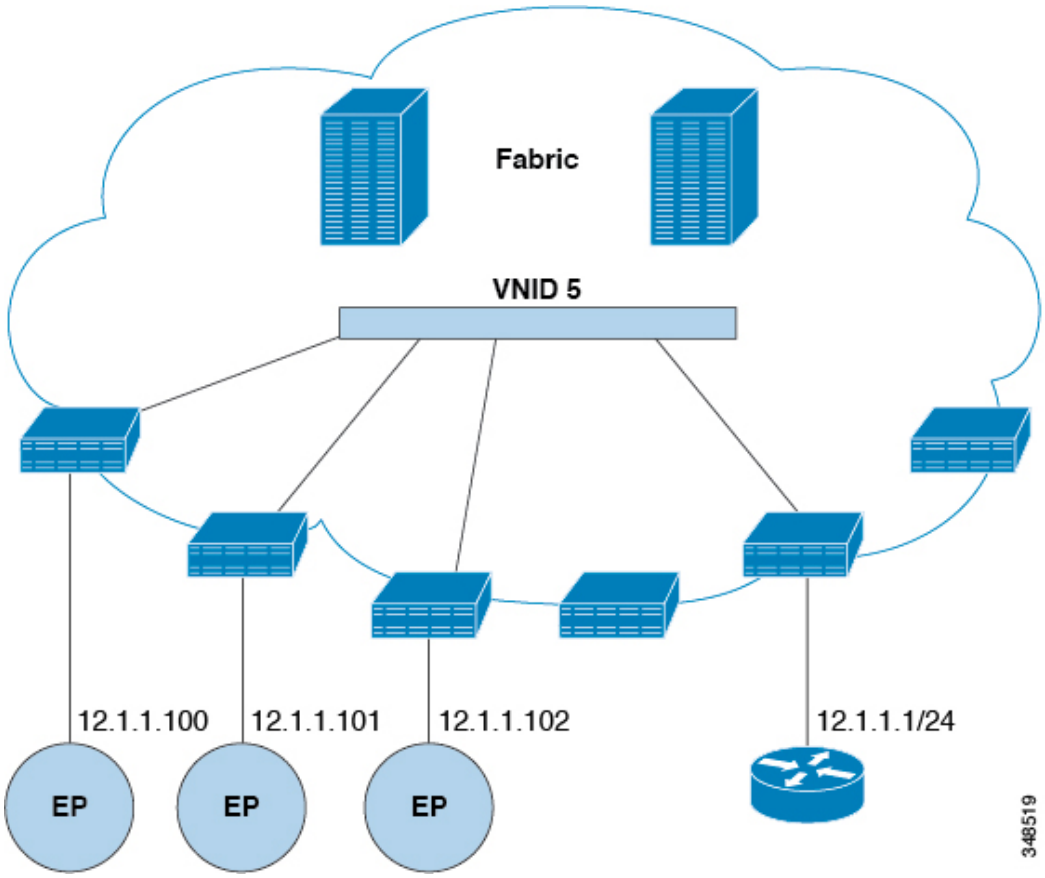
ブリッジング

この章は、次の内容で構成されています。

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 *1:* ブリッジド外部ルータ

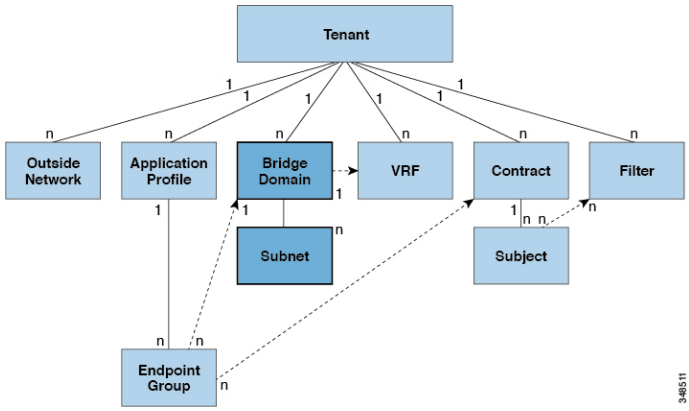


ACI ファブリックは、外部ルータの存在を認識せず、APIC はリーフ スイッチのインターフェイスを EPG に静的に割り当てます。

ブリッジ ドメインとサブネット

ブリッジ ドメイン（`fvBD`）は、ファブリック内のレイヤ 2 フォワーディングの構造を表します。次の図は、管理情報ツリー（MIT）内のブリッジ ドメイン (BD) の場所とテナントの他のオブジェクトとの関係を示します。

図 *2:* ブリッジ ドメイン



BD は、VRF (コンテキストまたはプライベート ネットワークとも呼ばれる) にリンクする必要があります。レイヤ 2 VLAN を除いて、少なくとも 1 つのサブネット（`fvSubnet`）が関連付けられている必要があります。BDは、このようなフラッディングが有効の場合に、一意のレイヤ 2 MAC アドレス空間およびレイヤ 2 フラッド ドメインを定義します。VRF が一意の IP アドレス空間を定義する一方で、そのアドレス空間は複数のサブネットで構成できます。これらのサブネットは、対応する VRF を参照する 1 つ以上のブリッジ ドメインで定義されます。

BD下または EPG 下のサブネットのオプションは次のとおりです:

- *Public*：サブネットをルーテッド接続にエクスポートできます。
- *Private*：サブネットはテナント内にのみ適用されます。
- *Shared*：共有サービスの一部として、同じテナントまたは他のテナントにわたる複数の VRF に対してサブネットの共有やエクスポートを行うことができます。共有サービスの例としては、異なるテナントの別の VRF に存在する EPG へのルーテッド接続などがあります。これにより、トラフィックが VRF 間で双方向に移動することが可能になります。共有サービスを提供する EPG のサブネットは （BD 下ではなく） その EPG 下で設定する必要があり、そのスコープは外部的にアドバタイズされ、VRF 間共有されるのように設定する必要があります。

（注） 共有サブネットは、通信に含まれる VRF 全体で一意でなければなりません。EPG 下のサブネットがレイヤ 3 外部ネットワーク共有サービスを提供する場合、このようなサブネットは、ACI ファブリック内全体でグローバルに一意である必要があります。

BD パケットの動作は次の方法で制御できます:

パケット タイプ	モード
ARP	**ARP フラッディング**は有効または無効にできます。フラッディングを行わない場合、ARP パケットはユニキャストで送信されます。 （注） `limitIpLearnToSubnets` を `fvBD` で設定すると、BD の設定済みサブネット内または共有サービス プロバイダーである EPG サブネット内に IP アドレスが存在する場合のみ、エンドポイントの学習が BD に限定されます。
未知のユニキャスト	**L2 Unknown Unicast** は、**Flood** または **Hardware Proxy** になり得ます。 （注） BD が **L2 Unknown Unicast** を持っており、それが **Flood** に設定されている場合、エンドポイントが削除されると、システムはそれを両方のローカル リーフ スイッチから削除します。そして、**Clear Remote MAC Entries** を選択すると、BD が展開されているリモートのリーフ スイッチからも削除されます。この機能を使用しない場合、リモート リーフは、タイマーが時間切れになるまで、学習したこのエンドポイントの情報を保持します。 **L2 Unknown Unicast** の設定を変更すると、このブリッジ ドメインに関連付けられた EPG にアタッチされているデバイスのインターフェイス上で、トラフィックがバウンスします (アップ ダウンします)。

パケット タイプ	モード
未知の IP マルチキャスト	**L3 の不明なマルチキャスト フラッディング** **Flood** — パケットは入力および境界リーフ スイッチノードでのみフラッディングされます。N9K-93180YC-EX では、パケットは、ブリッジ ドメインが導入されているすべてのノードでフラッディングされます。 **Optimized** — 1 リーフあたり 50 のブリッジ ドメインのみサポートされます。この制限は N9K-93180YC-EX には該当しません。
L2 マルチキャスト、ブロードキャスト、ユニキャスト	**マルチ宛先フラッディング**、次のいずれかになり得ます。 • **Flood in BD** — ブリッジ ドメインにフラッドします。 • **Flood in Encapsulation** — カプセル化でフラッドします。 • **Drop** — パケットをドロップします。

（注） Cisco APIC リリース 3.1(1) 以降では、Cisco Nexus 9000 シリーズ スイッチで (EX と FX で終わる名前を持つものとそれ以降)、次のプロトコルのカプセル化のフラッディングまたはブリッジ ドメインにフラッディングが可能です。OSPF/OSPFv3、BGP、EIGRP、CDP、LACP、LLDP、ISIS、IGMP、PIM、ST-BPDU、ARP/GARP、RARP、ND。

ブリッジ ドメインは複数のスイッチにまたがることができます。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が、サブネットは単一のブリッジ ドメイン内に含まれます。ブリッジ ドメイン（fvBD）の `limitIPLearnToSubnets` プロパティが `yes` に設定されていると、ブリッジ ドメインの設定済みサブネットのいずれかの中に IP アドレスがあるとき、または EPG が共有サービス プロバイダーである場合には EPG サブネット内に IP アドレスがあるときのみ、ブリッジ ドメイン内でエンドポイントの学習が行われます。サブネットは複数の EPG にまたがることができ、1 つ以上の EPG を 1 つのブリッジ ドメインまたはサブネットに関連付けることができます。ハードウェアのプロキシ モードでは、異なるブリッジ ドメインのエンドポイントがレイヤ 3 のルックアップ動作の一部として学習されると、そのエンドポイントに ARP トラフィックが転送されます。

ブリッジ ドメイン オプション

ブリッジ ドメインは、不明なユニキャスト フレームのフラッド モードで、またはこれらのフレームのフラッディングを排除する最適化されたモードで動作するように設定できます。フ

ラッディング モードで使用する場合、レイヤ 2 の不明なユニキャスト トラフィックはブリッジ ドメイン（GIP）のマルチキャスト ツリーでフラッディングされます。最適化されたモードでブリッジ ドメインを動作するようにするには、ハードウェア プロキシに設定する必要があります。この状況では、レイヤ 2 の不明なユニキャスト フレームはスパイン プロキシ エニーキャスト VTEP アドレスに送信されます。

⚠

注意 不明なユニキャスト フラッディング モードから hw プロキシ モードに変更すると、ブリッジ ドメイン内のトラフィックが停止します。

ブリッジ ドメインで IP ルーティングが有効になっている場合、マッピング データベースは、MAC アドレスだけでなく、エンドポイントの IP アドレスを学習します。

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を有効にすると、マッピングデータベースがこのブリッジドメインのエンドポイントに付与された IP アドレスと VTEP の対応関係を学習します。IP 学習は、ブリッジドメイン内にサブネットが構成されているかどうかに左右されません。
- **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。

拡張 L2 専用モード：レガシーモード

Cisco ACI では、VLAN が異なるリーフ ノードに展開されている限り、任意の目的で同じ VLAN ID を再利用できます。これにより、Cisco ACI ファブリックは、ファブリックとしての VLAN の理論上の最大数、4094 を超えることができます。ただし、これを実現するため、および基盤となる VxLAN 実装の複雑さを隠すために、個々のリーフノードに含めることのできる VLAN の数は少なくなります。このことは、リーフノードあたりの VLAN の密度が必要な場合に問題の原因となる可能性があります。このようなシナリオでは、ブリッジ ドメインで以前はレガシーモードと呼ばれていた、拡張 L2 専用モードを有効にできます。拡張 L2 専用モードのブリッジドメインでは、リーフノードごとに多数の VLAN を使用できます。ただし、このようなブリッジ ドメインにはいくつかの制限があります。

拡張 L2 専用モードとそれ以外のモードで、リーフ ノードごとにサポートされる VLAN またはブリッジ ドメインの数については、ご使用のリリースの Verified Scalability Guideを参照してください。

拡張 L2 専用モードの制限事項

レガシー モードまたは拡張 L2 専用モードの制限は次のとおりです。

- ブリッジ ドメインには、1 つの EPG と 1 つの VLAN のみを含めることができます。
- ユニキャスト ルーティングはサポートされていません。
- コントラクトはサポートされていません。
- VMM 統合のダイナミック VLAN 割り当てはサポートされていません。
- サービス グラフはサポートされていません。
- QoS ポリシーはサポートされていません。
- ブリッジ ドメインは、スタンドアロン Cisco NX-OS では基本的に VLAN として動作します。

拡張 L2 専用モードの設定

次に、拡張 L2 専用 モードでブリッジ ドメインを設定する際の考慮事項を示します。

- VLAN ID はブリッジドメインで設定されます。
- EPG で設定された VLAN ID は上書きされます。
- 既存のブリッジ ドメインで拡張 L2 専用モードの有効と無効を切り替えると、サービスに影響します。

  VLAN API が変更前に使用されていたものと異なる場合、Cisco APIC は自動的にブリッジドメインの展開解除と再展開を行います。

  モード変更の前後で同じ VLAN ID が使用された場合、Cisco APIC はブリッジ ドメインの自動的な展開解除と再展開は行いません。手動でブリッジドメインを展開解除して再展開する必要があります。これは、 EPG で静的ポート設定を削除して再作成することで実行できます。

- 拡張 L2 専用モードの VLAN ID を変更する場合は、まずモードを無効にしてから、新しい VLAN ID で拡張 L2 専用モードを有効にする必要があります。

ブリッジ ドメインごとの IP 学習の無効化

2 つのホストが Cisco ACI スイッチにアクティブおよびスタンバイのホストとして接続されている場合、ブリッジ ドメインごとの IP 学習は無効になります。MAC 学習は引き続きハードウェアで発生しますが、IP 学習は ARP/GARP/ND プロセスからのみ発生します。この機能は、ファイアウォールまたはローカル ゲートウェイのような、柔軟な導入を可能にします。

ブリッジ ドメインごとに IP 学習を無効化するには、次の注意事項と制限事項を参照してください。

- remote top-of-rack（ToR）スイッチで送信元 IP アドレスが S,G 情報を入力するように学習していないため、レイヤ 3 マルチキャストはサポートされていません。
- DL ビットが iVXLAN ヘッダーで設定されているため、MAC アドレスはリモート TOR のデータ パスから学習されません。BD が展開されているファブリックで、リモート TOR からすべての TOR に不明なユニキャスト トラフィックをフラッディングします。エンドポイント データプレーン ラーニングが無効になっている場合は、この状況を克服するようにプロキシ モードで BD を設定することをお勧めします。
- ARP がフラッド モードであり、GARP ベースの検出を有効にする必要があります。
- IP ラーニングを無効にすると、対応する VRF でレイヤ 3 エンドポイントがフラッシュされません。同じ TOR を永遠に指すエンドポイントになる可能性があります。この問題を解決するには、すべての TOR のこの VRF 内ですべてのリモート IP エンドポイントをフラッシュします。

BD の設定を変更して、データプレーン学習を無効にしても、以前にローカルに学習したエンドポイントはフラッシュされません。これにより、既存のトラフィック フロー中断の影響は限られます。Cisco ACI リーフが特定の送信元 MAC を持つトラフィックをエンド ポイント保持ポリシーよりも長く見ない場合、MAC が学習したエンドポイントは通常どおりエージングします。

（注） IP データプレーン ラーニングを無効にすると、トラフィック転送の結果としてエンドポイント IP 情報が更新されることはなくなりますが、Cisco ACI は ARP/ND を使用してエンドポイント IP 情報を更新できます。つまり、ローカル エンドポイントのエージング（設定変更前に学習されたか、設定変更後に学習されたか）は、通常のエージングとは若干異なり、[システム (System)] > [システム設定 (System Settings)] > [エンドポイント制御 (Endpoint Controls)] > [IP エージング (IP Aging)] にも依存します。

IP エージングが無効の場合、すでに学習されたエンドポイント MAC と一致する送信元 MAC からのトラフィックは、エンドポイントテーブルの MAC アドレス情報を更新し、その結果、IP 情報も更新します（これは IP データプレーンの学習が有効になっている場合と同じです）。

IP エージングが有効の場合、ACI はエンドポイント IP アドレスを個別にエージング アウトします（これは IP データプレーン ラーニングが有効になっている場合と同じです）が、すでに学習したエンドポイントとマッチする既知の送信元 MAC および IP からのトラフィックにより、エンドポイント テーブルの MAC アドレス情報は更新されるのに対し、IP 情報は更新されないという点で、IP データプレーン ラーニングを有効にした設定とは異なります。

GUI を使用したテナント、VRF およびブリッジ ドメインの作成

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。

手順

ステップ 1 メニュー バーで、**[テナント（Tenants）]** > **[テナントの追加（Add Tenant）]** を選択します。

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) **[セキュリティ ドメイン（Security Domains）]** セクションで、**[+]** をクリックして、**[セキュリティ ドメインの作成（Create Security Domain）]** ダイアログ ボックスを開きます。

c) **[名前（Name）]** フィールドに、セキュリティ ドメインの名前を入力し、**[送信（Submit）]** をクリックします。

d) **[テナントの作成（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 **[更新（Update）]** をクリックします。

e) 必要に応じて他のフィールドに入力します。

f) [送信（Submit）] をクリックします。

テナント名 > **[ネットワーキング（Networking）]**画面が表示されます。

ステップ 3 **[作業（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) 必要に応じて他のフィールドに入力します。

c) **[送信（Submit）]** をクリックして VRF インスタンスの設定を完了します。

ステップ 4 **[作業（Work）]** ペインで、VRF インスタンスを囲む円内のキャンバスに **[ブリッジ ドメイン（Brdige Domain）]** アイコンをドラッグして、2 つを接続します。[Create Bridge Domain] ダイアログボックスが表示されたら、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) 必要に応じて他のフィールドに入力します。

c) [次へ（Next）] をクリックします。

d) **[サブネット（Subnets）]** セクションで、**[+]** をクリックして、**[サブネットの作成（Create Subnet）]** ダイアログ ボックスを開きます。

e) **[ゲートウェイ IP**（Gateway IP）] フィールドに、IP アドレスとサブネット マスクを入力します。

f) 必要に応じて他のフィールドに入力します。

g) [OK] をクリックします。

h) **[ブリッジ ドメインの作成（Create Bridge Domain）]** ダイアログ ボックスに戻り、必要に応じて他のフィールドに入力します。
i) [次へ（Next）] をクリックします。
j) 必要に応じてフィールドに入力します。
k) **[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。

ステップ 5 **[作業（Work）]** ペインで、VRF インスタンスを囲む円内のキャンバスに **[L3]** アイコンをドラッグして、2 つを接続します。[Create Routed Outside] ダイアログボックスが表示されたら、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) **[ノードとインターフェイス プロトコル プロファイル（Nodes And Interfaces Protocol Profiles]** セクションで、**[+]** をクリックして **[ノード プロファイルの作成（Create Node Profile）]** ダイアログ ボックスを開きます。
c) [Name] フィールドに、名前を入力します。
d) **[ノード（Nodes）]** セクションで、**[+]** をクリックして **[ノードの選択（Select Node）]** ダイアログ ボックスを開きます。
e) **[ノード ID（Node ID）]** ドロップダウン リストから、ノードを選択します。
f) [Router ID] フィールドに、ルータ ID を入力します。
g) **[スタティック ルート（Static Routes）]** セクションで、**[+]** をクリックして**[スタティック ルートの作成（Create Static Routes）]** ダイアログ ボックスを開きます。
h) [Prefix] フィールドに、IPv4 アドレスまたは IPv6 アドレスを入力します。
i) **[ネクスト ホップ アドレス（Next Hop Addresses）]** セクションで、**[+]** をクリックして **[ネクスト ホップの作成（Create Next Hop）]** ダイアログ ボックスを開きます。
j) **[ネクスト ホップ アドレス（Next Hop Addresses）]** フィールドを展開し、IPv4 アドレスまたは IPv6 アドレスを入力します。
k) **[設定（Preference）]** フィールドに、数値を入力します。
l) 必要に応じて他のフィールドに入力します。
m) [OK] をクリックします。
n) **[静的ルートの作成（Create Static Route）]** ダイアログ ボックスで、必要に応じて他のフィールドに入力します。
o) [OK] をクリックします。
p) **[ノードの選択（Select Node）]** ダイアログ ボックスで、必要に応じて他のフィールドに入力します。
q) [OK] をクリックします。
r) **[ノード プロファイルの作成（Create Node Profile）]** ダイアログ ボックスで、必要に応じて他のフィールドに入力します。
s) [OK] をクリックします。
t) 必要に応じて **[BGP]**、**[OSPF]**、または **[EIGRP]** チェックボックスをオンにします。
u) 必要に応じて他のフィールドに入力します。
v) [次へ（Next）] をクリックします。
w) 必要に応じてフィールドに入力します。
x) **[OK]** をクリックしてレイヤ 3 の設定を完了します。

レイヤ 3 の設定を確認するには、**[ナビゲーション（Navigation）]** ペインで、**[ネットワーキング（Networking）]** > **[VRF]**の順に展開します。

NX-OS CLI を使用した、テナント、VRF およびブリッジ ドメインの作成

ここでは、テナント、VRF およびブリッジ ドメインを作成する方法を説明します。

（注） テナントの設定を作成する前に、vlan-domain コマンドを使用して VLAN ドメインを作成し、ポートを割り当てる必要があります。

手順

ステップ 1 次のように、VLAN ドメイン（一連のポートで許可される一連の VLAN を含む）を作成し、VLAN の入力を割り当てます。

例：

次の例（exampleCorp）では、VLAN 50 ～ 500 が割り当てられることに注意してください。

```
apic1# configure
apic1(config)# vlan-domain dom_exampleCorp
apic1(config-vlan)# vlan 50-500
apic1(config-vlan)# exit
```

ステップ 2 VLAN が割り当てられたら、これらの VLAN を使用できるリーフ（スイッチ）およびインターフェイスを指定します。次に、「vlan-domain member」と入力し、その後に作成したドメインの名前を入力します。

例：

次の例では、これらの VLAN（50 ～ 500）は、インターフェイス イーサネット 1/2 ～ 4（1/2、1/3、1/4 を含む 3 つのポート）上の leaf 101 で有効になっています。これは、このインターフェイスを使用すると、VLAN を使用できるあらゆるアプリケーションにこのポートの VLAN 50 ～ 500 を使用できることを意味します。

```
apic1(config-vlan)# leaf 101
apic1(config-vlan)# interface ethernet 1/2-4
apic1(config-leaf-if)# vlan-domain member dom_exampleCorp
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

ステップ 3 次の例に示すように、グローバル コンフィギュレーション モードでテナントを作成します。

例：

```
apic1(config)# tenant exampleCorp
```

ステップ 4 次の例に示すように、テナント コンフィギュレーション モードでプライベート ネットワーク（VRF とも呼ばれます）を作成します。

例：

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

ステップ 5 次の例に示すように、テナントの下にブリッジ ドメイン（BD）を作成します。

例：

```
apic1(config-tenant)# bridge-domain exampleCorp_b1
apic1(config-tenant-bd)# vrf member exampleCorp_v1
apic1(config-tenant-bd)# exit
```

（注） この場合、VRF は「exampleCorp_v1」です。

ステップ 6 次の例に示すように、BD の IP アドレス（IP および ipv6）を割り当てます。

例：

```
apic1(config-tenant)# interface bridge-domain exampleCorp_b1
apic1(config-tenant-interface)# ip address 172.1.1.1/24
apic1(config-tenant-interface)# ipv6 address 2001:1:1::1/64
apic1(config-tenant-interface)# exit
```

次のタスク

次の項では、アプリケーション プロファイルを追加し、アプリケーション エンドポイント グループ（EPG）を作成し、EPG をブリッジ ドメインに関連付ける方法について説明します。

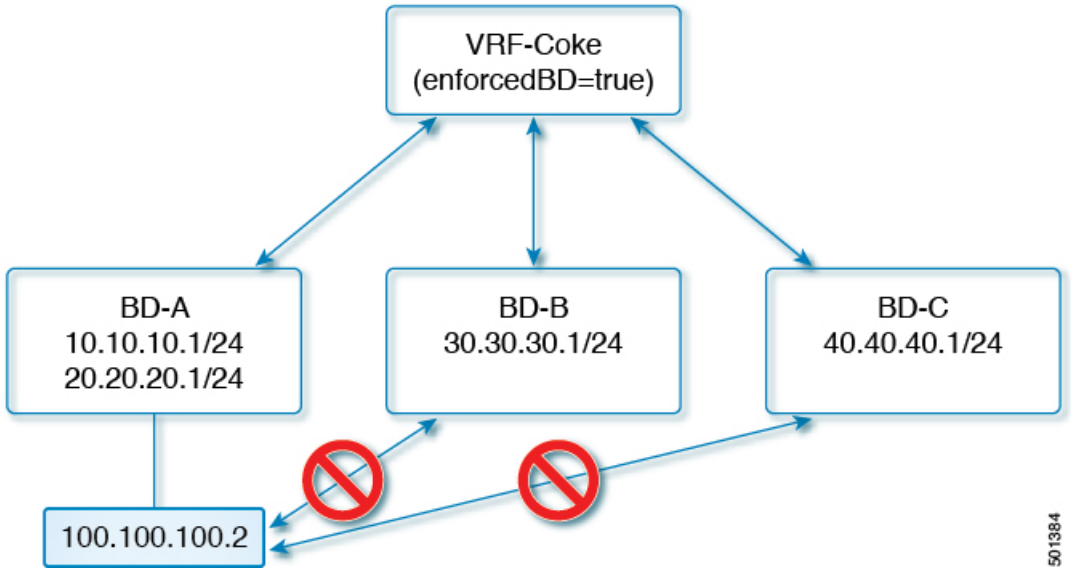
関連トピック

NX-OS スタイルの CLI を使用した VLAN ドメインの設定

適用されるブリッジ ドメインの設定

適用ブリッジ ドメインでは、関連付けられたブリッジ ドメイン内のサブネット ゲートウェイにしか ping を送信できない、対象のエンド ポイント グループ（EPG）内に、1 つのエンドポイントが作成されます。この設定を使用すると、任意のサブネットゲートウェイに ping を送信できる IP アドレスのグローバル例外リストを作成できます。

図 *3*: 適用されるブリッジ ドメイン



（注）

- 例外 IP アドレスは、すべての VRF インスタンスのすべてのブリッジ ドメイン ゲートウェイに ping を送信できます。
- L3Out 用に設定されたループバック インターフェイスでは、対象のループバック インターフェイスに合わせて設定された IP アドレスへの到達可能性は適用されません。
- eBGP ピアとなる IP アドレスが、L3Out インターフェイスのサブネットとは異なるサブネットに存在している場合には、許容例外サブネットにピア サブネットを追加する必要があります。そうしないと、送信元 IP アドレスが L3Out インターフェイスのサブネットとは異なるサブネットに存在するため、eBGP トラフィックがブロックされます。
- BGP プレフィックスベース ピアの場合は、許容例外サブネットのリストにピア サブネットを追加する必要があります。たとえば、20.1.1.0/24 が BGP プレフィックスベース ピアとして構成されている場合は、許容例外サブネットのリストに 20.1.1.0/24 を追加する必要があります。
- 適用ブリッジ ドメインは、VRFインスタンスがインバンドまたはアウトオブバンドであるかどうかにかかわらず、管理テナントではサポートされません。これらのVRFインスタンスへのトラフィックを制御するルールは、通常のコントラクトを使用して設定する必要があります。

NX-OS スタイル CLI を使用した適用されるブリッジ ドメインの設定

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、適用されるブリッジ ドメインを設定する方法について説明します。

手順

ステップ 1 テナントを作成し有効にします。

例：

次の例 (「cokeVrf」) が作成され有効になっています。

```
apic1(config-tenant)# vrf context cokeVrf
apic1(config-tenant-vrf)# bd-enforce enable
apic1(config-tenant-vrf)# exit
apic1(config-tenant)#exit
```

ステップ 2 例外リストに、サブネットを追加します。

例：

```
apic1(config)#bd-enf-exp-ip add1.2.3.4/24
apic1(config)#exit
```

適用されるブリッジドメインは次のようなコマンドを使用して動作可能かどうかを確認できます。

```
apic1# show running-config all | grep bd-enf
bd-enforce enable
bd-enf-exp-ip add 1.2.3.4/24
```

例

次のコマンドでは、除外リストからサブネットを削除します。

```
apic1(config)# no bd-enf-exp-ip 1.2.3.4/24
apic1(config)#tenant coke
apic1(config-tenant)#vrf context cokeVrf
```

次のタスク

適用されるブリッジ ドメインを無効にするには、次のコマンドを実行します。

```
apic1(config-tenant-vrf)# no bd-enforce enable
```

カプセル化によるすべてのプロトコルおよびプロキシ ARP のカプセル化のフラッディングを設定する

Cisco Application Centric Infrastructure（ACI）は、ブリッジ ドメインをレイヤ 2 ブロードキャスト境界として使用します。各ブリッジ ドメインには複数のエンドポイント グループ（EPG）

を含めることができ、各 EPG は複数の仮想ドメインまたは物理ドメインにマッピングできます。各 EPG は、ドメインごとに異なる VLAN カプセル化プールを使用することもできます。各 EPG は、ドメインごとに異なる VLAN または VXLAN カプセル化プールを使用することもできます。

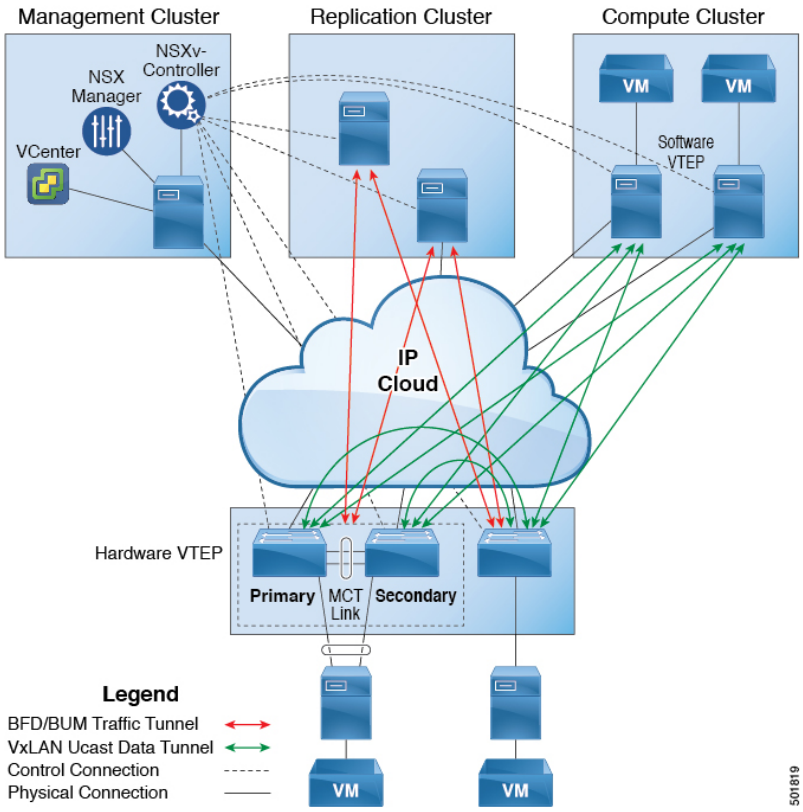
通常、ブリッジ ドメイン内に複数の EPG を配置すると、ブロードキャスト フラッディングはブリッジ ドメイン内のすべての EPG にトラフィックを送信します。EPG はエンドポイントをグループ化し、特定の機能を実行するためにトラフィックを管理するために使用されるものなので、ブリッジ ドメイン内のすべての EPG に同じトラフィックを送信することは必ずしも実用的ではありません。

カプセル化でのフラッディングは、ネットワーク内のブリッジ ドメインを統合するのに役立ちます。この機能は、EPG が関連付けられている仮想ドメインまたは物理ドメインのカプセル化に基づいて、ブリッジ ドメイン内のエンドポイントへのブロードキャスト フラッディングを制御できるようにするからです。

カプセル化でのフラッディングでは、同じブリッジ ドメインにおける異なる EPG のエンドポイント間の通信を許可するために、ブリッジ ドメインにサブネットと IP ルーティングを構成する必要があり、Cisco ACI がプロキシ ARP の役割を果たします。

トンネル モードで複数の VLAN を使用すると、いくつかの課題を導入できます。次の図に示すように、単一のトンネルでCisco ACIを使用する一般的な導入では、1 つのブリッジ ドメインの下に複数の EPG があります。この場合、特定のトラフィックがブリッジ ドメイン内（つまりすべての EPG 内）でフラッディングし、MAC アドレス学習があいまいになって転送エラーが発生するリスクがあります。

図 *4 : VLAN* トンネルモードの *Cisco ACI* の課題



このトポロジでは、ファブリックに、1つのアップリンクを使用してCisco ACIリーフノードに接続する単一のトンネルネットワークが定義されます。このリンクでは、2 人のユーザの VLAN、VLAN 10 と VLAN 11 が行われます。サーバーのゲートウェイが Cisco ACI クラウドの外部にあるため、ブリッジ ドメインはフラッディング モードに設定されます。次のプロセスで ARP 交渉が発生します。

- サーバは、VLAN 10 ネットワーク経由で 1 つの ARP ブロードキャスト要求を送信します。
- ARP パケットは、外部のサーバに向かってトンネル ネットワークを通過し、そのダウンリンクから学習した送信元 MAC アドレスを記録します。
- その後、サーバーはアップリンクからCisco ACIリーフスイッチにパケットを転送します。
- Cisco ACIファブリックは、アクセスポート VLAN 10に着信する ARP ブロードキャスト パケットを確認し、EPG1 にマッピングします。
- ブリッジ ドメインは ARP パケットをフラッディングするように設定されているため、パケットはブリッジ ドメイン内でフラッディングされます。したがって、両方の EPG が同じブリッジ ドメイン内にあるため、これらのポートにフラッディングされます。
- 同じ ARP ブロードキャスト パケットは、同じアップリンクで復帰します。
- 外部サーバは、このアップリンクから元の送信元 MAC アドレスを確認できます。

結果：外部デバイスは、単一 MAC 転送表内のダウンリンク ポートおよびアップリンク ポートの両方から同じ MAC デバイスを入手し、トラフィックの中断の原因となります。

推奨される解決策

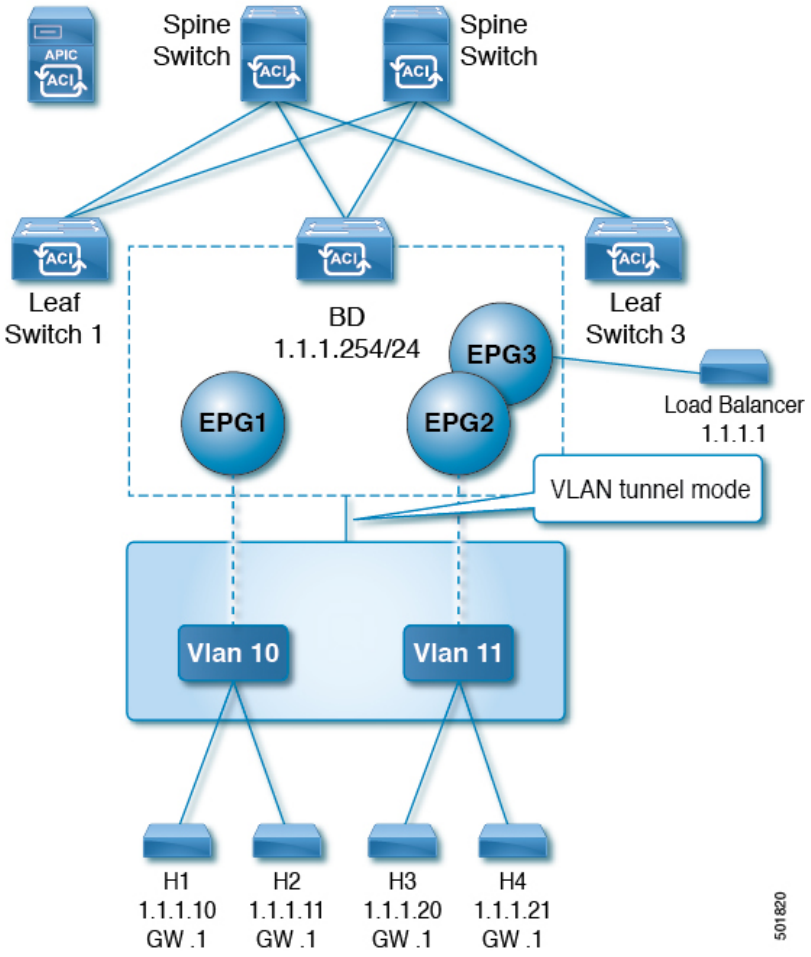
カプセル化内フラッディングは、ブリッジ ドメイン内のフラッディング トラフィックを単一のカプセル化に制限するために使用されます。2 つの EPG が同じブリッジ ドメインを共有し、**カプセル化内フラッディング**が有効になっている場合、EPGのフラッディング トラフィックは他の EPG に到達しません。

Cisco Application Policy Infrastructure Controller（APIC）リリース 3.1(1) 以降、Cisco Nexus 9000 シリーズスイッチ（名前の末尾が EX および FX 以降）では、すべてのプロトコルがカプセル化されます。VLAN 内部トラフィックに [Flood in Encapsulation] を有効にすると、プロキシ ARP でMAC フラップの問題が発生しておらず、カプセル化に対してすべてのフラッディング (ARP、GARP、BUNM) を制限します。これが有効になっていると、ブリッジ ドメインの下のすべての EPG に適用されます。

（注） Cisco APIC APIC リリース 3.1 (1) より前のリリースでは、これらの機能はサポートされていません（カプセル内でフラッディングするとき含まれるプロキシ ARP およびすべてのプロトコル）。Cisco APIC リリース以前の世代のスイッチ（名前に EX または FX が付かないもの）では、**カプセル化内フラッディング**を有効にしても機能せず、情報上の障害は発生しませんが、Cisco APIC は正常性スコアを 1 減らします。

推奨される解決策は、外部スイッチを追加して、1 つのブリッジ ドメインで複数の EPG をサポートすることです。外部のスイッチがある 1 つのブリッジ ドメイン下で複数の EPG を持つこの設計は、次の図に示されています。

図 *5*: 外部のスイッチがある *1* つのブリッジ ドメイン下で複数の *EPG* を持つ設計



同じブリッジ ドメイン内では、一部の EPG をサービス ノードにすることができ、他の EPG にはカプセル化でのフラッディングを設定できます。ロード バランサは、別の EPG 上にあります。ロードバランサは EPG からパケットを受信し、その他の EPG に送信します（プロキシ ARP はなく、カプセル化内フラッディングは発生しません）。

NX-OS スタイル CLI を使用して選択した EPG のみに対してカプセル化内フラッディングを追加する場合は、EPG 下で **flood-on-encapsulation enable** コマンドを入力します。

すべての EPG に対してカプセル化内フラッディングを追加する場合、ブリッジ ドメイン下で **multi-destination encap-flood** CLI コマンドを使用できます。

CLI を使用して、EPG に設定されるカプセルのフラッドが、ブリッジ ドメインに設定されているカプセルのフラッディングより優先されるようにします。

ブリッジ ドメインと EPG の両方が構成されている場合の動作は次のとおりです。

表 *1:* ブリッジ ドメインと *EPG* の両方が構成されている場合の動作

設定	動作
EPG でのカプセルのフラッディングとブリッジ ドメインでのカプセルのフラッディング	カプセルのフラッディングは、ブリッジ ドメイン内のすべての VLAN のトラフィックに行われます。
EPG でのカプセルのフラッディングが発生せずブリッジドメインでのカプセルのフラッディングが発生する	カプセルのフラッディングは、ブリッジ ドメイン内のすべての VLAN のトラフィックに行われます。
EPG でのカプセルのフラッディングが発生しブリッジ ドメインでのカプセルのフラッディングが発生しない	カプセルのフラッディングは、ブリッジ ドメインの EPG 内のすべての VLAN のトラフィックに行われます。
EPG でのカプセルのフラッディングが発生せずブリッジドメインでのカプセルのフラッディングも発生しない	ブリッジ ドメイン全体でフラッディングします。

マルチ宛先プロトコル トラフィック

EPG/ブリッジ ドメイン レベルのブロードキャスト セグメンテーションは、次のネットワーク制御プロトコルでサポートされます。

- OSPF
- EIGRP
- CDP
- LACP
- LLDP
- IS-IS
- BGP
- IGMP
- PIM
- STP BPDU（EPG 内フラッディング）
- ARP/GARP（ARP プロキシによって制御）
- ND

カプセル化でのフラッディングの制限事項

すべてのプロトコルのカプセル化でのフラッディングには、次の制限が適用されます。

- カプセルのフラッディングは、ARP ユニキャスト モードでは機能しません。

- ネイバー要請（NS/ND）は、このリリースではサポートされていません。
- カプセルのフラッディングでポートごとに CoPP を有効にする必要があります。
- カプセル化でのフラッディングは、フラッド モードのブリッジ ドメインおよびフラッド モードの ARP でのみサポートされます。ブリッジ ドメイン スパイン プロキシ モードはサポートされていません。
- IPv4 レイヤ 3 マルチキャストはサポートされていません。
- IPv6 はサポートされていません。
- 別の VLAN への仮想マシンの移行には、時間的な問題（60 秒）があります。
- たとえば、ゲートウェイとして機能するロードバランサは、仮想マシンと非プロキシモードのロードバランサ間の 1 対 1 通信でサポートされます。レイヤ 3 通信はサポートされません。仮想マシンとロードバランサ間のトラフィックは、レイヤ 2 です。ただし、内部 EPG 通信がロード バランサを通過する場合、ロード バランサが SIP および SMPC を変更します。さもなければ、 MAC フラップが発生する可能性があります。したがって、ダイナミック ソース ルーティング（DSR）モードは、ロード バランサでサポートされていません。
- 仮想マシンの IP アドレスを、ファイアウォールの IP アドレスではなく、ゲートウェイの IP アドレスに変更した場合、ファイアウォールはバイパスされため、ファイアウォールをゲートウェイにする仮想マシン間の通信設定は推奨されません。
- 以前のリリースではサポートされていません（以前と現在のリリース間の相互運用もサポートされていません）。
- 3.2(5) より前のリリースでは、プロキシ ARP およびカプセル化内フラッディング機能は、VXLAN カプセル化でサポートされません。
- アプリケーション リーフ エンジン（ALE）とアプリケーション スパイン エンジン（ASE）で混合モードのトポロジは推奨されておらず、カプセル化でフラッディングではサポートされていません。同時に有効にすると、QoS の優先順位が適用されるのを防ぐことができます。
- カプセル化のフラッディングは、リモート リーフ スイッチと Cisco ACI マルチサイト ではサポートされていません。
- カプセルのフラッディングは、一般的な拡散型ゲートウェイ（CPGW）ではサポートされていません。
- マイクロセグメンテーションが設定されている EPG では、カプセル化でのフラッディングはサポートされません。
- ブリッジ ドメインのすべてのEPGでカプセル化でのフラッディングを設定する場合は、ブリッジ ドメインでもカプセル化でのフラッディングを設定してください。
- IGMP スヌーピングは、カプセル化でのフラッディングではサポートされません。

- Cisco ACIにおいては、カプセル化でのフラッディングのために設定された EPG で受信されるパケットのフラッディングを、（カプセル化ではなく）ブリッジドメインで生じさせる条件が存在します。これは、管理者がカプセル化でのフラッディングを EPG で直接設定したか、ブリッジ ドメインで設定したかに関係なく発生します。この転送動作の条件は、入力リーフ ノードに宛先MACアドレスのリモートエンドポイントがあり、出力リーフ ノードに対応するローカル エンドポイントがない場合です。これは、インターフェイスのフラッピング、STP TCNによるエンドポイント フラッシュ、過剰な移動のためにブリッジ ドメインで学習が無効になっているなどの理由で発生する可能性があります。
- レイヤ 3 ゲートウェイは Cisco ACI ファブリック内にある必要があります。

カプセル化範囲限定のフラッディングの設定

NX-OS スタイルの CLI、REST API、またはCisco Application Policy Infrastructure Controller（APIC）GUI を使用して、カプセル化でフラッディングを設定します。

EPG に設定されたカプセル化のフラッディングは、ブリッジド メイン（BD）に設定されたカプセル化のフラッディングよりも優先されます。BD と EPG の両方を設定すると、動作は次に説明したようになります。

表 *2 : BD* と *EPG* の両方が設定されているときの動作

設定	動作
EPG でのカプセルのフラッディングとブリッジ ドメインでのカプセルのフラッディング	カプセル化のフラッディングは、ブリッジ ドメインのすべての VLAN および VXLAN 上のトラフィックに対して発生します。
EPG でのカプセルのフラッディングが発生せずブリッジドメインでのカプセルのフラッディングが発生する	カプセル化のフラッディングは、ブリッジ ドメイン内のすべての VLAN および VXLAN のトラフィックに対して発生します。
EPG でのカプセルのフラッディングが発生しブリッジ ドメインでのカプセルのフラッディングが発生しない	カプセル化のフラッディングは、ブリッジ ドメインの EPG 内のその VLAN または VXLAN のトラフィックに対して発生します。
EPG でのカプセルのフラッディングが発生せずブリッジドメインでのカプセルのフラッディングも発生しない	ブリッジ ドメイン全体でフラッディングします。

Cisco APIC GUI を使用したカプセル化範囲限定のフラッディングの設定

ブリッジドメイン（BD）またはエンドポイントグループ（EPG）を作成または変更する場合は、Cisco Application Policy Infrastructure Controller（APIC）GUIを使用してカプセル化でフラッディングを設定します。

手順

ステップ 1 BD の作成時にカプセル化でフラッディングを設定するには、次の手順を実行します。

a) Cisco APIC にログインします。
b) **[Tenants]** > ***[tenant]*** > **[Networking]** > **[Bridge Domains]** を選択します。
c) **Bridge Domains** を右クリックして、**Create Bridge Domain** を選択します。
d) 手順 1 の **[Create Bridge Domain]** ダイアログ ボックスで、**[Multi Destination Flooding]** ドロップダウン リストから、[Flood in Encapsulation] を選択します。
e) 設定に応じてダイアログボックスの他のフィールドに入力し、**[Finish]** をクリックします。

ステップ 2 BD の変更時にカプセル化でフラッディングを設定するには、次の手順を実行します。

a) Cisco APIC にログインします。
b) **[Tenants]** > ***<tenan>]*** > **[Networking]** > **[Bridge Domains]** > ***<bridge domain>*** を選択します。
c) BD の作業ウィンドウで、**[Policy]** タブを選択し、**[General]** タブを選択します。
d) **[Multi Destination Flooding]** 領域で、**[Flood in Encapsulation]** を選択します。
e) **[送信（Submit）]** をクリックします。`

ステップ 3 EPG の作成時にカプセル化でフラッディングを設定するには、次の手順を実行します。

a) Cisco APIC にログインします。
b) **[Tenants]** > ***<tenant>*** > **[Application Profiles]** に移動します。
c) **[Application Profiles]** を右クリックし、**[Create Application EPG]** を選択します。
d) **[Create Application EPG]** ダイアログボックスの **[Flood in Encapsulation]** 領域で、**[Enabled]** を選択します。

カプセル化のフラッディングはデフォルトで無効になっています。

e) 設定に応じてダイアログボックスの他のフィールドに入力し、**[Finish]** をクリックします。

ステップ 4 EPG の変更時にカプセル化でフラッディングを設定するには、次の手順を実行します。

a) **[Tenants]** > ***<tenant>*** > **[Application Profiles]** > **[Application EPG]** > ***<application EPG>*** に移動します。
b) EPG の作業ウィンドウで、**[Policy]** タブを選択し、**[General]** タブを選択します。
c) **[Flood in Encapsulation]** 領域で、**[Enabled]** を選択します。
d) [Submit] をクリックします。

NX-OS スタイル CLI を使用したカプセル化でのフラッディングの設定

NX-OS スタイル CLI を使用して選択したエンドポイント グループ（EPG）のみに対してカプセル化でフラッディングを追加する場合は、EPG 下で **flood-on-encapsulation enable** コマンドを入力します。

すべての EPG に対してカプセル化でフラッディングを追加する場合、ブリッジ ドメインに対して **multi-destination encap-flood** CLI コマンドを使用します。

手順

ステップ 1 ブリッジドメイン（BD）のカプセル化でフラッディングを設定します。

例：

```
APIC1#configure
APIC1(config)# tenant tenant
APIC1(config-tenant)# bridge-domain BD-name
APIC1(config-tenant-bd)# multi-destination encap-flood
APIC1(config-tenant)#exit
APIC1(config)#
```

ステップ 2 EPG のカプセル化でフラッディングを設定します。

例：

```
APIC1(config)# tenant tenant
APIC1(config-tenant)# application AP1
APIC1(config-tenant-app)# epg EPG-name
APIC1(config-tenant-app-epg)# flood-on-encapsulation
APIC1(config-tenant-app-epg)#no flood-on-encapsulation
```

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。