 </fvTenant>
```

ステップ 4 IGMP ポリシーを設定し、BD に割り当てます。

例：

```
<fvTenant dn="uni/tn-PIM_Tenant" name="PIM_Tenant">
     <igmpIfPol grpTimeout="260" lastMbrCnt="2" lastMbrRespTime="1" name="igmp_pol"
querierTimeout="255" queryIntvl="125" robustFac="2" rspIntvl="10" startQueryCnt="2"
startQueryIntvl="125" ver="v2">
     </igmpIfPol>
      <fvBD arpFlood="yes" mcastAllow="yes" name="bd2">
      <igmpIfP>
         <igmpRsIfPol tDn="uni/tn-PIM_Tenant/igmpIfPol-igmp_pol"/>
       </igmpIfP>
      </fvBD>
 </fvTenant>
```

ステップ 5 ルート マップ、PIM、および RP 設定 VRF のポリシー。

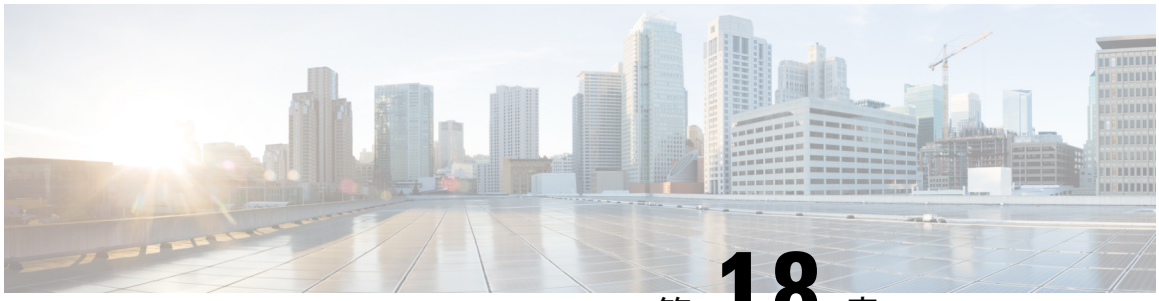
例：

```
<fvTenant dn="uni/tn-PIM_Tenant" name="PIM_Tenant">
     <pimRouteMapPol name="rootMap">
       <pimRouteMapEntry action="permit" grp="224.0.0.0/4" order="10" rp="0.0.0.0"
src="0.0.0.0/0"/>
     </pimRouteMapPol>
     <fvCtx knwMcastAct="permit" name="ctx1">
       <pimCtxP ctrl="" mtu="1500">
         <pimStaticRPPol>
           <pimStaticRPEntryPol rpIp="131.1.1.2">
             <pimRPGrpRangePol>
               <rtdmcRsFilterToRtMapPol tDn="uni/tn-PIM_Tenant/rtmap-rootMap"/>
             </pimRPGrpRangePol>
           </pimStaticRPEntryPol>
         </pimStaticRPPol>
       </pimCtxP>
   </fvCtx>
</fvTenant>
```

ステップ 6 PIM インターフェイス ポリシーを設定し、L3 アウトを適用します。

例：

```
<fvTenant dn="uni/tn-PIM_Tenant" name="PIM_Tenant">
  <pimIfPol authKey="" authT="none" ctrl="" drDelay="60" drPrio="1" helloItvl="30000"
itvl="60" name="pim_pol1"/>
  <l3extOut enforceRtctrl="export" name="l3out-pim_l3out1" targetDscp="unspecified">
       <l3extRsEctx tnFvCtxName="ctx1"/>
       <l3extLNodeP  name="bLeaf-CTX1-101">
         <l3extRsNodeL3OutAtt rtrId="200.0.0.1" rtrIdLoopBack="yes"
tDn="topology/pod-1/node-101"/>
         <l3extLIfP name="if-SIRI_VPC_src_recv-CTX1" tag="yellow-green">
           <pimIfP>
             <pimRsIfPol tDn="uni/tn-tn-PIM_Tenant/pimifpol-pim_pol1"/>
           </pimIfP>
         </l3extLIfP>
       </l3extLNodeP>
     </l3extOut>
 </fvTenant>
```



第 18 章

IGMP スヌーピング

この章の内容は、次のとおりです。

Cisco APIC および IGMP スヌーピングについて

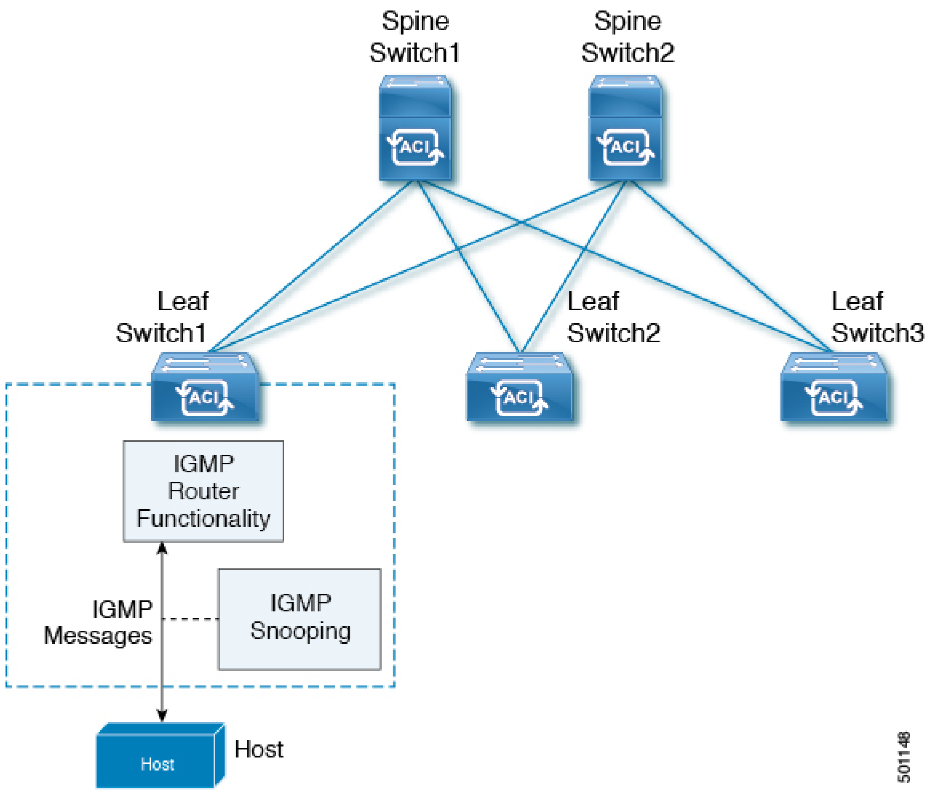
ACI ファブリックに IGMP スヌーピングを実装するには

（注） ブリッジ ドメインで IGMP スヌーピングをディセーブルにしないことを推奨します。IGMP スヌーピングをディセーブルにすると、ブリッジ ドメインで不正なフラッディングが過度に発生し、マルチキャストのパフォーマンスが低下する場合があります。

IGMP スヌーピング ソフトウェアは、ブリッジ ドメイン内の IP マルチキャスト トラフィックを調べて、該当する受信側が常駐するポートを検出します。IGMP スヌーピングではポート情報を利用することにより、マルチアクセスブリッジ ドメイン環境における帯域幅消費量を削減し、ブリッジ ドメイン全体へのフラッディングを回避します。デフォルトでは、IGMP スヌーピングがブリッジ ドメインでイネーブルにされています。

この図は、ホストへの接続を持つ ACI リーフ スイッチに含まれる IGMP ルーティング機能と IGMP スヌーピング機能を示しています。IGMP スヌーピング機能は、IGMP メンバーシップ レポートをスヌーピングし、メッセージを残し、必要な場合にのみIGMPルータ機能に転送します。

図 ***25 : IGMP*** スヌーピング機能



IGMP スヌーピングは、IGMPv1、IGMPv2、および IGMPv3 コントロール プレーン パケットの処理に関与し、レイヤ 3 コントロール プレーン パケットを代行受信して、レイヤ 2 の転送処理を操作します。

IGMP スヌーピングには、次の独自機能があります。

- 宛先および送信元の IP アドレスに基づいたマルチキャスト パケットの転送が可能な送信元フィルタリング
- MAC アドレスではなく、IP アドレスに基づいたマルチキャスト転送
- MAC アドレスに基づいた代わりのマルチキャスト転送

ACI ファブリックは、RFC 4541の2.1.1 項「IGMP 転送ルール」に記載されているガイドラインに従って、プロキシ レポーティング モードでのみ IGMP スヌーピングをサポートします。

IGMP □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□□□ □□□□□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ □□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□ IP □□□□□□□□□□□□□□□□□
□□
□□□□□□□ □□□□□□□□□□□ IGMP □□□□□□□□ □□□□□□□
□□□□ IP □□□□□□ 0.0.0.0 □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□

その結果、ACI ファブリックは送信元 IP アドレス 0.0.0.0 の IGMP レポートを送信します。

（注） IGMP スヌーピングの詳細については、RFC 4541 を参照してください。

仮想化のサポート

IGMP スヌーピングに対して、複数の仮想ルーティングおよび転送（VRF）インスタンスを定義できます。

リーフ スイッチでは、**show** コマンドに VRF 引数を指定して実行すると、表示される情報のコンテキストを確認できます。VRF 引数を指定しない場合は、デフォルト VRF が使用されます。

APIC IGMP スヌーピング機能、IGMPv1、IGMPv2、および高速リーブ機能

IGMPv1 と IGMPv2 は両方とも、メンバーシップ レポート抑制をサポートします。つまり、同一サブネット上の 2 つのホストが同一グループのマルチキャスト データを受信する場合、他方のホストからメンバー レポートを受信するホストは、そのレポートを送信しません。メンバーシップ レポート抑制は、同じポートを共有しているホスト間で発生します。

各スイッチ ポートに接続されているホストが 1 つしかない場合は、IGMPv2 の高速脱退機能を設定できます。高速脱退機能を使用すると、最終メンバーのクエリー メッセージがホストに送信されません。APIC は、IGMP 脱退メッセージを受信すると、ただちに該当するポートへのマルチキャスト データ転送を停止します。

IGMPv1 では、明示的な IGMP 脱退メッセージが存在しないため、 APIC の IGMP スヌーピング機能は、特定のグループについてマルチキャスト データを要求するホストが存続しないことを示すために、メンバーシップ メッセージ タイムアウトを使用する必要があります。

（注） 高速脱退機能がイネーブルになっている場合、他のホストの存在は確認されないため、IGMP スヌーピング機能は、最終メンバーのクエリー インターバル設定を無視します。

APIC IGMP スヌーピング ファンクション キーと IGMPv3

APIC での IGMPv3 スヌーピング ファンクションでは、完全な IGMPv3 スヌーピングがサポートされています。これにより、IGMPv3 レポートの （S、G） 情報に基づいて、抑制されたフラッディングが提供されます。この送信元ベースのフィルタリングにより、デバイスは対象のマルチキャスト グループにトラフィックを送信する送信元に基づいて、マルチキャスト トラフィックの宛先ポートを制限できます。

デフォルトでは、IGMP スヌーピング機能は、ブリッジ ドメインでは、各 VLAN ポート上のホストを追跡します。この明示的なトラッキング機能は、高速脱退メカニズムをサポートして

います。IGMPv3 ではすべてのホストがメンバーシップ レポートを送信するため、レポート抑制機能を利用すると、デバイスから他のマルチキャスト対応ルータに送信されるトラフィック量を制限できます。レポート抑制を有効にしていても、IGMPv1 または IGMPv2 ホストが同じグループをリクエストしなかった場合、IGMP スヌーピング機能はプロキシ レポートを作成します。プロキシ機能により、ダウンストリーム ホストが送信するメンバーシップ レポートからグループ ステートが構築され、アップストリーム クエリアからのクエリーに応答するためにメンバーシップ レポートが生成されます。

IGMPv3 メンバーシップ レポートには ブリッジ ドメインのグループ メンバの一覧が含まれていますが、最終ホストが脱退すると、ソフトウェアはメンバーシップ クエリーを送信します。最終メンバーのクエリー インターバルについてパラメータを設定すると、タイムアウトまでにどのホストからも応答がなかった場合、IGMP スヌーピングはグループ ステートを削除します。

Cisco APIC および IGMP スヌーピング クエリア関数

マルチキャスト トラフィックをルーティングする必要がないために、Protocol-Independent Multicast（PIM）がインターフェイス上でディセーブルになっている場合は、メンバーシップ クエリーを送信するように IGMP スヌーピング クエリア機能を設定する必要があります。APIC、IGMP スヌープ ポリシー内で定義マルチキャストのソースとレシーバが含まれているブリッジ ドメインでクエリアがないその他のアクティブなクエリアします。

Cisco ACI は、IGMP スヌーピングおよび IGMP スヌーピング クエリアを有効になっている by default(デフォルトで、デフォルトでは) があります。さらに、ブリッジ ドメイン サブネット制御は、「クエリア IP」を選択、リーフ スイッチによって、クエリアとして動作およびクエリ パケット送信を開始します。セグメントは、明示的なマルチキャスト ルータ (PIM が有効になっていません) があるないときに ACI Leaf スイッチでクエリアを有効にする必要があります。ブリッジ ドメインで、クエリアが設定されている、使用される IP アドレス マルチキャストのホストが設定されている同じサブネットからにする必要があります。

一意の IP アドレスは、簡単にクエリア機能を参照するように設定する必要があります。IGMP スヌーピング クエリア設定の一意の IP アドレスを使用して、ホスト IP アドレスまたは同じセグメント上にあるルータの IP アドレスが重複しないようにする必要があります。クエリア IP アドレスとして SVI IP アドレスを使用する必要がないか、クエリア選定の問題になります。例として、IGMP スヌーピング クエリアを使用する IP アドレスが、セグメント上の別のルータにも使用されている場合があります、IGMP クエリア選定プロトコルの問題。クエリア機能に使用される IP アドレスも使用しないでください HSRP または VRRP などの他の機能です。

（注） クエリアの IP アドレスは、ブロードキャスト IP アドレス、マルチキャスト IP アドレス、または 0（0.0.0.0）にしないでください。

IGMP スヌーピング クエリアがイネーブルな場合は、定期的に IGMP クエリーが送信されるため、IP マルチキャスト トラフィックを要求するホストから IGMP レポート メッセージが発信されます。IGMP スヌーピングはこれらの IGMP レポートを待ち受けて、適切な転送を確立します。

IGMP スヌーピング クエリアは、RFC 2236 に記述されているようにクエリア選択を実行します。クエリア選択は、次の構成で発生します。

- 異なるスイッチ上の同じ VLAN に同じサブネットに複数のスイッチ クエリアが設定されている場合。
- 設定されたスイッチ クエリアが他のレイヤ 3 SVI クエリアと同じサブネットにある場合。

APIC IGMP スヌーピング機能の注意事項と制約事項

APIC IGMP スヌーピング機能に関する注意事項および制約事項は次のとおりです:

- レイヤ 3 IPv6 マルチキャスト ルーティングはサポートされていません。
- レイヤ 2 IPv6 マルチキャスト パケットは、着信ブリッジ ドメインでフラッディングされます。

IGMP スヌーピング ポリシーの設定と割り当て

拡張 GUI のブリッジ ドメインへの IGMP スヌーピング ポリシーの設定と割り当て

IGMP スヌーピング機能を実装するには、IGMP スヌーピング ポリシーを設定し、そのポリシーを 1 つまたは複数のブリッジ ドメインに割り当てます。

GUI を使用した IGMP スヌーピング ポリシーの設定

IGMP 設定を 1 つまたは複数のブリッジ ドメインに割り当てることが可能な IGMP スヌーピング ポリシーを作成します。

手順

ステップ 1 **[テナント]** タブと、IGMPP スヌーピング サポートを設定することを意図したブリッジ ドメインのテナントの名前をクリックします。

ステップ 2 **[ナビゲーション]** ペインで、**[ネットワー キング]** > **[プロトコル ポリシー]** > **[IGMP スヌープ]** をクリックします。

ステップ 3 **[IGMP スヌープ]** を右クリックし、**[IGMP スヌープ ポリシーの作成]** を選択します。

ステップ 4 **[IGMP スヌープ ポリシーの作成]** ダイアログで、次のようにポリシーを設定します。

a) [Name] フィールドと [Description] フィールドに、ポリシーの名前と説明をそれぞれ入力します。

b) **[管理状態]** フィールドで **[有効]** または **[無効]** を選択して、このポリシー全体を有効または無効にします。

c) **[ファスト リーブ]** を選択または選択解除し、このポリシーを通してクエリが即時ドロップする IGMP V2 を有効または無効にします。

d) **[クエリアの有効化]** を選択または選択解除して、このポリシーを通して IGMP クエリア アクティビティを有効または無効にします。

（注） このオプションを効果的を有効にするには、ポリシーを適用するブリッジ ドメインに割り当てられるサブネットで **[サブネット制御: クエリア IP]** 設定も有効にする必要があります。この設定があるプロパティ ページへのナビゲーション パスは、**Tenants** > ***tenant_name*** > **Networking** > **Bridge Domains** > ***bridge_domain_name*** > **Subnets** > ***subnet_name*** です。

e) このポリシーの **[最後のメンバのクエリ間隔]** 値を秒で指定します。

IGMPv2 リーブ レポートを受信したら、IGMP がこの値を使用します。これは、少なくとも 1 個以上のホストをグループに残すことを意味します。リーブ レポートを受信した後、インターフェイスが IGMP ファスト リーブに設定されていないか確認し、されていない場合はout-of-sequence クエリを送信します。

f) このポリシーの **[クエリ間隔]** 値を秒で指定します。

この値は、グループ内でレポートを確認できない場合、IGMP 機能が特定の IGMP 状態を保存する合計時間を定義するために使用されます。

g) このポリシーの **[クエリの応答間隔]** 値を秒で指定します。

ホストがクエリ パケットを受信すると、最大応答所要時間以下のランダムな値でカウントが開始されます。このタイマーの期限が切れると、ホストはレポートで応答します。

h) このポリシーの **[クエリ カウントの開始]** を指定します。

スタートアップ クエリー インターバル中に送信される起動時のクエリー数。有効範囲は 1 ～ 10 です。デフォルトは 2 です。

i) このポリシーの **[クエリ間隔の開始]** を秒で指定します。

デフォルトでは、ソフトウェアができるだけ迅速にグループ ステートを確立できるように、このインターバルはクエリー インターバルより短く設定されています。有効範囲は 1 ～ 18,000 秒です。デフォルト値は 31 秒です。

ステップ 5 [Submit] をクリックします。`

新しい IGMP スヌープ ポリシーは、**[プロトコル ポリシー - IGMP スヌープ]** サマリ ページに一覧になっています。

次のタスク

このポリシーを有効にするには、ブリッジ ドメインに割り当てます。

GUI を使用した IGMP スヌーピング ポリシーのブリッジ ドメインへの割り当て

IGMP スヌーピング ポリシーをブリッジ ドメインに割り当てると、そのブリッジ ドメインは、そのポリシーで指定された IGMP スヌーピング ポリシーを使用するように設定されます。

始める前に

- テナントのブリッジ ドメインを設定します。
- ブリッジ ドメインにアタッチする IGMP スヌーピング ポリシーを設定します。

（注） 割り当てられるポリシーで **Enable Querier** オプションを効果的に有効にするには、ポリシーを適用するブリッジ ドメインに割り当てられるサブネットで **Subnet Control: Querier IP** 設定も有効にする必要があります。この設定があるプロパティ ページへのナビゲーション パスは、**Tenants** > ***tenant_name*** > **Networking** > **Bridge Domains** > ***bridge_domain_name*** > **Subnets** > ***subnet_name*** です。

手順

ステップ 1 テナントのブリッジ ドメインで IGMP スヌープ ポリシーを設定するには、APIC の **Tenants** タブをクリックして、テナントの名前を選択します。

ステップ 2 APIC のナビゲーション ウィンドウで **Networking** > **Bridge Domains** をクリックして、ポリシー指定の IGMP スヌープ設定を適用するブリッジ ドメインを選択します。

ステップ 3 メインの **Policy** タブで、**IGMP Snoop Policy** フィールドまでスクロールして、ドロップダウン メニューから適切な IGMP ポリシーを選択します。

ステップ 4 **Submit** をクリックします。

ターゲットのブリッジ ドメインは、指定された IGMP スヌーピング ポリシーに関連付けられます。

NX-OS スタイル CLI を使用した IGMP スヌーピング ポリシーの設定とブリッジ ドメインへの割り当て

始める前に

- IGMP スヌーピングのポリシーを消費するテナントを作成します。
- IGMP スヌーピング ポリシーを接続するテナントのブリッジ ドメインを作成します。

手順

	コマンドまたはアクション	目的
ステップ 1	デフォルト値に基づいてスヌーピング ポリシーを作成します。 例： **apic1(config-tenant)# template ip igmp snooping policy cookieCut1** **apic1(config-tenant-template-ip-igmp-snooping)# show run all** # Command: show running -config all tenant foo template ip igmp snooping policy cookieCut1 # Time: Thu Oct 13 18:26:03 2016 tenant t_10 template ip igmp snooping policy cookieCut1 ip igmp snooping no ip igmp snooping fast-leave ip igmp snooping last-member-query-interval 1 no ip igmp snooping querier ip igmp snooping query-interval 125 ip igmp snooping query-max-response-time 10 ip igmp snooping stqrtup-query-count 2 ip igmp snooping startup-query-interval 31 no description exit exit apic1(config-tenant-template-ip-igmp-snooping)#	例の NX-OS スタイル CLI シーケンス： • デフォルト値を持つ cookieCut1 という名前の IGMP スヌーピング ポリシーを作成します。 • ポリシー cookieCut1 のデフォルト IGMP スヌーピングの値が表示されます。
ステップ 2	必要に応じてスヌーピング ポリシーを変更します。 例： **apic1(config-tenant-template-ip-igmp-snooping)# ip igmp snooping query-interval 300** **apic1(config-tenant-template-ip-igmp-snooping)# show run all** # Command: show running -config all tenant foo template ip igmp snooping policy cookieCut1 #Time: Thu Oct 13 18:26:03 2016 tenant foo template ip igmp snooping policy cookieCut1 ip igmp snooping no ip igmp snooping fast-leave ip igmp snooping last-member-query-interval 1 no ip igmp snooping querier	例の NX-OS スタイル CLI シーケンス： • cookieCut1 という名前の IGMP スヌーピング ポリシーのクエリ間隔値のカスタム値を指定します。 • ポリシー cookieCut1 の変更された IGMP スヌーピング値を確認します。

	コマンドまたはアクション	目的

	`ip igmp snooping query-interval 300`
	`ip igmp snooping query-max-response-time 10`
	`ip igmp snooping stqrtup-query-count 2`
	`ip igmp snooping startup-query-interval 31`
	`no description`
	`exit`
	`exit`
	`apic1(config-tenant-template-ip-igmp-snooping)# exit`
	`apic1(config--tenant)#`	

ステップ 3	ブリッジ ドメインにポリシーを割り当てます。 **例：** **`apic1(config-tenant)# int bridge-domain bd3`** **`apic1(config-tenant-interface)# ip igmp snooping policy cookieCut1`**	例の NX-OS スタイル CLI シーケンス： • ブリッジ ドメインの BD3 に移動します。IGMP スヌーピング ポリシーのクエリ間隔値は cookieCut1 という名前です。 • ポリシー cookieCut1 の変更された IGMP スヌーピングの値を持つ IGMP スヌーピングのポリシーを割り当てます。

次のタスク

複数のブリッジ ドメインに IGMP スヌーピングのポリシーを割り当てることができます。

REST API を使用したブリッジ ドメインへの IGMP スヌーピング ポリシーの設定と割り当て

手順

IGMP スヌーピング ポリシーを設定してブリッジ ドメインに割り当てるには、次の例のように XML で POST を送信します。

例：

```
https://apic-ip-address/api/node/mo/uni/.xml
<fvTenant name="mcast_tenant1">

<!-- Create an IGMP snooping template, and provide the options -->
<igmpSnoopPol name="igmp_snp_bd_21"
              adminSt="enabled"
              lastMbrIntvl="1"
              queryIntvl="125"
              rspIntvl="10"
```

```
              startQueryCnt="2"
              startQueryIntvl="31"
              />
<fvCtx name="ip_video"/>

<fvBD name="bd_21">
  <fvRsCtx tnFvCtxName="ip_video"/>

  <!-- Bind IGMP snooping to a BD -->
  <fvRsIgmpsn tnIgmpSnoopPolName="igmp_snp_bd_21"/>
</fvBD></fvTenant>
```

この例では、次のプロパティで IGMP スヌーピング ポリシー、igmp_snp_bd_12 を作成および設定し、IGNPポリシー、igmp_snp_bd_12 をブリッジ ドメイン bd_21 にバインドします。

- 管理状態が有効です。
- 最後のメンバ クエリ間隔は、デフォルトでは、1 秒です。
- クエリ間隔は、デフォルトでは 125 です。
- クエリの応答間隔はデフォルトでは 10 秒です。
- クエリの開始カウントは、デフォルトでは 2 メッセージです。
- クエリの開始間隔は 35 秒です。

IGMP スヌーピングの静的ポート グループの有効化

静的ポート グループの IGMP スヌーピングを有効にする

IGMP静的ポートのグループ化により以前アプリケーションEPGに静的に割り当てられた事前プロビジョニングを有効にして、スイッチ ポートが IGMP マルチキャスト トラフィックを受信および処理できます。この事前プロビジョニングは、通常 IGMP スヌーピング スタックがポートを動的に学習するときに発生する参加遅延を防止します。

静的グループ メンバーシップは、アプリケーション EPG に割り当てられている静的ポートでのみ事前プロビジョニングできます。

APIC GUI、CLI、および REST API インターフェイスを通じて、静的グループ メンバーシップを設定できます。

前提条件: 静的ポートに EPG を導入する

ポートでIGMPスヌープ処理を有効にするには、前提条件として、ターゲットのポートを、関連付けられている EPG に静的に割り当てる必要があります。

ポートの静的な導入は、APIC GUI、CLI、または REST API インターフェイスを通じて構成できます。詳細については、 『*Cisco APIC* レイヤ *3* の設定ガイド』の次のトピックを参照してください:

- *GUI* を使用した *APIC* の特定のポートへの *EPG* の導入
- *NX-OS* スタイルの *CLI* を使用した *APIC* の特定のポートへの *EPG* の導入
- *REST API* を使用した *APIC* の特定のポートへの *EPG* の導入

GUI を使用した、スタティック ポートでの IGMP スヌーピングとマルチキャストの有効化

IGMP スヌーピングとマルチキャストは、EPG に静的に割り当てられているポートで有効にできます。その後、これらのポートで有効にされている IGMP スヌーピングとマルチキャストへのアクセスを許可または拒否されるユーザのアクセス グループを作成し、割り当てることができます。

始める前に

EPG の IGMP スヌーピングおよびマルチキャストを有効にする前に、次のタスクを実行します:

- この機能を有効にし、その EPG に静的に割り当てるインターフェイスを指定します。

（注） 静的ポート割り当ての詳細については、 *GUI* を使用した *APIC* の特定のポートへの *EPG* の導入 を参照してください。

- IGMP スヌーピングとマルチキャスト トラフィックの受信者とする IP アドレスを指定します。

手順

ステップ 1 **Tenant** > ***tenant_name*** > **Application Profiles** > ***application_name*** > **Application EPGs** > ***epg_name*** > **Static Ports** をクリックします。

このスポットに移動すると、ターゲット EPG に静的に割り当てたすべてのポートが表示されます。

ステップ 2 IGMP スヌーピングのグループ メンバーに静的に割り当てるポートをクリックします。
Static Path ページが表示されます。

ステップ 3 IGMP スヌープ スタティック グループの表で、+ をクリックして、IGMP スヌープ アドレス グループにエントリを追加します。

IGMP スヌープアドレス グループにエントリを追加すると、ターゲットの静的ポートが指定されたマルチキャスト IP アドレスに関連付けられ、そのアドレスで受信した IGMP スヌープ トラフィックを処理できるようになります。

a) **Group Address** フィールドに、このインターフェイスとこの EPG に関連付けるマルチキャスト IP アドレスを入力します。
b) 当てはまる場合には、**Source Address** フィールドに、マルチキャスト ストリームの送信元となる IP アドレスを入力します。
c) **Submit** をクリックします。

設定が完了したら、ターゲットインターフェイスは、それに関連付けられているマルチキャスト IP アドレスに送信される IGMP スヌーピング プロトコル トラフィックを処理できるようになります。

（注） ターゲットのスタティック ポートにさらにマルチ キャスト アドレスを関連付けるには、この手順を繰り返します。

ステップ 4 [送信（Submit）] をクリックします。

NX-OS スタイル CLI によりスタティック ポートで IGMP スヌーピングおよびマルチキャストの有効化

EPG に静的に割り当てられたポートで IGMP スヌーピングおよびマルチキャストをイネーブルにできます。それらのポートで有効な IGMP スヌーピングおよびマルチキャスト トラフィックへのアクセスを許可または拒否するアクセス ユーザーのグループを作成および割り当てることができます。

このタスクで説明されている手順には、次のエンティティの事前設定を前提とします。

- テナント：tenant_A
- アプリケーション：application_A
- EPG：epg_A
- ブリッジ ドメイン：bridge_domain_A
- vrf：vrf_A -- a member of bridge_domain_A
- VLAN ドメイン：vd_A（300 ～ 310 の範囲で設定される）
- リーフ スイッチ：101 およびインターフェイス 1/10

  スイッチ 101 のターゲット インターフェイス 1/10 が VLAN 305 に関連付けられており、enant_A、application_A、epg_A に静的にリンクされています。
- リーフ スイッチ：101 およびインターフェイス 1/11

  スイッチ 101 のターゲット インターフェイス 1/11 が VLAN 309 に関連付けられており、enant_A、application_A、epg_A に静的にリンクされています。

始める前に

EPG に IGMP スヌーピングおよびマルチキャストを有効にする前に、次のタスクを実行します。

- この機能を有効にして静的に EPG に割り当てるインターフェイスを特定する

（注） スタティック ポートの割り当てに関する詳細は、「*Cisco APIC* レイヤ *3* 設定ガイド」の「*NX-OS* スタイル *CLI* を使用した *APIC* で特定のポートの *EPG* を展開する」を参照してください。

- IGMP スヌーピング マルチキャスト トラフィックの受信者の IP アドレスを特定します。

手順

	コマンドまたはアクション	目的

ステップ 1	ターゲット インターフェイスで IGMP スヌーピングおよびレイヤ2マルチキャスティングを有効にします
	例：
	`apic1# conf t`
	`apic1(config)# tenant tenant_A`
	`apic1(config-tenant)# application application_A`
	`apic1(config-tenant-app)# epg epg_A`
	`apic1(config-tenant-app-epg)# ip igmp snooping static-group 225.1.1.1 leaf 101 interface ethernet 1/10 vlan 305`
	`apic1(config-tenant-app-epg)# end`
	
	`apic1# conf t`
	`apic1(config)# tenant tenant_A; application application_A; epg epg_A`
	`apic1(config-tenant-app-epg)# ip igmp snooping static-group 227.1.1.1 leaf 101 interface ethernet 1/11 vlan 309`
	`apic1(config-tenant-app-epg)# exit`
	`apic1(config-tenant-app)# exit`
		例のシーケンスでは次を有効にします。
		• 静的にリンクされているターゲット インターフェイス 1/10 の IGMP スヌーピング、そしてマルチキャスト IP アドレス、225.1.1.1 に関連付けます
		• 静的にリンクされているターゲット インターフェイス 1/11 の IGMP スヌーピング、そしてマルチキャスト IP アドレス、227.1.1.1 に関連付けます

REST API を使用した静的ポートでの IGMP スヌーピングとマルチキャストの有効化

EPG に静的に割り当てられているポートで、IGMP スヌーピングおよびマルチキャスト処理を有効にできます。それらのポートで有効な IGMP スヌープおよびマルチキャスト トラフィックへのアクセスを許可または拒否するアクセス ユーザーのグループを作成および割り当てることができます。

手順

スタティック ポートでアプリケーション EPG を設定するには、それらのポートを IGMP スヌーピングおよびマルチキャスト トラフィックを受信し処理するように有効にして、グループをアクセスに割り当てるかトラフィックへのアクセスを拒否するように割り当て、次の例のように XML で POST を送信します。

次の例では、IGMP スヌーピングが VLAN 202 上の leaf 102 インターフェイス 1/10 で有効になっています。マルチキャスト IP アドレス 224.1.1.1 および 225.1.1. がこのポートに関連付けられます。

例：

```
https://apic-ip-address/api/node/mo/uni/.xml
<fvTenant name="tenant_A">
  <fvAp name="application">
    <fvAEPg name="epg_A">
      <fvRsPathAtt encap="vlan-202" instrImedcy="immediate" mode="regular"
tDn="topology/pod-1/paths-102/pathep-[eth1/10]">
        <!-- IGMP snooping static group case -->
        <igmpSnoopStaticGroup group="224.1.1.1" source="0.0.0.0"/>
        <igmpSnoopStaticGroup group="225.1.1.1" source="2.2.2.2"/>
      </fvRsPathAtt>
    </fvAEPg>
  </fvAp>
</fvTenant>
```

IGMP スヌープ アクセス グループの有効化

IGMP スヌープ アクセス グループの有効化

「アクセス-グループ」ができるストリームを制御するために使用任意ポート背後に参加します。

実際に所属するするポートの設定を適用できることを確認するには、アプリケーション EPG に静的に割り当てられているインターフェイスでアクセス グループ設定を適用できる EPG。

ルート マップ ベースのアクセス グループのみが許可されます。

APIC GUI、CLI、および REST API インターフェイスを通じて、IGMP スヌープ アクセス グループを設定できます。

GUI を使用して、IGMP スヌーピングとマルチキャストへのグループ アクセスを有効にする

EPGに静的に割り当てられたポートでIGMPスヌーピングとマルチキャストを有効にしたら、ユーザのアクセス グループを作成して割り当て、それらのポートで有効にされたIGMPスヌーピングとマルチキャスト トラフィックへのアクセスを許可または拒否することができます。

始める前に

EPGにIGMPスヌーピングおよびマルチキャストへのアクセスを有効にする前に、この機能を有効にし、それらを静的に EPG に割り当てるインターフェイスを識別します。

（注） 静的ポート割り当ての詳細については、「*Deploying an EPG on a Specific Port with APIC Using the GUI*」を参照してください。

手順

ステップ 1 **Tenant** > ***tenant_name*** > **Application Profiles** > ***application_name*** > **Application EPGs** > ***epg_name*** > **Static Ports** をクリックします。

このスポットに移動すると、ターゲット EPG に静的に割り当てたすべてのポートが表示されます。

ステップ 2 マルチキャスト グループ アクセスを割り当てる予定のポートをクリックして、 **Static Port Configuration** ページを表示します。

ステップ 3 **Actions** > **Create IGMP Snoop Access Group** をクリックして、IGMP スヌープ アクセス グループ テーブルを表示します

ステップ 4 IGMP スヌープ アクセス グループのテーブルで + をクリックして、アクセスグループのエントリを追加します。

IGMPスヌープアクセス グループのエントリを追加すると、このポートへのアクセス権を持つユーザ グループを作成すること、それをマルチキャスト IP アドレスと関連付け、そのアドレスで受信された IGMP スヌープ トラフィックへのグループ アクセスを許可または拒否することができます。

a) **Create Route Map Policy** を選択して、**Create Route Map Policy** ウィンドウを表示します。
b) **Name** フィールドで、マルチキャスト トラフィックの許可または拒否の対象となるグループの名前を割り当てます。
c) **Route Maps** テーブルで、+ をクリックして、ルート マップ ダイアログを表示します:
d) **Order** フィールドでは、このインターフェイスに対して複数のアクセス グループを設定している場合に、このインターフェイスでのマルチキャスト トラフィックへのアクセスをどの順序で許可または拒否するかを反映する番号を選択します。番号の小さいアクセス グループの方が、番号の大きいアクセス グループよりも前の順番になります。

e) **Group IP** フィールドには、このアクセス グループに対してトラフィックが許可または阻止される、マルチキャスト IP アドレスを入力します。
f) **Source IP** フィールドでは、当てはまる場合に、送信元の IP アドレスを入力します。
g) **Action** フィールドでは、ターゲット グループのアクセスを拒否する場合には **Deny** を、ターゲット グループのアクセスを許可する場合には **Permit** を選択します。
h) **OK** をクリックします。
i) **Submit** をクリックします。

設定が完了すると、設定されている IGMP のスヌープ アクセス グループは、 ターゲットの静的ポートと、そのアドレスで受信したマルチキャスト ストリームへの許可または拒否アクセスを通して、マルチキャスト IP アドレスに割り当てられます。

（注）
- その他のアクセス グループを設定し、ターゲットの静的ポートを通してマルチキャスト IP アドレスに関連付けるには、この手順を繰り返します。
- 構成されているアクセス グループの設定を確認するには、**Tenant** > ***tenant_name*** > **Networking** > > **Protocol Policies** > **Route Maps** > ***route_map_access_group_name*** を選択します。

ステップ 5 [送信（Submit）] をクリックします。

NX-OS スタイル CLI を使用した IGMP スヌーピングおよびマルチ キャスト グループへのアクセスの有効化

EPGに静的に割り当てられたポートでIGMPスヌーピングおよびマルチキャストを有効にした後、それらのポートで有効なIGMPスヌーピングおよびマルチキャスト トラフィックへのアクセスを許可または拒否するユーザーのアクセス グループを作成および割り当てできます。

このタスクで説明されている手順には、次のエンティティの事前設定を前提とします。

- テナント：tenant_A
- アプリケーション：application_A
- EPG：epg_A
- ブリッジ ドメイン：bridge_domain_A
- vrf：vrf_A -- a member of bridge_domain_A
- VLAN ドメイン：vd_A（300 ～ 310 の範囲で設定される）
- リーフ スイッチ：101 およびインターフェイス 1/10

  スイッチ 101 のターゲット インターフェイス 1/10 が VLAN 305 に関連付けられており、enant_A、application_A、epg_A に静的にリンクされています。
- リーフ スイッチ：101 およびインターフェイス 1/11

スイッチ 101 のターゲット インターフェイス 1/11 が VLAN 309 に関連付けられており、enant_A、application_A、epg_A に静的にリンクされています。

（注） スタティック ポートの割り当てに関する詳細は、「*Cisco APIC* レイヤ *2* 設定ガイド」の「*NX-OS* スタイル *CLI* を使用した *APIC* で特定のポートの *EPG* を展開する」を参照してください。

手順

	コマンドまたはアクション	目的

ステップ 1	route-map「アクセス グループ」を定義します。
	例：
	`apic1# conf t`
	`apic1(config)# tenant tenant_A; application application_A; epg epg_A`
	`apic1(config-tenant)# route-map fooBroker permit`
	`apic1(config-tenant-rtmap)# match ip multicast group 225.1.1.1/24`
	`apic1(config-tenant-rtmap)# exit`
	
	`apic1(config-tenant)# route-map fooBroker deny`
	`apic1(config-tenant-rtmap)# match ip multicast group 227.1.1.1/24`
	`apic1(config-tenant-rtmap)# exit`
		例のシーケンスを設定します。
		• マルチキャスト グループ 225.1.1.1/24 にリンクされる Route-map-access グループ「foobroker」のアクセスが許可されています。
		• マルチキャスト グループ 225.1.1.1/24 にリンクされる Route-map-access グループ「foobroker」のアクセスが拒否されています。

ステップ 2	ルート マップ設定を確認します。
	例：
	`apic1(config-tenant)# show running-config tenant test route-map fooBroker`
	`# Command: show running-config tenant test route-map fooBroker`
	`# Time: Mon Aug 29 14:34:30 2016`
	`tenant test`
	`route-map fooBroker permit 10`
	`match ip multicast group 225.1.1.1/24`
	`exit`
	`route-map fooBroker deny 20`
	`match ip multicast group 227.1.1.1/24`
	`exit`
	`exit`	

ステップ 3	アクセス グループ接続パスを指定します。 **例**：	例のシーケンスを設定します。 • リーフ スイッチ 101、インターフェイス 1/10、VLAN 305 で接続されて

	コマンドまたはアクション	目的
	apic1(config-tenant)# application application_A apic1(config-tenant-app)# epg epg_A apic1(config-tenant-app-epg)# ip igmp snooping access-group route-map fooBroker leaf 101 interface ethernet 1/10 vlan 305 apic1(config-tenant-app-epg)# ip igmp snooping access-group route-map newBroker leaf 101 interface ethernet 1/10 vlan 305	いる Route-map-access グループ「foobroker」。 • リーフ スイッチ 101、インターフェイス 1/10、VLAN 305 で接続されている Route-map-access グループ「newbroker」。
ステップ 4	アクセスグループ接続を確認します。 **例：** apic1(config-tenant-app-epg)# show run # Command: show running-config tenant tenant_A application application_A epg epg_A # Time: Mon Aug 29 14:43:02 2016 tenant tenent_A application application_A epg epg_A bridge-domain member bridge_domain_A ip igmp snooping access-group route-map fooBroker leaf 101 interface ethernet 1/10 vlan 305 ip igmp snooping access-group route-map fooBroker leaf 101 interface ethernet 1/11 vlan 309 ip igmp snooping access-group route-map newBroker leaf 101 interface ethernet 1/10 vlan 305 ip igmp snooping static-group 225.1.1.1 leaf 101 interface ethernet 1/10 vlan 305 ip igmp snooping static-group 225.1.1.1 leaf 101 interface ethernet 1/11 vlan 309 exit exit exit	

IGMP スヌーピングを REST API を使用するマルチ キャスト グループのアクセスを有効化

IGMP を有効にした後にスヌーピングおよび、EPG に静的に割り当てられているポートでマルチキャストすることができますし、作成を許可または IGMP スヌーピングへのアクセスを拒否するユーザのアクセスのグループを割り当てるおよびマルチキャスト トラフィックは、これらのポートで有効になっています。

手順

アクセスグループを定義する `F23broker` 、送信 XML で post このような次の例のよ。

例は、設定アクセスグループ `F23broker` tenant_A、Rmap_A、application_A、リーフ 102、1/10、インターフェイス VLAN 202 で、epg_A に関連付けられている。Rmap_A、アクセスグループとの関連付けによって `F23broker` マルチキャスト アドレス 226.1.1.1/24 で受信したマルチキャスト トラフィックへのアクセスがあり、マルチキャスト アドレス 227.1.1.1/24 で受信したトラフィックへのアクセスは拒否されます。

例：

```
<!-- api/node/mo/uni/.xml --> <fvTenant name="tenant_A"> <pimRouteMapPol name="Rmap_A">
<pimRouteMapEntry action="permit" grp="226.1.1.1/24" order="10"/> <pimRouteMapEntry action="deny"
grp="227.1.1.1/24" order="20"/> </pimRouteMapPol> <fvAp name="application_A"> <fvAEPg
name="epg_A"> <fvRsPathAtt encap="vlan-202" instrImedcy="immediate" mode="regular"
tDn="topology/pod-1/paths-102/pathep-[eth1/10]"> <!-- IGMP snooping access group case -->
<igmpSnoopAccessGroup name="F23broker"> <igmpRsSnoopAccessGroupFilterRMap
tnPimRouteMapPolName="Rmap_A"/> </igmpSnoopAccessGroup> </fvRsPathAtt> </fvAEPg> </fvAp>
</fvTenant>
```

第 19 章

HSRP

この章は、次の項で構成されています。

HSRP について

HSRP はファーストホップ冗長プロトコル（FHRP）であり、ファーストホップ IP ルータの透過的なフェールオーバーを可能にします。HSRP は、デフォルト ルータの IP アドレスを指定して設定された、イーサネット ネットワーク上の IP ホストにファーストホップ ルーティングの冗長性を提供します。ルータ グループでは HSRP を使用して、アクティブ ルータおよびスタンバイ ルータを選択します。ルータ グループでは、アクティブ ルータはパケットをルーティングするルータであり、スタンバイ ルータはアクティブ ルータに障害が発生したときや、プリセット条件に達したときに使用されるルータです。

大部分のホストの実装では、ダイナミックなルータ ディスカバリ メカニズムをサポートしていませんが、デフォルトのルータを設定することはできます。すべてのホスト上でダイナミックなルータ ディスカバリ メカニズムを実行するのは、管理上のオーバーヘッド、処理上のオーバーヘッド、セキュリティ上の問題など、さまざまな理由で現実的ではありません。HSRP は、そうしたホストにフェールオーバー サービスを提供します。

HSRP を使用するとき、ホストのデフォルト ルータとして HSRP 仮想 IP アドレスを設定します（実際のルータ IP アドレスの代わりに）。仮想 IP アドレスは、HSRP が動作するルータのグループで共有される IPv4 または IPv6 アドレスです。

ネットワーク セグメントに HSRP を設定する場合は、HSRP グループ用の仮想 MAC アドレスと仮想 IP アドレスを設定します。グループの各 HSRP 対応インターフェイス上で、同じ仮想アドレスを指定します。各インターフェイス上で、実アドレスとして機能する固有の IP アドレスおよび MAC アドレスも設定します。HSRP はこれらのインターフェイスのうちの 1 つをアクティブ ルータにするために選択します。アクティブ ルータは、グループの仮想 MAC アドレス宛てのパケットを受信してルーティングします。

指定されたアクティブ ルータで障害が発生すると、HSRP によって検出されます。その時点で、選択されたスタンバイ ルータが HSRP グループの MAC アドレスおよび IP アドレスの制御を行うことになります。HSRP はこの時点で、新しいスタンバイ ルータの選択も行います。

HSRP ではプライオリティ指示子を使用して、デフォルトのアクティブ ルータにする HSRP 設定インターフェイスを決定します。アクティブ ルータとしてインターフェイスを設定するには、グループ内の他のすべての HSRP 設定インターフェイスよりも高いプライオリティを与えます。デフォルトのプライオリティは 100 なので、それよりもプライオリティが高いインターフェイスを 1 つ設定すると、そのインターフェイスがデフォルトのアクティブ ルータになります。

HSRP が動作するインターフェイスは、マルチキャスト ユーザ データグラム プロトコル（UDP）ベースの hello メッセージを送受信して、障害を検出し、アクティブおよびスタンバイ ルータを指定します。アクティブ ルータが設定された時間内に hello メッセージを送信できなかった場合は、最高のプライオリティのスタンバイ ルータがアクティブ ルータになります。アクティブ ルータとスタンバイ ルータ間のパケット フォワーディング機能の移動は、ネットワーク上のすべてのホストに対して完全に透過的です。

1 つのインターフェイス上で複数の HSRP グループを設定できます。仮想ルータは物理的には存在しませんが、相互にバックアップするように設定されたインターフェイスにとって、共通のデフォルト ルータになります。アクティブ ルータの IP アドレスを使用して、LAN 上でホストを設定する必要はありません。代わりに、仮想ルータの IP アドレス（仮想 IP アドレス）をホストのデフォルト ルータとして設定します。アクティブ ルータが設定時間内に hello メッセージを送信できなかった場合は、スタンバイ ルータが引き継いで仮想アドレスに応答し、アクティブ ルータになってアクティブ ルータの役割を引き受けます。ホストの観点からは、仮想ルータは同じままです。

（注） ルーテッド ポートで受信した HSRP 仮想 IP アドレス宛のパケットは、ローカル ルータ上で終端します。そのルータがアクティブ HSRP ルータであるのかスタンバイ HSRP ルータであるのかは関係ありません。このプロセスには ping トラフィックと Telnet トラフィックが含まれます。レイヤ 2（VLAN）インターフェイスで受信した HSRP 仮想 IP アドレス宛のパケットは、アクティブ ルータ上で終端します。

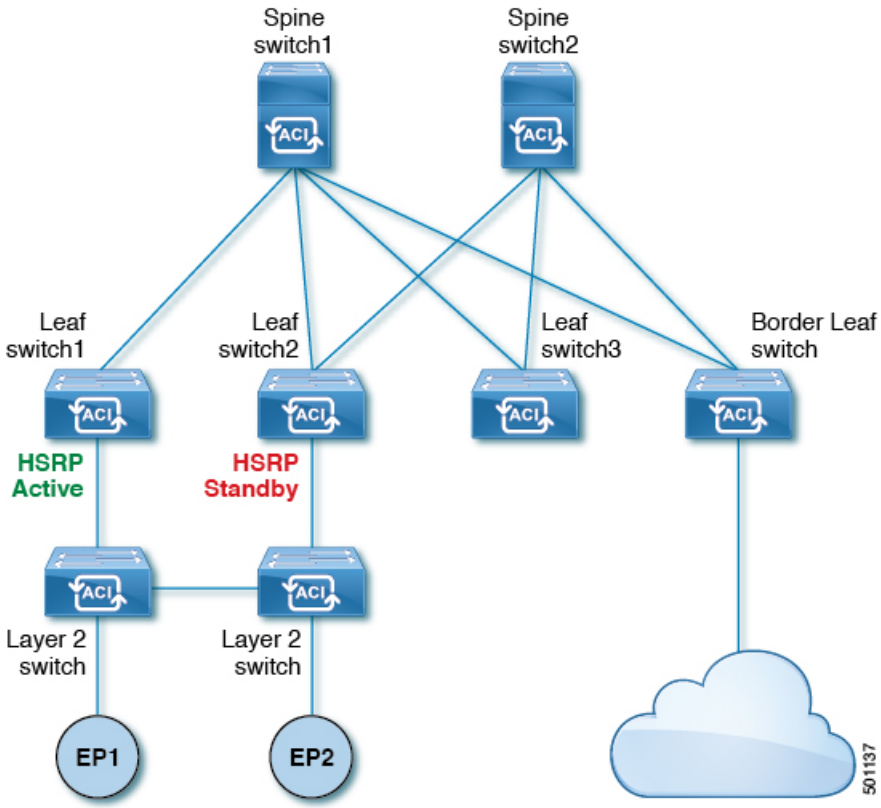
Cisco APIC と HSRP について

Cisco ACI の HSRP は、ルーテッド インターフェイスまたはサブインターフェイスでのみサポートされます。したがって HSRP は、レイヤ 3 Out でのみ設定できます。レイヤ 2 接続は、HSRP

を実行している ACI リーフ スイッチ間のレイヤ 2 スイッチなどの外部デバイスから提供される必要があります。HSRP は外部レイヤ 2 接続上で Hello メッセージを交換するリーフ スイッチ上で動作するからです。HSRP の hello メッセージは、スパイン スイッチではパス スルーされません。

次に示すのは、Cisco APIC での HSRP の導入のトポロジの例です。

図 *26 : HSRP* の配置トポロジ



HSRP のバージョン

Cisco APICは、デフォルトで HSRP バージョン 1 をサポートします。HSRP バージョン 2 を使用するようにインターフェイスを設定できます。

HSRP バージョン 2 では、HSRP バージョン 1 から次のように拡張されています。

- グループ番号の範囲が拡大されました。HSRP バージョン 1 がサポートするグループ番号は 0 ～ 255 です。HSRP バージョン 2 がサポートするグループ番号は 0 ～ 4095 です。
- IPv4 では、HSRP バージョン 1 で使用する IP マルチキャスト アドレス 224.0.0.2 の代わりに、IPv4 マルチキャスト アドレス 224.0.0.102 または IPv6 マルチキャスト アドレス FF02::66 を使用して hello パケットを送信します。

- IPv4 では 0000.0C9F.F000 ～ 0000.0C9F.FFFF、IPv6 アドレスでは 0005.73A0.0000 ～ 0005.73A0.0FFF の MAC アドレス範囲を使用します。HSRP バージョン 1 で使用する MAC アドレス範囲は、0000.0C07.AC00 ～ 0000.0C07.ACFF です。

注意事項と制約事項

次の注意事項と制約事項に従ってください。

- HSRP 状態は、HSRP IPv4 および IPv6 の両方で同じである必要があります。フェールオーバー後に同じ状態になるようにするには、プライオリティとプリエンプションを設定する必要があります。
- 現在、1 個の IPv4 と 1 個の IPv6 グループのみが Cisco ACI の同じサブインターフェイスでサポートされています。デュアル スタックが設定されている場合でも、仮想 MAC は IPv4 および IPv6 HSRP の設定で同じである必要があります。
- HSRP ピアに接続しているネットワークが純粋なレイヤ 2 ネットワークである場合、BFD IPv4 および IPv6 がサポートされています。リーフ スイッチでは、別のルータの MAC アドレスを設定する必要があります。BFD セッションは、リーフ インターフェイスで異なる MAC アドレスを設定する場合にのみアクティブになります。
- ユーザーは、デュアル スタック設定の IPv4 および IPv6 HSRP グループに同じ MAC アドレスを設定する必要があります。
- HSRP VIP はインターフェイス IP と同じサブネット内にある必要があります。
- HSRP 設定のインターフェイス遅延を設定することをお勧めします。
- HSRPは、ルーテッドインターフェイスまたはサブインターフェイスでのみサポートされます。HSRPは、VLANインターフェイスおよびスイッチ済み仮想インターフェイス（SVI）ではサポートされていません。したがって、HSRP の VPC サポートは使用できません。
- HSRP のオブジェクト トラッキングはサポートされていません。
- SNMP の HSRP 管理情報ベース（MIB）はサポートされません。
- HSRP では、複数グループの最適化（MGO） はサポートされていません。
- ICMP IPv4 および IPv6 のリダイレクトはサポートされていません。
- Cold Standby および Non-Stop Forwarding（NSF）は、Cisco ACI 環境で再起動できないためサポートされていません。
- HSRPはリーフ スイッチでのみサポートされているため、拡張ホールドダウン タイマーのサポートはありません。HSRP はスパイン スイッチでサポートされていません。
- APIC 内では、HSRP のバージョン変更はサポートされていません。設定を削除し、新しいバージョンを再設定する必要があります。

- HSRP バージョン 2 は HSRP バージョン 1 と相互運用できません。どちらのバージョンも相互に排他的なので、インターフェイスはバージョン 1 およびバージョン 2 の両方を運用できません。しかし、同一ルータの異なる物理インターフェイス上であれば、異なるバージョンを実行できます。
- ルート セグメンテーションは、HSRP がインターフェイスでアクティブな場合、Cisco Nexus 93128TX、Cisco Nexus 9396PX、および Cisco Nexus 9396TX リーフ スイッチでプログラムされています。したがって、インターフェイスでルート パケットに実施する DMAC=router MAC チェックはありません。この制限は、Cisco Nexus 93180LC EX、Cisco Nexus 93180YC-EX、Cisco Nexus 93108TC EX リーフ スイッチには適用されません。
- HSRP 設定は、基本的な GUI モードではサポートされていません。APIC リリース 3.0 (1) 以降、基本的な GUI モードが廃止されました。
- ファブリックからレイヤ 3 アウト トラフィックは、状態に関係なく HSRP リーフ スイッチ全体で常にロード バランスします。HSRP リーフ スイッチが複数のポッドにわたる場合、ファブリックからアウト トラフィックは同じポッドで常にリーフ スイッチを使用します。
- この制限は、以前の Cisco Nexus 93128TX、Cisco Nexus 9396PX と Cisco Nexus 9396TX スイッチの一部に適用されます。HSRP を使用すると、レイヤ 2 の外部デバイスのフラッピングを防ぐため、ルーテッド インターフェイスまたはルーテッド サブインターフェイスの MAC アドレスを 1 個変更する必要があります。これは、インターフェイス論理プロファイルの下で論理インターフェイスごとに Cisco APIC が同じ MAC アドレス（00:22:BD:F8:19:FF）を割り当てるためです。

デフォルトの HSRP 設定

パラメータ	デフォルト値
Version	1
Delay	0
Reload Delay	0
Interface Control	No 使用-焼き込みアドレス (BIA)
Group ID	0
Group Af	IPv4
IP Obtain Mode	admin
プライオリティ（Priority）	100
Hello Interval	3000 ミリ秒
Hold Interval	10000 ミリ秒

パラメータ	デフォルト値
Group Control	プリエンプションは無効
Preempt Delay	0
Authentication Type	プレーン テキスト
Authentication Key Timeout	0
VMAC	導出方法 (HSRP グループ Id)

GUI を使用した HSRP の設定

リーフ スイッチが設定されている場合、HSRP が有効になっています。

始める前に

- テナントと VRF が設定されています。
- VLAN プールは、適切な VLAN 範囲が定義され、レイヤ 3 ドメインが作成されて VLAN プールに接続されている状態で設定される必要があります。
- エンティティ プロファイルの接続も、レイヤ3 ドメインに関連付けられている必要があります。
- リーフ スイッチのインターフェイス プロファイルは必要に応じて設定する必要があります。

手順

ステップ 1 メニュー バーで、 > **Tenants** > **Tenant_name** をクリックします。**Navigation** ペインで、**Networking** > **External Routed Networks** > **External Routed Network_name** > **Logical Node Profiles** > **Logical Interface Profile** をクリックします。

ここで、HSRP インターフェイス プロファイルが作成されます。

ステップ 2 論理インターフェイス プロファイルを選択し、**Create HSRP Interface Profile** をクリックします。

ステップ 3 **Create HSRPInterface Profile** ダイアログボックスで、次の操作を実行します。

a) **Version** フィールドで、該当するバージョンを選択します。
b) **HSRP Interface Policy** フィールドで、ドロップダウンから **Create HSRP Interface Policy** を選択します。
c) **Create HSRP Interface Policy** ダイアログボックスの **Name** フィールドに、ポリシーの名前を入力します。
d) **Control** フィールドで、該当するコントロールを選択します。

e) **Delay** フィールドと **Reload Delay** フィールドで、該当する値を設定します。**Submit** をクリックします。

HSRPインターフェイスポリシーが作成され、インターフェイスプロファイルに関連付けられます。

ステップ 4 **Create HSRP Interface Profile** ダイアログボックスで、 **HSRP Interface Groups** を展開します。

ステップ 5 **Create HSRP Group 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、HSRP インターフェイスのグループ名を入力します。

b) **Group ID** フィールドで、適切な ID を選択します

使用可能な値は、HSRP バージョン 1 または 2 のバージョンのいずれがインターフェイスプロファイルに選択されたかに応じて異なります。

c) **IP** フィールドに、IP アドレスを入力します。

この IP アドレスはインターフェイスと同じサブネット内になければなりません。

d) **MAC Address** フィールドに、Mac アドレスを入力します。

e) **Group Name** フィールドにグループ名を入力します。

これは、HSRP MGO 機能の HSRP により、プロトコルで使用する名前です。

f) **Group Type** フィールドで、該当するタイプを選択します。

g) **IP Obtain Mode** フィールドで、該当するモードを選択します。

h) **HSRP Interface Policy** フィールドで、ドロップダウンから **Create HSRP Interface Policy** を選択します。

ステップ 6 **Create HSRP Group 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、HSRP グループポリシーの名前を入力します。

b) **Key or Password** フィールドが自動的に設定されます。

認証タイプのデフォルト値はシンプルで、キーは、「cisco」です。これはユーザーが新規ポリシーを作成するときに、デフォルトで選択されます。

c) **Type** フィールドで、必要とするセキュリティのレベルを選択します。

d) **Priority** フィールドで、アクティブ ルータとスタンバイ ルータを定義する優先度を選択します。

e) 残りのフィールドで、該当する値を選択し、**Submit** をクリックします。
HSRP グループ ポリシーが作成されます。

f) **Secondary Virtual IPs** フィールドに自動記入することにより、セカンダリ バーチャル IP を作成します。

これは、セカンダリ バーチャル IP で各サブインターフェイスで HSRP を有効にするために使用できます。また、ここで指定するIPアドレスは、インターフェイスのサブネットになければなりません。

g) **OK** をクリックします。

ステップ 7 **Create HSRP Interface Profile** ダイアログボックスで、**Submit** をクリックします。
これで HSRP の設定は完了です。

ステップ 8 ナビゲーション ペインで、作成した HSRP インターフェイスとグループ ポリシーを確認するには、**Networking** > **Protocol Policies** > **HSRP** をクリックします。

NX-OS スタイル CLI での Cisco APIC を使用してインライン パラメータで HSRP の設定

リーフ スイッチが設定されている場合、HSRP が有効になっています。

始める前に

- テナントと VRF が設定されています。
- VLAN プールは、適切な VLAN 範囲が定義され、レイヤ 3 ドメインが作成されて VLAN プールに接続されている状態で設定される必要があります。
- エンティティ プロファイルの接続も、レイヤ3 ドメインに関連付けられている必要があります。
- リーフ スイッチのインターフェイス プロファイルは必要に応じて設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	コンフィギュレーション モードに入ります。

ステップ 2	インライン パラメータを作成することにより、HSRP を設定します。
	例：
	`apic1(config)# leaf 101`
	`apic1(config-leaf)# interface ethernet 1/17`
	`apic1(config-leaf-if)# hsrp version 1`
	`apic1(config-leaf-if)# hsrp use-bia`
	`apic1(config-leaf-if)# hsrp delay minimum 30`
	`apic1(config-leaf-if)# hsrp delay reload 30`
	`apic1(config-leaf-if)# hsrp 10 ipv4`
	`apic1(config-if-hsrp)# ip 182.16.1.2`
	`apic1(config-if-hsrp)# ip 182.16.1.3 secondary`
	`apic1(config-if-hsrp)# ip 182.16.1.4 secondary`	

	コマンドまたはアクション	目的
	apic1(config-if-hsrp)# **mac-address 5000.1000.1060** apic1(config-if-hsrp)# **timers 5 18** apic1(config-if-hsrp)# **priority 100** apic1(config-if-hsrp)# **preempt** apic1(config-if-hsrp)# **preempt delay minimum 60** apic1(config-if-hsrp)# **preempt delay reload 60** apic1(config-if-hsrp)# **preempt delay sync 60** apic1(config-if-hsrp)# **authentication none** apic1(config-if-hsrp)# **authentication simple** apic1(config-if-hsrp)# **authentication md5** apic1(config-if-hsrp)# **authentication-key <mypassword>** apic1(config-if-hsrp)# **authentication-key-timeout <timeout>**	

NX-OS スタイル CLI のテンプレートとポリシーを使用した Cisco APIC の HSRP の設定

リーフ スイッチが設定されている場合、HSRP が有効になっています。

始める前に

- テナントと VRF が設定されています。
- VLAN プールは、適切な VLAN 範囲が定義され、レイヤ 3 ドメインが作成されて VLAN プールに接続されている状態で設定される必要があります。
- エンティティ プロファイルの接続も、レイヤ3ドメインに関連付けられている必要があります。
- リーフ スイッチのインターフェイス プロファイルは必要に応じて設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： apic1# **configure**	コンフィギュレーション モードに入ります。

	コマンドまたはアクション	目的

ステップ 2	HSRPポリシーテンプレートを設定します。
	例：
	`apic1(config)# leaf 101`
	`apic1(config-leaf)# template hsrp interface-policy hsrp-intfPol1 tenant t9`
	`apic1(config-template-hsrp-if-pol)# hsrp use-bia`
	`apic1(config-template-hsrp-if-pol)# hsrp delay minimum 30`
	`apic1(config-template-hsrp-if-pol)# hsrp delay reload 30`
	
	`apic1(config)# leaf 101`
	`apic1(config-leaf)# template hsrp group-policy hsrp-groupPol1 tenant t9`
	`apic1(config-template-hsrp-group-pol)# timers 5 18`
	`apic1(config-template-hsrp-group-pol)# priority 100`
	`apic1(config-template-hsrp-group-pol)# preempt`
	`apic1(config-template-hsrp-group-pol)# preempt delay minimum 60`
	`apic1(config-template-hsrp-group-pol)# preempt delay reload 60`
	`apic1(config-template-hsrp-group-pol)# preempt delay sync 60`	

ステップ 3	設定されているポリシー テンプレートを使用します。
	例：
	`apic1(config)# leaf 101`
	`apic1(config-leaf)# interface ethernet 1/17`
	`apic1(config-leaf-if)# hsrp version 1`
	`apic1(config-leaf-if)# inherit hsrp interface-policy hsrp-intfPol1`
	`apic1(config-leaf-if)# hsrp 10 ipv4`
	`apic1(config-if-hsrp)# ip 182.16.1.2`
	`apic1(config-if-hsrp)# ip 182.16.1.3 secondary`
	`apic1(config-if-hsrp)# ip 182.16.1.4 secondary`
	`apic1(config-if-hsrp)# mac-address 5000.1000.1060`
	`apic1(config-if-hsrp)# inherit hsrp group-policy hsrp-groupPol1`	

REST API を使用した APIC 内の HSRP の設定

リーフ スイッチが設定されている場合、HSRP が有効になっています。

始める前に

- テナントおよび VRF を設定する必要があります。
- VLAN プールは、適切な VLAN 範囲が定義され、レイヤ 3 ドメインが作成されて VLAN プールに接続されている状態で設定される必要があります。
- エンティティ プロファイルの接続も、レイヤ3ドメインに関連付けられている必要があります。
- リーフ スイッチのインターフェイス プロファイルは必要に応じて設定する必要があります。

手順

ステップ 1 ポート セレクタを作成します。

例：

```
<polUni>
  <infraInfra dn="uni/infra">
    <infraNodeP name="TenantNode_101">
      <infraLeafS name="leafselector" type="range">
        <infraNodeBlk name="nodeblk" from_="101" to_="101">
            </infraNodeBlk>
      </infraLeafS>
      <infraRsAccPortP tDn="uni/infra/accportprof-TenantPorts_101"/>
    </infraNodeP>
    <infraAccPortP name="TenantPorts_101">
      <infraHPortS name="portselector" type="range">
        <infraPortBlk name="portblk" fromCard="1" toCard="1" fromPort="41" toPort="41">
            </infraPortBlk>
        <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-TenantPortGrp_101"/>
      </infraHPortS>
    </infraAccPortP>
    <infraFuncP>
      <infraAccPortGrp name="TenantPortGrp_101">
        <infraRsAttEntP tDn="uni/infra/attentp-AttEntityProfTenant"/>
        <infraRsHIfPol tnFabricHIfPolName="default"/>
      </infraAccPortGrp>
    </infraFuncP>
  </infraInfra>
</polUni>
```

ステップ 2 テナント ポリシーを作成します。

例：

```
<polUni>
  <fvTenant name="t9" dn="uni/tn-t9" descr="">
```

```
    <fvCtx name="t9_ctx1" pcEnfPref="unenforced">
    </fvCtx>
    <fvBD name="t9_bd1" unkMacUcastAct="flood" arpFlood="yes">
      <fvRsCtx tnFvCtxName="t9_ctx1"/>
      <fvSubnet ip="101.9.1.1/24" scope="shared"/>
    </fvBD>
    <l3extOut dn="uni/tn-t9/out-l3extOut1" enforceRtctrl="export" name="l3extOut1">
      <l3extLNodeP name="Node101">
        <l3extRsNodeL3OutAtt rtrId="210.210.121.121" rtrIdLoopBack="no"
tDn="topology/pod-1/node-101"/>
      </l3extLNodeP>
      <l3extRsEctx tnFvCtxName="t9_ctx1"/>
      <l3extRsL3DomAtt tDn="uni/l3dom-dom1"/>
      <l3extInstP matchT="AtleastOne" name="extEpg" prio="unspecified"
targetDscp="unspecified">
        <l3extSubnet aggregate="" descr="" ip="176.21.21.21/21" name=""
scope="import-security"/>
      </l3extInstP>
    </l3extOut>
  </fvTenant>
</polUni>
```

ステップ 3 LLDP インターフェイス ポリシーを作成します。.

例：

```
<polUni>
  <fvTenant name="t9" dn="uni/tn-t9" descr="">
    <hsrpIfPol name="hsrpIfPol" ctrl="bfd" delay="4" reloadDelay="11"/>
  </fvTenant>
</polUni>
```

ステップ 4 HSRP グループ ポリシーを作成します。.

例：

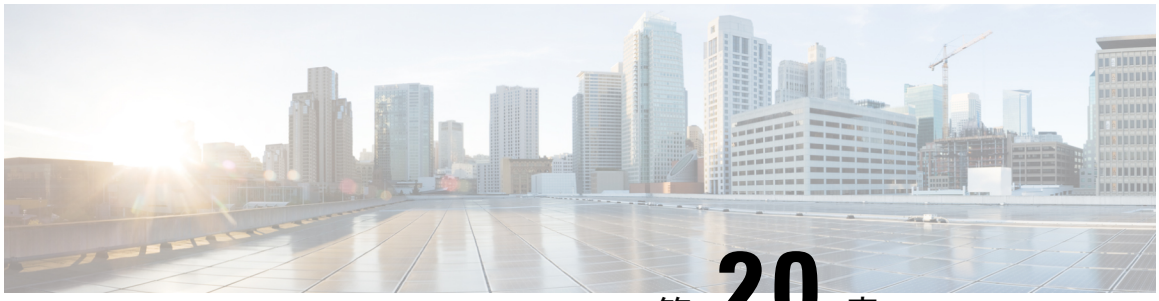
```
<polUni>
  <fvTenant name="t9" dn="uni/tn-t9" descr="">
    <hsrpIfPol name="hsrpIfPol" ctrl="bfd" delay="4" reloadDelay="11"/>
  </fvTenant>
</polUni>
```

ステップ 5 HSRP インターフェイス プロファイルおよび HSRP グループ プロファイルを作成します。

例：

```
<polUni>
  <fvTenant name="t9" dn="uni/tn-t9" descr="">
    <l3extOut dn="uni/tn-t9/out-l3extOut1" enforceRtctrl="export" name="l3extOut1">
      <l3extLNodeP name="Node101">
        <l3extLIfP name="eth1-41-v6" ownerKey="" ownerTag="" tag="yellow-green">
          <hsrpIfP name="eth1-41-v6" version="v2">
            <hsrpRsIfPol tnHsrpIfPolName="hsrpIfPol"/>
           <hsrpGroupP descr="" name="HSRPV6-2" groupId="330" groupAf="ipv6" ip="fe80::3"
 mac="00:00:0C:18:AC:01" ipObtainMode="admin">
              <hsrpRsGroupPol tnHsrpGroupPolName="G1"/>
            </hsrpGroupP>
          </hsrpIfP>
          <l3extRsPathL3OutAtt addr="2002::100/64" descr="" encap="unknown"
encapScope="local" ifInstT="l3-port" llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular"
 mtu="inherit" tDn="topology/pod-1/paths-101/pathep-[eth1/41]" targetDscp="unspecified">

            <l3extIp addr="2004::100/64"/>
          </l3extRsPathL3OutAtt>
```

```
        </l3extLIfP>
        <l3extLIfP name="eth1-41-v4" ownerKey="" ownerTag="" tag="yellow-green">
          <hsrpIfP name="eth1-41-v4" version="v1">
            <hsrpRsIfPol tnHsrpIfPolName="hsrpIfPol"/>
            <hsrpGroupP descr="" name="HSRPV4-2" groupId="51" groupAf="ipv4"
ip="177.21.21.21" mac="00:00:0C:18:AC:01" ipObtainMode="admin">
              <hsrpRsGroupPol tnHsrpGroupPolName="G1"/>
            </hsrpGroupP>
          </hsrpIfP>
          <l3extRsPathL3OutAtt addr="177.21.21.11/24" descr="" encap="unknown"
encapScope="local" ifInstT="l3-port" llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular"
 mtu="inherit" tDn="topology/pod-1/paths-101/pathep-[eth1/41]" targetDscp="unspecified">

            <l3extIp addr="177.21.23.11/24"/>
          </l3extRsPathL3OutAtt>
        </l3extLIfP>
      </l3extLNodeP>
    </l3extOut>
  </fvTenant>
</polUni>
```



第 20 章

Cisco ACI GOLF

この章の内容は、次のとおりです。

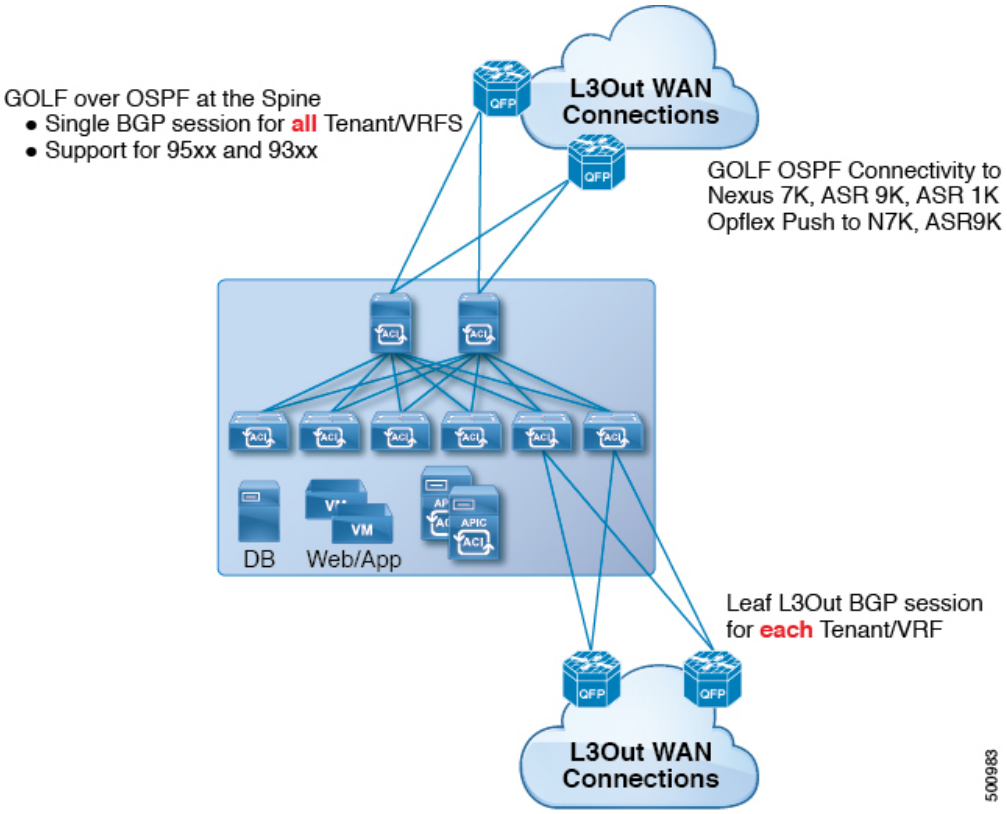
Cisco ACI GOLF

Cisco ACI GOLF

Cisco ACI GOLF 機能 (ファブリック WAN のレイヤ 3 EVPN サービス機能とも呼ばれる) では、より効率的かつスケーラブルな ACI ファブリック WAN 接続が可能になります。スパイン スイッチに接続されている WAN に OSPF 経由で BGP EVPN プロトコルが使用されます。

Cisco ACI GOLF

図 *27 : Cisco ACI GOLF* のトポロジ



すべてのテナント WAN 接続が、WAN ルータが接続されたスパイン スイッチ上で単一のセッションを使用します。データセンター相互接続ゲートウェイ（DCIG）へのテナント BGP セッションのこの集約では、テナント BGP セッションの数と、それらすべてに必要な設定の量を低減することによって、コントロールプレーンのスケールが向上します。ネットワークは、スパイン ファブリック ポートに設定された レイヤ 3 サブインターフェイスを使用して拡張されます。GOLF を使用した、共有サービスを伴うトランジット ルーティングはサポートされていません。

スパイン スイッチでの GOLF 物理接続のためのレイヤ 3 外部外側ネットワーク (`L3extOut`) は、`infra` テナントの下で指定され、次のものを含みます:

- `LNodeP` (infra テナントの L3Out では、`l3extInstP` は必要ありません)。
- infra テナントの GOLF 用の `L3extOut` のプロバイダ ラベル。
- OSPF プロトコル ポリシー
- BGP プロトコル ポリシー

すべての通常テナントが、上記で定義した物理接続を使用します。通常のテナントで定義した `L3extOut` では、次が必要です:

- サブネットとコントラクトを持つ `l3extInstP` (EPG)。サブネットの範囲を使用して、ルート制御ポリシーとセキュリティポリシーのインポートまたはエクスポートを制御します。ブリッジドメインサブネットは外部的にアドバタイズするように設定される必要があり、アプリケーション EPG および GOLF L3Out EPG と同じ VRF に存在する必要があります。
- アプリケーション EPG と GOLF L3Out EPG の間の通信は、(契約優先グループではなく) 明示的な契約によって制御されます。
- `l3extConsLbl` コンシューマ ラベル。これは `infra` テナントの GOLF 用の `L3Out` の同じプロバイダ ラベルと一致している必要があります。ラベルを一致させることにより、他のテナント内のアプリケーション EPG が `LNodeP` 外部 `L3Out` EPG を利用することが可能になります。
- `infra` テナント内のマッチング プロバイダ `L3extOut` の BGP EVPN セッションは、この `L3Out` で定義されたテナント ルートをアドバタイズします。

次に示す GOLF のガイドラインおよび制限事項に従ってください。

- すべての Cisco Nexus 9000 シリーズ ACI モードのスイッチと、すべての Cisco Nexus 9500 プラットフォーム ACI モード スイッチライン カードおよびファブリック モジュールが GOLF をサポートします。Cisco APIC、リリース 3.1(x) 以降では、これに N9K-C9364C スイッチが含まれます。
- 現時点では、ファブリック全体のスパイン スイッチインターフェイスに展開できるのは、単一の GOLF プロバイダ ポリシーだけです。
- APIC リリース 2.0(2) までは、 GOLF はマルチポッドでサポートされていません。リリース 2.0 (2) では、同じファブリックでの 2 つの機能を、スイッチ名の末尾に「EX」のない Cisco Nexus N9000K スイッチ上でのみサポートしています。たとえば N9K-9312TX です。2.1(1) リリース以降では、2 つの機能を、マルチポッドおよび EVPN トポロジで使用されているすべてのスイッチでともに展開できるようになりました。
- スパイン スイッチで GOLF を設定する場合、コントロール プレーンがコンバージするまでは、別のスパイン スイッチで GOLF の設定を行わないでください。
- スパイン スイッチは複数のプロバイダの GOLF 外側ネットワーク (GOLF L3Outs) に追加できますが、GOLF L3Out ごとのプロバイダ ラベルは異なっている必要があります。また、この例では、OSPF エリアも `L3extOut` ごとに異なっていて、異なるループバック アドレスを使用する必要があります。
- `infra` テナント内のマッチング プロバイダ `L3Out` の BGP EVPN セッションは、この `L3extOut` で定義されたテナント ルートをアドバタイズします。
- 3 つの GOLF Outs を展開する場合、1 つだけが GOLF, and 0/0 エクスポート集約のプロバイダ/コンシューマ ラベルを持っているなら、APIC はすべてのルートをエクスポートします。これは、テナントのリーフ スイッチ上の既存の `L3extOut` と同じです。
- スパイン スイッチとデータセンター相互接続（DCI）ルータ間に直接ピアリングがある場合、リーフ スイッチから ASR へのトランジット ルートには、リーフ スイッチの PTEP として次のホップが存在することになります。この場合、その ACI ポッドの TEP 範囲に対

して ASR の静的ルートを定義します。また、DCI が同じポッドにデュアルホーム接続されている場合は、静的ルートの優先順位（管理距離）は、他のリンクを通じて受信するルートと同じである必要があります。

- デフォルトの `bgpPeerPfxPol` ポリシーは、ルートを 20,000 に制限します。ACI WANインターコネクト ピアの場合には、必要に応じてこれを増やしてください。
- 1 つのスパイン スイッチ上に 2 つの `L3extOut` が存在し、そのうちの一方のプロバイダ ラベルが `prov1` で DCI 1 とピアリングしており、もう一方の `L3extOut` のプロバイダ ラベルが `prov2` で DCI 2 とピアリングしているという、展開シナリオを考えます。テナント VRF に、プロバイダ ラベルのいずれか一方 (prov1 または prov2) をポイントしているコンシューマ ラベルがある場合、テナント ルートは DCI 1 と DCI 2 の両方に送信されます。
- GOLF OpFlex Vrf を集約する場合、ACI ファブリックまたは GOLF OpFlex VRF とシステム内のその他の VRF 間の GOLF デバイスでは、ルートのリーキングは発生しません。VRF リーキングのためには、(GOLF ルータではなく) 外部デバイスを使用する必要があります。

（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 multipod 接続を設定する場合は、MTU が両側で適切に設定されていることが重要です。ACI、Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定された MTU 値は IP ヘッダーを考慮に入れています（結果として、最大パケット サイズは、ACI で 9216 バイト、NX-OS および IOS で 9000 バイトに設定されます）。ただし、IOS XR などの他のプラットフォームは、パケット ヘッダーのを除く MTU 値を設定します（結果として最大パケット 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。

Multi-Site サイト間の共有 GOLF 接続を使用する

複数のサイトで共有 APIC ゴルフ接続

トポロジでは、複数のサイト、APIC サイトの拡大 Vrf は、ゴルフ接続を共有している場合、リスクのクロス VRF トラフィックの問題を回避する次のガイドラインに従います。

スパイン スイッチと、DCI の間でルート ターゲットの設定

ゴルフ Vrf の EVPN ルート ターゲット (RTs) を設定する 2 つの方法があります: 手動 RT と自動 RT. ルート ターゲットは、ACI 背表紙と OpFlex を介して DCIs の間で同期されます。ゴルフ Vrf の自動 RT は、形式に組み込まれて Fabric ID: – *ASN* : [*FabricID*] *VNID*

2 つのサイトには、次の図のように導入の Vrf がある、Vrf 間のトラフィックを混在させることができます。

サイト 1	サイト 2
ASN: 100、ファブリック ID: 1	ASN: 100、ファブリック ID: 1
VRF A：VNID 1000 インポート/エクスポート ルート ターゲット：100：[1] 1000	VRF A：VNID 2000 インポート/エクスポート ルート ターゲット：100：[1] 2000
VRF B：VNID 2000 インポート/エクスポート ルート ターゲット：100：[1] 2000	VRF B：VNID 1000 インポート/エクスポート ルート ターゲット：100：[1] 1000

Dci のために必要なルート マップ

トンネルは、中継ルートは、[DCI を介してリークとサイト間では作成されません、ため、コントロール プレーンの手間をも削減する必要があります。もう 1 つのサイトでゴルフ スパインに、DCI への 1 つのサイトでゴルフ スパインから送信される EVPN タイプ 5 およびタイプ 2 ルートを送信できませんする必要があります。これが発生スパイン スイッチに dci のために次のタイプの BGP セッションが必要がある場合。

Site1: IBGP--DCI--EBGP--サイト 2

Site1: EBGP--DCI--IBGP--サイト 2

Site1:--DCI--EBGP EBGP--サイト 2

Site1: IBGP RR クライアント--DCI (RR)----IBGP サイト 2

Dci のためにこの問題を避けるためには、ルートマップは、インバウンドおよびアウトバウンドのピア ポリシーのさまざまな BGP コミュニティで使用されます。

ルートを 1 つのサイト、もう 1 つのサイト フィルタ着信ピア ポリシーでコミュニティに基づくルートでゴルフ スパインへのアウト バウンド ピア ポリシー ゴルフ スパインから受信します。別のアウト バウンド ピア ポリシーは、WAN へコミュニティを取り除き。すべてのルート マップは、ピアのレベルでです。

NX-OS スタイル CLI を使用した推奨される共有 GOLF 設定

マルチサイトで管理されている複数の APIC サイト間で、DCI による GOLF 接続を共有する場合、ルート マップと BPG を設定し VRF 間のトラフィックの問題を避けるために次の手順を使用します。

手順

ステップ 1 インバウンド ルート マップ

例：

```
Inbound peer policy to attach community:

 route-map multi-site-in permit 10

  set community 1:1 additive
```

ステップ 2 アウトバウンド ピア ポリシーを設定し、インバウンド ピア ポリシーのコミュニティに基づいてルートをフィルタします。

例：

```
ip community-list standard test-com permit 1:1

route-map multi-site-out deny 10

  match community test-com exact-match

route-map multi-site-out permit 11
```

ステップ 3 アウトバウンド ピア ポリシーを設定し、WAN へのコミュニティをフィルタします。

例：

```
ip community-list standard test-com permit 1:1

route-map multi-site-wan-out permit 11

  set comm-list test-com  delete
```

ステップ 4 BGP を設定します。

例：

```
router bgp 1

  address-family l2vpn evpn

  neighbor 11.11.11.11 remote-as 1

    update-source loopback0

    address-family l2vpn evpn

      send-community both

      route-map multi-site-in in

  neighbor 13.0.0.2 remote-as 2

    address-family l2vpn evpn

      send-community both

      route-map multi-site-out out
```

GUI を使用した ACI GOLF の設定

次に、任意のテナント ネットワークが使用できるインフラ GOLF サービスを設定する手順について説明します。

手順

ステップ 1 メニュー バーで、をクリックして **テナント** 、] をクリックし、 **インフラ** を選択、テナントインフラ。

ステップ 2 **ナビゲーション**] ペインで、展開、 **ネットワーキング** オプションし、次の操作を行います。

a) 右クリックして **外部ルーテッド ネットワーク**] をクリックし、 **作成ルーティング外部 EVPN の** ウィザードを開きます。

b) [Name] フィールドにポリシーの名前を入力します。

c) **ルート ターゲット** フィールドで、自動または明示的なポリシーを持つ BGP ルート ターゲットをフィルタリング ポリシーを使用するかどうかを選択します。

- **自動** -自動 BGP ルート ターゲット Vrf でフィルタ リングは、これに関連付けられている実装は、外部設定をルーティングします。
- **明示的な** -ルート ターゲットの明示的にフィルタ リングの実装では、この設定の外部ルーティングに関連付けられている Vrf に BGP ルート ターゲット ポリシーが設定されています。

（注） 明示的なルート ターゲット ポリシーが設定されている、 **BGP ルート ターゲット プロファイル** テーブルで、 **BGP ページ** の **VRF ウィザードの作成** します。選択した場合、 **自動** オプションで **ルート ターゲット**] フィールドで明示ルート ターゲット ポリシーの設定、 **VRF ウィザードの作成** BGP ルーティングの中断を引き起こす可能性があります。

（注） 明示的なルート ターゲット ポリシーが設定されている、 **BGP ルート ターゲット プロファイル** テーブルで、 **BGP ページ** の **VRF ウィザードの作成** します。選択した場合、 **自動** オプションで **ルート ターゲット**] フィールドで明示ルート ターゲット ポリシーの設定、 **VRF ウィザードの作成** BGP ルーティングの中断を引き起こす可能性があります。

d) レイヤ 3 接続の要件に従って設定オプションを実行します。

（注） プロトコルのチェック ボックス エリアで、[BGP] および [OSPF] の両方がチェックされていることを確認します。GOLFBGP と OSPF の両方が必要です。

e) をクリックして **次** を表示する、 **ノードとインターフェイス プロトコル プロファイル** ()] タブ。

f) **[名前]** フィールドの **[ルーテッド アウトサイドの定義]** で名前を入力します。

g) [スパイン] **テーブル**で、**[+]** をクリックしてノード エントリを追加します。

h) **[ノード ID]** ドロップダウン リストで、スパイン スイッチ ノード ID を選択します。

i) [Router ID] フィールドに、ルータ ID を入力します。
j) **ループバック アドレス** 、(IP)] フィールドに、IP アドレスを入力します。[Update] をクリックします。
k) Name フィールドに Interfaces サブ/ルーテッド サブインターフェイス] セクションの OSPF プロファイルでは、日曜日インターフェイスの OSPF プロファイルの名前を入力します。
l) [OK] をクリックします。

（注） ウィザードを作成、 **論理ノード プロファイル > 設定されているノード > ノードの関連付け** プロファイル設定を **制御ピアリングの拡張**] フィールドを有効になっています。

ステップ 3 **インフラ** > **ネットワー キング** > **外部ルーテッド ネットワーク** のセクションで、 **ナビゲーション** ペインで、作成したゴルフ ポリシーを選択する] をクリックします。入力してください、 **プロバイダー ラベル** 、(たとえば、 ゴルフ)] をクリックし、 **Submit** 。

ステップ 4 **ナビゲーション** 、テナントのウィンドウを展開、 ***tenant_name*** > **ネットワー キング** し、次のアクションを実行します。

a) 右クリックして **外部ルーテッド ネットワーク**] をクリックし、 **外部ルーティングの作成** ウィザードを開きます。
b) **[ID]** ダイアログ ボックスで、**[名前]** フィールドに、ポリシーの名前を入力します。
c) レイヤ 3 接続の要件に従って設定オプションを実行します。

（注） プロトコルのチェック ボックス エリアで、[BGP] および [OSPF] の両方がチェックされていることを確認します。GOLFBGP と OSPF の両方が必要です。

d) **[コンシューマ ラベル]** を割り当てます。この例では使用 ゴルフ (が作成した上記。
e) [Next] をクリックします。
f) 外部 EPG ネットワーク ダイアログボックスを設定し、をクリックして **終了** ポリシーを展開します。

NX-OS スタイル CLI を使用した Cisco ACI GOLF 設定の例:

次の例を設定する CLI コマンドの show GOLF サービスで、OSPF over スパイン スイッチに接続されている WAN ルータの BGP EVPN プロトコルを使用します。

設定、BGP EVPN のテナント インフラ

次の例を設定する方法を示しています、インフラ VLAN ドメイン、VRF、インターフェイスの IP アドレッシングを含む、BGP EVPN および OSPF のテナントします。

```
configure
  vlan-domain evpn-dom dynamic
  exit
  spine 111
       # Configure  Tenant Infra VRF overlay-1 on the spine.
    vrf context tenant infra vrf overlay-1
```

```
    router-id 10.10.3.3
    exit

interface ethernet 1/33
     vlan-domain member golf_dom
     exit
interface ethernet 1/33.4
     vrf member tenant infra vrf overlay-1
     mtu 1500
     ip address 5.0.0.1/24
     ip router ospf default area 0.0.0.150
     exit
interface ethernet 1/34
     vlan-domain member golf_dom
    exit
interface ethernet 1/34.4
    vrf member tenant infra vrf overlay-1
    mtu 1500
    ip address 2.0.0.1/24
    ip router ospf default area 0.0.0.200
   exit

router ospf default
   vrf member tenant infra vrf overlay-1
       area 0.0.0.150 loopback 10.10.5.3
       area 0.0.0.200 loopback 10.10.4.3
       exit
   exit
```

スパイン ノード上の BGP の設定

次の例では、BGP EVPN をサポートする BGP を設定する方法を示します。

```
Configure
spine 111
router bgp 100
    vrf member tenant infra vrf overlay- 1
         neighbor 10.10.4.1 evpn
             label golf_aci
             update-source loopback 10.10.4.3
             remote-as 100
             exit
         neighbor 10.10.5.1 evpn
             label golf_aci2
             update-source loopback 10.10.5.3
             remote-as 100
             exit
    exit
exit
```

BGP EVPN のテナントの設定

次の例では、BGP EVPN、BGP EVPN セッションで提供されるゲートウェイ サブネットを含むのテナントを設定する方法を示します。

```
configure
  tenant sky
    vrf context vrf_sky
      exit
    bridge-domain bd_sky
      vrf member vrf_sky
```

```
  exit
interface bridge-domain bd_sky
  ip address 59.10.1.1/24
  exit
bridge-domain bd_sky2
  vrf member vrf_sky
  exit
interface bridge-domain bd_sky2
  ip address 59.11.1.1/24
  exit
exit
```

BGP EVPN ルート ターゲット、ルート マップと、テナントのプレフィックス EPG の設定

次の例では、BGP EVPN を介してブリッジ ドメイン サブネットをアドバタイズするルート マップを設定する方法を示します。

```
configure
spine 111
    vrf context tenant sky vrf vrf_sky
        address-family ipv4 unicast
            route-target export 100:1
            route-target import 100:1
             exit

        route-map rmap
            ip prefix-list p1 permit 11.10.10.0/24
            match bridge-domain bd_sky
                exit
            match prefix-list p1
                exit

         evpn export map rmap label golf_aci

          route-map rmap2
           match bridge-domain bd_sky
               exit
           match prefix-list p1
              exit
          exit

         evpn export map rmap label golf_aci2

    external-l3 epg l3_sky
      vrf member vrf_sky
      match ip 80.10.1.0/24
      exit
```

REST API を使用した GOLF の設定

手順

ステップ 1 次の例では、REST API を使用して GOLF のノードおよびスパイン スイッチ インターフェイスを展開する方法を示しています。

例：

```
POST
https://192.0.20.123/api/mo/uni/golf.xml
```

ステップ 2 次の XML で、スパイン スイッチ インターフェイスと GOLF サービスのインフラ テナント プロバイダを設定します。次の XML 構造を POST メッセージの本文に含めます。

例：

```
<l3extOut descr="" dn="uni/tn-infra/out-golf" enforceRtctrl="export,import"
    name="golf"
    ownerKey="" ownerTag="" targetDscp="unspecified">
    <l3extRsEctx tnFvCtxName="overlay-1"/>
    <l3extProvLbl descr="" name="golf"
         ownerKey="" ownerTag="" tag="yellow-green"/>
    <l3extLNodeP configIssues="" descr=""
         name="bLeaf" ownerKey="" ownerTag=""
         tag="yellow-green" targetDscp="unspecified">
         <l3extRsNodeL3OutAtt rtrId="10.10.3.3" rtrIdLoopBack="no"
             tDn="topology/pod-1/node-111">
             <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
             <l3extLoopBackIfP addr="10.10.3.3" descr="" name=""/>
         </l3extRsNodeL3OutAtt>
         <l3extRsNodeL3OutAtt rtrId="10.10.3.4" rtrIdLoopBack="no"
             tDn="topology/pod-1/node-112">
         <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
         <l3extLoopBackIfP addr="10.10.3.4" descr="" name=""/>
         </l3extRsNodeL3OutAtt>
         <l3extLIfP descr="" name="portIf-spine1-3"
             ownerKey="" ownerTag="" tag="yellow-green">
             <ospfIfP authKeyId="1" authType="none" descr="" name="">
               <ospfRsIfPol tnOspfIfPolName="ospfIfPol"/>
             </ospfIfP>
             <l3extRsNdIfPol tnNdIfPolName=""/>
             <l3extRsIngressQosDppPol tnQosDppPolName=""/>
             <l3extRsEgressQosDppPol tnQosDppPolName=""/>
             <l3extRsPathL3OutAtt addr="7.2.1.1/24" descr=""
                encap="vlan-4"
                encapScope="local"
                ifInstT="sub-interface"
                llAddr="::" mac="00:22:BD:F8:19:FF"
                mode="regular"
                mtu="1500"
                tDn="topology/pod-1/paths-111/pathep-[eth1/12]"
                targetDscp="unspecified"/>
          </l3extLIfP>
          <l3extLIfP descr="" name="portIf-spine2-1"
              ownerKey=""
              ownerTag=""
              tag="yellow-green">
              <ospfIfP authKeyId="1"
                   authType="none"
                   descr=""
                   name="">
                   <ospfRsIfPol tnOspfIfPolName="ospfIfPol"/>
              </ospfIfP>
              <l3extRsNdIfPol tnNdIfPolName=""/>
              <l3extRsIngressQosDppPol tnQosDppPolName=""/>
              <l3extRsEgressQosDppPol tnQosDppPolName=""/>
              <l3extRsPathL3OutAtt addr="7.1.0.1/24" descr=""
                   encap="vlan-4"
                   encapScope="local"
                   ifInstT="sub-interface"
                   llAddr="::" mac="00:22:BD:F8:19:FF"
                   mode="regular"
```

```
        mtu="9000"
        tDn="topology/pod-1/paths-112/pathep-[eth1/11]"
        targetDscp="unspecified"/>
</l3extLIfP>
<l3extLIfP descr="" name="portif-spine2-2"
   ownerKey=""
   ownerTag=""
   tag="yellow-green">
   <ospfIfP authKeyId="1"
        authType="none" descr=""
        name="">
        <ospfRsIfPol tnOspfIfPolName="ospfIfPol"/>
  </ospfIfP>
  <l3extRsNdIfPol tnNdIfPolName=""/>
  <l3extRsIngressQosDppPol tnQosDppPolName=""/>
  <l3extRsEgressQosDppPol tnQosDppPolName=""/>
  <l3extRsPathL3OutAtt addr="7.2.2.1/24" descr=""
        encap="vlan-4"
        encapScope="local"
        ifInstT="sub-interface"
               llAddr="::" mac="00:22:BD:F8:19:FF"
               mode="regular"
               mtu="1500"
               tDn="topology/pod-1/paths-112/pathep-[eth1/12]"
               targetDscp="unspecified"/>
  </l3extLIfP>
  <l3extLIfP descr="" name="portIf-spine1-2"
       ownerKey="" ownerTag="" tag="yellow-green">
       <ospfIfP authKeyId="1" authType="none" descr="" name="">
            <ospfRsIfPol tnOspfIfPolName="ospfIfPol"/>
       </ospfIfP>
       <l3extRsNdIfPol tnNdIfPolName=""/>
       <l3extRsIngressQosDppPol tnQosDppPolName=""/>
       <l3extRsEgressQosDppPol tnQosDppPolName=""/>
       <l3extRsPathL3OutAtt addr="9.0.0.1/24" descr=""
        encap="vlan-4"
        encapScope="local"
        ifInstT="sub-interface"
             llAddr="::" mac="00:22:BD:F8:19:FF"
             mode="regular"
             mtu="9000"
             tDn="topology/pod-1/paths-111/pathep-[eth1/11]"
             targetDscp="unspecified"/>
  </l3extLIfP>
  <l3extLIfP descr="" name="portIf-spine1-1"
        ownerKey="" ownerTag="" tag="yellow-green">
        <ospfIfP authKeyId="1" authType="none" descr="" name="">
             <ospfRsIfPol tnOspfIfPolName="ospfIfPol"/>
        </ospfIfP>
        <l3extRsNdIfPol tnNdIfPolName=""/>
        <l3extRsIngressQosDppPol tnQosDppPolName=""/>
        <l3extRsEgressQosDppPol tnQosDppPolName=""/>
        <l3extRsPathL3OutAtt addr="7.0.0.1/24" descr=""
          encap="vlan-4"
          encapScope="local"
          ifInstT="sub-interface"
          llAddr="::" mac="00:22:BD:F8:19:FF"
          mode="regular"
          mtu="1500"
          tDn="topology/pod-1/paths-111/pathep-[eth1/10]"
               targetDscp="unspecified"/>
  </l3extLIfP>
  <bgpInfraPeerP addr="10.10.3.2"
     allowedSelfAsCnt="3"
```

```
                    ctrl="send-com,send-ext-com"
                    descr="" name="" peerCtrl=""
                    peerT="wan"
                    privateASctrl="" ttl="2" weight="0">
                    <bgpRsPeerPfxPol tnBgpPeerPfxPolName=""/>
                    <bgpAsP asn="150" descr="" name="aspn"/>
                 </bgpInfraPeerP>
                 <bgpInfraPeerP addr="10.10.4.1"
                    allowedSelfAsCnt="3"
                    ctrl="send-com,send-ext-com" descr="" name="" peerCtrl=""
                    peerT="wan"
                    privateASctrl="" ttl="1" weight="0">
                    <bgpRsPeerPfxPol tnBgpPeerPfxPolName=""/>
                    <bgpAsP asn="100" descr="" name=""/>
                  </bgpInfraPeerP>
                  <bgpInfraPeerP addr="10.10.3.1"
                    allowedSelfAsCnt="3"
                    ctrl="send-com,send-ext-com" descr="" name="" peerCtrl=""
                    peerT="wan"
                    privateASctrl="" ttl="1" weight="0">
                    <bgpRsPeerPfxPol tnBgpPeerPfxPolName=""/>
                    <bgpAsP asn="100" descr="" name=""/>
                 </bgpInfraPeerP>
          </l3extLNodeP>
         <bgpRtTargetInstrP descr="" name="" ownerKey="" ownerTag="" rtTargetT="explicit"/>

          <l3extRsL3DomAtt tDn="uni/l3dom-l3dom"/>
          <l3extInstP descr="" matchT="AtleastOne" name="golfInstP"
                    prio="unspecified"
                    targetDscp="unspecified">
                    <fvRsCustQosPol tnQosCustomPolName=""/>
           </l3extInstP>
           <bgpExtP descr=""/>
           <ospfExtP areaCost="1"
                  areaCtrl="redistribute,summary"
                  areaId="0.0.0.1"
                  areaType="regular" descr=""/>
</l3extOut>
```

ステップ 3 次の XML で、GOLF サービスのインフラ部分のテナント コンシューマを設定します。次の XML 構造を POST メッセージの本文に含めます。

例：

```
<fvTenant descr="" dn="uni/tn-pep6" name="pep6" ownerKey="" ownerTag="">
     <vzBrCP descr="" name="webCtrct"
          ownerKey="" ownerTag="" prio="unspecified"
          scope="global" targetDscp="unspecified">
          <vzSubj consMatchT="AtleastOne" descr=""
               name="http" prio="unspecified" provMatchT="AtleastOne"
               revFltPorts="yes" targetDscp="unspecified">
               <vzRsSubjFiltAtt directives="" tnVzFilterName="default"/>
          </vzSubj>
      </vzBrCP>
      <vzBrCP descr="" name="webCtrct-pod2"
           ownerKey="" ownerTag="" prio="unspecified"
           scope="global" targetDscp="unspecified">
           <vzSubj consMatchT="AtleastOne" descr=""
                name="http" prio="unspecified"
                provMatchT="AtleastOne" revFltPorts="yes"
                targetDscp="unspecified">
                <vzRsSubjFiltAtt directives=""
                      tnVzFilterName="default"/>
```

```
    </vzSubj>
</vzBrCP>
<fvCtx descr="" knwMcastAct="permit"
     name="ctx6" ownerKey="" ownerTag=""
     pcEnfDir="ingress" pcEnfPref="enforced">
     <bgpRtTargetP af="ipv6-ucast"
          descr="" name="" ownerKey="" ownerTag="">
          <bgpRtTarget descr="" name="" ownerKey="" ownerTag=""
          rt="route-target:as4-nn2:100:1256"
          type="export"/>
          <bgpRtTarget descr="" name="" ownerKey="" ownerTag=""
               rt="route-target:as4-nn2:100:1256"
               type="import"/>
     </bgpRtTargetP>
     <bgpRtTargetP af="ipv4-ucast"
          descr="" name="" ownerKey="" ownerTag="">
          <bgpRtTarget descr="" name="" ownerKey="" ownerTag=""
               rt="route-target:as4-nn2:100:1256"
               type="export"/>
          <bgpRtTarget descr="" name="" ownerKey="" ownerTag=""
               rt="route-target:as4-nn2:100:1256"
               type="import"/>
     </bgpRtTargetP>
     <fvRsCtxToExtRouteTagPol tnL3extRouteTagPolName=""/>
     <fvRsBgpCtxPol tnBgpCtxPolName=""/>
     <vzAny descr="" matchT="AtleastOne" name=""/>
     <fvRsOspfCtxPol tnOspfCtxPolName=""/>
     <fvRsCtxToEpRet tnFvEpRetPolName=""/>
     <l3extGlobalCtxName descr="" name="dci-pep6"/>
</fvCtx>
<fvBD arpFlood="no" descr="" epMoveDetectMode=""
     ipLearning="yes"
     limitIpLearnToSubnets="no"
     llAddr="::" mac="00:22:BD:F8:19:FF"
     mcastAllow="no"
     multiDstPktAct="bd-flood"
     name="bd107" ownerKey="" ownerTag="" type="regular"
     unicastRoute="yes"
     unkMacUcastAct="proxy"
     unkMcastAct="flood"
     vmac="not-applicable">
     <fvRsBDToNdP tnNdIfPolName=""/>
     <fvRsBDToOut tnL3extOutName="routAccounting-pod2"/>
     <fvRsCtx tnFvCtxName="ctx6"/>
     <fvRsIgmpsn tnIgmpSnoopPolName=""/>
     <fvSubnet ctrl="" descr="" ip="27.6.1.1/24"
          name="" preferred="no"
          scope="public"
          virtual="no"/>
          <fvSubnet ctrl="nd" descr="" ip="2001:27:6:1::1/64"
               name="" preferred="no"
               scope="public"
               virtual="no">
               <fvRsNdPfxPol tnNdPfxPolName=""/>
          </fvSubnet>
          <fvRsBdToEpRet resolveAct="resolve" tnFvEpRetPolName=""/>
</fvBD>
<fvBD arpFlood="no" descr="" epMoveDetectMode=""
     ipLearning="yes"
     limitIpLearnToSubnets="no"
     llAddr="::" mac="00:22:BD:F8:19:FF"
     mcastAllow="no"
     multiDstPktAct="bd-flood"
     name="bd103" ownerKey="" ownerTag="" type="regular"
```

```
     unicastRoute="yes"
     unkMacUcastAct="proxy"
     unkMcastAct="flood"
     vmac="not-applicable">
     <fvRsBDToNdP tnNdIfPolName=""/>
     <fvRsBDToOut tnL3extOutName="routAccounting"/>
     <fvRsCtx tnFvCtxName="ctx6"/>
     <fvRsIgmpsn tnIgmpSnoopPolName=""/>
     <fvSubnet ctrl="" descr="" ip="23.6.1.1/24"
          name="" preferred="no"
          scope="public"
          virtual="no"/>
     <fvSubnet ctrl="nd" descr="" ip="2001:23:6:1::1/64"
          name="" preferred="no"
          scope="public" virtual="no">
          <fvRsNdPfxPol tnNdPfxPolName=""/>
     </fvSubnet>
     <fvRsBdToEpRet resolveAct="resolve" tnFvEpRetPolName=""/>
</fvBD>
<vnsSvcCont/>
<fvRsTenantMonPol tnMonEPGPolName=""/>
<fvAp descr="" name="AP1"
     ownerKey="" ownerTag="" prio="unspecified">
     <fvAEPg descr=""
          isAttrBasedEPg="no"
          matchT="AtleastOne"
          name="epg107"
          pcEnfPref="unenforced" prio="unspecified">
          <fvRsCons prio="unspecified"
               tnVzBrCPName="webCtrct-pod2"/>
          <fvRsPathAtt descr=""
               encap="vlan-1256"
               instrImedcy="immediate"
               mode="regular" primaryEncap="unknown"
               tDn="topology/pod-2/paths-107/pathep-[eth1/48]"/>
          <fvRsDomAtt classPref="encap" delimiter=""
               encap="unknown"
               instrImedcy="immediate"
               primaryEncap="unknown"
               resImedcy="lazy" tDn="uni/phys-phys"/>
          <fvRsCustQosPol tnQosCustomPolName=""/>
          <fvRsBd tnFvBDName="bd107"/>
          <fvRsProv matchT="AtleastOne"
               prio="unspecified"
               tnVzBrCPName="default"/>
     </fvAEPg>
     <fvAEPg descr=""
          isAttrBasedEPg="no"
          matchT="AtleastOne"
          name="epg103"
          pcEnfPref="unenforced" prio="unspecified">
          <fvRsCons prio="unspecified" tnVzBrCPName="default"/>
          <fvRsCons prio="unspecified" tnVzBrCPName="webCtrct"/>
          <fvRsPathAtt descr="" encap="vlan-1256"
               instrImedcy="immediate"
               mode="regular" primaryEncap="unknown"
               tDn="topology/pod-1/paths-103/pathep-[eth1/48]"/>
               <fvRsDomAtt classPref="encap" delimiter=""
                    encap="unknown"
                    instrImedcy="immediate"
                    primaryEncap="unknown"
                    resImedcy="lazy" tDn="uni/phys-phys"/>
               <fvRsCustQosPol tnQosCustomPolName=""/>
               <fvRsBd tnFvBDName="bd103"/>
```

```
            </fvAEPg>
        </fvAp>
        <l3extOut descr=""
            enforceRtctrl="export"
            name="routAccounting-pod2"
            ownerKey="" ownerTag="" targetDscp="unspecified">
            <l3extRsEctx tnFvCtxName="ctx6"/>
            <l3extInstP descr=""
                matchT="AtleastOne"
                name="accountingInst-pod2"
                prio="unspecified" targetDscp="unspecified">
            <l3extSubnet aggregate="export-rtctrl,import-rtctrl"
                descr="" ip="::/0" name=""
                scope="export-rtctrl,import-rtctrl,import-security"/>
            <l3extSubnet aggregate="export-rtctrl,import-rtctrl"
                descr=""
                ip="0.0.0.0/0" name=""
                scope="export-rtctrl,import-rtctrl,import-security"/>
            <fvRsCustQosPol tnQosCustomPolName=""/>
            <fvRsProv matchT="AtleastOne"
                prio="unspecified" tnVzBrCPName="webCtrct-pod2"/>
            </l3extInstP>
            <l3extConsLbl descr=""
                name="golf2"
                owner="infra"
                ownerKey="" ownerTag="" tag="yellow-green"/>
        </l3extOut>
        <l3extOut descr=""
            enforceRtctrl="export"
            name="routAccounting"
            ownerKey="" ownerTag="" targetDscp="unspecified">
            <l3extRsEctx tnFvCtxName="ctx6"/>
            <l3extInstP descr=""
                matchT="AtleastOne"
                name="accountingInst"
                prio="unspecified" targetDscp="unspecified">
            <l3extSubnet aggregate="export-rtctrl,import-rtctrl" descr=""
                ip="0.0.0.0/0" name=""
                scope="export-rtctrl,import-rtctrl,import-security"/>
            <fvRsCustQosPol tnQosCustomPolName=""/>
            <fvRsProv matchT="AtleastOne" prio="unspecified" tnVzBrCPName="webCtrct"/>
            </l3extInstP>
            <l3extConsLbl descr=""
                name="golf"
                owner="infra"
                ownerKey="" ownerTag="" tag="yellow-green"/>
        </l3extOut>
</fvTenant>
```

DCIG への BGP EVPN タイプ 2 ホスト ルートの分散化

DCIG への BGP EVPN タイプ 2 のホスト ルートの配信

APIC ではリリース 2.0(1f) まで、ファブリック コントロール プレーンは EVPN ホスト ルートを直接送信してはいませんでしたが、Data Center Interconnect Gateway（DCIG）にルーティン

グしている BGP EVPN タイプ 5（IP プレフィックス）形式のパブリック ドメイン（BD）サブネットをアドバタイズしていました。これにより、最適ではないトラフィックの転送となる可能性があります。転送を改善するため APIC リリース 2.1 x では、ファブリック スパインを有効にして、パブリック BD サブネットとともに DCIG に EVPN タイプ 2（MAC-IP）ホスト ルートを使用してホスト ルートをアドバタイズできます。

そのためには、次の手順を実行する必要があります。

1. BGP アドレス ファミリ コンテキスト ポリシーを設定する際に、ホスト ルート リークを有効にします。
2. GOLF セットアップで BGP EVPN へのホスト ルートをリークする場合：
    1. GOLF が有効になっている場合にホスト ルートを有効にするには、インフラストラクチャ テナント以外に、BPG アドレス ファミリ コンテキスト ポリシーがアプリケーション テナント（アプリケーション テナントはコンシューマ テナントであり、エンドポイントを BGP EVPN にリークします）で設定されている必要があります。
    2. 単一ポッド ファブリックについては、ホスト ルート機能は必要ありません。ホスト ルート機能は、マルチポッドファブリック セットアップで最適ではない転送を避けるために必要です。ただし、単一ポッドファブリックがセットアップされる場合、エンドポイントから BGP EVPN にリークするため、ファブリック外部接続ポリシーを設定し ETEP IP アドレスを提供する必要があります。そうしないと、ホスト ルートは、BGP EVPN にはリークされません。
3. VRF のプロパティを設定する場合：
    1. IPv4 および IPv6 の各アドレス ファミリの BGP コンテキストに BGP アドレス ファミリ コンテキスト ポリシーを追加します。
    2. VRF からインポートまたはエクスポート可能なルートを特定する BGP ルート ターゲット プロファイルを設定します。

GUI を使用して DCIG への BGP EVPN タイプ 2 のホスト ルートを分散する

次の手順で BGP EVPN タイプ 2 のホスト ルートの分散を有効にします。

始める前に

インフラ テナントでのACI の WAN 相互接続サービスをすでに設定しており、サービスを使用するテナントを設定している

手順

ステップ 1 メニュー バーで、**Tenants** > **infra** をクリックします。

ステップ 2 [Navigation] ウィンドウで、**External Routed Networks** を展開し、その後 **Protocol Policies** および **BGP** を展開します。

ステップ 3 **BGP Address Family Context** を右クリックし、**Create BGP Address Family Context Policy** を選択し、次の手順を実行します:

a) ポリシーの名前を入力し、必要に応じて説明を追加します。

b) **Enable Host Route Leak** チェック ボックスをクリックします。

c) **Submit** をクリックします。

ステップ 4 **Tenants** > **tenant-name** (BGP アドレス ファミリ コンテキスト ポリシーを使用するテナント) をクリックし、**Networking** を展開します。

ステップ 5 **VRF** を展開し、分散するホスト ルートを含む VRF をクリックします。

ステップ 6 VRF のプロパティを設定するときには、**BGP Address Family Context Policy** を IPv4 と IPv6 の **BGP Context Per Address Families** に追加します。

ステップ 7 [送信（Submit）] をクリックします。

NX-OS スタイル CLI を使用して DCIG への配布の BGP EVPN タイプ 2 のホスト ルートの有効化

手順

	コマンドまたはアクション	目的

ステップ 1	BGP アドレス ファミリ configuration mode(設定モード、コンフィギュレーション モード) で、次のコマンドを DCIG に配布 EVPN タイプ 2 のホスト ルートを設定します。
	例：
	`apic1(config)# leaf 101`
	`apic1(config-leaf)# template bgp address-family bgpAf1 tenant bgp_t1`
	`apic1(config-bgp-af)# distance 250 240 230`
	`apic1(config-bgp-af)# host-rt-enable`
	`apic1(config-bgp-af)# exit`
		このテンプレートは、テナント bgp_t1 は VRF の導入を持つすべてのノードで利用可能になります。配布 EVPN タイプ 2 のホスト ルートを無効にするには、次のように入力します。、 **no ホスト -rt-enable** コマンド。

REST API を使用した DCIG への BGP EVPN タイプ 2 ホスト ルート配信の有効化

次のように REST API を使用して、BGP EVPN タイプ 2 ホスト ルートの配信を有効にします。

始める前に

EVPN サービスを設定する必要があります。

手順

ステップ 1 次の例のように、XML が含まれている POST で、ホスト ルート リーク ポリシーを設定します。

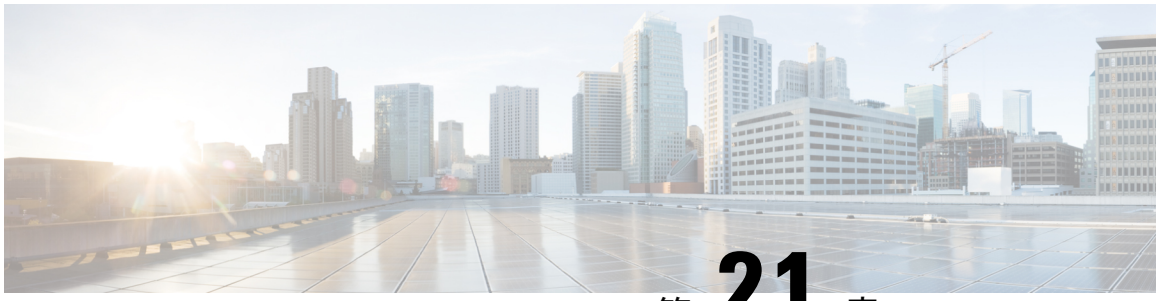
例：

```
<bgpCtxAfPol descr="" ctrl="host-rt-leak" name="bgpCtxPol_0 status=""/>
```

ステップ 2 次の例のように、XML が含まれている POST を使用してアドレス ファミリの一方または両方の VRF BGP アドレス ファミリ コンテキスト ポリシーに、ポリシーを適用します。

例：

```
<fvCtx name="vni-10001">
<fvRsCtxToBgpCtxAfPol af="ipv4-ucast" tnBgpCtxAfPolName="bgpCtxPol_0"/>
<fvRsCtxToBgpCtxAfPol af="ipv6-ucast" tnBgpCtxAfPolName="bgpCtxPol_0"/>
</fvCtx>
```



第 21 章

マルチポッド

この章は、次の項で構成されています。

マルチポッドについて

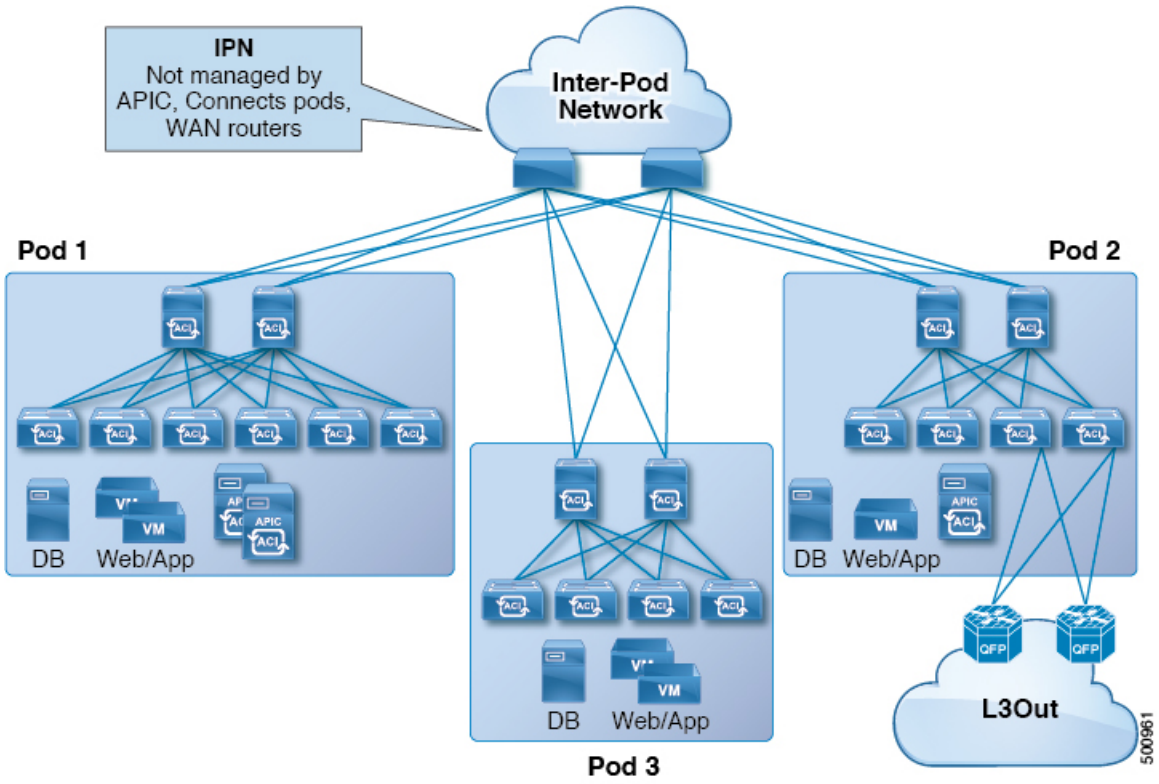
マルチポッドは、隔離されたコントロール プレーン プロトコルを持つ複数のポッドで構成された、障害耐性の高いファブリックのプロビジョニングを可能にします。また、マルチポッドでは、さらに柔軟にリーフとスパインスイッチ間のフル メッシュ配線を行うことができます。たとえば、リーフ スイッチが異なるフロアや異なる建物にまたがって分散している場合、マルチポッドでは、フロアごと、または建物ごとに複数のポッドをプロビジョニングし、スパインスイッチを通じてポッド間を接続することができます。

マルチポッドは、異なるポッドの ACI スパイン間のコントロール プレーン通信プロトコルとして MP-BGP EVPN を使用します。

WAN ルータは、ポッド間ネットワーク（IPN）でプロビジョニング可能で、スパイン スイッチに直接接続されるか、境界リーフ スイッチに接続されます。IPN に接続されるスパイン スイッチは、ポッド内ので少なくとも 1 個のリーフ スイッチに接続されます。

マルチポッドはすべてのポッドに単一の APIC クラスタを使用します。そのため、すべてのポッドが単一のファブリックとして機能します。ポッド全体にわたって個々の APIC コントローラが配置されますが、それらはすべて単一の APIC クラスタの一部です。

図 *28 :* マルチポッドの概要



複数ポッドのプロビジョニング

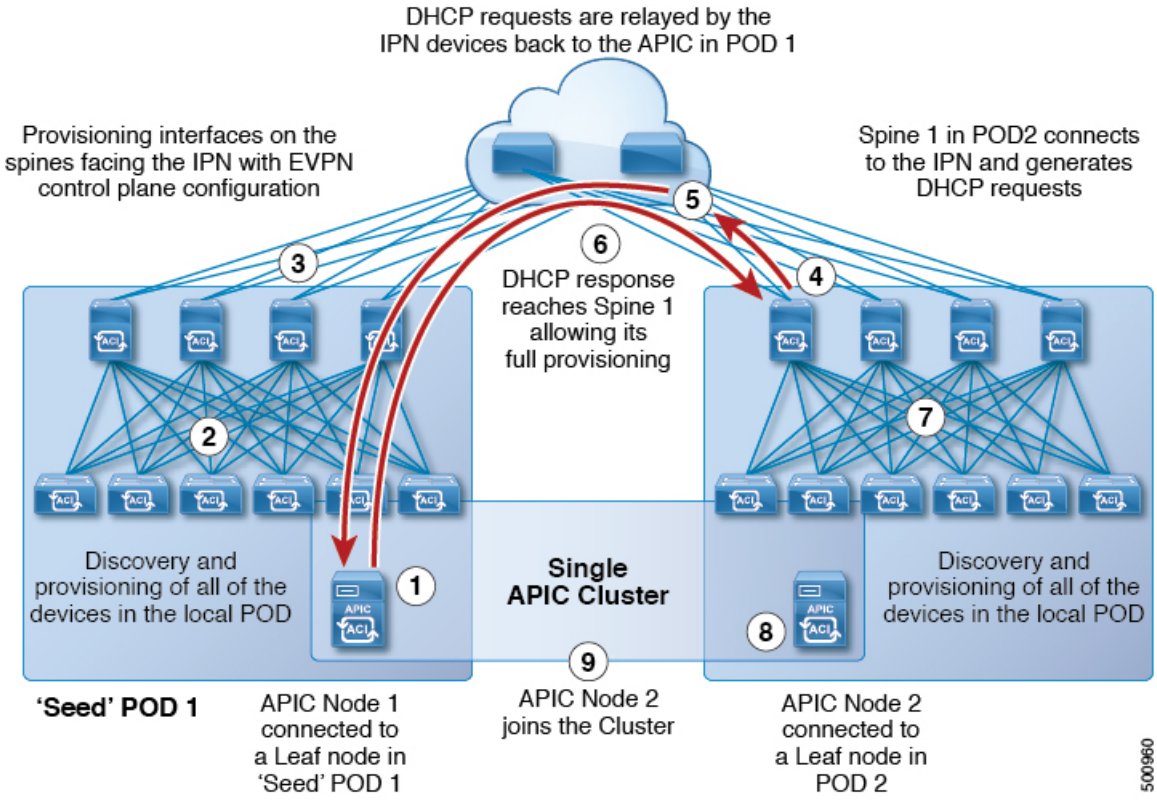
IPN は APIC では管理されません。これは、次の情報が事前する必要があります。

- すべてのポッドの背表紙に接続されているインターフェイスを設定します。VLAN 4 または VLAN 5 を使用し、 **MTU** 9150 のおよび正しい IP アドレスが関連付けられています。リモート リーフ スイッチが、ポッドに含まれている場合は、multipod インターフェイス/サブ-インターフェイスの VLAN 5 を使用します。
- 正しいエリア ID を持つサブインターフェイスで OSPF を有効にします。
- すべての背表紙に接続されている IPN インターフェイスで DHCP リレーを有効にします。
- PIM をイネーブルにします。
- PIM 双方向としてブリッジ ドメイン GIPO 範囲の追加 (**bidir**) の範囲をグループ化 (デフォルトでは 225.0.0.0/8)。

  グループを **bidir** モードが機能の転送を共有ツリーのみ。
- PIM として 239.255.255.240/28 を追加 **bidir** 範囲をグループ化します。
- PIM およびすべての背表紙に接続されたインターフェイスで IGMP を有効にします。

（注） PIM を展開する際に **bidir** 、いつでもでも特定のみすることが特定のマルチキャスト グループ範囲の 1 つのアクティブ RP (ランデブー ポイント) があります。RP の冗長性が活用することで実現そのため、 **ファントム RP** 設定します。希薄モードの冗長性を提供するために使用するエニー キャストまたは MSDP メカニズムはのオプションではありませんマルチキャスト ソースの情報は、Bidir で利用可能なは不要であるため **bidir** 。

図 *29* : 複数ポッドのプロビジョニング



マルチポッド ファブリックを設定する場合の注意事項

マルチポッド ファブリックを設定するには、次の注意事項に従います。

- すべての Cisco Nexus 9000 シリーズ ACI モードのスイッチと、すべての Cisco Nexus 9500 プラットフォーム ACI モード スイッチライン カードおよびファブリック モジュールがマルチポッドをサポートします。Cisco APIC では、3.1(x) リリース以降の場合、これに N9K C9364C スイッチが含まれます。
- 関連付けられたノード グループおよびレイヤ 3 アウト ポリシーを作成します。

- スパイン スイッチを変更する前に、マルチポッド トポロジに参加している運用「アップ」外部リンクが少なくとも 1 個あることを確認します。失敗すると、マルチポッド接続がダウンする可能性があります。
- マルチポッドセットアップをダウングレードする必要があり、単一ポッドにセットアップを変換する必要がある場合（pod1 のみを含む）、ダウングレードを実行する前に、最初に pod-1 のみのコントローラ数にコントローラを縮小し、ほかのポッドからすべてのノードをデコミッションします。TEP プール設定を削除する必要があります。このダウングレードでは、ほかのポッドのすべてのノードがダウンすることに注意してください。
- OSPF 定期エリアのみが、［インフラ］テナントでサポートされています。
- APIC リリース 2.0(2) までマルチポッドは Cisco ACI GOLF でサポートされていません。APIC リリース 2.0 (2) では、2 つの機能は、たとえば、N9K 9312TX などスイッチの名前の末尾に「EX」が付かない Cisco Nexus 9000 スイッチでのみ同じファブリックでサポートされています。2.1(1) のリリース以降、 2 つの機能はマルチポッド トポロジで使用されるすべてのスイッチで、一緒に展開できます。
- マルチポッド ファブリックで、POD 1 のスパインがインフラ テナント L3extOut 1 を使用する場合、他のポッド（POD 2、POD 3）の TOR は同じインフラ L3extOut（L3extOut 1）をレイヤ 3 EVPN コントロール プレーンの接続には使用できません。他のポッドの WAN 接続のトランジットとしてポッドを使用することはサポートされていないため、各ポッドは独自のスパイン スイッチとインフラ L3extOut を使用する必要があります。
- マルチポッド ファブリック セットアップで、新しいスパイン スイッチがポッドに追加される場合、最初にポッド内の少なくとも 1 個のリーフ スイッチに接続する必要があります。これにより、APIC がスパイン スイッチを検出し、ファブリックに参加できるようにします。
- ポッドが作成されポッドにノードが追加された後、ポッドを削除するとファブリック内でアクティブなポッドから古いエントリになります。これは、APIC がオープン ソース DHCP を使用しており、ポッドが削除されると APIC が削除できない一部のリソースを作成するため発生します。
- 前方誤り訂正（FEC）は、すべての 100G トランシーバがデフォルトで、デフォルトで有効です。マルチポッド設定に QSFP 100 G LR4 S/QSFP-100 G-LR4 トランシーバを使用しないでください。
- 次は、ポッド上で Active/Standby Firewalls（FW）のペアを展開するときに必要です。

  シナリオ 1：FW を通過するトラフィックをリダイレクトするため PBR を使用します。

  - サービス グラフの使用を委任し、ACI ファブリックに FW 内部/外部インターフェイスを接続できるようにします。この機能は、2.1(1) リリースから完全にサポートされます。
  - すべてのコンピューティング リーフ ノードからのフローは、アクティブな FW に接続されている境界リーフ ノードに常に送信されます。

  シナリオ 2:ファブリックおよび FW 間の L3Out 接続の使用：

- この機能は、2.0(1) リリースから完全にサポートされます。
- ダイナミック ルーティング（スタティック ルーティングではない）およびCisco ASA (VRRP を使用した FW ではない）でのみサポートされます。
- アクティブな FW はローカル ポッドの BL ノードとのみピアリングします。リーフはファブリックに外部ルーティング情報を挿入します。
- ダイナミック ピアリング セッションは、FW のフェールオーバー後に長期的なトラフィックの停止のため、新しいポッドが再確立されている必要があります。

シナリオ 3：ポッド上で単一の L3Out を使用します。

- 物理リンク（またはローカル ポート チャネル）を持つ単一のリーフ ノードへ接続している Active および Standby FW は、すべての ACI リーフ ノード（E、EX、FX）のリリース 2.1(2e) および 2.2(2e) でサポートされています。
- リーフ ノードのペアに対して、各ポッドの vPC モードに接続されている Active および Standby FW は、リリース 2.3(1) から EX、FX、それ以降の ACI リーフでのみサポートされます。

- ポリシーの名前を変更するなど、マルチポッド L3out を削除し再作成する場合、ファブリックのスパイン スイッチの一部でクリーン リロードを実行する必要があります。マルチポッドL3Outを削除することで、ファブリック内の1個以上のスパイン スイッチがAPICへの接続を失う可能性があり、これらのスパイン スイッチが APIC から更新されたポリシーをダウンロードできなくなります。どのスパインスイッチがそのような状態になるかは、展開されているトポロジによって異なります。この状態から回復するには、これらスパイン スイッチでクリーン リロードを実行する必要があります。スパイン スイッチでコマンドをリロードしたら、**setup-clean-config.sh** コマンドを使用してリロードを実行します。

（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multipod接続を設定する場合は、MTU が両側で適切に設定されていることが重要です。ACI、Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定された MTU 値は IP ヘッダーを考慮に入れています（結果として、最大パケット サイズは、ACI で 9216 バイト、NX-OS および IOS で 9000 バイトに設定されます）。ただし、IOS XR などの他のプラットフォームは、パケット ヘッダーのを除く MTU 値を設定します（結果として最大パケット 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。

Fabric > **Access Policies** > **Global Policies** > **CP MTU Policy** のファブリックのノード（APIC およびスイッチ）により送信された、コントロールプレーン（CP）のグローバルMTUを設定できます。.

マルチポッド トポロジでは、ファブリック外部ポートの MTU 設定は CP MTU 値設定以上にする必要があります。そうしないと、ファブリックの外部ポートはCPMTUパケットをドロップする可能性があります。

IPN または CP MTU を変更する場合、Cisco では CP MTU 値を変更し、次にリモート ポッドのスパイン上のMTU値を変更することをお勧めします。これで、MTUの不一致によりポッド間の接続が失われるリスクが減少します。

ポッドをデコミッションするには、ポッドのすべてのノードをデコミッションします。詳細については、「*Cisco APIC* トラブルシューティング ガイド」の「ポッドのデコミッションと再コミッション」を参照してください。

APIC GUI, リリース 3.1(x) 以降でウィザードを称してマルチポッド ファブリックをセット アップする

Cisco APIC リリース 3.1(x) 以降、GUI にウィザードが追加され、マルチポッド設定をシンプルにします。この章で説明されているマルチポッドを設定する他の方法を引き続き使用できます。ウィザードを使用してマルチポッドを設定するには、このトピックの手順を実行します。

始める前に

ノード グループ ポリシーと L3Out ポリシーがすでに作成されています。

IPN への接続に使用されるスパイン スイッチは、ポッドで少なくとも 1 個のリーフ スイッチに接続されます。

ポッド間ネットワーク（IPN）はすでに設定されています。設定例については、次を参照してください。 Cisco Nexus 9000 の IPN Multipod の設定を例シリーズ スイッチ （291 ページ）

手順

ステップ 1 メニュー バーで、**[ファブリック]** > **[インベントリ]** をクリックします。

ステップ 2 **[ナビゲーション]** ペインで、**[クイック スタート]** をクリックし、**[ノードまたはポッドのセット アップ]** をクリックします。

ステップ 3 **[マルチポッドのセットアップ]** をクリックし、次の詳細情報を設定する手順に従ってください。

- **[ポッドのファブリック]**：ポッド ID を選択し、POD TEP Pool の IP アドレスとサブネットマスクを入力します。
- **[ポッド間のネットワーク]**：コミュニティ名を入力します（**extended:as2-nn4:5:16** にする必要があります）。また、**[ポッド接続プロファイル]** を設定します（データプレーン TEP

Pool ネットマスクを /23 以下に設定する必要があり、一度設定されると削除できません）。また、**[ファブリック外部ルーティング プロファイル]** サブネットを追加します。

（注） **[ピアリング タイプ]** フィールドの **[ルート リフレクタ]** を選択し、今後一部のポイントのコントローラからスパイン スイッチを削除する場合、コントローラからスパイン スイッチを削除する前に、BGP ルート リフレクタ ページのルート リフレクタを無効にすることを忘れないでください。そうしないとエラーが発生します。

ルート リフレクタを無効にするには、[BGP ルート リフレクタ] ページの [ルート リフレクタ ノード] エリアで適切なルート リフレクタを右クリックし、**[削除]** を選択します。BGP ルート リフレクタ ページにアクセスする方法については、MP-BGP ルート リフレクタ （159 ページ） の「GUI を使用した MP-BGP ルート リフレクタの設定」セクションを参照してください。

- **[接続]**：OSPF の詳細、スパイン スイッチのルータ Id、スパイン スイッチのサブインターフェイスを入力します。

（注） ポッド間ネットワーク（IPN）リンクへのスパイン スイッチ リンクのデフォルトまたは継承 MTU は 9150 です。スパインに接続されているすべての IPN インターフェイスで、9150 の MTU 値を設定していることを確認します。

IPN 経由で外部接続の一部を担う既存のポッドからすべてのスパイン ノードを追加し、作成される新しいポッドからノードを追加します。

ステップ 4 **[更新]** をクリックし、**[完了]** をクリックします。
[ポッド ファブリック セットアップ ポリシー] ページには、ポッドの詳細が表示されます。

APIC GUI を使用したマルチポッド ファブリックの設定

始める前に

- ノード グループ ポリシーと L3Out ポリシーがすでに作成されています。
- IPN はすでに設定されています。IPN の設定例については、Cisco Nexus 9000 の IPN Multipod の設定を例シリーズ スイッチ （291 ページ）を参照してください。
- ポッド間ネットワーク (IPN) を接続するために使用されるスパイン スイッチは、少なくとも 1つの、ポッドのリーフ スイッチに接続しています。

手順

ステップ 1 メニュー バーで、**Fabric** > **Inventory** をクリックします。

ステップ 2 **Navigation** ウィンドウで、**Pod Fabric Setup Policy** を右クリックし、**Setup Pods** をクリックし、次の手順を実行します:

a) **Fabric Setup Policies** ダイアログボックスで、**Pod ID** と **TEP Pool** の IP アドレスとネットマスクを入力します。

（注） いったん TEP プールを競ってしたら、削除するべきではありません。

b) [+] をクリックして **Remote Pools** を作成し、リモート ID とリモート プール (IP アドレスとサブネット) を入力し、**Update** をクリックします。

c) **Submit** をクリックします。

ステップ 3 **Navigation** ウィンドウで、**Pod Fabric Setup Policy** を右クリックし、**Create Multi-Pod** をクリックします。

ステップ 4 **Create Multi-Pod** ダイアログボックスで、次のエントリを作成します:

a) **Community** フィールドには、コミュニティ名を入力します。マルチポッドで許可されているのは、コミュニティ名 **extended:as2-nn4:5:16** だけです。

b) ルート ピアリング タイプとして、**Peering Type** フィールドでで、**Full Mesh** または **Route Reflector** のいずれかを選択します。

（注） **Route Reflector** を **Peering Type** フィールドで選択した場合には、将来のある時点でスパイン スイッチからコントローラを外そうとするとき、コントローラからスパイン スイッチを外す前に、[BGP Route Reflector] ページでルート リフレクタを無効にする必要があることを忘れてはなりません。そうしないとエラーが発生します。

ルート リフレクタを無効にするには、[BGP ルート リフレクタ] ページの [ルート リフレクタ ノード] エリアで適切なルート リフレクタを右クリックし、**[削除]** を選択します。[BGP Route Reflector] ページへのアクセスの手順については、MP-BGP ルート リフレクタ （159 ページ）の「Configuring an MP-BGP Route Reflector Using the GUI」のセクションを参照してください。

c) **Pod Connection Profile** テーブルを展開し、ポッドごとに **Dataplane TEP** アドレスを入力します。

d) **Fabric External Routing Profile** テーブルを展開し、プロファイルの **Name** と **Subnet** アドレスを入力します。**Submit** をクリックします。

ステップ 5 **Navigation** ウィンドウで、**Pod Fabric Setup Policy** を右クリックし、**Create Routed Outside for Multipod** を選択し、次の手順を実行します:

a) BGP、OSPF の両方を有効にして、IPN で設定されているとおりに、OSPF の詳細を入力します。

b) **Next** をクリックします。

c) **Spines** テーブルで、ノードごとに **Router ID** を入力し、**Update** をクリックします。

d) ドロップダウンリストから **OSPF Policy** を選択するか、 **Create OSPF Interface Policy** を選択して作成し、**Submit** をクリックします。

（注） スパインからポッド間ネットワーク (IPN) へのリンクのデフォルトまたは継承した MTU は 9150 です。スパインに接続されているすべての IPN インターフェイスの MTU 値が 9150 に設定されていることを確認してください。

e) IPN を通して外部接続に参加する、既存のポッドからのすべてのスパイン ノードに対してこれを繰り返し、作成される新しいポッドからのノードを追加します。

f) **Routed Sub-Interfaces** テーブルを展開し、**Path** フィールドでインターフェイス ID を探し、**IPv4 Primary Address** フィールドにアドレス情報を入力します。**Update** をクリックし、**Finish** をクリックします。

（注）
- ポッド 2 のスパインが [Fabric Membership] の下に表示されるはずなので、確認できます。
- **手順 6**に進む前に、このスパインのノード ID と名前が設定されていることを確認してください。

ステップ 6 単一のポッドの L3Out を設定するには、**Navigation** ウィンドウで、**Pod Fabric Setup Policy** を右クリックし、**Config Routed Outside for a Pod** を選択し、次の手順を実行します:

a) **Spines** テーブルを展開し、ノードごとの **outer ID** を入力します。それぞれの後に **Update** をクリックします。

b) **Routed Sub-Interfaces** テーブルを展開し、**Path** フィールドでインターフェイス ID を探し、**IPv4 Primary Address** フィールドにアドレス情報を入力します。**Update** をクリックし、**Submit** をクリックします。

これによってマルチポッドの設定は完了です。

ステップ 7 マルチポッドの設定を確認するには、メニューバーで**Tenants**>**Infra** をクリックし、**Networking** と **External Routed Networks** を展開します。

マルチポッド L3Out をクリックして詳細を表示します。

ポッド 2 スパインは、TEP IP アドレスでアクティブになりました。ポッド 2 の各リーフは表示されるようになっており、そのノード ID と名前は確認することができます。

NX-OS は、CLI を使用して Multipod ファブリックの設定

始める前に

- ノード グループ ポリシーと L3Out ポリシーがすでに作成されています。

手順

ステップ 1 次の例に示すように、multipod を設定します。

例：

```
ifav4-ifc1#  show run system
# Command: show running-config system
# Time: Mon Aug  1 21:32:03 2016
  system cluster-size 3
  system switch-id FOX2016G9DW 204 ifav4-spine4 pod 2
  system switch-id SAL1748H56D 201 ifav4-spine1 pod 1
  system switch-id SAL1803L25H 102 ifav4-leaf2 pod 1
  system switch-id SAL1819RXP4 101 ifav4-leaf1 pod 1
  system switch-id SAL1931LA3B 203 ifav4-spine2 pod 2
  system switch-id SAL1934MNY0 103 ifav4-leaf3 pod 1
  system switch-id SAL1934MNY3 104 ifav4-leaf4 pod 1
  system switch-id SAL1938P7A6 202 ifav4-spine3 pod 1
  system switch-id SAL1938PHBB 105 ifav4-leaf5 pod 2
  system switch-id SAL1942R857 106 ifav4-leaf6 pod 2
  system pod 1 tep-pool 10.0.0.0/16
  system pod 2 tep-pool 10.1.0.0/16
ifav4-ifc1#
```

ステップ 2 次の例のよ、VLAN ドメインを設定します。

例：

```
ifav4-ifc1# show running-config vlan-domain l3Dom
# Command: show running-config vlan-domain l3Dom
# Time: Mon Aug  1 21:32:31 2016
  vlan-domain l3Dom
    vlan 4
    exit
ifav4-ifc1#
```

ステップ 3 次の例のよ、ファブリックの外部接続を設定します。

例：

```
ifav4-ifc1# show running-config fabric-external
# Command: show running-config fabric-external
# Time: Mon Aug  1 21:34:17 2016
  fabric-external 1
    bgp evpn peering
    pod 1
      interpod data hardware-proxy 100.11.1.1/32
      bgp evpn peering
      exit
    pod 2
      interpod data hardware-proxy 200.11.1.1/32
      bgp evpn peering
      exit
    route-map interpod-import
      ip prefix-list default permit 0.0.0.0/0
      exit
    route-target extended 5:16
    exit
ifav4-ifc1#
```

ステップ 4 スパイン スイッチ インターフェイスと次の例のよの OSPF 設定を構成します。

例：

```
# Command: show running-config spine
# Time: Mon Aug  1 21:34:41 2016
  spine 201
    vrf context tenant infra vrf overlay-1
      router-id 201.201.201.201
```

```
    exit
  interface ethernet 1/1
    vlan-domain member l3Dom
    exit
  interface ethernet 1/1.4
    vrf member tenant infra vrf overlay-1
    ip address 201.1.1.1/30
    ip router ospf default area 1.1.1.1
    ip ospf cost 1
    exit
  interface ethernet 1/2
    vlan-domain member l3Dom
    exit
  interface ethernet 1/2.4
    vrf member tenant infra vrf overlay-1
    ip address 201.2.1.1/30
    ip router ospf default area 1.1.1.1
    ip ospf cost 1
    exit
  router ospf default
    vrf member tenant infra vrf overlay-1
      area 1.1.1.1 loopback 201.201.201.201
      area 1.1.1.1 interpod peering
      exit
    exit
  exit
spine 202
  vrf context tenant infra vrf overlay-1
    router-id 202.202.202.202
    exit
  interface ethernet 1/2
    vlan-domain member l3Dom
    exit
  interface ethernet 1/2.4
        vrf member tenant infra vrf overlay-1
    ip address 202.1.1.1/30
    ip router ospf default area 1.1.1.1
    exit
  router ospf default
    vrf member tenant infra vrf overlay-1
      area 1.1.1.1 loopback 202.202.202.202
      area 1.1.1.1 interpod peering
      exit
    exit
  exit
spine 203
  vrf context tenant infra vrf overlay-1
    router-id 203.203.203.203
    exit
  interface ethernet 1/1
    vlan-domain member l3Dom
    exit
  interface ethernet 1/1.4
    vrf member tenant infra vrf overlay-1
    ip address 203.1.1.1/30
    ip router ospf default area 0.0.0.0
    ip ospf cost 1
    exit
  interface ethernet 1/2
    vlan-domain member l3Dom
    exit
  interface ethernet 1/2.4
    vrf member tenant infra vrf overlay-1
    ip address 203.2.1.1/30
```

```
      ip router ospf default area 0.0.0.0
      ip ospf cost 1
      exit
    router ospf default
      vrf member tenant infra vrf overlay-1
        area 0.0.0.0 loopback 203.203.203.203
        area 0.0.0.0 interpod peering
        exit
      exit
    exit
  spine 204
    vrf context tenant infra vrf overlay-1
      router-id 204.204.204.204
      exit
    interface ethernet 1/31
      vlan-domain member l3Dom
      exit
    interface ethernet 1/31.4
      vrf member tenant infra vrf overlay-1
      ip address 204.1.1.1/30
      ip router ospf default area 0.0.0.0
      ip ospf cost 1
      exit
    router ospf default
      vrf member tenant infra vrf overlay-1
        area 0.0.0.0 loopback 204.204.204.204
        area 0.0.0.0 interpod peering
        exit
      exit
    exit
ifav4-ifc1#
```

REST API を使用したマルチポッド ファブリックの設定

手順

ステップ 1 Csico APIC へのログイン：

例：

```
http://<apic-name/ip>:80/api/aaaLogin.xml

data: <aaaUser name="admin" pwd="ins3965!”/>
```

ステップ 2 TEP プールの設定：

例：

```
http://<apic-name/ip>:80/api/policymgr/mo/uni/controller.xml

<fabricSetupPol status=''>
    <fabricSetupP podId="1" tepPool="10.0.0.0/16" />
    <fabricSetupP podId="2" tepPool="10.1.0.0/16" status='' />
</fabricSetupPol>
```

ステップ 3 ノード ID ポリシーの設定：

例：

```
http://<apic-name/ip>:80/api/node/mo/uni/controller.xml

<fabricNodeIdentPol>
<fabricNodeIdentP serial="SAL1819RXP4" name="ifav4-leaf1" nodeId="101" podId="1"/>
<fabricNodeIdentP serial="SAL1803L25H" name="ifav4-leaf2" nodeId="102" podId="1"/>
<fabricNodeIdentP serial="SAL1934MNY0" name="ifav4-leaf3" nodeId="103" podId="1"/>
<fabricNodeIdentP serial="SAL1934MNY3" name="ifav4-leaf4" nodeId="104" podId="1"/>
<fabricNodeIdentP serial="SAL1748H56D" name="ifav4-spine1" nodeId="201" podId="1"/>
<fabricNodeIdentP serial="SAL1938P7A6" name="ifav4-spine3" nodeId="202" podId="1"/>
<fabricNodeIdentP serial="SAL1938PHBB" name="ifav4-leaf5" nodeId="105" podId="2"/>
<fabricNodeIdentP serial="SAL1942R857" name="ifav4-leaf6" nodeId="106" podId="2"/>
<fabricNodeIdentP serial="SAL1931LA3B" name="ifav4-spine2" nodeId="203" podId="2"/>
<fabricNodeIdentP serial="FGE173400A9" name="ifav4-spine4" nodeId="204" podId="2"/>
</fabricNodeIdentPol>
```

ステップ 4 インフラ L3Out および外部接続プロファイルの設定：

例：

```
http://<apic-name/ip>:80/api/node/mo/uni.xml

<polUni>

<fvTenant descr="" dn="uni/tn-infra" name="infra" ownerKey="" ownerTag="">

   <l3extOut descr="" enforceRtctrl="export" name="multipod" ownerKey="" ownerTag=""
targetDscp="unspecified" status=''>
      <ospfExtP areaId='0' areaType='regular' status=''/>
      <bgpExtP status='' />
      <l3extRsEctx tnFvCtxName="overlay-1"/>
     <l3extProvLbl descr="" name="prov_mp1" ownerKey="" ownerTag="" tag="yellow-green"/>


      <l3extLNodeP name="bSpine">
         <l3extRsNodeL3OutAtt rtrId="201.201.201.201" rtrIdLoopBack="no"
tDn="topology/pod-1/node-201">
            <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
            <l3extLoopBackIfP addr="201::201/128" descr="" name=""/>
            <l3extLoopBackIfP addr="201.201.201.201/32" descr="" name=""/>
         </l3extRsNodeL3OutAtt>

         <l3extRsNodeL3OutAtt rtrId="202.202.202.202" rtrIdLoopBack="no"
tDn="topology/pod-1/node-202">
            <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
            <l3extLoopBackIfP addr="202::202/128" descr="" name=""/>
            <l3extLoopBackIfP addr="202.202.202.202/32" descr="" name=""/>
         </l3extRsNodeL3OutAtt>

         <l3extRsNodeL3OutAtt rtrId="203.203.203.203" rtrIdLoopBack="no"
tDn="topology/pod-2/node-203">
            <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
            <l3extLoopBackIfP addr="203::203/128" descr="" name=""/>
            <l3extLoopBackIfP addr="203.203.203.203/32" descr="" name=""/>
         </l3extRsNodeL3OutAtt>

         <l3extRsNodeL3OutAtt rtrId="204.204.204.204" rtrIdLoopBack="no"
tDn="topology/pod-2/node-204">
            <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
            <l3extLoopBackIfP addr="204::204/128" descr="" name=""/>
            <l3extLoopBackIfP addr="204.204.204.204/32" descr="" name=""/>
         </l3extRsNodeL3OutAtt>
```

```
         <l3extLIfP name='portIf'>
          <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-1/paths-201/pathep-[eth1/1]"
 encap='vlan-4'  ifInstT='sub-interface' addr="201.1.1.1/30" />
          <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-1/paths-201/pathep-[eth1/2]"
 encap='vlan-4'  ifInstT='sub-interface' addr="201.2.1.1/30" />
          <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-1/paths-202/pathep-[eth1/2]"
 encap='vlan-4'  ifInstT='sub-interface' addr="202.1.1.1/30" />
          <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-2/paths-203/pathep-[eth1/1]"
 encap='vlan-4'  ifInstT='sub-interface' addr="203.1.1.1/30" />
          <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-2/paths-203/pathep-[eth1/2]"
 encap='vlan-4'  ifInstT='sub-interface' addr="203.2.1.1/30" />
           <l3extRsPathL3OutAtt descr='asr'
tDn="topology/pod-2/paths-204/pathep-[eth4/31]" encap='vlan-4'  ifInstT='sub-interface'
 addr="204.1.1.1/30" />

           <ospfIfP>
               <ospfRsIfPol tnOspfIfPolName='ospfIfPol'/>
           </ospfIfP>

         </l3extLIfP>
      </l3extLNodeP>

      <l3extInstP descr="" matchT="AtleastOne" name="instp1" prio="unspecified"
targetDscp="unspecified">
          <fvRsCustQosPol tnQosCustomPolName=""/>
      </l3extInstP>
   </l3extOut>

  <fvFabricExtConnP descr="" id="1" name="Fabric_Ext_Conn_Pol1" rt="extended:as2-nn4:5:16"
 status=''>
      <fvPodConnP descr="" id="1" name="">
         <fvIp addr="100.11.1.1/32"/>
      </fvPodConnP>
      <fvPodConnP descr="" id="2" name="">
         <fvIp addr="200.11.1.1/32"/>
      </fvPodConnP>
      <fvPeeringP descr="" name="" ownerKey="" ownerTag=""
type="automatic_with_full_mesh"/>
     <l3extFabricExtRoutingP descr="" name="ext_routing_prof_1" ownerKey="" ownerTag="">

         <l3extSubnet aggregate="" descr="" ip="100.0.0.0/8" name=""
scope="import-security"/>
         <l3extSubnet aggregate="" descr="" ip="200.0.0.0/8" name=""
scope="import-security"/>
         <l3extSubnet aggregate="" descr="" ip="201.1.0.0/16" name=""
scope="import-security"/>
         <l3extSubnet aggregate="" descr="" ip="201.2.0.0/16" name=""
scope="import-security"/>
         <l3extSubnet aggregate="" descr="" ip="202.1.0.0/16" name=""
scope="import-security"/>
         <l3extSubnet aggregate="" descr="" ip="203.1.0.0/16" name=""
scope="import-security"/>
         <l3extSubnet aggregate="" descr="" ip="203.2.0.0/16" name=""
scope="import-security"/>
         <l3extSubnet aggregate="" descr="" ip="204.1.0.0/16" name=""
scope="import-security"/>
      </l3extFabricExtRoutingP>
   </fvFabricExtConnP>
</fvTenant>
</polUni>
```

Cisco Nexus 9000 の IPN Multipod の設定を例シリーズ スイッチ

手順

設定例

例：

```
Sample IPN configuration for Cisco Nexus 9000 series switches:
================================

  (pod1-spine1)-----2/7[ IPN-N9K ]2/9-----(pod2-spine1)


feature dhcp
feature pim

# Enable Jumbo frames
policy-map type network-qos jumbo
  class type network-qos class-default
    mtu 9216

system qos
  service-policy type network-qos jumbo


service dhcp
ip dhcp relay
ip pim ssm range 232.0.0.0/8

# Create a new VRF for Multipod.
vrf context fabric-mpod
  ip pim rp-address 12.1.1.1 group-list 225.0.0.0/8 bidir
  ip pim rp-address 12.1.1.1 group-list 239.255.255.240/28 bidir
  ip pim ssm range 232.0.0.0/8

interface Ethernet2/7
  no switchport
  mtu 9150
  no shutdown

interface Ethernet2/7.4
  description pod1-spine1
  mtu 9150
  encapsulation dot1q 4
  vrf member fabric-mpod
  ip address 201.1.2.2/30
  ip router ospf a1 area 0.0.0.0
  ip pim sparse-mode
  ip dhcp relay address 10.0.0.1
  ip dhcp relay address 10.0.0.2
  ip dhcp relay address 10.0.0.3
  no shutdown


interface Ethernet2/9
```

```
  no switchport
  mtu 9150
  no shutdown

interface Ethernet2/9.4
  description to pod2-spine1
  mtu 9150
  encapsulation dot1q 4
  vrf member fabric-mpod
  ip address 203.1.2.2/30
  ip router ospf a1 area 0.0.0.0
  ip pim sparse-mode
  ip dhcp relay address 10.0.0.1
  ip dhcp relay address 10.0.0.2
  ip dhcp relay address 10.0.0.3
  no shutdown

interface loopback29
  vrf member fabric-mpod
  ip address 12.1.1.1/32

router ospf a1
  vrf fabric-mpod
    router-id 29.29.29.29
```

APIC をあるポッドから別のポッドに移動する

マルチポッドのセットアップにおいて、APIC をあるポッドから別のポッドに移動するには、次の手順に従います。

手順

ステップ 1 クラスタ内の APIC をデコミッションします。

a) メニューバーで、 **System** > **Controllers** を選択します。

b) **Navigation** ウィンドウで、 **Controllers** > **apic_controller_name** > **Cluster as Seen by Node** を展開します。

c) **Navigation** ウィンドウで、**apic_controller_name** をクリックします。これは、クラスタ内のものですが、デコミッションしているコントローラではありません。

d) 継続する前に、**Work** ウィンドウで、クラスタの **Health State** (**Active Controllers** サマリテーブルに示されているもの) が **Fully Fit** になっていることを確認します。

e) **Work** ウィンドウで、**Actions** > **Decommission** をクリックします。

f) **Yes** をクリックします。
解放されたコントローラは [Operational State] 列に [Unregistered] と表示されます。コントローラは稼動対象外になり、**Work** ウィンドウには表示されなくなります。

ステップ 2 デコミッションされた APIC を目的のポッドに移動します。

ステップ 3 次のコマンドを入力して、APIC をリブートします。

```
apic1# acidiag touch setup
apic1# acidiag reboot
```

ステップ 4 ポッドの ID 番号を、APIC の現在のポッドを反映するように変更します。

a) Cisco Integrated Management Controller (CIMC) にログインします。

b) ポッド ID のプロンプトで、ポッド ID を入力します。

（注） **TEP Pool** のアドレス情報は変更しないでください。

ステップ 5 APIC をリコミッションします。

a) メニュー バーで、 **SYSTEM** > **Controllers** を選択します。

b) **Navigation** ウィンドウで、 **Controllers** > **apic_controller_name** > **Cluster as Seen by Node** を展開します。

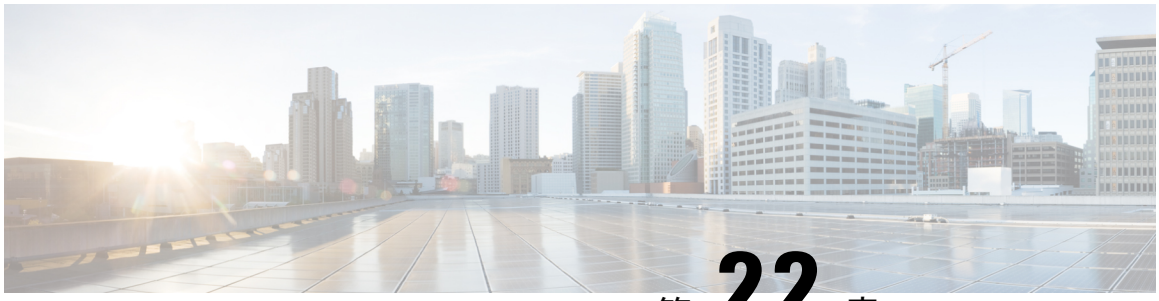
c) 継続する前に、**Work** ウィンドウで、**Active Controllers** サマリ テーブルのクラスタの **Health State** が **Fully Fit** になっていることを確認します。

d) **Work** ウィンドウで、**Unregistered** と **Operational State** カラムに表示されている、デコミッションされたコントローラをクリックします。

e) **Work** ウィンドウで、**Actions** > **Commission** をクリックします。

f) **Confirmation** ダイアログボックスで **Yes** をクリックします。

g) コミッションされた Cisco APIC コントローラが動作状態であり、ヘルス ステータスが、**Fully Fit** であることを確認します。



第 22 章

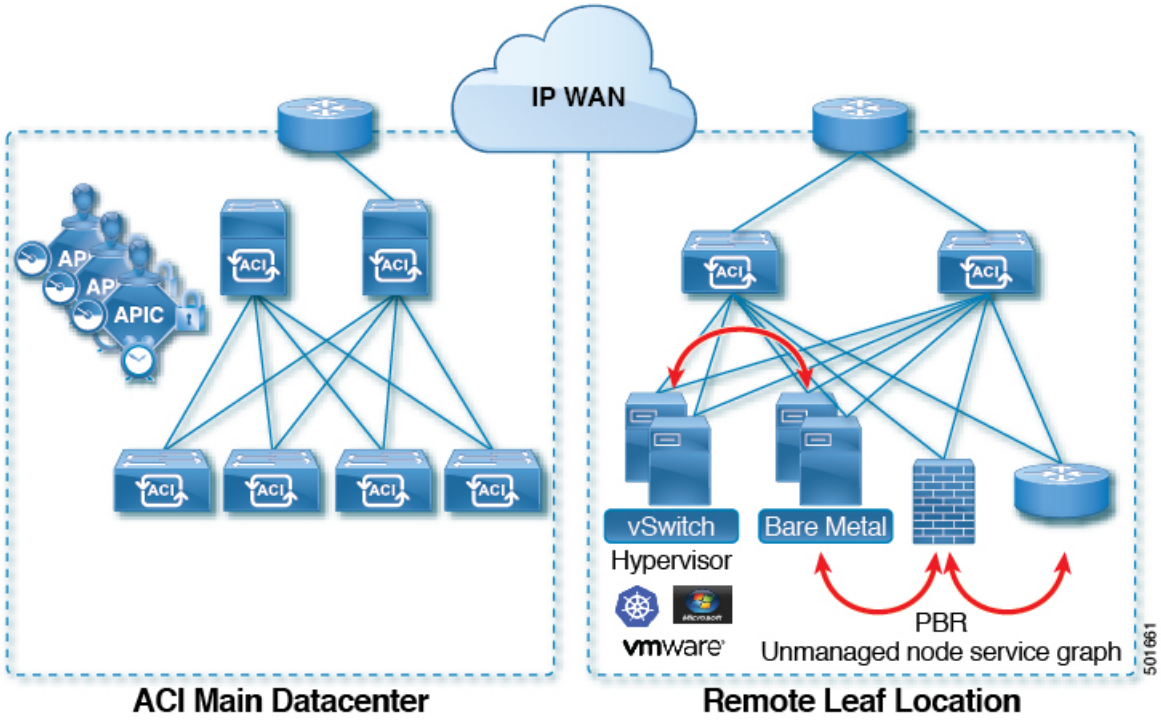
リモート リーフ スイッチ

この章の内容は、次のとおりです。

ACI ファブリックのリモート リーフ スイッチについて

ACI ファブリックの展開では、ローカル スパイン スイッチまたは APIC が接続されていない Cisco ACI リーフ スイッチのリモート データセンタに、ACI サービスと APIC 管理を拡張できます。

図 *30 :* リモート リーフ トポロジ



リモート リーフ スイッチがファブリックの既存のポッドに追加されます。メイン データ センタに展開されるすべてのポリシーはリモート スイッチで展開され、ポッドに属するローカル リーフ スイッチのように動作します。このトポロジでは、すべてのユニキャスト トラフィックはレイヤ 3 上の VXLAN を経由します。レイヤ 2 ブロードキャスト、不明なユニキャスト、マルチキャスト（BUM）メッセージは、マルチキャストを使用することなく、 Head End Replication（HER）トンネルを使用して送信されます。リモート サイトのすべてのローカル トラフィックは、物理または仮想にかかわらずエンドポイント間で直接切り替えられます。スパイン スイッチ プロキシを使用する必要があるすべてのトラフィックは、メイン データ センタに転送されます。

APIC システムは、起動時にリモート リーフ スイッチを検出します。その時点から、ファブリックの一部として APIC で管理できます。

（注）

- VRF 間のすべてのトラフィックは、転送される前にスパイン スイッチに移動します。
- リモート リーフを解除する前に、vPC を最初に削除する必要があります。

ウィザードを使用するか（使用しない場合も）、REST API または NX-OS スタイル CLI を使用して、APIC GUI のリモート リーフを設定できます。

リモートのリーフ ハードウェアの要件

リモートのリーフ スイッチの機能には、次のスイッチがサポートされています。

ファブリック スパイン スイッチ

WAN ルータに接続された ACI メイン データ センターにスパイン スイッチでの次のスパイン スイッチがサポートされています。

- 固定スパイン スイッチの Cisco Nexus 9000 シリーズ N9K C9364C

  N9K-X9732C-EX または N9K-X9736C-FX ラインカードをモジュラ スパイン スイッチ

- 古い生成スパイン スイッチは、固定スパイン スイッチ N9K C9336PQ または N9K X9736PQ ラインカードでモジュラ スパイン スイッチなどのメイン データ センターではサポートが次世代のみのスパイン スイッチは、WAN への接続をサポートします。

リモート リーフ スイッチ

- リモートのリーフ スイッチ、後で (たとえば N9K-C93180LC-EX) EX で終了する名前と Cisco Nexus 9000 シリーズ スイッチのみがサポートされています。

  （注） Cisco Nexus 9000 N9K-C9336C-FX スイッチは、リモートのリーフ スイッチのサポートされていません。

- リモートのリーフ スイッチする必要がありますにイメージを実行する、スイッチ 13.1.x 以降 (aci n9000 dk9.13.1.x.x.bin) 検出できる前にします。これにより、リーフ スイッチでの手動アップグレードが必要があります。

制約事項と制限

（注） Cisco APIC のリリースでは、以前にサポートされていませんでした 3.2(x) が、次の機能がサポートされます。

- リモートのリーフ スイッチに接続されている FEX デバイス
- リモートのリーフ スイッチまたはリモート リーフ スイッチとローカル リーフ スイッチ間でという原子カウンタという
- Cisco VXLAN での VLAN とシスコの AV で AV
- VXLAN での VLAN と ACI の仮想エッジで Cisco ACI 仮想エッジ

リモート リーフ機能では、次の導入と設定がサポートされていません。

- APIC コントローラは、リモートのリーフ スイッチに直接接続
- (この制限は、リリース 3.1 以降に適用) vPC ドメインでのリモート リーフ スイッチで孤立ポート チャネルまたは物理ポート
- コンシューマ、プロバイダー、およびサービス ノードがすべてスイッチ vPC モードでは、リモートのリーフに接続されている場合に、リモート ロケーション内で転送ローカル トラフィックがサポートのみとサービス ノードの統合がなければ、

このリリースでは、次の機能を除くで、リモートのリーフ スイッチでは、ファブリックおよびテナントの完全なポリシーがサポートされています。

- ACI マルチサイト
- レイヤ 2 (スタティック Epg) を除く接続外部
- 802.1 q トンネリング
- EPG のための Q-in-Q カプセル化マッピング
- VzAny 契約とサービスをコピーします。
- リモートのリーフ スイッチの FCoE 接続
- ブリッジ ドメインまたは Epg のカプセル化をフラッディングします。
- 高速リンク フェールオーバー ポリシー
- 遠隔地での管理対象のサービス グラフに接続されたデバイス
- NetFlow
- トラフィック ストーム制御
- クラウド秒および MacSec 暗号化
- ファーストホップ セキュリティ
- PTP
- レイヤ 3 マルチキャスト リモート リーフ スイッチ上のルーティング
- リモートのリーフ スイッチでの PBR トラッキング
- Openstack および Kubernetes VMM ドメイン
- メンテナンス モード
- ウィザードのトラブルシューティング
- 遠隔地での中継 L3Out
- 同じリモート データ センターで同じポッドおよびポッド全体の 2 つのリモート リーフ スイッチ間で直接トラフィックの転送

WAN ルータとリモート リーフ設定の注意事項

リモート リーフが検出され APIC 管理に組み込まれる前に、WAN ルータとリモート リーフ スイッチを設定する必要があります。

次の要件に従い、ファブリック スパイン スイッチの外部インターフェイスとリモート リーフ スイッチ ポートに接続する WAN ルータを接続します。

WAN ルータ

- エリア ID、タイプ、コストなど、同じ詳細を有するインターフェイスで OSPF を有効にします。
- メイン ファブリックの各 APIC の IP アドレスにつながるインターフェイスで DHCP リレーを設定します。
- スパイン スイッチで VLAN 5 インターフェイスに接続する WAN ルータのインターフェイスは、通常のマルチポッド ネットワークに接続するインターフェイス以外に、異なる VRF に存在する必要があります。

リモート リーフ スイッチ

- ファブリック ポートの 1 つから直接接続して、アップストリーム ルータにリモート リーフ スイッチを接続します。アップストリーム ルータへの次の接続がサポートされています。
  - 40 Gbps 以上の接続
  - QSFP-SFP アダプタでは、1/10 G SFP がサポートされています

  WAN の帯域幅は最小で 100 Mbps、最大 。サポートされている遅延は 300 ミリ秒です。
- 上記が推奨されますが、vPC とリモート リーフ スイッチのペアを接続する必要はありません。vPC の両端にあるスイッチは、同じリモート データセンタのリモート リーフ スイッチである必要があります。
- 一意の IP アドレスを持つ VLAN 4 でレイヤ 3 サブインターフェイスとしてノース バウンド インターフェイスを設定します。

  リモートのリーフ スイッチからルータに 1 個以上のインターフェイスを接続する場合、一意の IP アドレスで各インターフェイスを設定します。
- インターフェイスで OSPF を有効にします。
- リモート リーフ スイッチ内の TEP プール サブネットの IP アドレスは、ポッド TEP サブネット プールと重複しないようにする必要があります。使用されるサブネットは /24 以下である必要があります。
- マルチポッドがサポートされますが、リモート リーフ機能は必要ありません。

- 単一ポッド ファブリックのポッドをリモート リーフ スイッチに接続するとき、スパイン スイッチから WAN ルータへ 、リモート リーフ スイッチから WAN ルータへ L3Out を設定し、これは両方ともスイッチ インターフェイスで VLAN-4 を使用します。
- マルチポッド ファブリックのポッドをリモート リーフ スイッチに接続するとき、スパイン スイッチから WAN ルータへ 、リモート リーフ スイッチから WAN ルータへ L3Out を設定し、これは両方ともスイッチ インターフェイスで VLAN-4 を使用します。また、VLAN-5 を使用してマルチポッド内部 L3Out を設定し、リモート リーフ スイッチを宛先としてポッドを通過するトラフィックをサポートします。VLAN 4 および VLAN 5 を使用する限り、通常のマルチポッドおよびマルチポッド内部接続は、同じ物理インターフェイスで設定できます。
- マルチポッド内部L3Outを設定している場合、通常のマルチポッドL3Outとして同じルータ ID を使用しますが、ルータ ID の **[ループバック アドレスとしてルータ ID を使用する]** オプションを選択解除して、異なるループバックIPアドレスを設定します。これでECMPが機能します。

REST API を使用したリモート リーフ スイッチの設定

Cisco APIC を有効にして IPN ルータとリモートリーフ スイッチを検出し接続するには、このトピックの手順を実行します。

この例では、マルチポッド トポロジで、ポッドにリモート リーフ スイッチが接続されていることを前提としています。VRF オーバーレイ 1 とともに、インフラ テナントに設定されている 2 個の L3Outs が含まれます。

- 1 個は VLAN 4 に設定され、リモート リーフ スイッチとスパイン スイッチ両方が WAN ルータに接続されている必要があります。
- 1 個はマルチポッド内部 L3Out が VLAN5 で設定されており、一緒に展開する場合はマルチポッドとリモート リーフ機能に必要です。

手順

ステップ 1 ポッドに接続されるように 2 個のリモート リーフ スイッチに TEP プールを定義するには、次の例のように XML で POST を送信します。

例：

```
<fabricSetupPol>
      <fabricSetupP tepPool="10.0.0.0/16" podId="1" >
           <fabricExtSetupP tepPool="30.0.128.0/20" extPoolId="1"/>
     </fabricSetupP>
     <fabricSetupP tepPool="10.1.0.0/16" podId="2" >
          <fabricExtSetupP tepPool="30.1.128.0/20" extPoolId="1"/>
     </fabricSetupP>
</fabricSetupPol>
```

ステップ 2 ノードのアイデンティティ ポリシーを定義するには、次の例のように XML で POST を送信します。

例：

```
<fabricNodeIdentPol>
     <fabricNodeIdentP serial="SAL17267Z7W" name="leaf1" nodeId="101" podId="1"
extPoolId="1" nodeType="remote-leaf-wan"/>
     <fabricNodeIdentP serial="SAL27267Z7W" name="leaf2" nodeId="102" podId="1"
extPoolId="1" nodeType="remote-leaf-wan"/>
     <fabricNodeIdentP serial="SAL17267Z7Z" name="leaf3" nodeId="201" podId="1"
extPoolId="1" nodeType="remote-leaf-wan"/>
     <fabricNodeIdentP serial="SAL17267Z7Z" name="leaf4" nodeId="201" podId="1"
extPoolId="1" nodeType="remote-leaf-wan"/>
</fabricNodeIdentPol>
```

ステップ 3 ファブリック外部接続プロファイルを設定するには、次の例のように XML で POST を送信します。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<imdata totalCount="1">
     <fvFabricExtConnP dn="uni/tn-infra/fabricExtConnP-1" id="1"
name="Fabric_Ext_Conn_Pol1" rt="extended:as2-nn4:5:16" siteId="0">
           <l3extFabricExtRoutingP name="test">
                <l3extSubnet ip="150.1.0.0/16" scope="import-security"/>
           </l3extFabricExtRoutingP>
          <l3extFabricExtRoutingP name="ext_routing_prof_1">
               <l3extSubnet ip="204.1.0.0/16" scope="import-security"/>
               <l3extSubnet ip="209.2.0.0/16" scope="import-security"/>
               <l3extSubnet ip="202.1.0.0/16" scope="import-security"/>
               <l3extSubnet ip="207.1.0.0/16" scope="import-security"/>
               <l3extSubnet ip="200.0.0.0/8" scope="import-security"/>
               <l3extSubnet ip="201.2.0.0/16" scope="import-security"/>
               <l3extSubnet ip="210.2.0.0/16" scope="import-security"/>
               <l3extSubnet ip="209.1.0.0/16" scope="import-security"/>
               <l3extSubnet ip="203.2.0.0/16" scope="import-security"/>
               <l3extSubnet ip="208.1.0.0/16" scope="import-security"/>
               <l3extSubnet ip="207.2.0.0/16" scope="import-security"/>
               <l3extSubnet ip="100.0.0.0/8" scope="import-security"/>
               <l3extSubnet ip="201.1.0.0/16" scope="import-security"/>
               <l3extSubnet ip="210.1.0.0/16" scope="import-security"/>
               <l3extSubnet ip="203.1.0.0/16" scope="import-security"/>
               <l3extSubnet ip="208.2.0.0/16" scope="import-security"/>
           </l3extFabricExtRoutingP>
           <fvPodConnP id="1">
                 <fvIp addr="100.11.1.1/32"/>
          </fvPodConnP>
          <fvPodConnP id="2">
                <fvIp addr="200.11.1.1/32"/>
          </fvPodConnP>
          <fvPeeringP type="automatic_with_full_mesh"/>
     </fvFabricExtConnP>
</imdata>
```

ステップ 4 VLAN 4 で L3Out を設定するには、リモート リーフ スイッチとスパイン スイッチ両方が WAN ルータに接続され、次の例のように XML を入力する必要があります。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<polUni>
```

```
  <fvTenant  name="infra" >
    <l3extOut name="ipn-multipodInternal">
      <ospfExtP areaCost="1" areaCtrl="inherit-ipsec,redistribute,summary"
areaId="0.0.0.5"areaType="nssa" multipodInternal="yes" />
      <l3extRsEctx tnFvCtxName="overlay-1" />
      <l3extLNodeP name="bLeaf">
        <l3extRsNodeL3OutAtt rtrId="202.202.202.202" rtrIdLoopBack="no"
tDn="topology/pod-2/node-202">
            <l3extLoopBackIfP addr="202.202.202.212"/>
       </l3extRsNodeL3OutAtt>
        <l3extRsNodeL3OutAtt rtrId="102.102.102.102" rtrIdLoopBack="no"
tDn="topology/pod-1/node-102">
            <l3extLoopBackIfP addr="102.102.102.112"/>
       </l3extRsNodeL3OutAtt>
        <l3extLIfP name="portIf">
          <ospfIfP authKeyId="1" authType="none">
            <ospfRsIfPol tnOspfIfPolName="ospfIfPol" />
          </ospfIfP>
          <l3extRsPathL3OutAtt addr="10.0.254.233/30" encap="vlan-5"
ifInstT="sub-interface" tDn="topology/pod-2/paths-202/pathep-[eth5/2]"/>
          <l3extRsPathL3OutAtt addr="10.0.255.229/30" encap="vlan-5"
ifInstT="sub-interface" tDn="topology/pod-1/paths-102/pathep-[eth5/2]"/>
        </l3extLIfP>
      </l3extLNodeP>
      <l3extInstP matchT="AtleastOne" name="ipnInstP" />
    </l3extOut>
  </fvTenant>
</polUni>
```

ステップ 5 VLAN-5 で L3Out を設定するには、マルチポッドとリモート リーフ トポロジの両方と、次の例のように XML を送信する必要があります。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<polUni>
<fvTenant name="infra">
  <l3extOut name="rleaf-wan-test">
    <ospfExtP areaId='57' multipodinternal='yes'/>

    <bgpExtP/>
    <l3extRsEctx tnFvCtxName="overlay-1"/>
    <l3extRsL3DomAtt tDn="uni/l3dom-l3extDom1"/>
    <l3extProvLbl descr="" name="prov_mp1" ownerKey="" ownerTag="" tag="yellow-green"/>

    <l3extLNodeP name="rleaf-101">
      <l3extRsNodeL3OutAtt rtrId="202.202.202.202" tDn="topology/pod-1/node-101">
      </l3extRsNodeL3OutAtt>
      <l3extLIfP name="portIf">
        <l3extRsPathL3OutAtt ifInstT="sub-interface"
tDn="topology/pod-1/paths-101/pathep-[eth1/49]" addr="202.1.1.2/30" mac="AA:11:22:33:44:66"
 encap='vlan-4'/>

        <ospfIfP>

          <ospfRsIfPol tnOspfIfPolName='ospfIfPol'/>

        </ospfIfP>

      </l3extLIfP>

    </l3extLNodeP>
    <l3extLNodeP name="rlSpine-201">
      <l3extRsNodeL3OutAtt rtrId="201.201.201.201" rtrIdLoopBack="no"
```

```
tDn="topology/pod-1/node-201">
        <!--
        <l3extLoopBackIfP addr="201::201/128" descr="" name=""/>
        <l3extLoopBackIfP addr="201.201.201.201/32" descr="" name=""/>
        -->
        <l3extLoopBackIfP addr="::" />
      </l3extRsNodeL3OutAtt>
      <l3extLIfP name="portIf">
        <l3extRsPathL3OutAtt ifInstT="sub-interface"
tDn="topology/pod-1/paths-201/pathep-[eth8/36]" addr="201.1.1.1/30" mac="00:11:22:33:77:55"
 encap='vlan-4'/>
        <ospfIfP>
          <ospfRsIfPol tnOspfIfPolName='ospfIfPol'/>
        </ospfIfP>
      </l3extLIfP>
    </l3extLNodeP>

    <l3extInstP descr="" matchT="AtleastOne" name="instp1" prio="unspecified"
targetDscp="unspecified">
      <fvRsCustQosPol tnQosCustomPolName=""/>
    </l3extInstP>
  </l3extOut>
  <ospfIfPol name="ospfIfPol" nwT="bcast"/>
</fvTenant>
</polUni>
```

NX-OS スタイル CLI を使用したリモート リーフの設定

この例では、リーフ スイッチがメインのファブリック ポッドと通信できるようにするため、スパイン スイッチとリモート リーフ スイッチを設定しています。

始める前に

- IPN ルータとリモート スイッチはアクティブで設定されています。WAN ルータとリモート リーフ設定の注意事項 （299 ページ） を参照してください。
- リモート リーフ スイッチは、13.1.x 以降 (aci n9000 dk9.13.1.x.x.bin) のスイッチ イメージを実行しています。
- リモート リーフ スイッチを追加する予定のポッドが作成され、設定されています。

手順

ステップ 1 ポッド 2 のリモート ロケーション 5 で TEP プールを定義します。

ネットワーク マスクは /24 以下である必要があります。

次の新しいコマンドを使用します：**system remote-leaf-site** *site-id* **pod** *pod-id* **tep-pool** *ip-address-and-netmask*

例：

```
apic1(config)# system remote-leaf-site 5 pod 2 tep-pool 192.0.0.0/16
```

ステップ 2 ポッド 2 の、リモート リーフ サイト 5 にリモート リーフ スイッチを追加します。

次のコマンドを使用します：**system switch-id** *serial-number node-id leaf-switch-name***pod** *pod-id* **remote-leaf-site** *remote-leaf-site-id* **node-type remote-leaf-wan**

例：

```
apic1(config)# system switch-id FDO210805SKD 109 ifav4-leaf9 pod 2
remote-leaf-site 5 node-type remote-leaf-wan
```

ステップ 3 VLAN 4 を含む VLAN で VLAN ドメインを設定します。

例：

```
apic1(config)# vlan-domain ospfDom
apic1(config-vlan)# vlan 4-5
apic1(config-vlan)# exit
```

ステップ 4 インフラ テナントに 2 つの L3Out を設定します。1 つはリモート リーフ接続のためで、もう 1 つはマルチポッド IPN のためです。

例：

```
apic1(config)# tenant infra
apic1(config-tenant)# l3out rl-wan
apic1(config-tenant-l3out)# vrf member overlay-1
apic1(config-tenant-l3out)# exit
apic1(config-tenant)# l3out ipn-multipodInternal
apic1(config-tenant-l3out)# vrf member overlay-1
apic1(config-tenant-l3out)# exit
apic1(config-tenant)# exit
apic1(config)#
```

ステップ 5 L3Out が使用する、スパイン スイッチ インターフェイスとサブインターフェイスを設定します。

例：

```
apic1(config)# spine 201
apic1(config-spine)# vrf context tenant infra vrf overlay-1 l3out rl-wan-test
apic1(config-spine-vrf)# exit
apic1(config-spine)# vrf context tenant infra vrf overlay-1 l3out ipn-multipodInternal
apic1(config-spine-vrf)# exit
apic1(config-spine)#
apic1(config-spine)# interface ethernet 8/36
apic1(config-spine-if)# vlan-domain member ospfDom
apic1(config-spine-if)# exit
apic1(config-spine)# router ospf default
apic1(config-spine-ospf)# vrf member tenant infra vrf overlay-1
apic1(config-spine-ospf-vrf)# area 5 l3out rl-wan-test
apic1(config-spine-ospf-vrf)# exit
apic1(config-spine-ospf)# exit
apic1(config-spine)#
apic1(config-spine)# interface ethernet 8/36.4
apic1(config-spine-if)# vrf member tenant infra vrf overlay-1 l3out rl-wan-test
apic1(config-spine-if)# ip router ospf default area 5
apic1(config-spine-if)# exit
apic1(config-spine)# router ospf multipod-internal
apic1(config-spine-ospf)# vrf member tenant infra vrf overlay-1
apic1(config-spine-ospf-vrf)# area 5 l3out ipn-multipodInternal
```

```
apic1(config-spine-ospf-vrf)# exit
apic1(config-spine-ospf)# exit
apic1(config-spine)#
apic1(config-spine)# interface ethernet 8/36.5
apic1(config-spine-if)# vrf member tenant infra vrf overlay-1 l3out ipn-multipodInternal
apic1(config-spine-if)# ip router ospf multipod-internal area 5
apic1(config-spine-if)# exit
apic1(config-spine)# exit
apic1(config)#
```

ステップ 6 メインのファブリック ポッドと通信するために使用するリモートのリーフ スイッチ インターフェイスとサブインターフェイスを設定します。

例：

```
(config)# leaf 101
apic1(config-leaf)# vrf context tenant infra vrf overlay-1 l3out rl-wan-test
apic1(config-leaf-vrf)# exit
apic1(config-leaf)#
apic1(config-leaf)# interface ethernet 1/49
apic1(config-leaf-if)# vlan-domain member ospfDom
apic1(config-leaf-if)# exit
apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant infra vrf overlay-1
apic1(config-leaf-ospf-vrf)# area 5 l3out rl-wan-test
apic1(config-leaf-ospf-vrf)# exit
apic1(config-leaf-ospf)# exit
apic1(config-leaf)#
apic1(config-leaf)# interface ethernet 1/49.4
apic1(config-leaf-if)# vrf member tenant infra vrf overlay-1 l3out rl-wan-test
apic1(config-leaf-if)# ip router ospf default area 5
apic1(config-leaf-if)# exit
```

例

次の例は、ダウンロード可能な設定を示しています:

```
apic1# configure
apic1(config)# system remote-leaf-site 5 pod 2 tep-pool 192.0.0.0/16
apic1(config)# system switch-id FDO210805SKD 109 ifav4-leaf9 pod 2
remote-leaf-site 5 node-type remote-leaf-wan
apic1(config)# vlan-domain ospfDom
apic1(config-vlan)# vlan 4-5
apic1(config-vlan)# exit
apic1(config)# tenant infra
apic1(config-tenant)# l3out rl-wan-test
apic1(config-tenant-l3out)# vrf member overlay-1
apic1(config-tenant-l3out)# exit
apic1(config-tenant)# l3out ipn-multipodInternal
apic1(config-tenant-l3out)# vrf member overlay-1
apic1(config-tenant-l3out)# exit
apic1(config-tenant)# exit
apic1(config)#
apic1(config)# spine 201
apic1(config-spine)# vrf context tenant infra vrf overlay-1 l3out rl-wan-test
apic1(config-spine-vrf)# exit
apic1(config-spine)# vrf context tenant infra vrf overlay-1 l3out ipn-multipodInternal
apic1(config-spine-vrf)# exit
apic1(config-spine)#
apic1(config-spine)# interface ethernet 8/36
```

```
apic1(config-spine-if)# vlan-domain member ospfDom
apic1(config-spine-if)# exit
apic1(config-spine)# router ospf default
apic1(config-spine-ospf)# vrf member tenant infra vrf overlay-1
apic1(config-spine-ospf-vrf)# area 5 l3out rl-wan-test
apic1(config-spine-ospf-vrf)# exit
apic1(config-spine-ospf)# exit
apic1(config-spine)#
apic1(config-spine)# interface ethernet 8/36.4
apic1(config-spine-if)# vrf member tenant infra vrf overlay-1 l3out rl-wan-test
apic1(config-spine-if)# ip router ospf default area 5
apic1(config-spine-if)# exit
apic1(config-spine)# router ospf multipod-internal
apic1(config-spine-ospf)# vrf member tenant infra vrf overlay-1
apic1(config-spine-ospf-vrf)# area 5 l3out ipn-multipodInternal
apic1(config-spine-ospf-vrf)# exit
apic1(config-spine-ospf)# exit
apic1(config-spine)#
apic1(config-spine)# interface ethernet 8/36.5
apic1(config-spine-if)# vrf member tenant infra vrf overlay-1 l3out ipn-multipodInternal
apic1(config-spine-if)# ip router ospf multipod-internal area 5
apic1(config-spine-if)# exit
apic1(config-spine)# exit
apic1(config)#
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant infra vrf overlay-1 l3out rl-wan-test
apic1(config-leaf-vrf)# exit
apic1(config-leaf)#
apic1(config-leaf)# interface ethernet 1/49
apic1(config-leaf-if)# vlan-domain member ospfDom
apic1(config-leaf-if)# exit
apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant infra vrf overlay-1
apic1(config-leaf-ospf-vrf)# area 5 l3out rl-wan-test
apic1(config-leaf-ospf-vrf)# exit
apic1(config-leaf-ospf)# exit
apic1(config-leaf)#
apic1(config-leaf)# interface ethernet 1/49.4
apic1(config-leaf-if)# vrf member tenant infra vrf overlay-1 l3out rl-wan-test
apic1(config-leaf-if)# ip router ospf default area 5
apic1(config-leaf-if)# exit
```

GUI を使用してリモート リーフ スイッチを構成する

ウィザードを使用してリモートリーフスイッチのポッドとファブリック メンバーシップを設定する

IPN ルータとリモート スイッチを検出して接続するために、 Cisco APIC を設定して有効にすることができます。このトピックで説明するようにウィザードを使用して、または APIC GUI を使用する代替の方法で行えます。GUI を使用してリモート リーフ スイッチのポッドとファブリック メンバーシップを設定する (ウィザードは使用しない)（308 ページ）を参照してください。

始める前に

- IPN と WAN ルータとリモートのリーフ スイッチがアクティブで設定されています。WAN ルータとリモート リーフ設定の注意事項 （299 ページ）を参照してください。
- リモート リーフ スイッチ ペアは、vPC で接続されています。
- リモート リーフ スイッチは、13.1.x 以降 (aci n9000 dk9.13.1.x.x.bin) のスイッチ イメージを実行しています。
- リモート リーフ スイッチを追加する予定のポッドが作成され、設定されています。
- ポッドをリモート リーフ スイッチに接続するために使用するスパイン スイッチは IPN ルータに接続されています。

手順

ステップ 1 メニュー バーで、**Fabric** > **Inventory** をクリックします。

ステップ 2 ナビゲーション ウィンドウで、**Quick Start** を展開し、**Node or Pod Setup** をクリックします。

ステップ 3 作業ウィンドウの **Remote Leaf** ペインで、**Setup Remote Leaf** をクリックするか、**Node or Pod Setup** を右クリックして、 **Setup Remote Leaf** をクリックします。

ステップ 4 指示に従って、次の項目を設定します:

- **Pod Fabric** — リモート リーフ スイッチのためのポッドと TEP プール サブネットを識別します。

  リモート リーフ スイッチにつながるアンダーレイ ルートのサブネットを、カンマ区切りで追加します。

  ポッドに追加する他のリモート リーフ スイッチについても、これを繰り返します。

- **Fabric Membership** — リモート リーフ スイッチのファブリック メンバーシップをセットアップします。これにはノード ID、リモート リーフの TEP プール ID、およびリモート リーフ スイッチの名前が含まれます。

- **Remote Leaf** — リモート リーフ スイッチのためのレイヤ 3 の詳細を設定します。これには OSPF の詳細 (WAN ルータでの OSPF 設定と同じ)、ルータ ID とループバック アドレス、およびノードのためにルーティングされたサブインターフェイスが含まれます。

- **Connections** — リモート リーフ スイッチへのルート上にある L3Out のためのスパイン スイッチのために、レイヤ 3 の詳細を設定します (リモート リーフ スイッチをシングルポッドのファブリックに追加する場合にのみ必要です)。これには OSPF の詳細 (IPN および WAN ルータでの設定と同じ)、OSPF プロファイル、ルータ ID とスパイン スイッチのためのルーティング サブインターフェイスが含まれます。

GUIを使用してリモートリーフスイッチのポッドとファブリックメンバーシップを設定する (ウィザードは使用しない)

リモート リーフ スイッチを設定するには、GUI の手順を使用できます。または、ウィザードを使用します。ウィザードを使用する手順については、次を参照してください: ウィザードを使用してリモート リーフ スイッチのポッドとファブリック メンバーシップを設定する （306 ページ)

始める前に

- ルータ (IPN と WAN) とリモートのリーフ スイッチはアクティブで設定されています。WAN ルータとリモート リーフ設定の注意事項 （299 ページ）を参照してください。
- リモート リーフ スイッチは、13.1.x 以降 (aci n9000 dk9.13.1.x.x.bin) のスイッチ イメージを実行しています。
- リモート リーフ スイッチを追加する予定のポッドが作成され、設定されています。
- ポッドをリモート リーフ スイッチに接続するために使用するスパイン スイッチは IPN ルータに接続されています。

手順

ステップ 1 次の手順で、リモート リーフ スイッチの TEP プールを設定します:

a) メニュー バーで、**Fabric** > **Inventory** をクリックします。
b) [Navigation] ウィンドウで、**Pod Fabric Setup Policy** をクリックします。
c) **Fabric Setup Policy** パネルで、リモート リーフ スイッチのペアを追加するポッドをダブルクリックします。
d) **Remote Pools** テーブルで [+] をクリックします。
e) リモート TEP プールのリモート ID とサブネットを入力し、**Submit** をクリックします。
f) **Fabric Setup Policy** パネルで、**Submit** をクリックします。

ステップ 2 次の手順で、IPN ルータに接続されているスパイン スイッチの L3Out を設定します:

a) メニュー バーで、**Tenants** > **infra** をクリックします。
b) [Navigation] ウィンドウで、**Networking** を展開し、**External Routed Networks** を右クリックし、**Create Routed Outside** を選択します。
c) L3Out の名前を入力します。
d) **OSPF** チェック ボックスをオンにして OSPF を有効にし、IPN および WAN ルータと同じ方法で OSPF の詳細を設定します。
e) リモート リーフ スイッチを追加するポッドがマルチポッド ファブリックの一部である場合には、**Enable Remote Leaf** チェック ボックスだけをオンにします。

このオプションは、マルチポッドのための VLAN-5 を使用する第2の OSPF インスタンスを有効にします。これにより、リモート リーフ スイッチのルートが、スイッチが所属しているポッド内にのみアドバタイズされるようにします。

f) **overlay-1** VRF を選択します。

ステップ 3 次の手順に従って、L3Out で使用されるスパインとインターフェイスの詳細を設定します:

a) **Nodes and Interfaces Protocol Profiles** テーブルの [+] アイコンをクリックします。
b) ノード プロファイル名を入力します。
c) **Nodes** テーブルで [+] アイコンをクリックし、以下の詳細を入力します。
   - Node ID — IPN ルータに接続されているスパイン スイッチの ID。
   - Router ID — IPN ルータの IP アドレス
   - External Control Peering — リモート リーフ スイッチを追加するポッドがシングルポッド ファブリックの場合には無効にします。

d) **OK** をクリックします。
e) **OSPF Interfaces Profiles** テーブルの [+] アイコンをクリックします。
f) インターフェイス プロファイルの名前を入力して **Next** をクリックします。
g) **OSPF Profile** で、**OSPF Policy** をクリックし、前に作成したポリシーを選択します。または、**Create OSPF Interface Policy** をクリックします。
h) **Next** をクリックします。
i) **Routed Sub-Interface** をクリックし、**Routed Sub-Interfaces** テーブルの [+] をクリックして、以下の詳細を入力します:
   - Node — インターフェイスが所在するスパイン スイッチです。
   - Path — IPN ルータに接続されたインターフェイス
   - Encap — VLAN の場合には **4** を入力します。

j) **OK** をクリックし、**Next** をクリックします。
k) **External EPG Networks** テーブルの [+] をクリックします。
l) 外部ネットワークの名前を入力し、 **OK** をクリックします。
m) **Finish** をクリックします。

ステップ 4 リモート リーフ スイッチのファブリック メンバーシップ設定を完了するには、次の手順を実行します:

a) **Fabric** > **Inventory** > **Fabric Membership** に移動します。

この時点で、新しいリモート リーフ スイッチが、ファブリックに登録されているスイッチのリストに表示されるようになります。ただし、次の手順で説明する方法でノードアイデンティティ ポリシーを設定するまでは、これらはリモート リーフ スイッチとは認識されません。

b) それぞれのリモート リーフ スイッチについてに、リストのノードをダブルクリックし、次の詳細情報を設定し、**Update** をクリックします:

- Node ID — リモート リーフ スイッチの ID
- RL TEP Pool — 以前に設定した、リモート リーフ TEP プールの識別子
- Node Name — リモート リーフ スイッチの名前

リモート リーフ スイッチごとにノード アイデンティティ ポリシーを設定すると、**Fabric Membership** テーブルに、`remote leaf` ロールを持つものとしてリストされます。

ステップ 5 次の手順で、リモート リーフ ロケーションの L3Out を設定します:

a) **Tenants** > **infra** > **Networking** に移動します。
b) **External Routed Networks** を右クリックし、**Create Routed Outside** を選択します。
c) L3Out の名前を入力します。
d) **OSPF** チェック ボックスをオンにして OSPF を有効にし、IPN および WAN ルータと同じ方法で OSPF の詳細を設定します。
e) リモート リーフ スイッチを追加するポッドがマルチポッド ファブリックの一部である場合には、**Enable Remote Leaf** チェック ボックスだけをオンにします。
f) **overlay-1** VRF を選択します。

ステップ 6 次の手順で、ノードと、リモート リーフ スイッチから WAN ルータに向かうインターフェイスを設定します:

a) [Create Routed Outside] パネルで、**Nodes and Interfaces Protocol Profiles** テーブルの [+] をクリックします。
b) [Nodes] テーブルで [+] をクリックし、次の詳細を入力します:
   - Node ID — WAN ルータに接続されているリモート リーフの ID
   - Router ID— WAN ルータの IP アドレス
   - External Control Peering — リモート リーフ スイッチがマルチポッド ファブリック内のポッドに追加される場合にのみ、有効にしてください
c) **OK** をクリックします。
d) **OSPF Interface Profiles** の [+] をクリックし、リモート リーフ スイッチを WAN ルータに接続するために使用されるルーテッドサブインターフェイスについて、次の詳細を設定します。
   - Identity — OSPF インターフェイスのプロファイルの名前
   - Protocol Profiles — 以前に設定した OSPF プロファイル。または新たに作成
   - Interfaces — **Routed Sub-Interface** タブの、WAN ルータに向かうルーテッド サブインターフェイスのパスと IP アドレス

ステップ 7 次の手順で、ファブリック外部接続プロファイルを設定します。

a) **Tenants** > **infra** > **Policies** > **Protocol** に移動します。
b) **Fabric Ext Connection Policies** を右クリックし、**Create Intrasite/Intersite Profile** を選択します。

c) **Fabric External Routing Profile** で [+] をクリックします。
d) プロファイルの名前を入力し、リモート リーフ スイッチの 1 つのサブネットを追加します。
e) **Update** をクリックし、**Submit** をクリックします。
f) 同じ場所で、2 番目のリモート リーフ スイッチのサブネットを追加するには、作成した [Fabric Ext Connection Profile] をクリックし、ファブリック外部ルーティング プロファイルをダブルクリックします。
g) その他のリモート リーフ スイッチのサブネットを追加し、**Update** と **Close** ををクリックします。

ステップ 8 リモートのリーフ スイッチが、apic 内で検出されたことを確認するには、**Fabric** > **Inventory** > **Fabric Membership**、または **Fabric** > **Inventory** > **Pod** > **Topology** に移動します。

ステップ 9 ファブリックとリモート リーフ スイッチ間のリンクのステータスを表示するには、IPN ルータに接続されているスパイン スイッチで、**show ip ospf neighbors vrf overlay-1** コマンドを入力します。

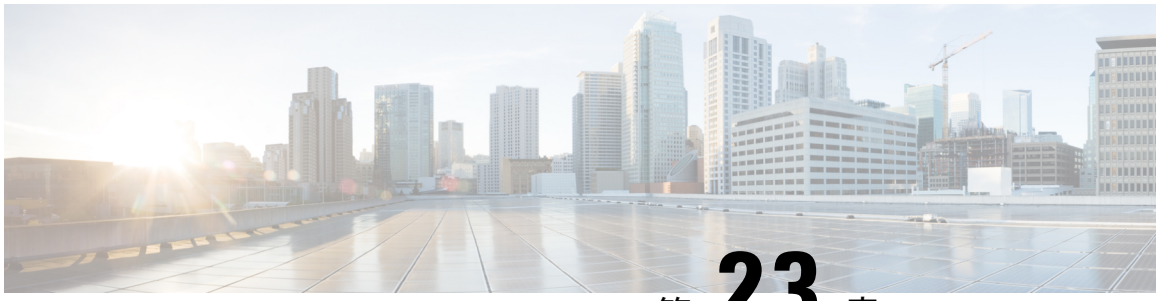
ステップ 10 CLI を使用する APIC で、ファブリック内のリモート リーフ スイッチのステータスを表示するには、**acidiag fnvread** という NX-OS スタイルのコマンドを入力します。

リモートのリーフスイッチのダウングレードする前に必要な前提条件

（注） リモート ノードの使用停止し、リモート リーフに関連するポリシー(を削除する必要がありますがあれば導入で、リモートのリーフ スイッチ リリース 3.1 (1) から以降、リモート リーフ機能をサポートしていない以前のリリースには、APIC ソフトウェアのダウン グレードする場合、というプールにある) を含む前にダウン グレードします。スイッチの使用停止の詳細についてを参照してください。 使用停止およびスイッチの再稼働 で、 *Cisco APIC* トラブルシューティング ガイド 。

リモート リーフ スイッチをダウン グレードする前に、いずれかのタスクが完了することを確認します。

- vPC ドメインを削除します。
- SCVMM を使用している場合は、vTEP - 仮想ネットワーク アダプタを削除します。
- リモート リーフノードの使用停止および10を待機-15分を完了するタスクの使用停止後。
- 削除に WAN L3out にリモート リーフ、テナント インフラ。
- Multipod を使用している場合、インフラ-l3out VLAN 5 とを削除します。
- リモートというプールを削除します。



第 23 章

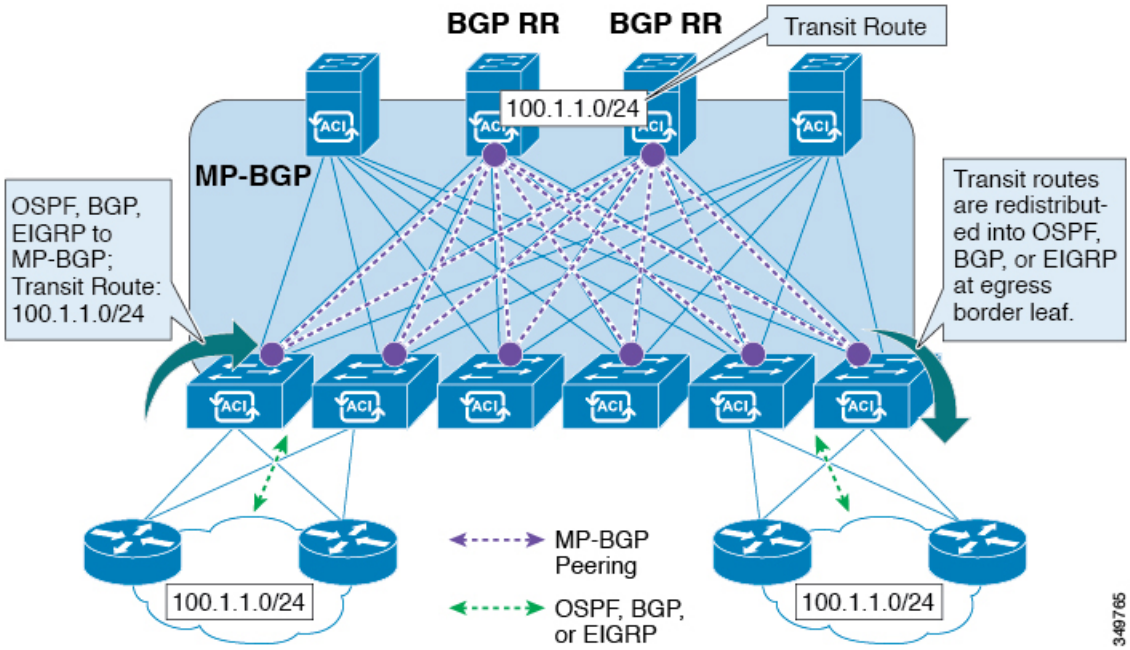
トランジット ルーティング

この章の内容は、次のとおりです。

中継 ACI ファブリックのルーティング

Cisco APIC ソフトウェアは、OSPF（NSSA）および iBGP を使用した外部レイヤ 3 接続をサポートします。ファブリックは、外部レイヤ3アウトサイド（l3out）接続の外部ルータにテナントブリッジドメインのサブネットをアドバタイズします。外部ルータから学習されたルートは、他の外部ルータにアドバタイズされません。ファブリックはスタブネットワークと同じように動作し、外部レイヤ 3 ドメイン間のトラフィックの伝送に使用できます。

図 *31 :* ファブリックでルーティング中継



中継のルーティングで1つのテナントとVRF内の複数のL3Out接続がサポートされているし、APIC は別の L3Out 接続を 1 つの L3Out 接続から学習したルートをアドバタイズします。外部レイヤ 3 ドメインは、境界リーフ スイッチの ファブリックとピアリングします。ファブリックはピア間の Multiprotocol-Border Gateway Protocol（MP-BGP）中継ドメインです。

外部L3Out接続の設定は、テナントとVRFレベルで実行されます。外部ピアから学習したルートは、VRF ごとに入力リーフの MP-BGP にインポートされます。L3Out 接続から学習したプレフィックスは、テナント VRF が存在するリーフ スイッチにのみエクスポートされます。

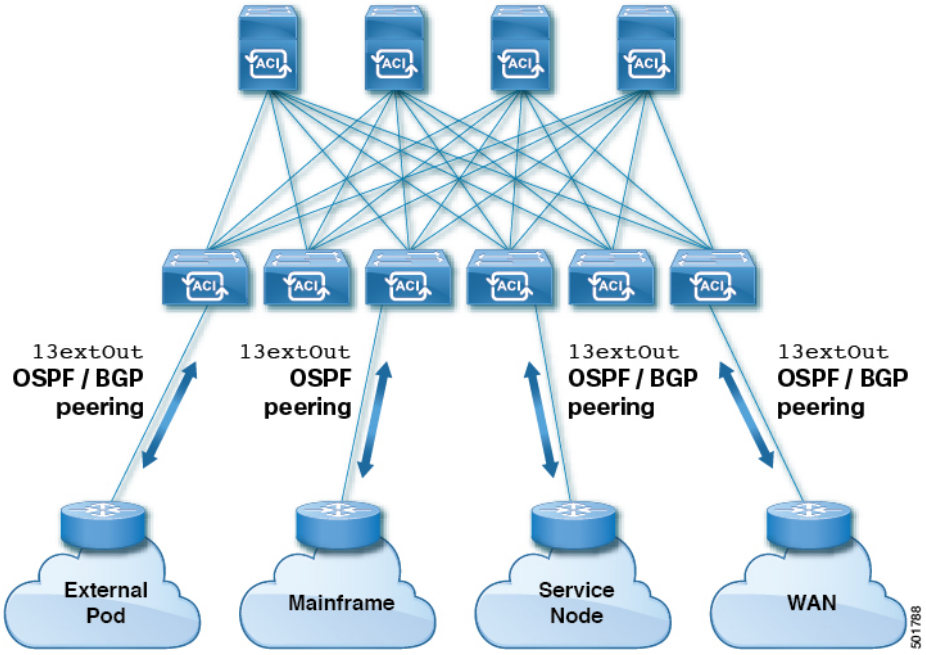
（注） 注意事項と中継ルーティングの設定のガイドラインは、次を参照してください。中継ルーティングのガイドライン （322 ページ）

トランジット ルーティングの使用例

レイヤ 3 ドメイン間のトランジット ルーティング

外部ポッド、メインフレーム、サービス ノード、WAN ルータなどの複数のレイヤ 3 ドメインがACIファブリックとピアリングして、それらの間のトランジット機能を提供することができます。

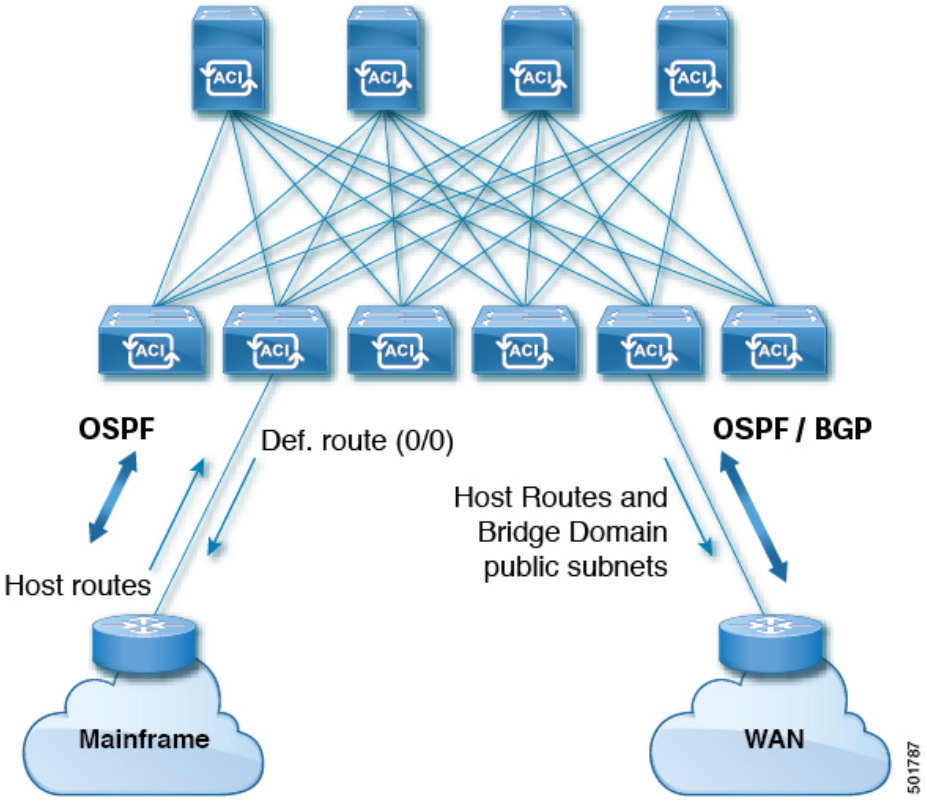
図 *32 :* レイヤ *3* ドメイン間のトランジット ルーティング



ACI ファブリックで中継されるメインフレーム トラフィック

メインフレームは、論理パーティション（LPAR）および仮想 IP アドレッシング（VIPA）の要件に対応する標準 IP ルーティング プロトコルを実行する IP サーバとして機能します。

図 *33 :* メインフレームのトランジット接続

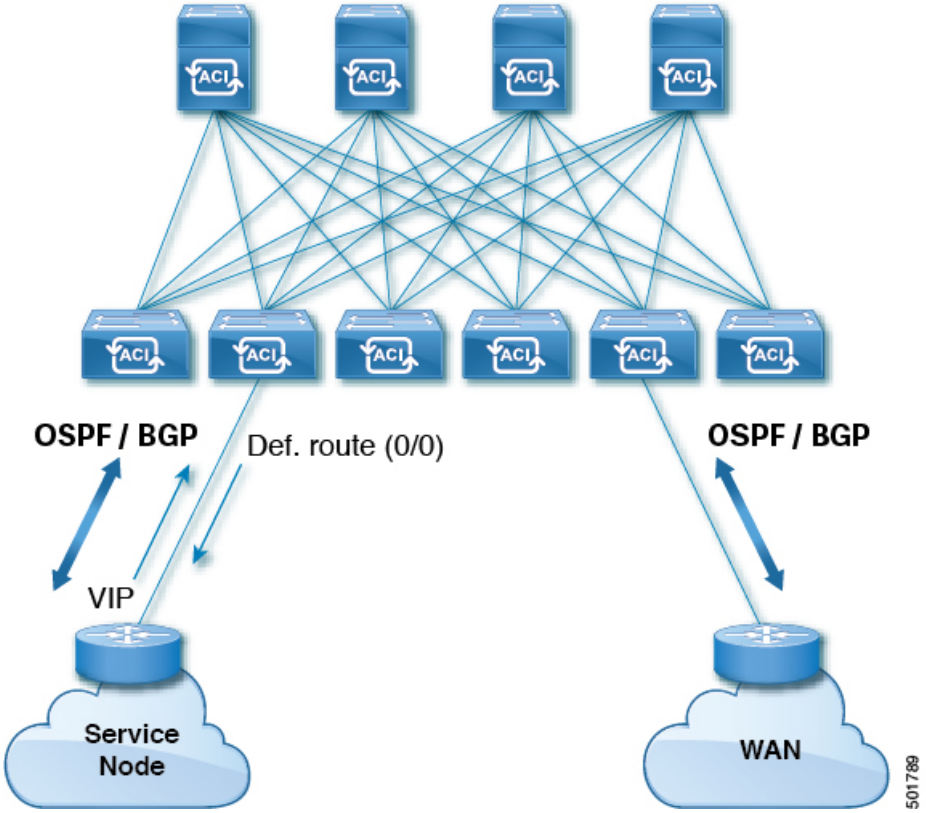


このトポロジにおいて、メインフレームは、ACI ファブリックが WAN ルータを経由して外部と接続するため、およびファブリック内の East-West トラフィックのための中継ドメインとなることを必要とします。これらは、ホストルートをファブリックにプッシュして、ファブリック内、および外部インターフェイスに再配布されるようにします。

サービス ノードのトランジット接続

サービス ノードは ACI ファブリックとピアリングし、外部 WAN インターフェイスに再配布される仮想 IP (VIP) ルートをアドバタイズすることができます。

図 *34* : サービス ノードのトランジット接続

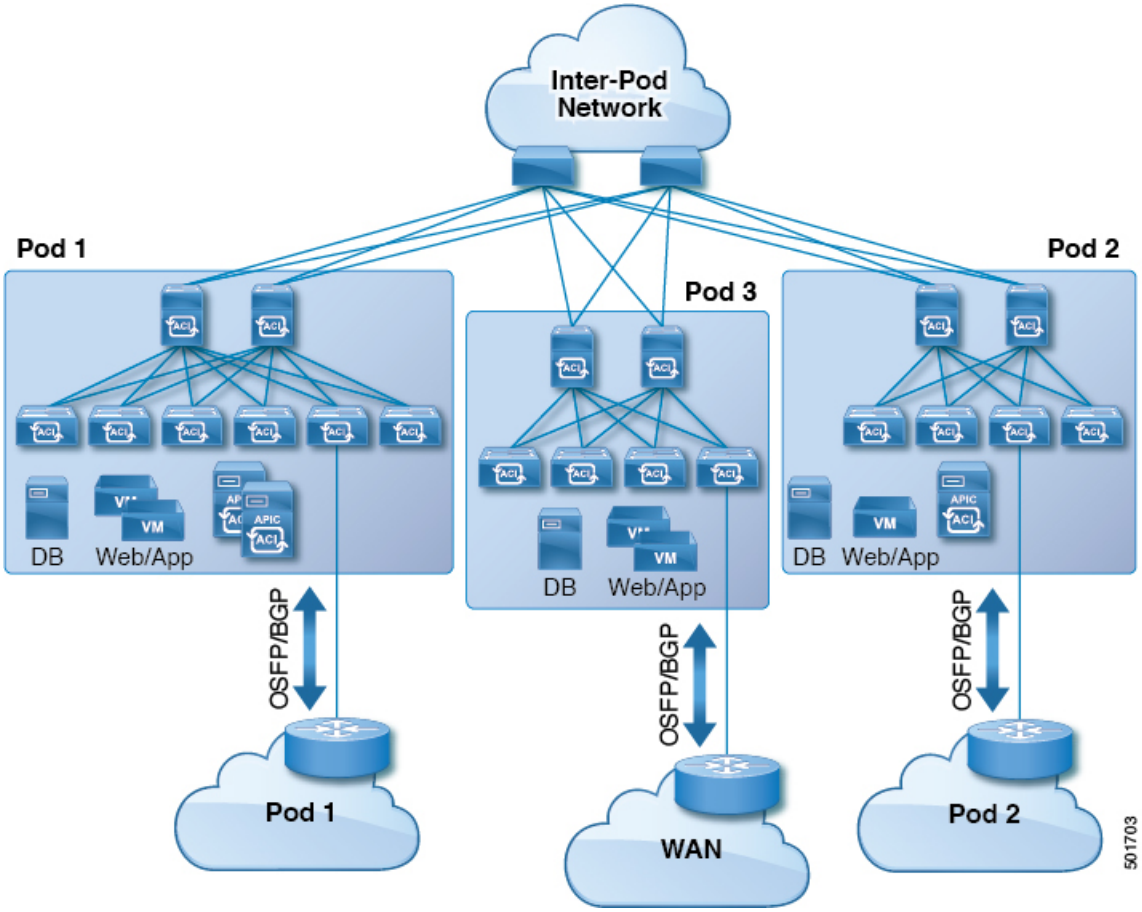


VIP は、特定のサイトやサービスの外部向けの IP アドレスです。VIP は、サービス ノードの背後にある 1 つ以上のサーバまたはノードに関連付けられています。

中継ルーティング設定でのマルチポッド

マルチポッド トポロジでは、ファブリックは、外部接続と複数のポッド間の相互接続の中継として機能します。クラウド プロバイダは、顧客データセンター内に管理対象のリソース ポッドを展開できます。責任分界点は、ファブリックとのピアリングを行っている OSPF または BGP を伴う L3Out にすることができます。

図 *35 :* 中継ルーティング設定における *L3Out* を伴う複数のポッド



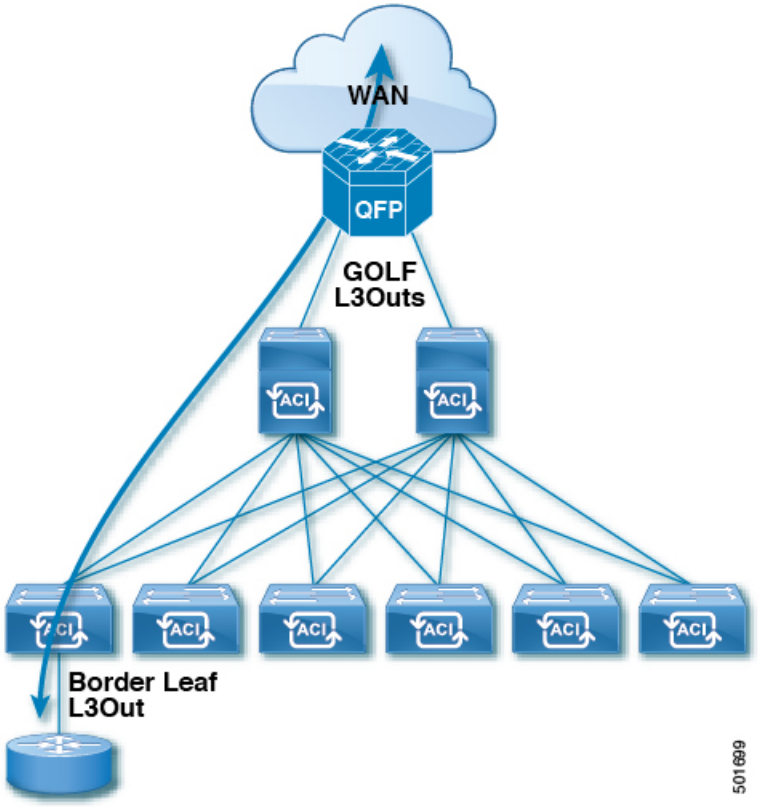
このようなシナリオでは、ポリシーは責任分界点で管理され、ACI ポリシーを設定する必要はありません。

レイヤ4 ～ レイヤ 7 ルート ピアリングはファブリックを中継として使用する特殊な使用例であり、ファブリックは複数ポッドに対する中継 OSPF または BGP ドメインの役目を果たします。ルート ピアリングは、接続されているリーフ ノードとルートを交換できるようにするため、レイヤ4 ～ レイヤ 7 サービス デバイス上で OSPF または BGP ピアリングを有効にするように設定します。ルート ピアリングの一般的な使用例として、SLB VIP が OSPF および iBGP を介して ファブリック外のクライアントにアドバタイズされる、ルート ヘルス インジェクションがあります。このシナリオの詳細については、『*L4-L7 Route Peering with Transit Fabric - Configuration Walkthrough*』を参照してください。

中継ルーティング設定での GOLF

APIC、リリース 2.0 以降では、Cisco ACI は、GOLF L3Out での中継ルーティング (BGP と OSPF) をサポートしています。 たとえば、次の図は、GOLF L3Out と境界リーフ L3Out を伴うファブリックで中継されるトラフィックを示しています。

図 *36* : 中継ルーティング設定での *GOLF L3Out* と境界リーフ *L3Out*



サポートされるトランジットの組み合わせのマトリックス

レイヤ 3 Outside 接続タイプ		OSPF	iBGP			eBGP			EIGRP v4	EIGRP v6	スタティック ルート
			OSPF 上の iBGP	スタティック ルート上の iBGP	直接接続上の iBGP	OSPF 上の eBGP	スタティック ルート上の eBGP	直接接続上の eBGP			
OSPF		対応	○*	○	○* (APIC リリース 1.3 c でテスト)	対応	対応	対応	対応	○* (APIC リリース 1.2 g でテスト)	○
iBGP	OSPF 上の iBGP	○*	×	×	×	○* (APIC リリース 1.3 c でテスト)	X	対応	対応	×	○
	スタティック ルート上の iBGP	○	×	×	×	○* (APIC リリース 1.2 g でテスト)	×	○* (APIC リリース 1.2 g でテスト)	○	×	○
	直接接続上の iBGP	○	×	×	×	-	×	○* (APIC リリース 1.2 g でテスト)	○	×	○

レイヤ 3 Outside 接続タイプ		OSPF	iBGP			eBGP			EIGRP v4	EIGRP v6	スタティック ルート
			OSPF 上の iBGP	スタティック ルート上の iBGP	直接接続上の iBGP	OSPF 上の eBGP	スタティック ルート上の eBGP	直接接続上の eBGP			
eBGP	OSPF 上の eBGP	○	○* (APIC リリース 1.3 c でテスト)	○* (APIC リリース 1.3 c でテスト)	○* (APIC リリース 1.3 c でテスト)	○	○* (APIC リリース 1.3 c でテスト)	○* (APIC リリース 1.3 c でテスト)	○	×	○* (APIC リリース 1.3 c でテスト)
	スタティック ルート上の eBGP	○	×	×	×	○* (APIC リリース 1.2 g でテスト)	○ (APIC リリース 3.0 でテスト)	○* (APIC リリース 1.2 g でテスト)	○	×	○
	直接接続上の eBGP	対応	対応	○* (APIC リリース 1.3 c でテスト)	○* (APIC リリース 1.3 c でテスト)	○* (APIC リリース 1.3 c でテスト)	○* (APIC リリース 1.3 c でテスト)	対応	対応	×	○
EIGRPv4		対応	対応	対応	対応	対応	対応	対応	○ (APIC リリース 1.3 c でテスト)	X	○

レイヤ 3 Outside 接続タイプ	OSPF	iBGP			eBGP			EIGRP v4	EIGRP v6	スタティック ルート
		OSPF 上の iBGP	スタティック ルート上の iBGP	直接接続上の iBGP	OSPF 上の eBGP	スタティック ルート上の eBGP	直接接続上の eBGP			
EIGRPv6	○ (APIC リリース 1.2 g でテスト)	×	×	×	×	×	×	×	○ (APIC リリース 1.3 c でテスト)	○ (APIC リリース 1.2 g でテスト)
スタティック ルート	対応	対応	対応	対応	○ (APIC リリース 1.3 c でテスト)	対応	対応	対応	○ (APIC リリース 1.2 g でテスト)	○

- 接続= 接続
- * = 同じリーフ スイッチではサポートされません
- × = サポートされていないかテストされていない組み合わせ

トランジット ルーティングの注意事項

中継ルーティングのガイドライン

作成し、中継ルーティング接続を維持する場合は、次のガイドラインを使用します。

トピック	注意またはガイドライン
中継が1つのL3Outプロファイルを使用してルーティング	

トピック	注意またはガイドライン
	前にAPIC 2.3(1f)のリリースでは、ルーティングを通過、1 つの L3Out プロファイル内ではサポートされていませんでした。APIC2.3(1f)のリリース、および以降では、中継が単一L3Outプロファイルで、次の制限でルーティングを設定できます。 • VRF が適用されるではない場合は、同じ L3EPG を共有ルータ間のトラフィックを許可する 0.0.0.0/0 の外部のサブネット (l3extSubnet) を使用できます。 • 外部デフォルト サブネット (0.0.0.0/0) の場合は、VRF を適用すると、 **できません** 同一のレイヤ 3 EPG内のトラフィックの送信元と宛先の両方のプレフィックスに一致するために使用します。同一のレイヤ3 EPG内のすべてのトラフィックを一致するには、次のプレフィックスがサポートされています。 • **IPv4** • 外部 EPG の 0.0.0.0/1—with 外部サブネット • 外部 EPG の 128.0.0.0/1—with 外部サブネット • 0.0.0.0/0—with インポート ルート制御サブネット、集約のインポート • **IPv6** • 0::0/1: 外部 EPG の外部のサブネットを持つ • 8000::0/1: 外部 EPG の外部のサブネットを持つ • 0:0/0: インポート ルート制御のサブネットで集約のインポート • また、VzAny 契約と組み合わせると、1 つのデフォルトのサブネット (0.0.0.0/0) を使用できます。次に例を示します。 • 使用契約とレイヤ 3 EPG の提供 VzAny 消費契約 (一致する 0.0.0.0/0)、または、VzAny には、契約とレイヤ3 EPGが提供される契約 (0.0.0.0/0 に一致する) が使用された行数。 • サブネット 0.0.0.0/0—with インポート/エクスポートルート制御サブネット、集約のインポートおよび集約エクスポートを使用します。

トピック	注意またはガイドライン
ハードウェア サポートの違いを共有ルート:	第 2 世代のスイッチの VRF 機能間で正常にルートが共有されます（N9K-93108TC-EX など、スイッチモデル名の最後やその後に「EX」や「FX」がつく Cisco Nexus N9K）。第 1 世代のスイッチですが、ルートを保存する物理的な 3 進コンテンツ対応メモリ（TCAM）にルートの解析を完全にサポートするだけの容量がないため、この設定のパケットは失敗する可能性があります。
背面に戻る設定で EIGRP や OSPF	Cisco APIC では、中継が、L3Out に設定されているエクスポートルート制御ポリシーのルーティングをサポートします。ルート(プレフィックス)を通過するこれらのポリシー制御は、L3Out でルーティングプロトコルに再配送されます。これらの中継ルートは、EIGRP や OSPF に再配布されたが、これらはルーティングループを防ぐためにタグ付けされた 4294967295 です。Cisco ACI ファブリックは、OSPF または EIGRP L3Out で学習すると、このタグに一致するルートを受け入れません。ただし、次の場合、この動作をオーバーライドする必要があります。 • EIGRP や OSPF を使用して、2 つの Cisco ACI ファブリックを接続します。 • EIGRP や OSPF を使用して、同じ Cisco ACI ファブリックで 2 つの異なる Vrf を接続します。 APIC GUI の次の場所にある別のタグのポリシーを使用して、VRF を設定する必要がありますをオーバーライドする必要がある場所: **テナント** > ***Tenant_name*** > **ネットワー キング** > **プロトコル ポリシー** > **ルート タグ** . 異なるタグを適用します。 新しいルート タグ ポリシーを作成するには、だけでなく、APIC GUI の次の場所でこのポリシーを使用する VRF を更新: **テナント** > ***Tenant_name*** > **ネットワー キング** > **Vrf** > ***Tenant_VRF*** . VRF を作成したルート タグ ポリシーを適用します。 （注） 複数 L3Outs または同じ L3Out で複数のインターフェイスは同じリーフスイッチに導入し、中継ルーティングに使用、(、IGP に再配布されません) IGP 内で、ルートをアドバタイズします。この状況では、ルート タグ ポリシーは適用されません。

トピック	注意またはガイドライン
BD サブネットをファブリック外にアドバタイズする	インポートおよびエクスポートのルート制御ポリシーは、中継ルート（他の外部ピアから学習したルート）およびスタティック ルートのみに適用されます。テナント BD サブネット上に設定されているファブリック内部のサブネットは、エクスポート ポリシー サブネットを使用して外部にアドバタイズされません。IP プレフィックス リストおよびルート マップを使用すると IP テナント サブネットは許可されますが、これらは別の設定手順を使用して実装されます。テナント サブネットをファブリックの外部にアドバタイズする場合は、次の設定手順を参照してください。 **1.** [subnet properties] ウィンドウで、テナント サブネットのスコープを [Public Subnet] として設定します。 **2.** オプション。[subnet properties] ウィンドウで、[Subnet Control] を [ND RA Prefix] として設定します。 **3.** テナント ブリッジ ドメイン（BD）を外部レイヤ 3 Outside に関連付けます (L3Out)。 **4.** テナント EPG と外部 EPG 間にコントラクト（プロバイダ/コンシューマ）の関連付けを作成します。 BD サブネットを Public 範囲に設定し、BD をレイヤ 3 Out に関連付けると、BD サブネット プレフィックスの境界リーフに IP プレフィックスおよびルート マップの連続エントリが作成されます。

トピック	注意またはガイドライン
デフォルト ルートのアドバタイズ	デフォルトルートのみを必要とするファブリックへの外部接続の場合、OSPF、EIGRP、および BGP の L3Out 接続をデフォルトルートの起点とすることがサポートされます。外部ピアからデフォルトルートが受信されると、この文書で説明されている中継エクスポートルート制御に従って、このルートを別のピアに再配布できます。 デフォルト ルートは、デフォルト ルート リーク ポリシーを使用してアドバタイズすることもできます。このポリシーは、デフォルト ルートがルーティング テーブル内にあるか、または常にデフォルトルートをアドバタイズすることがサポートされている場合、デフォルトルートのアドバタイズをサポートします。デフォルトルート リーク ポリシーは、L3Out 接続で設定されます。 デフォルト ルート リーク ポリシーを作成するときは、以下のガイドラインに従ってください: • BGP の場合、**Always** プロパティは適用されません。 • BGP の場合、**Scope** プロパティを設定するときには、**Outside** を選択します。 • OSPF の場合、範囲の値が **Context** だとタイプ 5 LSA が作成されるのに対し、**Outside** だとタイプ 7 LSA が作成されます。選択したは、L3Out で設定されたエリアのタイプによって異なります。エリア タイプが場合 **定期的な** 、範囲を設定します **コンテキスト** 。エリア タイプが場合 **NSSA** 、範囲を設定します **外部** 。 • EIGRP で、**Scope** プロパティを選択する場合には、**Context** を選択する必要があります。

トピック	注意またはガイドライン
MTU	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 multipod 接続を設定する場合は、MTU が両側で適切に設定されていることが重要です。ACI、Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定された MTU 値は IP ヘッダーを考慮に入れています（結果として、最大パケット サイズは、ACI で 9216 バイト、NX-OS および IOS で 9000 バイトに設定されます）。ただし、IOS XR などの他のプラットフォームは、パケット ヘッダーのを除く MTU 値を設定します（結果として最大パケット 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。

トランジット ルート制御

ルート トランジットは、インポートされるレイヤ 3 アウトサイド ネットワーク `L3extOut` プロファイル（`l3extInstP`）を通してトラフィックをインポートするために定義されます。異なるルート トランジットは、エクスポートされる別の `l3extInstP` を通してトラフィックをエクスポートするために定義されます。

ファブリック内の 1 つまたは複数のノードに複数の `l3extOut` ポリシーを配置できるので、プロトコルのさまざまな組み合わせがサポートされます。プロトコルの組み合わせはすべて、複数の `l3extOut` ポリシーを使用して 1 つのノードに配置することも、または複数の `l3extOut` ポリシーを使用して複数のノードに配置することも可能です。同じファブリック内の異なる `l3extOut` ポリシーに 3 つ以上のプロトコルを配置することもできます。

エクスポート ルートマップは、プレフィックス リストの一致から構成されます。各プレフィックス リストは、VRF 内のブリッジ ドメイン（BD）パブリック サブネット プレフィクスと、外部にアドバタイズする必要のあるエクスポート プレフィクストから構成されます。

ルート制御ポリシーは、`l3extOut` ポリシーで定義され、`l3extOut` に関連付けられたプロパティおよび関係によって制御されます。APIC は `l3extOut` の `enforceRtctrl` プロパティを使用して、ルート制御方向を適用します。デフォルトでは、エクスポートの制御を適用し、インポートのすべてを許可します。インポートおよびエクスポートされたルート（`l3extSubnets`）は、`l3extInstP` で定義されます。すべてのルートのデフォルト スコープはインポートです。これらは、プレフィックス ベースの EPG を形成するルートおよびプレフィックスです。

インポート ルート マップからのすべてのインポート ルートは、BGP および OSPF によってインポートを制御するために使用されます。エクスポート ルート マップからのすべてのエクスポート ルートは OSPF および BGP によってエクスポートを制御するために使用されます。

インポートとエクスポートのルート制御ポリシーは、異なるレベルで定義されます。IPv6 ではすべての IPv4 ポリシー レベルがサポートされます。`l3extInstP` および `l3extSubnet` MO で定義されている追加の関係でインポートを制御します。

デフォルト ルート リークは、`l3extOut` の下の `l3extDefaultRouteLeakP` MO の定義によって有効になります。

OSPF のエリアごと、BGP のピアごとに `l3extDefaultRouteLeakP` は Virtual Routing and Forwarding（VRF）範囲または `L3extOut` 範囲を有することができます。

次の設定ルールは、ルート制御を提供します。

- `rtctrlSetPref`
- `rtctrlSetRtMetric`
- `rtctrlSetRtMetricType`

`rtctrlSetComm` MO の追加構文には以下が含まれています。

- `no-advertise`
- `no-export`
- `no-peer`

BGP

ACI ファブリックは、外部ルータとの BGP ピアリングをサポートします。BGP ピアは `l3extOut` ポリシーに関連付けられており、`l3extOut` ごとに複数の BGP ピアを設定することができます。BGP は、`l3extOut` の下で `bgpExtP` MO を定義することにより `l3extOut` レベルで有効化できます。

（注） `l3extOut` ポリシーにルーティング プロトコル（たとえば、関連する VRF を含む BGP）が含まれる一方で、L3Out インターフェイスのプロファイルには必要な BGP インターフェイス設定の詳細が含まれます。いずれも BGP の有効化に必要です。

BGP ピアには、OSPF、EIGRP、接続されたインターフェイス、スタティック ルート、またはループバック経由で到達できます。外部ルータとのピアリングには iBGP または eBGP を使用できます。ファブリック内への外部ルートの配付には MP-BGP が使用されるため、外部ルータからの BGP ルート属性は保持されます。BGP は `l3extOut` に関連付けられた VRF に Ipv4 や IPv6 アドレス ファミリを有効にすることができます。スイッチ上で有効になるアドレス ファミリは、`bgpPeerP` ポリシーで `l3extOut` のために定義した IP アドレス タイプによって決まります。ポリシーは省略可能です。定義しない場合はデフォルトが使用されます。ポリシーはテナントに対して定義され、名前で参照される VRF によって使用できます。

ピア ポリシーを少なくとも 1 つのピアを定義して、境界リーフ（BL）の各スイッチでプロトコルを有効にする必要があります。ピア ポリシーは 2 つの場所で定義できます。

- `l3extRsPathL3OutAtt` の下：送信元インターフェイスとして物理インターフェイスが使用されます。
- `l3extLNodeP` の下：送信元インターフェイスとしてループバック インターフェイスが使用されます。

OSPF

接続を有効にして冗長性を提供するために、さまざまなホスト タイプが OSPF を必要とします。これらには、たとえばファブリック内および WAN へのレイヤ 3 中継として ACI ファブリックを使用するサービス ノード、外部ポッド、メインフレーム デバイスなどがあります。このような外部デバイスは、OSPF を実行している非境界リーフ スイッチを介してファブリックとピアリングします。デフォルト ルートは受信し、全域ルーティングには参加しないよう、OSPF エリアを NSSA（スタブ）エリアとして設定します。通常は、既存のルーティングの導入によって設定の変更が回避されるため、スタブ エリアの設定は必須ではありません。

`l3extOut` で `ospfExtP` 管理対象オブジェクトを設定して、OSPF を有効にします。BL スイッチ上で設定されている OSPF IP アドレス ファミリ バージョンは、OSPF インターフェイス IP アドレスに設定されているアドレス ファミリによって決まります。

（注） `l3extOut` ポリシーにルーティング プロトコル（たとえば、関連する VRF とエリア ID を含む OSPF）が含まれる一方で、レイヤ 3 外部インターフェイスのプロファイルには必要な OSPF インターフェイスの詳細が含まれます。いずれも OSPF のイネーブル化に必要です。

アドレス ファミリごとに設定可能な `fvRsCtxToOspfCtxPol` 関係を使用して、VRF レベルで OSPF ポリシーを設定します。設定していない場合、デフォルト パラメータが使用されます。

要求されるエリア プロパティ Ipv6 を公開する `ospfExtP` 管理対象オブジェクトで OSPF を設定します。

サブネットの範囲と集約コントロール

次のセクションでは、サブネットを作成するときに利用できるいくつかの範囲と集約に関するオプションについて説明します:

Export Route Control Subnet: コントロールは、ファブリック外の特定の中継ルートをアドバタイズします。これは中継ルートにのみ影響するもので、内部ルートやブリッジ ドメインで設定されるデフォルトのゲートウェイには影響しません。

このコントロールは、インポート ルート制御の強制が設定されている場合 (BGP でのみサポート)、ルートを Border Gateway Protocol (BGP) でファブリックにアドバタイズすることを可能にします。

External Subnets for the External EPG (セキュリティ インポート サブネットとも呼ばれる): このオプションは、ルーティング情報のファブリックへの出入りはコントロールしません。トラ

フィックがある外部 EPG から別の外部 EPG に、または内部 EPG に流れるようにするには、サブネットにはこのコントロールでマークを付ける必要があります。このコントロールを使用してサブネットにマークしなかった場合には、ある EPG から学習したルートが他の外部 EPG にもアドバタイズされますが、パケットはファブリックでドロップされます。パケットがドロップされるのは、APIC がホワイトリスト モデルで動作するからです。そのデフォルトの動作は、契約で明示的に許可されていない限り、EPG 間の全データ プレーン トラフィックをドロップするというものです。このホワイトリスト モデルは外部 EPG とアプリケーション EPG に適用されます。このオプションが設定されているセキュリティ ポリシーを使用する場合には、契約とセキュリティ プレフィックスを設定する必要があります。

Shared Route Control Subnet: VRF 間のリーキングの共有 L3Outs から学習されたサブネットは、他の VRF にアドバタイズされる前に、このコントロールでマークされる必要があります。APIC リリース 2.2(2e) 以降では、異なる VRF の共有 L3Outs は契約を使用して相互に通信できます。異なる VRF の共有 L3Outs 間の通信の詳細については、『*Cisco APIC* レイヤ *3* ネットワー キング構成定ガイド』を参照してください。

Shared Security Import Subnet: このコントロールは、共有 L3Out 学習ルートについては、[External Subnets for the External EPG] と同じです。トラフィックがある外部 EPG から別の外部 EPG に、または別の内部 EPG に流れるようにするには、サブネットにはこのコントロールでマークを付ける必要があります。このコントロールを使用してサブネットにマークしなかった場合には、ある EPG から学習したルートが他の外部 EPG にもアドバタイズされますが、パケットはファブリックでドロップされます。このオプションが設定されているセキュリティ ポリシーを使用する場合には、契約とセキュリティ プレフィックスを設定する必要があります。

Aggregate Export, Aggregate Import, and Aggregate Shared Routes: このオプションは、0.0.0.0/0 プレフィックスの前に 32 を追加します。現在、インポート/エクスポート ルート制御サブネットに集約できるのは、0.0.0.0/0 プレフィクスのみです。0.0.0.0/0 プレフィックスを集約すると、制御プロファイルを 0.0.0.0/0 ネットワークに適用することはできなくなります。

Aggregate Shared Route: このオプションは、共有ルート制御サブネットとしてマークされている任意のプレフィックスに使用できます。

Route Control Profile: ACI ファブリックは、ファブリックの内部と外部にアドバタイズされるルート用に、ルート マップの set 句もサポートします。ルート マップの set ルールは、ルート制御プロファイル ポリシーとアクション ルール プロファイルで設定されます。

プロパティ	OSPF	EIGRP	BGP	注
コミュニティの設定	×	×	○	標準コミュニティと拡張コミュニティをサポートします。

プロパティ	OSPF	EIGRP	BGP	注
ルート タグ	対応	対応	×	BDのサブネットのみでサポートされます。中継プレフィックスには、常にタグ4294967295が割り当てられます。
優先順位	×	×	○	BGP ローカル プリファレンスを設定します。
メトリック	○	×	○	BGP に MED を設定し、EIGRP のメトリックを変更しますが、EIGRP 複合メトリックは指定できません。
メトリック タイプ	○	×	×	OSPF タイプ 1 と OSPF タイプ 2。

ルート制御プロファイル ポリシー

ACI ファブリックは、ファブリックの内部と外部にアドバタイズされるルート用に、ルート マップの set 句もサポートします。ルート マップの set ルールは、ルート制御プロファイル ポリシーとアクション ルール プロファイルで設定されます。

ACI は以下の set オプションをサポートします。

表 *22 :* アクション ルール プロファイルのプロパティ（ルートマップ の *set* 句）

プロパティ	OSPF	EIGRP	BGP	注
コミュニティの設定			○	標準コミュニティと拡張コミュニティをサポートします。
追加のコミュニティを設定			○	標準コミュニティと拡張コミュニティをサポートします。

プロパティ	OSPF	EIGRP	BGP	注
ルート タグ	対応	対応		BD のサブネットのみでサポートされます。中継プレフィックスには、常にタグ 4294967295 が割り当てられます。
優先順位			○	BGP ローカル プリファレンスを設定します。
メトリック	対応		対応	BGP の MED を設定します。EIGRP のメトリックを変更しますが、EIGRP 複合メトリックは指定できません。
メトリック タイプ	○			OSPF タイプ 1 と OSPF タイプ 2。

ルート プロファイル ポリシーは、レイヤ 3 Outside 接続の下に作成されます。ルート制御ポリシーは、以下のオブジェクトで参照できます。

- テナント BD サブネット
- テナント BD
- 外部 EPG
- 外部 EPG のインポート/エクスポート サブネット

以下に、BGP のインポート ルート制御を使用し、2 つの異なるレイヤ 2 Outside から学習した外部ルートのローカル プリファレンスを設定する例を示します。AS300 への外部接続用のレイヤ 3 Outside 接続は、インポート ルート制御を適用して設定されています。アクション ルール プロファイルの設定では、[Local Preference] ウィンドウの [Action Rule Profile] でローカル プリファレンスが 200 に設定されています。

レイヤ 3 Outside 接続の外部 EPG は、0.0.0.0/0 インポート集約ポリシーを使用してすべてのルートを許可するように設定されています。これは、インポート ルート制御が適用されていますが、どのプレフィックスもブロックされてはならないためです。ローカルプリファレンスの設定を許可するために、インポート ルート制御が適用されています。また、[Route Control Profile] ウィンドウの [External EPG] で [Action Rule Profile] を参照するルート プロファイルを使用して、別のインポート サブネット 151.0.1.0/24 が追加されています。

MP-BGP テーブルを表示するには、show ip bgp vrf overlay-1 コマンドを使用します。スパインの MP-BGP テーブルには、プレフィックス 151.0.1.0/24 とローカル プリファレンス 200、および BGP 300 レイヤ 3 Outside 接続の境界リーフの次のホップが表示されます。

default-import と default-export という、2 つの特殊なルート制御プロファイルがあります。名前 default-import および default-export を使用して設定すると、ルート制御プロファイルはインポートとエクスポート両方のレイヤ 3 Outside レベルで自動的に適用されます。default-import および default-export のルート制御プロファイルは、0.0.0.0/0 集約を使用して設定することはできません。

ルート制御プロファイルは、次の順序でファブリック ルートに適用されます。

1. テナント BD サブネット
2. テナント BD
3. レイヤ 3 Outside

ルート制御プロファイルは、次の順序で中継ルートに適用されます。

1. 外部 EPG プレフィックス
2. 外部 EPG
3. レイヤ 3 Outside

セキュリティ インポート ポリシー

本書で説明されているポリシーでは、ACI ファブリックの内外へのルーティング情報の交換、およびルートの制御とタグ付けに使用する方法を取り扱ってきました。ファブリックはホワイトリスト モデルで動作します。そのデフォルトの動作は、契約によって明示的に許可されていない限り、エンドポイント グループ間のすべてのデータプレーン トラフィックをドロップするというものです。このホワイトリスト モデルは外部 EPG とテナント EPG に適用されます。

中継トラフィックの場合、テナント トラフィックとは、セキュリティ ポリシーの設定方法と実装方法が少し異なります。

中継セキュリティ ポリシー

- プレフィックス フィルタリングを使用します。
- リリース 2.0(1m) 以降では、Ethertype、プロトコル、L4 ポート、および TCP フラグ フィルタのサポートが利用できるようになりました。
- セキュリティ インポート サブネット（プレフィックス）と外部 EPG で設定されたコントラクトを使用して実装されます。

テナント EPG セキュリティ ポリシー

- プレフィックス フィルタリングは使用しないでください。
- Ethertype、プロトコル、L4 ポート、および TCP フラグ フィルタをサポートします。

- テナント EPG←→EPG およびテナント EPG←→外部 EPG でサポートされます。

外部プレフィックス ベースの EPG 間に契約が存在しない場合、トラフィックはドロップされます。2 つの外部 Epg の間のトラフィックを許可するには、契約とセキュリティ プレフィックスを設定する必要があります。プレフィックス フィルタリングのみがサポートされるため、契約ではデフォルト フィルタを使用できます。

外部 L3Out 接続契約

L3Out 接続が展開されているすべてのリーフ ノードでは、L3Out 接続のプレフィックスの結合がプログラムされます。3 つ以上の L3Out 接続が展開されている場合、集約ルール 0.0.0.0/0 を使用すると、契約のない L3Out 接続間でもトラフィックのフローが許可されます。

L3Out インスタンス プロファイル (instP) で、プロバイダーとコンシューマの契約の関連づけとセキュリティ インポート サブネットを設定します。

セキュリティ インポート サブネットが設定されており、集約ルール、0.0.0.0/0 がサポートされている場合、セキュリティ インポート サブネットは ACL タイプのルールに従います。セキュリティ インポート サブネットのルール 10.0.0.0/8 は、 10.0.0.0～10.255.255.255 の範囲のすべてのアドレスに適合します。ルート制御サブネットで許可されているプレフィックスに対して正確なプレフィックス照合を設定する必要はありません。

3 つ以上の L3Out 接続が同じ VRF 内に設定されている場合は、ルールの結合が問題となるため、セキュリティ インポート サブネットを設定するときに注意する必要があります。

同じ L3Out で入出力する中継トラフィック フローは、0.0.0.0/0 セキュリティ インポート サブネットを設定すると、ポリシーによってドロップされます。この動作は、ダイナミックまたはスタティック ルーティングに当てはまります。この動作を防ぐためには、より詳細なサブネットを定義してください。

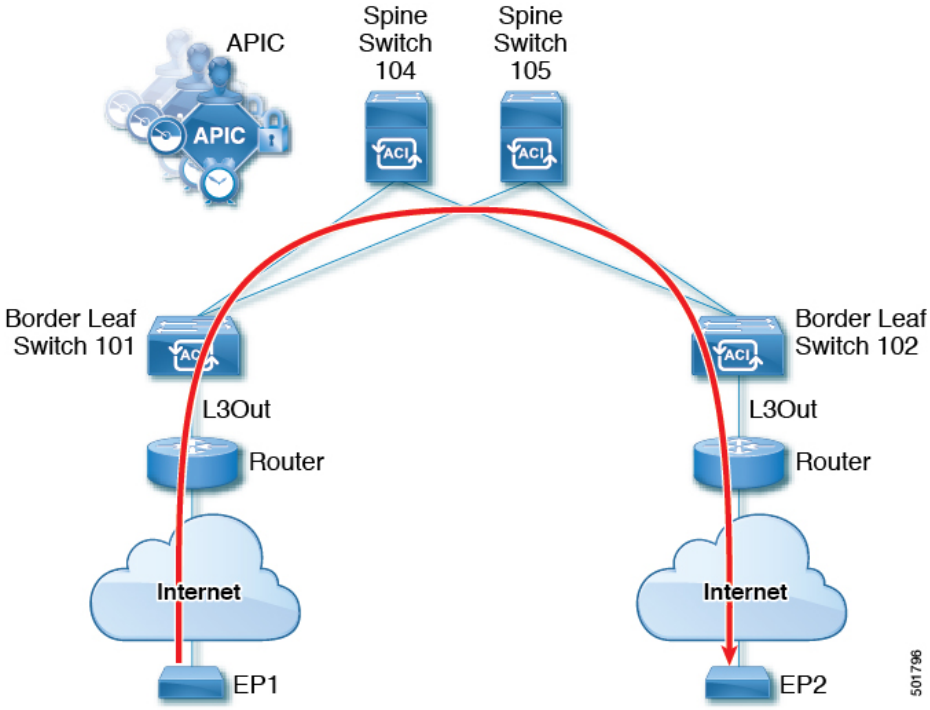
トランジット ルーティングの設定

トランジット ルーティングの概要

このトピックでは、CiscoAPIC を使用する際のトランジット ルーティングを設定する方法の一般的な例を説明します。

この章にある例では、次のトポロジを使用します。

図 *37 :*



この章の例では、Cisco ACI ファブリックには APIC クラスタによって制御される 2 個のリーフ スイッチと 2 個のスパイン スイッチがあります。境界リーフ スイッチ 101 と 102 には L3Out があり、2 t のルータに接続することでインターネットにも接続しています。この例の目標は、2 つの L3Out を通して、インターネット上の EP 1 から EP2 へ、ファブリック内外をトラフィックが行き来できるようにすることです。

この例では、両方の L3Out に関連付けられているテナントは、`t1` と、VRF がつく `v1` です。

L3Out を設定する前に、ノード、ポート、機能プロファイル、AEP、レイヤ 3 ドメインを設定します。BGP ルート リフレクタとして 104 と 105 スパイン スイッチを設定する必要があります。

トランジット ルーティングの設定には、次のコンポーネントの定義が含まれます。

1. テナントおよび VRF
2. リーフ 101 と 102 上のノードおよびインターフェイス
3. 各 L3Out のプライマリ ルーティング プロトコル（境界リーフ スイッチと外部ルータ間のルートの交換に使用。この例では BGP）
4. 各 L3Out のルーティング プロトコルの接続性（プライマリ プロトコルへの到達可能性情報の提供。この例では、OSPF）
5. 2 個の外部 EPG
6. 1 個のルート マップ

7. 少なくとも 1 つのフィルタと 1 つのコントラクト
8. 外部 EPG とコントラクトを関連付ける

（注） トランジット ルーティングの注意事項については、中継ルーティングのガイドライン （322 ページ） を参照してください。

次の表では、この章で使用される名前を一覧にしています。

プロパティ	ノード 101 の L3Out1 の名前	ノード 102 の L3Out2 の名前
テナント	t1	t1
VRF	v1	v1
ノード	ルータ ID 11.11.11.103 を持つ nodep1	ルータ ID 22.22.22.203 を持つ nodep2
OSPF インターフェイス	Eth/1/3 の ifp1	Eth/1/3 の ifp2
BPG ピア アドレス	15.15.15.2/24	25.25.25.2/24
外部 EPG	192.168.1.0/24 の extnw1	192.168.2.0/24 の extnw2
ルート マップ	Ctx1 を持つ rp1 とルートの宛先 192.168.1.0/24	ctx2 を持つ rp2 とルートの宛先 192.168.2.0/24
フィルタ	http-filter	http-filter
コントラクト	extnw1 によって提供される httpCtrct	extnw2 によって消費される httpCtrct

REST API を使用したトランジット ルーティングの設定

次の手順では、テナントのトランジットルーティングを設定する方法を説明します。この例では、別のルータにそれぞれ接続された 2 つの境界リーフ スイッチで、1 つの VRF 内に 2 つの L3Out を展開します。

始める前に

- 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。
- 外部ルーテッド ドメインを作成し、L3Out のインターフェイスに関連付けます。
- ファブリック内でルートを伝播させるために、BGP ルート リフレクタ ポリシーを設定します。

これらの前提条件の XML の例については、REST API の例: L3Out の前提条件 （32 ページ）を参照してください。

手順

ステップ 1 テナントおよび VRF を設定します。

この例ではテナント `t1` および VRF `v1` を設定します。VRF はまだ展開されていません。

例：

```
<fvTenant  name="t1">
    <fvCtx name="v1"/>
</fvTenant>
```

ステップ 2 ノードおよびインターフェイスを設定します。

この例では、2 つの境界リーフ スイッチで、テナント t1 と VRF v1 に 2 つの L3Outs を設定します。VRF は、レイヤ 3 ドメイン `dom1` です。

- 最初の L3Out はノード 101 上にあり、`nodep1` という名前です。ノード 101 はルータ ID `11.11.11.103` で設定されます。ルーテッド インターフェイス `ifp1` が `eth1/3` にあり、IP アドレス `12.12.12.3/24` です。
- 2 番目の L3Out が ノード 102 上にあり、`nodep2` という名前です。ノード 102 はルータ ID `22.22.22.203` に設定されています。IP アドレス、`23.23.23.1/24` を持つ `eth1/3` でルーテッド インターフェイス `ifp2` があります。

例：

```
<l3extOut name="l3out1">
    <l3extRsEctx tnFvCtxName="v1"/>
    <l3extLNodeP name="nodep1">
        <l3extRsNodeL3OutAtt rtrId="11.11.11.103" tDn="topology/pod-1/node-101"/>
        <l3extLIfP name="ifp1"/>
        <l3extRsPathL3OutAtt addr="12.12.12.3/24" ifInstT="l3-port"
tDn="topology/pod-1/paths-101/pathep-[eth1/3]"/>
        </l3extLIfP>
    </l3extLNodeP>
    <l3extRsL3DomAtt tDn="uni/l3dom-dom1"/>
</l3extOut>

<l3extOut name="l3out2">
    <l3extRsEctx tnFvCtxName="v1"/>
    <l3extLNodeP name="nodep2">
        <l3extRsNodeL3OutAtt rtrId="22.22.22.203" tDn="topology/pod-1/node-102"/>
        <l3extLIfP name="ifp2"/>
        <l3extRsPathL3OutAtt addr="23.23.23.3/24" ifInstT="l3-port"
tDn="topology/pod-1/paths-102/pathep-[eth1/3]"/>
        </l3extLIfP>
    </l3extLNodeP>
    <l3extRsL3DomAtt tDn="uni/l3dom-dom1"/>
</l3extOut>
```

ステップ 3 両方の境界リーフ スイッチのルーティング プロトコルを設定します。

この例では、両方の境界リーフ スイッチに対して、ASN 100 でプライマリ ルーティング プロトコルとしてBGPを設定します。BGP ピア 15.15.15.2 を持つノード101とBGP ピア 25.25.25.2 を持つノード102を設定します。

例：

```
<l3extOut name="l3out1">
    <l3extLNodeP name="nodep1">
        <bgpPeerP addr="15.15.15.2/24"
            <bgpAsP asn="100"/>
        </bgpPeerP>
    </l3extLNodeP>
</l3extOut>

<l3extOut name="l3out2">
    <l3extLNodeP name="nodep2">
        <bgpPeerP addr="25.25.25.2/24"
            <bgpAsP asn="100"/>
        </bgpPeerP>
    </l3extLNodeP>
</l3extOut>
```

ステップ 4 接続ルーティング プロトコルを設定します。

この例では、定期的なエリア ID 0.0.0.0 で両方の L3Outs に対して通信プロトコルとしてOSPFを設定します 。

例：

```
<l3extOut name="l3out1">
    <ospfExtP areaId="0.0.0.0" areaType="regular"/>
    <l3extLNodeP name="nodep1">
        <l3extLIfP name="ifp1">
            <ospfIfP/>
        <l3extIfP>
    <l3extLNodeP>
</l3extOut>
<l3extOut name="l3out2">
    <ospfExtP areaId="0.0.0.0" areaType="regular"/>
    <l3extLNodeP name="nodep2">
        <l3extLIfP name="ifp2">
            <ospfIfP/>
        <l3extIfP>
    <l3extLNodeP>
</l3extOut>
```

ステップ 5 外部 EPG を設定します。

この例では、ノード101上の外部ネットワーク extnw1 としてネットワーク 192.168.1.0/24 と、ノード 102 上の外部ネットワーク extnw2 として 192.168.2.0/24 を設定します。また、ルート制御プロファイル rp1 および rp2.と外部 EPG を関連付けます。

例：

```
<l3extOut name="l3out1">
     <l3extInstP name="extnw1">
          <l3extSubnet ip="192.168.1.0/24" scope="import-security"/>
          <l3extRsInstPToProfile direction="export" tnRtctrlProfileName="rp1"/>
    </l3extInstP>
</l3extOut>
<l3extOut name="l3out2">
     <l3extInstP name="extnw2">
          <l3extSubnet ip="192.168.2.0/24" scope="import-security"/>
```

```
            <l3extRsInstPToProfile direction="export" tnRtctrlProfileName="rp2"/>
    </l3extInstP>
</l3extOut>
```

ステップ 6 オプション。ルート マップを設定します。

この例では、インバウンドおよびアウトバウンド方向で各 BGP ピアのルート マップを設定します。`L3out1` では、ルート マップ `rp1` が `192.168.1.0/24` のインポート宛先に一致するルートに適用され、ルート マップ `rp2` が `192.168.2.0/24` のエクスポート宛先に一致するルートに適用されます。`L3out2` では、ルート マップの方向を反転します。

例：

```
<fvTenant name="t1">
    <rtctrlSubjP name="match-rule1">
        <rtctrlMatchRtDest ip="192.168.1.0/24" />
    </rtctrlSubjP>
    <rtctrlSubjP name="match-rule2">
        <rtctrlMatchRtDest ip="192.168.2.0/24" />
    </rtctrlSubjP>
    <l3extOut name="l3out1">
        <rtctrlProfile name="rp1">
            <rtctrlCtxP name="ctxp1" action="permit" order="0">
                <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule1" />
            </rtctrlCtxP>
        </rtctrlProfile>
        <rtctrlProfile name="rp2">
            <rtctrlCtxP name="ctxp1" action="permit" order="0">
                <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule2" />
            </rtctrlCtxP>
        </rtctrlProfile>
        <l3extInstP name="extnw1">
            <l3extRsInstPToProfile direction="import" tnRtctrlProfileName="rp1" />
            <l3extRsInstPToProfile direction="export" tnRtctrlProfileName="rp2" />
        </l3extInstP>
    </l3extOut>
    <l3extOut name="l3out2">
        <rtctrlProfile name="rp1">
            <rtctrlCtxP name="ctxp1" action="permit" order="0">
                <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule1" />
            </rtctrlCtxP>
        </rtctrlProfile>
        <rtctrlProfile name="rp2">
            <rtctrlCtxP name="ctxp1" action="permit" order="0">
                <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule2" />
            </rtctrlCtxP>
        </rtctrlProfile>
        <l3extInstP name="extnw2">
            <l3extRsInstPToProfile direction="import" tnRtctrlProfileName="rp2" />
            <l3extRsInstPToProfile direction="export" tnRtctrlProfileName="rp1" />
        </l3extInstP>
    </l3extOut>
</fvTenant>
```

ステップ 7 フィルタおよびコントラクトを作成し、EPG が通信できるようにします。

この例では、フィルタ `http-filter` とコントラクト `httpCtrct` を設定します。外部 EPG およびアプリケーション EPG は、それぞれプロバイダおよびコンシューマとして、すでにコントラクト `httpCtrct` と関連付けられています。

例：

```
<vzFilter name="http-filter">
    <vzEntry  name="http-e" etherT="ip" prot="tcp"/>
</vzFilter>
<vzBrCP name="httpCtrct" scope="context">
    <vzSubj name="subj1">
        <vzRsSubjFiltAtt tnVzFilterName="http-filter"/>
    </vzSubj>
</vzBrCP>
```

ステップ 8 コントラクトと外部 EPG を関連付けます。

この例では、外部 EPG `extnw1` をプロバイダとして、外部 EPG `extnw2` をコントラクト `httpCtrct` のコンシューマとして関連付けます。

```
 <l3extOut name="l3out1">
    <l3extInstP name="extnw1">
        <fvRsProv tnVzBrCPName="httpCtrct"/>
    </l3extInstP>
</l3extOut>
<l3extOut name="l3out2">
    <l3extInstP name="extnw2">
        <fvRsCons tnVzBrCPName="httpCtrct"/>
    </l3extInstP>
</l3extOut>
```

REST API の例: 中継ルーティング

次の例では、REST API を使用して、2 つの境界リーフ スイッチで 2 つの L3Outs を設定します。

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/policymgr/mo/.xml -->
<polUni>
    <fvTenant name="t1">
        <fvCtx name="v1"/>
        <l3extOut name="l3out1">
            <l3extRsEctx tnFvCtxName="v1"/>
            <l3extLNodeP name="nodep1">
                <bgpPeerP addr="15.15.15.2/24">
                    <bgpAsP asn="100"/>
                </bgpPeerP>
              <l3extRsNodeL3OutAtt rtrId="11.11.11.103" tDn="topology/pod-1/node-101"/>

                <l3extLIfP name="ifp1">
                    <l3extRsPathL3OutAtt addr="12.12.12.3/24" ifInstT="l3-port"
tDn="topology/pod-1/paths-101/pathep-[eth1/3]" />
                    <ospfIfP/>
                </l3extLIfP>
            </l3extLNodeP>
            <l3extInstP name="extnw1">
                <l3extSubnet ip="192.168.1.0/24" scope="import-security"/>
                <l3extRsInstPToProfile direction="import" tnRtctrlProfileName="rp1"/>
                <l3extRsInstPToProfile direction="export" tnRtctrlProfileName="rp2"/>
                <fvRsProv tnVzBrCPName="httpCtrct"/>
            </l3extInstP>
            <bgpExtP/>
            <ospfExtP areaId="0.0.0.0" areaType="regular"/>
            <l3extRsL3DomAtt tDn="uni/l3dom-dom1"/>
            <rtctrlProfile name="rp1">
                <rtctrlCtxP name="ctxp1" action="permit" order="0">
```

```
                        <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule1"/>
                    </rtctrlCtxP>
                </rtctrlProfile>
                <rtctrlProfile name="rp2">
                    <rtctrlCtxP name="ctxp1" action="permit" order="0">
                        <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule2"/>
                    </rtctrlCtxP>
                </rtctrlProfile>
            </l3extOut>
            <l3extOut name="l3out2">
                <l3extRsEctx tnFvCtxName="v1"/>
                <l3extLNodeP name="nodep2">
                    <bgpPeerP addr="25.25.25.2/24">
                        <bgpAsP asn="100"/>
                    </bgpPeerP>
                    <l3extRsNodeL3OutAtt rtrId="22.22.22.203" tDn="topology/pod-1/node-102"
 />
                    <l3extLIfP name="ifp2">
                        <l3extRsPathL3OutAtt addr="23.23.23.3/24" ifInstT="l3-port"
tDn="topology/pod-1/paths-102/pathep-[eth1/3]" />
                        <ospfIfP/>
                    </l3extLIfP>
                </l3extLNodeP>
                <l3extInstP name="extnw2">
                    <l3extSubnet ip="192.168.2.0/24" scope="import-security"/>
                    <l3extRsInstPToProfile direction="import" tnRtctrlProfileName="rp2"/>
                    <l3extRsInstPToProfile direction="export" tnRtctrlProfileName="rp1"/>
                    <fvRsCons tnVzBrCPName="httpCtrct"/>
                </l3extInstP>
                <bgpExtP/>
                <ospfExtP areaId="0.0.0.0" areaType="regular"/>
                <l3extRsL3DomAtt tDn="uni/l3dom-dom1"/>
                <rtctrlProfile name="rp1">
                    <rtctrlCtxP name="ctxp1" action="permit" order="0">
                        <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule1"/>
                    </rtctrlCtxP>
                </rtctrlProfile>
                <rtctrlProfile name="rp2">
                    <rtctrlCtxP name="ctxp1" action="permit" order="0">
                        <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule2"/>
                    </rtctrlCtxP>
                </rtctrlProfile>
            </l3extOut>
            <rtctrlSubjP name="match-rule1">
                <rtctrlMatchRtDest ip="192.168.1.0/24"/>
            </rtctrlSubjP>
            <rtctrlSubjP name="match-rule2">
                <rtctrlMatchRtDest ip="192.168.2.0/24"/>
            </rtctrlSubjP>
            <vzFilter name="http-filter">
                <vzEntry name="http-e" etherT="ip" prot="tcp"/>
            </vzFilter>
            <vzBrCP name="httpCtrct" scope="context">
                <vzSubj name="subj1">
                    <vzRsSubjFiltAtt tnVzFilterName="http-filter"/>
                </vzSubj>
            </vzBrCP>
        </fvTenant>
    </polUni>
```

NX-OS スタイル CLI を使用したトランジット ルーティングの設定

次の手順では、テナントのトランジットルーティングを設定する方法を説明します。この例では、別々にルータに接続された 2 つの境界リーフ スイッチ上の 1 個の VRF で、2 個の L3Outs を展開します。

始める前に

- 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。
- 使用して VLAN ドメイン設定、 **vlan ドメイン** ドメイン および **vlan** *vlan* 範囲 コマンド。
- BGP ルート リフレクタ ポリシーを設定し、ファブリック内でルーテッドを伝達します。

これらの前提条件のコマンド例については、NX-OS スタイル CLI の例: L3Out の前提条件 （38 ページ） を参照してください。

手順

ステップ 1 テナントおよび VRF を設定します。

この例では VRF `v1` でテナント `t1` を設定します。VRF はまだ展開されていません。

例：

```
apic1# configure
apic1(config)# tenant t1
apic1(config-tenant)# vrf context v1
apic1(config-tenant-vrf)# exit
apic1(config-tenant)# exit
```

ステップ 2 ノードおよびインターフェイスを設定します。

この例では、2 つの境界リーフ スイッチでテナント t1 の 2 つの L3Outs を設定します。

- 最初の L3Out はノード 101 上にあり、`nodep1` という名前です。ノード 101 はルータ ID `11.11.11.103` で設定されます。ルーテッド インターフェイス `ifp1` が `eth1/3` にあり、IP アドレス `12.12.12.3/24` です。
- 2 番目の L3Out が ノード 102 上にあり、`nodep2` という名前です。ノード 102 はルータ ID `22.22.22.203` で設定されます。ルーテッド インターフェイス `ifp2` が `eth1/3` に存在し、IP アドレスは `23.23.23.1/24` です。

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# router-id 11.11.11.103
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# interface ethernet 1/3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vrf member tenant t1 vrf v1
```

```
apic1(config-leaf-if)# ip address 12.12.12.3/24
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config)# leaf 102
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# router-id 22.22.22.203
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# interface ethernet 1/3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vrf member tenant t1 vrf v1
apic1(config-leaf-if)# ip address 23.23.23.3/24
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

ステップ 3 両方のリーフ スイッチのルーティング プロトコルを設定します。

この例では、両方の境界リーフ スイッチに対して、ASN 100 でプライマリ ルーティング プロトコルとしてBGPを設定します。BGP ピア `15.15.15.2` を持つノード101と BGP ピア `25.25.25.2` を持つノード102を設定します。

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 15.15.15.2
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# exit
apic1(config)# leaf 102
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 25.25.25.2
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# exit
```

ステップ 4 接続ルーティング プロトコルを設定します。

この例では、定期的なエリア ID `0.0.0.0` で両方の L3Outs に対して通信プロトコルとして OSPF を設定します 。

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant t1 vrf v1
apic1(config-leaf-ospf-vrf)# area 0.0.0.0 loopback 40.40.40.1
apic1(config-leaf-ospf-vrf)# exit
apic1(config-leaf-ospf)# exit
apic1(config-leaf)# exit
apic1(config)# leaf 102
apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant t1 vrf v1
apic1(config-leaf-ospf-vrf)# area 0.0.0.0 loopback 60.60.60.1
apic1(config-leaf-ospf-vrf)# exit
apic1(config-leaf-ospf)# exit
apic1(config-leaf)# exit
```

ステップ 5 外部 EPG を設定します。

この例では、ネットワーク 192.168.1.0/24 をノード 101 上の外部ネットワーク extnw1 として、ネットワーク 192.168.2.0/24 をノード 102 上の外部ネットワーク extnw2 として設定します。

例：

```
apic1(config)# tenant t1
apic1(config-tenant)# external-l3 epg extnw1
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# match ip 192.168.1.0/24
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# external-l3 epg extnw2
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# match ip 192.168.2.0/24
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# exit
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# external-l3 epg extnw1
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# exit
apic1(config)# leaf 102
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# external-l3 epg extnw2
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# exit
```

ステップ 6 オプション。ルート マップを設定します。

この例では、インバウンドおよびアウトバウンド方向で各 BGP ピアのルート マップを設定します。

例：

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# template route group match-rule1 tenant t1
apic1(config-route-group)# ip prefix permit 192.168.1.0/24
apic1(config-route-group)# exit
apic1(config-leaf)# template route group match-rule2 tenant t1
apic1(config-route-group)# ip prefix permit 192.168.2.0/24
apic1(config-route-group)# exit
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# route-map rp1
apic1(config-leaf-vrf-route-map)# match route group match-rule1 order 0
apic1(config-leaf-vrf-route-map-match)# exit
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf)# route-map rp2
apic1(config-leaf-vrf-route-map)# match route group match-rule2 order 0
apic1(config-leaf-vrf-route-map-match)# exit
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 15.15.15.2
apic1(config-leaf-bgp-vrf-neighbor)# route-map rp1 in
apic1(config-leaf-bgp-vrf-neighbor)# route-map rp2 out
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# exit
```

```
apic1(config)# leaf 102
apic1(config-leaf)# template route group match-rule1 tenant t1
apic1(config-route-group)# ip prefix permit 192.168.1.0/24
apic1(config-route-group)# exit
apic1(config-leaf)# template route group match-rule2 tenant t1
apic1(config-route-group)# ip prefix permit 192.168.2.0/24
apic1(config-route-group)# exit
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# route-map rp1
apic1(config-leaf-vrf-route-map)# match route group match-rule2 order 0
apic1(config-leaf-vrf-route-map-match)# exit
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf)# route-map rp2
apic1(config-leaf-vrf-route-map)# match route group match-rule1 order 0
apic1(config-leaf-vrf-route-map-match)# exit
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 25.25.25.2
apic1(config-leaf-bgp-vrf-neighbor)# route-map rp2 in
apic1(config-leaf-bgp-vrf-neighbor)# route-map rp1 out
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# exit
```

ステップ 7 フィルタ（アクセス リスト）およびコントラクトを作成し、EPGが通信できるようにします。

例：

```
apic1(config)# tenant t1
apic1(config-tenant)# access-list http-filter
apic1(config-tenant-acl)# match ip
apic1(config-tenant-acl)# match tcp dest 80
apic1(config-tenant-acl)# exit
apic1(config-tenant)# contract httpCtrct
apic1(config-tenant-contract)# scope vrf
apic1(config-tenant-contract)# subject subj1
apic1(config-tenant-contract-subj)# access-group http-filter both
apic1(config-tenant-contract-subj)# exit
apic1(config-tenant-contract)# exit
apic1(config-tenant)# exit
```

ステップ 8 コントラクトを設定し、EPG に関連付けます。

例：

```
apic1(config)# tenant t1
apic1(config-tenant)# external-l3 epg extnw1
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# contract provider httpCtrct
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# external-l3 epg extnw2
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# contract consumer httpCtrct
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# exit
apic1(config)#
```

例：中継ルーティング

この例では、中継ルーティングのマージされた設定を提供します。設定は別々のルータに接続されている 2 個の障壁リーフ スイッチで、2 つの L3Outs を持つ単一のテナントと VRF のためにあります。

```
apic1# configure
apic1(config)# tenant t1
apic1(config-tenant)# vrf context v1
apic1(config-tenant-vrf)# exit
apic1(config-tenant)# exit

apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# router-id 11.11.11.103
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# interface ethernet 1/3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vrf member tenant t1 vrf v1
apic1(config-leaf-if)# ip address 12.12.12.3/24
apic1(config-leaf-if)# exit
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 15.15.15.2
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant t1 vrf v1
apic1(config-leaf-ospf-vrf)# area 0.0.0.0 loopback 40.40.40.1
apic1(config-leaf-ospf-vrf)# exit
apic1(config-leaf-ospf)# exit
apic1(config-leaf)# exit

apic1(config)# leaf 102
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# router-id 22.22.22.203
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# interface ethernet 1/3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vrf member tenant t1 vrf v1
apic1(config-leaf-if)# ip address 23.23.23.3/24
apic1(config-leaf-if)# exit
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 25.25.25.2/24
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant t1 vrf v1
apic1(config-leaf-ospf-vrf)# area 0.0.0.0 loopback 60.60.60.3
apic1(config-leaf-ospf-vrf)# exit
apic1(config-leaf-ospf)# exit
apic1(config-leaf)# exit

apic1(config)# tenant t1
apic1(config-tenant)# external-l3 epg extnw1
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# match ip 192.168.1.0/24
apic1(config-tenant-l3ext-epg)# exit
```

```
apic1(config-tenant)# external-l3 epg extnw2
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# match ip 192.168.2.0/24
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# exit

apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# external-l3 epg extnw1
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# exit
apic1(config)# leaf 102
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# external-l3 epg extnw2
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# exit

apic1(config)# leaf 101
apic1(config-leaf)# template route group match-rule1 tenant t1
apic1(config-route-group)# ip prefix permit 192.168.1.0/24
apic1(config-route-group)# exit
apic1(config-leaf)# template route group match-rule2 tenant t1
apic1(config-route-group)# ip prefix permit 192.168.2.0/24
apic1(config-route-group)# exit
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# route-map rp1
apic1(config-leaf-vrf-route-map)# match route group match-rule1 order 0
apic1(config-leaf-vrf-route-map-match)# exit
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf)# route-map rp2
apic1(config-leaf-vrf-route-map)# match route group match-rule2 order 0
apic1(config-leaf-vrf-route-map-match)# exit
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 15.15.15.2
apic1(config-leaf-bgp-vrf-neighbor)# route-map rp1 in
apic1(config-leaf-bgp-vrf-neighbor)# route-map rp2 out
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# exit

apic1(config)# leaf 102
apic1(config-leaf)# template route group match-rule1 tenant t1
apic1(config-route-group)# ip prefix permit 192.168.1.0/24
apic1(config-route-group)# exit
apic1(config-leaf)# template route group match-rule2 tenant t1
apic1(config-route-group)# ip prefix permit 192.168.2.0/24
apic1(config-route-group)# exit
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# route-map rp1
apic1(config-leaf-vrf-route-map)# match route group match-rule1 order 0
apic1(config-leaf-vrf-route-map-match)# exit
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf)# route-map rp2
apic1(config-leaf-vrf-route-map)# match route group match-rule2 order 0
apic1(config-leaf-vrf-route-map-match)# exit
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 25.25.25.2
```

```
apic1(config-leaf-bgp-vrf-neighbor)# route-map rp2 in
apic1(config-leaf-bgp-vrf-neighbor)# route-map rp1 out
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# exit

apic1(config)# tenant t1
apic1(config-tenant)# access-list http-filter
apic1(config-tenant-acl)# match ip
apic1(config-tenant-acl)# match tcp dest 80
apic1(config-tenant-acl)# exit
apic1(config-tenant)# contract httpCtrct
apic1(config-tenant-contract)# scope vrf
apic1(config-tenant-contract)# subject http-subj
apic1(config-tenant-contract-subj)# access-group http-filter both
apic1(config-tenant-contract-subj)# exit
apic1(config-tenant-contract)# exit
apic1(config-tenant)# exit

apic1(config)# tenant t1
apic1(config-tenant)# external-l3 epg extnw1
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# contract provider httpCtrct
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# external-l3 epg extnw2
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# contract consumer httpCtrct
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# exit
apic1(config)#
```

GUI を使用した中継ルーティングの設定

これらの手順は、テナントの中継ルーティングを設定する方法を示しています。この例では、2 つの L3Outs を、1 つの VRF 内、2 つの境界リーフ スイッチ上に展開します。スイッチは別々のルータに接続されています。

テナントと VRF を作成する手順を除き、これらの手順を 2 回繰り返して、同じテナントと VRF の下に 2 つの L3Out を作成します。

サンプルの名前については、中継 ACI ファブリックのルーティング （313 ページ）を参照してください。。

始める前に

- 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。
- 外部ルーテッド ドメインを作成し、L3Out のインターフェイスに関連付けます。
- 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 テナントと VRF を作成するには、メニュー バーで、**Tenants** > **Add Tenant** を選択し、**Create Tenant** ダイアログボックスで、次のタスクを実行します:

a) **Name** フィールドに、テナント名を入力します。
b) In the **VRF Name** フィールドに、VRF 名を入力します。
c) **Submit** をクリックします。

（注） この手順の後の手順は2回実行して、中継ルーティングのための同じテナントと VRF に 2 つの L3Out を作成します。

ステップ 2 L3Out の作成を開始するには、**Navigation** ウィンドウで、**Tenant** と **Networking** を展開し、以下の手順を実行します:

a) **External Routed Networks** を右クリックして、**Create Routed Outside** を選択します。
b) **Name** フィールドに、L3Out の名前を入力します。
c) **VRF** ドロップダウンリストから、先ほど作成した VRF を選択します。
d) **External Routed Domain** ドロップダウンリストで、先ほど作成した、外部ルーテッド ドメインを選択します。
e) ルーテッド プロトコルのチェックボックスがある領域で、目的のプロトコル (BGP、OSPF、または EIGRP) をオンにします。

この章の例では、**BGP** および **OSPF** を選択します。

選択するプロトコルに応じて、設定する必要のあるプロパティに入力します。

f) OSPF を有効にした場合は、OSPF の詳細を入力します。

この章の例では、OSPF エリア **0** を使用し、**Regular area** に入力します。

g) + アイコンをクリックして **Nodes and Interfaces Protocol Profiles** を展開します。
h) **Name** フィールドに、名前を入力します
i) + アイコンをクリックして **Nodes** を展開します。
j) **Node ID** フィールドのドロップダウンリストから、L3Out のノードを選択します。
k) **Router ID** フィールドで、ルータ ID (L3Out に接続されているルータの IPv4 または IPv6 アドレス) を入力します。
l) （任意） ループバック アドレスに別の IP アドレスを設定することができます。**Use Router ID as Loopback Address** をオフにし、**Loopback Addresses** を展開し、IP アドレスを入力し、**Update** をクリックします。
m) **Select Node** ダイアログボックスで、**OK** をクリックします。

ステップ 3 BGP を有効にしている場合には、+ アイコンをクリックして **BGP Peer Connectivity Profiles** を展開し、次の手順を実行します:

a) **Peer Address** フィールドに、BGP ピアのアドレスを入力します。
b) **Local-AS Number** フィールドに、BGP AS 番号を入力します。
c) **OK** をクリックします。

ステップ 4 + アイコンをクリックして **Interface Profiles** (OSPF を有効にしていた場合には **OSPF Interface Profiles**) を展開し、次のアクションを実行します:

a) **Name** フィールドに、インターフェイス プロファイルの名前を入力します。
b) **Next** をクリックします。
c) **Protocol Profiles** ダイアログボックスの **OSPF Policy** フィールドで、OSPF ポリシーを選択します。
d) **Next** をクリックします。
e) + アイコンをクリックして **Routed Interfaces** を展開します。
f) **Select Routed Interface** ダイアログボックスで、**Node** ドロップダウンリストからノードを選択します。
g) **Path** ドロップダウンリストから、インターフェイスのパスを選択します。
h) **IPv4 Primary/IPv6 Preferred Address** フィールドに、インターフェイスの IP アドレスとネットワーク マスクを入力します。

（注） IPv6 を設定するには、**Link-local Address** フィールドにリンクローカル アドレスを入力します。

i) **OK (Select Routed Interface** ダイアログボックス) をクリックします。
j) **OK (Create Interface Profile** ダイアログボックス) をクリックします。

ステップ 5 [Create Node Profile] ダイアログボックスで、[OK] をクリックします。

ステップ 6 [Create Routed Outside] ダイアログボックスで、[Next] をクリックします。

ステップ 7 **External EPG Networks** タブで、**Create Route Profiles** をクリックします。

ステップ 8 + アイコンをクリックして **Route Profiles** を展開し、次のアクションを実行します:

a) **Name** フィールドに、ルート マップ名を入力します。
b) **Type** を選択します。

この例では、デフォルトの **Match Prefix AND Routing Policy** のままにします。

c) + アイコンをクリックして **Contexts** を展開し、ルート マップのルート コンテキストを作成します。
d) プロファイル コンテキストの順序と名前を入力します。
e) このコンテキストで実行されるアクションとして、**Deny** または **Permit** を選択します。
f) （任意） **Set Rule** フィールドで、**Create Set Rules for a Route Map** を選択します。

セット ルールのための名前を入力し、ルールで使用するオブジェクトをクリックし、**Finish** をクリックします。

g) **Associated Matched Rules** フィールドで、+ アイコンをクリックしてルート マップの一致ルールを作成します。
h) 一致ルールの名前を入力し、ルールで一致させる対象として **Match Regex Community Terms**、**Match Community Terms**、または **Match Prefix** を入力します。
i) ルール名をクリックして、**Update** をクリックします。
j) **Create Match Rule** ダイアログボックスで、**Submit** をクリックし、**Update** をクリックします。

k) **Create Route Control Context** ダイアログボックスで、**OK** をクリックします。
l) **Create Route Map** ダイアログボックスで、**OK** をクリックします。

ステップ 9 + アイコンをクリックして、**External EPG Networks** を展開します。

ステップ 10 **Name** フィールドに、外部ネットワークの名前を入力します。

ステップ 11 + アイコンをクリックして、**Subnet** を展開します。

ステップ 12 **Create Subnet** ダイアログボックスで、次の操作を実行します。

a) **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。
b) **Scope** フィールドで、L3Out のプレフィックスのエクスポートとインポートを制御するための適切なチェック ボックスをオンにします。

（注） [Scope] オプションの詳細については、この **Create Subnet** パネルのオンライン ヘルプを参照してください。

c) （任意） **Route Summarization Policy** フィールドでは、ドロップダウンリストから既存のルート集約ポリシーを選択するか、必要に応じて新しいユーザを作成します。また、**Export Route Control Subnet** のチェック ボックスもオンにします。

ルート集約ポリシーのタイプは、L3Out に対して有効になっているルーティング プロトコルに依存します。

d) + アイコンをクリックして **Route Control Profile** を展開します。
e) **Name** フィールドのドロップダウン リストから、前に作成したルート制御プロファイルを選択します。
f) **Direction** フィールドで、**Route Export Policy** を選択します。
g) **Update** をクリックします。
h) **Create Subnet** ダイアログボックスで、**OK** をクリックします。
i) （任意） より多くのサブネットを追加するにはこれを繰り返します。
j) **[Create External Network]** ダイアログボックスで、**[OK]** をクリックします。

ステップ 13 **[Create Routed Outside]** ダイアログボックスで、**[Finish]** をクリックします。

ステップ 14 **Navigation** ウィンドウの **External Routed Networks** の下で、前に作成した L3Out を展開し、**Route Maps/Profiles** を右クリックします。

（注） 受信ルートについて BGP、OSPF、または EIGRP の属性を設定するには、default-import ルート制御プロファイルを作成し、適切な set アクションと、 no match のアクションを作成します。

ステップ 15 **Create Route Map/Profile** を選択し**Create Route Map/Profile** ダイアログボックスで、次の手順を実行します:

a) **Name** フィールドのドロップダウンリストから、**default-import** を選択します。
b) **Type** フィールドで、**Match Routing Policy Only** をクリックします。**Submit** をクリックします。

ステップ 16 （任意） 次の手順を使用して、BGP を使用する追加のコミュニティを有効にします:

a) **Set Rules for Route Maps** を右クリックして、**Create Set Rules for a Route Map** をクリックします。
b) **Create Set Rules for a Route Map** ダイアログボックスで、**Add Communities** フィールドをクリックします。
c) ルート プレフィックスごとに複数の BGP コミュニティを割り当てる手順に従います。

ステップ 17 L3Out を使用していた EPG 間の通信を有効にするには、次の手順を使用して、少なくとも 1 つのフィルタと契約を作成します:

a) **Navigation** ウィンドウの L3Out を使用するテナントの下で、**Contracts** を展開します。
b) **Filters** を右クリックして **Create Filter** を選択します。
c) **Name** フィールドに、フィルタのの名前を入力します。

フィルタは基本的にはアクセス コントロール リスト (ACL) です。

d) + アイコンをクリックして **Entries** を展開し、フィルタ エントリを追加します。
e) エントリ の詳細を追加します。。

たとえば、単純な Web フィルタの場合には、次のような条件を設定します:

- **EtherType—IP**
- **IP Protocol—tcp**
- **Destination Port Range From—Unspecified**
- **Destination Port Range To** to **https**

f) **Update** をクリックします。
g) **Create Filter** ダイアログボックスで、**Submit** をクリックします。

ステップ 18 契約を追加するには、次の手順を実行します:

a) **Contracts** の下で、**Standard** を右クリックして、**Create Contract** を選択します。
b) 契約の名前を入力します。
c) + アイコンをクリックして **Subjects** を展開し、刑や訓示情報カテゴリを追加します。
d) 情報カテゴリの名前を入力します。
e) + アイコンをクリックして **Filters** を展開し、ドロップダウンリストから、前に作成したフィルタを選択します。
f) **Update** をクリックします。
g) **Create Contract Subject** ダイアログボックスで、**OK** をクリックします。
h) **Create Contract** ダイアログボックスで、**Submit**をクリックします。

ステップ 19 次の手順で、L3Out の EPGを契約に関連付けます:

最初の L3 外部 EPG、`extnw1` が契約のプロバイダーとなり、2 番目の外部 EPG、`extnw2` がコンシューマとなります。

a) 契約をプロバイダーとしての L3 外部 EPG に関連付けるには、テナントの下で **Networking** をクリックし、**External Routed Networks** をクリックし、L3Out を展開します。
b) **Networks** を展開し、L3 外部 EPG をクリックし、**Contracts** をクリックします。
c) + アイコンをクリックして **Provided Contracts** を展開します。

2 番目の L3 外部 EPG で、+ アイコンをクリックして **Consumed Contracts** を展開します。

d) **Name** フィールドで、前に作成した契約をリストから選択します。
e) **Update** をクリックします。
f) [送信（Submit）] をクリックします。