



WAN およびその他の外部ネットワーク フォワーディング

この章は、次の内容で構成されています。

- [ネットワーク ドメイン \(1 ページ\)](#)
- [ルータ ピアリングおよびルート配布 \(2 ページ\)](#)
- [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 \(3 ページ\)](#)
- [ACI のルート再配布 \(8 ページ\)](#)
- [ACI ファブリック内のルート配布 \(8 ページ\)](#)
- [外部レイヤ 3 Outside 接続タイプ \(9 ページ\)](#)
- [レイヤ 3 外部接続の設定のモードについて \(12 ページ\)](#)
- [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 \(13 ページ\)](#)
- [ACI レイヤ 3 Outside ネットワークのワークフロー \(15 ページ\)](#)

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VLAN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。

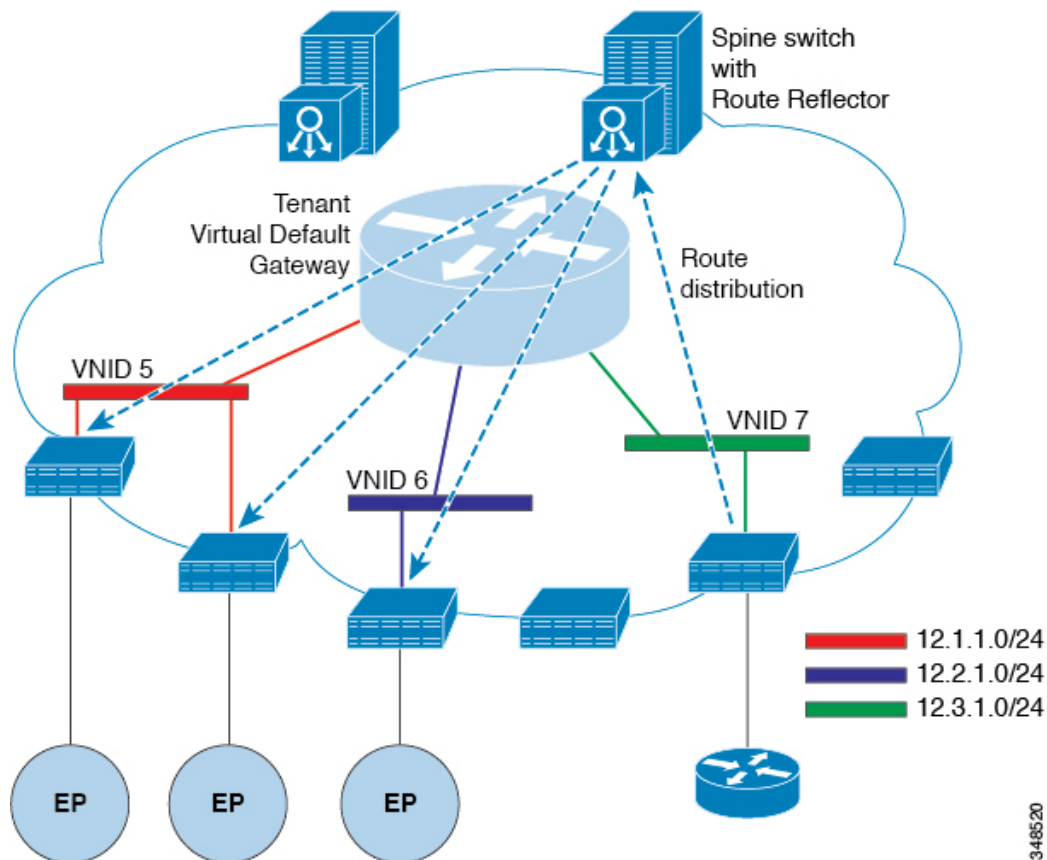


- (注) EPG ポートと VLAN の設定は、EPG が関連付けられているドメインインフラストラクチャ設定で指定されている設定に一致する必要があります。一致しない場合、APIC でエラーが発生します。そのようなエラーが発生した場合は、ドメインインフラストラクチャ設定が EPG ポートと VLAN の設定に一致していることを確認してください。

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 1: 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: どの外部サブネットが、特定の外部 L3Out EPG (l3extInstP) の一部として適用されるコントラクトを保持するか指定します。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、レイヤ 3 外部の外部ネットワーク (L3extOut) の ACI スイッチでトラフィックが開始する場合、 l3extInstP に関連付けられている送信元 IP アドレスを判断するための検索が行われます。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せん。

- 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。

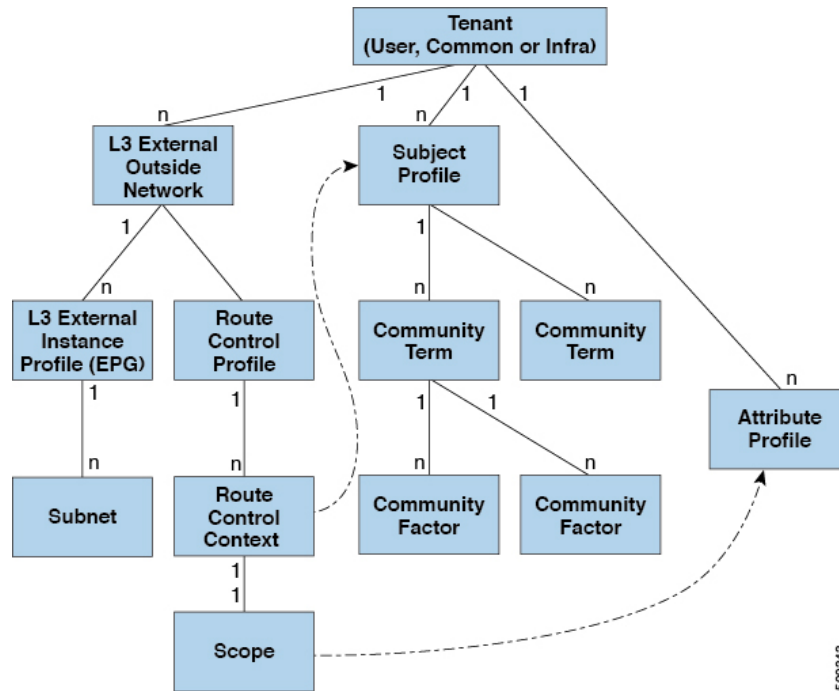
ルート集約では、多数の具体的なアドレスを 1 つのアドレスに置き換えることで、ルートテーブルが簡素化します。たとえば、10.1.1.0/24、10.1.2.0/24、10.1.3.0/24 は 10.1.0.0/16 に置き換えられます。ルート集約ポリシーにより、ボーダー リーフ スイッチとそのネイバー リーフ スイッチの間でルートを効率的に共有することができます。BGP、OSPF、あるいは EIGRP のルート集約ポリシーは、ブリッジドメインまたは中継サブネットに適用されます。OSPF では、エリア間ルート集約と外部ルート集約がサポートされます。集約ルートはエクスポートされません。ファブリッ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、プレフィックススペ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 2: 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 (rtctrlProfile) 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 rtctrlProfile が含まれているケースを示しています。rtctrlProfile 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 rtctrlProfile 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、rtctrlProfile 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 `rtctrtrlProfile` 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。

`rtctrtrlProfile` 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る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 `rtctrtrlProfile` 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 `rtctrtrlProfile` 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 `rtctrtrlProfile` ポリシーを設定できます。

`rtctrtrlProfile` 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 `rtctrtrlProfile` 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 `rtctrtrlProfile` を定義します。

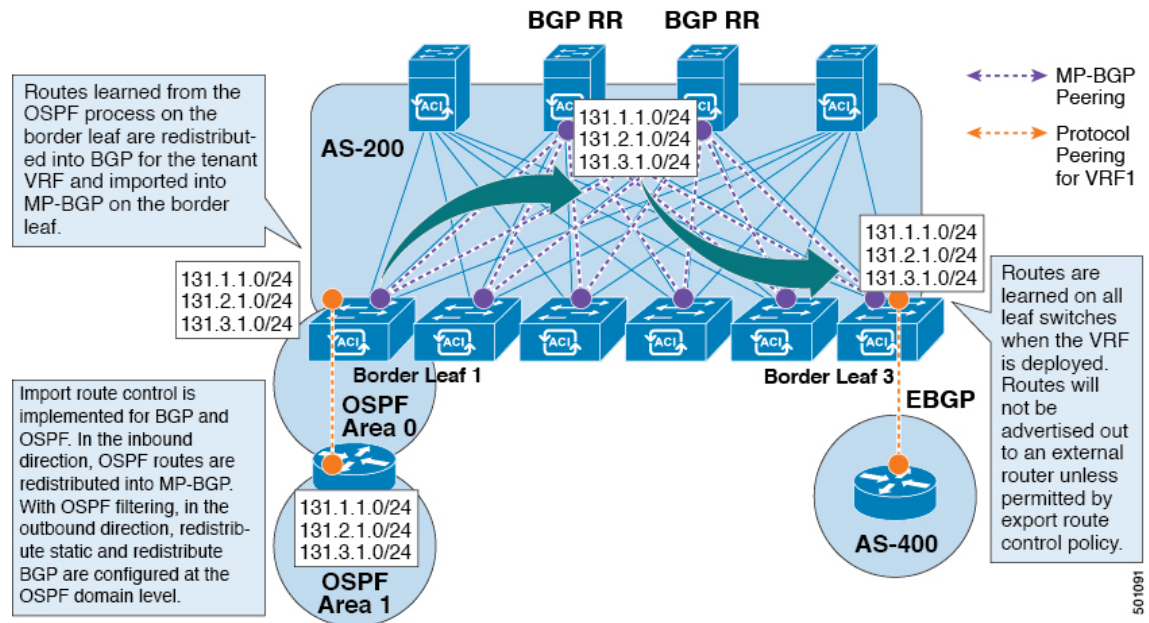


- (注) 1 つのスイッチ上で複数の `l3extOut` 接続を設定することは可能ですが、スイッチは 1 つのルートマップしか持つことができないため、スイッチで設定されているすべてのレイヤ 3 外側ネットワークが同じ `rtctrtrlProfile` を使用する必要があります。

プロトコル相互リン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。相互リンクポリシーは、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、相互リン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 `rtctrtrlProfile` は、相互リン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 3: 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。

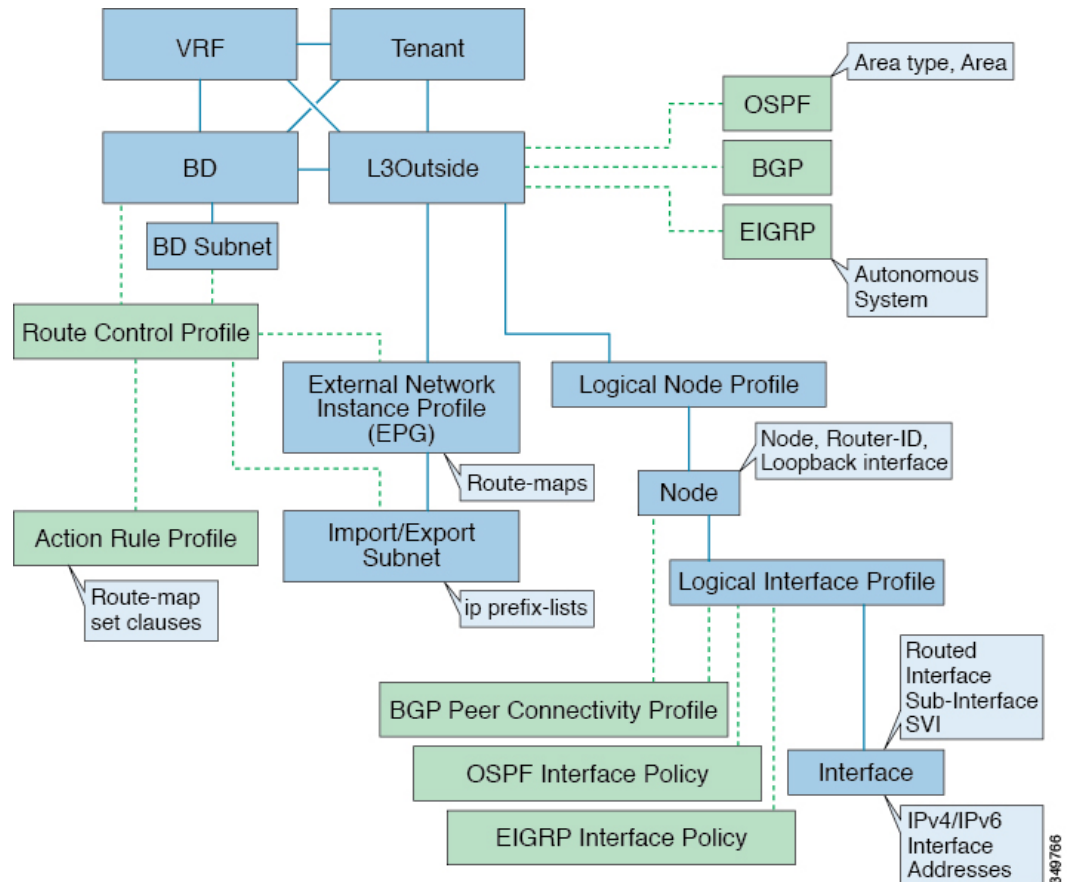
- スタティック ルーティング (IPv4 および IPv6 でサポート)
- 標準および NSSA エリアの OSPFv2 (IPv4)
- 標準および NSSA エリアの OSPFv3 (IPv6)
- iBGP (IPv4 および IPv6)
- eBGP (IPv4 および IPv6)
- BGP (IPv4 および IPv6)

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 4: 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 自律システム、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の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。
- 外部レイヤ 3 Outside 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 の下に複数の外部 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せん。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。
- 場合によっては、Cisco APIC クラスタへの着信設定で不整合が検証されます。外部から確認できる設定（L3Out を通過するノースパウンドトラフィック）も検証の対象です。設定が無効な場合は、「Invalid Configuration」エラー メッセージが表示されます。
- 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 1: ルート制御オプション

ルート制御設定	用途	オプション (Options)
エクスポート ルート制御	ルートマップと IP プレフィッ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、 [L3Out の作成 (Create L3Out)] 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せん。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。

ルート制御設定	用途	オプション (Options)
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。
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プレフィックスリストエントリ (permit 0.0.0.0/0 le 32) 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。

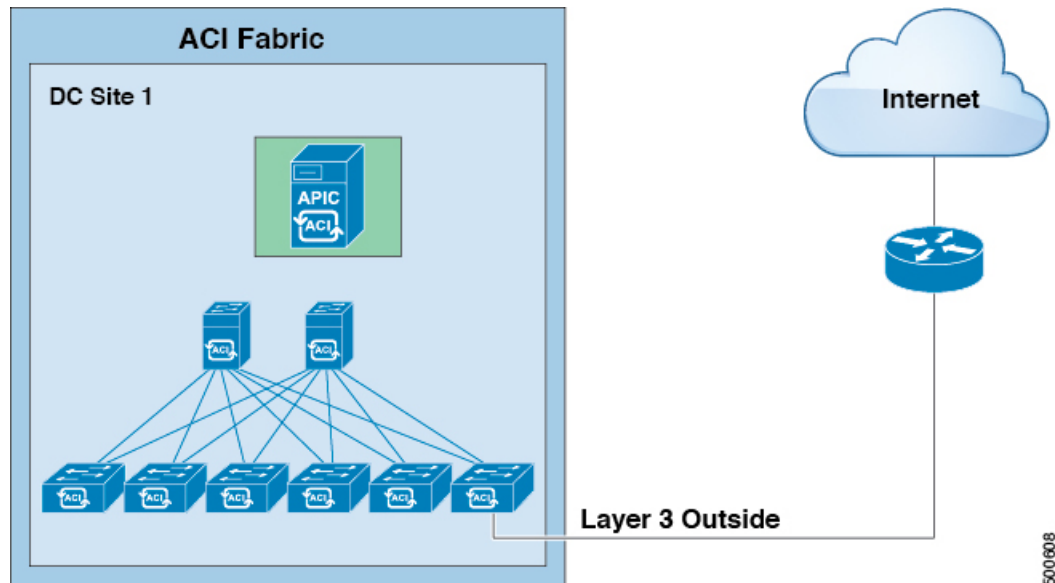


- (注) 第2世代のスイッチの VRF 機能間で正常にルートが共有されます (N9K-93108TC-EX など、スイッチモデル名の最後やその後に「EX」や「FX」がつく Cisco Nexus N9K)。第1世代のスイッチですが、ルートを保存する物理的な3進コンテンツ対応メモリ (TCAM) にルートの解析を完全にサポートするだけの容量がないため、この設定のパケットは失敗する可能性があります。

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 5: 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 L3Out 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。

注：この機能には APIC リリース 1.2 (1x) 以降が必要です。

翻訳について

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