テナント

ACI テナント モデル

いくつかの使用例で ACME 社はテナントを使用しています。ACME 社は、現在の展開におけるアプリケーション ライフサイクルのテナント コンストラクトを使用して、開発者がアプリケーションの作成に使用するリソースの個々のテナントを保守します。テナントは自動テストに使用され、最終的には実稼働テナントになります。また、概要で説明したように、ACME は、今後の同様のイニシアティブで活用できるインフラストラクチャを構築することも目指しています。テナントは各種業務の仮想境界を設けるために使用されます。情報セキュリティ チームはこれを社内 LDAP システムに統合し、他のグループに影響を及ぼすような変更を防ぐことができます。

Cisco Application Centric Infrastructure (ACI) は「マルチテナント」として新規に設計されています。つまり、使用者の観点から見ると、使用者に応じて内容が異なる（「クラウド」に類似）ということです。従来のサービス プロバイダーの場合、テナントとはひとつのカスタマーであり、一般的なエンドカスタマー環境では、運用グループ、営業部門、アプリケーション オーナーなどがテナントになります。

テナント モデルの使用方法は、いくつかの要因によって決まります。

1. アプリケーション、ネットワーク、サーバ、セキュリティなど、組織における全体的な IT 運用とサポート モデル。
2. ソフトウェアの開発ライフサイクルから見た、環境の分離（開発、品質保証、実稼働）。
3. ドメイン所有者別（Web、アプリケーション、データベースの所有者など）の業務の分離。
4. フォールトの影響を限定するためのフォールトドメインのサイズとスコープ（さまざまな事業部門など）。

従来のネットワーク環境では、ルータまたはレイヤ 3 スイッチでルーティング プロトコルを変更すると、多数の固有の VLAN やサブネットに影響が及びます。それによって、変更管理とアプリケーションの影響に関する保証レベルの注意が喚起されます。ACI ポリシー モデルを活用すると、論理構造から物理ハードウェアが抽出されます。テナント オブジェクトによって、

使用している論理および具象オブジェクトに焦点を当て、基本およびオーバーレイ ネットワークの構造的依存関係について統一見解を持つことができます。

ACIオブジェクトモデル内のテナントは、最上位のオブジェクトを表します。内部では、プライベート ネットワーク（VRF）、ブリッジ ドメイン、サブネットなどのテナント ネットワークを定義するオブジェクトと、アプリケーション プロファイルやエンドポイント グループなどのテナント ポリシーを定義するオブジェクトを区別できます。

ACIでは、テナントポリシーによってアプリケーションを定義します。アプリケーションは、物理サーバ、またはサーバを呼び出す仮想マシンの組み合わせから構成されます。たとえば、Web サイトでは、Web サーバ、アプリケーション サーバ、データベース サーバから構成される 3 層のアプリケーションのモデルを使用できます。ユーザが Web サイトを参照する際は、実際にはロード バランサの仮想 IP アドレスと通信しており、ロード バランサは Web 要求を多数の Web サーバに分配します。次に、それらの Web サーバがコア アプリケーションと通信します。コア アプリケーションは、ロード バランシングやハイ アベイラビリティのために、複数のアプリケーション サーバ間に分割できます。最後に、アプリケーション サーバがサーバのクラスタであるデータベースと通信します。

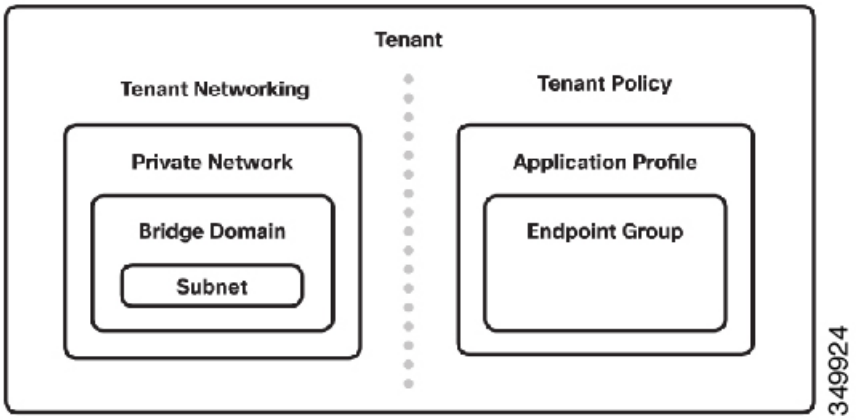
ACIでは、各サーバはエンドポイントと呼ばれます。エンドポイントはACIで分類され、ポリシーが適用されます。同じタイプのポリシー（通信する相手、必要な通信や制限のタイプなど）を共有するエンドポイントを含むエンドポイントグループを作成します。つまり、アプリケーションは複数のエンドポイント グループから構成することができ、アプリケーション プロファイルでグループ化されます。

テナント ネットワーキングは、ネットワーク ポリシーの定義に使用され、透過的な方法で基盤ハードウェアに適用されます。これは、プライベート ネットワーク、ブリッジ ドメイン、サブネットを使用してACIが提供する、抽象レイヤによるものです。この章の次の項では、これらの概念について詳しく説明します。下記の図は、テナントを形成しているさまざまなオブジェクトとそれらの関係を示しています。

テナント ネットワーキングとテナント ポリシーは個々に定義されますが、アプリケーションで使用されるネットワーク ポリシーは、エンドポイント グループとブリッジ ドメイン間の関係によって定義されます。

次の図は、テナント内で設定できるすべてのコンポーネントを示しています。以降の項の各図は、ACME 社が各コンポーネントを追加していく様子を示しています。

図 *1:* テナントの論理モデル



デフォルトでは、システムで事前設定された次の 3 種類のテナントがあります。

1. Common（共通）：ACI ファブリックの他のテナントに「共通」のサービスを提供するための特別なテナント。共通テナントの基本原則はグローバルな再利用です。共通サービスの例：
    1. 共有 L3Out
    2. 共有プライベート ネットワーク
    3. 共有ブリッジ ドメイン
    4. DNS
    5. DHCP
    6. アクティブ ディレクトリ
2. Infra（インフラストラクチャ）：トンネルやポリシー展開など、ファブリック内部の通信に使用されるインフラストラクチャテナント。これには、スイッチ（リーフ、スパイン、アプリケーション仮想スイッチ（AVS））間およびスイッチと Application Policy Infrastructure Controller (APIC) 間の通信が含まれます。インフラストラクチャ テナントは、ユーザ領域（テナント）には公開されず、独自のプライベート ネットワーク領域とブリッジ ドメインを備えています。ファブリックの検出、イメージ管理、ファブリック機能用の DHCP は、すべてこのテナント内で処理されます。
3. Mgmt（管理）：管理テナントには、ファブリック ノードのアクセス ポリシーの設定に役立つ便利な機能があります。ファブリック ノードは APIC を介してアクセスおよび設定できますが、インバンドとアウトバンド接続を使用して直接アクセスできます。インバンドおよびアウトオブバンド ポリシーは管理テナントで設定されます。
    - インバンド管理アクセス
    - アウトオブバンド管理アクセス

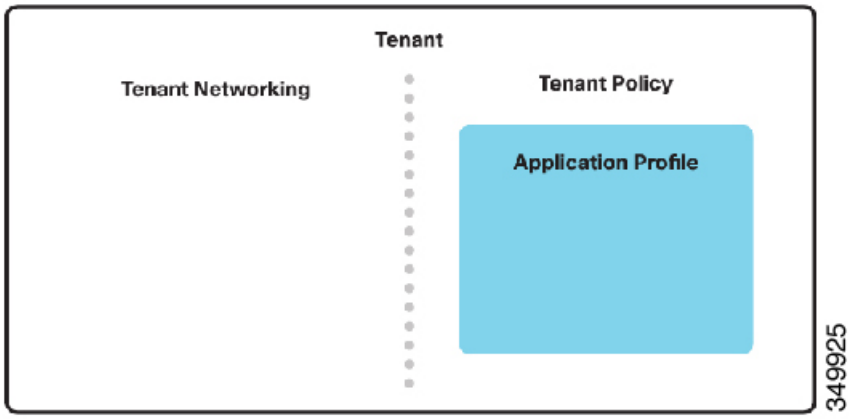
アプリケーション プロファイル

アプリケーションプロファイルは、複数のホスト（物理または仮想）用の便利な論理コンテナです。さまざまな基準に基づいてアプリケーション プロファイル コンテナを作成できます。たとえば、アプリケーションが提供する機能、エンドユーザから見たアプリケーションの様子、アプリケーションを配置するデータセンターのコンテキスト内の場所、実装に関連する他の論理グループ化など。アプリケーション プロファイル サーバは、共通ポリシーの使用に応じてエンドポイント グループにグループ化されます。

アプリケーション プロファイルのメカニズムによって、サーバ グループを 1 つのアプリケーションとして把握することができます。このアプローチにより Cisco Application Centric Infrastructure (ACI) はアプリケーション認識型となり、アプリケーションの一部であるすべてのサーバを全体としてモニタしながらアプリケーションの動作状態をチェックできるようになります。さらに、その特定のアプリケーションに関連するエラーおよびヘルス ステータスが管理者に通知されるようにすることができます。作成する各アプリケーション プロファイルには、一意のモニタリング ポリシーと、適用する QoS ポリシーを含めることができます。

アプリケーションプロファイルはテナントの子オブジェクトであり、1つのテナントに複数のアプリケーション プロファイルを含めることができます。

図 *2:* テナントへのコンポーネントの追加 - *1.* アプリケーション プロファイル



アプリケーション プロファイルの設定

Name：アプリケーション プロファイルの名前。

Tags：タグまたはメタデータは、ファブリック モジュールに割り当てられる非階層型のキーワードまたは条件です。

Monitoring Policy：（任意）EPG セマンティック スコープのモニタリング ポリシー名。

GUI を使用した新しいアプリケーション プロファイルの作成

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、***[Tenant_Name]*** を選択します。
3. ナビゲーション ウィンドウで、***[Tenant_Name]*** > **[Application Profiles]** の順に選択します。
4. [Work] ペインで、[Actions] > [Create Application Profile] の順に選択します。
5. [Create Application Profile] ダイアログボックスで、次の操作を実行します。
   1. アプリケーション プロファイルの名前を入力します。
   2. （任意）説明を入力します。
   3. （任意）TAG を入力します。
   4. （任意）[Monitoring Policy] を選択します。
6. [送信（Submit）] をクリックします。

GUI を使用したアプリケーション プロファイル変更

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、***[Tenant_Name]*** を選択します。
3. ナビゲーション ウィンドウで、***[Tenant_Name]*** > **[Application Profiles]** > ***[Application_Profile]*** の順に選択します。
4. [Work] ペインで、[policy] を選択します。
5. [Work] ペインで、次の操作を実行します。
   1. （任意）説明を入力します。
   2. （任意）適切な [TAG] を入力します。
   3. （任意）ラベルを入力します。
   4. （任意）[QoS Class] を選択します。
   5. （任意）[Monitoring Policy] を選択します。
6. [送信（Submit）] をクリックします。

GUI を使用したアプリケーション プロファイルの削除

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、***[Tenant_Name]*** を選択します。

3. ナビゲーション ウィンドウで、***[Tenant_Name]*** > **[Application Profiles]** > ***[Application_Profile]*** の順に選択します。
4. [Work] ペインで、[Policy] を選択します。
5. [Work] ペインで、[Actions] > [Delete] の順に選択します。

アプリケーション プロファイルの確認

```
REST :: /api/node/class/fvAp.xml
```

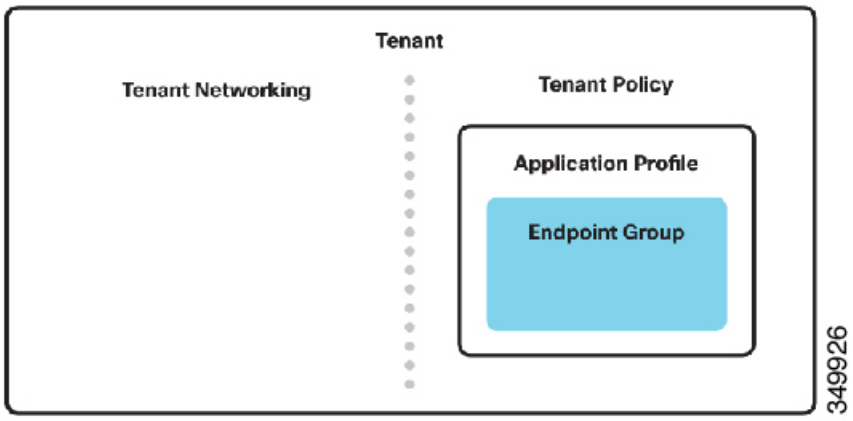
```
CLI :: moquery -c fvAp
```

エンドポイント グループ

エンドポイント グループ（EPG）は、ファブリック内で類似の機能を実行し、類似のポリシーを共有するサーバまたはホストを論理グループ化するために使用されます。作成する各エンドポイント グループには、固有のモニタリング ポリシーまたは QoS ポリシーを含めることができ、1 つのブリッジ ドメインに関連付けられます。

エンドポイント グループはアプリケーション プロファイルの子オブジェクトであり、1 つのアプリケーション プロファイルに複数のエンドポイント グループを含めることができます。エンドポイント グループ内の各エンドポイントはファブリック内で同じポリシーの影響を受けます。

図 *3:* テナントへのコンポーネントの追加 - *2.* アプリケーション プロファイルのエンドポイント グループ



EPG 内のすべてのエンドポイントは相互に通信できます。EPG コントラクト間の通信は、従来のレイヤ 2/レイヤ 3 フォワーディング コンストラクトではなく、コントラクトによって制御されます。たとえば、EPG-A の ホストA は IP アドレス/マスク 10.1.1.10/24 を持ち、EPG B のホストB は IP アドレス/マスク 10.1.1.20/24 を持つことができます（両方のホストが互いに「同じサブネット」に存在していると認識している場合）。この例では、EPG-A と EPG-B 間の接続を許可するコントラクトがない場合、これらのホストは通信できません。コントラクトについては次の項で詳しく説明します。

アプリケーション エンドポイント グループ、外部ブリッジ ネットワーク（別名、外部レイヤ 2）、外部ルーテッド ネットワーク（別名、外部レイヤ 3）、管理エンドポイント グループなど、ファブリック内の一部のエンドポイント グループはアプリケーション プロファイルに含まれていないので注意してください。これらのエンドポイント グループには特別な要件があります。たとえば、外部ブリッジ ネットワークの場合、エンドポイントの MAC アドレスはリーフ スイッチで学習されません。

エンドポイント グループはブリッジ ドメインにリンクされますが、ブリッジ ドメインのレガシー モードを使用しない限り、ブリッジ ドメインとは異なる VLAN ID を受け取ります。

1 つのサブネットを複数の EPG 間に拡張できることを理解する必要があります。各 EPG はカプセル化 VLAN または VXLAN によって識別されるので、同じサブネットがファブリック全体で異なるカプセル化 ID を使用できます。この概念は従来のネットワーキングとは異なります。

エンドポイント グループのサブタイプ

Application Policy Infrastructure Controller (APIC) ソフトウェア バージョン 1.1 では、従来のエンドポイント グループは次の 2 つのタイプに分けられます。

アプリケーション エンドポイント グループ

従来のエンドポイント グループです。静的パス バインディング、VMM 統合、またはレイヤ 2/レイヤ 3 ドメイン バインディングを使用して、仮想または物理エンドポイントに適用できます。

マイクロセグメント（**uSeg**）エンドポイント グループ

この分類のエンドポイント グループを使用すると、エンドポイントにさまざまな「属性」をマッチングして、uSeg エンドポイント グループに自動的に割り当てることができます。このタイプのエンドポイント グループは、属性ベースのエンドポイント グループとも呼ばれます。マッチングできる属性には、VM プロパティ（VM 名、VM ID、およびハイパーバイザなど）、MAC アドレス、IP 設定が含まれます。

uSeg エンドポイント グループは、作成されて VMM ドメインに割り当てられると、テナント内に存在する VMM ドメイン内の任意のエンドポイントに対して自動マッチングを行い、エンドポイントを、割り当てられていたアプリケーション エンドポイント グループから uSeg エンドポイント グループに移動します。これが実行されると、uSeg EPG（コントラクト、QoS、モニタリング ポリシーなど）に適用されるポリシーが適用されるようになります。元のアプリケーション EPG のポリシーは、エンドポイントに適用されなくなります。

（注） VM エンドポイントは、そのアプリケーションのエンドポイント グループに割り当てられていますが、属性の一致があると、ファブリックにより uSeg エンドポイント グループに自動的に移動されます。つまり、仮想マシン マネージャ（vCenter）では、エンドポイントは引き続きアプリケーションの EPG/ポート グループに割り当てられものとして表示されます。ただし、**[uSeg EPG]** > **[Operational]** > **[Client End Points]** で確認すると、新しい uSeg EPG の下に既知のエンドポイントが表示さます。

属性を uSeg エンドポイント グループに追加する場合、そのエンドポイント グループは現在どの VMM ドメインにも割り当てられていないことが必要です。これは、エンドポイント グループが現在、どの VM エンドポイントにも割り当てられていないことを確実にします。これにより、常にバインドされた VM ドメインに誤って属性を割り当てることによって機能エンドポイントをうっかり移動することを防ぐことができます。このため、uSeg エンドポイント グループの作成手順では、最初にエンドポイント グループを作成し、VMM ドメインはその後に追加する必要があります。これにより、VMM ドメインが追加される前に uSeg エンドポイント グループの属性が割り当てられるようになります。

新しいエンドポイント グループの作成

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、 ***[Tenant_Name]*** を選択します。
3. [Navigation] ペインで、 ***[Tenant_Name]*** **> [Application Profiles] >** ***[Application_Profile]*** **> [Application EPGs]** の順に選択します。
4. [Work] ペインで、[Actions] > [Create Application EPG] の順に選択します。
5. [Create Application EPG] ダイアログボックスで、次の操作を実行します。
   1. [Application EPG Name] を入力します。
   2. （任意）[Tag] を入力します。
   3. （任意）[Qos Class] を入力します。
   4. （任意）[Custom Qos] を入力します。
   5. ブリッジ ドメイン名を選択するか作成します。
   6. （任意）[Monitoring Policy] を選択します。
   7. （任意）VM ドメイン プロファイルへの関連付けを選択します。
   8. （任意）リーフ/パスと静的にリンクすることを選択します。
6. [Finish] をクリックします。

エンドポイント グループの変更

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、 ***[Tenant_Name]*** を選択します。
3. ナビゲーション ウィンドウで、 ***[Tenant_Name]*** **> [Application Profiles] >** ***[Application_Profile]*** **> [Application EPGs] >** ***[Application_EPG]*** を選択します。
4. [Work] ペインで、[policy] を選択します。
   1. [Application EPG Name] を入力します。

2. （任意）[Tag] を入力します。
3. （任意）[Qos Class] を入力します。
4. （任意）[Custom Qos] を入力します。
5. [Bridge Domain Name] を入力します。
6. （任意）必要に応じて適切な [Monitoring Policy] を選択します。
7. [Associated Domain Profile Name] を入力します。

5. [Finish] をクリックします。

エンドポイント グループの削除

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、***[Tenant_Name]*** を選択します。
3. [Navigation] ペインで、***[Tenant_Name]*** > **[Application Profiles]** > ***[Application_Profile]*** > **[Application EPGs]** > ***[Application_EPG]*** を選択します。
4. [Work] ペインで、[Actions] > [Delete] の順に選択します。

エンドポイント グループの確認

```
REST :: /api/node/class/fvAEPg.xml
CLI :: moquery -c fvAEPg
```

エンドポイント

エンドポイントとは、ネットワークに直接的または間接的に接続されたデバイスです。エンドポイントはアドレス（ID）、ロケーション、属性を備えており、仮想または物理のいずれでもかまいません。各エンドポイントには、パス、カプセル化、展開の即時モードが関連付けられています。

エンドポイントはエンドポイント グループの子オブジェクトであり、エンドポイント グループの構成には複数のエンドポイントを含めることができます。ファブリック内で参照されるエンドポイントは、スタティック（APIC 内で定義）またはダイナミック（vCenter/Openstack で自動化）のいずれでもかまいません。

エンドポイント グループ内でスタティック バインディングを作成することによって、スタティック エンドポイントを追加できます。スタティック バインディングの例を次に示します。ダイナミック バインディングの例については、VVM の項を参照してください。

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、***[Tenant_Name]*** を選択します。
3. [Navigation] ペインで、***[Tenant_Name]*** > **[Application Profiles]** > *[Application_Profile_Name]* > [Application EPGs] > *[EPG_Name]* > **[Static Bindings (Paths)]** の順に選択します。

4. [Work] ペインで、[Actions] > [Deploy Static EPG on PC, VPC or Interface] の順に選択します。
5. [Deploy Static EPG on PC, VPC or Interface] ダイアログボックスで、次の操作を実行します。
    1. [Path Type] を選択します。
    2. [Path] を選択します。
    3. カプセル化 VLAN を入力します。
    4. [Submit] をクリックします。`

特定の EPG のファブリックに接続されたエンドポイントを表示する手順：

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、***[Tenant_Name]*** を選択します。
3. [Navigation] ペインで、***[Tenant_Name]*** > **[Application Profiles]** > ***[Application_Profile]*** > **[Application EPGs]** > ***[Application_EPG]*** を選択します。
4. [Work] ペインで、[Operational] を選択します。

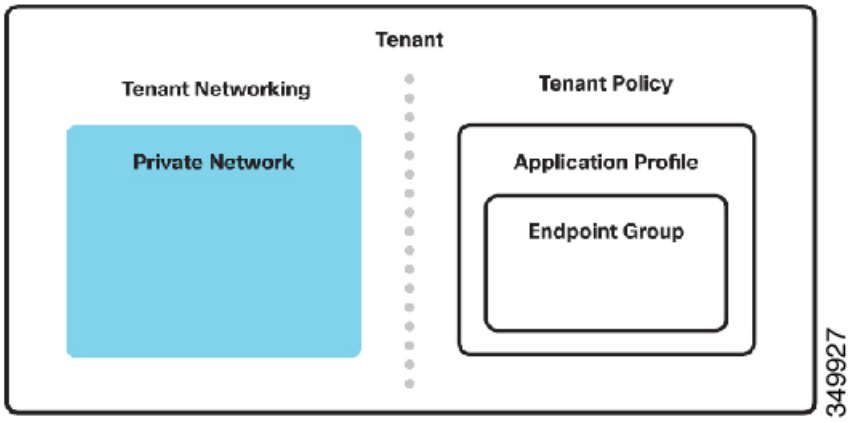
エンドポイントの確認

```
REST :: /api/node/class/fvCEp.xml
CLI  :: moquery -c fvCEp
```

プライベート ネットワーク

プライベート ネットワークは、仮想ルーティングおよびフォワーディング（VRF）、プライベート レイヤ3ネットワーク、またはコンテキストとも呼ばれます。プライベート ネットワークは、一意のレイヤ 3 フォワーディングおよびアプリケーション ポリシー ドメインです。プライベート ネットワークはテナント オブジェクトの子です。プライベート ドメイン内のすべてのエンドポイントは一意の IP アドレスを持つ必要があります。ポリシーで許可されている場合は、これらのデバイス間で直接パケットを転送できるからです。1つ以上のブリッジ ドメインがプライベート ネットワークに関連付けられます。

図 *4:* テナントへのコンポーネントの追加 - *3.* テナント論理モデルの一部としてのプライベート ネットワーク



テナント間でプライベート ネットワークを共有する最も一般的な方法は、共通テナントを介して共有することです。共通テナントの詳細については、この章の概要の項を参照してください。共通テナントで作成されたプライベート ネットワークは、ファブリック内でグローバルに共有されます。ただし、複数のテナントで使用されることを目的とした、共通テナントで作成されないプライベート ネットワークは、共有されることを明示的に設定する必要があります。

個々のプライベート ネットワーク インスタンス間へのトラフィックのルーティングに関する要件がある場合は、サブネットの設定について特に考慮する必要があります。この詳細については、ブリッジ ドメインとエンドポイント グループの設定に関する項で説明されています。

プライベート ネットワークの設定パラメータ

次のリストに、プライベート ネットワークの設定パラメータを示します。

- Name：プライベート ネットワークの名前。
- Policy Control Enforcement Preference：優先ポリシー制御。値は [enforced] または [unenforced] です。[enforced] を選択した場合は、トラフィックを許可するエンドポイント グループ間のコントラクトが必要です。[unenforced] を選択した場合は、プライベート ネットワーク内のすべてのトラフィックが許可されます。デフォルトは [enforced] です。
- Policy Control Enforcement Direction：ポリシーが適用される関係性（つまり方向）での優先ポリシー制御。デフォルトでは入力になっています。
- End Point Retention Policy：（任意）エンドポイント保持ポリシーの名前。
- Monitoring Policy：（任意）テナント セマンティック スコープのモニタリング ポリシーの名前。
- DNS Label：ネットワーク ドメインのネーム ラベル。（任意）ラベルにより、互いに通信できるオブジェクトとできないオブジェクトを分類できます。
- BGP Timers：このオブジェクトに関連する BGP タイマー ポリシーの名前。
- OSPF Timers：このオブジェクトに関連する OSPF タイマー ポリシーの名前。
- OSPF Address Family Context：OSPF アドレス ファミリ コンテキストのポリシー名。
- EIGRP Address Family Context：EIGRP アドレス ファミリ コンテキストのポリシー名。

新しいプライベート ネットワークの作成

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、***[Tenant_Name]*** を選択します。
3. ナビゲーション ウィンドウで、***[Tenant_Name]*** > **[Networking]**> **[VRFs]**の順に選択します。
4. 作業ウィンドウで、**[Actions]** > **[Create VRF]** の順に選択します。
5. [Create VRF] ダイアログボックスで、次の操作を実行します。

1. プライベート ネットワークまたは VRF の名前を入力します。
2. （任意）ポリシー制御適用のプリファレンスを選択します。
3. （任意）ポリシー制御適用の方向を選択します。
4. （任意）エンドポイント保持ポリシーの名前を選択します。
5. （任意）必要に応じて適切なモニタリング ポリシーを選択します。
6. （任意）必要に応じて適切な DNS ラベルを選択します。
7. （任意）必要に応じて適切なルート タグ ポリシーを選択します。
8. （任意）ブリッジ ドメインを作成します。
9. （任意）BGP ポリシーを設定します。
10. （任意）EIGRP ポリシーを選択します。

6. [Finish] をクリックします。ブリッジ ドメインの作成や、BGP、OSPF、または EIGRP ポリシーの設定など、オプションの作成や、設定手順のいずれかを実行する場合は、[Next] をクリックします。
7. [Next] をクリックした場合は、画面の指示に従って関連する追加ポリシーを設定します。

GUI を使用したプライベート ネットワークの変更

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、***[Tenant_Name]*** を選択します。
3. ナビゲーション ウィンドウで、***[Tenant_Name]*** > **[Networking]** > **[VRFs]** > ***[Private_Network]*** を選択します。
4. [Work] ペインで、[Policy] を選択します。
   1. （任意）ポリシー制御適用のプリファレンスを選択します。
   2. （任意）ポリシー制御適用の方向を選択します。
   3. （任意）BGP タイマー ポリシーを選択します。
   4. （任意）追加/削除アイコンを使用して、アドレス ファミリごとの BGP コンテキストを変更します。
   5. OSPF タイマー ポリシーを選択します。
   6. （任意）追加/削除アイコンを使用して、アドレス ファミリごとの OSPF コンテキストを変更します。
   7. （任意）エンドポイント保持ポリシーの名前を選択します。
   8. （任意）必要に応じて適切なモニタリング ポリシーを選択します。

9. （任意）追加/削除アイコンを使用して、アドレス ファミリごとの EIGRP コンテキストを変更します。
10. （任意）必要に応じて適切な DNS ラベルを選択します。
11. （任意）必要に応じてルート タグ ポリシーを選択します。

5. [送信（Submit）] をクリックします。

VRF ポリシー コントロール適用方向の変更

（注） ポリシー制御の適用方向の変更は、トラフィックに影響を与える操作です。この変更を行う最適なタイミングを慎重に検討してください。

VRFポリシー制御の適用方向を変更するには、コントローラと境界リーフスイッチで変更を行う必要があります。

- コントローラで必要な変更を行う （13 ページ）
- ボーダー リーフ スイッチで必要な変更を行う （13 ページ）

コントローラで必要な変更を行う

1. メニュー バーで、**[Tenants]** > **[ALL TENANTS]** の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。
3. ナビゲーション ウィドウで、 ***[Tenant_Name]*** > **[Networking]** > **[VRFs]** > ***[Private_Network]*** の順に選択します。
4. [Work] ペインで、[Policy] を選択します。
    1. **[ポリシー制御適用向き指定（Policy Control Enforcement Direction）]** ドロップダウンリストから、**[入力（Ingress）]** または **[出力（Egress）]** を選択します。
    2. [送信（Submit）] をクリックします。

ボーダー リーフ スイッチで必要な変更を行う

vPCペア設定にボーダーリーフスイッチがある場合は、エンドポイントの同期の問題がないように、両方のボーダーリーフスイッチで次の手順を順番に実行します。

1. メニュー バーで、 **[Fabric]** > **[Inventory]** を選択します。
2. ナビゲーション ウィンドウで、レイヤ 3 外部ネットワーク（L3Outs）が展開されている境界リーフ スイッチに移動します。

    [Pod_Number] > ***[Leaf_Switch_Number]*** > **[VRF Contexts]**

3. この境界リーフ スイッチのVRFコンテキストを右クリックし、**[エンドポイントのクリア（Clear End-Points）]** を選択して、現在学習したエンドポイントをフラッシュします。

GUI を使用したプライベート ネットワークの削除

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、***[Tenant_Name]*** を選択します。
3. ナビゲーション ウィンドウで、***[Tenant_Name]*** > **[Networking]** > **[VRFs]** > ***[Private_Network]*** を選択します。
4. [Work] ペインで、[Actions] > [Delete] の順に選択します。

プライベート ネットワークの確認

```
REST :: /api/node/class/fvCtx.xml
```

```
CLI :: moquery -c fvCtx
```

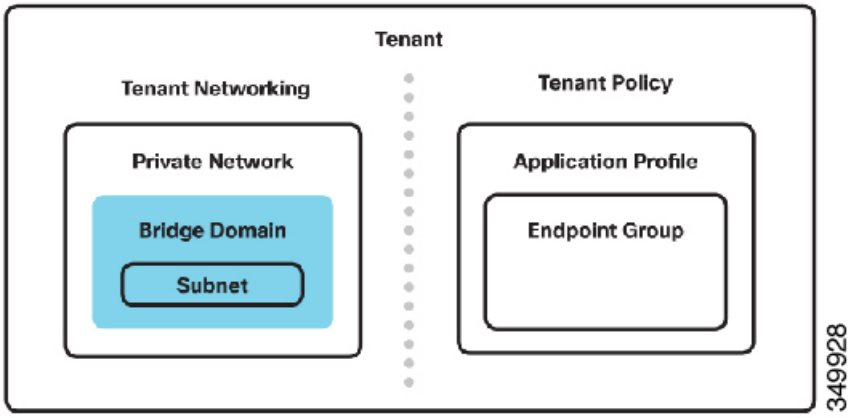
ブリッジ ドメイン

ブリッジ ドメインは、ファブリック内のレイヤ 2 転送ドメインの論理表現です。ブリッジ ドメインは、テナント オブジェクトの子であり、プライベート ネットワークにリンクしている必要があります。

フラッディングが有効な場合、ブリッジ ドメインは、一意のレイヤ 2 MAC アドレス空間とレイヤ 2 フラッド ドメインを定義します。プライベート ネットワークは一意の IP アドレス空間を定義しますが、そのアドレス空間は複数のサブネットから構成できます。これらのサブネットは、プライベート ネットワークに含まれる 1 つ以上のブリッジ ドメインに拡散されます。

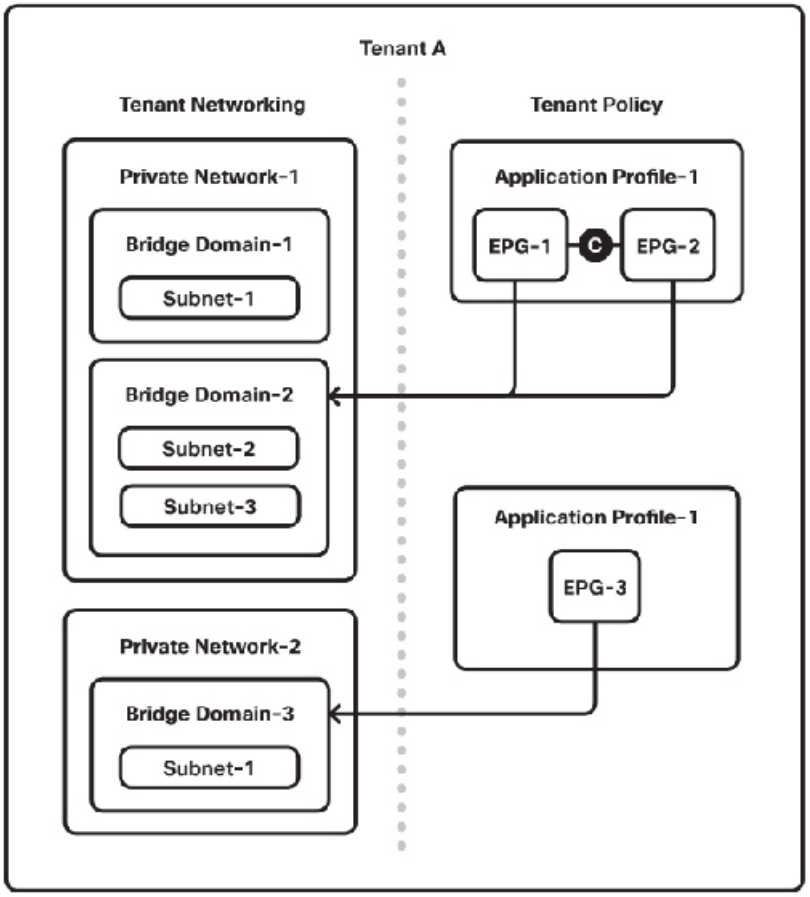
ブリッジ ドメインは、関連付けられているエンドポイント グループが設定されているすべてのスイッチにまたがります。ブリッジ ドメインには複数のサブネットを含めることができます。ただし、サブネットは 1 つのブリッジ ドメイン内に含まれます。

図 *5:* テナントへのコンポーネントの追加 - *4.* テナント アプリケーション プロファイルの一部としてのブリッジ ドメイン



次の図のテナントの例は、ブリッジ ドメインがプライベート ネットワーク内に含まれる仕組みと、エンドポイント グループなどの要素にリンクされる仕組みを示しています。

図 *6:* テナント アプリケーション プロファイルの一部としてのエンドポイント グループ



ブリッジ ドメインは VLAN のように動作できますが、VLAN ではありません。ブリッジ ドメインを分散スイッチと見なす必要があります。この分散スイッチは、リーフ上で、ローカル シグニフィカンスを持つ VLAN としてローカルに変換できます。

実用的観点から、エンドポイント グループに属する接続エンドポイントがある場合、各ブリッジ ドメインは特定のリーフ内に存在します。各ブリッジ ドメインはリーフ スイッチで VLAN ID を受信します。

使用される VLAN ID は、プラットフォーム非依存型 VLAN または PI VLAN と呼ばれます。この VLAN の概念は従来のネットワーキングとは異なっており、VLAN はトラフィックの転送には使用されず、ID として使用されます。各 PI VLAN は、ファブリック内で転送に使用される VXLAN ID にリンクされます。

次の例では、テナント Acme の下のブリッジ ドメイン Acme-Applications-BD に、Leaf-1 で PI VLAN ID 42 が割り当てられています。

エンドポイント グループには、各リーフのローカル シグニフィカンスである PI VLAN ID も割り当てられます。この VLAN ID はブリッジ ドメインとは異なります。したがって、 Cisco Application Centric Infrastructure (ACI) では、1 つのブリッジ ドメイン内のエンドポイントに対

して複数の VLAN が使用されます。詳細については、この章のエンドポイントに関する項を参照してください。

サブネットがブリッジ ドメインで定義された場合、リーフ スイッチはそのサブネットを使用するエンドポイント グループのデフォルト ゲートウェイになります。エンドポイント グループが複数のリーフにエンドポイントを持っている場合、各リーフはデフォルト ゲートウェイを設定します。この方法では、常に、ファブリック内の最初に到達するスイッチがエンドポイントのデフォルト ゲートウェイとなり、拡散型ゲートウェイとも呼ばれます。つまり、SVI はブリッジ ドメインがリンクされているプライベート ネットワークを表す VRF で設定されます。ブリッジ ドメインに複数のサブネットがある場合、ブリッジ ドメインごとに 1 つの SVI がありますが、セカンダリ IP アドレスが使用されます。

ブリッジ ドメインの設定パラメータ

- Name：ブリッジ ドメインの名前。
- Network：関連するレイヤ 3 コンテキスト。
- **Forwarding**：[Optimize] または [Custom] を選択。
- L2 Unknown Unicast：不明なレイヤ 2 宛先の転送方式。デフォルトのメソッドは、[Proxy] です。これは、リーフによりグローバルデータベースを使用して検索用のスパインに転送されることを意味します。宛先が検出されない場合はドロップされます。2 番目の方法は [Flood] で、特定のブリッジ ドメインに対しスパインに基づくマルチキャスト ツリーが使用されます。
- L3 Unknown Multicast Flooding：不明なマルチキャスト宛先へのノード転送パラメータ。[Flood] または [Optimized Flood] を選択できます。
- Multidestination Flood：このパラメータは、レイヤ 2 マルチデスティネーション フラッドのフラッディング動作（マルチキャスト、ブロードキャスト、リンク ローカル固有のトラフィックなど）を設定します。ブリッジ ドメイン内でのフラッディング（デフォルト）、すべてのトラフィックのドロップ、カプセル化または VLAN でのフラッディングを選択できます。
- ARP Flooding：ARP フラッディングを有効にするかどうかを指定するプロパティ。フラッディングがディセーブルである場合、ユニキャスト ルーティングはターゲット IP アドレスで実行されます。ARP フラッディングはデフォルトでディセーブルに設定されています。
- Unicast Routing：事前定義済みの転送基準に基づく転送方式です（IP または MAC アドレス）。ユニキャスト ルーティングはデフォルトでイネーブルに設定されています。ユニキャスト ルーティングは、宛先 IP アドレスを使用して、ハードウェア内に特定の /32 ルートを作成することにより、トラフィックを転送します。
- Config BD MAC Address：ブリッジ ドメインまたはスイッチ仮想インターフェイス（SVI）の MAC アドレス。デフォルトで、各ブリッジ ドメインはファブリック全体のデフォルトの MAC アドレスを使用します。

- IGMP Snoop Policy：IGMP スヌーピング ポリシーの名前。対象ホストからの IGMP メンバーシップ レポート メッセージを確認（スヌーピング）して、マルチキャスト トラフィックの範囲を当該ホストが接続されている各 VLAN インターフェイスの一部だけに限定します。
- Associated L3 Outs：このオブジェクトに関連するレイヤ 3 外部インターフェイスの名前。
- L3 Out for Route Profile：外部ネットワークへの接続を制御するレイヤ 3 外部インターフェイスの ID。
- Route Profile：関連するルート プロファイルの名前。
- Monitoring Policy：（任意）テナント セマンティック スコープのモニタリング ポリシーの名前。
- Subnets：サブネットのネットワーク可視性。 サブネットは、特定のサブネット アドレスを共有するネットワークの一部です。スコープは次のようになります。
  - **Shared Between VRFs**：ファブリック内の他のテナントにルート リークするには、エンドポイント グループにサブネットを定義し、[Shared] オプションを設定します。
  - **Advertise Externally**：レイヤ 3 アウトバウンドと共有するには、ブリッジ ドメインにサブネットを定義し、[Public] オプションを設定します。
  - Private to VRF：そのテナントでのみ使用される（リークされない）ようにするには、ブリッジ ドメインにサブネットを定義し、[Private] オプションを設定します。デフォルトは [Private] です。
- Subnet Control：制御は、IGMP スヌーピングなど、サブネットに適用される特定のプロトコルによって行われます。制御は次のとおりです。
  - Querier IP：サブネットで IGMP スヌーピングを有効にします。
- DHCP Labels：ネットワーク ドメインのネーム ラベル。

GUI を使用した新しいブリッジ ドメインの作成

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、***[Tenant_Name]*** を選択します。
3. ナビゲーション ウィンドウで、***[Tenant_Name]*** > **[ネットワーキング（Networking）]** > **[ブリッジ ドメイン（Bridge Domains）] を選択します**。
4. [Work] ペインで、[Actions] > [Create Bridge Domain] の順に選択します。
5. [Create Bridge Domain] ダイアログボックスで、次の操作を実行します。
   1. [Bridge Domain Name] を入力します。
   2. [Network] を選択します。
   3. （任意）[Forwarding Semantics] を選択します。
   4. （任意）[IGMP Snoop Policy] を選択します。

5. （任意）[Associated L3 Outs] を選択します。
6. （任意）[L3 Out for Route Profile] を選択します。
7. （任意）[Route Profile] を選択します。
8. （任意）必要に応じて [Monitoring Policy] を選択します。
9. （任意）[Subnets] を選択します。
10. （任意）必要に応じて [DNS Label] を選択します。

6. [送信（Submit）] をクリックします。

NX-OS スタイルの CLI を使用した新しいブリッジ ドメインの作成

NX OS スタイルの CLI を使用して、ブリッジ ドメインを作成できます。

手順

ステップ 1 ファブリックの APIC に SSH 接続します。

```
# ssh admin@node_name
```

ステップ 2 設定モードを開始します。

```
apic1# configure
```

ステップ 3 テナントの設定モードを入力します。

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

ステップ 4 ブリッジ ドメインの設定モードを入力します。

```
apic1(config-tenant)# bridge-domain bd1
```

ステップ 5 VRF の設定モードを入力します。

```
apic1(config-bd)# vrf vrf1
```

ステップ 6 コマンドのリストについては、**?** を入力してください。

GUI を使用したブリッジ ドメインの変更

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、***[Tenant_Name]*** を選択します。
3. ナビゲーション ウィドウで、***[Tenant_Name]*** > **[Networking]** > **[Bridge Domains]** > ***[Bridge_Domain_Name]*** を選択します。
4. [Work] ペインで、[Policy] タブを選択し、次の操作を実行します。

1. [Network] を選択します。
2. （任意）[Forwarding Semantics] を選択します。
3. （任意）[IGMP Snoop Policy] を選択します。
4. （任意）[Associated L3 Outs] を選択します。
5. （任意）[L3 Out for Route Profile] を選択します。
6. （任意）[Route Profile] を選択します。
7. （任意）必要に応じて [Monitoring Policy] を選択します。
8. （任意）[Subnets] を選択します。
9. （任意）必要に応じて [DNS Label] を選択します。

5. [完了（Finish）] をクリックします。

NX-OS スタイルの CLI を使用したブリッジ ドメインの変更

NX OS スタイルの CLI を使用して、ブリッジ ドメインを変更できます。

手順

ステップ 1 ファブリックの APIC に SSH 接続します。

```
# ssh admin@node_name
```

ステップ 2 設定モードを開始します。

```
apic1# configure
```

ステップ 3 テナントの設定モードを入力します。

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

ステップ 4 ブリッジ ドメインの設定モードを入力します。

```
apic1(config-tenant)# bridge-domain bd1
```

ステップ 5 コマンドのリストについては、**?** を入力してください。

GUI を使用したブリッジ ドメインの削除

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. 作業ウィンドウで、***[Tenant_Name]*** を選択します。
3. [Navigation] ペインで、[Tenant_Name] > [Networking] > [Bridge Domains] > [Bridge Domain_Name] の順に選択します。

4. [Work] ペインで、[Actions] > [Delete] の順に選択します。

NX-OS スタイルの CLI を使用したブリッジ ドメインの削除

NX OS スタイルの CLI を使用して、ブリッジ ドメインを削除できます。

手順

ステップ 1 ファブリックの APIC に SSH 接続します。

```
# ssh admin@node_name
```

ステップ 2 設定モードを開始します。

```
apic1# configure
```

ステップ 3 テナントの設定モードを入力します。

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

ステップ 4 ブリッジ ドメインを削除します。

```
apic1(config-tenant)# no bridge-domain bd1
```

オブジェクト モデル CLI を使用したブリッジ ドメインの確認

オブジェクト モデル CLI を使用して、ブリッジ ドメインを確認できます。

手順

ステップ 1 ファブリックの APIC に SSH 接続します。

```
# ssh admin@node_name
```

ステップ 2 オブジェクト モデル CLI に切り替えます。

```
apic1# bash
admin@apic1:~>
```

ステップ 3 実体ブリッジ ドメインを確認します。

```
admin@apic1:~> moquery -c l2BD
```

ステップ 4 解決されたブリッジ ドメインを確認します。

```
admin@apic1:~> moquery -c fvBDDef
```

ステップ 5 ローカル ブリッジ ドメインを確認します。

```
admin@apic1:~> moquery -c fvBD
```

テナント ネットワーキングの使用例

すべてのテナント用の共通プライベート ネットワーク

この使用例は、複数のテナントを作成して、そのすべてをファブリックの1つのプライベートネットワーク内に配置することを ACI 管理者が望んでいる環境で一般的です。

この方法には、次の利点と欠点があります。

利点：

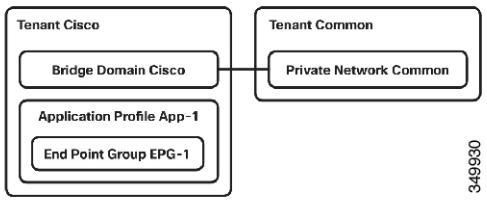
- すべての内部および外部ファブリック接続に対して1つのプライベート ネットワークを使用できる
- 異なる VRF の EPG 間でルート リーキングが不要
- 1 つのレイヤ 3 外部接続をすべてのテナントで使用できる

欠点：

- ルーティングの変更がすべてのテナントに影響する

含有と関係の観点から、このトポロジは次のように表されます。

図 *7:* すべてのテナント用の共通プライベート ネットワーク



共通のテナント プライベート ネットワークを設定する手順：

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで [common] を選択します。
3. [Navigation] ペインで、[common] > [Networking] > [Private Networks] > [default] の順に選択します。
4. [Work] ペインで、[policy] を選択します。
    1. （任意）[Policy Enforcement] を選択します。
    2. （任意）[BGP Policy Name] を選択します。
    3. （任意）[OSPF Policy Name] を選択します。
    4. （任意）[End Point Retention Policy Name] を選択します。
    5. （任意）必要に応じて適切な [Monitoring Policy] を選択します。
    6. （任意）必要に応じて適切な [DNS Label] を選択します。
5. [Finish] をクリックします。

テナントが作成されました。ネットワーク管理者は、最初にブリッジドメインを作成して、共通のプライベート ネットワークをテナントに関連付ける必要があります。

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。
3. [Navigation] ペインで、[Tenant_Name] > [Networking] > [Bridge Domains] の順に選択します。
4. [Work] ペインで、[Actions] > [Create Bridge Domain] の順に選択します。
5. [Create Bridge Domain] ダイアログボックスで、次の操作を実行します。
    1. [Bridge Domain Name] を入力します。
    2. ネットワークを選択します。
    3. [Subnets] フィールドで、[+] をクリックします。
    4. [Gateway IP] フィールドに、サブネットの IP アドレスを入力します。
    5. [Scope] フィールドで、[Private]、[Public]、または [Shared] を選択します。**注**：デフォルトでは、[Private] オプションが選択されます。何を選択するかの詳細については、「外部レイヤ 3」の項を参照してください。
6. [**OK**] をクリックします。
7. [完了（Finish）] をクリックします。

この使用例の設定は、次の CLI 設定を通じて適用できます。

CLI：**テナント Cisco**

```
# tenant
cd '/aci/tenants'
mocreate 'Cisco'
moconfig commit
# bridge-domain
cd '/aci/tenants/Cisco/networking/bridge-domains'
mocreate 'Cisco'
cd 'Cisco'
moset network 'default'
moconfig commit
# subnet
cd '/aci/tenants/Cisco/networking/bridge-domains/Cisco/subnets'
mocreate '172.16.0.1/24'
moconfig commit
# application-profile
cd '/aci/tenants/Cisco/application-profiles'
mocreate 'App1'
moconfig commit
# application-epg
cd '/aci/tenants/Cisco/application-profiles/App1/application-epgs'
mocreate 'EPG1'
cd 'EPG1'
moset bridge-domain 'Cisco'
moconfig commit
# criterion
cd
'/aci/tenants/Cisco/application-profiles/App1/application-epgs/EPG1/vm-attributescriteria'
mocreate 'default'
moconfig commit
```

この設定は、APIC REST API にポストされる次の XML を使用して適用することもできます。

XML：**テナント Cisco**

```
<fvTenant name="Cisco">
```

```
<fvBD arpFlood="no" multiDstPktAct="bd-flood" name="Cisco" unicastRoute="yes"
unkMacUcastAct="proxy" unkMcastAct="flood">
<fvRsCtx tnFvCtxName="default"/>
<fvSubnet ctrl="nd" descr="" ip="172.16.0.1/24" preferred="no"
scope="private"/>
</fvBD>
<fvAp name="App1">
<fvAEPg matchT="AtleastOne" name="EPG1">
<fvRsBd tnFvBDName="Cisco"/>
</fvAEPg>
</fvAp>
<fvRsTenantMonPol tnMonEPGPolName=""/>
</fvTenant>
```

多くのマルチテナント環境では、各テナントが独自のアドレス空間を管理および所有できるようにして、他のテナントとの重複が生じないようにすると良いでしょう。この特定の使用例では、プライベートネットワークと各テナントとを関連付ける方法を説明します。テナントごとのプライベート ネットワーク

利点：

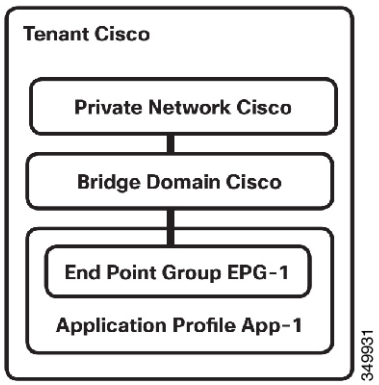
- テナント間を最大限に分離できる
- 複数のテナント内にある IP アドレスが重複するホスト群に対処できる

欠点：

- 専用 VRF で異なるテナント間での EPG 通信を実現する必要がある場合は複雑性が拡大する

この特定の設定のオブジェクト間の関係は次のように表すことができます。

図 *8:* テナントあたりのプライベート ネットワーク



テナントを作成する方法：

1. メニュー バーで [Tenants] > [Add Tenant] の順に選択します。
2. [Create Subnet] ダイアログボックスで、次の操作を実行します。
    1. テナントの**名前**を入力します。
    2. [Next] をクリックします。
3. [Finish] をクリックします。

テナントが作成されました。これで、テナント管理者はプライベート ネットワークを作成できます。

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。
3. [Navigation] ペインで、[Tenant_Name] > [Networking] > [Private Networks] の順に選択します。
4. [Work] ペインで、[Actions] > [Create Private Network] の順に選択します。
5. [Create Private Network] ダイアログボックスで、次の操作を実行します。
    1. プライベート ネットワークの**名前**を入力します。
    2. [Next] をクリックします。
    3. 関連付けられているブリッジ ドメインの**名前**を入力します。
    4. [Subnets] フィールドで、[+] をクリックします。
    5. [Gateway IP] フィールドに、サブネットの IP アドレスを入力します。
    6. [Scope] フィールドで、[Private]、[Public]、または [Shared] を選択します。**注**：デフォルトでは、[Private] オプションが選択されます。何を選択するかの詳細については、「外部レイヤ 3」の項を参照してください。
6. [OK] をクリックします。
7. [完了（Finish）] をクリックします。

この使用例の設定は、次の CLI 設定を通じて適用できます。

CLI：**テナント Cisco**

```
# tenant
cd '/aci/tenants'
mocreate 'Cisco'
moconfig commit
# bridge-domain
cd '/aci/tenants/Cisco/networking/bridge-domains'
mocreate 'Cisco'
cd 'Cisco'
moset network 'Cisco'
moconfig commit
# subnet
cd '/aci/tenants/Cisco/networking/bridge-domains/Cisco/subnets'
mocreate '172.16.0.1/24'
moconfig commit
# private-network
cd '/aci/tenants/Cisco/networking/private-networks'
mocreate 'Cisco'
moconfig commit
# application-profile
cd '/aci/tenants/Cisco/application-profiles'
mocreate 'App1'
moconfig commit
# application-epg
cd '/aci/tenants/Cisco/application-profiles/App1/application-epgs'
mocreate 'EPG1'
cd 'EPG1'
moset bridge-domain 'Cisco'
moconfig commit
```

この設定は、APIC REST API にポストされる次の XML を使用して適用することもできます。

XML：**テナント Cisco**

```
<fvTenant name="Cisco">
<fvBD arpFlood="no" multiDstPktAct="bd-flood" name="Cisco" unicastRoute="yes"
unkMacUcastAct="proxy" unkMcastAct="flood">
<fvRsCtx tnFvCtxName="Cisco"/>
<fvSubnet ctrl="nd" ip="172.16.0.1/24" name="" preferred="no" scope="private"/>
</fvBD>
<fvCtx knwMcastAct="permit" name="Cisco" pcEnfPref="enforced"/>
<fvAp name="App1" prio="unspecified">
<fvAEPg name="EPG1">
<fvRsBd tnFvBDName="Cisco"/>
</fvAEPg>
</fvAp>
</fvTenant>
```

テナント内通信を行う複数のプライベート ネットワーク

サポートすることが望ましい別の使用例として、複数のプライベート ネットワークを持つ単一テナントを所有するというオプションがあります。これは、管理レベルではなく、ネットワーク レベルでマルチテナント機能を提供する必要があるためです。また、合併やその他のビジネス上の変更により、単一テナント内で重複しているサブネットをサポートする場合にも発生します。

この方法には、次の利点と欠点があります。

利点：

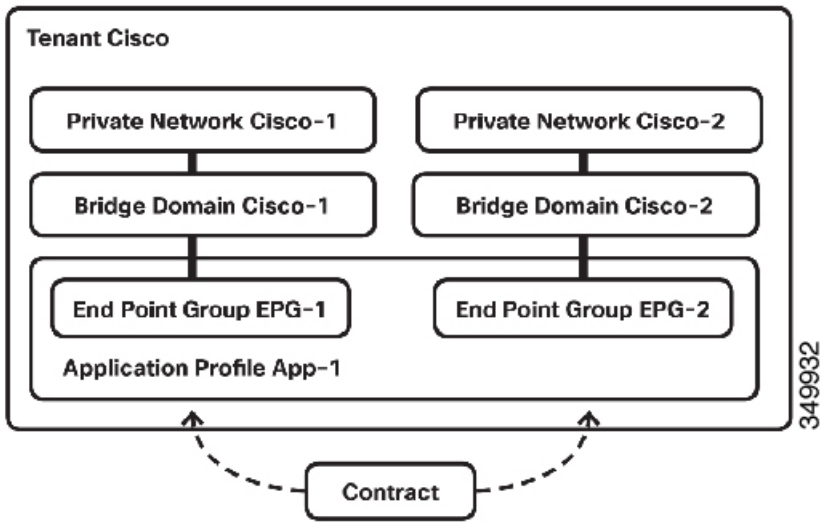
- 単一テナント内で重複するサブネットを所有できる

欠点：

- 重複するサブネットに存在する EPG は互いに適用し合うポリシーを所有できない

この特定の設定のオブジェクト間の関係は次のように表すことができます。

図 *9:* テナント内通信を行う複数のプライベート ネットワーク



テナントを作成する方法：

1. メニュー バーで [Tenants] > [Add Tenant] の順に選択します。
2. [Create Tenant] ダイアログボックスで、次の操作を実行します。
    1. テナントの**名前**を入力します。
3. [Next] をクリックします。
4. [Finish] をクリックします。

テナントが作成されました。これで、テナント管理者はプライベート ネットワークを作成できます。

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。
3. [Navigation] ペインで、[Tenant_Name] > [Networking] > [Private Networks] の順に選択します。
4. [Work] ペインで、**[Actions]** > **[Create Private Network]** の順に選択します。
5. [Create Private Network] ダイアログボックスで、次の操作を実行します。
    1. [Name] フィールドに、プライベート ネットワークの名前を入力します。
    2. [Next] をクリックします。
    3. [Name] フィールドに、ブリッジ ドメインの名前を入力します。
    4. [Subnets] フィールドで、[+] をクリックします。
    5. [Gateway IP] フィールドに、サブネットの IP アドレスを入力します。
    6. [Scope] フィールドで [Shared] を選択します。**注**：共有サブネットのタイプによって、ACI で、何が 2 つのプライベート ネットワーク（VRF）間のルート リークであるかが決まります。

6. [OK] をクリックします。
7. [Finish] をクリックします。
8. [Navigation] ペインで、[Tenant_Name] > [Networking] > [Private Networks] の順に選択します。
9. [Work] ペインで、**[Actions]** > **[Create Private Network]** の順に選択します。
10. [Create Private Network] ダイアログボックスで、次の操作を実行します。
    1. [Name] フィールドに、2 つ目のプライベート ネットワークの名前を入力します。
    2. [Next] をクリックします。
    3. [Name] フィールドに、2 つ目のブリッジ ドメインの名前を入力します。
    4. [Subnets] フィールドで、[+] をクリックします。
    5. [Gateway IP] フィールドに、サブネットの IP アドレスを入力します。
    6. [Scope] フィールドで [Shared] を選択します。
11. [**OK**] をクリックします。
12. [Finish] をクリックします。

これで 2 つのプライベート ネットワークとブリッジ ドメインが作成されました。アプリケーション プロファイルに移動できます。

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。
3. [Navigation] ペインで、[Tenant_Name] > [Networking] > [Application Profiles] の順に選択します。
4. [Action] タブで、[Create Application Profile] を選択します。
5. [Create Application Profile] ダイアログボックスで、次の操作を実行します。
    1. [Name] フィールドに、アプリケーション プロファイルの名前を入力します。
6. [Submit] をクリックします。

2 つのエンドポイント グループを作成する方法：

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。
3. [Navigation] ペインで、[Tenant_Name] > [Networking] > [Application Profiles] > [Application Profile_Name] の順に選択します。
4. [Work] ペインで、[Actions] > [Create Application EPG] の順に選択します。
5. [Create Application EPG] ダイアログボックスで、次の操作を実行します。
    1. [Name] フィールドに、エンド ポイント グループの名前を入力します。
    2. [Bridge Domain] フィールドで適切なブリッジ ドメインを選択します。
6. [Finish] をクリックします。

2 つ目の EPG にこれらの手順を繰り返します。

ここでテナント管理者は、コントラクトを作成し、2つのEPG間でフィルタ処理する必要があります。

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。
3. [Navigation] ペインで、[Tenant_Name] > [Security Policies] > [Filters] の順に選択します。
4. [Work] ペインで、[Actions] > [Create Filters] の順に選択します。
5. [Create Filter] ダイアログボックスで、次の操作を実行します。
    1. [Name] フィールドにフィルタの名前を入力します。
    2. [+] をクリックします。
    3. [Name] 列に **ICMP** と入力します。
    4. [Ethertype] フィールドで [IP] を選択します。
    5. [IP Protocol] 列で [ICMP] を選択します。
6. [Update] をクリックします。
7. [Submit] をクリックします。

テナント管理者は、2つのEPG間のトラフィックで許可するフィルタ情報を把握している必要があります。フィルタでは、アプリケーションに必要なさまざまなネットワーク プロトコルを必要な数だけを定義します。ここで、2つのEPGが使用または提供するコントラクトを定義する必要があります。

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。
3. [Navigation] ペインで、[Tenant_Name] > [Security Policies] > [Contracts] の順に選択します。
4. [Work] ペインで、[Actions] > [Create Contract] の順に選択します。
5. [Create Contract] ダイアログボックスで、次の操作を実行します。
    1. [Name] フィールドにフィルタの名前を入力します。
    2. [Scope] フィールドで [Global] を選択します。
    3. [Subjects] フィールドで、[+] をクリックします。
    4. [Name] フィールドに**サブジェクト**の名前を入力します。
    5. [Filter Chain] フィールドで、[+] をクリックします。
    6. 作成したフィルタを選択します。
6. [Update] をクリックします。
7. **OK** をクリックします。
8. [Submit] をクリックします。

EPG間にコントラクトを設定します。使用されたコントラクトまたは提供されたコントラクトのいずれかとして、コントラクトがEPGに割り当てられます。作成した各EPGは、両方のEPG間の関係を確立するためにそのコントラクトを使用、または提供します。

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。
3. [Navigation] ペインで、[Tenant_Name] > [Application Profiles] > [Application Profile Name] > [Application EPGs] > [EPG_Name] > [Contracts] の順に選択します。
4. [Work] ペインで、[Actions] > [Add Provided Contract] の順に選択します。
5. [Add Provided Contract] ダイアログボックスで、次の操作を実行します。

1. 作成したコントラクトを選択します。
2. [Submit] をクリックします。

6. 2 つ目の EPG の下にある [Navigation] ペインで、[Contracts] を選択します。
7. [Action] タブで、[Add Consume Contract] を選択します。
   1. 作成したコントラクトを選択します。
8. [Submit] をクリックします。`

この使用例の設定は、次の CLI 設定を通じて適用できます。

CLI：テナント Cisco

```
# tenant
cd '/aci/tenants'
mocreate 'Cisco'
moconfig commit
# bridge-domain
cd '/aci/tenants/Cisco/networking/bridge-domains'
mocreate 'Cisco'
cd 'Cisco'
moset network 'Cisco'
moconfig commit
# bridge-domain
cd '/aci/tenants/Cisco/networking/bridge-domains'
mocreate 'Cisco1'
cd 'Cisco1'
moset network 'Cisco1'
moconfig commit
# private-network
cd '/aci/tenants/Cisco/networking/private-networks'
mocreate 'Cisco'
moconfig commit
# private-network
cd '/aci/tenants/Cisco/networking/private-networks'
mocreate 'Cisco1'
moconfig commit
# application-profile
cd '/aci/tenants/Cisco/application-profiles'
mocreate 'App1'
moconfig commit
# application-epg
cd '/aci/tenants/Cisco/application-profiles/App1/application-epgs'
mocreate 'EPG1'
cd 'EPG1'
moset bridge-domain 'Cisco'
moconfig commit
# fv-rscon
cd '/aci/tenants/Cisco/application-profiles/App1/applicationepgs/
EPG1/contracts/consumed-contracts'
mocreate 'ICMP'
moconfig commit
# fv-subnet
cd '/aci/tenants/Cisco/application-profiles/App1/application-epgs/EPG1/subnets'
mocreate '172.16.1.1/24'
cd '172.16.1.1:24'
moset scope 'private,shared'
moconfig commit
# application-epg
cd '/aci/tenants/Cisco/application-profiles/App1/application-epgs'
```

```
mocreate 'EPG2'
cd 'EPG2'
moset bridge-domain 'Cisco1'
moconfig commit
# fv-rsprov
cd '/aci/tenants/Cisco/application-profiles/App/applicationepgs/
EPG2/contracts/provided-contracts'
mocreate 'ICMP'
moconfig commit
# fv-subnet
cd '/aci/tenants/Cisco/application-profiles/CCO/application-epgs/EPG2/subnets'
mocreate '172.16.2.1/24'
cd '172.16.2.1:24'
moset scope 'private,shared'
moconfig commit
```

この設定は、APIC REST API にポストされる次の XML を使用して適用することもできます。

XML：**テナント Cisco**

```
<fvTenant dn="uni/tn-Cisco" name="Cisco">
<vzBrCP name="ICMP" scope="tenant">
<vzSubj consMatchT="AtleastOne" name="icmp" provMatchT="AtleastOne"
revFltPorts="yes">
<vzRsSubjFiltAtt tnVzFilterName="icmp"/>
</vzSubj>
</vzBrCP>
<fvCtx knwMcastAct="permit" name="CiscoCtx" pcEnfPref="enforced"/>
<fvCtx knwMcastAct="permit" name="CiscoCtx2" pcEnfPref="enforced"/>
<fvBD arpFlood="yes" mac="00:22:BD:F8:19:FF" name="CiscoBD2" unicastRoute="yes"
unkMacUcastAct="flood" unkMcastAct="flood">
<fvRsCtx tnFvCtxName="CiscoCtx2"/>
</fvBD>
<fvBD arpFlood="yes" mac="00:22:BD:F8:19:FF" name="CiscoBD" unicastRoute="yes"
unkMacUcastAct="flood" unkMcastAct="flood">
<fvRsCtx tnFvCtxName="CiscoCtx"/>
</fvBD>
<fvAp name="CCO">
<fvAEPg matchT="AtleastOne" name="Web">
<fvRsCons tnVzBrCPName="ICMP"/>
<fvRsPathAtt encap="vlan-1201" instrImedcy="immediate" mode="native"
tDn="topology/pod-1/paths-201/pathep-[eth1/16]"/>
<fvSubnet ip="172.16.2.1/24" scope="private,shared"/>
<fvRsDomAtt instrImedcy="lazy" resImedcy="lazy" tDn="uni/phys-
PhysDomainforCisco"/>
<fvRsBd tnFvBDName="CiscoBD2"/>
</fvAEPg>
<fvAEPg matchT="AtleastOne" name="App">
<fvRsPathAtt encap="vlan-1202" instrImedcy="immediate" mode="native"
tDn="topology/pod-1/paths-202/pathep-[eth1/2]"/>
<fvSubnet ip="172.16.1.1/24" scope="private,shared"/>
<fvRsDomAtt instrImedcy="lazy" resImedcy="lazy" tDn="uni/phys-
PhysDomainforCisco"/>
<fvRsBd tnFvBDName="CiscoBD"/>
<fvRsProv matchT="AtleastOne" tnVzBrCPName="ICMP"/>
</fvAEPg>
</fvAp>
</fvTenant>
```

テナント間通信を行う複数のプライベート ネットワーク

この使用例は一般的に、ACIの管理者が、テナント間通信の機能を持つ複数のテナントを作成し、サポートしたい場合に使用されます。

この方法には、次の利点と欠点があります。

利点

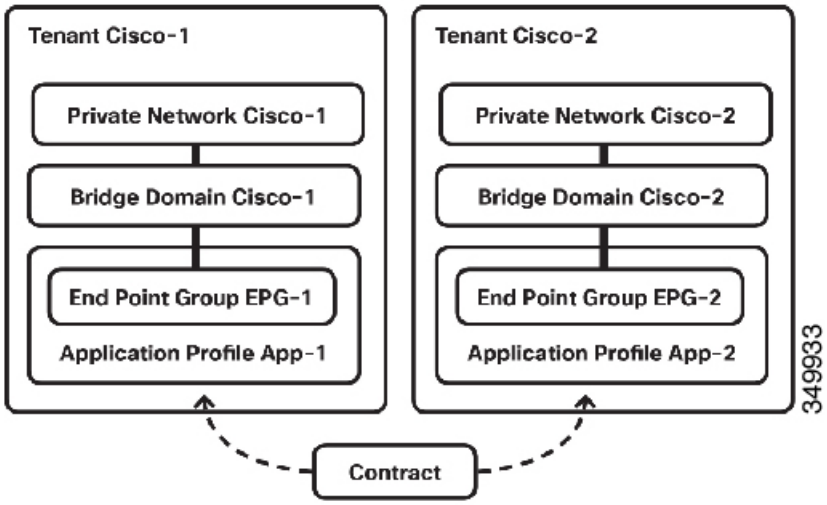
- 各テナント コンテナの個別管理が可能
- テナント間の最大分離を実現

欠点

- テナントのアドレス空間は一意である必要がある

オブジェクト間の関係とコントラクトの観点から、このトポロジは次のように表されます。

図 *10 :* テナント間通信を行う複数のプライベート ネットワーク



テナントを作成する方法：

1. GUI を使用して、[Tenants] > [ADD TENANT] に移動します。
2. [Create Tenant] ダイアログボックスで、次の操作を実行します。
    1. [Name] フィールドに最初のテナントの名前を入力します。
3. [Next] をクリックします。
4. [Finish] をクリックします。

テナントが作成されました。これで、テナント管理者はプライベート ネットワークを作成できます。

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。

3. [Navigation] ペインで、[Tenant_Name] > [Networking] > [Private Networks] の順に選択します。
4. [Work] ペインで、[Actions] > [Create Private Network] の順に選択します。
5. [Create Private Network] ダイアログボックスで、次の操作を実行します。
    1. [Name] フィールドに、プライベート ネットワークの名前を入力します。
    2. [Next] をクリックします。
    3. [Name] フィールドに、ブリッジ ドメインの名前を入力します。
    4. [Subnets] フィールドで、[+] をクリックします。
    5. [Gateway IP] フィールドに、サブネットの IP アドレスを入力します。
    6. [Scope] フィールドで [Shared] を選択します。**注**：共有サブネットのタイプによって、ACI で、何が 2 つのプライベート ネットワーク（VRF）間のルート リークであるかが決まります。
6. [**OK**] をクリックします。
7. [完了（Finish）] をクリックします。

アプリケーション プロファイルを作成する方法：

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。
3. [Navigation] ペインで、[Tenant_Name] > [Networking] > [Application Profiles] の順に選択します。
4. [Work] ペインで、[Actions] > [Create Application Profile] の順に選択します。
5. [Create Application Profile] ダイアログボックスで、次の操作を実行します。
    1. [Name] フィールドに、アプリケーション プロファイルの名前を入力します。
6. [Submit] をクリックします。

エンドポイント グループを作成する方法：

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。
3. [Navigation] ペインで、[Tenant_Name] > [Networking] > [Application Profiles] > [Application Profile_Name] の順に選択します。
4. [Work] ペインで、[Actions] > [Create Application EPG] の順に選択します。
5. [Create Application EPG] ダイアログボックスで、次の操作を実行します。
    1. [Name] フィールドに、エンド ポイント グループの名前を入力します。
    2. [Bridge Domain] フィールドで適切なブリッジ ドメインを選択します。
6. [Finish] をクリックします。

2 つ目のテナントやアプリケーション プロファイルを作成する方法：

1. GUI を使用して、[Tenants] > [ADD TENANT] に移動します。
2. [Create Tenant] ダイアログボックスで、次の操作を実行します。
    1. [Name] フィールドに最初のテナントの名前を入力します。

3. [Next] をクリックします。
4. [Finish] をクリックします。

テナントが作成されました。これで、テナント管理者はプライベート ネットワークを作成できます。

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。
3. [Navigation] ペインで、[Tenant_Name] > [Networking] > [Private Networks] の順に選択します。
4. [Work] ペインで、[Actions] > [Create Private Network] の順に選択します。
5. [Create Private Network] ダイアログボックスで、次の操作を実行します。
    1. [Name] フィールドに、プライベート ネットワークの名前を入力します。
    2. [Next] をクリックします。
    3. [Name] フィールドに、ブリッジ ドメインの名前を入力します。
    4. [Subnets] フィールドで、[+] をクリックします。
    5. [Gateway IP] フィールドに、サブネットの IP アドレスを入力します。
    6. [Scope] フィールドで [Shared] を選択します。**注**：共有サブネットのタイプによって、ACI で、何が 2 つのプライベート ネットワーク（VRF）間のルート リークであるかが決まります。
6. [OK] をクリックします。
7. [完了（Finish）] をクリックします。

アプリケーション プロファイルを作成する方法：

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。
3. [Navigation] ペインで、[Tenant_Name] > [Networking] > [Application Profiles] の順に選択します。
4. [Work] ペインで、[Actions] > [Create Application Profile] の順に選択します。
5. [Create Application Profile] ダイアログボックスで、次の操作を実行します。
    1. [Name] フィールドに、アプリケーション プロファイルの名前を入力します。
6. [Submit] をクリックします。

エンドポイント グループを作成する方法：

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。
3. [Navigation] ペインで、[Tenant_Name] > [Networking] > [Application Profiles] > [Application Profile_Name] の順に選択します。
4. [Work] ペインで、[Actions] > [Create Application EPG] の順に選択します。
5. [Create Application EPG] ダイアログボックスで、次の操作を実行します。
    1. [Name] フィールドに、エンド ポイント グループの名前を入力します。
    2. [Bridge Domain] フィールドで適切なブリッジ ドメインを選択します。

6. [Finish] をクリックします。

ここでテナント管理者は、コントラクトを作成し、2つのEPG間でフィルタ処理する必要があります。

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。
3. [Navigation] ペインで、[Tenant_Name] > [Security Policies] > [Filters] の順に選択します。
4. [Work] ペインで、[Actions] > [Create Filters] の順に選択します。
5. [Create Filter] ダイアログボックスで、次の操作を実行します。
    1. [Name] フィールドにフィルタの名前を入力します。
    2. [+] をクリックします。
    3. [Name] 列に **ICMP** と入力します。
    4. [Ethertype] フィールドで [IP] を選択します。
    5. [IP Protocol] 列で [ICMP] を選択します。
6. [Update] をクリックします。
7. [Submit] をクリックします。

テナント管理者には、2つのEPG間で許可するトラフィックのフィルタを把握している必要があります。フィルタでは、アプリケーションに必要なさまざまなネットワーク プロトコルを必要な数だけ定義します。ここで、2つのEPGが使用または提供するコントラクトを定義する必要があります。

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。
3. [Navigation] ペインで、[Tenant_Name] > [Security Policies] > [Contracts] の順に選択します。
4. [Work] ペインで、[Actions] > [Create Contract] の順に選択します。
5. [Create Contract] ダイアログボックスで、次の操作を実行します。
    1. [Name] フィールドにフィルタの名前を入力します。
    2. [Scope] フィールドで [Global] を選択します。
    3. [Subjects] フィールドで、[+] をクリックします。
    4. [Name] フィールドに**サブジェクト**の名前を入力します。
    5. [Filter Chain] フィールドで、[+] をクリックします。
    6. 作成したフィルタを選択します。
6. [Update] をクリックします。
7. **OK** をクリックします。
8. [Submit] をクリックします。

EPG間にコントラクトを設定します。使用されたコントラクトまたは提供されたコントラクトのいずれかとして、コントラクトがEPGに割り当てられます。作成した各EPGは、両方のEPG間の関係を確立するためにそのコントラクトを使用、または提供します。

1. メニュー バーで、[Tenants] > [ALL TENANTS] の順に選択します。
2. [Work] ペインで、[Tenant_Name] を選択します。

3. [Navigation] ペインで、[Tenant_Name] > [Application Profiles] > [Application Profile Name] > [Application EPGs] > [EPG_Name] > [Contracts] の順に選択します。
4. [Work] ペインで、[Actions] > [Add Provided Contract] の順に選択します。
5. [Add Provided Contract] ダイアログボックスで、次の操作を実行します。
    1. 作成した**コントラクト**を選択します。
    2. [Submit] をクリックします。`
6. GUI を使用して、[Tenants] > [ALL TENANTS] に移動します。
7. **2 つ目**に作成したテナントを選択します。
8. [Navigation] ペインで、[Tenant_Name] > [Application Profiles] > [Application Profile Name] > [Application EPGs] > [EPG_Name] > [Contracts] の順に選択します。
9. [Work] ペインで、[Actions] > [Add Consume Contract] の順に選択します。
    1. 作成した**コントラクト**を選択します。
10. [Submit] をクリックします。`

この使用例の設定は、次の CLI 設定を通じて適用できます。

CLI：**テナント Cisco1**

```
# tenant
cd '/aci/tenants'
mocreate 'Cisco1'
moconfig commit
# bridge-domain
cd '/aci/tenants/Cisco1/networking/bridge-domains'
mocreate 'Cisco1'
cd 'Cisco1'
moset network 'Cisco1'
moconfig commit
# private-network
cd '/aci/tenants/Cisco1/networking/private-networks'
mocreate 'Cisco1'
moconfig commit
# application-profile
cd '/aci/tenants/Cisco1/application-profiles'
mocreate 'App1'
moconfig commit
# application-epg
cd '/aci/tenants/Cisco1/application-profiles/App1/application-epgs'
mocreate 'EPG1'
cd 'EPG1'
moset bridge-domain 'Cisco1'
moconfig commit
# fv-rsprov
cd '/aci/tenants/Cisco/application-profiles/CCO/applicationepgs/
App/contracts/provided-contracts'
mocreate 'ICMP'
moconfig commit
# fv-subnet
cd '/aci/tenants/Cisco/application-profiles/CCO/application-epgs/App/subnets'
mocreate '172.16.1.1/24'
cd '172.16.1.1:24'
moset scope 'private,shared'
moconfig commit
# contract
```

```
cd '/aci/tenants/Cisco/security-policies/contracts'
mocreate 'ICMP'
cd 'ICMP'
moset scope 'global'
moconfig commit
# contract-subject
cd '/aci/tenants/Cisco/security-policies/contracts/ICMP/subjects'
mocreate 'icmp'
moconfig commit
# vz-rssubjfiltatt
cd '/aci/tenants/Cisco/security-policies/contracts/ICMP/subjects/icmp/common-filters'
mocreate 'icmp'
moconfig commit
```

CLI：テナント **Cisco2**

```
# tenant
cd '/aci/tenants'
mocreate 'Cisco'
moconfig commit
# bridge-domain
cd '/aci/tenants/Cisco/networking/bridge-domains'
mocreate 'Cisco'
cd 'Cisco'
moset network 'Cisco'
moconfig commit
# private-network
cd '/aci/tenants/Cisco/networking/private-networks'
mocreate 'Cisco'
moconfig commit
# application-profile
cd '/aci/tenants/Cisco/application-profiles'
mocreate 'App1'
moconfig commit
# application-epg
cd '/aci/tenants/Cisco2/application-profiles/App1/application-epgs'
mocreate 'EPG1'
cd 'EPG1'
moset bridge-domain 'Cisco'
moconfig commit
# fv-rsconsif
cd '/aci/tenants/Cisco1/application-profiles/CCO/applicationepgs/
Web/contracts/consumed-contract-interfaces'
mocreate 'CiscoInterTenantICMP'
moconfig commit
# fv-subnet
cd '/aci/tenants/Cisco1/application-profiles/CCO/application-epgs/Web/subnets'
mocreate '172.16.2.1/24'
cd '172.16.2.1:24'
moset scope 'shared-subnet'
moconfig commit
# imported-contract
cd '/aci/tenants/Cisco1/security-policies/imported-contracts'
mocreate 'CiscoInterTenantICMP'
cd 'CiscoInterTenantICMP'
moset contract 'tenants/Cisco/security-policies/contracts/ICMP'
moconfig commit
```

この設定は、APIC REST API にポストされる次の XML を使用して適用することもできます。

XML：テナント **Cisco1**

```
<fvTenant dn="uni/tn-Cisco1" name="Cisco1">
```

```
<vzBrCP name="ICMP" scope="global">
<vzSubj consMatchT="AtleastOne" name="icmp" provMatchT="AtleastOne"
revFltPorts="yes">
<vzRsSubjFiltAtt tnVzFilterName="icmp"/>
</vzSubj>
</vzBrCP>


<vzCPIf dn="uni/tn-Cisco1/cif-ICMP" name="ICMP">


<vzRsIf consMatchT="AtleastOne" name="icmp" provMatchT="AtleastOne"
revFltPorts="yes">
<vzRsSubjFiltAtt tDn="uni/tn-Cisco2/brc-default"/>
</vzRsIf>
</vzCPIf>
<fvCtx knwMcastAct="permit" name="CiscoCtx" pcEnfPref="enforced"/>


<fvBD arpFlood="yes" mac="00:22:BD:F8:19:FF" name="CiscoBD2" unicastRoute="yes"
unkMacUcastAct="flood" unkMcastAct="flood">
<fvRsCtx tnFvCtxName="CiscoCtx2"/>
</fvBD>
<fvBD arpFlood="yes" name="CiscoBD" unicastRoute="yes" unkMacUcastAct="flood"
unkMcastAct="flood">
<fvRsCtx tnFvCtxName="CiscoCtx"/>
</fvBD>
<fvAp name="CCO">
<fvAEPg matchT="AtleastOne" name="EPG1">
<fvRsPathAtt encap="vlan-1202" instrImedcy="immediate" mode="native"
tDn="topology/pod-1/paths-202/pathep-[eth1/2]"/>
<fvSubnet ip="172.16.1.1/24" scope="private,shared"/>


<fvRsDomAtt instrImedcy="lazy" resImedcy="lazy" tDn="uni/phys-
PhysDomainforCisco"/>


<fvRsBd tnFvBDName="CiscoBD"/>
<fvRsProv matchT="AtleastOne" tnVzBrCPName="ICMP"/>
</fvAEPg>
</fvAp>
</fvTenant>
```

XML：テナント Cisco2

```
<fvTenant dn="uni/tn-Cisco2" name="Cisco2">
<fvCtx knwMcastAct="permit" name="CiscoCtx" pcEnfPref="enforced"/>
<fvBD arpFlood="yes" mac="00:22:BD:F8:19:FF" name="CiscoBD2" unicastRoute="yes"
unkMacUcastAct="flood" unkMcastAct="flood">
<fvRsCtx tnFvCtxName="CiscoCtx"/>
</fvBD>
<fvBD arpFlood="yes" name="CiscoBD" unicastRoute="yes" unkMacUcastAct="flood"
unkMcastAct="flood">
<fvRsCtx tnFvCtxName="CiscoCtx"/>
</fvBD>
<fvAp name="CCO">
<fvAEPg matchT="AtleastOne" name="EPG2">
<fvRsPathAtt encap="vlan-1202" instrImedcy="immediate" mode="native"
tDn="topology/pod-1/paths-201/pathep-[eth1/2]"/>
<fvSubnet ip="172.16.1.1/24" scope="private,shared"/>


<fvRsDomAtt instrImedcy="lazy" resImedcy="lazy" tDn="uni/phys-
PhysDomainforCisco"/>
```

```
<fvRsBd tnFvBDName="CiscoBD"/>
<fvRsConsIf matchT="AtleastOne" tnVzBrCPIfName="ICMP"/>
</fvAEPg>
</fvAp>
</fvTenant>
```

一般的なパーベイシブ ゲートウェイを備えたデュアル ファブリック

この使用例は、Cisco Application Centric Infrastructure (ACI) 管理者が、デュアル ファブリックを管理してファブリック間でワークロードをシームレスに移動できるようにする必要がある環境での典型的な例です。

利点

- 異なるファブリックに接続されているハイパーバイザ ホスト間で仮想マシンを移行することができます。
- シームレスなワークロードの移行を可能にします。

欠点

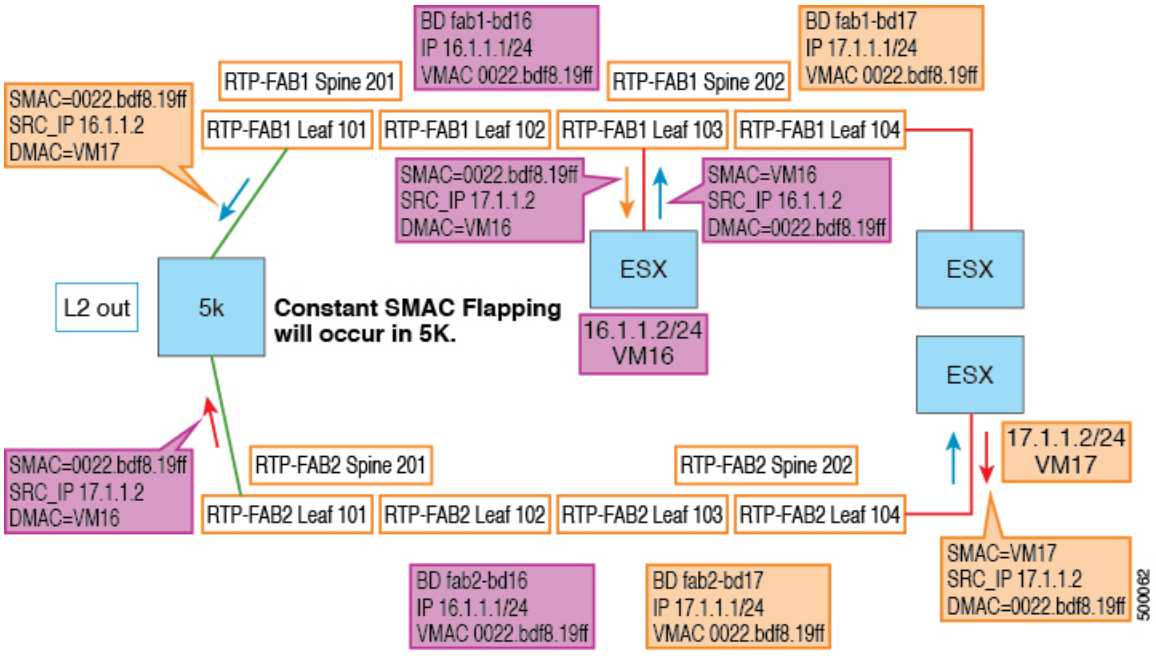
- デュアル ファブリックの設定間で調整が必要です。

「レイヤ 2 アウト上のルーティング/一般的なパーベイシブ ゲートウェイ」機能の目的は、エンドポイントがファブリック間をシームレスに移動するようにすることです。

次の情報は、一般的なパーベイシブ ゲートウェイを備えたデュアル ファブリックに適用されます。

- デュアル ファブリックが使用されていることが前提となります。
- この場合の「ルーティング」は、異なるブリッジ ドメイン（サブネット）のエンドポイント間のトラフィックを意味します。
- ブリッジ ドメインは、ファブリック間でミラーリングされます（ただし例外あり）。
- よく言われる「拡張されたブリッジ ドメイン」とは、実際にはファブリック間でミラーリングされたブリッジ ドメインを意味します。あくまでも 2 つの別々のブリッジ ドメインであり、独立した各ファブリックに属します。
- ゲートウェイとしてブリッジ ドメイン IP アドレスを使用しているレイヤ 2 ネットワークには、エンドポイントは存在しません。
- ユーザは、ブリッジ ドメインに関するファブリックをそれぞれ手動で設定するか、またはなんらかのオーケストレーション ツールを使用して、各ファブリックに同期設定を配布できます。
- これに役立つアプリケーションは、ACI ツール キットに含まれています。

VM16 と VM17 間のトラフィックを使用して、この機能が必要な理由について説明します。



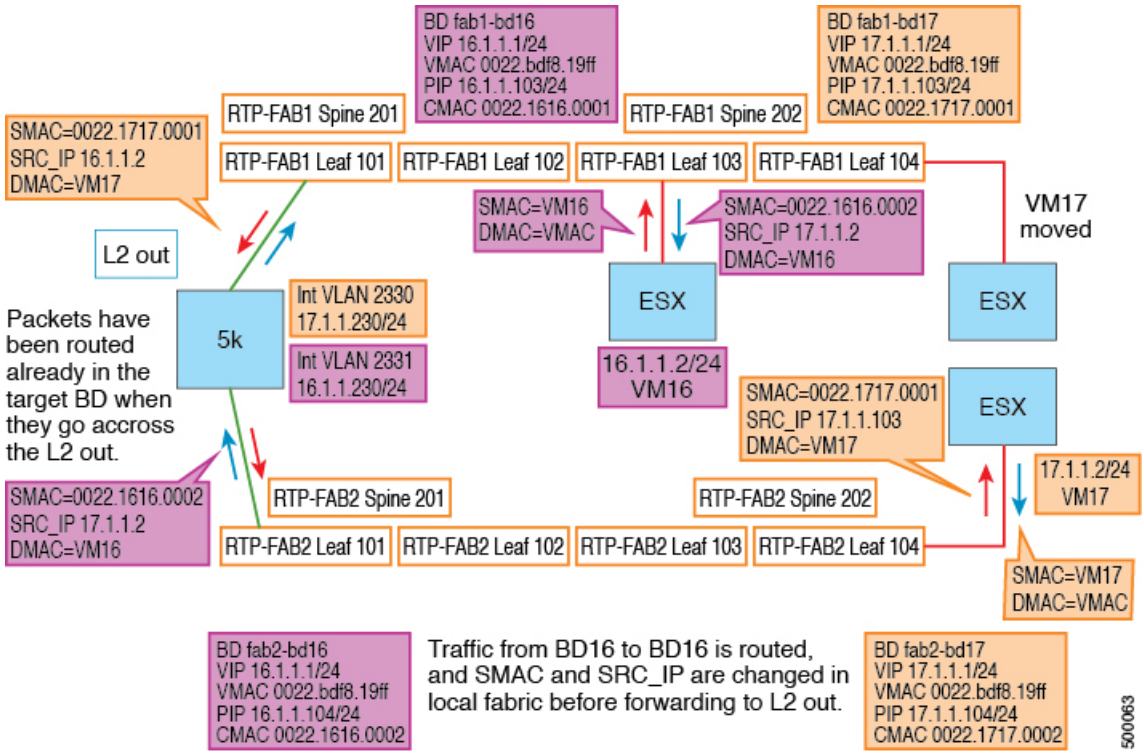
上の図で、VM17がVM16にパケットを送信する際、そのデフォルトゲートウェイに送信しているのが確認できます。その後、パケットはBD17からBD16に「ルーティング」されます。BD16はその後、パケットをレイヤ2パケットとして、BD16 SMAC（送信元MAC）からVM16に転送します。VM16が応答したら、逆の順序で同様の動作が行われます。結果として、ここではNexus 5Kとして表示されるレイヤ2ネットワークは、別のポートからBD16/BD17 SMACを学習し続けることになります。

ファブリック間で同じブリッジドメインIPアドレスおよびMACアドレスを保持する必要があります。これにより、VMがファブリック間を移行する際、そのデフォルトゲートウェイ用の新しいMACについてARPを発行する必要がなくなります。確認できるように、両方のファブリックで同じSMACを使用する場合、問題を引き起こす可能性があります。

解決策として、ブリッジドメインに追加の設定を導入します。新しいリリース（1.2）では、ブリッジドメインのサブネットIPアドレスを「仮想」として設定できるようになりました。これは、VMのデフォルトゲートウェイとして機能するアドレスです。また、VMAC（仮想MAC）も設定できます。これは、VMがそのデフォルトゲートウェイとしてARPを発行したときに解決されるMACです。これらは、ブリッジドメインのファブリック間で一致している必要があります。

また、この場合、ブリッジドメインのCMAC（設定済みMAC）、および仮想IPとして同じサブネット内の2番目のIPアドレスを設定する必要があります。これらは、ブリッジドメインのファブリック間で固有である必要があります。

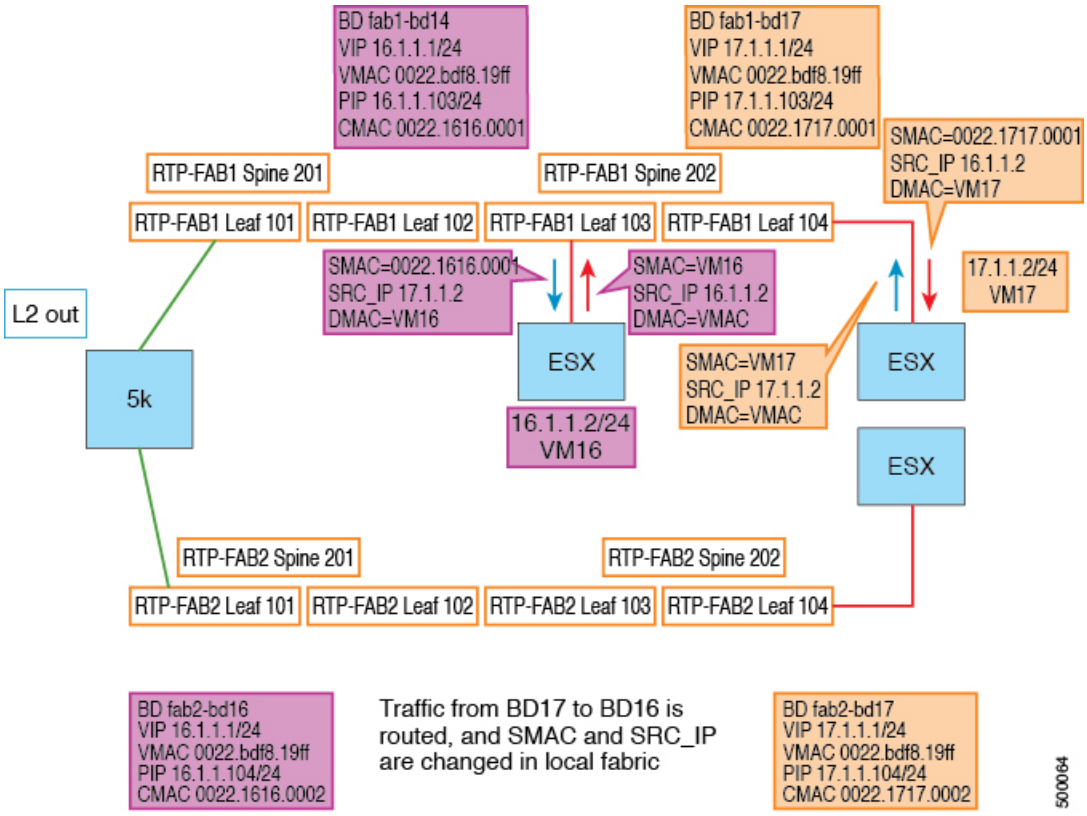
ルーテッドパケットにはCMACをSMACとして使用し、ARPグリーニングおよびエンドポイントトラッキングには2番目のIPを使用します。これについては後で説明します。



上の図では、BD16 および BD17 が上のファブリックと下のファブリックで複製されていることを確認できます。ブリッジ ドメイン設定に PIP と CMAC が追加されているのが確認できますが、これらはファブリック間で異なります。一方、VIP と VMAC はファブリック間で同じです。

パケット フローを見ると、VM17 は VM16 にパケットを送信します。下のファブリックの BD17 は、下のファブリックの BD16 にパケットをルーティングします。下のファブリックの BD16 は、VM16 にフレームを転送する際、SMAC として設定済みの CMAC を使用します。N5K は、下のファブリックから MAC 0022.1616.0002 を学習します。上のファブリックの VM16 が応答すると、同じことが上のファブリックで発生します。上のファブリックの BD17 は、レイヤ 2 アウトを終了する際、パケットの SMAC として設定済み CMAC を使用します。ここで、N5K は、上のファブリックから MAC 0022.1717.0001 を学習します。ブリッジ ドメイン間でルーティングされたパケットが通過する際に、Nexus 5K はもはや MAC フラップを参照しません。

ここで注目するべきことは、VM17 が上のファブリックに移動し、VM16 が上のファブリック上に残っていても、ブリッジ ドメインは、ルーテッド パケットをエンドポイントに転送する際に、設定済み CMAC を SMAC として使用し続けることです。



LINUX ホストとして VM17 を使用する場合は、TCPDUMP を使用して、VM16 へのパケットの MAC アドレスが VMAC に移り、そのリターン トラフィックが CMAC により受信されるのを確認できます。

```
[root@localhost ~]# ping 16.1.1.2
PING 16.1.1.2 (16.1.1.2) 56(84) bytes of data.
64 bytes from 16.1.1.2: icmp_seq=1 ttl=64 time=0.332 ms
64 bytes from 16.1.1.2: icmp_seq=2 ttl=64 time=0.376 ms
64 bytes from 16.1.1.2: icmp_seq=3 ttl=64 time=0.383 ms

--- 16.1.1.2 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.332/0.363/0.383/0.031 ms
[root@localhost ~]#

[root@localhost ~]# tcpdump -e -i eth1 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 96 bytes
04:06:59.130801 00:50:56:bb:a1:03 > 00:22:bd:f8:19:ff, ethertype IPv4
  (0x0800), length 98: 17.1.1.2 > 16.1.1.2: ICMP echo request, id 9583,
  seq 8796, length 64
04:06:59.131095 00:22:17:17:00:01 > 00:50:56:bb:a1:03, ethertype IPv4
  (0x0800), length 98: 16.1.1.2 > 17.1.1.2: ICMP echo reply, id 9583,
  seq 8796, length 64
04:07:00.131368 00:50:56:bb:a1:03 > 00:22:bd:f8:19:ff, ethertype IPv4
  (0x0800), length 98: 17.1.1.2 > 16.1.1.2: ICMP echo request, id 9583,
  seq 8797, length 64
04:07:00.131669 00:22:17:17:00:01 > 00:50:56:bb:a1:03, ethertype IPv4
  (0x0800), length 98: 16.1.1.2 > 17.1.1.2: ICMP echo reply, id 9583,
  seq 8797, length 64
```

```
04:07:01.131915 00:50:56:bb:a1:03 > 00:22:bd:f8:19:ff, ethertype IPv4
  (0x0800), length 98: 17.1.1.2 > 16.1.1.2: ICMP echo request, id 9583,
  seq 8798, length 64
04:07:01.132237 00:22:17:17:00:01 > 00:50:56:bb:a1:03, ethertype IPv4
  (0x0800), length 98: 16.1.1.2 > 17.1.1.2: ICMP echo reply, id 9583,
  seq 8798, length 64

6 packets captured
6 packets received by filter
0 packets dropped by kernel
[root@localhost ~]#
```

–e スイッチで **tcpdump** コマンドを使用する場合は、17.1.1.2 から 16.1.1.2 への PING が PING 要求で VMAC を SMAC として使用するのを確認でき、PING 応答は、エンドポイントが置かれた BD で設定されている CMAC から確認できます。

最初のハイライト表示された一連の文字は、BD17 の設定済み VMAC に送信される ICMP エコー要求（PING）を表します。2 つ目のハイライト表示された一連の文字は、BD17 の設定済み CMAC（VMAC ではなく）により受信された ICMP エコー応答を表します。

各ファブリックは、30 秒ごと（デフォルト）に、VIP および VMAC から送信された GARP を送信します。これらの GARP は低レートであるため、レイヤ 2 ネットワークの問題が発生することはありません。Nexus 5000 の **debug ip arp packet** コマンドを使用して、周波数を確認することができます。

```
2015 Oct 28 12:05:31.711090arp: (context 1) Receiving packet from Vlan2330,
  logical interface Vlan2330 physical interface Ethernet1/23, (prty 1) Hrd
  type 1 Prot type 800 Hrd len 6 Prot len 4 OP 1,  Pkt size 46
2015 Oct 28 12:05:31.711940 arp: Src 0022.bdf8.19ff/17.1.1.1 Dst
  ffff.ffff.ffff/17.1.1.1
2015 Oct 28 12:05:31.713557 arp: (context 1) Receiving packet from Vlan2331,
  logical interface Vlan2331 physical interface Ethernet1/23, (prty 1) Hrd
  type 1 Prot type 800 Hrd len 6 Prot len 4 OP 1,  Pkt size 46
2015 Oct 28 12:05:31.714382 arp: Src 0022.bdf8.19ff/16.1.1.1 Dst
  ffff.ffff.ffff/16.1.1.1
2015 Oct 28 12:06:01.717761 arp: (context 1) Receiving packet from Vlan2330,
  logical interface Vlan2330 physical interface Ethernet1/23, (prty 1) Hrd
  type 1 Prot type 800 Hrd len 6 Prot len 4 OP 1,  Pkt size 46
2015 Oct 28 12:06:01.718607 arp: Src 0022.bdf8.19ff/17.1.1.1 Dst
  ffff.ffff.ffff/17.1.1.1
2015 Oct 28 12:06:01.720627 arp: (context 1) Receiving packet from Vlan2331,
  logical interface Vlan2331 physical interface Ethernet1/23, (prty 1) Hrd
  type 1 Prot type 800 Hrd len 6 Prot len 4 OP 1,  Pkt size 46
2015 Oct 28 12:06:01.721457 arp: Src 0022.bdf8.19ff/16.1.1.1 Dst
  ffff.ffff.ffff/16.1.1.1
```

使用中のブリッジ ドメインで設定された 2 番目の IP アドレスを使用します。上の例では、BD17 は L2 out により EP 17.1.1.230 を学習しています。

次の出力例は、トポロジにおける Nexus 5000 での **debug ip arp packet** コマンドによるものです。BD17 PIP と CMAC がエンドポイント トラッキングを実行しているのを確認できます。フレームは、設定済みの BD17 PIP および CMAC を使用して ACI リーフから送信されて、エンドポイント 17.1.1.1 がレイヤ 2 エンドポイント グループ上にまだ保持されていることを確認します。

```
2015 Oct 28 12:05:31.711090arp: (context 1) Receiving packet from Vlan2330,
  logical interface Vlan2330 physical interface Ethernet1/23, (prty 1) Hrd
  type 1 Prot type 800 Hrd len 6 Prot len 4 OP 1,  Pkt size 46
2015 Oct 28 12:05:31.711940 arp: Src 0022.bdf8.19ff/17.1.1.1 Dst
  ffff.ffff.ffff/17.1.1.1
```

```
2015 Oct 28 12:05:31.713557 arp: (context 1) Receiving packet from Vlan2331,
  logical interface Vlan2331 physical interface Ethernet1/23, (prty 1) Hrd
  type 1 Prot type 800 Hrd len 6 Prot len 4 OP 1,  Pkt size 46
2015 Oct 28 12:05:31.714382 arp: Src 0022.bdf8.19ff/16.1.1.1 Dst
  ffff.ffff.ffff/16.1.1.1
2015 Oct 28 12:06:01.717761 arp: (context 1) Receiving packet from Vlan2330,
  logical interface Vlan2330 physical interface Ethernet1/23, (prty 1) Hrd
  type 1 Prot type 800 Hrd len 6 Prot len 4 OP 1,  Pkt size 46
2015 Oct 28 12:06:01.718607 arp: Src 0022.bdf8.19ff/17.1.1.1 Dst
  ffff.ffff.ffff/17.1.1.1
2015 Oct 28 12:06:01.720627 arp: (context 1) Receiving packet from Vlan2331,
  logical interface Vlan2331 physical interface Ethernet1/23, (prty 1) Hrd
  type 1 Prot type 800 Hrd len 6 Prot len 4 OP 1,  Pkt size 46
2015 Oct 28 12:06:01.721457 arp: Src 0022.bdf8.19ff/16.1.1.1 Dst
  ffff.ffff.ffff/16.1.1.1
```

GUI を使用した共通パーベイシブ ゲートウェイを備えたデュアル ファブリックの設定

次の手順は、このユースケースに対し、GUIを使用して共通パーベイシブ ゲートウェイによってデュアル ファブリックを設定す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、**[Tenants]** > **[ALL TENANTS]** の順に選択します。

ステップ 2 [Work] ペインで、[Tenant_Name] をダブルクリックします。

ステップ 3 ナビゲーション ウィンドウで、***[Tenant_Name]*** > **[Networking]** > **[Bridge Domains]** > ***[BD_name]*** の順に選択します。

ステップ 4 [Work] ペインで、[Properties] に次の値を設定します。

a) [L2 Unknown Unicast] ボタンでは [Flood] をクリックします。

b) [L3 Unknown Multicast Flooding] ボタンでは [Flood] をクリックします。

c) [Multi Destination Flooding] ボタンでは、[Flood in BD] をクリックします。

ステップ 5 [L3 Configurations] タブを選択します。

ステップ 6 [Work] ペインで、[Properties] に次の値を設定します。

a) [Custom MAC Address] フィールドには、ブリッジ ドメインのカスタム MAC アドレスを入力します。

カスタム MAC アドレスは、ファブリック間で異なる必要があります。

b) [Virtual MAC Address] フィールドには、ブリッジ ドメインの仮想 MAC アドレスを入力します。

仮想 MAC アドレスは、ファブリックの間で一致している必要があります。

ステップ 7 [Submit] をクリックします。`

ステップ 8 ナビゲーション ウィンドウで、***[Tenant_Name]*** > **[Networking]** > **[Bridge Domains]** > ***[BD_name]*** > **[Subnets]** > ***[Subnet_IP]*** の順に選択します。

ステップ 9 [Work] ペインで、[Treat as virtual IP address] ボックスにチェックマークを付けてください。

これで、VIP（仮想 IP アドレス）としてブリッジ ドメインのゲートウェイ IP アドレスが設定されます。

また、[Subnets] フォルダの下も、ARP グリーニングおよびエンドポイント トラッキングに使用される 16.1.1.103 アドレスです。このアドレスは、ファブリック全体でブリッジ ドメインで一意である必要があります。

ステップ 10 ファブリック間でミラーリングされる各ブリッジ ドメインに対してステップ 3 ～ 9 を繰り返します。