ネットワーキングと管理接続

この章の内容は、次のとおりです。

テナント内のルーティング

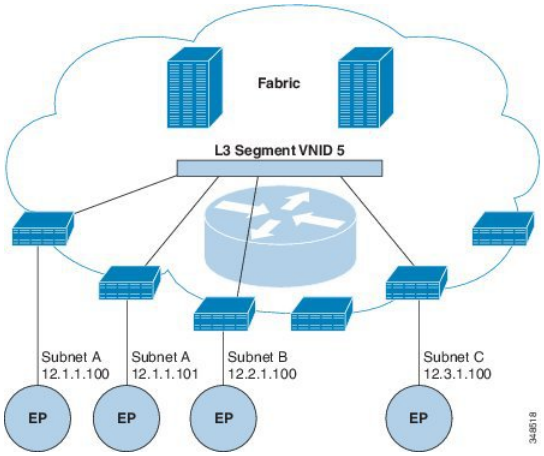
アプリケーション セントリック インフラストラクチャ（ACI）のファブリックでは、テナントのデフォルト ゲートウェイ機能が提供され、ファブリックの Virtual Extensible Local Area（VXLAN）ネットワーク間のルーティングが行えます。 各テナントでは、ファブリックにより仮想デフォルト ゲートウェイが提供され、エンドポイントに接続された最初のリーフ スイッチの入力インターフェイスでテナントが接続するすべてのリーフ スイッチを拡張できます。 各入力インターフェイスはデフォルトのゲートウェイ インターフェイスをサポートし、ファブリック全体のすべての入力インターフェイスは任意のテナント サブネットに対する同一のルータの IP アドレスと MAC アドレスを共有します。

Intersubnet のテナント トラフィックを転送するために使用されるレイヤ 3 VNID

ACI モデルでは、ACI ファブリックのデフォルト ゲートウェイに送信されるファブリックのイングレスに到達するトラフィックは、レイヤ 3 VNID として知られる仮想ネットワーク セグメント

にルーティングされます。 単一のレイヤ 3 VNID が、各テナント コンテキストに割り当てられます。 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 *1*：*Intersubnet* のテナント トラフィックを転送するレイヤ *3 VNID*



レイヤ 3 VNID は、APIC によって割り当てられます。 ファブリックを経由するトラフィックは、レイヤ 3 セグメントの VNID を使用して転送されます。 出力リーフ スイッチでは、パケットはレイヤ 3 セグメントの VNID から出力サブネットの VNID にルーティングされます。

ACI モデルでは、テナント内でルーティングされるトラフィックのファブリックでより効率的な転送が提供されます。 このモデルでは、2 台の仮想マシン（VM）間のトラフィックは同じ物理ホスト上の同じテナントに属しますが、異なるサブネット上にあります。 トラフィックは、（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前に、入力スイッチのみに伝送されます。 現在の VM 環境では、トラフィックは正しい宛先にルーティングされる前に、（異なる物理サーバ上にあると思われる）エッジ VM に伝送されます。

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。

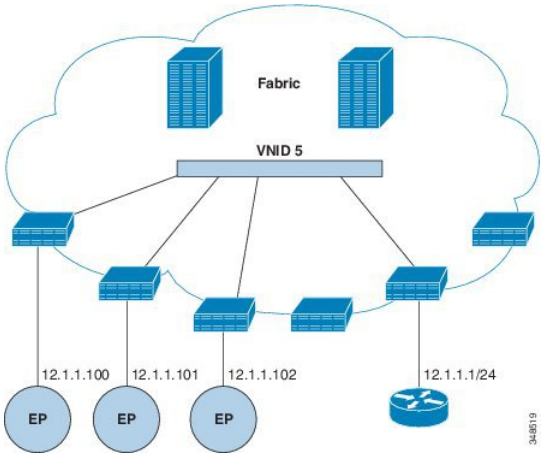
WAN およびその他の外部ネットワーク

WAN およびエンタープライズ コアに接続する外部ルータは、リーフ スイッチの前面パネルのインターフェイスに接続します。 外部ルータに接続するリーフ スイッチ インターフェイスは、ブリッジ インターフェイスまたはルーティング ピアとして設定できます。

外部ルータへのブリッジド インターフェイス

次の図に示すように、リーフスイッチのインターフェイスがブリッジドインターフェイスとして設定されている場合、テナント VNID のデフォルト ゲートウェイが外部ルータとなります。

図 *2*：ブリッジド外部ルータ

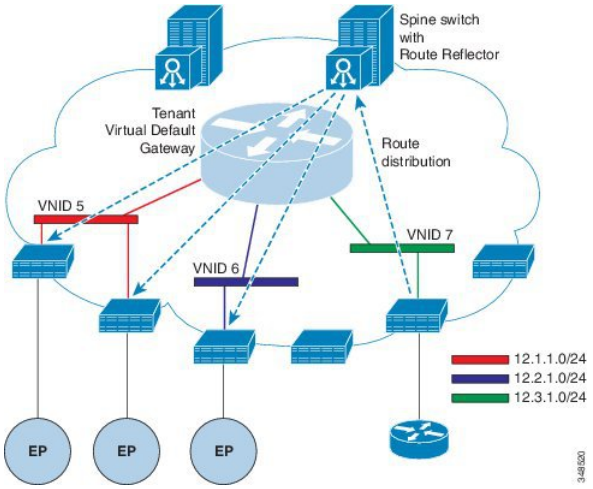


ACI ファブリックは、外部ルータの存在を認識せず、APIC はリーフ スイッチのインターフェイスを EPG に静的に割り当てます。

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 *3*: ルータのピアリング



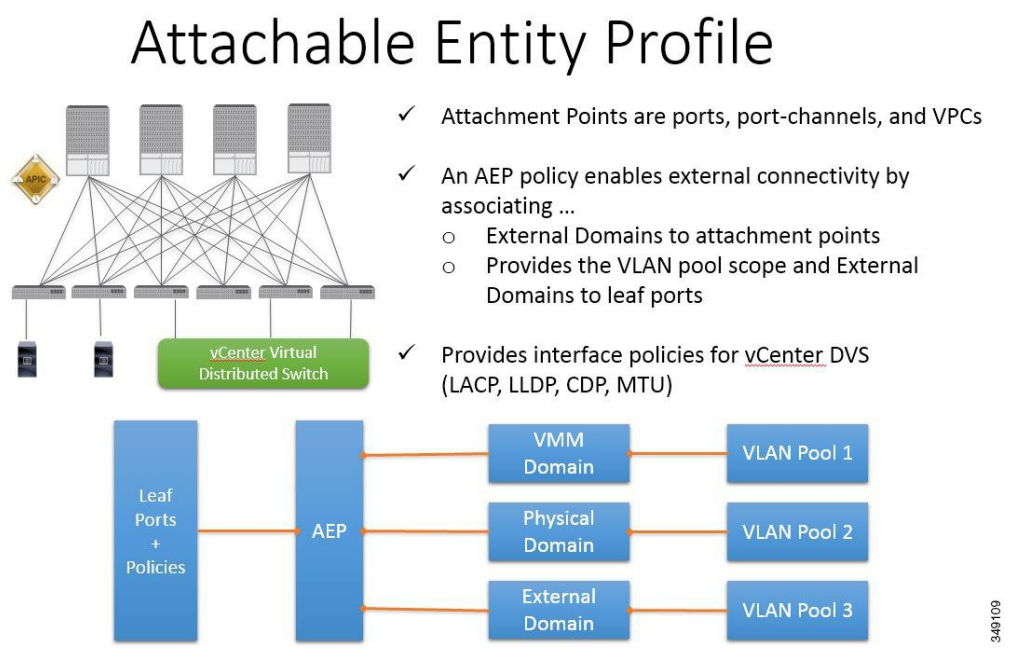
ピアリングによって学習されるルートは、スパイン スイッチに送信されます。 スパイン スイッチはルート リフレクタとして動作し、外部ルートを同じテナントに属するインターフェイスを持つすべてのリーフ スイッチに配布します。 これらのルートは、最長プレフィクス照合（LPM）により集約されたアドレスで、外部ルータが接続されているリモートのリーフ スイッチの VTEP IP アドレスが含まれるリーフ スイッチの転送テーブルに配置されます。 WAN ルートには転送プロキシはありません。 WAN ルートがリーフ スイッチの転送テーブルに適合しない場合、トラフィックはドロップされます。 外部ルータがデフォルト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

接続エンティティ プロファイル

ACI ファブリックにより、リーフ ポートを通して baremetal サーバ、ハイパーバイザ、レイヤ 2 スイッチ（たとえば、Cisco UCS ファブリック インターコネクト）、またはレイヤ 3 ルータ（たとえば、Cisco Nexus 7000 シリーズ スイッチ）などのさまざまな外部エンティティに接続する複数の接続ポイントが提供されます。 これらの接続ポイントは、下の図に示すように、リーフ スイッ

チ上の物理ポート、ポート チャネル、または仮想ポート チャネル（vPC）にすることができます。

図 *4*：接続可能エンティティ プロファイル



接続可能エンティティ プロファイル（AEP）は、同様のインフラストラクチャ ポリシー要件を持つ外部エンティティのグループを表します。 インフラストラクチャ ポリシーは、物理インターフェイス ポリシーで構成され、たとえば Cisco Discovery Protocol（CDP）、Link Layer Discovery Protocol（LLDP）、最大伝送単位（MTU）、Link Aggregation Control Protocol（LACP）などがあります。

AEP は、リーフ スイッチで VLAN プールを展開するのに必要です。 カプセル化プール（および関連 VLAN）は、リーフ スイッチで再利用可能です。 AEP は、VLAN プールの範囲を物理インフラストラクチャに暗黙的に提供します。

（注） 次の AEP の要件と依存関係は、さまざまな設定シナリオでも考慮する必要があります。

- AEP がリーフ スイッチで VLAN プール（および関連 VLAN）をプロビジョニングしている間、エンドポイント グループ（EPG）は、ポートで VLAN をイネーブルにします。EPG がポートに展開されていない限り、トラフィックは流れません。
- AEP VLAN プールを展開しないと、EPG がプロビジョニングされても VLAN はリーフ ポートでイネーブルになりません。
- リーフ ポートで静的にバインディングしている EPG イベントに基づいて、または VMware vCenter などの外部コントローラからの VM イベントに基づいて、特定の VLAN がリーフ ポート上でプロビジョニングされるかイネーブルになります。
- リーフ スイッチは、重複した VLAN プールをサポートしていません。 異なる重複した VLAN プールを同一の AEP に関連付けることはできません。

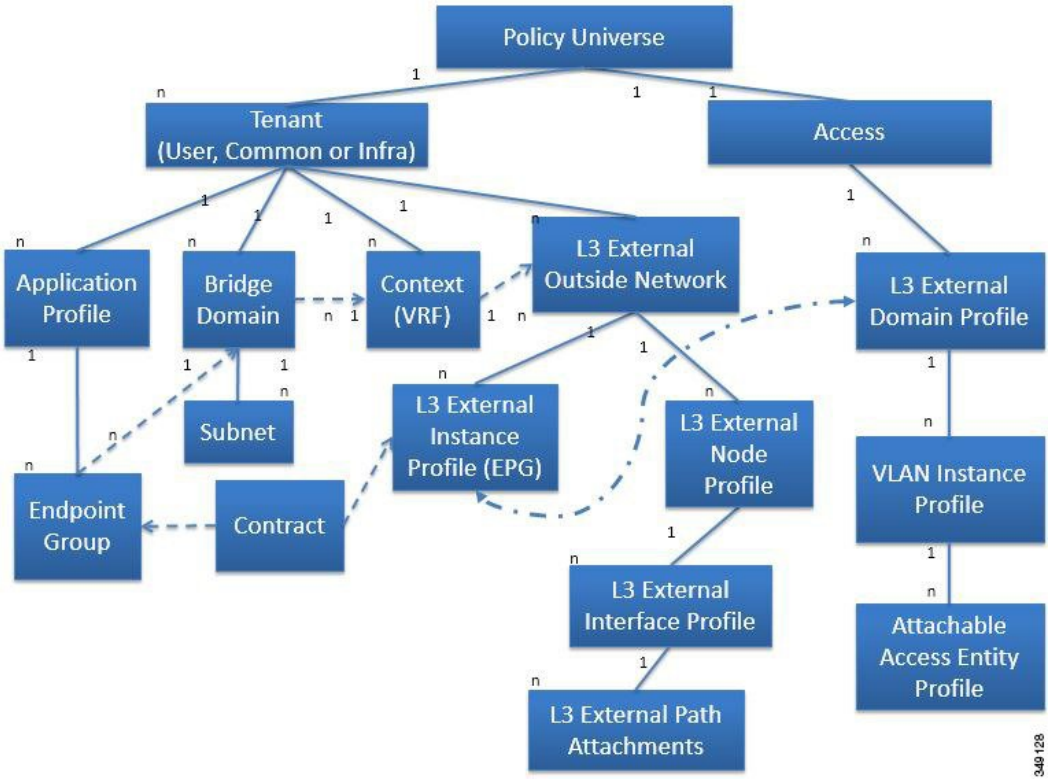
外部ネットワークへのブリッジドおよびルーテッド接続

外部ネットワークの管理対象オブジェクトにより、外部ネットワークへのレイヤ 2 およびレイヤ 3 のテナント接続が可能になります。 GUI、CLI、または REST API は、外部ネットワークへのテナント接続を設定するために使用できます。 付録 D「テナントのレイヤ 3 外部ネットワーク ポリシーの例」には、サンプルの XML ポリシーが含まれます。 ファブリック内のそのような外部ネットワーク アクセス ポイントすべてを簡単に検索するために、レイヤ 2 およびレイヤ 3 の外部リーフ ノードを「ボーダー リーフ ノード」としてタグ付けできます。

外部ネットワークへのテナント ルーテッド接続は、次の図に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）に関連付けることによってイネーブルになります。

図 *5*：外部ネットワークへのテナント ルーテッド接続



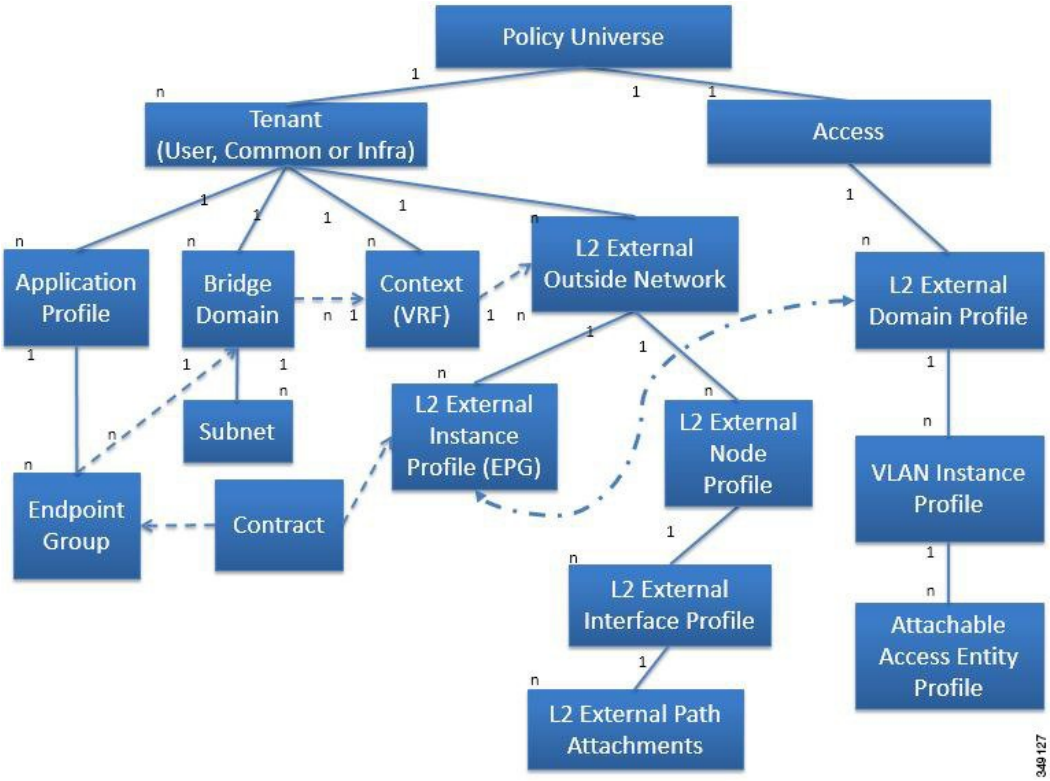
l3extOut には、ルーティング プロトコル オプション（BGP、OSPF または両方）とスイッチ固有の設定およびインターフェイス固有の設定が含まれます。

（注） レイヤ 3 外部外側ネットワークにルーティング プロトコル（たとえば、関連するコンテキストとエリア 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 インターフェイス設定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 はレイヤ 3 外部外側ネットワークに含まれるネットワーク構成に応じてコントラクトを介して l3extInstP EPG と通信できます。 リーフ スイッチ（ノード）1 個につき設定できる外部ネットワークは 1 つのみです。 ただし、外部ネットワーク設定は、複数のノードを 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。

同様のプロセスが外部ネットワークへのテナントブリッジド接続の設定に使用されます。テナント レイヤ 2 ブリッジド外部ネットワーク接続は、次の図に示すようにファブリック アクセス（infraInfra）外部ブリッジド ドメイン（L2extDomP）をレイヤ2外部外側ネットワーク（l2extOut）のレイヤ 2 外部インスタンス プロファイル（l2extInstP）に関連付けることによってイネーブルになります。

図 *6*：外部ネットワークへのテナント ブリッジド接続



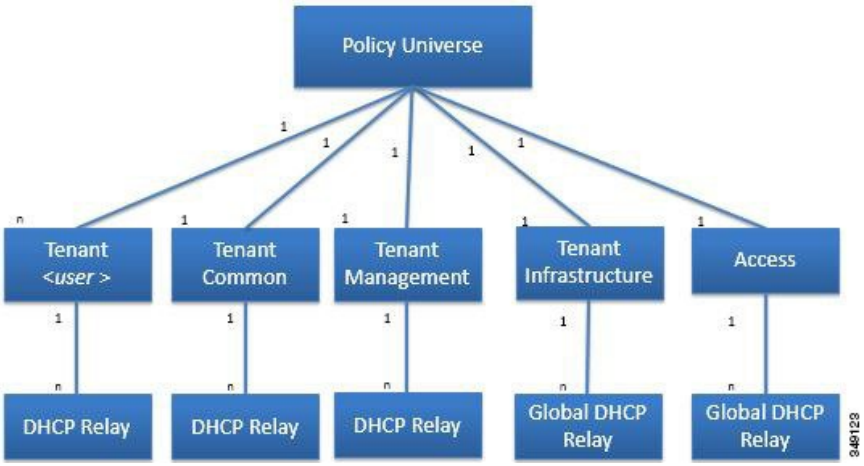
l2extOut には、スイッチ固有の設定およびインターフェイス固有の設定が含まれます。l2extInstP EPGは、コントラクトを通してテナントEPGに外部ネットワークを公開します。たとえば、ネットワーク接続ストレージ デバイスのグループを含むテナント EPG は、レイヤ 2 外部外側ネットワークに含まれるネットワーク構成に応じてコントラクトを介して l2extInstP EPG と通信できます。リーフ スイッチ 1 個につき設定できる外部ネットワークは 1 つのみです。ただし、外部ネットワーク設定は、複数のノードを L2 外部ノード プロファイルに関連付けることで複数のノードに容易に再利用できます。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。

DHCP リレー

ACI のファブリック全体のフラッディングはデフォルトでディセーブルになっている一方で、ブリッジ ドメイン内のフラッディングはデフォルトでイネーブルになっています。ブリッジ ドメ

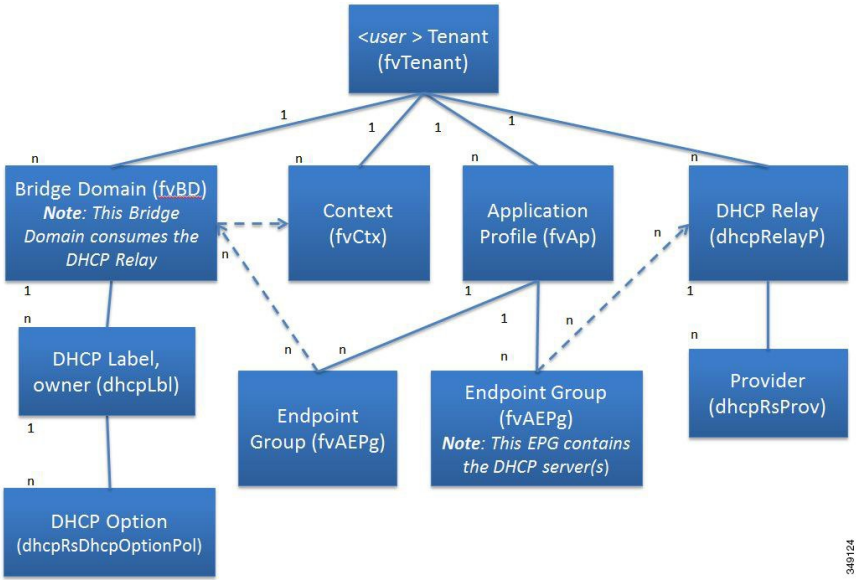
イン内のフラッディングがデフォルトでイネーブルになっているため、クライアントは同じ EPG 内の DHCP サーバに接続できます。 ただし、DHCP サーバがクライアントとは別の EPG またはコンテキストにある場合は、DHCP リレーが必要です。また、レイヤ2フラッディングがディセーブルの場合、DHCP リレーが必要です。 次の図は、DHCP リレー（ユーザ テナント、共通テナント、インフラストラクチャテナント、管理テナントおよびファブリック アクセス）を含むことができる管理情報ツリー（MIT）内の管理対象オブジェクトを示します。

図 *7*：*MIT* 内の *DHCP* リレーの場所



次の図は、ユーザ テナント内の DHCP リレー オブジェクトの論理関係を示します。

図 *8*：テナント *DHCP* リレー



DHCP リレー プロファイルには、1 つ以上のプロバイダーが含まれます。 EPG には 1 つ以上の DHCP サーバが含まれ、EPG と DHCP リレーの関係は DHCP サーバの IP アドレスを指定します。

コンシューマ ブリッジ ドメインには、プロバイダーの DHCP サーバをブリッジ ドメインと関連付ける DHCP ラベルが含まれます。 ラベルの一致により、ブリッジ ドメインは DHCP リレーを消費できます。

（注） ブリッジ ドメインの DHCP ラベルは、DHCP リレーの名前と一致する必要があります。

DHCP ラベル オブジェクトは、所有者も指定します。 所有者には、テナントまたはアクセス インフラストラクチャを指定できます。 所有者がテナントの場合、ACI ファブリックは最初にテナント内で一致する DHCP リレーを検索します。 ユーザ テナント内で一致するものが見つからなかった場合、ACI ファブリックは次に共通テナント内を検索します。

DHCP リレーは、次の 2 つのモードのいずれかで動作します。

- 可視：プロバイダーの IP およびサブネットは、コンシューマのコンテキストにリークされます。 DHCP リレーが表示されているときは、コンシューマのコンテキストに限定されます。
- 非可視：プロバイダーの IP およびサブネットは、コンシューマのコンテキストにリークされません。

（注） DHCP リレーが非可視モードで動作している場合、プロバイダーのブリッジ ドメインはコンシューマと同じリーフ スイッチ上にある必要があります。

テナントおよびアクセスの DHCP リレーが同じ方法で設定されている一方で、以下の使用例はそれに応じて異なります。

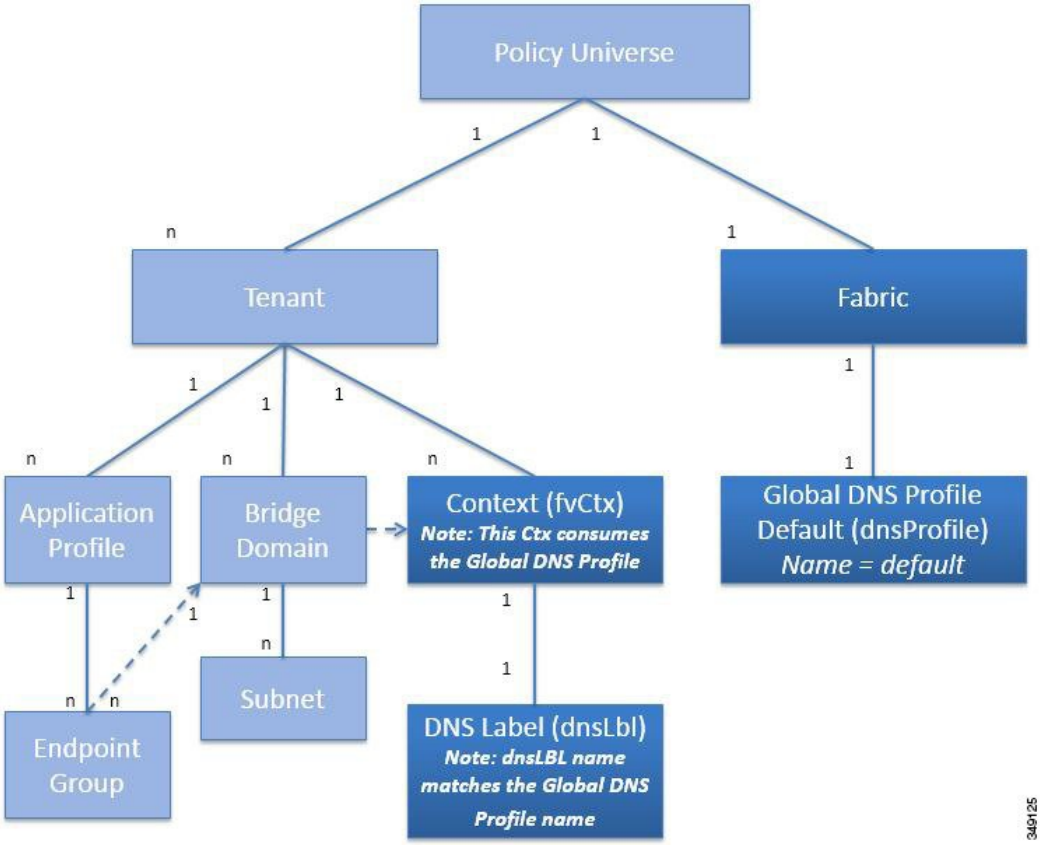
- 共通テナントの DHCP リレーは、どのテナントでも使用できます。
- インフラストラクチャ テナントの DHCP リレーは、ACI ファブリックのサービス プロバイダーによって他のテナントに選択的に公開されます。
- ファブリック アクセス（`infraInfra`）の DHCP リレーは、どのテナントでも使用でき、DHCP サーバのより細かい設定が可能になります。 この場合、同じブリッジ ドメイン内の別個の DHCP サーバをノード プロファイルの各リーフ スイッチ用にプロビジョニングすることができます。

DNS

ACI ファブリックの DNS サービスは、ファブリックの管理対象オブジェクトに含まれます。 ファブリックのグローバル デフォルト DNS プロファイルには、ファブリック全体でアクセスできます。 次の図は、ファブリック内の DNS 管理対象オブジェクトの論理関係を示します。 付録 F

「DNS for sample DNS XMP policies（サンプルの DNS XMP ポリシー用の DNS）」を参照してください。

図 *9*：*DNS*



コンテキストには、グローバル デフォルト DNS サービスを使用するために `dnsLBL` オブジェクトを含める必要があります。 ラベルの一致により、テナント コンテキストはグローバル DNS プロバイダーを消費することができます。 グローバル DNS プロファイルの名前が「default」なので、コンテキスト ラベル名は「default」になります（`dnsLBL name = default`）。

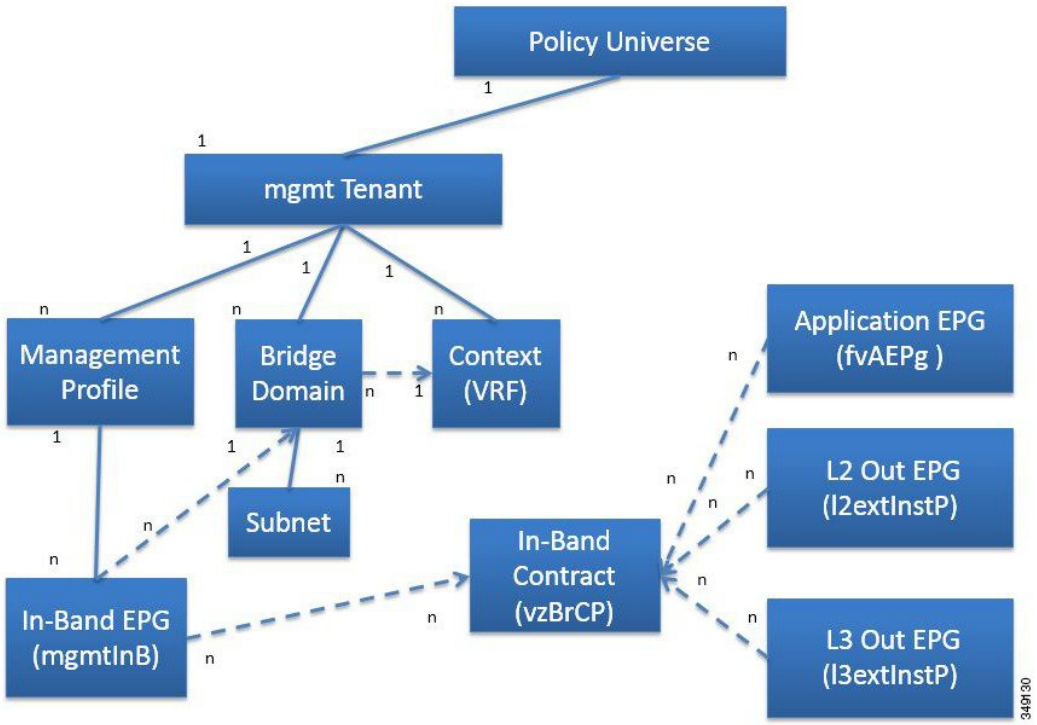
インバンドおよびアウトオブバンド管理アクセス

管理テナントでは、ファブリック管理機能へのアクセスを設定するための便利な方法が提供されます。 APIC を介してファブリック管理機能にアクセスできると同時に、インバンドおよびアウトオブバンドのネットワーク ポリシー経由で直接アクセスすることもできます。

インバンド管理アクセス

次の図は、管理テナントのインバンド ファブリック管理アクセス ポリシーの概要を示します。

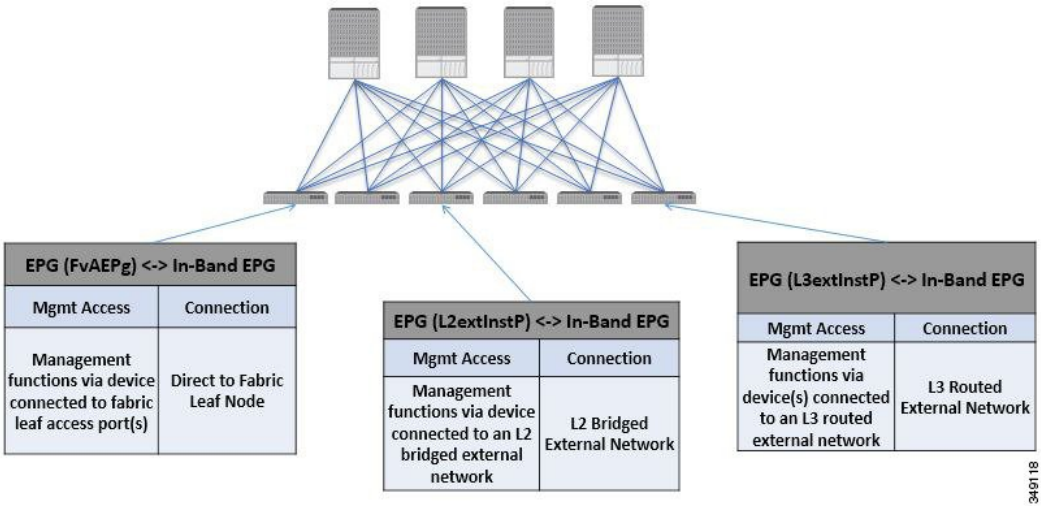
図 *10*：インバンド管理アクセス ポリシー



管理プロファイルには、インバンド コントラクト（`vzBrCP`）を介した管理機能へのアクセスを提供するインバンド EPG MO が含まれます。 `vzBrCP` は、`fvAEPg`、`l2extInstP`、および `l3extInstP` EPG がインバンド EPG を消費することを可能にします。 これにより、ローカルで接続されたデバイスや、レイヤ 2 ブリッジド外部ネットワークおよびレイヤ 3 ルーテッド外部ネットワーク経由で接続されたデバイスにファブリック管理が提供されます。 コンシューマおよびプロバイダー EPG が異なるテナントにある場合は、共通テナントからブリッジ ドメインおよびコンテキストを使用できます。 認証、アクセス、および監査のロギングはこれらの接続に適用され、インバンド EPG を通して管理機能にアクセスしようとするユーザには適切なアクセス権が必要です。

次の図は、インバンド管理のアクセス シナリオを示します。

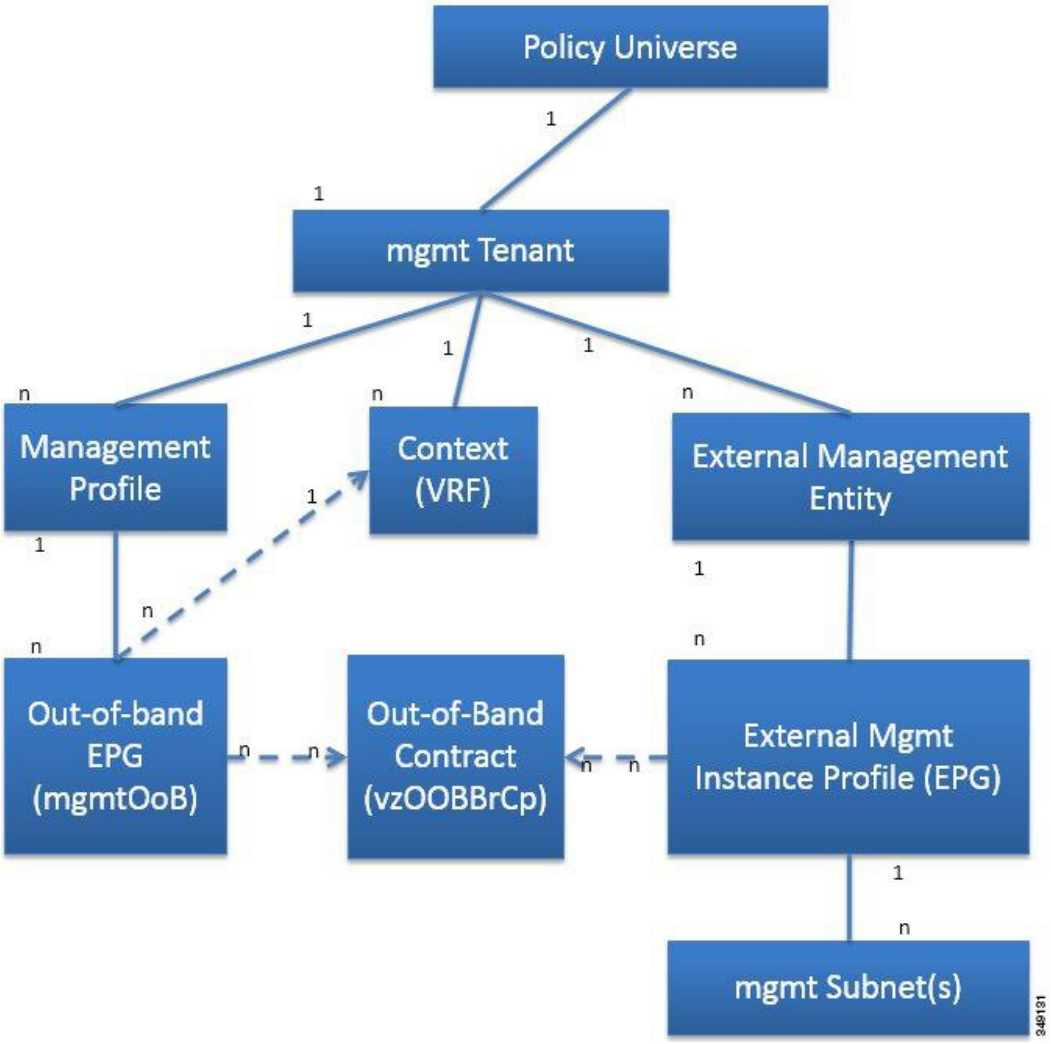
図 *11*：インバンド管理のアクセス シナリオ



アウトオブバンド管理アクセス

次の図は、管理テナントのアウトオブバンドファブリック管理アクセスポリシーの概要を示します。

図 *12*：アウトオブバンド管理アクセス ポリシー

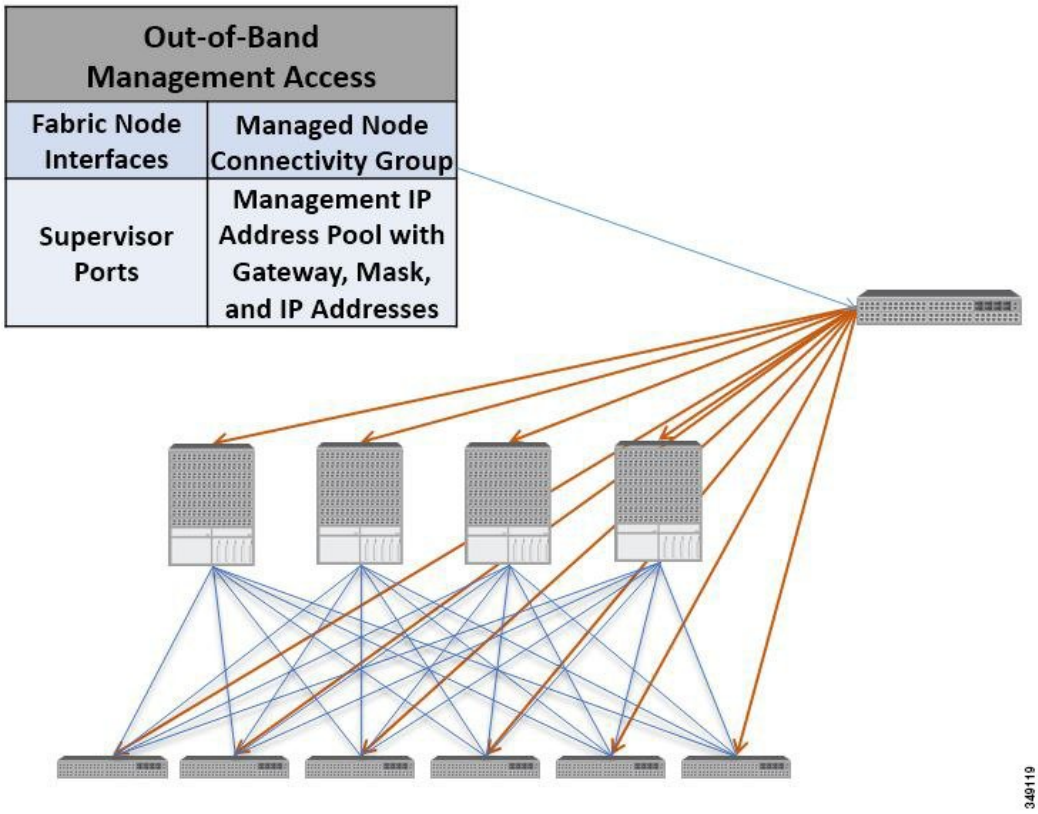


管理プロファイルには、アウトオブバンドコントラクト（`vzOOBBrCp`）を介した管理機能へのアクセスを提供するアウトオブバンド EPG MO が含まれます。 `vzOOBBrCp` により、外部管理インスタンスプロファイル（`mgmtExtInstP`）EPG はアウトオブバンド EPG を消費できます。 これにより、サービス プロバイダーのプリファレンスに応じて、ローカルまたはリモートで接続されたデバイスにファブリック ノードのスーパーバイザ ポートが公開されます。 スーパーバイザ ポートの帯域幅がインバンドポート未満である間は、インバンドポートを介したアクセスが利用できない場合、スーパーバイザ ポートがダイレクト アクセスを提供できます。 認証、アクセス、および監

査のロギングはこれらの接続に適用され、アウトオブバンドEPGを通して管理機能にアクセスしようとするユーザには適切なアクセス権が必要です。

次の図は、アウトオブバンド管理アクセスを専用スイッチを通じてどのように統合できるかについて示します。

図 *13*：アウトオブバンド アクセスのシナリオ



（注） サービス プロバイダーによってはローカル接続へのアウトオブバンド接続を制限するように選択します。また、外部ネットワークからルーテッドまたはブリッジド接続を有効にすることを選択するサービス プロバイダーも存在します。 また、サービス プロバイダーはローカル デバイスのみ、またはローカルおよびリモート デバイス両方に対するインバンドおよびアウトオブバンド管理アクセスの両方を含む一連のポリシーを設定することを選択することもできます。

共有サービス コントラクトの使用

共有サービス コントラクトの設定時は、次のガイドラインに従ってください。

- インバンドとアウトオブバンドのエンドポイントグループ（EPG）間のコントラクト：コントラクトがインバンドとアウトオブバンドのEPG間に設定されている場合、次の制限が適用されます。
  - 両方の EPG は同じコンテキスト（VRF）にする必要があります。
  - フィルタは、着信方向のみに適用されます。
  - レイヤ 2 フィルタはサポートされません。
  - QoS は、インバンド レイヤ 4 ～ レイヤ 7 のサービスには適用されません。
  - 管理統計情報は利用できません。
  - CPU 宛てトラフィックの共有サービスはサポートされません。
- プライベート ネットワークを適用しない場合、コントラクトがブリッジ間ドメインのトラフィックに必要です。
- プレフィクスベースの EPG はサポートされません。

  共有サービスはレイヤ 3 外部外側ネットワークではサポートされません。 外部のレイヤ 3 外部外側ネットワークによって提供または消費されるコントラクトは、同じレイヤ 3 コンテキストを共有する EPG により消費または提供される必要があります。
- 共有サービスは、重複しないサブネットのみでサポートされます。 次の注意事項に従ってください。
  - 共有サービス プロバイダーのサブネットは、ブリッジ ドメイン下ではなく EPG 下で設定します。
  - 同じコンテキストを共有する EPG で設定されたサブネットは、統合および重複してはなりません。
  - あるコンテキストから他のコンテキストへ漏れたサブネットは統合および重複してはなりません。
  - 複数のコンシューマ ネットワークからあるコンテキストへ漏れたサブネットまたはその逆で漏れたサブネットは統合および重複してはなりません。

  2 人のコンシューマが誤って同じサブネットに設定されている場合は、両方のサブネットの設定を削除してこの状態からリカバリし、その後サブネットを正しく再設定します。
- プロバイダー コンテキストで共有サービスを AnyToProv で設定しないでください。 APIC は内部的に拒否し障害を発生させます。
- 共有サービスを提供している間は、プロバイダーのプライベート ネットワークは非強制モードにできません。