ACI ボーダー ゲートウェイ

リリース 6.1（1）以降、 [Cisco ACI]の新機能として、新しいノード タイプの ACI ボーダー ゲートウェイ（BGW）が使用できるようになりました。

（注） このドキュメントの手順では、GUI と REST API を使用して ACI ボーダーゲートウェイを構成する方法について説明します。現時点では、NX-OS スタイルの CLI を使用して ACI ボーダーゲートウェイを構成することはできません。

ACI ボーダーゲートウェイについて

ACI ボーダー ゲートウェイ ソリューションを使用することにより、仮想ルーティングおよびフォワーディング（VRF）インスタンスと Cisco ACI と VXLAN EVPN ドメイン間のブリッジ ドメインを、シームレスに拡張できるようになりました。さらに、Cisco ACIリリース 6.1（4）

からは、ACI ポリシードメインを VXLAN EVPN ドメインにエンドツーエンドで拡張することもできます。これにより、各ドメインで定義したり、ドメイン間で拡張したりすることができるセキュリティ グループ間でセキュリティを適用できます。

ACI ボーダー ゲートウェイ は、サイト内のノードおよびサイトの外部にあるノードと対話するノードです。ACI ボーダー ゲートウェイと VXLAN EVPN ボーダー ゲートウェイは、マルチファブリック ドメインを構築することを可能にし、単一の共通 EVPN 制御および IP 転送ドメインを介して相互接続された複数のサイト ローカル EVPN コントロール プレーンおよび IP 転送ドメインとして概念化できます。

Virtual eXtensible Local Area ネットワーク （VXLAN）イーサネットバーチャル プライベート ネットワーク（EVPN）ボーダー ゲートウェイは、IP 専用ネットワーク上で 2 つ以上の BGP ベースの EVPN サイトまたはファブリック（オーバーレイ ドメイン）をスケーラブルな方法で相互接続するマルチサイト ソリューションです。 エニーキャストモードのボーダーゲートウェイ（BGW）を使用して、Cisco ACI側を 1 つ以上の NX-OS サイトとインターコネクトし、ファブリックのスケーリング、コンパートメント化、および DCI の使用に対する新しいアプローチを可能にします。ボーダー ゲートウェイ は、トラフィックの適用と障害の封じ込め機能に必要なネットワーク制御境界を提供します。

サイトローカル EVPN ドメインは、同じ VXLAN サイト識別子を持つ EVPN ノードで構成されます。ボーダー ゲートウェイは一方ではサイト固有の EVPN ドメインの一部であり、他方では他のサイトからのボーダー ゲートウェイと相互接続するための共通 EVPN ドメインの一部です。特定のサイトに対して、これらのボーダー ゲートウェイはサイト固有のノードを促進し、他のすべてのサイトがそれらを介してのみ到達可能であることを可視化します。これは、以下を意味します：

- サイト ローカル ブリッジング ドメインは、他のサイトからのブリッジング ドメインとボーダー ゲートウェイを介してのみ相互接続が可能です。
- サイト ローカル ルーティング ドメインは、ブリッジング ドメインを介してのみ、他のサイトからのルーティング ドメインと相互接続が可能です。

ACI ボーダー ゲートウェイの ACI 実装について

ACI は、Cisco APIC で導入された次の ACI コンポーネントを使用して ACI ボーダー ゲートウェイを実装します。

VXLAN サイト ID

Cisco ACI 6.1 リリース（2）以降では、サイト ID を構成する必要があります。このサイト ID がないと、ボーダー ゲートウェイ セット ポリシーを構成することはできません。

VXLAN サイトのサイト ID の作成について詳しく説明するには、VXLAN サイト ID （28 ページ） を参照します。

（注） Cisco APIC 6.1（1）の ACI ボーダー ゲートウェイ機能をすでに構成しているのに、VXLAN サイト ID を作成せずに Cisco APIC 6.1（2）にアップグレードすると、すべての拡張 VRF およびブリッジ ドメインで障害が発生します。

ACI ボーダーゲートウェイ セット

これらは、リモート VXLAN EVPN ファブリックへの接続に使用される一連のボーダー ゲートウェイ ノードです。これらのボーダー ゲートウェイ ノードは、ACI ポッドの一部にすることも、ACI ファブリックがマルチポッド ファブリックの場合は異なるポッドに展開することもできます。ポッド内のすべてのボーダー ゲートウェイには、ポッドごとの同じ一意の外部エニーキャスト TEP が割り当てられ、リモート ファブリックからこのポッド内のエンドポイントのトラフィックを引き付けます。

Cisco APIC は、ボーダー ゲートウェイ セットの一意の内部エニーキャスト TEP を割り当てます。これは、全てのポッドに対して展開した全てのボーダー ゲートウェイ ノードで共通です（即ち、同じボーダー ゲートウェイ セットに属します）。構成できるボーダーゲートウェイ セットは 1 つのみです。

詳細については、GUI を使用してボーダー ゲートウェイ セットを作成 （29 ページ） を参照してください。

VXLAN リモート ファブリック

リモート ファブリック 構成では、リモート ボーダー ゲートウェイ上のリモート非 ACI サイトのループバック IP アドレスを指定します。これは、MP-BGP EVPN 隣接関係（アジャセンシー）を確立するために使用されます。複数の VXLAN リモート ファブリック ポリシー（リモート サイトごとに 1 つずつ）を同じボーダー ゲートウェイ セットに関連付けることができます。

詳細については、GUI を使用したリモート VXLAN ファブリックの構成 （30 ページ） を参照してください。

VXLAN インフラ L3 送信

VXLAN インフラ L3Out は、ボーダー ゲートウェイ ノードのグループと、外部サイト間ネットワーク インフラストラクチャ（ISN)のアンダーレイ接続の関連インターフェイスを定義します。Cisco ACI ボーダーゲートウェイ ノードと直接接続された ISN デバイス間のアンダーレイ プロトコルとしてサポートされるのは、eBGP のみです。必要に応じて、ボーダー ゲートウェイ ノードと ISN デバイス間で BFD を有効にして、デバイス間のポイントツーポイント インターフェイスでリンクダウンイベントが発生せずにトラフィック転送が影響を受ける特定の障害シナリオから保護できます。

詳細については、GUI を使用した VXLAN インフラ L3Out の構成 （21 ページ） を参照してください。

VXLAN VRF ストレッチ

Cisco ACI リリース 6.1（1）では、ユーザー VRF をストレッチするには、ボーダー ゲートウェイ セットに関連付けられているユーザー VXLAN L3Out を構成します。すべてのリモート ファブリックをこの L3Out にも関連付けて、対応する非 ACI サイトに VRF をストレッチします。VXLAN ファブリックに拡張される VRF は、非適用モードにすることができます。

Cisco ACI リリース 6.1（4）以降、ACI ボーダー ゲートウェイに正規化機能が導入され、Cisco APIC によってローカルに ACI ファブリックの VRF にローカルに割り当てられた VNID を、VXLAN EVPN ドメインにストレッチ時に同じ VRF に割り当てられた VNID に変換できます。

VXLAN リモート ファブリックの VRF をストレッチするには、「GUI を使用して VRF ストレッチでの VXLAN の構成 （31 ページ） 」を参照してください。

VXLAN ブリッジ ドメイン ストレッチ

Cisco ACI リリース 6.1（1）以降、VXLAN ブリッジ ドメイン ストレッチを活用して、ブリッジ ドメインを非 ACI ファブリックに拡張します。複数のリモート ファブリックを関連付けて、ブリッジ ドメインを対応する非 ACI サイトに拡張できます。

Cisco ACI リリース 6.1（4）以降、ACI ボーダー ゲートウェイに正規化機能が導入され、APIC によってローカルに ACI ファブリックのブリッジドメインにローカルに割り当てられた VNID を、VXLAN EVPN ドメインにストレッチ時に同じブリッジドメインに割り当てられた VNID に変換できます。

VXLAN リモート ファブリックのブリッジ ドメインを拡張する方法については、「GUI を使用してブリッジ ドメイン ストレッチでの VXLAN の構成 （33 ページ） 」を参照してください。

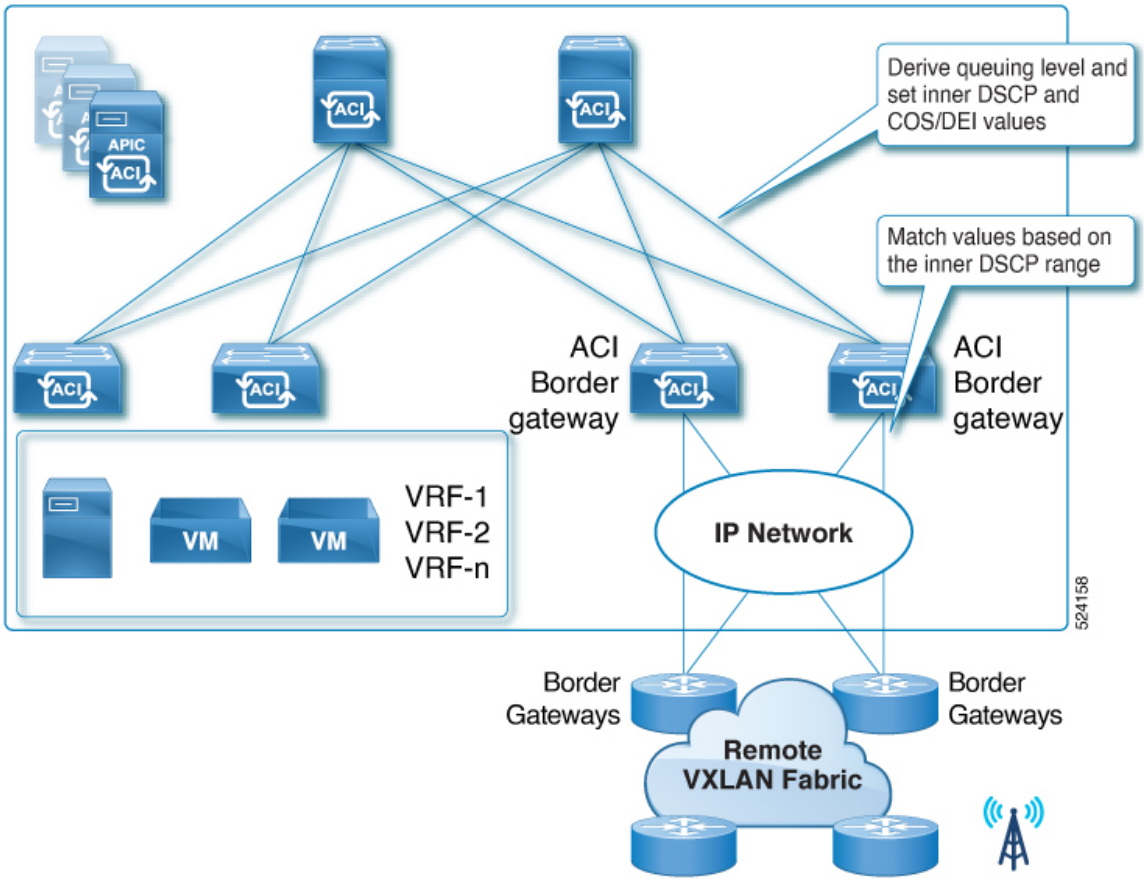
VXLAN QoS ポリシー

Cisco ACI Quality of Service（QoS）機能を使用すると、ファブリック内のネットワーク トラフィックを分類し、トラフィック フローの優先順位付けとポリシングを行って、ネットワークの輻輳を回避できます。トラフィックがファブリック内で分類されると、QoS 優先度レベルが割り当てられます。この優先度レベルは、ネットワーク全体で最も望ましいパケットフローを実現するためにファブリック全体で使用されます。

カスタム VXLAN QoS ポリシーを使用して、VXLAN EVPN ドメインからのトラフィックを ACI ファブリック内で優先順位付けする方法を定義できます。これらのポリシーを使用して、ACI ボーダー ゲートウェイを介してトラフィックが ACI ファブリックを離れるときに、VXLAN EVPN ドメイン宛へのトラフィックを再マーキングすることもできます。カスタム QoS ポリシーは、入力 QoS ポリシーと出力 QoS ポリシーに分かれています。

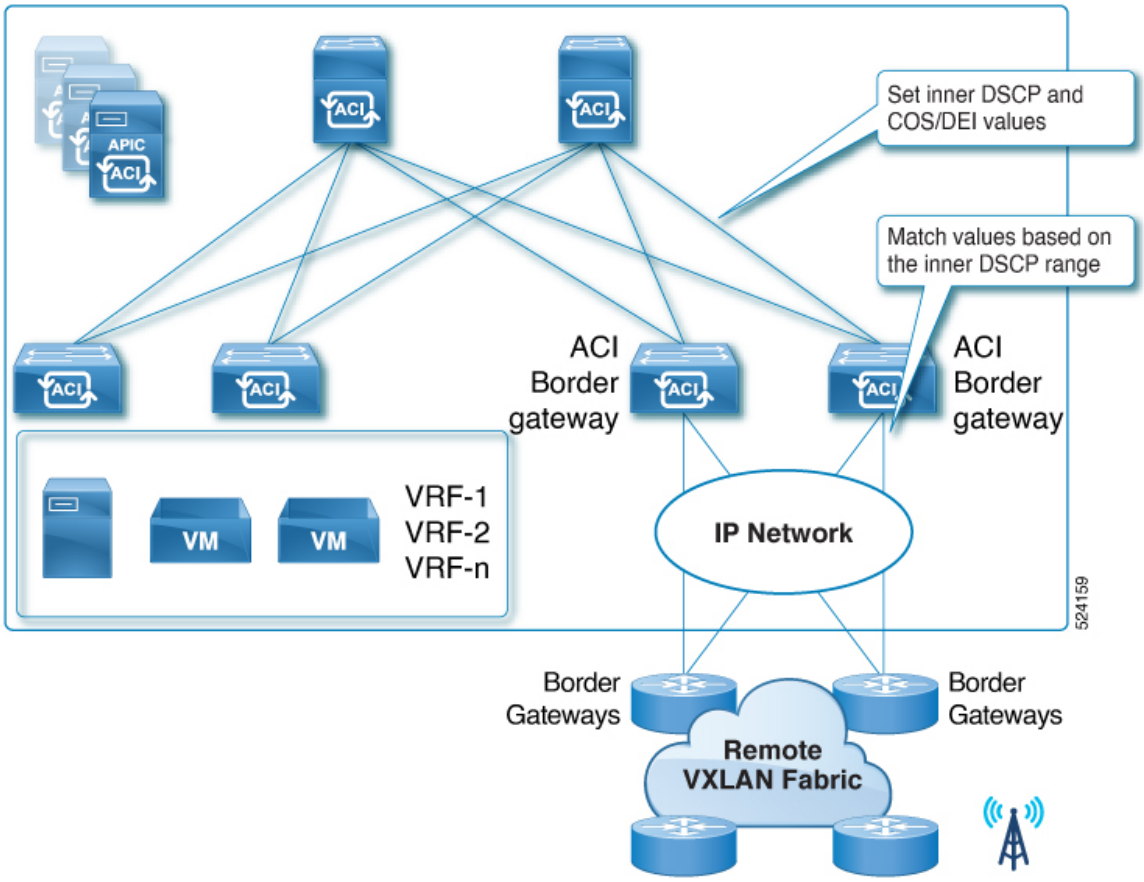
- **入力ルール**： 入力 VXLAN ポリシーの一部として、 VXLAN EVPN ドメインから発信され、ACI ボーダーゲートウェイで受信したトラフィックがファブリック内でどのように処理されるかを定義できます（キューイング優先順位）。リモート VXLAN EVPN ドメインから発信された着信 VXLAN トラフィックの内部 DSCP 値を一致させることで、結果として QoS 優先順位を設定し、 ACI ファブリック内のそのトラフィックの内部 CoS および DSCP 値も設定できます。

図 *1* : 入力 ***VXLAN QoS*** ポリシーを示す例。



- **出力ルール**： 出力 VXLANポリシーの一部として、外部の DSCP および COS フィールドでマークする必要がある値を制御できます。ACI リーフ ノードから発信された iVXLAN カプセル化トラフィックの内部DSCP値は、 ACI ボーダーゲートウェイで一致します。この一致に基づいて、リモート VXLAN EVPN ドメインに送信される VXLAN トラフィックの外部 CoS 値と DSCP 値が設定されます。値を指定しない場合、外部の DSCP および CoS の値はデフォルト値のゼロに設定されます。

図 *2*: 出力 *VXLAN QoS* ポリシーを示す例。



強制モードの VRF

Cisco ACI リリース 6.1（2）以降、VRF は強制モードで構成できます。リモート VXLAN EVPN ファブリックからアドバタイズされたエンドポイントとプレフィックスは、エンドポイント セキュリティ グループ オブジェクト (ESG) によって表されるエンドポイントグループに分類できます。異なる ESG に属するエンドポイント間の通信を有効にするには、コントラクトを通じて表されるポリシーを設定する必要があります。

次のセクションでは、enforced モードでVRFを設定するために必要なさまざまなビルディングブロックについて説明します。

Cisco ACIリリース 6.1（4）以降、リモート SGT 値はドメイン間で伝送されます。Cisco ACI ボーダーゲートウェイでは、リモートVXLAN EVPN ファブリックからアドバタイズされたエンドポイントと外部プレフィックスを分類する必要はありません。

エンドポイント セキュリティ グループ

エンドポイント セキュリティ グループ（ESG）は、Cisco ACI のネットワーク セキュリティ コンポーネントです。これは、物理または仮想ネットワークエンドポイントの収集を含む論理エンティティです。ESG はどのエンドポイントが ESG に属するかを定義する特定の一致基準

を持つセキュリティ コンストラクトであり、コントラクトまたはポリシーを使用してセキュリティ基準を定義します。管理者は契約を使用して、許可されているプロトコルとポートを含む ESG 間をパス可能なトラフィックの種類を選択します。

[コントラクト（Contracts）]

コントラクトは、アクセスコントロールリスト（ACL）に相当する Cisco ACI です。端末セキュリティ グループ（ESGs）は、コントラクト規則に従う場合に限り、他の ESG と通信できます。契約を使用して、許可されているプロトコルとポートを含む ESG 間をパス可能なトラフィックの種類を選択することができます。ESGは、コントラクトのプロバイダー、コンシューマー、またはプロバイダーとコンシューマーの両方になることができ、複数のコントラクトを同時に使用できます。複数の ESG が優先グループに属する他の ESG と自由に通話できるように、ESG は優先グループに属することもできます。

一致基準は、関連付けられた VRF インスタンスのブリッジドメインにまたがる IPv4 または IPv6 アドレス、またはエンドポイント MAC アドレスに関連付けられたタグなどの属性に基づく ESG セレクタと呼ばれます。異なる ESG に属するエンドポイント間の通信を有効にするには、ESG 間のコントラクトを構成する必要があります。Cisco ACI ファブリックの外部にあるデバイスと通信するには、L3Out 外部 EPG（**l3extInstP**）と ESG の間のコントラクトを構成する必要があります。EPG セレクタ、 IP サブネットセレクタ、タグ セレクタなどのセレクタのいずれかを使用して、L3Out 接続を通じて学習した ACI ファブリック内と外部ネットワークプレフィックスを分類できます。

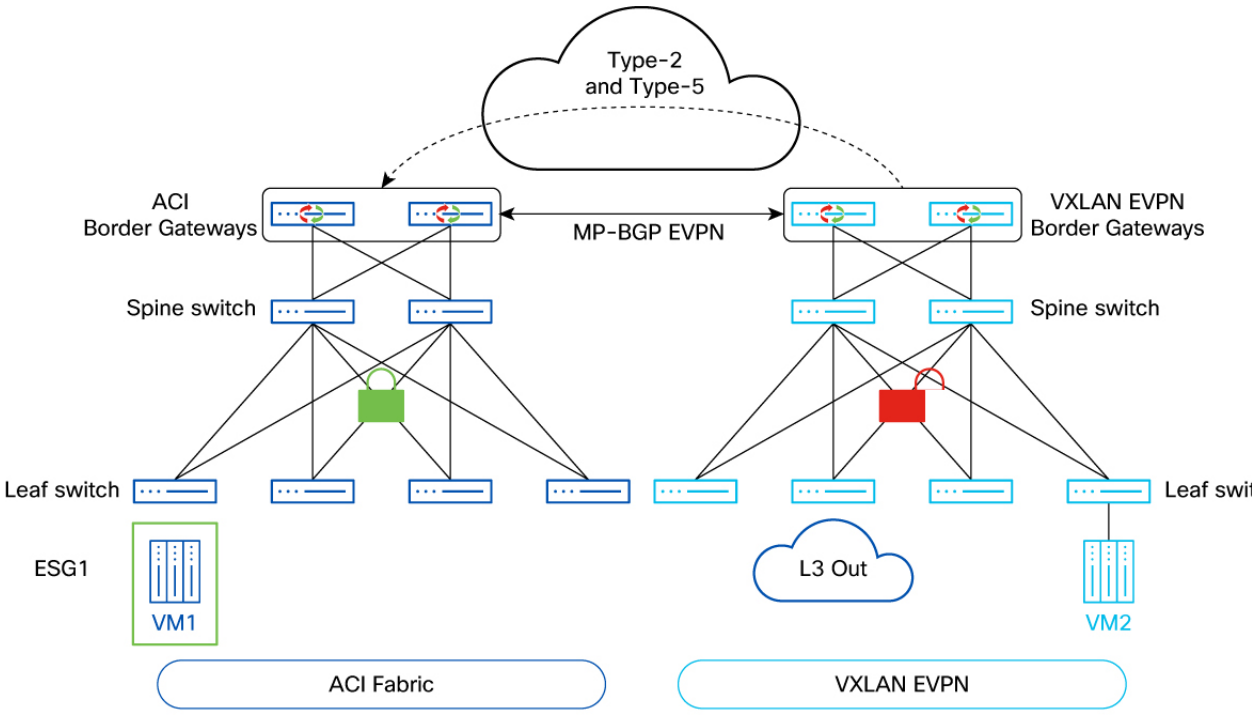
Cisco APIC で使用可能な既存のセレクタの詳細については、Cisco APIC セキュリティ構成ガイド リリース 6.1（x）の エンドポイント セキュリティ グループ セクションを参照してください。

Cisco ACIからポリシー非認識リモートVXLAN EVPN への活用例

Cisco ACI は、構成されているさまざまなセレクタに基づいて、着信トラフィックを ESG に分類します。これらのセレクタは、さまざまなマッチング基準を使用し、各 ESG の下に構成されます。

Cisco ACIリリース 6.1（2）以降、リモートVXLAN EVPN ファブリックから学習したエンドポイントと外部接続先を分類するための 2 つの新しいセレクタが追加されました。

図 *3 : [Cisco ACI]* からポリシー非認識 *VXLAN EVPN* オプションへ



[外部サブネット セレクタ（External Subnet Selector）]

Cisco APICリリース 6.1（2）および 6.1（3）では、これはACI VXLAN ボーダー ゲートウェイ（BGW）の VXLAN 外部サブネット セレクタと呼ばれていました。Cisco APICリリース 6.1（4）以降、これは通常の L3Out サブネットに使用できる汎用の外部サブネット セレクタとして機能拡張されています。

このセレクタは、別のファブリックからACIボーダーゲートウェイノードで受信される EVPN タイプ 5 ルートと一致します。照合は、最長プレフィックス マッチ（LPM）方式で行われます。

6.1（4）以降、このセレクタは、ボーダー ゲートウェイなしで通常の L3Out を通じて学習した外部プレフィックスともマッチします。これは、L3Out 外部 EPG の下で「外部 EPG の外部サブネット」スコープを持つ L3Out 外部サブネットの代わりに使用できます。

外部サブネットセレクタの下の「共有」フラグは、コントラクトを通じて接続された他の VRF へのESGおよびプレフィックスのマッピングをリークするために使用されます。これは、L3Out 外部サブネットの場合の「共有インポートセキュリティ サブネット」スコープに相当します。このフラグはセキュリティ情報のみをリークし、実際のルート リークはVRFレベルで個別に設定する必要があることに注意してください。

（注） デフォルト ルート（`0.0.0.0:0` または `000`）を外部サブネット セレクタとして構成することはできません。回避策としては、`0.0.0.0/1` と `128.0.0.0/1` または `0::0/1` と `8000::/1` はすべてに一致するために使用できます。

詳細については、外部サブネット セレクタ （34 ページ） を参照してください。

VXLAN ストレッチされたブリッジ ドメイン セレクタ

このセレクタを活用、リモート VXLAN ファブリックから学習した特定のストレッチブリッジドメインに関連付けられているすべての L2 MAC アドレスを対応する ESG に分類します。このセレクタは、VXLAN ストレッチのブリッジドメイン用にのみ構成できます。このブリッジドメインに属するすべてのリモート ファブリックからのエンドポイントは、同じ ESG の一部として分類されます。

詳細については、VXLAN ストレッチ ブリッジ ドメイン セレクタ （34 ページ） を参照してください。

リモート エンドポイント サブネットの分類

ポリシー非認識 VXLAN EVPN ファブリックの場合、既存の IP サブネットセレクタを使用して、リモート VXLAN EVPN ファブリックでのみローカルに定義されている（つまり、ACI および VXLAN EVPN ドメイン間で拡張されていない）IP サブネットのエンドポイント（接続されたホスト）部分を分類できます。

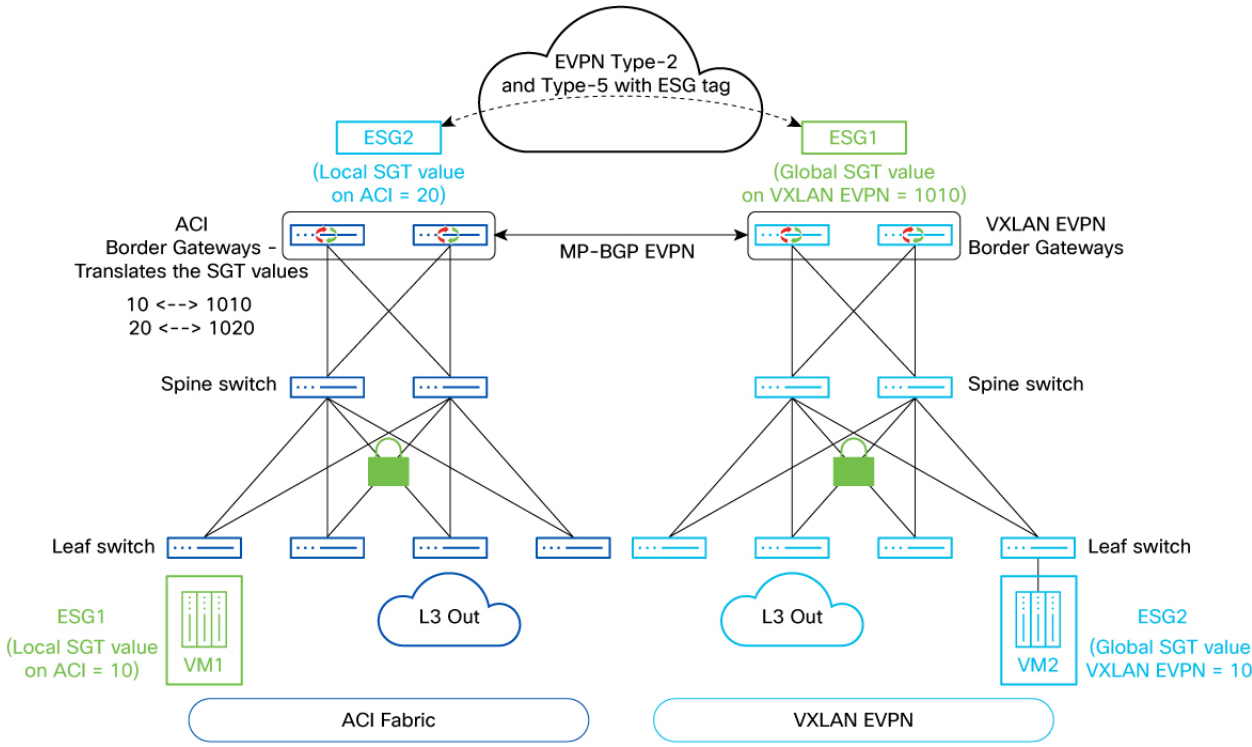
（注） これは、VXLAN 外部サブネットセレクタとは異なり、つまり、正確に一致するプレフィックスのみを使用してリモート DC サブネットを分類できます。スーパーネットをカバーするプレフィックスは実現できません。

既存の MAC タグ セレクタまたは IP タグ セレクタを使用して、特定の L2 MAC アドレスと特定の L3 IP アドレスをリモート VXLAN ファブリックから ESG に分類できます。

Cisco ACI からポリシー認識 VXLAN EVPN への活用例（Cisco ACIリリース 6.1（4）以降）

ACI リリース 6.1（4）および NX-OS リリース 10.5（3）からサポートされているこの最初の使用例では、Cisco ACI ドメインはポリシー認識リモート VXLAN EVPN ドメインに接続されます。ACI ボーダー ゲートウェイと NX-OS ボーダー ゲートウェイ間の EVPN コントロール プレーンは、各ドメインで定義されたセキュリティ グループを識別するタグを伝送するように強化されました。これは、内部リソースと外部リソースの両方の分類が、各ドメイン内で独立して実行されることを意味します。

図 *4 : [Cisco ACI]* からポリシー対応 *VXLAN EVPN* オプションへ



[セキュリティ グループ タグ（SGT）（Security Group Tag (SGT)）]

セキュリティ グループ タグ（SGT）は、属性/セレクタに基づいて分類される物理または仮想ネットワーク エンドポイントおよび外部情報技術の収集を含む論理エンティティの識別子（セキュリティ グループ）です。ACI リリース 6.1（4）以降、 ACI ドメインと VXLAN EVPN ドメイン間の EVPN コントロール プレーンを介して SGT 値を伝送する新しい機能が導入されています。ポリシー認識リモート EVPN ファブリックでは、このリモート SGT は必須の構成です。

これは、リモート VXLAN EVPN ドメインがポリシー対応であり、 ACI ボーダー ゲートウェイとリモート NX-OS ボーダー ゲートウェイ間の EVPN コントロール プレーンがポリシー情報を伝送できる場合に必要な構成です。リモート SGT 値は、Cisco APIC で Cisco ACI ファブリックでローカルに定義されたすべての ESG に関連付ける必要があります。これは、リモート VXLAN EVPN ドメインでそれらのセキュリティ グループを識別するために使用される SGT を表すためです。

リモート セキュリティ グループ タグの使用方法を理解するために、前の図のシナリオを考えてみましょう 図 4 : [Cisco ACI] からポリシー対応 VXLAN EVPN オプションへ （10 ページ）。ESG1 は、ローカルの内部技術情報や外部技術情報を分類するために ACI ファブリックでローカルに定義され、 APIC によって SGT 値（この特定の例では 10）が割り当てられます。これは、ACI ドメインでローカルに重要です。ACI ボーダー ゲートウェイがリモート VXLAN EVPN ドメインに向けた ESG1 の一部としてプレフィックスをアドバタイズする場合、最初にローカル値 **10** をリモート VXLAN EVPN ドメインへ ESG1 と識別するグローバルに重要なリモート SGT 値（1010）へ翻訳します。同様に、ローカルの内部技術情報や外部リソースを分類するために VXLAN EVPN ドメインで ESG2 グループが定義されると、グローバル SGT 値（1020）が

割り当てられます。この値は、NX- OS ボーダー ゲートウェイによって ACI ドメインに ESG2 プレフィックスをアドバタイズするために使用されます。ACIボーダー ゲートウェイがそれらを受信すると、そのリモート SGT 値を ACI ドメイン内の ESG2 グループを識別するローカル SGT 値（20）に変換します。その後、ESG1 と ESG2 間の通信を制御するために、グローバル セキュリティ ポリシーをプロビジョニングする必要があります。

（注） 図 4 : [Cisco ACI] からポリシー対応 VXLAN EVPN オプションへ （10 ページ） 図の中の例は、2 つの異なるセキュリティ グループが各ドメイン内で定義されているシナリオを示していますが、2 つのドメイン間でセキュリティ グループを機能的に拡張することもできます。このような場合、同じ ESG 名がそのようなグループを識別し、Cisco ACI および VXLAN EVPN ドメイン内のリソースを分類するために使用されます。 ACI ローカル SGT 値とリモート SGT 値間の単一の変換は ACI ボーダー ゲートウェイによって実行されます。

リモート EVPN ファブリックの場合、ACI ファブリックのどの ESG にもマッピングされていない SGT タグは、値 **12**として分類されます。これはデフォルトのドロップクラスです。このタグは、リモート EVPN ファブリックからのエンドポイントとプレフィックスの両方に適用できます。リモート SGT のない ESG に属するエンドポイントとプレフィックスの場合、 ACI はタグ値 0 のタグをリモート EVPN ファブリックにアドバタイズします。0 は、NX OSベースの EVPN ファブリックのドロップ SGT タグのデフォルト値です。

[VXLAN EVPN ルート マップ（VXLAN EVPN Route-Maps）]

Cisco ACI リリース 6.1（2）以降、 ACI ボーダー ゲートウェイ機能は、拡張された VRF で構成できる VRF レベルのルート マップをサポートします。これらのルート マップは、ボーダー ゲートウェイ セットに関連付けられているすべてのリモート ファブリックに適用できます。ルートマップの set ルールは、ルート制御プロファイル ポリシーとアクション ルール プロファイルで構成されます。一致基準に基づく **[許可（Permit）]** または **[拒否（Deny）]**ステートメントを指定します。

リモート EVPN ファブリックにインポートまたはエクスポートできるルートを制御できます。インバウンド ルート マップは、タイプ 5 およびタイプ 2 ルートのIP部分に適用されます。タイプ 2 の MAC ルートは影響を受けず、 IP インポート ステータスに関係なくインポートされます。

発信ルート マップは、タイプ 5 ルートにのみ適用されます。

アウトバウンドおよびインバウンドのルートマップを GUI を使用して VRF ストレッチでの VXLAN の構成 （31 ページ） 使用して指定します。

ルート マップの構成方法の詳細については、 GUI を使用した VRF でのルート制御ポリシーの構成を参照してください。

（注） この構成は、オプションです。インポート ルートマップを構成しない場合、リモートVXLAN EVPN ファブリックから受信したすべてのルートが受け入れられます。エクスポート ルートマップを構成しない場合、すべてのローカル ブリッジドメインサブネットと外部ルートがリモート VXLAN EVPN ファブリックにアドバタイズされます。このためには、ブリッジ ドメイン サブネットの **[外部にアドバタイズ（Advertised Externally）]** フラグをが有効になっていることを確認する必要があります。

次に、インバウンドルート マップとアウトバウンドルート マップの両方でサポートされている match 句と set 句のリストを示します。

- **サポートされる match 句**
  - IP プレフィックス リスト
  - AS 経路
  - コミュニティ
  - 拡張コミュニティ（マッチオンカラー拡張コミュニティはサポートされていません）
  - 正規表現コミュニティ
  - 正規表現拡張コミュニティ
- **[サポートされる設定句（Supported Set Clauses）]**
  - コミュニティ
  - 拡張コミュニティ
  - 重量
  - 環境設定
  - メトリック

[Cisco ACI Border Gateway のスイッチド ポート アナライザ（ SPAN ）]

Switched Port Analyzer（SPAN; スイッチド ポート アナライザ）は、効率な高性能トラフィック モニタリング システムです。これは、送信元ポートまたは、VLAN から宛て先ポートまでトラフィックの指示またはミラーをします。Encapsulated Remote SPAN （ERSPAN）は、キャプチャされたすべてのトラフィックに Generic Routing カプセル化 （GRE）を提供し、レイヤ 3 ドメイン全体に拡張できます。

ACI ボーダー ゲートウェイでは、次の SPAN 機能がサポートされています：

- ローカル スパンはボーダーゲートウェイで構成する必要があります。ここで、送信元をインフラ L3Out インターフェイス、接続先をボーダーゲートウェイの別のポートとして構成します。

- インフラ L3Out インターフェイスの ERSPAN モニタリング セッションは、入力通信と出力通信の両方のモニタリングをサポートします。モニタリングはポート レベルでのみ機能するため、フィルタリングはサポートされていません。
- ボーダーゲートウェイでのファブリック インターフェイスの ERSPAN モニタリング セッションは、入力通信と出力通信の両方のモニタリングをサポートします。モニタリングはポート レベルでのみ機能するため、フィルタリングはサポートされていません。

  オンドロップ SPAN のサポートは有効になっています。

Cisco ACIリリース 6.1（4）以降、ERSPAN のサポートが有効になり、接続先 ERSPAN がリモート VXLAN ファブリックに展開されます。ローカル ERSPAN は Cisco ACI で使用でき、接続先 ERSPAN はリモート VXLAN ファブリックで使用できます。

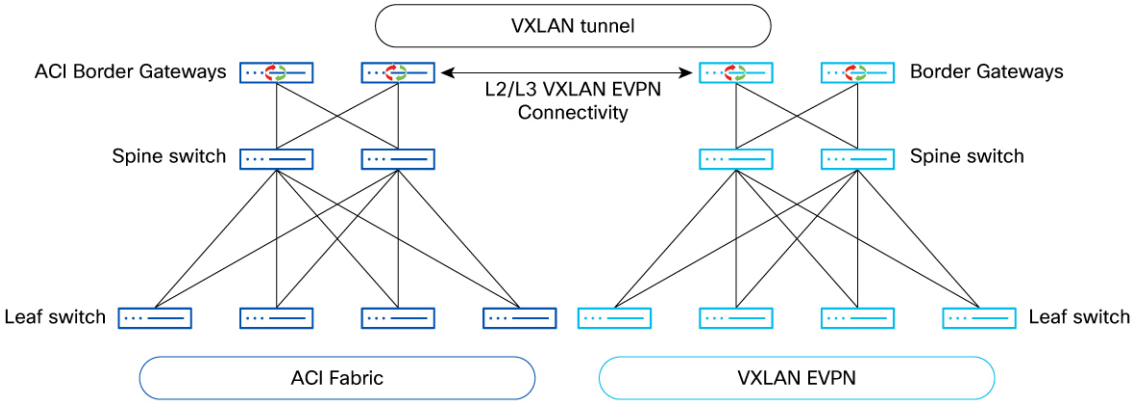
次の ERSPAN ガイドラインは、 ACIボーダーゲートウェイの ERSPAN セッションに適用されます。

- ERSPAN 接続先 IP は、Cisco ACI ブリッジドメイン EPG から構成する必要があります。これにより、リモート VXLAN NX-OS ファブリックの接続されたエンドポイントがマッピングされます。
- リモート VXLAN ファブリックのプレフィックス サブネットを介して接続先 IP にアクセスできない、NX-OS L3Out の背後にある ERSPAN 接続先 IP は、サポートされていません。
- ESG EP プレフィックスは ERSPAN 接続先として構成できません。
- ERSPAN 送信元 IP は、タグを使用してリモート VXLAN ボーダーゲートウェイに存在する必要があります。
- VXLAN プレフィックスの接続先への ERSPAN トラフィックのスムーズなフローを確保するには、リモート VXLAN サイト上の ERSPAN 送信元 IP と ERSPAN 接続先 IP の間に契約が存在する必要があります。
- が EPG ブリッジドメインを ERSPAN 接続先として使用するようにするには、ブリッジドメインをリモート VXLAN NX-OS ファブリックから ACI ファブリックに拡張する必要があります。
- ERSPAN トラフィックを確認する前に、EP の移動が正常に完了したことを確認してください。

ACI ボーダーゲートウェイ デプロイメントについて

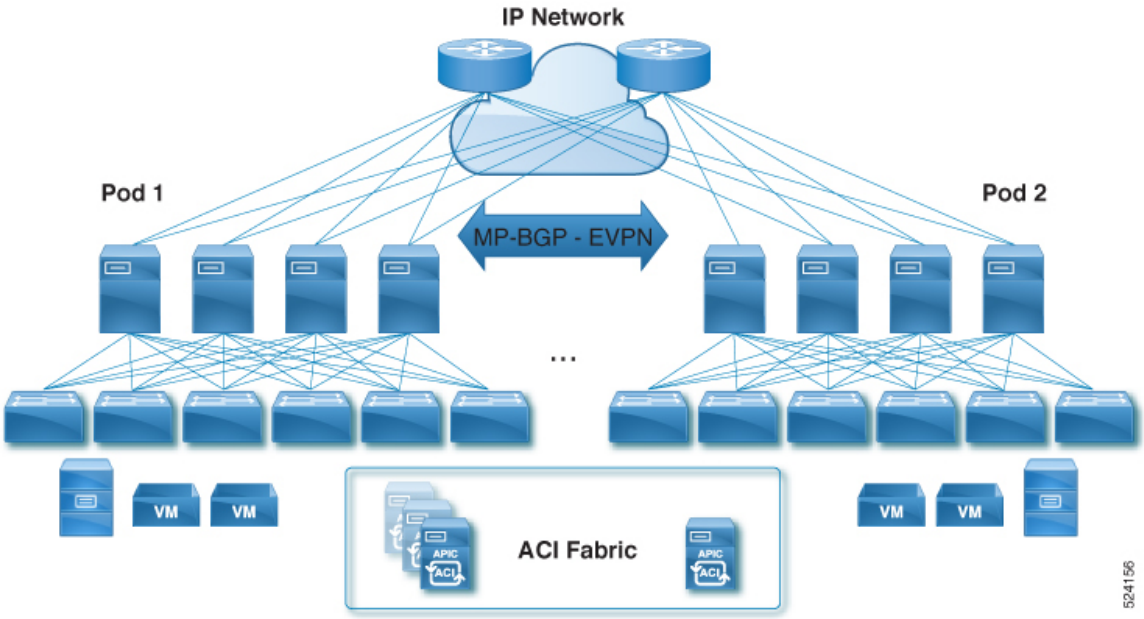
次の図は、Cisco ACI でのACI ボーダー ゲートウェイの展開を示しています。

図 *5 : Cisco ACI* での *ACI* ボーダー ゲートウェイの展開



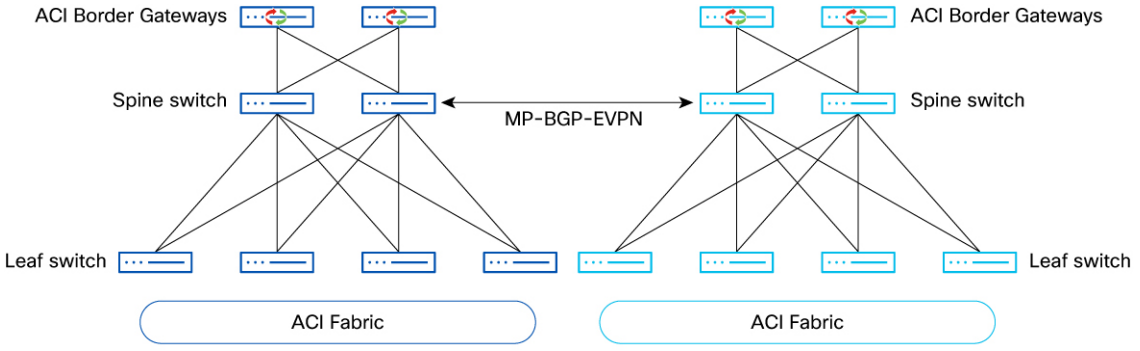
- データパケットをカプセル化し、トラフィックをレイヤ 3 サイト間ネットワーク（ISN）上でトンネリングするためのオーバーレイ テクノロジーとして VXLAN が使用されます。
- VXLAN ハンドオフは、特定の各 ACI および VXLAN EVPN ドメイン内で使用される VXLAN トンネルをドメイン間で使用される VXLAN トンネルとステッチするボーダー ゲートウェイ ノードによって実行されます。
- 同じファブリックの一部である Cisco ACI ポッド間の L2/L3 VXLAN 接続は、IPN を介したスパイン間データ パスを介して引き続き実現されます。
- Cisco ACI ボーダー ゲートウェイは、各ポッドにローカルに存在する必要があります。ACI ボーダー ゲートウェイがポッドにローカルに存在しない場合、特定のポッドに属するエンドポイントは、別のポッドに展開されている ACI ボーダー ゲートウェイを介してリモート VXLAN EVPN ドメインと通信できません。

図 *6 :* ポッド内の *Cisco ACI* ボーダー ゲートウェイ



- ドメイン間で拡張されたブリッジ ドメインごとに、特定の Cisco ACI ボーダー ゲートウェイが、すべてのポッド内のすべてのボーダー ゲートウェイで指定フォワーダとして選択されます。指定フォワーダ BGW は、そのボーダー ゲートウェイのフラッド トラフィックをリモート VXLAN EVPN ドメインと送受信します。
- Cisco ACI リリース 6.1（4）より前は、各ファブリックに展開されたボーダーゲートウェイ ノードを使用して、 ACI ファブリック間のレイヤ 2 および/またはレイヤ 3 接続を確立することはサポートされていませんでした。Cisco ACI ボーダー ゲートウェイは、接続とポリシーをリモート VXLAN EVPN ドメインに拡張するためにのみ使用できます。ACI ファブリック間の接続とポリシーを拡張する唯一の方法は、 ACI マルチサイト アーキテクチャを利用することです。この場合、下図のとおり、スパイン ノードを介したサイト間接続を利用します。

図 *7*: ボーダー ゲートウェイ ノードを使用した *ACI* ファブリック間のレイヤ *2*/レイヤ *3* 接続



ACI ボーダー ゲートウェイに関する注意事項と制限事項

以下は ACI ボーダー ゲートウェイ機能の注意事項と制限事項です。

- ACI ボーダーゲートウェイのハードウェアサポートは、32GB のRAM をサポートしている限り、FX モデル以降の Nexus 9000 プラットフォームです（したがって、FX2 プラットフォームはサポートされません）。
- ACIボーダー ゲートウェイ機能の専用リーフ ノード。ボーダー ゲートウェイ のボーダー リーフ機能（テナント L3Outs）との共存は、今後のリリースで計画されています。
- BUM として転送される L2 マルチキャスト トラフィック。
- Cisco APIC（1）以降、ストレッチする必要がある VRF 構成の Cisco ACIファブリックには、適用されていない VRF が必要です。この制限は、Cisco APIC 6.1（1）でのみ適用されます。

  Cisco APIC 6.1（2）以降、Cisco ACI ファブリックで強制モードでストレッチ VRF を構成し、ESG を使用して VXLAN EVPN ドメインの内部/外部リソースでセキュリティ ポリシーを適用できます。
- 単一の ACI ファブリックのサポート（マルチポッドの場合もあります）。

- Cisco APIC 6.1（2）以降、 ACIファブリックは、 **vxlanSiteId** によって定義された EVPN ドメインの一意のサイト ID を指定する必要があります。
- Cisco ACI リリース 6.1（4）より前は、ブリッジドメインまたは VRF の VNI は、Cisco ACI と NX-OS ファブリック間で対称である必要があります。Cisco APIC によって VRF またはブリッジドメインに割り当てられたブリッジは制御できないため、初期サポートは、一致する VNID がリモート VXLAN EVPN ファブリック上で構成可能なのかを確認するため、VRF または、Cisco ACI から VXLAN EVPN ドメインへストレッチしたブリッジ ドメインのみに使用可能です。

  Cisco ACIリリース 6.1（4）以降では、正規化された VNI を指定できます。これは、リモート EVPN ファブリックで使用される VRF またはブリッジドメインストレッチの一部として使用される VNI です。
- ACIマルチポッド/マルチサイトと VXLAN インターサイトの両方に同じ IPN/ISN デバイスを使用する場合は、マルチポッド/マルチサイト ネットワークと VXLAN サイト間ネットワークを異なる VRF に分離することを推奨します。
- Cisco APIC 6.1（1）では、 ACI と VXLAN EVPN ドメイン間で拡張される VRF を、 VXLAN EVPN ファブリックの非 VLAN ベースの L3 VNI 構成で構成する必要があります。これは、*[VRF* 構成の新しい方法（*new way of VRF configuration*）*]*と呼ばれます。

  Cisco APIC 6.1（2）以降、NX- OS L3VNI 構成は、非 VLAN ベースまたは VLAN ベースの L3 VNI 構成で構成できます。
- ACI ボーダーゲートウェイ機能では、ファブリック内のすべてのノードが、Cisco 6.1（4）で実行されているのと同じバージョンを実行している必要があります。
- 特定のポッド内の内部ルートリフレクタおよび mpod-spine と同じスパイン ノードのセットを選択する必要があります。
- Cisco ACI VXLAN ボーダーゲートウェイと NX-OS ボーダーゲートウェイ間のバックツーバック接続はサポートされていません。
- Cisco APIC 6.1（4）以降、 VRF のブリッジドメインに属するすべてのエンドポイントは、ブリッジドメインが拡張されている場合にのみアドバタイズされます。すべてのエンドポイントをアドバタイズする場合は、 VRF 内のすべてのブリッジ ドメインを拡張する必要があります。
- Cisco APIC 6.1（1）から Cisco APIC 6.1（4）にアップグレードする場合は、最初にサイト ID を構成し、以前の Cisco APIC バージョンから既存の障害をすべてクリアし、アップグレードを実行する前に BGP が収束するのを待ってから、次に進んでください。
- ロードバランサ SNAT があり、サービスブリッジドメインが Cisco ACI ファブリックのボーダー ゲートウェイに拡張されていない場合、次の条件がロード バランサによるサービス リダイレクトに適用可能であることを確認する必要があります：
  - LB サーバーが Cisco ACI サイトにあることを確認します。
  - サービス EPG がサービス ESG に引き上げられ、ESG の内部レッグと NX-OS サイトのプロバイダー SGT の間でコントラクトを作成することを確認します。

- 次の機能はこのリリースでサポートされていません：
  - ACL を使用した SPAN
  - ERSPAN の接続先は、 ACI ファブリックに対してローカルなエンドポイントまたはプレフィックスにすることができます。
  - マルチサイト EVPN 展開は、フルメッシュ モードまたはルートサーバー モードのいずれかで実行できます。Cisco ACI 6.1（1）リリースと統合するには、Cisco ACI と NX-OS ファブリック間のフルメッシュ EVPN モードでのみ実行できます。したがって、ルートサーバー モデルはサポートされていません。
  - VXLAN サイトに拡張された VRF またはブリッジ ドメインは、リモート リーフ スイッチに展開しないでください。
  - ボーダー ゲートウェイを備えた Cisco ACI ファブリックは、 ACI マルチサイト ドメインの一部にすることができます。ただし、VXLAN EVPN ドメインに拡張されている VRF またはブリッジドメインは、他の ACI マルチサイト ファブリックに拡張することはできず、その逆も同様です。
  - NX- OS ファブリックと ACI ファブリックの間では、マイクロセグメンテーションで EPG に関連付けられているブリッジ ドメインの拡張はサポートされていません。
  - Cisco APIC 6.1（1）では、ACI の EVPN ピアでは、入力または出力ルートマップはサポートされていません。ルートフィルタリングは、リモートNX-OSファブリックBGWでのみ実行できます。

    Cisco APIC 6.1（2）以降、ルートマップのサポートが導入されました。リモートEVPNファブリックからインポートまたはリモートEVPNファブリックにエクスポートできるルートを制御できます。

    インバウンド ルート マップは、タイプ 5 およびタイプ 2 ルートのIP部分に適用されます。タイプ 2 の MAC ルートは影響を受けず、 IP インポート ステータスに関係なくインポートされます。

    発信ルート マップは、タイプ 5 ルートにのみ適用されます。
  - IGMP スヌーピングおよびL3マルチキャスト トラフィックは、ドメイン間ではサポートされません。
  - VRF 間トラフィック フロー（共有サービス）は、Cisco ACI 6.1（4）より前のリリースではサポートされていません。

    Cisco APIC 6.1（4）以降、VRF間トラフィック フロー（共有サービス）がサポートされていますが、共有サービスの一部であるすべての VRF は、 ACI ボーダー ゲートウェイとリモート EVPN ボーダーゲー トウェイに展開する必要があります。
  - リークされたルートを VRF からピアにアドバタイズしてはなりません。
  - VXLAN EVPN ドメインがポリシーを認識していない場合、ドメイン間のトラフィック フローのサービス リダイレクション（PBR）は、L3（Go-To）モードで展開され、

Cisco ACI ファブリックに接続されているサービス デバイスに対してのみサポートされます。

- Cisco APIC 6.1（4）以降、 ACIファブリックがポリシー認識リモートVXLANファブリックと相互接続すると、リモートVXLANファブリックから受信したポリシーまたはクラスの詳細は、リモートと対話している場合、ACIボーダーゲートウェイノードによって無視されます。 EVPN NX- OS 10.5（3）バージョンのファブリック。また、ACI ファブリックは、そのポリシーまたはクラス情報をリモート VXLAN ファブリックにアドバタイズしません。

- Cisco ACI 6.1（4）および NX- OS 10.5（3）バージョンは、ポリシー認識サイト間の相互運用性のための最小の実行可能な組み合わせです。NX- OS 10.5（3）より前のバージョンの場合は、ポリシー非認識相互運用モードでのみ Cisco ACIに接続できます。
- ポリシー認識相互運用性サイトの外部プレフィックスには、次の制限が適用されます：
  - 外部サブネット セレクタを構成するときは、サブネットセレクタが常に L3Out ピアから学習するプレフィックスのスーパーネットであることを確認する必要があります。サブネット構成がプレフィックスのサブネットである場合は、プレフィックスのエンドポイントとして分類されません。

    たとえば、 `50.1.0.0/16` の学習された ACI 外部ルートおよび ESG プレフィックス セレクタが `50.1.1.0/24`として構成されている場合、Cisco ACI は外部ルート `50.1.0.0/16` をデフォルトの ESG タグを持つタイプ 5 ルートとしてアドバタイズします。これは、`0`のデフォルトの ESG タグです。
  - 外部プレフィックスを構成する場合、重複するプレフィックスセレクタを構成することはできません。たとえば、2 つの ESG があり、ESG-1 に `50.1.1.0/24` としてのプレフィックス セレクタであり、2 番目の ESG-2 を `50.1.0.0/16` 外部ルートの場合、Cisco ACI はESG1 または ESG2 のいずれかを選択できます。この分類は確定的なではないためです。
  - VXLAN 拡張 VRF の VRF ルート リークを構成する場合は、ルートをリークするために内部プレフィックスのリーク オプションを使用する必要があります。

    内部プレフィックスをリークする方法の詳細については、「Cisco APICSecurity 構成ガイド」の「GUIを使用した内部プレフィックスのルートリークの構成」セクションを参照してください。

ACI ボーダー ゲートウェイの検出

ノード タイプをボーダーゲートウェイとして登録するには、次の手順を実行します：

始める前に

ACI ボーダー ゲートウェイとして表示されるようにするには、各リーフ ノードをノード タイプ border-gateway に登録する必要があります。

（注） ノードタイプ border-gateway を使用してスパインを登録することはできません。検出がブロックされます。

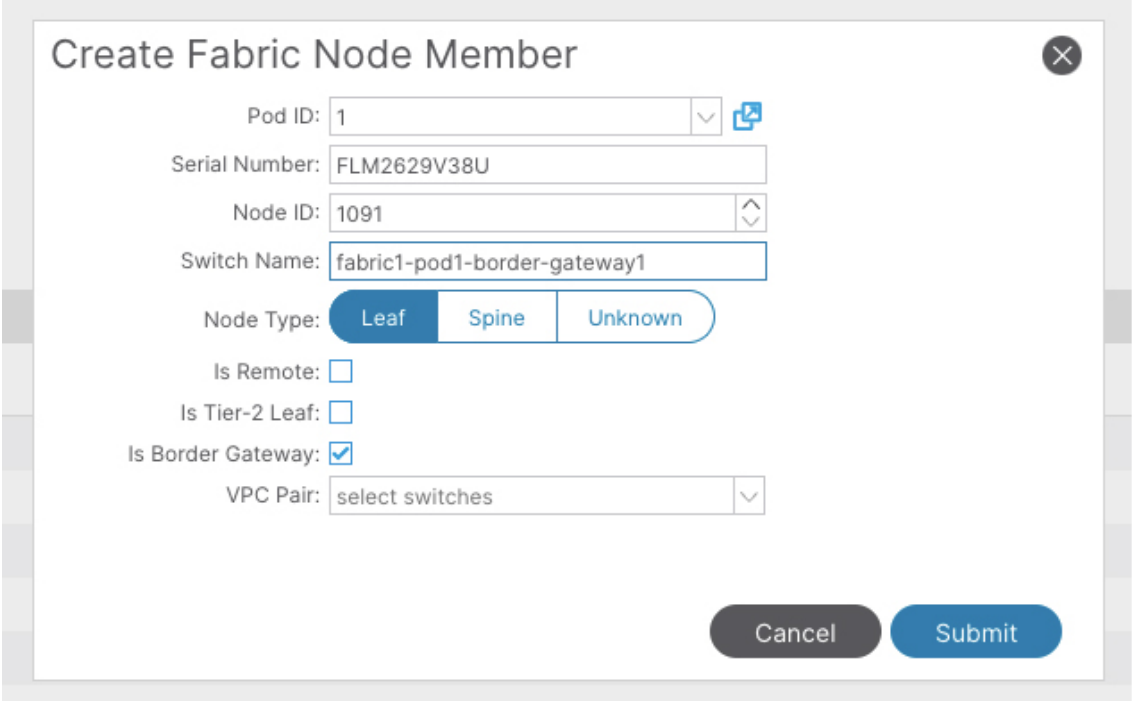
手順

ステップ 1 ノード登録ポリシーを事前構成するには、シリアル番号がすでにわかっている場合は、次の手順を実行します：

a) **[ファブリック（Fabric）] > [インベントリ（Inventory）] > [ファブリック メンバーシップ（Fabric Membership）] > [登録済みノード（Registered Node）]**タブに移動します。

b) **[作業（Work）]** ペインで、**[アクション（Actions）] > [ファブリック ノード メンバーの作成（Create Fabric Node Member）]** をクリックして次の手順を実行します。

図 *8 : ACI* ボーダー ゲートウェイの検出



a) **[ポッド ID（Pod ID）]** フィールドで、ドロップ ダウン メニューからポッド ID を選択します。

b) **[シリアル番号（Serial Number）]** フィールドに、リーフ スイッチのシリアル番号を入力します。

c) **[ノード ID（Node ID）]** フィールドで、ノード ID をリーフ スイッチに割り当てます。

d) **[スイッチ名（Switch Name）]** フィールドで、リーフ スイッチに名前を割り当てます。

e) **[ノード タイプ（Node Type）]** フィールドで、ノード タイプとしてリーフを選択します。

f) **[ボーダーゲートウェイです（Is Border Gateway）]** チェックボックスをオンにして、リーフをノード タイプとして登録します。

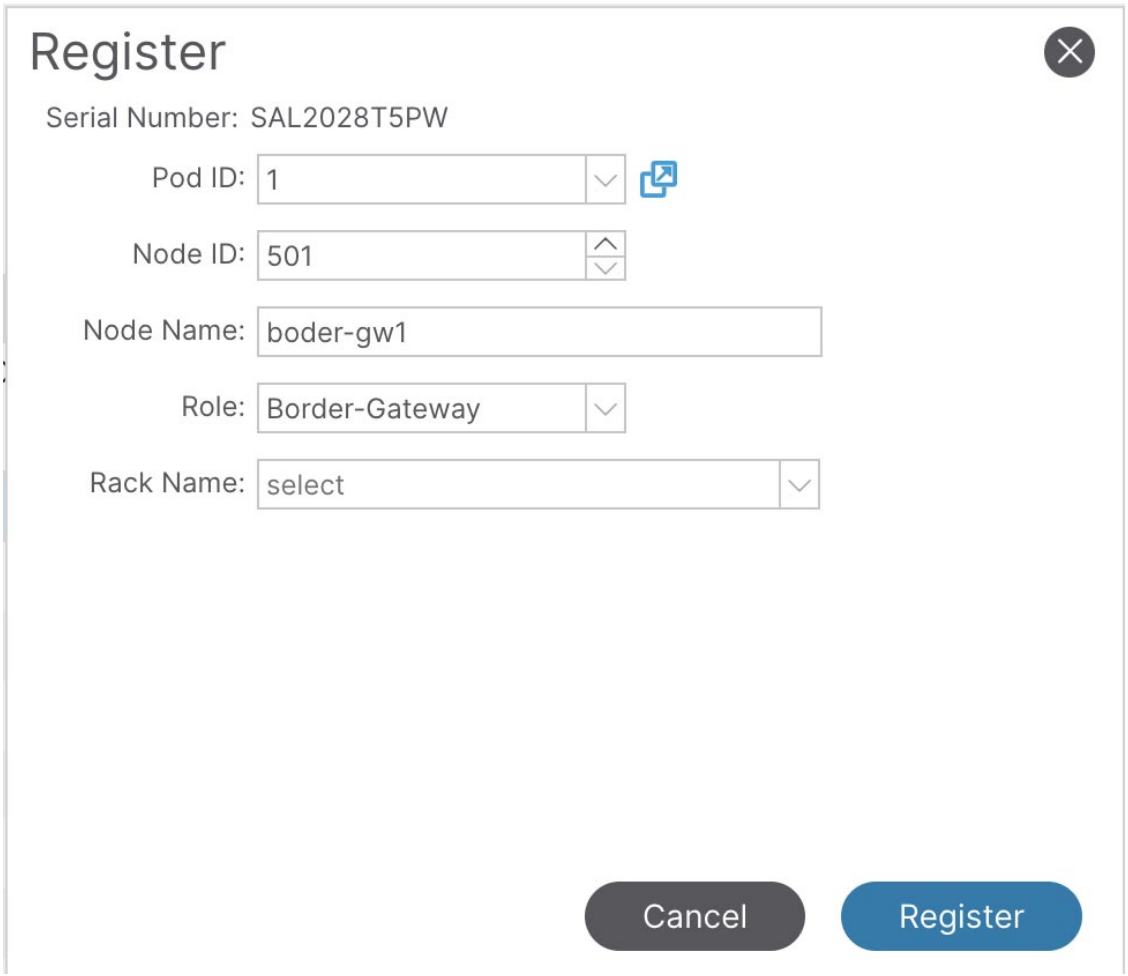
g) **[送信（Submit）]**をクリックします。

ステップ 2 DHCP 検出に基づいてノードを構成するには、次の手順を実行します。

a) **[ファブリック（Fabric）] > [インベントリ（Inventory）] > [ファブリック メンバーシップ（Fabric Membership）] > [ノード保留登録（Nodes Pending Registration）]**タブを移動します。

b) 次に **[作業（Work）]** ペインで、新しく検出されたリーフのシリアル番号を右クリックし、**[登録（Register）]** をクリックして次の手順を実行します。

図 *9 : ACI* ボーダー ゲートウェイの検出



a) **[ポッド ID（Pod ID）]** フィールドで、ドロップ ダウン メニューからポッド ID を選択します。

b) **ノード ID** フィールドで、ノード ID をリーフ スイッチに割り当てます。

c) **[ノード名（Node Name）]** フィールドで、リーフ スイッチに名前を割り当てます。

d) **[ロール（Role）]** フィールドで、ロール タイプとしてボーダー ゲートウェイを選択します。

e) （オプション） **[ラック名（Rack Name）]**でラック名を指定します。

f) **[登録（Register）]**をクリックします。

次のタスク

に記載されている手順を使用して、ボーダー ゲートウェイ セットを作成します。 GUI を使用してボーダー ゲートウェイ セットを作成 （29 ページ）

GUI を使用した VXLAN インフラ L3Out の構成

VXLAN インフラ L3Out 構成では、 ACI ボーダー ゲートウェイ ノードとインターフェイスを選択して、サイト間ネットワーク インフラストラクチャ（ISN）のネットワーク デバイス部分との EBGP アンダーレイ隣接関係を確立できます。これは、リモート NX-OS ボーダー ゲートウェイとアンダーレイ到達可能性情報を交換し、それらとのオーバーレイ EVPN 隣接関係を確立するために必要です。

VXLAN インフラ L3Out を構成する場合は、次の項目を構成します：

- ACI ボーダー ゲートウェイ セットを構成します。 GUI を使用してボーダー ゲートウェイ セットを作成 （29 ページ）を参照してください。
- リモート VXLAN ファブリックを構成します。 GUI を使用したリモート VXLAN ファブリックの構成 （30 ページ）を参照してください。
- **[ノード（Nodes）]**
  - ボーダーゲートウェイのみが VXLAN インフラ L3Out のノードとして構成できます。
  - 各 VXLAN インフラ L3Out は、同じ ACI マルチポッド ファブリックの一部である複数のポッドからのボーダー ゲートウェイを持つことが必要です。
  - ボーダー ゲートウェイは、単一の VXLAN インフラ L3Out またはお使いの QoS ポリシーに基づいて複数の VXLAN インフラ L3Out で構成できます。
  - ノード プロファイルを構成するときに、ノードの下にルータ識別子とループバック インターフェイスを構成できます。ボーダーゲートウェイのループバック インターフェイスに割り当てられたIPアドレスは、リモート ファブリックの NX- OSボーダーゲートウェイとの BGP EVPN コントロール プレーン ピアリングを確立するために使用されます。
- **[インターフェイス（Interfaces）]**
  - サポートされるインターフェイスのタイプは次のとおりです：
    - ルーテッド インターフェイスまたはサブインターフェイス
  - また、VXLAN infra L3Out のインターフェイス タブ内にアンダーレイ BGP ピアポリシーを構成します。これは、アンダーレイ BGP 隣接関係（アジャセンシー）を持ち上げて接続済みデバイスとループバック アドレスを交換するために必要な基本的なアンダーレイ構成です。
- **[QoS ルール（QoS rules）]**

- VXLAN 入力ルールと VXLAN 出力ルールは、VXLAN インフラ インフラ L3Out の VXLAN QoS ポリシーを使用して構成できます。 GUI を使用した VXLAN カスタム QoS ポリシーの作成 （36 ページ） を参照してください。
- VXLAN QoS ポリシーを作成しない場合、入力 VXLAN トラフィックにはデフォルトの QoS レベルが割り当てられます。

また、VXLAN インフラ L3Out を使用してアンダーレイとオーバーレイ BGP 構成を構成します：

- **[アンダーレイ（Underlay）]**：インターフェイス設定の一部としての BGP ピア IP 構成。
- **[オーバーレイ（Overlay）]**：BGP EVPN リモート構成は、リモートファブリック構成の一部です。

始める前に

VXLAN EVPN ボーダー ゲートウェイとして表示するためにリーフノードが新しいノード タイプ *border-gateway* として登録されていることを確認します。詳細については、ACI ボーダー ゲートウェイの検出 （18 ページ） を参照してください。

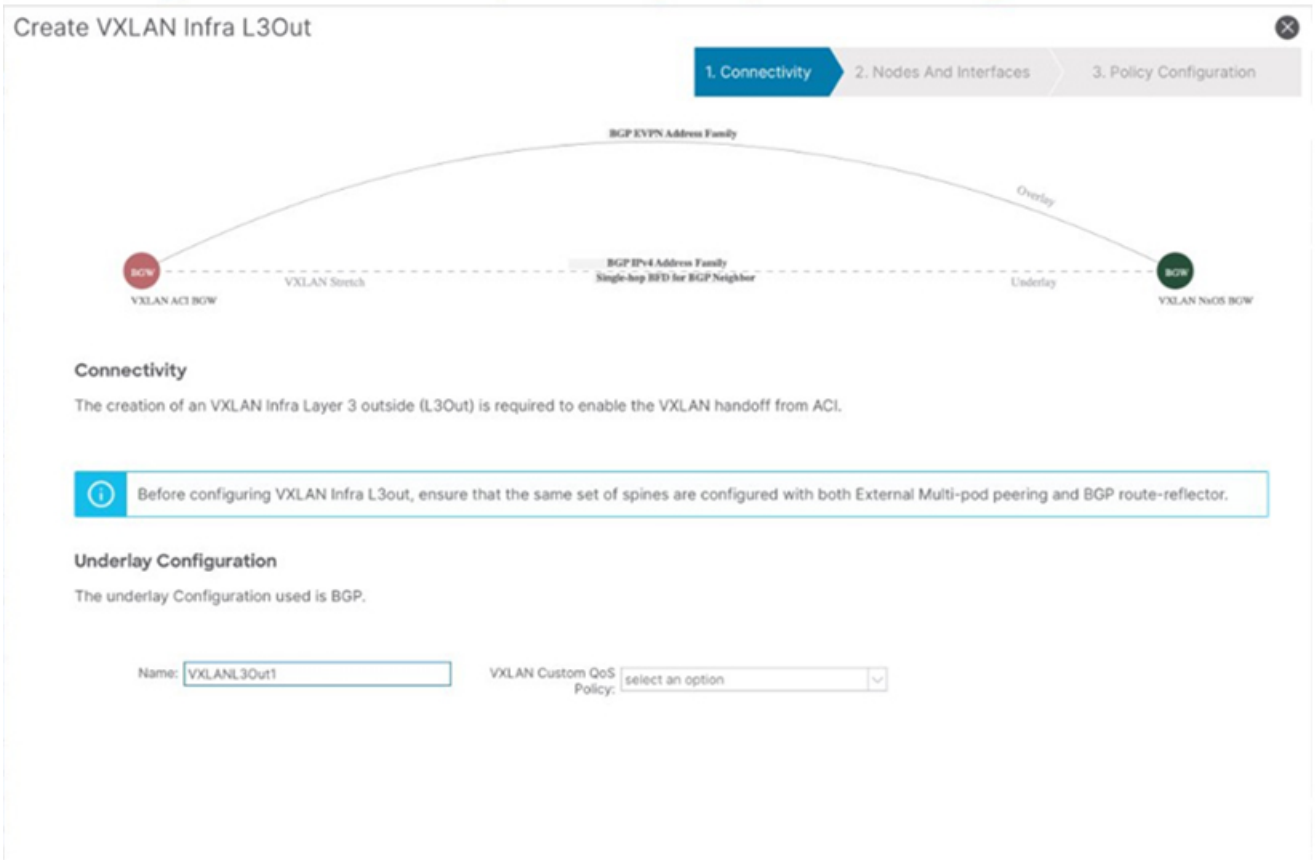
手順

ステップ 1 **[テナント（Tenants）] > [インフラ（infra）] > [ネットワーキング（Networking）] > [VXLAN L3Out（VXLAN L3Outs）]**に移動します。

ステップ 2 **[VXLAN L3Out（VXLAN L3Outs）]** を右クリックし、**[VXLAN L3Out を作成（Create VXLAN L3Out）]** を選択します。

[接続（Connectivity）] ウィンドウが表示されます。

図 *10 : VXLAN* インフラ *L3Out* 接続ウィンドウ



ステップ 3　**[接続（Connectivity）]** ウィンドウで、必要な情報を入力します。

a)　**[名前（Name）]** フィールドに VXLAN インフラ L3Out の名前を入力します。

これは外部への接続を制御するポリシーに付ける名前です。名前では最大 64 文字までの英数字を使用できます。

（注）
オブジェクトの作成後は、この名前は変更できません。

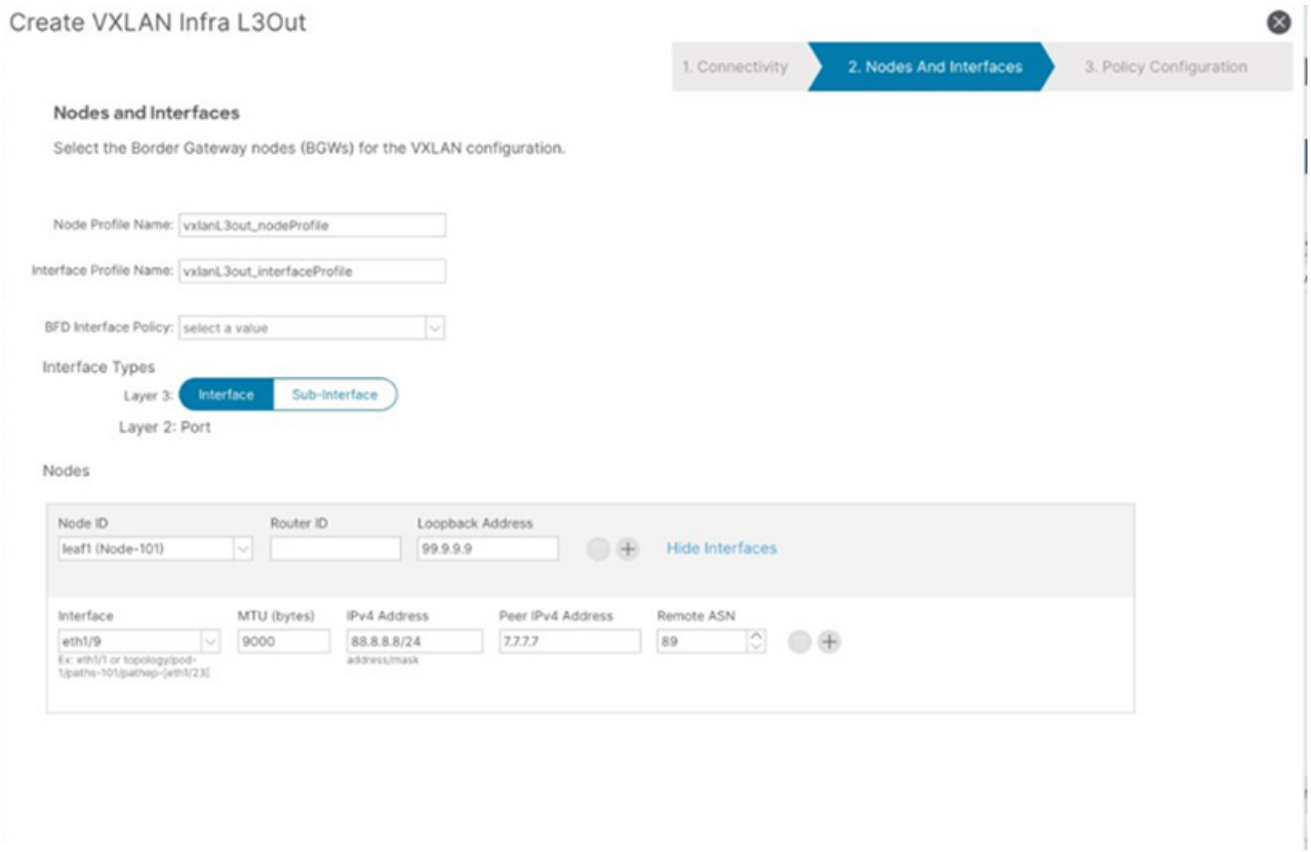
b)　（任意）　**[VXLAN カスタム QoS ポリシー（VXLAN Custom QoS Policy）]** フィールドで既存のポリシーを選択するか **[VXLAN カスタム QoS ポリシーの作成（Create VXLAN Custom QoS Policy）]** を選択して新しい QoS ポリシーを作成します。

新しい QoS ポリシーの作成の詳細については、GUI を使用した VXLAN カスタム QoS ポリシーの作成（36 ページ）を参照してください。

c)　**[次へ（Next）]**をクリックします。

[ノードとインターフェイス（Nodes and Interfaces）] ウィンドウが表示されます。

図 *11 : VXLAN* インフラ *L3Out* ノードとインターフェイスのウィンドウ



ステップ 4 **[ノードとインターフェイス（Nodes and Interfaces）]** ウィンドウで、境界ゲートウェイ ノードとインターフェイスを構成するために必要な情報を入力します。

a) **[ノード プロファイル名（Node Profile Name）]** フィールドおよび **[インターフェイス プロファイル名（Interface Profile Name）]** フィールドで、ノード プロファイル名とインターフェイス プロファイル名にデフォルトの命名規則を使用するかどうかを決定します。

デフォルト ノード プロファイル名前は、 *[L3Out-name]*[_nodeProfile]であり、デフォルトのインターフェイス プロファイル名は *[L3Out-name]*[_interfaceProfile]です。これには、*[L3Out-name]* が **[名前（Name）]** フィールドに入力した名前です。このフィールドは、**[接続（Connectivity）]** ページにあります。必要に応じて、これらのフィールドのプロファイル名を変更します。

b) （任意） **[BFD インターフェイス ポリシー（BFD Interface Policy）]** フィールドで、既存の BFD インターフェイス ポリシーを選択するか、新しい BFD インターフェイス ポリシーを作成するために **[BFD インターフェイス ポリシーを作成（Create BFD Interface Policy）]** を選択します。

c) **[インターフェイス タイプ（Interface Types）]** エリアで、レイヤ 3 およびレイヤ 2 フィールドで必要な選択を行います。

次のオプションがあります：

- レイヤ 3：

- **[インターフェイス（Interface）]**：境界リーフ スイッチを外部ルータに接続するためのレイヤ 3 インターフェイスを設定するには、このオプションを選択します。
- **[サブインターフェイス（Sub-Interface）]**：境界リーフ スイッチを外部ルータに接続するようにレイヤ 3 サブインターフェイスを設定するには、このオプションを選択します。

d) **[ノード ID（Node ID）]** フィールドのドロップダウン メニューで、 VXLAN インフラ L3Out のボーダー ゲートウェイ ノードを選択します。

ルータ ID の構成方法を説明する次の警告メッセージが画面に表示される場合があります。

リーフスイッチ 103 の動作ルータ ID は 3.3.3.3 で、このリーフとスパイン間で実行される MP-BGP セッションに使用されます。ユーザは 3.3.3.3 とは異なるルート ID を構成できますが、このリーフですでに実行されている MP-BGP セッションがフラップされます。

- このノードにルータID がまだ構成されていない場合は、 4.e （25 ページ） へ移動してこのノードのルータ ID の構成手順を参照してください。
- このノードにルータ ID がすでに設定されている場合（たとえば、以前に MP-BGP ルート リフレクタを構成していた場合）、次のオプションがあります。 **[VXLAN 構成に同じルータ ID を使用（Use the same router ID for the VXLAN configuration）]**：複数のインフラ L3Out を使用する場合は同じルータ ID です。これが推奨オプションです。次の手順で使用するためにこの警告に表示されるルータ ID をメモし、 4.e （25 ページ）。

e) **[ルータ ID（Router ID）]** フィールドに、Infra L3Out の境界ゲートウェイ スイッチ部分の一意のルータ ID（IPv4 アドレス）を入力します。

ルータ IDは、すべてのボーダー ゲートウェイ スイッチと非 ACI ファブリック ボーダー ゲートウェイで一意である必要があります。

4.d （25 ページ）で説明したように、ルータ ID がこのノードですでに構成されている場合、いくつかのオプションがあります。

- VXLAN 構成に同じルータ ID を使用する場合は、 4.d （25 ページ）の警告メッセージに表示されたルータ ID を入力します。
- 複数のインフラ L3Out を使用する場合は、同じルータID を構成する必要があります。

f) **[ループバック（Loopback）]** フィールドに IP アドレスを入力します。これは、EVPN ピアリングに使用されるルーティング可能なコントロールプレーン アドレスです。アンダーレイ プロトコルをピアてアドバタイズされます。

g) **[インターフェイス（Interface）]** フィールドで、ドロップダウン リストからポートを選択します。

h) 上記のレイヤ 3 エリアで **[サブインターフェイス（Sub-Interface）]** を選択した場合、 **[VLAN カプセル化（VLAN Encap）]** フィールドが表示されます。レイヤ 3 外部プロファイルに使用されるカプセル化を入力します。

i) **[MTU（バイト）（MTU（bytes））]** フィールドで、外部ネットワークの最大転送単位を入力します。

j) **[IPv4 アドレス（IPv4 Address）]** フィールドに、eBGP アンダーレイ構成の IP アドレスを入力します。

これは、前の手順で構成したACI ボーダー ゲートウェイ レイヤ 3 インターフェイス/サブインターフェイスに割り当てられた IP アドレスです。

k) **[ピア IPv4 アドレス（Peer IPv4 Address）]** フィールドに、eBGP アンダーレイ ユニキャスト ピア IP アドレスを入力します。

これは、ボーダー ゲートウェイ スイッチに直接接続されているルータのインターフェイスのIPアドレスです。

l) **[リモート ASN（Remote ASN）]** フィールドに、直接接続されたルータの BGP 自律システム番号を入力します。

m) VXLANインフラL3Outのこのノードに追加のインターフェイスを構成するかどうかを決定します。

- この VXLAN インフラ L3Out のこのノードに追加のインターフェイスを構成しない場合は、4.o（26 ページ）に進みます。
- このVXLANインフラL3Outのこのノードに追加のインターフェイスを構成するためにこのノードの別のインターフェイスに同じオプションを表示する場合、**[+]**をクリックします。これは、**[インターフェイス（Interfaces）]** エリアにあります。

（注）
このノードのインターフェイスに入力した情報を削除する場合、または誤って追加したインターフェイス行を削除する場合は、削除するインターフェイス行のごみ箱アイコンをクリックします。

n) この VXLAN インフラ L3Out に追加のボーダー ゲートウェイを構成するかどうかを決定します。

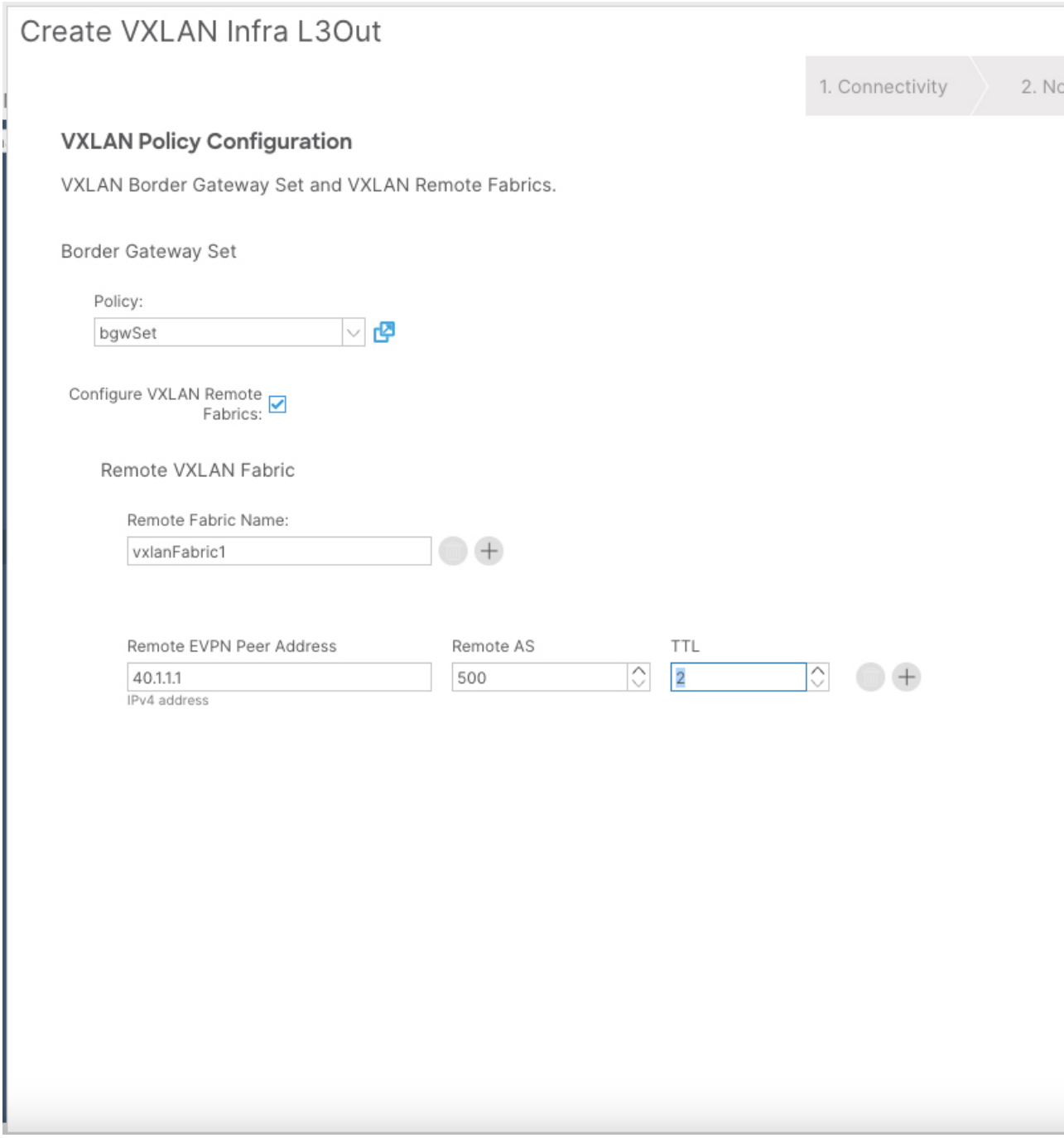
- この VXLAN インフラ L3Out に追加のボーダー ゲートウェイを構成しない場合は、4.o （26 ページ）に進みます。
- この VXLAN infra L3Out に追加のボーダー ゲートウェイを構成するために別のノード用の同じオプションを表示する場合は、**[+]** をクリックします。これは、**[ノード（Nodes）]** エリアにあります。

（注）
ノードに入力した情報を削除する場合、または誤って追加したノード行を削除する場合は、削除するノード行のごみ箱アイコンをクリックします。

o) **[次へ（Next）]**をクリックします。

[ポリシーの構成（Policy Configuration）] ウィンドウが表示されます。

図 *12 : VXLAN* インフラ *L3Out* ポリシーの構成ウィンドウ



ステップ 5 **[ポリシーの構成（Policy Configuration）]** ウィンドウで、境界ゲートウェイ ノードとインターフェイスを構成するために必要な情報を入力します。

a) **[ボーダー ゲートウェイ セット（Border Gateway Set）]** フィールドで、既存のボーダー ゲートウェイ セットを使用するか、新しいボーダー ゲートウェイ セットを作成するかを決定します。

b) **[リモート VXLAN ファブリックの構成（Configure VXLAN Remote Fabrics ）]** をチェックして次のフィールドを構成します：

1. **[リモート VXLAN ファブリック（Remote VXLAN Fabrics）]** フィールドで、既存のリモート VXLANファブリックを指定するか、 **[+]** をクリックして新しいリモート VXLAN ファブリックを作成します。
2. **[リモート EVPN ピア アドレス（Remote EVPN Peer Address）]** フィールドで、リモート EVPN アドレスを指定します。

   これは、ローカル デバイスが通信しているリモート デバイスを識別するために使用される EVPN アドレスです。リモート EVPN アドレスは、2 つのデバイス間の最初の接続を確立するために使用され、デバイス間の暗号化されたトラフィックをルーティングするためにも使用されます。
3. **[リモート AS（Remote AS）]** フィールドに、リモート NX-OS ボーダーゲート ウェイ ノードの BGP 自律システム番号を入力して、各リモート ファブリック ピアのリモート AS を構成します。
4. **[TTL]** フィールドに、接続存続可能時間（TTL）を入力します。値は、1 より大きくする必要があります。

ステップ 6 **[終了（Finish）]**をクリックして **[VXLAN インフラ L3Out ウィザードの作成（Create VXLAN Infra L3Out wizard）]**で必要な構成を完了します。

次のタスク

GUI を使用して VRF ストレッチでの VXLAN の構成 （31 ページ）に記載されている手順を使用して、VXLAN VRF ストレッチを構成します。

VXLAN サイト ID

Cisco APIC 6.1（2）以降では、サイト ID を構成する必要があります。このサイト ID がないと、ボーダー ゲートウェイ セット ポリシーを構成することはできません。

（注） Cisco APIC 6.1（1）の ACI ボーダー ゲートウェイ機能をすでに構成しているのに、VXLAN サイト ID を作成せずに Cisco APIC 6.1（2）にアップグレードすると、すべての拡張 VRF およびブリッジ ドメインで障害が発生します。

手順

ステップ 1 上部のメニュー バーから **[テナント（Tenants）] > [インフラ（infra）] > [ポリシー（Policies）] > [VXLAN ゲートウェイ（VXLAN Gateway）] > [VXLAN サイト（VXLAN Site）]** の順に選択します。。

ステップ 2 次の項目を右クリックします。**[¥VXLAN サイト（VXLAN Site）]**そして**[VXLAN の作成（Create VXLAN Site）]**を選択します。

[VXLAN の作成（Create VXLAN Site）]ウィンドウが表示されます。

ステップ 3 **[名前（Name）]** フィールドに VXLAN サイトの名前を入力します。

ステップ 4 **[ID]** フィールドに、VXLAN サイトに固有のサイト ID を入力します。

ステップ 5 （任意） **[説明（Description）]** フィールドに、説明を入力します。

ステップ 6 **[送信（Submit）]**をクリックします。

GUI を使用してボーダー ゲートウェイ セットを作成

ボーダー ゲートウェイ セットを作成するには、次の手順を実行します。：

始める前に

このポリシーは、リモートの非 ACI ファブリックとの通信に使用される、各 Pod のボーダー ゲートウェイのデータ プレーン TEP を割り当てます。これは、Pod の外部エニーキャスト TEP です。また、Cisco APIC は、ファブリック内のすべてのボーダー ゲートウェイに 1 つの内部エニーキャストTEP を割り当てます。

手順

ステップ 1 上部のメニュー バーから **[テナント（Tenants）] > [インフラ（infra）] > [ポリシー（Policies）] > [VXLAN ゲートウェイ（VXLAN Gateway）] > [ボーダー ゲートウェイ セット（Border Gateway Sets）]**の順に選択します。

ステップ 2 ボーダー ゲートウェイ設定作業ペインで、**[アクション（Actions）]>[ボーダーゲートウェイ設定ポリシーの作成（Create Border Gateway Set Policy）]**をクリックします。

ステップ 3 **[VXLAN サイト ID（VXLAN Site ID）]** フィールドは、**[VXLAN の作成（Create VXLAN Site）]** ウィンドウで以前に作成した一意のサイト ID を表示します。 **[VXLAN サイト ID（VXLAN site ID）]** を作成していない場合、作成を要求するプロンプトが表示されます。

ステップ 4 リスト **[名前（Name）]** フィールドで、ボーダー ゲートウェイ セット ポリシーに名前を割り当てます。

ステップ 5 **[外部データ プレーン IP（External Data Plane IP）]** フィールドに、各ポッドの一意のルーティング可能な IP アドレスを入力します。 **+** をクリックして **[ポッド ID（POD ID）]** および **[アドレス（Address）]**を入力します。

ステップ 6 **[送信（Submit）]**をクリックします。

次のタスク

GUI を使用したリモート VXLAN ファブリックの構成 （30 ページ）で提供されている手順を使用して、リモート VXLAN ファブリックを作成します。

GUI を使用したリモート VXLAN ファブリックの構成

リモート VXLAN ファブリックを作成するには、次の手順を実行します：

始める前に

このポリシーは、一意のリモート非ACIファブリックと、このファブリックに固有の構成を表します。リモートファブリック ポリシーは、リモートファブリックに関連付けられたボーダー ゲートウェイ セットでコントロール プレーン ピアリング接続を提供します。

手順

ステップ 1 上部のメニュー バーから **[テナント（Tenants）] > [インフラ（infra）] > [ポリシー（Policies）] > [VXLAN ゲートウェイ（VXLAN Gateway）] > [リモート VXLAN ファブリック（Remote VXLAN Fabrics）]**へ移動します。

ステップ 2 **[リモート VXLAN ファブリック（Remote VXLAN Fabrics）]** 作業ペインで、**[アクション（Actions）] > [リモートVXLANファブリックの作成（Create Remote VXLAN Fabric）]**をクリックします。

ステップ 3 **[名前（Name）]** フィールドで、VXLAN ファブリックに名前を割り当てます。

ステップ 4 ピアの IP アドレスとそれに関連するTTLを入力するには、リモート EVPN ピア セクションの **[+]** をクリックします。そして **[リモート EVPN ピアの作成（Create Remote EVPN Peer）]** ダイアログ ボックスで以下の操作を実行します：

（注）
インフラ ピア TTL の場合は、1 より大きい値を指定する必要があります。

a) **[ピア アドレス（Peer Address）]**：ピア IP アドレスを入力しますこれは、EVPN コントロールプレーン隣接関係（アジャセンシー）を確立するために使用されるリモートNX-OS BGWデバイスのループバック IP アドレスです。
b) （オプション） **[説明（Description）]** フィールドに、リモート EVPN ポリシーの説明の詳細を入力します。
c) **[リモート ASN（Remote ASN）]**：ネイバー自律システムを固有に識別する番号を入力します。自律システム番号は、1 ー 4294967295 のプレーン形式で 4 バイトにすることができます。
d) ピア タイプ フィールドで、VXLAN BGW 接続がすでに選択されています。

ステップ 5 **Ok**をクリックします。

ステップ 6 を入力します。**[関連付けられたボーダーゲートウェイ設定（Associated Border Gateway Set）]**を入力するには、ドロップダウンリストから既存のボーダーゲートウェイセットを選択するか、**[+]** をクリックし、既存のボーダー ゲートウェイ セットを選択します。これは、**[関連付けられたボーダーゲートウェイ設定（Associated Border Gateway Set）]**ボックスにあります。

ステップ 7　**[送信（Submit）]**をクリックします。

次のタスク

GUI を使用した VXLAN インフラ L3Out の構成 （21 ページ） セクションの手順に従って、VXLAN インフラ L3Out を構成します。

GUI を使用して VRF ストレッチでの VXLAN の構成

このセクションの手順を使用して、 ACIドメインと VXLAN EVPN ドメイン間でテナントVRFをストレッチできます。これにより、VXLAN データプレーンのカプセル化を利用して、これらのドメイン間のテナントのルーテッド通信を確実に実行できます。テナントVRFをストレッチする場合の特定の展開に関する考慮事項は次のとおりです。

- ストレッチされたユーザー テナント VRF は、VXLAN インフラ L3Out に関連付けられている BGW セットに関連付けられます。
- 各 VRF でサポートされる VXLAN VRF L3Out は 1 つだけです。これは、VRF を BGW に拡張するために使用されます。

始める前に

- ACI ボーダー ゲートウェイに関する注意事項と制限事項 （15 ページ）をレビューします。
- 172 ページの「GUI を使用した VXLAN ゲートウェイ インフラ L3Out の構成」に提供されている手順に従って、VXLAN ゲートウェイ インフラ L3Out を構成します。

手順

ステップ 1　**[テナント（Tenants）] > [ネットワーキング（Networking）] > [VXLAN ストレッチ（VXLAN Stretch）]** に移動します。

ステップ 2　**[VXLAN ストレッチ（VXLAN Stretch）]** を右クリックし、**[VXLAN VRF ストレッチの作成（Create VXLAN VRF Stretch）]**を選択します。

[VXLAN VRF ストレッチの作成（Create VXLAN VRF Stretch）] ウィンドウが表示されます。

ステップ 3　**[VRF]** フィールドで、既存の VRF を選択するか、FCoE の新しい VRF を作成するには、**[VRF の作成（Create VRF）]** クリックします：

a)　**[名前（Name）]** フィールドに、VRF の名前を入力します。
b)　**[エイリアス（Alias）]** フィールドに、VRF のエイリアス名を入力します。
c)　（オプション）**[説明（Description）]**フィールドに VRF も説明を入力します。

d) **[ポリシー制御適用優先設定（Policy Control Enforcement Preference）]** フィールドで、**[非強制（unenforced）]**を選択します。これにより、すべての EPG が制限なしで自由に通信できます。

各 VRF には、セキュリティ ポリシーが VRF で適用されるかどうかを定義するポリシー適用オプションがあります。デフォルトでは、 VRF は強制モードになっています。つまり、EPG 間の通信にコントラクトが必要です。VRF が非強制モードに設定されている場合、 VRF 内のすべての EPG は自由に通信できます。

e) **[ポリシー コントロール適用方向（Policy Control Enforcement Direction）]** フィールドで、**[入力（Ingress）]**を選択します。

f) **[OSPF タイマー（OSPF Timers）]** フィールドに、ドロップダウンリストから、この特定の VRF（デフォルトまたは、OSPF タイマーポリシーを作成）に関連付ける OSPF タイマーポリシー選択します。

g) **[モニタリング ポリシー（Monitoring Policy ）]** フィールドに、ドロップ ダウン リストから、この特定の VRF に関連付けるモニタリング ポリシー選択します。

h) **[送信（Submit）]**をクリックします。

ステップ 4 **[ボーダー ゲートウェイ セット（Border Gateway Set）]** フィールドで、既存のボーダー ゲートウェイ セットを選択するか、新しいボーダー ゲートウェイ セットを作成するために **[ボーダー ゲートウェイ セット（Border Gateway Set）]** をクリックします。

ステップ 5 Cisco APIC 6.1（2）以降、**[リモート ファブリック名（Remote Fabric Name）]** または **[リモート VNI（Remote VNI）]** のオプションが事前に選択されているため指定する必要がありません。

Cisco APIC 6.1（4）以降、 **[正規化された VNI（Normalized VNI）]** またはVRFのリモート EVPN ファブリックで使用されるVNI 。

（注）
[ローカル VNI（Local VNI）] は、Cisco APIC で割り当てられます。ACI ボーダー ゲートウェイは、 Cisco APIC に割り当てられたローカル VNI と構成済みの正規化された VNI 間で双方向の翻訳を実行します。

ステップ 6 **[アウトバウンド（Outbound）]**フィールドで、NX- OSサイトにアドバタイズされるルートを制御するアウトバウンドルート マップを指定します。

ルート マップの作成方法の詳細については、 ルート制御プロファイル ポリシーを参照してください。

ステップ 7 **[着信（Inbound）]**フィールドで、NX- OSファブリックからインポートされるルートを制御するインバウンドルート マップを指定します。

ルート マップの作成方法の詳細については、 ルート制御プロファイル ポリシーを参照してください。

ステップ 8 **[送信（Submit）]**をクリックします。

次のタスク

GUI を使用してブリッジ ドメイン ストレッチでの VXLAN の構成 （33 ページ）に記載されている手順を使用して、VXLAN ブリッジ ドメイン ストレッチを構成します。

GUI を使用してブリッジ ドメイン ストレッチでの VXLAN の構成

このセクションの手順を使用して、 ACI ドメインと VXLAN EVPN ドメイン間でテナント ブリッジ ドメインをストレッチできます。これにより、VXLANデータプレーンのカプセル化を活用して、これらのドメイン間のテナントのブリッジ通信を確実に実行できます。

始める前に

- ACI ボーダー ゲートウェイに関する注意事項と制限事項 （15 ページ）をレビューします。
- 172 ページの「GUI を使用した VXLAN ゲートウェイ インフラ L3Out の構成」に提供されている手順に従って、VXLAN ゲートウェイ インフラ L3Out を構成します。

手順

ステップ 1 **[テナント（Tenants）] > [ネットワーキング（Networking）] > [VXLAN ストレッチ（VXLAN Stretch）]** に移動します。

ステップ 2 **[VXLAN ストレッチ（VXLAN Stretch）]** を右クリックし、**[VXLAN BD ストレッチの作成（Create VXLAN BD Stretch）]**を選択します。

[VXLAN BD ストレッチの作成（Create VXLAN BD Stretch）] ウィンドウが表示されます。

ステップ 3 **[ブリッジ ドメイン（Bridge Domain）]** フィールドで、既存のブリッジドメインを選択するか、FCoE の新しいブリッジ ドメインを作成するには、**[ブリッジドメインの作成（Create Bridge Domain）]** をクリックします。

ステップ 4 **[ボーダー ゲートウェイ セット（Border Gateway Set）]** フィールドで、既存のボーダー ゲートウェイ セットを選択します。GUI のテキストボックスに記載されているように、ストレッチされているブリッジ ドメインに対して L2 不明ユニキャストがフラッディングに設定されていることを確認します。

ステップ 5 Cisco APIC 6.1（2）の場合、**[リモート ファブリック名（Remote Fabric Name）]** または **[リモート VNI（Remote VNI）]** のオプションはすでに指定されているので指定する必要はありません。

Cisco APIC 6.1（4）以降、**[正規化された VNI（Normalized VNI）]** または VRF のリモート EVPN ファブリックで使用される VNI を指定する必要があります。

（注）
[ローカル VNI（Local VNI）] は、Cisco APIC で割り当てられます。ACI ボーダー ゲートウェイは、 Cisco APIC に割り当てられたローカル VNI と構成済みの正規化された VNI 間で双方向の翻訳を実行します。

4

ステップ 6 **[送信（Submit）]**をクリックします。

VXLAN ストレッチ ブリッジ ドメイン セレクタ

VXLAN ストレッチ ブリッジ ドメイン セレクタを作成するには、次の手順に従います。ポリシー非認識 VXLAN EVPN ドメインを使用してこの VXLAN 拡張ブリッジ ドメイン セレクタを作成して、リモート NX-OS ボーダー ゲートウェイから受信したすべてのタイプ 2 プレフィックス（エンドポイント）を特定の ESG の一部として分類する必要があります。

手順

ステップ 1 メニューバーで、**[テナント（Tenants）]** を選び、適切なテナントを選択します。

ステップ 2 ナビゲーション ペインで、**[tenant_name]** > **[アプリケーション プロファイル（Application Profiles）]** > **[application-profile-name]** > **[エンドポイント セキュリティ グループ（Endpoint Security Groups）]** > **[esg_name]** > **[セレクタ（Selectors）]**を拡張します。

ステップ 3 次を右クリックします。**[VXLAN BD セレクタ（VXLAN BD Selector）]** そして、**[VXLAN BD セレクタの作成（Create a VXLAN BD Selector）]**を選択します。

ステップ 4 **[VXLAN BD セレクタの作成（Create a VXLAN BD Selector）]** ダイアログ ボックスに、次の情報を入力します：

a) **[ブリッジ ドメイン（Bridge Domain）]**：ドロップダウンから、マッピングするストレッチ ブリッジ ドメインを選択します。

b) **[説明（Description）]**：（オプション）セレクタの説明。

c) **[送信（Submit）]**をクリックします

外部サブネット セレクタ

次の手順に従って、外部サブネット セレクタを作成します。リモート NX- OS ボーダー ゲートウェイから受信する特定の ESG タイプ 5 プレフィックス（内部サブネットまたは外部リソース）の一部として分類するポリシー非認識 VXLAN EVPN ドメインを使用して、外部サブネット セレクタを作成する必要があります。

手順

ステップ 1 メニューバーで、**[テナント（Tenants）]** を選択し、適切なテナントを選びます。

ステップ 2 ナビゲーション ペインで、**[tenant_name]** > **[アプリケーション プロファイル（Application Profiles）]** > **[application-profile-name]** > **[エンドポイント セキュリティ グループ（Endpoint Security Groups）]** > **[esg_name]** > **[セレクタ（Selectors）]**を展開します。

ステップ 3 **[外部サブネット セレクタ（External Subnet Selectors）]** を右クリックして、**[外部サブネット セレクタの作成（Create a External Subnet Selector）]**を選択します。

ステップ 4 **[外部サブネット セレクタの作成（Create a External Subnet Selector）]** ダイアログ ボックスに、次の情報を入力します：

a) **[IP]**：照合する IP プレフィックスを指定します。

b) **[説明（Description）]**：（オプション）セレクタの説明。

c) **[共有（Shared）]**VRF に渡って外部サブネットを共有するためにチェックボックスにチェックを入れます。共有セキュリティを有効にするには、共有する共有セキュリティ フラグとサブネットを使用して外部 EPG を構成します。

d) **[送信（Submit）]**をクリックします。

（注）
完全一致は、ブリッジ ドメイン サブネットに関連するリモート プレフィックスに必要です。

VXLAN外部サブネットセレクタとして指定されたプレフィックスは、VXLAN EVPNファブリックから受信したEVPNプレフィックスと正確に一致している必要はありません。スーパーネットプレフィックスを使用して、ファブリックの外部のリソースに関するリモート プレフィックスと一致させることができ、catch-all 動作は、 **0.0.0.0/1** および **128.0.0.1** プレフィックスを指定することで（ **0.0.0.0/0**を使用できないため）を実現できます。

エンドポイント セキュリティ グループの下でリモート セキュリティ グループ タグを構成

この手順を活用、端末セキュリティ グループの下にリモート セキュリティ グループ タグを作成します。

手順

ステップ 1 メニューバーで、 **[テナント（Tenants）]** を選択し、適切なテナントを選びます。

ステップ 2 ナビゲーション ペインで ***tenant_name*** > **[アプリケーション プロファイル（Application Profiles）]** > ***application_profile_name*** > **[エンドポイント セキュリティ グループ（Endpoint Security Groups）]**を選択します。

ステップ 3 **[エンドポイント セキュリティ グループ（Endpoint Security Groups）]** を右クリックして、 **[エンドポイント セキュリティ グループの作成（Create Endpoint Security Group)]**を選択します。

ステップ 4 **[ステップ 1 > アイデンティティ（STEP 1 > Identity）]** ページの **[エンドポイント セキュリティ グループの作成（Create Endpoint Security Group)]** ダイアログ ボックスに、次の情報を入力します：

a) **[名前（Name）]**：ESG の名前を入力します。

b) （任意） **[説明（Description）]**：ESG の説明を入力します。

c) **[VRF]**：ESG に関連付けられる VRF を入力します。

d) **[リモート pcTag の設定（Set Remote pcTag）]**： **[リモート pcTag の設定（Set Remote pcTag）]** チェックボックスをオンにして、リモート pcTag を設定します。

e) **[リモート pcTag（Remote pcTag）]**：Cisco ACI ファブリックと NX-OS サイト間のセキュリティで保護されたグループ変換（SGT）に使用されるリモート pcTag の値を指定します。

f) **[管理状態（Admin State）]**：ESG をシャットダウンするには、**[管理シャットダウン（Admin Shut）]** を選択します。デフォルトで、**[ESG 管理状態（ESG Admin State）]** には、**[管理アップ（Admin Up）]** の値があります。このフィールドは、5.2（3）リリースから追加されました。

g) **[展開の緊急性（Deployment Immediacy）]**：ESG のデプロイメントの即時性を指定するには、**[オンデマンド（On Demand）]** または **[即時（Immediate）]**を選択します。

ESG は常に **[オンデマンド（On-demand）]**の即時展開によって展開され、関連するコントラクトルールは、ESG セレクタに一致するエンドポイントが特定のリーフノードで学習された後にのみプログラムされます。Cisco ACI リリース 6.1（4）以降、**[即時（Immediate）]**オプションを選択して ESG を展開することもできます。

ESG で構成された外部プレフィックス/サブネットと一致する外部サブネット セレクタ、外部 EPG セレクタ、またはタグ セレクタのいずれかがある場合、**[即時（Immediate）]**オプションは自動的に適用されます。

h) **[次へ（Next）]**をクリックします。

[ステップ 2 > セレクタ（STEP 2 > Selectors）] ページ（**[エンドポイント セキュリティ グループの作成（Create Endpoint Security Group)]** ダイアログ ボックス内）が開きます。

GUI を使用した VXLAN カスタム QoS ポリシーの作成

VXLAN カスタム QoS ポリシーは、VXLAN QoS 入力ポリシーで定義されている着信内部 DSCP 値に基づいて ACI ファブリック内の転送時に VXLAN EVPN ファブリックから来るパケットのプライオリティを定義します。これらの CoS / DSCP 値は、内部ヘッダーで設定されます。また、VXLAN CoS 出力ポリシーで定義された IPv4 DSCP 値に基づくリモート VXLAN EVPN ファブリックへ向かって ACI ファブリックから離れる VXLAN カプセル化されたパケットの外部ヘッダーの CoS 値および DSCP 値をマーキングします。カスタム イーグレス ポリシーが定義されていない場合、ACI ファブリックを離れる前に、外部 DSCP および CoS の値はデフォルト値のゼロに設定されます。

手順

ステップ 1 上部のメニューバーから **[テナント（Tenants）] > [インフラ（infra）] > [ネットワーキング（Networking）] > [VXLAN L3Out（VXLAN L3Outs）]**に移動します。

ステップ 2 **[VXLAN L3Out（VXLAN L3Outs）]**を右クリックし、**[VXLAN L3Out を作成（Create VXLAN L3Out）]** を選択します。

ステップ 3 **[接続（Connectivity）]** ウィンドウで、必要な情報を入力します。

ステップ 4 **[VXLAN カスタム QoS ポリシー（VXLAN Custom QoS Policy）]** フィールドで既存のポリシーを選択するか **[VXLAN カスタム QoS ポリシーの作成（Create VXLAN Custom QoS Policy）]** を選択します。

ステップ 5 開く **[VXLAN カスタム QoS ポリシーの作成（Create VXLAN Custom QoS Policy）]** ウィンドウで、作成するポリシーの名前と説明を入力します。

ステップ 6 **[VXLAN 入力ルール（VXLAN Ingress Rule）]** エリアで、入力 QoS 変換ルールを追加するには、**[+]** をクリックします。

ACI ファブリックに接続されている境界ゲートウェイに着信するデータ トラフィックは、内部 DSCP 値に対してチェックされ、一致が検出されると、トラフィックは ACI QoS レベルに分類され、内部ヘッダーに設定されている適切な COS および DSCP 値でマークされます。

a) **[優先順位（Priority）]** フィールドで、入力ルールの優先順位を選択します。

これは、ACI ファブリック内のトラフィックに割り当てる QoS レベルで、ACI はファブリック内のトラフィックのプライオリティを決めるために使用します。これにより、iVXLAN カプセル化トラフィックの外部ヘッダーに設定されている COS 値が決定され、 ACI ファブリック内で優先順位を付けることができます。

オプションの範囲は レベル 1 ー レベル 6です。デフォルト値は、レベル 3です。このフィールドで選択しない場合、トラフィックには自動的に レベル 3 の優先順位が割り当てられます。

b) **[DSCP 照合開始（Match DSCP From）]** および **[DSCP 照合終了（Match DSCP To）]** ドロップダウンを使用して、照合するリモートVXLAN EVPNドメインからのVXLANトラフィックの内部DSCP値の範囲を指定します。

c) **[ターゲット DSCP（Target DSCP）]**で、パケットが ACI ファブリック内にある場合にパケットに割り当てる外部 DSCP 値を選択します。

d) **[ターゲット COS（Target COS）]** フィールドで、ヘッダー内のパケットが ACI ファブリック内にある場合にパケットに割り当てる COS 値を選択します。

指定された COS 値は、VXLAN EVPN ドメインから受信した元のトラフィックに設定されるため、トラフィックが宛先 ACI リーフ ノードで VXLAN カプセル化解除された場合にのみ再公開されます。

デフォルトは未指定です。つまり、ファブリックで COS 保存オプションが有効になっている場合にのみ、パケットの元の COS 値が保持されます。

e) 入力ルールを保存するには、**[更新（Update）]** をクリックします。

f) 追加の入力 COS ポリシー ルールについて、この手順を繰り返します。

ステップ 7 **[VXLAN 出力ルール（VXLAN Egress Rule）]** エリアで、出力 QoS 変換ルールを追加するには **[+]** をクリックします。

a) **[DSCP 照合開始（Match DSCP From）]** および **[DSCP 照合終了（Match DSCP To）]** ドロップダウンを使用して、ACI リーフ ノードによって発信され、一致させたい ACI ボーダー ゲートウェイによって受信される iVXLAN トラフィックの内部 DSCP 値の範囲を指定し、リモートVXLAN EVPN ドメイン宛ての VXLAN トラフィックに外部 COS および DSCP 値を割り当てます。

b) **[ターゲット オーバーレイ DSCP（Target Overlay DSCP）]** ドロップダウンから、出力 VXLAN パケットに割り当てる外部 DSCOP 値を選択します。

c) **[ターゲット COS（Target COS）]** ドロップダウンから、出力 VXLAN パケットに割り当てる外部 COS 値を選択します。

d) 入力ルールを保存するために **[更新（Update）]** をクリックします。

e) 追加の出力 QoS ポリシー ルールについて、この手順を繰り返します。

ステップ 8 カスタム VXLAN QoS の作成を完了させるために **[OK]** をクリックします。

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