Cisco APIC レイヤ 3 ネットワーク構成ガイド、リリース 5.3(x)

最終更新：2024 年 10 月 25 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

Trademarks

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: http://www.cisco.com/go/softwareterms.Cisco product warranty information is available at http://www.cisco.com/go/warranty. US Federal Communications Commission Notices are found here http://www.cisco.com/c/en/us/products/us-fcc-notice.html.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

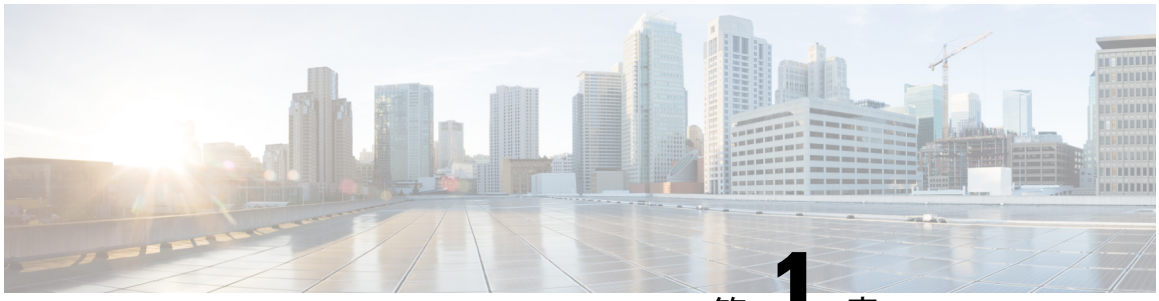
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com go trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

Trademarks

目 次



第 1 章

新機能および変更された機能に関する情報

この章は、次の内容で構成されています。

新機能および変更された機能に関する情報

次の表は、現行リリースに至るまでにガイドの編成と特徴に加えられた主な変更点の概要を示しています。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

表 *1 : Cisco APIC* リリース *6.0(4)* の新機能と変更された動作

機能または変更	説明	参照先
該当なし	このドキュメントには、以前のリリースからの変更はありません。	なし

表 *2 : Cisco APIC* リリース *6.0(3)* の新機能と変更された動作

機能または変更	説明	参照先
該当なし	このドキュメントには、以前のリリースからの変更はありません。	なし

新機能および変更された機能に関する情報

表 *3 : Cisco APIC* リリース *6.0(2)* の新機能と変更された動作

機能または変更	説明	参照先
BGP の追加パス	BGP は、以前のパスに代わる新しいパスなしで、BGP スピーカが同じプレフィックスに対して複数のパスを伝播し、受け入れることを可能にする追加のパス機能をサポートします。この機能は、BGP スピーカのピアが、プレフィックスごとの複数パスのアドバタイズおよび受信をサポートし、また、そのパスのアドバタイズをサポートするかどうかネゴシエートすることを可能にします。	BGP 付加パス （321 ページ）
ストライプ ウィナー ポリシーの設定について	ファブリックは、特定のマルチキャスト グループやグループ範囲、送信元や送信元範囲向けのポッドを選択できる、構成可能なストライプ ウィナー ポリシーをサポートするようになりました。これにより、ストライプ ウィナーとして選択されたボーダー リーフが、選択されたポッドからのものであることが保証されます。	ストライプ ウィナー ポリシーの設定について （83 ページ）

新機能および変更された機能に関する情報

機能または変更	説明	参照先
比例等コスト マルチパス（ECMP）ルーティング	ネクストホップ伝播および接続ホスト再配布機能を使用して、Cisco ACI ファブリック内の最適でないルーティングを回避できます。これらの機能が有効になっている場合、非境界リーフ スイッチからのパケット フローは、ネクストホップ アドレスに接続されているリーフ スイッチに直接転送されます。すべてのネクストホップがハードウェアからの ECMP 転送に使用されるようになりました。さらに、Cisco ACI は、直接接続されたネクストホップと再帰ネクストホップの両方の ECMP パスを BGP に再配布するようになりました。	Cisco ACI の等コスト マルチパス ルーティングについて（315 ページ）

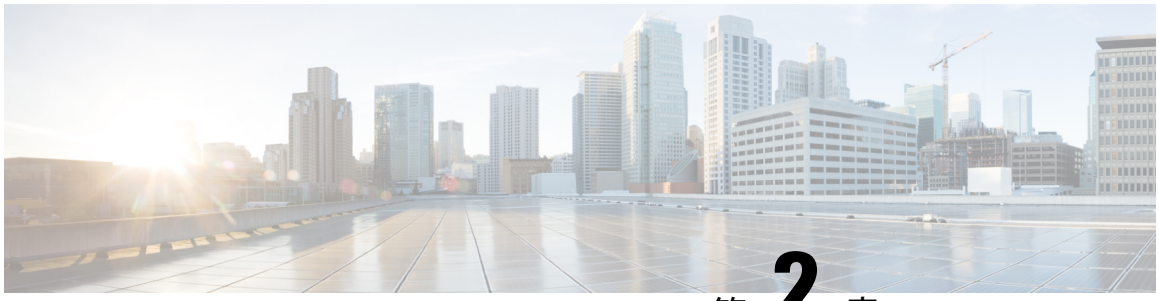
表 *4 : Cisco APIC* リリース *6.0(1)* の新機能と変更された動作

機能または変更	説明	参照先
最大 /28 のサブネット マスクのリモート プール	/28 までのサブネットマスクを使用してリモート プールを構成できるようになりました。	リモート リーフ スイッチ（141 ページ）
BGP 自律システム（AS）番号	• **[プライベート AS の削除（Remove Private AS）]** オプションを使用して、eBGP ルートの AS_path からプライベート AS 番号を削除できるようになりました。 • BGP ピアごとのルートマップを作成する際の AS-Path マッチ句のサポート。	GUI を使用したセカンダリ IP アドレスでの双方向フォワーディング検出の構成（344 ページ） GUI を使用した BGP ピアごとのルート制御の設定（377 ページ）

新機能および変更された機能に関する情報

第 部

レイヤ 3 の設定



第 2 章

Cisco ACI 転送

ファブリック内での転送

ACI ファブリックは現代のデータ センター トラフィック フローを最適化する

Cisco ACI アーキテクチャは、従来のデータセンター設計から来る制限を解放して、最新のデータセンターで増大する East-West トラフィックの需要に対応します。

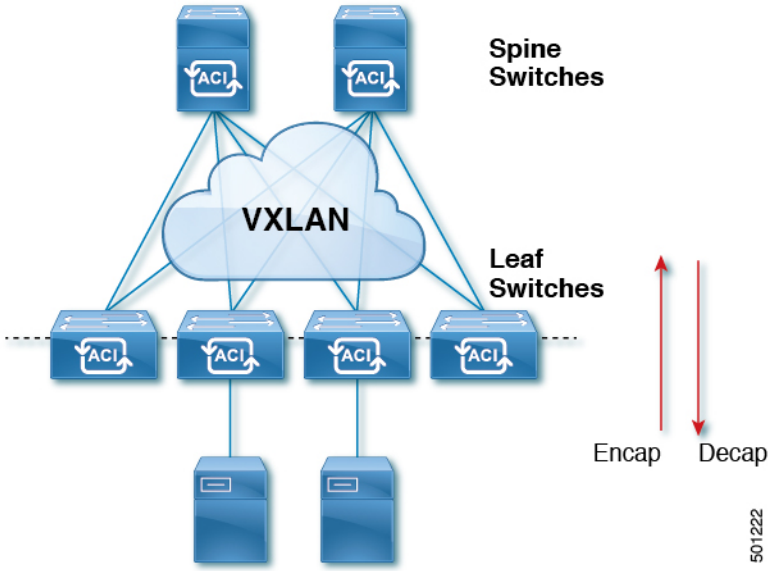
今日のアプリケーション設計は、データセンターのアクセス レイヤを通る、サーバ間の East-West トラフィックを増大させています。このシフトを促進しているアプリケーションには、Hadoop のようなビッグデータの分散処理の設計 、VMware vMotion のようなライブの仮想マシンまたはワークロードの移行、サーバのクラスタ リング、および多層アプリケーションなどが含まれます。

North-South トラフィックは、コア、集約、およびアクセス レイヤ、またはコラプスト コアとアクセス レイヤが重要となる、従来型のデータセンター設計を推進します。クライアントデータはWAN またはインターネットで受信され、サーバの処理を受けた後、データセンターを出ます。このような方式のため、WAN またはインターネットの帯域幅の制限により、データセンターのハードウェアは過剰設備になりがちです。ただし、スパニング ツリー プロトコルが、ループをブロックするために要求されます。これは、ブロックされたリンクにより利用可能な帯域幅を制限し、トラフィックが準最適なパスを通るように強制する可能性があります。

従来のデータセンター設計においては、、IEEE 802.1Q VLAN がレイヤ 2 境界の論理セグメンテーションまたはまたはブロードキャスト ドメインを提供します。ただし、ネットワーク リンクの VLAN の使用は効率的ではありません。データセンター ネットワークでデバイスの配置要件は柔軟性に欠け、VLAN の最大値である 4094 の VLAN が制限となり得ます。IT 部門とクラウドプロバイダが大規模なマルチテナント データセンターを構築するようになるにつれ、VLAN の制限は問題となりつつあります。

スパイン リーフ アーキテクチャは、これらの制限に対処します。ACI ファブリックは、外界からは、ブリッジングとルーティングが可能な単一のスイッチに見えます。レイヤ 3 のルーティングをアクセス レイヤに移動すると、最新のアプリケーションが必要としている、レイヤ 2 の到達可能性が制限されます。仮想マシン ワークロード モビリティや一部のクラスタ リングのソフトウェアのようなアプリケーションは、送信元と宛先のサーバ間がレイヤ 2 で隣接していることを必要とします。アクセス レイヤでルーティングを行えば、トランク ダウンされた同じ VLAN の同じアクセス スイッチに接続したサーバだけが、レイヤ 2 で隣接します。ACI では、VXLAN が、基盤となるレイヤ 3 ネットワーク インフラストラクチャからレイヤ 2 のドメインを切り離すことにより、このジレンマを解決します。

図 *1 : ACI* ファブリック



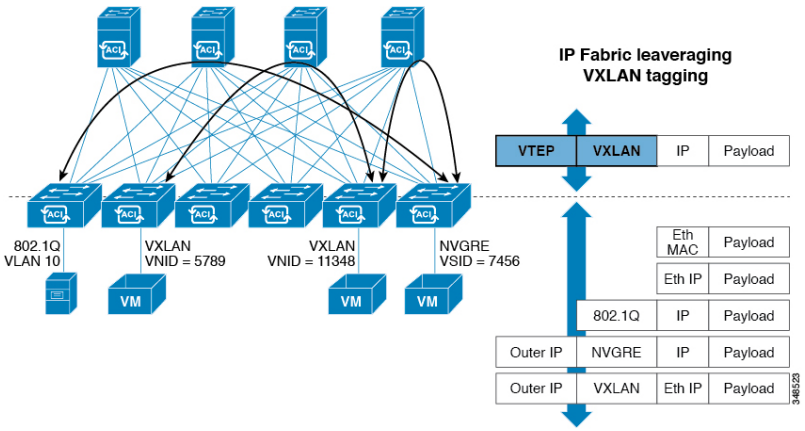
トラフィックがファブリックに入ると、ACIがカプセル化してポリシーを適用し、必要に応じてスパイン スイッチ (最大 2 ホップ) によってファブリックを通過させ、ファブリックを出るときにカプセル化を解除します。ファブリック内では、ACIはエンドポイント間通信でのすべての転送について、Intermediate System-to-Intermediate System プロトコル (IS-IS) および Council of Oracle Protocol (COOP) を使用します。これにより、すべての ACI リンクがアクティブで、ファブリック内での等コストマルチパス (ECMP) 転送と高速再コンバージョンが可能になります。ファブリック内と、ファブリックの外部のルータ内でのソフトウェア定義ネットワーク間のルーティング情報を伝播するために、 ACI はマルチプロトコル Border Gateway Protocol (MP-BGP) を使用します。

ACI で VXLAN

VXLAN は、レイヤ 2 オーバーレイの論理ネットワークを構築するレイヤ 3 のインフラストラクチャ上でレイヤ 2 のセグメントを拡張する業界標準プロトコルです。ACIインフラストラクチャ レイヤ 2 ドメインが隔離ブロードキャストと障害ブリッジ ドメインをオーバーレイ内に存在します。このアプローチは大きすぎる、障害ドメインの作成のリスクなしで大きくなるデータセンター ネットワークを使用できます。

すべてのトラフィック、ACIファブリックはVXLANパケットとして正規化されます。入力でACI VXLANパケットで外部VLAN、VXLAN、およびNVGREパケットをカプセル化します。次の図は、ACIカプセル化の正規化を示します。

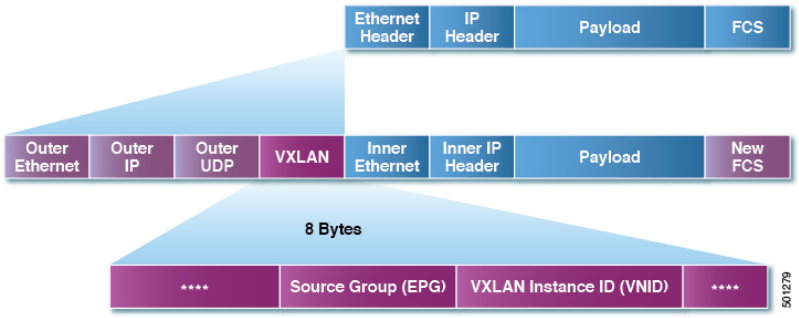
図 *2 : ACI* カプセル化の正規化



ACI ファブリックでの転送は、カプセル化のタイプまたはカプセル化のオーバーレイ ネットワークによって制限または制約されません。ACI ブリッジ ドメインのフォワーディング ポリシーは、必要な場合に標準の VLAN 動作を提供するために定義できます。

ファブリック内のすべてのパケットにACIポリシー属性が含まれているため、ACIは完全に分散された方法でポリシーを一貫して適用できます。ACIにより、アプリケーション ポリシーのEPG IDが転送から分離されます。次の図に示すように、ACI VXLANヘッダーは、ファブリック内のアプリケーション ポリシーを特定します。

図 *3 : ACI VXLAN* のパケット形式



ACIVXLAN パケットには、レイヤ 2 の MAC アドレスとレイヤ 3 IP アドレスの送信元と宛先フィールド、ファブリック内の効率的なと拡張性の転送を有効にします。ACIVXLAN パケット ヘッダーの送信元グループ フィールドは、パケットが属するアプリケーション ポリシー エンドポイント グループ (EPG) を特定します。VXLAN インスタンス ID (VNID) は、テナントの仮想ルーティングおよび転送 (VRF) ドメイン ファブリック内で、パケットの転送を有効にします。VXLAN ヘッダーで 24 ビット VNID フィールドでは、同じネットワークで一意レイヤ 2 のセグメントを最大 16 個の拡張アドレス空間を提供します。この拡張アドレス空間は、大規模なマルチ テナント データセンターを構築する柔軟性 IT 部門とクラウド プロバイダーを提供します。

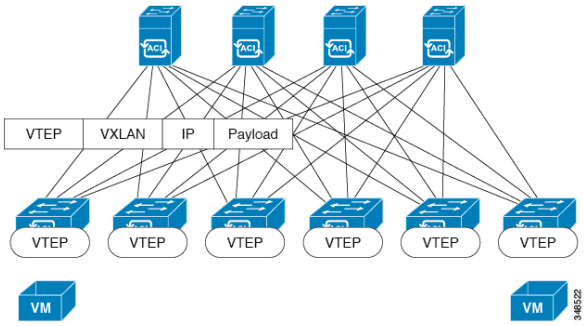
VXLANを有効にACIファブリック全体にわたってスケールでの仮想ネットワーク インフラストラクチャのレイヤ 3 のアンダーレイ レイヤ 2 を展開します。アプリケーション エンドポイント ホスト柔軟に配置できます、アンダーレイ インフラストラクチャのレイヤ 3 バウンダリのリスクなしでデータセンター ネットワーク間をオーバーレイ ネットワーク、VXLANでレイヤ 2 の隣接関係を維持します。

サブネット間のテナント トラフィックの転送を促進するレイヤ3VNID

ACI ファブリックは、ACI ファブリック VXLAN ネットワーク間のルーティングを実行するテナントのデフォルト ゲートウェイ機能を備えています。各テナントに対して、ファブリックはテナントに割り当てられたすべてのリーフ スイッチにまたがる仮想デフォルト ゲートウェイを提供します。これは、エンドポイントに接続された最初のリーフ スイッチの入力インターフェイスで提供されます。各入力インターフェイスはデフォルト ゲートウェイ インターフェイスをサポートします。ファブリック全体のすべての入力インターフェイスは、特定のテナント サブネットに対して同一のルータの IP アドレスと MAC アドレスを共有します。

ACI ファブリックは、エンドポイントのロケータまたは VXLAN トンネル エンドポイント (VTEP) アドレスで定義された場所から、テナント エンドポイント アドレスとその識別子を切り離します。ファブリック内の転送は VTEP 間で行われます。次の図は、ACI で切り離された ID と場所を示します。

図 *4: ACI* によって切り離された *ID* と場所



VXLAN は VTEP デバイスを使用してテナントのエンド デバイスを VXLAN セグメントにマッピングし、VXLAN のカプセル化およびカプセル化解除を実行します。各 VTEP 機能には、次の 2 つのインターフェイスがあります。

- ブリッジングを介したローカル エンドポイント通信をサポートするローカル LAN セグメントのスイッチ インターフェイス
- 転送 IP ネットワークへの IP インターフェイス

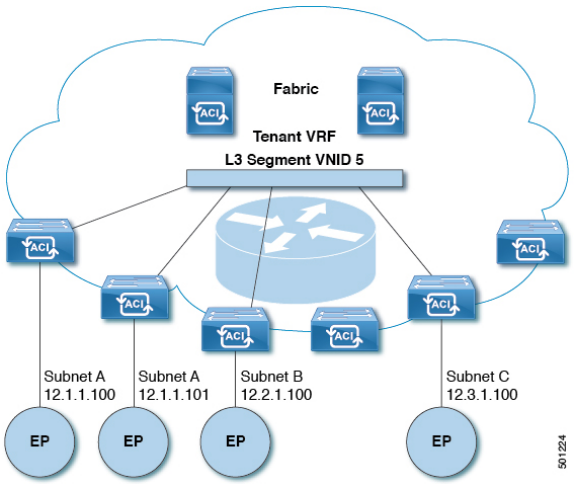
IPインターフェイスには一意のIPアドレスがあります。これは、インフラストラクチャ VLAN として知られる、転送 IP ネットワーク上の VTEP を識別します。VTEP デバイスはこの IP アドレスを使用してイーサネット フレームをカプセル化し、カプセル化されたパケットを、IP インターフェイスを介して転送ネットワークへ送信します。また、VTEP デバイスはリモート VTEP で VXLAN セグメントを検出し、IP インターフェイスを介してリモートの MAC Address-to-VTEP マッピングについて学習します。

ACI の VTEP は分散マッピング データベースを使用して、内部テナントの MAC アドレスまたは IP アドレスを特定の場所にマッピングします。VTEP はルックアップの完了後に、宛先リーフ スイッチ上の VTEP を宛先アドレスとして、VXLAN 内でカプセル化された元のデータ パケットを送信します。宛先リーフ スイッチはパケットをカプセル化解除して受信ホストに送信します。このモデルにより、ACI はスパニングツリー プロトコルを使用することなく、フル メッシュでシングル ホップのループフリー トポロジを使用してループを回避します。

VXLAN セグメントは基盤となるネットワーク トポロジに依存しません。逆に、VTEP 間の基盤となる IP ネットワークは、VXLAN オーバーレイに依存しません。これは送信元 IP アドレスとして開始 VTEP を持ち、宛先 IP アドレスとして終端 VTEP を持っており、外部 IP アドレス ヘッダーに基づいてパケットをカプセル化します。

次の図は、テナント内のルーティングがどのように行われるかを示します。

図 *5 : ACI* のサブネット間のテナント トラフィックを転送するレイヤ *3 VNID*



ACI はファブリックの各テナント VRF に単一の L3 VNID を割り当てます。ACI は、L3 VNID に従ってファブリック全体にトラフィックを転送します。出力リーフ スイッチでは、ACI によって L3 VNID からのパケットが出力サブネットの VNID にルーティングされます。

ACI のファブリック デフォルト ゲートウェイに送信されてファブリック入力に到達したトラフィックは、レイヤ 3 VNID にルーティングされます。これにより、テナント内でルーティングされるトラフィックはファブリックで非常に効率的に転送されます。このモデルを使用すると、たとえば同じ物理ホスト上の同じテナントに属し、サブネットが異なる 2 つの VM 間では、トラフィックが (最小パス コストを使用して) 正しい宛先にルーティングされる際に経由する必要があるは入力スイッチ インターフェイスのみです。

ACI ルート リフレクタは、ファブリック内での外部ルートの配布にマルチプロトコル BGP（MP-BGP）を使用します。ファブリック管理者は自律システム (AS) 番号を提供し、ルート リフレクタにするスパイン スイッチを指定します。

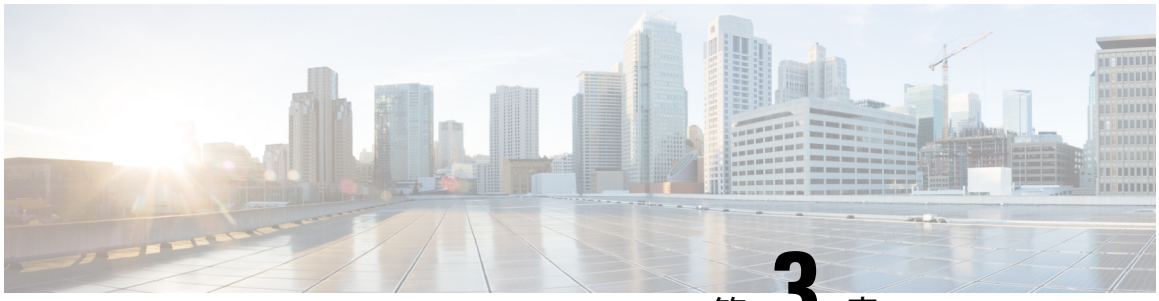
（注） Cisco ACI は IP フラグメンテーションをサポートしていません。したがって、外部ルータへのレイヤ 3 Outside（L3Out）接続、または Inter-Pod Network（IPN）を介したマルチポッド接続を設定する場合は、インターフェイス MTU がリンクの両端で適切に設定することを推奨します。

IGP プロトコル パケット（EIGRP、OSPFv3）は、インターフェイス MTU サイズに基づいてコンポーネントによって構築されます。Cisco ACI では、CPU MTU サイズがインターフェイス MTU サイズよりも小さく、構築されたパケットサイズが CPU MTU より大きい場合、パケットはカーネルによってドロップされます（特に IPv6）。このような制御パケットのドロップを回避するには、コントロールプレーンとインターフェイスの両方で常に同じ MTU 値を設定します。

Cisco ACI、Cisco NX-OS、および Cisco IOS などの一部のプラットフォームでは、設定可能な MTU 値はイーサネット ヘッダー (一致する IP MTU、14-18 イーサネット ヘッダー サイズを除く) を考慮していません。また、IOS XR などの他のプラットフォームには、設定された MTU 値にイーサネットヘッダーが含まれています。設定された値が 9000 の場合、Cisco ACI、Cisco NX-OS および Cisco IOS の最大 IP パケット サイズは 9000 バイトになりますが、IOS-XR のタグなしインターフェイスの最大 IP パケットサイズは 8986 バイトになります。

各プラットフォームの適切な MTU 値については、それぞれの設定ガイドを参照してください。

CLI ベースのコマンドを使用して MTU をテストすることを強く推奨します。たとえば、Cisco NX-OS CLI で、コマンド、ping 1.1.1.1 df-bit packet-size 9000 source-interface ethernet 1/1 を使用してください。



第 3 章

レイヤ 3 ネットワーク設定の前提条件

この章は、次の内容で構成されています。

レイヤ 3 前提条件

このガイドのタスクを開始する前に、次のことを行ってください。

- ACI ファブリックと APIC コントローラがオンラインであり、APIC クラスタが形成され健全であることを確認します— 詳細については、*Cisco APIC Getting Started Guide, Release 2.x* を参照してください。
- レイヤ 3 ネットワークを構成する管理者のファブリック管理者アカウントが使用可能であることを確認します— 詳細については、*Cisco APIC Basic Configuration Guide* の *User Access, Authentication, and Accounting* および *Management* の章を参照してください。
- 目的のリーフ スイッチとスパイン スイッチ (必要なインターフェイスを使用可能) が使用可能であることを確認します— 詳細については、*Cisco APIC Getting Started Guide, Release 2.x* を参照してください。

  仮想スイッチのインストールと登録の詳細については、*Cisco ACI Virtualization Guide* を参照してください。
- レイヤ 3 ネットワークを消費するテナント、ブリッジドメイン、VRF、および EPG (アプリケーションプロファイルとコントラクトを含む) を設定します— 詳細については、*Cisco APIC Basic Configuration Guide* の *Basic User Tenant Configuration* の章を参照してください。
- NTP、DNS サービス、および DHCP リレー ポリシーを設定します— 詳細については、*Cisco APIC Basic Configuration Guide, Release 2.x* の *Provisioning Core ACI Fabric Services* の章を参照してください。

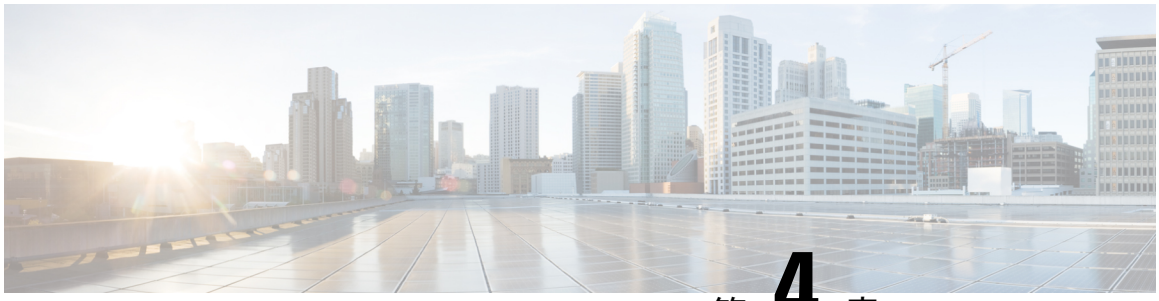
注意 ファブリックのリーフ スイッチとスパイン スイッチの間に 1 ギガビット イーサネット (GE) または 10GE リンクを設置すると、帯域幅が不十分なために、パケットが転送されずにドロップされる可能性があります。これを避けるためには、リーフ スイッチとスパイン スイッチの間で 40GE または 100GE リンクを使用してください。

ブリッジ ドメインの設定

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。



第 4 章

共通パーベイシブ ゲートウェイ

この章は、次の内容で構成されています。

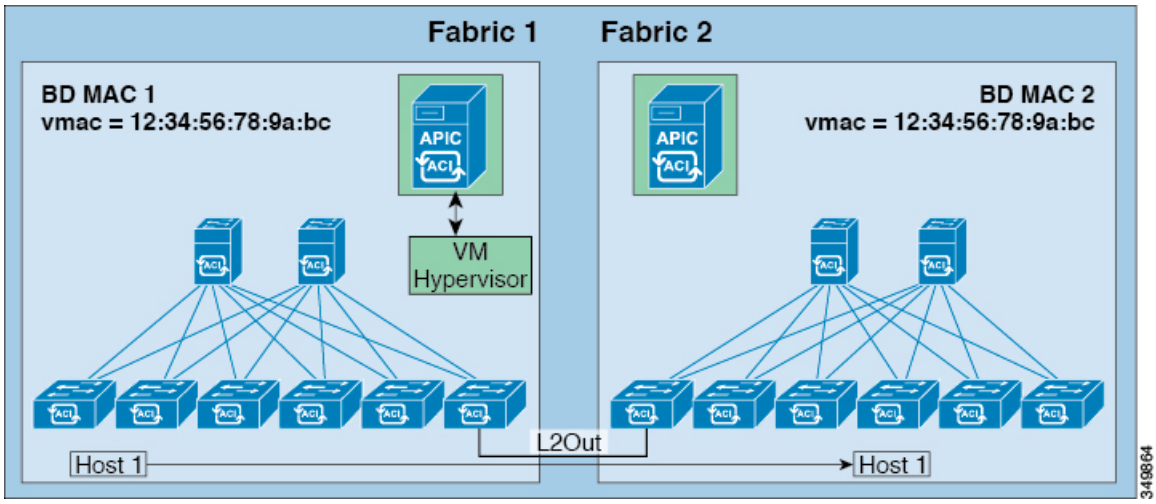
概要

（注） Common Pervasive Gateway 機能は廃止されており、アクティブに維持されていません。

複数の Cisco ACI ファブリックを運用する場合は、共通パーベイシブ ゲートウェイ機能を使用してリーフ スイッチを介して複数の個々の ACI ファブリックを相互接続するのではなく、マルチサイトを導入することを強く推奨します。Common Pervasive Gateway 機能は現在サポートされていません。これは、このトポロジでは L3 マルチキャストなどの他の多くの新機能の検証および品質保証テストが実行されないためです。したがって、Cisco ACI には Multi-Site の前に ACI ファブリックを相互接続するための共通パーベイシブ ゲートウェイ機能がありましたが、個別の APIC ドメインを相互接続する必要がある場合は、代わりに Multi-Site を使用して新しい ACI ファブリックを設計することを強く推奨します。

この例は、Cisco APIC を使用して、IPv4 共通パーベイシブ ゲートウェイを設定する方法について示しています。

ブリッジ ドメインごとに IPv4 共通ゲートウェイを使用して 2 つの ACI ファブリックを設定できます。これにより、1 つ以上の仮想マシン（VM）または従来型のホストを、ホストの IP アドレスを保持したまま、ファブリック間で移動できます。ファブリック間の VM ホストの移動は、VM ハイパーバイザによって自動的に行うことができます。ACI ファブリックは、同じ場所に配置することも、複数のサイト間でプロビジョニングすることもできます。ACI ファブリック間のレイヤ 2 接続は、ローカル リンクか、ブリッジ型ネットワークにわたるものになります。次の図は、基本的な共通パーベイシブ ゲートウェイ トポロジを示しています。



（注） 2 つの Cisco ACI ファブリックを相互接続するために用いられるトポロジによっては、相互接続するデバイスが、ゲートウェイ スイッチの仮想インターフェイス (SVI) の仮想 MAC アドレスを持つトラフィックの送信元を除外することが必要となります。

GUI を使用した共通パーベイシブ ゲートウェイの設定

始める前に

- テナントおよび VRF が作成されていること。
- ブリッジ ドメインの仮想 MAC アドレスとサブネットの仮想 IP アドレスは、ブリッジ ドメインのすべての Cisco Application Centric Infrastructure (ACI) ファブリックで同じにする必要があります。複数のブリッジ ドメインを、接続されている Cisco ACI ファブリック間で通信するように設定できます。仮想 MAC アドレスと仮想 IP アドレスは、ブリッジ ドメイン間で共有できます。
- Cisco ACI ファブリック間で通信するように設定されているブリッジ ドメインは、[**フラッド（flood）**] モードである必要があります。
- BD に複数の EPG がある場合、ブリッジ ドメインの 1 つの EPG のみを、2 つ目のファブリックに接続されているポートの境界リーフ上に設定する必要があります。
- 2 つの Cisco ACI ファブリック間のパーベイシブ共通ゲートウェイを有効にする相互接続されたレイヤ 2 ネットワークには、ホストを直接接続しないでください。

手順

ステップ 1 メニュー バーで、**[テナント]** をクリックします。

ステップ 2 [**ナビゲーション（Navigation）**] ペインで、**[*Tenant_name*]** > **[ネットワーキング（Networking）]** > **[ブリッジ ドメイン（Bridge Domains）]** の順に展開します。

ステップ 3 **[Bridge Domains]** を右クリックし、**[Create Bridge Domain]** をクリックします。

ステップ 4 **[Create Bridge Domain]** ダイアログ ボックスで、必要な操作を実行し、適切な属性を選択します。

a) **[Main]** タブで、**[Name]** フィールドにブリッジ ドメインの名前を入力し、残りのフィールドに必要な値を選択します。

b) **[L3 configurations]** タブで **[Subnets]** を展開し、**[Create Subnets]** ダイアログボックスの **[Gateway IP]** フィールドに IP アドレスを入力します。

たとえば、192.0.2.1/24 です。

c) **[Treat as virtual IP address]** フィールドで、チェックボックスをオンにします。

d) **[Make this IP address primary]** フィールドで、DHCP リレーにこの IP アドレスを指定するチェックボックスをオンにします。

このチェック ボックスをオンにすると、DHCP リレーにのみ影響します。

e) [OK] をクリックし、[次（Next）] をクリックして [アドバンス/トラブルシューティング（Advanced/Troubleshooting）] タブに進み、[終了（Finish）] をクリックします。

ステップ 5 **[Work]** ペインで作成した**Bridge Domain** をダブルクリックし、次の操作を実行します。

a) [**ポリシー（Policy**）] タブをクリックして、[**L3 コンフィグレーション（L3 Configurations**）] サブタブをクリックします。

b) もう一度 [**サブネット（Subnets**）] を展開し、仮想 IP アドレスとして設定されているものと同じサブネットを使用して、[**サブネットの作成（Create Subnets**）] ダイアログ ボックスの [**ゲートウェイ IP（Gateway IP**）] フィールドで物理 IP アドレスを作成します。

たとえば、仮想 IP アドレスに 192.0.2.1/24 を使用した場合、物理 IP アドレスには 192.0.2.2/24 を使用できます。

（注） 物理 IP アドレスは Cisco ACI ファブリック全体で一意である必要があります

c) [送信（Submit）] をクリックして [サブネットの作成（Create Subnet）] ウィンドウで設定を完了します。

ステップ 6 作成したブリッジ ドメインと同じブリッジ ドメインの [L3 コンフィグレーション（L3 Configurations）] タブで、[仮想 MAC アドレス（Virtual MAC Address）] フィールドをクリックし、[設定なし（Not Configured）] を適切な値に変更して、[送信（Submit）] をクリックします。

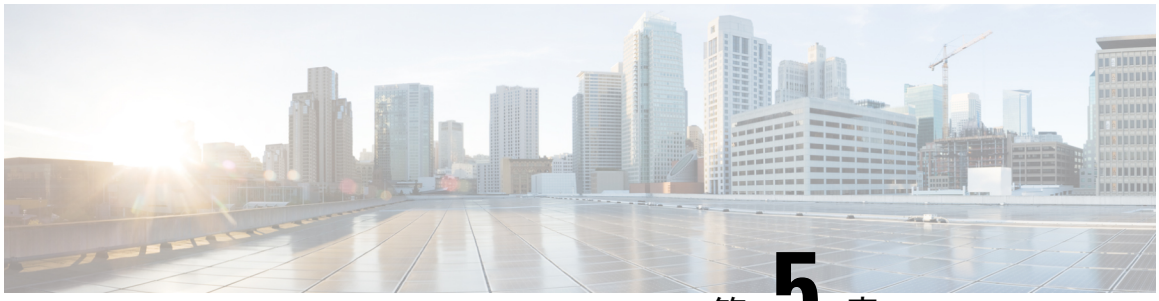
（注） デフォルト ブリッジ ドメインの MAC アドレス値はすべての Cisco ACIファブリックで同じです。この設定では、ブリッジ ドメイン MAC 値が各 Cisco ACIファブリックで一意である必要があります。

各ファブリックのブリッジ ドメイン MAC (pMAC) 値が一意であることを確認してください。

（注） この手順では、基本的に、このフィールドに入力した仮想 MAC アドレスと前の手順で入力した仮想 IP アドレスを関連付けます。将来のある時点で仮想 MAC アドレスを削除する場合は、前の手順で入力した IP アドレスの [仮想 IP アドレスとして扱う（Treat as virtual IP address）] フィールドのチェックも外す必要があります。

ステップ 7 ブリッジドメインを別のファブリックに拡張するために L2Out EPG を作成するには、[ナビゲーション（Navigation）] ペインで **[L2Outs]** を右クリックし、**[L2Out の作成（Create L2Out）]** をクリックして、次のアクションを実行します。

a) **[Name]** フィールドに、ブリッジされる Outside の名前を入力します。
b) **[Bridge Domain]** フィールドで、すでに作成されているブリッジ ドメインを選択します。
c) **[Encap]** フィールドに、その他のファブリック l2out カプセル化に一致する VLAN カプセル化を入力します。
d) **[Path Type]** フィールドで、**[Port]**、**[PC]**、または **[VPC]** を選択して EPG を導入し、**[Next]** をクリックします。
e) 外部 EPG ネットワークを作成するには、**[Name]** フィールドをクリックしてネットワークの名前を入力し (QoS クラスの指定も可能) 、**[Finish]** をクリックして共通パーベイシブ設定を完了します。



第 5 章

IP エージング

この章は、次の内容で構成されています。

概要

IP エージング ポリシーは、エンドポイントの未使用の IP アドレスを追跡しエージングが行われます。トラッキングはブリッジ ドメインに設定されたエンドポイント保持ポリシーを使用して実行され、ローカル エンドポイント エージング間隔の 75% で、ARP 要求（IPv4）やネイバー要請（IPv6）を送信します。IP アドレスから応答を受信しなかった場合、その IP アドレスはエージング アウトします。

このドキュメントでは、IP エージング ポリシーを設定する方法について説明します。

GUI を使用した IP エージングポリシーの設定

このセクションでは、IP エージング ポリシーの有効と無効を切り替え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、**System** タブをクリックします。

ステップ 2 サブメニュー バーで、**System Settings** をクリックします。

ステップ 3 ナビゲーション ウィンドウで、**Endpoint Controls** をクリックします。

ステップ 4 作業ウィンドウで、**Ip Aging** をクリックします。
IP Aging Policy が、**Administrative State** の **Disabled** ボタンが選択された状態で表示されます。

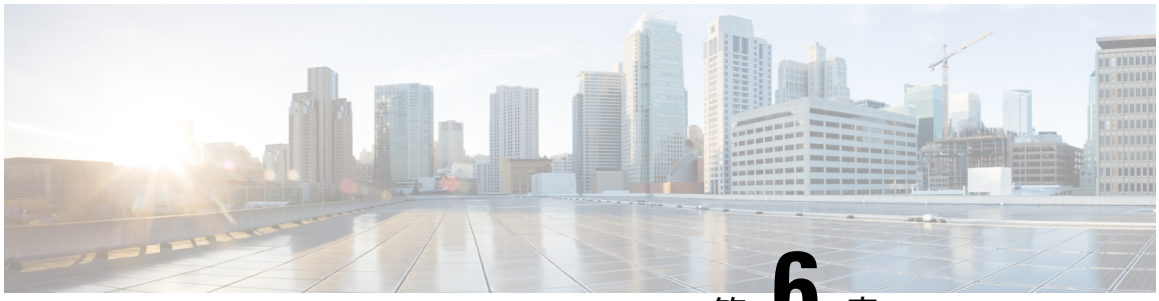
ステップ 5 **Administrative State** で、次のオプションのいずれかをクリックします:

- **Enabled**— IP エージングを有効にします。

- **Disabled**— IP エージングを無効にします。

次のタスク

エンドポイントの IP アドレスを追跡するために使用される間隔を指定するには、エンド ポイント保持ポリシーを作成します。**Tenants** > ***tenant-name*** > **Policies** > **Protocol** に移動し、**End Point Retention** を右クリックし、**Create End Point Retention Policy** を選択します。



第 6 章

スタティック ルート ブリッジ ドメイン

この章は、次の内容で構成されています。

スタティック ルート ブリッジ ドメインについて

Cisco APIC リリース 3.0(2) では、ファイアウォールの背後にある仮想サービスへのルーティングを可能にする、パーベイシブ ブリッジ ドメイン (BD) でのスタティック ルート設定へのサポートが追加されました。

この機能は、通常の EPG の使用を通して、エンドポイント (EP) がパーベイシブ ブリッジ ドメインに直接には接続されていない IP アドレスへ到達することを可能にします。

スタティック ルートを設定すると、APIC は、それをブリッジ ドメインを使用しているすべてのリーフ スイッチ、およびそのブリッジ ドメインに関連付けられた契約を有しているすべてのリーフ スイッチに展開します。

エンドポイントの到達可能性は、APIC GUI、NX-OS スタイル CLI および REST API を使用して設定できます。

注意事項と制約事項

- サブネットマスクは、/32（IPv6 の場合は /128） にしてファブリック内の 1 つの IP アドレスをポイントする必要があります。すでに定義されているブリッジ ドメインサブネット内にルートを追加しないでください。
- ネクストホップは、この EPG が関連付けられているのと同じブリッジ ドメイン内にある必要があります。
- この機能は、名前の末尾が EX である Cisco Nexus 9000 シリーズ スイッチとそれ以降の機種によりサポートされています (たとえば N9K-C93180LC-EX)。

GUI を使用してブリッジ ドメインでのスタティック ルートを設定する

- スタティック ルートのサブネットを作成するには、epg (fvAEPg で fvSubnet オブジェクト)、普及 BD (fvBD) 自体 BD しないに関連付けられているように構成されます。
- サブネットマスクが/32 にする必要があります (128/for IPv6) 1 つの IP アドレスまたは 1 つのエンドポイントをポイントします。これは、パーベイシブ BD に関連付けられている EPG に含まれます。

始める前に

テナント、VRF、BD、および EPG の作成

手順

ステップ 1 メニュー バーで、**Tenants** > ***tenant-name*** の順にクリックします。

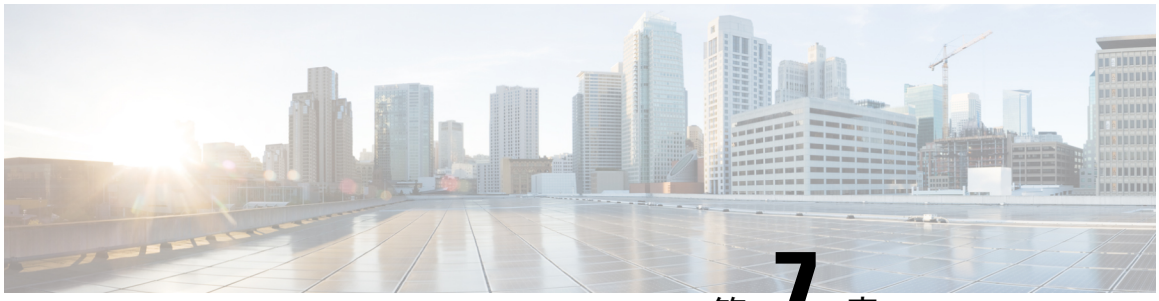
ステップ 2 ナビゲーション ウィンドウで **Application Profiles** を展開し、アプリケーション プロファイル名をクリックします。

ステップ 3 **Application EPGs** をクリックして、スタティック ルートの EPG を展開します。

ステップ 4 **Subnets** を展開して、スタティック ルートのサブネットを右クリックし、**Create Endpoints Behind EPG Subnet** を選択します。

ステップ 5 エンドポイントの **NextHop IP Address** を入力して、**Update** をクリックします。

ステップ 6 [Submit] をクリックします。



第 7 章

データプレーン IP アドレス学習

この章は、次の内容で構成されています。

データプレーン IP アドレス ラーニングの概要

エンドポイントの IP アドレスと MAC アドレスは、ARP、GARP、ND などの一般的なネットワーク方式を通じて（）ファブリックによって学習されます。また、データプレーンを介して IP アドレスと MAC アドレスを学習する内部方式も使用します。Cisco Application Centric InfrastructureACICisco ACIファブリックでは、データプレーン IP アドレスの学習がデフォルトで有効になっています。Cisco ACI

VRF インスタンスごとのデータプレーン IP アドレス ラーニングは、エンドポイント ラーニングと同じように Cisco ACI ネットワークに固有です。エンドポイント ラーニングが IP アドレスおよび MAC アドレスの両方として特定される一方、データプレーン IP ラーニングは VRF インスタンスのみの IP アドレッシングに固有です。Cisco Application Policy Infrastructure Controller（APIC）では、VRF インスタンス レベルでデータプレーン IP アドレス ラーニングを有効または無効にできます。

リリース5.2(1) 以降では、より詳細な制御のために、特定のエンドポイントまたはサブネットのデータプレーン IP アドレス ラーニングをディセーブルにできます。Cisco APIC

データプレーンIPアドレス ラーニングのガイドラインと制限事項

VRF インスタンス、ブリッジ ドメイン サブネット、および EPG サブネットごとのデータプレーン IP アドレス学習には、次のガイドラインと制約事項が適用されます。

- データプレーン IP アドレス ラーニングを無効にすると、テナント VRF 内のリモート IP アドレスのすべてのエントリが削除されます。ローカル IP エントリは エージ アウトされ、その後、データプレーンを通じて再学習されることはありませんが、コントロールプレーンからは引き続き学習できます。
- データプレーン IP アドレス ラーニングを無効にすると、すでに学習したローカル IP エンドポイントは保持され、動作を維持するにはコントロールプレーンの更新が必要になります（IP エージングも有効であると想定）。データプレーン レイヤ 3 トラフィックは IP エンドポイントの動作を維持しません。
- EPG-to-EPG イントラ VRF インスタンス レイヤ 3 トラフィックの場合、入力リーフ スイッチは宛先クラスを解決できないため、ポリシーは常に出力リーフ スイッチに適用されます。リモート IP アドレスは学習されません。
- EPG-to-EPG イントラ VRF インスタンス レイヤ 2 トラフィックでは、スイッチはリモート MAC アドレスを学習できますが、リモート IP アドレスは学習できないため、入力リーフ スイッチにポリシーを適用できます。
- データプレーン IP アドレスの学習がエンドポイントまたはサブネットに対して有効になっている場合、データプレーン IP アドレスは、CPU に到達しないエンドポイント間 ARP 要求を使用して学習されません。ただし、ブリッジ ドメイン SVI ゲートウェイへの ARP 要求は引き続き学習されます。
- データプレーン IP アドレス ラーニングが VRF インスタンスに対して有効になっている場合、ローカルおよびリモート MAC アドレスは、エンドポイント間 ARP 要求を使用して学習されます。

エンドポイントまたはサブネットごとのデータプレーン IP アドレス ラーニングの無効化には、次のガイドラインと制約事項が適用されます。

- 同じブリッジ ドメイン内のエンドポイント間に通信がある場合は、ブリッジドメインで L2 unknown Unicast プロパティを Flood に設定する必要があります。ARP フラッディングも有効にする必要があります。そうしないと、ローカル MAC アドレスとリモート MAC アドレスがエンドポイント間エンドポイント ARP 要求によって学習されないため、同じブリッジ ドメイン内のエンドポイント間の ARP は機能しません。
- フラッシュする代わりに、ローカル IP アドレスは dp-lrn-dis（データプレーン学習ディセーブル）状態に変換されます。
- エンドポイントのサブネットがデータプレーン IP アドレス学習を無効に設定されている場合、エンドポイント データプレーン IP アドレス学習を有効にすることはできません。

たとえば、学習が無効になっているサブネット 100.10.0.1/24 と、学習が有効になっている 100.10.0.100/32 の EPG を持つブリッジ ドメインはありません。

- エンドポイントまたはサブネットでデータプレーン IP アドレスの学習が無効になっている場合、スイッチは、ルーティングされたレイヤ 3 データ トラフィックからレイヤ 2 MAC アドレスを学習または更新しません。レイヤ 2 MAC アドレスは、レイヤ 2 データ トラフィックまたは ARP パケットからのみ学習されます。
- エンドポイントまたはサブネットのデータプレーン IP アドレス学習が無効になっている場合、GARP パケットからトリガーされた IP アドレス学習または移動は、ARP フラッド モードと GARP ベースのエンドポイント移動検出が有効になっている場合にのみ可能です。

無効にするデータプレーンIPアドレス ラーニングの機能相互作用

ここでは、無効にするデータプレーン IP アドレス ラーニングとその他の機能との相互作用についての情報を示します。

- エニーキャスト
  - 有効：ローカル エニーキャスト IP アドレスは、データプレーンとコントロール プレーンのどちらからでも学習できます。
  - 無効：ローカル エニーキャスト IP アドレスはエージ アウトしますが、コントロール プレーンとホストトラッキングから学習することができます。
  - リモート IP アドレスは、VRF インスタンスごとのデータプレーン IP アドレス ラーニングの設定方法を問わず、エニーキャストで学習されません。
- 不正なエンドポイントの検出
  - 有効：不正な IP アドレスが生成され、移動は意図したとおりに検出されます。
  - 無効：リモート IP アドレスがフラッシュされ、不正な IP アドレスはエージ アウトされます。不正な IP アドレスはローカルの移動では検出されません。検出される唯一の移動は、コントロール トラフィックからのものです。バウンスは COOP から学習されますが、バウンス タイマーが時間切れになるとこれらはドロップされます。
- レイヤ 4 ーレイヤ 7 サービス仮想 IP（VIP）アドレス
  - 有効：レイヤ 4 からレイヤ 7 サービス VIP アドレスは期待どおりに機能します（VIP アドレスのエンドポイント IP アドレス ラーニングはコントロール プレーン経由のみ）。次の機能ストリームを考えます。
    1. クライアントからロード バランサへ（レイヤ 3 トラフィック）
    2. サーバへのロード バランサ（レイヤ 2 トラフィック）

3. サーバからクライアント（レイヤ 3）

EPG の背後のクライアント（IP エンドポイント）は、データ/コントロール プレーンを通じて学習されます。VIP アドレスはロード バランサ EPG のコントロール プレーン経由でのみ学習されます。コントロールプレーン経由であっても、VIP アドレスは他の EPG では学習されません。

- [Disabled]：
  - クライアントからロード バランサ：VIP アドレスではリモート IP アドレスが学習されません。リモート IP アドレスはクリアされます。spine-proxy を使用します。VIP の IP アドレスが学習されると、spine-proxy ルックアップは成功します。そうでない場合は VIP アドレスにグリーニングを生成し、コントロール プレーンを通じて学習します。
  - ロード バランサからサーバへ：影響なし。DSR の使用例では、ロード バランサ/サーバー間のブリッジだけがサポートされています。
  - サーバからクライアント：クライアントのリモート IP アドレスはクリアされ、spine-proxy が使用されます。クライアント エントリのリモート IP アドレスがスパイン スイッチで削除された場合、グリーニングを通じて再学習されます。L3out の背後にあるクライアントの場合、レイヤ 3 リモート IP アドレスはありません。

GUI を使用した VRF インスタンスごとのデータプレーン IP アドレス ラーニングの設定

このセクションでは、VRF インスタンスごとのデータプレーン IP ラーニングを無効にする方法について説明します。

次の手順では、テナントと VRF インスタンスがすでに設定されていると仮定します。

手順

ステップ 1 **[テナント（Tenants）>[*tenant_name*]>[ネットワーキング（Networking）]>[VRFs]>[*vrf_name*]** に移動します。

ステップ 2 [VRF - *vrf_name*] 作業ペインで、[Policy] タブをクリックします。

ステップ 3 [Policy] 作業ペインの下にスクロールし、[IP Data-plane Learning] を探します。

ステップ 4 次のいずれかをクリックします。

- [**無効化（Disabled**）]：VRF インスタンスでのデータプレーン IP アドレス ラーニングを無効にします。

- [有効化（Enabled）]：VRF インスタンスでのデータプレーン IP アドレス ラーニングを有効にします。

ステップ 5 [Submit] をクリックします。

GUI を使用したエンドポイントごとのデータ プレーン IP アドレス ラーニングの設定

次の手順では、選択したエンドポイント グループのエンドポイントのデータ プレーン IP アドレス学習を有効または無効にします。エンドポイントのデータ プレーン IP アドレス ラーニングを設定できるのは、EPG サブネット IP アドレスのマスクが IPv4 アドレスの場合は /32、IPv6 アドレスの場合は /128 です。データ プレーン IP アドレスの学習は、デフォルトで有効になっています。

手順

ステップ 1 メニュー バーで、[テナント（Tenants）] > [すべてのテナント（ALL Tenants）] の順に選択します。 >

ステップ 2 作業ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 既存のサブネットを変更する場合は、次のサブステップを実行します。

a) ナビゲーション ペインで、**[テナント（Tenant）*tenant_name]* > [アプリケーション プロファイル（Application Profiles）] > [*app_profile_name*] > [アプリケーション EPG（Application EPGs）] > [*app_epg_name*] > [サブネット（Subnets）] > [*subnet_address*]** の順に選択します。

選択したサブネットは、次の要件を満たしている必要があります。

- [デフォルト ゲートウェイ IP（Default Gateway IP）] フィールドのマスクは、IPv4 アドレスの場合は /32、IPv6 アドレスの場合は /128です。
- [デフォルト SVI ゲートウェイなし（No Default SVI Gateway）] チェック ボックスをオンにする必要があります。
- [Behind Subnet のタイプ（Type Behind Subnet）] は [なし（None）] または [エニキャスト MAC（Anycast MAC）] である必要があります。

b) [ワーク（Work）] ペインの [IP データプレーンの学習（IP Data-plane Learning）] で、[有効（Enable）] または [無効（Disable）] を選択します。

これにより、エンドポイントの IP アドレス データ プレーンの学習が有効または無効になります。

ステップ 4 新しいサブネットを作成する場合は、次のサブステップを実行します。

a) ナビゲーション ペインで、**[テナント（Tenant）*tenant_name]*** > **[アプリケーション プロファイル（Application Profiles）]** > **[*app_profile_name*]** > **[アプリケーション EPG（Application EPGs）]** > **[*app_epg_name*]** > **[サブネット（Subnets）]** の順に選択します。

b) [サブネット（Subnets）] を右クリックし、[EPG サブネットの作成（Create EPG Subnet）] を選択します。

c) [デフォルト ゲートウェイ IP（Default Gateway IP）] フィールドには、IPv4 アドレスの場合は /32、IPv6 アドレスの場合は /128 のマスクを指定する必要があります。

d) [デフォルト SVI ゲートウェイなし（No Default SVI Gateway）] チェック ボックスをオンにする必要があります。

e) [Behind Subnet のタイプ（Type Behind Subnet）] ボタンで、[なし（None）] または[エニキャスト MAC（Anycast MAC）] を選択します。

f) [IP データプレーンの学習（IP Data-plane Learning）]トグルで、必要に応じて[有効化（Enable）]または[無効化（Disable）]を選択します。

これにより、エンドポイントの IP アドレス データ プレーンの学習が有効または無効になります。

g) 必要に応じて、残りのフィールドに入力します。

ステップ 5 [Submit] をクリックします。

GUI を使用したサブネットごとのデータ プレーン IP アドレス ラーニングの設定

次の手順では、サブネットのデータプレーン IP アドレス学習を有効または無効にします。データ プレーン IP アドレスの学習は、デフォルトで有効になっています。

手順

ステップ 1 メニュー バーで、[テナント（Tenants）] > [すべてのテナント（ALL Tenants）] の順に選択します。 >

ステップ 2 作業ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 既存のサブネットを変更する場合は、次のサブステップを実行します。

a) [ナビゲーション（Navigation）] ペインで、**[テナント（Tenant）*tenant_name]*** > **[ネットワーキング（Networking）]** > **[ブリッジ ドメイン（Bridge Domains）]** > **[*bridgeg_domain_name*]** > **[サブネット（Subnets）]** > **[*subnet_address*]** の順に選択します。

データプレーンの IP アドレス ラーニングを無効にする場合は、**[デフォルト SVI ゲートウェイなし（No Default SVI Gateway）]** チェックボックスをオンにしないでください。

b) [作業（Work）] ペインの [IP データプレーンの学習（IP Data-plane Learning）] で、[有効化（Enable）] または [無効化（Disable）] を選択します。

これにより、サブネットのIPアドレスデータプレーンの学習が有効または無効になります。

ステップ 4 新しいサブネットを作成する場合は、次のサブステップを実行します。

a) [ナビゲーション（Navigation）]ペインで、**[テナント（Tenant）*tenant_name]*>[ネットワーキング（Networking）]>[ブリッジ ドメイン（Bridge Domains）]>[*bridgeg_domain_name*]>[サブネット（Subnets）]** の順に選択します。

b) [サブネット（Subnets）] を右クリックし、[サブネットの作成（Create Subnet）] を選択します。

c) [デフォルト ゲートウェイ IP（Default Gateway IP）] フィールドで、IP アドレスとマスクを入力します。

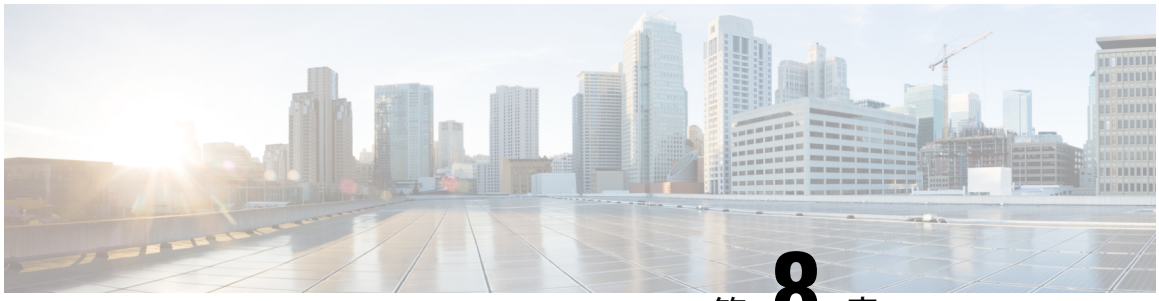
d) データプレーンの IP アドレス ラーニングを無効にする場合は、[**デフォルト SVI ゲートウェイなし（No Default SVI Gateway**）] チェックボックスをオンにしないでください。

e) [IP データプレーンの学習（IP Data-plane Learning）] トグルで、必要に応じて [有効化（Enable）] または [無効化（Disable）] を選択します。

これにより、サブネットの IP アドレス データプレーンの学習が有効または無効になります。

f) 必要に応じて、残りのフィールドに入力します。

ステップ 5 [Submit] をクリックします。



第 8 章

IPv6 ネイバー探索

この章は、次の内容で構成されています。

ネイバー探索

IPv6 ネイバー探索（ND）は、ノードのアドレスの自動設定、リンク上の他のノードの探索、他のノードのリンク層アドレスの判別、重複アドレスの検出、使用可能なルータと DNS サーバの検出、アドレス プレフィックスの探索、および他のアクティブなネイバー ノードへのパスに関する到達可能性情報の維持を担当します。

ND 固有のネイバー要求/ネイバー アドバタイズメント（NS/NA）およびルータ要求/ルータ アドバタイズメント（RS/RA）パケット タイプは、物理、層3 サブ インターフェイス、および SVI（外部およびパーベイシブ）を含むすべての ACI ファブリックのレイヤ 3 インターフェイスでサポートされます。APIC リリース 3.1(1x) まで、RS/RA パケットはすべてのレイヤ 3 インターフェイスの自動設定のために使用されますが、拡散型 SVI の設定のみ可能です。

APIC リリース 3.1(2x) より、RS/RA パケットは自動設定のため使用され、ルーテッド インターフェイス、レイヤ 3 サブ インターフェイス、SVI（外部および拡散）を含むレイヤ 3 インターフェイスで設定できます。

ACI のブリッジ ドメイン ND は常にフラッド モードで動作します。ユニキャスト モードはサポートされません。

ACI ファブリック ND サポートに含まれるもの：

- インターフェイス ポリシー（`nd:IfPol`）は、NS/NA メッセージに関する ND タイマーと動作を制御します。
- ND プレフィックス ポリシー（`nd:PfxPol`）コントロール RA メッセージ。
- ND の IPv6 サブネット（fv:Subnet）の設定。

- 外部ネットワークの ND インターフェイス ポリシー。
- 外部ネットワークの設定可能 ND サブネットおよびパーベイシブ ブリッジ ドメインの任意サブネット設定はサポートされません。

設定可能なオプションは次のとおりです。

- 隣接関係
  - 設定可能な静的 Adjacencies：（<vrf、L3Iface < ipv6 address> --> mac address）
  - 動的 Adjacencies：NS/NA パケットの交換経由で学習
- インターフェイス単位
  - ND パケットの制御（NS/NA）
    - ネイバー要求間隔
    - ネイバー要求再試行回数
  - RA パケットの制御
    - RA の抑制
    - RA MTU の抑制
    - RA 間隔、RA 最小間隔、再送信時間
- プレフィックス単位（RA でアドバタイズ）の制御
  - ライフタイム、優先ライフタイム
  - プレフィックス コントロール（自動設定、リンク上）
- ネイバー検索重複アドレスの検出（DAD）

ブリッジ ドメインでの IPv6 ネイバー探索の設定

GUI を使用して、ブリッジ ドメイン上に IPv6 ネイバー探索対応のテナント、VRF、およびブリッジ ドメインを作成する

このタスクでは、テナント、VRF、およびブリッジ ドメイン（BD）を作成し、それらの中に 2 つの異なるタイプのネイバー探索（ND）ポリシーを作成する方法を示します。これらは ND インターフェイス ポリシーと ND プレフィックス ポリシーです。ND インターフェイス ポリシーは BD に導入されますが、ND プレフィックス ポリシーは個々のサブネットに導入されます。各 BD に独自の ND インターフェイス ポリシーを適用することができます。ND インターフェイス ポリシーは、デフォルトですべての IPv6 インターフェイスに導入されます。Cisco

APIC には、使用可能なデフォルトの ND インターフェイス ポリシーがすでに存在します。必要に応じて、代わりに使用するカスタム ND インターフェイス ポリシーを作成できます。ND プレフィックス ポリシーはサブネット レベルにあります。すべての BD が複数のサブネットを持つことができ、各サブネットが異なる ND プレフィックスを持つことができます。

手順

ステップ 1 メニュー バーで、**[テナント（TENANT）]** > **[テナントの追加（Add Tenant）]** の順にクリックします。

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) [Security Domains +] アイコンをクリックして [Create Security Domain] ダイアログボックスを開きます。
c) [Name] フィールドに、セキュリティ ドメインの名前を入力します。**Submit** をクリックします。
d) [Create Tenant] ダイアログボックスで、作成したセキュリティ ドメインのチェックボックスをオンにし、[Submit] をクリックします。

ステップ 3 [Navigation] ペインで、***[Tenant-name]*** > **[Networking]** の順に展開します。

ステップ 4 [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) [Submit] をクリックして VRF の設定を完了します。

ステップ 5 [**ネットワーキング（Networking**）] 領域で、[**ブリッジ ドメイン（Bridge Domain**）] アイコンを [**VRF**] アイコンにつなげながらキャンバスにドラッグします。[Create Bridge Domain] ダイアログボックスが表示されたら、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) [L3 Configurations] タブをクリックし、[Subnets] を展開して [Create Subnet] ダイアログボックスを開き、[Gateway IP] フィールドにサブネット マスクを入力します。

ステップ 6 [Subnet Control] フィールドで、[ND RA Prefix] チェックボックスがオンになっていることを確認します。

ステップ 7 [ND Prefix policy] フィールドのドロップダウン リストで、[Create ND RA Prefix Policy] をクリックします。

（注） すべての IPv6 インターフェイスに導入される使用可能なデフォルト ポリシーがすでに存在しています。または、この例で示されているように、使用する ND プレフィックス ポリシーを作成できます。デフォルトでは、IPv6 ゲートウェイのサブネットは ND RA メッセージの ND プレフィックスとしてアドバタイズされます。ユーザは、[ND RA prefix] チェックボックスをオフにして、ND RA メッセージでサブネットをアドバタイズしないことを選択できます。

ステップ 8 [Create ND RA Prefix Policy] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドにプレフィックス ポリシーの名前を入力します。

（注） 特定のサブネットに対して存在できるプレフィックス ポリシーは 1 つのみです。サブネットは共通プレフィックスポリシーを使用できますが、各サブネットに異なるプレフィックス ポリシーを適用することが可能です。

b) [Controller State] フィールドで、目的のチェックボックスをオンにします。
c) [Valid Prefix Lifetime] フィールドで、プレフィックスを有効にする期間について目的の値を選択します。
d) [Preferred Prefix Lifetime] フィールドで、目的の値を選択します。[OK] をクリックします。

（注） NDプレフィックスポリシーが作成され、特定のサブネットに接続されます。

ステップ 9 [ND policy] フィールドのドロップダウン リストで、[Create ND Interface Policy] をクリックし、次のタスクを実行します。

a) [Name] フィールドにポリシーの名前を入力します。
b) [Submit] をクリックします。`

ステップ 10 [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。

同様に、さまざまなプレフィックス ポリシーが適用された追加のサブネットを必要に応じて作成できます。

IPv6 アドレスのサブネットが BD に作成され、ND プレフィックス ポリシーが関連付けられています。

レイヤ 3 インターフェイス上での IPv6 ネイバー探索の設定

注意事項と制約事項

次の注意事項と制約事項は、レイヤ 3 インターフェイスのネイバー探索ルータ アドバタイズメント（ND RA）プレフィックスに適用されます。

- ND RA 設定は、IPv6 プレフィクスにのみ適用されます。IPv4 プレフィクスでネイバー探索ポリシーを構成しようとしても、失敗します。

GUI を使用して、レイヤ 3 インターフェイス上の RA の IPv6 ネイバー探索インターフェイス ポリシーの設定

（注） 次の手順では、レイヤ 3 インターフェイスで IPv6 ネイバー探索インターフェイス ポリシーを関連付ける方法を表示します。この特定の例は、非 VPC インターフェイスを使用して設定する方法を示しています。

始める前に

- テナント、VRF、BD が作成されていること。
- 外部ルーテッド ネットワークで、L3Out が作成されます。

手順

ステップ 1 **ナビゲーション**] ペインで、適切なテナントで、適切な外部ルーテッド ネットワークに移動します。

ステップ 2 [**L3Outs**] で、> **[論理ノード プロファイル（Logical Node Profiles）]** > **[*Logical Node Profile_name*]** > **[論理インターフェイス プロファイル（Logical Interface Profiles）]** を展開します。

ステップ 3 適切な [**論理インターフェイス プロファイル（Logical Interface Profile**）] をダブルクリックし、[**作業（Work**）] ペインで **[ポリシー（Policy）]** > **[ルーテッド インターフェイス（Routed Interfaces）]**をクリックします。

（注） 作成論理インターフェイス プロファイルを持っていない場合は、ここにプロファイルを作成することができます。

ステップ 4 **Routed Interface** ダイアログボックスで、次の操作を実行します:

a) **ND RA プレフィックス** フィールドで、インターフェイスの ND RA プレフィックスを有効にするチェック ボックスをチェックします。

有効にすると、ルーテッド インターフェイスは自動設定使用できます。

また、 **ND RA プレフィックス ポリシー** フィールドが表示されます。

b) **ND RA Prefix Policy** フィールドで、ドロップダウンリストから、適切なポリシーを選択します。

c) 必要に応じて、画面上の他の値を選択します。[Submit] をクリックします。`

（注） **VPC インターフェイスを使用してを設定する際に、VPC の設定内のメンバは、その両方としてに、サイド A とサイド B の両方の ND RA プレフィックスが有効にする必要があります** 。**作業** ()] ペインで、 **論理インターフェイス プロファイル** 画面で、をクリックします **SVI** ()] タブ。**プロパティ** 、有効にするチェックボックスをオン、**ND RA プレフィックス** サイド A とサイド B の両方を選択、同一の **ND RA プレフィックス ポリシー** サイド A とサイド B の

IPv6 ネイバー探索重複アドレス検出の設定

ネイバー探索重複アドレス検出について

重複アドレス検出 (DAD) は、ネットワーク内で重複アドレスを検出するためにネイバー探索が使用するプロセスです。デフォルトでは、ACI ファブリック リーフ レイヤ 3 インターフェイスで使用されているリンクローカル アドレスとグローバルサブネット IPv6 アドレスの DAD が有効になっています。オプションとして、REST API (**ipv6Dad="disabled"** 設定を使用)または GUI を通してノブを構成することにより、IPv6 グローバルサブネットの DAD プロセスを無効にすることができます。外部接続されたデバイスに境界リーフ冗長性を提供するため、異なる境界リーフ スイッチ上の L3Outs にわたって同じ共有セカンダリ アドレスが必要な場合には、このノブを構成します。このような場合、DAD プロセスを無効にすれば、DAD が複数の境界リーフ スイッチ上の同じ共有セカンダリ アドレスを重複と見なすことを避けられます。このような場合には DAD プロセスを無効にしないと、共有セカンダリ アドレスが DUPLICATE DAD 状態に入り、使用できなくなることがあります。

GUI を使用したネイバー探索重複アドレス検出の設定

サブネットのネイバー探索重複アドレス検出プロセスを無効にするには、このセクションの手順に従ってください。

手順

ステップ 1 適切なページに移動して、そのインターフェイスの DAD フィールドにアクセスします。次に例を示します。

a) **[テナント（Tenants）]** > **[テナント（Tenant）]** > **[ネットワーキング（Networking）]** > **[L3Outs]** > ***[L3Out]*** > **[論理ノード プロファイル（Logical Node Profiles）** > **[ノード（*node*）]** > **[論理インターフェイス プロファイル（Logical Interface Profiles）]** に移動し、設定するインターフェイスを選択します。

b) *Routed Sub-interfaces* または *SVI* をクリックし、作成 (+) ボタンをクリックしてインターフェイスを設定します。

ステップ 2 このインターフェイスで、DAD エントリを次のように設定します:

- プライマリ アドレスでは、DAD エントリの値を **enabled** に設定します。
- 共有セカンダリ アドレスでは、DAD エントリの値を **disabled** に設定します。セカンダリ アドレスが境界リーフ スイッチ間で共有されていない場合には、そのアドレスの DAD を無効にする必要がないことに注意してください。

例:

たとえば、SVI インターフェイスのこの設定を構成する場合には、次のようになります:

- サイド A の IPv6 DAD を **enabled** に設定します。
- サイド B の IPv6 DAD を **disabled** に設定します。

例:

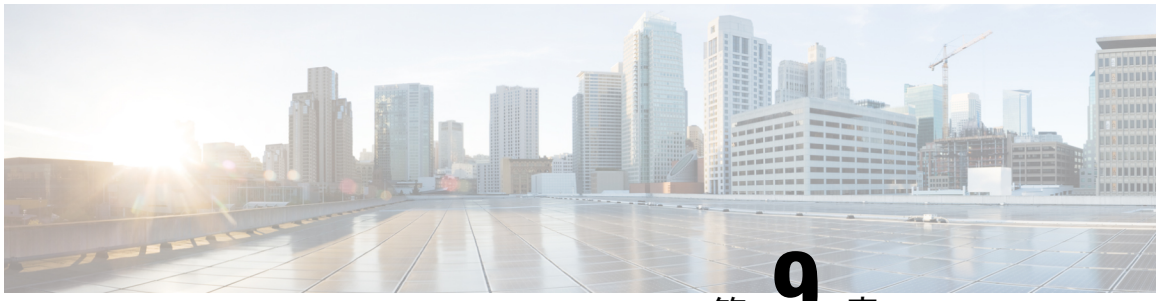
別の例として、ルーテッドサブインターフェイスの設定を構成する場合には、次のようになります:

- メインの [Select Routed Sub-Interface] ページで、ルーテッド サブインターフェイスの IPv6 DAD を **enabled** に設定します。
- [IPv4 Secondary/IPv6 Additional Addresses] エリアで作成 (+) ボタンをクリックして [Create Secondary IP Address] ページにアクセスし、IPv6 DAD の値を **disabled** に設定します。[OK] ボタンをクリックして、この画面での変更点を適用します。

ステップ 3 [Submit] ボタンをクリックして、変更を適用します。

ステップ 4 リーフ スイッチで **show ipv6 int** コマンドを入力して、設定がリーフ スイッチに正しくプッシュされたか確認してください。例:

```
swtb23-leaf5# show ipv6 int vrf icmpv6:v1
IPv6 Interface Status for VRF "icmpv6:v1"(9)

vlan2, Interface status: protocol-up/link-up/admin-up, iod: 73
if_mode: ext
  IPv6 address:
    2001:DB8:A::2/64 [VALID] [PREFERRED]
    2001:DB8:A::11/64 [VALID] [dad-disabled]
  IPv6 subnet:  2001:DB8:A::/64
  IPv6 link-local address: fe80::863d:c6ff:fe9f:eb8b/10 (Default) [VALID]
```



第 9 章

Microsoft NLB

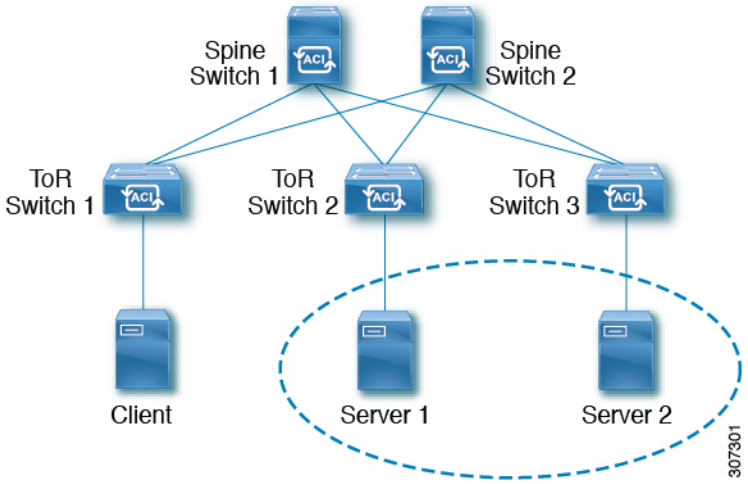
この章は、次の内容で構成されています。

Microsoft NLB について

Microsoft ネットワーク ロード バランシング（NLB）機能は、クライアント トラフィックを多数のサーバに分散し、各サーバがアプリケーションの個別のコピーを実行します。ネットワーク ロードバランシングは、レイヤ 2 の不明なユニキャストまたはマルチキャストを使用して、着信ネットワーク トラフィックをすべてのクラスタ ホストに同時に分散します。

Microsoft NLB ノードのグループは、NLB クラスタと総称されます。NLB クラスタは、1 つ以上の仮想 IP（VIP）アドレスのサービスを提供します。NLB クラスタ内のノードは、ロードバランシング アルゴリズムを使用して、NLB VIP 宛ての特定のトラフィック フローを処理する個々のノードを決定します。クラスタ内のすべてのノードはトラフィックのすべてのパケットを受信しますが、1 つのノードだけが要求を処理します。

次の図に、Microsoft NLB の実装方法を図で示します。Cisco APIC



この図では、サーバ 1 とサーバ 2 が MS NLB クラスタにあります。これらのサーバは、外部クライアントには単一ホストサーバとして表示されます。MS NLB クラスタ内のすべてのサーバがすべての着信要求を受信すると、MS NLB はサーバ間で負荷を分散します。

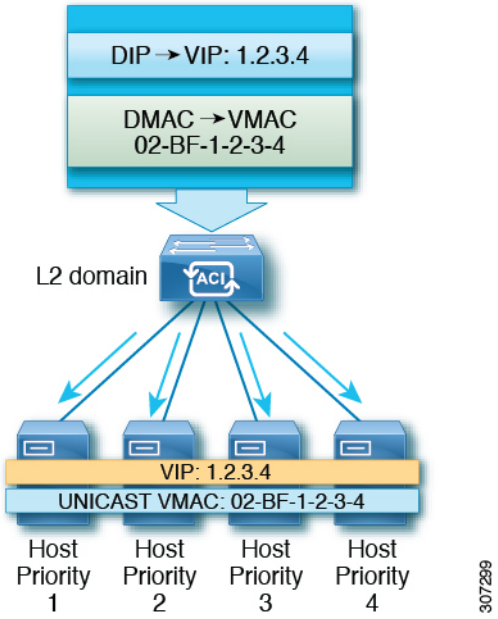
3 種類の異なる動作モードでの Microsoft NLB の機能：

- ユニキャスト モード：このモードでは、各 NLB クラスタ VIP にユニキャスト MAC アドレスが割り当てられます。このモードは、トラフィックをクラスタに配信するために不明なユニキャスト フラッディングに依存します。
- **マルチキャスト モード**：このモードでは、各 NLB クラスタ VIP が非 Internet Assigned Numbers Authority（IANA）マルチキャスト MAC アドレス（03xx.xxxx.xxxx）に割り当てられます。
- **IGMPモード**：このモードでは、NLB クラスタ VIP が一意の IPv4 マルチキャスト グループ アドレスに割り当てられます。このためのマルチキャスト MAC アドレスは、IPv4 マルチキャスト アドレスの標準 MAC 導出から導出されます。

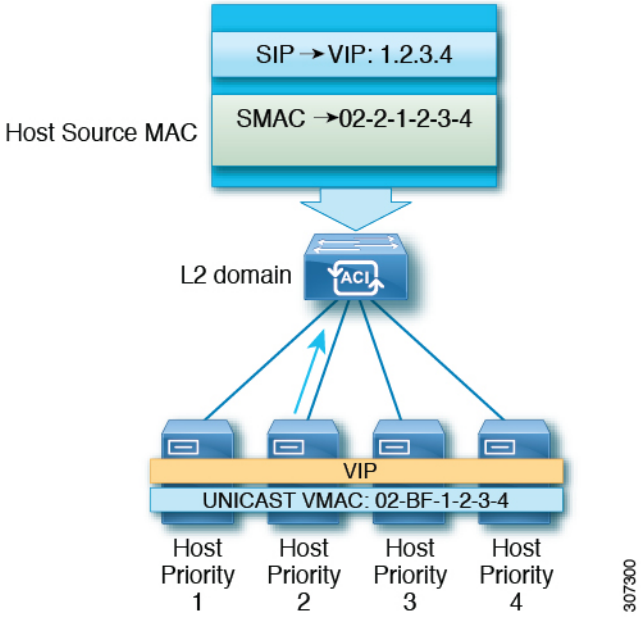
ユニキャスト モードについて

ユニキャスト動作モードでは、ネットワーク負荷分散は、それが有効になっているネットワーク アダプタ（クラスタ アダプタと呼ばれる）の MAC アドレスを再割り当てし、すべてのクラスタ ホストに同じ MAC アドレスが割り当てられます。この MAC アドレスは、クラスタのプライマリ IP アドレスから取得されます。たとえば、プライマリ IP アドレスが 1.2.3.4 の場合、ユニキャスト MAC アドレスは 02-BF-1-2-3-4 に設定されます。

ネットワーク ロードバランシングのユニキャスト モードでは、次の図に示すように、着信ネットワーク トラフィックをすべてのクラスタ ホストに同時に配信します。

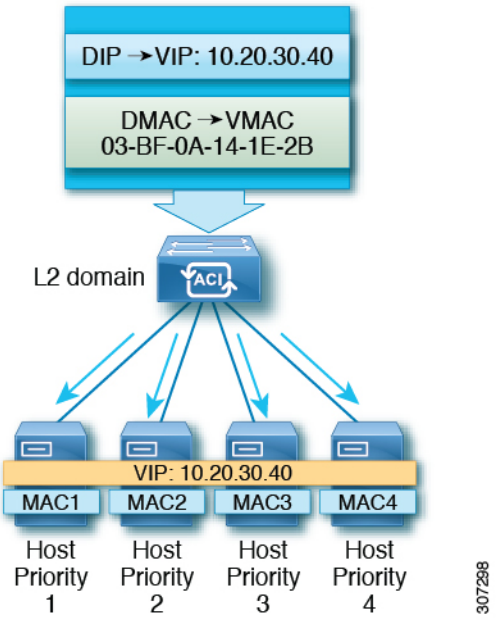


レイヤ 2 スイッチでは、すべてのスイッチ ポートで一意の送信元 MAC アドレスが認識されるため、共通の MAC アドレスを使用すると、通常は競合が発生します。この問題を回避するために、ネットワーク ロード バランシングは発信パケットの送信元 MAC アドレスを一意に変更します。クラスタの MAC アドレスが 02-BF-1-2-3-4 の場合、各ホストの送信元 MAC アドレスは 02- x -1-2-3-4 に設定されます。x はクラスタ内のホストの優先順位です。次の図に示します。



マルチキャスト モードについて

ネットワーク ロード バランシングは、着信ネットワーク トラフィックをすべてのクラスタ ホストに分散するためのマルチキャスト モードも提供します。マルチキャスト モードは、アダプタの MAC アドレスを変更する代わりに、レイヤ 2 マルチキャスト アドレスをクラスタ アダプタに割り当てます。たとえば、マルチキャスト MAC アドレスは、クラスタのプライマリ IP アドレス 10.20.30.40 に対して 03-BF-0A-14-1E-28 に設定できます。クラスタ通信には別のアダプタは必要ありません。

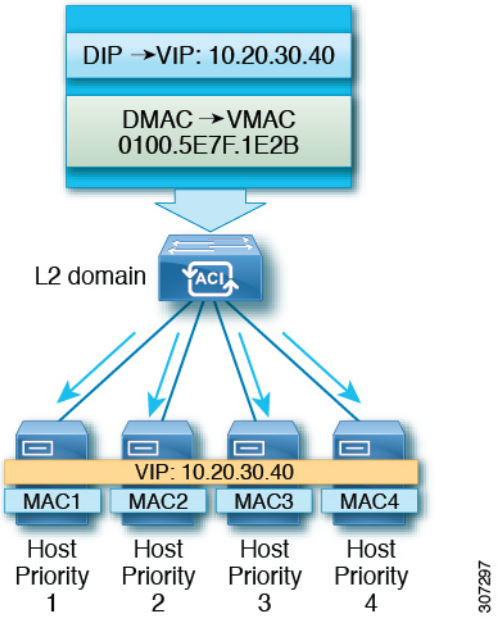


IGMP モードについて

Microsoft NLB サーバは、IGMP を使用してマルチキャスト グループに参加するように設定することもできます。これをスイッチのクエリアおよびIGMP スヌーピングと組み合わせることで、マルチキャスト メッセージのフラッディングの範囲を最適化できます。

Microsoft NLB サーバは、マルチキャスト グループ アドレスに IGMP Join を送信します。マルチキャスト アドレスの最後の 2 つのオクテットは、クラスタ IP の最後の 2 つのオクテットに対応します。たとえば、Microsoft NLB サーバが 239.255.xx のマルチキャスト アドレスに IGMP Join を送信する状況では、次のようになります。

- クラスタ IP：10.20.**30.40**
- IGMP が 239.255. に送信されました。**30.40**
- クライアントからサーバ方向で使用される MAC：0100.5E7F.**1E28**
- クラスタ通信には別のアダプタは必要ありません



Cisco ACI Microsoft NLB サーバの設定

リリース 4.1 より前の Microsoft NLB 導入では、ファブリックはレイヤ 2 のみである必要があり、エンドポイントのレイヤ 3 ゲートウェイとして外部ルータを使用します。Cisco ACI リリース 4.1 以降、ファブリックは Microsoft NLB 導入のレイヤ 3 ゲートウェイになります。Cisco ACI

次の表に、各 Microsoft NLB 導入モードの導入に関する考慮事項の概要を示します。

表 *5 : Cisco ACI Microsoft NLB* を使用した導入モード

	ユニキャスト モード	マルチキャスト モード	IGMP モード
Cisco ACI レイヤ 2 ネットワークとして、レイヤ 3 ゲートウェイとして外部ルータを使用	スイッチ名の末尾に -EX、-FX、または -FX2 があるリーフ スイッチ モデルでサポートされます。	スイッチ名の末尾に -EX、-FX、または -FX2 が付いたリーフ スイッチ モデル、およびスイッチ名の末尾にサフィックスがないリーフ スイッチ モデルでサポートされます。	スイッチ名の末尾に -EX、-FX、または -FX2 が付いたリーフ スイッチ モデル、およびスイッチ名の末尾にサフィックスがないリーフ スイッチ モデルでサポートされます。ただし、Microsoft NLB トラフィックは IGMP によってスコープされず、代わりにフラッディングされます。
Cisco ACI レイヤ 3 ゲートウェイとして	リリース 4.1 以降でサポートされます。	リリース 4.1 以降でサポートされます。	リリース 4.1 以降でサポートされます。

次の表に、Cisco ACI をレイヤ 2 として使用して Microsoft NLB を導入するために使用できる設定オプションの詳細を示します。

表 *6 : 3* つの *Microsoft NLB* モードの外部ルータおよび *ACI* ブリッジ ドメインの設定

	ユニキャスト モード	マルチキャスト モード	**IGMP** モード リリース **3.2** では、**Microsoft NLB** マルチキャスト モードと比較して **Microsoft NLB IGMP** モードを使用しても、複数宛先トラフィックのスコーピングに関して利点はありません。[1]
ACI ブリッジ ドメインの設定	• 不明なユニキャスト フラッディング用に設定されたブリッジ ドメイン（hw-proxy 以外） • No IP routing	• 不明なユニキャスト フラッディング用に設定されたブリッジ ドメイン（hw-proxy 以外） • No IP routing • レイヤ 3 不明なマルチキャスト：フラッディング（最適化されたマルチキャスト フラッディングでも、Microsoft NLB トラフィックがフラッディングされる） • IGMP スヌーピング設定：該当なし	• 不明なユニキャスト フラッディング用に設定されたブリッジ ドメイン（hw-proxy 以外） • No IP routing • レイヤ 3 不明なマルチキャスト：オプションですが、将来の互換性のために設定可能 • クエリア設定：オプションですが、将来の互換性のために有効にできます。ブリッジ ドメインの下にサブネットを設定します。IP ルーティングは不要です。 • IGMP スヌーピング設定：オプションですが、将来の互換性のためにイネーブルにできます。
外部ルータ ARP テーブルの設定	• 特別な ARP 設定なし • 外部ルータが VIP から VMAC へのマッピングを学習する	ユニキャスト VIP からマルチキャスト MAC へのスタティック ARP 設定	ユニキャスト VIP からマルチキャスト MAC へのスタティック ARP 設定

1

リリース 4.1 以降、Microsoft NLB サーバを接続するための設定は、次の一般的なタスクで構成されています。Cisco ACI

- VRF の設定。出力または入力モードで VRF を設定できます。
- Microsoft NLB サーバのブリッジ ドメイン（BD）を設定します。ハードウェア プロキシ モードではなく、フラッディング モードで L2 ユニキャストを使用します。
- 同じ VIP を共有するすべての Microsoft NLB サーバの EPG を定義します。この EPG を以前に定義した BD に関連付ける必要があります。
- EPG でサブネットとして Microsoft NLB VIP を入力します。Microsoft NLB は、次のモードで設定できます。
  - ユニキャスト モード：Microsoft NLB VIP 設定の一部としてユニキャスト MAC アドレスを入力します。このモードでは、クライアントから Microsoft NLB VIP へのトラフィックは、Microsoft NLB BD 内のすべての EPG にフラッディングされます。
  - マルチキャスト モード：Microsoft NLB VIP 自体の設定時にマルチキャスト MAC アドレスを入力します。Microsoft NLB EPG の静的ポートに移動し、Microsoft NLB サーバが接続されている EPG ポートに Microsoft NLB マルチキャスト MAC を追加します。このモードでは、トラフィックはスタティック MAC バインディングを持つポートに転送されます。
  - IGMPモード：Microsoft NLB VIP 自体の設定時に Microsoft NLB グループ アドレスを入力します。このモードでは、クライアントから Microsoft NLB VIP へのトラフィックは、Microsoft NLB グループ アドレスの IGMP Join を受信するポートに転送されます。
- Microsoft NLB EPG とクライアント EPG 間のコントラクトの設定。Microsoft NLB EPG を契約のプロバイダー側として設定し、クライアント EPG を契約のコンシューマ側として設定する必要があります。

Microsoft NLB は、ルート プラス フラッディング ソリューションです。クライアントから Microsoft NLB VIP へのトラフィックは、まずコンシューマ ToR スイッチでルーティングされ、次に Microsoft NLB BD でプロバイダー ToR スイッチに向けてフラッディングされます。

トラフィックがコンシューマ ToR スイッチを出ると、トラフィックはフラッディングされ、コントラクトはフラッディング トラフィックに適用できません。したがって、契約の適用はコンシューマ ToR スイッチで行う必要があります。

入力モードの VRF の場合、境界リーフ スイッチ（コンシューマ ToR スイッチ）にポリシーがないため、L3Out から Microsoft NLB EPG への VRF 内トラフィックがコンシューマ ToR スイッチでドロップされることがあります。この問題を回避するには、次のいずれかのオプションを使用します。

- オプション 1：出力モードで VRF を設定します。出力モードで VRF を設定すると、ポリシーは境界リーフ スイッチにダウンロードされます。
- オプション 2：Microsoft NLB EPG と L3Out の L3external を優先グループに追加します。トラフィックは、コンシューマ ToR スイッチのデフォルト許可ポリシーにヒットします。
- オプション 3：アップ状態の未使用ポート、または境界リーフ スイッチ上の Microsoft NLB サーバに接続されているポートに Microsoft NLB EPG を展開します。これにより、Microsoft

NLB EPG は境界リーフ スイッチのローカル エンドポイントになります。ポリシーはローカル エンドポイント用にダウンロードされるため、境界リーフ スイッチにはポリシーがダウンロードされます。

- オプション 4：共有サービスを使用します。プロバイダーの Microsoft NLB VRF とは異なる、コンシューマ VRF に L3Out を展開します。Microsoft NLB EPG の Microsoft NLB VIP の場合は、[VRF 間で共有（Shared VRFs）]ボックスをオンにします。コンシューマ VRF からの L3Out と Microsoft NLB EPG 間のコントラクトを設定します。共有サービスを使用すると、ポリシーは境界リーフ スイッチにダウンロードされます。

次の表に、Microsoft NLB モードでサポートされる EPG および BD 構成の詳細を示します。

表 *7: Cisco ACI Microsoft NLB* モードの *EPG* および *BD* の設定

	ユニキャスト モード	マルチキャスト モード	IGMP モード
ブリッジ ドメインの設定	• IP ルーティング • 不明なユニキャスト フラッディング用に設定されたブリッジ ドメイン（hw-proxy 以外） • ブリッジド メインの MAC アドレスは変更しないでください。	• IP ルーティング • 不明なユニキャスト フラッディング用に設定されたブリッジ ドメイン（hw-proxy 以外） • ブリッジド メインの MAC アドレスは変更しないでください。	• IP ルーティング • 不明なユニキャスト フラッディング用に設定されたブリッジ ドメイン（hw-proxy 以外） • ブリッジド メインの MAC アドレスは変更しないでください。
EPG の設定	• VIP のサブネット • サブネットの一部として定義されたユニキャスト MAC アドレス	• VIP のサブネット • サブネットの一部として定義されたマルチキャスト MAC アドレス • サーバが存在するポートへのスタティック バインディング • 各パスのスタティック グループ MAC アドレス	• VIP のサブネット • MAC アドレスを入力する必要はありません • ダイナミック グループまたはスタティック グループを選択できます • スタティック グループ オプションを選択した場合は、スタティック パスを入力し、各パスにマルチキャスト グループを入力します。
VMM ドメイン	VMM ドメインを入力できます。	マルチキャスト モードにはスタティック パスが必要であるため、この状況では VMM ドメインを使用できません。	ダイナミック グループ モードでは、VMM ドメインを使用できます。

Microsoft Network Load Balancing の注意事項と制限事項

次は、Microsoft Network Load Balancing（NLB）の注意事項と制限事項です。

- ブリッジ ドメインの**ポリシー** > **の詳細/トラブルシューティング プロパティ**で、Microsoft NLB VIP アドレスがそのブリッジ ドメインのいずれかの EPG で設定されている場合は、**[マルチキャスト SMAC ノブを使用して ARP をドロップする]** を無効にする必要があります。
- ブリッジ ドメインのマルチデスティネーション フラッディングが**ドロップ**に設定されている場合、Microsoft NLB はサポートされません。
- レイヤ 3 マルチキャストはサポートされていません（Microsoft NLB BD で PIM を有効にすることはできません）。
- IGMP の場合、許容されるモード グループは IPv4 です（IPv6 はサポートされません）。
- EX で終了する名前の Cisco Nexus 9000 シリーズ スイッチ、およびそれ以降のみがサポートされています。
- Microsoft NLB では、共有サービスおよびマイクロセグメント（uSeg）EPG がサポートされています。
- Cisco ACI マルチサイト は現在サポートされていません。
- レイヤ 2 不明ユニキャスト フラッディング モードで Microsoft NLB を設定する必要があります。

  代わりにブリッジ ドメインをハードウェア プロキシ用に設定すると、Cisco ACI はブリッジ ドメインの設定を修正することでクリアされる障害を発生させます。ブリッジ ドメインがハードウェア プロキシ用に誤って設定されたままの場合、ACI は 30 秒ごとに障害のある設定を起動しようとしますが、これはスイッチにとって不要なオーバーヘッドです。
- デフォルトの SVI MAC アドレスを使用して Microsoft NLB ブリッジ ドメインを設定する必要があります。レイヤ 3 設定では、ブリッジ ドメインの MAC アドレスをデフォルト設定の 00:22:BD:F8:19:FF に設定する必要があります。Microsoft NLB ブリッジ ドメインのこのデフォルト SVI MAC アドレスは変更しないでください。
- ファブリックあたり 128 の Microsoft NLB VIP のハードウェア制限があります。
- Microsoft NLB 用に設定された仮想サーバは、すべてのモード（ユニキャスト、マルチキャスト、および IGMP）で静的バインディングを使用してに接続できます。Cisco ACI
- Microsoft NLB 用に設定された仮想化されたサーバは、ユニキャスト モードと IGMP モードの VMM 統合を介してCisco ACIに接続できます。
- Microsoft NLB ユニキャスト モードは、エンドホスト モードの Cisco UCS B シリーズ ブレード サーバの背後にある VMM 統合ではサポートされません。

  ユニキャスト モードの Microsoft NLB は、クラスタ バウンド パケットの配信について不明なユニキャストのフラッディングに依存します。ユニキャスト モードは、ファブリック

インターコネクトがエンドホスト モードの場合、Cisco UCS B シリーズ ブレード サーバでは機能しません。このモードでは、不明なユニキャスト フレームがフラッディングされないためです。エンドホスト モードでの Cisco UCS B シリーズ ブレード サーバのレイヤ 2 転送動作の詳細については、以下を参照してください。

https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/unified-computing/whitepaper_c11-701962.html

GUI を使用したユニキャスト モードでの Microsoft NLB の設定

このタスクは、ブリッジ ドメインのすべてのポートに Microsoft NLB がフラッドするように設定します。

始める前に

これらの手順を進める前に次の使用可能な情報を準備してください。

- Microsoft NLB クラスタ VIP
- Microsoft NLB クラスタ MAC アドレス

手順

ステップ 1 [ナビゲーション（**Navigation**）] ペインで、**[テナント（Tenant）]** > **[*tenant_name*]** > **[アプリケーション プロファイル（Application Profiles）]** > **[*app_profile_name*]** > **[アプリケーション EPG（Application EPGs）]** > **[*application_EPG_name*]** > **[サブネット（Subnets）]** の順に選択します。

ステップ 2 **Subnets** を右クリックして、**Create EPG Subnet** を選択します。

ステップ 3 **Create EPG Subnet** ダイアログ ボックスで、次のフィールドに入力します。

a) **Default Gateway IP** フィールドで Microsoft NLB cluster VIP を入力します。

たとえば、`192.0.2.1/32` です。

b) **Scope** 領域で、共有サービスに **Shared between VRFs** のチェックをオンにします。

選択されている場合は、**Private to VRF** のチェックをオフにします。

c) **Subnet Control** で **No Default SVI Gateway** チェックボックスをオンにします。

d) **Type Behind Subnet** 領域で **EpNlb** をクリックします。

[**モード（Mode）**] フィールドが表示されます。

e) [**モード（Mode）**] ドロップダウン リストから、[**ユニキャスト モードの NLB（NLB in unicast mode）**] を選択します。

MAC Address フィールドが表示されます。

f) [**MAC アドレス（MAC Address**）] フィールドに Microsoft NLB クラスタ MAC アドレスを入力します。

たとえば、`00:01:02:03:04:05` です。

ステップ 4 [Submit] をクリックします。

GUI を使用したマルチキャスト モードでの Microsoft NLB の設定

このタスクは、ブリッジ ドメインの特定のポートでのみ Microsoft NLB がフラッドするように設定します。

始める前に

これらの手順を進める前に次の使用可能な情報を準備してください。

- Microsoft NLB クラスタ VIP
- Microsoft NLB クラスタ MAC アドレス

手順

ステップ 1 [**ナビゲーション（Navigation**）] ペインで、**[テナント（Tenant）]** > **[*tenant_name*]** > **[アプリケーション プロファイル（Application Profiles）]** > **[*app_profile_name*]** > **[アプリケーション EPG（Application EPGs）]** > **[*application_EPG_name*]** > **[サブネット（Subnets）]** の順に選択します。

ステップ 2 **Subnets** を右クリックして、**Create EPG Subnet** を選択します。

ステップ 3 **Create EPG Subnet** ダイアログ ボックスで、次のフィールドに入力します。

a) **Default Gateway IP** フィールドで Microsoft NLB cluster VIP を入力します。

たとえば、`192.0.2.1/32` です。

b) **Scope** 領域で、共有サービスに **Shared between VRFs** のチェックをオンにします。

選択されている場合は、**Private to VRF** のチェックをオフにします。

c) **Subnet Control** で **No Default SVI Gateway** チェックボックスをオンにします。

d) **[サブネットの背後のタイプ（Type Behind Subnet）]** 領域で、**[MSNLB]** をクリックします。

[**モード（Mode**）] フィールドが表示されます。

e) [**モード（Mode**）] ドロップダウン リストから、[**スタティック マルチキャスト モードの NLB（NLB in static multicast mode**）] を選択します。

MAC Address フィールドが表示されます。

f) [**MAC アドレス（MAC Address**）] フィールドに Microsoft NLB クラスタ MAC アドレスを入力します。

マルチキャスト モードの Microsoft NLB クラスタ MAC アドレスの場合、クラスタ MAC アドレスは 03 で始まる必要があります。

たとえば、`03:BF:01:02:03:04` です。

g) マルチキャスト モードでこのフィールドに入力した Microsoft NLB クラスタの MAC アドレスをコピーします。

ステップ 4 **[送信（Submit）]** をクリックします。`

ステップ 5 [**ナビゲーション（Navigation**）] ペインで、**[テナント（Tenant）][*tenant_name*]** > **[アプリケーション プロファイル（Application Profiles）]** > **[*application_profile_name*]** > **[アプリケーション EPG（Application EPGs）]** > **[*application_EPG_name*]** > **[スタティック ポート（Static Ports）]** > **[*static_port*]** の順に選択します。

ブリッジ ドメインで Microsoft NLB をフラッドに設定するスタティック ポートを選択します。

ステップ 6 このポートの **スタティック パス** ページで、次のフィールドに入力します。

a) [NLB スタティック グループ（NLB Static Group）] 領域で [+]（Create）をクリックし、コピーした MAC アドレスを [MAC アドレス（Mac Address）] フィールドに貼り付けます。3.g （50 ページ）

b) [MAC アドレス（Mac Address）] フィールドの下にある [更新（Update）] をクリックします。

ステップ 7 [スタティック パス（Static Path）] ページで、[送信（Submit）] をクリックします。

この Microsoft NLB クラスタ MAC アドレスへのトラフィックは、このスタティック ポートに送信されます。

GUI を使用した IGMP モードでの Microsoft NLB の設定

このタスクは、ブリッジ ドメインの特定のポートでのみ Microsoft NLB がフラッドするように設定します。

始める前に

これらの手順を進める前に次の使用可能な情報を準備してください。

- Microsoft NLB クラスタ VIP

手順

ステップ 1 [ナビゲーション（**Navigation**）] ペインで、**[テナント（Tenant）]** > **[*tenant_name*]** > **[アプリケーション プロファイル（Application Profiles）]** > **[*app_profile_name*]** > **[アプリケーション EPG（Application EPGs）]** > **[*application_EPG_name*]** > **[サブネット（Subnets）]** の順に選択します。

ステップ 2 **Subnets** を右クリックして、**Create EPG Subnet** を選択します。

ステップ 3 **Create EPG Subnet** ダイアログ ボックスで、次のフィールドに入力します。

a) **Default Gateway IP** フィールドで Microsoft NLB cluster VIP を入力します。

たとえば、`192.0.2.1/32` です。

b) **Scope** 領域で、共有サービスに **Shared between VRFs** のチェックをオンにします。

選択されている場合は、**Private to VRF** のチェックをオフにします。

c) **Subnet Control** で **No Default SVI Gateway** チェックボックスをオンにします。

d) **Type Behind Subnet** 領域で **EpNlb** をクリックします。

[**モード（Mode）**] フィールドが表示されます。

e) [**モード（Mode）**] ドロップダウン リストから、[**IGMP モードの NLB（NLB in IGMP mode）**] を選択します。

[グループ ID（Group Id）] フィールドが表示されます。

f) [グループ ID（Group Id）] フィールドに、Microsoft NLB マルチキャスト グループ アドレスを入力します。

Microsoft NLB マルチキャスト グループ アドレスの場合、アドレスの最後の 2 オクテットは、インスタンス クラスタ IP アドレスの最後の 2 オクテットに対応します。たとえば、インスタンス クラスタの IP アドレスが 10.20.30.40 の場合、このフィールドに入力する Microsoft NLB マルチキャスト グループ アドレスは 239.255.30.40 になります。

ステップ 4 **[送信（Submit）]** をクリックします。`

Microsoft NLB クラスタ VIP へのトラフィックは、APIC から静的に、または NLB クラスタからの IGMP 参加に基づいて動的に設定された発信インターフェイス リストにフラッディングされます。

ステップ 5 スタティック結合とダイナミック結合のどちらを使用するかを決定します。

スタティック結合とダイナミック結合を組み合わせて使用できます。一部のポートはスタティック結合を使用でき、他のポートはダイナミック結合を使用できます。

- Dinamic Join：ダイナミック結合では、それぞれのポートで Microsoft NLB クラスタによって結合が送信され、スイッチはその発信インターフェイス リストを使用して動的に起動します。

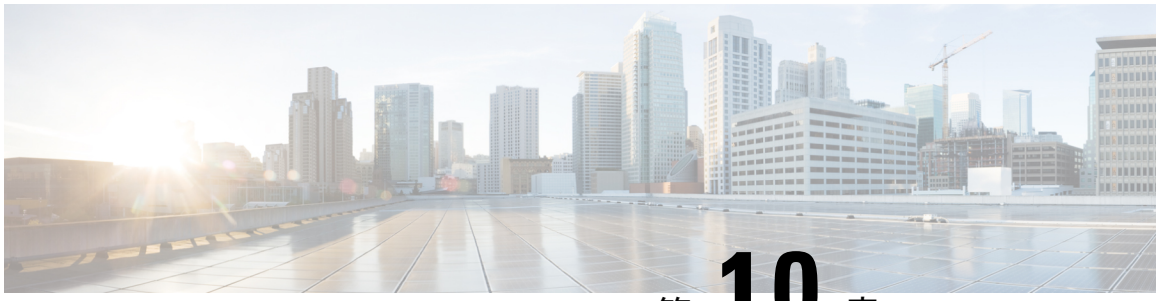
- Static Join：スタティック結合では、Microsoft NLB クラスタ VIP へのトラフィックは、次の手順で設定したポートに送信されます。

  スタティック結合を使用する場合：

  1. [グループ ID（Group Id）] フィールドに入力した Microsoft NLB マルチキャスト グループ アドレスをコピーします。3.f （51 ページ）
  2. **[ナビゲーション（Navigation）]** ペインで、**[テナント（Tenant）] > [*tenant_name*] > [アプリケーション プロファイル（Application Profiles）] > [*app_profile_name*] > [アプリケーション EPG（Application EPGs）] > [*application_EPG_name*] > [スタティック ポート（Static Ports）] > [*static_port*]** の順に選択します。

     ブリッジ ドメインで Microsoft NLB をフラッドに設定するスタティック ポートを選択します。
  3. このポートの **スタティック パス** ページで、次のフィールドに入力します。
     - **[IGMP スヌープ スタティック グループ（IGMP Snoop Static Group）]** 領域で **[+]**（作成（Create））をクリックし、3.f （51 ページ） からコピーしたグループ アドレスを **[グループ アドレス（Group Address）]** フィールドに貼り付けます。
     - [グループ アドレス（Group Address）] フィールドの下にある [更新（Update）] をクリックします。
  4. **スタティック パス** ページで **[送信（Submit）]** をクリックします。

ブリッジ ドメインではデフォルトで IGMP スヌーピングがオンになっています。これは、ブリッジ ドメインに関連付けられた IGMP スヌーピングポリシー「デフォルト」により、ポリシーの管理状態として [有効化（Enabled）] になるためです。詳細については、GUI を使用した IGMP スヌーピング ポリシーの設定 （57 ページ） を参照してください。



第 10 章

IGMP スヌーピング

Cisco APIC および IGMP スヌーピングについて

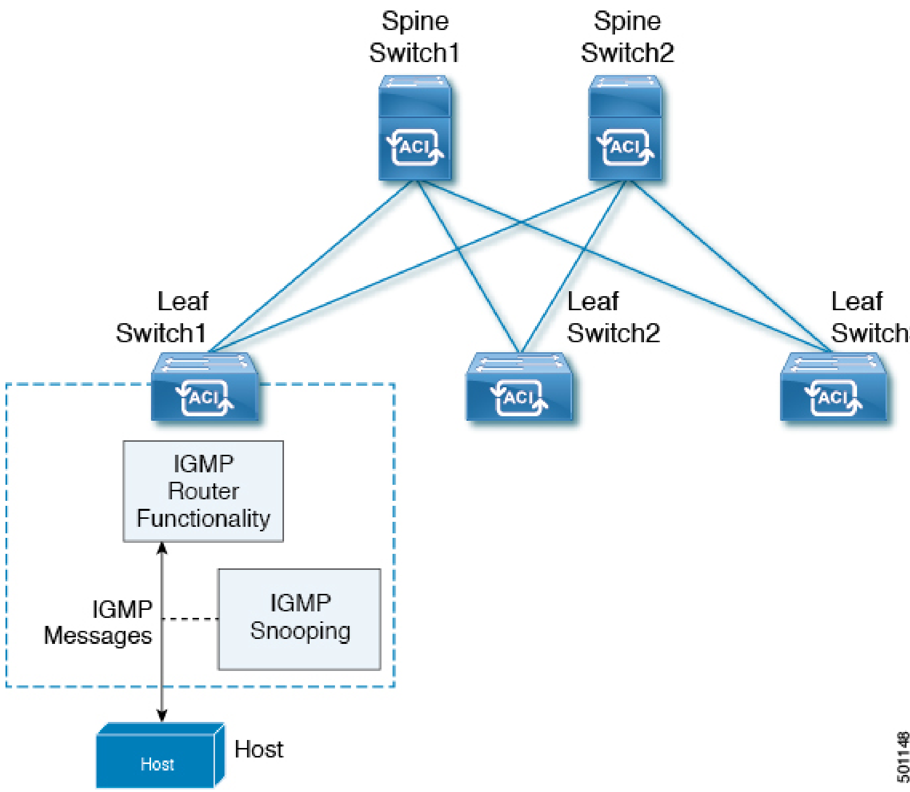
ACI ファブリックに IGMP スヌーピングを実装するには

（注） ブリッジ ドメインで IGMP スヌーピングをディセーブルにしないことを推奨します。IGMP スヌーピングをディセーブルにすると、ブリッジ ドメインで不正なフラッディングが過度に発生し、マルチキャストのパフォーマンスが低下する場合があります。

IGMP スヌーピング ソフトウェアは、ブリッジ ドメイン内の IP マルチキャスト トラフィックを調べて、該当する受信側が常駐するポートを検出します。IGMP スヌーピングではポート情報を利用することにより、マルチアクセスブリッジ ドメイン環境における帯域幅消費量を削減し、ブリッジ ドメイン全体へのフラッディングを回避します。デフォルトでは、IGMP スヌーピングがブリッジ ドメインでイネーブルにされています。

この図は、ホストへの接続を持つ ACI リーフ スイッチに含まれる IGMP ルーティング機能と IGMP スヌーピング機能を示しています。IGMP スヌーピング機能は、IGMP メンバーシップ レポートをスヌーピングし、メッセージを残し、必要な場合にのみIGMPルータ機能に転送します。

図 *6 : IGMP* スヌーピング機能



IGMP スヌーピングは、IGMPv1、IGMPv2、および IGMPv3 コントロールプレーンパケットの処理に関与し、レイヤ 3 コントロール プレーン パケットを代行受信して、レイヤ 2 の転送処理を操作します。

IGMP スヌーピングには、次の独自機能があります。

- 宛先および送信元の IP アドレスに基づいたマルチキャスト パケットの転送が可能な送信元フィルタリング
- MAC アドレスではなく、IP アドレスに基づいたマルチキャスト転送
- MAC アドレスに基づいた代わりのマルチキャスト転送

ACI ファブリックは、RFC 4541の2.1.1 項「IGMP 転送ルール」に記載されているガイドラインに従って、プロキシ レポーティング モードでのみ IGMP スヌーピングをサポートします。

IGMP □□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□□□ □□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□ □□□□□
□□□□□□□□□□□□□□□□□□□□□□□ IP □□□□□□□□□□□□□□
□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□□
□□□□□□ □□□□□□□□□ IGMP □□□□□□□ □□□□□□
□□□ IP □□□□□ 0.0.0.0 □□□□□□□□□□□□□□□□□□□□□□□□□

その結果、ACI ファブリックは送信元 IP アドレス 0.0.0.0 の IGMP レポートを送信します。

（注） IGMP スヌーピングの詳細については、RFC 4541 を参照してください。

仮想化のサポート

IGMP スヌーピングに対して、複数の仮想ルーティングおよび転送（VRF）インスタンスを定義できます。

リーフ スイッチでは、**show** コマンドに VRF 引数を指定して実行すると、表示される情報のコンテキストを確認できます。VRF 引数を指定しない場合は、デフォルト VRF が使用されます。

APIC IGMP スヌーピング機能、IGMPv1、IGMPv2、および高速リーブ機能

IGMPv1 と IGMPv2 は両方とも、メンバーシップ レポート抑制をサポートします。つまり、同一サブネット上の 2 つのホストが同一グループのマルチキャスト データを受信する場合、他方のホストからメンバー レポートを受信するホストは、そのレポートを送信しません。メンバーシップ レポート抑制は、同じポートを共有しているホスト間で発生します。

各スイッチ ポートに接続されているホストが 1 つしかない場合は、IGMPv2 の高速脱退機能を設定できます。高速脱退機能を使用すると、最終メンバーのクエリー メッセージがホストに送信されません。APIC は、IGMP 脱退メッセージを受信すると、ただちに該当するポートへのマルチキャスト データ転送を停止します。

IGMPv1 では、明示的な IGMP 脱退メッセージが存在しないため、 APIC の IGMP スヌーピング機能は、特定のグループについてマルチキャスト データを要求するホストが存続しないことを示すために、メンバーシップ メッセージ タイムアウトを使用する必要があります。

（注） 高速脱退機能がイネーブルになっている場合、他のホストの存在は確認されないため、IGMP スヌーピング機能は、最終メンバーのクエリー インターバル設定を無視します。

APIC IGMP スヌーピング ファンクション キーと IGMPv3

APIC での IGMPv3 スヌーピング ファンクションでは、完全な IGMPv3 スヌーピングがサポートされています。これにより、IGMPv3 レポートの （S、G） 情報に基づいて、抑制されたフラッディングが提供されます。この送信元ベースのフィルタリングにより、デバイスは対象のマルチキャスト グループにトラフィックを送信する送信元に基づいて、マルチキャスト トラフィックの宛先ポートを制限できます。

デフォルトでは、IGMP スヌーピング機能は、ブリッジ ドメインでは、各 VLAN ポート上のホストを追跡します。この明示的なトラッキング機能は、高速脱退メカニズムをサポートして

います。IGMPv3 ではすべてのホストがメンバーシップ レポートを送信するため、レポート抑制機能を利用すると、デバイスから他のマルチキャスト対応ルータに送信されるトラフィック量を制限できます。レポート抑制を有効にしていても、IGMPv1 または IGMPv2 ホストが同じグループをリクエストしなかった場合、IGMP スヌーピング機能はプロキシ レポートを作成します。プロキシ機能により、ダウンストリーム ホストが送信するメンバーシップ レポートからグループ ステートが構築され、アップストリーム クエリアからのクエリーに応答するためにメンバーシップ レポートが生成されます。

IGMPv3 メンバーシップ レポートには ブリッジ ドメインのグループ メンバの一覧が含まれていますが、最終ホストが脱退すると、ソフトウェアはメンバーシップ クエリーを送信します。最終メンバーのクエリーインターバルについてパラメータを設定すると、タイムアウトまでにどのホストからも応答がなかった場合、IGMP スヌーピングはグループ ステートを削除します。

Cisco APIC および IGMP スヌーピング クエリア関数

マルチキャスト トラフィックをルーティングする必要がないために、Protocol-Independent Multicast（PIM）がインターフェイス上でディセーブルになっている場合は、メンバーシップ クエリーを送信するように IGMP スヌーピング クエリア機能を設定する必要があります。APIC、IGMP スヌープ ポリシー内で定義マルチキャストのソースとレシーバが含まれているブリッジ ドメインでクエリアがないその他のアクティブなクエリアします。

Cisco ACI はデフォルトで、IGMP スヌーピングが有効になっています。さらに、ブリッジ ドメイン サブネット制御は、「クエリア IP」を選択、リーフ スイッチによって、クエリアとして動作およびクエリ パケット送信を開始します。セグメントは、明示的なマルチキャスト ルータ (PIM が有効になっていません) があるないときに ACI Leaf スイッチでクエリアを有効にする必要があります。ブリッジ ドメインで、クエリアが設定されている、使用される IP アドレス マルチキャストのホストが設定されている同じサブネットからにする必要があります。

（注） クエリアの IP アドレスは、ブロードキャスト IP アドレス、マルチキャスト IP アドレス、または 0（0.0.0.0）にしないでください。

IGMP スヌーピング クエリアがイネーブルな場合は、定期的に IGMP クエリーが送信されるため、IP マルチキャスト トラフィックを要求するホストから IGMP レポート メッセージが発信されます。IGMP スヌーピングはこれらの IGMP レポートを待ち受けて、適切な転送を確立します。

IGMP スヌーピング クエリアは、RFC 2236 に記述されているようにクエリア選択を実行します。クエリア選択は、次の構成で発生します。

- 異なるスイッチ上の同じ VLAN に同じサブネットに複数のスイッチ クエリアが設定されている場合。
- 設定されたスイッチ クエリアが他のレイヤ 3 SVI クエリアと同じサブネットにある場合。

APIC IGMP スヌーピング機能の注意事項と制約事項

APIC IGMP スヌーピング機能に関する注意事項および制約事項は次のとおりです:

- レイヤ 3 IPv6 マルチキャスト ルーティングはサポートされていません。
- レイヤ 2 IPv6 マルチキャスト パケットは、着信ブリッジ ドメインでフラッディングされます。
- IGMPv3 スヌーピングは、ブリッジ ドメインで PIM が有効になっている場合にのみ、グループと送信元エントリに基づいてマルチキャストを転送します。PIM が有効になっていない場合、転送はグループのみに基づいて行われます。

IGMP スヌーピング ポリシーの設定と割り当て

拡張 GUI のブリッジ ドメインへの IGMP スヌーピング ポリシーの設定と割り当て

IGMP スヌーピング機能を実装するには、IGMP スヌーピング ポリシーを設定し、そのポリシーを 1 つまたは複数のブリッジ ドメインに割り当てます。

GUI を使用した IGMP スヌーピング ポリシーの設定

IGMP 設定を 1 つまたは複数のブリッジ ドメインに割り当てることが可能な IGMP スヌーピング ポリシーを作成します。

手順

ステップ 1 **[テナント]** タブと、IGMPP スヌーピング サポートを設定することを意図したブリッジ ドメインのテナントの名前をクリックします。

ステップ 2 [**ナビゲーション**（**Navigation**）] ペインで、**[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[IGMP スヌープ（IGMP Snoop）]** をクリックします。

ステップ 3 **[IGMP スヌープ]** を右クリックし、**[IGMP スヌープ ポリシーの作成]** を選択します。

ステップ 4 **Create IGMP Snoop Policy** ダイアログで、次のようにポリシーを設定します。

a) [Name] フィールドと [Description] フィールドに、ポリシーの名前と説明をそれぞれ入力します。

b) [**管理状態**（**Admin State**）] フィールドで [**有効化**（**Enables**）] または [**無効化**（**Disabled**）] を選択して、この特定のポリシーの IGMP スヌーピングを有効または無効にします。

c) [**ファスト リーブ**（**Fast Leave**）] を選択または選択解除し、このポリシーを通してクエリが即時ドロップする IGMP V2 を有効または無効にします。

d) [**クエリアの有効化（Enable querier**）] を選択して、このポリシーを通して IGMP クエリア アクティビティを有効または無効にします。

（注） このオプションを効果的を有効にするには、ポリシーを適用するブリッジ ドメインに割り当てられるサブネットで **[サブネット制御: クエリア IP]** 設定も有効にする必要があります。この設定のプロパティ ページへのナビゲーション パスは次のとおりです。**[テナント（Tenants）]** > **[*tenant_name*]** > **[ネットワーキング（Networking）]** > **[ブリッジ ドメイン（Bridge Dmains）]** > **[*bridge_domain_name*]** > **[サブネット（Subnets）]** > **[*subnet_subnet*]**

e) [クエリア バージョン（Querier Version）] フィールドで、[バージョン 2（Version 2）] または [バージョン 3（Version 3）] を選択して、この特定のポリシーの IGMP スヌーピング クエリア バージョンを選択します。

f) このポリシーの **[最後のメンバのクエリ間隔]** 値を秒で指定します。

IGMPv2 リーブ レポートを受信したら、IGMP がこの値を使用します。これは、少なくとも 1 個以上のホストをグループに残すことを意味します。リーブ レポートを受信した後、インターフェイスが IGMP ファスト リーブに設定されていないか確認し、されていない場合はout-of-sequence クエリを送信します。

g) このポリシーの **[クエリ間隔]** 値を秒で指定します。

この値は、グループ内でレポートを確認できない場合、IGMP 機能が特定の IGMP 状態を保存する合計時間を定義するために使用されます。

h) このポリシーの **[クエリの応答間隔]** 値を秒で指定します。

ホストがクエリ パケットを受信すると、最大応答所要時間以下のランダムな値でカウントが開始されます。このタイマーの期限が切れると、ホストはレポートで応答します。

i) このポリシーの **[クエリ カウントの開始]** を指定します。

スタートアップ クエリー インターバル中に送信される起動時のクエリー数。有効範囲は 1 ～ 10 です。デフォルトは 2 です。

j) このポリシーの **[クエリ間隔の開始]** を秒で指定します。

デフォルトでは、ソフトウェアができるだけ迅速にグループ ステートを確立できるように、このインターバルはクエリー インターバルより短く設定されています。有効範囲は 1 ～ 18,000 秒です。デフォルト値は 31 秒です。

ステップ 5 [送信（Submit）] をクリックします。

新しい IGMP スヌープ ポリシーは、**[プロトコル ポリシー - IGMP スヌープ]** サマリ ページに一覧になっています。

次のタスク

このポリシーを有効にするには、ブリッジ ドメインに割り当てます。

GUI を使用した IGMP スヌーピング ポリシーのブリッジ ドメインへの割り当て

IGMP スヌーピング ポリシーをブリッジ ドメインに割り当てると、そのブリッジ ドメインは、そのポリシーで指定された IGMP スヌーピング ポリシーを使用するように設定されます。

始める前に

- テナントのブリッジ ドメインを設定します。
- ブリッジ ドメインにアタッチする IGMP スヌーピング ポリシーを設定します。

（注） 割り当てられるポリシーで **Enable Querier** オプションを効果的に有効にするには、ポリシーを適用するブリッジ ドメインに割り当てられるサブネットで **Subnet Control: Querier IP** 設定も有効にする必要があります。この設定があるプロパティ ページへのナビゲーション パスは、**Tenants** > ***tenant_name*** > **Networking** > **Bridge Domains** > ***bridge_domain_name*** > **Subnets** > ***subnet_name*** です。

手順

ステップ 1 テナントのブリッジ ドメインで IGMP スヌープ ポリシーを設定するには、APIC の **Tenants** タブをクリックして、テナントの名前を選択します。

ステップ 2 APIC のナビゲーション ウィンドウで **Networking** > **Bridge Domains** をクリックして、ポリシー指定の IGMP スヌープ設定を適用するブリッジ ドメインを選択します。

ステップ 3 メインの **Policy** タブで、**IGMP Snoop Policy** フィールドまでスクロールして、ドロップダウン メニューから適切な IGMP ポリシーを選択します。

ステップ 4 **Submit** をクリックします。

ターゲットのブリッジ ドメインは、指定された IGMP スヌーピング ポリシーに関連付けられます。

IGMP スヌーピングの静的ポート グループの有効化

静的ポート グループの IGMP スヌーピングを有効にする

IGMP 静的ポートのグループ化により以前アプリケーション EPG に静的に割り当てられた事前プロビジョニングを有効にして、スイッチ ポートが IGMP マルチキャスト トラフィックを受

信および処理できます。この事前プロビジョニングは、通常 IGMP スヌーピング スタックがポートを動的に学習するときに発生する参加遅延を防止します。

静的グループ メンバーシップは、アプリケーション EPG に割り当てられている静的ポートでのみ事前プロビジョニングできます。

APIC GUI、CLI、および REST API インターフェイスを通じて、静的グループ メンバーシップを設定できます。

前提条件: 静的ポートに EPG を導入する

ポートで IGMP スヌープ処理を有効にするには、前提条件として、ターゲットのポートを、関連付けられている EPG に静的に割り当てる必要があります。

ポートの静的な導入は、APIC GUI、CLI、または REST API インターフェイスを通じて構成できます。詳細については、『*Cisco APIC* レイヤ *2* ネットワーキング設定ガイド』の次のトピックを参照してください：

- *GUI* を使用して特定のノードまたはポートへ *EPG* を導入する
- *NX-OS* スタイルの *CLI* を使用した *APIC* の特定のポートへの *EPG* の導入
- *REST API* を使用した *APIC* の特定のポートへの *EPG* の導入

GUI を使用した、スタティック ポートでの IGMP スヌーピングとマルチキャストの有効化

IGMP スヌーピングとマルチキャストは、EPG に静的に割り当てられているポートで有効にできます。その後、これらのポートで有効にされている IGMP スヌーピングとマルチキャストへのアクセスを許可または拒否されるユーザのアクセス グループを作成し、割り当てることができます。

始める前に

EPG の IGMP スヌーピングおよびマルチキャストを有効にする前に、次のタスクを実行します:

- この機能を有効にし、その EPG に静的に割り当てるインターフェイスを指定します。

（注） スタティック ポートの割り当てに関する詳細は、『*Cisco APIC* レイヤ *2* ネットワーキング設定ガイド』の「*GUI* を使用した特定のノードまたはポートで *EPG* を展開する」を参照してください。

- IGMP スヌーピングとマルチキャスト トラフィックの受信者とする IP アドレスを指定します。

手順

ステップ 1 **Tenant** > ***tenant_name*** > **Application Profiles** > ***application_name*** > **Application EPGs** > ***epg_name*** > **Static Ports** をクリックします。

このスポットに移動すると、ターゲット EPG に静的に割り当てたすべてのポートが表示されます。

ステップ 2 IGMP スヌーピングのグループ メンバーに静的に割り当てるポートをクリックします。
Static Path ページが表示されます。

ステップ 3 IGMP スヌープ スタティック グループの表で、+ をクリックして、IGMP スヌープ アドレス グループにエントリを追加します。

IGMP スヌープ アドレス グループにエントリを追加すると、ターゲットの静的ポートが指定されたマルチキャスト IP アドレスに関連付けられ、そのアドレスで受信した IGMP スヌープ トラフィックを処理できるようになります。

a) **Group Address** フィールドに、このインターフェイスとこの EPG に関連付けるマルチキャスト IP アドレスを入力します。
b) 当てはまる場合には、**Source Address** フィールドに、マルチキャスト ストリームの送信元となる IP アドレスを入力します。
c) **Submit** をクリックします。

設定が完了したら、ターゲットインターフェイスは、それに関連付けられているマルチキャスト IP アドレスに送信される IGMP スヌーピング プロトコル トラフィックを処理できるようになります。

（注） ターゲットのスタティック ポートにさらにマルチキャストアドレスを関連付けるには、この手順を繰り返します。

ステップ 4 [Submit] をクリックします。

IGMP スヌープ アクセス グループの有効化

IGMP スヌープ アクセス グループの有効化

「アクセス-グループ」ができるストリームを制御するために使用任意ポート背後に参加します。

実際に所属するするポートの設定を適用できることを確認するには、アプリケーション EPG に静的に割り当てられているインターフェイスでアクセス グループ設定を適用できる EPG。

ルート マップ ベースのアクセス グループのみが許可されます。

APIC GUI、CLI、および REST API インターフェイスを通じて、IGMP スヌープ アクセス グループを設定できます。

GUI を使用して、IGMP スヌーピングとマルチキャストへのグループ アクセスを有効にする

EPGに静的に割り当てられたポートでIGMPスヌーピングとマルチキャストを有効にしたら、ユーザのアクセス グループを作成して割り当て、それらのポートで有効にされたIGMPスヌーピングとマルチキャスト トラフィックへのアクセスを許可または拒否することができます。

始める前に

EPGにIGMPスヌーピングおよびマルチキャストへのアクセスを有効にする前に、この機能を有効にし、それらを静的に EPG に割り当てるインターフェイスを識別します。

（注） スタティック ポートの割り当てに関する詳細は、『*Cisco APIC* レイヤ *2* ネットワーキング設定ガイド』の「*GUI* を使用した特定のノードまたはポートで *EPG* を展開する」を参照してください。

手順

ステップ 1 **[テナント（Tenant）]** > **[*tenant_name*]** > **[アプリケーション プロファイル（Application Profiles）]** > **[*application_name*]** > **[アプリケーション EPG（Application EPGs）]** > **[*epg_name*]** > **[スタティック ポート（Static Ports）]** をクリックします。

このスポットに移動すると、ターゲット EPG に静的に割り当てたすべてのポートが表示されます。

ステップ 2 マルチキャスト グループ アクセスを割り当てる予定のポートをクリックして、 **Static Port Configuration** ページを表示します。

ステップ 3 **[アクション（Actions）]** > **[IGMP アドレス グループの作成（Create IGMP Access Group）]** をクリックして、IGMP スヌープ アクセス グループ テーブルを表示します

ステップ 4 IGMP スヌープ アクセス グループのテーブルで **+** をクリックして、アクセスグループのエントリを追加します。

IGMPスヌープアクセスグループのエントリを追加すると、このポートへのアクセス権を持つユーザ グループを作成すること、それをマルチキャスト IP アドレスと関連付け、そのアドレスで受信された IGMP スヌープ トラフィックへのグループ アクセスを許可または拒否することができます。

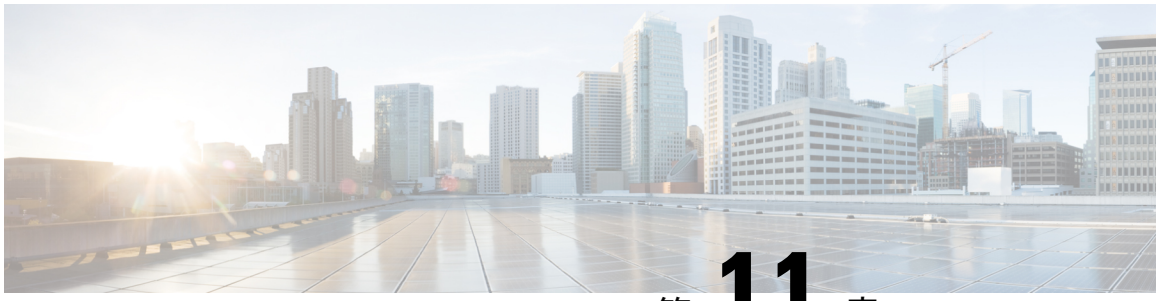
a) [**マルチキャスト向けルート マップ ポリシーの作成（Create Route Map Policy for Multicast）**] を選択して、[**マルチキャスト向けルート マップ ポリシーの作成（Create Route Map Policy for Multicast）**] ウィンドウを表示します。

b) **Name** フィールドで、マルチキャスト トラフィックの許可または拒否の対象となるグループの名前を割り当てます。
c) **Route Maps** テーブルで、+ をクリックして、ルート マップ ダイアログを表示します:
d) **Order** フィールドでは、このインターフェイスに対して複数のアクセス グループを設定している場合に、このインターフェイスでのマルチキャスト トラフィックへのアクセスをどの順序で許可または拒否するかを反映する番号を選択します。番号の小さいアクセス グループの方が、番号の大きいアクセス グループよりも前の順番になります。
e) **Group IP** フィールドには、このアクセス グループに対してトラフィックが許可または阻止される、マルチキャスト IP アドレスを入力します。
f) **Source IP** フィールドでは、当てはまる場合に、送信元の IP アドレスを入力します。
g) **Action** フィールドでは、ターゲット グループのアクセスを拒否する場合には **Deny** を、ターゲット グループのアクセスを許可する場合には **Permit** を選択します。
h) [OK] をクリックします。
i) **[送信（Submit）]** をクリックします。

設定が完了すると、設定されている IGMP のスヌープ アクセス グループは、 ターゲットの静的ポートと、そのアドレスで受信したマルチキャスト ストリームへの許可または拒否アクセスを通して、マルチキャスト IP アドレスに割り当てられます。

（注）
- その他のアクセス グループを設定し、ターゲットの静的ポートを通してマルチキャスト IP アドレスに関連付けるには、この手順を繰り返します。
- 構成されているアクセス グループの設定を確認するには、**[テナント（Tenant）]** > **[*tenant_name*]** > **[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[マルチキャスト向けルート マップ（Route Maps for Multicast）]** > **[*route_map_access_group_name*]** を選択します。

ステップ 5 [Submit] をクリックします。



第 11 章

MLD スヌーピング

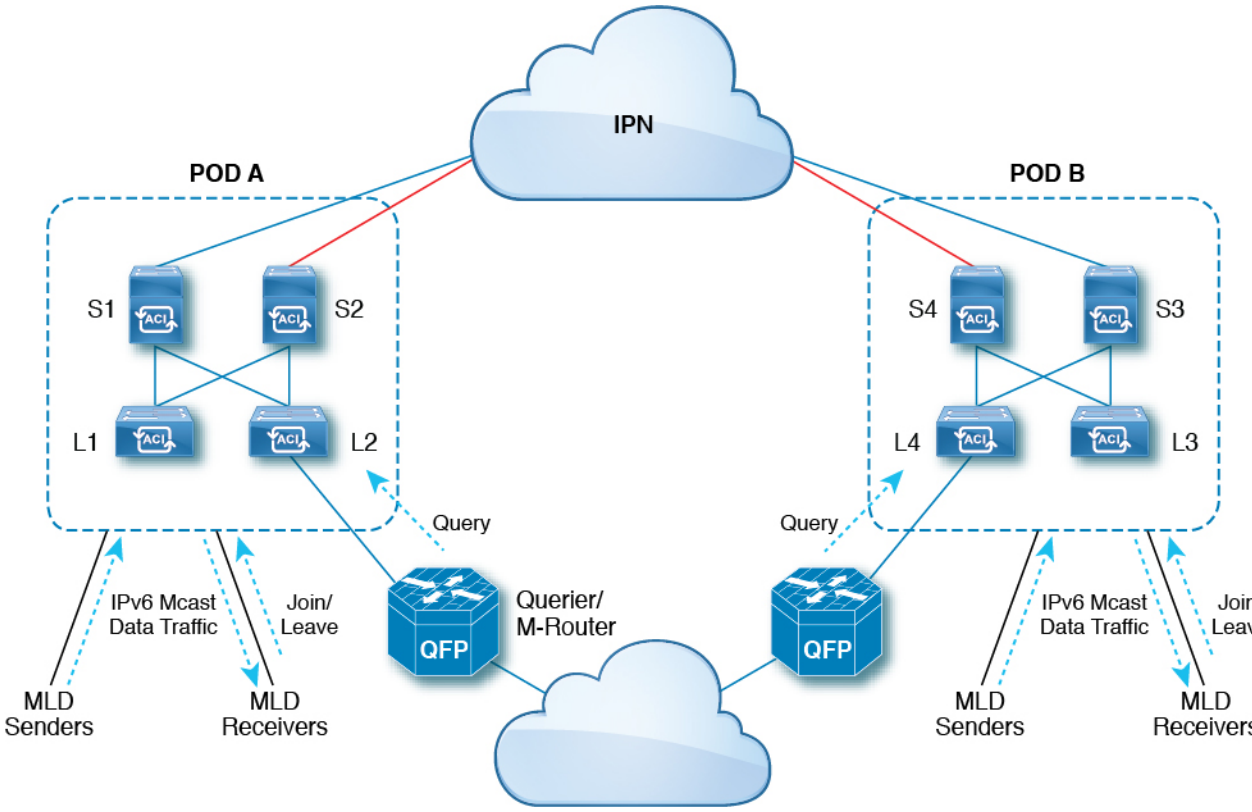
この章は、次の内容で構成されています。

Cisco APIC および MLD スヌーピングについて

マルチキャスト リスナー検出（MLD）スヌーピングにより、ホストとルータ間で IPv6 マルチキャスト トラフィックを効率的に配信できます。これは、MLD クエリまたはレポートを送受信したポートのサブセットにブリッジ ドメイン内の IPv6 マルチキャスト トラフィックを制限する レイヤ 2 機能です。このように、MLD スヌーピングは、マルチキャスト トラフィックの受信に関心を示しているノードがないネットワークのセグメントでは帯域幅を節約できるという利点があります。これにより、ブリッジ ドメインでフラッディングが生じることがなく、帯域幅の使用量が削減され、ホストとルータで不要なパケット処理を節約できます。

MLD スヌーピング機能は、IGMP スヌーピングと似ていますが、MLD スヌーピング機能は IPv6 マルチキャスト トラフィックをスヌーピングし、MLDv1（RFC 2710）および MLDv2（RFC 3810）コントロール プレーン パケットで動作します。MLD は ICMPv6 のサブプロトコルであるため、MLD メッセージのタイプは ICMPv6 メッセージのサブセットであり、MLD メッセージは IPv6 パケット内で先頭の Next Header 値 58 により識別されます。MLDv1 のメッセージ タイプには、リスナー クエリ、マルチキャスト アドレス固有（MAS）クエリ、リスナー レポート、完了メッセージが含まれます。MLDv2 は、追加のクエリ タイプであるマルチキャスト アドレスおよびソース固有（MASS）クエリを除き、MLDv1 と相互運用できるように設計されています。MLD で使用可能なプロトコル レベル タイマーは、IGMP で使用可能なものと同様です。

次の図に、MLD スヌーピング配置のさまざまなコンポーネントを示します。



次に、図のコンポーネントについて説明します。

- MLD 送信者（送信元）：IPv6 トラフィックをファブリックに送信するホスト。
- MLD レシーバ：IPv6 マルチキャスト パケットの受信に関係するホスト。セッションに参加するか、セッションから離脱するかを選択できます。
- クエリア/M ルータ：定期的にクエリを送信し、グループ メンバーシップ データベースを維持するルータまたはスイッチ。クエリアは定期的にクエリーを送信して、マルチキャスト ストリームへの参加に関心のあるユーザを特定します。M ルータ（マルチキャスト ルータ）は、ファブリック外の世界へのゲートウェイです。ファブリック内にマルチキャスト データ トラフィックがある場合、そのストリームはマルチキャスト ルータを介してファブリックの外部に出ることができます。

MLD スヌーピングがディセーブルの場合、すべてのマルチキャスト トラフィックは、関係があるかどうかに関係なく、すべてのポートにフラッディングされます。MLD スヌーピングがイネーブルの場合、ファブリックは MLD インタレストに基づいて IPv6 マルチキャスト トラフィックを転送します。不明な IPv6 マルチキャスト トラフィックは、ブリッジ ドメインの IPv6 L3 不明マルチキャスト フラッディング設定に基づいてフラッディングされます。

不明な IPv6 マルチキャスト パケットを転送するには、次の 2 つのモードがあります。

- フラッディング モード：ブリッジ ドメイン内のすべての EPG およびすべてのポートがフラッディング パケットを受信します。

- OMF（最適化済みマルチキャスト フラッディング）モード：マルチキャスト ルータ ポートのみがパケットを取得します。

注意事項と制約事項

MLD スヌーピング機能には、次のガイドラインと制約事項があります。

- MLD スヌーピングは、新世代 ToR スイッチでのみサポートされます。これらのスイッチモデルでは、スイッチ名の最後に「EX」、「FX」または「FX2」が付きます。
- ファブリック全体でスヌーピングされる最大 2000 の IPv6 マルチキャスト グループのサポートが有効になります。
- ハードウェア転送は、MLDv2 の送信元固有のスヌープ エントリに対しても、（*、G）ルックアップで行われます。
- このリリースの MLD スヌーピングでは、次の機能はサポートされていません。
  - ブリッジ ドメインまたは VRF にわたる レイヤ 3 マルチキャスト ルーティングは、IPv6 マルチキャスト トラフィックではサポートされません。
  - スタティック MLD スヌーピング エントリ
  - ルートマップを介した MLD スヌープ エントリのアクセス フィルタ
  - VTEP（VL）の背後にある仮想エンドポイント

GUI を使用した MLD スヌーピング ポリシーの設定とブリッジ ドメインへの割り当て

MLD スヌーピング機能を実装するには、MLD スヌーピング ポリシーを設定し、そのポリシーを 1 つまたは複数のブリッジ ドメインに割り当てます。

GUI を使用した MLD スヌーピング ポリシーの設定

MLD スヌーピング設定を 1 つまたは複数のブリッジ ドメインに割り当てることが可能な MLD スヌーピング ポリシーを作成します。

手順

ステップ 1 [テナント（**Tenants**）] タブと、MLD スヌーピング サポートを設定することを意図したブリッジ ドメインのテナントの名前をクリックします。

ステップ 2 [ナビゲーション（**Navigation**）] ペインで、**[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[MLD スヌープ（MLD Snoop）]** をクリックします。

ステップ 3 [**MLD スヌープ（MLD Snoop**）] を右クリックし、[**MLD スヌープ ポリシーの作成（Create MLD Snoop Policy**）] を選択します。

ステップ 4 [**MLD スヌープ ポリシーの作成（Create MLD Snoop Policy**）] ダイアログで、次のようにポリシーを設定します。

a) [Name] フィールドと [Description] フィールドに、ポリシーの名前と説明をそれぞれ入力します。

b) [**管理状態（Admin State**）] フィールドで [**有効化（Enables**）] または [**無効化（Disabled**）] を選択して、このポリシー全体を有効または無効にします。

デフォルトでは、このフィールドは [**無効化（Disabled**）] です。

c) [**コントロール（Control**）] フィールドで [**ファスト リーブ（Fast Leave**）] を選択または選択解除し、このポリシーを通してクエリが即時ドロップする MLD v1 を有効または無効にします。

d) **[コントロール（Control）]** フィールドで **[クエリアの有効化（Enable querier）]** を選択または選択解除して、MLD スヌープ ポリシーを通して MLD クエリア アクティビティを有効または無効にします。

（注） このオプションを効果的に有効にするには、このポリシーが適用されるブリッジドメインの MLD スヌープ ポリシーの **[クエリア（Querier）]** も有効にする必要があります。この設定のプロパティ ページへのナビゲーション パスは、**[テナント（Tenants）] > [tenant_name] > [ネットワーキング（Networking）] > [ブリッジドメイン（Bridge Dmains）] > [bridge_domain_name] . [MLD スヌープ ポリシー（MLD Snoop Policy）]** です。

e) このポリシーの **[クエリ間隔]** 値を秒で指定します。

クエリ間隔は、クエリアによって送信される全般的なクエリ間の間隔です。このフィールドのデフォルトエントリは 125 秒です。

f) このポリシーの **[クエリの応答間隔]** 値を秒で指定します。

ホストがクエリ パケットを受信すると、最大応答所要時間以下のランダムな値でカウントが開始されます。このタイマーの期限が切れると、ホストはレポートを出して応答します。

これは、ホストが MLD クエリ メッセージに応答するまでの最大応答時間を制御するために使用されます。値を 10 秒未満に設定すると、ルータによる、グループのプルーニングがより高速に行われるようになります。ただし、ホストの応答時間が短く制限されることになるため、ネットワークのバースト性が生じます。

g) このポリシーの **[最後のメンバのクエリ間隔]** 値を秒で指定します。

MLDは、MLD Leave レポートを受信すると、この値を使用します。これは、少なくとも 1 個以上のホストをグループに残すことを意味します。リーブ レポートを 受信した後、インターフェイスが IGMP ファスト リーブに設定されていないか確認し、されていない場合は out-of-sequence クエリを送信します。

このインターバル中に応答が受信されない場合、グループ ステートは解除されます。この値を小さく設定すると、グループの最終メンバーまたは送信元が脱退したことを、より短時間で検出できます。有効範囲は 1 ～ 25 秒です。デフォルト値は 1 秒です。

h) このポリシーの [**クエリ カウントの開始（Start Query Count**）] の値を指定します。

スタートアップ クエリー インターバル中に送信される起動時のクエリー数。有効範囲は 1 ～ 10 です。デフォルトは 2 です。

i) このポリシーの **[クエリ間隔の開始]** を秒で指定します。

デフォルトでは、ソフトウェアができるだけ迅速にグループ ステートを確立できるように、このインターバルはクエリー インターバルより短く設定されています。有効範囲は 1 ～ 18,000 秒です。デフォルト値は 31 秒です。

ステップ 5 [送信（Submit）] をクリックします。

新しい MLD スヌープ ポリシーは、[**プロトコル ポリシー - MLD スヌープ（Protocol Policies - MLD Snoop**）] サマリー ページに表示されています。

次のタスク

このポリシーを有効にするには、ブリッジ ドメインに割り当てます。

GUI を使用した MLD スヌーピング ポリシーのブリッジ ドメインへの割り当て

MLD スヌーピング ポリシーをブリッジ ドメインに割り当てると、そのブリッジ ドメインは、そのポリシーで指定された MLD スヌーピング ポリシーを使用するように設定されます。

始める前に

- テナントのブリッジ ドメインを設定します。
- ブリッジ ドメインにアタッチする MLD スヌーピング ポリシーを設定します。

（注） 割り当てられるポリシーで **Enable Querier** オプションを効果的に有効にするには、ポリシーを適用するブリッジ ドメインに割り当てられるサブネットで **Subnet Control: Querier IP** 設定も有効にする必要があります。この設定のプロパティ ページへのナビゲーション パスは次のとおりです。**Tenants** > ***tenant_name*** > **Networking** > **Bridge Dmains** > ***bridge_domain_name*** > **Subnets** > ***bd_subnet***

手順

ステップ 1 テナントのブリッジ ドメインで MLD スヌープ ポリシーを設定するには、APIC の [**テナント（Tenants**）] タブをクリックして、テナントの名前を選択します。

ステップ 2 APIC のナビゲーション ウィンドウで **[ネットワーキング（Networking）]** > **[ブリッジ ドメイン（Bridge Domains）]** をクリックして、ポリシー指定の MLD スヌープ設定を適用するブリッジ ドメインを選択します。

ステップ 3 メインの [**ポリシー（Policy**）] タブで、[**MLD スヌープ ポリシー（MLD Snoop Policy**）] フィールドまでスクロールして、ドロップダウン メニューから適切な MLD ポリシーを選択します。

ステップ 4 **[送信（Submit）]** をクリックします。`

ターゲットのブリッジ ドメインは、指定された MLD スヌーピング ポリシーに関連付けられます。

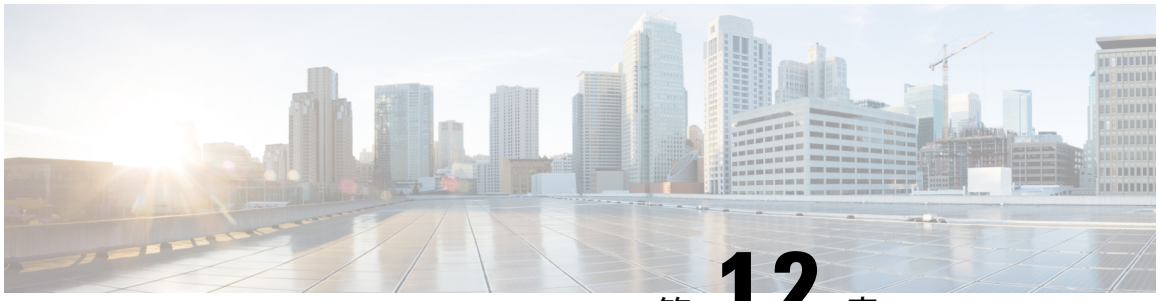
ステップ 5 ブリッジ ドメインのレイヤ 3 不明 IPv6 マルチキャスト宛先のノード転送パラメータを設定するには、次の手順を実行します。

a) 設定したブリッジ ドメインを選択します。
b) [ポリシー（Policy）] タブをクリックし、[全般（General）] サブタブをクリックします。
c) [IPv6 L3 不明なマルチキャスト（IPv6 L3 Unknown Multicast）] フィールドで、[フラッド（Flood）] または [最適化済みフラッド（Optimized Flood）] を選択します。

ステップ 6 スイッチ クエリア機能のリンクローカル IPv6 アドレスを変更するには、次の手順を実行します。

a) 設定したブリッジ ドメインを選択します。
b) [**ポリシー（Policy**）] タブをクリックして、[**L3 コンフィグレーション（L3 Configurations**）] サブタブをクリックします。
c) [**リンクローカル IPv6 アドレス（Link-local IPv6 Address**）] フィールドに、必要に応じてリンクローカル IPv6 アドレスを入力します。

ブリッジ ドメインのデフォルトのリンクローカル IPv6 アドレスは、内部的に生成されます。必要に応じて、このフィールドにブリッジ ドメインの別のリンクローカル IPv6 アドレスを設定します。



第 12 章

テナント ルーテッド マルチキャスト

この章は、次の内容で構成されています。

テナント ルーテッド マルチキャスト

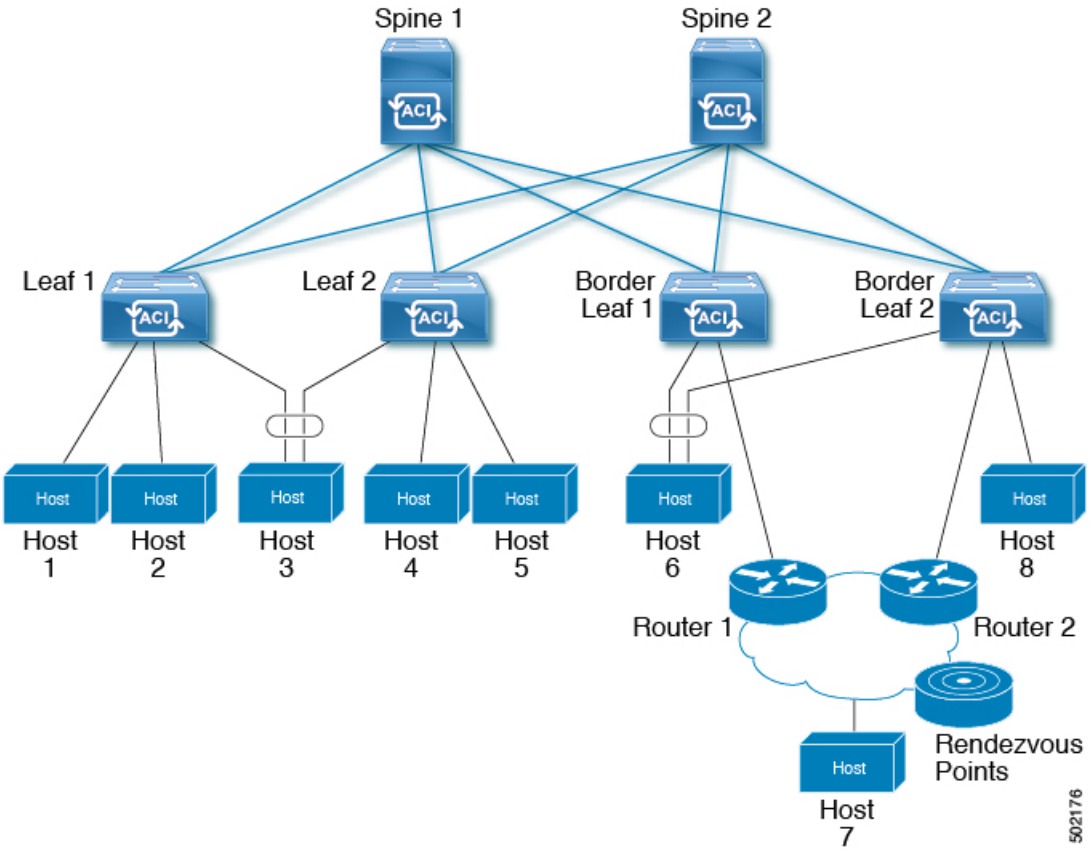
Cisco Application Centric Infrastructure （ACI）テナント ルーテッド マルチキャスト（TRM）は、Cisco ACI テナント VRF インスタンスでレイヤ 3 マルチキャスト ルーティングを有効にします。TRMは、同じサブネット内または異なるサブネット内の送信者と受信者の間のマルチキャスト転送をサポートしています。マルチキャストの送信元と受信者は、同じまたは異なるリーフ スイッチに接続することや、L3Out接続を使用してファブリックの外部に接続することができます。

Cisco ACI ファブリックでは、ほとんどのユニキャストと IPv4/IPv6 マルチキャスト ルーティングが同じ境界リーフ スイッチで稼働しており、ユニキャスト ルーティング プロトコル上でマルチキャスト プロトコルが稼働しています。

このアーキテクチャでは、境界リーフ スイッチのみが完全な Protocol Independent Multicast （PIM）または PIM6 プロトコルを実行します。非境界リーフ スイッチは、インターフェイス上でパッシブ モードの PIM/PIM6 を実行します。これらは、その他の PIM/PIM6 ルータとピアリングしません。境界リーフ スイッチは、L3Out を介してそれらの接続された他の PIM/PIM6 ルータとピアリングし、またそれら相互にもピアリングします。

次の図は、IPv4/IPv6 マルチキャスト クラウド内のルータ 1 とルータ 2 に接続する境界リーフ スイッチ 1 と境界リーフ スイッチ 2 を示しています。IPv4/IPv6 マルチキャスト ルーティングを必要とするファブリック内の各 Virtual Routing and Forwarding（VRF）インスタンスは、それぞれ別に外部マルチキャスト ルータとピアリングします。

図 7: マルチキャスト クラウドの概要



リモート リーフ スイッチでのレイヤ 3 マルチキャストのサポート

リリース 5.1(3) より以前では、ローカル リーフ スイッチのシングルポッド、マルチポッド、およびマルチサイト トポロジでのレイヤ 3 マルチキャスト ルーティングがサポートされていました。リリース 5.1(3) 以降では、リモート リーフ スイッチのレイヤ 3 マルチキャスト ルーティングもサポートされます。このサポートの一部として、リモート リーフ スイッチは境界リーフ スイッチまたは非境界リーフ スイッチとして機能できます。

新しくサポートされたリモート リーフ スイッチと以前にサポートされたローカル リーフ スイッチには、レイヤ 3 マルチキャスト ルーティングまたは Cisco の実装に関して違いはありません。Cisco APICACI マルチサイト オーケストレータこの 2 つの主な違いは、トラフィックの転送方法に基づいています。

- 単一ファブリック内のローカル リーフ スイッチ間のレイヤ 3 マルチキャストは、外部宛先 IP アドレスが VRF GIPo マルチキャスト アドレスである VXLAN マルチキャスト パケットとして転送されます。
- リモート リーフ スイッチとの間で送受信されるレイヤ 3 マルチキャスト パケットは、VXLAN ユニキャスト ヘッドエンド複製パケットとしてカプセル化されます。

レイヤ 3 マルチキャスト ルーティングが VRF に対して有効になっている場合、VRF GIPo マルチキャスト アドレスは、VRF が展開されているすべてのリーフ スイッチでプログラムされます。レイヤ 3 マルチキャスト パケットは、ポッド全体またはポッド間でマルチキャスト パケットとして転送され、VRF が導入されているすべてのリーフ スイッチで受信されます。リモート リーフ スイッチの場合、レイヤ 3 マルチキャスト パケットは、ヘッドエンド複製を使用して、VRF が導入されているすべてのリモート リーフ スイッチに転送されます。このヘッドエンド複製は、マルチキャスト ソースが接続されているポッドまたはリモート リーフで行われます。たとえば、マルチキャスト送信元がローカル リーフ スイッチに接続されている場合、これらのリモート リーフ スイッチが他のポッドと関連付けられていても、そのポッド内のスパイン スイッチの 1 つが選択され、VRF が導入されているすべてのリモート リーフ スイッチにこれらのマルチキャスト パケットが複製されます。レイヤ 3 マルチキャスト送信元がリモート リーフ スイッチに接続されている場合、リモート リーフ スイッチもヘッドエンド複製を使用して、マルチキャスト パケットのコピーをすべてのポッドのスパイン、および VRF が導入されているその他すべてのリモート リーフ スイッチへ送信します。

ヘッドエンド複製を使用したマルチキャスト転送は、マルチキャスト パケットをすべてのヘッドエンド複製トンネルの個別のユニキャスト パケットとして複製します。リモート リーフ スイッチ設計のレイヤ 3 マルチキャストでは、リモート リーフ スイッチが接続されている IP ネットワーク（IPN）に、マルチキャスト トラフィック要件をサポートするのに十分な帯域幅があることを確認する必要があります。

リモート リーフ スイッチは、PIM が有効または無効の L3Out 接続をサポートします。PIM 対応 L3Out を持つ VRF 内のすべてのリーフ スイッチは、外部ソースおよびランデブー ポイントに向けてファブリックから PIM Join を送信できます。ファブリックに接続されたマルチキャスト レシーバがグループの IGMP 加入を送信すると、ファブリックは PIM 対応境界リーフ スイッチの 1 つを選択して加入を送信します（ストライプ勝者（stripe winner）として）。グループのレシーバがメイン ポッドのローカル リーフ スイッチに接続されている場合でも、PIM 対応 L3Out を備えたリモート リーフ スイッチをグループのストライプ勝者として選択できます。レイヤ3マルチキャストトラフィックの準最適な転送の可能性があるため、リモートリーフスイッチにPIM対応L3Outを導入することは推奨されません。

注意事項と制約事項

- ポッドの冗長性は、リモート リーフ スイッチによるレイヤ 3 マルチキャスト転送でサポートされます。リモート リーフ スイッチが関連付けられているポッド内のすべてのスパイン スイッチに障害が発生した場合、リモート リーフ スイッチは別のポッド内のスパイン スイッチへのコントロール プレーン接続を確立できます。
- リモート リーフ スイッチは、ポッド内の少なくとも 1 つのスパイン スイッチに接続できる必要があります。リモート リーフ スイッチがすべてのスパイン スイッチへの接続を失った場合、レイヤ 3 マルチキャスト トラフィックは転送されません。これには、同じリーフ スイッチ上の送信者と受信者間のレイヤ 3 マルチキャスト トラフィックが含まれます。

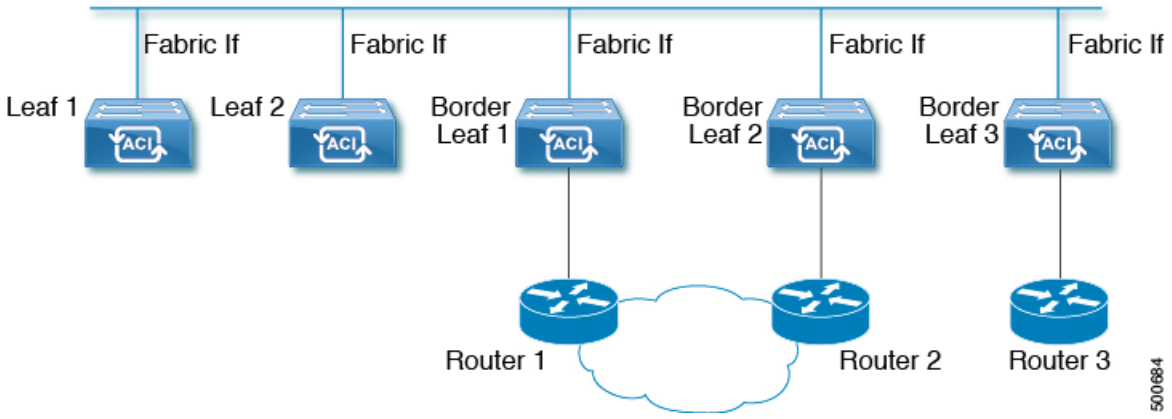
ファブリック インターフェイスについて

ファブリック インターフェイスはソフトウェア モジュール間の仮想インターフェイスであり、IPv4/IPv6 マルチキャスト ルーティングのファブリックを表します。インターフェイスは、宛先が VRF GIPo（グループ IP 外部アドレス）であるトンネル インターフェイスの形式を取ります。[2]. PIM6 は、PIM4 が使用するものと同じトンネルを共有します。たとえば、境界リーフがグループのトラフィックの転送を担当する指定フォワーダの場合、ファブリック インターフェイスはグループの発信インターフェイス (OIF) となります。ハードウェアのインターフェイスに相当するものはありません。ファブリック インターフェイスの動作状態は、intermediate system-to-intermediate system（IS-IS）によって公開される状態に従ったものとなります。

（注） マルチキャスト対応の各 VRF には、ループバック インターフェイスで構成された 1 つ以上の境界リーフ スイッチが必要です。PIM 対応の L3Out のすべてのノードで、一意の IPv4 ループバック アドレスを設定する必要があります。Router-ID ループバックまたは別の一意のループバック アドレスを使用できます。

ユニキャスト ルーティング用に設定された任意のループバックは再利用できます。このループバック アドレスは、外部ネットワークからルーティングする必要があり、VRF のファブリック MP-BGP (マルチプロトコル境界ゲートウェイ プロトコル) ルートに挿入されます。ファブリック インターフェイスの送信元 IP は、このループバックに、ループバック インターフェイスとして設定されます。次の図は、IPv4/IPv6 マルチキャスト ルーティング用のファブリックを示しています。

図 *8 : IPv4/IPv6* マルチキャスト ルーティング用のファブリック



[2] GIPo（グループ IP 外部アドレス）とは、ファブリック内で転送されたすべてのマルチデスティネーション パケット（ブロードキャスト、未知のユニキャストおよびマルチキャスト）で、VXLAN パケットの外部 IP ヘッダーで使用される宛先マルチキャスト IP アドレスです。

IPv4/IPv6 テナント ルート マルチキャストの有効化

ファブリックで IPv4 または IPv6 マルチキャスト ルーティングを有効または無効にするプロセスは、次の 3 つのレベルで実行されます。Cisco ACI

- VRF レベル：VRF レベルでマルチキャスト ルーティングを有効にします。
- **L3Out レベル**：VRFインスタンス で構成された 1 つ以上の L3Out に対して PIM/PIM6 を有効にします。
- ブリッジ ドメイン レベル：マルチキャスト ルーティングが必要な 1 つ以上のブリッジ ドメインに対して PIM/PIM6 を有効にします。

トップ レベルでは、IPv4/IPv6 マルチキャスト ルーティングは、任意のマルチキャスト ルーティングが有効なブリッジ ドメインを持つ VRF インスタンスで有効にする必要があります。IPv4/IPv6 マルチキャスト ルーティングが有効な VRF インスタンスでは、IPv4/IPv6 マルチキャスト ルーティングが有効なブリッジ ドメインおよび IPv4/IPv6 マルチキャスト ルーティングが無効なブリッジ ドメインの組み合わせにすることができます。IPv4 / IPv6マルチキャスト ルーティングが無効になっているブリッジドメインは、VRF IPv4 / IPv6マルチキャストパネルに表示されません。IPv4/IPv6 マルチキャスト ルーティングが有効な L3Out はパネル上でも表示されますが、IPv4/IPv6 マルチキャスト ルーティングが有効なブリッジ ドメインは常に IPv4/IPv6 マルチキャスト ルーティングが有効な VRF インスタンスの一部になります。

Cisco Nexus 93128TX、9396PX、9396TX などのリーフ スイッチでは、IPv4/IPv6 マルチキャスト ルーティングはサポートされていません。すべての IPv4/IPv6 マルチキャスト ルーティングと IPv4/IPv6 マルチキャストが有効な VRF インスタンスは、製品 ID に -EX および -FX という名前を持つスイッチでのみ展開される必要があります。

（注） L3Out ポートとサブインターフェイスがサポートされています。外部 SVI のサポートは、リリースによって異なります。

- リリース 5.2(3) より前のリリースでは、外部 SVI はサポートされていません。
- リリース 5.2(3) 以降では、SVI L3Out のレイヤ 3 マルチキャストがサポートされます。PIM は、物理ポートおよびポート チャネルの SVI L3Out でサポートされますが、vPC ではサポートされません。PIM6 は L3Out SVI ではサポートされません。

VRF GIPo の割り当て

VRF GIPo は、構成に基づいて暗黙的に割り当てられます。VRF に対して 1 つの GIPoが、そしてその VRF の下の各 BD に対して 1 つの GIPo があります。さらに、任意の GIPo は、複数の BD または複数の VRF の間で共有される可能性がありますが、しかし、VRF と BD の組み合わせで共有されることはありません。APIC は、この点を確認する必要があります。すでに処理

され、VRF GIPo ツリーが構築された BD GIPo に加えて VRF GIPo を処理する場合には、IS-IS が変更されます。

（注） 同じ VRF の場合、VRF GIPo は IPv4 と IPv6 の両方に共通です。

PIM/PIM6 が有効な BD のすべてのマルチキャスト トラフィックは、VRF GIPo を使用して、ファブリックに転送されます。これには、レイヤ 2 およびレイヤ 3 IPv4/IPv6 マルチキャストの両方が含まれます。マルチキャストが有効な BD 上のブロードキャストまたはユニキャスト フラッド トラフィックは、引き続き BD GIPo を使用します。非 IPv4/IPv6 マルチキャストが有効な BD は、すべてのマルチキャスト、ブロードキャスト、およびユニキャスト フラッド トラフィックで BD GIPo を使用します。

APIC GUI は、すべての BD と VRF で GIPo マルチキャスト アドレスを表示します。表示されるアドレスは常に、/28 ネットワーク アドレスとなります（最後の 4 ビットは 0）。VXLAN パケットがファブリックで送信されると、宛先マルチキャスト GIPo アドレスは、この /28 ブロック内のアドレスとなり、16 FTAG ツリーのいずれかを選択するために使用されます。これにより、ファブリック全体のマルチキャスト トラフィックをロード バランシングします。

表 *8 : GIPo* の使用方法

トラフィック	非 **MC** ルーティングが有効な **BD**	**MC** ルーティングが有効な **BD**
ブロードキャスト	BD GIPo	BD GIPo
不明なユニキャスト フラッディング	BD GIPo	BD GIPo
マルチキャスト	BD GIPo	VRF GIPo

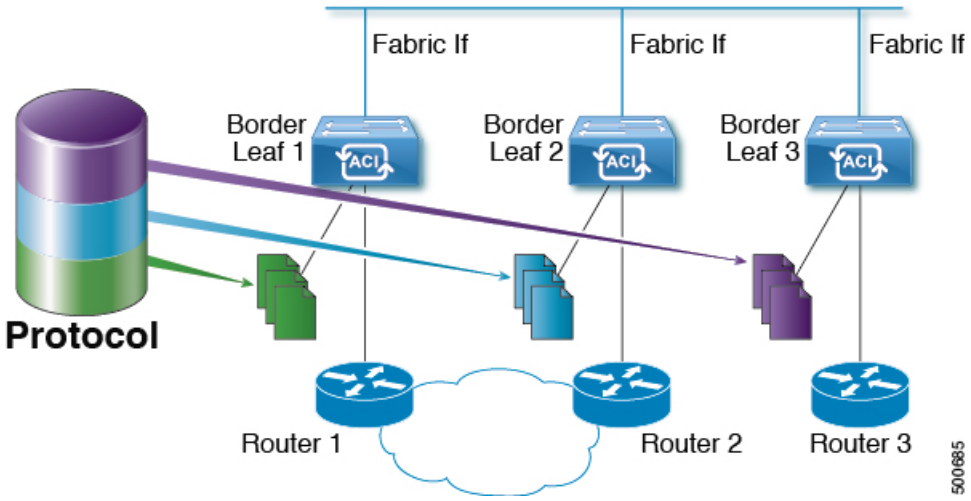
指定フォワーダーとしての複数のボーダー リーフ スイッチ

ファブリック内に、IPv4/IPv6 マルチキャスト ルーティングを行う複数の境界スイッチ (BL) がある場合、境界リーフのうちの 1 台だけが、外部 IPv4/IPv6 マルチキャスト ネットワークからのトラフィックを集めてファブリックに転送する、指定されたフォワーダとして選択されます。これによってトラフィックの複数のコピーが発生することを防ぎ、複数の BL スイッチの間でバランスが取れるようにします。

このことは利用可能な BL スイッチにわたる、これはグループ アドレスと VRF ネットワーク ID (VNID) としてのグループの所有権を、ストライピングすることによって行われます。グループの責任を担う BL は、外部ネットワークへの PIM/PIM6 の参加を送信して、ファブリックのレシーバの代わりにファブリックへのトラフィックを集めます。

ファブリックの各 BL は、その VRF の他のすべてのアクティブな BL スイッチのビューを持ちます。それでそれぞれの BL スイッチは、独立に矛盾なく、グループのストライピングを行えます。各 BL は、アクティブな BL スイッチのリストを取得するために、ファブリック インターフェイス上の PIM/PIM6 ネイバーの関係をモニターします。BL スイッチが削除または検出されたときには、その時点でのアクティブな BL スイッチ間で、グループの再ストライピングが行われます。ストライピングは、マルチポッド環境で GIPos を外部リンクにハッシュするために用いられる方法に似ています。それで、グループから BL へのマッピングは持続性があり、アップ時やダウン時の変化が少なくてすみます。

図 *9:* 指定されたフォワーダとしての複数の境界リーフのモデル



PIM/PIM6 指定ルータの選定

ACI ファブリックのレイヤ 3 IPv4/IPv6 マルチキャストでは、異なるインターフェイス タイプの PIM/PIM6 DR（代表ルータ）メカニズムは次の通りです。

- PIM/PIM6 が有効な L3 Out インターフェイス：これらのインターフェイス タイプの標準の PIM/PIM6 DR メカニズムに従います。
- [ファブリック インターフェイス]：このインターフェイスの DR 選定は、ストライピングにより決定される DR 機能ほど重要ではありません。PIM/PIM6 DR の選定は、引き続きこのインターフェイスに残ります。
- IPv4/IPv6 マルチキャスト ルーティングが有効なパーベイシブ BD：ファブリックのパーベイシブ BD はすべて、IPv4/IPv6 マルチキャスト ルーティングに関するスタブです。そのため、すべてのリーフ スイッチで、vPC を含む普及 BD の SVI インターフェイスがセグメントの DR と見なされます。

非境界リーフ スイッチの動作

非境界リーフ スイッチ上の PIM/PIM6 は、ファブリック インターフェイスとパーベイシブ BD SVI では、パッシブ モードで動作します。PIM/PIM6 は新しいパッシブ プローブ モードになっており、*hellos* だけを送信します。これらのパーベイシブ BD SVI では、PIM/PIM6 ネイバーは想定されていません。PIM/PIM6 がパーベイシブ BD から *hello* を受信した場合には、障害が発生するのが望ましい動作です。非境界リーフ スイッチ上の PIM/PIM6 は、パーベイシブ BD上の *hellos* と、ファブリック インターフェイス上のソース登録パケットを除き、PIM/PIM6 プロトコルパケットを送信しません。

同時に、PIM/PIM6 はファブリック インターフェイス上の次の PIM/PIM6 パケットを受信して処理します:

- **PIM/PIM6 Hellos**: これはファブリック インターフェイス上でアクティブな BL リストを追跡するために使用されます。パーベイシブ BD上では、フォールトを発生するために使用されます。
- PIM BSR、Auto-RP アドバタイズメント：PIM でのみサポートされ、PIM6 ではサポートされません。これはファブリック インターフェイスで受信され、RP からグループ範囲へのマッピングを収集するために処理されます。

アクティブな境界リーフ スイッチ リスト

すべてのリーフ スイッチで、PIM/PIM6 はストライピングとその他の目的に使用されるアクティブな境界リーフ スイッチのリストを保持しています。境界リーフ スイッチ自体で、このアクティブな境界リーフ リストはアクティブな PIM/PIM6 のネイバー関係から導出されます。非境界リーフ スイッチで、リストファブリック インターフェイス上のモニター対象の PIM/PIM6 *Hello* メッセージを使用して PIM/PIM6 によりリストが生成されます。*Hello* メッセージの送信元 IP は、各境界リーフ スイッチに割り当てられた IPv4/IPv6 ループバック IP です。

ブート時のオーバーロード動作

境界リーフ スイッチが起動後、または接続を失った後に初めてファブリックへの接続を得たとき、境界リーフ スイッチが **COOP** リポジトリ情報を受信する機会を得るまでは、境界リーフ スイッチがアクティブな境界リーフ スイッチ リストの一部になることは望ましくありません。すべての IPv4/IPv6 マルチキャスト グループ メンバーシップ情報は、スパイン上の COOP データベースに保管されます。[3]境界リーフ スイッチがアクティブな境界リーフ スイッチのリストに加えられるのは望ましいことではありません。これは、PIM/PIM6 の *hello* メッセージの伝送を、設定されていない期間だけ遅らせることで実現できます。

[3] 境界リーフはブート時にスパインからこの情報を取得します。

ファーストホップ機能

リーフ スイッチへの直接接続は、PIM/PIM6 sparse モードに必要なファーストホップ機能を処理します。

ラストホップ

ラストホップ ルータは受信側に接続されるもので、PIM/PIM6 の any-source マルチキャスト (ASM) が発生した場合、最短パスツリー (SPT) スイッチオーバーを実行する責任を負います。境界リーフ スイッチはこの機能を処理します。境界非リーフ スイッチはこの機能には参加しません。

高速コンバージェンス モード

ファブリックはすべての境界リーフ スイッチがルートへの接続性の外部で設定可能な高速コンバージェンス モードをサポートしています (の *RP (*、G)* の送信元と *(S, G)*)、外部ネットワークからのトラフィックを停止します。重複を防ぐためには、1 人だけ、BL スイッチ転送トラフィック、ファブリックにします。ファブリックに、グループのトラフィックを転送する BL グループの代表フォワーダ (DF) と呼びます。グループのストライプ受賞は、DF を決定します。ストライプ受賞にルートへの到達可能性がある場合は、ストライプ受賞も DF です。ストライプで優先されるデータが、ルートへの外部接続を持たない場合、その BL は、ファブリック インターフェイス経由で PIM/PIM6 join を送信することによって、DF を選択します。外部からルートに到達可能なすべての非ストライプ優先 BL スイッチは PIM/PIM6 join を送信してトラフィックを引きこみまずが、ルート向けの RPF インターフェイスとしてファブリック インターフェイスを保持します。これは、結果、トラフィックをドロップされたが、外部のリンク上で BL スイッチに到達します。

高速コンバージェンス モードの利点はプログラミング右のリバース パス フォワーディング（RPF） インターフェイスの新しいストライプ受賞 BL スイッチのみに必要なアクションになどの損失のためのストライプ所有者変更がある場合にです。新しいストライプ優先から PIM/PIM6 ツリーに参加することによって発生する遅延はありません。これは、非ストライプ受賞の外部リンクで追加帯域幅の使用増やしますが機能します。

（注） 追加の帯域幅のコストが保存コンバージェンス時間を上回る導入では、高速コンバージェンス モードを無効にできます。

ランデブー ポイントについて

ランデブー ポイント（RP）は、マルチキャスト ネットワーク ドメイン内にあるユーザーが選択した IP アドレスで、マルチキャスト共有ツリーの共有ルートとして動作します。必要に応じて複数の RP を設定し、さまざまなグループ範囲をカバーすることができます。複数の RP を設定する場合は、各 RP を一意のグループ範囲に設定する必要があります。

マルチキャスト ルーティングが有効になっている VRF には、PIM 対応境界リーフ スイッチが必要です。PIM は、L3Out レベルで PIM を有効にすることで、境界リーフに対して有効になります。L3Out に対して PIM を有効にすると、その L3Out で設定されているすべてのノードとインターフェイスに対して PIM が有効になります。

RP には 2 つのタイプを設定することができます。

- **スタティック RP**：マルチキャスト グループ範囲の RP を静的に設定できます。この場合、ドメイン内のすべてのルータに RP のアドレスを設定する必要があります。
- **ファブリック RP**：VRF 内のすべての PIM 対応ボーダー リーフ スイッチで PIM エニーキャスト RP ループバック インターフェイスを有効にします。これは、VRF 間マルチキャストをサポートするために必要です（Inter-VRF マルチキャストについて （82 ページ）を参照）。ファブリック RP 設定には、PIM 対応の L3Out（ループバック インターフェイスあり）が必要です。設定すると、外部ルータはファブリック RP を使用できます。Auto-RP および BSR はファブリック RP ではサポートされません。外部エニーキャスト RP メンバーとのファブリック RP ピアリングはサポートされていません。

（注） ファブリック RP には、次の制限があります。

- ファブリック RP は高速コンバージェンス モードをサポートしていません。
- ファブリック IP：
  - スタティック RP とファブリック RP 内のすべてのスタティック RP エントリで一意でなければなりません。
  - レイヤ 3 out ルータ ID のいずれかにすることはできません。

RP の設定については、次のセクションを参照してください。

- GUI を使用したレイヤ 3 マルチキャストの設定 （95 ページ）
- NX-OS スタイルの CLI を使用したレイヤ 3 マルチキャストの設定 （519 ページ）
- REST API を使用したレイヤ 3 マルチキャストの設定 （601 ページ）

Inter-VRF マルチキャストについて

（注） Inter-VRF マルチキャストは、IPv6 マルチキャストではサポートされません。

マルチキャスト ネットワークを持つ一般的なデータセンターでは、マルチキャストのソースおよびレシーバは同じ VRF にあり、すべてのマルチキャスト トラフィックはその VRF 内で転送されます。マルチキャストのソースとレシーバが異なる VRF に存在する使用例があります。

- 監視カメラは 1 つの VRF 内にありますが、カメラ フィードは異なる VRF 内のコンピュータで閲覧します。
- マルチキャスト コンテンツ プロバイダーは 1 つの VRF 内にありますが、組織のさまざまな部門は、異なる VRF でマルチキャスト コンテンツを受信します。

ACI リリース 4.0 は、送信元と受信側が異なる VRF 内にあることを可能にする inter-VRF マルチキャストのサポートを追加します。これにより受信側の VRF は、送信元 VRF のマルチキャスト ルートに対して、リバース パス フォワーディング（RPF）ルックアップを実行できるようになります。送信元 VRF で有効な RPF インターフェイスが形成されると、受信側の VRF で発信インターフェイス（OIF）が有効になります。すべての inter-VRF マルチキャスト トラフィックは、送信元 VRF のファブリック内で転送されます。inter-VRF 転送と変換は、受信側が接続されているリーフ スイッチで実行されます。

（注）
- Any-source マルチキャストでは、使用される RP は送信元と同じ VRF 内にある必要があります。
- Inter-VRF マルチキャストは、共有サービスと共有 L3Out 構成の両方をサポートします。ソースとレシーバは、異なる VRF の EPG または L3Out に接続できます。

ACI の場合、inter-VRF マルチキャストは受信側の VRF ごとに設定されます。受信側 VRF を持つすべての NBL/BL は、同じ inter-VRF 設定となります。直接接続されたレシーバを持つ各 NBL、および外部レシーバを持つ BL では、送信元 VRF が展開されている必要があります。コントロール プレーンのシグナリングとデータプレーンの転送は、レシーバを持つ NBL/BL 内の VRF 間で必要な変換と転送を行います。ファブリックで転送されるすべてのパケットは、送信元 VRF 内にあります。

Inter-VRF マルチキャストの要件

このセクションでは、Inter-VRF マルチキャストの要件について示します。

- 特定のグループのすべての送信元は、同じ VRF（送信元 VRF）でなければなりません。

- 送信元 VRF と送信元 EPG は、受信側 VRF があるすべてのリーフ上に存在している必要があります。
- ASM の場合：
  - RP は送信元（送信元 VRF）と同じ VRF 内になければなりません。
  - リリース 4.2(4) 以前で、送信元 VRF は、ファブリック RP を使用する必要があります。この制限は、リリース 4.2(4) 以降には適用されません。
  - 特定のグループ範囲の送信元およびすべての受信側 VRF で、同じ RP アドレス設定を適用する必要があります。

ストライプ ウィナー ポリシーの設定について

VRF に複数の PIM 対応ボーダー リーフ スイッチがある場合、デフォルトの動作では、PIM-SM のマルチキャスト グループまたは PIM-SSM のグループおよびソースのストライプ ウィナーとして 1 つのボーダー リーフ スイッチを選択します。ストライプ ウィナー として選択されたボーダー リーフは、グループのラスト ホップ ルータ（LHR）として機能し、外部接続されたリンクで外部ソースに向けて PIM 参加/プルーニング メッセージを送信します。指定フォワーダとしての複数のボーダー リーフ スイッチを参照してください。ストライプ ウィナーとして選択されたボーダー リーフは、ファブリック全体の任意のポッドの任意のボーダー リーフにすることができます。このデフォルトの動作により、次のいくつかのシナリオではマルチキャスト ストリームの遅延が増大する可能性があります。

- 既知のマルチキャストグループまたはグループ範囲のすべてまたはほとんどのレシーバが 1 つのポッドに接続されます。グループのストライプ ウィナーが別のポッドで選択された場合、外部ソースからのマルチキャスト ストリームが IPN を介して転送されるため、遅延が増大します。
- 外部マルチキャスト送信元が、いずれかのポッドと同じ物理的な場所にあります。マルチキャスト グループのストライプ ウィナーが別のポッドで選択されている場合、フローが送信元に最も近いポッド内の受信者に向かう場合でも、外部ネットワークを通過してリモート ポッドのボーダー リーフに到達し、その後 IPN を通過するため、フローの遅延が増大する可能性があります。

ACI リリース 6.0(2) 以降、ファブリックは、特定のマルチキャスト グループやグループ範囲、送信元や送信元範囲向けのポッドを選択できる、構成可能なストライプ ウィナー ポリシーをサポートしています。これにより、ストライプ ウィナーとして選択されたボーダー リーフが、選択されたポッドからのものであることが保証され、上記のシナリオは解決されます。

この機能は、リモート リーフ スイッチを除外するオプションもサポートしています。このオプションを有効にすると、PIM が有効になっている L3Outs を持つリモート リーフ スイッチは、ストライプ ウィナーの選択から除外されます。

構成ベースのストライプ ウィナー選定のガイドラインと要件：

- この構成が存在すると、POD 内の BL のみがストライプウィナー選択の対象と見なされます。存在しなければ、すべての POD からのすべての BL が考慮されます。
- POD 内の BL のうち、1 つの BL のみが構成ベースのストライプ ウィナーとして選択されます。
- **RL 除外オプション** を選択すると、RL は構成ストライプ ウィナーの選択から除外されます。
- POD 内のすべての BL は、ストライプと通常のストライプ ウィナーの候補と見なされ、（POD 内の）1 つの BL がストライプウィナーとして選択されます。
- 構成された POD に BL がない場合、またはどの BL も構成ストライプ ウィナー選択の候補でない場合、選択方式はデフォルトのストライプ ウィナー選択ロジックに切り替わり、すべての POD のすべての BL が候補と見なされます。
- VRF の削除操作と再追加操作を実行するときには、ストライプ ウィナーの構成を VRF 構成に追加し直さないでください。
- 最初に VRF 構成を追加し、その 4 分後にストライプ ウィナー構成を追加する必要があります。
- 構成ストライプウィナーが存在すると、構成された（S,G）ストライプウィナーと、（*,G）ストライプ ウィナーとが、異なるボーダー リーフになる可能性があります。この場合、（*,G）ストライプ ウィナーである BL が、（S,G）mroute もインストールします。構成された（S,G）ストライプウィナーと（*,G）ストライプウィナーの両方が外部ソースからマルチキャスト トラフィックを受信しますが、構成された（S,G）ストライプウィナーだけがマルチキャストをファブリックに転送します。
- アドレス範囲の重複はサポートされていません。たとえば、`224.1.0/16` がすでに設定されている場合、`224.1.0/24` を設定することはできません。ただし、`224.1.0/16` で、異なる送信元範囲を持つ任意の数の構成を使用することはできます。
- 構成ストライプ ウィナー ポリシーは、IPv6 マルチキャストではサポートされていません。
- 構成できる範囲の最大数は、VRF あたり 500 です。
- ストライプ ウィナー ポリシーの構成は、ACI リリース 6.0(2) の VRF 間マルチキャストではサポートされていません。

ACI マルチキャスト機能のリスト

ここでは、ACI マルチキャスト機能のリストと、類似の NX-OS 機能との比較を示します。

- IGMP 機能 （85 ページ）
- IGMP スヌーピング機能 （87 ページ）
- MLD スヌーピング機能 （88 ページ）

• PIM 機能（インターフェイス レベル） （88 ページ）
• PIM 機能（VRF レベル） （90 ページ）

IGMP 機能

ACI 機能名	NX-OS 機能	説明
V3 ASM を許可	ip igmp allow-v3-asm	SSM 範囲外のマルチキャスト グループの IGMP バージョン 3 送信元固有レポートの受け入れを許可します。この機能がイネーブルの場合、グループが設定された SSM 範囲外であっても、グループと送信元の両方を含む IGMP バージョン 3 レポートを受信すると、スイッチは（S, G）mroute エントリを作成します。ホストが SSM 範囲外の（*, G）レポートを送信する場合、または SSM 範囲の（S、G）レポートを送信する場合、この機能は不要です。
Fast Leave	ip igmp immediate-leave	デバイスからグループ固有のクエリーが送信されないため、所定の IGMP インターフェイスで IGMPv2 グループ メンバーシップの脱退のための待ち時間を最小限にできるオプション。即時脱退をイネーブルにすると、デバイスではグループに関する Leave メッセージの受信後、ただちにマルチキャスト ルーティング テーブルからグループ エントリが削除されます。デフォルトではディセーブルになっています。 注意：このコマンドは、所定のグループに対する BD/インターフェイスの背後に 1 つの受信者しか存在しない場合に使用します。
レポートリンクローカルグループ	ip igmp report-link-local-groups	224.0.0.0/24 に含まれるグループに対して、レポート送信をイネーブルにします。非リンク ローカル グループには、常にレポートが送信されます。デフォルトでは、リンク ローカル グループにレポートは送信されません。
グループタイムアウト(秒)	ip igmp group-timeout	IGMPv2 のグループ メンバーシップ タイムアウトを設定します。有効範囲は 3 ～ 65,535 秒です。デフォルト値は 260 秒です。
クエリ間隔(秒)	ip igmp query-interval	IGMP ホスト クエリー メッセージの送信頻度を設定します。有効範囲は 1 ～ 18,000 秒です。デフォルト値は 125 秒です。
クエリ応答間隔(秒)	ip igmp query-max-response-time	IGMP クエリーでアドバタイズされる応答時間を設定します。有効範囲は 1 ～ 25 秒です。デフォルトは 10 秒です。
最終メンバーカウント	ip igmp last-member-query-count	ホストの Leave メッセージを受信してから、IGMP クエリーが送信される回数を設定します。有効範囲は 1 ～ 5 です。デフォルトは 2 です。
最終メンバー応答時間(秒)	ip igmp last-member-query-response-time	メンバーシップ レポートを送信してから、ソフトウェアがグループ ステートを解除するまでのクエリー インターバルを設定します。有効範囲は 1 ～ 25 秒です。デフォルト値は 1 秒です。

ACI 機能名	NX-OS 機能	説明
スタートアップクエリーの回数	ip igmp startup-query-count	ソフトウェアの起動時に使用されるクエリー数を設定します。有効範囲は 1 ～ 10 です。デフォルトは 2 です。
クエリアタイムアウト	ip igmp querier-timeout	クエリアとして処理を引き継ぐかどうかをソフトウェアが判断するための、クエリー タイムアウト値を設定します。有効範囲は 1 ～ 65,535 秒です。デフォルト値は 255 秒です。
堅牢性変数	ip igmp robustness-variable	ロバストネス変数を設定します。ネットワークのパケット損失が多い場合は、この値を大きくします。有効値の範囲は、1～7です。デフォルトは 2 です。
バージョン	ip igmp version <2-3>	ブリッジ ドメインまたはインターフェイスでイネーブルにする IGMP のバージョン。有効な IGMP バージョンは 2 または 3 です。デフォルトは 2 です。
レポート ポリシー ルート マップ*	ip igmp report-policy <route-map>	ルートマップ ポリシーに基づく、IGMP レポートのアクセス ポリシー。IGMPグループレポートは、ルートマップで許可されたグループに対してのみ選択されます
静的レポート ルート マップ*	ip igmp static-oif	マルチキャスト グループを発信インターフェイスに静的にバインドし、スイッチ ハードウェアで処理します。グループ アドレスのみを指定した場合は、（*, G）ステートが作成されます。送信元アドレスを指定した場合は、（S, G）ステートが作成されます。グループ プレフィックス、グループ範囲、および送信元プレフィックスを示すルートマップ ポリシー名を指定できます。IGMPv3 をイネーブルにした場合にのみ、（S, G）ステートに対して送信元ツリーが作成されることに注意してください。
最大マルチキャストエントリ	ip igmp state-limit	IGMP レポートによって作成される BD またはインターフェイスの mroute 状態を制限します。 デフォルトは無効で、制限はありません。有効な範囲は1～4294967295です。
予約済みマルチキャストエントリ	ip igmp state-limit <limit> reserved <route-map>	予約ポリシーにルート マップ ポリシー名を使用するように指定し、インターフェイスで許可される（*, G）および（S, G）エントリの最大数を設定します。
ステート制限ルート マップ*	ip igmp state-limit <limit> reserved <route-map>	予約済みマルチキャスト エントリ機能で使用

IGMP スヌーピング機能

ACI 機能名	NX-OS 機能	説明
IGMP スヌーピングの管理状態	[no] ipigmp snooping	IGMP スヌーピング機能を有効または無効にします。PIM 対応ブリッジ ドメインでは無効にできません
Fast Leave	ip igmp snooping fast-leave	デバイスからグループ固有のクエリーが送信されないため、所定の IGMP インターフェイスで IGMPv2 グループ メンバーシップの脱退のための待ち時間を最小限にできるオプション。即時脱退をイネーブルにすると、デバイスではグループに関する Leave メッセージの受信後、ただちにマルチキャスト ルーティング テーブルからグループ エントリが削除されます。デフォルトではディセーブルになっています。 注意：このコマンドは、所定のグループに対する BD/インターフェイスの背後に 1 つの受信者しか存在しない場合に使用します。
クエリアの有効化	ip igmp snooping querier <ip address>	ブリッジ ドメインで IP IGMP スヌーピング クエリア機能をイネーブルにします。BD サブネット クエリア IP 設定とともに使用して、ブリッジ ドメインの IGMP スヌーピング クエリアを設定します。 注意：PIM 対応ブリッジ ドメインでは使用しないでください。ブリッジ ドメインで PIM が有効になっている場合、IGMP クエリア機能は自動的に有効になります。
クエリ間隔	ip igmp snooping query-interval	IGMP ホスト クエリー メッセージの送信頻度を設定します。有効範囲は 1 ～ 18,000 秒です。デフォルト値は 125 秒です。
クエリ応答間隔	ip igmp snooping query-max-response-time	IGMP クエリーでアドバタイズされる応答時間を設定します。有効範囲は 1 ～ 25 秒です。デフォルトは 10 秒です。
最終メンバークエリ間隔	ip igmp snooping last-member-query-interval	メンバーシップ レポートを送信してから、ソフトウェアがグループ ステートを解除するまでのクエリー インターバルを設定します。有効範囲は 1 ～ 25 秒です。デフォルト値は 1 秒です。
開始クエリ数	ip igmp snooping startup-query-count	マルチキャスト トラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、起動時に送信されるクエリー数に対してスヌーピングを設定します。有効範囲は 1 ～ 10 です。デフォルトは 2 です。
開始クエリ間隔（秒）	ip igmp snooping startup-query-interval	マルチキャスト トラフィックをルーティングする必要がないため、PIM をイネーブルにしていない場合に、起動時のスヌーピング クエリー インターバルを設定します。有効範囲は 1 ～ 18,000 秒です。デフォルト値は 31 秒です。

MLD スヌーピング機能

ACI 機能名	NX-OS 機能	説明
MLD スヌーピング管理状態	ipv6 mld snooping	IPv6 MLD スヌーピング機能。デフォルトは無効
Fast Leave	ipv6 mld snooping fast-leave	ブリッジ ドメインごとに高速脱退機能をオンまたはオフにできます。これは MLDv2 ホストに適用され、1 つのホストだけがそのポートの背後で MLD を実行することがわかっているポートで使用されます。このコマンドはデフォルトでは無効になっています。
クエリアの有効化	ipv6 mld snooping querier	IPv6 MLD スヌーピング クエリア処理を有効または無効にします。MLD スヌーピング クエリアは、マルチキャスト トラフィックをルーティングする必要がないため、PIM および MLD を設定していないブリッジ ドメイン内で MLD スヌーピングをサポートします。
クエリ間隔	ipv6 mld snooping query-interval	MLD ホスト クエリー メッセージの送信頻度を設定します。有効範囲は 1 ～ 18,000 秒です。デフォルト値は 125 秒です。
クエリ応答間隔	ipv6 mld snooping query-interval	MLD クエリーでアドバタイズされる応答時間を設定します。有効範囲は 1 ～ 25 秒です。デフォルトは 10 秒です。
最終メンバークエリ間隔	ipv6 mld snooping last-member-query-interval	メンバーシップ レポートを送信してから、ソフトウェアがグループ ステートを解除するまでのクエリー応答時間を設定します。有効範囲は 1 ～ 25 秒です。デフォルト値は 1 秒です。

PIM 機能（インターフェイス レベル）

ACI 機能名	NX-OS 機能	説明
認証	ip pim hello-authentication ah-md5	PIM IPv4 ネイバーの MD5 ハッシュ認証をイネーブルにします。
マルチキャスト ドメイン境界	ip pim border	インターフェイスを PIM ドメインの境界として設定し、対象のインターフェイスで、ブートストラップ、候補 RP、または Auto-RP の各メッセージが送受信されないようにします。デフォルトではディセーブルになっています。
パッシブ	ip pim passive	パッシブ設定がインターフェイスで設定されている場合、IP マルチキャストのインターフェイスが有効になります。PIM は、passive モードのインターフェイスで動作します。これは、リーフがインターフェイス上で PIM メッセージを送信せず、このインターフェイス全体にわたる他のデバイスからの PIM メッセージも受け入れないことを意味します。リーフは、ネットワーク上の唯一の PIM デバイスであると見なし、DR として機能します。IGMP の動作は、このコマンドの影響を受けません。

ACI 機能名	NX-OS 機能	説明
厳格な RFC 準拠	ip pim strict-rfc-compliant	設定すると、スイッチは不明なネイバーからの参加を処理せず、不明なネイバーに PIM 参加を送信しません。
指定ルータの遅延（秒）	ip pimdr-delay	PIM hello メッセージでアドバタイズされる DR プライオリティを指定期間にわたり 0 に設定することで、指定ルータ（DR）の選定への参加を遅延させます。この遅延中、DR は変更されず、現在のスイッチにはそのインターフェイスでのすべてのマルチキャストの状態を把握する時間が与えられます。遅延期間が終了すると、DR 選出を再び開始するために、正しい DR プライオリティが hello パケットで送信されます。値は 1 ー 65,535 です。デフォルト値は 3 です。 注意：このコマンドは、起動時にのみ、または IP アドレスかインターフェイスの状態が変更された後にのみ、DR 選定に参加することを遅延させます。これは、マルチキャスト アクセスの非 vPC レイヤ 3 インターフェイス専用です。
指定ルータの優先順位	ip pim dr-priority	PIM hello メッセージの一部としてアドバタイズされる指定ルータ（DR）プライオリティを設定します。有効範囲は 1 ～ 4294967295 です。デフォルトは 1 です。
Hello間隔(ミリ秒)	ip pim hello-interval	hello メッセージの送信インターバルを、ミリ秒単位で設定します。範囲は 1000 ～ 18724286 です。デフォルト値は 30000 です。
Join-Prune 間隔ポリシー（秒）	ip pim jp-interval	PIM Join および Prune メッセージを送信する間隔（秒単位）。有効な範囲は 60 ～ 65520 です。値は 60 で割り切れる必要があります。デフォルト値は 60 です。
インターフェイス レベルのインバウンド Join-Prune フィルタ ポリシー*	ip pimjp-policy	ルートマップ ポリシーに基づく、インバウンド Join/Prune メッセージのフィルタリングをイネーブルにします。ここで、グループ、グループおよび送信元、および RP アドレスを指定できます。デフォルトでは、Join/Prune メッセージはフィルタリングされません。
インターフェイスレベルのアウトバウンド Join-Prune フィルタ ポリシー*	ip pim jp-policy	ルートマップ ポリシーに基づく、アウトバウンド Join/Prune メッセージのフィルタリングをイネーブルにします。ここで、グループ、グループおよび送信元、および RP アドレスを指定できます。デフォルトでは、Join/Prune メッセージはフィルタリングされません。
インターフェイス レベルのネイバーフィルタ ポリシー*	ip pim neighbor-policy	許可される PIM ネイバーの送信元アドレス/アドレス範囲を指定するルート マップ ポリシーに基づいて、隣接する PIM ネイバーを制御します。

PIM 機能（VRF レベル）

ACI 機能名	NX-OS 機能	説明
スタティック RP	ip pim rp-address	マルチキャスト グループ範囲に、PIM スタティック RP アドレスを設定します。スタティック RP のマルチキャスト グループ範囲をリストするオプションのルートマップ ポリシーを指定できます。ルートマップが設定されていない場合、スタティック RP は、設定された SSM グループ範囲を除くすべてのマルチキャスト グループ範囲に適用されます。 モードは ASM です。
ファブリック RP	該当なし	ファブリック内のすべてのマルチキャスト対応境界リーフ スイッチでエニーキャスト RP を設定します。エニーキャスト RP は、PIM エニーキャスト RP を使用して実装されます。スタティック RP のマルチキャスト グループ範囲をリストするオプションのルートマップ ポリシーを指定できます。
Auto-RP Forward Auto-RP Updates	ip pim auto-rp forward	Auto-RP メッセージの転送をイネーブルにします。デフォルトではディセーブルになっています。
Auto-RP Listen to Auto-RP Updates	ip pim auto-rp listen	Auto-RP メッセージのリッスンをイネーブルにします。デフォルトではディセーブルになっています。
Auto-RP MA Filter *	ip pim auto-rp mapping-agent-policy	ルートマップ ポリシーに基づく境界リーフによって Auto-RP Discovery メッセージのフィルタリングをイネーブルにします。ここで、マッピング エージェント送信元アドレスを指定できます。この機能は、境界リーフが Auto-RP メッセージをリッスンするように設定されている場合に使用されます。デフォルトでは、Auto-RP メッセージはフィルタリングされません。
BSR Forward BSR Updates	ip pim bsr forward	BSR メッセージの転送をイネーブルにします。デフォルトではディセーブルになっているため、リーフは BSR メッセージの転送を行いません。
BSR Listen to BRS Updates	ip pim bsr listen	BSR メッセージのリッスンをイネーブルにします。デフォルトではディセーブルになっているため、リーフは BSR メッセージのリッスンを行いません。
BSR Filter	ip pim bsr bsr-policy	ルートマップ ポリシーに基づく境界リーフによって BSR メッセージのフィルタリングをイネーブルにします。ここで、BSR 送信元を指定できます。このコマンドは、境界リーフが BSR メッセージをリッスンするように設定されている場合に使用できます。デフォルトでは、BSR メッセージはフィルタリングされません。
ASM ソース、グループ有効期限タイマー ポリシー*	ip pim sg-expiry-timer <timer> sg-list	調整された有効期限タイマーのグループ/グループを指定するために、ASM ソース、グループ有効期限タイマーにルート マップを適用します。

ACI 機能名	NX-OS 機能	説明
ASM Source, Group Expiry Timer Expiry (sec)	ip pim sg-expiry-timer	プロトコル独立マルチキャスト スパース モード（PIM-SM）（S, G）マルチキャスト ルートの（S, G）期限切れタイマーの間隔を調節します。このコマンドは、断続的な送信元に対してデフォルトの 180 秒を超える SPT（送信元ベースのツリー）の永続性を作成します。指定できる範囲は 1 ～ 604801 秒です。
Register Traffic Policy: Max Rate	ip pim register-rate-limit	レート制限を毎秒のパケット数で設定します。指定できる範囲は 1 ～ 65,535 です。デフォルト設定は無制限です。
Register Traffic Policy: Source IP	ip pim register-source	登録メッセージの送信元 IP アドレスを設定するために使用されます。この機能は、RP がメッセージを送信できるネットワークで登録メッセージの送信元アドレスがルーティングされる場合に使用できます。これは、送信元が接続されているブリッジ ドメインが、ファブリックの外部にサブネットをアドバタイズするように設定されていない場合に発生することがあります。
SSM グループ範囲ポリシー*	ip pim ssm route-map	デフォルトの範囲 232.0.0.0/8 以外の異なる SSM グループ範囲を指定するために使用できます。デフォルトのグループ範囲のみを使用する場合は、このコマンドは不要です。デフォルト範囲を含め、SSM マルチキャストに最大 4 つの範囲を設定できます。
	ip pim ssm-range none	デフォルト SSM グループ範囲 232.0.0.0/8 を拒否するために使用できます。代わりに、この範囲を ASM グループ範囲として処理できます。これは、ルート マップ エントリのない（空のルート マップ）SSM グループ範囲ポリシーを作成することによっても実現できます。
短時間でのコンバージェンス	該当なし	高速コンバージェンス モードが有効になっている場合、ファブリック内のすべての境界リーフは、外部ネットワークのルート（（*, G）および送信元（S, G）の RP）に向けて PIM Join を送信します。これにより、ファブリック内のすべての PIM 対応 BL が外部ソースからマルチキャスト トラフィックを受信できますが、1 つの BL のみがトラフィックをファブリックに転送します。マルチキャスト トラフィックをファブリックに転送する BL が指定フォワーダです。グループのストライプ優先は、DF を決定します。高速コンバージェンス モードの利点は、BL の障害によりストライプの優先が変更された場合、新しい BL が join を送信してマルチキャスト状態を作成することで、外部ネットワークで遅延が発生しないことです。 注意：追加の帯域幅のコストが保存コンバージェンス時間を上回る場合、高速コンバージェンス モードを導入時に無効にできることに注意してください。
厳格な RFC 準拠	ip pim strict-rfc-compliant	設定すると、スイッチは不明なネイバーからの参加を処理せず、不明なネイバーに PIM 参加を送信しません。

ACI 機能名	NX-OS 機能	説明
MTU ポート	ip pim mtu	PIM コントロール プレーン トラフィックのフレーム サイズを大きくし、コンバージェンスを向上させます。範囲は 1500 ー 9216 バイトです。
リソースポリシーの上限	ip pim state-limit	VRF ごとに許可される最大 (*, G)/(S, G) エントリを設定します。範囲は 1 ～ 4294967295 です。
リソースポリシー予約済みルート マップ*	ip pim state-limit <limit> reserved <route-map>	リソース ポリシーの最大制限の予約済みエントリに適用されるマルチキャスト グループまたはグループと送信元を照合するルートマップ ポリシーを設定します。
Resource Policy Reserved Multicast Entries	ip pim state-limit <limit> reserved <route-map> <limit>	この VRF で許可される最大予約済み（*, G）および（S, G）エントリです。最大許可ステート数以下である必要があります。リソース ポリシーの予約済みルート マップ ポリシーで使用されます。

レイヤ3IPv4/IPv6マルチキャストの設定のガイドライン、制約事項、および予想される動作

次のガイドラインと制限を確認します。

- IPv4/IPv6 マルチキャストのガイドラインと制約事項 （92 ページ）
- IPv4 マルチキャストのガイドラインと制約事項 （94 ページ）
- IPv6 マルチキャストのガイドラインと制約事項 （95 ページ）

IPv4/IPv6 マルチキャストのガイドラインと制約事項

IPv4 マルチキャストと IPv6 マルチキャストの両方に次の制限が適用されます。

- 第 2 世代リーフスイッチでレイヤ 3 IPv4/IPv6 マルチキャスト機能がサポートされています。第 2 世代スイッチは、製品 ID に -EX、-FX、-FX2、-FX3、-GX、またはそれ以降のサフィックスが付いたスイッチです。
- カスタム QoS ポリシーは、Cisco Application Centric Infrastructure（ACI）ファブリックの外部から送信された（L3Out から受信した）レイヤ 3 マルチキャスト トラフィックではサポートされません。
- ブリッジドメインでの PIMv4/PIM6 およびアドバタイズ ホスト ルートの有効化がサポートされています。
- レイヤ 3 マルチキャストは VRF レベルで有効になり、マルチキャスト プロトコルは VRF インスタンス内で機能します。各 VRF インスタンスでは、マルチキャストを個別に有効化または無効化できます。

- マルチキャストで VRF インスタンスが有効になると、有効になった VRF インスタンスの個別のブリッジドメインと L3Out を有効にしてマルチキャストを構成できます。デフォルトでは、マルチキャストはすべてのブリッジ ドメインと L3Out で無効になっています。
- 双方向 PIMv4/PIM6 は現在サポートされていません。
- マルチキャスト ルータは、パーペイシブ ブリッジ ドメインではサポートされていません。
- サポートされるルートスケールは 2,000 です。マルチキャスト スケール番号は、IPv4 と IPv6 の両方を含む複合スケールです。合計ルート制限は、ルート カウントとして定義されます。各 IPv4 ルートは 1 としてカウントされ、各 IPv6 ルートは 4 としてカウントされます。より多くのマルチキャスト スケールをサポートするノードプロファイルでも、IPv6 ルート スケールは 2,000 のままです。
- PIMv4/PIM6 は、レイヤ 3 ポートチャネル インターフェイスおよび SVI インターフェイスを含む、レイヤ 3 Out ルーテッドインターフェイスおよびルーテッド サブインターフェイスでサポートされます。
- L3Out で PIMv4/PIM6 を有効にすると、暗黙的な外部ネットワークが設定されます。このアクションの結果、L3Out が導入され、外部ネットワークを定義していない場合でもプロトコルが発生する可能性があります。
- マルチキャスト送信元が孤立ポートとしてリーフA に接続され、リーフB に L3Out があり、リーフA とリーフB が vPC ペアにある場合、マルチキャスト送信元に関連付けられた EPG カプセル化 VLAN はリーフB に展開されます。
- ブリッジ ドメインに接続されている送信元からパケットを受信する入力リーフ スイッチの動作は、レイヤ 3 IPv4 または IPv6 マルチキャスト サポートによって異なります。
  - レイヤ 3 IPv4 マルチキャスト サポートは、IPv4 マルチキャスト ルーティングのために有効になっているブリッジドメインに接続された送信元からのパケットを入力リーフスイッチが受信した場合、その入力リーフスイッチは、ルーテッド VRF インスタンスのコピーのみをファブリックに送信します（ルーテッドは、TTL が 1 ずつ減少し、送信元 MAC がパーベイシブ サブネット MAC で書き換えられることを意味します）。また、出力リーフ スイッチも、関連するすべてのブリッジ ドメイン内の受信者へパケットをルーティングします。そのため、受信者のブリッジ ドメインが送信元と同じで、リーフ スイッチが送信元とは異なる場合、その受信者は同じブリッジ ドメイン内ですが、ルーティングされたコピーを受け取り続けます。これは、送信元と受信者が同じブリッジ ドメインおよび同じリーフ スイッチ上にあり、このブリッジ ドメインで PIM が有効になっている場合にも適用されます。

    詳細については、次のリンク ポッドの追加 で、既存のレイヤ 2 設計を活用するマルチポッドをサポートする、レイヤ 3 マルチキャストに関する詳細情報を参照してください。

  - レイヤ 3 IPv6 マルチキャスト サポートは、IPv6 マルチキャスト ルーティングのために有効になっているブリッジドメインに接続された送信元からのパケットを入力リーフスイッチが受信した場合、その入力リーフスイッチは、ルーテッド VRF インスタンスのコピーのみをファブリックに送信します（ルーテッドは、TTL が 1 ずつ減少し、送信元 MAC がパーベイシブ サブネット MAC で書き換えられることを意味しま

す）。また、出力リーフスイッチも、受信者へパケットをルーティングします。出力リーフは、パケット内の TTL を 1 だけ減らします。これにより、TTL が 2 回減少します。また、ASM の場合、マルチキャスト グループに有効な RP が設定されている必要があります。

- VRF 間マルチキャスト通信ではフィルタを使用できません。

（注） Cisco ACI は IP フラグメンテーションをサポートしていません。したがって、外部ルータへのレイヤ 3 Outside（L3Out）接続、または Inter-Pod Network（IPN）を介したマルチポッド接続を設定する場合は、インターフェイス MTU がリンクの両端で適切に設定されていることが推奨されます。Cisco ACI、 Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定可能な MTU 値はイーサネット ヘッダー (一致する IP MTU、14-18 イーサネット ヘッダー サイズを除く) を考慮していません。また、IOS XR などの他のプラットフォームには、設定された MTU 値にイーサネット ヘッダーが含まれています。設定された値が 9000 の場合、Cisco ACI、Cisco NX-OS Cisco IOS の最大 IP パケット サイズは 9000 バイトになりますが、IOS-XR のタグなしインターフェイスの最大 IP パケットサイズは 8986 バイトになります。

各プラットフォームの適切な MTU 値については、それぞれの設定ガイドを参照してください。

CLI ベースのコマンドを使用して MTU をテストすることを強く推奨します。たとえば、Cisco NX-OS CLI で `ping 1.1.1.1 df-bit packet-size 9000 source-interface ethernet 1/1` などのコマンドを使用します。

IPv4 マルチキャストのガイドラインと制約事項

IPv4 マルチキャストには、特に次の制限が適用されます。

- Cisco ACI ファブリックの境界リーフスイッチがマルチキャストを実行しており、L3Out でマルチキャストを無効にしているときにユニキャスト到達可能性がある場合、外部ピアが Cisco Nexus 9000 スイッチの場合、トラフィック損失が発生します。これは、トラフィックがファブリックに送信される場合（送信元はファブリックの外部にあり、受信者はファブリックの内部にある場合）、またはファブリックを通過する場合（送信元と受信者がファブリックの外部にあり、ファブリックが送信中の場合）に影響します。
- Any Source Multicast (ASM) と Source-Specific Multicast (SSM) は IPv4 向けにサポートされています。
- VRF インスタンスごとにルートマップで SSM マルチキャストの範囲を最大 4 つ構成できます。
- IGMP スヌーピングは、マルチキャスト ルーティングが有効になっているパーペイシブ ブリッジ ドメインでは無効にできません。
- FEX ではレイヤ 3 マルチキャストはサポートされていません。FEX ポートに接続されているマルチキャストの送信元または受信先がサポートされています。テスト環境で FEX を追加する方法についての詳細は、次の URL の『アプリケーション セントリック インフラストラクチャとファブリック エクステンダの構成』を参照してください：

https://www.cisco.com/c/en/us/support/docs/cloud-systems-management/application-policy-infrastructure-controller-apic/200529-Configure-a-Fabric-Extender-with-Applica.html。FEX ポートに接続されているマルチキャストの送信元または受信先はサポートされていません。

IPv6 マルチキャストのガイドラインと制約事項

IPv6 マルチキャストには、特に次の制限が適用されます。

- Source Specific Multicast（SSM）はサポートされていますが、RFC 3306-Unicast-Prefix-based IPv6 Multicast Addresses で固定 SSM 範囲が指定されています。したがって、SSM の範囲は IPv6 では変更できません。
- VRF インスタンスごとにルートマップで SSM マルチキャストの範囲を最大 4 つ構成できます。
- Any Source Multicast（ASM）は IPv6 でサポートされます。
- IPv6 の OIF および VRF スケール番号は、IPv4 の場合と同じです。
- スタティック RP 設定のみの PIM6 をサポートしています。Auto-RP および BSR は PIM6 ではサポートされません。
- ファブリック内のレシーバはサポートされません。IPv6 マルチキャストを有効にする場合は、MLD スヌープ ポリシーを無効にする必要があります。MLD スヌーピングと PIM6 を同じ VRF インスタンスで有効にすることはできません。
- 現在、レイヤ 3 マルチキャストリスナー検出（MLD）は Cisco ACI ではサポートされていません。
- ファブリック ランデブー ポイント（RP）は、IPv6 マルチキャストではサポートされません。
- Cisco Multi-Site Orchestrator のサポートは利用できません。

GUI を使用したレイヤ 3 マルチキャストの設定

このセクションでは、Cisco APIC GUI を使用してレイヤ 3 マルチキャストを設定する方法について説明します。

（注） [Work] ペインおよび各ダイアログボックスの右上隅にあるヘルプ アイコン（**?**）をクリックすると、表示されているタブまたはフィールドについての情報が表示されます。

始める前に

- 目的の VRF、ブリッジ ドメイン、IP アドレスを持つレイヤ 3 Out インターフェイス は、PIM および IGMP が有効になるように設定する必要があります。
- 基本的なユニキャスト ネットワークを設定する必要があります。

手順

ステップ 1 **[テナント（Tenants）** > **[*Tenant_name*]** > **[ネットワーキング（Networking）]** > **[VRFs]** > **[*VRF_name*]** > **[マルチキャスト（Multicast）]** に移動します。
[Work] ペインに、**PIM is not enabled on this VRF. Would you like to enable PIM?** というメッセージが表示されます。

ステップ 2 **YES, ENABLE MULTICAST** をクリックします。

ステップ 3 インターフェイスを設定します。

a) [Work] ペインから、[Interfaces] タブをクリックします。
b) [Bridge Domains] テーブルを展開して [Create Bridge Domain] ダイアログを表示し、各フィールドに適切な値を入力します。
c) **Select** をクリックします。
d) [Interfaces] テーブルを展開し、[Select an L3 Out] ダイアログを表示します。
e) [L3 Out] ドロップダウン矢印をクリックして L3 Out を選択します。
f) **Select** をクリックします。

ステップ 4 ランデブー ポイント（RP） を設定します。

a) [Work] ペインで [Rendezvous Points] タブをクリックし、次のランデブー ポイント（RP） オプションから選択します。

- **スタティック RP**
  1. [Static RP] テーブルを展開します。
  2. 各フィールドに適切な値を入力します。
  3. [Update] をクリックします。
- **ファブリック RP**
  1. [Fabric RP] テーブルを展開します。
  2. 各フィールドに適切な値を入力します。
  3. [Update] をクリックします。
- **Auto-RP**
  1. 各フィールドに適切な値を入力します。
- **ブートストラップ ルータ（BSR）**

1. 各フィールドに適切な値を入力します。

ステップ 5 パターン ポリシーを設定します。

a) [Work] ペインで [Pattern Policy] タブをクリックし、[Any Source Multicast (ASM)] または [Source Specific Multicast (SSM)] オプションを選択します。

b) 各フィールドに適切な値を入力します。

ステップ 6 PIM を設定します。

a) [PIM Setting] タブをクリックします。

b) 各フィールドに適切な値を入力します。

ステップ 7 IGMP 設定を行います。

a) **IGMP Setting** タブをクリックします。

b) [IGMP Context SSM Translate Policy] テーブルを展開します。

c) 各フィールドに適切な値を入力します。

d) [Update] をクリックします。

ステップ 8 Inter-VRF マルチキャストを設定します。

a) [Work] ペインの [Inter-VRF Multicast] タブをクリックします。

b) [Inter-VRF Multicast] テーブルを展開します。

c) 各フィールドに適切な値を入力します。

d) [Update] をクリックします。

ステップ 9 構成ストライプ ウィナー ポリシーを構成します。

a) **[作業（Work）]** ペインで、**[構成ストライプ ウィナー（Config Stripe Winner）]** タブをクリックします。

b) 送信元アドレス/アドレス範囲を指定します。

c) マルチキャスト グループ範囲のプレフィックスを指定します。プレフィックス長は */32* ～ */4* です。すべてのマルチキャスト グループに **224.0.0.0/4** と入力します。

d) ストライプ ウィナーを選出する必要がある POD のPod ID を選択します。

e) リモート リーフ スイッチを除外するには、[リモート リーフを除外（Exclude Remote Leaf）] オプションを選択します。

ステップ 10 完了したら、[送信（Submit）] をクリックします。

ステップ 11 メニューバーで、**[テナント（Tenants）]** > **[** ***Tenant_name*****]** > **[ネットワーキング（Networking）]** > **[VRFs]** > **[** ***VRF_name*****]** > **[マルチキャスト（Multicast）]**に移動し、次の操作を実行します。

a) [**作業（Work**）] ペインの [**インターフェイス（Interfaces**）] タブで、適切な L3 Out を選択し、[**PIM ポリシー（PIM Policy**）] ドロップダウンリストから、接続する適切な PIM ポリシーを選択します。

b) **[送信（Submit）]** をクリックします。`

ステップ 12 設定を確認するには次のアクションを実行します:

a) **Work** ウィンドウで、**Interfaces** をクリックして、関連付けられた **Bridge Domains** を表示します。

b) **Interfaces** をクリックして、関連付けられた **L3 Out** インターフェイスを表示します。
c) **Navigation** ウィンドウで、**BD** に移動します。
d) **Work** ウィンドウに、設定された IGMP ポリシーと PIM の機能が、先ほど設定されたように表示されます。
e) **Navigation** ウィンドウに、L3 Out インターフェイスが表示されます。
f) **Work** ウィンドウに、PIM の機能が先ほど設定されたように表示されます。
g) **Work** ウィンドウで、**Fabric** > **Inventory** > **Protocols** > **IGMP** に移動して、設定した IGMP インターフェイスの動作状態を表示します。
h) [作業（**Work**）] ウィンドウで、[**ファブリック（Fabric**）] > [**インベントリ（Inventory**）] > **[ポッド名（*Pod name*）] > [*Leaf_Node*]** > [**プロトコル（Protocols**）] > [**IGMP**] > [**IGMP ドメイン（IGMP Domains**）] に移動して、マルチキャストが有効化/無効化されたノードのドメイン情報を表示します。

GUI を使用したレイヤ 3 IPv6 マルチキャストの設定

始める前に

- 目的の VRF、ブリッジ ドメイン、IPv6 アドレスを持つレイヤ 3 Out インターフェイスは、PIM6 が有効になるように設定する必要があります。レイヤ 3 Out の場合、IPv6 マルチキャストが機能するために、論理ノード プロファイルのノードに IPv6 ループバック アドレスが設定されます。
- 基本的なユニキャスト ネットワークを設定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**） > **[*Tenant_name*]** > **[ネットワーキング（Networking**）] > **[VRFs]** > **[*VRF_name*]** > **[マルチキャスト IPv6（Multicast IPv6**）] に移動します。
[作業（**Work**） ペインで次のメッセージが表示されます。**PIM6 はこの VRF で有効化されていません。（PIM6 is not enabled on this VRF.）PIM6 を有効化しますか？（Would you like to enable PIM6 ?**）

ステップ 2 [**はい、マルチキャスト IPv6 を有効化します。（YES, ENABLE MULTICAST IPv6**）] をクリックします。

ステップ 3 インターフェイスを設定します。
a) [Work] ペインから、[Interfaces] タブをクリックします。
b) [**ブリッジ ドメイン（Bridge Domains**）] テーブルを展開して [**ブリッジ ドメインの作成（Create Bridge Domain**）] ダイアログを表示し、ドロップダウン リストから適切な BD を選択します。
c) [選択（Select）] をクリックします。

d) [**インターフェイス（Interfaces**）] テーブルを展開し、[**L3Out の選択（Select an L3 Out**）] ダイアログ ボックスを表示します。
e) [L3 Out] ドロップダウン矢印をクリックして L3 Out を選択します。
f) **Select** をクリックします。

ステップ 4 ランデブー ポイント（RP） を設定します。

a) [作業（Work）] ペインで [ランデブー ポイント（Rendezvous Points）] タブをクリックし、[スタティック RP（Static RP）] を選択します。
b) 各フィールドに適切な値を入力します。
c) [Update] をクリックします。

ステップ 5 パターン ポリシーを設定します。

a) [**作業（Work**）] ペインで [**パターン ポリシー（Pattern Policy**）] タブをクリックし、[**任意の送信元マルチキャスト（ASM）（Any Source Multicast（ASM**））] を選択します。
b) 各フィールドに適切な値を入力します。

ステップ 6 PIM を設定します。

a) [PIM Setting] タブをクリックします。
b) 各フィールドに適切な値を入力します。

ステップ 7 完了したら、[送信（Submit）] をクリックします。

ステップ 8 メニューバーで、**[テナント（Tenants）]** > **[** ***Tenant_name*****]** > **[ネットワーキング（Networking）]** > **[VRFs]** > **[** ***VRF_name*****]** > **[マルチキャスト IPv6（Multicast IPv6）]**に移動し、次の操作を実行します。

a) [**作業（Work**）] ペインの [**インターフェイス（Interfaces**）] タブで、適切な [**L3 Out**] を選択し、[**PIM ポリシー（PIM Policy**）] ドロップダウン リストから、接続する適切な PIM ポリシーを選択します。
b) **[送信（Submit）]** をクリックします。`

ステップ 9 設定を確認するには次のアクションを実行します:

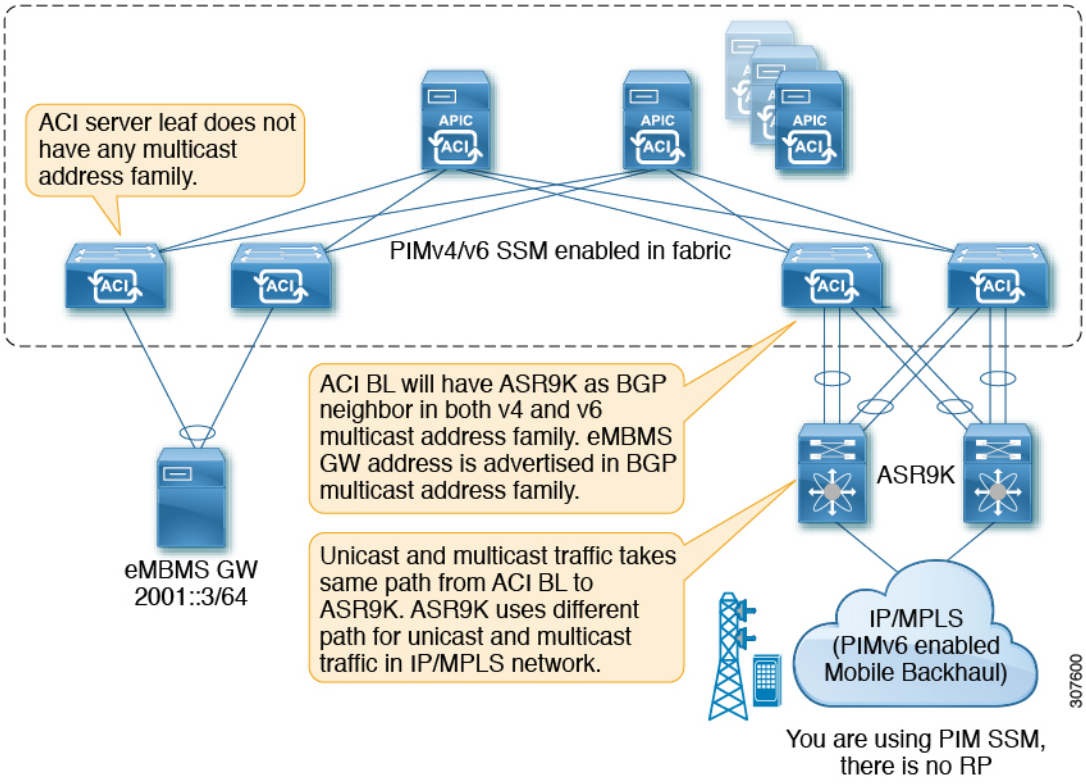
a) **Work** ウィンドウで、**Interfaces** をクリックして、関連付けられた **Bridge Domains** を表示します。
b) [ナビゲーション（Navigation）] ペインで、関連付けられている BD with IPv6 マルチキャストに移動します。
[**作業（Work**）] ウィンドウに、PIM の機能が先ほど設定されたように表示されます。
c) [ナビゲーション（Navigation）] ペインで、関連付けられている L3 Out インターフェイスに移動します。
[**作業（Work**）] ペインで、PIM6 チェックボックスをオンにします。
d) [**作業（Work**）] ペインで、[**ファブリック（Fabric**）] > [**インベントリ（Inventory**）] > [**ポッド（Pod**）] [**ノード（Node**）] [**プロトコル（Protocols**）] > [**PIM6**] の順に移動し、[PIM] を展開します。
以前に作成された適切な PIM6 プロトコルで、関連付けられているネイバー、PIM インターフェイス、ルート、グループ範囲、および RP に関する情報を表示できます。これらすべてのオブジェクトが設定されていることを確認できます。

BGP IPv4/IPv6 マルチキャスト アドレス ファミリについて

（注） BGP IPv4/IPv6 マルチキャスト アドレス ファミリ機能の IPv4 バージョンは、Cisco APIC リリース 4.1 の一部として使用できました。

Cisco APICリリース4.2（1）以降、BGPマルチキャストアドレスファミリ機能は、ボーダーリーフスイッチ上のテナントVRFのBGPピアに対するIPv6のサポートを追加します。ピアがIPv4/IPv6 マルチキャスト アドレス ファミリでマルチキャスト ルートを伝送するために個別に使用されるかどうかを指定できます。

次の図に、この機能の実装方法を示します。



BGP IPv4/IPv6 マルチキャスト アドレス ファミリのガイドラインと制約事項

IPv6 の BGP マルチキャスト アドレス ファミリ機能のガイドラインと制約事項

- ランデブー ポイント（RP）は、Cisco ACI ファブリックの外部にある IP アドレスです。ファブリック RP は IPv6 マルチキャストではサポートされません。

- マルチキャスト送信元は Cisco ACI ファブリック内にあり、レシーバはファブリック外にあります。
- 中継 L3Out は BGPv4/v6 アドレス ファミリではサポートされません。

IPv4 と IPv6 の両方に対する BGP マルチキャスト アドレス ファミリ機能のガイドラインと制約事項

- Cisco ACI ファブリック内の BGPv4/v6マルチキャスト アドレス ファミリはサポートされません。
- ユニキャスト アドレス ファミリが使用されている場合は、RP の到達可能性が存在する必要があります。PIM Source-Specific Multicast（SSM）の場合、RP は必要ありません。

GUI を使用した BGP IPv4/IPv6 マルチキャストの設定

次の手順では、GUI を使用して BGP IPv4/IPv6 マルチキャスト アドレスファミリ機能を設定する方法について説明します。

始める前に

L3Out を設定する前に、次のような標準的な前提条件を満たします。

- テナント、ノード、ポート、AEP、機能プロファイル、レイヤ 3 ドメインを設定します。
- ファブリック内でルートを伝播させるための、BGP ルート リフレクタ ポリシーを設定します。

手順

ステップ 1 L3Out で使用する VRF を特定するか、必要に応じて VRF を作成します。

[テナント（Tenants）] > [テナント（*tenant*）] > [ネットワーキング（Networking） > [VRFs]

ステップ 2 VRF で PIMv4 または PIMv6 を有効にします。

- VRF の下で PIMv4 を有効化するには、メニュー バーで **[テナント（Tenants） > [*Tenant_name*] > [ネットワーキング（Networking）] > [VRFs] > [*VRF_name*] > [マルチキャスト（Multicast）]** に移動します。
  - メッセージ **が表示された場合、この VRF で PIM が有効になっていません。[PIM を有効化しますか？（Would you like to enable PIM？）] をクリックし、[はい、マルチキャストを有効化します（Yes, enable Multicast）] をクリックします。**
  - メインの [マルチキャスト（Multicast）] ウィンドウが表示されている場合は、[有効化（Enable）] ボックスをオンにします（オンになっていない場合）。

- VRF の下で PIMv6 を有効化するには、メニュー バーで **[テナント（Tenants）] > [*Tenant_name*] > [ネットワーキング（Networking）] > [VRFs] > [*VRF_name*] > [マルチキャスト IPv6（Multicast IPv6）]** に移動します。
  - この VRFで「PIMv6 は有効化されていません（PIMv6 is not enabled）」というメッセージが表示される場合。**[PIMv6 を有効化しますか？（Would you like to enable PIMv6？）] をクリックし、[はい、マルチキャスト IPv6 を有効化します（Yes, enable multicast IPv6）] をクリックします。**
  - メインの [マルチキャスト IPv6（Multicast IPv6）] ウィンドウが表示されている場合は、[有効化（Enable）] ボックスをオンにします（オンになっていない場合）。

ステップ 3 L3Out を作成し、L3Out の BGP を設定します。

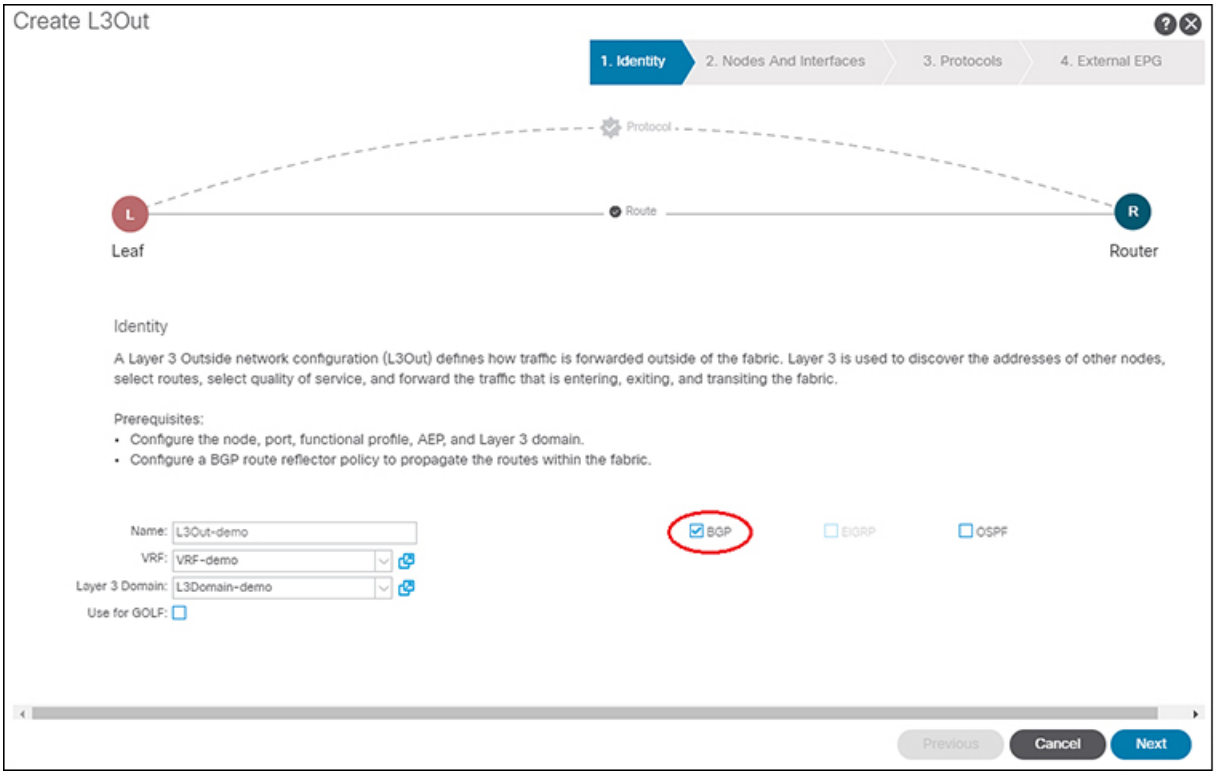
a) **[ナビゲーション（Navigation）]** ペインで **[テナント（Tenant）]** および **[ネットワーキング（Networking）]** を展開します。

b) [L3Outs] を右クリックし、[L3Out の作成（Create L3Out）] を選択します。

c) L3Out の BGP を設定するために必要な情報を入力します。

[識別（Identity）] ページ

- 前の手順で設定した VRF を選択します。
- L3Out 作成ウィザードの [識別（Identity）] ページで [BGP] を選択して、L3Out 向け BGP プロトコルの設定を行います。



d) 残りのページを続けて行い（[**ノードとインターフェイス（Nodes and Interfaces**）]、[**プロトコル（Protocols**）]、および [**外部 EPG（External EPG**）]）、L3Out の設定を完了します。

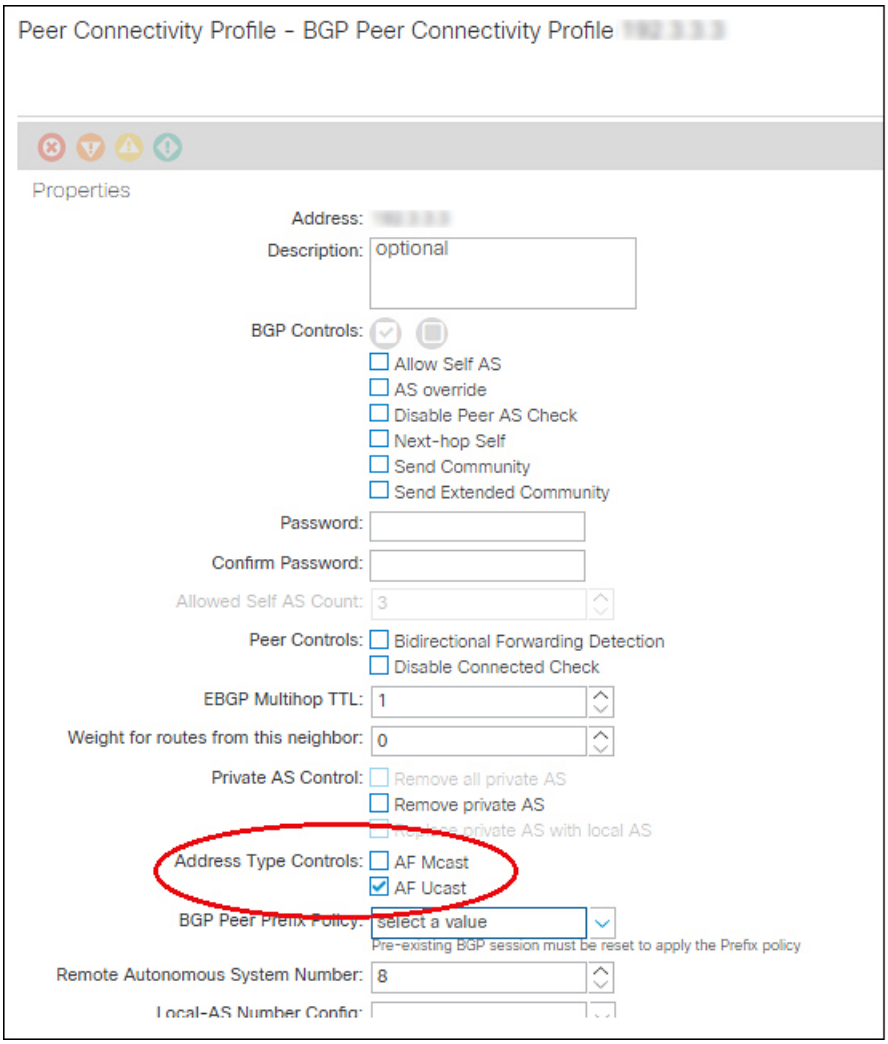
ステップ 4 L3Out の設定が完了したら、BGP IPv4/IPv6 マルチキャスト アドレス ファミリ機能を設定します。

a) BGP ピア接続プロファイル スクリーンに移動します。

[テナント（Tenants）] > [テナント（*tenant*）] > [ネットワーキング（Networking）] > [L3Outs] > [*L3out-name*] > [論理ノード プロファイル（Logical Node Profiles）] > [*logical-node-profile-name*] > [論理インターフェイス プロファイル（Logical Interface Profiles）] > [*logical-interface-profile-name*] > [BGP ピア接続プロファイル（BGP Peer Connectivity Profile） *] [IP-address*]

b) [アドレス タイプ制御（Address Type Controls）] フィールドまで下にスクロールし、次のように選択します。

- [AF Mcast] を選択します。
- [AF Ucast] が選択されている場合は、選択したままにします。



c) **[送信（Submit）]** をクリックします。`

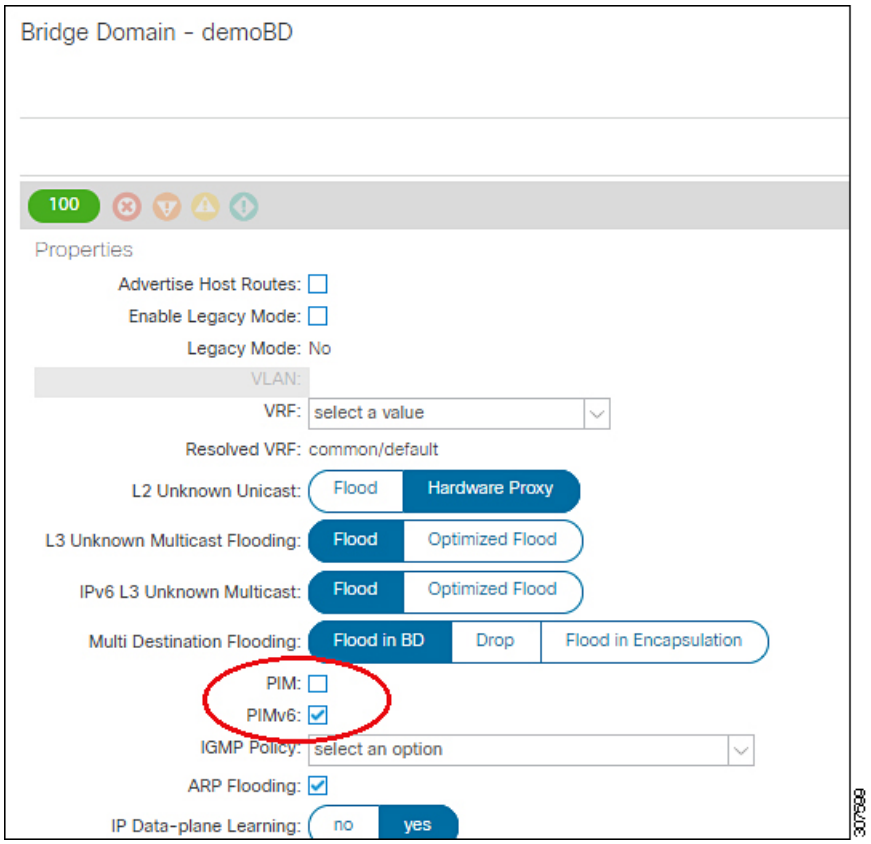
d) ピアの IPv4 または IPv6 マルチキャスト アドレス ファミリに再配布する必要があるサブネットを持つブリッジ ドメインに移動します。

[テナント（Tenants）] > [*tenant*] > [ネットワーキング（Networking）] > [ブリッジ ドメイン（Bridge Domains）] > [*bridge_domain-name*]

e) メイン ペインで、[ポリシー/全般（Policy/General）] タブをクリックします。

f) ブリッジ ドメインで PIMv4 または PIMv6 を有効にします。

- ブリッジ ドメインで PIMv4 を有効にするには、[PIM] フィールドまでスクロールし、そのフィールドの横にあるチェックボックスをオンにして有効にします。
- ブリッジ ドメインで PIMv6 を有効にするには、[PIMv6] フィールドまでスクロールし、そのフィールドの横にあるチェックボックスをオンにして有効にします。



g) [Submit] をクリックします。

マルチキャスト フィルタリングについて

ACI は、誰がマルチキャスト フィードを受信でき、どのソースから受信できるかを制御するために使用できるコントロール プレーン構成をサポートしています。フィルタリング オプションには、IGMP レポート フィルタ、PIM Join または Prune フィルタ、PIM ネイバー フィルタ、およびランデブー ポイント（RP）フィルタがあります。これらのオプションは、コントロール プレーン プロトコル（IGMP および PIM）に依存します。

一部の展開で、データプレーン レベルでマルチキャスト ストリームの送信および/または受信を制限することが望ましい場合があります。たとえば、LAN 内のマルチキャスト送信者が特定のマルチキャスト グループにのみ送信できるようにするか、受信者がすべての可能な送信元から、または特定の送信元からの特定のマルチキャスト グループを受信のみできるようにする必要がある場合があります。

Cisco APIC リリース 5.0(1) 以降では、マルチキャスト フィルタリング機能を使用できるようになりました。これにより、二方向からのマルチキャスト トラフィックをフィルタリングできます。

- マルチキャスト フィルタリングの設定：ファースト ホップ ルータでの送信元フィルタリング （106 ページ）
- マルチキャスト フィルタリングの設定：ラストホップ ルータでの送信元 フィルタリング （106 ページ）
- 同じブリッジ ドメインでの送信元と受信者の複合フィルタリング （107 ページ）

マルチキャスト フィルタリングの設定：ファースト ホップ ルータでの送信元フィルタリング

ブリッジ ドメインでトラフィックを送信している送信元について、そのブリッジ ドメインのマルチキャスト送信元フィルタを設定している場合、送信元とグループは送信元フィルタ ルートマップのエントリの1つと照合されます。そのエントリに関連付けられているアクションに応じて、アクションが実行されます。

- 送信元およびグループが、ルートマップの **許可** アクションを持つエントリと一致する場合、ブリッジ ドメインはその送信元からそのグループへのトラフィック送信を許可します。
- 送信元およびグループが、ルートマップの **拒否** アクションを持つエントリと一致する場合、ブリッジドメインはその送信元からそのグループへのトラフィック送信をブロックします。
- ルート マップ内のどのエントリとも一致しない場合、ブリッジ ドメインは、デフォルト オプションとして、その送信元からそのグループへのトラフィックの送信をブロックします。つまり、ルート マップが適用されると、最後に暗黙の「deny all（すべて拒否）」ステートメントが常に有効になります。

シングル ルート マップに複数のエントリを設定できます。ここで一部のエントリは **許可** アクションで設定、その他のエントリは **拒否** アクションで設定が可能です。すべてが同じルートマップ内で行われます。

（注） 送信元フィルタがブリッジ ドメインに適用されると、送信元でマルチキャスト トラフィックがフィルタリングされます。フィルタは、異なるブリッジドメイン内の受信先、同じブリッジドメイン内の受信先、および外部受信先がマルチキャストを受信するのを防ぎます。

マルチキャスト フィルタリングの設定：ラストホップ ルータでの送信元 フィルタリング

マルチキャスト送信元フィルタリングは、ブリッジドメイン内の受信者が特定のグループのマルチキャストを受信できる送信元を制限するために使用されます。この機能は、IGMPv3 がコントロール プレーンで提供するものと同様に、送信元またはグループのデータ プレーン フィルタリング機能を提供します。

ブリッジ ドメインで join を送信する受信者について、そのブリッジ ドメインのマルチキャスト受信者フィルタを設定している場合、送信元とグループは受信者フィルタ ルート マップのエントリの1つと照合されます。ここで、そのエントリに関連付けられているアクションに応じて、次のいずれかのアクションが実行されます。

- 送信元およびグループが、ルートマップの **許可** アクションを持つエントリと一致する場合、ブリッジドメインはその送信元からそのグループへのトラフィックの受信を許可します。
- 送信元およびグループが、ルートマップの **拒否** アクションを持つエントリと一致する場合、ブリッジドメインはその送信元からそのグループへのトラフィック受信をブロックします。
- ルート マップ内のどのエントリとも一致しない場合、ブリッジ ドメインは、デフォルト オプションとして、その送信元からそのグループへのトラフィックの受信をブロックします。つまり、ルート マップが適用されると、最後に暗黙の「deny all（すべて拒否）」ステートメントが常に有効になります。

シングル ルート マップに複数のエントリを設定できます。ここで一部のエントリは **許可** アクションで設定、その他のエントリは **拒否** アクションで設定が可能です。すべてが同じルートマップ内で行われます。

同じブリッジ ドメインでの送信元と受信者の複合フィルタリング

同じブリッジドメインでマルチキャスト送信元フィルタリングとマルチキャスト受信者フィルタリングの両方を有効にすることもできます。この場合、1つのブリッジドメインがブロッキングを実行したり、トラフィックをグループ範囲に送信する際に送信元のフィルタリングを許可したり、送信元からグループ範囲へのトラフィックを受信する場合にフィルタリングを制限したり、フィルタリングを制限したりできます。

マルチキャスト フィルタリングのガイドラインと制約事項

マルチキャストフィルタリング機能のガイドラインと制約事項は次のとおりです。

- ブリッジ ドメインでマルチキャスト送信元フィルタリングまたはレシーバ フィルタリングを有効にできますが、同じブリッジドメインでマルチキャスト送信元フィルタリングとレシーバ フィルタリングの両方を有効にすることもできます。
- マルチキャスト フィルタ処理は、IPv4 でのみサポートされています。
- ブリッジ ドメインにマルチキャスト フィルタを設定しない場合は、そのブリッジドメインで送信元フィルタまたは宛先フィルタ ルート マップを設定しないでください。デフォルトでは、ルートマップはブリッジドメインに関連付けられていません。これは、すべての送信元とグループが許可されることを意味します。送信元フィルタまたは宛先フィルタを持つルート マップがブリッジ ドメインに関連付けられている場合、そのルート マップ内の許可エントリのみが許可され、すべての拒否エントリがブロックされます（常に末尾に暗黙の「deny-all」ステートメントを含みます）。
- 空のルートマップをブリッジ ドメインに接続すると、ルートマップはデフォルトで deny all を想定するため、すべての送信元とグループがそのブリッジ ドメインでブロックされます。
- マルチキャスト フィルタリング機能は、ブリッジ ドメイン レベルで適用されます。ACI は、単一のブリッジドメインでの複数のEPGの設定をサポートします。この設定をブリッ

ジ ドメイン フィルタリング機能とともに使用すると、ブリッジ ドメイン レベルの設定であるため、フィルタはブリッジ ドメイン内のすべての EPG に適用されます。

- マルチキャスト フィルタリング機能は、任意の送信元マルチキャスト（ASM）範囲にのみ使用することを目的としています。ただし、送信元固有のマルチキャスト（SSM）範囲をサポートしている場合は、IGMPv3 を使用した SSM join itself で送信元と結合をフィルタ処理することを推奨します。

  マルチキャスト フィルタ処理機能の SSM 範囲を設定する場合は、次の制約事項が適用されます。

  - **Bridge domain source filtering with SSM**：送信元フィルタリングは SSM ではサポートされていません。
  - **Bridge domain receiver filtering with SSM**：受信者フィルタリングは SSM グループ範囲で使用できます。受信者フィルタリングの主な使用例の 1 つは、特定の送信元からのマルチキャスト ストリームをフィルタリングすることです。この機能はすでに SSM プロトコルによって提供されているため、ほとんどの場合、SSM では受信者フィルタリングは必要ありません。

- 送信元と受信者のフィルタリングでは、ルートマップエントリの順序付きリストが使用されます。ルートマップエントリは、一致するまで最も小さい番号から実行されます。一致がある場合、リスト内で最長一致ではない場合でも、プログラムは終了し、残りのエントリは考慮されません。

  たとえば、次のエントリを持つ特定の送信元（192.0.3.1/32）の次のルート マップがあるとします。

表 *9:* ルートマップ

順位	送信元 IP	アクション
1	192.0.0.0/16	許可
2	192.0.3.0/24	拒否

ルートマップは、オーダー番号に基づいて評価されます。したがって、2 番目のエントリ（192.0.3.0/24）が送信元 IP と一致する場合でも、最初のエントリ（192.0.0.0/16）は、下位の番号が原因で照合されます。

GUI を使用したマルチキャスト フィルタリングの設定

ブリッジ ドメイン レベルでマルチキャスト フィルタリングを設定します。このトピックの手順を使用して、ブリッジ ドメイン レベルで送信元フィルタリングまたは受信者フィルタリング、あるいはその両方を設定します。

始める前に

- マルチキャスト フィルタリングを設定するブリッジ ドメインはすでに作成されています。

- ブリッジ ドメインは PIM 対応ブリッジ ドメインです。
- レイヤ 3 マルチキャストは VRF レベルで有効になります。

手順

ステップ 1 マルチキャスト フィルタリングを設定するブリッジ ドメインに移動します。

[テナント（Tenant）] > [*tenant-name*] > [ネットワーキング（Networking）] > [ブリッジ ドメイン（Bridge Domains）] > [*bridge-domain-name*]

このブリッジ ドメインの [サマリ（Summary）] ページが表示されます。

ステップ 2 [**ポリシー（Policy）**] タブを選択し、[**全般（General）**] サブタブを選択します。

ステップ 3 [**全般（General）**] ウィンドウで、[**PIM**] フィールドを見つけ、PIM が有効になっていることを確認します（[**PIM**] フィールドの横にあるチェックボックスがオンになっていること）。

PIM が有効になっていない場合は、[PIM] フィールドの横にあるチェック ボックスをオンにして有効にします。[送信元フィルタ（Source Filter）] フィールドと [宛先フィルタ（Destination Filter）] フィールドが使用可能になります。

（注） マルチキャスト フィルタリングは IPv4（PIM）でのみサポートされており、現時点では IPv6（PIM6）ではサポートされていません。

ステップ 4 マルチキャスト [送信元] または [受信者] のフィルタリングを有効にするかどうかを決定します。

（注） 送信元フィルタリングと受信先フィルタリングの両方を同じブリッジ ドメインで有効にできます。

- ファーストホップ ルータでマルチキャスト [送信元] フィルタリングを有効にする場合は、[送信元フィルタ（Source Filter）] フィールドで、次のいずれかを選択します。
  - 既存のルート マップ ポリシー：送信元フィルタリングのマルチキャストの既存のルート マップ ポリシーを選択します。ステップ 7 （112 ページ）
  - 新しいルート マップ ポリシー：[マルチキャスト向けのルート マップ ポリシーの作成（Create Route Map Policy for Multicast）] を選択し、に進みます。ステップ 5 （110 ページ）
- ラストホップ ルータでマルチキャスト [受信者] フィルタリングを有効にする場合は、[宛先フィルタ（Destination Filter）] フィールドで、次のいずれかを選択します。
  - **既存のルート マップ ポリシー**：受信者フィルタリング用のマルチキャストの既存ルート マップ ポリシーを選択してステップ 7 （112 ページ）に移動します。
  - 新しいルート マップ ポリシー：[マルチキャスト向けのルート マップ ポリシーの作成（Create Route Map Policy for Multicast）] を選択し、に進みます。ステップ 6 （111 ページ）

ステップ 5 [マルチキャストのルート マップ ポリシーの作成（Create Route Map Policy for Multicast）] オプションを選択して、最初のホップルータでマルチキャスト[送信元]フィルタリングを有効にした場合は、[マルチキャストのルート マップ ポリシーの作成（Create Route Map Policy for Multicast）] ウィンドウが表示されます。このウィンドウに次の情報を入力します。

a) [名前（Name）] フィールドにこのルート マップの名前を入力し、必要に応じて [説明（Description）] フィールドに説明を入力します。

b) [ルート マップ（Route Maps）] 領域で、[+]をクリックします。

[**ロールの作成（Create a Role**）] ウィンドウが表示されます。

c) **Order** フィールドでは、このインターフェイスに対して複数のアクセス グループを設定している場合に、このインターフェイスでのマルチキャスト トラフィックへのアクセスをどの順序で許可または拒否するかを反映する番号を選択します。

小さい番号のエントリは、大きい番号のエントリの前に並べられます。範囲は 0 ～ 65535 です。

d) マルチキャスト送信元フィルタリングのためにトラフィックの送信を許可または拒否する方法を決定します。

- 特定の送信元から任意のグループへのマルチキャスト トラフィックの送信を許可または拒否する場合は、[送信元 IP（Source IP）] フィールドに、トラフィックの送信元となる特定の送信元の IP アドレスを入力し、[グループ IP（Group IP）] フィールドは空のままにします。
- 任意の送信元から特定のグループへのマルチキャスト トラフィックの送信を許可または拒否する場合は、[グループ IP（Group IP）] フィールドに、トラフィックの送信先のマルチキャスト IP アドレスを入力し、[送信元 IP（Source IP）] フィールドは空のままにします。
- 特定の送信元から特定のグループへのマルチキャスト トラフィックの送信を許可または拒否する場合は、[グループ IP（Group IP）] フィールドと [送信元 IP（Source IP）] フィールドの両方に必要な情報を入力します。

（注） [RP IP] フィールドは、マルチキャスト送信元フィルタリングまたはマルチキャスト受信者フィルタリングには適用されません。このフィールドのエントリはマルチキャスト フィルタリングでは無視されるため、この機能のこのフィールドには値を入力しないでください。

e) [**アクション（Action**）] フィールドでは、ターゲット送信元のアクセスを拒否する場合には [**拒否（Deny**）] を、ターゲット送信元のアクセスを許可する場合には [**許可（Permit**）] を選択します。

f) **[OK]** をクリックします。

[マルチキャストのルート マップ ポリシーの作成（Create Route Map Policy for Multicast）] ウィンドウが再び表示され、設定したルート マップ エントリが [ルート マップ（Route Maps）] テーブルに表示されます。

g) このルートマップに追加のルート マップ エントリを作成するかどうかを決定します。

1 つのルート マップに対して複数のルート マップ エントリを作成できます。各エントリには、独自の IP アドレスと関連アクションがあります。たとえば、同じルート マップ内に、[許可（Permit）] アクションが適用された IP アドレスのセットと、[拒否（Deny）] アクションが適用された IP アドレスの別のセットが必要な場合があります。

このルート マップに追加のルート マップ エントリを作成する場合は、[ルート マップ（Route Maps）] 領域で [+] をもう一度クリックし、に移動して、このルート マップの追加のルートマップエントリを [ルートマップエントリの作成（Create Route Map Entry）] ウィンドウで必要な情報をフィルタリングするステップを繰り返します。5.c （110 ページ）

h) このルート マップのすべてのルート マップ エントリを完了したら、[送信（Submit）] をクリックします。ステップ 7 （112 ページ）に進みます。

ステップ 6 [マルチキャストのルート マップ ポリシーの作成（Create Route Map Policy for Multicast）] オプションを選択して、ラストホップルータでのマルチキャスト宛先（レシーバ）フィルタリングを有効にした場合は、[マルチキャストのルートマップポリシーの作成（Create Route Map Policy for Multicast）] ウィンドウが表示されます。このウィンドウに次の情報を入力します。

a) [名前（Name）] フィールドにこのルート マップの名前を入力し、必要に応じて [説明（Description）] フィールドに説明を入力します。

b) [ルート マップ（Route Maps）] 領域で、[+]をクリックします。

[**ロールの作成（Create a Role**）] ウィンドウが表示されます。

c) **Order** フィールドでは、このインターフェイスに対して複数のアクセス グループを設定している場合に、このインターフェイスでのマルチキャスト トラフィックへのアクセスをどの順序で許可または拒否するかを反映する番号を選択します。

小さい番号のエントリは、大きい番号のエントリの前に並べられます。範囲は 0 ～ 65535 です。

d) マルチキャスト レシーバ フィルタリングで受信するトラフィックを許可するか拒否するかを決定します。

- 任意の送信元から特定のグループへのトラフィックの送信を許可または拒否する場合は、[グループ IP（Group IP）] フィールドに、トラフィックの送信先のマルチキャスト IP アドレスを入力し、[送信元 IP（Source IP）] フィールドは空のままにします。
- 特定の送信元から任意のグループへのトラフィックの送信を許可または拒否する場合は、[送信元 IP（Source IP）] フィールドに、トラフィックの送信元となる特定の送信元の IP アドレスを入力し、[グループ IP（Group IP）] フィールドは空のままにします。
- 特定の送信元から特定のグループへのトラフィックの受信を許可または拒否する場合は、[グループ IP（Group IP）] フィールドと [送信元 IP（Source IP）] フィールドの両方に必要な情報を入力します。

（注） [RP IP] フィールドは、マルチキャスト送信元フィルタリングまたはマルチキャスト受信者フィルタリングには適用されません。このフィールドのエントリはマルチキャスト フィルタリングでは無視されるため、この機能のこのフィールドには値を入力しないでください。

e) [**アクション（Action**）] フィールドでは、ターゲット グループのアクセスを拒否する場合には [**拒否（Deny**）] を、ターゲットグループのアクセスを許可する場合には [**許可（Permit**）] を選択します。

f) **[OK]** をクリックします。

[マルチキャストのルート マップ ポリシーの作成（Create Route Map Policy for Multicast）] ウィンドウが再び表示され、設定したルート マップ エントリが [ルート マップ（Route Maps）] テーブルに表示されます。

g) このルートマップに追加のルート マップ エントリを作成するかどうかを決定します。

1 つのルート マップに対して複数のルート マップ エントリを作成できます。各エントリには、独自の IP アドレスと関連アクションがあります。たとえば、同じルート マップ内に、[許可（Permit）] アクションが適用された IP アドレスのセットと、[拒否（Deny）] アクションが適用された IP アドレスの別のセットが必要な場合があります。

このルート マップに追加のルート マップ エントリを作成する場合は、[ルート マップ（Route Maps）] 領域で [+] をもう一度クリックし、に移動して、このルートマップの追加のルートマップエントリを [ルートマップ エントリの作成（Create Route Map Entry）] ウィンドウで必要な情報をフィルタリングするステップを繰り返します。6.c （111 ページ）

h) このルート マップのすべてのルート マップ エントリを完了したら、[送信（Submit）] をクリックします。ステップ 7 （112 ページ）に進みます。

ステップ 7 [ポリシー/全般（Policy/General）] ページの右下隅にある [送信（Submit）] をクリックします。

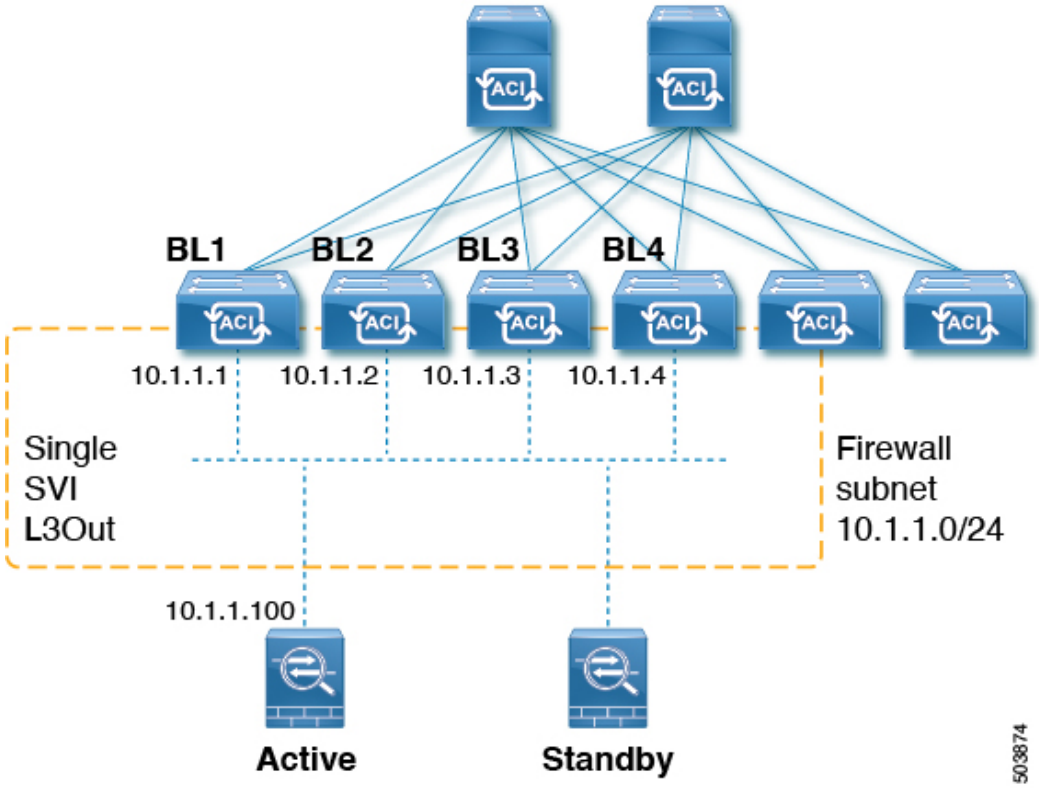
[ポリシー使用の警告（Policy Usage Warning）] ウィンドウが表示されます。

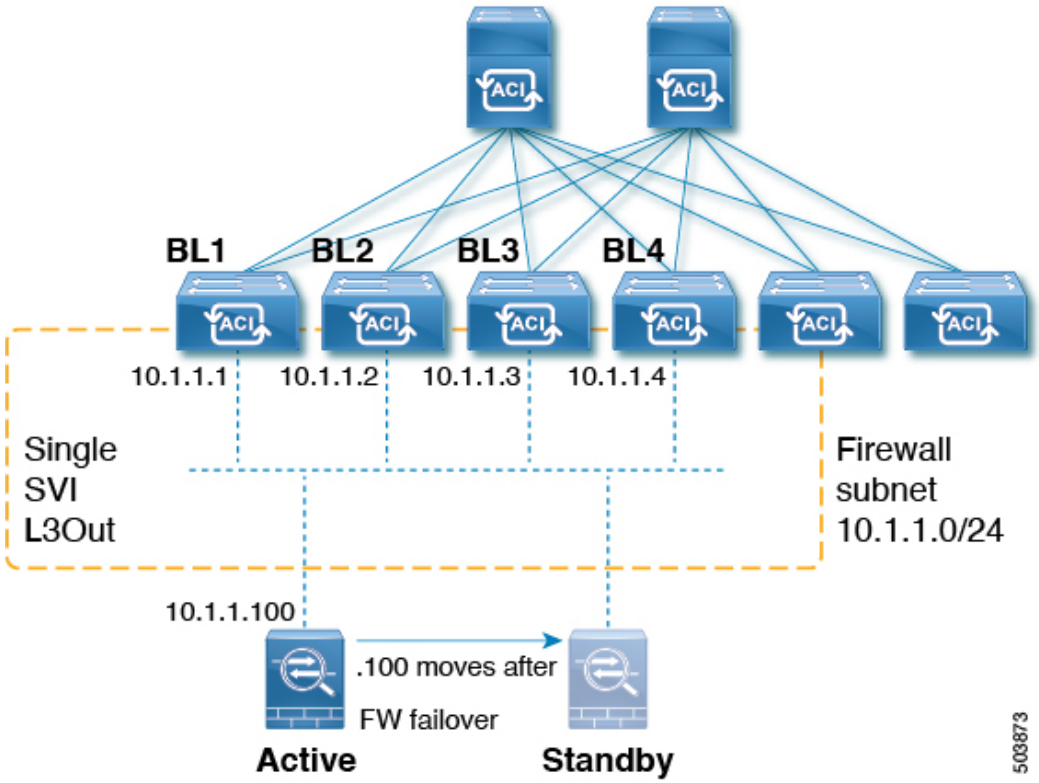
ステップ 8 [ポリシー使用の警告（Policy Usage Warning）] ウィンドウのテーブルに表示されているノードとポリシーがこのポリシーの変更の影響を受けることを確認し、マルチキャストの送信元や宛先のフィルタリングを有効にし、[変更の送信（Submit Changes）] をクリックします。

SVI L3Out のレイヤ 3 マルチキャストについて

L3Out SVI でのレイヤ 3 マルチキャストにより、L3Out SVI で PIM を有効にするためのサポートが追加されます。これにより、L3Out SVI で構成された ACI 境界リーフ スイッチは、外部マルチキャスト ルータまたはファイアウォールとの PIM 隣接関係を確立できます。

ファイアウォールは通常、アクティブ/スタンバイ ペアで展開されます。ここでは、両方のファイアウォールが同じ VLAN とサブネット上のファブリックに接続されます。


BL1
BL2
BL3
BL4
10.1.1.1
10.1.1.2
10.1.1.3
10.1.1.4
Single
SVI
L3Out
Firewall
subnet
10.1.1.0/24
10.1.1.100
Active
Standby
503874

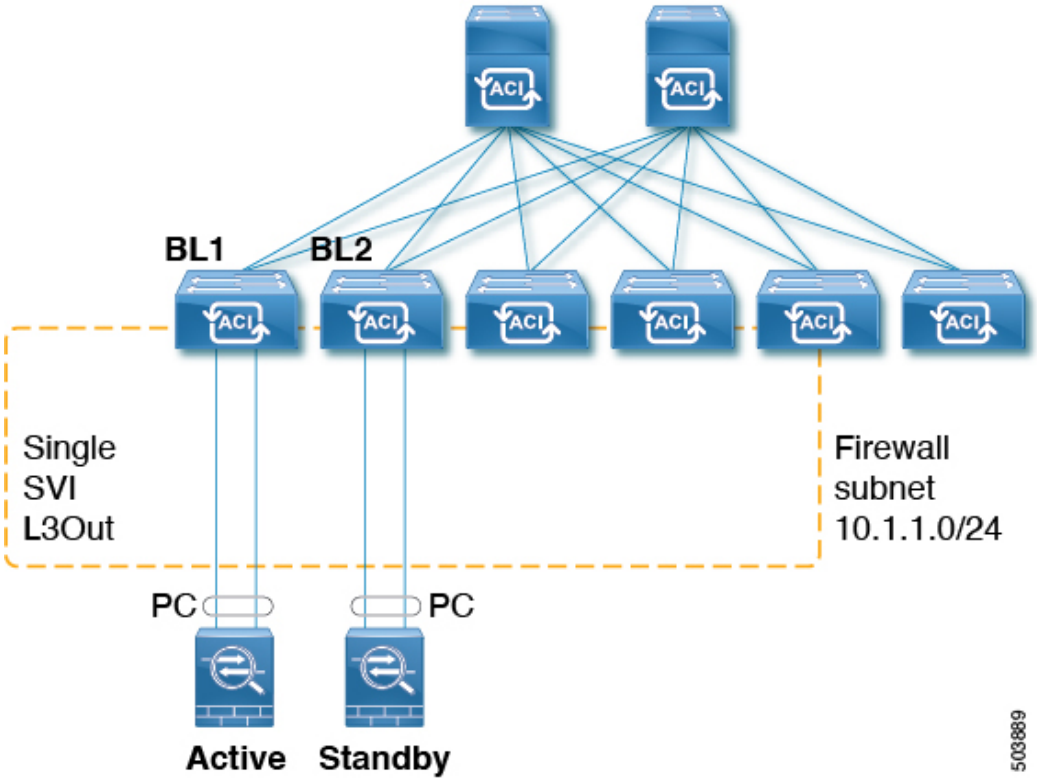

BL1
BL2
BL3
BL4
10.1.1.1
10.1.1.2
10.1.1.3
10.1.1.4
Single
SVI
L3Out
Firewall
subnet
10.1.1.0/24
10.1.1.100
.100 moves after
FW failover
Active
Standby
503873

これは LAN に似たトポロジであるため、ファブリック側に SVI L3Out が必要です。リリース 5.2(3) 以降では、SVI L3Out のレイヤ 3 マルチキャストがサポートされます。

L3Out SVI は、SVI が展開されているすべての境界リーフ スイッチでレイヤ 3 SVI インターフェイスが構成されているインターフェイス タイプです。SVI が設定されている L3Out で PIM が有効になっている場合、SVI の一部である境界リーフ スイッチで PIM プロトコルが有効になります。すべての SVI は、相互に、および外部の PIM 対応デバイスと PIM 隣接関係を形成します。

L3Out からファイアウォールへのトポロジ例

次の図は、ファイアウォールへの L3Out のトポロジ例を示しています。



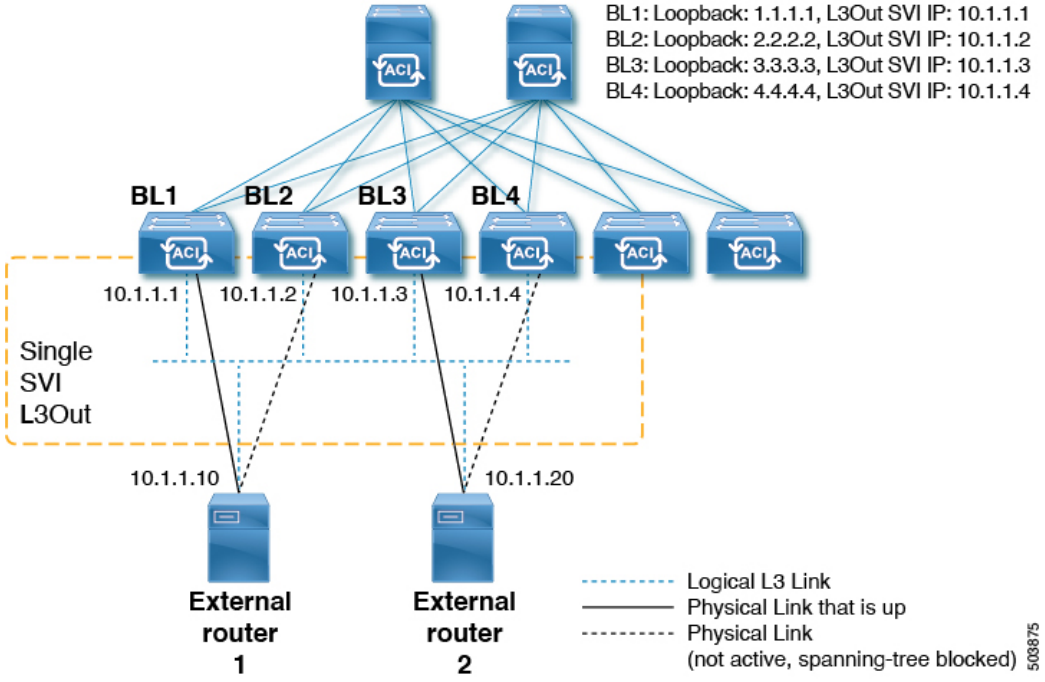
この例では、BL1、BL2 は、ファブリック上の境界リーフ スイッチです。両方の境界リーフ スイッチは、外部ファイアウォールに接続するのと同じ SVI L3Out 上にあります。各ファイアウォールは、ポート チャネル (非 vPC) を介して 2 つの境界リーフ スイッチのいずれかに接続されます。

- 各境界リーフ スイッチは、アクティブ ファイアウォールへの PIM ネイバー隣接関係を形成します。
- この例の BL2 は、L3Out 外部ブリッジ ドメインのファブリック トンネルを介してアクティブなファイアウォールにピアリングします。
- アクティブなファイアウォールは、BL1 と BL2 の両方に PIM 参加/プルーニングを送信できます。

- 2 つの境界リーフ スイッチの 1 つが PIM 加入をファイアウォールに送信します。ファイアウォールに向けて PIM Join を送信する境界リーフ スイッチは、マルチキャスト グループ（SSM のグループとソース）のストライプ勝者選択によって決定されます。
- BL2 は、マルチキャスト グループのストライプ勝者として選択できます。トポロジ例の BL2 は、アクティブなファイアウォールに直接接続されていません。BL1 は BL2 に、ソースに直接接続されたリバース パス フォワーディング（RPF）であることを通知します。BL2 は BL1 経由で PIM を送信できます。BL2 は、ファイアウォールの IP アドレスの再帰ルックアップを実行できる必要があります。この機能は、接続されたホストの再配布機能によって提供されます。ファイアウォール サブネットに一致するルート マップは、L3Out での接続ホストの再配布用に構成する必要があります。

L3Out SVI から外部スイッチ/ルータへのトポロジ例

次の図は、外部スイッチまたはルータへの L3Out SVI のトポロジ例を示しています。



レイヤ 3 マルチキャスト ステートおよびマルチキャスト データ トラフィックに関して、上記の図のコンポーネントは次のように影響を受けます。

- BL1、BL2、BL3、および BL4 は、ファブリック上の境界リーフ スイッチです。これらの境界リーフ スイッチはすべて、外部ボックスに接続する同じ SVI L3Out 上にあります。外部ボックスは、任意の外部スイッチまたはルータである可能性があります。
- 論理的には、レイヤ 3 リンクは境界リーフ スイッチと外部ルータの間でアップ状態です。したがって、SVI L3Out の境界リーフ スイッチおよび外部ルータをまたがるユニキャスト ルーティング プロトコルまたは PIM に関して、フルメッシュ隣接関係が存在します。

- SVI L3Out はブリッジドメインであるため、境界リーフ スイッチから外部ルータへの複数の物理接続がある場合でも、それらの間の 1 つのリンクだけがレイヤ 2 レベルで各外部ルータにアップします。他のすべてのリンクは STP によってブロックされます。

  たとえば、上の図では、レイヤ 2 レベルの次のリンクだけがアップしています。

  - BL1 と外部ルータ 1 間のリンク
  - BL3 と外部ルータ 2 間のリンク

  したがって、他のすべての境界リーフ スイッチでは、IP アドレス 10.1.1.10 は BL1 を介してのみ到達可能であり、10.1.1.20 は BL3 を介してのみ到達可能です。

注意事項と制約事項

- PIM 対応の SVI L3Out には、接続されたホストルートマップを設定する必要があります。このルート マップは、直接接続されたすべての外部 PIM ネイバーと一致する必要があります。0.0.0.0/0 サブネットを使用できます。
- SVI L3Out 機能のレイヤ 3 マルチキャストでは、次の領域がサポートされます。
  - **サポート対象**:
    - Protocol Independent Multicast（PIM）Any Source Multicast（ASM）および Source-Specific Multicast（SSM）
    - 物理インターフェイスを使用した SVI
    - ダイレクト ポート チャネルを使用した SVI（非 vPC）
    - すべてのトポロジの組み合わせ：
      - Source Inside Receiver Inside（SIRI）
      - Source Inside Receiver Outside（SIRO）
      - Source Outside Outside Receiver Inside（SORI）
      - Source Outside Outside Receiver Outside（SORO）
  - **サポート対象外**：
    - SVI L3Out を介した VPC によるレイヤ 3 マルチキャスト
    - SVI サブネットに直接接続された送信元または受信者ホスト（送信元または受信者ホストは SVI L3Out 上のルータの背後に接続されている必要があります）
    - ローカル リーフ スイッチ（ACI メイン データ センター スイッチ）とリモート リーフ スイッチ間のストレッチ SVI L3out はサポートされていません。
    - 複数のサイト（Cisco ACI マルチサイト）にまたがるストレッチ SVI L3Out
    - PIMv6 の SVI L3Out

- セカンダリ IP アドレス境界リーフ スイッチのセカンダリ IP アドレスに送信された場合、PIM の参加/プルーニングは処理されません。セカンダリ IP アドレスは、通常、静的ルーティング用の境界リーフ スイッチ間で共有 (仮想) IP アドレスを構成するために使用されます。PIM over SVI を設定するときはダイナミック ルーティングを使用するか、各境界リーフ スイッチのプライマリ アドレスへのスタティック ルートを作成することをお勧めします。

GUI を使用した SVI L3Out 上のレイヤ 3 マルチキャストの設定

手順

ステップ 1 レイヤ 3 インターフェイス タイプとして [SVI] を設定した [L3Out の作成（Create L3Out）] ウィザードを使用して、標準 L3Out を設定します。

a) GUI の [ナビゲーション（Navigation）] ペインの、[テナント例（Tenant Example）] で [ネットワーキング（Networking）] [L3Out] の順に移動します。 >
b) [L3Out の作成（Create L3Out）] を右クリックして選択します。
c) [L3Out の作成（Create L3Out）] 画面の [識別（Identity）] ウィンドウで、L3Out の名前を入力し、この L3Out に関連付ける VRF および L3 ドメインを選択します。
d) [識別（Identity）] ウィンドウに必要な情報を入力したら、[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。
e) [**ノードとインターフェイス（Nodes and Interfaces**）] ウィンドウの [インターフェイス タイプ：レイヤ 3（Interface Types: Layer 3）] フィールドで、レイヤ 3 インターフェイス タイプとして [SVI] を選択します。
f) L3Out の設定が完了するまで、[L3Out の作成（Create L3Out）] ウィザードを使用して個々のフィールドの設定を続けます。

ステップ 2 設定された L3Out に移動します。

[テナント（Tenants）] > [*tenant_name*] > [ネットワーキング（Networking）] > [L3Outs] > [*L3Out_name*]

設定された L3Out の [サマリー（Summary）] ページが表示されます。

ステップ 3 [ポリシー（Policy）] タブをクリックし、次に [メイン（Main）] サブタブをクリックします。

設定された L3Out の [プロパティ（Properties）] ページが表示されます。

ステップ 4 [再配布用のルート プロファイル（Route Profile for Redistribution）] フィールドで、[+] をクリックして再配布用のルート プロファイルを設定します。

ステップ 5 [送信元（Source）] フィールドで、[attached-host] を選択します。

ステップ 6 [ルート マップ（Route Map）] フィールドで、すべてを許可するルート マップを設定します。

a) [ルート制御のルート マップの作成（Create Route Maps for Route Control）] をクリックします。

[ルート制御のルート マップの作成（Create Route Maps for Route Control）] ウィンドウが表示されます。

b) このルートマップの名前と説明を入力し、[コンテキスト（Contexts）]領域で[+]をクリックします。

[ルート制御コンテキストの作成（Create Route Control Context）] ウィンドウが表示されます。

c) [ルート制御コンテキストの作成（Create Route Control Context）] ウィンドウで必要なパラメータを設定し、[アクション（Action）] フィールドの値を [許可（Permit）] に設定します。

d) [関連付けられた一致ルール（Associated Match Rules）] 領域で [+] をクリックし、[ルートマップの一致ルールの作成（Create Match Rule for a Route Map）] を選択して、このルート制御コンテキストの一致ルールを設定します。

[**一致ルールの作成（Create Match Rule**）] ウィンドウが開きます。

e) [一致 プレフィックス（Match Prefix）] 領域で [+] をクリックします。

[一致ルート宛先ルールの作成（Create Match Route Destination Rule）] ウィンドウが表示されます。

f) **[一致ルート宛先ルールの作成（Create Match Route Destination Rule）]** ウィンドウで、これらのフィールドに次の値を入力して、サブネットまたは 0.0.0.0/0 ルートおよび集約設定で一致する集約ルートをもつルールを設定します。

- IP：0.0.0.0/0
- 集約（Aggregate）：このフィールドのボックスをオンにします。[マスクより大きい（Greater Than Mask）] フィールドと [マスク未満（Less Than Mask）] フィールドが表示されます。
- **マスクより大きい**： 0
- **マスク未満**：0

g) [送信（Submit）]をクリックして、この一致ルート宛先ルールを設定します。

ステップ 7 すべてを許可するルートマップを設定したら、集約ルートまたは 0.0.0.0 / 0 ルートの集約エクスポートを行うエクスポートルート制御サブネットで外部EPGを設定します。

a) 設定済みの外部 EPG に移動します。

[テナント（Tenants）] > [*tenant_name*] > [ネットワーキング（Networking）] > [L3Outs] > [*L3Out_name*] > [外部 EPG（External EPGs）] > [*external_EPG_name*]

設定された L3Out の [プロパティ（Properties）] ページが表示されます。デフォルトでは、[ポリシー/全般（Policy / General）] ページが表示されます。

b) [サブネット（Subnets）] 領域で、設定した 0.0.0.0/0 エントリをダブルクリックします。

設定されたサブネットの [プロパティ（Properties）] ウィンドウが表示されます。

c) [ルート制御（Route Control）] 領域で、次の項目を選択します。

- [**ルート制御サブネットのエクスポート（Export Route Control Subnet**）] の隣のチェック ボックスをオンにします。
- [集約（Aggregate）] 領域で、[エクスポートの集約（Aggregate Export）] フィールドの横にあるボックスをオンにします。

d) [Submit] をクリックします。

PIM インターフェイスが作成されなかった理由の判別

PIM インターフェイスが L3Out インターフェイス用に作成されていない

L3Out インターフェース用に PIM インターフェース（pim:If）が作成されていない場合は、以下を確認してください。

1. PIM が L3Out で有効になっています。PIM が無効になっている場合は、有効にします。
2. コンテナ L3Out で PIM が有効になっている場合は、マルチキャスト l3ext:InstP がプレフィックス名として「__int_」で作成されていることを確認します。このマルチキャスト l3ext:InstP は、L3Out PIM ポリシーをスイッチに展開するために使用されます。L3Out ごとに 1 つのマルチキャスト l3ext:InstP が必要です。

（注）
- マルチキャスト l3ext:InstP が IFC に存在する場合、対応する fv:RtdEpP が作成され、その L3Out にインターフェイスがある各スイッチに展開されているかどうかを確認できます。
- PIM の L3Out SVI インターフェイスはサポートしていません。

PIMインターフェイスがマルチキャストトンネルインターフェイス用に作成されていない

マルチキャストトンネルインターフェイス（tunnel:If）に対して PIM インターフェース（pim:if）が作成されていない場合は、以下を確認してください。

1. 対応するトンネル:If が作成されました。

（注） tunnel:If のタイプは「underlay-mcast」である必要があります。

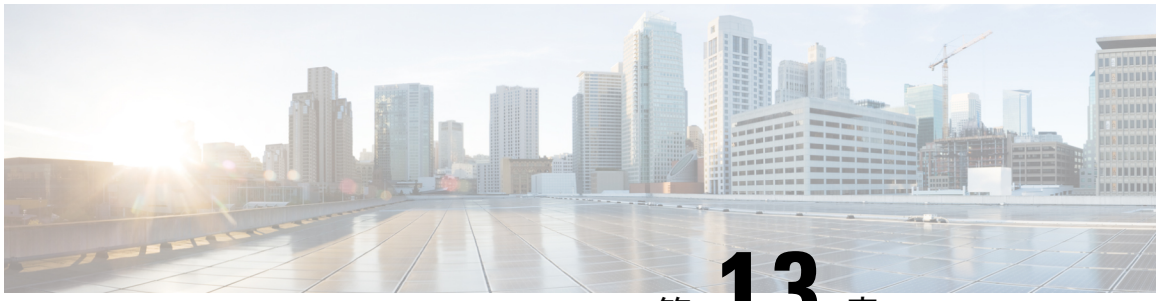
2. 各 mcast 対応 VRF は、mcast トンネルを作成しています。
3. tunnel:If の宛先 IP フィールドには、有効な GIPO アドレスが入力されています。
4. tunnel:If に有効な GIPO アドレスが入力されていない場合は、IFC の pim:CtxP とスイッチの pim:CtxDef をチェックして、GIPO が正しく割り当てられていることを確認します。
5. トンネルの送信元 IP:If には、BL の場合は L3Out のループバック アドレス、NBL の場合は「127.0.0.100」があります。

PIM インターフェイスがマルチキャスト対応ブリッジ ドメインに作成されない

マルチキャスト対応のブリッジ ドメイン（BD）に対して PIM インターフェイス（pim:if）が作成されていない場合は、次のことを確認します。

1. 対応する BD または対応する Ctx で PIM が有効になっています。
2. 対応する BD が普及しています。
3. 普及している BD ベースの pim:If は、デフォルトのパラメータを受け取ります。

（注） igmp snooping との相互作用については、普及 BD で PIM が有効になっている場合、対応する igmpsnoop:If に対してルーティング ビットが自動的に有効になっている必要があります。



第 13 章

Cisco ACI Multi-Pod

マルチポッドについて

マルチポッドは、隔離されたコントロール プレーン プロトコルを持つ複数のポッドで構成された、障害耐性の高いファブリックのプロビジョニングを可能にします。また、マルチポッドでは、さらに柔軟にリーフとスパイン スイッチ間のフル メッシュ配線を行うことができます。たとえば、リーフ スイッチが異なるフロアや異なる建物にまたがって分散している場合、マルチポッドでは、フロアごと、または建物ごとに複数のポッドをプロビジョニングし、スパイン スイッチを通じてポッド間を接続することができます。

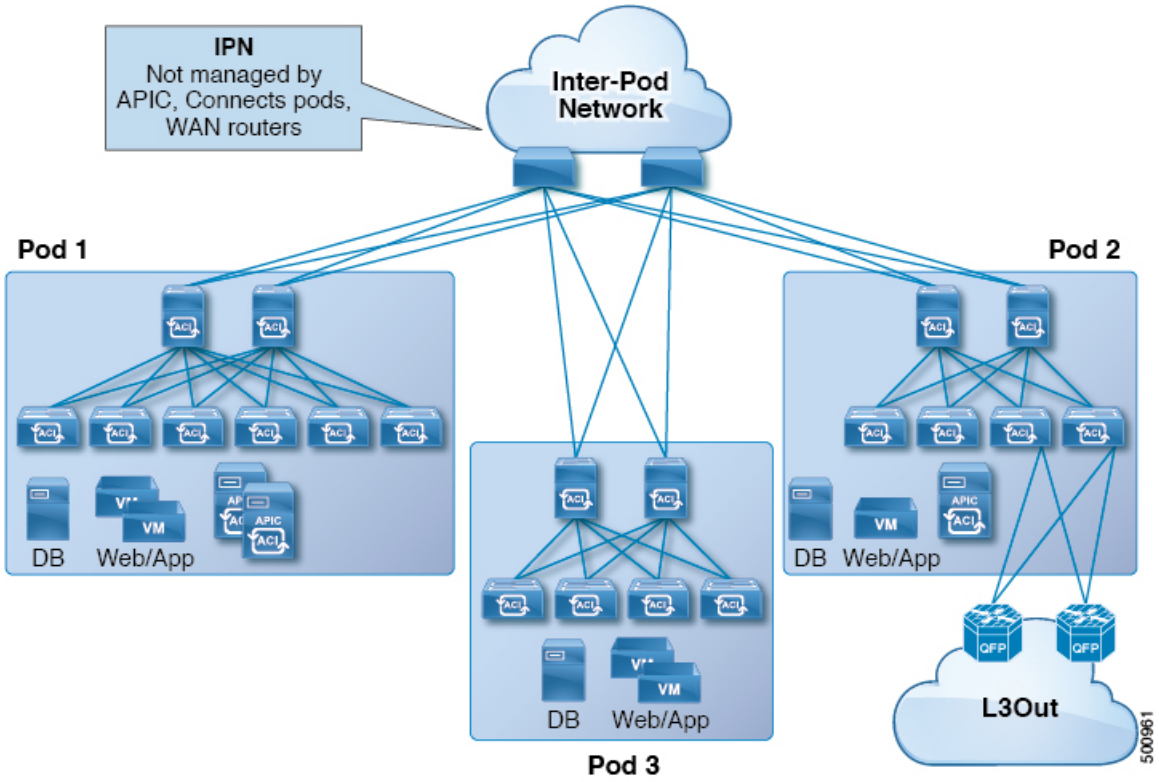
マルチポッドは、異なるポッドの ACI スパイン間のコントロール プレーン通信プロトコルとして MP-BGP EVPN を使用します。

Cisco APIC リリース 5.2(3) よりも前のリリースでは、物理スパインと IPN の間をピアリングするためにアンダーレイで OSPF が使用されます。Cisco APIC リリース 5.2(3) 以降、アンダーレイ プロトコルは OSPF または BGP（eBGP のみ）または混合で、OSPF を使用するポッドと BGP を使用するポッドがあります。

WAN ルータは、ポッド間ネットワーク（IPN）でプロビジョニング可能で、スパイン スイッチに直接接続されるか、境界リーフ スイッチに接続されます。IPN に接続されるスパイン スイッチは、ポッド内ので少なくとも 1 個のリーフ スイッチに接続されます。

マルチポッドはすべてのポッドに単一の APIC クラスタを使用します。そのため、すべてのポッドが単一のファブリックとして機能します。ポッド全体にわたって個々の APIC コントローラが配置されますが、それらはすべて単一の APIC クラスタの一部です。

図 *10 :* マルチポッドの概要



（注） Cisco APIC リリース 5.2(3) 以降、2 つのポッドのみで構成されるファブリックは、IPN なしで直接接続できます。このマルチポッド スパイン バックツーバックトポロジについては、マルチポッド スパイン バックツーバック について （137 ページ）を参照してください。

マルチポッドのプロビジョニング

IPN は APIC では管理されません。これは、次の情報が事前する必要があります。

- すべてのポッドの背表紙に接続されているインターフェイスを設定します。VLAN-4 でトラフィックをタグ付けするレイヤ 3 サブインターフェイスを使用し、MTU をサイト間コントロール プレーンおよびデータ プレーン トラフィックに必要な最大 MTU より 50 バイト以上増やします。

  リモート リーフ スイッチがいずれかのポッドに含まれている場合は、『Cisco ACI Remote Leaf Architecture White Paper』を参照してください。リモート リーフ スイッチ （141 ペー

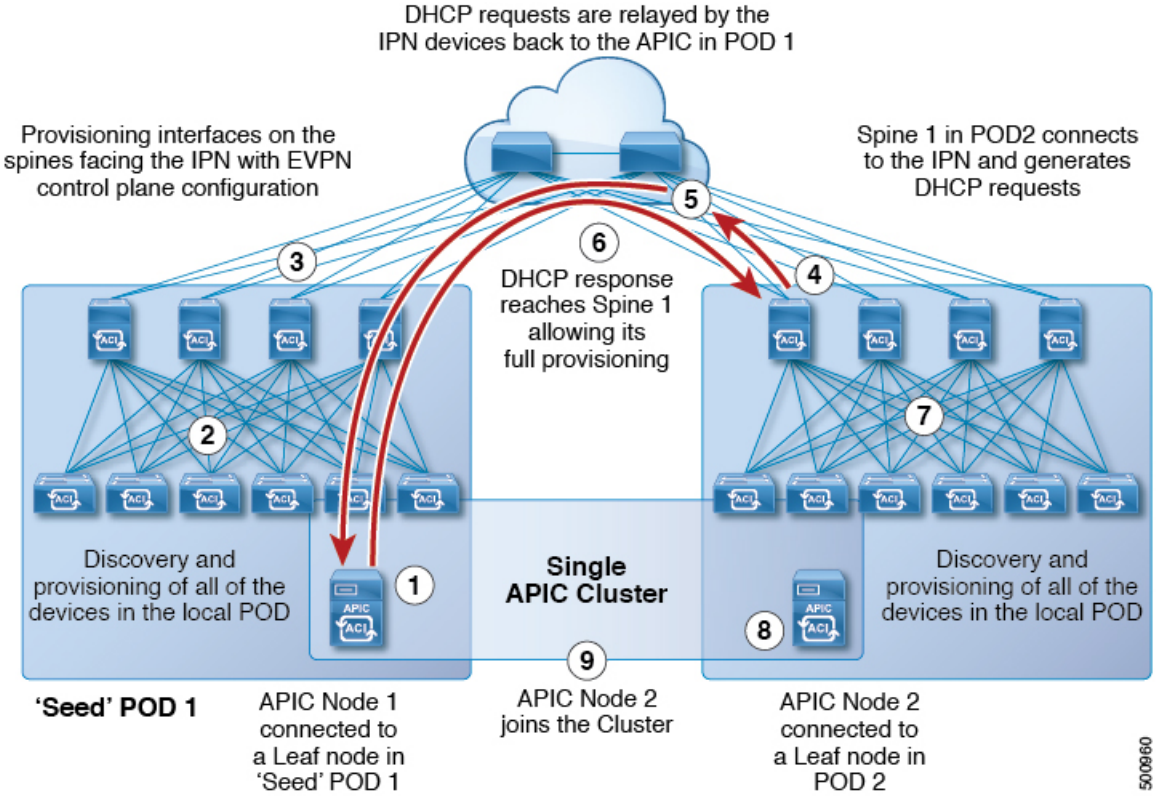
ジ）https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-740861.html

- IPN アンダーレイ プロトコルが OSPF の場合は、正しいエリア ID を持つサブインターフェイスで OSPF を有効にします。Cisco APIC リリース 5.2(3) 以降、IPN アンダーレイ プロトコルは OSPF または BGP（eBGP のみ）になることが可能です。
- すべての背表紙に接続されている IPN インターフェイスで DHCP リレーを有効にします。
- PIM をイネーブルにします。
- PIM 双方向としてブリッジ ドメイン GIPO 範囲の追加（**bidir**）の範囲をグループ化 (デフォルトでは 225.0.0.0/15)。

  グループを **bidir** モードが機能の転送を共有ツリーのみ。
- PIM として 239.255.255.240/28 を追加 **bidir** 範囲をグループ化します。
- PIM およびすべての背表紙に接続されたインターフェイスで IGMP を有効にします。

（注） PIM **bidir** を展開する際には、どの時点であっても、特定のマルチキャスト グループ範囲に対して、1 つのアクティブな RP（ランデブー ポイント）を設定することだけが可能です。RP の冗長性が活用することで実現そのため、 **ファントム RP** 設定します。希薄モードの冗長性を提供するために使用するエニー キャストまたは MSDP メカニズムはのオプションではありませんマルチキャスト ソースの情報は、Bidir で利用可能なは不要であるため **bidir** 。

図 *11* : マルチポッドのプロビジョニング



Cisco ACI マルチポッド ファブリックの設定に関するガイドライン

Cisco ACI マルチポッド ファブリックを設定するには、次のガイドラインに従います。

- Cisco ACI マルチポッド は次でサポートされます。
  - すべての ACI モード スパイン スイッチ
  - すべての Cisco Nexus 9000 シリーズ ACI モード リーフ スイッチ
  - すべての Cisco Nexus 9500 プラットフォーム ACI モード スイッチ ライン カードおよびファブリック モジュール
- 関連付けられたノード グループおよびレイヤ 3 外部（L3Out）ポリシーを作成します。
- スパイン スイッチを変更する前に、Cisco ACI マルチポッド トポロジに参加している運用「アップ」外部リンクが少なくとも 1 個あることを確認します。失敗すると、Cisco ACI マルチポッド接続がダウンする可能性があります。

- Cisco ACI マルチポッド のセットアップを単一のポッド（ポッド 1 のみを含む）に変換する必要がある場合は、デコミッションされたポッドに接続されている Cisco Application Policy Infrastructure Controller（APIC）を再初期化し、ポッド 1 のリーフ スイッチに接続する必要があります。これにより、初期セットアップ スクリプトの実行後にクラスタに再参加できるようになります。手順については、APIC を 1 つのポッドから別のポッドに移動する （134 ページ）を参照してください。TEP プール設定を削除する必要があります。
- （ファブリック WAN のレイヤ 3 EVPN サービスとも呼ばれます）。Cisco ACI GOLFCisco ACI マルチポッドCisco ACI マルチポッド

  GOLF の詳細については、Cisco ACI GOLF （481 ページ）を参照してください。
- Cisco ACI マルチポッド ファブリックでは、Cisco APIC ノードは常にPod 1 TEPプールからアドレス指定されるため、Pod 1設定（関連付けられているTEPプールを含む）は常に Cisco APIC 上に存在する必要があります。これは、元の Pod 1 TEP プールがファブリックに追加される可能性のある他の Pod に再割り当てされないように、Pod 1 が物理的にデコミッションされるシナリオでも有効です。
- Cisco ACI マルチポッドファブリック セットアップで、新しいスパイン スイッチがポッドに追加される場合、最初にポッド内の少なくとも 1 個のリーフ スイッチに接続する必要があります。これにより、Cisco APIC がスパイン スイッチを検出し、ファブリックに参加できるようにします。
- ポッドが作成されポッドにノードが追加された後、ポッドを削除するとファブリック内でアクティブなポッドから古いエントリになります。これは、Cisco APIC がオープン ソース DHCP を使用しており、ポッドが削除されると Cisco APIC が削除できない一部のリソースを作成するため発生します。
- 個別のポッドに属するスパイン スイッチを直接バックツーバック リンクで接続すると、2 つのスパイン スイッチ間のピア インターフェイスで OSPF ネイバーシップが確立される場合があります。ピア インターフェイス間で不一致が発生し、いずれかのピアで Cisco ACI マルチポッド ダイレクト フラグが無効になっている場合、セッションは起動せず、転送は行われません。この状況ではシステムが障害をスローしますが、これは予期された動作です。
- Cisco APIC リリース 5.2(3) 以降では、IPN アンダーレイ プロトコルを外部 BGP（eBGP）にすることができます。内部 BGP（iBGP）は、アンダーレイ プロトコルとしてサポートされていません。

  OSPF と BGP の間で IPN アンダーレイとして Cisco ACI マルチポッド ファブリックを移行する準備をする場合は、次のガイドラインに従ってください。

  - Cisco ACI ファブリックがクラウド サイトまたは GOLF ルータに接続されている場合、BGP アンダーレイはサポートされません。
  - BGP アンダーレイは、IPv6 アドレス ファミリではなく、IPv4 アドレス ファミリのみをサポートします。
- Cisco APIC リリース 5.2(1) で導入された、レイヤ 3 ネットワークを介したファブリックへの Cisco APIC クラスタ接続を展開する場合、IPN ネットワークは OSPF をアンダーレイ

プロトコルとして使用できます。または、Cisco APIC が Cisco ACI マルチポッドまたはリモートリーフ接続を提供しているのと同じネットワークを使用してファブリックに接続する場合、BGP アンダーレイを使用できます。

- ポリシーの名前を変更するなど、Cisco ACI マルチポッド L3Out を削除し再作成する場合、ファブリックのスパイン スイッチの一部でクリーン リロードを実行する必要があります。Cisco ACI マルチポッド L3Out を削除すると、ファブリック内の 1 台以上のスパイン スイッチが Cisco APIC への接続を失う可能性があり、そのためこれらのスパイン スイッチは Cisco APIC から更新されたポリシーをダウンロードできなくなります。どのスパイン スイッチがそのような状態になるかは、展開されているトポロジによって異なります。この状態から回復するには、これらスパイン スイッチでクリーン リロードを実行する必要があります。スパイン スイッチでコマンドをリロードしたら、**setup-clean-config.sh** コマンドを使用してリロードを実行します。

（注） Cisco ACI は IP フラグメンテーションをサポートしていません。したがって、外部ルータへのレイヤ 3 Outside（L3Out）接続、または Inter-Pod Network（IPN）を介した マルチポッド 接続を設定する場合は、インターフェイス MTU がリンクの両端で適切に設定されていることが推奨されます。Cisco ACI、 Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定可能な MTU 値はイーサネット ヘッダー (一致する IP MTU、14-18 イーサネット ヘッダー サイズを除く) を考慮していません。また、IOS XR などの他のプラットフォームには、設定された MTU 値にイーサネット ヘッダーが含まれています。設定された値が 9000 の場合、Cisco ACI、Cisco NX-OS Cisco IOS の最大 IP パケット サイズは 9000 バイトになりますが、IOS-XR のタグなしインターフェイスの最大 IP パケットサイズは 8986 バイトになります。

各プラットフォームの適切な MTU 値については、それぞれの設定ガイドを参照してください。

CLI ベースのコマンドを使用して MTU をテストすることを強く推奨します。たとえば、Cisco NX-OS CLI で `ping 1.1.1.1 df-bit packet-size 9000 source-interface ethernet 1/1` などのコマンドを使用します。

（注） Cisco APIC は、CP-MTU 設定に関係なく、常に 1496 バイト（TCP MSS 1456）の MTU でファブリック スイッチへの TCP 接続を確立します。リモート ポッドおよびリモート リーフ スイッチの IPN ネットワークは、ファブリック ディスカバリのために少なくとも 1500 バイトの MTU をサポートする必要があります。

- **[システム（System）] > [システム設定（System Settings）] > [コントロール プレーン MTU（Control Plane MTU）]** のファブリックのノード（Cisco APIC およびスイッチ）により送信される、コントロール プレーン（CP）パケットのグローバル MTU を設定できます。
- Cisco ACI マルチポッド トポロジでは、ファブリック外部ポートの MTU 設定は CP MTU 値セット以上にする必要があります。そうしないと、ファブリックの外部ポートが CP MTU パケットをドロップする可能性があります。

- IPN または CP MTU を変更する場合、CP MTU 値を変更し、次にリモート ポッドのスパイン上の MTU 値を変更することをお勧めします。これで、MTU の不一致によりポッド間の接続が失われるリスクが減少します。これは、ポッド間の IPN デバイスのすべてのインターフェイスの MTU が、常にコントロールプレーンと VXLAN データプレーンの両方のトラフィックに十分な大きさであることを保証するためです。データ トラフィックの場合、VXLAN による余分な 50 バイトに注意してください。
- ポッドをデコミッションするには、ポッドのすべてのノードをデコミッションします。詳細については、「*Cisco APIC* トラブルシューティング ガイド」の「ポッドのデコミッションと再コミッション」を参照してください。
- Cisco APIC 6.0(2) リリース以降では、OSPF Cisco ACI マルチポッド セッションを構成し、そのセッションが実行されている場合は、L3Out インターフェイス プロパティにパッシブ インターフェイスを構成しないでください。

マルチポッド ファブリックの設定

Cisco Application Policy Infrastructure Controller（APIC）4.0(1) 以降、GUI にウィザードが追加され、マルチポッド設定がシンプルになりました。GUI を使用してマルチポッドを設定するには、このセクションの手順に従います。

2 つの物理ポッドの間にマルチポッドを設定する手順には、既存の物理ポッドが新しいポッドとインターポッド ネットワーク（IPN）経由で通信するための準備が含まれます。その後物理ポッドを追加したら、シスコ Cisco APIC がマルチポッド ファブリックを作成します。

NX-OS スタイルの CLI と REST API を使用してマルチポッドを設定することもできます。手順については、このガイドの「NX-OS CLI を使用したマルチポッド ファブリックのセットアップ （524 ページ）」および「REST API を使用したマルチポッド ファブリックのセットアップ（607 ページ）」のセクションを参照してください。

IPN 接続のためのポッドの準備

新しいポッドを作成する前に、最初に、既存の物理ポッドから新しいポッドに通信できることを確認する必要があります。

手順

ステップ 1 Cisco APICにログインします。

ステップ 2 **[ファブリック（Fabric）] > [インベントリ（Inventory）]** に移動します。

ステップ 3 [Quick Start] を展開し、[Add Pod] をクリックします。

ステップ 4 作業ペインで、[Add Pod] をクリックします。

ステップ 5 [Configure Interpod Connectivity STEP 1 > Overview] パネルで、ポッド間ネットワーク（IPN）接続の設定に必要なタスクを確認し、[Get Started] をクリックします。

ステップ 6 [Configure Interpod Connectivity STEP 2 > IP Connectivity] ダイアログボックスで、次の手順を実行します。

a) [L3 Outside 設定（L3 Outside Configuration）] 領域の [名前（Name）] フィールドがある場合、[名前（Name）] ドロップダウン リストから既存のファブリック外部ルーティング プロファイルを選択します。

b) [Spine ID] セレクタを使用して、スパインを選択します。

さらにスパインの ID を追加するには [+]（プラス記号）をクリックします。

c) [Interfaces] 領域の [Interface] フィールドで、IPN への接続に使用されるスパイン スイッチ インターフェイス（スロットおよびポート）を入力します。

さらにインターフェイスを追加するには [+]（プラス記号）をクリックします。

d) [IPV4 Address] フィールドに、インターフェイスの IPv4 ゲートウェイ アドレスとネットワーク マスクを入力します。

e) [MTU（bytes）] ドロップダウンリストで、外部ネットワークの最大伝送ユニットの値を選択します。

範囲は 1500 ～ 9216 です。

f) [次へ] をクリックします。

ステップ 7 **ポッド間接続の設定 STEP 3> ルーティング プロトコル** ダイアログ ボックスで、物理スパインと IPN の間でピアリングするアンダーレイ プロトコルを設定します。Cisco APIC リリース 5.2(3) よりも前のリリースでは、Open Shortest Path First（OSPF）が唯一サポートされているアンダーレイです。これらの以前のリリース、または [アンダーレイ（Underlay）] として [OSPF] を選択した場合の以降のリリースでは、[OSPF] エリアで次のサブステップを実行します。

a) [Use Defaults] をオンのままにするか、オフにします。

[デフォルトの使用（Use Defaults）] チェックボックスをオンにすると、GUI は OSPF を設定するためのオプションフィールドを非表示にします。オフにした場合は、すべてのフィールドが表示されます。デフォルトでは、このチェックボックスはオフになっています。

b) [Area ID] フィールドに OSPF エリア ID を入力します。

c) [Area Type] 領域で、OSPF エリア タイプを選択します。

[NSSA エリア（NSSA area）] または **[通常のエリア（Regular area）]**から選択できます。**スタブ エリア**はサポートされていません。

d) （オプション）[Area Cost] セレクタで、適切な OSPF エリア コスト値を選択します。このフィールドは、[デフォルトの使用（Use Defaults）] チェックボックスがオフの場合にのみ表示されます。

e) [Interface Policy] ドロップダウン リストで、OSPF インターフェイス ポリシーを選択するか設定します。

既存のポリシーを選択するか、[Create OSPF Interface Policy] ダイアログボックスでポリシーを作成できます。

ステップ 8 Cisco APIC リリース 5.2(3) 以降、アンダーレイ プロトコルは OSPF または BGP になることが可能です。Cisco APIC リリース 5.2(3) より前のリリースの場合、または前の手順で[アンダーレイ（Underlay）] として [OSPF] を選択した場合は、この手順をスキップします。**[ポッド間接続の設定 STEP 3 > ルーティング プロトコル]** ダイアログボックスで **[アンダーレイ（Underlay）]** として **[BGP]** を選択した場合、**[BGP]** エリアで、次の手順を実行して BGP アンダーレイを構成します。

MP-BGP エリアで、**[デフォルトを使用]** チェックボックスをオンのままにします。Multiprotocol Border Gateway Protocol（MP-BGP）を構成するための GUI のフィールドが非表示になります。

a) [**スパイン ID**（**Spine ID**）]、[**インターフェイス**（**Interface**）]、および [**IPv4 アドレス**（**IPv4 Address**）] フィールドでは値は設定不可であることに注意してください。
b) [**ピア アドレス**（**Peer Address**） フィールドで、BGP ネイバーの IP アドレスを入力します。
c) [**リモート AS**（**Remote AS**） フィールドで、BGP ネイバーの自動システム（AS）番号を入力します。
d) [次へ] をクリックします。

ステップ 9 [Configure Interpod Connectivity STEP 4 > External TEP] ダイアログボックスで、次の手順を実行します。

a) [Use Defaults] をオンのままにするか、オフにします。

[Use Defaults] チェックボックスをオンにすると、外部 TEP プールを設定するための GUI のオプション フィールドが非表示になります。オフにした場合は、すべてのフィールドが表示されます。デフォルトでは、このチェックボックスはオフになっています。

b) [Pod] および [Internal TEP Pool] フィールドの設定できない値に注意してください。
c) [External TEP Pool] フィールドに、物理ポッドの外部 TEP プールを入力します。

外部 TEP プールは、内部 TEP プール、または他のポッドに属する外部 TEP プールと重複しないようにする必要があります。

d) [**データ プレーン TEP IP**（**Data Plane TEP IP**）] フィールドに、ポッド間のトラフィックのルーティングに使用されるアドレスを入力します。このアドレスには、/32 サブネットマスクが必要です。

[**外部 TEP プール**（**External TEP Pool**）] を設定するときに生成されるデフォルト アドレスを受け入れることができます。別のアドレスを入力することもできますが、外部 TEP プールの外部にある必要があります。

e) [ルータ ID（Router ID）] フィールドに、IPN ルータ IP アドレスを入力します。
f) （オプション）[Loopback Address] フィールドに、IPN ルータ ループバック IP アドレスを入力します。

[Use Defaults] をオフにすると、Cisco APIC によって、[Unicast TEP IP] フィールドと [Spine ID] フィールドが設定できない状態で表示されます。

g) [Finish] をクリックします。

[Summary] パネルが表示され、IPN 設定の詳細が表示されます。[View JSON] をクリックすると、REST API の設定を表示することもできます。REST API を保存して後で使用することができます。

次のタスク

次のいずれかを実行します。

- このまま直接ポッドの追加に進み、このガイドの「マルチポッドファブリックを作成するポッドの追加 （130 ページ）」の手順を続けることができます。
- [Configure Interpod Connectivity] ダイアログボックスを閉じてポットを後で追加し、このガイドの「マルチポッドファブリックを作成するポッドの追加 （130 ページ）」の手順に戻ります。

マルチポッド ファブリックを作成するポッドの追加

[物理ポッドの追加（Add Physical Pod）] ダイアログを使用すると、マルチポッド環境を設定できます。新しい物理ポッド ID とトンネル エンドポイント（TEP）プールを定義します。また、新しいポッド ネットワーク設定を行い、物理スパインのサブインターフェイスを設定します。

始める前に

ここまで次のタスクを実行しました。

- ノード グループおよび L3Out ポリシーが作成されました。
- ポッド間ネットワーク（IPN）を設定しました。設定の例については、このガイドの「Cisco Nexus 9000 シリーズ スイッチでのマルチポッド IPN 設定の例 （132 ページ）」を参照してください。
- 新しいポッドと IPN 経由で通信できるように既存のポッドを準備しました。このガイドの手順IPN 接続のためのポッドの準備 （127 ページ）を参照してください。
- IPN に接続するスパイン スイッチが、ポッド内にある少なくとも 1 個のリーフ スイッチにも接続することを確認しました。
- トンネル エンドポイント（TEP）プールを作成しました。このガイドの手順IPN 接続のためのポッドの準備 （127 ページ）を参照してください。

手順

ステップ 1 Cisco Application Policy Infrastructure Controller（APIC）にログインします。

ステップ 2 次のいずれかを実行します。

- 手順「IPN 接続のためのポッドの準備 （127 ページ）」を完了して、まだ [Configure Interpod Connectivity] ダイアログボックスを閉じていない場合は、ステップ 3 ～ 5 を省略し、この手順のステップ 6 から再開します。
- 手順「IPN 接続のためのポッドの準備 （127 ページ）」を完了して、すでに [Configure Interpod Connectivity] ダイアログボックスを閉じた場合は、この手順のステップ 3 に進みます。

ステップ 3 **[Fabric]** > **[Inventory]** を選択します。

ステップ 4 [Quick Start] をクリックし、[Add Pod] をクリックします。

ステップ 5 作業ペインで、[Add Pod] をクリックします。

ステップ 6 [Add Physical Pod STEP 2 > Pod Fabric] ダイアログボックスで、次の手順を実行します。

a) [ポッド ID（Pod ID）] フィールドで、ポッド ID を選択します。

ポッド ID には任意の正の整数を指定できます。ただし、Cisco ACI ファブリック内で一意である必要があります。

b) [Pod TEP Pool] フィールドで、プール アドレスとサブネットを入力します。

ポッド TEP プールは、トラフィックのカプセル化識別子の範囲を表します。共有リソースであり、複数のドメインが使用できます。

c) [Spine ID] セレクタを使用して、スパイン ID を選択します。

複数のスパイン ID を選択するには [+]（プラス記号）アイコンをクリックします。

d) [Interfaces] 領域の [Interface] フィールドで、IPN への接続に使用されるスパイン スイッチ インターフェイス（スロットおよびポート）を入力します。

e) [IPv4 Address] フィールドに、インターフェイスの IPv4 ゲートウェイ アドレスとネットワーク マスクを入力します。

f) [MTU（bytes）] フィールドで、外部ネットワークの最大伝送ユニット（MTU）の値を選択します。

[+]（プラス記号）アイコンをクリックすると、もう 1 つのインターフェイスを設定できます。

ステップ 7 [Add Physical Pod STEP 3 > External TEP] ダイアログボックスで、次の手順を実行します。

a) [Use Defaults] チェックボックスをオンまたはオフのままにして、外部 TEP プールを設定するためのオプション フィールドを表示します。

b) [Pod] フィールドと [Internal TEP Pool] フィールドの値はすでに設定済みであることがわかります。

c) [External TEP Pool] フィールドに、物理ポッドの外部 TEP プールを入力します。

外部 TEP プールは内部 TEP プールと重ならないようにする必要があります。

d) [Dataplane TEP IP] フィールドに、ポッド間のトラフィックのルーティングに使用されるアドレスを入力します。

e) （オプション）[Unicast TEP IP] フィールドに、ユニキャスト TEP IP アドレスを入力します。

Cisco APIC によって、データ プレーン TEP IP アドレスを入力するときにユニキャスト TEP IP アドレスが自動的に設定されます。

f) （オプション）[Node] フィールドの値は設定できないことに注意してください。

g) （オプション）[Router ID] フィールドに、IPN ルータ IP アドレスを入力します。

Cisco APIC によって、データ プレーン TEP アドレスを入力するときにルータ IP アドレスが自動的に設定されます。

h) [Loopback Address] フィールドに、ルータ ループバック IP アドレスを入力します。

ルータ IP アドレスを使用する場合は、[Loopback Address] は空白のままにします。

i) **[完了（Finish）]** をクリックします。

Cisco Nexus 9000 シリーズ スイッチでのマルチポッド IPN 設定の例

Cisco APIC リリース 5.2(3) よりも前のリリースでは、IPN アンダーレイ プロトコルは OSPF です。Cisco APIC リリース 5.2(3) 以降、IPN アンダーレイ プロトコルは OSPF または BGP（eBGP のみ）になることが可能です。

（注）
- ポッド間接続用の IPN での専用 VRF の展開はオプションですが、ベスト プラクティスとして推奨されます。代わりにグローバル ルーティング ドメインを使用することもできます。
- ip dhcp relay address 10.0.0.1 を示す設定例の領域では、この設定は Pod 1 の TEP プールが 10.0.0.0/x であるという前提に基づいています。

OSPF アンダーレイ プロトコルを使用した IPN の設定例

```
  (pod1-spine1)-----2/7[ IPN-N9K ]2/9-----(pod2-spine1)


feature dhcp
feature pim

service dhcp
ip dhcp relay
ip pim ssm range 232.0.0.0/8

# Create a new VRF for Multipod.
vrf context fabric-mpod
  ip pim rp-address 12.1.1.1 group-list 225.0.0.0/15 bidir
  ip pim rp-address 12.1.1.1 group-list 239.255.255.240/28 bidir
```

```
  ip pim ssm range 232.0.0.0/8

interface Ethernet2/7
  no switchport
  mtu 9150
  no shutdown

interface Ethernet2/7.4
  description pod1-spine1
  mtu 9150
  encapsulation dot1q 4
  vrf member fabric-mpod
  ip address 201.1.2.2/30
  ip router ospf a1 area 0.0.0.0
  ip pim sparse-mode
  ip dhcp relay address 10.0.0.1
  ip dhcp relay address 10.0.0.2
  ip dhcp relay address 10.0.0.3
  no shutdown


interface Ethernet2/9
  no switchport
  mtu 9150
  no shutdown

interface Ethernet2/9.4
  description to pod2-spine1
  mtu 9150
  encapsulation dot1q 4
  vrf member fabric-mpod
  ip address 203.1.2.2/30
  ip router ospf a1 area 0.0.0.0
  ip pim sparse-mode
  ip dhcp relay address 10.0.0.1
  ip dhcp relay address 10.0.0.2
  ip dhcp relay address 10.0.0.3
  no shutdown

interface loopback29
  vrf member fabric-mpod
  ip address 12.1.1.1/32

router ospf a1
  vrf fabric-mpod
    router-id 29.29.29.29
```

BGP アンダーレイ プロトコルを使用した IPN の設定例

Cisco APIC リリース 5.2(3) 以降、IPN アンダーレイ プロトコルは OSPF ではなく BGP になることが可能です。次の設定を前の例に追加し、OSPF 設定を削除できます。

```
router bgp 200
  router-id 29.29.29.29
  vrf fabric-mpod
  address-family ipv4 unicast
neighbor 201.1.2.3
  remote-as 65000
  address-family ipv4 unicast
  disable-peer-as-check
```

```
neighbor 203.1.2.3
  remote-as 65000
  address-family ipv4 unicast
  disable-peer-as-check
```

APIC を 1 つのポッドから別のポッドに移動する

マルチポッドのセットアップにおいて、APIC をあるポッドから別のポッドに移動するには、次の手順に従います。

手順

ステップ 1 クラスタ内の APIC をデコミッションします。

a) メニューバーで、 **System** > **Controllers** を選択します。

b) **Navigation** ウィンドウで、 **Controllers** > **apic_controller_name** > **Cluster as Seen by Node** を展開します。

c) **Navigation** ウィンドウで、**apic_controller_name** をクリックします。これは、クラスタ内のものですが、デコミッションしているコントローラではありません。

d) 継続する前に、**Work** ウィンドウで、クラスタの **Health State** (**Active Controllers** サマリテーブルに示されているもの) が **Fully Fit** になっていることを確認します。

e) **Work** ウィンドウで、**Actions** > **Decommission** をクリックします。

f) **Yes** をクリックします。
解放されたコントローラは [Operational State] 列に [Unregistered] と表示されます。コントローラは稼動対象外になり、**Work** ウィンドウには表示されなくなります。

ステップ 2 デコミッションされた APIC を目的のポッドに移動します。

ステップ 3 次のコマンドを入力して、APIC をリブートします。

```
apic1# acidiag touch setup
apic1# acidiag reboot
```

ステップ 4 APIC セットアップ スクリプトで、APIC ノードが移動されたポッド ID を指定します。

a) Cisco Integrated Management Controller (CIMC) にログインします。

b) ポッド ID のプロンプトで、ポッド ID を入力します。

（注） **TEP Pool** のアドレス情報は変更しないでください。

ステップ 5 APIC をリコミッションします。

a) メニュー バーで、 **SYSTEM** > **Controllers** を選択します。

b) **Navigation** ウィンドウで、 **Controllers** > **apic_controller_name** > **Cluster as Seen by Node** を展開します。

c) 継続する前に、**Work** ウィンドウで、**Active Controllers** サマリ テーブルのクラスタの **Health State** が **Fully Fit** になっていることを確認します。

d) **Work** ウィンドウで、**Unregistered** と **Operational State** カラムに表示されている、デコミッションされたコントローラをクリックします。
e) **Work** ウィンドウで、**Actions** > **Commission** をクリックします。
f) **Confirmation** ダイアログボックスで **Yes** をクリックします。
g) コミッションされた Cisco APIC コントローラが動作状態であり、ヘルス ステータスが、**Fully Fit** であることを確認します。

OSPF IPN アンダーレイから BGP IPN アンダーレイへの移行

Cisco APIC リリース 5.2(3) 以降、IPN アンダーレイ プロトコルは OSPF または BGP になることが可能です。ポッドを OSPF アンダーレイの使用から BGP アンダーレイに移行するには、既存の IPN 接続 L3Out の下の論理インターフェイス プロファイルに BGP インターフェイスを追加します。そのインターフェイスが実行中の BGP ピアに正常に接続されたら、OSPF インターフェイス プロファイルを削除できます。

（注） OSPF と BGP の両方が Multi-Pod、Multi-Site、またはリモート リーフのアンダーレイで使用されている場合、 IPN ルータの OSPF から router-id を BGP に再配布しないでください。そうすると、ルーティング ループが生じ、スパイン スイッチと IPN ルータの間の OSPF と BGP セッションを停止してしまいます。

（注） アンダーレイ プロトコルの移行は中断を伴うアクションであり、メンテナンス期間中にのみ実行する必要があります。

手順

ステップ 1 APIC 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）] > [L3Outs] > [使用する *IPN L3Out*（*your IPN L3Out*）]**に移動します。ここで、**[使用する *IPN L3Out*（*your IPN L3Out*）]** は IPN に接続する L3Out です。

ステップ 2 [Navigation] ペインで、**[使用する *IPN L3Out*（*your IPN L3Out*）]** を展開し **[論理ノード プロファイル（Logical Node Profiles）] > [使用する *IPN* ノード プロファイル（*your IPN node profile*）] > [論理インターフェイス プロファイル（Logical Interface Profiles）] > [使用する *IPN* インターフェイス（*your IPN interface*）]**に移動します。ここで **[使用する *IPN* インターフェイス（*your IPN interface*）]** は現在の IPN 接続の論理インターフェイス プロファイルです。

[論理インターフェイス プロファイル（Logical Interface Profile）] テーブルが作業ペインに表示されます。

ステップ 3 作業ウィンドウで、[ポリシー（Policy）] タブをクリックし、[ポリシー（Policy）] タブの下にある [ルーテッド サブインターフェイス（Routed Sub-Interfaces）] タブをクリックします。

ステップ 4 [ルーテッドサブインターフェイス（Routed Sub-Interfaces）] テーブルで、現在の IPN 接続のインターフェイスをダブルクリックします。

[ルーテッドサブインターフェイス（Routed Sub-Interface）] ダイアログ ボックスが開きます。

ステップ 5 [**ルーテッド サブインターフェイス（Routed Sub-Interface**）] ダイアログ ボックスで、次の操作を実行します:

a) [BGPピア接続プロファイル（BGP Peer Connectivity Profiles）] バーの [+] アイコンをクリックして、BGP ピア接続を追加します。

[**ピア接続プロファイルの作成（Create Peer Connectivity Profiles**）] ダイアログ ボックスが開きます。

b) [**ピア IPv4 アドレス（Peer IPv4 Address**）] フィールドで、BGP ピアの IP アドレスを入力します。

c) BGP ピア接続に必要なその他の設定を行います。

（注） 移行を設定しているが、実際には移行していない場合は、[管理状態（Admin State）] を [無効化（Disabled）] に設定し、移行の準備ができたらこの手順に戻ります。移行はメンテナンス期間中に行う必要があります。

d) [送信（Submit）] をクリックして、[ルーテッド サブインターフェイス（Routed Sub-Interface）] ダイアログ ボックスに戻ります。

ステップ 6 [ルーテッド サブインターフェイス（Routed Sub-Interface）] ダイアログ ボックスで、[送信（Submit）] をクリックします。

ステップ 7 [ナビゲーション（Navigation）] ペインで、**[論理ノード プロファイル（Logical Node Profiles）]** > **[使用する *IPN* ノード プロファイル（*your IPN node profile*）]** > **[設定済みノード（Configured Nodes）]** > **[使用する *IPN* ノード（*your IPN node*）]** に移動します。次の手順に従って、BGP ネイバーが UP であることを確認します。

a) **[使用する *IPN* ノード（*your IPN node*）]** を展開し、**[*VRF-overlay-1* の *BGP*（*BGP for VRF-overlay-1*）]** などの BGP エントリを見つけます。

b) [BGP] エントリを展開し、[ネイバー（Neighbors）] をクリックします。

c) [ネイバー（Neighbors）] テーブルで、[ピア IPv4 アドレス（Peer IPv4 Address）] で設定したピア IP アドレスを検索し、[状態（State）] が「established」であることを確認します。

ステップ 8 [ナビゲーション（Navigation）] ペインで、[**論理インターフェイス プロファイル（Logical Interface Profile**）] の下で現在の OSPF Interface Profile を右クリックして [**削除（Delete**）] を選択します。

（注） OSPF インターフェイス プロファイルを削除する前に、BGP ネイバーが UP であることを確認します。

ステップ 9 [ナビゲーション（Navigation）]ペインで、**[テナント（Tenants）]**>**[インフラ（infra）]**>**[ネットワーキング（Networking）]** > **[L3Outs]** > **[使用する *IPN L3Out*（*your IPN L3Out*）]**に移動します。

ステップ 10 作業ウィンドウで、[ポリシー（Policy）]タブをクリックし、[ポリシー（Policy）]タブの下の[メイン（Main）] タブをクリックします。

ステップ 11 作業ウィンドウの [BGP/EIGRP/OSPF の有効化（Enable BGP/EIGRP/OSPF）] セクションで、[OSPF] をオフにし、[BGP] をオンのままにします。

ステップ 12 [Submit] をクリックします。

マルチポッド スパイン バックツーバック について

Cisco APIC リリース 5.2(3) 以降、ACI マルチポッド アーキテクチャが拡張され、2 つのポッドのスパインをバックツーバック（「B2B」）リンクで直接接続できるようになりました。このソリューションを呼び出すと、小規模な ACI マルチポッドの導入で IPN 要件を削除できます。また、設定が必要な外部デバイスがないため、運用の簡素化とエンドツーエンドのファブリックの可視性も実現します。マルチポッド スパイン バックツーバックマルチポッド スパイン バックツーバック

トポロジでは、バックツーバック スパイン リンク インターフェイスがインフラ テナントの L3Out として実装されます。マルチポッドスパインバックツーバックこれらのリンクは通常、ポッド間の直接ケーブル接続またはダーク ファイバ接続で伝送されます。は、異なるポッドに属するスパイン スイッチ間の Open Shortest Path First（OSPF）接続のみをサポートします。マルチポッド スパイン バックツーバック

次の図は、Pod1 と Pod2 の間にバックツーバック スパインが接続された、2 つの可能な マルチポッド スパイン バックツーバックトポロジを示しています。最初の図は、Pod1 スパインと Pod2 スパイン間のフル メッシュ相互接続を使用した推奨トポロジを示しています。ポッド間のよりシンプルな相互接続を示す 2 番目の図もサポートされています。

図 *12* : 推奨フルメッシュ相互接続

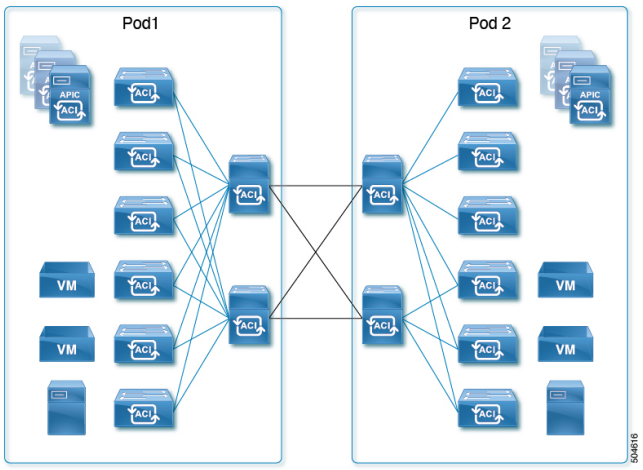
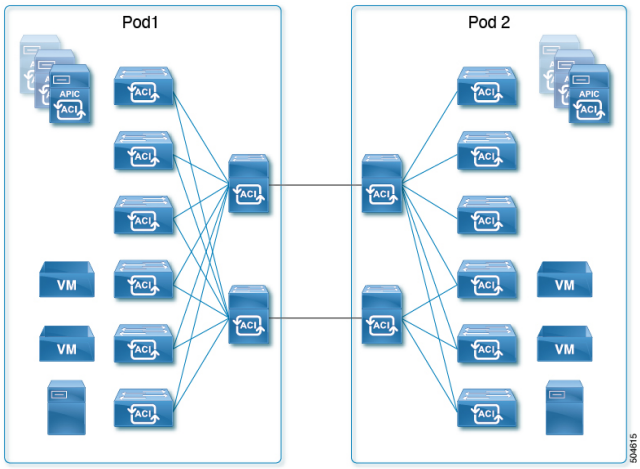


図 *13 :* シンプルな相互接続



詳細については、シスコのナレッジベース記事「Cisco ACI Multi-Podスパイン バックツーバック」を参照してください。マルチポッド スパイン バックツーバックhttps://www.cisco.com/c/en/us/td/docs/dcn/aci/apic/kb/cisco-multipod-b2b.html

マルチサイトとマルチポッドのトラブルシューティング

このセクションでは、マルチサイトおよびマルチポッドをトラブルシューティングする方法を説明します。

エラー：400

次のエラーが表示される場合

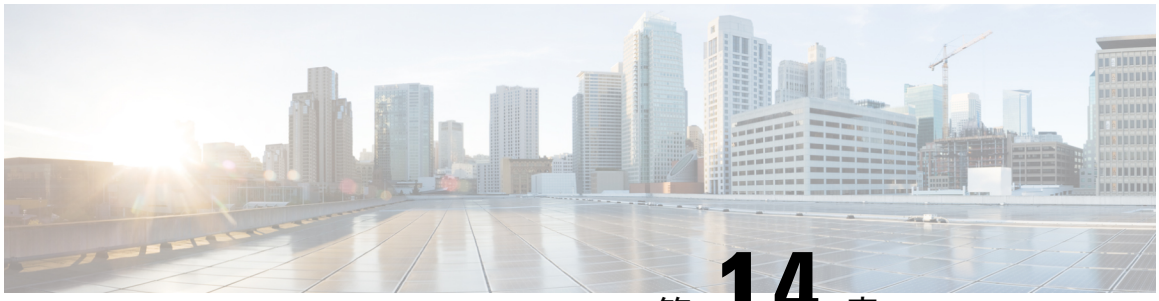
```
Error:400 - Invalid Configuration Following Intersite Spines are not configured as Mpod
 Spines: 1202
```

既存のすべてのスパインに対してファブリック外部接続を有効にする必要があります。新しいスパインを追加する場合は、**Setup Multipod** GUI ウィザードを使用します。

この問題を解決するには 2 つの方法があります。

- 外部ルーティング ネットワークの下ですべてのスパインを有効にします。
  - APIC GUI のメニュー バーで、**[テナント（Teant）]** > **[インフラ（infra）]** をクリックします。
  - **[Navigation（ナビゲーション）]** ペインで、**[ネットワーキング（Networking）]** > **[外部ルーテッド ネットワーク（External Routed Networks）]**を展開し、外部ルーテッド ネットワークを右クリックして、**[ファブリック外部接続を有効にする（Enable Fabric External Connectivity）]** を選択します。
- 外部ルーテッド ネットワークの下に新しいスパインを追加します。
  - APIC GUI のメニュー バーで、**[ファブリック（Fabric）]** をクリックします。

- **[ナビゲーション（Navigation）]** ペインで、**[クイック スタート（Quick Start）]** > **[ノードまたはポッド セットアップ（Node or Pod Setup）]** > **[マルチポッドのセットアップ（Setup Multipod）]** を展開し、マルチポッド セットアップを完了します。



第 14 章

リモート リーフ スイッチ

この章は、次の内容で構成されています。

ACI ファブリックのリモート リーフ スイッチについて

ACI ファブリックの展開では、ローカルスパインスイッチまたは APIC が接続されていない Cisco ACI リーフスイッチのリモートデータセンタに、ACI サービスと APIC 管理を拡張できます。

リモート リーフ スイッチがファブリックの既存のポッドに追加されます。メインデータセンターに展開されるすべてのポリシーはリモートスイッチで展開され、ポッドに属するローカルリーフスイッチのように動作します。このトポロジでは、すべてのユニキャストトラフィックはレイヤ 3 上の VXLAN を経由します。レイヤ 2 ブロードキャスト、不明なユニキャスト、マルチキャスト（BUM）メッセージは、WAN を使用するレイヤ 3 マルチキャスト（bidirectional PIM）を使用することなく、 Head End Replication（HER）トンネルを使用して送信されます。スパイン スイッチ プロキシを使用する必要があるすべてのトラフィックは、メイン データセンターに転送されます。

APIC システムは、起動時にリモート リーフ スイッチを検出します。その時点から、ファブリックの一部として APIC で管理できます。

（注）
- すべての inter-VRF トラフィック（リリース 4.0(1) 以前）は、転送される前にスパイン スイッチに移動します。
- リリース 4.1(2) 以前では、リモート リーフを解除する前に、vPC を最初に削除する必要があります。

リリース 4.0(1) でのリモート リーフ スイッチの動作の特性

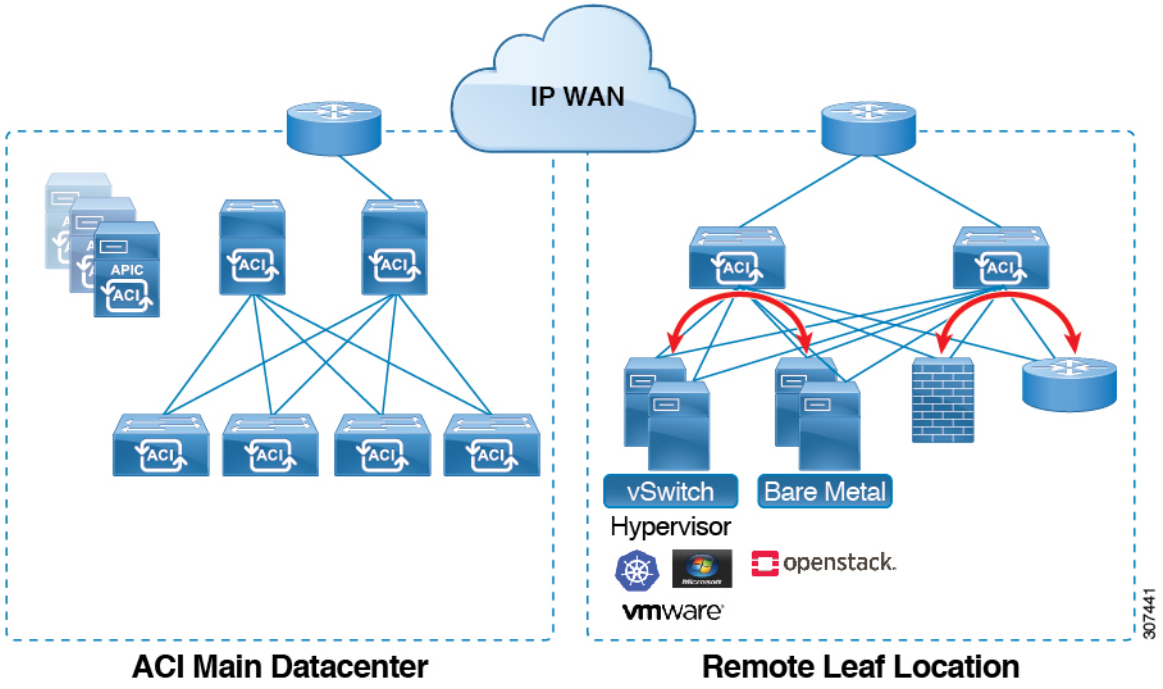
リリース 4.0(1) 以降、リモート リーフ スイッチの動作には次の特徴があります。

- spine-proxy からサービスを切り離すことによって WAN 帯域幅の使用量を削減します。
  - PBR：ローカル PBR デバイスまたは vPC の背後にある PBR デバイスでは、ローカル スイッチングはスパイン プロキシに移動せずに使用されます。ピア リモート リーフ上の孤立ポートの PBR デバイスでは、RL-vPC トンネルを使用します。これは、主要 DC へのスパイン リンクが機能しているか否かを問わず該当します。
  - ERSPAN：ピア接続先 EPG では、RL-vPC トンネルが使用されます。ローカルな孤立ポートまたは vPC ポート上の EPG は、宛先 EPG へのローカル スイッチングを使用します。これは、主要 DC へのスパイン リンクが機能しているか否かを問わず該当します。
  - 共有サービス：パケットはスパイン プロキシ パスを使用しないため WAN 帯域幅の使用量を削減します。
  - Inter-VRF トラフィックは上流に位置するルータ経由で転送され、スパインには配置されません。
  - この機能強化は、リモート リーフ vPC ペアにのみ適用されます。リモート リーフ ペアを介した通信では、スパイン プロキシは引き続き使用されます。
- spine-proxy に到達不能な場合のリモート リーフ ロケーション内の（ToR グリーニング プロセスを通じた）不明な L3 エンドポイントの解像度。

リリース4.1(2) でのリモート リーフ スイッチ動作の特性

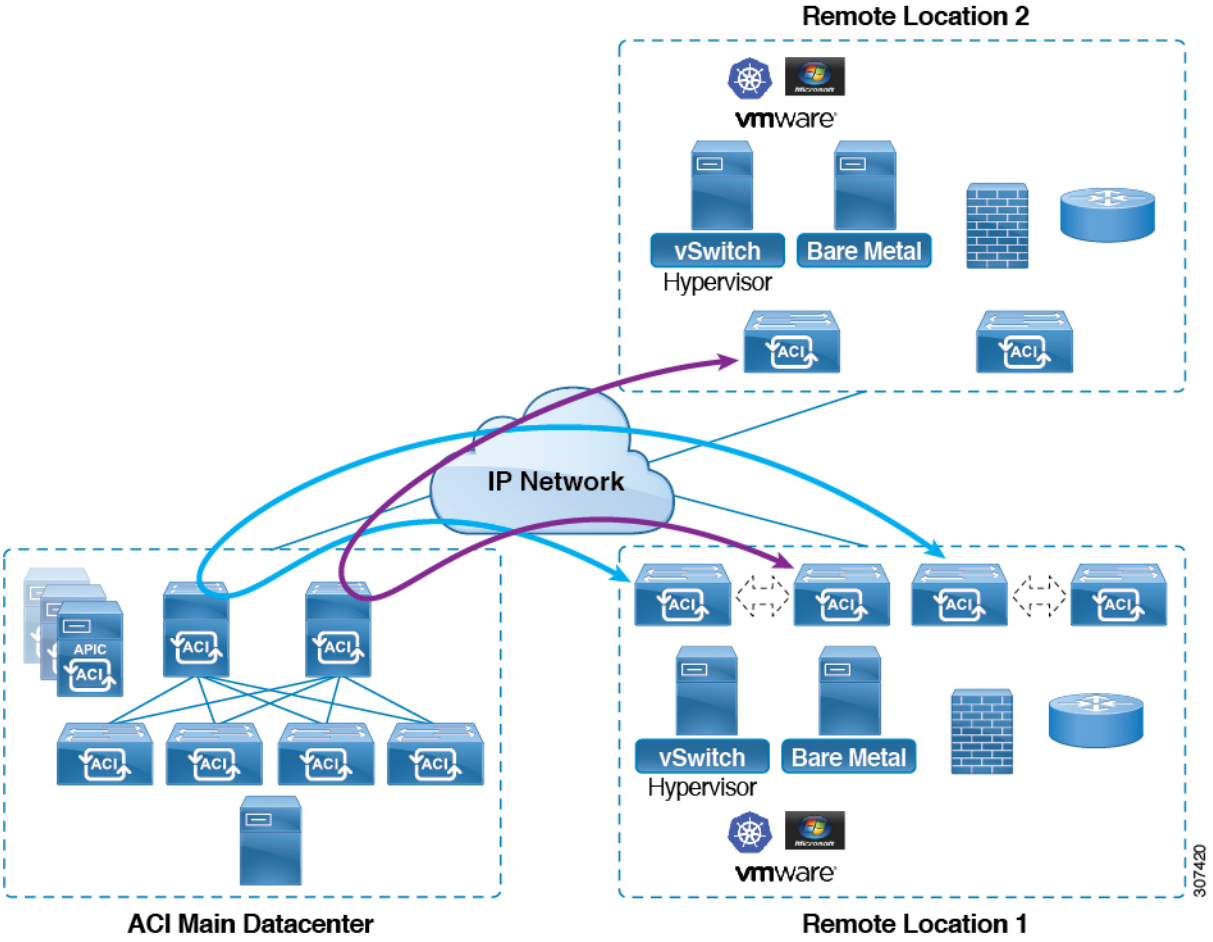
リリース4.1(2) よりも前のリリースでは、次の図に示すように、リモートリーフロケーション上のすべてのローカル スイッチング（リモート リーフ vPC ピア内）トラフィックは、物理的または仮想的にエンドポイント間で直接スイッチングされます。

図 *14 : Local Switching Traffic* : リリース *4.1(2)* 以前



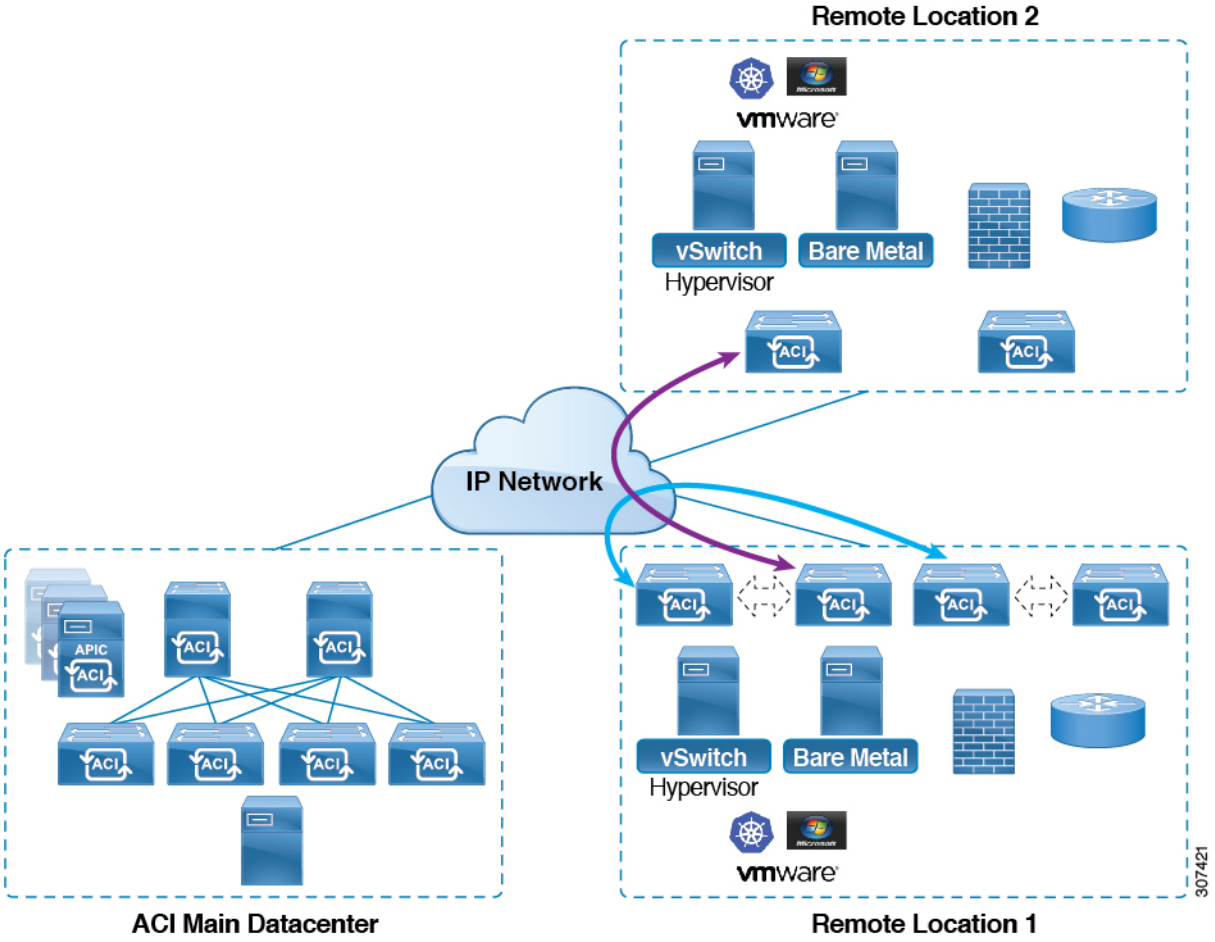
さらに、リリース4.1(2)よりも前では、次の図に示すように、リモートロケーション内またはリモート ロケーション間のリモート リーフ スイッチ vPC ペア間のトラフィックは、ACI メイン データ センター ポッドのスパイン スイッチに転送されます。

図 *15 : Remote Switching Traffic* : リリース *4.1(2)* より以前



リリース 4.1(2) 以降では、異なるリモート ロケーションにあるリモート リーフ スイッチ間の直接トラフィック転送がサポートされるようになりました。この機能は、次の図に示すように、リモート ロケーション間の接続に一定レベルの冗長性と可用性を提供します。

図 *16 : Remote Leaf Switch Behavior* : リリース *4.1(2)*



また、リリース 4.1(2) 以降でも、リモート リーフ スイッチの動作には次の特徴があります。

- リリース 4.1(2) 以降、ダイレクト トラフィック転送では、シングル ポッド設定内でスパイン スイッチに障害が発生すると、次のようになります。
  - ローカル スイッチングは、上記の「ローカル スイッチング トラフィック：リリース 4.1(2) 以前」に示すように、リモート リーフ スイッチ vPC ピア間の既存および新規のエンドポイント トラフィックに対して機能し続けます。
  - リモート ロケーション間のリモート リーフ スイッチ間のトラフィックの場合：
    - リモート リーフ スイッチからスパイン スイッチへのトンネルがダウンするため、新しいエンドポイント トラフィックは失敗します。リモート リーフ スイッチから、新しいエンドポイントの詳細はスパイン スイッチに同期されないため、同じまたは異なる場所にある他のリモート リーフ スイッチ ペアは、COOP から新しいエンドポイント情報をダウンロードできません。
    - 単方向トラフィックの場合、既存のリモートエンドポイントは300秒後にエージングアウトするため、そのポイント以降のトラフィックは失敗します。ポッド内

のリモート リーフ サイト内（リモート リーフ VPC ペア間）の双方向トラフィックは更新され、引き続き機能します。リモート ロケーション（リモート リーフ スイッチ）への双方向トラフィックは、900 秒のタイムアウト後に COOP によってリモートエンドポイントが期限切れになるため、影響を受けることに注意してください。

- 共有サービス（VRF 間）の場合、同じポッド内の 2 つの異なるリモート ロケーションに接続されたリモート リーフ スイッチに属するエンドポイント間の双方向トラフィックは、リモート リーフ スイッチ COOP エンドポイントのエージアウト時間（900秒）後に失敗します。これは、リモートリーフスイッチからスパインへの COOP セッションがこの状況でダウンするためです。ただし、2 つの異なるポッドに接続されたリモート リーフ スイッチに属するエンドポイント間の共有サービス トラフィックは、COOP 高速エージング タイムである 30 秒後に失敗します。
- スパイン スイッチへの BGP セッションがダウンするため、L3Out 間通信は続行できません。

- トラフィックが 1 つのリモート リーフ スイッチから送信され、別のリモート リーフ スイッチ（送信元の vPC ピアではない）に送信されるリモート リーフ直接単方向トラフィックがある場合は、300 秒のリモート エンド ポイント（XR EP）タイムアウトが発生するたびに、ミリ秒単位のトラフィック損失が発生します。
- ACI Multi-Site 設定を使用したリモート リーフ スイッチでは、スパイン スイッチに障害が発生しても、リモート リーフ スイッチから他のポッドおよびリモート ロケーションへのすべてのトラフィックが継続します。これは、この状況ではトラフィックが代替の使用可能なポッドを通過するためです。

リモート リーフ スイッチの IPN での 10 Mbps 帯域幅のサポート

リモート リーフ スイッチからのデータ トラフィックのほとんどがローカルで、ポッド間ネットワーク（IPN）が管理目的でのみ必要な場合があります。このような状況では、100 Mbps の IPN は必要ない場合があります。これらの環境をサポートするために、リリース 4.2(4) 以降、IPN の最小帯域幅として 10 Mbps のサポートが利用可能になりました。

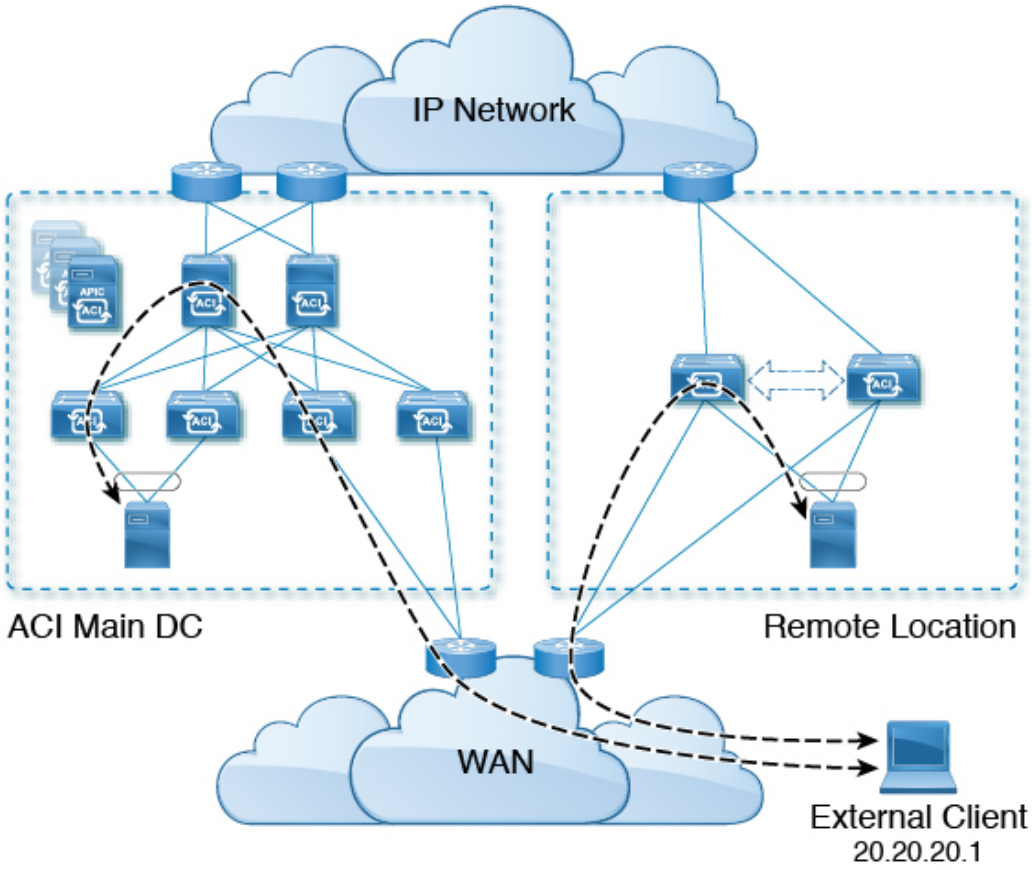
これをサポートするには、次の要件を満たす必要があります。

- IPN パスは、リモート リーフ スイッチ（アップグレードおよびダウングレード、ディスカバリ、COOP、ポリシー プッシュなどの管理機能）の管理にのみ使用されます。
- 「Cisco APIC GUI を使用した DSCP 変換ポリシーの作成」の項に記載されている情報に基づいて、Cisco ACI データセンターとリモート リーフ スイッチ ペア間のコントロールおよび管理プレーン トラフィックに優先順位を付けるために、QoS 設定を使用して IPN を設定します。
- データセンターおよびリモート リーフ スイッチからのすべてのトラフィックは、ローカル L3Out を経由します。Cisco ACI

- EPG またはブリッジ ドメインは、リモート リーフ スイッチと ACI メイン データセンター間で拡張されません。
- アップグレード時間を短縮するには、リモート リーフ スイッチにソフトウェア イメージを事前にダウンロードする必要があります。

次の図に、この機能のグラフィカル表示を示します。

図 *17*: リモート リーフ スイッチ動作（リリース *4.2(4)*）：*IPN* でのリモート リーフ スイッチの管理

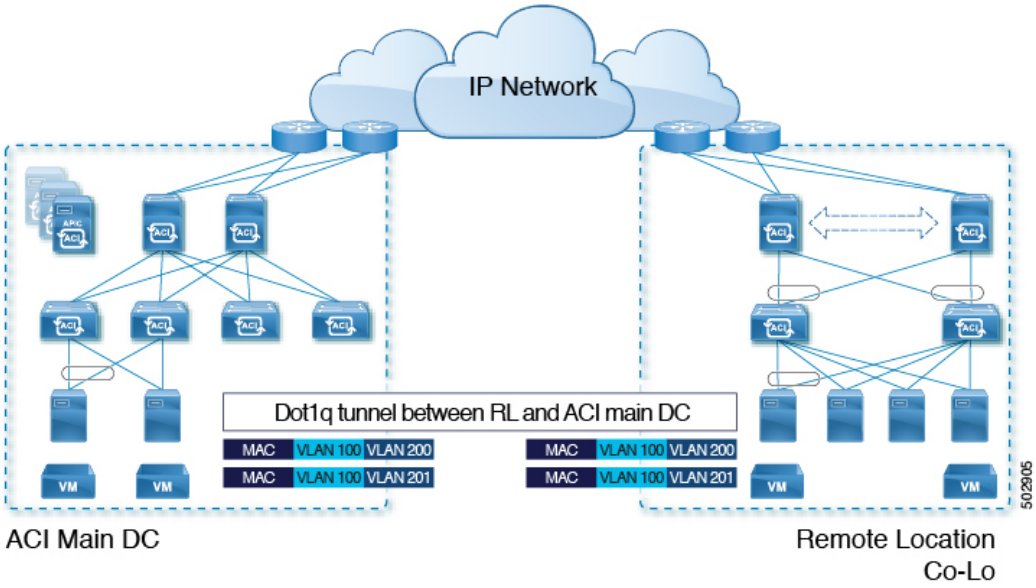


リモート リーフ スイッチでの Dot1q トンネルのサポート

状況によっては、コロケーションプロバイダーが複数のカスタマーをホストしており、各カスタマーがリモート リーフ スイッチ ペアごとに数千の VLAN を使用している場合があります。リリース 4.2(4) 以降では、リモート リーフ スイッチと ACI メイン データセンター間に 802.1Q トンネルを作成するためのサポートを利用できます。これにより、複数の VLAN を単一の 802.1Q トンネルに柔軟にマッピングできるため、EPG の拡張要件が軽減されます。

次の図に、この機能のグラフィカル表示を示します。

図 *18 :* リモート リーフ スイッチの動作、リリース *4.2*（*4*）：リモート リーフ スイッチでの *802.1Q* トンネル サポート



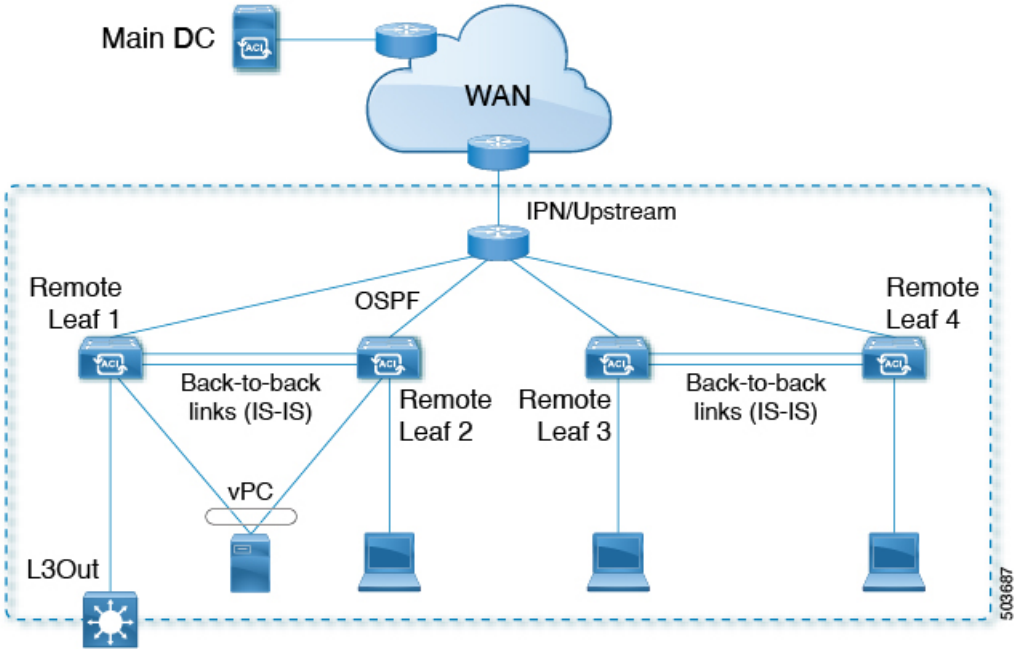
Cisco APIC ドキュメンテーションのランディング ページにある『Cisco APIC Layer 2 Networking Configuration Guide』の「802.1Q Tunnels」の章に記載されている手順を使用して、リモート リーフ スイッチと ACI メイン データセンター間にこの 802.1Q トンネルを作成します。
https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

ウィザードを使用するか（使用しない場合も）、REST API または NX-OS スタイル CLI を使用して、APIC GUI のリモート リーフ スイッチを設定できます。

リモート リーフ バックツーバック接続について

Cisco APIC リリース 5.2(1) 以降では、ファブリック リンクによってリモート リーフ スイッチ ペアを相互に直接接続（「バックツーバック」）して、ローカルの東西トラフィックを伝送できます。重要な東西データ トラフィックのシナリオの例は、次の図に示すように、vPC ペアの EPG から L3Out へのユニキャスト トラフィックです。

図 *19* : リモート リーフ バックツーバック接続



非 vPC 接続ホスト間のトラフィックのみがバックツーバック リンクを通過します。vPC に接続されたホストは、宛先に最も近いリモート リーフ スイッチからローカルにトラフィックを送信できるため、このようなトラフィックはバックツーバック リンクを使用しません。

リモート リーフ スイッチのペア間でアップリンクとバックツーバック接続がアクティブな場合、バックツーバック リンクが東西トラフィックに優先されますが、アップリンクは、主要なデータ センターにある他のリモート リーフ スイッチおよびスイッチとの間でトラフィックを伝送します。

リモートリーフアーキテクチャでは、通常、隣接するリモートリーフスイッチ間でトラフィックをルーティングするためにスパイン スイッチまたは IPN ルータが必要ですが、直接バックツーバック リーフ接続を使用すると、アップストリーム デバイスの帯域幅を節約できます。

リモート リーフ バックツーバック接続のガイドラインと制限事項

- リモート リーフ スイッチ間のバックツーバック リンクは、中間デバイスのない直接リンクである必要があります。
- バックツーバック接続では、ファブリック ポートまたはファブリック ポートに変換された前面パネル ポートを使用できます。
- リモート リーフ スイッチは、ペアでのみバックツーバック リンクで接続できます。バックツーバック リンクによる 3 つ以上のリモート リーフ スイッチの相互接続はサポートされていません。
- リモート リーフ スイッチのペアがバックツーバックで接続され、ペアの 1 つがアップリンク接続を失った場合、同じリモート リーフ スイッチは、バックツーバック リンクを介

して他のリモート リーフ スイッチ経由で到達可能になります。この場合、メイン データセンターからのトラフィックもバックツーバック リンクで伝送されます。

- PTP および SyncE は、バックツーバック リンクではサポートされません。

リモート リーフ バックツーバック接続の展開

Cisco APIC リリース 5.2(1) よりも前のリリースでは、リモート リーフ スイッチ ファブリック ポート間のバックツーバック接続により、配線エラーが発生しました。Cisco APIC リリース 5.2(1) では、次のいずれかの状況でこのような接続が自動的に認識されます。

- 2 つのリモート リーフ vPC ピア間で接続が確立されます。
- 接続は、単一のリモート ロケーションにある vPC のメンバーではないリモート リーフ スイッチ間で行われます。

このような場合、特別な設定は必要ありません。

リモート リーフ スイッチのハードウェアの要件

リモート リーフ スイッチの機能には、次のスイッチがサポートされています。

ファブリック スパイン スイッチ

WAN ルータに接続される Cisco Application Centric Infrastructure（ACI）メイン データ センターでのスパイン スイッチとしては、次のスパイン スイッチがサポートされています。

- 固定スパイン スイッチ Cisco Nexus 9000 シリーズ
  - N9K-C9332C
  - N9K-C9364C
  - すべての GX および GX2 スイッチ
- モジュラー スパイン スイッチとしては、EX 以降で終了する名前の Cisco Nexus 9000 シリーズ スイッチのみがサポートされます（たとえば N9K-X9732C- EX ）。
- 古い世代のスパイン スイッチ、たとえば固定スパイン スイッチ N9K-C9336PQ や、N9K X9736PQ ライン カードを搭載したモジュラー スパイン スイッチなどは、メイン データセンターではサポートされますが、WAN への接続がサポートされるのは次世代のスパイン スイッチのみです。

リモートのリーフ スイッチ

- リモートのリーフ スイッチ、後で (たとえば N9K-C93180LC-EX) EX で終了する名前と Cisco Nexus 9000 シリーズ スイッチのみがサポートされています。

- リモートのリーフ スイッチする必要がありますにイメージを実行する、スイッチ 13.1.x 以降 (aci n9000 dk9.13.1.x.x.bin) 検出できる前にします。これにより、リーフ スイッチでの手動アップグレードが必要があります。

リモート リーフ スイッチの制約事項と制限事項

リモート リーフには、次の注意事項および制約事項が適用されます。

- リモート リーフ ソリューションでは、リモート リーフ スイッチとメイン データ センターのリーフ/スパイン スイッチの /32 トンネル エンド ポイント（TEP）IP アドレスが、要約なしでメイン データ センターとリモート リーフ スイッチ間でアドバタイズされる必要があります。
- リモート リーフ スイッチを同じポッド内の別のサイトに移動し、新しいサイトに元のサイトと同じノード ID がある場合は、仮想ポート チャネル（vPC）を削除して再作成する必要があります。
- Cisco N9K-C9348GC-FXP スイッチでは、ポート 1/53 または 1/54 でのみ最初のリモート リーフスイッチディスカバリを実行できます。その後、リモート リーフスイッチの ISN/IPN へのファブリック アップリンクに他のポートを使用できます。

ここでは、リモート リーフ スイッチでサポートされるものとサポートされないものについて説明します。

- Supported Features （151 ページ）
- サポートされない機能 （152 ページ）
- リリース 5.0(1) の変更点 （154 ページ）
- リリース 5.2(3) での変更点 （154 ページ）

Supported Features

vPC リモート リーフスイッチ ペア内の L3Out SVI のストレッチがサポートされています。

Cisco APIC リリース 4.2(4) 以降、802.1Q（Dot1q）トンネル機能がサポートされています。

Cisco APIC リリース 4.1(2) 以降、次の機能がサポートされています。

- ACI Multi-Site を使用したリモート リーフ スイッチ
- 同じリモート データ センター内の 2 つのリモート リーフ vPC ペア間またはデータ センター間でのトラフィック転送（これらのリモート リーフ ペアが同じポッドまたは同じマルチポッド ファブリックの一部であるポッドに関連付けられている場合）
- 主要な Cisco ACI データ センター ポッドが 2 つのリモート ロケーションの間の中継である場合、リモート ロケーションでの L3Out の中継（RL `location-1`の L3Out と RL`location-2` の L3Out がそれぞれのプレフィックスをアドバタイズしている）

Cisco APIC リリース 4.0(1) 以降、次の機能がサポートされています。

- Epg の Q-で-Q カプセル化のマッピング
- リモート リーフ スイッチでの PBR トラッキング（システムレベルのグローバル GIPo が有効になっている場合）
- PBR の復元力のあるハッシュ
- Netflow
- MacSec の暗号化
- ウィザードのトラブルシューティング
- アトミック カウンタ

サポートされない機能

このリリースで、サポート対象外の次の機能を除き、ファブリックおよびテナントの完全なポリシーがリモート リーフ スイッチでサポートされています。

- GOLF
- vPod
- フローティング L3Out
- ローカル リーフ スイッチ（ACI 主要データ センター スイッチ）とリモート リーフ スイッチ間の L3out SVI のストレッチ、または 2 つの異なるリモート リーフ スイッチの vPC ペア間のストレッチ
- コピー サービスは、ローカル リーフ スイッチに導入されている場合、および送信元または宛先がリモート リーフ スイッチにある場合はサポートされません。この状況では、ルーティング可能な TEP IP アドレスはローカル リーフ スイッチに割り当てられません。詳細については、『APIC ドキュメンテーション ページ』で入手可能な『Cisco APIC Layer 4 to Layer 7 Services Deployment Guide』の「Configuring Copy Services」の章の「Copy Services Limitations」を参照してください。https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html
- レイヤ 2 (スタティック Epg) を除く接続外部
- VzAny 契約とサービスをコピーします。
- リモートのリーフ スイッチの FCoE 接続
- ブリッジ ドメインまたは Epg のカプセル化をフラッディングします。
- Fast Link Failover ポリシーは、リーフ スイッチとスパイン スイッチ間の ACI ファブリック リンク用であり、リモート リーフ接続には適用されません。リモート リーフ接続のコンバージェンスを高速化するために、Cisco APICリリース 5.2(1) で代替方法が導入されています。

- 遠隔地での管理対象のサービス グラフに接続されたデバイス
- トラフィック ストーム制御
- Cloud Sec 暗号化
- ファーストホップ セキュリティ
- レイヤ 3 マルチキャスト リモート リーフ スイッチ上のルーティング
- メンテナンス モード
- TEP 間アトミック カウンタ

Multi-Site アーキテクチャでリモート リーフ スイッチをサイト間 L3Out 機能と統合する場合、次のシナリオはサポートされません。

- 別々のサイトに関連付けられたリモート リーフ スイッチのペアに展開された L3Out 間のトランジット ルーティング
- リモート サイトに関連付けられたリモート リーフ スイッチのペアに展開された L3Out と通信するサイトに関連付けられたリモート リーフ スイッチのペアに接続されたエンドポイント
- リモート サイトに関連付けられたリモート リーフ スイッチのペアに展開された L3Out と通信するローカル サイトに接続されたエンドポイント
- リモート サイトに展開された L3Out と通信するサイトに関連付けられたリモート リーフ スイッチのペアに接続されたエンドポイント

（注） 異なるデータ センター サイトが同じマルチポッド ファブリックの一部としてポッドとして展開されている場合、上記の制限は適用されません。

リモート リーフ スイッチ機能では、次の導入と設定がサポートされていません。

- 特定のサイト（APIC ドメイン）に関連付けられたリモート リーフ ノードとマルチサイト展開の別のサイトのリーフ ノード部分の間でブリッジドメインを拡張することはサポートされていません（これらのリーフ ノードがローカルまたはリモート）、この制限を強調表示するために障害が APIC に生成されます。これは、Multi-Site Orchestrator（MSO）でストレッチ ブリッジドメインを構成するときに、BUM フラッディングが有効または無効であることとは無関係です。ただし、ブリッジドメインは、同じサイト（APIC ドメイン）に属するリモート リーフ ノードとローカル リーフ ノード間で常に拡張できます（BUM フラッディングを有効または無効にします）。
- リモート リーフスイッチ ロケーションおよび主要データセンター全体でのスパニング ツリープロトコル
- APIC は、リモート リーフスイッチに直接接続されます。

- vPC ドメインでの、リモート リーフスイッチ上の孤立ポート チャネルまたは物理ポート（この制限は、リリース 3.1 以降に適用します）。
- コンシューマ、プロバイダー、およびサービス ノードがすべてリモート リーフスイッチに接続されていて、vPC モードである場合、サービス ノード統合の有無に関わらず、リモート ロケーション内でのローカル トラフィック転送のみサポートされます。
- スパイン スイッチから IPN にアドバタイズされる /32 ループバックは、リモート リーフスイッチに向けて抑制/集約してはなりません。/32 ループバックは、リモート リーフスイッチにアドバタイズする必要があります。

リリース 5.0(1) の変更点

Cisco APIC リリース 5.0(1) 以降では、リモート リーフスイッチに次の変更が適用されています。

- 直接トラフィック転送機能はデフォルトでイネーブルになっており、ディセーブルにできません。
- リモート リーフ スイッチの直接トラフィック転送を使用しない設定はサポートされなくなりました。リモート リーフ スイッチがあり、Cisco リリース 5.0(1) にアップグレードする場合は、「Direct Traffic Forwardingについて」の項に記載されている情報を確認し、その項の手順を使用して直接トラフィック転送をイネーブルにします。APIC

リリース 5.2(3) での変更点

Cisco APIC リリース 5.2(3) 以降では、リモート リーフスイッチに次の変更が適用されています。

- リモート リーフ スイッチとアップストリーム ルータ間のピアへの IPN アンダーレイ プロトコルは、OSPF または BGP のいずれかです。以前のリリースでは、OSPF アンダーレイのみがサポートされています。

WAN ルータとリモート リーフ スイッチ設定の注意事項

リモート リーフが検出され APIC 管理に組み込まれる前に、WAN ルータとリモート リーフ スイッチを設定する必要があります。

次の要件に従い、ファブリック スパイン スイッチの外部インターフェイスとリモート リーフ スイッチ ポートに接続する WAN ルータを接続します。

WAN ルータ

- エリア ID、タイプ、コストなど、同じ詳細を有するインターフェイスで OSPF を有効にします。
- メイン ファブリックの各 APIC の IP アドレスにつながるインターフェイスで DHCP リレーを設定します。

- スパイン スイッチで VLAN 5 インターフェイスに接続する WAN ルータのインターフェイスは、通常のマルチポッド ネットワークに接続するインターフェイス以外に、異なる VRF に存在する必要があります。

リモート リーフ スイッチ

- ファブリック ポートの 1 つから直接接続して、アップストリーム ルータにリモート リーフ スイッチを接続します。アップストリーム ルータへの次の接続がサポートされています。
  - 40 Gbps 以上の接続
  - QSFP-SFP アダプタでは、1/10 G SFP がサポートされています

  WAN の帯域幅は、リリースによって異なります。
  - 4.2(4) 以前のリリースでは、WAN の帯域幅は最小で 100 Mbps、サポートされている最大遅延は 300 ミリ秒です。
  - 4.2(4) 以降のリリースでは、WAN の帯域幅は最小で 10 Mbps、サポートされている最大遅延は 300 ミリ秒です。
- 上記が推奨されますが、vPC とリモート リーフ スイッチのペアを接続する必要はありません。vPC の両端にあるスイッチは、同じリモートデータセンタのリモート リーフ スイッチである必要があります。
- 一意の IP アドレスを持つ VLAN 4 でレイヤ 3 サブインターフェイスとしてノース バウンド インターフェイスを設定します。

  リモートのリーフ スイッチからルータに 1 個以上のインターフェイスを接続する場合、一意の IP アドレスで各インターフェイスを設定します。
- インターフェイスで OSPF をイネーブルにしますが、OSPF エリア タイプをスタブ エリアとして設定しないでください。
- リモート リーフ スイッチ内の TEP プール サブネットの IP アドレスは、ポッド TEP サブネット プールと重複しないようにする必要があります。使用されるサブネットは /24 以下である必要があります。
- マルチポッドがサポートされますが、リモート リーフ機能は必要ありません。
- 単一ポッド ファブリックのポッドをリモート リーフ スイッチに接続するとき、スパイン スイッチから WAN ルータへ 、リモート リーフ スイッチから WAN ルータへ L3Out を設定し、これは両方ともスイッチ インターフェイスで VLAN-4 を使用します。
- マルチポッド ファブリックのポッドをリモート リーフ スイッチに接続するとき、スパイン スイッチから WAN ルータへ 、リモート リーフ スイッチから WAN ルータへ L3Out を設定し、これは両方ともスイッチ インターフェイスで VLAN-4 を使用します。また、VLAN-5 を使用してマルチポッド内部 L3Out を設定し、リモート リーフ スイッチを宛先としてポッドを通過するトラフィックをサポートします。VLAN 4 および VLAN 5 を使用

する限り、通常のマルチポッドおよびマルチポッド内部接続は、同じ物理インターフェイスで設定できます。

- マルチポッド内部L3Outを設定している場合、通常のマルチポッドL3Outとして同じルータ ID を使用しますが、ルータ ID の **[ループバック アドレスとしてルータ ID を使用する]** オプションを選択解除して、異なるループバックIPアドレスを設定します。これでECMPが機能します。
- 6.0(1) リリース以降、リモート リーフ スイッチは、サブネット マスクが最大 /28 のリモート プールをサポートします。以前のリリースでは、リモート リーフ スイッチは、サブネット マスクが最大 /24 のリモート プールをサポートしていました。リモート プールを削除できるのは、使用を停止し、そのプールを使用しているすべてのノードを含むファブリックから削除した後でのみです。

  /28 リモート TEP プールは、2 つの vPC ペアを持つ最大 4 つのリモート リーフ スイッチをサポートします。RMA の目的では、2 つの IP アドレスを未使用のままにしておくことをお勧めします。これらの 2 つの IP アドレスは、1 つのスイッチの RMA を行うのに十分です。次の表は、リモート リーフ スイッチがこれらの IP アドレスをどのように使用するかを示しています。

（注） 2 つの IP アドレスが内部ファブリックの使用に使用されます。

IP アドレスタイプ	数量
/28 プールで使用可能な使用可能な IP アドレスの合計	16 - 2 = 14
ファブリックが内部的に使用する IP アドレスの数	2
ノードで使用可能な使用可能な IP アドレスの合計	14 - 2 = 12
4 つのリモート リーフ スイッチに必要な IP アドレスの数	4 * 2 = 8
2 つの vPC ペアに必要な IP アドレスの数	2 * 1 =2
リモート プールで使用されているIPアドレスの合計	8 + 2 = 10
/28 リモート プールの空き IP アドレス	12 - 10 = 2

リモート リーフ スイッチを廃止すると、2 つの IP アドレスが解放されますが、24 時間が経過した後にのみ再利用できます。

GUI を使用してリモート リーフ スイッチのポッドとファブリック メンバーシップを設定する

IPN ルータとリモート スイッチを検出して接続するために、Cisco APIC を設定して有効にすることができます。ウィザードを使用するか、またはウィザードを使用せずに APIC GUI を使用する方法があります。

ウィザードを使用してリモートリーフスイッチのポッドとファブリック メンバーシップを設定する

IPN ルータとリモート スイッチを検出して接続するために、 Cisco APIC を設定して有効にすることができます。このトピックで説明するようにウィザードを使用して、または APIC GUI を使用する代替の方法で行えます。「GUI を使用してリモート リーフ スイッチのポッドとファブリック メンバーシップを設定する (ウィザードは使用しない)（165 ページ）」を参照してください。

始める前に

- IPN と WAN ルータとリモートのリーフ スイッチがアクティブで設定されています。WAN ルータとリモート リーフ スイッチ設定の注意事項 （154 ページ）を参照してください。

（注） ウィザードを起動する前に、物理ポッドと IPN 間の接続を設定することを推奨します。ポッド間接続の設定については、IPN 接続のためのポッドの準備 （127 ページ）を参照してください。

- リモート リーフ スイッチ ペアは、vPC で接続されています。
- リモート リーフ スイッチは、14.1.x 以降 (aci-n9000-dk9.14.1.x.x.bin) のスイッチ イメージを実行しています。
- リモート リーフ スイッチを追加する予定のポッドが作成され、設定されています。
- ポッドをリモート リーフ スイッチに接続するために使用するスパイン スイッチは IPN ルータに接続されています。

手順

ステップ 1 メニュー バーで、**[ファブリック（Fabric）]** > **[インベントリ（Inventory）]** をクリックします。

ステップ 2 [ナビゲーション（Navigation）] ペインで、[**クイック スタート（Quick Start）** を展開し、[**リモート リーフの追加（Add Remote Leaf**）] をクリックします。

ステップ 3 ワーク ペインの [**リモート リーフ（Remote Leaf**）] ペインで、[**リモート リーフの追加（Add Remote Leaf**）] をクリックします。

[リモート リーフの追加（Add Remote Leaf）] ウィザードが表示されます。

まだポッド間接続を設定していない場合は、[**ポッド間接続の設定（Configure Interpod Connectivity**）] 画面が表示され、他のウィザード手順の順序はこの手順で説明されている順序とは異なります。この状況では、IP 接続、ルーティング プロトコル、および外部 TEP アドレスを設定します。ACI を別の場所に拡張する前に、ポッド間接続が前提条件となります。

ポッド間接続の設定については、IPN 接続のためのポッドの準備 （127 ページ）を参照してください。

ステップ 4 [リモートリーフの追加（Add Remote Leaf）] ウィザードで、[概要（Overview）] ページの情報を確認します。

このパネルには、ファブリック内のポッドにリモート リーフ スイッチを追加するために必要な手順に関する高度な情報が表示されます。[**概要（Overview**）] パネルに表示される情報、および後続のページで設定する領域は、既存の設定によって異なります。

- シングルポッドまたはマルチポッドの設定に新しいリモートリーフスイッチを追加する場合は、通常、[**概要（Overview**）] パネルに次の項目が表示され、これらの後続のページでこれらの領域を設定します。
  - **外部 TEP**
  - **ポッドの選択**
  - **ルーティング プロトコル**
  - **リモート リーフ**

  また、新しいリモート リーフ スイッチを追加するため、ダイレクト トラフィック転送機能が自動的に設定されます。
- すでにリモート リーフ スイッチが設定されており、リモート リーフ ウィザードを使用してこれらの既存のリモート リーフ スイッチを設定しているが、既存のリモート リーフ スイッチがリリース 4.1(2) より前のソフトウェア リリースからアップグレードされている場合、それらのリモート リーフ スイッチは直接トラフィック転送機能を設定しないでください。この場合、[リモートリーフ直接コミュニケーションは有効化されていません（Remote Leaf Direct Communication is not enabled）] で始まる [概要（Overview）] ページの上部に警告が表示されます。

  この状況でウィザードを使用してリモート リーフ スイッチを追加する場合、2 つのオプションがあります。
  - **これらの既存のリモート リーフ スイッチでの直接トラフィック転送機能を有効にします。**これは、この状況で推奨される一連のアクションです。最初に、リモート リーフ スイッチのアップグレードおよび直接トラフィック転送の有効化 （171 ページ）に

記載されている手順に従って、スイッチの直接トラフィック転送機能を手動でイネーブルにする必要があります。これらの手順を使用して直接トラフィック転送機能を手動で有効にしたら、このリモート リーフ スイッチ ウィザードに戻り、ウィザードのプロセスに従って、ファブリック内のポッドにリモート リーフ スイッチを追加します。

- **直接トラフィック転送機能をイネーブルにせずに、リモート リーフ スイッチを追加します。**これは許容可能なオプションですが、推奨されません。直接トラフィック転送機能を有効にせずにリモートリーフスイッチを追加するには、リモートトラフィック転送機能を手動で有効にせずにリモート リーフ スイッチ ウィザードの設定を続行します。

ステップ 5 [概要（Overview）] パネルの情報を確認したら、ページの右下隅にある [開始（Get Started）] をクリックします。

- 新しいリモート リーフ スイッチを追加すると、リリース 4.1(2) 以降が実行され、直接トラフィック転送機能が自動的に設定され、[**外部 TEP**（**External TEP**）] ページが表示されます。ステップ 6 （159 ページ）に進みます。
- 直接トラフィック転送機能をイネーブルにせずにリモート リーフ スイッチを追加する場合、またはスイッチをリリース 4.1(2) にアップグレードし、リモート リーフ スイッチのアップグレードおよび直接トラフィック転送の有効化 （171 ページ） の指示に従ってスイッチで直接トラフィック転送機能を手動でイネーブルにした場合は、**ポッド選択** ページが表示されます。ステップ 7 （160 ページ）に進みます。

ステップ 6 **外部 TEP** ページで、必要なパラメータを設定します。

外部 TEP アドレスは、リモート ロケーションと通信するために物理ポッドで使用されます。このページでは、異なるロケーションを接続するネットワーク全体でルーティング可能なサブネットを設定します。外部 TEP プールは、他の内部 TEP プール、リモート リーフ TEP プール、または他のポッドからの外部 TEP プールと重複できません。ウィザードは、外部 TEP プールからポッド固有の TEP アドレスおよびスパイン ルータ ID のアドレスを自動的に割り当てます。必要に応じて、提案されたアドレスを変更できます。

a) **[デフォルトを使用（Use Defaults）]** チェックボックスをオンのままにするか、必要に応じてオフにします。

オンにすると、ウィザードは自動的にデータ プレーンおよびユニキャスト TEP アドレスを割り当てます。[**デフォルトを使用（Use Defaults）**] ボックスがオンの場合、これらのフィールドは表示されません。必要に応じて、提案されたアドレスを表示または変更するには、[**デフォルトを使用（Use Defaults）**] ボックスをオフにします。

b) [**外部 TEP プール（External TEP Pool）**] フィールドに、物理ポッドの外部 TEP を入力します。

外部 TEP プールは内部 TEP プールと重ならないようにする必要があります。

c) [**ユニキャスト TEP IP（Unicast TEP IP）**] フィールドで、必要に応じてこのフィールドに自動的に入力される値を変更します。

このアドレスは、外部 TEP プールからCisco APICによって自動的に割り当てられ、リモート リーフ スイッチからそのポッドのローカル リーフ スイッチにトラフィックを送信するために使用されます。

Cisco APIC によって、外部 TEP プール アドレスを入力するときにユニキャスト TEP IP アドレスが自動的に設定されます。

d) マルチポッド構成の場合は、ポッドごとにこれらの手順を繰り返します。
e) このページに必要な情報をすべて入力したら、ページの右下隅にある [**次（Next）**] ボタンをクリックします。

[**ポッド選択（Pod Selection**）] ページが表示されます。

ステップ 7 [**ポッド選択（Pod Selection**）] ページで、必要なパラメータを設定します。

リモート リーフ スイッチは、Cisco ACI ファブリック内のいずれかのポッドに論理的に接続します。このページで、リモート リーフ スイッチが関連付けられるポッドのポッド ID を選択します。リモート リーフ スイッチに IP アドレスを割り当てるには、リモート リーフ TEP プールが必要です。既存のリモート リーフ TEP プールを選択するか、リモート リーフ TEP プールを入力して新しいプールを作成します。リモート リーフ TEP プールは、既存の TEP プールとは異なる必要があります。複数のリモート リーフ ペアを同じリモート TEP プールに含めることができます。

a) [**ポッド ID（Pod ID**）] フィールドで、リモート リーフ スイッチが関連付けられるポッドのポッド ID を選択します。
b) [**リモート リーフ TEP プール（Remote Leaf TEP Pool**）] フィールドで、既存のリモート リーフ TEP プールを選択するか、リモート リーフ TEP プールを入力して、リモート リーフ スイッチに IP アドレスを割り当てます。

[リモート リーフ TEP プール（Remote Leaf TEP Pool）] フィールドの下にある [既存の TEP プールの表示（View existing TEP Pools）] リンクをクリックして、既存の TEP プール（内部 TEP プール、リモート リーフ TEP プール、および外部 TEP プール）を表示します。この情報を使用して、プールの重複または重複を回避します。

c) このページに必要な情報をすべて入力したら、ページの右下隅にある [**次（Next**）] ボタンをクリックします。

[**ルーティング プロトコル（Routing Protocol**）] ページが表示されます。

ステップ 8 [ルーティング プロトコル（Routing Protocol）] ページで、リモート リーフ スイッチとアップストリーム ルータ間でピアリングするアンダーレイ プロトコルに必要なパラメータを選択して設定します。次のサブステップに従います。

a) [L3 Outside 設定（L3 Outside Configuration）] セクションの [L3 Outside] フィールドで、リモート リーフ スイッチとアップストリーム ルータ間の接続を表す既存の L3Out を作成または選択します。複数のリモート リーフ ペアは、アップストリーム接続を表すために同じ L3 Outside を使用できます。

リモート リーフ スイッチの設定では、マルチポッド設定で使用される L3Out とは異なる L3Out を使用または作成することを推奨します。

b) Cisco APIC リリース 5.2(3) 以降のリリースでは、**[アンダーレイ（Underlay）]** コントロールを **[OSPF]** または **[BGP]** に設定します。

Cisco APIC リリース 5.2(3) よりも前のリリースでは、OSPF が唯一サポートされているアンダーレイ プロトコルであるため、選択する必要はありません。

（注） OSPF と BGP の両方が Multi-Pod、Multi-Site、またはリモート リーフのアンダーレイで使用されている場合、 IPN ルータの OSPF から router-id を BGP に再配布しないでください。そうすると、ルーティング ループが生じ、スパイン スイッチと IPN ルータの間の OSPF と BGP セッションを停止してしまいます。

c) 適切な次の構成手順を選択します。

- OSPF アンダーレイの場合は、ステップ ステップ 9 （161 ページ） で OSPF パラメータを構成し、ステップ ステップ 10 （162 ページ） をスキップします。
- BGP アンダーレイの場合は、ステップ ステップ 9 （161 ページ） をスキップし、ステップ ステップ 10 （162 ページ） の BGP パラメータを設定します。

ステップ 9 （OSPF アンダーレイの場合のみ）OSPF アンダーレイを設定するには、**[ルーティング プロトコル（Routing Protocol）]** ページで次の手順を実行します。

このページで、OSPF エリア ID、エリア タイプ、および OSPF インターフェイス ポリシーを設定します。OSPF インターフェイス ポリシーには、OSPF ネットワーク タイプ、インターフェイス コスト、タイマーなどの OSPF 固有の設定が含まれています。**[デフォルトの使用（Use Defaults）]** チェックボックスをオフにして、OSFP 認証キーと OSPF エリア コストを設定します。

（注） Cisco ACIモードのスイッチを、デフォルトの OSPF 認証キー ID が 0 であるスタンドアロン Cisco Nexus 9000 スイッチとピアリングした場合、OSPF セッションは起動しません。 Cisco ACI では、1 ～ 255 の OSPF 認証キー ID のみが許可されます。

a) **[OSPF]** セクションで、**[デフォルトの使用（Use Defaults）]** チェックボックスをオンのままにするか、必要に応じてオフにします。

チェックボックスはデフォルトでオンになります。チェックをオフにすると、エリア コストや認証設定などのオプション フィールドが表示されます。

b) 必要に応じて、IPN から設定情報を収集します。

たとえば、IPN から次のコマンドを入力して、特定の設定情報を収集できます。

```
IPN# show running-config interface ethernet slot/chassis-number
```

次に例を示します。

```
IPN# show running-config interface ethernet 1/5.11
...
ip router ospf infra area 0.0.0.59
...
```

c) [Area ID] フィールドに OSPF エリア ID を入力します。

前のステップの出力に示されているOSPFエリア59の情報を見ると、[Area ID（エリア ID）] フィールドに別のエリアに（たとえば、0）を入力し、別の L3Out を設定できます。リモー

トリーフ スイッチに別のエリアを使用している場合は、別の L3Out を作成する必要があります。同じ OSPF エリア ID を使用している場合でも、別の L3Out を作成できます。

d) [**エリア タイプ（Area Type**）] フィールドで、OSPF エリア タイプを選択します。

次の OSPF タイプのいずれかを選択できます。

- [**NSSA エリア（NSSA area**）]
- [**通常エリア（Regular area**）]

（注） [エリア タイプ（Area Type）] フィールドのオプションとして [スタブ エリア（Stub area）] が表示される場合があります。ただし、スタブ エリアは IPN にルートをアドバタイズしないため、スタブ エリアはインフラ L3Out でサポートされません。

[**通常エリア（Regular area**）] がデフォルトです。

e) [**インターフェイス ポリシー（Interface Policy**）] フィールドで、OSPF インターフェイス ポリシーを入力または選択します。

既存のポリシーを選択するか、[**OSPF インターフェイス ポリシーの作成（Create OSPF Interface Policy**）] ダイアログ ボックスを使用して新しいポリシーを作成できます。OSPF インターフェイス ポリシーには、OSPF ネットワーク タイプ、インターフェイス コスト、タイマーなどの OSPF 固有の設定が含まれています。

f) このページに必要な情報をすべて入力したら、ページの右下隅にある [**次へ（Next**）] ボタンをクリックします。

[**リモート リーフ（Remote Leafs**）] ページが表示されます。

ステップ 10 (BGP アンダーレイの場合のみ) 次の BGP フィールドが **[ルーティング プロトコル]** ページに表示される場合は、次のサブステップに従います。それ以外の場合は、**[次へ]** をクリックして続行します。

a) **[BGP]** セクションで、**[デフォルトの使用（Use Defaults）]** チェックボックスをオンのままにするか、必要に応じてオフにします。

チェックボックスはデフォルトでオンになります。チェックを外すと、ピアリング タイプ、ピア パスワード、ルート リフレクタ ノードなどのオプション フィールドが表示されます。

b) [**スパイン ID（Spine ID**）]、[**インターフェイス（Interface**）]、および [**IPv4 アドレス（IPv4 Address**）] フィールドでは値は設定不可であることに注意してください。

c) [**ピア アドレス（Peer Address**）] フィールドで、BGP ネイバーの IP アドレスを入力します。

d) [**リモート AS（Remote AS**）] フィールドで、BGP ネイバーの自動システム（AS）番号を入力します。

e) このページに必要な情報をすべて入力したら、ページの右下隅にある [**次へ（Next**）] ボタンをクリックします。

[**リモート リーフ（Remote Leafs**）] ページが表示されます。

ステップ 11 [**リモート リーフ（Remote Leafs**）] ページで、必要なパラメータを設定します。

インターポッド ネットワーク（IPN）は、Cisco ACI ロケーションを接続して、エンドツーエンドのネットワーク接続を提供します。これを実現するには、リモート リーフ スイッチにアップストリーム ルータへの IP 接続が必要です。リモート リーフ スイッチごとに、アップストリーム ルータおよび残りの Cisco ACI ファブリックとのコントロールプレーン通信を確立するために使用されるルータ ID を入力します。また、各リモート リーフ スイッチの少なくとも 1 つのインターフェイスの IP 設定を指定します。複数のインターフェイスがサポートされます。

a) [**シリアル（Serial**）] フィールドに、リモート リーフ スイッチのシリアル番号を入力するか、ドロップダウン メニューから検出されたリモート リーフ スイッチを選択します。

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

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

d) [**ルータ ID（Router ID**）] フィールドに、アップストリーム ルータおよびその他の Cisco ACI ファブリックとのコントロールプレーン通信を確立するために使用されるルータ ID を入力します。

e) [**ループバック アドレス（Loopback Address**）] フィールドに、必要に応じて IPN ルータ ループバック IP アドレスを入力します。

ルータ ID アドレスを使用する場合は、このフィールドを空白のままにします。

f) [インターフェイス（Interfaces）] セクションの [インターフェイス（Interface）] フィールドに、このリモート リーフ スイッチのインターフェイス情報を入力します。

g) [インターフェイス（Interfaces）] セクションの [IPv4 アドレス（IPv4 Address）] フィールドに、インターフェイスの IPv4 IP アドレスを入力します。

h) **[インターフェイス]** セクションの **[MTU]** フィールドで、外部ネットワークの最大送信単位の値を割り当てます。

範囲は 1500 ～ 9216 です。

i) BGP アンダーレイを選択した場合は、BGP ネイバーの IP アドレスを **[ピア アドレス]** フィールドに入力し、BGP ネイバーの自律システム（AS）番号を **[リモート AS]** フィールドに入力します。

j) 必要に応じて、追加のインターフェイスに関する情報を入力します。

[インターフェイス（Interfaces）] ボックス内の [+] をクリックして、複数のインターフェイスの情報を入力します。

k) このリモート リーフ スイッチに必要な情報をすべて入力したら、必要に応じて追加のリモート リーフ スイッチの情報を入力します。

[インターフェイス（Interfaces）] ボックスの右側にある [+] をクリックして、複数のリモート リーフ スイッチの情報を入力します。

l) このページに必要な情報をすべて入力したら、ページの右下隅にある [**次へ（Next**）] ボタンをクリックします。

[**確認（Confirmation**）] ページが表示されます。

ステップ 12 [確認（Confirmation）] ページで、ウィザードが作成するポリシーのリストを確認し、必要に応じて任意のポリシーの名前を変更し、ページの右下隅にある [完了（Finish）] をクリックします。

[**リモート リーフ サマリ（Remote Leaf Summary**）] ページが表示されます。

ステップ 13 [**リモート リーフ サマリ（Remote Leaf Summary**）] ページで、適切なボタンをクリックします。

- JSON ファイル内の設定の API を表示するには、[**JSON の表示（View JSON**）] をクリックします。API をコピーして、後で使用するために保存できます。
- このページの情報に問題がなく、JSON ファイルを表示しない場合は、[**OK**] をクリックします。

ステップ 14 [ナビゲーション（Navigation）]ペインで、[**ファブリック メンバーシップ（Fabric Membership**）] をクリックし、[**ノード保留レジストレーション（Nodes Pending Registration**）] タブをクリックして、リモート リーフ スイッチ設定のステータスを表示します。

追加したリモート リーフ スイッチの [ステータス（Status）] カラムに [検出なし（Undiscovered）] と表示されます。

ステップ 15 IPN を使用してスパイン スイッチにログインし、次のコマンドを入力します。

```
switch# show nattable
```

次のような出力が表示されます。

```
------- NAT TABLE ----------
Private Ip   Routeable Ip
10.0.0.1     192.0.2.100
10.0.0.2     192.0.2.101
10.0.0.3     192.0.2.102
```

ステップ 16 リモート リーフ スイッチを接続する IPN サブインターフェイスで、各インターフェイスの DHCP リレーを設定します。

次に例を示します。

```
switch# configure terminal
switch(config)# interface ethernet 1/5.11
switch(config-subif)# ip dhcp relay address 192.0.2.100
switch(config-subif)# ip dhcp relay address 192.0.2.101
switch(config-subif)# ip dhcp relay address 192.0.2.102
switch(config-subif)# exit
switch(config)# interface ethernet 1/7.11
switch(config-subif)# ip dhcp relay address 192.0.2.100
switch(config-subif)# ip dhcp relay address 192.0.2.101
switch(config-subif)# ip dhcp relay address 192.0.2.102
switch(config-subif)# exit
switch(config)# exit
switch#
```

ステップ 17 [ナビゲーション（Navigation）]ペインで、[**ファブリック メンバーシップ（Fabric Membership）**] をクリックし、[**登録済みのノード（Registered Nodes）**] タブをクリックして、リモート リーフ スイッチ設定のステータスを表示します。

しばらくすると、追加したリモートリーフスイッチの [ステータス（Status）] カラムに [アクティブ（Active）] と表示されます。

ステップ 18 メニュー バーで、**[システム（System）]** > **[システム設定（System Settings）]** の順にクリックします。

ステップ 19 [ナビゲーション（Navigation）]ペインで、**[システム グローバル GIPo（System Global GIPo）]** を選択します。

ステップ 20 **[インフラ GIPo をシステム GIPo として使用（Use Infra GIPo as System GIPo）]** で、**[有効（Enabled）]** を選択します。

GUI を使用してリモートリーフスイッチのポッドとファブリック メンバーシップを設定する (ウィザードは使用しない)

[リモート リーフの追加（Add Remote Leaf）] ウィザード（ウィザードを使用してリモート リーフ スイッチのポッドとファブリック メンバーシップを設定する （157 ページ） を参照）を使用してリモート リーフ スイッチを設定することをお勧めしますが、代わりにこの GUI 手順を使用することもできます。

始める前に

- ルータ (IPN と WAN) とリモートのリーフ スイッチはアクティブで設定されています。WAN ルータとリモート リーフ スイッチ設定の注意事項 （154 ページ） を参照してください。
- リモート リーフ スイッチは、13.1.x 以降 (aci n9000 dk9.13.1.x.x.bin) のスイッチ イメージを実行しています。
- リモート リーフ スイッチを追加する予定のポッドが作成され、設定されています。
- ポッドをリモート リーフ スイッチに接続するために使用するスパイン スイッチは IPN ルータに接続されています。

手順

ステップ 1 次の手順で、リモート リーフ スイッチの TEP プールを設定します:

a) メニュー バーで、**[ファブリック（Fabric）]** > **[インベントリ（Inventory）]** をクリックします。

b) [ナビゲーション (Navigation)] ウィンドウで、**[ポッド ファブリック セットアップ ポリシー (Pod Fabric Setup Policy)]** をクリックします。

c) **Fabric Setup Policy** パネルで、リモート リーフ スイッチのペアを追加するポッドをダブルクリックします。
d) **[リモート プール（Remote Pools）]** テーブルで **[+]** をクリックします。
e) リモート TEP プールのリモート ID とサブネットを入力し、**Submit** をクリックします。
f) **Fabric Setup Policy** パネルで、**Submit** をクリックします。

ステップ 2 次の手順で、IPN ルータに接続されているスパイン スイッチの L3Out を設定します:

a) メニュー バーで **[テナント（Tenants）]** > **[インフラ（infra）]** をクリックします。
b) [ナビゲーション（Navigation）] ペインで [ネットワーキング（Networking）] を展開し、[L3Outs] を右クリックして [L3Out の作成（Create L3Out）] を選択します。
c) **Name** フィールドに、L3Out の名前を入力します。
d) [**VRF**] ドロップダウン リストから [**overlay-1**] を選択します。
e) [**L3 ドメイン（L3 Domain**）] ドロップダウン リストで、先ほど作成した、外部ルーテッド ドメインを選択します。
f) [**制御の使用（Use for control**）] で、[**リモート リーフ（Remote Leaf**）] を選択します。
g) IPN アンダーレイ プロトコルとして BGP を使用するには、[**OSPF**] チェックボックスをオフにします。

Cisco APIC リリース 5.2(3) 以降、IPN アンダーレイ プロトコルは OSPF または BGP になることが可能です。

h) OSPF が IPN アンダーレイ プロトコルとして使用されるようにするには、OSPF がデフォルトで選択されている OSPF エリアで、リモート リーフ スイッチを追加するポッドがマルチポッド ファブリックの一部である場合に、[マルチポッドのリモート リーフの有効化（Enable Multi Leaf with Multipod）] の横にあるチェックボックスをオンにします。

このオプションは、マルチポッドのための VLAN-5 を使用する第2の OSPF インスタンスを有効にします。これにより、リモート リーフ スイッチのルートが、スイッチが所属しているポッド内にのみアドバタイズされるようにします。

i) [**次へ（Next**）] をクリックして [**ノードとインターフェイス（Nodes and Interfaces**）] ウィンドウに移動します。

ステップ 3 次の手順に従って、L3Out で使用されるスパインとインターフェイスの詳細を設定します:

a) 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。

[**デフォルトの使用（Use Defaults**）] フィールドで、デフォルトのノード プロファイル名およびインターフェイス プロファイル名を使用する場合は、チェックをオンにします。

- デフォルトのノード プロファイル名は `[L3Out-name _nodeProfile]` です。ここで、[*L3Out-name*] は [識別（Identity）] ページの [名前（Name）] フィールドに入力した名前です。
- 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。ここで、*L3Out-name* は、[識別（Identity）] ページの [名前（Name）] フィールドに入力した名前です。

b) 次の詳細を入力します。

- **ノード ID** — IPN ルータに接続されているスパイン スイッチの ID。
- **ルータ ID** — IPN ルータの IP アドレス
- **外部制御ピアリング** — リモート リーフ スイッチを追加するポッドがシングルポッド ファブリックの場合には無効にします。

c) [ノードとインターフェイス（Nodes and Interfaces）] ウィンドウに追加の必要な情報を入力します。

d) [ノードとインターフェイス（Nodes and Interfaces）] ウィンドウで残りの追加の情報を入力したら、[次（Next）] をクリックします。

[**プロトコル（Protocols**）] ウィンドウが表示されます。

ステップ 4 [L3Out の作成（Create L3Out）] ウィザードの [プロトコル（Protocols）] ウィンドウに必要な情報を入力します。

a) IPN アンダーレイ プロトコルとして BGP を選択した場合は、BGP ピアの [ピア アドレス（Peer Address）] と [リモート AS（Remote AS）] を入力します。

b) IPN アンダーレイ プロトコルとして OSPF を選択した場合は、[ポリシー（Policy）] フィールドで OSPF ポリシーを選択します。

c) **[次へ（Next）]** をクリックします。

[**外部 EPG（External EPG**）] ウィンドウが表示されます。

ステップ 5 [L3Out の作成（Create L3Out）] ウィザードの [外部 EPG（External EPG）] ウィンドウに必要な情報を入力し、[完了（Finish）] をクリックして [L3Out の作成（Create L3Out）] ウィザードで必要な設定を完了します。

ステップ 6 **[テナント（Tenants）] > [インフラ（infra）] > [ネットワーキング（Networking）] > [L3Outs] > [*L3Out_name*] > [論理ノード プロファイル（Logical Node Profiles）] > [bLeaf] > [論理インターフェイス プロファイル（Logical Interface Profiles）] > [portIf] > [OSPF インターフェイス プロファイル（OSPF Interface Profile）]**に移動します。

ステップ 7 インターフェイス プロファイルの名前を入力します。

ステップ 8 [関連付けされた OSPF インターフェイス ポリシーの名前（Associated OSPF Interface Policy Name）] フィールドで、以前に作成したポリシーを選択するか、[OSPF インターフェイス ポリシーの作成（Create OSPF Interface Policy）] をクリックします。

ステップ 9 a) **OSPF Profile** で、**OSPF Policy** をクリックし、前に作成したポリシーを選択します。または、**Create OSPF Interface Policy** をクリックします。

b) **Next** をクリックします。

c) **[ルーテッド サブインターフェイス（Routed Sub-Interface）]** をクリックし、**[ルーテッド サブインターフェイス（Routed Sub-Interface）]** テーブルの **[+]** をクリックして、以下の詳細を入力します:

- Node — インターフェイスが所在するスパイン スイッチです。
- Path — IPN ルータに接続されたインターフェイス
- Encap — VLAN の場合には **4** を入力します。

d) **OK** をクリックし、**Next** をクリックします。
e) **External EPG Networks** テーブルの [+] をクリックします。
f) 外部ネットワークの名前を入力し、 **OK** をクリックします。
g) **Finish** をクリックします。

ステップ 10 リモート リーフ スイッチのファブリック メンバーシップ設定を完了するには、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）]** に移動します。

この時点で、新しいリモート リーフ スイッチが、ファブリックに登録されているスイッチのリストに表示されるようになります。ただし、次の手順で説明する方法でノードアイデンティティ ポリシーを設定するまでは、これらはリモート リーフ スイッチとは認識されません。

b) それぞれのリモート リーフ スイッチについてに、リストのノードをダブルクリックし、次の詳細情報を設定し、**Update** をクリックします:

- Node ID — リモート リーフ スイッチの ID
- RL TEP Pool — 以前に設定した、リモート リーフ TEP プールの識別子
- Node Name — リモート リーフ スイッチの名前

リモート リーフ スイッチごとにノード アイデンティティ ポリシーを設定すると、**Fabric Membership** テーブルに、`remote leaf` ロールを持つものとしてリストされます。

ステップ 11 次の手順で、リモート リーフ ロケーションの L3Out を設定します:

a) **[テナント（Tenants）]** > **[インフラ（infra）]** > **[ネットワーキング（Networking）]** に移動します。
b) [L3Outs] を右クリックして、[L3Out の作成（Create L3Out）] を選択します。
c) L3Out の名前を入力します。
d) **OSPF** チェック ボックスをオンにして OSPF を有効にし、IPN および WAN ルータと同じ方法で OSPF の詳細を設定します。

（注） リリース 4.1(2) 以降を実行している新しいリモート リーフ スイッチを導入し、それらのリモート リーフ スイッチで直接トラフィック転送を有効にする場合は、[マルチポッドのリモート リーフを有効化（Enable Remote Leaf with Multipod）] チェックボックスをオンにしないでください。このオプションは、マルチポッドに VLAN-5 を使用する OSPF インスタンスを有効にしますが、このケースでは必要ありません。詳細については、「ダイレクト トラフィック フォワーディングについて（170 ページ）」を参照してください。

e) **overlay-1** VRF を選択します。

ステップ 12 次の手順で、ノードと、リモート リーフ スイッチから WAN ルータに向かうインターフェイスを設定します:

a) [L3Out の作成（Create L3Out）] ウィザードの [ノードとインターフェイス（Nodes and Interfaces）] ウィンドウで、次の詳細を入力します。

- Node ID — WAN ルータに接続されているリモート リーフの ID
- Router ID— WAN ルータの IP アドレス
- External Control Peering — リモート リーフ スイッチがマルチポッド ファブリック内のポッドに追加される場合にのみ、有効にしてください

ステップ 13 **[テナント（Tenants）] > [インフラ（infra）] > [ネットワーキング（Networking）] > [L3Outs] > [*L3Out_name*] > [論理ノード プロファイル（Logical Node Profiles）] > [bLeaf] > [論理インターフェイス プロファイル（Logical Interface Profiles）] > [portIf] > [OSPF インターフェイス プロファイル（OSPF Interface Profile）]**に移動します。

ステップ 14 [**OSPF インターフェイス プロファイル（OSPF Interface Profiles**）] で、リモート リーフ スイッチを WAN ルータに接続するために使用されるルーテッド サブインターフェイスについて、次の詳細を設定します。

- Identity — OSPF インターフェイスのプロファイルの名前
- Protocol Profiles — 以前に設定した OSPF プロファイル。または新たに作成
- Interfaces — **Routed Sub-Interface** タブの、WAN ルータに向かうルーテッド サブインターフェイスのパスと IP アドレス

ステップ 15 次の手順で、ファブリック外部接続プロファイルを設定します。

a) **[テナント（Tenants）] [インフラ（infra）] [ポリシー（Policies）] [プロトコル（Protocol）]** に移動します。
b) **Fabric Ext Connection Policies** を右クリックし、**Create Intrasite/Intersite Profile** を選択します。
c) 例に示されている形式で必須の [**コミュニティ（Community**）] 値を入力します。
d) **[ファブリック外部ルーティング プロファイル（ファブリック外部ルーティング プロファイル）]** で **[+]** をクリックします。
e) プロファイルの名前を入力し、すべてのリモート リーフ スイッチのアップリンク インターフェイス サブネットを追加します。
f) **Update** をクリックし、**Submit** をクリックします。

ステップ 16 メニュー バーで、**[システム（System）] > [システム設定（System Settings）]** の順にクリックします。

ステップ 17 [ナビゲーション（Navigation）] ペインで、**[システム グローバル GIPo（System Global GIPo）]** を選択します。

ステップ 18 **[インフラ GIPo をシステム GIPo として使用（Use Infra GIPo as System GIPo）]** で、**[有効（Enabled）]** を選択します。

ステップ 19 リモートのリーフ スイッチが、apic 内で検出されたことを確認するには、**[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）]**、または **[ファブリック（Fabric）] > [インベントリ（Inventory）] > [ポッド（Pod）] > [トポロジー（Topology）]** に移動します。

ステップ 20 ファブリックとリモート リーフ スイッチ間のリンクのステータスを表示するには、IPN ルータに接続されているスパイン スイッチで、**show ip ospf neighbors vrf overlay-1** コマンドを入力します。

ステップ 21 CLI を使用する APIC で、ファブリック内のリモート リーフ スイッチのステータスを表示するには、**acidiag fnvread** という NX-OS スタイルのコマンドを入力します。

ダイレクト トラフィック フォワーディングについて

で説明されているように、直接トラフィック転送のサポートはリリース 4.1(2) 以降でサポートされ、リリース 5.0(1) 以降ではデフォルトで有効になっており、無効にすることはできません。リリース4.1(2) でのリモート リーフ スイッチ動作の特性 （142 ページ）ただし、直接トラフィック転送を有効または無効にするために使用する方法は、リモート リーフ スイッチで実行されているソフトウェアのバージョンによって異なります。

- リモート リーフ スイッチが現在リリース 4.1(2) 以降で実行されている場合（リモート リーフ スイッチが 4.1(2) より前のリリースで実行されていない場合）、ウィザードを使用してリモート リーフ スイッチのポッドとファブリック メンバーシップを設定する （157 ページ） に移動してください。
- リモート リーフ スイッチが現在 4.1(2) よりも前のリリースで稼働している場合は、に移動してスイッチをリリース 4.1(2) 以降にアップグレードし、必要な設定変更を行い、それらのリモート リーフ スイッチで直接トラフィック転送を有効にします。リモート リーフ スイッチのアップグレードおよび直接トラフィック転送の有効化 （171 ページ）
- リモート リーフ スイッチがリリース 4.1(2) 以降で実行されており、直接トラフィック転送が有効になっているが、4.1(2) より前のリリースにダウングレードする場合は、に移動して、それらのリモート リーフ スイッチをダウングレードする前に直接トラフィック転送機能を無効にします。直接トラフィック転送を無効化、およびリモート リーフ スイッチのダウングレード （175 ページ）
- リモート リーフ スイッチがリリース 5.0(1) より前のリリースで実行されており、リリース 5.0(1) 以降にアップグレードする場合：
  1. リモート リーフ スイッチが 4.1(2) より前のリリースで実行されている場合は、最初にリリース 4.1(2) にアップグレードし、で説明されている手順を使用してそれらのリモート スイッチで直接トラフィック転送を有効にします。リモート リーフ スイッチのアップグレードおよび直接トラフィック転送の有効化 （171 ページ）
  2. リモート リーフ スイッチがリリース 4.1(2) にあり、ダイレクト トラフィック転送が有効になっている場合は、リモート リーフ スイッチをリリース 5.0(1) 以降にアップグレードします。
- リモート リーフ スイッチがリリース 5.0(1) 以降で実行されており、直接トラフィック転送がデフォルトで有効になっている場合、直接トラフィック転送もサポートしている次の以前のリリースにダウングレードする必要があります。

- リリース 4.2(x)
- リリース 4.1(2)

直接トラフィック転送は、設定に応じてデフォルトで有効になっている場合とされていない場合があります。

- ルーティング可能なサブネットとルーティング可能な Ucast の両方がダウングレード前にすべてのポッドで有効にされていた場合、ダウングレード後も直接トラフィック転送はデフォルトで有効のままになります。
- ルーティング可能なサブネットがすべてのポッドで有効になっているが、ルーティング可能な Ucast が有効になっていない場合、ダウングレード後に直接トラフィック転送は有効になりません。

リモート リーフ スイッチのアップグレードおよび直接トラフィック転送の有効化

リモート リーフ スイッチが現在 4.1(2) よりも前のリリースで稼働している場合は、これらの手順に従ってスイッチをリリース 4.1(2) 以降にアップグレードし、必要な設定変更を行い、それらのリモート リーフ スイッチで直接トラフィック転送を有効にします。

（注） リリース 4.1(2) 以降にアップグレードする場合、アップグレード先のリリースに応じて、直接トラフィック転送の有効化はオプションまたは必須になります。

- リリース 5.0(1) よりも前のリリースにアップグレードする場合、ダイレクト トラフィック転送の有効化はオプションです。ダイレクト トラフィック転送機能をイネーブルにしなくても、スイッチをアップグレードできます。必要に応じて、アップグレードを行った後のある時点で、この機能を有効にできます。
- リリース 5.0(1) 以降にアップグレードする場合は、直接トラフィック転送を有効にする必要があります。ダイレクト トラフィック転送は、リリース 5.0(1) 以降ではデフォルトで有効になっており、無効にすることはできません。

後日、リモート リーフ スイッチのソフトウェアを、リモート リーフ スイッチの直接トラフィック転送をサポートしないバージョン（リリース 4.1(2) よりも前のリリース）にダウングレードする必要がある場合は、直接トラフィック転送を無効化、およびリモート リーフ スイッチのダウングレード（175 ページ）の手順に従って、リモート リーフ スイッチのソフトウェアをダウングレードする前に、直接トラフィック転送機能を無効にします。

手順

ステップ 1 ファブリック内のすべてのノードをリリース 4.1(2) 以降にアップグレードします。Cisco APIC

ステップ 2 設定するルーティング可能なサブネットのルートがポッド間ネットワーク（IPN）で到達可能であること、およびサブネットがリモート リーフ スイッチから到達可能であることを確認します。

ステップ 3 ファブリック内のすべてのポッドでルーティング可能なサブネットを設定します。

a) メニュー バーで、**Fabric** > **Inventory** をクリックします。

b) [Navigation] ウィンドウで、**Pod Fabric Setup Policy** をクリックします。

c) [**ファブリック セットアップ ポリシー**（**Fabric Setup Policy**）] パネルで、ルータブル サブネットを設定するポッドをダブルクリックします。

d) APIC ソフトウェアのリリースに応じて、サブネットまたは TEP テーブルの情報にアクセスします。

- 4.2(3) よりも前のリリースでは、[ルータブル サブネット（Routable Subnets）] テーブルで [+] をクリックします。
- 4.2(3) の場合のみ、[外部サブネット（External Subnets）] テーブルで [+] をクリックします。
- 4.2(4) 以降では、[外部 TEP（External TEP）] テーブル で [+] をクリックします。

e) 必要に応じてIPアドレスと予約アドレスを入力し、状態を**アクティブ**または**非アクティブ**に設定します。

- IP アドレスは、ロータブル IP スペースとして設定するサブネット プレフィックスです。
- 予約アドレスは、スパイン スイッチおよびリモート リーフ スイッチに動的に割り当ててはいけないサブネット内のアドレスの数です。カウントは常にサブネットの最初のIPから始まり、順番に増加します。このプールからユニキャストTEP（これらの手順の後で変換されます）を割り当てる場合は、予約する必要があります。

f) [**更新**（**Update**）] をクリックして、新しい外部ルータブル サブネットをサブネットまたは TEP テーブルに追加します。

g) **Fabric Setup Policy** パネルで、**Submit** をクリックします。

（注） これらの設定を行った後、サブネットまたはTEPテーブルの情報を変更する必要がある場合に、 *Cisco APIC Getting Started Guide* 内の「Changing the External Routable Subnet」の手順に従い、これらの変更を行います。

ステップ 4 各ポートのルータブル Ucast を追加します。

a) メニュー バーで、**[テナント（Tenants）]** > **[インフラ（infra）]** > **[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[ファブリック外部接続ポリシー（Fabric Ext Connection Policies）]** > **[*intrasite-intersite_profile_name*]**の順にクリックします。

b) このサイト内/サイト間プロファイルのプロパティ ページで、[ポッド接続プロファイル（Pod Connection Profile）] 領域の [+] をクリックします。

[ポッド接続プロファイルの作成（Create Pod Connection Profile）] ウィンドウが表示されます。

c) ポッドを選択し、[ポッド接続プロファイルの作成（Create Pod Connection Profile）] ウィンドウに必要な情報を入力します。

[ユニキャスト TEP（Unicast TEP）] フィールドに、IPN を介したユニキャスト トラフィックに使用される、ルーティング可能な TEP IP アドレス（プレフィックスのビット長を含む）を入力します。この IP アドレスは、特定のシナリオでユニキャスト トラフィックのそれぞれのポッドのスパイン スイッチによって使用されます。たとえば、リモート リーフ スイッチの直接展開にはユニキャスト TEP が必要です。

（注） リリース 4.2(5) 以降、APIC ソフトウェアは、次のいずれかの誤った設定がある場合、4.2(5) より前のリリースから 4.2(5) 以降へのアップグレード後に、適切な障害を自動的に発生させます。

- 予約アドレス数が 0 または 0 以外のポッドの外部 TEP プールの非予約部分のいずれかの IP アドレスで設定された 1 つのポッドのユニキャスト TEP IP アドレス
- 1 つのポッドのユニキャスト TEP IP アドレスが、ファブリック内の他のポッドのユニキャスト TEP IP アドレスと一致します
- ユニキャスト TEP IP アドレスが、ファブリック内のすべてのポッドのリモート リーフ TEP プールと重複しています

この場合、障害をクリアするには、リリース 4.2(5) 以降へのアップグレード後に適切な設定変更を行う必要があります。何らかの設定のエクスポートを試行する前に、これらの設定を変更する必要があります。そうしないと、リリース 4.2(5) 以降からの設定のインポート、設定のロールバック、または ID リカバリで障害が発生します。

ステップ 5 **[送信（Submit）]** をクリックします。`

各ポッドにルーティング可能なサブネットとルーティング可能な Ucast を設定すると、次の領域が設定されます。

- スパイン スイッチで、リモート リーフ マルチキャスト TEP インターフェイス（rl-mcast-hrep）とルーティング可能な CP TEP インターフェイス（rt-cp-etep）が作成されます。
- リモート リーフ スイッチでは、プライベート リモート リーフ マルチキャスト TEP インターフェイス（rl-mcast-hrep）はそのままです。
- トラフィックは引き続きプライベート リモート リーフ マルチキャスト TEP インターフェイス（rl-mcast-hrep）を使用します。
- トラフィックは、新しく設定されたルーティング可能な Ucast TEP インターフェイスで再開されます。プライベート リモート リーフ ユニキャスト TEP インターフェイス（rl_ucast）トンネルがリモート リーフ スイッチから削除されます。新しく設定されたユニキャスト TEP でトラフィックが収束しているため、サービスの中断は非常に短時間です。

- リモート リーフ スイッチおよびスパイン スイッチ COOP（オラクル プロトコル会議）セッションは、プライベート IP アドレスのままです。
- BGP ルート リフレクタは、ルーティング可能な CP TEP インターフェイス（rt-cp-etep）に切り替わります。

ステップ 6 COOP が正しく設定されていることを確認します。

```
# show coop internal info global
# netstat -anp | grep 5000
```

ステップ 7 リモート リーフ スイッチの BGP ルート リフレクタ セッションが正しく設定されていることを確認します。

```
remote-leaf# show bgp vpnv4 unicast summary vrf all | grep 14.0.0
 14.0.0.227 4 100 1292 1164 395 0 0 19:00:13 52
 14.0.0.228 4 100 1296 1164 395 0 0 19:00:10 52
```

ステップ 8 リモート リーフ スイッチの直接トラフィック転送を有効にします。

a) メニュー バーで、**[System]** > **[System Settings]** の順にクリックします。

b) **[Fabric Wide Setting]** をクリックします。

c) [**リモート リーフ ダイレクト トラフィック転送の有効化（Enable Remote Leaf Direct Traffic Forwarding**）] でチェック ボックスをクリックします。

これを有効にすると、リモート リーフ スイッチが各リモート リーフ スイッチの TEP 間で直接送信するようになるため、スパイン スイッチはアクセス制御リスト（ACL）をインストールして、リモート リーフ スイッチからのトラフィックが返送されないようにします。リモート リーフ スイッチ間にトンネルが構築されている間、サービスが短時間中断する場合があります。

d) **[送信（Submit）]** をクリックします。`

e) コンフィギュレーションが正しく設定されているか確認するには、スパイン スイッチで次のコマンドを入力します。

```
spine# cat /mit/sys/summary
```

出力内容で次のハイライトされているラインを確認してください。コンフィギュレーションが正しく設定されているかの確認ができます（フル出力の省略形）。

```
...
podId : 1
remoteNetworkId : 0
remoteNode : no
rldirectMode : yes
rn : sys
role : spine
...
```

この時点で、次の領域が設定されます。

- ネットワーク アドレス変換アクセス コントロール リスト（NAT ACL）は、データ センターのスパイン スイッチで作成されます。
- リモート リーフ スイッチでは、プライベート リモート リーフ ユニキャスト TEP インターフェイス（rl_ucast）およびリモート リーフ マルチキャスト TEP インターフェイス（rl-mcast-hrep）トンネルが削除され、ルータブル トンネルが作成されます。
- 次の例に示すように、**rlRoutableMode** および **rldirectMode** 属性は **yes** に設定されます。

```
remote-leaf# moquery -d sys | egrep "rlRoutableMode|rldirectMode"
rlRoutableMode : yes
rldirectMode : yes
```

ステップ 9 リモート リーフ スイッチに接続する IPN インターフェイスで DHCP が遅延するため、Cisco APIC のルータブル IP アドレスを追加します。

クラスタ内の各APICには、プールからアドレスが割り当てられます。これらのアドレスは、リモート リーフ スイッチ側のインターフェイスに DHCP リレー アドレスとして追加する必要があります。これらのアドレスを検索するには、APIC CLI から次のコマンドを実行します。

```
remote-leaf# moquery -c infraWiNode | grep routable
```

ステップ 10 各リモート リーフ スイッチを一度に 1 つずつ解放し、再起動して、ルーティング可能な IP アドレスで検出します。Cisco APIC

COOP 設定が Routable CP TEP Interface（rt-cp-etep）に変更されます。各リモート リーフ スイッチがデコミッションされて再コミッションされると、DHCP サーバ ID にルーティング可能な IP アドレスが割り当てられます。Cisco APIC

直接トラフィック転送を無効化、およびリモート リーフ スイッチのダウングレード

リモート リーフ スイッチがリリース 4.1(2) 以降で実行されており、直接トラフィック転送が有効になっているが、4.1(2) より前のリリースにダウングレードする場合は、リモート リーフ スイッチをダウングレードする前に、直接トラフィック転送機能を無効にするこれらの手順に従います。

始める前に

手順

ステップ 1 マルチポッド設定の場合は、VLAN-5 を使用してマルチポッド内部 L3Out を設定します。

ステップ 2 リモート リーフ スイッチで直接トラフィック転送機能をイネーブルにしたときに削除された場合は、プライベート ネットワークの到達可能性をプロビジョニングします。

たとえば、IPN でプライベート IP ルートの到達可能性を設定し、リモート リーフ スイッチに接続された IPN のレイヤ 3 インターフェイスでのプライベート IP アドレスを DHCP リレー アドレスとして設定します。Cisco APIC

ステップ 3 次のポリシーをポストして、すべてのリモート リーフ スイッチのリモート リーフ スイッチの直接トラフィック転送を無効にします。

```
POST URL : https://<ip address>/api/node/mo/uni/infra/settings.xml
<imdata>
    <infraSetPol dn="uni/infra/settings" enableRemoteLeafDirect="no" />
</imdata>
```

これにより、MO が Cisco APIC にポストされ、設定が Cisco APIC からファブリック内のすべてのノードにプッシュされます。

この時点で、次の領域が設定されます。

- ネットワーク アドレス変換アクセス コントロール リスト（NAT ACL）は、データ センターのスパイン スイッチで削除されます。
- 次の例に示すように、**rlRoutableMode** および **rldirectMode** 属性は **no** に設定されます。

```
remote-leaf# moquery -d sys | egrep "rlRoutableMode|rldirectMode"
rlRoutableMode : no
rldirectMode : no
```

ステップ 4 ファブリック内のポッドからルーティング可能なサブネットとルーティング可能な Ucast を削除します。

各ポッドからルーティング可能なサブネットとルーティング可能な Ucast を削除すると、次の領域が設定されます。

- スパイン スイッチで、リモート リーフ マルチキャスト TEP インターフェイス（rl-mcast-hrep）およびルーティング可能な CP TEP インターフェイス（rt-cp-etep）が削除されます。
- リモート リーフ スイッチでは、ルーティング可能なリモート リーフ マルチキャスト TEP インターフェイス（rl-mcast-hrep）へのトンネルが削除され、プライベート リモート リーフ マルチキャスト TEP インターフェイス（rl-mcast-hrep）が作成されます。リモート リーフ ユニキャスト TEP インターフェイス（rl_ucast）トンネルは、この時点でルーティング可能です。
- リモート リーフ スイッチおよびスパイン スイッチ COOP（オラクル プロトコルのカウンシル）およびルート リフレクタ セッションはプライベートに切り替わります。
- ルーティング可能なリモート リーフ ユニキャスト TEP インターフェイス（rl_ucast）へのトンネルが削除され、プライベート リモート リーフ ユニキャスト TEP インターフェイス（rl_ucast）トンネルが作成されます。

ステップ 5 各リモート リーフ スイッチをデコミッションして再起動し、Cisco APIC のルーティング不可能な内部 IP アドレスで検出します。

ステップ 6 ファブリック内のおよびすべてのノードを 4.1(2) より前のリリースにダウングレードします。Cisco APIC

リモート リーフ スイッチのフェールオーバー

(APIC) リリース 4.2(2) 以降、リモート リーフ スイッチはポッド冗長です。Cisco Application Policy Infrastructure Controllerつまり、マルチポッドのセットアップでは、ポッド内のリモート リーフ スイッチがスパイン スイッチへの接続を失うと、別のポッドに移動されます。これにより、元のポッドに接続されているリモート リーフ スイッチのエンドポイント間のトラフィックが機能します。

リモート リーフ スイッチはポッドに関連付けられ、ピン接続され、スパイン プロキシ パスは設定によって決定されます。以前のリリースでは、Council of Oracle Protocol（COOP）はマッピング情報をスパイン プロキシに伝達していました。現在、スパイン スイッチへの通信が失敗すると、COOP セッションは別のスパイン スイッチのポッドに移動します。

以前は、Border Gateway Protocol（BGP）ルート リフレクタをポッドに追加しました。ここで、外部ルート リフレクタを使用し、ポッド内のリモート リーフ スイッチが他のポッドと BGP 関係を持っていることを確認します。

リモート リーフ スイッチのフェールオーバーは、デフォルトでは無効になっています。[システム（Systems）] [システム設定（System Settings）] タブの（APIC）GUIで、リモート リーフ ポッド冗長性ポリシーを有効にします。Cisco Application Policy Infrastructure Controller > 冗長プリエンプションを有効にすることもできます。プリエンプションを有効にすると、リモート ポッドがバックアップされると、リモート リーフ スイッチは親ポッドに再関連付けされます。プリエンプションを有効にしない場合、リモート リーフは、親ポッドが復帰しても動作ポッドに関連付けられたままになります。

（注） あるポッドから別のポッドにリモート リーフ スイッチを移動すると、数秒のトラフィックの中断が発生する可能性があります。

リモート リーフ フェールオーバーの要件

ここでは、リモート リーフ スイッチのフェールオーバーが機能するために満たす必要がある要件を示します。この要件は、この章のリモート リーフ スイッチのハードウェア要件に追加されるものです。リモート リーフ スイッチのハードウェアの要件 （150 ページ）

- フル メッシュ モードではなく、ルート リフレクタ モードでマルチポッドを設定します。
- リモート リーフ スイッチのルート可能な IP アドレスで直接トラフィック転送を有効にします。
- 外部 Border Gateway Protocol（BGP）ルート リフレクタを設定します。

- スパイン スイッチ間の BGP セッションを減らすために、マルチポッドに外部ルート リフレクタを使用することを推奨します。

  各ポッドの 1 つのスパイン スイッチを外部ルート リフレクタ専用にすることができます。

- フル メッシュ モードですべてのリモート リーフ ポッドの外部 BGP ルート リフレクタ ノードを設定します。
- すでにフル メッシュ モードでマルチポッドを使用している場合は、フル メッシュを引き続き使用できます。ただし、リモート リーフ スイッチのルート リフレクタを有効にします。

リモート リーフ スイッチ フェールオーバーの有効化

リモート リーフ スイッチ ポッドの冗長性ポリシーを作成して、リモート リーフ スイッチのフェールオーバーを有効にします。冗長プリエンプションを有効にすることもできます。この場合、ポッドがバックアップされると、リモート リーフ スイッチと親ポッドが再度関連付けられます。

始める前に

リモート リーフ スイッチのフェールオーバーをイネーブルにする前に、次のタスクを実行します。

- セクション「リモート リーフ フェールオーバーの要件 （177 ページ）」の前提条件を満たします。
- リモート リーフ ダイレクト（RLD）を有効にします。
- すべてのポッドが（APIC）リリース 4.2(2) 以降を実行していることを確認します。Cisco Application Policy Infrastructure Controller
- すべてのポッドに少なくとも 2 つの Date Center Interconnect（DCI）対応スパイン スイッチがあることを確認します。

  製品名にサフィックス「EX」が付いた Cisco Nexus 9000 シリーズ スパイン スイッチを使用していることを確認します。たとえば、N9K-C93180YC-EX です。

（注） ポッドに単一のリモート リーフ スイッチがあり、スイッチがクリーン リロードされると、スイッチはスパインスイッチのフェールオーバーポッド（親設定ポッド）に接続されます。ポッドに複数のリモート リーフ スイッチがある場合は、少なくとも 1 つのスイッチがクリーン リロードされていないことを確認します。これにより、他のリモートリーフスイッチは、リロードされなかったリモート リーフ スイッチが存在するポッドに移動できます。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 **[システム (System)]** > **[システム設定 (System Settings)]** に移動します。

ステップ 3 [システム設定（System Settings）] ナビゲーション ウィンドウで、[リモート リーフ ポッド冗長性ポリシー（Remote Leaf POD Redundancy Policy）] を選択します。

ステップ 4 [リモート リーフ ポッド冗長性ポリシー（Remote Leaf POD Redundancy Policy）] 作業ウィンドウで、[リモートリーフ ポッド冗長性ポリシーの有効化（Enable Remote Leaf Pod Redundancy Policy）] チェックボックスをオンにします。

ステップ 5 （任意）[リモートリーフ ポッド冗長性プリエンプションの有効化（Enable Remote Leaf Pod Redundancy pre-emption）] チェックボックスをオンにします。

ポッドが復旧すると、親ポッドにリモート リーフ スイッチが再度関連付けられたチェック ボックスをオンにします。このチェックボックスをオフのままにすると、親ポッドが復帰しても、リモート リーフは動作ポッドに関連付けられたままになります。

次のタスク

フェールオーバーが発生したときにリモート リーフ スイッチで次のコマンドを入力し、どのポッド リモート リーフ スイッチが動作しているかを確認します。

```
cat /mit/sys/summary
moquery -c rlpodredRlSwitchoverPod
```

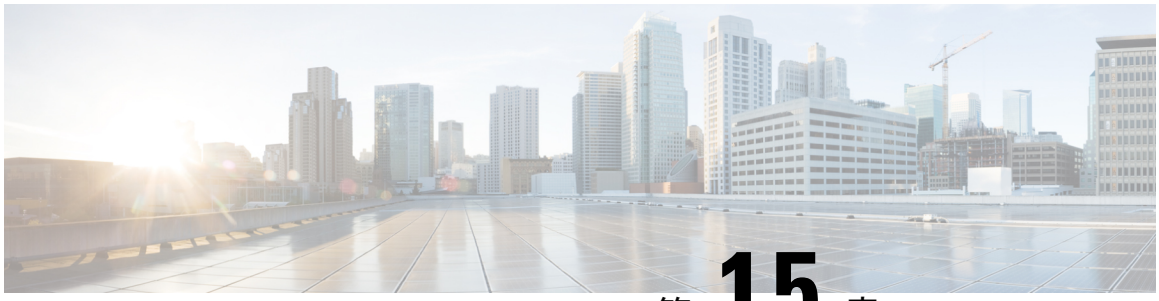
リモートのリーフスイッチのダウングレードする前に必要な前提条件

（注） リモート ノードの使用停止し、リモート リーフに関連するポリシー(を削除する必要がありますがあれば導入で、リモートのリーフ スイッチ リリース 3.1 (1) から以降、リモート リーフ機能をサポートしていない以前のリリースには、APIC ソフトウェアのダウン グレードする場合、というプールにある) を含む前にダウン グレードします。スイッチの使用停止の詳細についてを参照してください。 使用停止およびスイッチの再稼働 で、 *Cisco APIC* トラブルシューティング ガイド 。

リモート リーフ スイッチをダウン グレードする前に、いずれかのタスクが完了することを確認します。

- vPC ドメインを削除します。

- SCVMM を使用している場合は、vTEP - 仮想ネットワーク アダプタを削除します。
- リモート リーフ ノードの使用停止および 10 を待機-15 分を完了するタスクの使用停止後。
- 削除に WAN L3out にリモート リーフ、テナント インフラ。
- Multipod を使用している場合、インフラ-l3out VLAN 5 とを削除します。
- リモートというプールを削除します。



第 15 章

SR-MPLS ハンドオフ

リリース 5.0(1) 以降、境界リーフ スイッチでのセグメント ルーティング（SR）マルチプロトコル ラベル スイッチング（MPLS）ハンドオフは、新機能として使用できます。Cisco ACI

（注） このドキュメントの手順では、GUI と REST API を使用して SR-MPLS ハンドオフを設定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 SR-MPLS ハンドオフを設定することはできません。

ACI ハンドオフについて

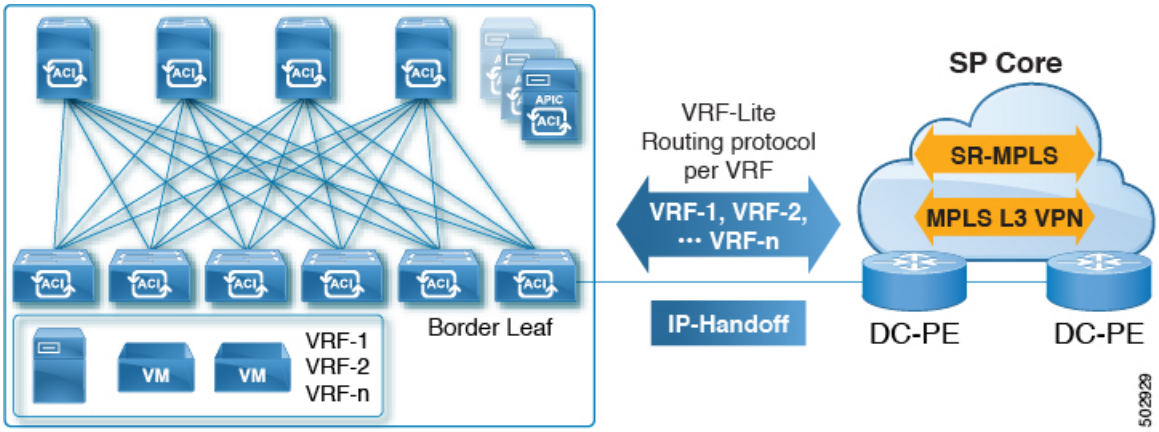
ここでは、IP ハンドオフを使用したリリース 5.0(1) より前のリリースでの ACI ハンドオフの処理方法と、リリース 5.0(1) 以降の SR-MPLS ハンドオフを使用した処理方法について説明します。Cisco APICCisco APIC

リリース 5.0(1) 以前の ACI ハンドオフ：IP ハンドオフ

リリース5.0(1) 以前では、ACI 境界リーフ ノードをデータ センター プロバイダー エッジ（DC-PE）に接続する ACI ファブリックを設定するときに、マルチテナント ネットワークを

使用する構成の場合は、複数の VRF があり、各 VRF にルーティング プロトコルが必要です。Cisco APICまた、各 VRF のインターフェイスを専用にする必要があります。このインターフェイスは、物理インターフェイスまたは論理インターフェイスのいずれかです。次の図に示すように、この設定は通常 VRF-Lite と呼ばれます。

図 *20 : IP* ハンドオフを使用した *DC-PE* への *ACI* ハンドオフ（*VRF-Lite*）



この設定では、境界リーフ スイッチは VRF-Lite を使用して DC-PE に接続されます。境界リーフ スイッチと DC-PE 間のインターフェイスおよびルーティング プロトコル セッションの設定は、個別の VRF を使用して行われます。差別化サービス コード ポイント（DSCP）は、発信トラフィックの境界リーフ スイッチで設定されます。DC-PE では、DSCP は、トラフィック エンジニアリング（SR-TE）ポリシーのセグメント ルーティングにマッピングされます。このポリシーは、トランスポート ネットワーク経由でトラフィックを誘導するために使用されます。

境界リーフ スイッチとデータ センターの間に多数のセッションがある場合、この設定は面倒になります。したがって、自動化と拡張性は、VRF-Lite を使用して設定する際の重要な課題です。

リリース 5.0(1) での ACI ハンドオフ：SR ハンドオフ

リリース 5.0(1) 以降、SR-MPLS ハンドオフを使用して、境界リーフ スイッチと DC-PE ルータ間の ACI ファブリック接続を設定できるようになりました。Cisco APICSR は他のオプションよりも優れたソリューションです。VXLAN などの他のオプションは SP コアでは一般的なテクノロジーではないため、SR はトランスポート デバイスよりもはるかに一般的で成熟したソリューションです。

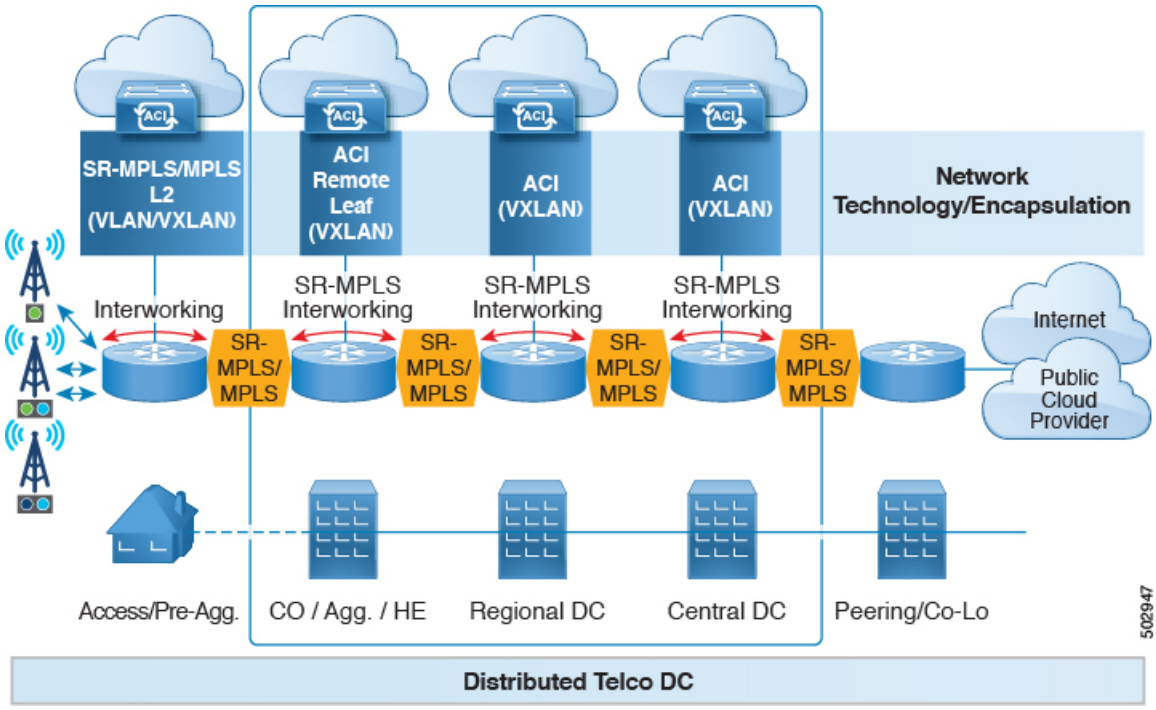
次のシナリオは、SR-MPLS を使用した DC-PE への ACI ハンドオフの設定がどのように役立つかを示しています。

- 統合セグメント ルーティングの転送 （183 ページ）
- トランスポート ネットワークでの DC-to-DC フローのモニタリング （183 ページ）
- 複数の VRF の単一コントロール プレーン セッション （184 ページ）

- [カラー コミュニティ（Color Community）] または [宛先プレフィックス（Destination Prefix）] を使用したトランスポートの SR-TE / Flex Algo （185 ページ）
- SR または MPLS による DC およびトランスポート QoS （186 ページ）

統合セグメント ルーティングの転送

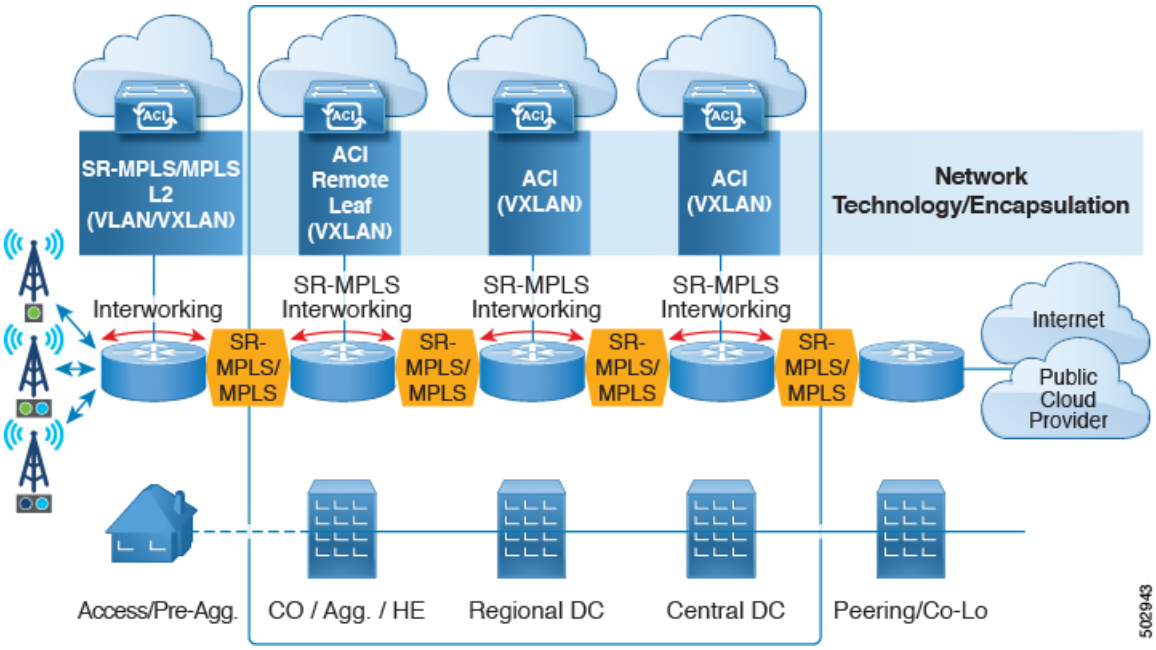
次のシナリオでは、異なる ACI DC ネットワークを相互接続するための統合 SR または MPLS トランスポート ネットワークの導入について説明します。VXLAN から SR-MPLS へのハンドオフは、ACI ネットワークと DC-PE ルータ間の各ロケーションで活用されます。



このシナリオでは、VXLAN は ACI ファブリック エリアで使用され、セグメント ルーティングはトランスポート ネットワークで使用されます。ACI ファブリック エリアの外部で VXLAN を使用するのではなく、同じ SR ベースのルーティングを使用することをお勧めします。この場合、トランスポート デバイスに対して SR ハンドオフまたは MPLS ハンドオフを実行します。ACI 境界で VXLAN を SR に変更すると、トランスポート デバイスは SR または MPLS を実行するだけでよく、VXLAN を実行する必要はありません。

トランスポート ネットワークでの DC-to-DC フローのモニタリング

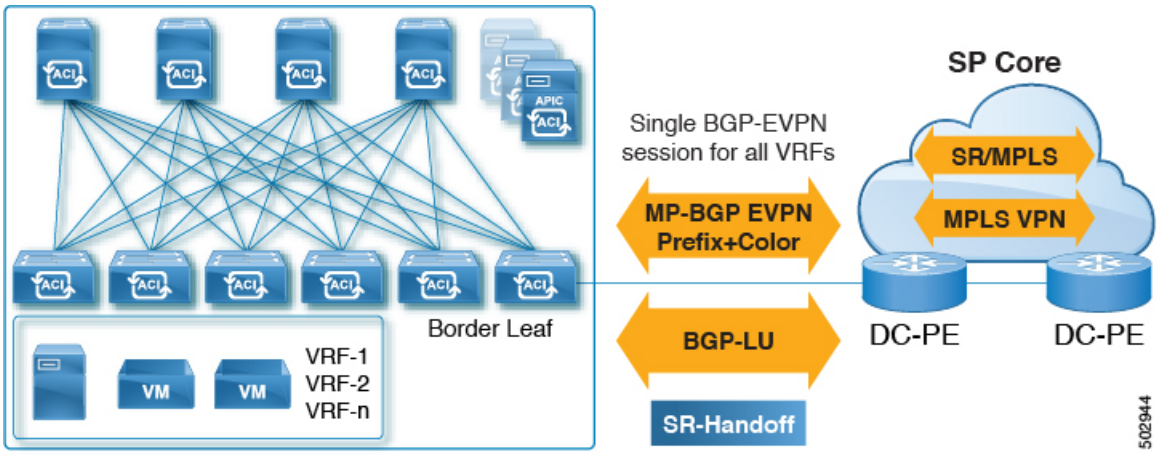
次のシナリオでは、DC-to-DC フローは VXLAN ではなくセグメント ルーティングを使用してカプセル化されます。



このシナリオでは、トランスポート ネットワークに使用される既存のモニタリング ツールは MPLS トラフィックをモニタできますが、VXLAN パケットはモニタできません。ACI から SR-MPLS へのハンドオフを使用することで、トランスポート チームは既存のモニタリング ツールを使用して DC-to-DC フローをモニタできます。

複数の VRF の単一コントロール プレーン セッション

SR ハンドオフを使用すると、単一のコントロール プレーン セッション（MP-BGP EVPN）が、IP ハンドオフ設定で使用する必要がある VRF 単位のセッションではなく、すべての VRF に使用されます。これにより、ACI データ センターと DC-PE 間の複数の VRF の自動化とスケーラビリティのオプションが向上します。

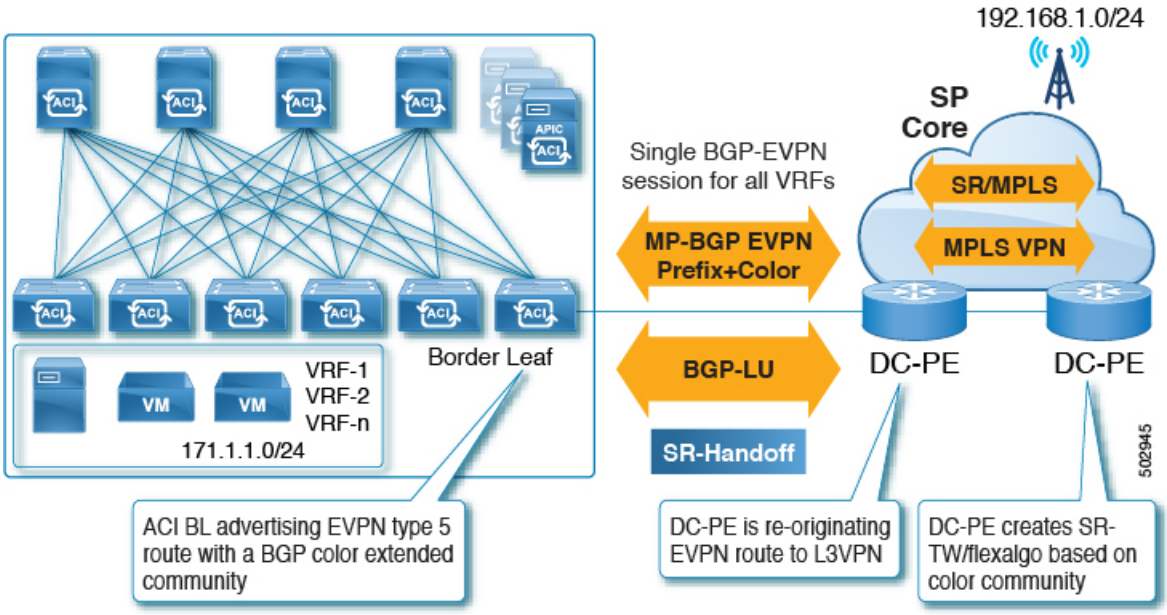


SR ハンドオフでは、VRF 単位のコントロール プレーンおよびデータ プレーン セッションの代わりに単一のコントロール プレーンおよびデータ プレーン セッションが使用され、Cisco ACI ファブリックから SP コアへの統合 SR トランスポートが使用されます。BGP ラベル ユニ

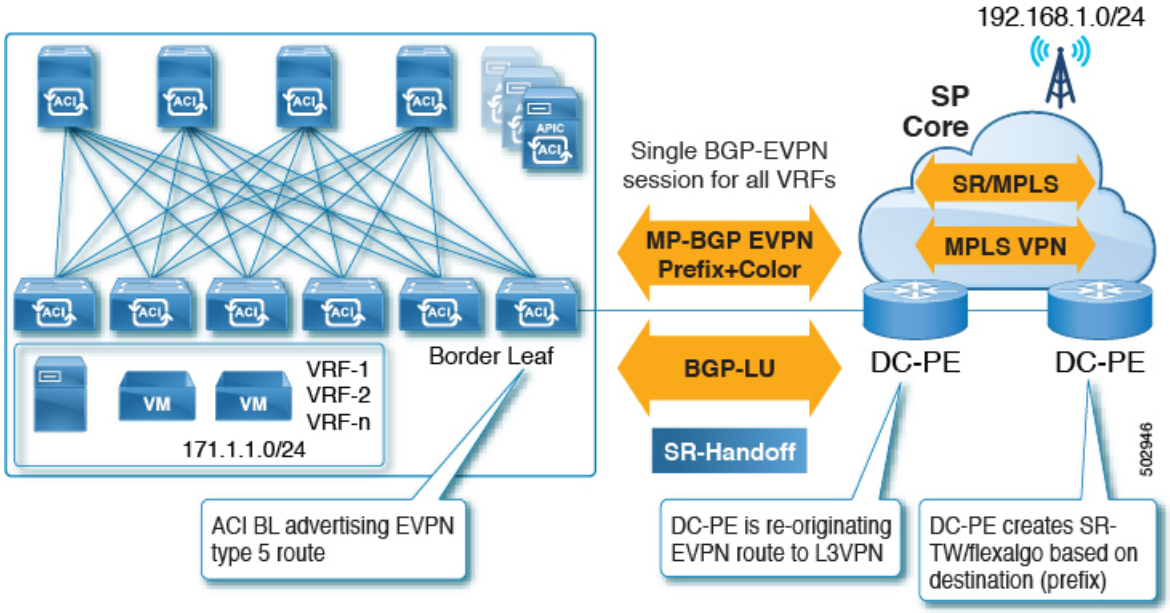
キャスト（BGP LU）アドレス ファミリは、アンダーレイ ラベル交換に使用されます。MP-BGP EVPN アドレス ファミリは、VRF 情報ごとにプレフィックスと MPLS ラベルを伝送します。

[カラー コミュニティ（Color Community）] または [宛先プレフィックス（Destination Prefix）] を使用したトランスポートの SR-TE / Flex Algo

SR ハンドオフは、SP コアで SR のシグナリングを自動化するため、有益です。この場合、ACI 境界リーフ スイッチは、BGP カラー拡張コミュニティを持つ EVPN タイプ 5 ルートを DC-PE にアドバタイズします。DC-PE は、ACI 境界リーフ スイッチから受信したカラー コミュニティまたは宛先プレフィックスに基づいてセグメント ルーティング ポリシーを作成できます。この機能により、DC とトランスポート ネットワークをシームレスに統合できます。



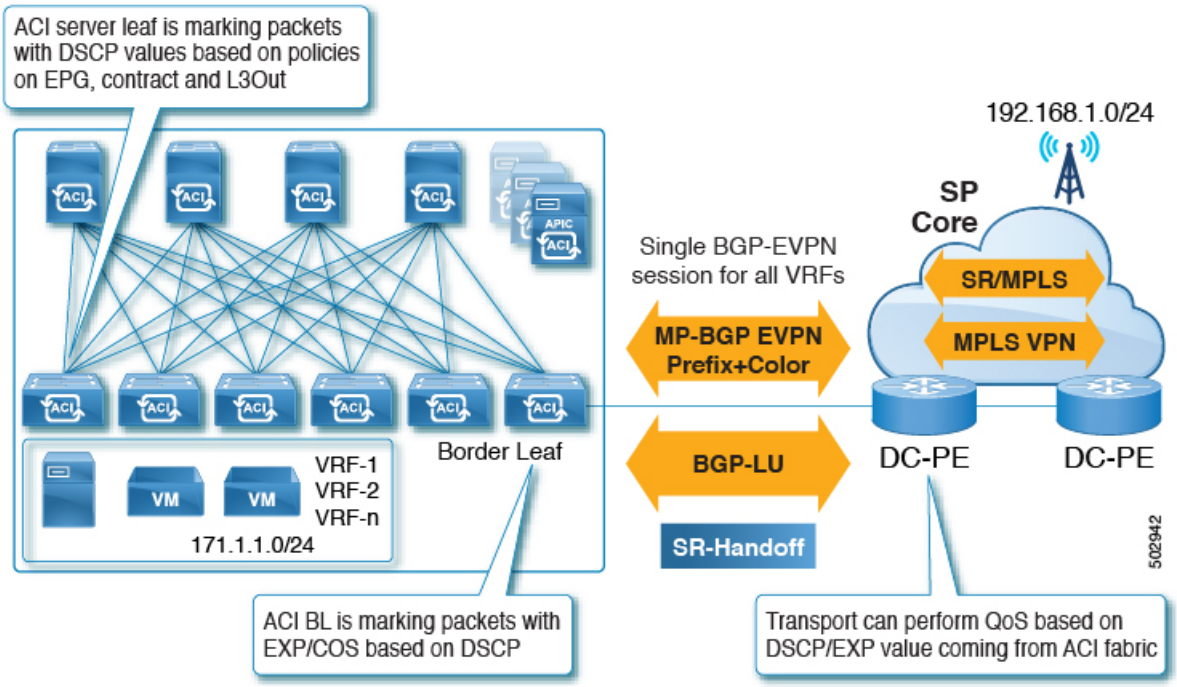
同様に、次の図に示すように、ACI 境界リーフ スイッチから EVPN タイプ 5 プレフィックスをアドバタイズでき、DC-PE は宛先プレフィックスに基づいて SR-TE または Flex Algo ルーティング ポリシーを作成できます。



2 つの方法のうち、カラー コミュニティを使用して DC-PE の設定を減らすことを推奨します。ただし、いずれの場合も、この方法で SR-MPLS を使用する前に、DC-PE にこの機能をサポートする機能があることを確認する必要があります。

SR または MPLS による DC およびトランスポート QoS

ACI ファブリック内では、非境界リーフ スイッチは、EPG、コントラクト、および L3Out QoS ポリシーを使用して DSCP 値でパケットをマーキングできます。これらの DSCP 値を使用して、ACI 境界リーフ スイッチで MPLS 出力ルールを設定し、Experimental Bit（EXP）または Class of Service（COS）値でパケットをマーキングできます。トランスポート ネットワークは、データ センターからの DSCP または EXP 値に基づいて、QoS アクションを実行したり、異なる SR または MPLS パスを選択したりできます。



同様に、MPLS 入力ルールを使用して、ACI 境界リーフ スイッチは、EXP 値に基づいてファブリックに着信する入力パケットを COS、DSCP、および QoS レベルでマーキングできます。QoS レベルはファブリック内の QoS アクションを定義します。

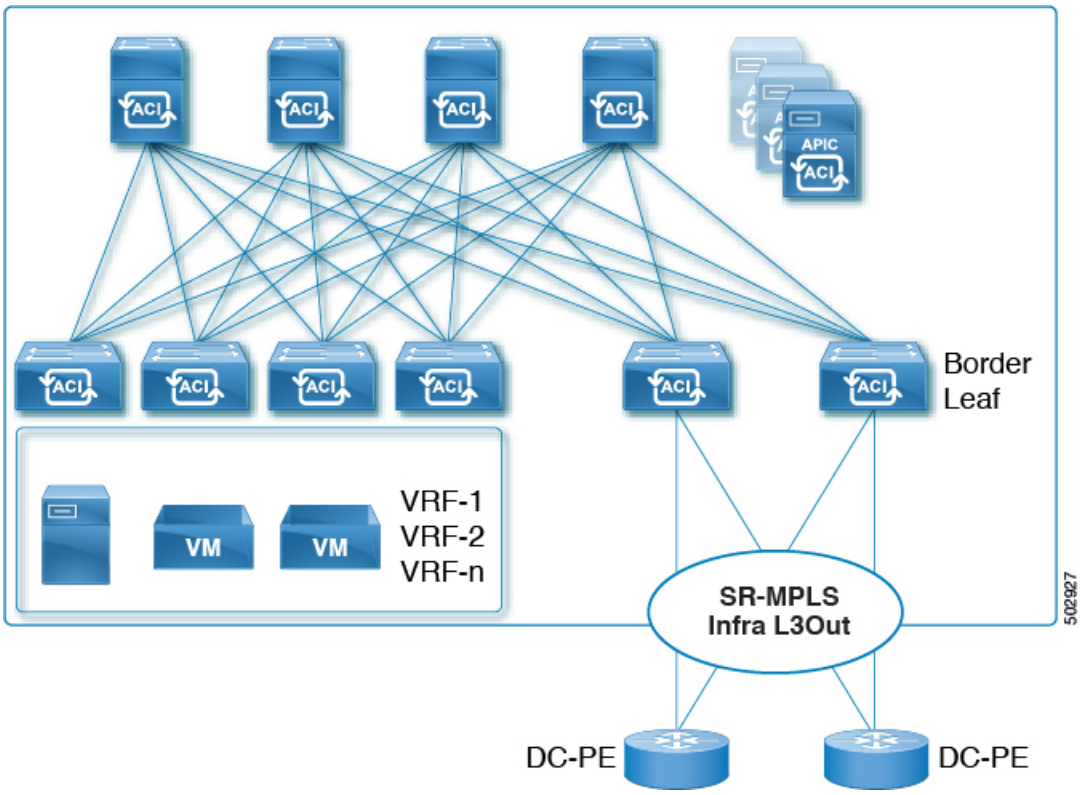
SR-MPLS ハンドオフの ACI 実装について

ACIは、Cisco APIC リリース 5.0(1) で導入された次の ACI コンポーネントを使用して SR-MPLS ハンドオフを実装します。

SR-MPLS インフラ L3Out

SR-MPLS インフラ L3Out は SR-MPLS 接続を提供します。境界リーフ スイッチのインフラ テナントで SR-MPLS インフラ L3Out を設定して、アンダーレイ MP-BGP EVPN セッションを SR-MPLS ハンドオフ用に設定します。テナント VRF インスタンスは Cisco Application Centric Infrastructure（ACI）SR-MPLS インフラ L3Out に選択的にマッピングされ、テナント サブネットを DC-PE ルータにアドバタイズし、DC-PE から MPLS VPN ルートをインポートします。SR-MPLS インフラ L3Out は、ポッドまたはリモート リーフ スイッチ サイトにスコープされ、ポッドまたはリモート リーフ スイッチ ペアに拡張されません。

図 *21 : SR-MPLS* インフラ *L3Out*



ポッドまたはリモート リーフ スイッチ サイトには、1 つ以上の SR-MPLS インフラ L3Out を設定できます。

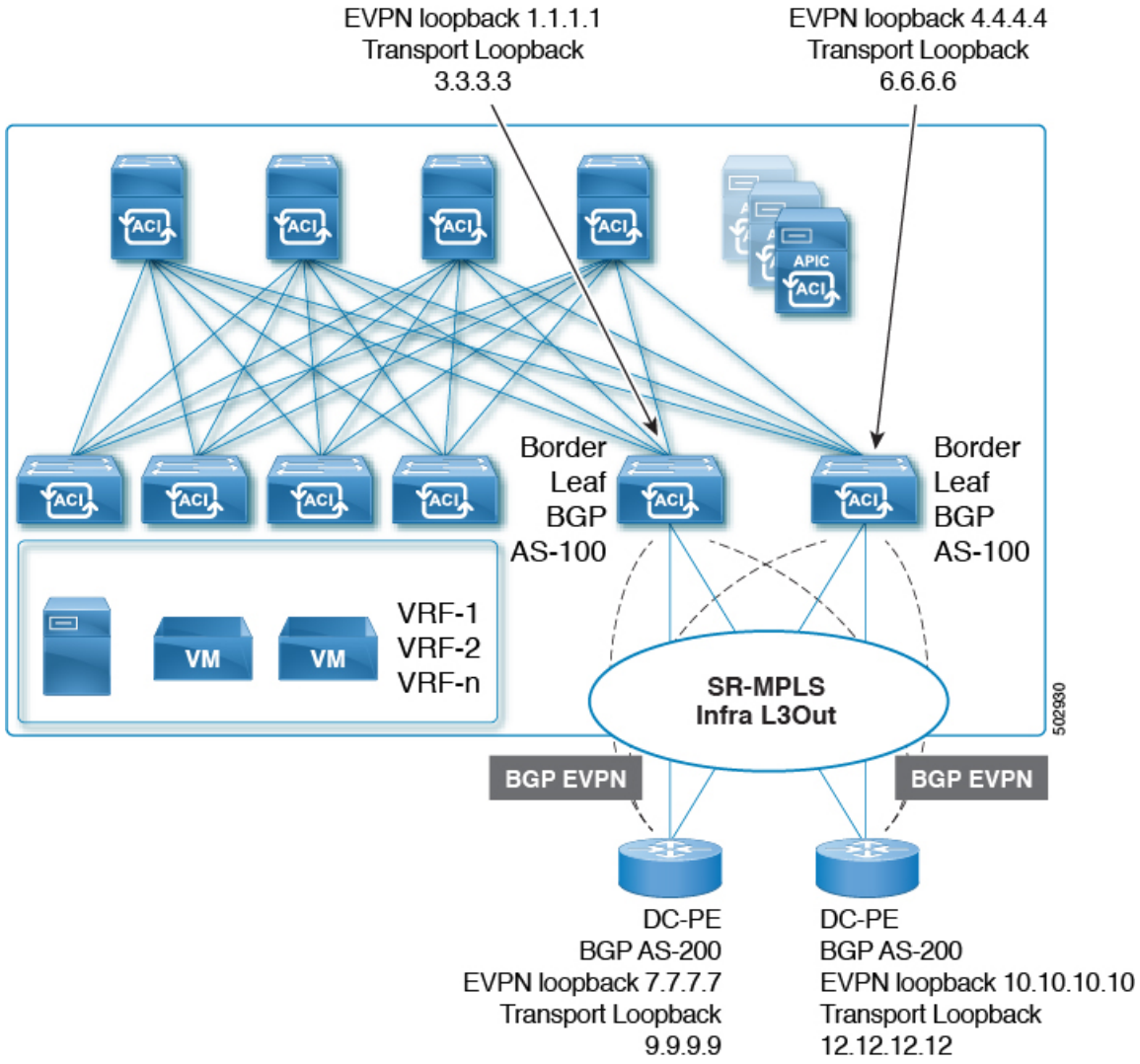
SR-MPLS インフラ L3Out の設定手順については、GUI を使用した SR-MPLS インフラ L3Out の設定 （208 ページ）を参照してください。

SR-MPLS インフラ L3Out の設定プロセスの一環として、次の領域を設定します。

- Cisco ACI 境界リーフ スイッチと DC-PE 間の MP-BGP EVPN セッション （188 ページ）
- BGP EVPN セッションのマルチホップ BFD （190 ページ）
- Cisco ACI 境界リーフ スイッチおよびネクストホップ ルータでのアンダーレイ BGP セッション（BGP ラベル付きユニキャストおよび IPv4 アドレス ファミリ） （190 ページ）
- BGP ラベル付きユニキャスト セッションのシングルホップ BFD （191 ページ）

Cisco ACI 境界リーフ スイッチと DC-PE 間の MP-BGP EVPN セッション

次の図に示すように、境界リーフ スイッチの EVPN ループバックと DC-PE ルータ間の MP-BGP EVPN セッションを設定するために必要な情報を提供する必要があります。



この領域では、次の設定が行われます。

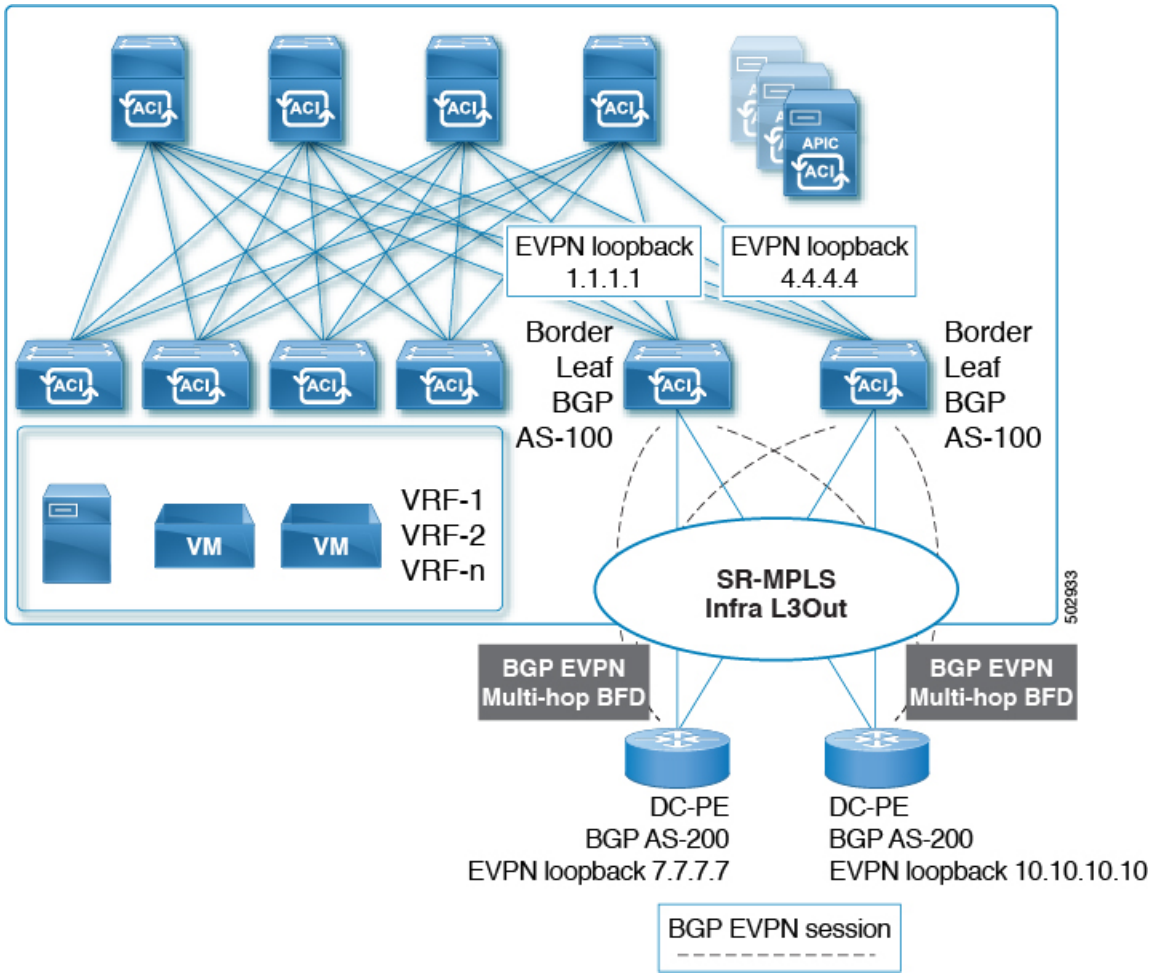
- BGP ラベル付きユニキャスト アドレス ファミリを使用したトランスポート ループバックのラベル アドバタイズメント。
- SR-MPLS インフラ VRF インスタンスの境界リーフ スイッチ上の一意のルータ ID。
- ルータ ID は、BGP-EVPN ループバックおよびトランスポート ループバック アドレスとは異なる必要があります。

図に示すように、MP-BGP EVPN とトランスポートのループバックに異なる IP アドレスを使用できますが、MP-BGP EVPN と Cisco ACI 境界リーフ スイッチのトランスポート ループバックに同じループバックを使用することを推奨します。

現時点では、eBGP セッションのみがサポートされています。

BGP EVPN セッションのマルチホップ BFD

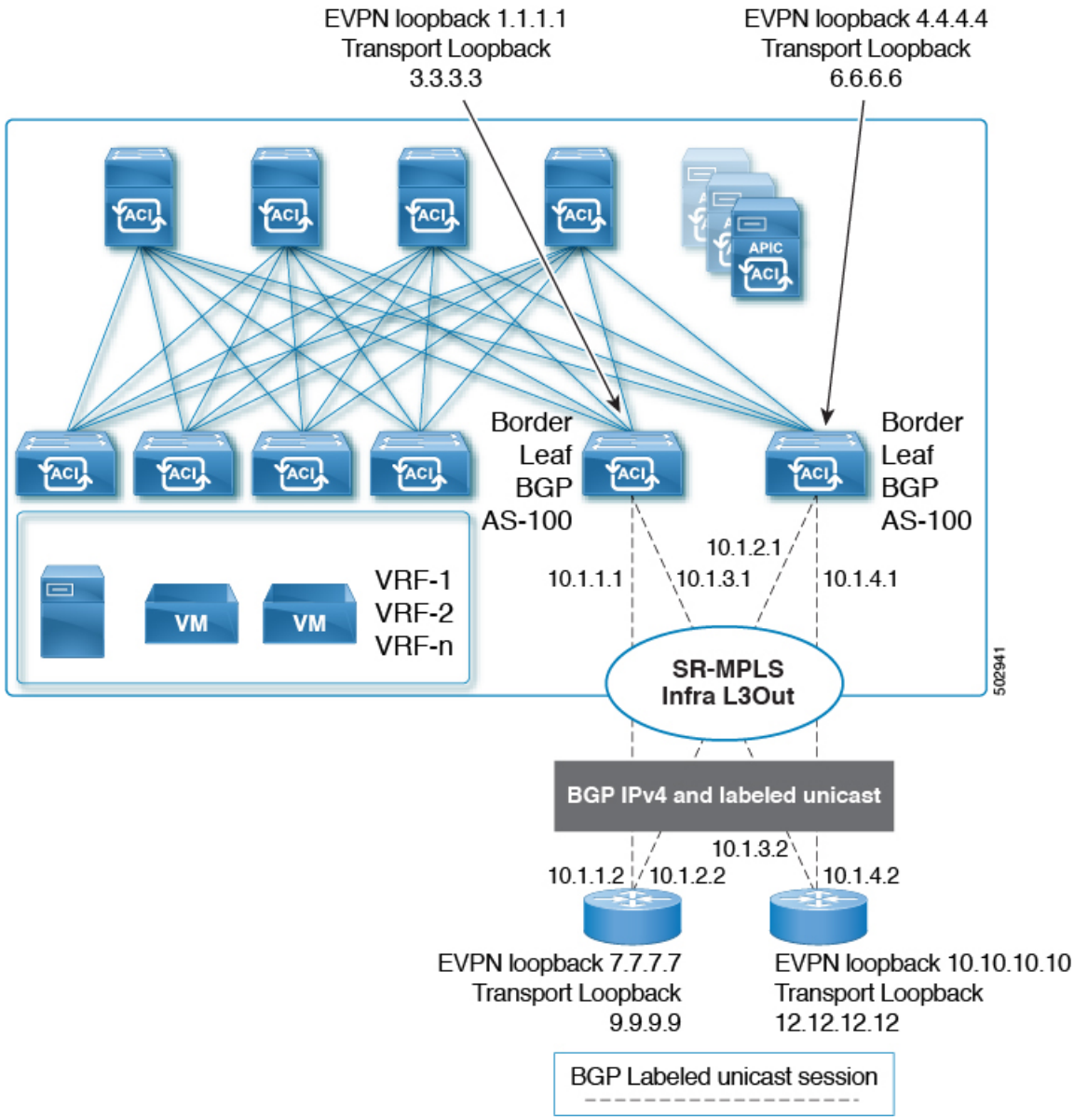
リリース5.0(1) から、次の図に示すように、マルチホップ BFD のサポートが可能になりました。この場合、EVPNループバック間にマルチホップBFDEVPNセッションを設定できます。



Cisco ACI 境界リーフ スイッチと DC-PE 間の BGP EVPN セッションでは、最小タイマーが 250 ミリ秒、検出乗数が 3 のマルチホップ BFD がサポートされます。要件に基づいてこのタイマー値は変更できます。

Cisco ACI 境界リーフ スイッチおよびネクストホップ ルータでのアンダーレイ BGP セッション（BGP ラベル付きユニキャストおよび IPv4 アドレス ファミリ）

また、次の図に示すように、Cisco ACI 境界リーフ スイッチと DC-PE 間のインターフェイスごとに、BGP IPv4 とラベル付きユニキャスト アドレス ファミリを設定します。

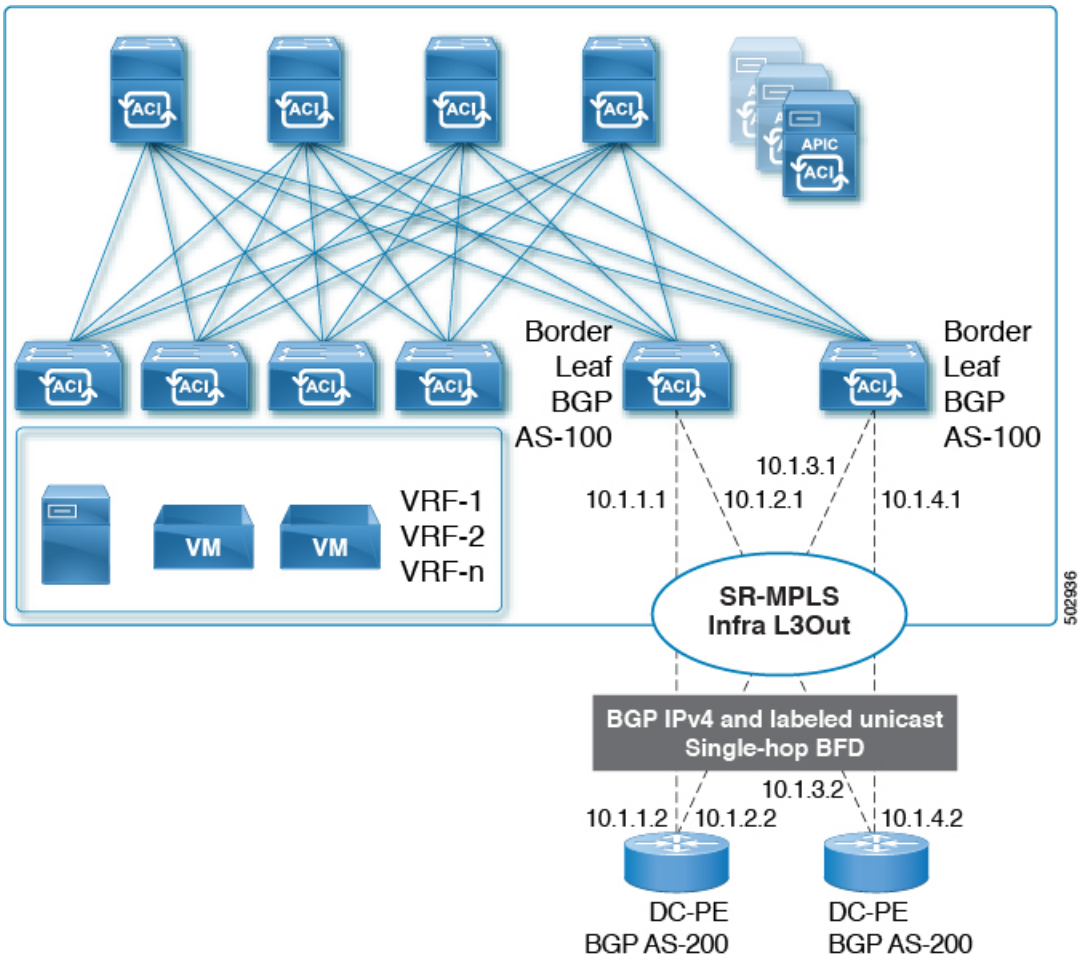


BGP IPv4アドレス ファミリは EVPN ループバックを自動的にアドバタイズし、BGP ラベル付きユニキャスト アドレス ファミリは SR-MPLS ラベルを使用して SR トランスポート ループバックを自動的にアドバタイズします。

現時点では、eBGP セッションのみがサポートされています。

BGP ラベル付きユニキャスト セッションのシングルホップ BFD

リンクがアップしたままで、リンクの転送機能が影響を受けるソフト障害に関連する問題を防ぐために、次に示すように、IPv4 および BGP ラベル付きユニキャスト セッションのアンダーレイ BGP セッションのシングルホップ BFD セッションを設定できます。次の図を参照してください。



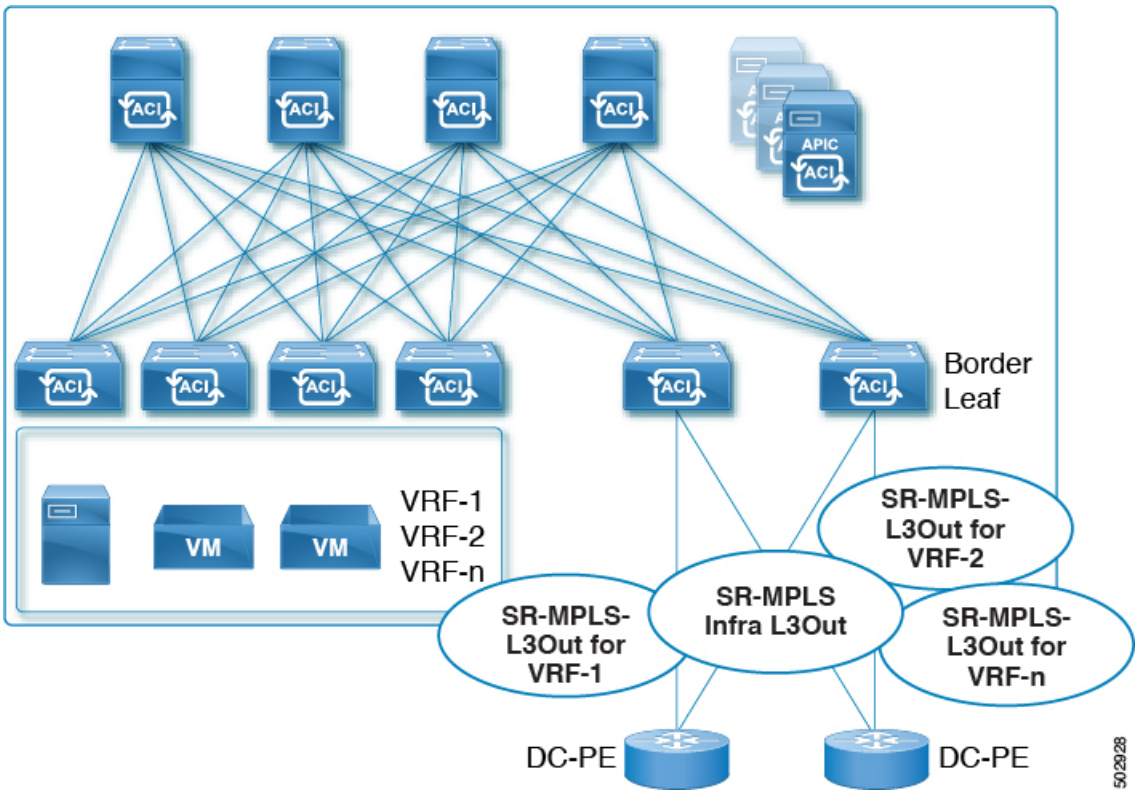
Cisco ACI 境界リーフ スイッチと DC-PE 間の BGP EVPN セッションでは、最小タイマーが 50 ミリ秒、検出乗数が 3 のシングルホップ BFD がサポートされます。要件に基づいてこのタイマー値は変更できます。

BFD モニタ対象リンクの一端または両端で BFD エコー機能を設定できます。エコー機能は設定された slow timer に基づいて必要最小受信間隔を遅くします。*[RequiredMinEchoRx]* BFD セッションパラメータは、エコー機能がディセーブルの場合、ゼロに設定されます。slow timer は、エコー機能がイネーブルの場合、必要最小受信間隔になります。

SR-MPLS VRF L3Out

SR-MPLS トランスポートに対してプレフィックスをアドバタイズする必要がある各 VRF は、SR-MPLS インフラ L3Out に関連付ける必要があります。SR-MPLS インフラ L3Out に接続されている SR-MPLS VRF L3Out を使用して、これらのアソシエーションを設定します。

図 *22 : User Tenant SR-MPLS L3Out*



1 つ以上の SR-MPLS VRF L3Out を同じ SR-MPLS インフラ L3Out に接続できます。SR-MPLS VRF L3Out を使用して、インポートおよびエクスポート ルート マップを設定し、次のことを実行できます。

- プレフィックスやコミュニティに基づいてルート ポリシーを適用する
- SR ネットワークにプレフィックスをアドバタイズする
- SR ネットワークから受信したプレフィックスを除外する

また、外部 EPG を各 SR-MPLS VRF L3Out テナントの 1 つ以上のサブネットで設定します。これは次の目的で使用されます。

- セキュリティ ポリシー（コントラクト）
- ポリシーベース リダイレクト（PBR）ポリシー
- VRF 間のルート リーク

SR-MPLS VRF L3Out の設定手順については、GUI を使用した SR-MPLS VRF L3Out の設定 （217 ページ）を参照してください。

SR-MPLS カスタム QoS ポリシー

カスタムQoSポリシーを使用して、MPLSネットワーク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、MPLS L3Out を介してトラフィックがファブリックを離れるときに、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 ポリシーを設定する場合、境界リーフ スイッチに適用される次の 2 つのルールを定義します。

- **入力ルール**：MPLSネットワークに接続されている境界リーフ スイッチに着信するすべてのトラフィックは、MPLS Experimental ビット（EXP）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、適切なCoSおよびDifferentiated Services Code Point（DSCP）値でマークされます。

  値は、境界リーフでカスタム QoS 変換ポリシーを使用して取得されます。SR-MPLS からのトラフィックの元のDSCP値は、再マーキングなしで保持されます。カスタムポリシーが定義されていないか、一致していない場合、デフォルトのQoSレベル（`Level3`）が割り当てられます。

- **出力ルール**：トラフィックが境界リーフのMPLSインターフェイスから離れていくと、パケットのDSCP値に基づいて照合され、一致が見つかると、MPLS EXPおよびCoS値がポリシーに基づいて設定されます。

  出力MPLS QoSポリシーが設定されていない場合、MPLS EXPはデフォルトでゼロになります。MPLS カスタム QoS ポリシーに基づいて設定されている場合は、EXP が再マーキングされます。

次の2つの図は、入力および出力ルールが適用されるタイミングと、内部ACIトラフィックがファブリック内でパケットの QoS フィールドを再マーキングする方法を要約しています。

図 *23* : 入力 *QoS*

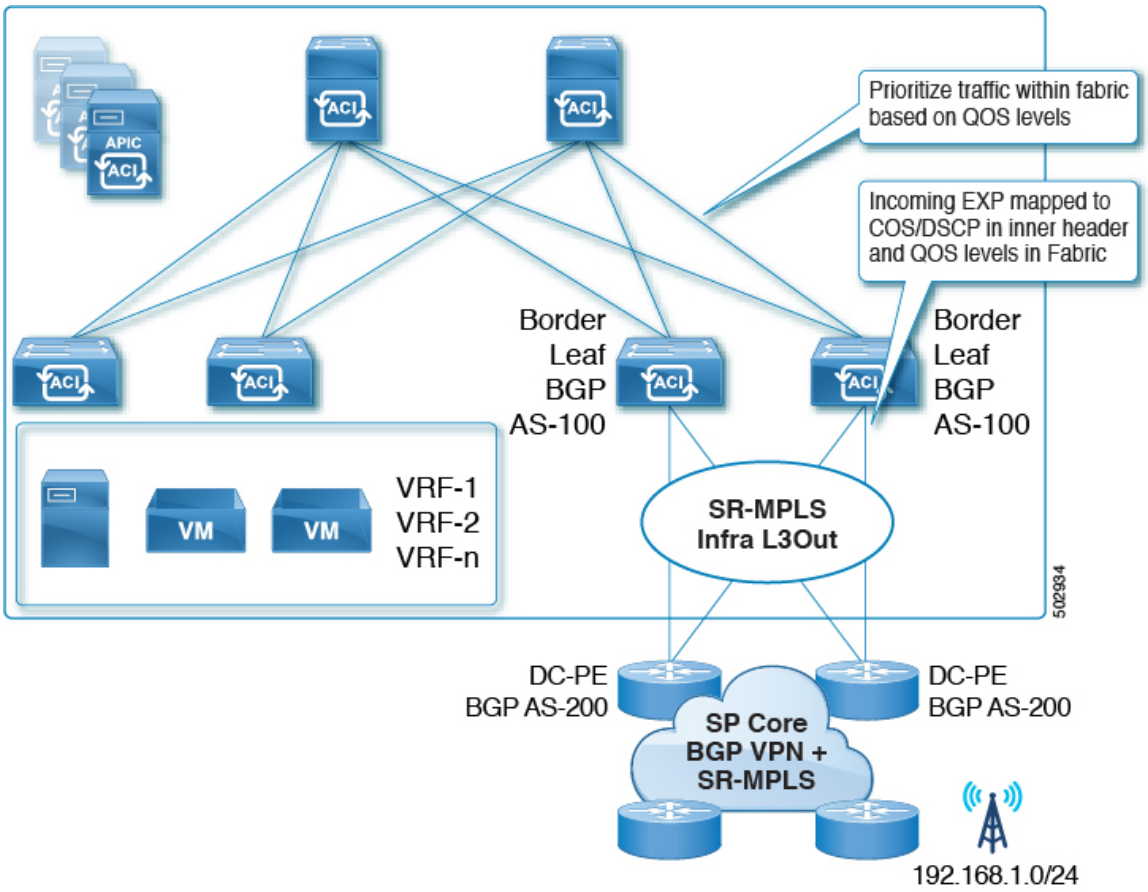
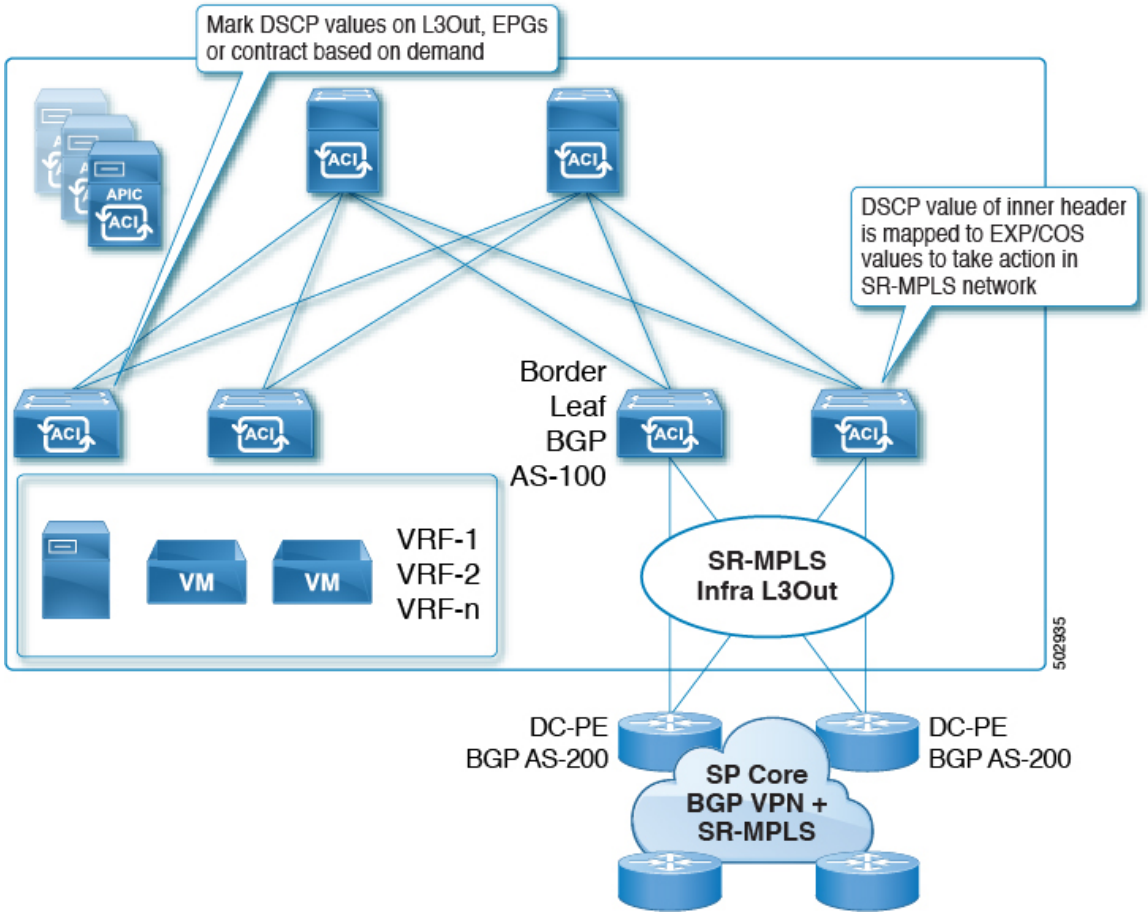

APIC
ACI
Prioritize traffic within fabric based on QOS levels
Incoming EXP mapped to COS/DSCP in inner header and QOS levels in Fabric
Border Leaf BGP AS-100
Border Leaf BGP AS-100
VM
VM
VRF-1
VRF-2
VRF-n
SR-MPLS Infra L3Out
502934
DC-PE BGP AS-200
DC-PE BGP AS-200
SP Core BGP VPN + SR-MPLS
192.168.1.0/24

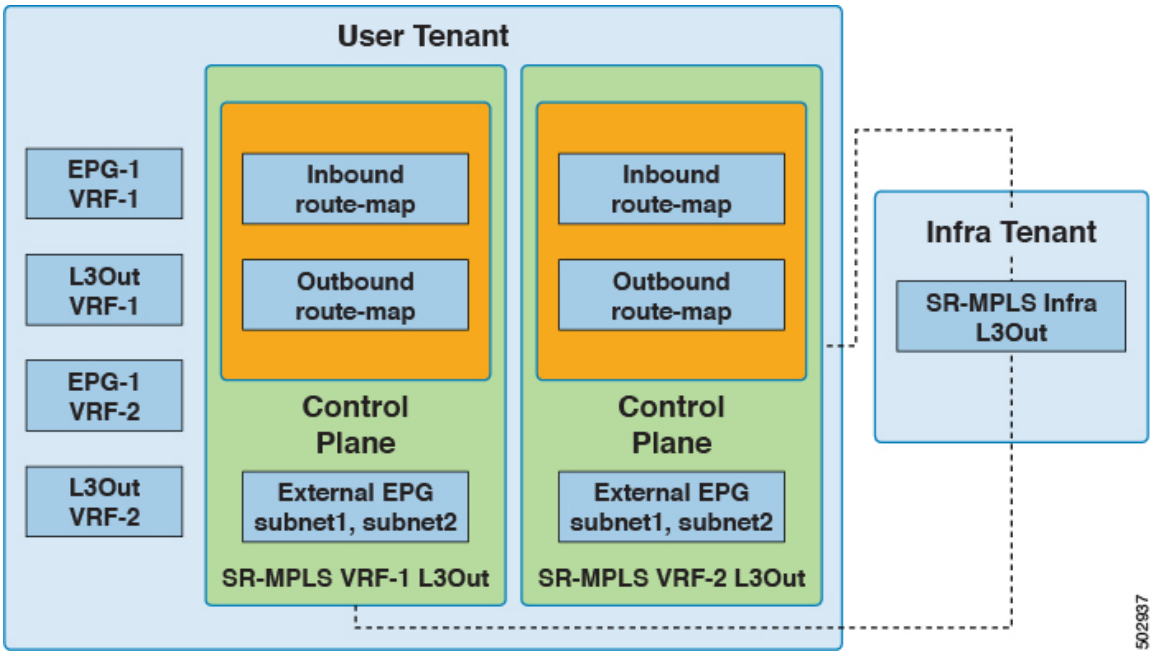
図 *24 :* 入力 *QoS*



GUI を使用した SR-MPLS カスタム QoS ポリシーの作成 （221 ページ）の説明に従って、複数のカスタム QoS ポリシーを定義し、作成した各 SR-MPLS インフラ L3Out に適用できます。

SR-MPLS 設定モデルについて

次の図に、SR-MPLS ハンドオフの ACI 実装の設定モデルを示します。



SR-MPLS ハンドオフの設定は、次のテナント内で行われます。

- **Infra Tenant**：インフラ テナントの下で、SR-MPLS インフラ L3Out （187 ページ）の説明に従って SR-MPLS インフラ L3Out を設定します。SR-MPLS インフラ L3Out では、ACI ファブリックと境界リーフ スイッチに接続された外部デバイス間の接続を定義します。SR-MPLS インフラ L3Out でオーバーレイおよびアンダーレイ ノード パスを指定します。
- **ユーザ テナント**：ユーザ テナントの下に、図の左側の領域に示すように、複数の VRF、EPG、および L3Out がある場合があります。ユーザ テナント内で、SR-MPLS ハンドオフ設定の一部として使用する SR-MPLS VRF L3Out を設定します。SR-MPLS VRF L3Out （192 ページ）

  SR-MPLS VRF L3Out 内では、次のルート マップも設定します。

  - **着信ルート マップ**：デフォルトでは、着信ルート マップのポリシーはすべてのプレフィックスを受け入れます。

    明示的な着信ルート マップは、次のように設定できます。

    - ファブリック内のアドバタイズメントを選択的に拒否するプレフィックスを一致させる
    - プレフィックスとコミュニティを照合して、ファブリック内のアドバタイズメントを選択的に拒否する

  - **アウトバウンド ルート マップ**：ブリッジ ドメイン サブネットを含む任意のプレフィックスをアドバタイズするために、アウトバウンド ルート マップのポリシーを設定する必要があります。デフォルトでは、アウトバウンド ルート マップのポリシーはプレフィックスをアドバタイズしません。

    明示的なアウトバウンド ルート マップは、次のように設定できます。

- SR-MPLS ネットワークにアドバタイズされるプレフィックスの照合
- SR-MPLS ネットワークにプレフィックスをアドバタイズするためのプレフィックスとコミュニティの照合
- プレフィックスやコミュニティの一致に基づいて、カラーコミュニティを含むコミュニティを設定します。

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がコントロールプレーンに使用され、ファブリック内外で許可または拒否されるプレフィックスを設定します。

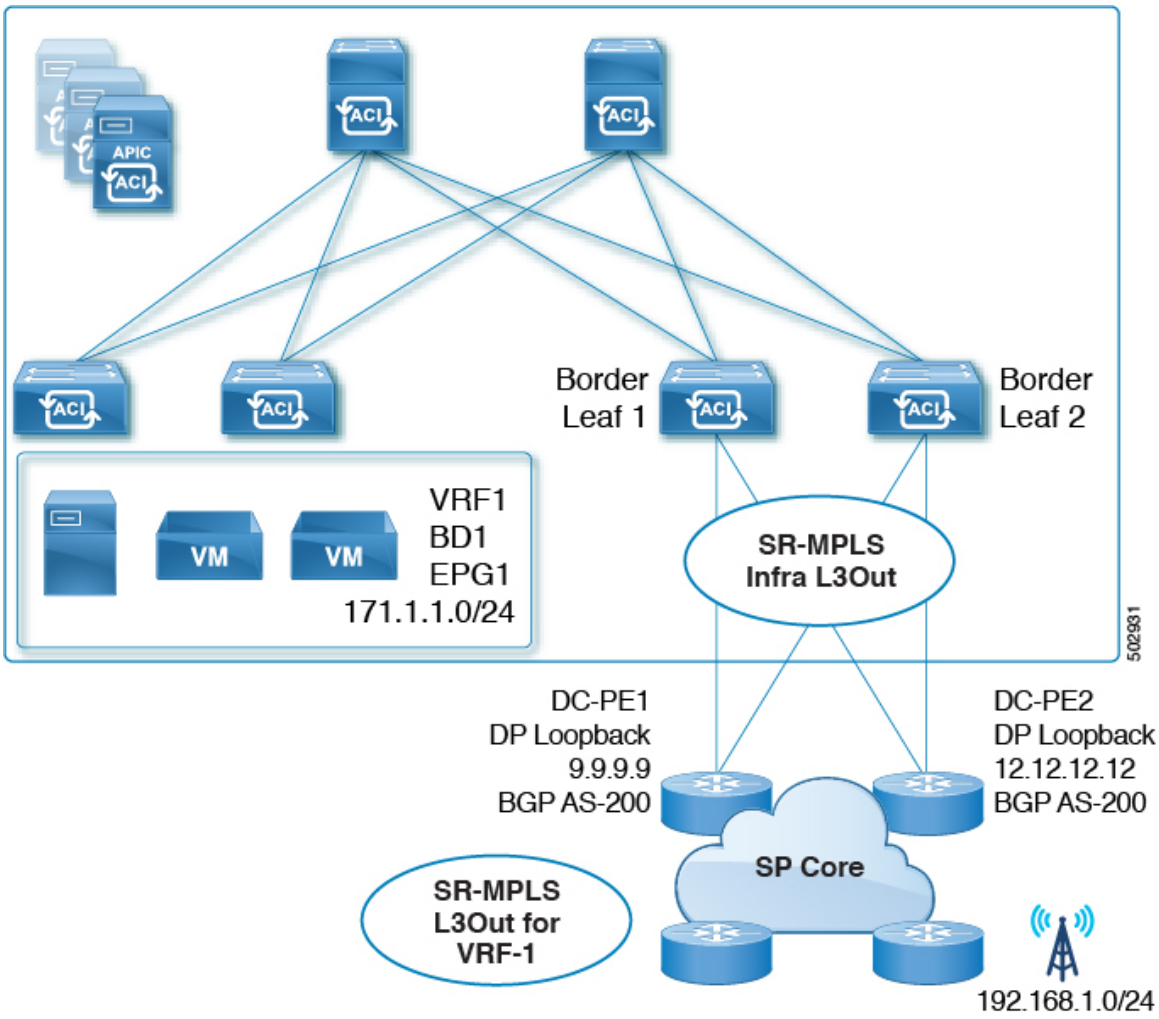
SR-MPLS VRF L3Out 内で、外部 EPG と、データ プレーンに使用される該当の外部 EPG 内のサブネットも設定します。これらのサブネットは、ACIセキュリティ ポリシーを適用するために使用されます。外部 EPG サブネットは、フラグを使用して別の VRF のプレフィックスをリークするためにも使用されます。外部 EPG サブネットでルート リークとセキュリティ フラグを有効にすると、そのサブネットは別の VRF にリークされる可能性があります。集約フラグを使用して外部 EPG サブネットを設定し、プレフィックスを別の VRF にリークすることもできます。この場合、リーフ スイッチ プレフィックスへのコントラクトを定義し、VRF 間の通信を許可する必要があります。

（注） SR-MPLS VRF L3Out 上の外部 EPG は、ルート マップを適用してプレフィックスアドバタイズメントを拒否するなど、ルーティング ポリシーには使用されません。

この例では、ユーザ テナント内の SR-MPLS VRF-1 L3Out が SR-MPLS インフラ L3Out に接続され、ユーザ テナント内の SR-MPLS VRF-2 L3Out も SR-MPLS インフラ L3Out に接続されます。

EPG to SR-MPLS L3Out

次の図は、EPG to SR-MPLS L3Out 設定の例を示します。

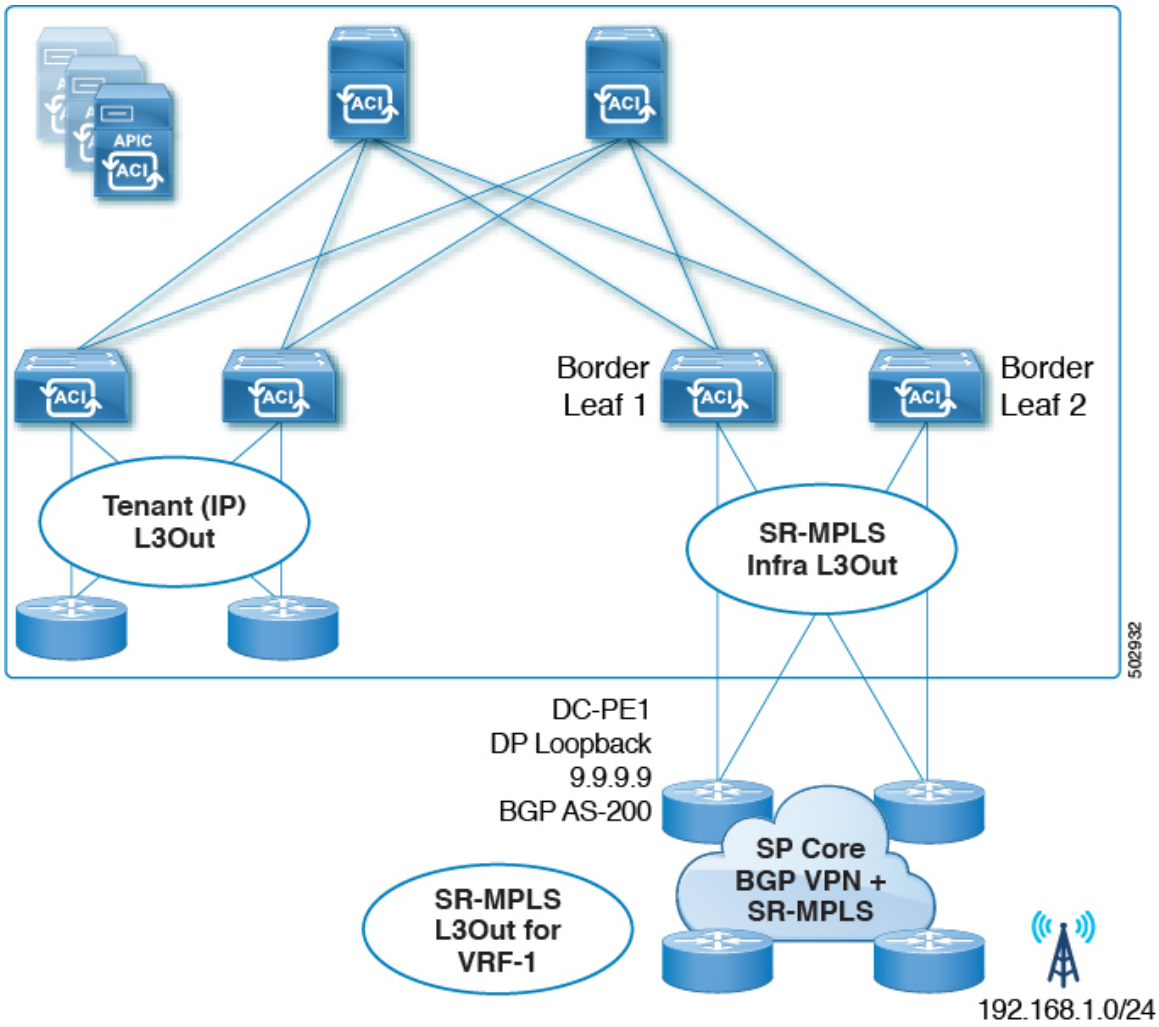


このシナリオでは、次の設定を行います。

- 境界リーフ スイッチ（上図の BL1 と BL2）で SR-MPLS infra L3Out を設定します。
- EPG、ブリッジドメイン、およびユーザ VRF とともに、ユーザテナントで SR-MPLS VRF L3Out を設定します。
- プレフィックスのエクスポートおよびインポート用のルートマップを設定し、SR-MPLS VRF L3Out に適用します。
- EPG と SR-MPLS L3Out 間のトラフィック転送のために、EPG と SR-MPLS VRF L3Out で定義された外部 EPG の間に契約を設定し、適用します。

IP L3Out to SR-MPLS L3Out

次の図に、通常の IP L3Out と SR-MPLS L3Out の間の中継ルーティングを有効にする設定の例を示します。



このシナリオでは、前述の EPG から SR-MPLS L3Out への設定と同様の設定を行いますが、その違いは次のとおりです。

- 境界リーフ スイッチ（上図の BL1 と BL2）で SR-MPLS infra L3Out を設定します。
- IP L3Out およびユーザ VRF とともに、ユーザ テナントで SR-MPLS VRF L3Out を設定します。
- プレフィックスのエクスポートおよびインポート用のルート マップを設定し、SR-MPLS VRF L3Out に適用します。
- IP L3Out と SR-MPLS L3Out 間のトラフィック転送のために、IP L3Out と SR-MPLS VRF L3Out に関連付けられた外部 EPG 間にコントラクトを設定し、適用します。

SR-MPLS のガイドラインおよび制限事項

次は、SR-MPLS ハンドオフ機能のガイドラインおよび制限事項です。

SR-MPLS でサポートされるプラットフォーム

SR-MPLS ハンドオフ機能は、次のプラットフォームでサポートされます。

- **ボーダー リーフ スイッチ** : -FX スイッチ モデル以降 (たとえば、スイッチ名の末尾に「FX」、「FX2」、「FX3」、「GX」... が付いているスイッチ モデル)
- **スパイン スイッチ**:
  - ラインカード名の末尾に「LC-EX」、「LC-FX」、および「GX」が付いたモジュラ スパイン スイッチ モデル
  - 固定スパイン スイッチの Cisco Nexus 9000 シリーズ N9K-C9364C および N9K-C9332C
- DC-PEルータ：
  - Network Convergence System（NCS）5500 シリーズ
  - ASR 9000 シリーズ
  - NCS 540 または 560 ルータ
  - ASR1000/IOS-XE プラットフォーム
- Cisco Application Centric Infrastructure（ACI）から SR-MPLS へのハンドオフ ソリューションは、SR-MPLS、BGP-LU、BGP EVPN、および BGP EVPN と VPNv4/v6 間のプレフィックス再発信を使用した標準ベースの実装を使用します。これらのテクノロジーをサポートする DC-PE は、Cisco ACI から SR-MPLS へのハンドオフをサポートできる必要があります。

（注） SR-MPLS ハンドオフを備えた Cisco Application Centric Infrastructure（ACI） ボーダー リーフ スイッチが IOS-XE ソフトウェアを実行している PE デバイスに接続されている場合、IOS-XE デバイスは、BGP L2VPN EVPN アドレス ファミリー下において、「neighbor <aci-leaf> next-hop-unchanged」で構成する必要があります。next-hop-unchanged 構成では、Cisco ACI ボーダー リーフ スイッチはリモート PE ループバックを学習する必要があります。

SR-MPLS のプラットフォーム制限

- FX プラットフォームでは、SR-MPLS 機能を有効にすると、MPLS が有効になっていない、または展開されていないポートを含むすべてのポートで MPLS 解析が有効になります。FX2 プラットフォーム以降では、MPLS 解析は、SR-MPLS が有効化または展開されているポートでのみ有効化されます。
- MPLS 解析が有効になっているポートでは、MPLS カプセル化パケットの純粋なレイヤ 2 スイッチングはサポートされていません。非 MPLS レイヤー 2 トラフィックは、問題なく、レイヤー 2 トランジットとして Cisco ACI ファブリックを使用できます。

SR-MPLS インフラ L3Out のガイドラインと制約事項

- ボーダー リーフ スイッチが複数の SR-MPLS Infra L3Out にあることができる場合でも、ボーダー リーフ スイッチ/プロバイダ エッジ ルーターの組み合わせは 1 つの SR-MPLS L3Out になければなりません。ユーザ VRF/ボーダー リーフ スイッチ/プロバイダ エッジ ルートの組み合わせに対して 1 つのルーティング ポリシーのみが存在できるからです。
- 複数のポッドおよびリモート ロケーションから SR-MPLS 接続を確立する必要がある場合は、SR-MPLS 接続を使用するポッドおよびリモート リーフ ロケーションのそれぞれに異なる SR-MPLS インフラ L3Out があることを確認します。
- SR-MPLS インフラ L3Out はマルチキャストをサポートしていません。

Routing Policy

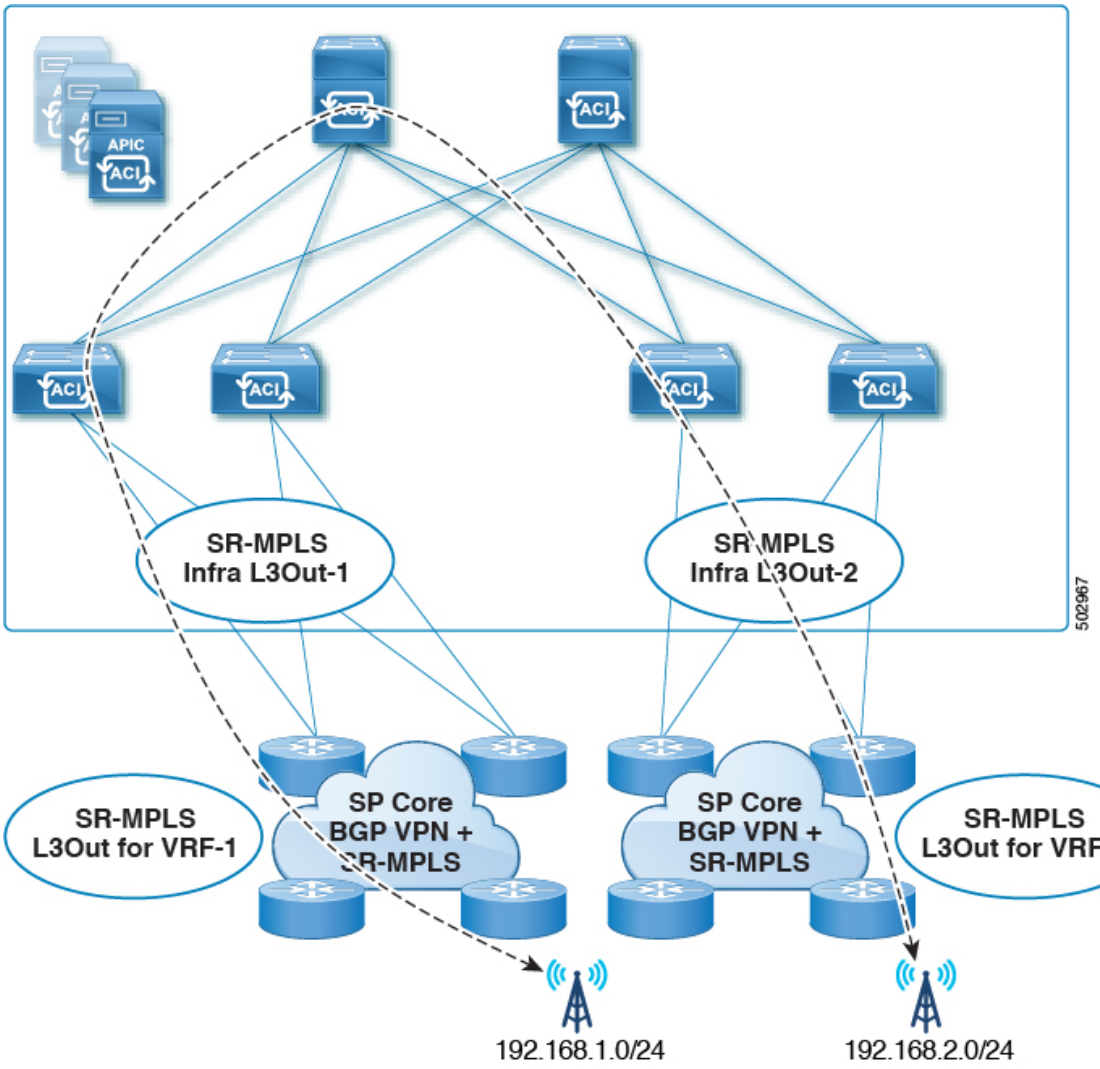
- **サポート対象**：Cisco APIC リリース 6.1(1) 以降では、リモートリーフのファブリック ポートを、ルーテッド サブ インターフェイスとして SRMPLS インフラ l3out に展開できるようになりました。

SR-MPLS VRF L3Out のガイドラインと制約事項

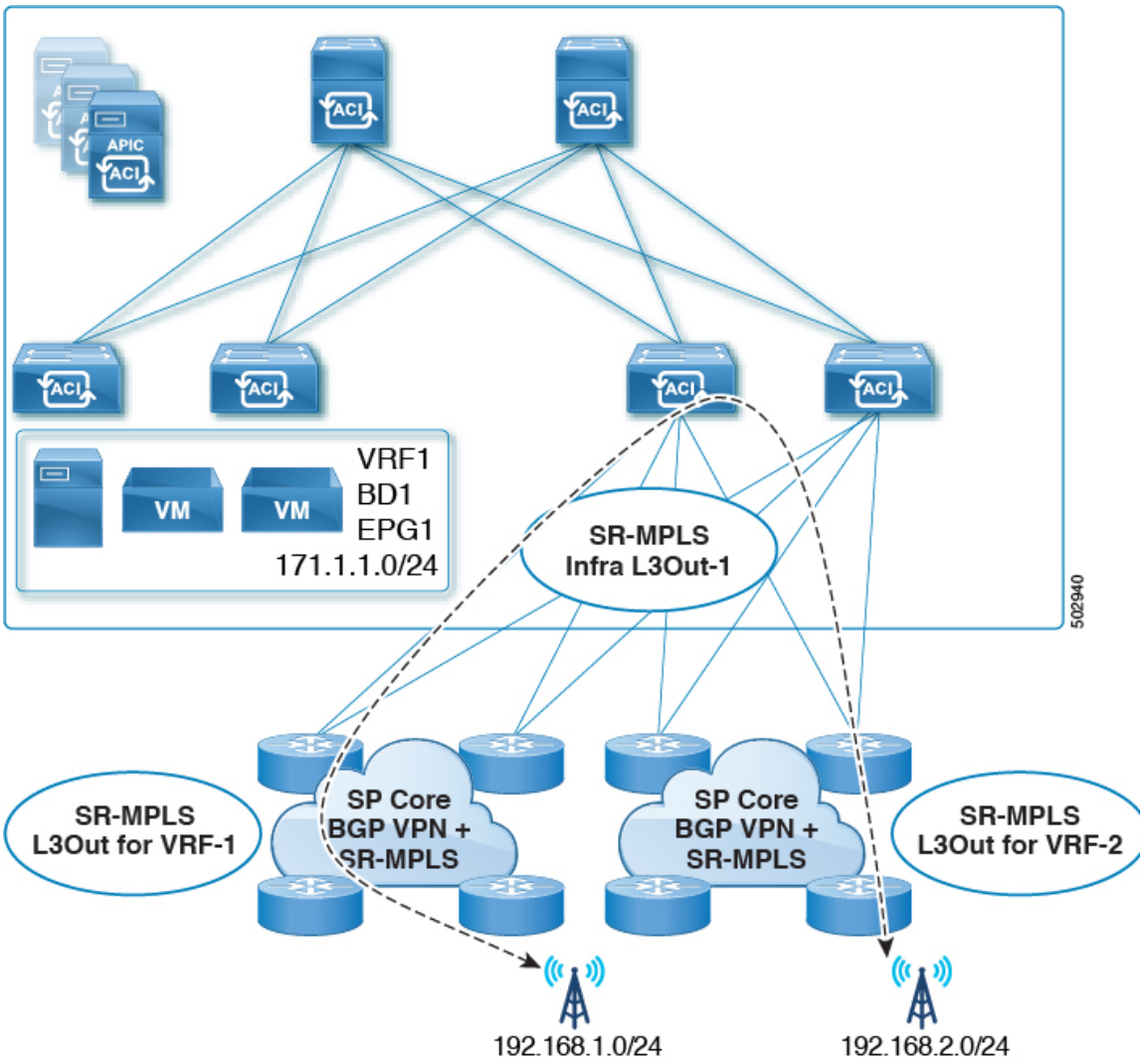
Routing Policy

- 各 SR-MPLS VRF L3Out 内では、アウトバウンド ルート マップ（エクスポート ルーティング ポリシー）の定義は必須ですが、インバウンド ルート マップ（インポート ルーティング ポリシー）の定義はオプションです。

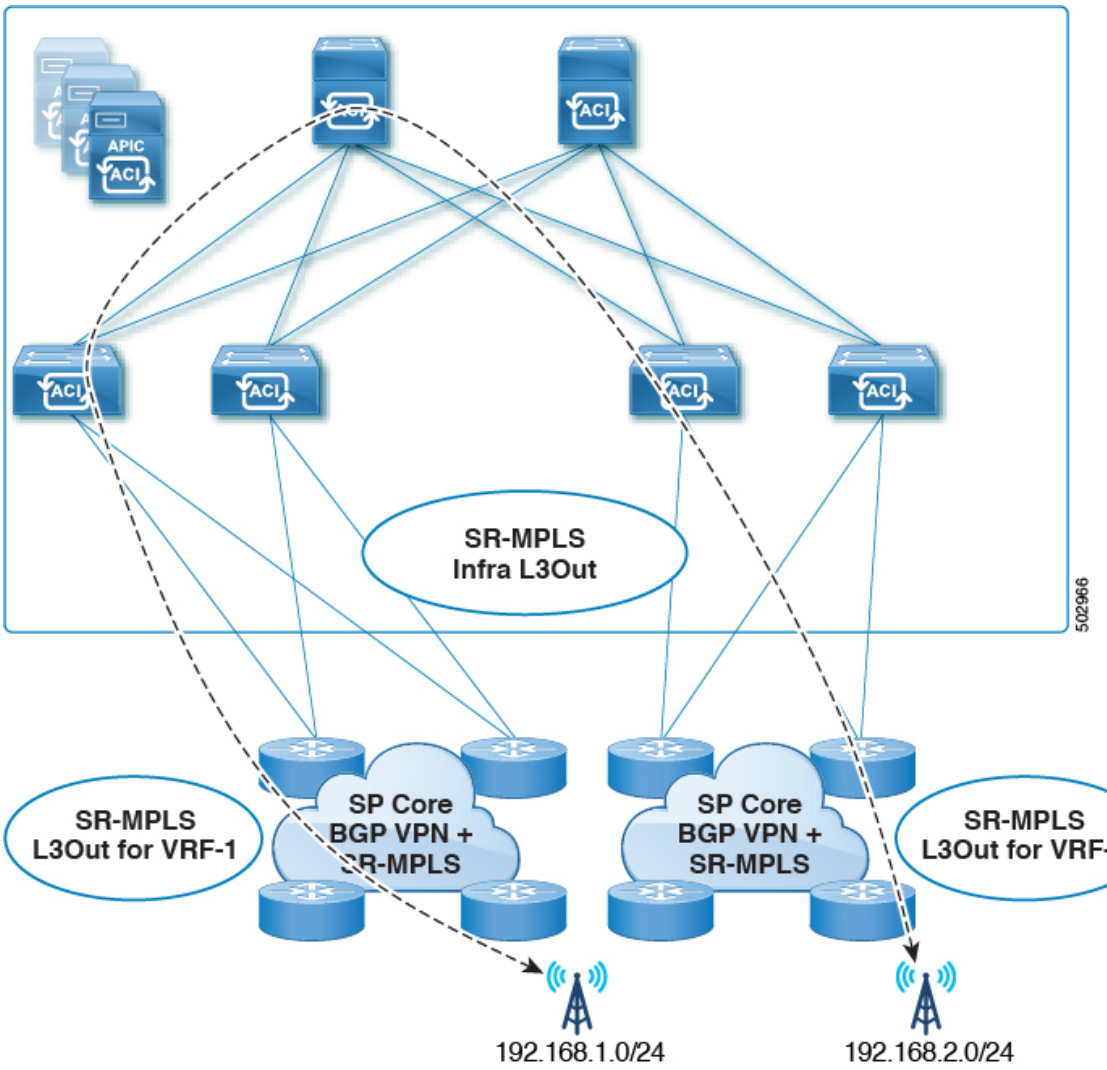
- SR-MPLS VRF L3Out に関連付けられているルーティング ポリシーは、グローバル タイプである必要があります。つまり、ブリッジ ドメイン サブネットを含むすべてのルートを明示的に追加する必要があります。
- ホストベース ルーティングは SR-MPLS ではサポートされません。
- 移行ルーティングがサポートされますが、一部の制約があります。
  - サポート対象：次の図に示すように、異なるボーダー リーフ ペアを使用する単一の VRF での SR-MPLS トラフィック。この設定では、各 SR-MPLS インフラ L3out（ボーダー リーフ ペア）を介して一意のプレフィックス範囲をアドバタイズする必要があります。また、トランスポート ネットワークにルーティング ループがないことを確認する必要があります（つまり、ファブリックがハブとして機能し、2 つのトランスポート ネットワークがスポークとして機能している）。



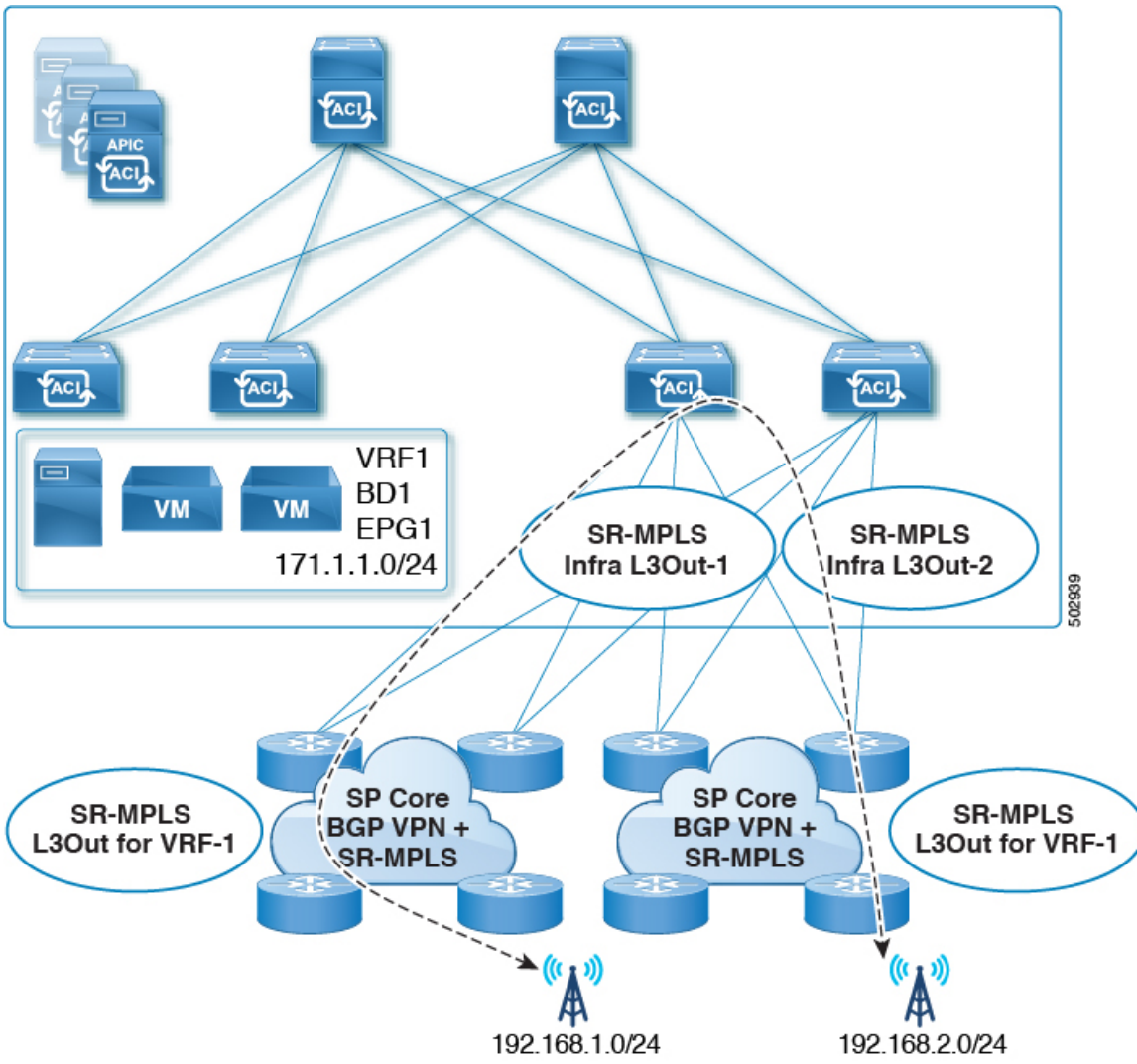
  - サポート対象：次の図に示すように、同じ境界リーフ ペアと異なる VRF を持つ SR-MPLS トラフィック。



- サポート対象：次の図に示すように、異なる境界リーフ ペアと異なる VRF を持つ SR-MPLS トラフィック。



- 次の図に示すように、同じ VRF 内および同じ境界リーフ ペア上の SR-MPLS トラフィックを中継します。
  - リリース 5.1(1) よりも前のリリースではサポートされません。
  - リリース 5.1(1) 以降でサポートされます。システムでの一時的なループを回避するために、再発信されたルートが同じ Infra L3Out ピアにアドバタイズされないようにします。



- リーフ スイッチが複数の SR-MPLS インフラ L3Out で設定されている場合、プレフィックスが単一のプレフィックス リスト（1 つの一致ルール）で設定されていれば、同じサブネットをすべての L3Out からアドバタイズできます。その後、そのプレフィックス リストのルート マップは、すべての SR-MPLS VRF L3Out に関連付けられます。

  たとえば、次のようなコンフィギュレーションがあるものとします。

  - サブネット S1 と S2 を持つ単一のプレフィックス リスト P1
  - ルート マップ R1 に関連付けられている SR-MPLS VRF L3Out 1（プレフィックス リスト P1）
  - ルート マップ R2 に関連付けられている SR-MPLS VRF L3Out 2（プレフィックス リスト P1）

プレフィックスは同じプレフィックス リスト（P1）に設定されているため、異なるSR-MPLS VRF L3Out に関連付けられていても、プレフィックス リスト P1 内の同じサブネットが両方の L3Out からアドバタイズされます。

一方、次の設定を検討します。

- 2 つのプレフィックス リスト
  - プレフィックス リスト P1、サブネット S1 および S2
  - プレフィックス リスト P2、サブネット S1 および S2
- ルート マップ R1 に関連付けられている SR-MPLS VRF L3Out 1（プレフィックス リスト P1）
- ルート マップ R2 に関連付けられている SR-MPLS VRF L3Out 2（プレフィックス リスト P2）

プレフィックスは2つのプレフィックス リスト（P1 と P2）で設定され、異なる SR-MPLS VRF L3Out に関連付けられているため、サブネット S1 と S2 は両方の L3Out からアドバタイズされません。

- SR-MPLS VRF L3Out はマルチキャストをサポートしていません。

Security Policy

- SR-MPLS VRF L3Out 内で定義されている外部 EPG インスタンス プロファイルを使用してセキュリティ ポリシーを設定できます。外部 EPG インスタンス プロファイルには、1 つ以上の SR-MPLS インフラ L3Out から SR-MPLS ネットワークを介して到達可能な IP プレフィックスが含まれており、同じセキュリティ ポリシーが必要です。
- 外部 EPG インスタンス プロファイルで 0/0 プレフィックスを設定して、外部 EPG の一部として、任意の外部IPアドレスから発信された着信トラフィック フローを分類できます。
- 外部 EPG インスタンス プロファイルの外部 EPG を 1 つ以上の SR-MPLS VRF L3Out に関連付けることができます。外部 EPG インスタンス プロファイルが複数の SR-MPLS インフラ L3Out の外部にある場合、複数の SR-MPLS VRF L3Out は同じ外部 EPG インスタンス プロファイルを指します。
- ローカル EPG と外部 EPG インスタンス プロファイル間、または異なる VRF L3Out に関連付けられた外部 EPG 間でコントラクトを設定する必要があります（中継ルーティングを有効にするため）。

MPLS スイッチングに関するガイドラインと制限事項

次に、MPLS QoS のデフォルトの動作を示します。

- サービスクラス（COS）の保持は、宛先ポートが MPLS ポートである ToR 内 MPLS 出力 QoS ポリシーではサポートされません。

- 境界リーフ スイッチ上のすべての受信 MPLS トラフィックは QoS レベル 3（デフォルトの QoS レベル）に分類されます。
- 境界リーフ スイッチは、再マーキングなしで SR-MPLS からのトラフィックの元の DSCP 値を保持します。
- 境界リーフ スイッチは、デフォルトの MPLS EXP（0）のパケットを SR-MPLS ネットワークに転送します。

次に、MPLS カスタム QoS ポリシーを設定する際のガイドラインと制約事項を示します。

- データ プレーン ポリサー（DPP）は、SR-MPLS L3Out ではサポートされていません。
- レイヤ 2 DPP は、MPLS インターフェイスの入力方向で動作します。
- レイヤ 2 DPP は、出力カスタム MPLS QoS ポリシーがない場合、MPLS インターフェイスの出力方向で動作します。
- VRF レベルのポリシングはサポートされていません。

SR-MPLS 統計情報のガイドラインと制約事項

次に、SR-MPLS 統計情報のガイドラインと制限事項を示します。

- SR-MPLS 統計情報を表示するには、リーフ スイッチで SR-MPLS 設定をイネーブルにするときに、ワンタイム ステートフル リロードを実行する必要があります。
- SR-MPLS インターフェイスの統計情報は、スイッチ名の末尾に「FX2」または「GX」がある境界リーフ スイッチ モデルでのみサポートされます。
- SR-MPLS VRF インスタンス統計情報は、スイッチ名の末尾が「FX」、「FX2」、または「GX」である境界リーフ スイッチ モデルでサポートされます。
- 15 分間の履歴統計の場合、15 分の間隔データを更新するのに 20 分かかることがあります。
- スイッチの CLI に表示される SR-MPLS インターフェイス統計情報は、管理または動作のダウンイベント後にクリアされます。
- スイッチの CLI の SR-MPLS インターフェイス統計情報は、10 秒ごとに報告されます。たとえば、統計情報の収集から 3 秒後にインターフェイスがダウンした場合、CLI は 3 秒間の統計情報のみを報告し、他のすべての統計情報をクリアします。

GUI を使用した SR-MPLS インフラ L3Out の設定

- SR-MPLS インフラ L3Out は、境界リーフスイッチで設定され、SR-MPLS ハンドオフに必要なアンダーレイ BGP-LU およびオーバーレイ MP-BGP EVPN セッションを設定するために使用されます。

- SR-MPLS インフラ L3Out は、ポッドまたはリモート リーフ スイッチ サイトにスコープされます。
- ポッドまたはリモートリーフスイッチサイトには、1 つ以上の SR-MPLS インフラ L3Out を設定できます。

SR-MPLS インフラ L3Out を設定する場合は、次の項目を設定します。

- **ノード**
  - リーフ スイッチのみが SR-MPLS インフラ L3Out のノードとして設定できます（境界リーフ スイッチおよびリモート リーフ スイッチ）。
  - 各 SR-MPLS インフラ L3Out は、1 つのポッドからの境界リーフ スイッチまたは同じサイトからのリモート リーフ スイッチを持つことができます。
  - 各境界リーフ スイッチまたはリモート リーフ スイッチは、複数の SR-MPLS ドメインに接続する場合、複数の SR-MPLS インフラ L3Out で設定できます。
  - また、ノードの下にループバック インターフェイスを設定し、ループバック インターフェイスの下にノード SID ポリシーを設定します。
- **インターフェイス**
  - 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
    - ルーテッド ポートチャネルまたはポートチャネル サブインターフェイス

    サブインターフェイスでは、任意の VLAN タグがサポートされます。
  - また、SR-MPLS infra L3Out のインターフェイス エリアの下にアンダーレイ BGP ピア ポリシーを設定します。
- **QoS ルール**
  - MPLS 入力ルールと MPLS 出力ルールは、SR-MPLS インフラ L3Out の MPLS QoS ポリシーを使用して設定できます。
  - MPLS QoS ポリシーを作成しない場合、入力 MPLS 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、SR-MPLS インフラ L3Out を使用してアンダーレイとオーバーレイを設定します。

- アンダーレイ：インターフェイス設定の一部としての BGP ピア IP（BGP LU および IPv4 ピア）設定。
- オーバーレイ：論理ノードプロファイル設定の一部としての MP-BGP EVPN リモート IPv4 アドレス（MP-BGP EVPN ピア）設定。

始める前に

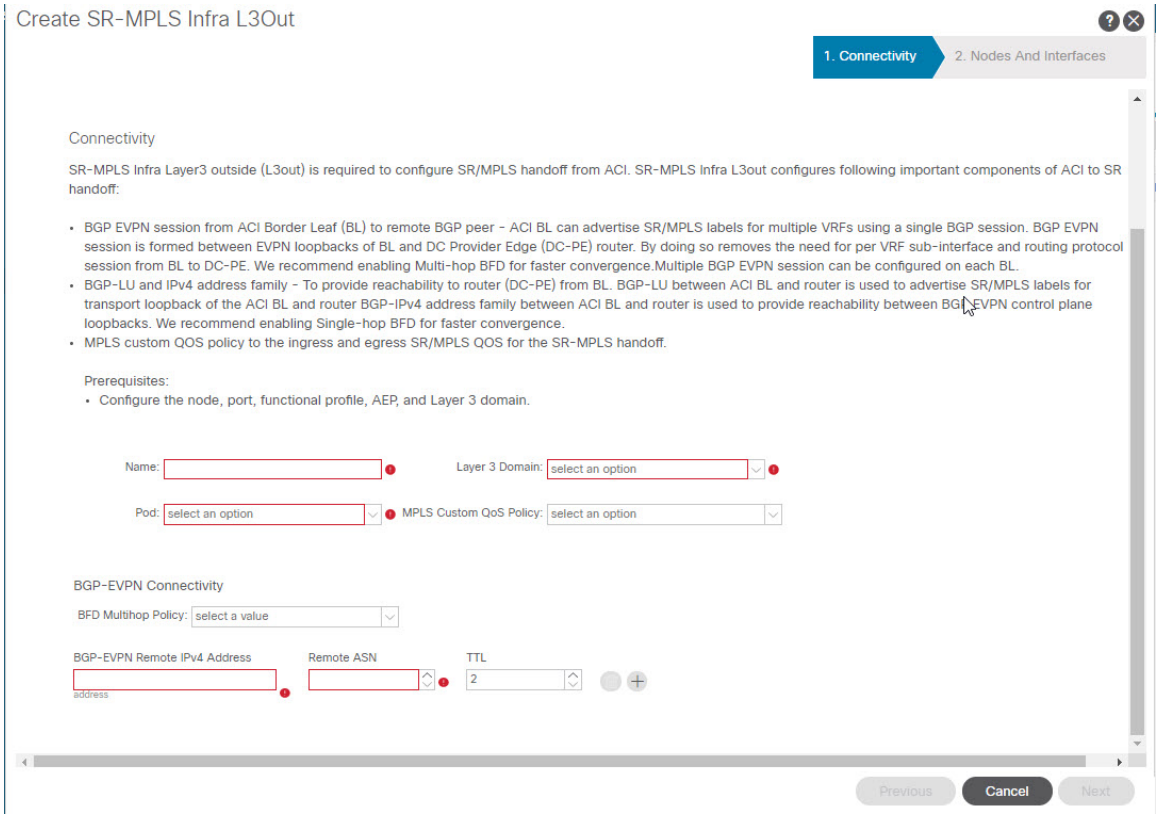
- SR-MPLS のガイドラインおよび制限事項 （201 ページ） で提供されている SR-MPLS ガイドラインと制約事項を確認します。特に、SR-MPLS インフラ L3Out のガイドラインと制約事項 （202 ページ） で提供されているガイドラインと制約事項を確認してください。
- に示す手順を使用して、MPLS カスタム QoS ポリシーを設定します。 GUI を使用した SR-MPLS カスタム QoS ポリシーの作成 （221 ページ）

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）]>[SR-MPLS Infra L3Outs]** に移動します。

ステップ 2 [SR-MPLS Infra L3Outs] を右クリックし、[SR-MPLS インフラ L3Out の作成（Create SR-MPLS Infra L3Out）] を選択します。

[接続（Connectivity）] ウィンドウが表示されます。



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。

a) [名前（Name）] フィールドに、SR-MPLS Infra 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) [レイヤ 3 ドメイン（Layer 3 Domain）] フィールドで、既存のレイヤ 3 ドメインを選択するか、[L3 ドメインの作成（Create L3 Domain）] を選択して新しいレイヤ 3 ドメインを作成します。

c) マルチポッド設定がある場合は、[ポッド（Pod）] フィールドでポッドを選択します。

マルチポッド設定がない場合は、選択をポッド 1 のままにします。

d) （任意） [MPLS カスタム QoS ポリシー（MPLS Custom QoS Policy）] フィールドで、既存の QoS ポリシーを選択するか、[MPLS カスタム QoS ポリシーの作成（Create MPLS 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、を参照してください。GUI を使用した SR-MPLS カスタム QoS ポリシーの作成 （221 ページ）

カスタム QoS ポリシーを作成しない場合は、次のデフォルト値が割り当てられます。

- 境界リーフ スイッチ上のすべての着信 MPLS トラフィックは、QoS レベル 3（デフォルトの QoS レベル）に分類されます。
- 境界リーフ スイッチは次の処理を実行します。
  - 再マーキングなしで SR-MPLS からのトラフィックの元の DSCP 値を保持します。
  - COS 保存が有効な場合、テナント トラフィックの元の COS 値を使用してパケットを MPLS ネットワークに転送します。
  - デフォルトの MPLS EXP 値（0）のパケットを SR-MPLS ネットワークに転送します。
- また、境界リーフ スイッチは、SR ネットワークへの転送中に、アプリケーション サーバから着信するテナント トラフィックの元の DSCP 値を変更しません。

e) [BGP-EVPN 接続（BGP-EVPN Connectivity）] 領域に移動します。

f) （任意） [BFD マルチホップ ポリシー（BFD Multihop Policy）] フィールドで、既存の BFD マルチホップ ポリシーを選択するか、[BFD マルチホップ ノード ポリシーの作成（Create BFD Multihop Node Policy）] を選択して新しいポリシーを作成します。

境界リーフ スイッチから DC-PE への MP-BGP EVPN マルチホップ セッションがある場合、BFD マルチホップ ポリシー オプションを有効にすると、BGP セッションは通常の BGP タイマーに依存しません。代わりに、BFD タイマーに基づいて、より速く終了します。詳細については、「BGP EVPN セッションのマルチホップ BFD （190 ページ）」を参照してください。

g) [BGP-EVPN リモート IPv4 アドレス（BGP-EVPN Remote IPv4 Address）] フィールドに、MP-BGP EVPN リモート IPv4 アドレスを入力します。

この BGP ピア IP アドレスは、オーバーレイ設定の一部です。これは、DC-PE のループバック アドレスです（リモート DC-PE ごとに 1 エントリ）。

h) [リモート ASN（Remote ASN）] フィールドに、DC-PE のネイバー自律システムを一意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。

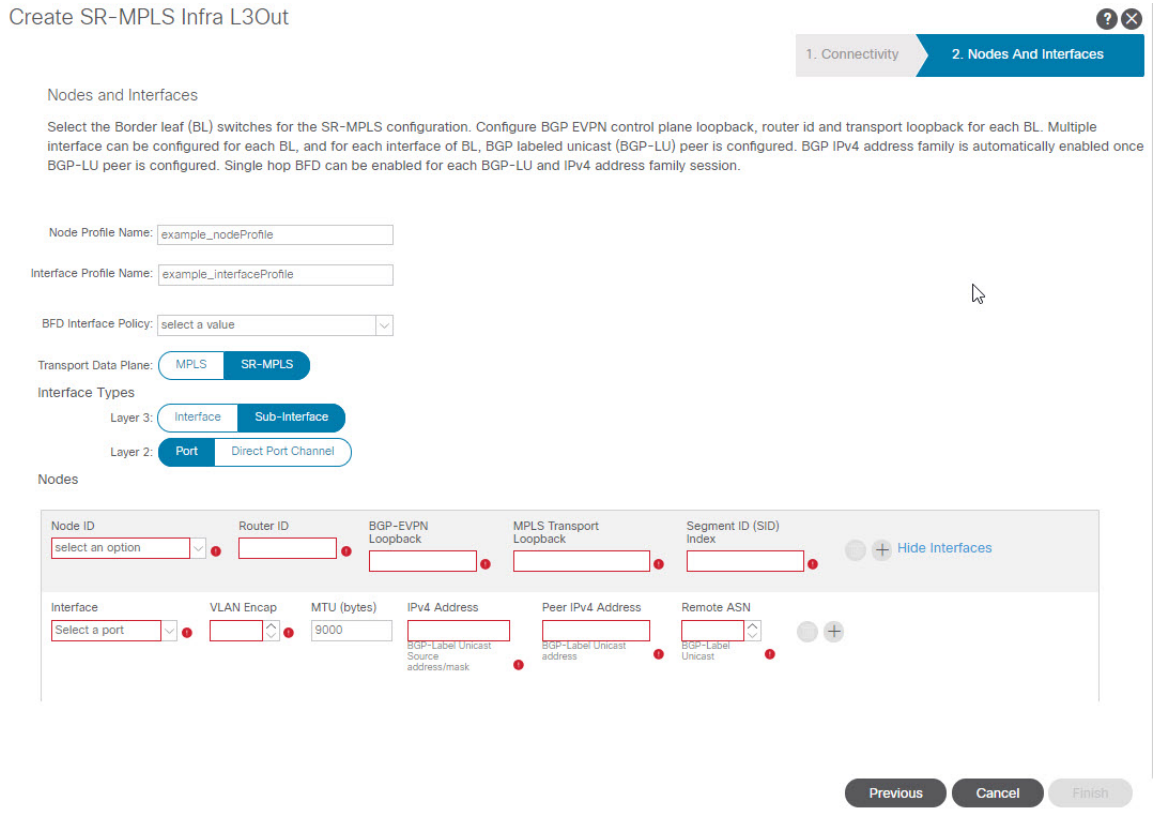
（注） ACI は asdot または asdot＋形式の AS 番号をサポートしていません。asdot または asdot＋形式の AS 番号の詳細については、『Explaining 4-Byte Autonomous System（AS）ASPLAIN and ASDOT Notation for Cisco IOS』を参照してください。https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/border-gateway-protocol-bgp/white_paper_c11_516829.html

i) [TTL] フィールドに、接続存続可能時間（TTL）を入力します。

有効な範囲は 1 ～ 255 ホップです。

j) **[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。



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、境界リーフノードとインターフェイスを設定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）] フィールドと [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。

デフォルトのノード プロファイル名は L3Out-name _nodeProfile で、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。[L3Out-name] は、[接続（Connectivity）] ページの [名前（Name）] フィールドに入力した名前です。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、[BFD インターフェイス ポリシーの作成（Create BFD Interface Policy）] を選択して新しい BFD インターフェイス ポリシーを作成します。

c) [データ プレーンのトランスポート（Transport Data Plane）] フィールドで、Cisco ACI境界リーフスイッチのハンドオフに使用するルーティングのタイプを決定します。

次のオプションがあります。

- [MPLS]：トランスポートデバイスへのハンドオフにマルチプロトコル ラベル スイッチング（MPLS）を使用するには、このオプションを選択します。
- [SR-MPLS]：トランスポート デバイスへのハンドオフにセグメント ルーティング（SR）マルチプロトコル ラベル スイッチング（MPLS）を使用するには、このオプションを選択します。

d) [インターフェイス タイプ（Interface Types）] 領域で、[レイヤ 3（Layer 3）] および [レイヤ 2（Layer 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：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。

    このオプションを選択すると、レイヤ3インターフェイスは、このページの [レイヤ2（Layer2）] フィールドで選択した特定のオプションに応じて、物理ポートまたは直接ポートチャネルのいずれかになります。
  - サブインターフェイス：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。

    このオプションを選択すると、このページの [レイヤ 2（Layer 2）] フィールドで選択した特定のオプションに応じて、物理ポートまたはダイレクト ポート チャネルのいずれかに対して、レイヤ3サブインターフェイスが作成されます。
- レイヤ 2：
  - **[ポート（Port）]**
  - **ダイレクトポートチャネル(Direct Port Channel)**

e) [**ノード ID（Node ID）**] フィールドのドロップダウン メニューで、L3Out のリーフ スイッチ、またはノードを選択します。

マルチポッド設定の場合、前の画面で選択したポッドの一部であるリーフ スイッチ（ノード）のみが表示されます。

ルータ ID の設定方法を説明する警告メッセージが画面に表示される場合があります。

- このノードのルータ ID がまだ設定されていない場合は、に進み、このノードのルータ ID を設定する手順を参照してください。4.f （214 ページ）
- 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 リフレクタを設定していた場合）、次のオプションがあります。
  - SR-MPLS 設定に同じルータ ID を使用します。これは推奨オプションです。この場合、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、このノードのルータ ID の設定手順を参照してください。4.f （214 ページ）
  - SR-MPLS 設定に別のルータ ID を使用します。この状況では、次の手順でルータ ID を入力する前に、既存のアプリケーションへのトラフィックの中断を回避するために、最初にノードをアクティブパスから外す必要があります。アクティブ パスからノードを削除するには、次の手順を実行します。
    1. ノードをメンテナンス モードにします。
    2. の説明に従って、SR-MPLS 設定に別のルータ ID を入力します。4.f （214 ページ）
    3. ノードをリロードします。

f) [ルータ ID（Router ID）] フィールドに、Infra L3Out の境界リーフ スイッチ部分の一意のルータ ID（IPv4 または IPv6 アドレス）を入力します。

ルータ IDは、すべての境界リーフ スイッチと DC-PE で一意である必要があります。

で説明したように、ルータ ID がこのノードですでに設定されている場合、いくつかのオプションがあります。4.e （214 ページ）

- SR-MPLS 設定に同じルータ ID を使用する場合は、の警告メッセージに表示されたルータ ID を入力します。4.e （214 ページ）
- SR-MPLS 設定に同じルータ ID を使用しない場合、またはルータ ID がまだ設定されていない場合は、の境界リーフ スイッチ部分の IP アドレス（IPv4 または IPv6）をこのフィールドに入力します。一意のルータ ID である必要があることに注意してください。

ルータ ID のエントリを決定すると、[BGP-EVPN ループバック（BGP-EVPN Loopback）] フィールドと [MPLS トランスポート ループバック（MPLS Transport Loopback）] フィールドのエントリに、[ルータ ID（Router ID）] フィールドに入力したエントリが自動的に入力されます。

g) （任意） 必要に応じて、[N ループバック（BGP-EVPN Loopback）] フィールドに IP アドレスを入力します。

BGP-EVPN セッションの場合、BGP-EVPN ループバックがコントロール プレーン セッションに使用されます。このフィールドを使用して、境界リーフ スイッチの EVPN ループバックと DC-PE 間の MP-BGP EVPN セッションを設定し、オーバーレイ プレフィックスをアドバタイズします。MP-BGP EVPN セッションは、BP-EVPN ループバックと BGP-EVPN リモート ピア アドレス（[接続（Connectivity）] ウィンドウの [BGP-EVPN リモート IPv4 アドレス（BGP-EVPN Remote IPv4 Address）] フィールドで設定）の間で確立されます。

[BP-EVPN ループバック（BGP-EVPN Loopback）] フィールドには、[ルータ ID（Router ID）] フィールドに入力したものと同じエントリが自動的に入力されます。BGP-EVPN ループバック アドレスとしてルータ ID を使用しない場合は、BGP-EVPN ループバック アドレスに別の IP アドレスを入力します。

次の点に注意してください。

- BGP-EVPN セッションでは、[BGP-EVPN ループバック（BGP-EVPN Loopback）] フィールドに、[ルータ ID（Router ID）] フィールドに入力した IP アドレスとは異なる IP アドレスを使用することを推奨します。
- BGP-EVPN ループバックと MPLS トランスポート ループバックに異なる IP アドレスを使用できますが、ACI 境界リーフ スイッチの BGP-EVPN と MPLS トランスポート ループバックに同じループバックを使用することを推奨します。

h) [MPLS トランスポート ループバック（MPLS Transport Loopback）] フィールドに、MPLS トランスポート ループバックのアドレスを入力します。

MPLS トランスポート ループバックは、ACI 境界リーフ スイッチと DC-PE 間のデータ プレーン セッションを構築するために使用されます。MPLS トランスポート ループバックは、境界リーフ スイッチから DC-PE ルータにアドバタイズされるプレフィックスのネクストホップになります。詳細については、「Cisco ACI 境界リーフ スイッチと DC-PE 間の MP-BGP EVPN セッション （188 ページ）」を参照してください。

次の点に注意してください。

- BGP-EVPN セッションでは、[MPLS トランスポート ループバック（MPLS Transport Loopback）] フィールドに、[ルータ ID（Router ID）] フィールドに入力した IP アドレスとは異なる IP アドレスを使用することを推奨します。
- BGP-EVPN ループバックと MPLS トランスポート ループバックに異なる IP アドレスを使用できますが、ACI 境界リーフ スイッチの BGP-EVPN と MPLS トランスポート ループバックに同じループバックを使用することを推奨します。

i) [セグメント ID（SID）インデックス（Segment ID（SID）Index）] フィールドに、SID インデックスを入力します。

SID インデックスは、MPLS トランスポートループバックの各ノードで設定されます。SID インデックス値は BGP-LU を使用してピア ルータにアドバタイズされ、ピア ルータは SID インデックスを使用してローカル ラベルを計算します。

SID インデックス エントリでサポートされる値は 0 ー 4294967295 です。SID インデックスは、セグメント ルーティング ドメイン全体で一意である必要があります。

j) 上記の [レイヤ 2（Layer 2）] 領域で [ポート（Port）] を選択した場合は、[インターフェイス（Interface）] フィールドが表示されます。ドロップダウン リストから [ポート（Port）] を選択します。

k) 上記の [レイヤ 2（Layer 2）] 領域で [ダイレクト ポート チャネル（Direct Port Channel）] を選択した場合は、[PC パス（PC Paths）] フィールドが表示されます。ドロップダウン リストからポート チャネルを選択します。これは、インターフェイス プロファイルのポート チャネル エンド ポイントへのパスです。

l) 上記の [レイヤ 3（Layer 3）] 領域で [サブインターフェイス（Sub-Interface）] を選択した場合は、[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。

m) **[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。

このフィールドの許容値は 576 ー 9216 です。値を継承するには、このフィールドに **inherit** を入力します。

n) [IPv4 アドレス（IPv4 Address）] フィールドに、BGP-Label ユニキャスト送信元の IP アドレスを入力します。

これは、前の手順で設定したレイヤ 3 インターフェイス/サブインターフェイス/ポート チャネルに割り当てられた IP アドレスです。

o) [IPv4 アドレス（IPv4 Address）] フィールドに、BGP-Label ユニキャスト ピア IP アドレスを入力します。

これは、境界リーフ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。

p) [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-Label Autonomous System Number を入力します。

q) SR-MPLS infra L3Out のこのノードに追加のインターフェイスを設定するかどうかを決定します。

- このSR-MPLS infra L3Out のこのノードに追加のインターフェイスを設定しない場合は、に進みます。4.s （217 ページ）
- この SR-MPLS infra L3Out のこのノードに追加のインターフェイスを設定する場合は、[インターフェイス（Interface）] 領域で [+] をクリックして、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します。

（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。

r) この SR-MPLS infra L3Out に追加のノードを設定するかどうかを決定します。

- この SR-MPLS infra L3Out の追加ノードを設定しない場合は、に進みます。4.s （217 ページ）
- この SR-MPLS infra L3Out に追加のノードを設定する場合は、[ノード（Nodes）] 領域で [+] をクリックして、別のノードに同じオプションを表示します。

（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。

s) [ノードとインターフェイス（Nodes and Interfaces）] ウィンドウに残りの追加情報を入力したら、[完了（Finish）] をクリックして、[SR-MPLS インフラ L3Out の作成（Create SR-MPLS Infra L3Out）] ウィザードで必要な設定を完了します。

次のタスク

の手順に従って、SR-MPLS VRF L3Out を設定します。GUI を使用した SR-MPLS VRF L3Out の設定 （217 ページ）

GUI を使用した SR-MPLS VRF L3Out の設定

この項の手順を使用して、SR-MPLS VRF L3Out を設定します。これは、前の手順で設定した SR-MPLS インフラ L3Out からのトラフィックの転送に使用されます。

- ユーザ テナント VRF は SR-MPLS インフラ L3Out にマッピングされ、テナント ブリッジ ドメイン サブネットを DC-PE ルータにアドバタイズし、DC-PE から受信した MPLS VPN ルートをインポートします。
- 各 VRF の SR-MPLS VRF L3Out でルーティング ポリシーとセキュリティ ポリシーを指定する必要があります。これらのポリシーは、1 つ以上の SR-MPLS インフラ L3Out をポイントします。
- VRF ごとに 1 つの SR-MPLS VRF L3Out がサポートされます。

始める前に

- SR-MPLS のガイドラインおよび制限事項 （201 ページ） で提供されている SR-MPLS ガイドラインと制約事項を確認します。特に、SR-MPLS VRF L3Out のガイドラインと制約事項 （202 ページ） で提供されているガイドラインと制約事項を確認してください。
- GUI を使用した SR-MPLS インフラ L3Out の設定 （208 ページ） の手順に従って、SR-MPLS インフラ L3Out を設定します。

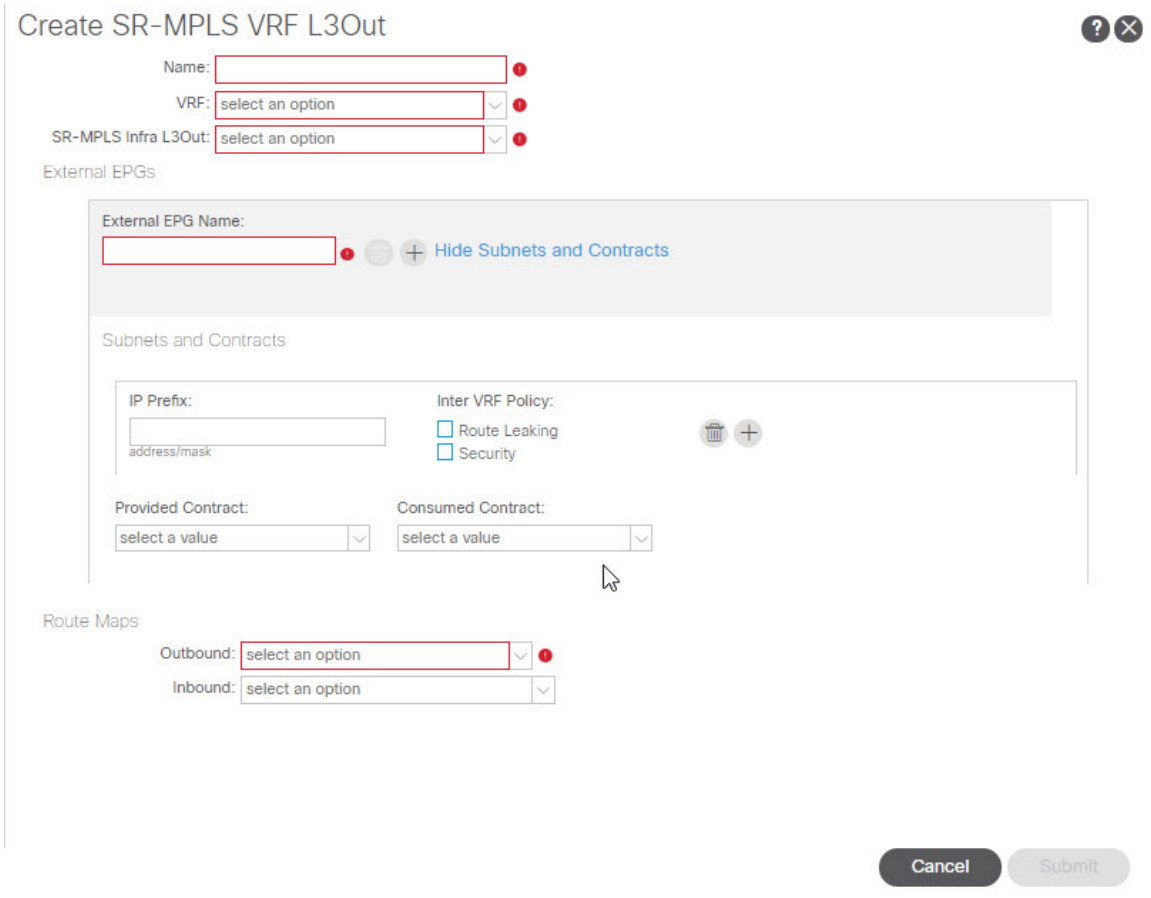
手順

ステップ 1 テナントの [SR-MPLS VRF L3Out の作成（Create SR-MPLS VRF L3Out）] ウィンドウ（[テナント（Tenants）] [テナント（tenant）] [ネットワーキング（Networking）] [SR-MPLS VRF L3Outs]）に移動して SR-MPLS VRF L3Out を設定します。 > > >

ステップ 2 [SR-MPLS VRF L3Outs] を右クリックし、[SR-MPLS VRF L3Out の作成（Create SR-MPLS VRF L3Out）]を選択します。

[SR-MPLS VRF L3Out の作成（Create SR-MPLS VRF L3Out）] ウィンドウが表示されます。

図 *25 : SR-MPLS L3Out* の作成



ステップ 3 [名前（Name）] フィールドに、SR-MPLS VRF 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。

ステップ 4 [VRF] フィールドで、既存の VRF を選択するか、[VRF の作成（Create VRF）] をクリックして新しい VRF を作成します。

ステップ 5 [SR-MPLS Infra L3Out] フィールドで、既存の SR-MPLS infra L3Out を選択するか、[SR-MPLS Infra L3Out の作成（Create SR-MPLS Infra L3Out）] をクリックして新しい SR-MPLS infra L3Out を作成します。

SR-MPLS インフラ L3Out の作成の詳細については、を参照してください。GUI を使用した SR-MPLS インフラ L3Out の設定 （208 ページ）

ステップ 6 [外部 EPG（External EPGs）] 領域に移動し、[外部 EPG 名（External EPG Name）] 領域で、この SR-MPLS VRF L3Out に使用する外部 EPG の一意の名前を入力します。

ステップ 7 [サブネットとコントラクト（Subnets and Contracts）] 領域に移動し、この EPG 内の個々のサブネットを設定します。

（注） サブネットフィールドを設定しても、次のフィールドが表示されない場合は、[サブネットとコントラクトの表示（Show Subnets and Contracts）] をクリックして次のフィールドを表示します。

a) [IP プレフィックス（IP Prefix）] フィールドに、サブネットの IP アドレスとネットマスクを入力します。

b) [インフラ VRF ポリシー（Inter VRF Policy）] フィールドで、VRF 間ポリシーを設定するかどうかを決定します。

- VRF 間ポリシーを設定しない場合は、に進みます。7.c （219 ページ）
- VRF 間ポリシーを設定する場合は、使用する適切な VRF 間ポリシーを選択します。

  次のオプションがあります。

  - **[ルート リーク（Route Leaking）]**

    [ルート リーク（Route Leaking）] を選択すると、[集約（Aggregate）] フィールドが表示されます。このオプションも有効にする場合は、[集約（Aggregate）] の横にあるボックスをクリックします。

  - **セキュリティ。**

  [インター VRF ポリシー（Inter VRF Policy）] フィールドでは、上記の 2 つのオプションのいずれかまたは両方を選択できます。

c) [提供されたコントラクト（Provided Contract）] フィールドで、既存のプロバイダー契約を選択するか、[コントラクトの作成（Create Contract）] をクリックしてプロバイダ契約を作成します。

d) [消費されたコントラクト（Consumed Contract）] フィールドで、既存のコンシューマ コントラクトを選択するか、[コントラクトの作成（Create Contract）] をクリックしてコンシューマ コントラクトを作成します。

e) この外部 EPG に追加のサブネットを設定するかどうかを決定します。

- この外部 EPG に追加のサブネットを設定しない場合は、に進みます。ステップ 8 （220 ページ）

- この外部 EPG に追加のサブネットを設定する場合は、[サブネットとコントラクト（Subnet and Contracts）] 領域で [+] をクリックして、別のサブネットに同じオプションを表示します。

  （注） サブネットに入力した情報を削除する場合、または誤って追加したサブネット行を削除する場合は、削除するサブネット行のゴミ箱アイコンをクリックします。

ステップ 8 この SR-MPLS VRF L3Out に使用する追加の外部 EPG を作成するかどうかを決定します。

- この SR-MPLS VRF L3Out に使用する追加の外部 EPG を設定しない場合は、に進みます。ステップ 9 （220 ページ）
- この SR-MPLS VRF L3Out に使用する追加の外部 EPG を設定する場合は、[外部 EPG 名（External EPG Name）] 領域で [+] をクリックして、別の外部 EPG に対して同じオプションを表示します。

  （注） 外部 EPG に入力した情報を削除する場合、または誤って追加した外部 EPG エリアを削除する場合は、削除する外部 EPG エリアのゴミ箱アイコンをクリックします。

ステップ 9 [ルート マップ（External EPG Name）] 領域で、発信および着信ルート マップを設定します。

各 SR-MPLS VRF L3Out 内：

- アウトバウンド ルート マップ（エクスポート ルーティング ポリシー）の定義は必須です。これは、外部 DC-PE ルータにプレフィックスをアドバタイズできるようにするために必要です。
- デフォルトでは、DC-PE ルータから受信したすべてのプレフィックスがファブリックに許可されるため、インバウンド ルート マップ（インポート ルーティング ポリシー）の定義はオプションです。

a) [アウトバウンド（Outbound）] フィールドで、既存のエクスポート ルート マップを選択するか、[ルート制御用ルート マップの作成（Create Route Maps for Route Control）] をクリックして新しいエクスポート ルート マップを作成します。

b) [インバウンド（Inbound）] フィールドで、既存のインポート ルート マップを選択するか、[ルート制御用ルート マップの作成（Create Route Maps for Route Control）] をクリックして新しいインポート ルート マップを作成します。

ステップ 10 [SR-MPLS VRF L3Out の作成（Create SR-MPLS VRF L3Out）] ウィンドウでの設定が完了したら、[送信（Submit）] をクリックします。

GUI を使用した SR-MPLS カスタム QoS ポリシーの作成

SR MPLS カスタム QoS ポリシーは、MPLS QoS 出力 ポリシーで定義された着信 MPLS EXP 値に基づいて、SR-MPLS ネットワークから送信されるパケットのプライオリティを定義します。これらのパケットは、ACI ファブリック内にあります。また、MPLS QoS 出力ポリシーで定義された IPv4 DSCP 値に基づく MPLS インターフェイスを介して ACI ファブリックから離れるパケットの CoS 値および MPLS EXP 値をマーキングします。

カスタム出力ポリシーが定義されていない場合、デフォルトの Qos レベル（`Level3`）がファブリック内のパケットに割り当てられます。カスタム出力ポリシーが定義されていない場合、デフォルトの EXP 値（`0`）がファブリックから離れるパケットにマーキングされます。

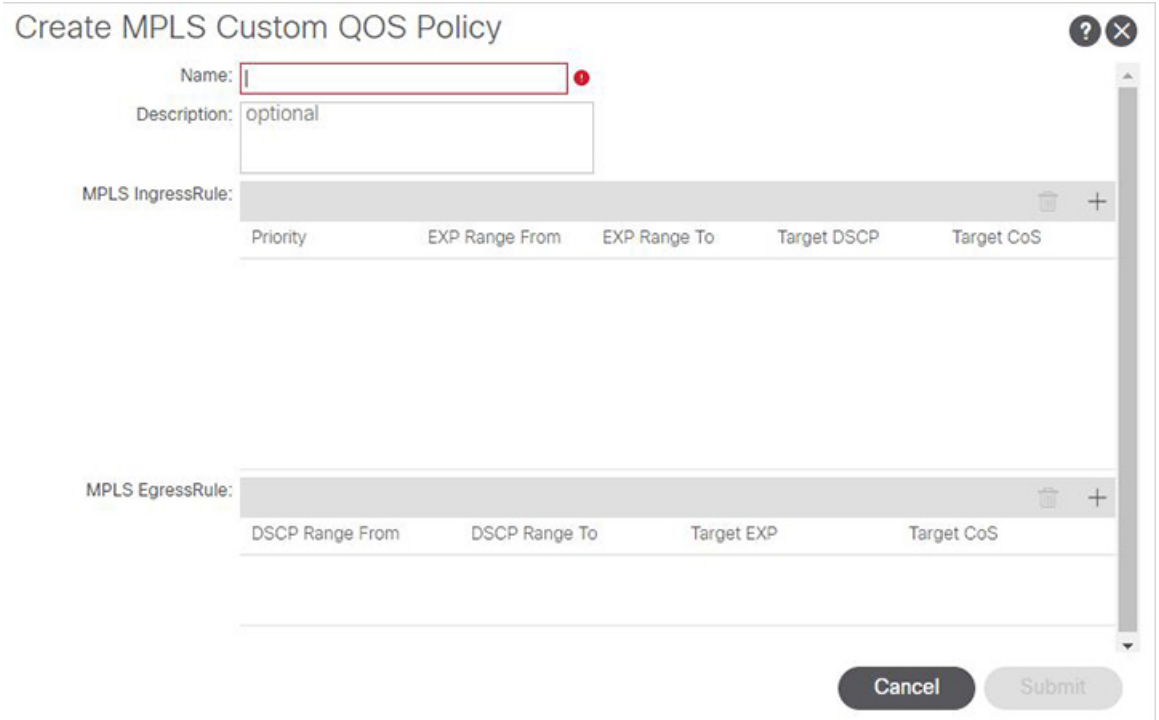
手順

ステップ 1 メニュー バーから **[Tenants（テナント）]** > **[インフラ（infra）]** を選択します。

ステップ 2 左側のペインで、[インフラ（infra）] [ポリシー（Policies）] [プロトコル（Protocol）] [MPLS カスタム QoS （MPLS Custom QoS）] を選択します。 > > >

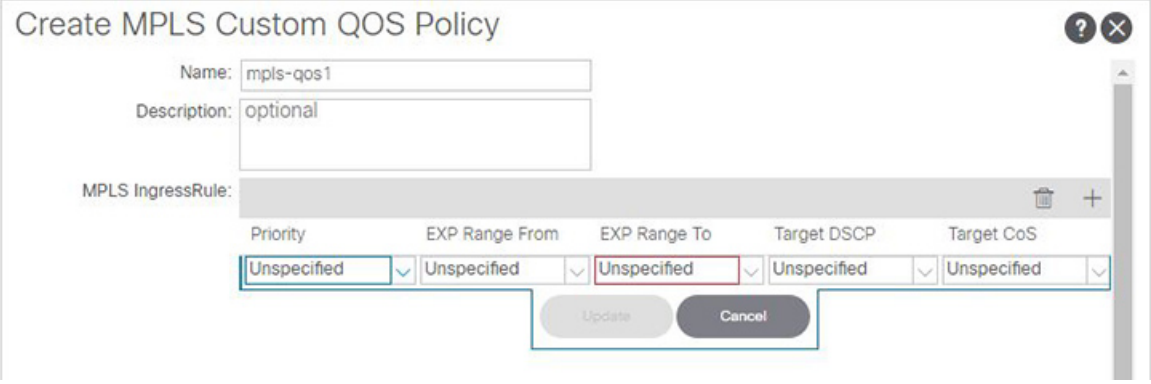
ステップ 3 [MPLS カスタム QoS （MPLS Custom QoS）] フォルダを右クリックし、[MPLS カスタム QoS ポリシーの作成（Create MPLS Custom QoS Policy）] を選択します。

ステップ 4 表示される [MPLS カスタム QoS ポリシーの作成（Create MPLS 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 5 [**MPLS 入力ルール（MPLS Ingress Rule**）] 領域で、[+] をクリックして入力 QoS 変換ルールを追加します。

MPLS ネットワークに接続されている境界リーフ (BL) に着信するすべてのトラフィックは、MPLS EXP 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、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。オプションの範囲は Level1 ー Level6 です。デフォルト値は `Level3` 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 `Level3` の優先順位が割り当てられます。

b) [**EXP 範囲開始（EXP Range From**）] と [**EXP 範囲終了（EXP Range To**）] フィールドで、照合する入力 MPLS パケットの EXP 範囲を指定します。

c) [**ターゲット DSCP（Target DSCP**）] フィールドで、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 DSCP 値を選択します。

指定された DSCP 値は、外部ネットワーク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（Unspecified）`] です。つまり、パケットの元の DSCP 値が保持されます。

d) [**ターゲット CoS（Target CoS**）] フィールドで、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 CoS 値を選択します。

指定された CoS 値は、外部ネットワーク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（Unspecified）`] 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) [**更新（Update**）] をクリックして入力ルールを保存します。

f) 追加の入力 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 6 [**MPLS 出力ルール（MPLS Egress Rule**）] 領域で、[+] をクリックして出力 QoS 変換ルールを追加します。

トラフィックが境界リーフの MPLS インターフェイスから離れていくと、パケットの DSCP 値に基づいて照合され、一致が見つかると、MPLS EXP および CoS 値がポリシーに基づいて設定されます。

a) [**DSCP 範囲開始（DSCP Range From**）] と [**DSCP 範囲終了（DSCP Range To**）] ドロップダウンを使用して、出力 MPLS パケットのプライオリティを割り当てるために一致させる ACI ファブリック パケットの DSCP 範囲を指定します。
b) [**ターゲット EXP（Target EXP**）] ドロップダウンから、出力 MPLS パケットに割り当てる EXP 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 MPLS パケットに割り当てる CoS 値を選択します。
d) [**更新（Update**）] をクリックして入力ルールを保存します。
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 7 [**OK**] をクリックし、MPLS カスタム QoS の作成を完了します。

MPLS 統計情報の表示

次に、このトピックで説明する統計画面に表示するために選択できる MPLS 固有の統計情報を示します。

- インターフェイスの SR-MPLS 統計情報の表示 （224 ページ） で説明されているように、インターフェイス レベルでは、
- VRS 向け SR-MPLS 統計情報の表示 （225 ページ） で説明されているように、VRF レベルでは、

システム内のすべてのインターフェイスおよび VRF の統計情報を表示するには、次の場所に移動します。

[テナント（Tenants）]>[インフラ（infra）]>[ネットワーキング（Networking）]>[SR-MPLS Infra L3Outs]

[SR-MPLS インフラ L3Outs（SR-MPLS Infra L3Outs）] パネルが表示され、システムで設定されているすべての SR-MPLS infra L3Outs が表示されます。上位レベルの [SR-MPLS インフラ L3Out（SR-MPLS Infra L3Outs）] パネルで、表示する統計情報のタイプに応じて、適切な統計情報ページに移動します。

- [インターフェイス統計情報（Interface Stats）] タブをクリックして、システム上のすべての MPLS インターフェイスの統計情報の概要を表示します。このウィンドウの各行には、特定のノード上の特定のインターフェイスの MPLS 統計情報が表示されます。

（注） メインの SR-MPLS infra L3Outs ページに表示されるインターフェイス統計情報は、スイッチ名の末尾に「FX2」または「GX」がある境界リーフ スイッチ モデル上のすべての SR-MPLS 対応インターフェイスのみを対象としています。

他のレベルの MPLS インターフェイス統計情報を確認するには、インターフェイスの SR-MPLS 統計情報の表示 （224 ページ）を参照してください。

- [VRF 統計情報（VRF Stats）] タブをクリックして、システム上のすべての MPLS VRF の統計情報の要約を表示します。このウィンドウの各行には、特定のノードに設定された特定の VRF の MPLS 統計情報が表示されます。

  SR-MPLS インフラ L3Out プロパティ ページで提供される VRF 統計情報は、SR-MPLS インフラ L3Out のプロバイダー ラベルが消費される特定の境界リーフ スイッチまたはリモート リーフ スイッチの個々の VRF 統計情報です。

  MPLS VRF統計情報のその他のレベルについては、VRS 向け SR-MPLS 統計情報の表示（225 ページ）を参照してください。

インターフェイスの SR-MPLS 統計情報の表示

次に、このトピックで説明する統計画面に表示するために選択できる MPLS 固有のインターフェイス統計情報を示します。

- Mpls 出力ドロップ バイト
- Mpls 出力許可バイト
- Mpls 出力ドロップ パケット
- Mpls 出力許可パケット
- Mpls 受信ドロップ バイト
- Mpls Ingress Admit Bytes
- Mpls 受信ドロップ パケット
- Mpls 受信許可パケット

統計情報ページに表示される統計情報のタイプを変更するには、チェックボックスをクリックして [**統計情報の選択（Select Stats）**] ウィンドウを開きます。エントリを左コラムから右コラムに移動して別の統計情報を表示し、右コラムから左コラムへ移動してビューから特定の統計情報を削除します。

このページの統計情報のレイアウトを変更して、統計情報を表形式で表示するには、3 本の横棒アイコンをクリックして [**テーブル ビュー（Table View）**] を選択します。

- SR-MPLS インフラ L3Out の SR-MPLS VRF L3Out 内のすべてのインターフェイスの詳細な集約インターフェイス統計情報を表示するには、その SR-MPLS インフラ L3Out に移動します。

  [テナント（Tenant）] > [インフラ（infra）] > [ネットワーキング（Networking）] > [SR-MPLS Infra L3Outs] > [*SR-MPLS_infra_L3Out_name*]

  特定の SR-MPLS インフラ L3Out の下にある SR-MPLS VRF L3Out のすべてのインターフェイスの詳細な集約インターフェイス統計情報を表示するには、[統計情報（Stats）] タブをクリックします。

- 特定のリーフ スイッチの特定のインターフェイスの統計情報を表示するには、リーフ スイッチのそのインターフェイス領域に移動します。

  [Fabric Inventory Pod # leaf_switch Interfaces] をクリックし、[ルーテッド インターフェイス（Routed Interfaces）] または [カプセル化されたルーテッドインターフェイス（Encapsulated Routed Interfaces）] をクリックします。 > > > >

  統計情報を取得する特定のインターフェイスをクリックし、[統計情報（Stats）] タブをクリックします。

VRS 向け SR-MPLS 統計情報の表示

次に、このトピックで説明する統計画面に表示するために選択できる MPLS 固有の VRF 統計情報を示します。

- Mpls Vrf 出力ドロップ バイト
- Mpls Vrf 出力許可バイト
- Mpls Vrf 出力ドロップ パケット
- Mpls Vrf 出力許可パケット
- Mpls Vrf 受信ドロップ バイト
- Mpls Vrf 受信許可バイト
- Mpls Vrf 受信ドロップ パケット
- Mpls Vrf 受信許可パケット

統計情報ページに表示される統計情報のタイプを変更するには、チェックボックスをクリックして **[統計情報の選択（Select Stats）]** ウィンドウを開きます。エントリを左コラムから右コラムに移動して別の統計情報を表示し、右コラムから左コラムへ移動してビューから特定の統計情報を削除します。

このページの統計情報のレイアウトを変更して、統計情報を表形式で表示するには、3 本の横棒アイコンをクリックして **[テーブル ビュー（Table View）]** を選択します。

- 特定の VRF の詳細な集約 VRF 統計情報を表示するには、その VRF に移動します。

[テナント（Tenants）] > **[*tenant_name*]** > **[ネットワーキング（Networking）]** > **[VRFs]** > **[*VRF_name*]** の順にクリックします。

[**統計情報（Stats）**] タブをクリックして、この特定の VRF の集約 VRF 統計情報を表示します。この VRF は SR-MPLS L3Out の 1 つで使用されており、この SR-MPLS L3Out には複数のリーフ スイッチがあり、各リーフ スイッチに複数のインターフェイスがあることに注意してください。このウィンドウに表示される統計情報は、この VRF で使用されているこの SR-MPLS L3Out 内のすべてのインターフェイスの集約です。

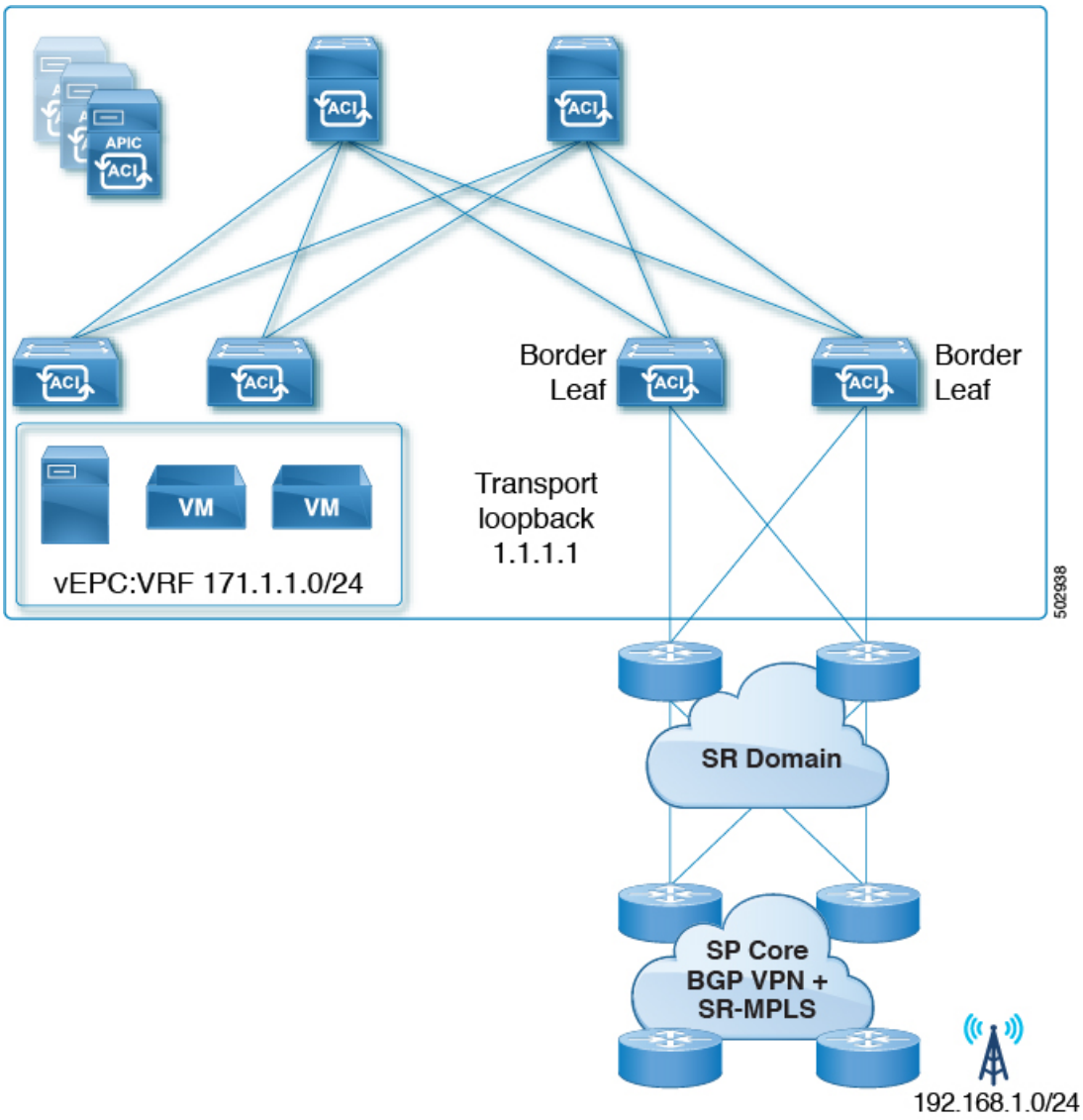
- 特定のリーフ スイッチの VRF 統計情報を表示するには、そのリーフ スイッチの VRF コンテキストに移動します。

  [ファブリック（Fabric） > **[インベントリ（Inventory）]** > **[ポッド #（Pod #）]** > **[*leaf_switch*]** > **[VRF コンテキスト（VRF Contexts）]** > **[*VRF_context_name*]**

  [**統計情報（Stats）**] タブをクリックして、この特定のリーフ スイッチのこの VRF の統計情報を表示します。

SR-MPLS グローバル ブロック（GB）の設定

次の図に示すように、ACI ファブリックの境界リーフ スイッチと DC-PE の間に SR ネットワークがある場合は、SR-MPLS グローバル ブロック（GB）を設定します。



SR ドメイン内のすべてのノードで同じ SR-GB 設定を使用することを推奨します。

次に、SR-MPLS グローバル ブロックを設定する際に考慮すべき重要なガイドラインを示します。

- 設定可能な SR-GB の範囲は 16000 ー 471804 です。
- ACI ファブリックのデフォルトの SR-GB 範囲は 16000 ～ 23999 です。
- ACI は、アンダーレイ ラベルに対して常にヌルをアドバタイズします（トランスポート ループバック）。

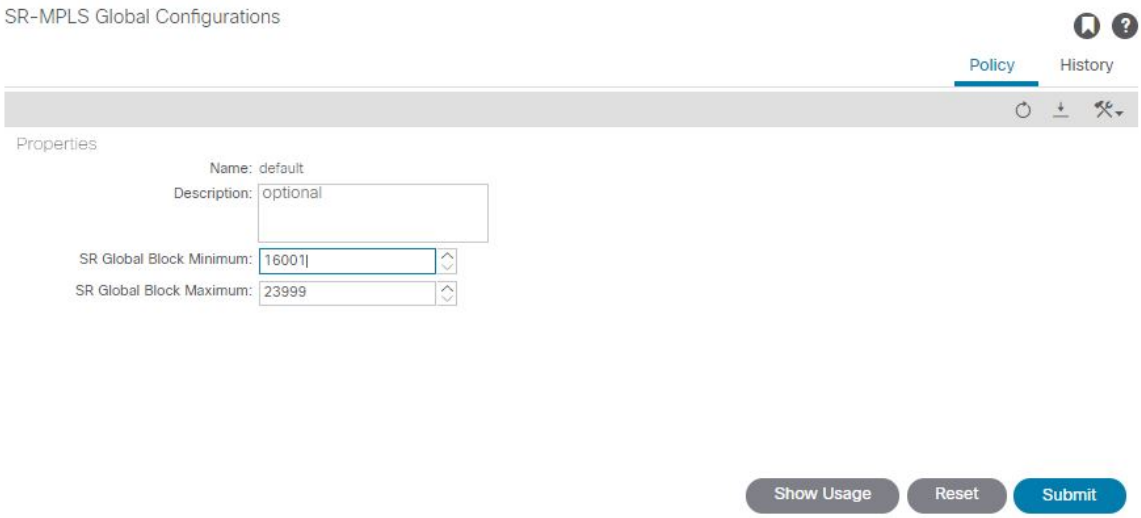
手順

ステップ 1 [SR-MPLS グローバル設定（SR-MPLS Global Configurations）] ウィンドウに移動します。

[テナント（Tenants）] > [インフラ（infra）] > [ポリシー（Policies）] > [プロトコル（Protocol）] > [MPLS グローバル設定（MPLS Global Configurations）]

ステップ 2 メインの [SR-MPLS グローバル設定（SR-MPLS Global Configurations）] 画面で [デフォルト（default）] をダブルクリックするか、左側のナビゲーション バーで [Mpls グローバル設定（Mpls Global Configurations）] の下にある [デフォルト（default）] をクリックして、デフォルトの MPLS Global Configurations 画面にアクセスします。

デフォルトの [SR-MPLS グローバル設定] ウィンドウが表示されます。



ステップ 3 [SR グローバル ブロック最小値（SR Global Block Minimum）] フィールドに、SR-GB 範囲の最小値を入力します。

このフィールドの最小許容値は 16000 です。

ステップ 4 [SR グローバル ブロック最小値（SR Global Block Maximum）] フィールドに、SR-GB 範囲の最大値を入力します。

このフィールドの最大許容値は 471804 です。

ステップ 5 [Submit] をクリックします。

IP ハンドオフ設定から SR ハンドオフ設定への移行

始める前に：

リリース 5.0(1) 以前の ACI ハンドオフ：IP ハンドオフ （181 ページ） で説明されているように、プレリリース 5.0(1) IP ハンドオフ設定を使用する、事前に設定された L3Out があること。

このタスクの概要：

これらの手順では、で説明したように、Cisco APIC リリース 5.0(1) で導入された新しい SR-MPLS コンポーネントを使用して、以前に IP ハンドオフ設定（ で説明されています）で設定した L3Out を SR ハンドオフ設定に移行する手順を示します。リリース 5.0(1) 以前の ACI ハンドオフ：IP ハンドオフ （181 ページ）リリース 5.0(1) での ACI ハンドオフ：SR ハンドオフ （182 ページ）

これらの手順では、2 つのハンドオフが同じ外部ネットワーク インフラ ストラクチャへの接続に使用され、外部デバイスが両方の L3Out を使用して ACI ファブリックにアクセスできることを前提としています。現在、外部クライアントは IP ハンドオフ設定で使用されている L3Out を介して着信することができますが、この項の手順を完了すると、外部クライアントは SR-MPLS ハンドオフ設定で使用されている L3Out を介して着信することができます。

（注） これらの手順では、次の用語を使用して 2 つのタイプの L3Out を区別します。

- IP ベースの L3Out：リリース 5.0(1) より前の IP ハンドオフ設定を使用している、以前に設定されたユーザ テナント L3Out に使用されます。
- SR-MPLS L3Out：Cisco APIC Release 5.0(1) で導入された新しい SR-MPLS コンポーネントを使用して設定された、新しく設定されたユーザ テナント L3Out に使用されます。

このプロセスの一部として実行する全体的な手順は次のとおりです。

- IP ベースの L3Out 設定をミラーリングするために、SR-MPLS VRF L3Out で外部 EPG を設定します。これには、着信トラフィックを分類するためのサブネット設定と、外部 EPG によって提供または消費されるコントラクトが含まれます。
- インバウンドおよびアウトバウンド トラフィックをリダイレクトして、SR-MPLS L3Out を優先するようにします。
- IP ベースの L3Out を切断します。

次の項では、上記の各手順の詳細な手順を示します。

SR-MPLS VRF L3Out での外部 EPG の設定

このタスクでは、SR-MPLS VRF L3Out で外部 EPG を設定して、IP ベースの L3Out 設定（以前に設定した、リリース 5.0(1) より前の IP ハンドオフ設定を使用する L3Out）をミラーリングします。これにはインバウンド トラフィックの分類のサブネット設定、および外部 EPG によって提供されるか消費されるコントラクトが含まれています。

始める前に

IP ハンドオフ設定から SR ハンドオフ設定への移行 （229 ページ）に記載の情報について、確認してください。

手順

ステップ 1 新しいインフラ SR-MPLS L3Out をまだ作成していない場合は、作成します。

これらの手順については、を参照してください。GUI を使用した SR-MPLS インフラ L3Out の設定 （208 ページ）

ステップ 2 新しいユーザ テナント SR-MPLS L3Out を作成します（まだ作成していない場合）。

これらの手順については、を参照してください。GUI を使用した SR-MPLS VRF L3Out の設定（217 ページ）この L3Out は、以前に設定した IP ベースの L3Out と同じ VRF に関連付ける必要があります。

新しいユーザ テナント SR-MPLS L3Out を作成するプロセスの一環として、この SR-MPLS L3Out の外部 EPG を設定するように求められます。

- 新しい SR-MPLS L3Out の外部 EPG には、以前に設定した IP ベースの L3Out に対して現在持っているものと同じ IP プレフィックス情報を入力します。
- 以前に設定した IP ベースの L3Out に複数の外部 EPG が設定されている場合は、新しい SR-MPLS L3Out に追加の外部 EPG を作成し、各 EPG に同じ IP プレフィックス情報を一致させます。

最終的に、新しい SR-MPLS L3Out 用に設定する外部 EPG 設定は、付随するサブネット設定とともに、以前に IP ベースの L3Out 用に設定した外部 EPG およびサブネット設定と一致する必要があります。

新しいユーザ テナント SR-MPLS L3Out の作成手順を完了すると、2 つの L3Out（BGP の 2 つのパス）が作成されます。

- プレリリース 5.0(1) IP ハンドオフ 設定を使用した、既存の、以前に設定した IP ベースの L3Out。内の [開始する前に（Before you begin）] 領域に記述があります。IP ハンドオフ設定から SR ハンドオフ設定への移行 （229 ページ）
- Cisco APIC リリース 5.0(1) で導入された新しい SR-MPLS コンポーネントを使用して作成した新しい SR-MPLS L3Out。

ステップ 3 IP ベースの L3Out と同じセキュリティ ポリシーが SR-MPLS L3Out の外部 EPG に適用されていることを確認します。

非境界リーフ スイッチおよび境界リーフ スイッチでは、新しい SR-MPLS L3Out の作成時に設定した外部 EPG の新しいセキュリティ ポリシーにより、以前に設定された IP ベース L3Out のすべての EPG サブネット プレフィックスと衝突するすべてのサブネットで障害が発生します。これは、同じセキュリティ ポリシーが両方の L3Out の同じ外部 EPG に適用される限り、機能に影響を与えない障害です。

次のタスク

インバウンドおよびアウトバウンド トラフィックをリダイレクトし、に示す手順を使用して SR-MPLS L3Out を優先して開始するようにします。SR-MPLS L3Out へのトラフィックのリダイレクト （231 ページ）

SR-MPLS L3Out へのトラフィックのリダイレクト

このタスクでは、着信トラフィックと発信トラフィックをリダイレクトして、SR-MPLS L3Out の優先を開始するようにします。

始める前に

- IP ハンドオフ設定から SR ハンドオフ設定への移行 （229 ページ）に記載の情報について、確認してください。
- に示す手順を使用して、IP ベースの L3Out 設定をミラーリングするように SR-MPLS VRF L3Out の外部 EPG を設定します。SR-MPLS VRF L3Out での外部 EPG の設定 （230 ページ）

手順

ステップ 1 以前に設定した IP ベースの L3Out の BGP ピア接続プロファイルに移動します。

[ナビゲーション（Navigation）]ペインで、**[テナント（Tenants）]** > ***[tenant_name_for_IP_handoff_L3Out]*** > **[ネットワーキング（Networking）]** > **[L3Outs]** > ***[L3Out_name]*** > **[論理ノード プロファイル（Logical Node Profiles）]** > ***[logical_profile_name]*** > **[論理インターフェイス プロファイル（Logical Interface Profiles）]** > ***[logical_interface_profile_name]*** > ***[BGP_peer_connectivity_profile]*** の順に移動します。

ステップ 2 左側のナビゲーションバーで [BGP ピア接続プロファイル（BGP Peer Connectivity Profile）] をクリックすると、[BGP ピア接続プロファイル（BGP Peer Connectivity Profile）] ページが右側のメイン ウィンドウに表示されます。

ステップ 3 [BGP ピア接続プロファイル（BGP Peer Connectivity Profile）] ページに [ルート制御プロファイル（Route Control Profile）] 領域が表示されるまでページを下にスクロールします。

ステップ 4 既存の IP ベースの L3Out に対してルート制御ポリシーがすでに設定されているかどうかを確認します。

既存の IP ベースの L3Out に対してルート制御ポリシーが設定されている場合と設定されていない場合があります。ただし、新しい SR-MPLS L3Out の場合は、ルート制御ポリシーを設定する必要があります。既存の IP ベースの L3Out にルート制御ポリシーが設定されている場合は、新しい SR-MPLS L3Out にそれらのルート制御ポリシーを使用できます。それ以外の場合は、SR-MPLS L3Out の新しいルート制御ポリシーを作成する必要があります。

- [ルート制御プロファイル（Route Control Profile）] テーブルに 2 つのルート制御プロファイルが表示されている場合：
  - エクスポート ルート制御ポリシー。表の [方向（Direction）] 列に [ルート エクスポート ポリシー（Route Export Policy）] と表示されます。
  - インポート ルート制御ポリシー。表の [方向（Direction）] 列に [ルート インポート ポリシー（Route Import Policy）] と表示されます。

  IP ベースの L3Out に対してルート制御ポリシーがすでに設定されています。ステップ 5（233 ページ）に進みます。
- [ルート制御プロファイル（Route Control Profiles）] テーブルに 2 つのルート制御プロファイルが表示されない場合は、SR-MPLS L3Out に使用する新しいルート マップを作成します。

a) [**ナビゲーション（Navigation）**] ペインで、**[テナント（Tenants）]** > **[*tenant_name_for_IP_handoff_L3Out*]** > **[ポリシー（Policies）]** > **[プロトコル（Protocol）]** を展開します。
b) [ルート制御のルート マップ（Route Maps for Route Control）] を右クリックし、[ルート制御のルート マップの作成（Create Route Maps for Route Control）] を選択します。
c) [**ルート制御のルート マップの作成（Create Route Maps for Route Control**）] ダイアログ ボックスで、[**名前（Name**）] フィールドに、ルート プロファイル名を入力します。
d) [**タイプ（Type**）] フィールドで、[**ルーティング ポリシーのみ照合（Match Routing Policy Only**）] を選択する必要があります。
e) [コンテキスト（Contexts）] 領域で [+] サインをクリックして、[**ルート制御コンテキスト作成（Create Route Control Context**）] ダイアログ ボックスを表示し、次のアクションを実行します。

1. 必要に応じて、[**順序（Order**）] と [**名前（Name**）] フィールドに入力します。
2. [一致ルール（Match Rule）] フィールドで、[一致ルールの作成（Create Match Rule）] をクリックします。
3. [**一致ルール（Match Rule**）] ダイアログ ボックスの [**名前（Name**）] フィールドに、一致ルールの名前を入力します。
4. 該当するフィールド（一致 Regex コミュニティ条件、一致コミュニティ条件、および一致プレフィックス）に必要な情報を入力し、[送信（Submit）] をクリックします。

5. [セット ルール（**Set Rule**）] フィールドで、[ルート マップのセット ルールの作成（**Create Set Rules for a Route Map**）] をクリックします。
6. [ルート マップのセット ルールの作成（**Create Set Rules for a Route Map**）] ダイアログボックスの [名前（**Name**）] フィールドに、ルールの名前を入力します。
7. 目的の属性および関連するコミュニティ、条件、タグ、および設定 (preferences) を選択します。[完了（Finish）] をクリックします。
8. [ルート制御コンテキストの作成（**Create Route Control Context**）] ダイアログボックスで、[**OK**] をクリックします。
9. [ルート マップの作成（**Create Route Map**）] ダイアログ ボックスで、[送信（**Submit**）] をクリックします。

f) BGP ピア接続プロファイル スクリーンに移動します。

[テナント（Tenants）] > [*tenant_name_for_IP_handoff_L3Out*] > [ネットワーキング（Networking]） > [L3Outs] > [*L3out-name*] > [論理ノード プロファイル（Logical Node Profiles）] > [*logical-node-profile-name*] > [論理インターフェイス プロファイル（Logical Interface Profiles）] > [*logical-interface-profile-name*] > [*BGP_peer_connectivity_profile*]

g) 左側のナビゲーションバーで [BGP ピア接続プロファイル（BGP Peer Connectivity Profile）] をクリックすると、[BGP ピア接続プロファイル（BGP Peer Connectivity Profile）] ページが右側のメイン ウィンドウに表示されます。

h) [ルート制御プロファイル（Route Control Profile）] フィールドまで下にスクロールし、[+] をクリックして次の項目を設定します。

- [名前（Name）] : ルート インポート ポリシー用に設定したルート マップを選択します。
- [方向（Direction）] : [方向（Direction）] フィールドで [ルート インポート ポリシー（Route Import Policy）] を選択します。

これらの手順を繰り返して、ルート エクスポート ポリシーのルート マップを選択し、[方向（Direction）] フィールドで [ルート エクスポート ポリシー（Route Export Policy）] を設定します。

ステップ 5 移行を実行する VRF の境界リーフ スイッチ内のすべてのピアにルート ポリシーを設定することにより、BGP に新しい SR パスを選択させます。

- 以前に設定された IP ベースの L3Out が eBGP 用に設定されている場合、IP ベースの L3Out ピアのルート インポート ポリシーとルート エクスポート ポリシーの両方に、追加の AS パス エントリ（ローカル エントリと同じ AS など）を設定します 。これが最も一般的なシナリオです。

（注） 次の手順では、ルート マップにルールが設定されていないことを前提としています。ルート マップに設定済みのルールをすでに設定している場合は、既存の設定済みルールを編集して AS パス エントリを追加します（[AS パスの設定（Set AS Path）] チェックボックスをオンにし、[AS 番号を付加（Prepend AS）] を選択して、[+] をクリックして AS 番号を付加します）。

1. **[テナント（Tenant）] > [*tenant_name_for_IP_handoff_L3Out*] > [ポリシー（Policies）] > [プロトコル（Protocol）] > [セット ルール（Set Rules）]** の順に移動し、**[ルート マップのセット ルールの作成（Create Set Rules for a Route Map）]** を右クリックします。

   [ルート マップの設定ルールの作成（Create Set Rules For A Route Map）] ウィンドウが表示されます。

2. **設定ルールの A ルート マップの作成** ダイアログボックス、次のタスクを実行します。

   1. [名前（Name）] フィールドに、これらの設定ルールの名前を入力します。
   2. [AS パスの設定（Set AS Path）] チェックボックスをオンにし、[次へ（Next）] をクリックします。
   3. **[AS パス（AS Path）]** ウィンドウで **[+]** をクリックして **[AS パスの設定を作成（Create Set AS Path）]** ダイアログ ボックスを開きます。

3. 基準に **[AS 番号の付加（Prepend AS）]** を選択し、**[+]** をクリックして AS 番号を先頭に付加します。

4. AS 番号とその順序を入力し、クリックして **更新** 。

5. **[OK]** をクリックします。

6. [ルート マップの設定ルールを作成（Create Set Rules For A Rout Map）] ウィンドウで AS パスに基づく設定ルールの基準を確認し、[完了（Finish）] をクリックします。

7. この既存の IP ベースの L3Out の [BGP ピア接続プロファイル（BGP Peer Connectivity Profile）] 画面に戻ります。

   [テナント（Tenants）] > [*tenant_name_for_IP_handoff_L3Out*] > [ネットワーキング（Networking）] > [L3Outs] > [*L3out-name*] > [論理ノード プロファイル（Logical Node Profiles）] > [*logical-node-profile-name*] > [論理インターフェイス プロファイル（Logical Interface Profiles）] > [*logical-interface-profile-name*] > [*BGP_peer_connectivity_profile*]

8. [ルート制御プロファイル（Route Control Profile）] 領域までスクロールし、この既存の IP ベースの L3Out に使用されているエクスポート ルート制御ポリシーとインポート ルート制御ポリシーの両方のルート プロファイル名を確認します。

9. **[テナント（Tenants）] > [*tenant_name_for_IP_handoff_L3Out*] > [ポリシー（Policies）] > [プロトコル（Protocol）] > [ルート制御のルート マップ（Route Maps for Route Control）]** の順に移動します。

10. 最初に、この既存の IP ベースの L3Out に使用されているエクスポート ルート制御プロファイルを見つけ、そのルート プロファイルをクリックします。

    このルート制御プロファイルのプロパティ ページがメイン パネルに表示されます。

11. ページでルート制御コンテキストエントリを見つけ、ルート制御コンテキストエントリをダブルクリックします。

    このルート制御コンテキストのプロパティ ページが表示されます。

12. [セット ルール（Set Rule）] 領域で、追加の AS パス エントリを使用してこれらの手順で前に作成した設定ルールを選択し、[送信（Submit）] をクリックします。

13. 次に、この既存の IP ベースの L3Out に使用されている import ルート制御プロファイルを見つけ、そのルートプロファイルをクリックしてから、インポートルート制御プロファイルの追加の AS パスエントリを使用してこれらの手順を繰り返します。これを行うと、外部ソースが優先を開始する必要がある着信トラフィックに影響します。

- 以前に設定された IP ベースの L3Out が iBGP 用に設定されている場合、SR-MPLS は eBGP のみをサポートするため、前の箇条書きの説明のように、eBGP が設定された SR-MPLS L3Out にトラフィックを誘導するためにローカル設定を使用する必要があります。IP ベースの L3Out ピアのルート インポート ポリシーとルート エクスポート ポリシーの両方を、より低いローカル プリファレンス値に設定します。

  1. **[テナント（Tenant）]** > **[*tenant_name_for_IP_handoff_L3Out*]** > **[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[セット ルール（Set Rules）]** の順に移動し、[**ルート マップのセット ルールの作成（Create Set Rules for a Route Map**）] を右クリックします。

     [**ルート マップの設定ルールの作成（Create Set Rules For A Route Map**）] ウィンドウが表示されます。

  2. [名前（Name）] フィールドに、名前を入力します。

  3. [プリファレンスの設定（Set Preference）] チェックボックスをオンにします。

     [プリファレンス（Preferences）] フィールドが表示されます。

  4. BGP ローカル プリファレンス パス値を入力します。

     範囲は 0 ～ 4294967295 です。

  5. [完了（Finish）] をクリックします。

  6. この既存の IP ベースの L3Out の [BGP ピア接続プロファイル（BGP Peer Connectivity Profile）] 画面に戻ります。

     [テナント（Tenants）] > **[*tenant_name_for_IP_handoff_L3Out*]** > **[ネットワーキング（Networking）]** > **[L3Outs]** > **[*L3out-name*]** > **[論理ノード プロファイル（Logical Node Profiles）]** > **[*logical-node-profile-name*]** > **[論理インターフェイス プロファイル（Logical Interface Profiles）]** > **[*logical-interface-profile-name*]** > **[*BGP_peer_connectivity_profile*]**

7. [ルート制御プロファイル（Route Control Profile）] 領域までスクロールし、この既存の IP ベースの L3Out に使用されているエクスポート ルート制御ポリシーとインポート ルート制御ポリシーの両方のルート プロファイル名を確認します。
8. **[テナント（Tenants）]** > **[*tenant_name_for_IP_handoff_L3Out*]** > **[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[ルート制御のルート マップ（Route Maps for Route Control）]** の順に移動します。
9. 最初に、この既存の IP ベースの L3Out に使用されているエクスポート ルート制御プロファイルを見つけ、そのルート プロファイルをクリックします。

   このルート制御プロファイルのプロパティ ページがメイン パネルに表示されます。
10. ページでルート制御コンテキスト エントリを見つけ、ルート制御コンテキスト エントリをダブルクリックします。

    このルート制御コンテキストのプロパティ ページが表示されます。
11. [セット ルール（Set Rule）] 領域で、BGP ローカル プリファレンス パスを使用してこれらの手順で作成した設定ルールを選択し、[送信（Submit）] をクリックします。
12. 次に、この既存の IP ベースの L3Out に使用されているインポート ルート制御プロファイルを見つけ、そのルート プロファイルをクリックしてから、インポート ルート制御プロファイルの BGP ローカル プリファレンス パス エントリを使用してこれらの手順を繰り返します。

ステップ 6 トラフィックが SR-MPLS パスを選択していることを確認します。

ルーティング/パスの選択は、SR-MPLS を使用する必要があります（BGP は、IP パスよりも SR-MPLS パスを選択する必要があります）。各 VRF の URIB のトラフィックとルートをモニタして、SR-MPLS パスが選択されていることを確認できます。

次のタスク

に示す手順を使用して、IP ベースの L3Out を切断します。IP ベースの L3Out の切断 （236 ページ）

IP ベースの L3Out の切断

このタスクでは、IP ベースの L3Out を切断します。

始める前に

- IP ハンドオフ設定から SR ハンドオフ設定への移行 （229 ページ）に記載の情報について、確認してください。

- に示す手順を使用して、IP ベースの L3Out 設定をミラーリングするように SR-MPLS VRF L3Out の外部 EPG を設定します。SR-MPLS VRF L3Out での外部 EPG の設定 （230 ページ）
- インバウンドおよびアウトバウンドトラフィックをリダイレクトし、に示す手順を使用して SR-MPLS L3Out を優先して開始するようにします。SR-MPLS L3Out へのトラフィックのリダイレクト （231 ページ）

手順

ステップ 1 IP パスをクリーン アップします。

次のいずれかの方法を使用して、IP パスをクリーン アップできます。

- 以前に設定した IP ベースの L3Out の外部 EPG で一度に 1 つのサブネットを削除します。
- 以前に設定した IP ベースの L3Out の外部 EPG を削除します。

上記のいずれかの方法では、障害がクリアされ、SR-MPLS L3Out の外部 EPG が展開されます。

セキュリティ ポリシーを IP ベースの L3Out から SR-MPLS L3Out に変更するプロセスの一環として、最大 15 秒のドロップが発生する可能性があります。その期間が経過すると、ACI から外部へのアウトバウンド トラフィックは SR-MPLS パスを使用します。

以前に設定した IP ベースの L3Out が新しい SR-MPLS L3Out に正常に移行された場合は、以前に設定した IP ベースの L3Out を削除できます。

ステップ 2 SR-MPLS に移行する追加の L3Out/VRF があるかどうかを確認します。

他のユーザ L3Out および VRF を SR-MPLS に移行するには、IP ハンドオフ設定から SR ハンドオフ設定への移行 （229 ページ）の手順を繰り返します。

IP ハンドオフ設定から SR ハンドオフ設定への移行 （229 ページ）の同じ手順を使用して、テナント GOLF L3Out とテナント SR-MPLS L3Out 間の移行を行うこともできます。

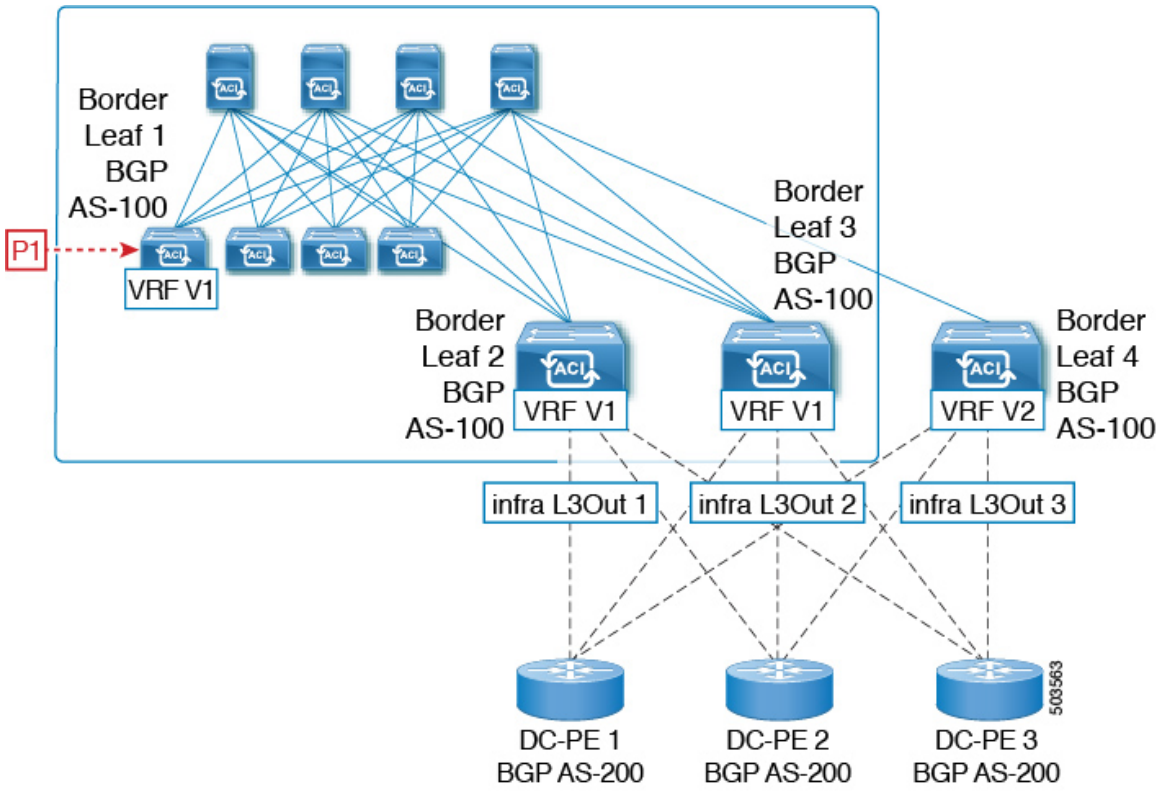
ループ防止のための BGP ドメインパス機能について

BGP ルーティング ループは、次のようなさまざまな条件が原因で発生することがあります。

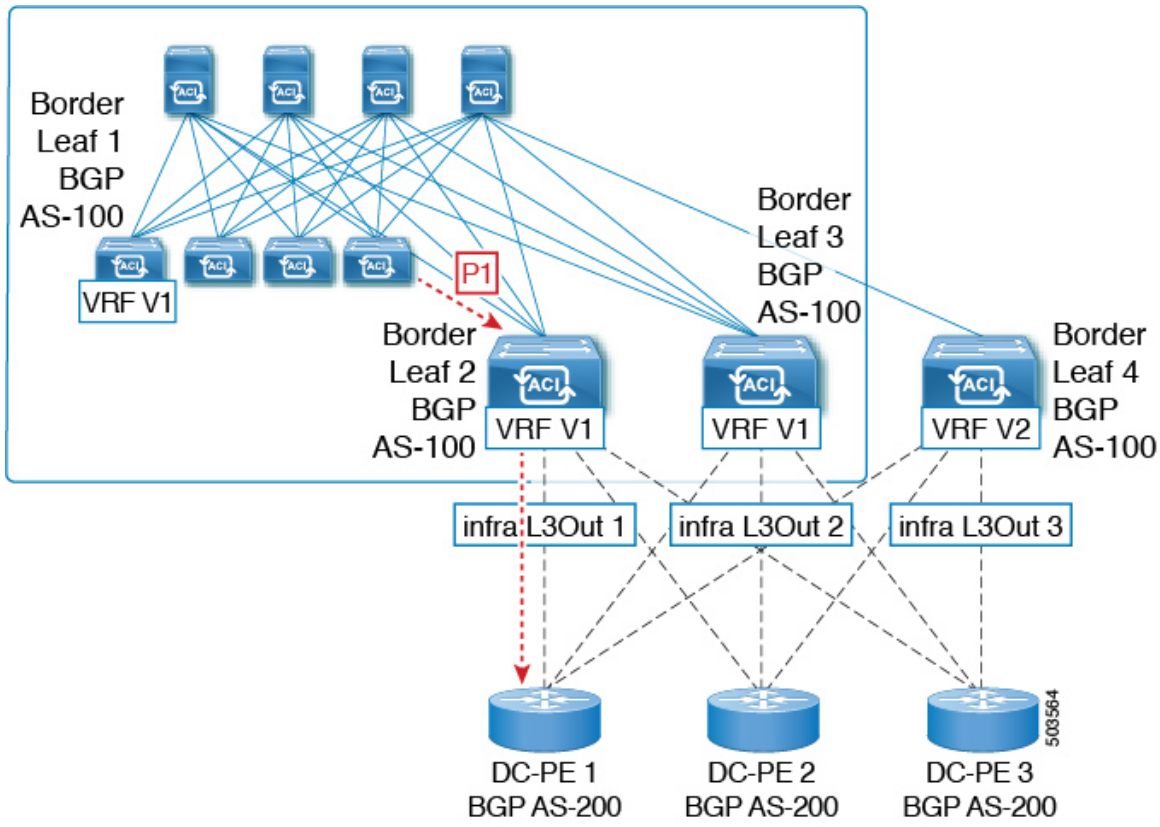
- AS パス チェックなどの既存の BGP ループ防止メカニズムの意図的な無効化
- 異なる VRF または VPN 間のルート リーク

次に、BGP ルーティング ループが発生するシナリオの例を示します。

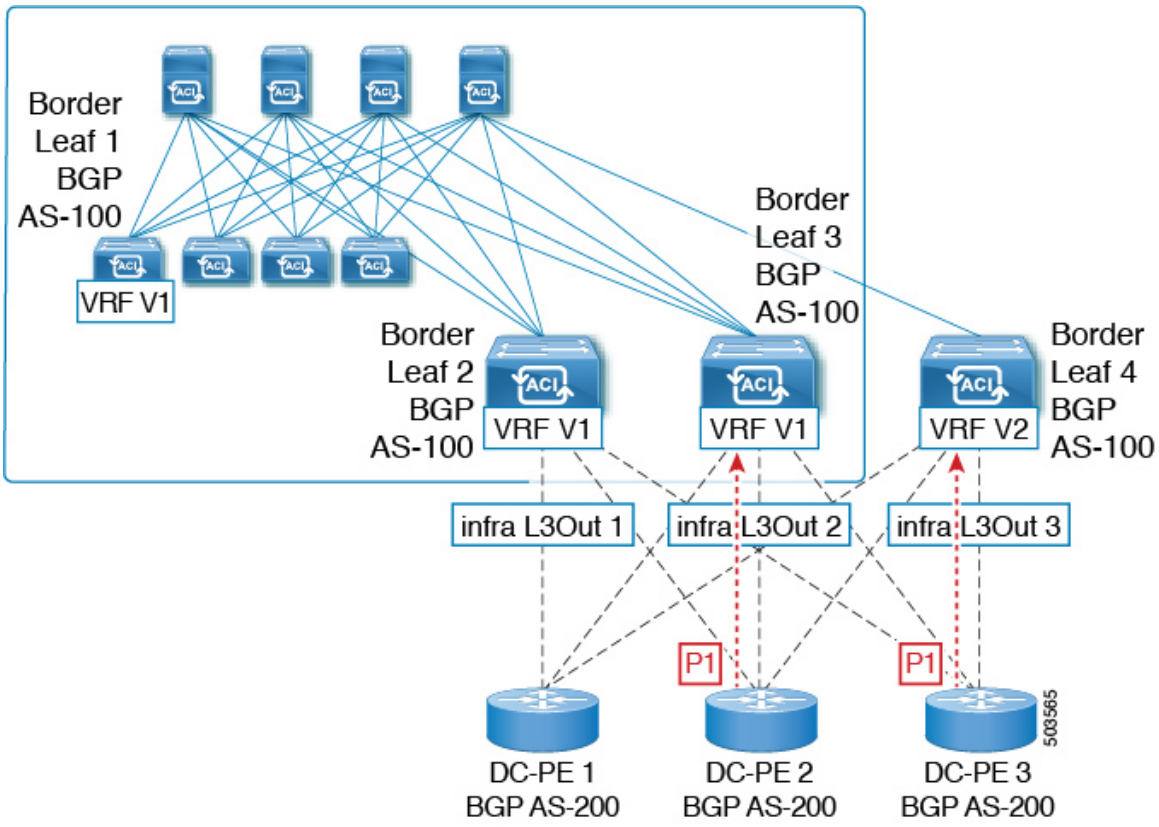
1. BGP IP L3Out ピアから受信したプレフィックス P1 は、Multiprotocol Border Gateway Protocol （MP-BGP）を使用して ACI ファブリックでアドバタイズされます。



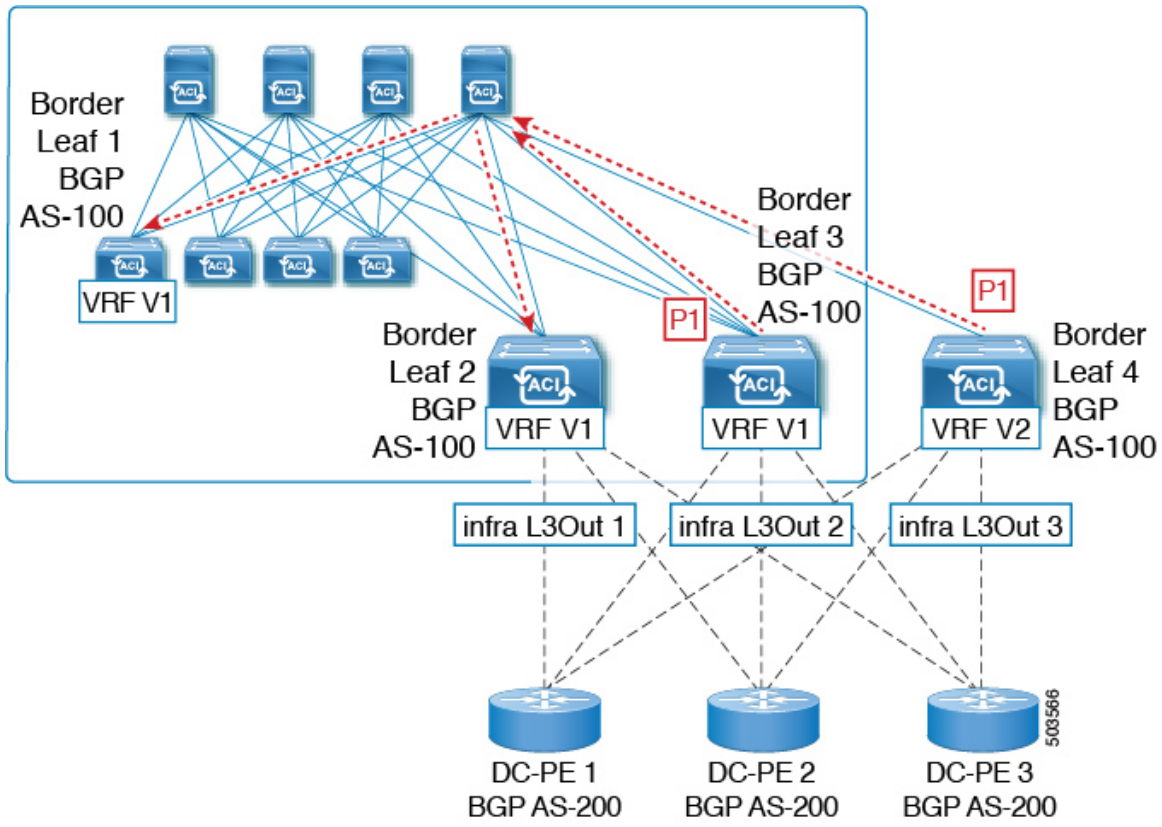
2. 中継のケースとして、このプレフィックスは SR-MPLS インフラ L3Out を介して外部にアドバタイズできます。



3. このプレフィックスは、同じ VRF または異なる VRF のいずれかで、コアから ACI ファブリックにインポートできます。



4. BGP ルーティング ループは、同じ VRF から、または別の VRF からのリークによって、このインポートされたプレフィックスが発信元スイッチにアドバタイズされるときに発生します。



リリース 5.1(3) 以降では、新しい BGP ドメイン パス機能を使用できます。これは、次の方法で BGP ルーティング ループを支援します。

- 同じ VPN または拡張 VRF 内、および異なる VPN または VRF 内のルートが通過する個別のルーティング ドメインを追跡します。
- ルートがすでに通過したドメイン内の VRF にループバックするタイミングを検出します（通常、ドメイン間のスティッチング ポイントである境界リーフ スイッチだけでなく、場合によっては内部スイッチでも）。
- ループにつながる場合に、ルートがインポートまたは受け入れられないようにします。

ACI ファブリック内では、VRF スコープはグローバルであり、設定されているすべてのスイッチに拡張されます。したがって、VRF のドメインからエクスポートされたルートは、他のスイッチの VRF に受信されないようにします。

次のコンポーネントは、ループ防止のためにBGPドメインパス機能で使用されます。

- **Routing domain ID**：ACI サイトのすべてのテナント VRF は、1 つの内部ファブリック ドメイン、各 SR-MPLS インフラ L3Out の各 VRF に 1 つのドメイン、および各 IP L3Out に 1 つのドメインに関連付けられます。BGP ドメインパス機能が有効になっている場合、これらの各ドメインには、次の形式で一意のルーティング ドメイン ID が割り当てられます。 *Base:<variable>*

- Base は、[BGP ルート リフレクタ ポリシー（BGP Route Reflector Policy）] ページの [ドメイン ID ベース（Domain ID Base）] フィールドに入力されたゼロ以外の値です。
- <variable> は、そのドメイン専用にランダムに生成された値です。

- **ドメイン パス（Domain path）**：ルートが通過するドメイン セグメントは、BGP ドメイン パス属性を使用して追跡されます。
  - ルートを受信する送信元ドメインの VRF のドメイン ID がドメイン パスの先頭に追加されます。
  - 送信元ドメイン ID はドメイン パスの先頭に追加され、境界リーフ スイッチのドメイン間でルートが再生成されます。
  - VRF のローカル ドメイン ID のいずれかがドメイン パスにある場合、外部ルートは受け入れられません。
  - ドメイン パスは、次のように表される各ドメイン セグメントとともに、オプションの遷移 BGP パス属性として伝送されます。<Domain-ID:SAFI>
  - ACI 境界リーフ スイッチは、ドメイン内のリークを追跡するために、ローカルに発信されたルートと外部ルートの両方に VRF 内部ドメイン ID を付加します。
  - 内部ドメインからのルートをインポートし、競合する外部ドメイン ID を持つノードの VRF にインストールして、内部バックアップまたは中継パスを提供できます。
  - インフラ L3Out ピアの場合、ピア ドメインのドメイン ID がルートのドメイン パスに存在する場合、ピアへのルートのアドバタイズメントはスキップされます（アウトバウンド チェックは IP L3Out ピアには適用されません）
  - 境界リーフ スイッチと非境界リーフ スイッチはどちらもドメイン パス属性を処理します。

（注） ループ防止のために BGP ドメイン パス機能を設定するか、GUI または REST API を使用して、受信したドメイン パスを送信するように設定をイネーブルにすることができます。ループ防止のために BGP ドメイン パス機能を設定したり、NX-OS スタイルの CLI を介して受信ドメイン パスを送信するように設定したりすることはできません。

（注） 以前のリリースからリリース 5.1(3) にアップグレードするときに、VRF 間共有サービス用に設定されたコントラクトがある場合、BGP ドメイン ID にリリース 5.1(3) にアップグレードする前に設定された契約で設定されています。このような状況では、契約を削除してから、契約を追加し直すと、BGP ドメインの更新が可能になります。これは、リリース 5.1(3) へのアップグレード前に設定された契約がある場合にのみ問題になります。これは、リリース 5.1(3) へのアップグレードの完了後に新しい契約を作成する場合は問題になりません。

GUI を使用したループ防止のための BGP ドメイン パス機能の設定

始める前に

ループ防止のための BGP ドメインパス機能について （237 ページ）に記載されている情報を使用して、BGP ドメイン パス機能に精通します。

手順

ステップ 1 ループ防止に BGP ドメイン パス機能を使用する場合は、BGP ルート リフレクタに BGP ドメイン パス属性を設定します。

（注） ループ防止に BGP ドメイン パス機能を使用しないが、受信したドメイン パスを送信する場合は、この手順で BGP ドメイン リフレクタの BGP ドメイン パス機能を有効にしないでください。代わりに、に直接移動して、適切な BGP 接続ウィンドウの [ドメイン パスの送信（Send Domain Path）] フィールドのみを有効にします。ステップ 2 （244 ページ）

a) **[システム（System）] > [システム設定（System Settings）] > [BGP ルート リフレクター（BGP Route Reflector）]** の順に移動します。

[BGP ルート リフレクター（BGP Route Reflector）] ウィンドウが表示されます。このウィンドウで [ポリシー（Policy）] ページ タブが選択されていることを確認します。

b) [ドメイン ID ベース（Domain ID Base）] フィールドを見つけます。

c) [ドメイン ID ベース（Domain ID Base）] フィールドに数値を入力します。

- BGP ドメインパス機能を有効にするには、1 ー 4294967295 の値を入力します。ACI ファブリックがマルチサイト環境の一部である場合は、この [ドメイン ID ベース（Domain ID Base）] フィールドでこの ACI ファブリックに固有の一意の値を使用してください。
- BGP ドメインパス機能を無効にするには、この [ドメイン ID ベース（ID Base）] フィールドに 0 を入力します。

ループ防止の BGP ドメインパス機能が有効になっている場合は、Base:<variable> 形式の暗黙のルーティング ドメイン ID が割り当てられます。

- [ベース（Base）] は、この [ドメイン ID ベース（Domain ID Base）] フィールドに入力したゼロ以外の値です。
- <変数（variable）> は、VRF または L3Out 用にランダムに生成された値で、ループ防止の BGP ドメインパス機能に使用されます。

このルーティング ドメイン ID は、次のドメインを識別するために BGP に渡されます。

- VRF：そのテナントの VRF ウィンドウの [ポリシー（Policy）] タブにある [ルーティング ドメイン ID（Routing Domain ID）] フィールドに示されているように、各 VRF にランダムに生成された値を使用して内部ドメイン ID によって識別されます。
- IP L3Out：IP L3Out の [BGP ピア接続プロファイル（BGP Peer Connectivity Profile）] ウィンドウの [ルーティング ドメイン ID（Routing Domain ID）] フィールドに示されているように、各 IP L3Out に対してランダムに生成された値を使用して、外部ドメイン ID によって識別されます。
- SR-MPLS infra L3Out：各 SR-MPLS VRFL3Out のウィンドウの [SR-MPLS Infra L3Outs] テーブルの [ルーティング ドメイン ID（Routing Domain ID）] 列に示されているように、各 SR-MPLS infra L3Out の各 VRF にランダムに生成された値を使用して、外部ドメイン ID によって識別されます。

Domain-Path 属性は、パス内のルーティングドメイン ID に基づいてループをチェックするために着信方向で処理されます。Domain-Path 属性はピアに送信されます。これは、次の手順で説明するように、IP L3Out または SR-MPLS infraL3OutのBGP ピアレベルの [ドメイン パスの送信（Send Domain Path）] フィールドを使用して個別に制御されます。

ステップ 2 BGP ドメイン パス属性をピアに送信するには、適切な BGP 接続ウィンドウで [ドメイン パスの送信（Send Domain Path）] フィールドを有効にします。

ループ防止のために BGP ドメインパス機能を使用する場合は、最初に [ドメイン ベース ID（Domain Base ID）] を設定してから、ここで [ドメインパスの送信（Send Domain Path）] フィールドを有効にします。ステップ 1 （243 ページ）ループ防止のために BGP ドメインパス機能を使用しない場合でも、受信したドメインパスを送信する場合は、ここで [ドメイン パスの送信（Send Domain Path）] フィールドのみを有効にします（その場合は [ドメインベース ID（Domain Base ID）] を設定しないでください）。ステップ 1 （243 ページ）

- IP L3Out ピアの [ドメイン パスの送信（Send Domain Path）] フィールドを有効にするには、次の手順を実行します。

1. IP L3Out ピアの [BGP ピア接続プロファイル（BGP Peer Connectivity Profile）] ウィンドウに移動します。

   [テナント（Tenant）] > [*tenant_name*] > [ネットワーキング（Networking）] > [L3Outs] > [*L3Out_name*] > [論理ノード プロファイル（Logical Node Profile）] > [*log_node_prof_name*] > [論理インターフェイス プロファイル（Logical Interface Profile）] > [*log_int_prof_name*] > [BGP ピア（BGP Peer） *]<address>-ノード（Node）-[<node_ID>]*

   この設定された L3Out の [BGP ピア接続プロファイル（BGP Peer Connectivity Profile）] ウィンドウが表示されます。

2. [BGP ピア接続プロファイル（BGP Peer Connectivity Profile）] ウィンドウで [BGP 制御（BGP Controls）] 領域を見つけます。
3. [BGP 制御（BGP Controls）] 領域で、[ドメインパスの送信（Send Domain Path）] フィールドの横にあるボックスをクリックします。
4. **[送信（Submit）]** をクリックします。`

このアクションは、BGP ドメイン パス属性をピアに送信します。

- SR-MPLS インフラ L3Out ピアの [ドメイン パスの送信（Send Domain Path）] フィールドを有効にするには、次の手順を実行します。

  1. **[テナント（Tenant）] > [infra] > [ネットワーキング（Networking）] > [SR-MPLS Infra L3Outs] > [*SR-MPLS-infra-L3Out_name*] > [論理ノード プロファイル（Logical Node Profiles）] > [*log_node_prof_name*]**の順に移動します。

     この設定済み SR-MPLS インフラ L3Out の [論理ノードプロファイル（Logical Node Profile）] ウィンドウが表示されます。

  2. [BGP-EVPN 接続プロファイル（BGP-EVPN Connectivity Profile）] 領域を見つけ、新しい BGP-EVPN 接続ポリシーを作成するか、または既存の BGP-EVPN 接続ポリシーの [ドメイン パスの送信（Send Domain Path）] フィールドを有効にするかを決定します。

     - 新しい BGP-EVPN 接続ポリシーを作成する場合は、[BGP-EVPN 接続プロファイル（BGP-EVPN Connectivity Profile）] 領域のテーブルの上にある [+] をクリックします。[BGP-EVPN 接続ポリシーの作成（Create BGP-EVPN Connectivity Policy）] ウィンドウが表示されます。
     - 既存の BGP-EVPN 接続ポリシーの [ドメイン パスの送信（Send Domain Path）] フィールドを有効にする場合は、[BGP-EVPN 接続プロファイル（BGP-EVPN Connectivity Profile）] 領域のテーブルでそのポリシーをダブルクリックします。[BGP-EVPN 接続ポリシー（BGP-EVPN Connectivity Policy）] ウィンドウが表示されます。

  3. ウィンドウで [BGP 制御（BGP Controls）] 領域を見つけます。
  4. [BGP 制御（BGP Controls）] 領域で、[ドメインパスの送信（Send Domain Path）] フィールドの横にあるボックスをクリックします。
  5. **[送信（Submit）]** をクリックします。`

     このアクションは、BGP ドメイン パス属性をピアに送信します。

ステップ 3 適切なエリアに移動して、さまざまなドメインに割り当てられたルーティング ID を確認します。

- VRF ドメインに割り当てられたルーティング ID を確認するには、次の手順を実行します。

  Tenant tenant_name Networking VRFs VRF_name をクリックし、その VRF の [ポリシー（Policy）] タブをクリックして、[VRF] ウィンドウの[ルーティング ドメイン ID（Routing Domain ID）] フィールドのエントリを見つけます。＞＞＞＞

- IP L3Out ドメインに割り当てられたルーティング ID を確認するには、次の手順を実行します。

  [テナント（Tenants）] > [*tenant_name*] > [ネットワーキング（Networking）] > [L3Outs] > [*L3Out_name*] > [論理ノード プロファイル（Logical Node Profiles）] > [*log_node_prof_name*] > [BGP ピア（BGP Peer）]の順に移動し、その後 [BGP ピア接続プロファイル（BGP Peer

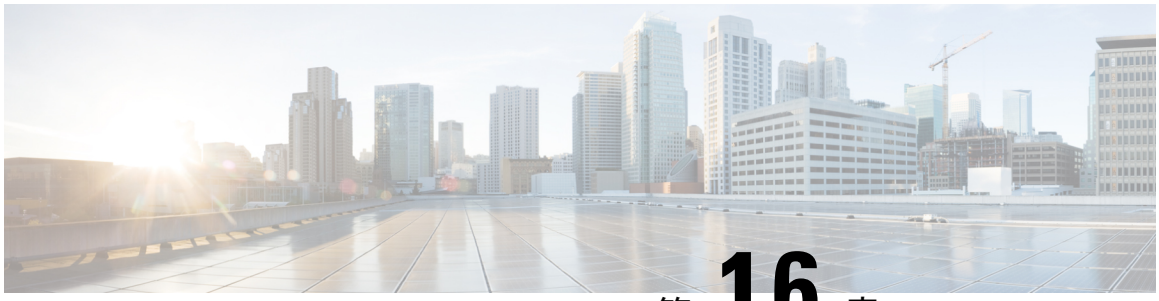
Connectivity Profile）] ウィンドウの [**ルーティング ドメイン ID（Routing Domain ID**）] フィールドでエントリを見つけます。

- SR-MPLS インフラ L3Out ドメインに割り当てられたルーティング ID を確認するには、次の場所に移動します。

  [テナント（Tenants）] [tenant_name] [ネットワーキング（Networking）] [SR-MPLS VRF L3Outs] [SR-MPLS_VRF_L3Out_name] をクリックし、[SR-MPLS VRFL3Out] のウィンドウで [SR-MPLS Infra L3Outs] テーブルの [ルーティング ドメイン ID（Routing Domain ID）] カラムのエントリを見つけます。 > > > >

第 II 部

外部ルーティング（L3Out）の設定



第 16 章

WAN およびその他の外部ネットワーク フォワーディング

この章は、次の内容で構成されています。

ネットワーク ドメイン

ファブリック管理者は、ポート、プロトコル、VLAN プール、およびカプセル化を設定するドメイン ポリシーを作成します。これらのポリシーは、単一テナント専用にすることも、共有することもできます。ファブリック管理者が ACI ファブリック内にドメインを設定すると、テナント管理者はテナント エンドポイント グループ（EPG）をドメインに関連付けることができます。

以下のネットワーク ドメイン プロファイルを設定できます。

- VMM ドメイン プロファイル（`vmmDomP`）は、仮想マシンのハイパーバイザ統合のために必要です。
- 物理ドメイン プロファイル（`physDomP`）は、ベア メタル サーバ接続と管理アクセスに使用します。

- ブリッジド外部ネットワーク ドメイン プロファイル（l2extDomP）は通常、ACI ファブリックのリーフ スイッチにブリッジド外部ネットワーク トランク スイッチを接続するために使用されます。
- ルーテッド外部ネットワーク ドメイン プロファイル（l3extDomP）は、ACI ファブリックのリーフ スイッチにルータを接続するために使用されます。
- ファイバチャネル ドメインプロファイル(fcDomP)は、ファイバチャネルの VLAN と VSAN を接続するために使用されます。

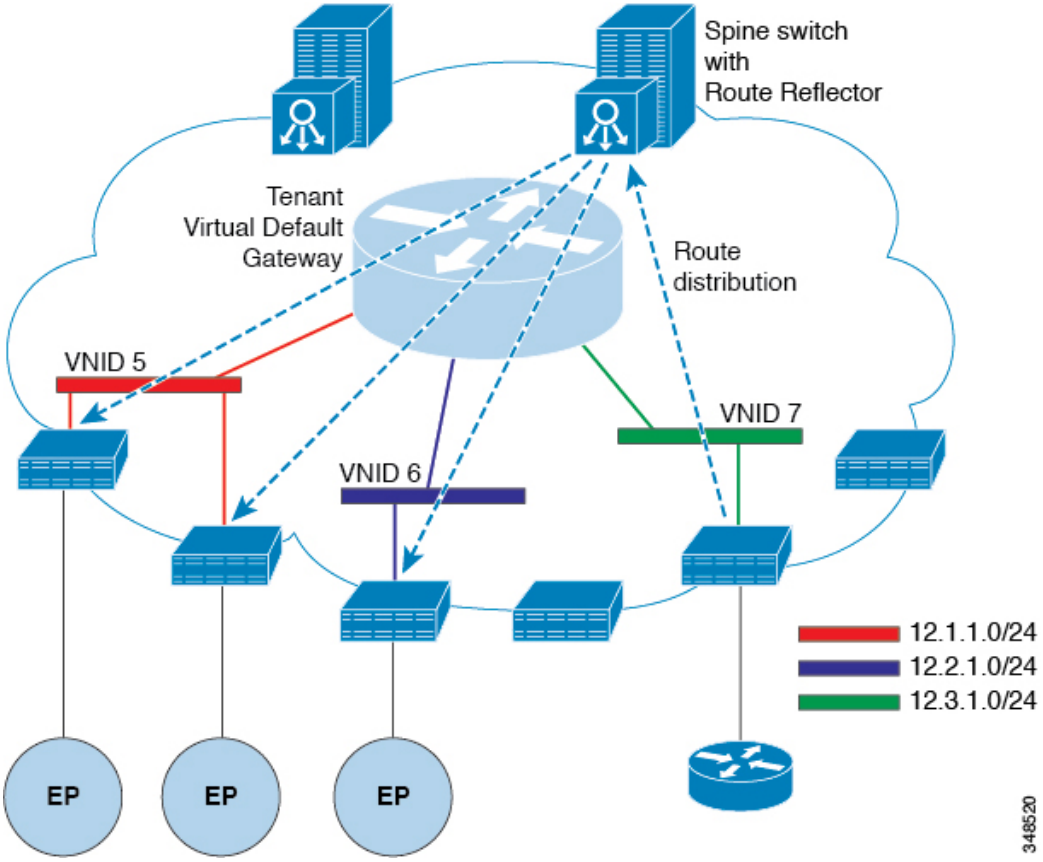
ドメインは VLAN プールに関連付けられるように設定されます。その後、EPG は、ドメインに関連付けられている VLAN を使用するように設定されます。

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

ルータ ピアリングおよびルート配布

次の図に示すように、ルーティング ピア モデルを使用すると、リーフ スイッチ インターフェイスが外部ルータのルーティング プロトコルとピアリングするように静的に設定されます。

図 *26 :* ルータのピアリング



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

ルートのインポートとエクスポート、ルート集約、ルート コミュニティの一致

サブネット ルートのエクスポートまたはインポート設定オプションは、次に説明するスコープおよび集約オプションに従って指定できます。

ルーティング対象サブネットについては、以下のスコープ オプションが使用可能です。

- エクスポート ルート制御サブネット：エクスポート ルート方向を制御します。
- インポート ルート制御サブネット：インポート ルート方向を制御します。

（注） インポート ルート コントロールは、BGP と、OSPF が EIGRP ではなく、サポートされています。

- 外部 EPG (セキュリティ インポート サブネット) の外部サブネット: どの外部サブネットが、特定の外部 L3Out EPG（ `l3extInstP` ）の一部として適用されるコントラクトを保持するか指定します。サブネットの `l3extInstP` 外部 EPG として分類、サブネット上の範囲を「インポートセキュリティ」に設定する必要があります。この範囲のサブネットを決定する IP アドレスが関連付けられています、 `l3extInstP` 。これが決定されると、契約は、他のどの Epg でその外部のサブネットが通信を許可を決定します。たとえば、レイヤ 3 外部の外部ネットワーク (`L3extOut`) の ACI スイッチでトラフィックが開始する場合、`l3extInstP` に関連付けられている送信元 IP アドレスを判断するための検索が行われます。このアクションより一般的なサブネット上で複数の特定のサブネットが優先されるようにで最長プレフィックス一致 (ほか) に基づいて行われます。
- 共有ルート制御サブネット — 共有サービス設定においては、この特性が有効になっているサブネットだけが、コンシューマ EPG の Virtual Routing and Forwarding （VRF）にインポートされます。これは VRF 間の共有サービスのルート方向を制御します。
- 共有セキュリティ インポート サブネット：インポート対象サブネットに共有コントラクトを適用します。デフォルトの仕様では、外部 EPG 用外部サブネットが設定されています。

ルート対象サブネットを集約することができます。集約が設定されていない場合は、サブネットが正確に照合されます。たとえば、サブネットが 11.1.0.0/16 の場合、11.1.1.0/24 ルートにはポリシーが適用されず、ルートが 11.1.0.0/16 である場合のみ適用されます。すべてのサブネットを 1 つずつ定義する作業は面倒でエラーが発生しやすいので、それを回避するために、サブネットのセットを 1 つのエクスポート、インポートまたは共有ルート ポリシーに集約することができます。現時点では、0/0 サブネットのみ集約可能です。0/0 に集約を指定すると、次の選択オプションに基づき、すべてのルートがインポート、エクスポートされ、異なる VRF と共有されます:

- 集約エクスポート — VRF (サブネット 0/0) のすべての中継ルートをエクスポートします。
- 集約インポート — 所定の L3 ピア (サブネット 0/0) のすべて着信ルートをインポートします。

（注） BGP、OSPF が EIGRP の集約インポート ルート制御はサポートされます。

- 集約共有ルート — 1 つの VRF で学習されているルートを別の VRF にアドバタイズする必要がある場合、サブネットとの正確な一致、またはサブネット マスクに従った方法で共有

できます。集約共有ルートでは、複数のサブネットマスクを使用して、どの特定のルートグループをVRF間で共有するかを決定できます。たとえば、10.1.0.0/16と12.1.0.0/16を指定してこれらのサブネットを集約することができます。あるいは、0/0を使用すると、複数のVRFのすべてのサブネット ルートを共有できます。

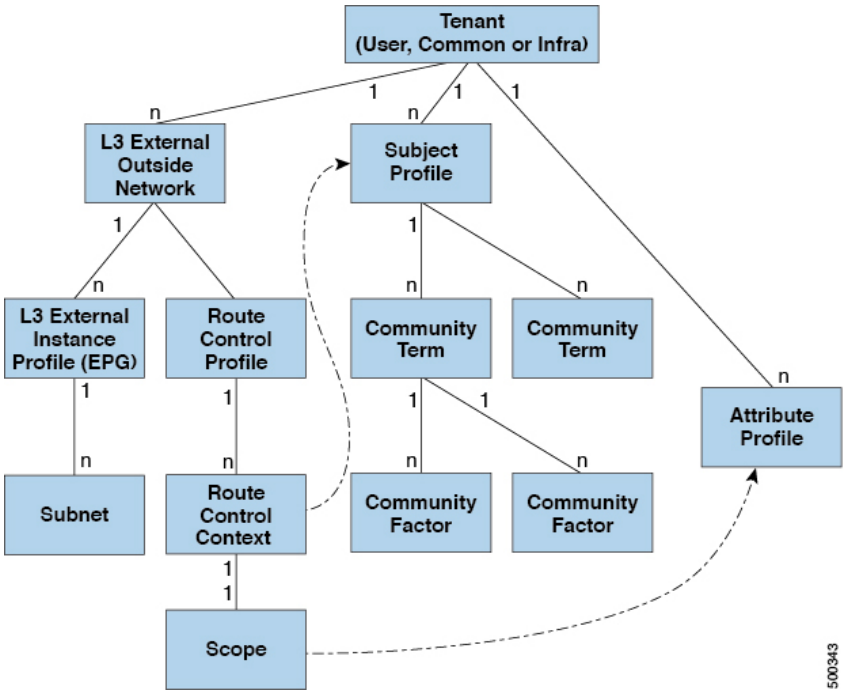
（注） 第2世代のスイッチのVRF機能間で正常にルートが共有されます（N9K-93108TC-EXなど、スイッチ モデル名の最後やその後に「EX」や「FX」がつくCisco Nexus N9K）。第1世代のスイッチですが、ルートを保存する物理的な3進コンテンツ対応メモリ（TCAM）にルートの解析を完全にサポートするだけの容量がないため、この設定のパケットは失敗する可能性があります。

ルート集約では、多数の具体的なアドレスを1つのアドレスに置き換えることで、ルートテーブルが簡素化します。たとえば、10.1.1.0/24、10.1.2.0/24、10.1.3.0/24は10.1.0.0/16に置き換えられます。ルート集約ポリシーにより、ボーダー リーフ スイッチとそのネイバー リーフ スイッチの間でルートを効率的に共有することができます。BGP、OSPF、あるいはEIGRPのルート集約ポリシーは、ブリッジ ドメインまたは中継サブネットに適用されます。OSPFでは、エリア間ルート集約と外部ルート集約がサポートされます。集約ルートはエクスポートされます。ファブリック内でのアドバタイズは行われません。上記の例では、ルート集約ポリシーが適用され、EPGが10.1.0.0/16サブネットを使用している場合、10.1.0.0/16の範囲全体がすべての隣接リーフ スイッチと共有されます。

（注） 同じリーフ スイッチで2つの `L3extOut` ポリシーにOSPFを設定している場合（1つはレギュラーで、もう1つはバックボーン）には、VRF内の全エリアに集約が適用されるため、一方の `L3extOut` で設定されているルート集約ポリシーが両方のL3extOutポリシーに適用されます。

次の図に示すように、ルート制御プロファイルは、プレフィックスベースおよびコミュニティベースの一致に基づいて、ルート マップを取得します。

図 *27 :* ルート コミュニティ マッチング



ルート制御プロファイル（rtctrtlProfile）は、許可される対象を指定します。ルート制御コンテキストは一致対象を指定し、スコープは設定すべき対象を指定します。サブジェクトプロファイルには、コミュニティ マッチの仕様が含まれます。これは複数の l3extOut で使用できます。サブジェクト プロファイル（SubjP）には、それぞれ 1 つまたは複数のコミュニティ ファクタ（コミュニティ）を含む複数のコミュニティ タームを含めることができます。これにより、次のブール演算を指定することができます。

- 複数コミュニティ ターム間の論理的 OR
- 複数コミュニティ ターム間の論理的 AND

たとえば、北東と呼ばれるコミュニティ タームに、それぞれ多くのルートを含む複数のコミュニティが含まれているとします。また、南東という別のコミュニティ タームにも、さまざまなルートが多数含まれているとします。管理者は、そのどちらかあるいは両方を一致させることを選択できます。コミュニティ ファクタ タイプには、レギュラーまたは拡張を使用できます。拡張タイプのコミュニティ ファクタを使用する際には、仕様間の重複がないよう注意することが必要です。

ルート制御プロファイルのスコープ部分は、属性プロファイル（rtctrlAttrP）を参照して、適用すべき設定-アクション（プリファレンス、ネクスト ホップ、コミュニティなど）を指定します。ルートを l3extOut から学習した場合は、ルートの属性を変更できます。

上の図は、l3extOut に rtctrtlProfile が含まれているケースを示しています。rtctrtlProfile はテナントの下にも配置できます。この例では、l3extOut に、自身をテナント下の rtctrtlProfile と関連付ける相互リーク関係ポリシー（L3extRsInterleakPol）が設定されています。この設定により、再利用、 rtctrtlProfile 複数の l3extOut 接続します。BGP 属性

(BGP は、ファブリック内で使用される) は、それを OSPF からは、ファブリックを学習ルートの追跡することもできます。L3extOut 下で定義された rtctrtlProfile の優先順位は、テナント下で定義されたものよりも高くなります。

rtctrtlProfile には、組み合わせ可能およびグローバルという 2 つのモードがあります。デフォルトの組み合わせ可能モードでは、パーベイシブ サブネット（fvSubnet）および外部サブネット（l3extSubnet）に一致/設定メカニズムを組み合わせてルート マップをレンダリングします。グローバル モードはテナント内のすべてのサブネットに適用され、そのほかのポリシー属性の設定が無効になります。グローバル rtctrtlProfile では、明示的な（0/0）サブネットを定義しなくても、すべての動作が許可されます。グローバル rtctrtlProfile は、コミュニティやネクストホップといった異なるサブネット属性を使用してマッチングが行われる非プレフィックス ベースの一致ルールと一緒に使用されます。1 つのテナント下で複数の rtctrtlProfile ポリシーを設定できます。

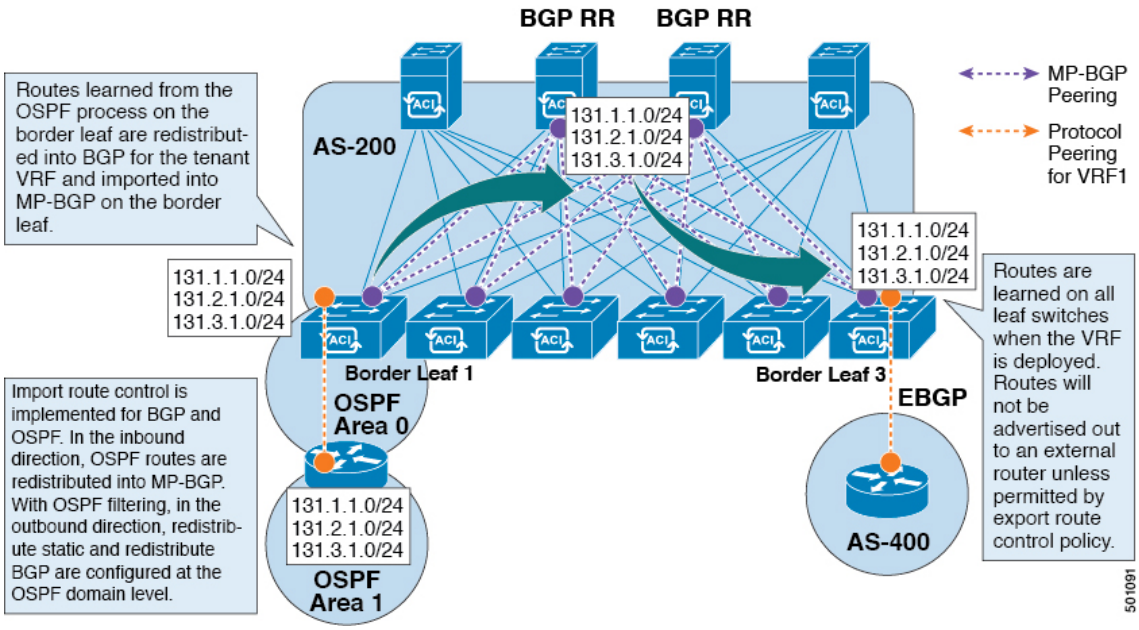
rtctrtlProfile ポリシーによって、デフォルト インポートおよびデフォルト エクスポートのルート制御の拡張が可能になります。集約インポートあるいはエクスポート ルートを伴う Layer 3 Outside ネットワークには、サポート対象デフォルト エクスポート/デフォルト インポートおよびサポート対象 0/0 集約ポリシーを指定するインポート/エクスポート ポリシーを設定できます。すべてのルート（着信または発信）に rtctrtlProfile ポリシーを適用するには、一致ルールのないグローバル デフォルト rtctrtlProfile を定義します。

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

プロトコル相互リークと再配布ポリシーは、ACI ファブリック BGP ルートで共有される外部学習ルートを制御します。設定属性はサポートされています。これらのポリシーは L3extOut 単位、ノード単位、VRF 単位でサポートされます。相互リークポリシーは、L3extOut 内のルーティング プロトコルによって学習されたルートに適用されます。現在のところ、相互リークと再配布ポリシーは、OSPF v2 および v3 でサポートされています。ルート制御ポリシー rtctrtlProfile は、相互リーク ポリシーによって消費される場合、グローバルとして定義する必要があります。

ACI のルート再配布

図 *28 : ACI* のルート再配布



- 境界リーフの OSPF プロセスで学習されたルートは、テナント VRF 用に BGP に再配布され、それらは境界リーフの MP-BGP にインポートされます。
- インポート ルート制御は、BGP および OSPF ではサポートされていますが、EIGRP ではサポートされていません。
- エクスポート ルート制御は、OSPF、BGP、および EIGRP でサポートされています。
- ルートは、VRF が導入されている境界リーフで学習されます。ルートは、エクスポート ルート制御で許可されていない限り、外部レイヤ 3 Outside 接続にアドバタイズされません。

（注） ブリッジ ドメイン/EPG のサブネットが [Advertise Externally] に設定されている場合、サブネットは境界リーフの静的ルートとしてプログラムされます。スタティック ルートがアドバタイズされると、ルーティング プロトコルに直接注入されない外部ネットワークとして EPG のレイヤ 3 ネットワーク ルーティング プロトコルに再配布されます。

ACI ファブリック内のルート配布

ACI は以下のルーティング メカニズムをサポートします。

- スタティック ルート
- OSPFv2（IPv4）
- OSPFv3（IPv6）
- iBGP
- eBGP（IPv4 および IPv6）
- EIGRP (IPv4 および IPv6) プロトコル

ACI は、外部ルータに接続する際に VRF-Lite の実装をサポートします。サブインターフェイスを使用して、境界リーフは 1 つの物理インターフェイスを持つ複数のテナントへのレイヤ 3 Outside 接続を提供できます。VRF-Lite の実装では、テナントごとに 1 つのプロトコル セッションが必要です。

ACI ファブリック内の外部ルートを伝播するために、ACI ファブリック内のリーフ スイッチとスパイン スイッチの間に Multiprotocol BGP（MP-BGP）が実装されています。単一ファブリック内で多数のリーフ スイッチをサポートするために、BGP ルート リフレクタ テクノロジーが導入されています。リーフ スイッチとスパイン スイッチはすべて 1 つの BGP 自律システム（AS）内にあります。境界リーフが外部ルートを学習すると、MP-BGP アドレス ファミリ VPN バージョン 4 または VPN バージョン 6 に特定の VRF の外部ルートを再配布できます。アドレス ファミリ VPN バージョン 4 を使用して、MP-BGP は VRF ごとに別の BGP ルーティング テーブルを維持します。MP-BGP 内で、境界リーフは BGP ルート リフレクタであるスパイン スイッチにルートをアドバタイズします。その後、ルートは VRF（APIC GUI の用語ではプライベート ネットワーク）がインスタンス化されているすべてのリーフに伝播されます。

外部レイヤ 3 Outside 接続タイプ

ACI は、以下の外部レイヤ 3 Outside 接続オプションをサポートします。

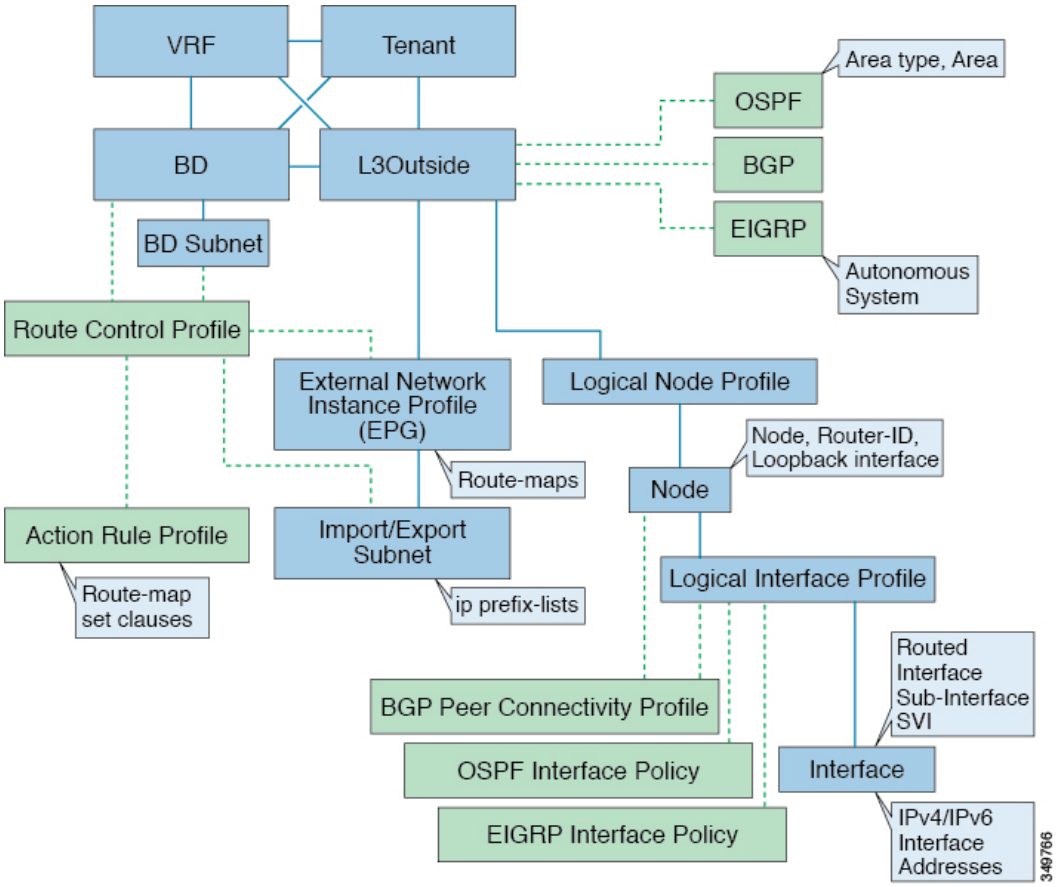
- スタティック ルーティング（IPv4 および IPv6 でサポート）
- 標準および NSSA エリアの OSPFv2（IPv4）
- 標準および NSSA エリアの OSPFv3（IPv6）
- iBGP（IPv4 および IPv6）
- eBGP（IPv4 および IPv6）
- BGP（IPv4 および IPv6）

外部レイヤ 3 Outside 接続は、以下のインターフェイスでサポートされます。

- レイヤ 3 ルーテッド インターフェイス
- 802.1Q タギング対応のサブインターフェイス：サブインターフェイスを使用すると、複数のプライベート ネットワークに対するレイヤ 2 外部接続を提供できます。

- スイッチ仮想インターフェイス（SVI）：SVI インターフェイスを使用すると、レイヤ 2 とレイヤ 3 をサポートする同じ物理インターフェイスをレイヤ 2 外部接続とレイヤ 3 外部接続に使用できます。

図 *29 : ACI* レイヤ *3* 管理対象オブジェクト



L3Outside 接続に使用される管理対象オブジェクトは、次のとおりです。

- 外部レイヤ 3 Outside（L3ext）：ルーティング プロトコル オプション（OSPF エリア タイプ、エリア、EIGRP 自律システム、BGP）、プライベート ネットワーク、外部物理ドメイン。
- 論理ノード プロファイル：外部レイヤ 3 Outside 接続に対して 1 つ以上のノードが定義されたプロファイル。ルータ ID とループバック インターフェイスの設定はプロファイルで定義されます。

（注） 複数の外部レイヤ 3 Outside 接続間の同じノードには同じルータ ID を使用してください。

（注） 単一の L3Out 内では、ノードは、1 つの論理ノード プロファイルの一部でのみあり得ます。単一の L3Out 内に複数の論理ノード プロファイルの一部であるノードを構成すると、1 つの論理ノード プロファイルからループバック アドレスがプッシュされるものの、他方からはそうならないなど、予測できない動作が生じる可能性があります。既存の論理インターフェイス プロファイルの下の追加パスのバインディングを使用します。または、既存の論理ノードのプロファイルの下に新しい論理インターフェイス プロファイルを作成してください。

- 論理インターフェイス プロファイル：IPv4 および IPv6 インターフェイスの IP インターフェイス設定。これは、ルート インターフェイス、ルーテッド サブインターフェイス、および SVI でサポートされます。SVI は、物理ポート、ポート チャネルまたは vPC で設定できます。
- OSPF インターフェイス ポリシー：OSPF のネットワーク タイプ、優先順位などの詳細が含まれています。
- EIGRP インターフェイス ポリシー：タイマー、スプリット ホライズン タイマーなどの詳細が含まれています。
- BGP ピア接続プロファイル：ほとんどの BGP ピア設定、リモート AS、ローカル AS、および BGP ピア接続オプションが設定されるプロファイル。BGP ピア接続プロファイルは、ノード プロファイルの下の論理インターフェイス プロファイルまたはループバック インターフェイスに関連付けることができます。これは、BGP ピアリング セッションの update-source 設定を決定します。
- 外部レイヤ 3 Outside EPG（l3extInstP）：外部 EPG はプレフィックス ベースの EPG または InstP とも呼ばれます。インポートおよびエクスポートのルート制御ポリシー、セキュリティ インポート ポリシー、およびコントラクトの関連付けは、このプロファイルで定義されます。単一 L3Out の下に複数の外部 EPG を設定できます。単一外部レイヤ 3 Outside 接続で別のルートまたはセキュリティ ポリシーが定義されている場合、複数の外部 EPG を使用できます。1 つの外部 EPG または複数の外部 EGP がルート マップにまとめられます。外部 EPG で定義されるインポート/エクスポート サブネットは、ルート マップの IP プレフィックス リストの match 句と関連しています。外部 EPG は、インポート セキュリティ サブネットとコントラクトが関連付けられる場所でもあります。これは、この L3out のトラフィックの許可またはドロップに使用されます。
- アクション ルール プロファイル：アクション ルール プロファイルは、L3Out のルート マップの set 句を定義するために使用されます。サポートされる set 句は、BGP communities（standard および extended）、Tags、Preference、Metric、および Metric type です。
- ルート制御プロファイル：ルート制御プロファイルは、アクション ルール プロファイルを参照するために使用されます。これは、アクション ルール プロファイルの順序付きプロファイルにすることができます。ルート制御プロファイルは、テナント BD、BD サブネット、外部 EPG、または外部 EPG サブネットで参照できます。

BGP、OSPF、およびEIGRP L3Out用の追加のプロトコル設定が存在します。これらの設定は、GUI の [ACI Protocol Policies] セクションでテナントごとに設定されます。

（注） 外部 EPG (中継ルーティング ケース) の間でポリシーの適用を設定する際には、エクスポートルート制御、集約エクスポート、および外部のセキュリティのために、デフォルトプレフィックスである 0/0 で 2 番目の外部 EPG (InstP) を設定する必要があります。さらに、優先グループを除外し、中継 InstPs 間では任意の契約 (または適切な契約) を使用する必要があります。

レイヤ 3 外部接続の設定のモードについて

APIC は設定のための複数のユーザ インターフェイス (UI) をサポートしているので、1 つの UI を使用して設定を作成し、その後、別の UI を使用して設定を変更する場合は、予期しないインタラクションが潜んでいます。ここでは、さらに他の APIC のユーザ インターフェイスを使用した可能性がある場合、APIC NX-OS スタイルの CLI を使用してレイヤ 3 外部接続を設定するための考慮事項を説明します。

APIC NX-OS スタイルの CLI を使用してレイヤ 3 外部接続を設定する場合、次の 2 つのモードを選択することができます。

- よりシンプルな暗黙 モードは、APIC GUI または REST API と互換性がありません。
- 名前付き（または明示) モードは、APIC GUI および REST API と互換性があります。

いずれの場合も、設定は互換性がない UI では読み取り専用であると考えてください。

モードの違いについて

どちらのモードでも、構成設定は API の **l3extOut** クラスのインスタンスである内部コンテナ オブジェクト「L3 Outside」（または「L3Out」）内で定義されます。2 つのモード間の主な違いは、このコンテナ オブジェクト インスタンスの命名にあります。

- 暗黙モード：コンテナのネーミングは潜在的であり、CLI コマンドには表示されません。CLI は、これらのオブジェクトを内部的に作成し保持します。
- 名前付きモード：名前はユーザーが決定します。名前付きモードの CLI コマンドには、追加の **l3Out** フィールドがあります。名前付き L3Out がを正常に設定され障害を回避するためには、ユーザーが外部レイヤ 3 用の API オブジェクト モデルを理解する必要があります。

（注） 「名前付きモードセクションを使用したレイヤ*3*外部接続の設定」セクションの手順を除き、このガイドでは、暗黙モードの手順を説明します。

注意事項および制約事項

- 同じ APIC インターフェイスでは、両方のモードを、次の制限でレイヤ 3 外部接続を設定するために一緒に使用することができます。テナント VRF、およびリーフの特定の組み合わせのレイヤ 3 外部接続設定は、1 つのモードを介してのみ実行できます。
- 特定のテナント VRF の場合、外部 L3 EPG を配置できるポリシー ドメインは、名前付きモードまたは暗黙モードのいずれかになります。推奨する設定方式は、特定のテナント VRF が、レイヤ 3 外部接続用に展開されたすべてのノード全体で、特定のテナント VRF の組み合わせに対して 1 つのモードだけを使用することです。モードは、異なるテナントまたは異なる VRF 全体で変えることができ、制限は適用されません。
- 場合によっては、Cisco APIC クラスタへの着信設定で不整合が検証されます。外部から確認できる設定（L3Out を通過するノースバウンド トラフィック）も検証の対象です。設定が無効な場合は、「Invalid Configuration」エラー メッセージが表示されます。
- 外部レイヤ 3 機能は、次の例外を除いて、両方の設定モードでサポートされます
  - L4 ～ L7 サービス アプライアンスを使用したルーティング ピアリングとルート ヘルス インジェクション (RHI) は、名前付きモードでのみをサポートされます。名前付きモードは、ルーティング ピアリングが含まれるテナント VRF のすべての境界リーフ スイッチ全体で使用する必要があります。
- 暗黙モード CLI 手順を使用して作成されたレイヤ 3 外部ネットワーク オブジェクト（l3extOut）は、「__ui_」で始まる名前で識別され、GUI で読み取り専用としてマークされます。CLI は、インターフェイス、プロトコル、ルートマップ、EPG などの機能で、これらの外部 L3 ネットワークを分割します。REST API を介して実行される設定変更は、この構造を破棄することができ、CLI を介してさらなる変更を防ぐことができます。

このようなオブジェクトを削除する手順については、『*APIC Troubleshooting Guide*』の「*Troubleshooting Unwanted _ui_ Objects*」を参照してください。

L3Out ネットワーク インスタンス プロファイルで設定されているサブネットで有効な制御

L3Out ネットワーク インスタンス プロファイルで設定されているサブネットに対して以下の制御を有効にすることができます。

表 *10 :* ルート制御オプション

ルート制御設定	用途	オプション（Options）
エクスポート ルート制御	ルートマップとIPプレフィクスリストを使用して、どの外部ネットワークがファブリックからアドバタイズされるかを制御します。IP プレフィックスリストは、定義されているサブネットごとにBLスイッチに作成されます。エクスポート制御ポリシーは、デフォルトで有効になっており、BGP、EIGRP、および OSPF でサポートされています。	特定の一致(プレフィックスとプレフィックス長)。
インポート ルート制御	ファブリックに許可されているサブネットを制御します。ルールを設定してルートをフィルタリングすることができます。BGP および OSPF ではサポートされますが、EIGRP ではサポートされません。サポートされていないプロトコルのインポート制御ポリシーを有効にすると、自動的に無視されます。インポート制御ポリシーは、デフォルトでは有効になっていませんが、[**L3Out の作成（Create L3Out**）]パネルで有効にすることができます。**[Identity]** タブで、**[Route Control Enforcement: Import]** を有効にします。	特定の一致(プレフィックスとプレフィックス長)。
セキュリティ インポート サブネット	2 つのプレフィックス ベースの EPG 間をパケットが流れるようにするために使用されます。ACL で実装されます。	ACL のプレフィックスまたはワイルドカードによる一致ルールを使用します。

ルート制御設定	用途	オプション（Options）
集約エクスポート	すべてのプレフィックスを外部ピアにアドバタイズできるようにするために使用されます。0.0.0.0/ le 32 IP プレフィックス リストで実装されます。	0.0.0.0/0 サブネット (すべてのプレフィックス) の場合にのみサポートされます。
集約インポート	外部 BGP ピアからの着信であるすべてのプレフィックスを許可するために使用されます。0.0.0.0/0 le 32 IP プレフィックス リストで実装されます。	0.0.0.0/0 サブネット (すべてのプレフィックス) の場合にのみサポートされます。

L3Out接続からすべての中継ルートをアドバタイズすることをお勧めします。この場合、プレフィックス0.0.0.0/0の集約エクスポートオプションを使用します。この集約エクスポートオプションを使用すると、APIC システムがエクスポート ルート マップのマッチ句として使用する IP プレフィクス リスト エントリ (permit 0.0.0.0/0 le 32) が作成されます。出力を表示するには、**show route-map <outbound route-map>** および **show ip prefix-list <match-clause>** コマンドを使用します。

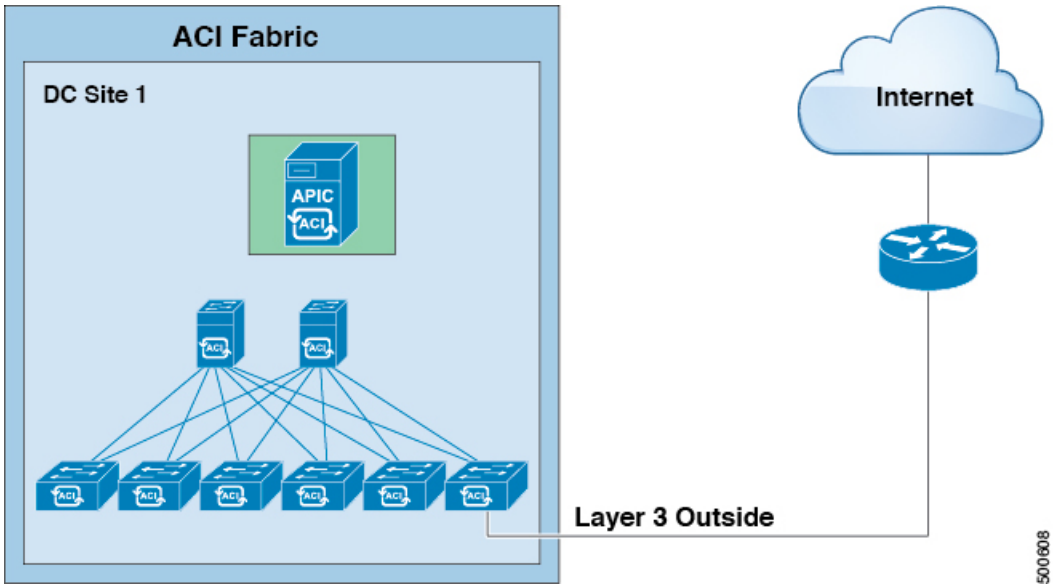
集約共有ルートを有効にすると、ある VRF で学習されたルートを別の VRF にアドバタイズする必要がある場合、サブネットを正確に一致させることでルートを共有するか、集約サブネットマスクを使用してルートを共有できます。複数のサブネットマスクを使用して、特定のルート グループを VRF 間で共有するかどうかを判断できます。たとえば、10.1.0.0/16 と 12.1.0.0/16 を指定してこれらのサブネットを集約することができます。あるいは、0/0 を使用すると、複数の VRF のすべてのサブネット ルートを共有できます。

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

ACI レイヤ 3 Outside ネットワークのワークフロー

このワークフローでは、レイヤ 3 Outside (L3Out) ネットワーク接続を設定するために必要なステップの概要を示します。

図 *30 :* レイヤ *3 Outside* ネットワーク接続



1. 前提条件

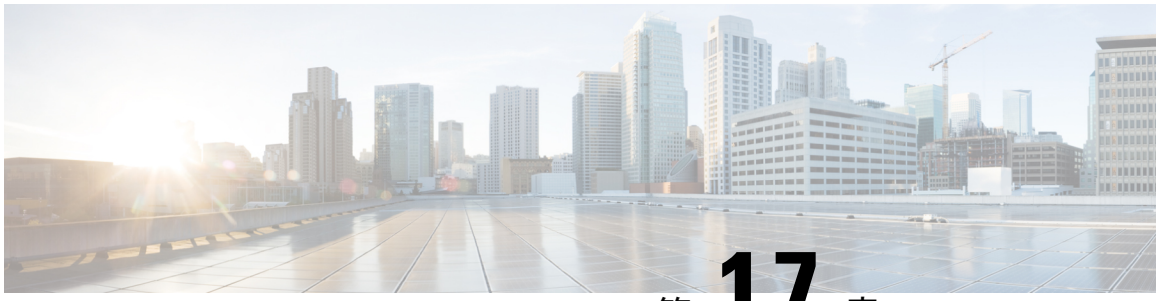
- インフラ セキュリティ ドメインに読み取り/書き込みアクセス権限があることを確認します。
- 必要なインターフェイスを持つターゲット リーフ スイッチが使用できることを確認します。

レイヤ 3 Outside ネットワークの設定

次の L3Outl シナリオのいずれかを選択します。

- 単一のテナント内で消費される L3Out について、BGP または OSPF の設定の指示に従います。
- 複数のテナント間で消費 (共有) される L3Out について、「共有レイヤ 3 Out」のガイドラインに従います。
- L3Out の中継ルーティング使用例については、ACI 中継ルーティング手順に従ってください。

  注：この機能には APIC リリース 1.2（1x）以降が必要です。



第 17 章

外部ネットワークへのルーテッド接続

この章は、次の内容で構成されています。

外部ネットワークへルートされた接続について

ネットワーク構成 (L3Out) 外部レイヤ 3 では、ファブリック以外のトラフィックを転送する方法を定義します。レイヤ3はし、他のノードのアドレスを見つける、ルートを選択して、サービスの品質を選択して、入力して、終了、およびファブリックを移動する際は、トラフィックを転送に使用されます。

（注） ガイドラインとの設定と接続の外部レイヤ3を維持するための注意事項は、次を参照してください。 レイヤ 3 ネットワーキングの注意事項 （278 ページ） 。

L3Outs の種類についての詳細は、外部レイヤ 3 Outside 接続タイプ （257 ページ） を参照してください。

MP-BGP ルート リフレクタ

GUI を使用した MP-BGP ルート リフレクタの設定

手順

ステップ 1 メニュー バーで、**[System]** > **[System Settings]** の順に選択します。

ステップ 2 [ナビゲーション（**Navigation**）] ペインで、[**BGP ルート リフレクタ（BGP Route Reflector**）] を右クリックして、[**ルート リフレクタ ノードの作成（Create Route Reflector Node**）] をクリックします。

ステップ 3 **[ルート リフレクタ ノードの作成（Create Route Reflector Node**）] ダイアログ ボックスで、[**スパイン ノード（Spine Node**）] ドロップダウン リストから、適切なスパイン ノードを選択します。**Submit** をクリックします。

（注） 必要に応じてスパイン ノードを追加するには、上記の手順を繰り返してください。

スパイン スイッチがルート リフレクタ ノードとしてマークされます。

ステップ 4 **BGP Route Reflector** プロパティ エリアの **Autonomous System Number** フィールドで、適切な番号を選択します。**Submit** をクリックします。

（注） 自律システム番号は、Border Gateway Protocol（BGP）がルータに設定されている場合は、リーフが接続されたルータ設定に一致する必要があります。スタティックまたは Open Shortest Path First（OSPF）を使用して学習されたルートを使用している場合は、自律システム番号値を任意の有効な値にできます。

ステップ 5 メニュー バーで、**[ファブリック（Fabric）]** > **[ファブリック ポリシー（Fabric Policies）]** > **[ポッド（Pods）]** > **[ポリシー グループ（Policy Groups）]** をクリックします。

ステップ 6 **[ナビゲーション（Navigation**）] ペインで、[**ポリシー グループ（Policy Groups**）] を展開して右クリックし、[**POD ポリシー グループの作成（Create POD Policy Group**）] をクリックします。

ステップ 7 **[ポッド ポリシー グループの作成（Create Pod Policy Group**）] ダイアログ ボックスで、[**名前（Name**）] フィールドに、ポッド ポリシー グループの名前を入力します。

ステップ 8 [BGP Route Reflector Policy] ドロップダウン リストで、適切なポリシー（デフォルト）を選択します。[Submit] をクリックします。`
BGP ルート リフレクタのポリシーは、ルート リフレクタのポッド ポリシー グループに関連付けられ、BGP プロセスはリーフ スイッチでイネーブルになります。

ステップ 9 メニュー バーで、**[ファブリック（Fabric）]** > **[ファブリック ポリシー（Fabric Policies）]** > **[プロファイル（Profiles）]** > **[ポッド プロファイル デフォルト（Pod Profile default）]** > **[デフォルト（default）]** を選択します。

ステップ 10 [Work] ペインで、[Fabric Policy Group] ドロップダウン リストから、前に作成されたポッド ポリシーを選択します。[Submit] をクリックします。`
ポッド ポリシー グループが、ファブリック ポリシー グループに適用されました。

MP-BGP ルート リフレクタ設定の確認

手順

ステップ 1 次の操作を実行して、設定を確認します。

a) セキュア シェル（SSH）を使用して、必要に応じて各リーフ スイッチへの管理者としてログインします。

b) show processes | grep bgp コマンドを入力して、状態が S であることを確認します。

状態が NR（実行していない）である場合は、設定が正常に行われませんでした。

ステップ 2 次の操作を実行して、自律システム番号がスパイン スイッチで設定されていることを確認します。

a) SSH を使用して、必要に応じて各スパイン スイッチへの管理者としてログインします。

b) シェル ウィンドウから次のコマンドを実行します。

例：

cd /mit/sys/bgp/inst

例：

grep asn summary

設定した自律システム番号が表示される必要があります。自律システム番号の値が 0 と表示される場合は、設定が正常に行われませんでした。

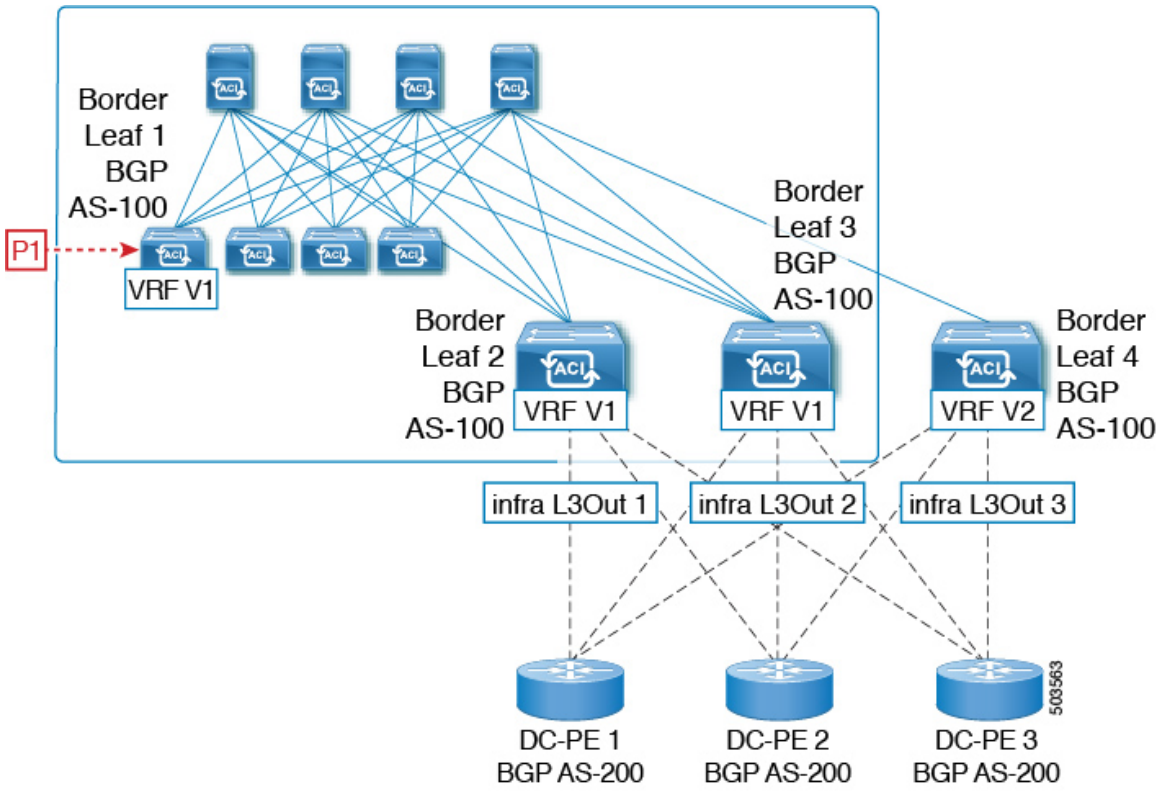
ループ防止のための BGP ドメインパス機能について

BGP ルーティング ループは、次のようなさまざまな条件が原因で発生することがあります。

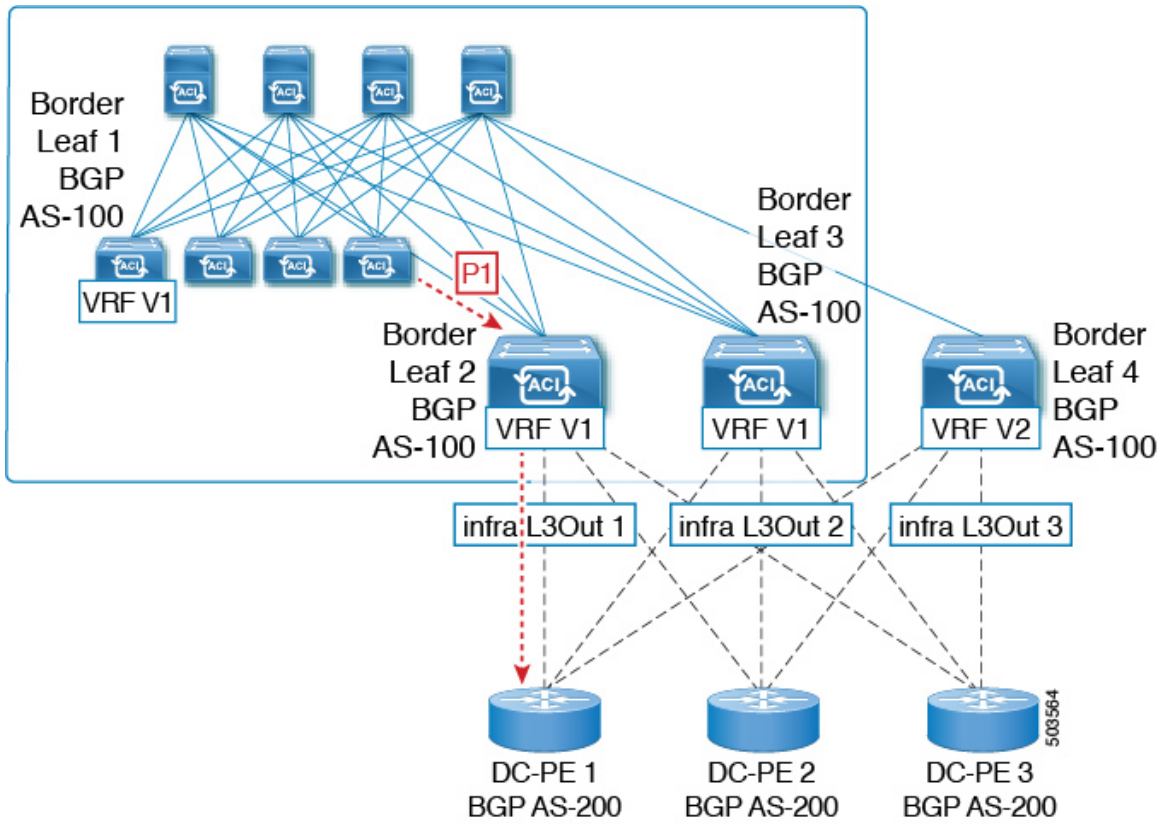
- AS パス チェックなどの既存の BGP ループ防止メカニズムの意図的な無効化
- 異なる VRF または VPN 間のルート リーク

次に、BGP ルーティング ループが発生するシナリオの例を示します。

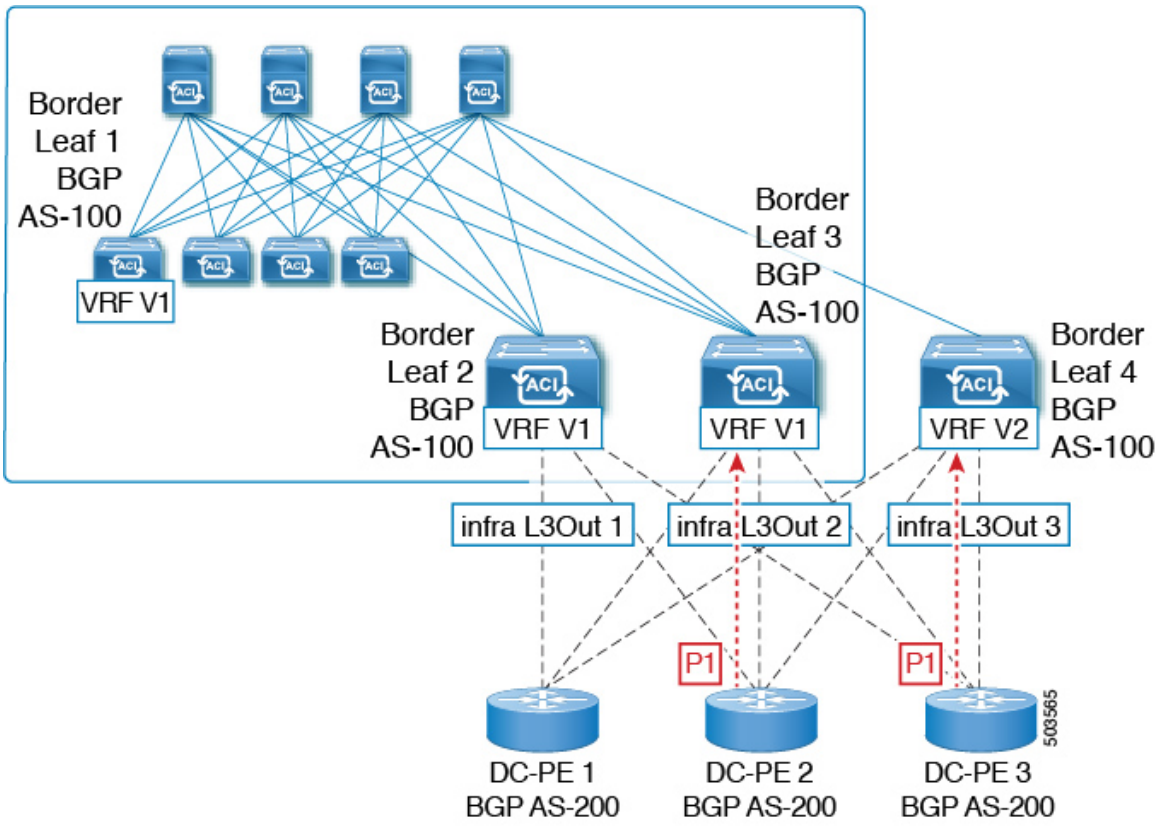
1. BGP IP L3Out ピアから受信したプレフィックス P1 は、Multiprotocol Border Gateway Protocol（MP-BGP）を使用して ACI ファブリックでアドバタイズされます。



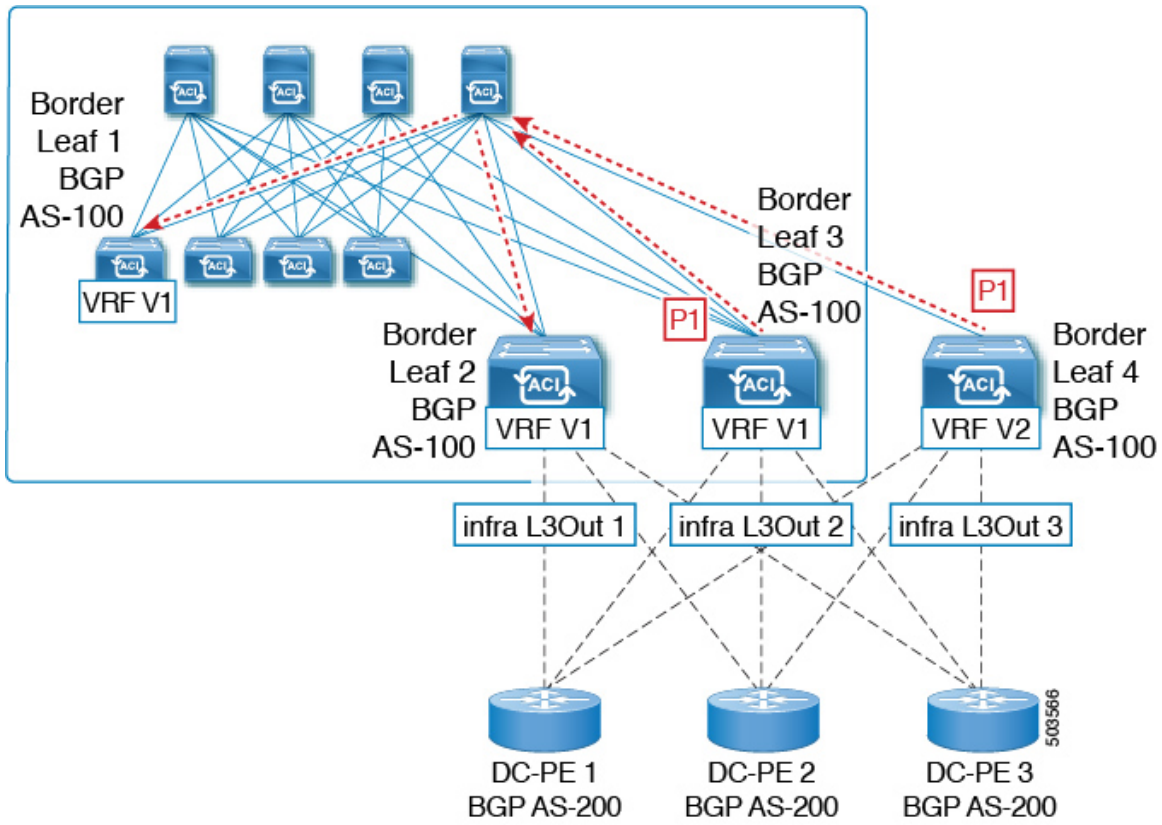
2. 中継のケースとして、このプレフィックスは SR-MPLS インフラ L3Out を介して外部にアドバタイズできます。



3. このプレフィックスは、同じ VRF または異なる VRF のいずれかで、コアから ACI ファブリックにインポートできます。



4. BGP ルーティング ループは、同じ VRF から、または別の VRF からのリークによって、このインポートされたプレフィックスが発信元スイッチにアドバタイズされるときに発生します。



リリース 5.1(3) 以降では、新しい BGP ドメイン パス機能を使用できます。これは、次の方法で BGP ルーティング ループを支援します。

- 同じ VPN または拡張 VRF 内、および異なる VPN または VRF 内のルートが通過する個別のルーティング ドメインを追跡します。
- ルートがすでに通過したドメイン内の VRF にループバックするタイミングを検出します（通常、ドメイン間のスティッチング ポイントである境界リーフ スイッチだけでなく、場合によっては内部スイッチでも）。
- ループにつながる場合に、ルートがインポートまたは受け入れられないようにします。

ACI ファブリック内では、VRF スコープはグローバルであり、設定されているすべてのスイッチに拡張されます。したがって、VRF のドメインからエクスポートされたルートは、他のスイッチの VRF に受信されないようにします。

次のコンポーネントは、ループ防止のためにBGPドメインパス機能で使用されます。

- **Routing domain ID**：ACI サイトのすべてのテナント VRF は、1 つの内部ファブリック ドメイン、各 SR-MPLS インフラ L3Out の各 VRF に 1 つのドメイン、および各 IP L3Out に 1 つのドメインに関連付けられます。BGP ドメインパス機能が有効になっている場合、これらの各ドメインには、次の形式で一意のルーティング ドメイン ID が割り当てられます。 *Base:<variable>*

- Base は、[BGP ルート リフレクタ ポリシー（BGP Route Reflector Policy）] ページの [ドメイン ID ベース（Domain ID Base）] フィールドに入力されたゼロ以外の値です。
- <variable> は、そのドメイン専用にランダムに生成された値です。

- **ドメイン パス（Domain path）**：ルートが通過するドメイン セグメントは、BGP ドメイン パス属性を使用して追跡されます。
  - ルートを受信する送信元ドメインの VRF のドメイン ID がドメイン パスの先頭に追加されます。
  - 送信元ドメイン ID はドメイン パスの先頭に追加され、境界リーフ スイッチのドメイン間でルートが再生成されます。
  - VRF のローカル ドメイン ID のいずれかがドメイン パスにある場合、外部ルートは受け入れられません。
  - ドメイン パスは、次のように表される各ドメイン セグメントとともに、オプションの遷移 BGP パス属性として伝送されます。<Domain-ID:SAFI>
  - ACI 境界リーフ スイッチは、ドメイン内のリークを追跡するために、ローカルに発信されたルートと外部ルートの両方に VRF 内部ドメイン ID を付加します。
  - 内部ドメインからのルートをインポートし、競合する外部ドメイン ID を持つノードの VRF にインストールして、内部バックアップまたは中継パスを提供できます。
  - インフラ L3Out ピアの場合、ピア ドメインのドメイン ID がルートのドメイン パスに存在する場合、ピアへのルートのアドバタイズメントはスキップされます（アウトバウンド チェックは IP L3Out ピアには適用されません）
  - 境界リーフ スイッチと非境界リーフ スイッチはどちらもドメイン パス属性を処理します。

（注） ループ防止のために BGP ドメイン パス機能を設定するか、GUI または REST API を使用して、受信したドメイン パスを送信するように設定をイネーブルにすることができます。ループ防止のために BGP ドメイン パス機能を設定したり、NX-OS スタイルの CLI を介して受信ドメイン パスを送信するように設定したりすることはできません。

（注） 以前のリリースからリリース 5.1(3) にアップグレードするときに、VRF 間共有サービス用に設定されたコントラクトがある場合、BGP ドメインID にリリース 5.1(3) にアップグレードする前に設定された契約で設定されています。このような状況では、契約を削除してから、契約を追加し直すと、BGP ドメインの更新が可能になります。これは、リリース 5.1(3) へのアップグレード前に設定された契約がある場合にのみ問題になります。これは、リリース 5.1(3) へのアップグレードの完了後に新しい契約を作成する場合は問題になりません。

GUI を使用したループ防止のための BGP ドメイン パス機能の設定

始める前に

ループ防止のための BGP ドメインパス機能について （237 ページ）に記載されている情報を使用して、BGP ドメイン パス機能に精通します。

手順

ステップ 1 ループ防止に BGP ドメイン パス機能を使用する場合は、BGP ルート リフレクタに BGP ドメイン パス属性を設定します。

（注） ループ防止に BGP ドメイン パス機能を使用しないが、受信したドメイン パスを送信する場合は、この手順で BGP ドメイン リフレクタの BGP ドメイン パス機能を有効にしないでください。代わりに、に直接移動して、適切な BGP 接続ウィンドウの [ドメイン パスの送信（Send Domain Path）] フィールドのみを有効にします。ステップ 2 （274 ページ）

a) **[システム（System）] > [システム設定（System Settings）] > [BGP ルート リフレクター（BGP Route Reflector）]** の順に移動します。

[BGP ルート リフレクター（BGP Route Reflector）] ウィンドウが表示されます。このウィンドウで [ポリシー（Policy）] ページ タブが選択されていることを確認します。

b) [ドメイン ID ベース（Domain ID Base）] フィールドを見つけます。

c) [ドメイン ID ベース（Domain ID Base）] フィールドに数値を入力します。

- BGP ドメインパス機能を有効にするには、1 ー 4294967295 の値を入力します。ACI ファブリックがマルチサイト環境の一部である場合は、この [ドメイン ID ベース（Domain ID Base）] フィールドでこの ACI ファブリックに固有の一意の値を使用してください。
- BGP ドメインパス機能を無効にするには、この [ドメイン ID ベース（ID Base）] フィールドに 0 を入力します。

ループ防止の BGP ドメインパス機能が有効になっている場合は、Base:<variable> 形式の暗黙のルーティング ドメイン ID が割り当てられます。

- [ベース（Base）] は、この [ドメイン ID ベース（Domain ID Base）] フィールドに入力したゼロ以外の値です。
- <変数（variable）> は、VRF または L3Out 用にランダムに生成された値で、ループ防止の BGP ドメインパス機能に使用されます。

このルーティング ドメイン ID は、次のドメインを識別するために BGP に渡されます。

- VRF：そのテナントの VRF ウィンドウの [ポリシー（Policy）] タブにある [ルーティング ドメイン ID（Routing Domain ID）] フィールドに示されているように、各 VRF にランダムに生成された値を使用して内部ドメイン ID によって識別されます。
- IP L3Out：IP L3Out の [BGP ピア接続プロファイル（BGP Peer Connectivity Profile）] ウィンドウの [ルーティング ドメイン ID（Routing Domain ID）] フィールドに示されているように、各 IP L3Out に対してランダムに生成された値を使用して、外部ドメイン ID によって識別されます。
- SR-MPLS infra L3Out：各 SR-MPLS VRFL3Out のウィンドウの [SR-MPLS Infra L3Outs] テーブルの [ルーティング ドメイン ID（Routing Domain ID）] 列に示されているように、各 SR-MPLS infra L3Out の各 VRF にランダムに生成された値を使用して、外部ドメイン ID によって識別されます。

Domain-Path 属性は、パス内のルーティングドメイン ID に基づいてループをチェックするために着信方向で処理されます。Domain-Path 属性はピアに送信されます。これは、次の手順で説明するように、IP L3Out または SR-MPLS infraL3OutのBGP ピアレベルの [ドメイン パスの送信（Send Domain Path）] フィールドを使用して個別に制御されます。

ステップ 2 BGP ドメイン パス属性をピアに送信するには、適切な BGP 接続ウィンドウで [ドメイン パスの送信（Send Domain Path）] フィールドを有効にします。

ループ防止のために BGP ドメインパス機能を使用する場合は、最初に [ドメイン ベース ID（Domain Base ID）] を設定してから、ここで [ドメインパスの送信（Send Domain Path）] フィールドを有効にします。ステップ 1 （273 ページ）ループ防止のために BGP ドメインパス機能を使用しない場合でも、受信したドメインパスを送信する場合は、ここで [ドメイン パスの送信（Send Domain Path）] フィールドのみを有効にします（その場合は [ドメインベース ID（Domain Base ID）] を設定しないでください）。ステップ 1 （273 ページ）

- IP L3Out ピアの [ドメイン パスの送信（Send Domain Path）] フィールドを有効にするには、次の手順を実行します。

1. IP L3Out ピアの [BGP ピア接続プロファイル（BGP Peer Connectivity Profile）] ウィンドウに移動します。

   [テナント（Tenant）] > [*tenant_name*] > [ネットワーキング（Networking）] > [L3Outs] > [*L3Out_name*] > [論理ノード プロファイル（Logical Node Profile）] > [*log_node_prof_name*] > [論理インターフェイス プロファイル（Logical Interface Profile）] > [*log_int_prof_name*] > [BGP ピア（BGP Peer） *]<address>-ノード（Node）-[<node_ID>]*

   この設定された L3Out の [BGP ピア接続プロファイル（BGP Peer Connectivity Profile）] ウィンドウが表示されます。

2. [BGP ピア接続プロファイル（BGP Peer Connectivity Profile）] ウィンドウで [BGP 制御（BGP Controls）] 領域を見つけます。
3. [BGP 制御（BGP Controls）] 領域で、[ドメインパスの送信（Send Domain Path）] フィールドの横にあるボックスをクリックします。
4. **[送信（Submit）]** をクリックします。`

このアクションは、BGP ドメイン パス属性をピアに送信します。

- SR-MPLS インフラ L3Out ピアの [ドメイン パスの送信（Send Domain Path）] フィールドを有効にするには、次の手順を実行します。

  1. **[テナント（Tenant）] > [infra] > [ネットワーキング（Networking）] > [SR-MPLS Infra L3Outs] > [*SR-MPLS-infra-L3Out_name*] > [論理ノード プロファイル（Logical Node Profiles）] > [*log_node_prof_name*]**の順に移動します。

     この設定済み SR-MPLS インフラ L3Out の [論理ノードプロファイル（Logical Node Profile）] ウィンドウが表示されます。

  2. [BGP-EVPN 接続プロファイル（BGP-EVPN Connectivity Profile）] 領域を見つけ、新しい BGP-EVPN 接続ポリシーを作成するか、または既存の BGP-EVPN 接続ポリシーの [ドメイン パスの送信（Send Domain Path）] フィールドを有効にするかを決定します。

     - 新しい BGP-EVPN 接続ポリシーを作成する場合は、[BGP-EVPN 接続プロファイル（BGP-EVPN Connectivity Profile）] 領域のテーブルの上にある [+] をクリックします。[BGP-EVPN 接続ポリシーの作成（Create BGP-EVPN Connectivity Policy）] ウィンドウが表示されます。
     - 既存の BGP-EVPN 接続ポリシーの [ドメイン パスの送信（Send Domain Path）] フィールドを有効にする場合は、[BGP-EVPN 接続プロファイル（BGP-EVPN Connectivity Profile）] 領域のテーブルでそのポリシーをダブルクリックします。[BGP-EVPN 接続ポリシー（BGP-EVPN Connectivity Policy）] ウィンドウが表示されます。

  3. ウィンドウで [BGP 制御（BGP Controls）] 領域を見つけます。
  4. [BGP 制御（BGP Controls）] 領域で、[ドメインパスの送信（Send Domain Path）] フィールドの横にあるボックスをクリックします。
  5. **[送信（Submit）]** をクリックします。`

     このアクションは、BGP ドメイン パス属性をピアに送信します。

ステップ 3 適切なエリアに移動して、さまざまなドメインに割り当てられたルーティング ID を確認します。

- VRF ドメインに割り当てられたルーティング ID を確認するには、次の手順を実行します。

  Tenant tenant_name Networking VRFs VRF_name をクリックし、その VRF の [ポリシー（Policy）] タブをクリックして、[VRF] ウィンドウの[ルーティング ドメイン ID（Routing Domain ID）] フィールドのエントリを見つけます。＞＞＞＞

- IP L3Out ドメインに割り当てられたルーティング ID を確認するには、次の手順を実行します。

  [テナント（Tenants）] > [*tenant_name*] > [ネットワーキング（Networking）] > [L3Outs] > [*L3Out_name*] > [論理ノード プロファイル（Logical Node Profiles）] > [*log_node_prof_name*] > [BGP ピア（BGP Peer）]の順に移動し、その後 [BGP ピア接続プロファイル（BGP Peer

Connectivity Profile）] ウィンドウの [**ルーティング ドメイン ID（Routing Domain ID**）] フィールドでエントリを見つけます。

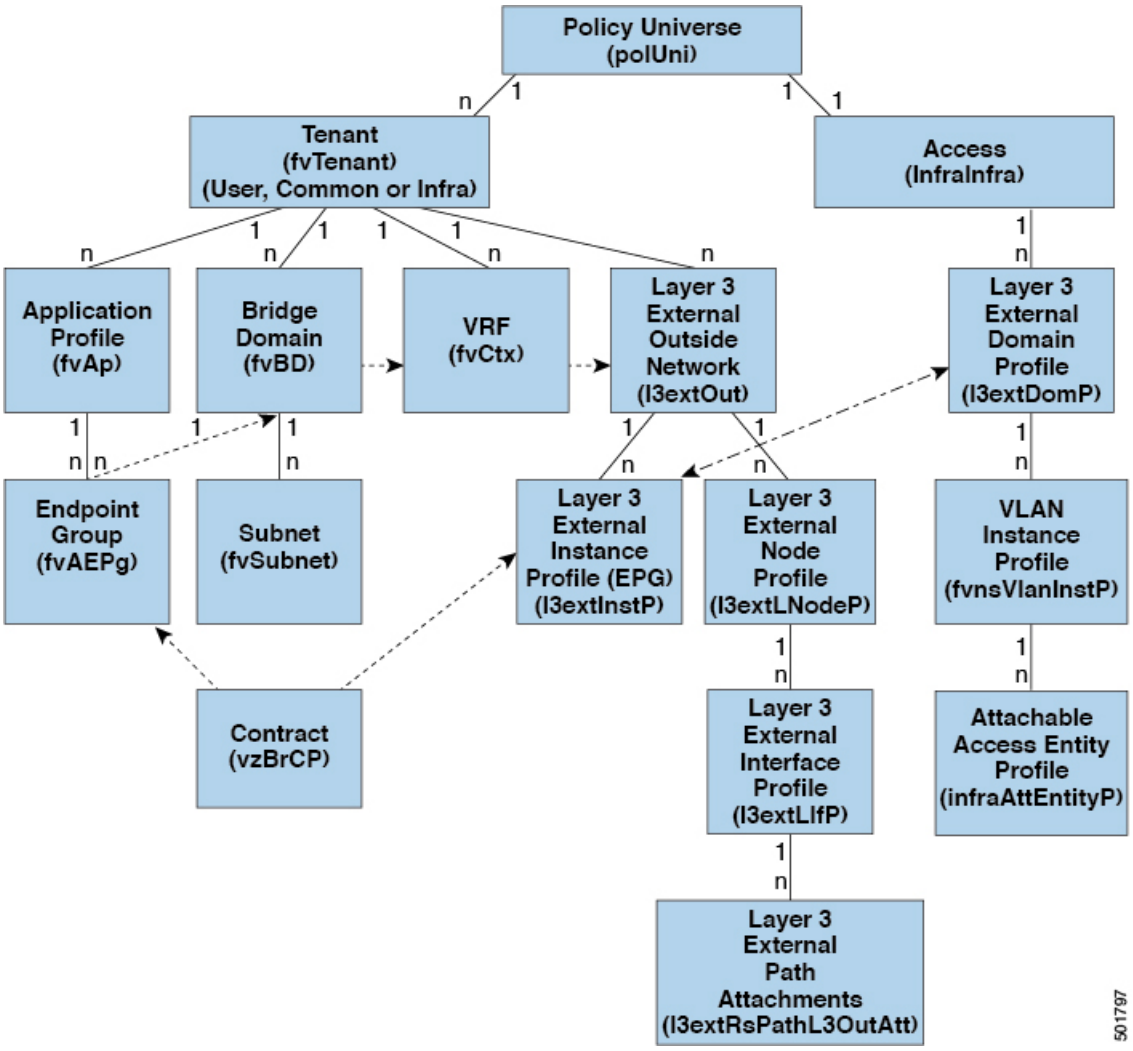
- SR-MPLS インフラ L3Out ドメインに割り当てられたルーティング ID を確認するには、次の場所に移動します。

  [テナント（Tenants）] [tenant_name] [ネットワーキング（Networking）] [SR-MPLS VRF L3Outs] [SR-MPLS_VRF_L3Out_name] をクリックし、[SR-MPLS VRFL3Out] のウィンドウで [SR-MPLS Infra L3Outs] テーブルの [ルーティング ドメイン ID（Routing Domain ID）] カラムのエントリを見つけます。 > > > >

外部ネットワークへのルーテッド接続のためのレイヤ 3 Out

外部ネットワークへのルーテッド接続は、次の図の階層で示すようにファブリック アクセス（`infraInfra`）外部ルーテッド ドメイン（`l3extDomP`）をレイヤ 3 外部外側ネットワーク（`l3extOut`）のテナント レイヤ 3 外部インスタンス プロファイル（`l3extInstP` または外部 EPG）に関連付けることによって有効になります。

図 *31 :* レイヤ *3* 外部接続のポリシー モデル



レイヤ 3 外部アウトサイドネットワーク（`l3extOut` オブジェクト）には、ルーティング プロトコルのオプション（BGP、OSPF、または EIGRP またはサポートされている組み合わせ）およびスイッチとインターフェイス固有の設定が含まれています。`l3extOut` にルーティング プロトコル（たとえば、関連する仮想ルーティングおよび転送（VRF）およびエリア ID を含む OSPF）が含まれる一方で、レイヤ 3 外部インターフェイスのプロファイルには必要な OSPF インターフェイスの詳細が含まれます。いずれも OSPF のイネーブル化に必要です。

`l3extInstP` EPG は、コントラクトを通してテナント EPG に外部ネットワークを公開します。たとえば、Web サーバのグループを含むテナント EPG は、`l3extOut` に含まれるネットワーク設定に応じてコントラクトを介して `l3extInstP` EPG と通信できます。外部ネットワーク設定は、ノードを L3 外部ノード プロファイルに関連付けることで複数のノードに容易に再利用できます。同じプロファイルを使用する複数のノードをフェールオーバーやロードバランシングのために設定できます。ノードを複数の l3extOuts に追加することで、l3extOuts に関連付けられている VRF がノードでも展開されます。拡張性に関する情報については、現行の「*Verified Scalability Guide for Cisco ACI*」を参照してください。

レイヤ 3 ネットワーキングの注意事項

レイヤ 3 外部接続を作成し、維持する際には、次のガイドラインを使用してください。

トピック	注意またはガイドライン
vPC ペアの境界リーフ スイッチが、誤った VNID を持つ BGP パケットをピア上で学習したエンドポイントに転送する問題	設定に次の条件が存在する場合： • 2 つのリーフ スイッチが vPC ペアの一部である • L3Out の背後に接続されている 2 つのリーフ スイッチの場合、宛先エンドポイントは 2 番目（ピア）の境界リーフ スイッチに接続され、エンドポイントはそのリーフ スイッチで学習されたピアです。 ピアが学習したエンドポイント宛ての BGP パケットを受信する入力リーフ スイッチでエンドポイントが学習した場合、L3Out の背後にある最初のレイヤ 3 スイッチ間で中継 BGP 接続が確立できないという問題が発生する可能性があります。および vPC ペアの 2 番目のリーフ スイッチ上のピア上で学習されたエンドポイント。これは、ポート 179 を持つ中継 BGP パケットが VRF VNID ではなくブリッジ ドメイン VNID を使用して誤って転送されるために発生します。 この問題を解決するには、エンドポイントをファブリック内の他の非ピア リーフ スイッチに移動して、リーフ スイッチで学習されないようにします。
境界リーフ スイッチおよび GIR（メンテナンス）モード	境界リーフ スイッチに静的ルートがあり、GIR（Graceful Insertion and Removal）モード、またはメンテナンス モードがある場合、境界リーフ スイッチからのルートは ACI ファブリックにあるルーティング テーブルから削除されない可能性があり、ルーティングの問題が発生します。 この問題を回避するには、次のいずれかを実行します。 • その他の境界リーフ スイッチで同じ管理ディスタンスを持つ同じ静的ルートを設定するか、 • 静的ルートの次のホップへの到達性を追跡するため IP SLA または BFD を使用します
L3Out 集約統計情報は出力ドロップ カウンタをサポートしません	[テナント（Tenants）] [tenant_name] [ネットワーキング（Networking）] [L3Out] [L3Out_name] [統計情報（Stats）] を介して、[統計情報の選択（Select Stats）] ウィンドウにアクセスすると、L3Out 集約統計情報が出力ドロップ カウンタをサポートしていないことがわかります。＞＞＞＞＞これは、EPG VLAN からの出力ドロップを記録する ASIC に現在ハードウェア テーブルがないため、これらのカウンタに統計情報が入力されないためです。EPG VLAN の入力ドロップだけがあります。

トピック	注意またはガイドライン
CLI による更新	API または GUI で作成され CLI を通して更新されたレイヤ 3 外部ネットワークについては、プロトコルは API または GUI を通して外部ネットワークでグローバルに有効にする必要があり、CLI を介してさらに更新を行う前に、すべての参加ノードのノード プロファイルは API または GUI を通して追加される必要があります。
同じノード上のレイヤ 3 ネットワークのループバック	同じノードで 2 つのレイヤ 3 の外部ネットワークを設定するときに、ループバックはレイヤ 3 ネットワークに別々に設定されます。
入力ベース ポリシーの適用	Cisco APIC リリース 1.2(1) 以降、入力ベース ポリシーの適用により、出入力両方向でレイヤ 3 アウトサイド（L3Out）トラフィックにポリシー適用を定義できます。デフォルトでは入力になっています。リリース 1.2(1) 以降にアップグレード中、既存の L3Out 設定が出力に設定され、動作が既存の設定と一致します。特別なアップグレードのシーケンスは必要ありません。アップグレード後、グローバル プロパティ値を入力に変更します。変更されると、システムがルールとプレフィックス エントリを再プログラミングします。規則は出力リーフから削除され、入力リーフ上に既存の規則がない場合は、入力リーフ上にインストールされます。既存の設定がない場合、`Actrl` プレフィックス エントリが入力リーフ上にインストールされます。ダイレクト サーバ リターン（DSR）および属性 EPG には入力ベースのポリシー適用が必要です。vzAny と禁止コントラクトは、入力ベースのポリシー適用を契約無視します。入力には中継規則が適用されます。
L3Outs によるブリッジ ドメイン	テナントのブリッジ ドメインには、共通テナントでプロビジョニングされている `l3extOut` によってアドバタイズされたパブリック サブネットを含めることができます。
OSPF と EIGRP のブリッジ ドメイン ルート アドバタイズメント	OSPF と EIGRP の両方があるノード上の同じ VRF で有効であり、ブリッジ ドメインのサブネットがいずれか 1 つの L3Out からアドバタイズされる場合、他の L3Out で有効になっているプロトコルからも同様にアドバタイズされます。 OSPF と EIGRP では、ブリッジ ドメイン ルート アドバタイズメントは VRF ごとに行われ、L3Out ごとには行われません。同じ VRF とノードで（複数エリアの）複数の OSPF L3Out が有効になっている場合、これと同じ動作が想定されます。この場合、ブリッジ ドメインのルートがいずれかの領域で有効になっていれば、すべての領域からアドバタイズされます。

トピック	注意またはガイドライン
BGP 最大プレフィックス制限	Cisco APICリリース 1.2（1x）以降、BGP `l3extOut` 接続のテナント ポリシーは、最大プレフィックス制限を使用して設定できます。これにより、ピアから受信されるルートプレフィックスの数をモニタし、制限することができます。最大プレフィックス制限を超えると、ログエントリが記録され、さらにプレフィックスが拒否されます。カウントが一定の間隔でしきい値を下回る場合、接続を再起動することができますが、そうしない場合接続がシャットダウンします。一度に1つのオプションだけを使用できます。デフォルト設定では20,000プレフィックスに制限され、その後は新しいプレフィックスは拒否されます。拒否オプションが導入されると、APICでエラーが発生する前に BGP は設定されている制限よりも 1 つ多くプレフィックスを受け入れます。

MTU	• Cisco ACI は IP フラグメンテーションをサポートしていません。したがって、外部ルータへのレイヤ 3 Outside（L3Out）接続、または Inter-Pod Network（IPN）を介した マルチポッド 接続を設定する場合は、インターフェイス MTU がリンクの両端で適切に設定されていることが推奨されます。Cisco ACI、 Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定可能な MTU 値はイーサネット ヘッダー (一致する IP MTU、14-18 イーサネット ヘッダー サイズを除く) を考慮していません。また、IOS XR などの他のプラットフォームには、設定された MTU 値にイーサネット ヘッダーが含まれています。設定された値が 9000 の場合、Cisco ACI、Cisco NX-OS Cisco IOS の最大 IP パケット サイズは 9000 バイトになりますが、IOS-XR のタグなしインターフェイスの最大 IP パケットサイズは 8986 バイトになります。
	• 物理インターフェイスの MTU 設定は次のように異なります。Cisco ACI
	  • サブインターフェイスの場合、物理インターフェイスの MTU は固定され、リーフ スイッチの前面パネルポートでは 9216 に設定されます。
	  • SVI の場合、物理インターフェイス MTU はファブリック MTU ポリシーに基づいて設定されます。たとえば、ファブリック MTU ポリシーが 9000 に設定されている場合、SVI の物理インターフェイスは 9000 に設定されます。

トピック	注意またはガイドライン
L3Outs の QoS	L3Out 用の QoS ポリシーを設定し、L3Out が存在する BL スイッチで適用されるポリシーを有効にするには、次の注意事項に従ってください。 • VRF ポリシー制御の適用方向を **出力** に設定する必要があります。 • VRF ポリシー制御適用の優先度設定を **有効** に設定する必要があります。 • L3Out を使用して EPG 間の通信を制御するコントラクトを設定する際に、コントラクトまたはコントラクトの件名に QoS クラスまたはターゲット DSCP を含めます。
ICMP 設定	ICMP リダイレクトおよび ICMP 到達不能は、スイッチ CPU がこれらのパケットを生成しないように、デフォルトで無効になっています。Cisco ACI

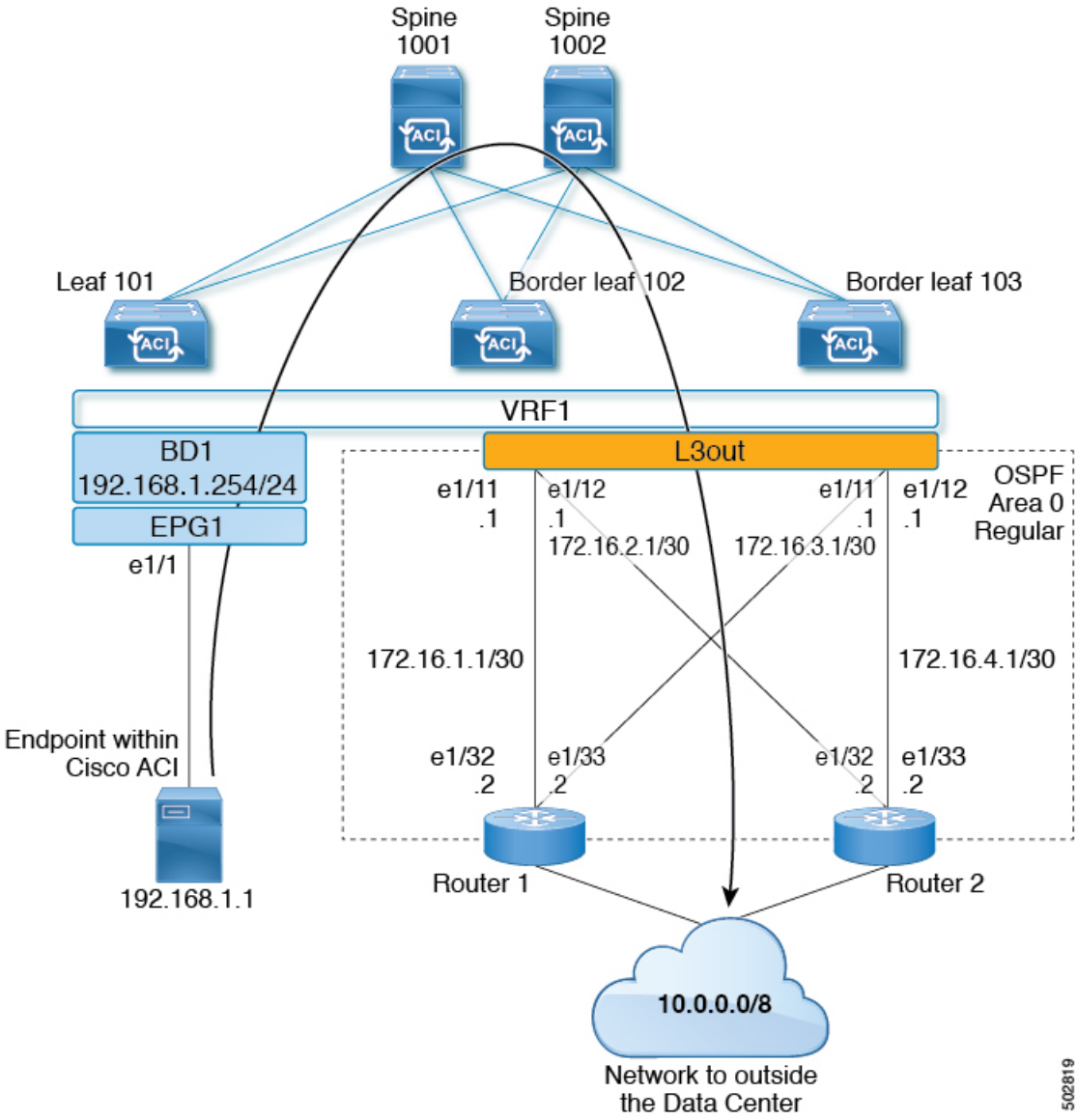
L3Out の設定例

[L3Outの作成（Create L3Out）] ウィザードを使用して L3Out を設定する場合は、さまざまなオプションを使用できます。次に、2 つの外部ルータで OSPF L3Out を設定する L3Out 設定の例を示します。これは、一般的な設定プロセスを理解するのに役立ちます。

（注） この例では、Cisco APIC リリース 4.2(x) および関連する GUI 画面を使用します。

トポロジの例

図 *32 : 2* つの外部ルータがある *OSPF L3Out* のトポロジ例

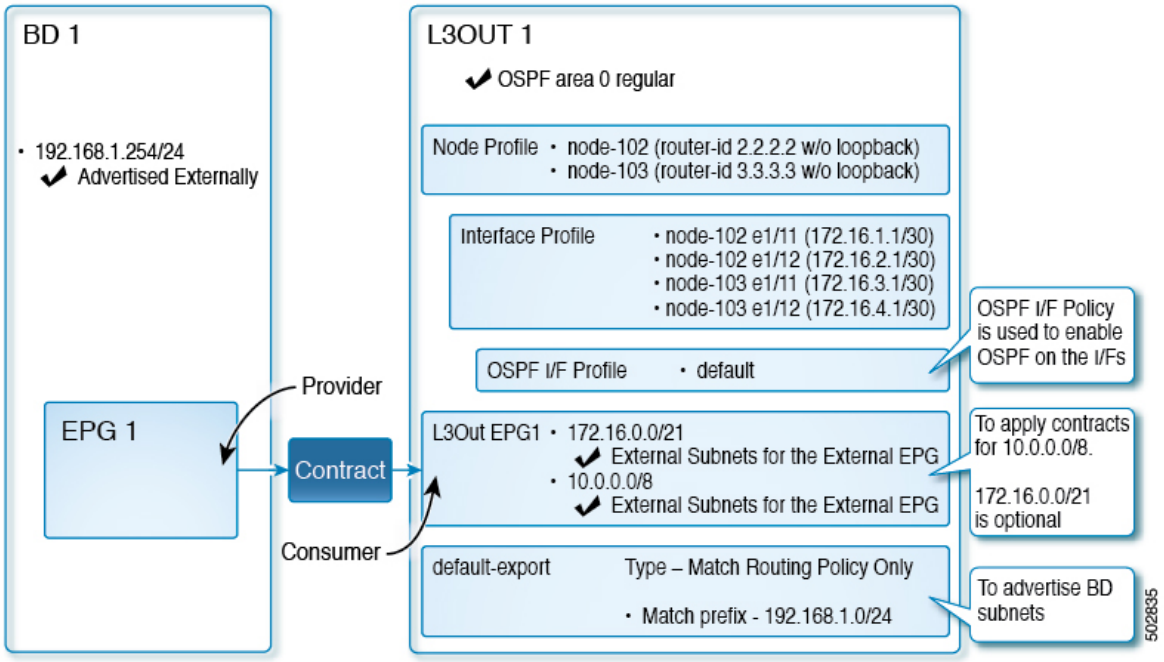


この基本的な L3Out の例は、次の方法を示しています。

- 次の仕様で L3Out を設定します。
  - エリア 0 の OSPF
  - 2 台の外部ルータを使用
  - ルーテッド インターフェイス
  - 2 つの境界リーフ スイッチ

- デフォルト ルートマップ（default-export）を使用して BD サブネットをアドバタイズします。
- EPG1 と外部ルート（10.0.0.0/8）間のコントラクトとの通信を許可する

図 *33 : OSPF* 構成図

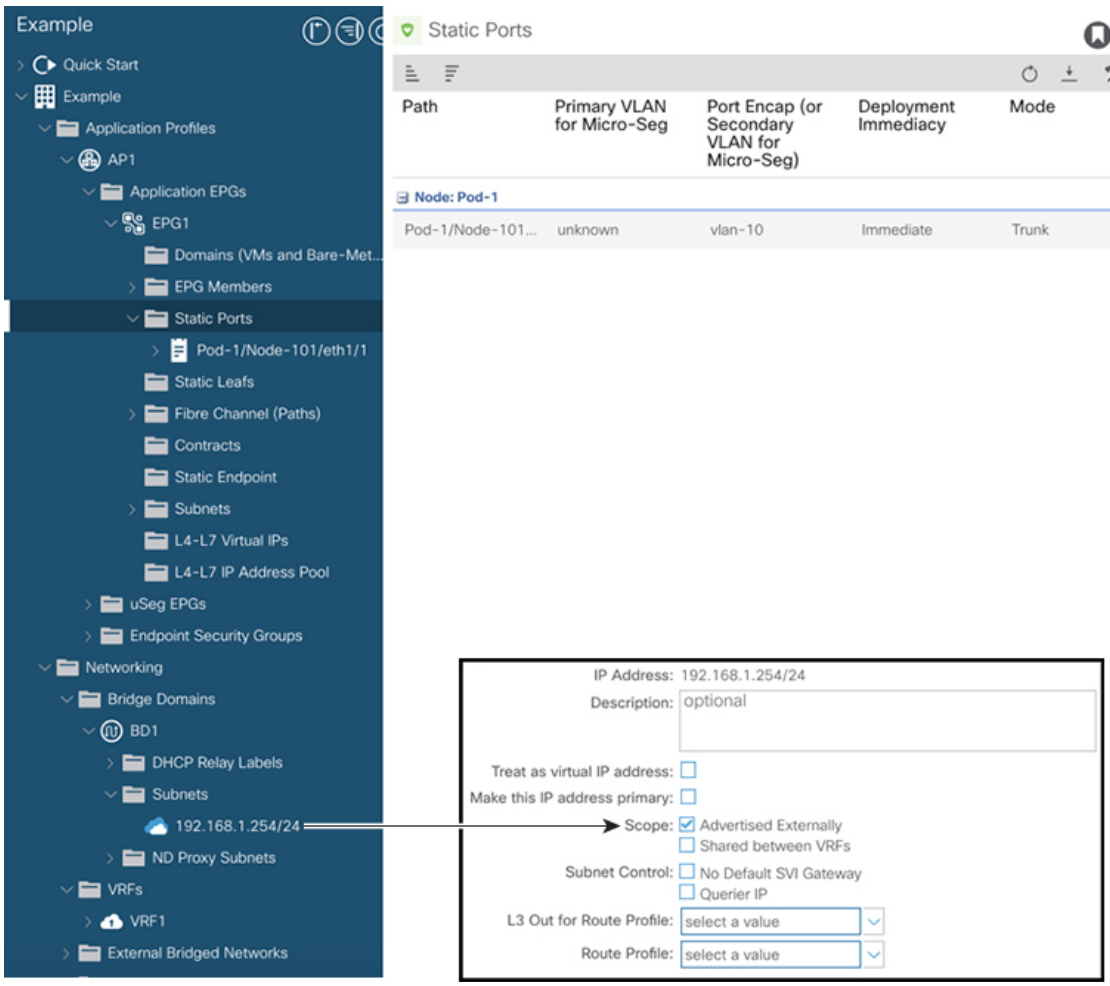


上記の図は、のトポロジ例の設定を示しています。図 32 : 2 つの外部ルータがある OSPF L3Out のトポロジ例 （282 ページ） この例の設定フローは次のとおりです。

1. L3Out：これにより、
   - L3Out 自体（OSPF パラメータ）
   - ノード、インターフェイス、OSPF I/ F プロファイル
   - **外部 EPG の範囲の外部サブネット**を持つ L3Out EPG
2. BD サブネットのアドバタイズ：
   - **default-export** route-map
   - **Advertise Externally**スコープを持つ BD サブネット
3. EPG - L3Out コミュニケーションを許可（Allow EPG-L3Out communication）：これは、EPG1 と L3Out EPG1 間のコントラクトを使用します。

前提条件

図 *34* : 前提条件として作成されたオブジェクトの画面例



- この設定例では、L3Out 設定部分のみに焦点を当てています。VRF、BD、EPG、アプリケーション プロファイル、アクセス ポリシー（レイヤ 3 ドメインなど）などの他の設定は対象外です。上記のスクリーンショットは、次のような前提条件のテナント設定を示しています。
  - VRF1
  - サブネット192.168.1.254/24 の BD1
  - エンドポイントへのスタティック ポートを持つ EPG1

Create L3Out Wizard を使用した L3Out の作成例

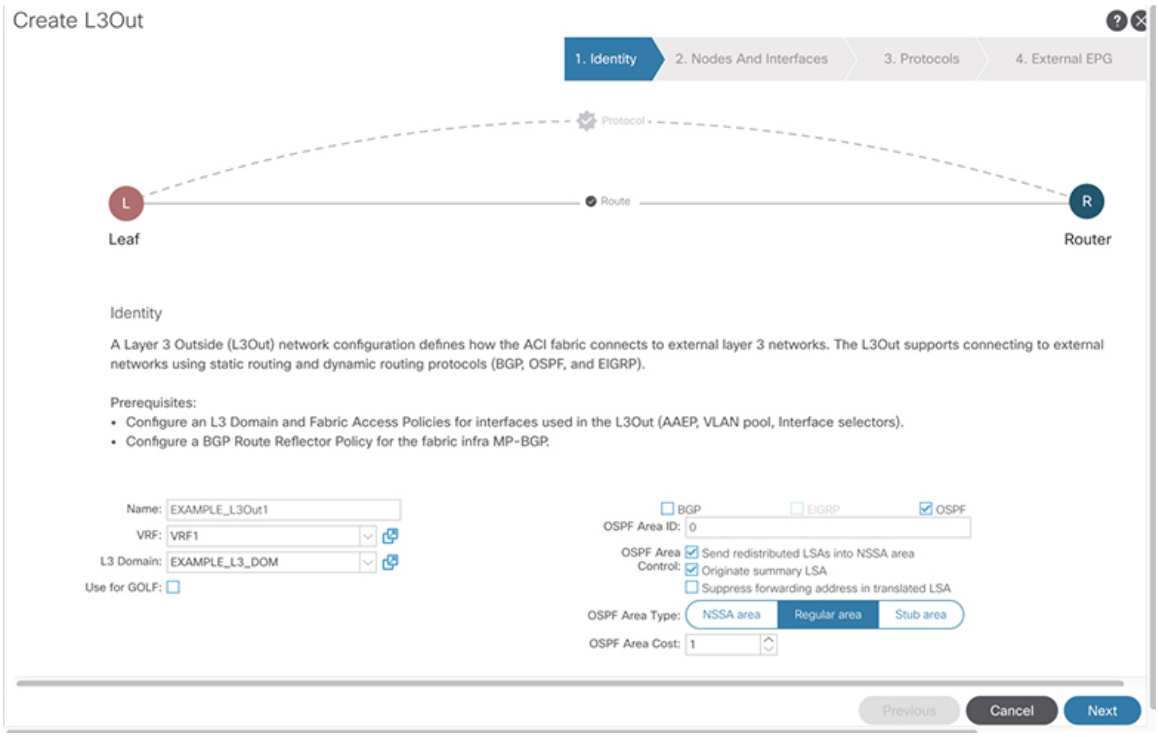
このタスクでは、「トポロジの例」で説明する OSPF L3Out を作成します。このタスクに続いて、に示すように、2 つの境界リーフ スイッチと 2 つの外部ルータとの OSPF ネイバーシップを設定します。Cisco ACI図 32 : 2 つの外部ルータがある OSPF L3Out のトポロジ例 （282 ページ）

手順

ステップ 1 GUI の [ナビゲーション（Navigation）] ペインの、[テナント例（Tenant Example）] で [ネットワーキング（Networking）] [L3Out] の順に移動します。 >

ステップ 2 [L3Out の作成（Create L3Out）] を右クリックして選択します。

ステップ 3 [L3Out の作成（Create L3Out）] スクリーンで、[識別（Identity）] タブを選択して次のアクションを実行します。



a) [名前（Name）] フィールドで、L3Out の名前を入力します。（EXAMPLE_L3Out1）

b) [VRF] フィールドおよび [L3 ドメイン（L3 Domain）] フィールドで、適切な値を選択します。(VRF1, EXAMPLE_L3DOM)

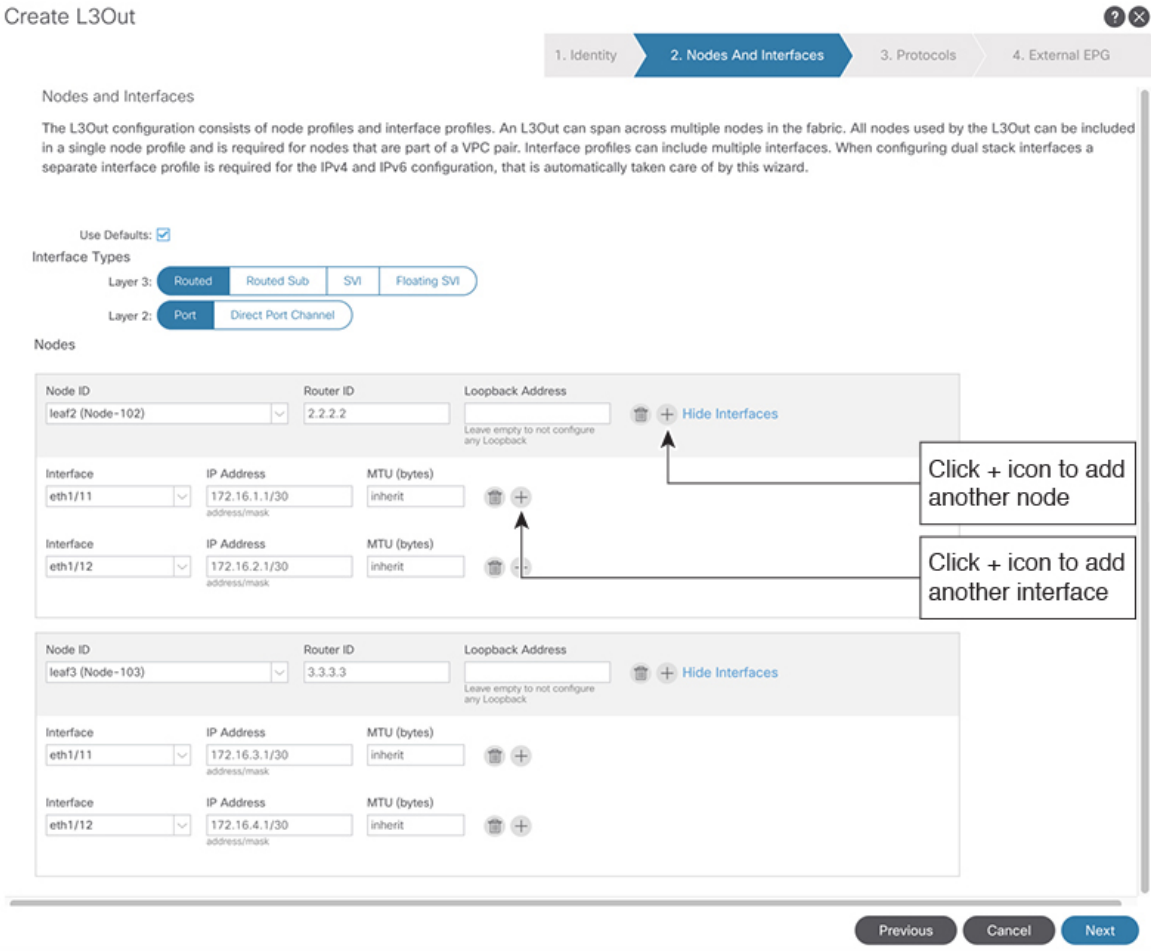
c) [OSPF] フィールドで、チェック ボックスをオンにします。

d) [OSPF 領域 ID（OSPF Area ID）] フィールドで、値 0 またはテキスト [バックボーン（backbone）] を選択します。

e) [OSPF 領域タイプ（OSPF Area Type）] フィールドで、[レギュラー領域（Regular area）] を選択します。

f) 残りのフィールドはデフォルト値のままにします。

ステップ 4 [次へ（Next）] をクリックして [ノードとインターフェイス（Nodes and Interfaces）] 画面を表示し、次の操作を実行します。



a) [インターフェイス タイプ（Interface Types）] 領域の [レイヤ 3（Layer 3）] フィールドと [レイヤ 2（Layer 2）] フィールドで、選択内容が上記のスクリーンショットの選択内容と一致することを確認します。

b) [ノード（Nodes）] 領域で、[ノード ID（Node ID）] フィールドのドロップダウン リストからノード ID を選択します。(leaf2 (Node 102))

c) [ルータ ID（Router ID）] フィールドに、適切なルータ ID を入力します。(2.2.2.2)

[ループバック アドレス（Loopback Address）] フィールドは、入力したルータ ID 値に基づいて自動的に入力されます。ループバック アドレスは必要ないため、値を削除し、フィールドを空白のままにします。

d) [インターフェイス（Interface）] フィールドで、インターフェイス ID を選択します。（eth1/11）

e) [IP アドレス（IP Address）] フィールドに、関連付けされた IP アドレスを入力します。(172.16.1.1/30)

f) [MTU] フィールドはデフォルト値のままにします。(inherit)

g) [MTU] フィールドの横にある [+] アイコンをクリックして、ノード leaf2 のインターフェイスを追加します。(Node-102)
h) [インターフェイス（Interface）] フィールドで、インターフェイス ID を選択します。（eth1/12）
i) [IP アドレス（IP Address）] フィールドに、関連付けされた IP アドレスを入力します。(172.16.2.1/30)
j) [MTU] フィールドはデフォルト値のままにします。(inherit)

ステップ 5 別のノードを追加するには、[ループバック アドレス（Loopback Address）] フィールドの横にある [+] アイコンをクリックし、次の操作を実行します。

（注） [+] アイコンをクリックすると、以前に入力した領域の下に新しい [ノード（Nodes）] 領域が表示されます。

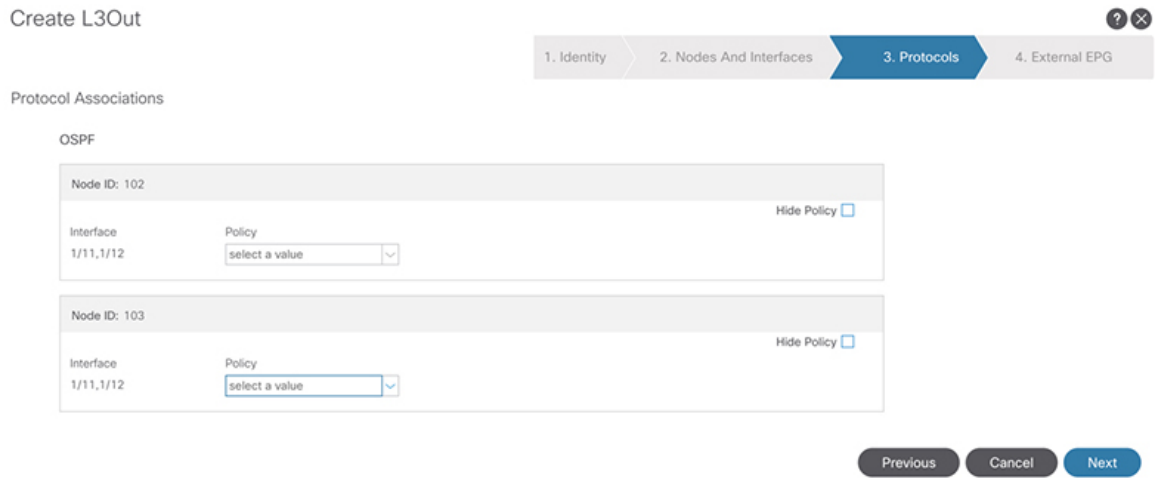
a) [ノード（Nodes）] 領域で、[ノード ID（Node ID）] フィールドのドロップダウン リストからノード ID を選択します。(leaf3 (Node-103))
b) [Router ID] フィールドに、ルータ ID を入力します。(3.3.3.3)

[ループバック アドレス（Loopback Address）] フィールドは、入力したルータ ID 値に基づいて自動的に入力されます。ループバック アドレスは必要ないため、値を削除し、フィールドを空白のままにします。

c) [インターフェイス（Interface）] フィールドで、インターフェイス ID を選択します。（eth1/11）
d) [IP Address] フィールドに、IP アドレスを入力します。(172.16.3.1/30)
e) [MTU] フィールドはデフォルト値のままにします。(inherit)
f) [MTU] フィールドの横にある [+] アイコンをクリックして、ノード leaf3 のインターフェイスを追加します。(Node-103)
g) [インターフェイス（Interface）] フィールドで、インターフェイス ID を選択します。（eth1/12）
h) [IP アドレス（IP Address）] フィールドに、関連付けされた IP アドレスを入力します。(172.16.4.1/30)
i) [MTU] フィールドはデフォルト値のままにします。(inherit)、[次へ（Next）] をクリックします。
各インターフェイスのノード、インターフェイス、および IP アドレスを指定しました。

ステップ 6 [次へ（Next）] をクリックして、[プロトコル（Protocols）] 画面を表示します。

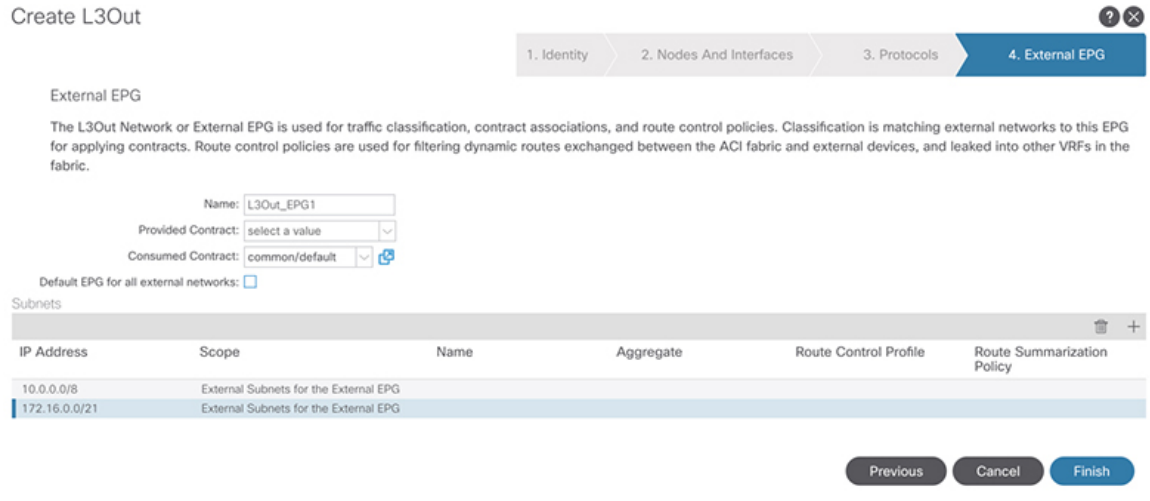
この画面では、hello-interval、network-type などを設定するための OSPF インターフェイス レベル ポリシーを指定できます。



この例では、何も選択されていません。したがって、デフォルト ポリシーが使用されます。デフォルトの OSPF インターフェイス プロファイルは、ネットワーク タイプとして Unspecified を使用します。デフォルトはブロードキャスト ネットワーク タイプです。サブインターフェイスのポイントツーポイント ネットワーク タイプでこれを最適化するには、「OSPF インターフェイス レベル パラメータの変更（任意）」を参照してください。

ステップ 7 **[次へ（Next）]** をクリックします。
[外部 EPG（External EPG）] 画面に L3Out EPG の詳細が表示されます。この設定では、コントラクトに適用する EPG にトラフィックを分類します。

ステップ 8 [外部 EPG（External EPG）] スクリーンで次のアクションを実行します。



a) [外部 EPG（External EPG）] 領域で、[名前（Name）] フィールドに、外部 EPG の名前を入力します。(L3Out_EPG1)
b) [提供されたコントラクト（Provided Contract）] フィールドでは、値を選択しないでください。

この例では、通常の EPG（EPG1）がプロバイダーであるため、L3Out_EPG1 に提供されるコントラクトはありません。

c) [消費されたコントラクト（Consumed Contract）] フィールドで、ドロップダウン リストから、[デフォルト（default）] を選択します。

ステップ 9 [すべての外部ネットワークのデフォルト EPG（Default EPG for all external networks）] フィールドで、チェックボックスをオフにし、次の操作を実行します。

a) [サブネット（Subnets）] 領域の [+] アイコンをクリックして、[サブネットの作成（Create Subnet）] ダイアログボックスを表示します。
b) [IP アドレス（IP Address）] フィールドに、サブネットを入力します。(10.0.0.0/8)
c) [外部 EPG 分類（External EPG Classification）] フィールドで、[外部 EPG の外部サブネット（External Subnets for the External EPG）] のチェックボックスをオンにします。[**OK**] をクリックします。

ステップ 10 [サブネット（Subnets）] 領域の [+] アイコンをもう一度クリックして [サブネットの作成（Create Subnet）] ダイアログボックスを表示し、次の操作を実行します。

（注） これはオプションの設定ですが、エンドポイントがこれらの IP と通信する必要がある場合に備えて、L3Out インターフェイス サブネットを指定することをお勧めします。

a) [IP アドレス（IP Address）] フィールドに、サブネットを入力します。(172.16.0.0/21)

このサブネットは、L3Out 内のすべてのインターフェイスをカバーします。代わりに、各ルーテッド インターフェイスの個々のサブネットを使用できます。

b) [外部 EPG 分類（External EPG Classification）] フィールドで、[外部 EPG の外部サブネット（External Subnets for the External EPG）] のチェックボックスをオンにします。[**OK**] をクリックします。
c) **[終了]** をクリックします。

L3Out OSPF が展開されました。

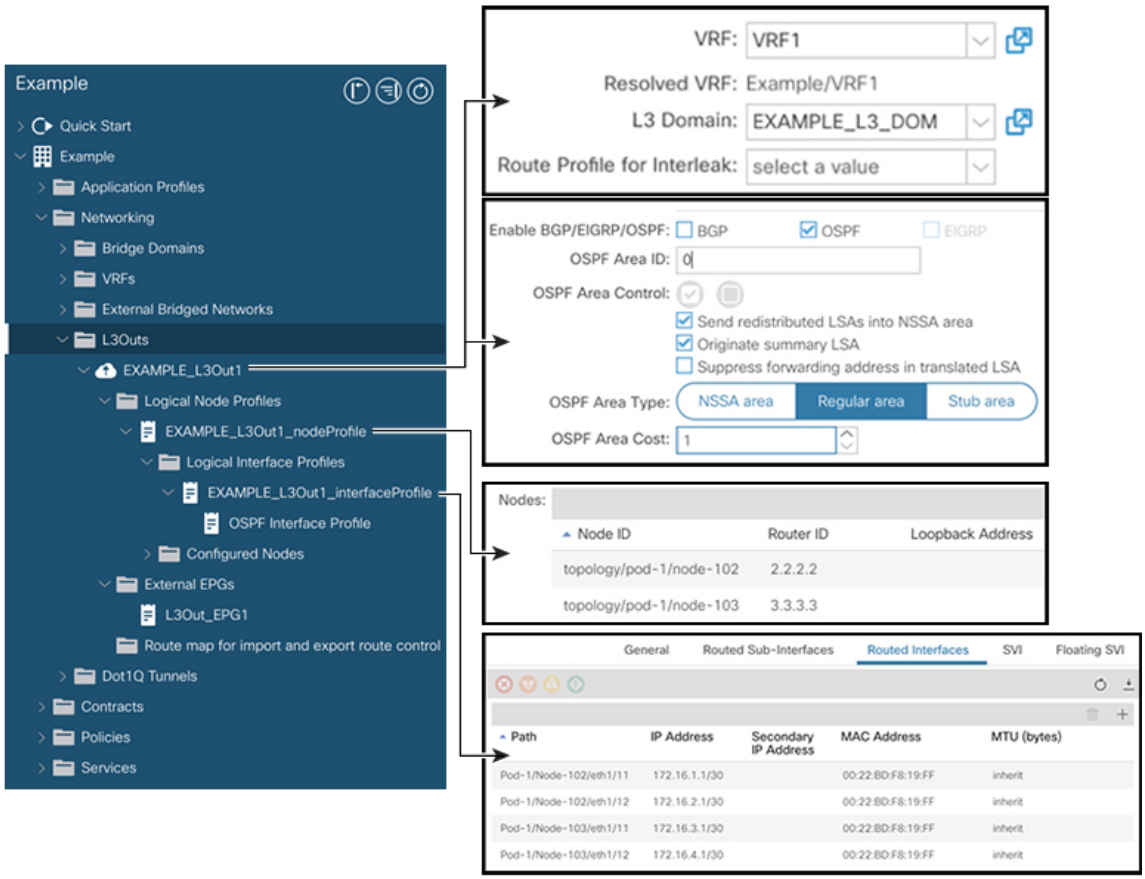
確認：Create L3Out Wizard を使用した L3Out の作成例

ウィザードを使用した設定が GUI にどのように表示されるかを確認し、設定が正確であることを確認します。Cisco APIC

手順

ステップ 1 [作業（Work）] ペインで、**[Tenant_name]** > **[ネットワーキング（Networking）]** > **[L3Outs]** > **[EXAMPLE_L3Out1]**の順に移動し、次のようにスクロールして詳細を表示します。

GUI のこの場所で、[L3Out の作成（Create L3Out）] ウィザードの [識別（Identity）] 画面で設定されている VRF、ドメイン、OSPF パラメータなどの主要な L3Out パラメータを確認します。



ステップ 2 OSPF がエリア ID やエリア タイプなどの指定されたパラメータで有効になっていることを確認します。

ステップ 3 [論理ノード プロファイル（Logical Node Profiles）] の下に、EXAMPLE_L3Out1_nodeProfile が作成され、ルータ ID で境界リーフ スイッチが指定されます。

ステップ 4 [論理インターフェイス プロファイル（Logical Interface Profile）] の下に、EXAMPLE_L3Out1_interfaceProfile が作成されます。

この例では、インターフェイス ID、IP アドレスなどのインターフェイス パラメータをルーテッド インターフェイスとして確認します。デフォルトの MAC アドレスが自動的に入力されます。OSPF インターフェイス プロファイルは、OSPF インターフェイス レベルのパラメータに対しても作成されます。

レビューが完了しました。

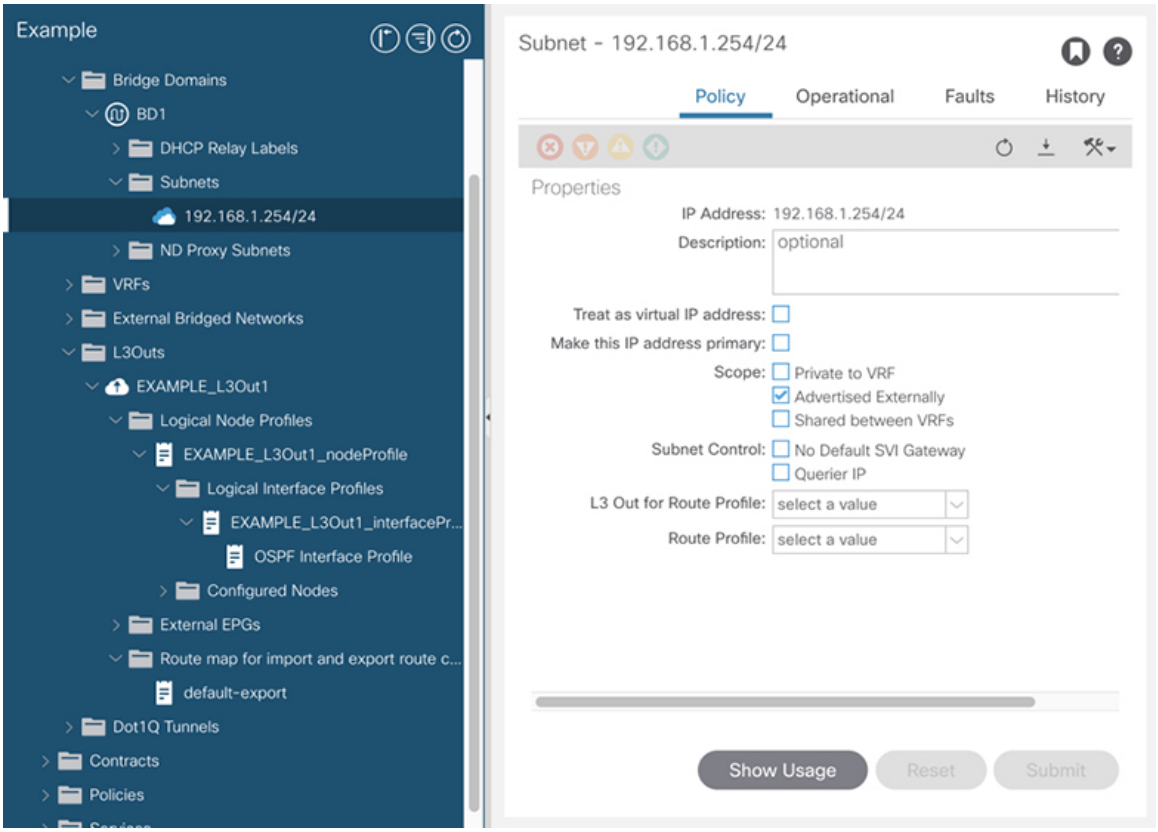
ルート マップによる BD サブネットのアドバタイズの設定

この例では、ルート マップ default-export を IP プレフィックス リストとともに使用して、BD サブネットをアドバタイズします。

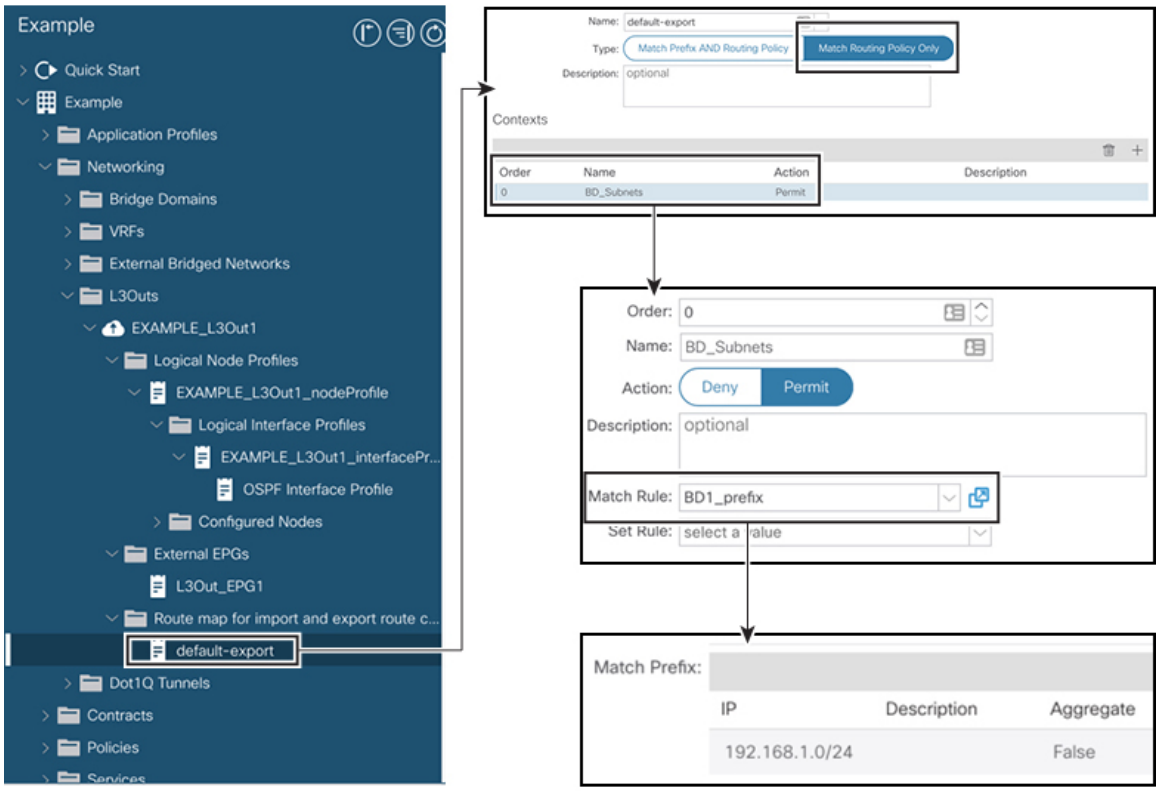
（注） このデフォルトエクスポートルートマップは、特定のものに関連付けられることなく、L3Out（EXAMPLE_L3Out1）に適用されます。

手順

ステップ 1 アドバタイズされる BD サブネットを有効にするには、[テナント（Tenant）] [ネットワーク（Networks）] [ブリッジ ドメイン（Bridge Domains）] [BD1] [サブネット（Subnets）] [192.168.1.254/24] に移動し、[外部的にアドバタイズ（Advertised Externally）] の範囲を選択します。 > > > > >



ステップ 2 L3Out（EXAMPLE_L3Out1）の下にルート マップを作成するには、[ルート制御のインポートおよびエクスポート向けルート マップ（Route map for import and export route control）] に移動します。



ステップ 3 右クリックして[ルート制御のインポートおよびエクスポート向けルートマップの作成（Create Route map for import and export route control）] を選択します。

ステップ 4 [ルート制御のインポートおよびエクスポート向けルート マップの作成（Create Route map for import and export route control）] ダイアログ ボックスの [名前（Name）] フィールドで、[default-export] を選択します。

ステップ 5 [タイプ（Type）] フィールドで、[ルート ポリシーの一致のみ（Match Routing Policy Only）] を選択します。

（注） [ルーティング ポリシーのみ照合（Match Routing Policy Only）]：この [タイプ（Type）] を default-export ルート マップで選択すると、すべてのルート アドバタイズメント設定がこのルートマップによって実行されます。外部EPGで設定されたBDアソシエーションおよびエクスポートルート制御サブネットは適用されません。このL3Outからアドバタイズされるすべてのルートに対して、このルートマップ内のすべての一致ルールを設定する必要があります。

[プレフィックスおよびルーティング ポシリーの照合（Match Prefix and Routing Policy）]：この [タイプ（Type）] を default-export ルート マップで選択すると、ルート アドバタイズメントは、外部 EPG で定義された BD から L3Out へのアソシエーションおよびエクスポート ルート制御サブネットに加えて、このルート マップで設定されたすべての一致ルールと照合されます。

ルートプロファイルを使用する場合は、メンテナンスが容易なシンプルな設定のために [ルーティング ポリシーのみ照合（Match Routing Policy Only）] を使用することを推奨します。

ステップ 6 [**コンテキスト（Contexts**）] 領域で [+] アイコンをクリックして、[**ルート制御コンテキストの作成（Create Route Control Context**）] ダイアログ ボックスを表示し、次のアクションを実行します。

a) [順序（Order）]フィールドで、順序を設定します。(0)

この例では、注文は 1 つだけです。

b) [**名前（Name**）]フィールドに、コンテキストポリシーの名前を入力します。（BD_Subnets）

c) [**アクション（Action**）] フィールドで [**許可（Permit**）] を選択します。

これにより、設定するプレフィックスを許可するルート マップが有効になります。

この例では、IP プレフィックス リスト [**BD1_prefix**] を必要とする一致ルールが必要です。この IP プレフィックス リストは、アドバタイズされた BD サブネットを指します。

ステップ 7 [一致ルール（Match Rule）] フィールドで、次の操作を実行して IP プレフィックス リストを作成します。

a) [ルートマップの一致ルールの作成（Create Match Rule for a Route-Map）] を選択します。

b) [名前（Name）] フィールドに、名前 [*BD1_prefix*] を入力します。

c) [プレフィクスの一致（Match Prefix）] 領域で、[+] アイコンをクリックし、BD サブネット（192.168.1.0/24）を入力します。

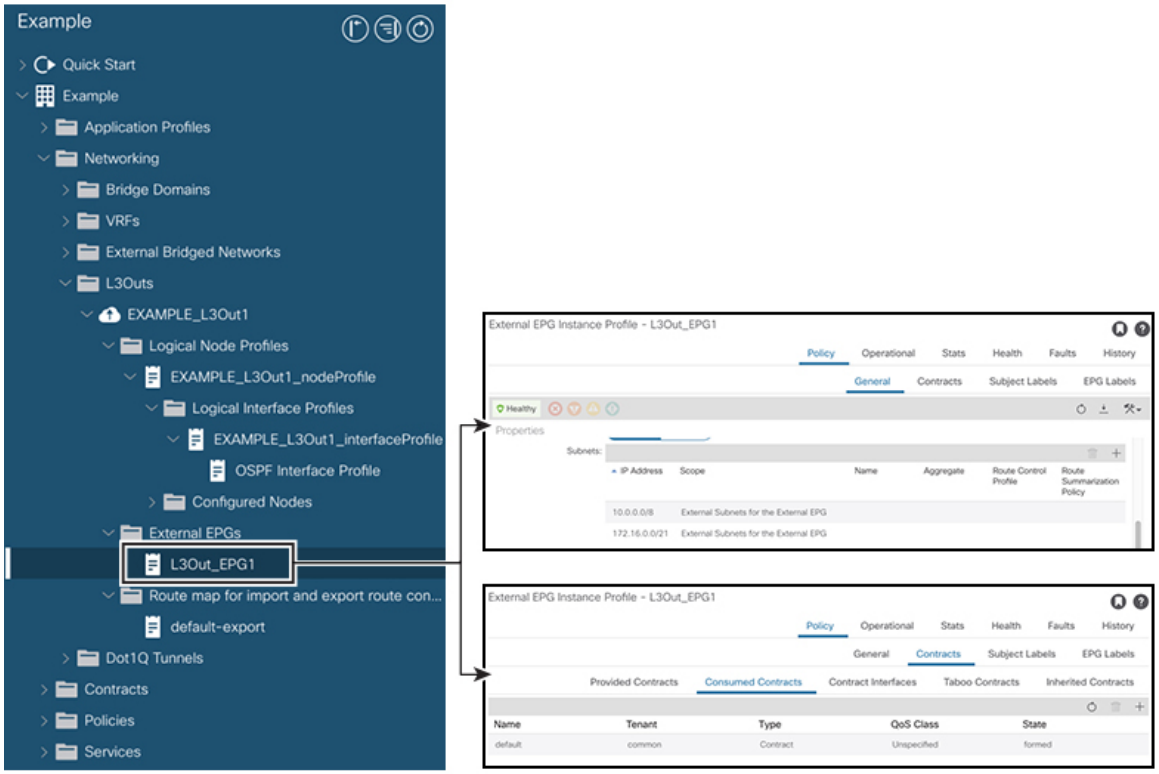
コントラクトの確認

このタスクでは、エンドポイント（192.168.1.1）と外部プレフィックス（10.0.0.0/8、およびオプションで 172.16.0.0/21）間の通信を有効にするためのコントラクトを確認します。この例では、エンドポイントの EPG は EPG1 で、外部プレフィックスの外部 EPG は L3Out_EPG1 です。

必要な設定は、[L3Out の作成（Create L3Out）] ウィザードにすでに表示されています。

手順

ステップ 1 L3Out で **[外部 EPG（External EPGs）]** > **[L3Out_EPG1]** に移動します。



ステップ 2 [作業（Work）] ペインの [外部 EPG インスタンス プロファイル（External EPG Instance Profile）] 領域の [ポリシー全般（Policy General）] サブタブで、[プロパティ（Properties）] を確認し、外部 EPG の [外部サブネット（External Subnets）] で 2 つのサブネットが表示されることを確認します。 >

ステップ 3 次に、[コントラクト（Contracts）] サブタブをクリックし、前に指定した契約が正しく使用されていることを確認します。さらにコントラクトを追加する場合は、GUI でこの場所からアクションを実行できます。

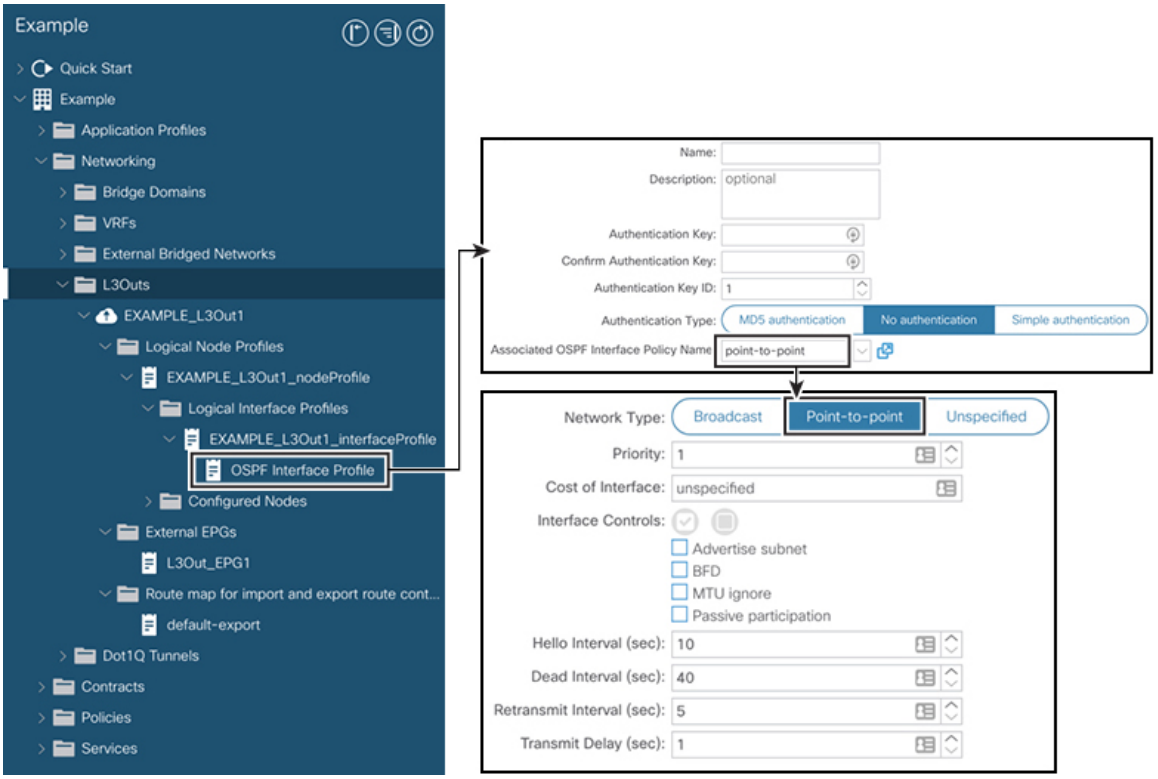
ステップ 4 [アプリケーション プロファイル（Application Profile）] [アプリケーション EPG（Application EPGs）] [EPG1] [コントラクト（Contracts）] に移動し、EPG1 が適切なコントラクトを提供していることを確認します。 > > >

OSPF インターフェイス レベル パラメータの変更（任意）

Hello Interval、OSPF ネットワーク タイプなどの OSPF インターフェイス レベルのパラメータを変更する場合は、OSPF インターフェイス プロファイルで設定できます。ノード レベルの OSPF パラメータはすでに設定されています。

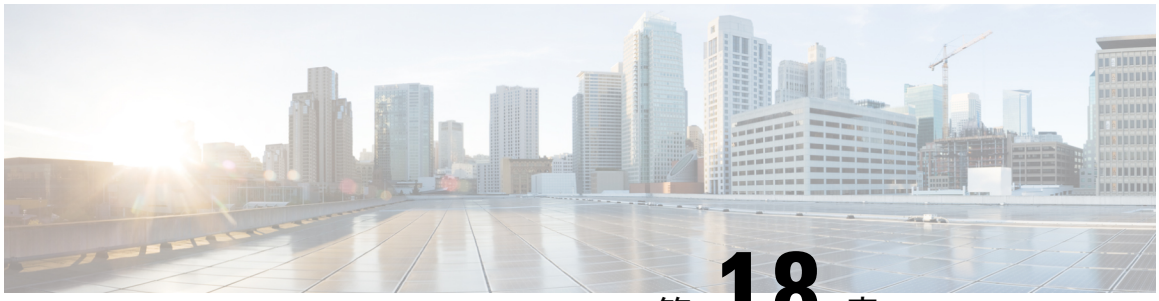
手順

ステップ 1 L3Out で、[論理インターフェイス プロファイル（Logical Interface Profile）] の [EXAMPLE_L3Out1_interfaceProfile] に移動します。 > >



ステップ 2 [ワーク（Work）] ペインの [プロパティ（Properties）] 領域で、使用する OSPF インターフェイス ポリシーを選択します。

これにより、OSPF インターフェイス レベルのパラメータが変更されます。



第 18 章

L3Out のノードとインターフェイス

L3Out のインターフェイスの変更

GUI を使用した L3Out のインターフェイスの変更

この手順では、L3Out インターフェイスを変更します。

（注） フィールドに入力する手順は、必ずしも GUI に表示される順序と同じ順序でリストされているわけではありません。

始める前に

- Cisco ACI ファブリックが設置され、Cisco APIC がオンラインになっており、Cisco APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる Cisco APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチが Cisco ACI ファブリックに登録され、使用可能であること。
- ポートチャネルは、L3Outインターフェイスにポート チャネルが使用される場合に設定されます。

手順

ステップ 1 メニュー バーで、**[テナント（Tenants）] > > [すべてのテナント（ALL Tenants）]** の順に選択します。

ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーション ペインで、**[tenant_name]** > **[ネットワーキング（Networking）]** > **[L3Outs]** > ***[L3Outs]*** > **[論理ノード プロファイル（Logical Node Profiles）]** > ***node_profile*** > **[論理インターフェイス プロファイル（Logical Interface Profiles）]**の順に移動し、変更したいプロファイルを選択します。

ステップ 4 [インターフェイス タイプ] タブを選択：**[ルーテッド サブインターフェイス（Routed Sub-Interfaces）]**、**[ルーテッド インターフェイス（Routed Interfaces）]**、**[SVI]**、または **[浮動 SVI（Floating SVI）]** を選択します。

ステップ 5 既存のインターフェイスをダブルクリックして変更するか、**[作成（Create）]**（+） ボタンをクリックして新しいインターフェイスを論理インターフェイス プロファイルに追加します。

ステップ 6 浮動 SVI 以外のインターフェイス タイプの場合は、次のサブステップを実行します。m

a) [**パス タイプ（Path Type**）] フィールドで新しいインターフェイスを追加し、適切なパス タイプを選択します。

ルーテッドサブインターフェイスまたはルーテッドインターフェイスタイプの場合、**ポート**または**ダイレクト ポートチャネル**を選択します。SVIインターフェイス タイプの場合、**ポート**、**ダイレクト ポート チャネル**、または**仮想ポート チャネル**を選択します。

b) **[ノード（Node）]** ドロップダウン リストから、ノードを選択します。

（注） これは、非ポート チャネル パス タイプにのみ適用されます。**[パス タイプ（Path Type）]** を **[ポート（Port）]** として選択した場合は、この手順を実行します。それ以外の場合は、次のステップに進みます。

c) **[パス（Path）]** ドロップダウン リストからインターフェイス ID またはポート チャネル名を選択します。

インターフェイス ID の例は eth 1/1 です。ポート チャネル名は、各直接または仮想ポート チャネルのインターフェイス ポリシー グループ名です。

ステップ 7 浮動 SVI インターフェイス タイプの場合、**[アンカー ノード]** ドロップダウン リストでノードを選択します。

ステップ 8 （任意）[**説明（Description**）] フィールドに、L3Out インターフェイスの説明を入力します。

ステップ 9 ルーテッド サブインターフェイス、SVI および浮動 SVI インターフェイスの場合、**[[カプセル化（Encap）]** ドロップダウン rストで、**[VLAN]** を選択し、このエントリの整数値を入力します。

ステップ 10 SVI および浮動 SVI インターフェイス タイプの場合は、次のサブステップを実行します。

a) **[カプセル化範囲（Encap Scope）]** ボタンで、レイヤ 3 Outside プロファイルに使用されるカプセル化の範囲を選択します。

- **VRF** : 特定の VLAN カプセル化の同じ VRF インスタンス内のすべてのレイヤ 3 外部で同じトランジット VLAN を使用します。これはグローバル値です。
- **Local** : レイヤ 3 外部ごとに一意のトランジット VLAN を使用します。

b) **[自動状態（Auto State）]** ボタンについては、この機能を有効にするか無効にするかを選択します。

- **disabled**：インターフェイスが対応する VLAN で動作していない場合、SVI がアクティブであることを意味します。
- **enabled**：VLAN インターフェイスが VLAN で複数のポートを有する場合、SVI は 浮動 SVI はVLAN のすべてのポートがダウンするとダウン状態になります。

c) **[モード]** ボタンで、VLAN タギング モードを選択します。

ステップ 11 **IPv4 Primary / IPv6 Preferred Address** フィールドに、レイヤ 3 外側プロファイルにアタッチされているパスのプライマリ IP アドレスを入力します。

ステップ 12 **[IPv4 セカンダリ/IPv6 追加アドレス]** テーブルで、+ をクリックして、レイヤ 3 外側プロファイルにアタッチされているパスのセカンダリ IP アドレスを入力します。

ステップ 13 （任意） **Link-local Address** フィールドに、 IPv6 リンクローカル アドレスを入力します。これは、システムによって生成された IPv6 リンクローカル アドレスをオーバーライドします。

ステップ 14 **[MAC アドレス]** フィールドに、レイヤ 3 外側プロファイルにアタッチされているパスの MAC アドレスを入力します。

ステップ 15 **[MTU（バイト）]** フィールドで、外部ネットワークの最大転送単位を設定します。指定できる範囲は 576 ～ 9216 です。値を継承するには、*inherit* フィールドに入力します。

ステップ 16 **[ターゲット DSCP]** ドロップダウンリストで、レイヤ 3 アウトサイド プロファイルに接続されているパスのターゲット Differentiated Services Code Point（DSCP）を選択します。

ステップ 17 [Submit] をクリックします。

OSPF インターフェイス プロファイルの作成

OSPF インターフェイス プロファイルは、インターフェイスで OSPF を有効にします。必要に応じて、OSPF インターフェイス プロファイルに OSPF インターフェイス ポリシーとの関係を設定すれば、インターフェイスのプロパティをより詳細に制御できます。

始める前に

- Cisco ACI ファブリックが設置され、Cisco APIC がオンラインになっていて、Cisco APIC クラスタが形成されていて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチが Cisco ACI ファブリックに登録され、使用可能であること。

- ポートチャネルは、L3Outインターフェイスにポートチャネルが使用される場合に設定されます。

手順

ステップ 1 メニュー バーで、**[テナント（Tenants）] > [すべてのテナント（All Tenants）]** の順に選択します。

ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーション ペインから、**[tenant_name] > [ネットワーキング（Networking）] > [L3Outs] > [L3Out] > [論理ノード プロファイル（Logical Node Profiles）] > [node_profil] > [論理インターフェイス プロファイル（Logical Interface Profiles）] > [OSPF インターフェイス プロファイル（OSPF Interface Profile）]** の順に移動します。

ステップ 4 **[名前（Name）]** フィールドに、OSPFインターフェイスの名前を入力します。この名前では最大 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。

ステップ 5 [オプション] **[説明（Description）]** フィールドに、この OSPF インターフェイス プロファイルの説明を入力します。説明には最大 128 文字までの英数字を使用できます（省略も可）。

ステップ 6 ターゲット インターフェイス ポリシー名の値を入力します。この名前では最大 64 文字までの英数字を使用できます。オブジェクトの作成後は、この名前は変更できません。

ステップ 7 **[OSPFv2 認証キー（OSPFv2 Authentication Key）]** フィールドに認証キーを入力します。認証キーは、一種のパスワードで（最大8文字）、インターフェイスごとに割り当てることができます。そのインターフェイス上の認証キーは、各ルータ間で一致させる必要があります。

（注） 認証を使用するには、このインターフェイスのエリアに対する OSPF 認証タイプを [シンプル（Simple）] に設定します（デフォルトは [なし（None）]）。

ステップ 8 **[OSPFv2 認証キーの確認（Confirm OSPFv2 Authentication Key）]** フィールドに認証キーをもう一度入力します。

ステップ 9 **[OSPFv2 認証キー ID（OSPFv2 Authentication Key ID）]** フィールドに認証キーの識別子を入力します。

ステップ 10 [OSPFv2 認証タイプ（OSPFv2 Authentication Type）] フィールドで、適切なオプションを選択します。

OSPF 認証タイプ。認証により、OSPF ネイバーを柔軟に認証できます。OSPF での認証を有効にすることにより、ルーティングの更新情報を安全な方法で交換できます。

（注） 認証を設定するときは、領域全体を同じタイプの認証で設定する必要があります。

認証タイプは次のとおりです。

- **[なし（None）]**：認証は使用されません。

- **[シンプル（Simple）]**：エリアのインターフェイスごとに、認証キーをインターフェイスのセクションに記述する必要があります。
- **[Md5]**：パスワードをネットワークを介して渡しません、MD5 は、RFC 1321 で規定されたメッセージダイジェスト アルゴリズムです。MD5 が最も安全な OSPF 認証モードと見なされています。認証を設定するときは、領域全体を同じタイプの認証で設定する必要があります。

デフォルトは [なし（None）] です。

ステップ 11 **[OSPF キーチェーン ポリシー（OSPFv2 KeyChain Policy）]** フィールドで、OSPFv2 キーチェーン ポリシーを選択します。

OSPFv2 キーチェーンポリシーは、簡易認証および MD5 認証とともに HMAC-SHA 認証をサポートします。このオプションを選択すると、同じキーチェーンの下に複数のキーを含めることができます。

セキュリティを強化するために、各キーの有効期間を指定して、キーのローテーションを設定できます。キーの有効期間が切れると、次のキーに自動的にローテーションされます。アルゴリズムを指定しなかった場合、OSPF はデフォルトの暗号化認証アルゴリズムである MD5 を使用します。

（注） 新しいキーが優先キーであり、既存のキーよりも優先されます。

次のタスク

OSPFv2 キーチェーンのローテーション キーを指定するには、次を使用します：

キー ポリシーの作成

始める前に

OSPFv2 インターフェイス プロファイルが作成されていることを確認します。詳細については、OSPF インターフェイス プロファイルの作成 （299 ページ）を参照してください。

手順

ステップ 1 メニュー バーで **[テナント（Tenants）] > [インフラ（infra）]** をクリックします。

ステップ 2 [ナビゲーション（Navigation）] ペインで、**[ポリシー（Policies）] > [プロトコル（Protocol）] > [キーチェーン（KeyChains）]** をクリックします。

ステップ 3 **[キーチェーン（KeyChains）]** を右クリックし、**[キーポリシーの作成（Create Key Policy）]** を選択して、次の手順を実行します。

a) ポリシーの名前を入力し、必要に応じて説明を追加します。

b) **[キー ID（Key ID）]** フィールドに、キー ID 番号を入力します。
c) **[事前共有キー（Pre-shared Key）]** フィールドに、事前共有キーの情報を入力します。
d) **[暗号化アルゴリズム（Cryptographic Algorithm）]** フィールドに、アルゴリズムを入力します。
e) **[開始時刻（Start Time）]** フィールドで、開始時刻を **YYYY-MM--DD-HH-MM-SS** 形式で指定します。
f) **[終了時刻（End Time）]** フィールドで、終了時刻を **YYYY-MM--DD-HH-MM-SS** 形式で指定します。
g) **[キー受け入れライフタイムの開始時刻（Key accept lifetime start time ）]** フィールドで、**YYYY-MM--DD-HH-MM-SS** 形式で開始時刻を指定します。

これはローテーションキーです。各キーの有効期間を指定します。キーのライフタイムが期限切れになると、次のキーに自動的にローテーションされます。アルゴリズムを指定しない場合、OSPF はデフォルトの暗号化認証アルゴリズムである MD5 を使用します。

（注） 新しいキーが優先キーであり、既存のキーよりも優先されます。

h) **[キー受け入れライフタイムの終了時刻（Key accept lifetime end time ）]** フィールドで、**YYYY-MM--DD-HH-MM-SS** 形式で終了時刻を指定します。

ステップ 4 [Submit] をクリックします。

L3Out の SVI のカスタマイズ

SVI 外部カプセル化の範囲

SVI 外部カプセル化の範囲について

レイヤ 3 アウト設定のコンテキストでは、スイッチ仮想インターフェイス（SVI）は ACI リーフ スイッチとルータ間に接続性を提供するように設定されます。

デフォルトで単一のレイヤ 3 アウトが SVI インターフェイスで設定されている場合、VLAN のカプセル化はファブリック内の複数のノードに範囲が及びます。これは、図で示されるように SVI インターフェイスが同じ外部カプセル化（SVI）を使用する限り、レイヤ 3 アウト SVI が展開されているファブリックで、ACI ファブリックがすべてのノード上に同じブリッジ ドメイン（VXLAN VN）を設定するため発生します。

ただし、異なるレイヤ 3 アウトが展開されている場合、同じ外部カプセル化 (SVI) を使用している場合でも ACI ファブリックは異なるブリッジ ドメインを使用します。

図 *35* : ローカル範囲のカプセル化と *1* 個のレイヤ *3* アウト

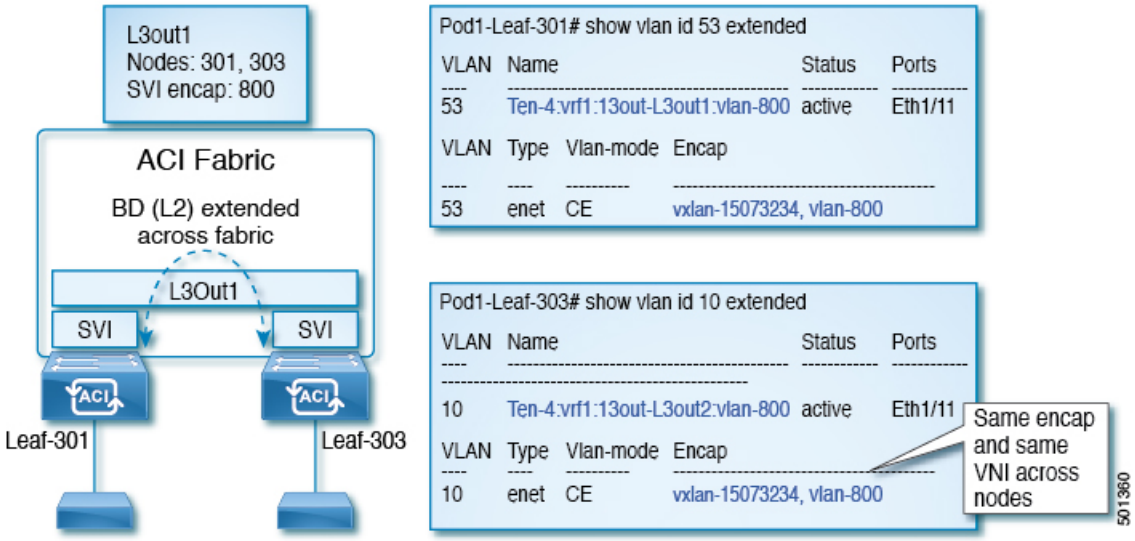
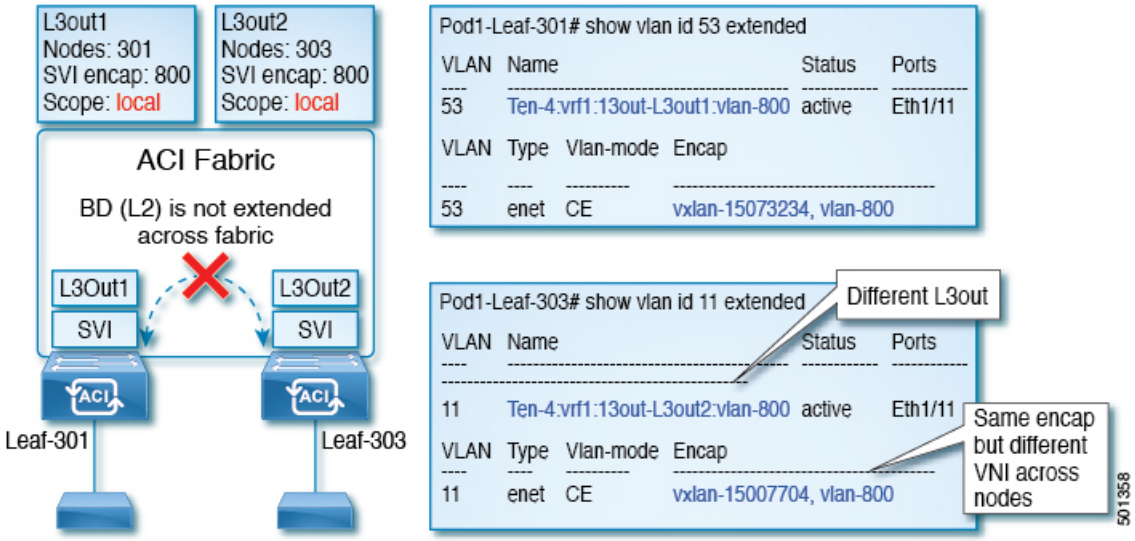


図 *36* : ローカル範囲のカプセル化と *2* 個のレイヤ *3* アウト

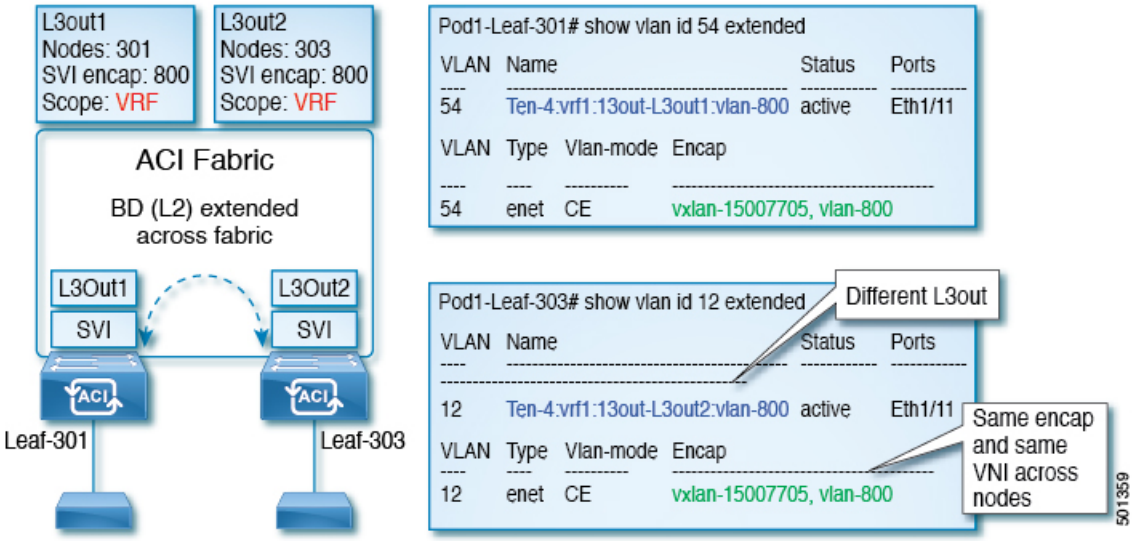


Cisco APIC リリース 2.3 以降、同じ外部カプセル化（SVI）を使用して、2 個以上のレイヤ 3 アウトを展開する場合の動作を選択できるようになりました。

カプセル化の範囲は、ローカルまたは VRF として設定できます。

- ローカル範囲（デフォルト）：例の動作が「ローカル範囲のカプセル化および *2* 個のレイヤ *3* アウト」というタイトルの図に表示されます。
- VRF 範囲：ACI ファブリックが、同じ外部カプセル化（SVI）が展開されているすべてのノードとレイヤ 3 アウト上で同じブリッジドメイン（VXLAN VNI）を設定します。「*VRF* 範囲のカプセル化および *2* 個のレイヤ *3* アウト」というタイトルの図の例を参照してください。

図 *37 : VRF* 範囲のカプセル化および *2* 個のレイヤ *3* アウト



カプセル化スコープ構文

レイヤ 3 Out プロファイルで使用されるカプセル化の範囲を設定するためのオプションは次のとおりです。

- **Ctx**]: 特定の VLAN のカプセル化の同じ VRF に、すべてのレイヤ 3 が記録されるで同じ外部 SVI。これはグローバル値です。
- **ローカル** : レイヤ 3 Out ごとの一意の外部 SVI。これはデフォルト値です。

CLI、API、および GUI 構文間のマッピングは次のとおりです。

表 *11 :* カプセル化スコープ構文

CLI	API	GUI
l3out	local	local
vrf	ctx	VRF

（注） カプセル化の範囲を設定する CLI コマンドでは、名前付きのレイヤ 3 アウト設定、VRF が設定されている場合にのみサポートされます。

SVI 外部カプセル化の範囲のガイドライン

SVI 外部カプセル化の範囲を使用する際には、次のガイドラインに従ってください:

- 同じノード上にレイヤ 3 Out を設定するためには、両方のレイヤ 3 Out の OSPF エリアが異なっている必要があります。

• 同じノード上にレイヤ 3 Out を設定するためには、両方のレイヤ 3 Out の BGP ピア設定が異なる必要があります。

GUI を使用して SVI 外部カプセル化の範囲の設定

始める前に

• テナントと VRF が設定されています。

• L3Out が設定されていて、L3Out で論理ノード プロファイルが設定されています。

手順

ステップ 1 メニュー バーで、 > **Tenants** > ***Tenant_name*** をクリックします。

ステップ 2 [ナビゲーション（Navigation）]ペインで、[ネットワーキング（Networking）] [L3Outs] [L3Out_name] [論理ノードプロファイル）Logical Node Profiles] [LogicalNodeProfile_name] [論理インターフェイスプロファイル（Logical Interface Profiles）]をクリックします。 > > > > >

ステップ 3 [**ナビゲーション**（**Navigation**）] ウィンドウで、[**論理インターフェイス プロファイル**（**Logical Interface Profile**）] を右クリックし、[**インターフェイス プロファイルの作成**（**Create Interface Profile**）] をクリックします。

ステップ 4 [Create Interface Profile] ダイアログボックスで、次の操作を実行します。

a) **Step 1 Identity** 画面の **Name** フィールドで、インターフェイス プロファイルの名前を入力します。

b) 残りのフィールドに、適切なオプションを選択し] をクリックして **次** 。

c) **ステップ 2 プロトコル プロファイル** 画面、目的のプロトコルを選択するには、プロファイルの詳細、および] をクリックして **次** 。

d) **ステップ 3 インターフェイス** 画面で、をクリックして、 **SVI**] タブをクリックして、 + を開くにアイコン、 **選択 SVI** ダイアログボックス。

e) **インターフェイスの指定**] 領域で、目的、さまざまなフィールド値を選択します。

f) **Encap スコープ** フィールドで、目的のカプセル化範囲の値を選択します。[OK] をクリックします。

デフォルト値は **Local** です。

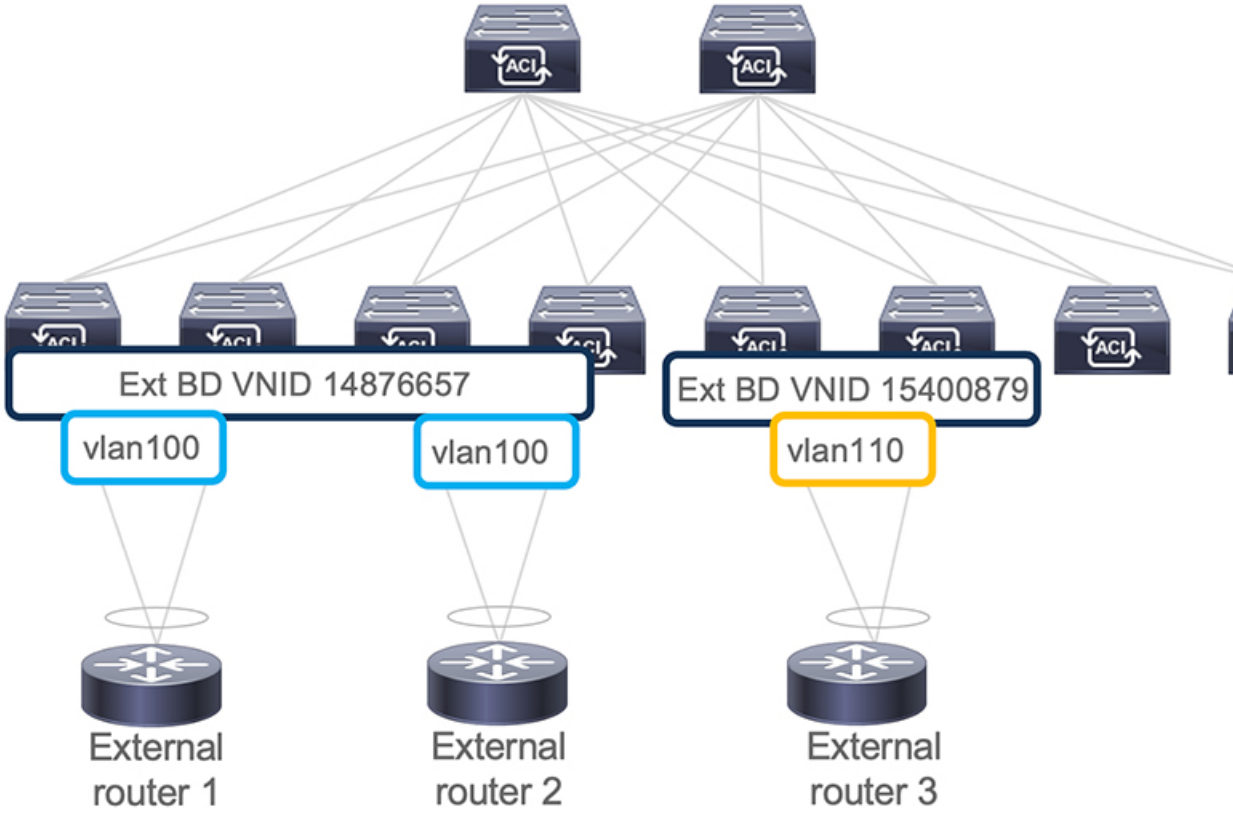
SVI 外部のカプセル化の範囲は、指定されたインターフェイスで設定されます。

SVI での複数の L3Out のカプセル化のサポート

同じカプセル化 VLAN を使用する異なるリーフ スイッチ上の SVI インターフェイスで L3Out が設定されている場合、SVI VLAN は同じ VXLAN ネットワーク識別子（VNID）にマッピングされます。これにより、ファブリック全体に単一のブリッジ ドメイン（外部ブリッジ ドメ

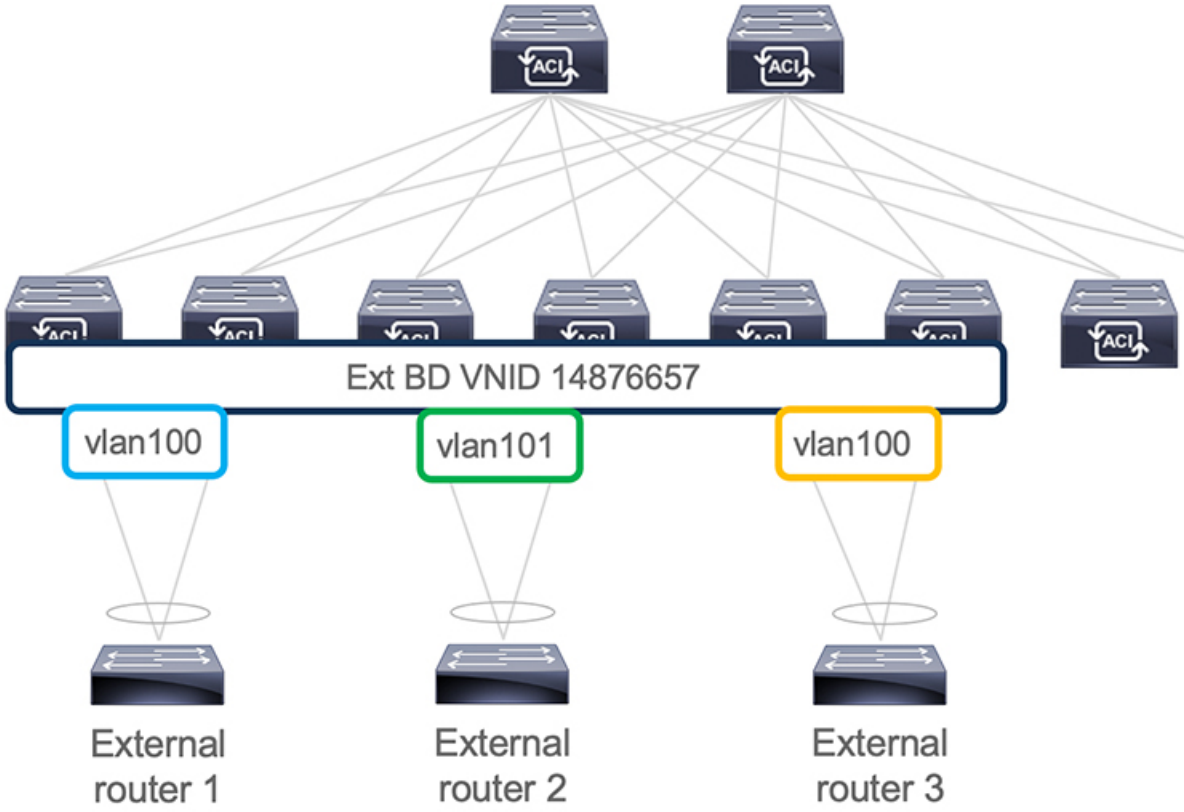
イン）とブロードキャスト ドメインが形成されます。次の図に示すように、異なる VLAN で設定された SVI インターフェイスは、別個の外部ブリッジ ドメインを形成します。リリース 5.2(3) より前は、異なるスイッチ上に異なるカプセル化 VLAN を持つ単一の外部ブリッジ ドメインを作成することはできませんでした。

図 *38 :* カプセル化が異なる外部ブリッジ ドメインに関連付けられた個別の *VNID*（*ACI 5.2(3)* より前のリリース）。



リリース 5.2(3) では、異なるリーフ スイッチ上の異なるカプセル化 VLAN で構成できる単一の外部ブリッジを構成するためのサポートが追加されました。複数カプセル化のサポート機能では、フローティング SVI オブジェクトを使用して、フローティング L3Out の外部ブリッジ ドメインを定義するか、または外部ブリッジ グループ プロファイルを使用して、通常の L3Out の外部ブリッジ ドメインを定義します。この機能の使用例としては、同じ VLAN がすでに使用されている可能性があるため、異なるリーフ スイッチで同じ VLAN を使用できない場合があります。

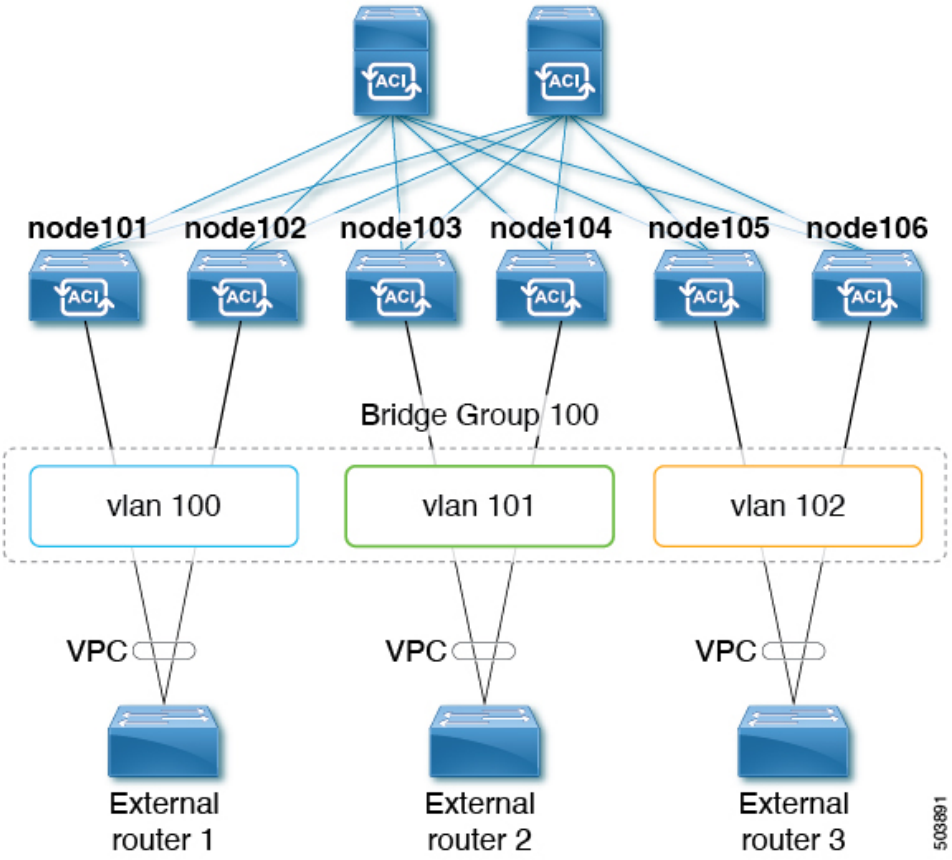
図 *39 :* 異なるカプセル化で外部ブリッジ ドメインに関連付けられた単一の *VNID*（*ACI 5.2(3)* 以降のリリース）。



ACI リリース 6.0(1) の時点で、この機能は物理ドメイン L3Out に対してのみサポートされ、VMM ドメイン L3Out に対してはサポートされません。

複数の SVI を異なるアクセスのカプセル化でグループ化する

次の図は、複数の SVI が異なるアクセス カプセル化でグループ化されている設定を示しています。



この使用ケースでは：

- 次のリーフ スイッチは VPC ペアです。
  - node101 および node102
  - node103 および node104
  - node105 および node106

複数の SVI をレイヤ 2 ブリッジ グループにグループ化する上記の使用例を設定します。

1. VPC ペアごとに 3 つの通常の SVI を作成します。
   - リーフ スイッチ node101 および node102 に通常の SVI **svi-100** を作成します。
   - リーフ スイッチ node103 および node104 に通常の SVI **svi-101** を作成します。
   - リーフ スイッチ node105 および node106 に通常の SVI **svi-102** を作成します。
2. リーフ スイッチをアクセス カプセル化に構成します。
   - アクセス カプセル化 **vlan100** を使用してリーフ スイッチ node101 および node102 を設定します。

- アクセス カプセル化 **vlan101** でリーフ スイッチ node103 および node104 を設定します。
- アクセス カプセル化 **vlan102** を使用してリーフ スイッチ node105 および node106 を設定します。

3. 通常の SVI **svi-100**、**svi-101**、および **svi-102** をグループ化して、単一のレイヤ 2 ブロードキャスト ドメインの一部として動作させます。
   1. ブリッジ ドメイン プロファイルを作成します。

      ブリッジドメインプロファイルは、新しいMO l3extBdProfileで表されます。
   2. ブリッジ ドメイン プロファイルの一意の名前文字列を指定します。
   3. 同じブリッジ ドメイン プロファイルにグループ化する必要がある通常およびSVIのそれぞれを関連付けます。

      この関連付けには、*l3extBdProfileCont* と *l3extRsBdProfile* の 2 つの新しい MO を使用できます。

注意事項と制約事項

- レイヤ 2 ループは、外部デバイス/ハイパーバイザによってブロックされます。ループを防止するためにスパニングツリープロトコルに依存する外部スイッチでこの機能を使用すると、ループが発生する可能性があります。
- SVI は、外部ブリッジ ドメイン プロファイルの設定後に削除され、再度追加されます。
- 外部ブリッジドメインプロファイルはL3Outスコープです。ノードでは、同じ外部ブリッジ ドメイン プロファイルに 2 つの異なるアクセス カプセル化マッピングを設定することはできません。
- ブリッジ ドメインのグループ化は、カプセル化スコープ **ctx**（APIC GUI の **VRF** オプション）ではサポートされていません。
- 異なる回線カプセル化を持つグループ化された SVI は、共通ノードを共有できません。
- リリース 5.2(3) から SVI による L3Out の複数のカプセル化がサポートされていない以前のリリースにダウングレードする場合、複数のカプセル化や外部ブリッジドメインプロファイルで設定された L3Out で次のアクションが実行されます。
  - 複数のカプセル化サポートに使用される新しいアロケータ（*l3extBdProfileEncapAllocator*）が削除されます。
  - すべての外部ブリッジ ドメイン プロファイル（新しい *l3extBdProfile* MO）が削除されます。
  - すべての新しい *l3extBdProfileCont* MO が削除されます。
  - すべての新しい *l3extRsBdProfile* MOが削除されます。

GUI を使用して SVI で複数の L3Out のカプセル化を設定する

手順

ステップ 1 通常の SVI を作成し、リーフ スイッチをカプセル化にアクセスして構成します。

これらの手順については、GUI を使用して SVI 外部カプセル化の範囲の設定 （305 ページ） を参照してください。

ステップ 2 SVI グループ化に使用される外部ブリッジ グループ プロファイルを作成します。

a) **[テナント（Tenants）]** > ***[tenant-name]*** > **[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[外部ブリッジ グループ プロファイル（External Bridge Group Profiles）]** に移動します。
設定済みの外部ブリッジ グループ プロファイルを示すページが表示されます。

b) [外部ブリッジ グループ プロファイル（External Bridge Group Profiles）] を右クリックし、[外部ブリッジ グループ プロファイルの作成（Create External Bridge Group Profile）] を選択します。
[外部ブリッジ グループ プロファイルの作成（Create External Bridge Group Profile）] ページが表示されます。

c) 外部ブリッジ グループ プロファイルの名前を入力し、[**送信（Submit）**] をクリックします。
すでに設定されている外部ブリッジ グループ プロファイルを示すページが、新しい外部ブリッジ グループ プロファイルで更新されます。

ステップ 3 通常の SVI をブリッジ ドメイン プロファイルに関連付けます。

a) **[テナント（Tenants）]** > ***[tenant-name]*** > **[ネットワーキング（Networking）]** > **[L3Outs]** > ***[L3Out-name]*** > **[論理ノード プロファイル（Logical Node Profile）** > ***[log-node-profile-name]*** > **[論理インターフェイス プロファイル（Logical Interface Profile）]** > ***[log-int-profile-name]*** に移動します。
この論理インターフェイス プロファイルの [**全般（General）**] ページが表示されます。

b) [SVI] タブをクリックします。
設定済みのスイッチ仮想インターフェイスを示すページが表示されます。

c) 外部ブリッジドメインプロファイルに関連付けるスイッチ仮想インターフェイスをダブルクリックします。
このスイッチ仮想インターフェイスの一般情報が表示されます。

d) [**外部ブリッジ グループ プロファイル（External Bridge Group Profile**）] フィールドで、このスイッチ仮想インターフェイスに関連付ける外部ブリッジ ドメイン プロファイルを選択します。

e) [Submit] をクリックします。

CLI を使用して SVI で複数の L3Out のカプセル化を設定する

手順

ステップ 1 通常の SVI を作成し、リーフ スイッチをカプセル化にアクセスして構成します。

これらの手順については、NX-OS スタイル CLI を使用して、SVI インターフェイスのカプセル化スコープの設定 （537 ページ） を参照してください。

ステップ 2 CLI を使用して APIC にログインし、コンフィギュレーション モードとテナント コンフィギュレーション モードを開始します。

```
apic1#
apic1# configuration
apic1(config)# tenant <tenant-name>
apic1(config-tenant)#
```

ステップ 3 次のコマンドを入力して、SVI グループ化に使用する外部ブリッジ プロファイルを作成します。

```
apic1(config-tenant)# external-bridge-profile <bridge-profile-name>
apic1(config-tenant-external-bridge-profile)# ?
```

ステップ 4 次のコマンドを入力して、通常の SVI をブリッジ ドメイン プロファイルに関連付けます。

```
apic1(config)# leaf <leaf-ID>
apic1(config-leaf)# interface vlan <vlan-num>
apic1(config-leaf-if)# vrf member tenant <tenant-name> vrf <VRF-name>
apic1(config-leaf-if)# ip address <IP-address>
apic1(config-leaf-if)# external-bridge-profile <bridge-profile-name>
```

REST API を使用した複数の SVI 付き L3Out のカプセル化の設定

手順

ステップ 1 通常の SVI を作成し、リーフ スイッチをカプセル化にアクセスして構成します。

これらの手順については、REST API を使用して、SVI インターフェイスのカプセル化スコープの設定 （622 ページ） を参照してください。

ステップ 2 次の例のような投稿を入力して、SVI グループ化に使用する外部ブリッジプロファイルを作成します。

```
<fvTenant name="t1" dn="uni/tn-t1" >
```

```
    <l3extBdProfile name="bd100" status=""/>
</fvTenant>
```

ステップ 3 次の例のように投稿を入力して、通常の SVI をブリッジ ドメイン プロファイルに関連付けます。

```
<fvTenant name="t1">
    <l3extOut name="l1">
        <l3extLNodeP name="n1">
            <l3extLIfP name="i1">
                <l3extRsPathL3OutAtt encap="vlan-108"
                    tDn="topology/pod-1/paths-108/pathep-[eth1/10]"
                    ifInstT="ext-svi">
                    <l3extBdProfileCont>
                        <l3extRsBdProfile tDn="uni/tn-t1/bdprofile-bd100" status=""/
                    </l3extBdProfileCont>
                </l3extRsPathL3OutAtt>
            </l3extLIfP>
        </l3extLNodeP>
    </l3extOut>
</fvTenant>
```

ステップ 4 フローティング ノードの個別のカプセル化を指定するには、次の例のような投稿を入力します。

```
<fvTenant name="t1">
    <l3extOut name="l1">
        <l3extLNodeP name="n1">
            <l3extLIfP name="i1">
                <l3extVirtualLIfP addr="10.1.0.1/24"
                    encap="vlan-100"
                    nodeDn="topology/pod-1/node-101"
                    ifInstT="ext-svi">
                    <l3extRsDynPathAtt floatingAddr="10.1.0.100/24"
                        encap="vlan-104"
                        tDn="uni/phys-phyDom"/>
                </l3extVirtualLIfP>
            </l3extLIfP>
    </l3extOut>
</fvTenant>
```

SVI 自動状態

SVI 自動状態について

（注） この機能は、APIC リリース 2.2(3x) リリースおよび APIC リリース 3.1 (1) で使用できます。APIC リリース 3.0(x) ではサポートされていません。

スイッチ仮想インターフェイス（SVI）は、デバイスの VLAN のブリッジング機能とルーティング機能間の論理インターフェイスを表します。SVIは、物理ポート、直接ポート チャネル、

仮想ポートチャネルのメンバーを有することができます。SVI論理インターフェイスはVLANに関連付けられ、VLAN ポート メンバーシップを有します。

SVI の状態はメンバーに依存しません。Cisco APIC の SVI のデフォルトの自動状態動作は、自動状態の値が無効になっているときに最新の状態になっていることを意味します。これは、インターフェイスが対応するVLANで動作していない場合、SVIがアクティブであることを意味します。

SVI 自動状態の値を有効に変更する場合、関連する VLAN のポート メンバーに依存します。VLANインターフェイスがVLANで複数のポートを有する場合、SVIはVLANのすべてのポートがダウンするとダウン状態になります。

表 *12 : SVI* 自動状態

SVI 自動状態	SVI 状態の説明
ディセーブル	インターフェイスが対応する VLAN で動作していない場合、SVI がアップ状態であることを意味します。 無効がデフォルトの SVI 自動状態の値です。
イネーブル	SVI は、関連付けられている VLAN のポート メンバによって異なります。VLAN インターフェイスに複数のポートを含む場合、SVIはVLANのすべてのポートがダウンするとダウン状態になります。

SVI 自動状態の動作のガイドラインと制限事項

次のガイドラインをお読みください。

- SVI の自動状態の動作を有効化または無効化にすると、SVI あたりの自動状態の動作を設定します。これらはグローバル コマンドではありません。

GUI を使用した SVI 自動状態の設定

始める前に

- テナントと VRF が設定されています。
- L3Outが設定されており、L3Outの論理ノードプロファイルと論理インターフェイス プロファイルが設定されています。

手順

ステップ 1 メニュー バーで、 > **Tenants** > ***Tenant_name*** をクリックします。

ステップ 2 [ナビゲーション（Navigation）]ペインで、[ネットワーキング（Networking）] [L3Outs] [L3Out_name] [論理ノードプロファイル）Logical Node Profiles] [LogicalNodeProfile_name] [論理インターフェイスプロファイル（Logical Interface Profiles）]をクリックします。 > > > > >

ステップ 3 **Navigation** ウィンドウで、**Logical Interface Profile** を展開し、適切な論理インターフェイス プロファイルをクリックします。

ステップ 4 [作業（**Work**）] ペインで、[+] 記号をクリックして [**SVI**] ダイアログボックスを表示します。

ステップ 5 付加的な SVI を追加するには、 **SVI** ダイアログボックスで、以下の手順を実行します:

a) **Path Type** フィールドで、適切なパス タイプを選択します。

b) **Path** フィールドで、ドロップダウンリストから適切な物理インターフェイスを選択します。

c) **Encap** フィールドで、適切な値を選択します。

d) **Auto State** フィールド (**Work** ウィンドウ) で SVI を選択し、自動状態を表示または変更します。

デフォルト値は **Disabled** です。

（注） 既存 SVI の自動状態の値を確認または変更するには、適切な SVI を選択して、値を確認または変更します。

Cisco フローティング L3Out について

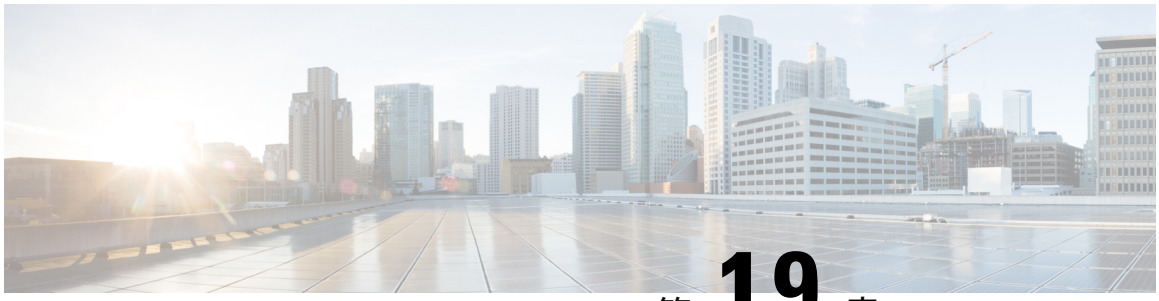
Cisco Application Policy Infrastructure Controller（APIC）リリース 4.2(1) 以降では、外部ネットワークデバイスに接続するための複数のレイヤ 3 外部ネットワーク接続（L3Out）論理インターフェイスパスを指定する必要がなくなりました。

このフローティング L3Out 機能を使用すると、論理インターフェイスを指定せずに L3Out を設定できます。この機能により、仮想マシン（特定の仮想ネットワーク機能を実行する）がホスト間を移動する際に、ルーティングを維持するために複数の L3Out 論理インターフェイスを設定する必要がなくなります。フローティング L3Out は、VMware vSphere 分散スイッチ（VDS）を持つ VMM ドメインでサポートされています。

Cisco APIC リリース 5.0(1) 以降のリリースでは、物理ドメインがサポートされています。これは、同じ単純化された構成を物理ルータの展開にも使用できることを意味します。

詳細については、「フローティング *L3Out* を使用して外部ネットワーク接続を簡素化する」のナレッジベース記事を参照してください。

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/Cisco-ACI-Floating-L3Out.html



第 19 章

ルーティング プロトコルのサポート

この章は、次の内容で構成されています。

ルーティング プロトコルのサポートについて

Cisco ACIファブリック内のルーティングは、BGP（BFDサポート）およびOSPFまたはEIGRPルーティング プロトコルを使用して実装されます。

IP 送信元ルーティングは ACI ファブリックではサポートされません。

Cisco ACI の等コスト マルチパス ルーティングについて

Cisco Application Centric Infrastructure（ACI）では、境界リーフ スイッチに接続されているすべてのネクストホップは、ハードウェアで転送されるときに、1つの等コストマルチパス（ECMP）ルーティングパスと見なされます。Cisco ACI は、直接接続されたネクストホップの場合は ECMP パスを BGP に再配布しませんが、再帰的なネクストホップの場合は再配布します。

次の例では、ボーダー リーフ スイッチ1および2が、ネクストホップ伝播を使用して10.1.1.0/24ルートをアドバタイズし、接続されたホスト機能を再配布します。

```
10.1.1.0/24
    through 192.168.1.1 (border leaf switch 1) -> ECMP path 1
    through 192.168.1.2 (border leaf switch 1) -> ECMP path 1
    through 192.168.1.3 (border leaf switch 1) -> ECMP path 1
    through 192.168.1.4 (border leaf switch 2) -> ECMP path 2
```

- ECMP パス 1：50%（ネクストホップ 192.168.1.1、192.168.1.2、192.168.1.3）
- ECMP パス 2：50%（ネクストホップ 192.168.1.4）

（注） 各ネクストホップのトラフィック ハッシュのパーセンテージは概算値です。実際のパーセンテージは異なります。

非境界リーフ スイッチのこのルート エントリは、非境界リーフから各境界リーフ スイッチへの 2 つの ECMP パスになります。これにより、ルートをアドバタイズするボーダー リーフ スイッチ間でネクストホップが均等に分散されていない場合、ボーダー リーフ スイッチへのロード バランシングが不均衡になる可能性があります。

Cisco ACI リリース 6.0(2) 以降では、ネクストホップ伝播および接続ホスト機能の再配布を使用して、Cisco ACI ファブリック内の最適でないルーティングを回避できます。これらの機能が有効になっている場合、非境界リーフ スイッチからのパケット フローは、ネクストホップ アドレスに接続されているリーフ スイッチに直接転送されます。すべてのネクストホップがハードウェアからの ECMP 転送に使用されるようになりました。さらに、Cisco ACI は、直接接続されたネクストホップと再帰ネクストホップの両方の ECMP パスを BGP に再配布するようになりました。

次の例では、リーフ スイッチ 1 と 2 がネクストホップで 10.1.1.0/24 ルートをアドバタイズし、接続されたホスト機能を再配布します。

```
10.1.1.0/24
    through 192.168.1.1 (border leaf switch 1) -> ECMP path 1
    through 192.168.1.2 (border leaf switch 1) -> ECMP path 2
    through 192.168.1.3 (border leaf switch 1) -> ECMP path 3
    through 192.168.1.4 (border leaf switch 2) -> ECMP path 4
```

- ECMP パス 1：25%（ネクストホップ 192.168.1.1）
- ECMP パス 2：25%（ネクストホップ 192.168.1.2）
- ECMP パス 3：25%（ネクストホップ 192.168.1.3）
- ECMP パス 4：25%（ネクストホップ 192.168.1.4）

BGP 外部ルーテッド ネットワークと BFD のサポート

ここでは、BFD をサポートする BGP 外部ルーテッド ネットワークの詳細について説明します。

BGP レイヤ 3 外部ネットワーク接続設定のガイドライン

BGP外部ルーテッドネットワークを設定するときは、以下のガイドラインに従ってください。

- BGP 直接ルート エクスポートの動作は、リリース 3.2(1) 以降に変更されました。この場合 ACI は、エクスポート ルート マップ節を照合するときに、発信元ルート タイプ（スタティック、ダイレクトなど）を評価しません。その結果、アウトバウンド ネイバー ルート マップに常に含まれる「match direct」deny 節は、直接ルートと一致しなくなり、ユー

ザ定義のルートマップ節が一致するかどうかに基づいて直接ルートがアドバタイズされるようになりました。

したがって、直接ルートはルートマップを介して明示的にアドバタイズする必要があります。そうしないと、アドバタイズされている直接ルートが暗黙的に拒否されます。

- L3Out の BGP ピア接続プロファイルの [BGP 制御（BGP Controls）] フィールドの [AS オーバーライド（AS override）] オプションは、リリース 3.1(2) で導入されました。これにより、Cisco Application Centric Infrastructure（ACI）は AS_PATH 内のリモート AS を ACI BGP AS で上書きできます。Cisco ACI において、これは通常、eBGP L3Out から同じ AS 番号を持つ別の eBGP L3Out への中継ルーティングを実行するときに使用されます。

  ただし、eBGP ネイバーの AS 番号が異なる場合に [AS オーバーライド（AS override）] オプションを有効にすると、問題が発生します。この状況では、ピアに反映するときに AS_PATH から peer-as を削除します。

- BGP ピア接続プロファイルの **[ローカル AS 番号（Local-AS Number）]**オプションは、eBGP ピアリングでのみサポートされます。これにより、Cisco ACI ボーダー リーフ スイッチは、ファブリック MP-BGP ルート リフレクタ ポリシーに割り当てられた実際の AS に加えて、別の AS のメンバーであるように見えます。そのため、ローカル AS 番号は Cisco ACI ファブリックの実際の AS 番号とは異なる必要があります。この機能が構成されている場合、Cisco ACI ボーダー リーフ スイッチは、ローカル AS 番号を着信更新の AS_PATH に付加し、同じ番号を発信更新の AS_PATH に付加します。**[ローカル AS 番号構成（Local-AS Number Config）]** の **no-prepend** 設定によって、ローカル AS 番号の着信更新への付加を無効にできます。**no-prepend + replace-as** 設定を使用すると、ローカル AS 番号が発信更新に付加されるのを防ぐことができます。

- ルーティング プロトコルの L3Out のルーター ID は、ルーテッド インターフェイス、サブインターフェイス、SVI などの L3Out インターフェイスと同じ IP アドレスまたは同じサブネットにすることはできません。ただし、必要に応じて、ルータ ID を L3Out ループバック IP アドレスの 1 つと同じにすることができます。

- 同じ VRF インスタンスの同じリーフ スイッチに同じルーティング プロトコルの複数の L3Out がある場合、それらのルータ ID は同じである必要があります。ルータ ID と同じ IP アドレスを持つループバックが必要な場合は、それらの L3Out の 1 つだけにループバックを構成できます。

- L3Out の BGP ピアを定義するには、次の 2 つの方法があります。

  - ループバック IP アドレスに BGP ピアを関連付ける論理ノード プロファイル レベル（l3extLNodeP）のBGPピア接続プロファイル（bgpPeerP）を介した方法。BGP ピアがこのレベルで設定されている場合は、BGP 接続にループバック アドレスが想定されます。そのため、ループバック アドレス設定が欠落していると、障害が発生します。

  - BGP ピアをそれぞれのインターフェイスまたはサブインターフェイスに関連付け、論理インターフェイス プロファイル レベル（l3extRsPathL3OutAtt）で BGP ピア接続プロファイル（bgpPeerP）を介した方法。

- IPv6 を使用したループバックを介したピアリングを有効にするには、ユーザーが IPv6 アドレスを構成する必要があります。
- BGP `l3extOut` 接続のテナント ネットワーキング プロトコル ポリシーは、最大プレフィックス制限を使用して構成できます。これにより、ピアから受信するルートプレフィックスの数をモニタし、制限することができます。最大プレフィックス制限を超えると、ログエントリの記録、それ以降のプレフィックスの拒否、固定期間中にカウントがしきい値未満になった場合の接続の再起動、または接続のシャットダウンを行うことができます。一度に 1 つのオプションだけを使用できます。デフォルト設定では 20,000 プレフィックスに制限され、その後は新しいプレフィックスは拒否されます。拒否オプションを展開すると、BGP は設定されている制限よりも 1 つ多くプレフィックスを受け入れるようになり、Cisco Application Policy Infrastructure Controller（APIC）はエラーを発生させます。

（注） Cisco ACI は IP フラグメンテーションをサポートしていません。したがって、外部ルータへのレイヤ 3 Outside（L3Out）接続、または Inter-Pod Network（IPN）を介した マルチポッド 接続を設定する場合は、インターフェイス MTU がリンクの両端で適切に設定されていることが推奨されます。Cisco ACI、 Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定可能な MTU 値はイーサネット ヘッダー (一致する IP MTU、14-18 イーサネット ヘッダー サイズを除く) を考慮していません。また、IOS XR などの他のプラットフォームには、設定された MTU 値にイーサネットヘッダーが含まれています。設定された値が 9000 の場合、Cisco ACI、Cisco NX-OS Cisco IOS の最大 IP パケット サイズは 9000 バイトになりますが、IOS-XR のタグなしインターフェイスの最大 IP パケットサイズは 8986 バイトになります。

各プラットフォームの適切な MTU 値については、それぞれの設定ガイドを参照してください。

CLI ベースのコマンドを使用して MTU をテストすることを強く推奨します。たとえば、Cisco NX-OS CLI で `ping 1.1.1.1 df-bit packet-size 9000 source-interface ethernet 1/1` などのコマンドを使用します。

BGP の接続タイプとループバックのガイドライン

ACI では次の BGP 接続の種類をサポートし、それらのループバックのガイドラインをまとめています。

BGP 接続タイプ	ループバックが必要	ルータ ID と同じループバック	スタティック ルートまたは OSPF ルートが必要
直接 iBGP	非対応	N/A	非対応

BGP 接続タイプ	ループバックが必要	ルータ ID と同じループバック	スタティック ルートまたは OSPF ルートが必要
iBGP ループバック ピアリング	はい（L3Out ごとに個別のループバック）	いいえ（同じノードに複数のレイヤ 3 Out がある場合）	はい
直接 eBGP	非対応	N/A	非対応
eBGP ループバック ピアリング（マルチホップ）	はい（L3Out ごとに個別のループバック）	いいえ（同じノードに複数のレイヤ 3 Out がある場合）	対応

外部 BGP スピーカーに対する BGP プロトコル ピアリング

ACI は、iBGP と eBGP を使用して境界リーフと外部 BGP スピーカーの間のピアリングをサポートします。ACI は、BGP ピアリングで以下の接続をサポートします。

- OSPF 上の iBGP ピアリング
- OSPF 上の eBGP ピアリング
- 直接接続上の iBGP ピアリング
- 直接接続上の eBGP ピアリング
- スタティック ルート上の iBGP ピアリング

（注） BGP ピアリングで OSPF が使用される場合、OSPF は BGP ピアリング アドレスへのルートの学習とアドバタイズのみに使用されます。レイヤ 3 Outside ネットワーク（EPG）に適用されるすべてのルート制御が BGP プロトコル レベルで適用されます。

ACI は、外部ピアへの iBGP および eBGP 接続用に多数の機能をサポートします。BGP 機能は、[BGP Peer Connectivity Profile] で設定されます。

BGP ピアの接続プロファイル機能について、次の表で説明します。

（注） ACI は、次の BGP 機能をサポートしています。以下にリストされていない NX-OS BGP 機能は、現在 ACI ではサポートされていません。

表 *13 : BGP* ピアの接続プロファイル機能

BGP 機能	機能の説明	NX-OS での同等のコマンド
Allow Self-AS	Allowed AS Number Count 設定と併用されます。	**allowas-in**
Disable peer AS check	アドバタイズ時のピア AS 番号のチェックを無効にします。	**disable-peer-as-check**
Next-hop self	常にローカル ピア アドレスにネクスト ホップ属性を設定します。	**next-hop-self**
Send community	ネイバーにコミュニティ属性を送信します。	**send-community**
Send community extended	ネイバーに拡張コミュニティ属性を送信します。	**send-community extended**
Password	BGP MD5 認証。	**password**
Allowed AS Number Count	Allow Self-AS 機能と併用されます。	**allowas-in**
Disable connected check	直接接続された EBGP ネイバーの接続チェックを無効にします（EBGP ネイバーがループバックからピアリングすることを許可）。	
TTL	EBGP マルチホップ接続の TTL 値を設定します。これは EBGP でのみ有効です。	**ebgp-multihop <TTL>**
Autonomous System Number	ピアのリモート自律システム番号。	**neighbor <x.x.x.x> remote-as**
Local Autonomous System Number Configuration	ローカル AS 機能を使用するときのオプション（No Prepend+replace-AS+dual-AS など）。	

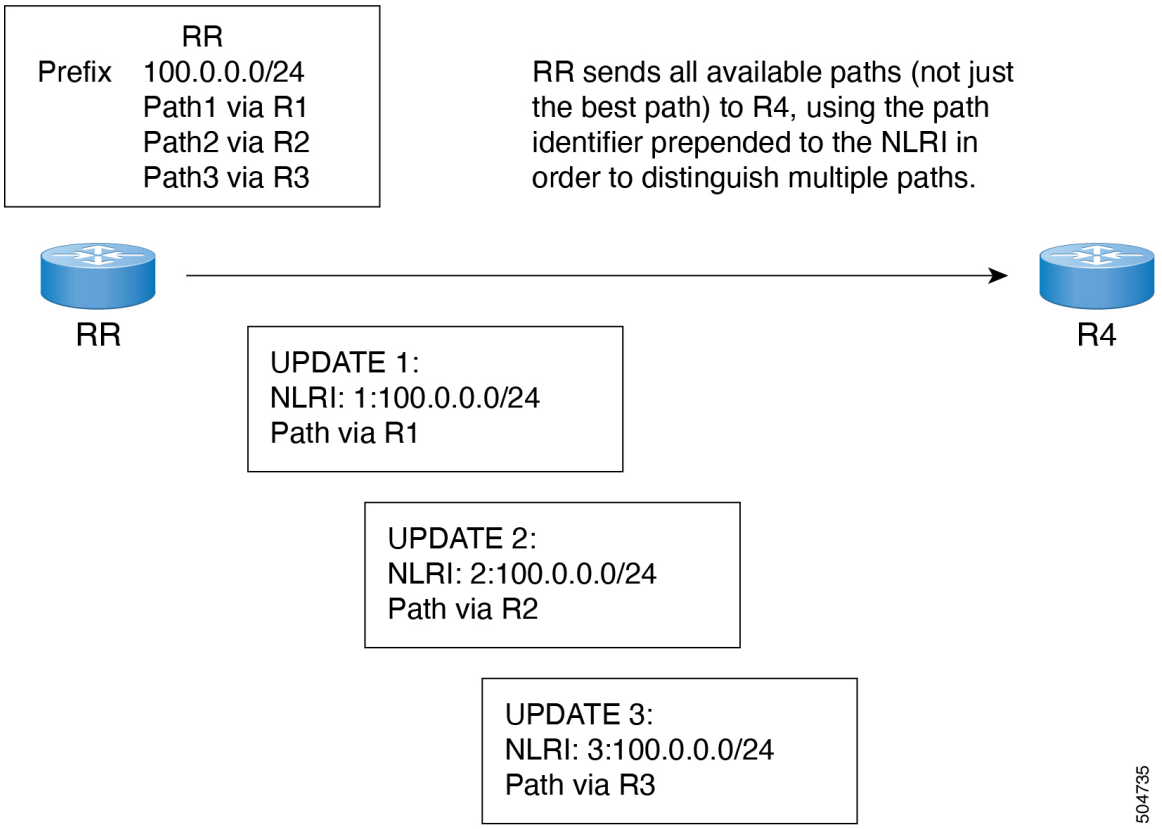
BGP 機能	機能の説明	NX-OS での同等のコマンド
Local Autonomous System Number	ファブリック MP-BGP ルート リフレクタ プロファイルに割り当てられている AS とは異なる AS 番号をアドバタイズするために使用されるローカル AS 機能。これは EBGP ネイバーの場合にのみサポートされ、ローカル AS 番号がルート リフレクタ ポリシー AS と異なっている必要があります。	**local-as xxx <no-prepend> <replace-as> <dual-as>**
Site of Origin	site-of-origin（SoO）は、ルーティング ループを防ぐためにルートを学習するサイトを一意に識別するために使用される BGP 拡張コミュニティ属性です。	**soo<value>**

BGP 付加パス

Cisco Application Policy Infrastructure Controller（APIC）6.0(2) リリース以降、BGP は、以前のパスに代わる新しいパスなしで、BGP スピーカが同じプレフィックスに対して複数のパスを伝播し、受け入れることを可能にする追加のパス機能をサポートします。この機能は、BGP スピーカのピアが、プレフィックスごとの複数パスのアドバタイズおよび受信をサポートし、また、そのパスのアドバタイズをサポートするかどうかネゴシエートすることを可能にします。特別な 4 バイトのパス ID は、ピア セッションを介して送信される同じプレフィックスに対して複数のパスを区別するため、ネットワーク層到達可能性情報（NLRI）に追加されます。

次の図に、追加の BGP 追加パス受信機能を示します。

図 *40 :* 追加パスの機能を持つ *BGP* ルート アドバタイズメント



次の制限が適用されます。

- Cisco APIC は受信機能のみをサポートします。
- セッションの確立後に BGP 追加パス受信機能を設定すると、その設定は次のセッション フラップで有効になります。

追加パス受信機能が導入される前は、BGP は 1 つのパスだけをアドバタイズし、BGP スピーカは特定ピアからの特定プレフィックスの1パスだけを受け入れました。BGPスピーカが同じセッション内で同じプレフィックスの複数のパスを受信した場合、最新のアドバタイズメントが使用されました。

BGP 外部ルーテッド ネットワークの設定

BGP 外部ルーテッド ネットワークを設定するには、次の項の手順を使用します。

GUI を使用した BGP L3Out の設定

始める前に

BGP L3Out を設定するテナント、VRF、およびブリッジ ドメインはすでに作成されており、VRF の作成時に [BGP ポリシーの設定（Configure BGP Policies）] オプションを選択しました。

手順

ステップ 1 **[メニュー（Menu）]** バーで、**[テナント（Tenants）]** > **[すべてのテナント（All Tenants）]**を選択します。

ステップ 2 作業ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 [**ナビゲーション（Navigation**）] ペインで、**[*Tenant_name*]** > **[ネットワーキング（Networking）]** > **[L3Outs]** の順に展開します。

ステップ 4 [L3Outs] を右クリックし、[L3Out の作成（Create L3Out）] を選択します。

[**L3Out の作成（Create L3Out**）] ウィザードが表示されます。

ステップ 5 **[L3Out の作成（Create L3Out）]** ウィザードの **[識別（Identity）]** ページに必要な情報を入力します。

a) [名前（Name）]、[VRF]、および [L3 ドメイン（L3 Domain）] フィールドに必要な情報を入力します。
b) ルーティング プロトコルのチェック ボックスがある領域で、[BGP] を選択します。
c) [**次（Next**）] をクリックして [**ノードとインターフェイス（Nodes and Interfaces**）] ウィンドウに移動します。

ステップ 6 **[L3Out の作成（Create L3Out）]** ウィザードの **[ノードとインターフェイス（Nodes and Interfaces）]** ページに必要な情報を入力します。

a) [レイヤ 3（Layer 3）] 領域で、[ルーテッド（Routed）] を選択します。
b) [**ノード ID**（**Node ID**）] フィールドのドロップダウン メニューで、L3Out のノードを選択します。

これらの例のトポロジでは、ノード `103` を使用します。

c) [Router ID] フィールドに、ルータ ID を入力します。
d) （任意） 必要に応じて、ループバック アドレスに別の IP アドレスを設定できます。

[ルータ ID（Router ID）] フィールドに入力したエントリと同じ内容が [ループバック アドレス（Loopback Address）] フィールドに自動で入力されます。これは以前のビルドでの [ループバック アドレスのルータ ID の使用（Use Router ID for Loopback Address）] と同等です。ループバック アドレスにルータ ID を使用しない場合は、ループバック アドレスに別の IP アドレスを入力します。または、ループバック アドレスにルータ ID を使用しない場合は、このフィールドを空のままにします。

e) **[ノードとインターフェイス（Nodes and Interfaces）]** ページに追加の必要な情報を入力します。

このページに表示されるフィールドは、**[レイヤ 3（Layer 3）]** および **[レイヤ 2（Layer 2）]** 領域で選択したオプションによって異なります。

f) **[ノードとインターフェイス（Nodes and Interfaces）]** ページで残りの追加の情報を入力したら、**[次へ（Next）]** をクリックします。

[プロトコル（Protocol）] ページが表示されます。

ステップ 7 **[L3Out の作成（Create L3Out）]** ウィザードの **[プロトコル（Protocols）]** ページに必要な情報を入力します。

a) [BGP ループバック ポリシー（BGP Loopback Policies）] および [BGP インターフェイス ポリシー（BGP Interface Policies）] 領域で、次の情報を入力します。

- **ピア アドレス（Peer Address）**：ピア IP アドレスを入力します
- **EBGP Multihop TTL（EBGP マルチホップ TTL）**：接続の存続可能時間（TTL）を入力します。範囲は 1 ー 255 ホップです。ゼロの場合、TTL は指定されません。デフォルトは 1 です。
- **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。

（注） ACI は asdot または asdot + 形式の AS 番号をサポートしていません。

b) **[次へ（Next）]** をクリックします。

[外部タスク（External Tasks）] ページが表示されます。

ステップ 8 **[L3Out の作成（Create L3Out）]** ウィザードで **[外部 EPG（External EPG）]** ページに必要な情報を入力します。

a) **Name** フィールドに、外部ネットワークの名前を入力します。
b) **[提供済みコントラクト（Provided Contract）]** フィールドで、提供済みコントラクトの名前を入力します。
c) **[消費済みコントラクト（Consumed Contract）]** フィールドで、消費済みコントラクトの名前を入力します。
d) [すべての外部ネットワークのデフォルト EPG（Default EPG for all external network）] フィールドで、この L3Out 接続からのすべての中継ルートをアドバタイズしない場合はオフにします。

このボックスをオフにすると、[Subnets] 領域が表示されます。次の手順に従って、必要なサブネットとコントロールを指定します。

e) [+] アイコンをクリックして [サブネット（Subnet）] を展開し、[サブネットの作成（Create Subnet）] ダイアログ ボックスで次の操作を実行します。
f) **IP address** フィールドに、外部ネットワークの IP アドレスとサブネット マスクを入力します。

（注） 前のステップで入力した内容に応じて、IPv4 または IPv6 のアドレスを入力します。

外部サブネットを作成するときに、プレフィックス EPG の BGP ループバックの両方を設定するか、またはどちらも設定しない必要があります。BGP ループバックを 1 つのみ設定すると、BGP ネイバーシップは確立されません。

g) [名前（**Name**）] フィールドに、サブネットの名前を入力します。

h) [Scope] フィールドで、[Export Route Control Subnet] 、[Import Route Control Subnet] 、および [Security Import Subnet] のチェックボックスをオンにします。[OK] をクリックします。

（注） BGP でインポート制御を適用する場合は、[Import Route Control Subnet] チェックボックスをオンにします。

i) [サブネットの作成（Create Subnet）] ウィンドウで必要な設定が完了したら、[OK] をクリックします。

j) [完了（Finish）] をクリックして、[L3Out の作成（Create L3Out）] ウィザードに必要な設定の入力を完了させます。

ステップ 9 （任意） 必要に応じて、[BGP ピア接続プロファイル（BGP Peer Connectivity Profile）] ウィンドウに移動して、BGP 外部ルーテッドネットワークの追加設定を行います。

[テナント（Tenants）] > [*tenant_name*] > [ネットワーキング（Networking）] > [L3Outs] > [*L3Out_name*] > [論理ノード プロファイル（Logical Node Profiles）] > [*log_node_prof_name*] > [BGP ピア（BGP Peer）*] <address>*

この L3Out の **[BGP ピア接続プロファイル（BGP Peer Connectivity Profile）]** ページが表示されます。

a) [BGP Controls] フィールドで、目的の制御をオンにします。

ピアは、ピアに送信される境界ゲートウェイ プロトコル（BGP）属性を指定します。ピア制御オプションは次のとおりです。

- **[自身の AS を許可（Allow Self AS）]**：自律番号チェックを自身で有効にします。これにより、同じ AS 番号が使用されている場合に BGP ピアが更新を挿入できます。
- **[AS オーバーライド（AS override）]**：BGP AS オーバーライド機能を有効にして、デフォルト設定をオーバーライドします。AS オーバーライド機能では、発信元のルータからの AS 番号を、アウトバウンド ルートの AS パスの BGP ルータ送信の AS 番号に置き換えます。アドレス ファミリごとにこの機能を有効にできます（IPv4 または IPv6）。

  AS オーバーライド機能を有効にするには、[ピア AS チェックを無効化（Disable Peer AS Check）] チェックボックスもオンにする必要があります。

- **[ピア AS チェックを無効化（Disable Peer AS Check）]**：ピア自律番号チェックを無効にします。このチェックボックスをオンにすると、アドバタイジング ルータが AS パスでレシーバの AS 番号を見つけた場合、そのルータはレシーバにルートを送信しません。

AS オーバーライド機能を有効にするには、[ピア AS チェックを無効化（Disable Peer AS Check）] チェックボックスをオンにする必要があります。

- **[自身にネクスト ホップを送信（Next-hop Self）]**：BGP ネクスト ホップ属性を自身に送信します。
- **[コミュニティの送信（Send Community）]**：ピアに BGP コミュニティ属性を送信します。
- **[拡張コミュニティの送信（Send Extended Community）]**：ピアに BGP 拡張コミュニティ属性を送信します。
- **[ドメイン パスの送信（Send Domain Path）]**：BGP ドメイン パスをピアに送信します。

b) **[追加パスの受信（Receive Additional Paths）]** チェックボックスをオンにして、この eBGP L3Out ピアが他の eBGP ピアからプレフィックスごとに追加のパスを受信できるようにします。

[追加パスの受信（Receive Additional Paths）] 機能がない場合、eBGP では、リーフ スイッチがプレフィックスのピアからネクスト ホップを 1 つだけ受信できます。

または、他の eBGP ピアからプレフィックスごとに追加のパスを受信するように、テナントの VRF インスタンス内のすべての eBGP ピアを設定できます。詳細については、GUI を使用した BGP Max Path の設定 （330 ページ）を参照してください。

c) [パスワード（Password）] フィールドと [パスワードの確認（Confirm Password）] フィールドに、管理パスワードを入力します。

d) [自身の AS 番号カウントを許可（Allow Self AS Number Count）] フィールドで、ローカル自律システム番号（ASN）の許可される発生回数を選択します。

値の範囲は 1 ～ 10 です。デフォルトは 3 です。

e) [ピア制御（Peer Controls）] フィールドに、ネイバー チェック パラメータを入力します。

次のオプションがあります。

- **[双方向フォワーディングの検出（Bidirectional Forwarding Detection）]**：ピアの BFD を有効にします。
- **[接続チェックの無効化（Disable Connected Check）]**：ピア接続のチェックを無効にします。

f) [アドレス タイプ制御（Address Type Controls）] フィールドで、必要に応じて BGP IPv4/IPv6 アドレスファミリ機能を設定します。

- [AF Mcast]：マルチキャスト アドレスファミリ機能を有効にする場合にオンにします。
- [AF Ucast]：ユニキャスト アドレスファミリ機能が有効にする場合にオンにします。

g) 必要に応じて、[ルーティング ドメイン ID（Routing Domain ID）] のエントリをメモします。

[ルーティング ドメイン ID（Routing Domain ID）] フィールドの値は、[BGP ルート リフレクタ ポリシー（BGP Route Reflector Policy）] ページに入力されたグローバル ドメイン ID ベース値を反映します。詳細については、「ループ防止のための BGP ドメインパス機能について （237 ページ）」を参照してください。

h) [EBGP マルチホップ TTL（EBGP Multihop TTL）] フィールドに、接続存続可能時間（TTL）を入力します。

範囲は 1 ー 255 ホップです。ゼロの場合、TTL は指定されません。デフォルトは 1 です。

i) [このネイバーからのルートの重み付け（Weight for routes from this neighbor）] フィールドで、ピアからのルートに許可される重みを選択します。

ルータにローカルに割り当てられた重みが、最適パスの選択に使用されます。範囲は 0 ～ 65535 です。

j) [プライベート AS 制御（Private AS Control）] フィールドで、プライベート AS 制御を設定します。

これらのオプションは、ACI BGP AS がパブリック AS 番号である場合、または [no-Prepend+replace-as] オプションを指定した [Local-AS 番号設定（Local-AS Number Config）] が、指定された BGP ピア接続プロファイル（BGP ネイバー コンフィギュレーション）。[プライベート AS 制御（Private AS Control）] 機能は自身のローカル プライベート AS を削除しないため、[replace-as] オプションを使用して、実際のローカル プライベート AS を AS_PATH から削除します。

次のオプションがあります。

- **[すべてのプライベート AS の削除（Remove all private AS）]**：発信 eBGP ルート更新ではこのネイバーを更新する際に、AS_PATH からすべてのプライベート AS 番号を削除します。eBGP ルートにプライベート AS 番号とパブリック AS 番号がある場合は、このオプションを使用します。パブリック AS 番号は保持されます。

  ネイバーのリモート AS が AS_PATH にある場合、このオプションは適用されません。

  このオプションを有効にするには、[プライベート AS の削除（Remove private AS）] を有効にする必要があります。

- **[プライベート AS の削除（Remove private AS）]**：このネイバーへの発信 eBGP ルート更新では、AS_PATH にプライベート AS 番号しかない場合、このオプションはすべてのプライベート AS 番号を削除します。eBGP ルートにプライベート AS 番号のみがある場合は、このオプションを使用します。

  ネイバーのリモート AS が AS_PATH にある場合、このオプションは適用されません。

- **[プライベート AS をローカル AS と置換（Replace private AS with local AS）]**：このネイバーへの発信 eBGP ルート更新では、このオプションは、パブリック AS またはネイバー リモート AS が AS_PATH に含まれているかどうかに関係なく、AS_PATH 内のすべてのプライベート AS 番号を ACI ローカル AS に置き換えます。

  このオプションを有効にするには、[すべてのプライベート AS を削除（Remove all private AS）] を有効にする必要があります。

k) [BGP ピア プレフィックス ポリシー（BGP Peer Prefix Policy）] フィールドで、既存のピア プレフィックス ポリシーを選択するか、新しいポリシーを作成します。

ピア プレフィックス ポリシーは、ネイバーから受信できるプレフィックスの数と、許可されるプレフィックスの数を超えた場合に実行するアクションを定義します。この機能は、外部 BGP ピアで一般的に使用されますが、内部 BGP ピアにも適用できます。

l) [Site of Origin] フィールドに、このピアを識別するための拡張コミュニティ値を入力します。

Site-of-Origin（SoO）拡張コミュニティは、サイトを発信元とするルートを識別し、そのプレフィックスの再アドバタイズメントが送信元のサイトに戻されることを防ぐために使用される BGP 拡張コミュニティ属性です。この SoO 拡張コミュニティは、ルータがルートを学んだサイトを一意に識別します。BGP は、ルートに関連付けられた SoO 値を使用し、ルーティング ループを防止できます。

有効な形式：

- extended:as2-nn2:<2-byte number>:<2-byte number>

  例：`extended:as2-nn2:1000:65534`

- extended:as2-nn4:<2-byte number>:<4-byte number>

  例： `extended:as2-nn4:1000:6554387`

- extended:as4-nn2:<4-byte number>:<2-byte number>

  例：`extended:as4-nn2:1000:65504`

- extended:ipv4-nn2:<IPv4 address>:<2-byte number>

  例： `extended:ipv4-nn2:1.2.3.4:65515`

（注） ユーザ テナント L3Out の SoO を設定する場合は、ACI ファブリック内で設定されたグローバル ファブリック、ポッド、またはマルチ サイト SoO と同じ SoO 値を設定しないようにしてください。スイッチで次のコマンドを実行すると、ファブリック内に設定されたファブリック、ポッド、およびマルチサイト SoO の値を表示できます。

```
show bgp process vrf overlay-1 | grep SOO
```

m) [リモート自律システム番号（Remote Autonomous System Number）] フィールドで、ネイバー自律システムを一意に識別する番号を選択します。

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。

（注） ACI は asdot または asdot + 形式の AS 番号をサポートしていません。

n) [ローカル AS 番号設定（Local-AS Number Config）] フィールドで、ローカル自律システム番号（ASN）設定を選択します。

グローバル AS ではなくローカル AS 番号を使用すると、関連付けられたネットワーク内のルーティング デバイスが以前の AS に属しているように見えます。設定は次のとおりです。

- **[no-Prepend+replace-as+dual-as]**：ローカル AS での先頭付加を許可せず、両方の AS 番号で置き換えます。

  AS パスの先頭に 1 つ以上の自律システム（AS）番号を付加できます。AS 番号は、ルートの発信元である実際の AS 番号がパスに追加された後に、パスの先頭に追加されます。AS パスの前に付加すると、AS パスが短く見えるため、BGP よりも優先度が低くなります。

- **[no-prepend]**：ローカル AS でのプリペンドを許可しません。
- **[no options]**：ローカル AS の変更を許可しません。
- **[no-Prepend+replace-as]**：ローカル AS での先頭追加を許可せず、AS 番号を置き換えます。

o) [ローカル AS 番号（Local-AS Number）] フィールドで、目的の値を選択します。

eBGP ピアのローカル自律システム機能の場合にオプションで必要です。ローカル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。ACI は asdot または asdot + 形式の AS 番号をサポートしていません。

p) [管理状態（Admin State）] フィールドで、[無効化（Disabled）] または [有効化（Enabled）] を選択します。

[管理状態（Admin State）] フィールドでは、対応する BGP ネイバーをシャットダウンできます。この機能を使用すると、BGP ピア設定を削除せずに BGP セッションがシャットダウンされます。

次のオプションがあります。

- 無効化：BGP ネイバーの管理状態を無効にします。
- 有効化：BGP ネイバーの管理状態を有効にします。

q) [ルート制御プロファイル（Route Control Profile）]フィールドで、BGP ピアごとにルート制御ポリシーを設定します。

[+] をクリックして、次を設定します。

- [名前（Name）]：ルート制御プロファイル名を選択します。
- [**方向（Direction**）]：次のいずれかのオプションを選択します。

- ルートインポートポリシー
- ルートエクスポートポリシー

r) **[送信（Submit）]** をクリックします。`

ステップ 10 **[テナント（Tenants）]** > **[*tenant_name*]** > **[ネットワーキング（Networking）]** > **[L3Outs]** > **[*L3Out_name*]** に移動します。

ステップ 11 [ポリシー/メイン（Policy/Main）] タブをクリックし、次の操作を実行します。

a) （任意） [Route Control Enforcement] フィールドで、[mport] チェックボックスをオンにします。

（注） BGP でインポート制御を適用する場合は、このチェックボックスをオンにします。

b) [Route Control for Dampening] フィールドを展開し、目的のアドレス ファミリ タイプとルート ダンプニング ポリシーを選択します。[Update] をクリックします。

このステップでは、ポリシーはステップ 4 で作成することができます。または、ポリシー名が選択されているドロップダウン リストで **[ルート プロファイルの作成（Create route profile）]** をするオプションがあります。

ステップ 12 **[テナント（Tenants）]** > **[*tenant_name*]** > **[ネットワーキング（Networking）]** > **[L3Outs]** > **[*L3Out_name*]** に移動します。

ステップ 13 **[ルート制御のインポートおよびエクスポートのルート マップ（Route Map for import and export rout control）]** を右クリックし、**[ルート制御のインポートおよびエクスポートのルート マップの作成（Create Route Map for import and export rout control）]** を選択します。

ステップ 14 このウィンドウに必要な情報を入力し、[コンテキスト（Context）] 領域で [+] をクリックして [ルート制御コンテキストの作成（Create Route Control Context）] ウィンドウを表示します。

a) **[名前（Name）]**フィールドに、ルート制御 VRF の名前を入力します。

b) [Set Attribute] ドロップダウン リストから、[Create Action Rule Profile] を選択します。

アクション ルールを作成するときに、必要に応じてルート ダンプニング属性を設定します。

BGP Max Path の設定

次の機能を使用すると、等コスト マルチパスのロード バランシングを有効にするルート テーブルへのパスの最大数を追加できます。

GUI を使用した BGP Max Path の設定

始める前に

適切なテナントと BGP 外部ルーティング ネットワークが作成され、使用可能になります。

手順

ステップ 1 **[メニュー（Menu）]** バーで、**[テナント（Tenants）]** > **[すべてのテナント（All Tenants）]** を選択します。

ステップ 2 作業ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 **[ナビゲーション（Navigation）]** ペインで、***[テナント名（Tenant_name）]*** > **[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[BGP]** > **[BGP アドレス ファミリ コンテキスト（BGP Address Family Context）]** を展開します。

ステップ 4 **[BGP アドレス ファミリ コンテキスト（BGP Address Family Context）]** を右クリックし、**[BGP アドレス ファミリ コンテキスト ポリシーの作成（Create BGP Address Family Context Policy）]** を選択します。

ステップ 5 **[Create BGP Address Family Context Policy]** ダイアログ ボックスで、次のタスクを実行します。

次のフィールドの許容値については、Cisco APIC ドキュメンテーション ページの *Cisco APIC* 検証済みスケーラビリティ ガイドを参照してください。

a) [Name] フィールドにポリシーの名前を入力します。
b) **[eBGP 距離（eBGP Distance）]** フィールドに、eBGP ルートの [管理距離（Administrative Distance）] の値を入力します。
c) **[iBGP 距離（iBGP Distance）]** フィールドに、iBGP ルートの [管理距離（Administrative Distance）] の値を入力します。
d) [ローカル距離（Local Distance）] フィールドに、ローカル距離の値を入力します。
e) [eBGP 最大 ECMP（eBGP Max ECMP）] フィールドに、eBGP ロード シェアリングの等コスト パスの最大数の値を入力します。
f) [iBGP 最大 ECMP（iBGP Max ECMP）] フィールドに、iBGP ロード シェアリングの等コスト パスの最大数の値を入力します。
g) DCIG への EVPN タイプ 2（MAC/IP）ホスト ルートの配布を有効にする場合には、**[ホスト ルート リークの有効化（Enable Host Route Leak）]** チェックボックスをオンにします。
h) エントリを更新した後、**[Submit]** をクリックします。

ステップ 6 **[テナント（Tenants）]** > **[*tenant_name*]** > **[ネットワーキング（Networking）]** > **[VRFs]** > **[*vrf_name*]** の順にクリックします。

ステップ 7 対象の VRF の設定の詳細を確認します。

ステップ 8 [アドレス ファミリごとの BGP コンテキスト（BGP Context Per Address Family）] フィールドを見つけ、[BGP アドレス ファミリ タイプ（BGP Address Family Type）] 領域で、IPv4 unicast address family または IPv6 unicast address family を選択します。

ステップ 9 **[BGP Address Family Context]** ドロップダウン リストで作成した [BGP Address Family Context] にアクセスし、それをサブジェクト VRF に関連付けます。

ステップ 10 [送信（Submit）] をクリックします。

AS パス プリペンドの設定

次の項の手順を使用して、AS パスのプリペンドを設定します。

AS パス プリペンドの設定

BGP ピアは、AS パス アトリビュートの長さを増やすことで、リモート ピアでベスト パス選択の影響を与えることができます。番号として指定桁の前に付加してASパス アトリビュートの長さを向上するために使用するメカニズムを提供する AS パス Prepend。

ASパス前に付加は、ルートマップを使用してアウトバウンド方向にのみ適用できます。パスとして前に付加が機能しない iBGP セッションで。

AS パス Prepend 機能は、次のように変更を有効に。

プリペンド	ルート マップと一致するルートの AS パスに、指定した AS 番号を付加します。 （注） • 1 個以上の AS 番号を設定できます。 • 4 バイト番号がサポートされています。 • 合計を prepend は 32 の AS 番号。AS 番号は、AS パス アトリビュートに挿入されます順序を指定する必要があります。
Prepend-最後-として	最後の前に付加 AS パス 1 から 10 までの範囲に番号として。

次の表では、AS パス Prepend の実装の選択基準について説明します。

プリペンド	1	指定された AS 番号を追加します。
Prepend-最後-として	2	最後のAS番号をASパスに付加します。
デフォルト	Prepend(1)	指定された AS 番号を追加します。

設定の AS パス Prepend GUI を使用して

始める前に

構成済みのテナント

手順

ステップ 1 APIC GUI にログインしメニュー バーで、**[テナント（Tenants）] > [*tenant_name*] > [ポリシー（Policies） > [プロトコル（Protocol）] > [設定ルール（Set Rules）]**の順にクリックし、**[ルート マップの設定ルールの作成（Create Set Rules for a Route Map）]** を右クリックします。

[ルート マップの設定ルールの作成（**Create Set Rules For A Route Map**）] ウィンドウが表示されます。

ステップ 2 **設定ルールの A ルート マップの作成** ダイアログボックス、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) [AS パスの設定（Set AS Path）] チェックボックスをオンにし、[次へ（Next）] をクリックします。

c) [**AS パス（AS Path**）] ウィンドウで [+] をクリックして [**AS パスの設定を作成（Create Set AS Path**）] ダイアログ ボックスを開きます。

ステップ 3 基準に [**AS 番号の付加（Prepend AS**）] を選択し、**[+]** をクリックして AS 番号を先頭に付加します。

ステップ 4 AS 番号とその順序を入力し、クリックして **更新** 。[+] をクリックして複数の AS 番号の先頭を追加する必要があるかどうかを繰り返します。

ステップ 5 AS 番号の先頭を追加する設定が完了したら、基準 [**AS 番号の末尾を追加（Prepend Last-AS**）] を選択し、指定された回数の数を AS 番号の末尾に付加します。

ステップ 6 **[カウント]**(1-10) を入力します。

ステップ 7 **[OK]** をクリックします。

ステップ 8 [ルート マップの設定ルールを作成（Create Set Rules For A Rout Map）] ウィンドウで AS パスに基づく設定ルールの基準を確認し、[完了（Finish）] をクリックします。

ステップ 9 APIC GUI メニューバーで、[テナント（Tenants）] [tenant_name] [ポリシー（Policies）] [プロトコル（Protocol）] [設定ルール（Set Rules）] の順にクリックし、プロファイルを右クリックします。 > > > >

ステップ 10 確認、 **AS パスの設定** 画面の下部の値します。

AS オーバーライドの BGP 外部ルーテッド ネットワーク

AS オーバーライドを使用して BGB 外部ルーテッド ネットワークを設定するには、次の項の手順を使用します。

BGP 自律システムのオーバーライドについて

BGP のループ防止は、自律システム パスの自律システム番号を確認することで行われます。受信側のルータが受信した BGP パケットの自律システム パスで独自の自律システム番号が表示される場合、パケットは廃棄されます。受信側のルータでは、パケットが独自の自律システムから発信され、最初に発信元から同じ場所に達したことが想定されます。この設定では、ルーティング ループが発生しないようにするためのデフォルトです。

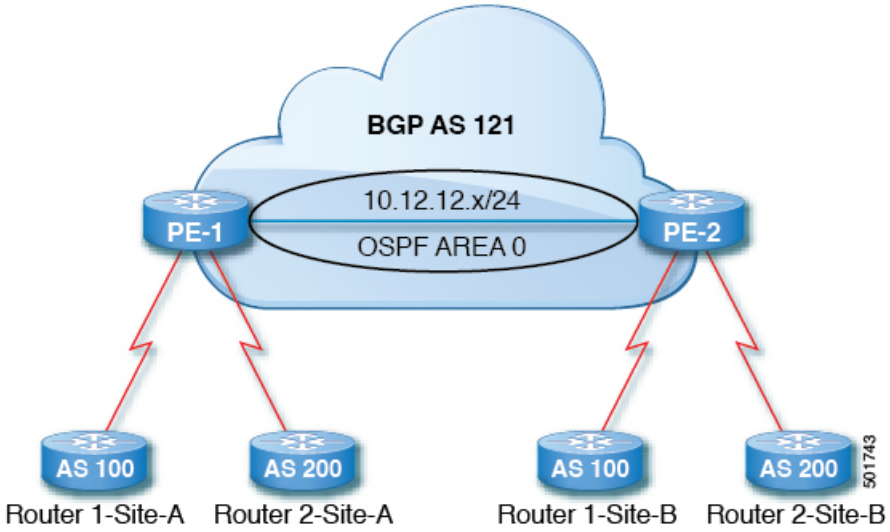
別の自立システム番号によりリンクする同一の自律システム番号を持つさまざまなサイトや禁止ユーザーのサイトを使用する場合、デフォルトルートのループが発生しないようにする設定によって問題が発生する可能性があります。このようなシナリオでは、その他のサイトが受信した場合 1 つのサイトからのルーティング更新は廃棄されます。

このような状況の発生を防ぐため、Cisco APIC リリース 3.1(2m) 以降、BGP 自律システムのオーバーライド機能を有効にして、デフォルトの設定をオーバーライドすることができます。同時に、ピア AS チェックの無効化も有効にする必要があります。

自律システム オーバライド機能では、発信元のルータからの自律システム番号を、アウトバウンド ルートの AS パスの BGP ルータ送信の自律システム番号に置き換えます。アドレス ファミリごとにこの機能を有効にできます（IPv4 または IPv6）。

自律システム オーバライド機能は、GOLF レイヤ 3 設定および非 GOLF レイヤ 3 の設定でサポートされています。

図 *41* : 自律システム オーバライド機能を説明するトポロジ例



ルータ 1 およびルータ 2 は、複数のサイトを持つ 2 つの顧客です（サイト A とサイト B）。顧客ルータ 1 は AS 100 で動作し、顧客ルータ 2 は AS 200 で動作します。

上の図は、次のような自律システム（AS）オーバーライド プロセスを示しています。

1. ルータ A サイト 1 では、AS100 でルート 10.3.3.3 をアドバタイズします。
2. ルータ PE-1 は、AS100 として PE2 へ内部ルートとして反映します。
3. ルータ PE-2 は AS121 で 10.3.3.3 をプリペンドし（AS パスの 100 を 121 に置き換えます）、プレフィックスをプロパゲートします。
4. ルータ 2 サイト B は 10.3.3.3 更新プログラムを承認します。

GUI を使用して、BGP 外部ルーテッド ネットワークと有効になっている自律システム オーバーライドを設定する

始める前に

- テナント、VRF、およびブリッジ ドメインが作成されています。

- 非 GOLF 設定の外部ルーテッド ネットワーク、論理ノード プロファイル、および BGP ピア接続プロファイルが作成されています。

手順

ステップ 1 メニューバーで、**[テナント（Tenants）]** > **[*Tenant_name*]** > **[ネットワーキング（Networking）]** > **[L3Outs]** > **[*Non-GOLF Layer 3 Out_name*]** > **[論理ノード プロファイル（Logical Node Profiles）]** を選択します。

ステップ 2 **Navigation** ウィンドウで、適切な **BGP Peer Connectivity Profile** を選択します。

ステップ 3 [作業（Work）] ペインで、[BGP ピア接続プロファイル（BGP Peer Connectivity Profile）] の [プロパティ（Properties）] 下の [BGP 制御（BGP Controls）] フィールドで、次の手順を実行します:

a) **AS override** フィールドのチェック ボックスをオンにして、**Autonomous System override** 機能を有効にします。

b) **Disable Peer AS Check** フィールドのチェック ボックスをオンにします。

（注） AS オーバーライド機能を有効にするには、**AS override** および **Disable Peer AS Check** チェック ボックスをオンにする必要があります。

c) 必要に応じてその他のフィールドを選択します。

ステップ 4 [Submit] をクリックします。

BGP ネイバー シャットダウンおよびソフト リセット

BGB ネイバーのシャットダウンとソフト リセットを設定するには、次の項の手順を使用します。

BGP ネイバー シャットダウンとソフト リセットについて

リリース 4.2(1) 以降、次の機能がサポートされるようになりました。

- BGP ネイバー シャットダウン （335 ページ）
- BGP ネイバー ソフト リセット （336 ページ）

BGP ネイバー シャットダウン

BGP ネイバー シャットダウン機能は、NX-OS の neighbor shutdown コマンドに似ており、対応する BGP ネイバーをシャットダウンします。このポリシーを使用して、BGP ネイバーの管理状態を無効または有効にします。この機能を使用すると、BGP ピア設定を削除せずに BGP セッションがシャットダウンされます。

BGP ネイバー ソフト リセット

BGP ネイバー ソフト リセット機能は、BGP ルート リフレッシュ機能を使用して、保存されているルーティング テーブル アップデート情報に依存しない着信および発信 BGP ルーティング テーブル アップデートのダイナミック ソフト リセットを自動的にサポートします。ソフト ダイナミック インバウンド リセットとソフト アウトバウンド リセットを有効にするには、このポリシーを使用します。

GUI を使用した BGP ネイバー シャットダウンの設定

次の手順では、GUI を使用して BGP ネイバー シャットダウン機能を使用する方法について説明します。

始める前に

L3Out を設定する前に、次のような標準的な前提条件を満たします。

- ノード、ポート、AEP、機能プロファイル、レイヤ 3 ドメインを設定します。
- ファブリック内でルートを伝播させるための、BGP ルート リフレクタ ポリシーを設定します。

手順

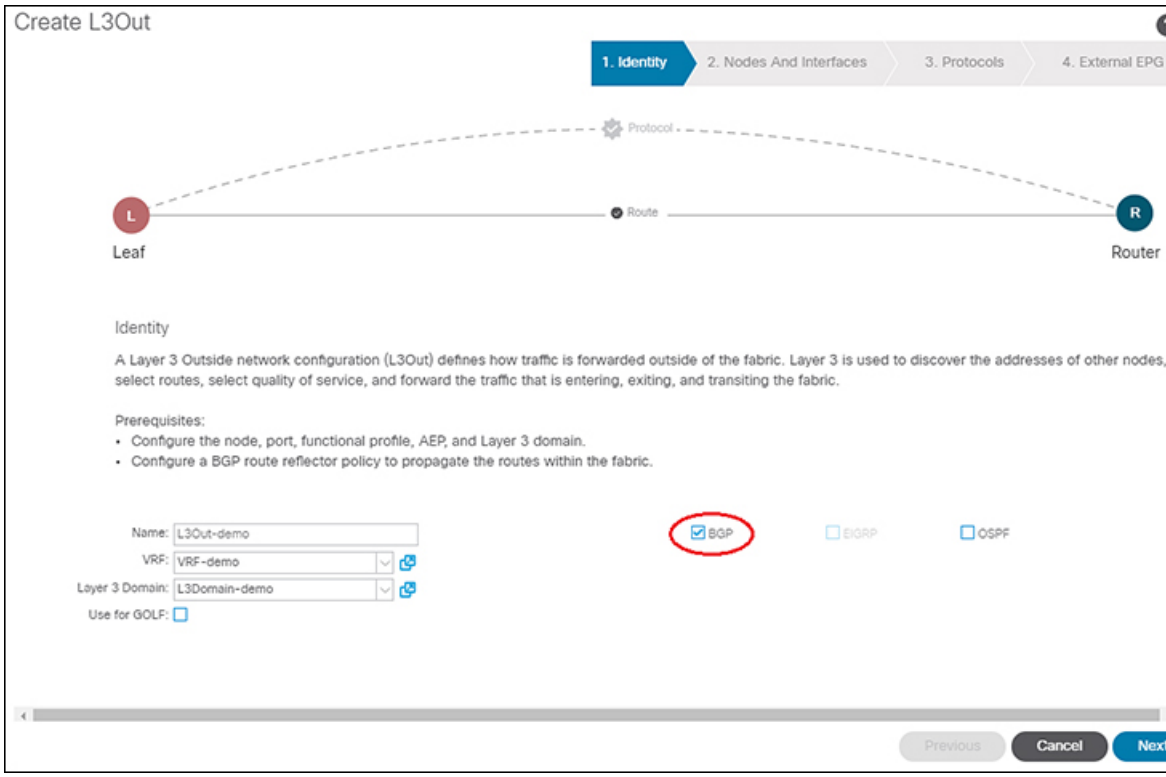
ステップ 1 L3Out を作成し、L3Out の BGP を設定します。

a) [**ナビゲーション（Navigation）**] ペインで [**テナント（Tenant）**] および [**ネットワーキング（Networking）**] を展開します。

b) [L3Outs] を右クリックし、[L3Out の作成（Create L3Out）] を選択します。

c) L3Out の BGP を設定するために必要な情報を入力します。

この L3Out の BGP プロトコルを設定するには、L3Out 作成ウィザードの [識別（Identity）] ページで [BGP] を選択します。



d) 残りのページを続けて行い（[**ノードとインターフェイス（Nodes and Interfaces）**]、[**プロトコル（Protocols）**]、および [**外部 EPG（External EPG）**]）、L3Out の設定を完了します。

ステップ 2 L3Out の設定が完了したら、BGP ネイバーのシャットダウンを設定します。

a) BGP ピア接続プロファイル画面に移動します。

[テナント（Tenants）] > [テナント（*tenant*）] > [ネットワーキング（Networking）] > [L3Outs] > [*L3out-name*] > [論理ノード プロファイル（Logical Node Profiles）] > [*logical-node-profile-name*] > [論理インターフェイス プロファイル（Logical Interface Profiles）] > [*logical-interface-profile-name*] > [BGP ピア接続プロファイル（BGP Peer Connectivity Profile） *] [IP-address*]

b) [管理状態（Admin State）] フィールドまでスクロールし、このフィールドで適切な選択を行います。

- 無効化：BGP ネイバーの管理状態を無効にします。
- 有効化：BGP ネイバーの管理状態を有効にします。

GUI を使用した BGP ネイバー ソフト リセットの設定

次の手順では、GUI を使用して BGP ネイバー ソフト リセット機能を使用する方法について説明します。

始める前に

L3Out を設定する前に、次のような標準的な前提条件を満たします。

- ノード、ポート、AEP、機能プロファイル、レイヤ 3 ドメインを設定します。
- ファブリック内でルートを伝播させるための、BGP ルート リフレクタ ポリシーを設定します。

手順

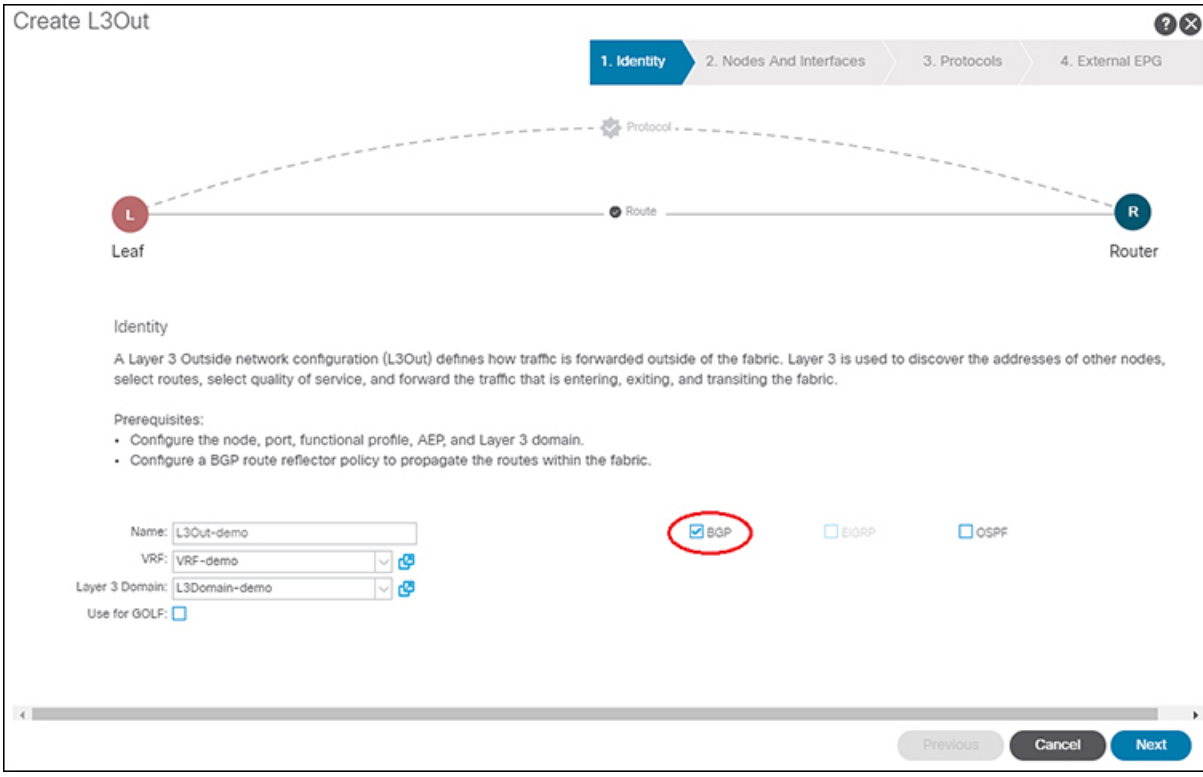
ステップ 1 L3Out を作成し、L3Out の BGP を設定します。

a) [**ナビゲーション（Navigation）**] ペインで [**テナント（Tenant）**] および [**ネットワーキング（Networking）**] を展開します。

b) [L3Outs] を右クリックし、[L3Out の作成（Create L3Out）] を選択します。

c) L3Out の BGP を設定するために必要な情報を入力します。

この L3Out の BGP プロトコルを設定するには、L3Out 作成ウィザードの [識別（Identity）] ページで [BGP] を選択します。



d) 残りのページを続けて行い（[**ノードとインターフェイス（Nodes and Interfaces**）]、[**プロトコル（Protocols**）]、および [**外部 EPG（External EPG**）]）、L3Out の設定を完了します。

ステップ 2 L3Out の設定が完了したら、BGP ネイバーのソフト リセットを設定します。

a) [BGP ピア エントリ（BGP Peer Entry）] 画面に移動します。

[テナント（Tenants）] > [テナント（*tenant*）] > [ネットワーキング（Networking）] > [L3Outs] > [*L3out-name*] > [論理ノード プロファイル（Logical Node Profiles）] > [*logical-node-profile-name*] > [設定済みノード（Configured Nodes）] > [ノード（*node*）] > [BGP for VRF-*vrf-name*] > [ネイバー（Neighbors）]

b) 適切なネイバー エントリを右クリックし、[BGP ピアのクリア（Clear BGP Peer）] を選択します。

[BGP をクリア（Clear BGP）] ページが表示されます。

c) [モード（Mode）] フィールドで、[ソフト（Soft）] を選択します。

[方向（Direction）] フィールドが表示されます。

d) [方向（Direction）] フィールドで適切な値を選択します。

- Incoming：ソフト ダイナミック インバウンド リセットを有効にします。
- Outgoing：ソフト アウトバウンド リセットを有効にします。

VRF ごと、ノード BGP ごとのタイマーの値の設定

ノードごとの BGP タイマー値を設定するには、次の項の手順を使用します。

ノード BGP タイマー値ごとの各 VRF

この機能を紹介する前に、特定の VRF について、すべてのノードには同じ BGP タイマーの値が使用されます。

ノード BGP タイマー値ごとの各 VRF 機能の導入により、BGP タイマーを定義し、各ノードベースの VRF ごとに関連付けることが可能です。ノードでは複数の VRF を所持することが可能で、それぞれ、`fvCtx` に対応しています。ノード設定（`l3extLNodeP`）には、 BGP プロトコル プロファイル（`bgpProtP`）の設定が含まれており、希望の BGP コンテキスト ポリシーを参照します（`bgpCtxPol`）。これにより、同じ VRF 内のさまざまなノードが異なる BGP タイマーの値を含めることが可能になります。

各 VRF ではノードに `bgpDom` の具体的な MO を含みます。その名前（プライマリ キー）は、VRF `<fvTenant>:<fvCtx>` です。属性として BGP タイマーの値が含まれています（例：`holdIntvl`、`kaIntvl`、`maxAsLimit`）。

有効なレイヤ 3 アウト設定を作成するために必要なすべての手順は、ノード BPG タイマーごとの各 VRF に正常に適用する必要があります。たとえば、次のような MO は必須です：`fvTenant`、`fvCtx`、`l3extOut`、`l3extInstP`、`LNodeP`、`bgpRR`。

ノードでは、BGP タイマー ポリシーは次のアルゴリズムに基づいて選択されます。

- `BgpProtP` が指定されると、`bgpProtP` の下で参照される `bgpCtxPol` を使用します。

- それ以外の場合、指定されると対応する `fvCtx` の下で参照される `bgpCtxPol` を使用します。
- それ以外の場合、指定されるとテナントでデフォルト ポリシーを使用します。例：`uni/tn-<tenant>/bgpCtxP-default`。
- それ以外の場合、テナント `common` の下の `default` ポリシーを使用します。例：`uni/tn-common/bgpCtxP-default`。これはプログラム済みです。

設定の高度な GUI を使用して BGP タイマーのノードごとの VRF あたり

BGP タイマーが特定のノードに設定されているときに、ノードで BGP タイマー ポリシーを使用し、VRF に関連付けられている BGP ポリシー タイマーはすべて無視されます。

始める前に

テナントと VRF はすでに設定されています。

手順

ステップ 1 メニュー バーで、**[テナント（Tenant）** > **[*Tenant_name*]** > **[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[BGP]** > **[BGP タイマー（BGP Timers）]** を選択し、[**BGP タイマー ポリシーの作成（Create BGP Timers Policy**）] を右クリックします。

ステップ 2 [**BGP タイマー ポリシーの作成（Create BGP Timers Policy**）] ダイアログ ボックスで、次の操作を実行します:

a) **Name** フィールドに、BGP タイマー ポリシーの名前を入力します。
b) 使用可能なフィールドには、必要に応じて、適切な値を選択します。[Submit] をクリックします。`

BGP タイマー ポリシーが作成されます。

ステップ 3 **[テナント（Tenant）]** > **[*Tenant_name*]** > **[ネットワーキング（Networking）]** > **[L3Outs]**に移動し、[**L3Out の作成（Create L3Out**）] を右クリックします。

Create L3Out ウィザードが表示されます。次の操作を実行して、BGP を有効にした L3Out を作成します。

ステップ 4 [L3Out の作成（Create L3Out）] ウィザードの [識別（Identity）] ウィンドウに必要な情報を入力します。

a) **Name** フィールドに L3Out の名前を入力します。
b) **VRF** ドロップダウンリストから VRF を選択します。
c) [**L3 ドメイン（L3 Domain**）]ドロップダウン リストから、適切なドメインを選択します。
d) ルーティング プロトコルのチェック ボックスがある領域で、[**BGP**] を選択します。
e) **Next** をクリックして **Nodes and Interfaces** ウィンドウに移動します。
f) [**L3Out の作成（Create L3Out**）] ウィザードの残りのウィンドウに進み、L3Out の作成プロセスを完了します。

ステップ 5 L3Out を作成したら、作成した L3Out の論理ノード プロファイル（[テナント（Tenant）] [Tenant_name] [ネットワーキング（Networking）] [L3Outs] [L3Out_name] [論理ノード プロファイル（Logical Node Profiles）] [LogicalNodeProfile-name]）に移動します。＞ ＞＞＞ ＞＞

ステップ 6 [論理ノード プロファイル（Logical Node Profile）] ウィンドウで、[BGP プロトコル プロファイルの作成（Create BGP Protocol Profile）] の横にあるチェックボックスをオンにします。

[ノード指定 BGP プロトコル プロファイルの作成（Create Node Specific BGP Protocol Profile）] ウィンドウが表示されます。

ステップ 7 **BGP タイマー**] フィールドに、ドロップダウンリストから、この特定のノードに関連付ける BGP タイマー ポリシー選択します。**[送信（Submit）]** をクリックします。`

特定の BGP タイマー ポリシーは、ノードに適用されます。

（注） BGP タイマー ポリシーと、既存のノードのプロファイルを関連付ける、ノードのプロファイルを右クリックし、タイマー ポリシーを関連付けます。

タイマー ポリシーが具体的に選択していない場合、 **BGP タイマー** されたノードのプロファイルが存在する自動的に VRF に関連付けられている BGP タイマー ポリシーは、このノードに適用を取得し、ノードのフィールドします。

ステップ 8 設定を確認するには、**Navigation** ウィンドウで、次の手順を実行します:

a) **[テナント（Tenants）]** > **[*Tenant_name*]** > **[ネットワーキング（Networking）]** > **[L3Outs]** > **[*L3Out_name*]** > **[論理ノード プロファイル（Logical Node Profiles）]** > **[*LogicalNodeProfile-name*]** > **[プロトコル プロファイル（Protocol Profiles）]**の順に移動します。

b) **作業**] ペインで、ノードのプロファイルに関連付けられている BGP プロトコル プロファイルが表示されます。

不整合や障害のトラブルシューティング

特定の状況下では、次のような不整合や障害が発生する可能性があります:

異なるレイヤ 3 Out (`l3Out`) が同じ VRF (`fvCtx`) に関連付けられているか、同じノードで `bgpProtP` が異なるポリシー (`bgpCtxPol`) に関連付けられていると、障害が発生します。次の例では、同じ Layer 3 Out (`out1` と `out2`) が同じ VRF (`ctx1`) に関連付けられています。`out1` の下では、`node1` は BGP タイマー プロトコル `pol1` に関連付けられており、`out2` の下では、`node1` は別の BGP タイマー プロトコル `pol2` に関連付けられています。。この場合、障害が発生します。

```
tn1
  ctx1
  out1
    ctx1
    node1
      protp pol1

  out2
    ctx1
    node1
      protp pol2
```

このような障害が発生した場合は、設定を変更して、BGP タイマー ポリシー間の競合を削除してください。

BFD サポートの設定

BFD サポートを設定するには、次の項の手順を使用します。

双方向フォワーディング検出

双方向フォワーディング検出（BFD）を使用して、ピアリング ルータの接続をサポートするように設定されたCisco Application Centric Infrastructure（ACI）ファブリック境界リーフ スイッチ間の転送パスのサブセカンド障害検出時間を可能にします。

BFD は、次のような場合に特に役立ちます。

- ルータ同士の間に直接的な接続がない場合に、レイヤ 2 デバイスまたはレイヤ 2 クラウド経由でピアリング ルータが接続されているとき。転送パスに障害があっても、ピア ルータにはそれがわからない可能性があります。プロトコルの制御に利用できるメカニズムは hello タイムアウトだけですが、タイムアウトまでには数十秒、さらには数分の時間がかかる場合があります。BFD では、障害を 1 秒未満で検出することが可能です。
- 信頼できる障害検出に非対応の物理メディア（共有イーサネットなど）経由でピアリング ルータが接続されているとき。この場合も、ルーティング プロトコルは、時間のかかる hello タイマーに頼るしかありません。
- 1 組のルータの間で多くのプロトコルが実行されているとき、各プロトコルは、独自のタイムアウトでリンク障害を検出する独自の hello メカニズムを持っています。BFD は、すべてのプロトコルに均一のタイムアウトを指定し、それによってコンバージェンス時間の一貫性を保ち、予測可能にします。

次に示す BFD の設定のガイドラインおよび制限事項に従ってください。

- Cisco APIC リリース 3.1(1) 以降、リーフおよびスパイン スイッチ間の BFD は IS-IS のファブリック インターフェイスでサポートされています。さらに、スパイン スイッチの BFD 機能は、OSPF ルートとスタティック ルートでサポートされます。
- Cisco APIC リリース 5.2(4) 以降、BFD 機能は、セカンダリ IPv4/IPv6 サブネットを使用して到達可能なスタティック ルートでサポートされています。サブネットに複数のアドレスが設定されている場合、スタティック BFD セッションは L3Out インターフェイスのセカンダリ サブネットから発信できません。共有サブネット アドレス (vPC シナリオに使用) と浮動 L3Out に使用される浮動 IP アドレスは、サブネットの追加アドレスとして許可され、自動的にスキップされ、静的 BFD セッションの発信元には使用されません。

（注） セッションのソースに使用されているセカンダリ アドレスを変更するには、同じサブネットに新しいアドレスを追加し、後で以前のアドレスを削除します。

- BFD は -EX および -FX ライン カード（または新しいバージョン）のモジュラ スパイン スイッチでサポートされ、また BFD は Nexus 9364C 非モジュラ スパイン スイッチ（または新しいバージョン）でサポートされます。
- vPC ピア間の BFD はサポートされません。
- Cisco APIC リリース 5.0(1) 以降、BFD マルチホップはリーフ スイッチでサポートされます。BFD マルチホップ セッションが合計に含まれるようになったため、BFD セッションの最大数は変更されません。
- Cisco APIC リリース 5.0(1) 以降、Cisco ACI は C ビット対応 BFD をサポートしています。BFD がコントロール プレーンに依存しているかいないかは、受信する BFD パケットの C ビットによって判別されます。
- ループバック アドレス ピアでの iBGP 上の BFD はサポートされません。
- インターフェイス ポリシーで BFD サブインターフェイス最適化を有効化できます。このフラグを 1 つのサブインターフェイスに立てることにより、その物理インターフェイス上のすべてのサブインターフェイスの最適化が有効になります。
- BGP プレフィクス ピアの BFD はサポートされません。

（注） Cisco ACI は IP フラグメンテーションをサポートしていません。したがって、外部ルータへのレイヤ 3 Outside（L3Out）接続、または Inter-Pod Network（IPN）を介した マルチポッド 接続を設定する場合は、インターフェイス MTU がリンクの両端で適切に設定されていることが推奨されます。Cisco ACI、 Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定可能な MTU 値はイーサネット ヘッダー (一致する IP MTU、14-18 イーサネット ヘッダー サイズを除く) を考慮していません。また、IOS XR などの他のプラットフォームには、設定された MTU 値にイーサネット ヘッダーが含まれています。設定された値が 9000 の場合、Cisco ACI、Cisco NX-OS Cisco IOS の最大 IP パケット サイズは 9000 バイトになりますが、IOS-XR のタグなしインターフェイスの最大 IP パケットサイズは 8986 バイトになります。

各プラットフォームの適切な MTU 値については、それぞれの設定ガイドを参照してください。

CLI ベースのコマンドを使用して MTU をテストすることを強く推奨します。たとえば、Cisco NX-OS CLI で `ping 1.1.1.1 df-bit packet-size 9000 source-interface ethernet 1/1` などのコマンドを使用します。

サブインターフェイスの BFD の最適化

サブインターフェイスの BFD は最適化できます。BFD により、設定されているすべてのサブインターフェイスのセッションが作成されます。BFD により、設定されている最小の VLAN ID を持つサブインターフェイスがマスター サブインターフェイスとして設定され、そのサブインターフェイスは親インターフェイスの BFD セッション パラメータを使用します。残りのサブインターフェイスは slow timer を使用します。

最適化サブインターフェイス セッションでエラーが検出されると、BFD により、その物理インターフェイスのすべてのサブインターフェイスがダウンとマークされます。

BFD モニタ対象リンクの一端または両端で BFD エコー機能を設定できます。エコー機能は設定された slow timer に基づいて必要最小受信間隔を遅くします。*[RequiredMinEchoRx]* BFD セッション パラメータは、エコー機能がディセーブルの場合、ゼロに設定されます。slow timer は、エコー機能がイネーブルの場合、必要最小受信間隔になります。

（注） サブインターフェイスの 1 つがフラップすると、その物理インターフェイスのサブインターフェイスが影響を受け、1 秒間ダウンします。

GUI を使用したセカンダリ IP アドレスでの双方向フォワーディング検出の構成

この手順では、GUI を使用して、セカンダリ IP アドレスで双方向フォワーディング検出（BFD）を構成します。

手順

ステップ 1 メニュー バーで、[テナント（Tenants）] > [すべてのテナント（ALL Tenants）] の順に選択します。 >

ステップ 2 作業ウィンドウで、テナントの名前をダブルクリックします。

ステップ 3 ナビゲーション ペインから、***[tenant_name]*** > **[ネットワーキング（Networking）]** > **[L3Outs]** > ***[l3Out_name]*** > **[論理ノード プロファイル（Logical Node Profiles）]** > ***[node_profile_name]*** > **[論理インターフェイス プロファイル（Logical Interface Profiles）]** > ***[interface_profile_name***] の順に移動します。

ステップ 4 [Work] ペインで、必要に応じて **[Policy（ポリシー）]** > **[ルーテッド サブインターフェイス（Routed Sub-interfaces）]**、**[Policy（ポリシー）]** > **Routed Interfaces**または **[Policy（ポリシー）]** > **[SVI]**を選択します。

ステップ 5 インターフェイスをダブルクリックして、そのプロパティを編集します。

ステップ 6 インターフェイスのタイプに応じて、次のサブステップのいずれかを実行します。

a) インターフェイスがルーテッド サブインターフェイスまたはルーテッド インターフェイス、または**[パス タイプ（Path Type）]**が**[ポート（Port）]**または**[ダイレクト ポート チャネル（Direct Port Channel）]**に設定されたスイッチ仮想インターフェイス (SVI) である場合は、**[IPv4 セカンダリ/IPv6 追加アドレス（IPv4 secondary/IPv6 Additional Addresses）]** テーブルで、**+** をクリックし、IP を入力します。アドレスとサブネットを選択し、**[送信（Submit）]** をクリックします。

b) インターフェイスがスイッチ仮想インターフェイス (SVI) で、パス タイプが仮想ポート チャネルに設定されている場合は、サイド B の IPv4 セカンダリ/IPv6 追加アドレス テーブルで、+ をクリックし、IP アドレスとサブネットを入力して、[OK] をクリックします。

ステップ 7 [ナビゲーション] ペインで、***[tenant_name]*** > **[ネットワーキング（Networking）]** > **[L3Outs]** > ***[l3out_name]*** > **[論理ノード プロファイル（Logical Node Profiles）]** > ***[node_profile_name]*** > **[構成済みノード（Configured Nodes）]** > ***[node_name]***を選択します。

ステップ 8 **[静的ルート（Static Routes）]** テーブルで、**[+]** をクリックして、次のサブステップを実行します。

a) **[プレフィックス（Prefix）]** フィールドに、外部ネットワークに割り当てられている静的ルートの IP アドレスとマスクを入力します。

b) **[BFD]** チェックボックスをオンにします。

c) **[次のホップ アドレス（Next Hop Addresses）]** テーブルで、**[+]** をクリックし、**[次のホップ アドレス（Next Hop Addresses）]** フィールドに、インターフェイスに指定したセカンダリ IP アドレスから到達可能な IP アドレスを入力します。

d) 必要に応じて、残りのフィールドに入力します。

e) [OK] をクリックします。

ステップ 9 必要に応じて、残りのフィールドに入力します。

ステップ 10 [Submit] をクリックします。

GUI を使用してリーフ スイッチの BFD をグローバルに設定する

手順

ステップ 1 メニュー バーで、**[Fabric]** > **[Access Policies]** の順に選択します。

ステップ 2 **[ナビゲーション（Navigation）]** ペインで、**[ポリシー（Policies）]** > **[スイッチ（Switch）]** > **[BFD]**の順に展開します。
設定を双方向フォワーディング検出 (BFD) には、使用可能な 2 つの種類があります:

- BFD IPV4
- BFD IPV6

これらのBFD設定ごとに、デフォルトポリシーを使用するか、特定のスイッチ(またはスイッチのセット) 用に新しいポリシーを作成できます。

（注） デフォルトでは、APICコントローラはシステムの起動時にデフォルトのポリシーを作成します。これらのデフォルトポリシーはグローバルなもので、双方向転送検出(BFD)の設定ポリシーです。デフォルト グローバルポリシー内の属性は、**作業**ウィンドウで設定できます。または、これらデフォルトのポリシーの値を変更することもできます。ただし、いったんデフォルトのグローバルポリシーを変更すると、システム全体(すべてのスイッチ)に影響することに注意してください。デフォルトではありませんが、特定のスイッチ (またはスイッチの設定) の特定の設定を使用する場合は、次の手順の説明に従って、スイッチのプロファイルを作成します。

ステップ 3 特定のグローバル BFD ポリシー（デフォルトではないもの）向けにスパイン スイッチ プロファイルを作成するには、[**ナビゲーション**（**Navigation**）] ペインで、**[スイッチ**（**Switches**）**]** > **[リーフ スイッチ**（**Leaf Switches**）**]** > **[プロファイル**（**Profiles**）**]**の順に展開します。
リーフ スイッチ - プロファイル（**Leaf Switches - Profiles**） 画面が [**作業**（**Work**）] ペインに表示されます。

ステップ 4 [**作業**（**Work**）] ペインの右側、アクション アイコンの下で、**リーフ プロファイルの作成**（**Create Leaf Profile**） を選択します。
[Create Leaf Profile] ダイアログボックスが表示されます。

ステップ 5 **Create Leaf Profile** ダイアログボックスで、次の操作を実行します:

a) **Name** フィールドに、リーフ スイッチ プロファイルの名前を入力します
b) （任意）[**説明**（**Description**）] フィールドに、プロファイルの説明を入力します。
c) （任意）[**リーフ セレクタ**（**Leaf Selectors**）] ツールバーで、[+] をクリックします。
d) [**名前**（**Name**）]（スイッチに名前を付けます）、[**ブロック**（**Blocks**）]（スイッチを選択します）、および [**ポリシー グループ**（**Policy Group**）]（[**アクセス スイッチ ポリシー グループの作成**（**Create Access Switch Policy Group**）]）に適切な値を入力します。
Create Access Switch Policy Group ダイアログボックスが表示されます。ここでは、ポリシー グループの識別プロパティを指定できます。

ステップ 6 (リーフセレクタを設定する場合）[**アクセス スイッチ ポリシー グループの作成**（**Create Access Switch Policy Group**）] ダイアログ ボックスで次のアクションを実行します。

a) [Name] フィールドにポリシー グループの名前を入力します。
b) （任意）[**説明**（**Description**）] フィールドで、ポリシー グループの説明を入力します。
c) BFD ポリシー タイプ (**BFD IPV4 Policy** または **BFD IPV6 Policy**) を選択し、値 (**default** または **Create BFD Global Ipv4 Policy**) を特定のスイッチまたはスイッチのセットに対して選択します。
d) [更新（Update）] をクリックします。

ステップ 7 [**次へ**（**Next**）] をクリックして [**関連付け**（**Associations**）] へ進みます。

（任意）[関連付け（Associations）] メニューで、リーフ プロファイルをリーフ インターフェイス プロファイルおよびアクセス モジュール プロファイルに関連付けることができます。

ステップ 8 [完了（Finish）] をクリックします。

BFD グローバルポリシーを作成するもう 1 つの方法は、**BFD IPV4** または **BFD IPV6** のいずれかを右クリックします (**Navigation** ウィンドウにあります)。

ステップ 9 作成した BFD グローバル コンフィギュレーションを確認するには、[**ナビゲーション**（**Navigation**）] ペインで、**[ポリシー**（**Policies**）**]** > **[スイッチ**（**Switch**）**]** > **[BFD]** の順に展開します。

GUI を使用してスパイン スイッチで BFD のグローバル設定

手順

ステップ 1 メニュー バーで、**[Fabric]** > **[Access Policies]** の順に選択します。

ステップ 2 [**ナビゲーション**（**Navigation**）] ペインで、 **[ポリシー（Policies）]** > **[スイッチ（Switch）]** > **[BFD]**の順に展開します。
設定を双方向フォワーディング検出 (BFD) には、使用可能な 2 つの種類があります:

- BFD IPV4
- BFD IPV6

これらのBFD設定ごとに、デフォルトポリシーを使用するか、特定のスイッチ(またはスイッチのセット) 用に新しいポリシーを作成できます。

（注） デフォルトでは、APICコントローラはシステムの起動時にデフォルトのポリシーを作成します。これらのデフォルトポリシーはグローバルなもので、双方向転送検出(BFD)の設定ポリシーです。デフォルト グローバルポリシー内の属性は、**作業**ウィンドウで設定できます。または、これらデフォルトのポリシーの値を変更することもできます。ただし、いったんデフォルトのグローバルポリシーを変更すると、システム全体(すべてのスイッチ)に影響することに注意してください。デフォルトではありませんが、特定のスイッチ (またはスイッチの設定) の特定の設定を使用する場合は、次の手順の説明に従って、スイッチのプロファイルを作成します。

ステップ 3 特定のグローバル BFD ポリシー（デフォルトではないもの）向けにスパイン スイッチ プロファイルを作成するには、[**ナビゲーション**（**Navigation**）]ペインで、**[スイッチ（Switches）]**> **[スパイン スイッチ（Spine Switches）]** > **[プロファイル（Profiles）]**の順に展開します。
スパイン スイッチ：**プロファイル** 画面が [**作業**（**Work**）] ペインに表示されます。

ステップ 4 [**作業**（**Work**）] ペインの右側、アクション アイコンの下で、[**スパイン プロファイルの作成**（**Create Spine Profile**）] を選択します。
Create Spine Profile ダイアログボックスが表示されます。

ステップ 5 **Create Spine Profile** ダイアログボックスで、次の操作を実行します:

a) **Name** フィールドに、スイッチ プロファイルの名前を入力します。
b) **Description**フィールドの隣にに、プロファイルの説明を入力します。（この手順は任意です）。
c) （任意）[スパイン セレクタ（Spine Selectors）] ツールバーで、[+] をクリックします。
d) [**名前**（**Name**）]（スイッチに名前を付けます）、[**ブロック**（**Blocks**）]（スイッチを選択します）、および [**ポリシー グループ**（**Policy Group**）]（[**スパイン スイッチ ポリシー グループの作成**（**Create Spine Switch Policy Group**）]）に適切な値を入力します。
スパイン スイッチ ポリシー グループの作成 ダイアログボックスはポリシー グループ id のプロパティを指定できますが表示されます。

ステップ 6 (スパイン セレクタを設定する場合）[**スパイン スイッチ ポリシー グループの作成**（**Create Spine Switch Policy Group**）] ダイアログ ボックスで次のアクションを実行します。

a) [Name] フィールドにポリシー グループの名前を入力します。
b) （任意）[**説明（Description**）] フィールドで、ポリシー グループの説明を入力します。
c) BFD ポリシー タイプ (**BFD IPV4 Policy** または **BFD IPV6 Policy**) を選択し、値 (**default** または **Create BFD Global Ipv4 Policy**) を特定のスイッチまたはスイッチのセットに対して選択します。
d) [更新（Update）] をクリックします。

ステップ 7 [**次へ（Next**）] をクリックして [**関連付け（Associations**）] へ進みます。

（任意）[関連付け（Associations）] メニューで、スパイン プロファイルをスパイン インターフェイス プロファイルに関連付けることができます。

ステップ 8 [完了（Finish）] をクリックします。

BFD グローバルポリシーを作成するもう 1 つの方法は、**BFD IPV4** または **BFD IPV6** のいずれかを右クリックします (**Navigation** ウィンドウにあります)。

ステップ 9 作成した BFD グローバル コンフィギュレーションを確認するには、[**ナビゲーション（Navigation**）] ペインで、**[ポリシー（Policies**）] > **[スイッチ（Switch**）] > **[BFD]** の順に展開します。

GUI を使用した BFD インターフェイスのオーバーライドの設定

明示的な双方向フォワーディング検出 (BFD) を設定できる、3 つのサポート対象のインターフェイス（ルーテッド レイヤ インターフェイス、外部インターフェイス SVI とルーテッド サブインターフェイス）があります。グローバル コンフィギュレーションを使用しないで、さらに特定のインターフェイスの明示的な設定をしたい場合、特定のスイッチまたは一連のすべてのインターフェイスに適用される独自のグローバル コンフィギュレーションを作成できます。特定のインターフェイス上の特定のスイッチの粒度がさらに必要な場合、このインターフェイス オーバーライド設定を使用する必要があります。

（注） BFD インターフェイス ポリシーが親ルーテッド インターフェイスに設定されている場合、デフォルトでは、親インターフェイスと同じアドレス ファミリを持つすべてのルーテッド サブインターフェイスがこのポリシーを継承します。継承された設定のいずれかを上書きする必要がある場合は、サブインターフェイスで明示的な BFD インターフェイス ポリシーを設定します。ただし、親インターフェイスで **Admin State** または **Echo Admin State** が無効になっている場合、サブインターフェイスでプロパティをオーバーライドすることはできません。

始める前に

テナントはすでに作成されています。

手順

ステップ 1 メニュー バーで、 **Tenant** を選択します。

ステップ 2 [**ナビゲーション（Navigation）**] ペイン (クイック スタートの下)、作成したテナント **[*Tenant_name*]** > **[ネットワー キング（Networking）]** > **[L3Outs]**を展開します。

ステップ 3 [**L3Outs**] を右クリックし、[**L3Out の作成（Create L3Out）**] を選択します。
[**L3Out の作成（Create L3Out）**] ウィザードが表示されます。

ステップ 4 [L3Out の作成（Create L3Out）] ウィザードの [識別（Identity）] ウィンドウに必要な情報を入力します。

a) [名前（Name）]、[VRF]、および [L3 ドメイン（L3 Domain）] フィールドに必要な情報を入力します。
b) ルーティング プロトコルのチェック ボックスがある領域で、[BGP] を選択します。
c) [**次（Next）**] をクリックして [**ノードとインターフェイス（Nodes and Interfaces**）] ウィンドウに移動します。

ステップ 5 [L3Out の作成（Create L3Out）] ウィザードの [ノードとインターフェイス（Nodes and Interfaces）] ウィンドウに必要な情報を入力します。

a) [レイヤ 3（Layer 3）] 領域で、[ルーテッド（Routed）] を選択します。
b) [**ノード ID（Node ID**）] フィールドのドロップダウン メニューで、L3Out のノードを選択します。

これらの例のトポロジでは、ノード `103` を使用します。

c) [Router ID] フィールドに、ルータ ID を入力します。
d) （任意） 必要に応じて、ループバック アドレスに別の IP アドレスを設定できます。

[ルータ ID（Router ID）] フィールドに入力したエントリと同じ内容が [ループバック アドレス（Loopback Address）] フィールドに自動で入力されます。これは以前のビルドでの [ループバック アドレスのルータ ID の使用（Use Router ID for Loopback Address）] と同等です。ループバック アドレスにルータ ID を使用しない場合は、ループバック アドレスに別の IP アドレスを入力します。または、ループバック アドレスにルータ ID を使用しない場合は、このフィールドを空のままにします。

e) [ノードとインターフェイス（Nodes and Interfaces）] ウィンドウに追加の必要な情報を入力します。

このウィンドウに表示されるフィールドは、[レイヤ 3（Layer 3）] および [レイヤ 2（Layer 2）] 領域で選択したオプションによって異なります。

f) [ノードとインターフェイス（Nodes and Interfaces）] ウィンドウで残りの追加の情報を入力したら、[次（Next）] をクリックします。

[**プロトコル（Protocols**）] ウィンドウが表示されます。

ステップ 6 [L3Out の作成（Create L3Out）] ウィザードの [プロトコル（Protocols）] ウィンドウに必要な情報を入力します。

a) [BGP ループバック ポリシー（BGP Loopback Policies）] および [BGP インターフェイス ポリシー（BGP Interface Policies）] 領域で、次の情報を入力します。

- **ピア アドレス（Peer Address）**：ピア IP アドレスを入力します
- **EBGP Multihop TTL（EBGP マルチホップ TTL）**：接続の存続可能時間（TTL）を入力します。範囲は 1 ー 255 ホップです。ゼロの場合、TTL は指定されません。デフォルトは 0 です。
- **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。

（注） ACI は asdot または asdot + 形式の AS 番号をサポートしていません。

b) [**OSPF**] 領域で、デフォルト OSPF ポリシー、以前に作成した OSPF ポリシー、または **[OSPF インターフェイス ポリシーの作成（Create OSPF Interface Policy）]** を選択します。

c) **[次へ（Next）]** をクリックします。

[**外部 EPG（External EPG）**] ウィンドウが表示されます。

ステップ 7 [L3Out の作成（Create L3Out）] ウィザードで [外部 EPG（External EPG）] ウィンドウに必要な情報を入力します。

a) **Name** フィールドに、外部ネットワークの名前を入力します。

b) [**提供済みコントラクト（Provided Contract**）] フィールドで、提供済みコントラクトの名前を入力します。

c) [**消費済みコントラクト（Consumed Contract**）] フィールドで、消費済みコントラクトの名前を入力します。

d) [すべての外部ネットワークのデフォルト EPG（Default EPG for all external network）] フィールドで、この L3Out 接続からのすべての中継ルートをアドバタイズしない場合はオフにします。

このボックスをオフにすると、[Subnets] 領域が表示されます。次の手順に従って、必要なサブネットとコントロールを指定します。

e) [完了（Finish）] をクリックして、[L3Out の作成（Create L3Out）] ウィザードに必要な設定の入力を完了させます。

ステップ 8 **[テナント（Tenants）] > [*tenant_name*] > [ネットワーキング（Networking）] > [L3Outs] > [*L3Out_name*] > [論理ノード プロファイル（Logical Node Profiles）] > [*logical_node_profile_name*] > [論理インターフェイス プロファイル（Logical Interface Profiles）] > [*logical_interface_profile_name*]** の順に移動します。

ステップ 9 [論理インターフェイス プロファイル（Logical Interface Profile）] ウィンドウで、[BFD インターフェイス プロファイルの作成（Create BFD Interface Profile）] フィールドまで下にスクロールし、このフィールドの横にあるボックスをオンにします。

ステップ 10 [**BFD インターフェイス プロファイルの作成（Create BFD Interface Profile**）] ウィンドウで、BFD の詳細を入力します。

- **認証タイプ** フィールドで、選択 **No authentication** または **キー SHA1** 。

  認証 (SHA1 のキーを選択) により、入力を選択すると、 **認証キー ID** を入力してください、 **の認証キーを** (パスワード)、再次を入力して、パスワードを確認 **キーの確認** 。

- [**BFD インターフェイス ポリシー（BFD Interface Policy**）] フィールドで、[**一般的な/デフォルト（common/default**）] 設定（デフォルト BFD ポリシー）のいずれかを選択、または、[**BFD インターフェイス ポリシーの作成（Create BFD Interface Policy**）] を選択することによって自分の BFD ポリシーを作成します。

  選択した場合 **BFD インターフェイス ポリシーの作成** 、 **BFD インターフェイス ポリシーの作成** BFD インターフェイス ポリシーの値を定義するダイアログボックスが表示されます。

ステップ 11 [Submit] をクリックします。

ステップ 12 設定したインターフェイス レベルの BFD ポリシーを確認するには、**[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[BFD]** に移動します。

GUI を使用して BFD コンシューマ プロトコルを設定する

この手順では、BFD機能の消費者であるコンシューマプロトコル(OSPF、BGP、EIGRP、スタティック ルート、および IS-IS) での双方向フォワーディング検出 (BFD) を有効にする方法を説明します。これらのプロトコルで BFD を使用するには、それらのフラグを有効にする必要があります。

（注） これらの 4 つのコンシューマ プロトコルは、左側のナビゲーション ペインの **[テナント（Tenant）]** > **[ポリシー（Policies）]** > **[プロトコル（Protocol）]** の下にあります。

始める前に

テナントはすでに作成されています。

手順

ステップ 1 [L3Out の作成（Create L3Out）] ウィザードを使用して L3Out を作成します。

ステップ 2 メニュー バーで、**[テナント（Tenant）]**を選択します。

ステップ 3 BGP プロトコルの BFD を設定するには、[**ナビゲーション（Navigation**）] ペイン（Quick Start の下）で、作成したテナント、**[*Tenant_name*]** > **[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[BGP]** > **[BGP ピア プレフィックス（BGP Peer Prefix）]** を展開します。

ステップ 4 **Work** ウィンドウの右側の **[ACTIONS]** の下で、**[Create BGP Peer Prefix Policy]** を選択します。**[Create BGP Peer Prefix Policy]** ダイアログボックスが表示されます。

（注） 左のナビゲーション ウィンドウで **[BGP Peer Prefix]** を右クリックして **[Create BGP Peer Prefix]** を選択し、ポリシーを作成することもできます。

ステップ 5 **[Name]** フィールドに名前を入力し、残りのフィールドに値を入力して BGP ピア プレフィックス ポリシーを定義します。

ステップ 6 **[送信（Submit）]** をクリックします。`
作成した BGP ピア プレフィックス ポリシーは、左のナビゲーション ウィンドウの **[BGP Peer Prefix]** の下に表示されます。

ステップ 7 **[テナント（Tenants）]** > **[*tenant_name*]** > **[ネットワーキング（Networking）]** > **[L3Outs]** > **[*L3Out_name*]** > **[論理ノード プロファイル（Logical Node Profiles）]** > **[*logical_node_profile_name*]** > **[論理インターフェイス プロファイル（Logical Interface Profiles）]** > **[*logical_interface_profile_name*]** > **[BGP ピア接続プロファイル（BGP Peer Connectivity Profile）]** の順に移動します。

ステップ 8 [BGP ピア接続プロファイル（BGP Peer Connectivity Profile）] ウィンドウで、[BGP ピア プレフィックス ポリシー（BGP Peer Prefix Policy）] フィールドまでスクロールし、作成した BGP ピア プレフィックス ポリシーを選択します。

ステップ 9 [**ピア制御（Peer Controls**）] フィールドで、[**双方向フォワーディング検出（Bidirectional Forwarding Detection**）] を選択して BGP コンシューマ プロトコルの BFD を有効にします（またはオフにして BFD を無効にします）。

ステップ 10 OSPF プロトコルの BFD を設定するには、[**ナビゲーション（Navigation**）] ペインで、**[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[OSPF]** > **[OSPF インターフェイス（OSPF Interface）]** に移動します。

ステップ 11 **Work** ウィンドウの右側の、**[ACTIONS]** の下で、**[Create OSPF Interface Policy]** を選択します。
[Create OSPF Interface Policy] ダイアログボックスが表示されます。

（注） 左のナビゲーション ウィンドウで **[OSPF Interface]** を右クリックして **[Create OSPF Interface Policy]** を選択し、ポリシーを作成することもできます。

ステップ 12 **[Name]** フィールドに名前を入力し、残りのフィールドに値を入力して OSPF インターフェイス ポリシーを定義します。

ステップ 13 このダイアログボックスの **[Interface Controls]** セクションでは、BFD の有効と無効を切り替えることができます。有効にするには、図のように、**[BFD]** の隣のボックスをオンにして OSPF コンシューマ プロトコルにフラグを追加します (またはボックスをオフにして BFD を無効にします)。

ステップ 14 **[送信（Submit）]** をクリックします。`

ステップ 15 EIGRP プロトコルの BFD を設定するには、[**ナビゲーション（Navigation**）] ペインで、**[*tenant_name*]** > **[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[EIGRP]** > **[EIGRP インターフェイス（EIGRP Interface）]** に移動します。

ステップ 16 **Work** ウィンドウの右側の、**[ACTIONS]** の下で、**[Create EIGRP Interface Policy]** を選択します。
[Create EIGRP Interface Policy] ダイアログボックスが表示されます。

（注） 左のナビゲーション ウィンドウで **[EIGRP Interface]** を右クリックして **[Create EIGRP Interface Policy]** を選択し、ポリシーを作成することもできます。

ステップ 17 **[Name]** フィールドに名前を入力し、残りのフィールドに値を入力して OSPF インターフェイス ポリシーを定義します。

ステップ 18 このダイアログボックスの **[Control State]** セクションでは、BFD の有効と無効を切り替えることができます。有効にするには、図のように、**[BFD]** の隣のボックスをオンにして EIGRP コンシューマ プロトコルにフラグを追加します (またはボックスをオフにして BFD を無効にします)。

ステップ 19 **[送信（Submit）]** をクリックします。`

ステップ 20 スタティック ルート プロトコルで BFD を設定するには、**[ナビゲーション（Navigation）]** ペインで **[ネットワーキング（Networking）] > [L3Outs] > [*L3Out_name*] > [設定済みのノード（Configured Nodes）]** に戻り、設定済みのノードをクリックして **[ノード関連付け（Node Association）]** ウィンドウを表示します。

ステップ 21 **[Static Routes]** セクションで、[+] (展開) ボタンをクリックします。
[Create Static Route] ダイアログボックスが表示されます。このセクションで、必要なフィールドの値を入力します。

ステップ 22 **[Route Control]** の隣で、**[BFD]** の隣のボックスをオンにして有効にします (または、無効にする場合にはオフにします)。

ステップ 23 **[送信（Submit）]** をクリックします。`

ステップ 24 IS-IS プロトコルの BFD を設定するには、**[ナビゲーション（Navigation）]** ペインで **[ファブリック（Fabric）] > [ファブリック ポリシー（Fabric Policies）] > [ポリシー（Policies）] > [インターフェイス（Interface）] > [L3 インターフェイス（L3 Interface）]** に移動します。

ステップ 25 **Work** ウィンドウの右側の、**[ACTIONS]** の下で、**[Create L3 Interface Policy]** を選択します。
[Create L3 Interface Policy] ダイアログボックスが表示されます。

（注） 左のナビゲーション ウィンドウで **[L3 Interface]** を右クリックして **[Create EIGRP Interface Policy]** を選択し、ポリシーを作成することもできます。

ステップ 26 **[Name]** フィールドに名前を入力し、残りのフィールドに値を入力して L3 インターフェイス ポリシーを定義します。

ステップ 27 BFD ISIS ポリシーを有効にするには、[BFD ISIS ポリシー設定（BFD ISIS Policy Configuration）] フィールドで **[有効化（enabled）]** をクリックします。

ステップ 28 [Submit] をクリックします。

BFD マルチホップ

BFD マルチホップでは、複数ホップ（最大 255 ホップ）の宛先に対する 1 秒未満の転送障害検出が可能になります。リリース 5.0(1) 以降、APIC は IPv4 の BFD マルチホップおよび IPv6 の BFD マルチホップを、RFC5883 に準拠してサポートします。BFD マルチホップ セッションは、固有のソースと宛先アドレス ペア間で設定されます。BFD マルチホップ セッションは、

シングルホップ BFD セッションの場合、インターフェイスではなく、送信元と宛先の間で作成されます。

BFD マルチホップは TTL フィールドを BGP によってサポートされる最大制限に設定し、受信時に値のチェックを行いません。ACI リーフは、BFD マルチホップ パケットが通過できるホップ数には影響しませんが、ホップ数は 255 に制限されます。

BFD マルチホップの注意事項と制約事項

- BFDマルチホップのデフォルトおよび最小送信/受信インターバル タイマーは 250 ミリ秒です。
- デフォルトの最小検出乗数は 3 です。
- エコー モードは BFD マルチホップではサポートされません。

BFD マルチホップ ポリシーの設定

ポリシーの目的に応じて、GUI の複数の場所で BFD マルチホップ ポリシーを設定できます。

- **グローバル ポリシー**：デフォルトでは、APIC コントローラはシステムの起動時にデフォルトのポリシーを作成します。これらのデフォルト ポリシーは、グローバル BFD マルチホップ設定ポリシーです。デフォルト グローバル ポリシー内の属性は、[作業（Work）] ペインで設定できます。または、これらデフォルトのポリシーの値を変更することもできます。ただし、いったんデフォルトのグローバル ポリシーを変更すると、システム全体(すべてのスイッチ)に影響が及びます。デフォルトではありませんが、特定のスイッチまたはスイッチのセットの特定の設定を使用する場合は、スイッチ プロファイルを作成し、そのスイッチ プロファイル内で BFD マルチホップの値を変更します。

  次の GUI の場所で、IPv4 または IPv6 のグローバル BFD マルチホップ設定ポリシーを作成または変更できます。

  - [ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）] > [ポリシー（Policies）] > [スイッチ（Switch）] > [BFD マルチホップ（BFD Multihop）] > [BFD マルチホップ IPv4（BFD Multihop IPv4)] : [BFD グローバル IPv4 MH ポリシーの作成（Create BFD Global IPv4 MH Policy）] を右クリックして選択します。
  - [ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）] > [ポリシー（Policies）] > [スイッチ（Switch）] > [BFD マルチホップ（BFD Multihop）] > [BFD マルチホップ IPv6（BFD Multihop IPv6)] : [BFD グローバル IPv6 MH ポリシーの作成（Create BFD Global IPv6 MH Policy）] を右クリックして選択します。

- ノード ポリシー：BFD マルチホップ ノード ポリシーは、ノード プロファイルの下のインターフェイスに適用されます。

  この GUI の場所で BFD マルチホップ ノード ポリシーを作成または変更できます。

  - [テナント（Tenants）] > [テナント（tenant）] > [ポリシー（Policies）] > [プロトコル（Protocol）] > [BFD マルチホップ（BFD Multihop）] > [ノード ポリシー（Node

Policies）]：[BFD マルチホップ ノード ポリシーの作成（Create BFD Multihop Node Policy）] を右クリックして選択します。

- インターフェイス ポリシー：BFD マルチホップ インターフェイス ポリシーは、インターフェイス プロファイルの下のインターフェイスに適用されます。

  この GUI の場所で BFD マルチホップ インターフェイス ポリシーを作成または変更できます。

  - [テナント（Tenants）] > [テナント（tenant）] > [ポリシー（Policies）] > [プロトコル（Protocol）] > [BFD マルチホップ（BFD Multihop）] > [インターフェイス ポリシー（Interface Policies）]：[BFD マルチホップ インターフェイス ポリシーの作成（Create BFD Multihop Interface Policy）] を右クリックして選択します。

- グローバル ポリシーの上書き：デフォルトのグローバル設定を使用せず、特定のインターフェイスで明示的な設定を行う場合は、独自のグローバル設定を作成できます。この設定は、特定のスイッチまたはスイッチセットのすべてのインターフェイスに適用されます。特定のインターフェイス上の特定のスイッチの粒度がさらに必要な場合、このインターフェイス オーバーライド設定を使用する必要があります。

  次の GUI ロケーションで、ノード プロファイルまたはインターフェイス プロファイルの BFD マルチホップ オーバーライド ポリシーを作成または変更できます。

  - [テナント（Tenants）] > [テナント（tenant）] > [ネットワーキング（Networking）] > [L3Outs] > [l3out] > [論理ノード プロファイル（Logical Node Profiles）] > [logical_node_profile]：[BFD インターフェイス プロトコル プロファイルの作成（Create BFD Interface Protocol Profile）] を右クリックして選択し、BFD マルチホップ ノード ポリシーを指定します。

  - [テナント（Tenants）] > [テナント（tenant）] > [ネットワーキング（Networking）] > [L3Outs] > [l3out] > [論理ノード プロファイル（Logical Node Profiles）] > [logical_node_profile] > [論理インターフェイス プロファイル（Logical Interface Profiles）] > [logical_interface_profile]：[MH-BFD インターフェイス プロトコル プロファイルの作成（Create MH-BFD Interface Protocol Profile）] を右クリックして選択し、BFD マルチホップ インターフェイス ポリシーを指定します。

  - [テナント（Tenants）] > [インフラ（infra）] > [ネットワーキング（Networking）] > [SR-MPLS Infra L3Outs] > [l3out] > [論理ノード プロファイル（Logical Node Profiles）] > [logical_node_profile] > [論理インターフェイス プロファイル（Logical Interface Profiles）] > [logical_interface_profile]：[MH-BFD インターフェイス プロトコル プロファイルの作成（Create MH-BFD Interface Protocol Profile）] を右クリックして選択し、BFD マルチホップ インターフェイス ポリシーを指定します。

手順

ステップ 1 BFD マルチホップ ポリシーを作成または設定する GUI の場所に移動します。

ステップ 2 既存のプロファイルまたはポリシーを編集するか、ダイアログボックスを起動して新しいプロファイルを作成します。

ステップ 3 プロファイルで、BFD マルチホップ セッションの [認証タイプ（Authentication Type）] を選択します。

認証なしまたは SHA-1 認証を要求するように選択できます。

ステップ 4 新しいポリシーを作成する場合は、ダイアログ ボックスで設定を行います。

a) ポリシーの [**名前（Name）**] を入力します。

b) [管理状態（Admin State）] を [有効（Enabled）] に設定します。

c) [検出乗数（Detection Multiplier）] の値を設定します。

セッションがダウンしたと BFD が宣言する前に失われた可能性のある連続するパケットの最小数を指定します。範囲は 1 ～ 50 パケットです。デフォルトは 3 です。

d) [最小送信間隔（Minimum Transit Interval）] の値を設定します。

送信されるパケットの最小間隔時間。指定できる範囲は 250 ～ 999 ミリ秒です。デフォルトは 250 です。

e) [最大受信間隔（Maximum Receive Interval）] の値を設定します。

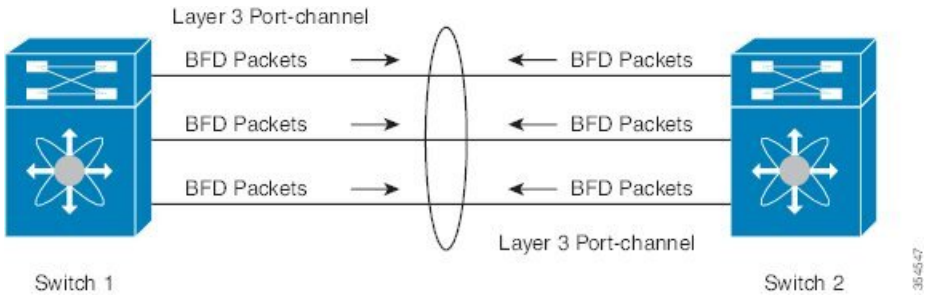
受信されたパケットの最大インターバル時間。指定できる範囲は 250 ～ 999 ミリ秒です。デフォルトは 250 です。

f) [Submit] をクリックします。

マイクロ BFD

Cisco APIC リリース 5.2(3) 以降、IETF RFC 7130 で定義されているように、APIC は マイクロ BFD をサポートします。Bidirectional Forwarding Detection（BFD）がポート チャネルで設定されている場合、キープアライブ パケットは使用可能なメンバー リンクで送信されます。キープアライブ パケットは残りのリンクを通過するだけであるため、単一のメンバー リンクの障害は検出されない場合があります。マイクロ BFD は、次の図に示すように、ポート チャネルの各メンバー リンクで個別の BFD セッションを確立する BFD の拡張機能です。

図 *42*：マイクロ *BFD* ポート チャネルでのセッション



リンク単位の BFD セッションがメンバー リンクで障害を検知すると、障害が発生したリンクは転送テーブルから削除されます。このメカニズムは、障害検出を高速化し、ポートチャネルで障害が発生したリンクを特定します。

に関する注意事項と制限事項 マイクロ BFD

- マイクロ BFD は、LACP ポートチャネルと非 LACP ポートチャネルの両方でサポートされます。
- マイクロ BFD は、同じポート チャネルでマルチホップ BFD と同時に実行できますが、シングルホップ BFD では実行できません。
- マイクロ BFD は、シングルホップ BFD 実装です。スイッチのメイン ポート チャネルとスイッチのピアの間にレイヤ 2 スイッチが存在する場合は機能しません。
- マイクロ BFD は、第 1 世代のリーフ スイッチではサポートされていません。第 1 世代のスイッチは、PID（製品識別子）に -EX や -FX などのサフィックスが含まれていないスイッチです。
- マイクロ BFD は、ポート チャネル上のルーテッド インターフェイスでのみサポートされます。
- クライアント プロトコルは、マイクロ BFD が有効になっている同じポート チャネル上のサブインターフェイスで実行できます。
- マイクロ BFD は、FEX ポートまたはファブリック ポートではサポートされません。
- BFD エコーは、マイクロ BFD セッションではサポートされません。
- マイクロ BFD が有効になっているデュアル IP スタック ポート チャネル（IPv4 および IPv6）では、IPv4 アドレスまたは IPv6 アドレスのいずれかを使用して マイクロ BFD を設定する必要がありますが、両方は必須ではありません。IPv4 と IPv6 の両方の マイクロ BFD セッションを設定することはできません。
- Cisco APIC リリース 5.2(3) 以降、Cisco APIC では、L3 ポート チャネルのメイン インターフェイスと同じ L3 ポート チャネル上のサブインターフェイスを使用できます。ただし、L3 ポート チャネルのメイン インターフェイスを作成または削除すると、ポート チャネルの物理メンバー ポートがフラップします。これにより、ポート チャネル サブインターフェイスがすでにアクティブな場合、トラフィックが失われます。

ポート チャネルでの マイクロ BFD の設定

この手順では、L3Outポートチャネルインターフェイスを有効に変更します。ポートチャネルの各メンバーリンクで個別のBFDセッションを確立します。マイクロ BFD マイクロ BFD

始める前に

- ダイレクト ポート チャネルが L3Out インターフェイスに設定されています。

手順

ステップ 1 **[テナント（Tenants）]** > **[*tenant_name*]** > **[ネットワーキング（Networking）]** > **[L3Outs]** > **[*L3Out_name*]** > **[論理ノード プロファイル（Logical Node Profiles]）** > **[*logical_node_profile_name*]** > **[論理インターフェイス プロファイル（Logical Interface Profiles）]**の順に移動します。

ステップ 2 変更する [論理インターフェイス プロファイル（Logical Interface Profile）] を選択します。

ステップ 3 [ルーテッド インターフェイス（Routed Interfaces）] タブを選択します。

マイクロ BFD は、ポート チャネル上のルーテッド インターフェイスでのみサポートされます。

ステップ 4 [ルーテッドインターフェイス（Routed Interfaces）]セクションで、既存のインターフェイスをダブル クリックして変更するか、[+] アイコンをクリックして新しいインターフェイスを論理インターフェイス プロファイルに追加します。

この手順の残りの手順では、既存の論理インターフェイスでのイネーブル化についてのみ説明します。マイクロ BFD 論理インターフェイス プロファイルに新しいインターフェイスを追加する場合は、GUI を使用した L3Out のインターフェイスの変更 （297 ページ） を参照してください。

ステップ 5 選択したインターフェイスの設定済みプロパティで、選択した [パス タイプ（Path Type）] が [ダイレクト ポート チャネル（Direct Port Channel）] であることを確認します。

マイクロ BFD は、ポート チャネルでのみ適用できます。

ステップ 6 [Micro BFD の有効化（Enable Micro BFD）] チェックボックスをオンにします。

ステップ 7 [Micro BFD 宛先アドレス（Micro BFD Destination Address）] にポート チャネルの宛先 IP アドレスを入力します。

ステップ 8 [Micro BFD 開始タイマー（秒）（Micro BFD Start Timer（sec））]に 60 ー 3600 秒の値を入力します。

開始タイマーは、BFD セッションの確立を可能にするためにメンバー リンクでの BFD モニタリングのアクティブ化を遅延させます。タイマーはオプションです。タイマーが設定されていない場合、アクティベーションは遅延しません。

ステップ 9 **[送信（Submit）]** をクリックします。`

次のタスク

次の例に示すように、CLI を使用して マイクロ BFD セッションを確認できます。

```
leaf4# show port-channel database interface port-channel 3
port-channel3
Last membership update is successful
4 ports in total, 4 ports up
First operational port is Ethernet1/44
Age of the port-channel is 0d:22h:46m:03s
```

```
Time since last bundle is 0d:22h:42m:43s
Last bundled member is Ethernet1/44
Ports: Ethernet1/41 [on] [up]
Ethernet1/42 [on] [up]
Ethernet1/43 [on] [up]
Ethernet1/44 [on] [up] *

leaf4# show bfd neighbors vrf tenant1:vrf1

OurAddr NeighAddr
LD/RD RH/RS Holdown(mult) State Int Vrf Type

2003:190:190:1::1 2003:190:190:1::2
1090519041/0 Up 6000(3) Up Po3 tenant1:vrf1 singlehop

2003:190:190:1::1 2003:190:190:1::2
1090519042/2148074790 Up 180(3) Up Eth1/44 tenant1:vrf1 singlehop

2003:190:190:1::1 2003:190:190:1::2
1090519043/2148074787 Up 180(3) Up Eth1/41 tenant1:vrf1 singlehop

2003:190:190:1::1 2003:190:190:1::2
1090519044/2148074789 Up 180(3) Up Eth1/43 tenant1:vrf1 singlehop

2003:190:190:1::1 2003:190:190:1::2
1090519045/2148074788 Up 180(3) Up Eth1/42 tenant1:vrf1 singlehop
```

OSPF 外部ルーテッド ネットワーク

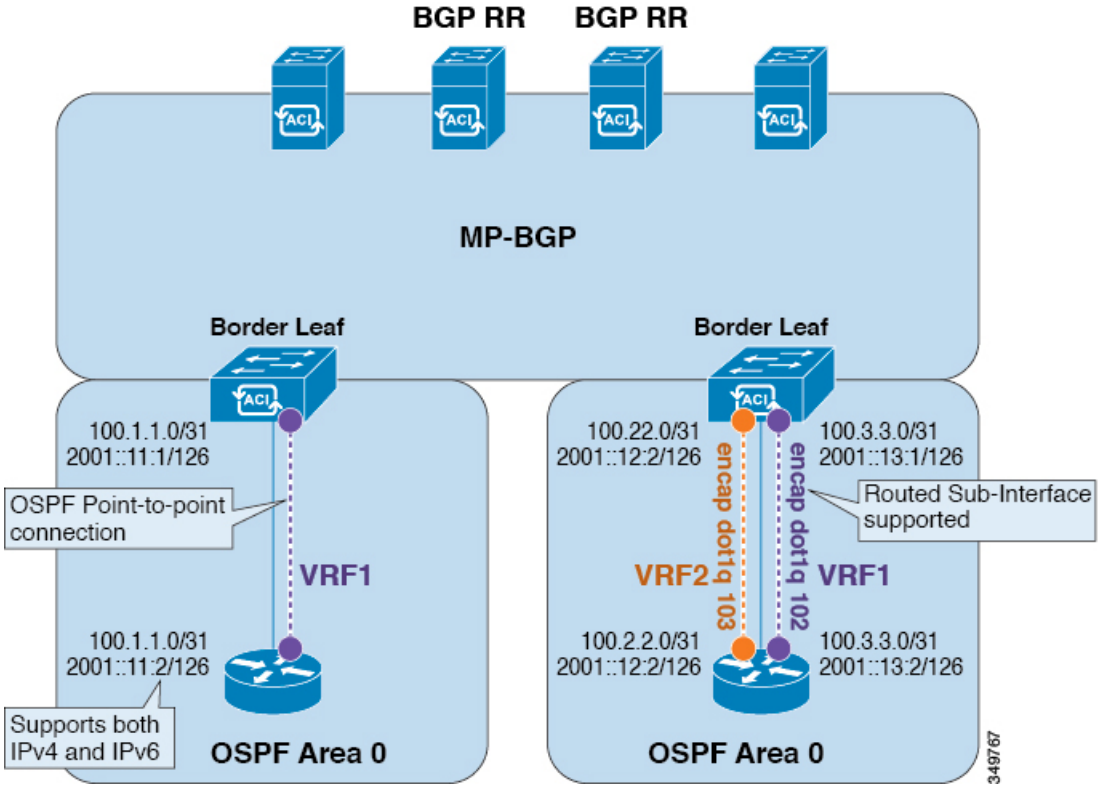
OSPF 外部ルーテッド ネットワークを設定するには、次の項の手順を使用します。

OSPF レイヤ 3 Outside 接続

OSPF レイヤ 3 Outside 接続は、標準または NSSA エリアです。バックボーン（エリア 0）エリアも、OSPF レイヤ 3 Outside 接続エリアとしてサポートされます。Cisco Application Centric Infrastructure（ACI）は、IPv4 の OSPFv2 と IPv6 の OSPFv3 の両方をサポートします。OSPF レイヤ 3 Outside を作成するときに、OSPF バージョンを設定する必要はありません。インターフェイス プロファイル設定（IPv4 または IPv6 アドレッシング）に基づいて、正しい OSPF プロセスが自動的に作成されます。IPv4 と IPv6 の両方のプロトコルが同じインターフェイス（デュアル スタック）でサポートされますが、2 つの個別インターフェイス プロファイルを作成する必要があります。

レイヤ 3 Outside 接続は、ルーテッド インターフェイス、ルーテッド サブインターフェイス、および SVI でサポートされます。SVI は、レイヤ 2 とレイヤ 3 両方のトラフィックで物理接続を共有する必要がある場合に使用されます。SVI は、物理ポート、ポート チャネル、および仮想ポート チャネルでサポートされています。

図 *43 : OSPF* レイヤ *3 Out* 接続



SVI がレイヤ 3 Outside 接続に使用されると、外部ブリッジ ドメインが境界リーフ スイッチに作成されます。外部ブリッジ ドメインは、Cisco ACI ファブリック上の 2 つの vPC スイッチ間の接続を可能にします。これにより、両方の vPC スイッチが、相互の、および外部 OSPF デバイスとの OSPF 隣接関係を確立できます。

ブロードキャスト ネットワークで OSPF を実行する場合、障害が発生したネイバーを検出する時間は dead 間隔（デフォルトは 40 秒）です。障害が発生した後でネイバー隣接関係を再確立する場合にも、代表ルータ（DR）の選定が原因で時間がかかる可能性があります。

（注）

- 1 つの vPC ノードへのリンクまたはポート チャネルに障害が発生しても、OSPF 隣接関係がダウンすることはありません。OSPF 隣接関係は、その他の vPC ノードを介してアクセスできる外部ブリッジ ドメインによりアップ状態を維持することができます。
- OSPF 時間ポリシーまたは OSPF、または EIGRP アドレス ファミリ ポリシーが L3Out に適用されると、次の動作を観察できます。
  - L3Out とポリシーが同じテナントで定義されている場合、動作に変更はありません。
  - 共通テナント以外のユーザー テナントで L3Out が設定されている場合、L3Out VRF インスタンスは共通テナントに解決され、ポリシーが共通テナントで定義されている場合、デフォルト値のみが適用されます。ポリシーの変更は有効になりません。
- 境界リーフ スイッチが 2 つの外部スイッチと OSPF 隣接関係を形成し、2 つのスイッチの 1 つでルート損失が発生し、隣接スイッチでは発生しない場合、Cisco ACI 境界リーフ スイッチは両方のネイバーのルートを再コンバージェンスします。
- OSPF はアグレッシブ タイマーをサポートします。ただし、これらのタイマーはすぐに隣接関係を損なうので、CPUの使用率急増を引き起こします。したがって、デフォルトのタイマーを使用し、双方向転送検出（BFD）を使用して 1 秒未満の障害検出を行うことを推奨します。

GUI を使用した管理テナントの OSPF L3Out の作成

- ルータ ID と論理インターフェイス プロファイルの IP アドレスが異なっていて重複していないことを確認します。
- 次の手順は、管理テナントの OSPF L3Out を作成するためのものです。テナントの OSPF L3Out を作成するには、テナントを選択し、テナント用の VRF を作成する必要があります。
- 詳細については、『*Cisco APIC and Transit Routing*』を参照してください。

手順

ステップ 1 メニュー バーで、**[Tenants]** > **[mgmt]** の順に選択します。

ステップ 2 [**ナビゲーション**（**Navigation**）] ペインで、**ネットワーキング**（**Networking**）>**L3Outs** を展開します。

ステップ 3 [L3Outs] を右クリックし、[L3Out の作成（Create L3Out）] をクリックします。

[**L3Out の作成**（**Create L3Out**）] ウィザードが表示されます。

ステップ 4 [L3Out の作成（Create L3Out）] ウィザードの [識別（Identity）] ウィンドウで、次の操作を実行します。

a) [Name] フィールドに、名前（RtdOut）を入力します。
b) [VRF] フィールドのドロップダウン リストから、VRF（inb）を選択します。

（注） このステップでは、ルーテッド Outside をインバンド VRF に関連付けます。

c) [L3 ドメイン（L3 Domain）] ドロップダウン リストから、適切なドメインを選択します。
d) [OSPF] チェックボックスをオンにします。
e) [OSPF Area ID] フィールドに、エリア ID を入力します。
f) [OSPF Area Control] フィールドで、適切なチェックボックスをオンにします。
g) [OSPF Area Type] フィールドで、適切なエリア タイプを選択します。
h) [OSPF Area Cost] フィールドで、適切な値を選択します。
i) **[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。

ステップ 5 [ノードとインターフェイス（Nodes and Interfaces）] ウィンドウで、次の操作を実行します。

a) [デフォルトを使用（Use Defaults）] ボックスをオフにします。

これにより、[ノードプロファイル名（Node Profile Name）] フィールドを編集できます。

b) [**ノード プロファイル名（Node Profile Name**）] フィールドに、ノードプロファイルの名前を入力します（borderLeaf）。
c) [Node ID] フィールドで、ドロップダウン リストから、最初のノードを選択します（leaf1）。
d) [Router ID] フィールドに、一意のルータ ID を入力します。
e) ループバック アドレスにルータ ID を使用しない場合は、[ループバック アドレス（Loopback Address）] フィールドで別の IP アドレスを使用するか、空のままにします。

（注） [ルータ ID（Router ID）] フィールドに入力したエントリと同じ内容が [ループバック アドレス（Loopback Address）] フィールドに自動で入力されます。これは以前のビルドでの [ループバック アドレスのルータ ID の使用（Use Router ID for Loopback Address）] と同等です。ループバック アドレスにルータ ID を使用しない場合は、別の IP アドレスを使用するか、このフィールドを空のままにします。

f) 必要に応じて、このノードの [インターフェイス（Interface）]、[IP アドレス（IP Address）]、[インターフェイス プロファイル名（Interface Profile Name）]、および [MTU] フィールドに適切な情報を入力します。
g) [ノード（Nodes）] フィールドで、[+] アイコンをクリックして、別のノードの 2 番目のフィールド セットを追加します。

（注） 2 つ目のノード ID を追加します。

h) [Node ID] フィールドで、ドロップダウン リストから、最初のノードを選択します（leaf1）。
i) [Router ID] フィールドに、一意のルータ ID を入力します。
j) ループバック アドレスにルータ ID を使用しない場合は、[ループバック アドレス（Loopback Address）] フィールドで別の IP アドレスを使用するか、空のままにします。

（注） [ルータ ID（Router ID）] フィールドに入力したエントリと同じ内容が [ループバック アドレス（Loopback Address）] フィールドに自動で入力されます。これは以前のビルドでの [ループバック アドレスのルータ ID の使用（Use Router ID for Loopback Address）] と同等です。ループバック アドレスにルータ ID を使用しない場合は、別の IP アドレスを使用するか、このフィールドを空のままにします。

k) 必要に応じて、このノードの [インターフェイス（Interface）]、[IP アドレス（IP Address）]、[インターフェイス プロファイル名（Interface Profile Name）]、および [MTU] フィールドに適切な情報を入力します。
l) **[次へ（Next）]** をクリックします。

[**プロトコル（Protocols**）] ウィンドウが表示されます。

ステップ 6 [プロトコル（Protocols）] ウィンドウの [ポリシー（Policy）] 領域で、[デフォルト（default）] をクリックし、[次（Next）] をクリックします。

[**外部 EPG（External EPG**）] ウィンドウが表示されます。

ステップ 7 [外部 EPG（External EPG）] ウィンドウで次のアクションを実行します。

a) [Name] フィールドに、外部ネットワークの名前（extMgmt）を入力します。
b) [すべての外部ネットワークのデフォルト EPG（Default EPG for all external network）]フィールドをオフにします。

[サブネット（Subnets）] 領域が表示されます。

c) [+] をクリックして [サブネットの作成（Create Subnet）] ダイアログ ボックスにアクセスします。
d) [サブネットの作成（Create Subnet）] ダイアログ ボックスで、[IP アドレス（IP address）] フィールドに、サブネットの IP アドレスとマスクを入力します。
e) [Scope] フィールドで、目的のチェックボックスをオンにします。[OK] をクリックします。
f) [外部 EPG（External EPG）] ダイアログ ボックスで、[完了（Finish）]をクリックします。

（注） [作業（Work）] ペインの [L3Outs] 領域に、[L3Out] アイコン（RtdOut）が表示されます。

EIGRP 外部ルーテッド ネットワーク

EIGRP 外部ルーテッド ネットワークを設定するには、次の項の手順を使用します。

EIGRP レイヤ 3 Outside 接続について

この例は、Cisco APIC を使用して、拡張内部ゲートウェイ ルーティング プロトコル（EIGRP）を設定する方法を示しています。次の情報は、EIGRP を設定するときに適用されます:

- テナント、VRF、およびブリッジ ドメインがすでに作成されている必要があります。
- レイヤ 3 外部テナント ネットワークがすでに設定されている必要があります。
- 外部ルーテッドのルート制御プロファイルがすでに設定されている必要があります。
- EIGRP VRF ポリシーは EIGRP ファミリ コンテキスト ポリシーと同じです。
- EIGRP はエクスポート ルート制御プロファイルをサポートしています。ルート制御に関する設定はすべてのプロトコルで共通です。

サブネット ルートをネットワーク レベルのルートへ自動的に要約するよう（ルート要約）、EIGRP を設定できます。たとえば、192.31.7.0 のサブネットが設定されているインターフェイス上で、サブネット 131.108.1.0 が 131.108.0.0 としてアドバタイズされるように設定することができます。自動集約は、EIGRP プロセスに設定されているネットワーク ルータ設定コマンドが 2 つまたはそれ以上ある場合に実行されます。デフォルトでは、この機能は有効です。詳細については、「*Route Summarization*」を参照してください。

EIGRP プロトコルのサポート

EIGRP プロトコルは、Cisco Application Centric Infrastructure（ACI）ファブリック内の他のルーティング プロトコルと同様にモデル化されています。

サポートされる機能

サポートされる機能は次のとおりです。

- IPv4 および IPv6 ルーティング
- 各アドレス ファミリの仮想ルーティングおよび転送（VRF）とインターフェイスの制御
- ノード間の OSPF による再配布
- VRF ごとのデフォルト ルート リーク ポリシー
- パッシブ インターフェイスおよびスプリット ホライズンのサポート
- エクスポートされたルートにタグを設定するためのルート マップ制御
- EIGRP インターフェイス ポリシーの帯域幅および遅延設定オプション

- 認証サポート

サポートされない機能

次の機能はサポートされていません。

- スタブ ルーティング
- BGP 接続に使用される EIGRP
- 同じノード上の複数の EIGRP `L3extOut`
- インターフェイスごとの集約（EIGRP サマリー ポリシーは、L3Out で設定されたすべてのインターフェイスに適用されます）
- インターフェイスごとのインポートおよびエクスポート用配布リスト

EIGRP 機能のカテゴリ

EIGRP の機能は、次のように大きく分類できます。

- プロトコル ポリシー
- `L3extOut` の設定
- インターフェイス設定
- ルート マップ サポート
- デフォルト ルート サポート
- 中継サポート

EIGRP をサポートしているプライマリ管理対象オブジェクト

次のプライマリ管理対象オブジェクトは、EIGRP サポートを提供します。

- .**EIGRP アドレス ファミリ コンテキスト ポリシー** `eigrpCtxAfPol`：`fvTenant`（テナント/プロトコル）で設定されているアドレス ファミリ コンテキスト ポリシー
- `fvRsCtxToEigrpCtxAfPol`：所定のアドレス ファミリ（IPv4 または Ipv6）についての VRF から `eigrpCtxAfPol` への関係。関係は、アドレス ファミリごとに 1 つのみ存在できます。
- `eigrpIfPol`：`fvTenant` で設定される EIGRP インターフェイス ポリシー。
- `eigrpExtP`：`L3extOut` 上で EIGRP のフラグを有効にします。
- `eigrpIfP`：`l3extLIfP` に接続された EIGRP インターフェイス プロファイル。
- `eigrpRsIfPol`：EIGRP インターフェイス プロファイルから `eigrpIfPol` への関係。
- `Defrtleak`：`l3extOut` 下のデフォルト ルート リーク ポリシー。

テナントでサポートされる EIGRP プロトコル ポリシー

テナント下では次の EIGRP プロトコル ポリシーがサポートされます。

- **EIGRP インターフェイス ポリシー（`eigrpIfPol`）**：インターフェイス上の所定のアドレス ファミリに適用される設定が含まれます。インターフェイス ポリシーでは次の設定が可能です。
  - 秒単位の *hello* 間隔
  - 分単位の *hold* 間隔
  - 次のインターフェイス制御フラグのうち 1 つ以上。
    - スプリット ホライズン
    - パッシブ
    - ネクスト ホップ セルフ

- **EIGRP アドレス ファミリ コンテキスト ポリシー（`eigrpCtxAfPol`）**：所定の VRF 内の所定のアドレス ファミリの設定が含まれます。`eigrpCtxAfPol` は、テナント プロトコル ポリシー下で設定され、テナント下の 1 つ以上の VRF に適用できます。`eigrpCtxAfPol` は、VRF-per-address ファミリの関係を通して VRF で有効にできます。所定のアドレス ファミリに関係がない場合、あるいは関係に記述されている `eigrpCtxAfPol` が存在しない場合は、`[共通]` テナント下に作成されたデフォルトの VRF ポリシーがそのアドレス ファミリに使用されます。

  次の設定では、`eigrpCtxAfPol` で許可されます。
  - 内部ルートのアドミニストレーティブ ディスタンス
  - 外部ルートのアドミニストレーティブ ディスタンス
  - 最大許容 ECMP パス数
  - アクティブ タイマー間隔
  - メトリック バージョン（32 ビット/64 ビット メトリック）

ガイドラインと EIGRP を設定するときの制限事項

EIGRP を設定する場合は、次の注意事項に従ってください。

- 外部同じレイヤ 3 の EIGRP および BGP を設定することはサポートされていません。
- 外部同じレイヤ 3 の EIGRP や OSPF を設定することはサポートされていません。
- 1 つ EIGRP レイヤ 3 Out VRF あたりノードごとできますがあります。ノードで複数の Vrf を導入している場合、自身レイヤ 3 Out 各 VRF ことができます。
- 複数の EIGRP ピア、1 つレイヤ 3 Out からがサポートされます。これにより、1 つレイヤ 3 Out と同じノードから複数の EIGRP デバイスに接続できます。

次の設定では、EIGRP ネイバーがフラップします。

- VRF の EIGRP アドレス ファミリ コンテキストによるアドミニストレーティブ ディスタンスまたはメトリック スタイル（ワイド/ナロー）の変更
- 内部で使用されるテーブルマップを更新する次の設定を設定します。
  - VRF のルート タグの変更
  - EIGRP L3Out と同じ境界リーフ スイッチ上の同じ VRF 内の OSPF L3Out のインポート方向ルート制御の設定の設定（たとえば、ルート制御適用「インポート」オプションの有効化または無効化、インポート方向）。この機能は EIGRP ではサポートされていないため、このような設定は EIGRP L3Out 自体では許可されないことに注意してください。ただし、OSPF L3Out の設定は、同じ VRF とリーフ スイッチの EIGRP L3Out に影響を与えます。これは、OSPF のインポート ルート制御が、同じ境界リーフ スイッチ上の同じ VRF の EIGRP と他の目的で共有されるテーブル マップを使用するためです。

GUI を使用したEIGRPの設定

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** ウィンドウで、テナントをダブルクリックします。

ステップ 3 [**ナビゲーション**（**Navigation**）] ペインで、**[*Tenant_name*]** > **[ポリシー**（**Policies**）**]** > **[プロトコル**（**Protocol**）**]** > **[EIGRP]** を展開します。

ステップ 4 右クリックして **EIGRP アドレス ファミリ コンテキスト**] を選択します **EIGRP アドレス ファミリ コンテキストのポリシーを作成** します。

ステップ 5 **Create EIGRP Address Family Context Policy** ダイアログボックスで、以下の操作を実行します:

a) **Name** フィールドに、コンテキスト ポリシーの名前を入力します。
b) **アクティブ間隔 (分)** フィールドで、インターバル タイマーを選択します。
c) **外部距離** 、および **内部距離** フィールドで、適切な値を選択します。
d) **パスの上限** フィールドで、[インターフェイス (ノードごと/リーフ スイッチごと) 間の値を適切なロード バランシングを選択します。
e) **メトリック スタイル** フィールドで、適切なメトリック スタイルを選択します。[Submit] をクリックします。`

Work ウィンドウに、コンテキスト ポリシーの詳細が表示されます。

ステップ 6 VRF のコンテキスト ポリシーを適用する、 **ナビゲーション**] ペインで、[展開 **ネットワー キング** > **Vrf** 。

ステップ 7 適切な VRF を選択し、[**作業**（**Work**）] ペインの [**ポリシー**（**Policy**）] タブで [**アドレス ファミリごとの EIGRP コンテキスト**（**EIGRP Context Per Address Family**）] を展開します。

ステップ 8 **EIGRP アドレス ファミリ タイプ** ドロップダウンリスト、IP バージョンを選択します。

ステップ 9 **EIGRP アドレス ファミリ コンテキスト** ドロップダウンリスト、コンテキスト ポリシーを選択します。**Update** をクリックし、**Submit** をクリックします。

ステップ 10 レイヤ 3 Out 内の EIGRP を有効にするには、[**ナビゲーション（Navigation**）] ペインで、**[ネットワーキング（Networking**）**] > [L3Out]**をクリックして目的のレイヤ 3 外部ネットワークをクリックします。

ステップ 11 [**作業（Work**）] ペインの [**ポシリー（Policy**）] タブで [**EIGRP**] のチェックボックスをオンにして EIGRP 自律システム番号を入力します。**[送信（Submit**）**]** をクリックします。`

ステップ 12 EIGRPインターフェイスポリシーを作成するには、[**ナビゲーション（Navigation**）ペインで、**[*Tenant_name*] > [ポリシー（Policies**）**] > [プロトコル（Protocol**）**] > [EIGRP]** をクリックして次のアクションを実行します。

a) 右クリックして **EIGRP インターフェイス** 、をクリックし、 **EIGRP インターフェイス ポリシーの作成** します。

b) **Create EIGRP Interface Policy** ダイアログボックスで、**Name** フィールドにポリシーの名前を入力します。

c) **制御状態** フィールドは、1 つまたは複数の制御を有効にする目的のチェック ボックスをチェックします。

d) **Helloインターバル (秒)** フィールドで、目的の間隔を選択します。

e) **保留間隔 (秒)** フィールドで、目的の間隔を選択します。[Submit] をクリックします。`

f) **Bandwidth** フィールドで、目的の帯域幅を選択します。

g) **遅延** フィールドで、10 マイクロ秒またはピコセル秒で、目的の遅延を選択します。

作業] ペインで、EIGRP インターフェイス ポリシーの詳細が表示されます。

ステップ 13 **ナビゲーション**] ペインで、適切な外部ルーテッド ネットワークの EIGRP が有効になってクリック展開 **論理ノード プロファイル** および次の操作の実行します。

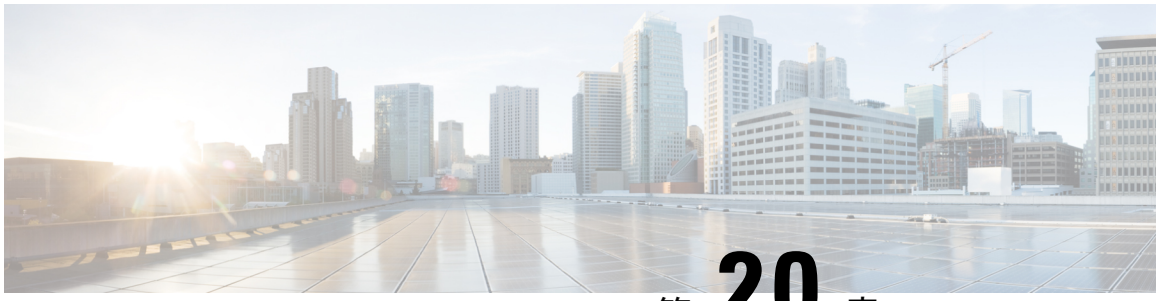
a) 適切なノードとそのノードの下にインターフェイスを展開します。

b) インターフェイスを右クリックし、をクリックして **EIGRP インターフェイス プロファイルの作成** します。

c) **EIGRP インターフェイス プロファイルの作成** ダイアログボックスで、 **EIGRP ポリシー** フィールドで、目的のEIGRPインターフェイスポリシーを選択します。[Submit]をクリックします。`

（注） EIGRP の VRF ポリシーおよびEIGRP インターフェイス ポリシーは、EIGRP が有効になっているときに使用するプロパティを定義します。EIGRP の VRF ポリシーおよびEIGRP インターフェイス ポリシーは、新しいポリシーを作成しない場合にもデフォルト ポリシーとして利用できます。したがって、ポリシーのいずれかを明示的に選択しない場合は、EIGRP が有効になっているとき、デフォルトのポリシーが自動的に利用されます。

これで EIGRP の設定は完了です。



第 20 章

ルート集約

この章は、次の内容で構成されています。

L3Out 外部 EPG レベルでのルート集約

BGP、OSPF、あるいは EIGRP のルート集約ポリシーは、ブリッジ ドメインまたは中継サブネットに適用されます。OSPF では、エリア間ルート集約と外部ルート集約がサポートされます。集約ルートはエクスポートされます。ファブリック内でのアドバタイズは行われません。

L3Out 外部 EPG でルート集約を有効にすると、ACI ファブリック内ではなく、L3Out ピアのみへのルート集約を実現できます。ACI ファブリックおよび外部 L3Out ピアへのルートの集約を実現するには、VRF レベルでのルート フィルタリングと集約 を参照してください。

また、このルート集約が設定されている場合、集約プレフィックスは外部 L3Out ピアにアドバタイズされ、より具体的なプレフィックスは L3Out ピアにアドバタイズされません。

注意事項と制約事項

外部 EPG で設定されたルート集約ポリシーにより、同じ境界リーフ スイッチに接続され、同じ VRF にあるすべての BGP ピアに集約されたプレフィックスがアドバタイズされます。これには、同じ境界リーフ スイッチと VRF 条件が満たされている場合に、異なる L3Out に属する BGP ピアが含まれます。

この動作を行わず、集約ルートを受信する BGP ピアを制限する場合は、該当する L3Out のアウトバウンド ルートマップを使用して、該当するルートをブロックします。

GUI を使用した L3out 外部 EPG レベルでのルート要約の設定

このセクションでは、L3Out 外部 EPG に関連付けられたルート集約を設定する手順について説明します。これらの構成手順を使用してルート集約を有効にすると、ACI ファブリック内ではなく、L3Out ピアのみへのルート集約を実現できます。

また、ルート集約が構成されている場合、集約プレフィックスは外部 L3Out ピアにアドバタイズされ、より具体的なプレフィックスは L3Out ピアにアドバタイズされません。

ACI ファブリックおよび外部 L3Out ピアへの ルートの集約を達成するには、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。

始める前に

次の設定のそれぞれに対して、L3 Out がすでに作成されていること。L3 Out については、外部ルーテッド ネットワーク、サブネット、およびルート集約ポリシーを作成することができます。

手順

ステップ 1 次のように、GUI を使用して BGP ルート集約を設定します:

a) メニュー バーで、**[テナント（Tenants）** > **common]** を選択します。

b) [ナビゲーション（Navigation）] ペインで、**[ネットワーキング（Networking）]** > **[L3Outs]** を展開します。

c) [L3Outs] を右クリックし、[L3Out の作成（Create L3Out）] を選択します。
[L3Out の作成（Create L3Out）] ウィザードが表示されます。

d) [作業（Work）] ペインで、必要な情報（[名前（Name）]、[VRF]、および [L3 ドメイン（L3 Domain）]）を入力し、[BGP] の横にあるチェックボックスをオンにします。

e) **[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。

f) [ノードとインターフェイス（Nodes and Interfaces）] ウィンドウで、適切なフィールドに入力し、[次へ（Next）] をクリックします。
[プロトコル（Protocols）] ウィンドウが表示されます。

g) [プロトコル（Protocols）] ウィンドウで、適切なフィールドに入力し、[次（Next）] をクリックします。
[外部 EPG（External EPG）] ウィンドウが表示されます。

h) [名前（Name）] フィールドに名前を入力し、[すべての外部ネットワークのデフォルト EPG（Default EPG for all external network）] フィールドをオフにします。
[サブネット（Subnets）] フィールドが表示されます。

i) [ルート集約ポリシー（Route Summarization Policy）] の上にある [+] をクリックします。
Create Subnet ダイアログボックスが表示されます。

j) **Specify the Subnet** ダイアログボックスでは、次の方法で、ルート集約ポリシーをサブネットに関連付けることができます。

例：

- IP アドレスを **IP Address** フィールドに入力します。
- **Export Route Control Subnet** の隣のチェック ボックスをオンにします。
- **External Subnets for the External EPG** の隣のチェック ボックスをオンにします。
- **BGP Route Summarization Policy** ドロップダウンメニューで、既存の (デフォルトの) ポリシーを選択する場合には **default** を、新しいポリシーを作成する場合には **Create BGP route summarization policy** を選択します。
- **Create BGP route summarization policy** を選択した場合には、**Create BGP Route Summarization Policy** ダイアログボックスが表示されます。[**名前**（**Name**）] フィールドに名前を入力し、[AS-SET 情報の生成（Generate AS-SET information）] で [**制御状態**（**Control State**）] チェック ボックスをオンにし 、[**送信**（**Submit**）] をクリックして [**OK**] 、[**完了**（**Finish**）] をクリックします。

  （注） **[より詳細な制御状態をアドバタイズしない]** オプションと **[アドレス タイプ制御**（**Address Type Contr**）**]** オプションは、ポリシーが VRF ルート制御ポリシーに適用されている場合にのみ適用されます。ここでは、AF Ucast と AF Mcast の両方がデフォルトで有効になっています。

ステップ 2 GUI を使用して、次のように OSPF のエリア間および外部の集約を設定します。

a) メニュー バーで、**[テナント**（**Tenants**） > **common**] を選択します。
b) [ナビゲーション（Navigation）] ペインで、**[ネットワーキング**（**Networking**）**]** > **[L3Outs]** > **[外部 EPG**（**External EPGs**）**]** を展開し、設定済みの外部 EPG をクリックします。
設定された外部 EPG の概要情報が表示されます。
c) 作業ウィンドウで、**+** 記号 (**Route Summarization Policy** の上) をクリックします。
Create Subnet ダイアログボックスが表示されます。
d) **Specify the Subnet** ダイアログボックスでは、次の方法で、ルート集約ポリシーをサブネットに関連付けることができます。

例：

- IP アドレスを **IP Address** フィールドに入力します。
- **Export Route Control Subnet** の隣のチェック ボックスをオンにします。
- **External Subnets for the External EPG** の隣のチェック ボックスをオンにします。
- **OSPF Route Summarization Policy** ドロップダウンメニューで、既存の (デフォルトの) ポリシーを選択する場合には **default** を、新しいポリシーを作成する場合には **Create OSPF route summarization policy** を選択します。
- **Create OSPF route summarization policy** を選択した場合には、**Create OSPF Route Summarization Policy** ダイアログボックスが表示されます。名前を **Name** フィールドに入

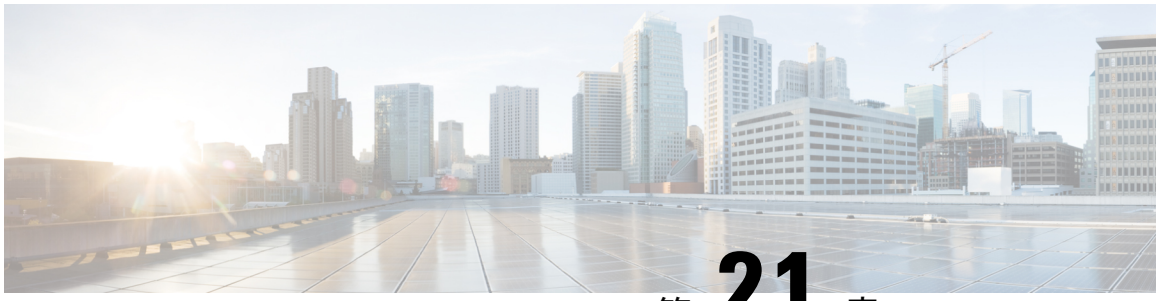
力し、**Inter-Area Enabled** の隣のチェック ボックスをオンにし、**Cost** の隣に値を入力し、**SUBMIT** をクリックします。

ステップ 3 次のように、GUI を使用して EIGRP の集約を設定します。

a) メニュー バーで、**Tenants > common** を選択します。
b) [ナビゲーション（Navigation）] ペインで、[**ネットワーキング（Networking）> L3Outs**] を展開します。
c) [**L3Outs**] を右クリックし、[**L3Out の作成（Create L3Out）**] を選択します。
[**L3Out の作成（Create L3Out）**] ダイアログ ボックスが表示されます。
d) 作業ウィンドウで、**EIGRP** の隣のチェック ボックスをオンにします。
e) **Name** フィールドに名前を入力し、**NEXT** をクリックします。
External EPG Networks ダイアログボックスが表示されます。
f) 作業ウィンドウで、**+** 記号をクリックします。
Define an External Network ダイアログボックスが表示されます。
g) **Name** フィールドに名前を入力し、**+** 記号 (**Route Summarization Policy** の上のもの) をクリックします。
Create Subnet ダイアログボックスが表示されます。
h) **Specify the Subnet** ダイアログボックスでは、次の方法で、ルート集約ポリシーをサブネットに関連付けることができます。

例：

- IP アドレスを **IP Address** フィールドに入力します。
- **Export Route Control Subnet** の隣のチェック ボックスをオンにします。
- **External Subnets for the External EPG** の隣のチェック ボックスをオンにします。
- **EIGRP Route Summarization** の隣のチェック ボックスをオンにし、**OK** をクリックし、**OK** をクリックし、 **FINISH** をクリックします。



第 21 章

ルート マップおよびルート プロファイルによるルート制御

この章は、次の内容で構成されています。

ルート制御プロファイル ポリシー

ACI ファブリックは、ファブリックの内部と外部にアドバタイズされるルート用に、ルート マップの set 句もサポートします。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 プロファイルで設定されます。

ACI は以下の set オプションをサポートします。

表 *14*：アクション ルール プロファイルのプロパティ（ルートマップ の *set* 句）

プロパティ	OSPF	EIGRP	BGP	注
コミュニティの設定			○	標準コミュニティと拡張コミュニティをサポートします。
追加のコミュニティを設定			○	標準コミュニティと拡張コミュニティをサポートします。

プロパティ	OSPF	EIGRP	BGP	注
ルート タグ	はい	はい		BD のサブネットのみでサポートされます。中継プレフィックスには、常にタグ 4294967295 が割り当てられます。
優先順位			○	BGP ローカル プリファレンスを設定します。
メトリック	はい		はい	BGP の MED を設定します。EIGRP のメトリックを変更しますが、EIGRP 複合メトリックは指定できません。
メトリック タイプ	○			OSPF タイプ 1 と OSPF タイプ 2。

ルート プロファイル ポリシーは、レイヤ 3 Outside 接続の下に作成されます。ルート制御ポリシーは、以下のオブジェクトで参照できます。

- テナント BD サブネット
- テナント BD
- 外部 EPG
- 外部 EPG のインポート/エクスポート サブネット

以下に、BGP のインポート ルート制御を使用し、2 つの異なるレイヤ 2 Outside から学習した外部ルートのローカル プリファレンスを設定する例を示します。AS300 への外部接続用のレイヤ 3 Outside 接続は、インポート ルート制御を適用して設定されています。アクション ルール プロファイルの設定では、[Local Preference] ウィンドウの [Action Rule Profile] でローカル プリファレンスが 200 に設定されています。

レイヤ 3 Outside 接続の外部 EPG は、0.0.0.0/0 インポート集約ポリシーを使用してすべてのルートを許可するように設定されています。これは、インポート ルート制御が適用されていますが、どのプレフィックスもブロックされてはならないためです。ローカルプリファレンスの設定を許可するために、インポート ルート制御が適用されています。また、[Route Control Profile] ウィンドウの [External EPG] で [Action Rule Profile] を参照するルート プロファイルを使用して、別のインポート サブネット 151.0.1.0/24 が追加されています。

MP-BGP テーブルを表示するには、show ip bgp vrf overlay-1 コマンドを使用します。スパインの MP-BGP テーブルには、プレフィックス 151.0.1.0/24 とローカル プリファレンス 200、および BGP 300 レイヤ 3 Outside 接続の境界リーフの次のホップが表示されます。

default-import と default-export という、2 つの特殊なルート制御プロファイルがあります。名前 default-import および default-export を使用して設定すると、ルート制御プロファイルはインポートとエクスポート両方のレイヤ 3 Outside レベルで自動的に適用されます。default-import および default-export のルート制御プロファイルは、0.0.0.0/0 集約を使用して設定することはできません。

ルート制御プロファイルは、次の順序でファブリック ルートに適用されます。

1. テナント BD サブネット
2. テナント BD
3. レイヤ 3 Outside

ルート制御プロファイルは、次の順序で中継ルートに適用されます。

1. 外部 EPG プレフィックス
2. 外部 EPG
3. レイヤ 3 Outside

BGP ピアごとのルート制御について

ルート制御ポリシーは、外部ネットワークにアドバタイズされるルート（エクスポート）またはファブリックに許可されるルート（インポート）を決定します。Cisco Application Policy Infrastructure Controller（APIC）リリース 4.2(1) よりも前の Cisco APIC リリースでは、これらのポリシーを、L3Out プロファイル（l3extInstP）の下の L3Out レベル、または L3Out（l3extSubnet）の下の L3Out サブネットを介して設定するため、これらのポリシーは L3Out に含まれるすべてのノードまたはパス向けに設定されるプロトコルに適用されます。この設定では、L3Outに複数のノードプロファイルが設定され、それぞれにBGPネイバーが指定された複数のノードまたはパスがあります。このため、個々のポリシーを各プロトコルエンティティに適用する方法はありません。

Cisco APIC リリース 4.2(1) 以降では、BGP ピアごとのルート制御機能が導入され、より詳細なルートのエクスポートおよびインポート制御が必要とされるこの状況に対処し始めています。

Cisco APIC リリース 6.0(1) 以降、一致ルールの作成中に `Match AS パス` パラメータを設定できます。1 つのルート マップで、複数の AS パス アクセス リスト名を一致させることができます。

BGP ピアごとのルート制御に関するガイドラインと制約事項

BGP ピアごとのルート制御機能のガイドラインと制約事項を次に示します。

- テナントの BGP ピアごとに使用されるルート プロファイルを設定する必要があります。
- ルートマップの一致を設定する方法、ルールまたはルートプロファイルを設定する方法、およびこれらの各コンポーネントの動作は、以前のリリースから変更されていません。
- この機能のルートプロファイルは、[ルーティング ポリシーのみ照合（Match Routing Policy Only）]（グローバル ポリシー）にのみ設定できます。ルート プロファイルは、BGP ピアごとのルートマップを生成する唯一の情報源です。この機能のルートプロファイルを [プレフィックスおよびルーティングポリシーの照合（Match Prefix and Routing Policy）] に設定することはできません。

  また、BD サブネットをエクスポートする場合は、プレフィックス リストで BD サブネットを明示的に指定する必要があります。
- 特定の方向の BGP ピアに関連付けることができるルート制御プロファイルは 1 つだけです。
- デフォルト ポリシーは、これらのルートマップではサポートされていません（名前付きルート プロファイルのみを BGP ピアに適用できます）。
- BGP ピアのルート制御プロファイルを指定すると、その情報だけに基づいてルートマップが生成されます。L3Out プロファイル（l3extInstP）または L3Out の下の L3Out サブネット（l3extSubnet）を介して設定されたルート制御プロファイルは、このルートマップに関与しません。同様に、BGP ピアごとのルート制御プロファイル設定がない場合、L3Out の下のルート制御プロファイルが有効になります。
- 一致プレフィックス リストでプライベート BD サブネットを指定すると、そのサブネットが含まれます。プライベート BD サブネットを除外するために追加の設定を行う必要はありません。
- 一致プレフィックス リストで 0.0.0.0/0 を設定すると、BD サブネットを含むすべてのプレフィックスに一致します。
- Cisco APIC は、境界リーフ スイッチにルートマップを作成して展開します。<tenant name> _<route profile name> _<L3Out name> -<direction> 。たとえば、次の設定のルート マップがあります。
  - [**テナント名（Tenant name**）]: t1
  - [**ルート プロファイル名（Route profile name**）]: rp1
  - [**L3Out name**]: l3out1
  - [**方向（Direction**）]: import

  will have this as the route map name: **t1_rp1_l3out1-in**
- BGP ピアごとのルート制御機能を設定しても、共有サービス ルートマップの動作には影響しません。
- APIC ソフトウェアをアップグレードまたはダウングレードする場合は、次の点に注意してください。

- **APIC ソフトウェアのアップグレード**：APIC ソフトウェアをアップグレードする前に L3Out でルート プロファイルを設定した場合、L3Out のルート プロファイルは、BGP ピアごとのルート プロファイルを設定するまで正常に動作し続けます。上記が適用されます。
- **APIC ソフトウェアのダウングレード**：BGP ピアごとのルート プロファイルを設定し、その後で APIC ソフトウェアをダウングレードする場合は、ダウングレードに進む前にポリシーを削除する必要があります。

- 順序が同じ場合、ルート制御プロファイルの許可エントリと拒否エントリの動作は決定論的ではありません。ルート制御プロファイルをピアごとに **instp** または BGP にマッピングする場合、エントリの順序によって動作が決まります。動作を確実に予測できるようにするには、最初にインストールする必要があるエントリに低い順序を指定し、後でインストールする必要があるエントリに高い順序を指定します。

GUI を使用した BGP ピアごとのルート制御の設定

次の手順では、GUI を使用して BGP ピア単位のルート制御を設定する方法について説明します。

始める前に

- ノード、ポート、AEP、機能プロファイル、レイヤ 3 ドメインを設定します。
- ファブリック内でルートを伝播させるための、BGP ルート リフレクタ ポリシーを設定します。

手順

ステップ 1 テナントおよび VRF の作成

a) メニュー バーで **[Tenants]** > **[Add Tenant]** の順に選択します。

[テナントの作成（Create Tenant）] ダイアログ ボックスが表示されます。

b) **Name** フィールドに、テナント名を入力します。
c) In the **VRF Name** フィールドに、VRF 名を入力します。
d) **Submit** をクリックします。

ステップ 2 ブリッジ ドメインを作成します。

a) **[ナビゲーション（Navigation）]** ペインで **[テナント（Tenant）]** および **[ネットワーキング（Networking）]** を展開します。
b) **Bridge Domains** を右クリックして、**Create Bridge Domain** を選択します。
c) **Name** フィールドに、ブリッジ ドメイン (BD) の名前を入力します。

d) （オプション）[Advertise Host Routes] ボックスをクリックすると、すべての導入済み境界リーフでアドバタイズメントが有効になります。
e) **VRF** フィールドのドロップダウンリストから、作成した VRF を選択します (この例では v1)。
f) **Next** をクリックします。
g) **+** アイコンを **Subnets** でクリックします。
h) **Gateway IP** フィールドに、BD のサブネットを入力します。
i) **Scope** フィールドで、**Advertised Externally** を選択します。

後ほど作成した後に、**L3 Out for Route Profile** を追加します。

（注） [**ホスト ルータのアドバタイズ（Advertise Host Routes**）] が有効になっている場合、ルートマップもすべてのホスト ルートを一致させます。

j) **OK** をクリックします。
k) **Next** をクリックし、 **Finish** をクリックします。

ステップ 3 アプリケーション EPG の作成

a) **Application Profiles** を右クリックし、**Create Application Profile** を選択します。
b) アプリケーションの名前を入力します。
c) EPG の **+** アイコンをクリックします。
d) EPG の名前を入力します。
e) BD ドロップダウンリストで、以前に作成したブリッジ ドメインを選択します。
f) **Update** をクリックします。
g) [Submit] をクリックします。

ステップ 4 BGP ピアごとのルートマップとして使用されるテナント レベルのルートマップを作成します。

a) [**ナビゲーション（Navigation**）] ペインで、**[テナント（Tenants）]** > **[*Tenant_name*]** > **[ポリシー（Policies）]** > **[プロトコル（Protocol）]** を展開します。
b) [BGP ダンプニング、リーク間のルートマップ（Route Maps for BGP Dampening, Inter-leak）] を右クリックし、[BGP ダンプニング、リーク間のルートマップの作成（Create Route Maps for BGP Dampening, Inter-leak）] を選択します。
c) [**BGP ダンプニング、リーク間のルート マップの作成（Create Route Maps for BGP Dampening, Inter-leak**）] ダイアログ ボックスで、[**名前（Name**）] フィールドに、ルートプロファイル名を入力します。
d) [**タイプ（Type**）] フィールドで、[**ルーティング ポリシーのみ照合（Match Routing Policy Only**）] を選択する必要があります。
e) [コンテキスト（Contexts）] 領域で [+] サインをクリックして、[**ルート制御コンテキスト作成（Create Route Control Context**）] ダイアログ ボックスを表示し、次のアクションを実行します。

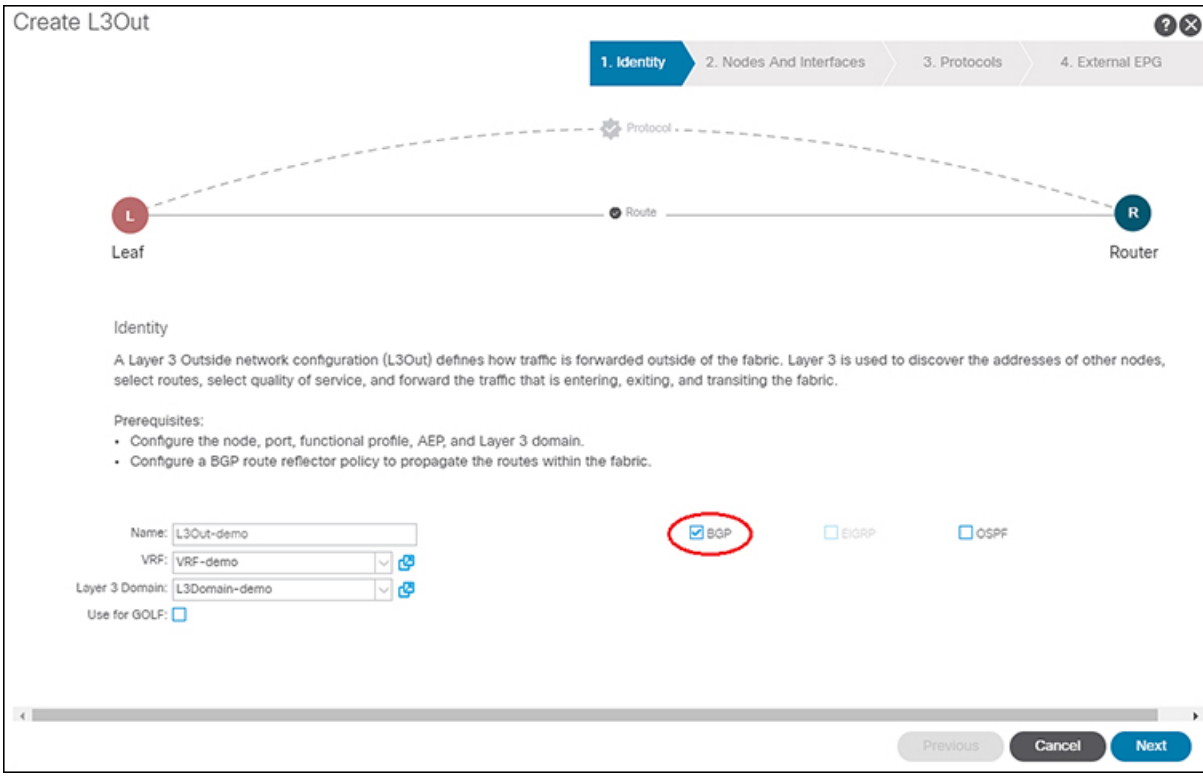
1. 必要に応じて、[**順序（Order**）] と [**名前（Name**）] フィールドに入力します。
2. [一致ルール（Match Rule）] フィールドで、[一致ルールの作成（Create Match Rule）] をクリックします。

3. [一致ルール（Match Rule）] ダイアログ ボックスの [名前（Name）] フィールドに、一致ルールの名前を入力します。
4. 該当するフィールド（一致 Regex コミュニティ条件、一致コミュニティ条件、および一致プレフィックス、一致 AS パス Regex 条件）に必要な情報を入力し、[送信（Submit）] をクリックします。
5. [セット ルール（Set Rule）] フィールドで、[ルート マップのセット ルールの作成（Create Set Rules for a Route Map）] をクリックします。
6. [ルート マップのセット ルールの作成（Create Set Rules for a Route Map）] ダイアログボックスの [名前（Name）] フィールドに、ルールの名前を入力します。
7. 目的の属性および関連するコミュニティ、条件、タグ、および設定 (preferences) を選択します。[完了（Finish）] をクリックします。
8. [ルート制御コンテキストの作成（Create Route Control Context）] ダイアログボックスで、[OK] をクリックします。
9. [BGP ダンプニング、インターリークのルートマップの作成（Create Route Maps for BGP Dampening, Inter-leak）] ダイアログ ボックスで、[送信（Submit）] をクリックします。

ステップ 5 L3Out を作成し、L3Out の BGP を設定します。

a) [ナビゲーション（Navigation）] ペインで [テナント（Tenant）] および [ネットワーキング（Networking）] を展開します。
b) [L3Outs] を右クリックし、[L3Out の作成（Create L3Out）] を選択します。
c) L3Out の BGP を設定するために必要な情報を入力します。

この L3Out の BGP プロトコルを設定するには、L3Out 作成ウィザードの[識別（Identity）] ページで [BGP] を選択します。



d) 残りのページを続けて行い（[**ノードとインターフェイス（Nodes and Interfaces）**]、[**プロトコル（Protocols）**]、および [**外部 EPG（External EPG）**]）、L3Out の設定を完了します。

ステップ 6 L3Out の設定が完了したら、BGP ピアごとのルート制御機能を設定します。

a) BGP ピア接続プロファイル画面に移動します。

[テナント（Tenants）] > [テナント（*tenant*）] > [ネットワーキング（Networking）] > [L3Outs] > [*L3out-name*] > [論理ノード プロファイル（Logical Node Profiles）] > [*logical-node-profile-name*] > [論理インターフェイス プロファイル（Logical Interface Profiles）] > [*logical-interface-profile-name*] > [BGP ピア接続プロファイル（BGP Peer Connectivity Profile） *] [IP-address*]

b) [ルート制御プロファイル（Route Control Profile）] フィールドまで下にスクロールし、[+] をクリックして次の項目を設定します。

- [**名前（Name）**]：設定したルートマップを選択します。ステップ 4 （378 ページ）
- [**方向（Direction）**]：次のいずれかのオプションを選択します。
  - **ルートインポートポリシー**
  - **ルートエクスポートポリシー**

明示的なプレフィクス リストでルート マップ/プロファイル

ルート マップ/プロファイルについて

ルートプロファイルは、関連付けられているセットアクションルールと一致する論理アクション ルールの順序付きのセット (rtctrlCtxP) を定義する論理ポリシーです。ルート プロファイルでは、ルート マップの論理抽象です。複数のルート プロファイルは、1 個のルート マップにマージすることができます。ルートプロファイルには、以下のいずれかのタイプを指定できます。

- プレフィックスとルーティング ポリシーと一致: 普及サブネット (fvSubnet) と外部のサブネット (l3extSubnet) がルート プロファイルと組み合わせるし、マージされ、1 つのルート マップ (またはルート マップ エントリ) になります。一致するプレフィックスとルーティング ポリシーは、デフォルト値です。
- 一致ルーティング ポリシーのみ: は、ルート プロファイルは、ルート マップを生成する情報の唯一のソースと、その他のポリシー属性が上書きされます。

（注） 明示的なプレフィクス リストを使用すると、「ルーティング ポリシーのみを一致」にルートプロファイルのタイプを設定する必要があります。

一致後の設定プロファイルが定義されていると、レイヤ 3 Out でルート マップを作成する必要があります。ルート マップは以下のいずれかの方法で作成できます。

- エクスポート ルート コントロールでは、「デフォルト エクスポート」ルート マップとインポート ルート制御の「デフォルト インポート」ルート マップを作成します。
- (デフォルトエクスポートまたはデフォルトインポートしないという名前)他のルートマップを作成し、l3extInstPs またはサブネット、l3extInstP の下の 1 つまたは複数の関係を設定します。
- いずれにしても、ルートマップ内で rtctrlSubjP を指しているによって明示的なプレフィックス リストでルート マップに一致します。

エクスポートとインポートルートマップでは、設定と一致のルールは、グループ間の相対シーケンス（rtctrlCtxP）とともにグループにまとめられます。一致の各グループの下でさらに、いずれかに関係ステートメント (rtctrlCtxP) を設定し、または一致プロファイルの詳細については、使用可能な (rtctrlSubjP)。

(たとえばBGPプロトコル)は、アウトのレイヤ3で有効になっているすべてのプロトコルは、エクスポートを使用し、ルート フィルタ リングのマップをインポート ルート。

ルートマップ/プロファイルの明示的なプレフィックスリストのサポートについて

Cisco APIC では、公開ブリッジ ドメイン（BD）サブネットと外部の中継ネットワークのインバウンドおよびアウトバウンド ルート コントロールは、明示的なプレフィックス リストを通して提供されます。レイヤ 3 アウトのインバウンドおよびアウトバウンド ルート コントロールは、ルート マップ/プロファイル（rtctrlProfile）によって管理されます。ルート マップ/プロファイル ポリシーは、Cisco ACI ファブリックでレイヤ 3 アウトを完全に管理するプレフィックス リストをサポートしています。

プレフィックス リストのサブネットは、ブリッジ ドメイン公開サブネットまたは外部のネットワークを表すことがあります。明示的なプレフィックス リストは別の方法を示し、次の代わりに使用できます。

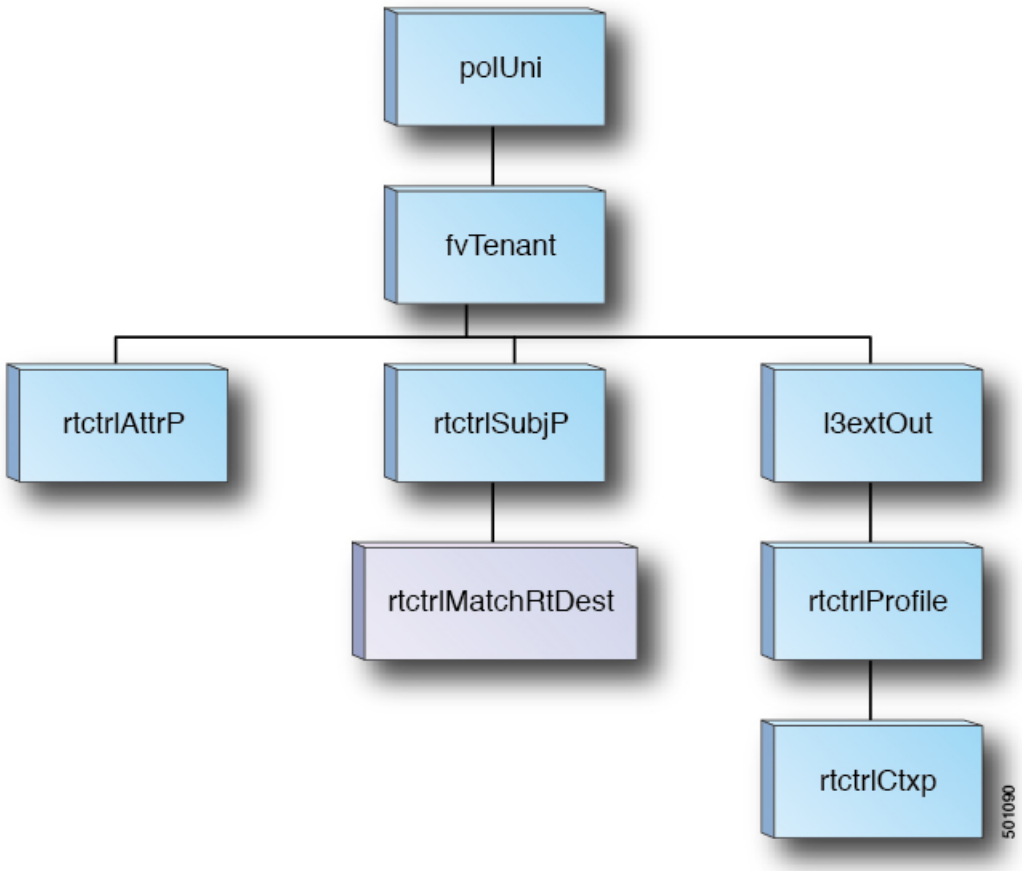
- BD を介して BD サブネットをレイヤ 3 アウト関係にアドバタイズします。

（注） BD のサブネットは、アドバタイズされるサブネットに公開としてマークする必要があります。

- 中継トラフィックと外部ネットワークをアドバタイジングするため、エクスポート/インポート ルート コントロールにより l3extInstP でサブネットを指定します。

明示的なプレフィックス リストは一致ルートの宛先（rtctrlMatchRtDest）と呼ばれる新しい一致タイプで定義されます。使用例は次の API の例で説明します。

図 *44 : API* の外部ポリシー モデル



明示的なプレフィクス リストを使用する場合の一致ルール、ルール設定に関する追加情報は次の通りです。

一致ルール

- テナント（fvTenant）で、ルートマップ フィルタリングの一致プロファイル（rtctrlSubjP）を作成できます。各一致プロファイルは1個以上の一致ルールを含めることができます。一致ルールでは、複数の一致タイプをサポートしています。Cisco APIC リリース 2.1 より前は、サポートされていた一致タイプは明示的なプレフィックス リストおよびコミュニティ リストでした。

  Cisco APIC リリース 2.1 以降では、明示的なプレフィックス一致またはルートの宛先（rtctrlMatchRtDest）の一致がサポートされています。

  一致プレフィックス リスト（rtctrlMatchRtDest）は、オプションの集約フラグで 1 つまたは複数のサブネットがサポートされています。集約フラグは、設定で言及されているマスクから始めて、プレフィックスのアドレスファミリで許可されている最大数のマスクに達するまで、プレフィックスが複数のマスクと一致できるようにするために使用されます。

これは、NX-OS ソフトウェアのプレフィックス リストの「le」オプションに相当します (たとえば 10.0.0.0/8 le 32)。

プレフィクス リストは、次のケースに対応するために使用できます。

- すべて許可 (集約フラグでは 0.0.0.0/0、0.0.0.0/0 le 32 と同等)
- 1 つ以上の特定のプレフィクス (たとえば 10.1.1.0/24)
- 1 つ以上の集約フラグを伴うプレフィックス (たとえば 10.1.1.0/24 le 32 と同等)。

（注） 一致 プレフィックス「0.0.0.0/0 with aggregate flag」を持つルートマップがエクスポート方向の L3Out EPG で使用される場合、ルールはダイナミック ルーティング プロトコルからの再配布にのみ適用されます。したがって、ルールは次のものには適用されません（OSPF や EIGRP などのルーティング プロトコル）。

- ブリッジ ドメイン（BD）のサブネット
- 境界リーフ スイッチに直接接続されたサブネット
- L3Out で定義されたスタティック ルート

- 明示的なプレフィックス一致ルールは、1 つ以上のサブネットを含めることができます。これらのサブネットとしては、ブリッジ ドメイン パブリック サブネットまたは外部ネットワークがあり得ます。またサブネットは、最大サブネットマスクまで集約することもできます (IPv4 では /32、IPv6 では /128)。
- さまざまなタイプの複数の一致ルールが存在する場合 (一致コミュニティや明示的なプレフィックスの一致など)、一致ルールは、個々の一致タイプすべての一致ステートメントが一致する場合だけを許可します。これは AND フィルタと等価です。明示的なプレフィクス一致はサブジェクト プロファイル (rtctrlSubjP) に含められ、サブジェクト プロファイル下に他の一致ルールが存在する場合には論理 AND を形成します。
- 特定の一致タイプ (一致プレフィックス リスト) 内では、少なくとも 1 つの一致ルール ステートメントが一致する必要があります。複数の明示的なプレフィックス一致 (rtctrlMatchRtDest) は、論理 OR を形成する同じサブジェクト プロファイル (rtctrlSubjP) 下で定義することができます。
- ピアごとのルート マップが、permit-all ルールの後に完全一致ルールが続くように構成されている場合、完全一致ルールで構成された特定のプロパティが処理されない可能性があります。
- ルートマップ内の空のルートが、match 句なしで許可または拒否のアクションと一致した場合、すべてのルートが許可または拒否されます。インポートまたはエクスポートルート制御用の通常のルート マップは、空のルートを許可しません。Cisco APIC 5.2(4) リリース以降では、静的ルートおよび直接ルートは、ルートが一致しない場合ルートを許可しません。

一致プレフィックスの機能拡張

Cisco APIC リリース 4.2(3) 以降、一致ルールを作成し、集約を有効にする場合に使用できる 2 つの新しいフィールドが、[一致プレフィックス（Match Prefix）] フィールドに設けられました。リリースに基づいて、これらのフィールドには、次の表に示すように異なる命名規則があります。

リリース	フィールド
Cisco APIC リリース 4.2(3)	**[開始プレフィックス（From Prefix）]**
	[終了プレフィックス（To Prefix）]
Cisco APIC リリース 5.2(2)	**[大きいマスク（Greater Than Mask）]**
	[小さいマスク（Less Than Mask）]
Cisco APIC リリース 5.2(6)	**[以上マスク（Greater Equal Mask）]**
	[以下マスク（Less Equal Mask）]

プレフィックス一致ルールを作成して集約を有効にする場合は、これらのフィールドを使用してマスク範囲を指定します。次に、これらのフィールドを使用する状況の例を示します。

- すべて許可（0.0.0.0/0、マスク長 24 ー 30、0.0.0.0/0 ge 24 le 30 に相当）
- 特定の IP アドレスと 28 より大きいネットマスクを持つプレフィックス（たとえば、10.1.1.0/24 ge 28 と同等）

次の表に、これら2つの新しいフィールドを使用するさまざまなシナリオと、各シナリオの結果の詳細を示します。次の点に注意してください。

- **[以上マスク（Greater Equal Mask）]** と **[以下マスク（Less Equal Mask）]** フィールドは、**[集約（Aggregate）]** オプションを **[一致ルート宛先ルールの作成（Create Match Route Destination Rule）]** ウィンドウで選択した場合にのみ使用できます。
- 値 **0** を **[以上マスク（Greater Equal Mask）]** および **[以下マスク（Less Equal Mask）]** フィールドに設定した場合、**未指定**と見なされ、次のデフォルト値が使用されます。
  - 以上マスク =0
  - 以下マスクは、IP アドレス ファミリが IPv4 か IPv6 かによって、32 または 128 になります。

  この状況は、従来の動作を前提としており、これらのプロパティが存在しない古い設定のインポートをサポートします。詳細については、次の表の 2 列目を参照してください。

IPアドレス/ネットマスク	集約	以上マスク エントリ（fromPfxLen）	以下マスク エントリ（toPfxLen）	結果	その他の情報
192.0.2.0/24	イネーブルになっていない	N/A	N/A	192.0.2.0/24	完全一致：
192.0.2.0/24	有効	0	0	192.0.2.0/24 le 32	従来の動作
192.0.2.0/24	有効	24	不適切な値（**[以上マスク（Greater Equal Mask）]** エントリに指定した値のためにエラーが発生した）	エラー：無効な設定です。	**[以上マスク（Greater Equal Mask）]** エントリは、ネットマスク長よりも大きい必要があります。
192.0.2.0/24	有効	28	30	192.0.2.0/24 ge 28 le 30	これらの新しいフィールドによる新しい動作
192.0.2.0/24	有効	30	0	192.0.2.0/24 ge 30	これらの新しいフィールドによる新しい動作
192.0.2.0/24	有効	28	28	192.0.2.0/24 eq 28	これらの新しいフィールドによる新しい動作
192.0.2.0/24	有効	0	28	192.0.2.0/24 le 28	これらの新しいフィールドによる新しい動作

IPアドレス/ネットマスク	集約	以上マスク エントリ（fromPfxLen）	以下マスク エントリ（toPfxLen）	結果	その他の情報
192.0.2.0/24	有効	30	28	エラー：無効な設定です。	**[以上マスク（Greater Equal Mask）]** エントリを **[以下マスク（Less Equal Mask）]** エントリより大きくすることはできません。

ルールの設定

設定ポリシーは、設定コミュニティおよび設定タグなど明示的なプレフィックスで実施される設定ルールを定義するために作成する必要があります。

明示プレフィックス リストの集約サポート

一致するプレフィックス リストの各プレフィックス（rtctrlMatchRtDest）は、1つのプレフィックス リスト エントリに一致する複数のサブネットをサポートするように集約できます。

集約されたプレフィックスと BD プライベート サブネット

明示的なプレフィックスリストマッチ内のサブネットは、集約されたマッチまたは正確なマッチにより BD プライベート サブネットとマッチする可能性がありますが、プライベート サブネットは明示的なプレフィックス リストを使用するルーティング プロトコルを通してアドバタイズされることはありません。BD サブネットの範囲は、BD サブネットをアドバタイズするため明示プレフィックス リスト機能に対して「public」に設定する必要があります。

集約による 0.0.0.0/0 の動作の違い

集約設定を使用した 0.0.0.0/0 は、「0.0.0.0/0 le 32」に相当する IP プレフィックス リストを作成します。集約設定の 0.0.0.0/0 は、主に次の 2 つの状況で使用できます。

- L3Out ネットワーク（L3Out EPG）下の L3Out サブネットの「Aggregate Export」スコープを持つ「Export Route Control Subnet」
- 「default-export」という名前のルート マップに割り当てられた明示的なプレフィックス リスト（Match Prefix ルール）

L3Out サブネット下の「Export Route Control Subnet」スコープで使用すると、ルート マップはダイナミック ルーティング プロトコルから学習したルートのみに一致します。BDサブネットまたは直接接続されたネットワークには一致しません。

明示的なルート マップ設定で使用すると、ルート マップは BD サブネットや直接接続ネットワークを含むすべてのルートに一致します。

上記の2つの状況で予想される動作と予期しない（一貫性のない）動作を理解するには、次の例を検討してください。

シナリオ 1

最初のシナリオでは、次のような設定ポストを使用して、ルート マップ（名前は rpm_with_catch_all）を設定します。

```
<l3extOut annotation="" descr="" dn="uni/tn-t9/out-L3-out" enforceRtctrl="export"
name="L3-out" nameAlias="" ownerKey="" ownerTag="" targetDscp="unspecified">
    <rtctrlProfile annotation="" descr="" name="rpm_with_catch_all" nameAlias=""
ownerKey="" ownerTag="" type="combinable">
        <rtctrlCtxP action="permit" annotation="" descr="" name="catch_all" nameAlias=""
 order="0">
            <rtctrlScope annotation="" descr="" name="" nameAlias="">
              <rtctrlRsScopeToAttrP annotation="" tnRtctrlAttrPName="set_metric_type"/>

            </rtctrlScope>
        </rtctrlCtxP>
    </rtctrlProfile>
   <ospfExtP annotation="" areaCost="1" areaCtrl="redistribute,summary" areaId="backbone"
 areaType="regular" descr="" multipodInternal="no" nameAlias=""/>
    <l3extRsEctx annotation="" tnFvCtxName="ctx0"/>
    <l3extLNodeP annotation="" configIssues="" descr="" name="leaf" nameAlias=""
ownerKey="" ownerTag="" tag="yellow-green" targetDscp="unspecified">
        <l3extRsNodeL3OutAtt annotation="" configIssues="" rtrId="20.2.0.2"
rtrIdLoopBack="no" tDn="topology/pod-1/node-104">
            <l3extLoopBackIfP addr="14.1.1.1/32" annotation="" descr="" name=""
nameAlias=""/>
            <l3extInfraNodeP annotation="" descr="" fabricExtCtrlPeering="no"
fabricExtIntersiteCtrlPeering="no" name="" nameAlias="" spineRole=""/>
        </l3extRsNodeL3OutAtt>
        <l3extLIfP annotation="" descr="" name="interface" nameAlias="" ownerKey=""
ownerTag="" tag="yellow-green">
            <ospfIfP annotation="" authKeyId="1" authType="none" descr="" name=""
nameAlias="">
                <ospfRsIfPol annotation="" tnOspfIfPolName=""/>
            </ospfIfP>
            <l3extRsPathL3OutAtt addr="36.1.1.1/24" annotation="" autostate="disabled"
descr="" encap="vlan-3063" encapScope="local" ifInstT="ext-svi" ipv6Dad="enabled"
llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
tDn="topology/pod-1/paths-104/pathep-[accBndlGrp_104_pc13]" targetDscp="unspecified"/>
            <l3extRsNdIfPol annotation="" tnNdIfPolName=""/>
            <l3extRsIngressQosDppPol annotation="" tnQosDppPolName=""/>
            <l3extRsEgressQosDppPol annotation="" tnQosDppPolName=""/>
        </l3extLIfP>
    </l3extLNodeP>
    <l3extInstP annotation="" descr="" exceptionTag="" floodOnEncap="disabled"
matchT="AtleastOne" name="epg" nameAlias="" prefGrMemb="exclude" prio="unspecified"
targetDscp="unspecified">
        <l3extRsInstPToProfile annotation="" direction="export"
tnRtctrlProfileName="rpm_with_catch_all"/>
        <l3extSubnet aggregate="" annotation="" descr="" ip="0.0.0.0/0" name=""
nameAlias="" scope="import-security"/>
        <fvRsCustQosPol annotation="" tnQosCustomPolName=""/>
    </l3extInstP>
</l3extOut>
```

```
<rtctrlAttrP annotation="" descr="" dn="uni/tn-t9/attr-set_metric_type"
name="set_metric_type" nameAlias="">
    <rtctrlSetRtMetricType annotation="" descr="" metricType="ospf-type1" name=""
nameAlias="" type="metric-type"/>
</rtctrlAttrP>


<rtctrlSubjP annotation="" descr="" dn="uni/tn-t9/subj-catch_all_ip" name="catch_all_ip"
 nameAlias="">
    <rtctrlMatchRtDest aggregate="yes" annotation="" descr="" ip="0.0.0.0/0" name=""
nameAlias=""/>
</rtctrlSubjP>
```

このルート マップでは、0.0.0.0/0 で予想されることは、すべてのルートが metricType = "ospf-type1" プロパティを使用することですが、OSPF ルートに対してのみです。

さらに、ブリッジ ドメイン（たとえば、209.165.201.0/27）の下に、スタティック ルートのパーベイシブ サブネット（fvSubnet）を持つルート マップを使用して、ブリッジ ドメインと L3Out の関係を設定したサブネットがあります。ただし、上記のルート マップは結合可能ですが、上記のルート マップで 0.0.0.0/0 を、スタティック ルートではなく、中継ルートにのみ適用するため、ブリッジ ドメインで設定されたサブネットには適用されません。

次に、`show route-map` および `show ip prefix-list` コマンドの出力を示します。`exp-ctx-st-2555939` は、ブリッジ ドメインで設定されたサブネットの発信ルート マップの名前、および、`show route-map` コマンドの出力に示されているプレフィックス リストの名前です。

```
leaf4# show route-map exp-ctx-st-2555939
route-map exp-ctx-st-2555939, deny, sequence 1
  Match clauses:
    tag: 4294967295
  Set clauses:
route-map exp-ctx-st-2555939, permit, sequence 15801
  Match clauses:
    ip address prefix-lists: IPv4-st16391-2555939-exc-int-inferred-export-dst
    ipv6 address prefix-lists: IPv6-deny-all
  Set clauses:

leaf4# show ip prefix-list IPv4-st16391-2555939-exc-int-inferred-export-dst
ip prefix-list IPv4-st16391-2555939-exc-int-inferred-export-dst: 1 entries
   seq 1 permit 209.165.201.0/27

leaf4#
```

この場合、ブリッジ ドメイン サブネットが外に出ると、`rpm_with_catch_all` ルート マップ ポリシーが適用されないため、すべてが予期したとおりに動作します。

シナリオ 2

2 番目のシナリオでは、エクスポート ルート制御用の「default-export」ルート マップを設定します。この場合、次のような設定ポストを使用して、明示的なプレフィックス リスト（Match Prefix ルール）が「default-export」ルート マップに割り当てられます。次のとおりです。

```
<l3extOut annotation="" descr="" dn="uni/tn-t9/out-L3-out" enforceRtctrl="export"
name="L3-out" nameAlias="" ownerKey="" ownerTag="" targetDscp="unspecified">
    <rtctrlProfile annotation="" descr="" name="default-export" nameAlias="" ownerKey=""
```

```
ownerTag="" type="combinable">
       <rtctrlCtxP action="permit" annotation="" descr="" name="set-rule" nameAlias=""
order="0">
           <rtctrlScope annotation="" descr="" name="" nameAlias="">
             <rtctrlRsScopeToAttrP annotation="" tnRtctrlAttrPName="set_metric_type"/>

           </rtctrlScope>
       </rtctrlCtxP>
   </rtctrlProfile>
  <ospfExtP annotation="" areaCost="1" areaCtrl="redistribute,summary" areaId="backbone"
areaType="regular" descr="" multipodInternal="no" nameAlias=""/>
   <l3extRsEctx annotation="" tnFvCtxName="ctx0"/>
   <l3extLNodeP annotation="" configIssues="" descr="" name="leaf" nameAlias=""
ownerKey="" ownerTag="" tag="yellow-green" targetDscp="unspecified">
       <l3extRsNodeL3OutAtt annotation="" configIssues="" rtrId="20.2.0.2"
rtrIdLoopBack="no" tDn="topology/pod-1/node-104">
           <l3extLoopBackIfP addr="14.1.1.1/32" annotation="" descr="" name=""
nameAlias=""/>
           <l3extInfraNodeP annotation="" descr="" fabricExtCtrlPeering="no"
fabricExtIntersiteCtrlPeering="no" name="" nameAlias="" spineRole=""/>
       </l3extRsNodeL3OutAtt>
       <l3extLIfP annotation="" descr="" name="interface" nameAlias="" ownerKey=""
ownerTag="" tag="yellow-green">
           <ospfIfP annotation="" authKeyId="1" authType="none" descr="" name=""
nameAlias="">
               <ospfRsIfPol annotation="" tnOspfIfPolName=""/>
           </ospfIfP>
           <l3extRsPathL3OutAtt addr="36.1.1.1/24" annotation="" autostate="disabled"
descr="" encap="vlan-3063" encapScope="local" ifInstT="ext-svi" ipv6Dad="enabled"
llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
tDn="topology/pod-1/paths-104/pathep-[accBndlGrp_104_pc13]" targetDscp="unspecified"/>
           <l3extRsNdIfPol annotation="" tnNdIfPolName=""/>
           <l3extRsIngressQosDppPol annotation="" tnQosDppPolName=""/>
           <l3extRsEgressQosDppPol annotation="" tnQosDppPolName=""/>
       </l3extLIfP>
   </l3extLNodeP>
   <l3extInstP annotation="" descr="" exceptionTag="" floodOnEncap="disabled"
matchT="AtleastOne" name="epg" nameAlias="" prefGrMemb="exclude" prio="unspecified"
targetDscp="unspecified">
       <l3extSubnet aggregate="" annotation="" descr="" ip="0.0.0.0/0" name=""
nameAlias="" scope="import-security"/>
       <fvRsCustQosPol annotation="" tnQosCustomPolName=""/>
   </l3extInstP>
</l3extOut>
```

この default-export ルート マップには、rpm_with_catch_all ルート マップと同様の情報があり、IP が 0.0.0.0/0（ip=0.0.0.0/0）に設定されており、default-export ルート マップの設定ルールが Set Metric Type（tnRtctrlAttrPName=set_metric_type）でのみ設定されます。

前の例の状況と同様にブリッジ ドメインの下に同じサブネットを設定し、前の例と同様にブリッジ ドメインと L3Out の関係を設定します。

ただし、このシナリオでは、show route-map コマンドと show ip prefix-list コマンドの出力を次に示します。

```
leaf4# show route-map exp-ctx-st-2555939
route-map exp-ctx-st-2555939, deny, sequence 1
  Match clauses:
    tag: 4294967295
  Set clauses:
route-map exp-ctx-st-2555939, permit, sequence 8201
```

```
  Match clauses:
    ip address prefix-lists:
IPv4-st16391-2555939-exc-int-out-default-export2set-rule0pfx-only-dst
    ipv6 address prefix-lists: IPv6-deny-all
  Set clauses:
    metric-type type-1

leaf4# show ip prefix-list IPv4-st16391-2555939-exc-int-inferred-export-dst
% Policy IPv4-st16391-2555939-exc-int-inferred-export-dst not found
ifav82-leaf4# show ip prefix-list
IPv4-st16391-2555939-exc-int-out-default-export2set-rule0pfx-only-dst
ip prefix-list IPv4-st16391-2555939-exc-int-out-default-export2set-rule0pfx-only-dst: 1
 entries
   seq 1 permit 209.165.201.0/27

leaf4#
```

この状況では、ブリッジドメインサブネットが発信されると、`default-export`ルートマップ ポリシーが適用されます。この状況では、そのルート マップは BD サブネットと直接接続ネットワークを含むすべてのルートに一致します。これは一貫性のない動作です。

注意事項と制約事項

- 次の2つの方法のいずれかを選択し、ルートマップの設定を行う必要があります。両方の方法を使用する場合は、二重エントリになり定義されていないルートマップになります。
  - レイヤ3アウトサイド関係にブリッジドメイン（BD）でルートを追加し、BDを設定します。
  - rtctrlSubjP マッチ プロファイルで、マッチ プレフィックスを構成します。
- 2.3(x) 以降、**[deny-static]** 暗黙エントリはエクスポート ルート マップから削除されています。ユーザ-は、静的ルートのエクスポートを制御するために必要な許可と拒否を暗黙で設定する必要があります。
- L3Oout ではピアごとの Route-map は OSPF および EIGRP でサポートされません。Route-map は、全体として L3Out にのみ適用できます。4.2(x) 以降、L3Out のピアごとのルートマップは BGP でサポートされます。

  この問題の回避策を次に示します。
  - ネイバーの反対側からアドバタイズされないようにプレフィックスをブロックします。
  - プレフィックスを学習したくない既存 L3Out で route-map のプレフィックスをブロックし、プレフィックスを学習したい別の L3Out にネイバーを移動して、別の route-map を作成します。
- GUI と API コマンドの組み合わせを使用した route-map の作成はサポートされません。考えられる解決策として、GUI を使用してデフォルトの route-map とは異なる route-map を作成することはできますが、L3Out で GUI を通じて作成された route-map をピアごとに適用することはできません。

GUI を使用した、明示的なプレフィックス リストでルート マップ/プロファイルの設定

始める前に

- テナントと VRF を設定する必要があります。
- リーフ スイッチで VRF をイネーブルに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（Tenant）] をクリックし、[ナビゲーション（Navigation）] ペインで[Tenant_name] [ポリシー（Policies）] [プロトコル（Protocol）] [一致ルール（Match Rules）] を展開します。 ＞＞＞

ステップ 2 [**一致ルール（Match Rules**）] を右クリックし、[**ルート マップの一致ルールの作成（Create Match Rule for a Route Map**）] をクリックします。

ステップ 3 [**一致ルールの作成（Create Match Rule**）] ウィンドウで、ルールの名前を入力し、必要なコミュニティ条件を選択します。

ステップ 4 一致プレフィックスに必要な情報を入力します。

一致プレフィックスの情報を入力する方法は、APIC のリリースによって異なります。

- APIC リリース 4.2(3) 以前では、[**一致ルールの作成（Create Match Rule**）] ウィンドウで、[**一致プレフィックス（Match Prefix**）] を展開し、次のアクションを実行します:

  1. **IP** フィールドで、明示的プレフィックス リストを入力します。

     明示的プレフィックスは、BD サブネットまたは外部ネットワークを表記できます。

  2. （任意）[説明（Description）] フィールドに、このポリシーの説明を入力します。

  3. **Aggregate** チェック ボックスは、集約プレフィックスが必要な場合にのみオンにします。

  4. [更新（Update）] をクリックします。

- APIC リリース 4.2(3) 以降では、[一致ルールの作成（Create Match Rule）] ウィンドウで、[一致プレフィックス（Match Prefix）] 領域の [+] をクリックします。

  [一致ルート宛先ルールの作成（Create Match Route Destination Rule）] ウィンドウが表示されます。このウィンドウで次のアクションを実行します。

  1. **IP** フィールドで、明示的プレフィックス リストを入力します。

     明示的プレフィックスは、BD サブネットまたは外部ネットワークを表記できます。

  2. （任意）[説明（Description）] フィールドに、このポリシーの説明を入力します。

3. 集約プレフィックスが必要かどうかを決定します。
   - 集約プレフィックスが不要な場合は、[集約（Aggregate）] をオフのままにし、[送信（Submit）] をクリックして に進みます。ステップ 5 （393 ページ）
   - 集約プレフィックスが必要な場合に [**集約（Aggregate**）] チェック ボックスをオンにします。

     [以上マスク（Greater Equal Mask）] フィールドと **[以下マスク（Less Equal Mask）]** フィールドが使用可能になります。

     1. **[以上マスク（Greater Equal Mask）]** フィールドで、一致させるプレフィックス長を指定します。

        有効な範囲は 0 ～ 128 です。値 0 は未指定と見なされます。

     2. **[以下マスク（Less Equal Mask）]** フィールドで、一致させるプレフィックス長を指定します。

        有効な範囲は 0 ～ 128 です。値 0 は未指定と見なされます。

     APIC リリース 4.2(3) 以降の **[以上マスク（Greater Equal Mask）]** および **[以下マスク（Less Equal Mask）]** フィールドの詳細については、一致プレフィックスの機能拡張 （385 ページ）を参照してください。

4. [一致ルート宛先ルールの作成（Create Match Route Destination Rule）] ウィンドウで [送信（Submit）] をクリックします。

ステップ 5 [一致ルールの作成（Create Match Rule）] ウィンドウで、[送信（Submit）] をクリックします。

一致ルールは、1 つ以上の一致宛先ルールと、1 つ以上の一致コミュニティ条件を持つことができます。一致の種類では AND フィルタがサポートされています。これを利用すると、受け入れられるためには、一致ルール内のすべて条件がルート一致ルールと一致することが必要になります。**Match Destination Rules** に複数の一致プレフィックスがある場合には、OR フィルタがサポートされます。これを利用すると、任意の一致プレフィックスがルートタイプとして受け入れられます。

ステップ 6 [**L3outs**] の下で、利用可能なデフォルト レイヤ 3 Out をクリックして選択します。

別のレイヤ 3 Out が必要な場合には、代わりにそれを選択することができます。

ステップ 7 [ルート制御のインポートおよびエクスポートのルート マップ（Route Map for import and export rout control）] を右クリックし、[ルート制御のインポートおよびエクスポートのルート マップの作成（Create Route Map for import and export rout control）] をクリックします。

ステップ 8 **ルート制御のインポートおよびエクスポートのルート マップの作成（Create Route Map for import and export rout control）** ダイアログボックスで、デフォルトのルート マップを使用するか、使用するルート マップの名前を入力します。

この例では、**default_export** ルート マップを使用します。

ステップ 9 **Type** フィールドで、**Match Routing Policy Only** を選択します。

一致ルーティング ポリシーは、グローバルな RPC 一致宛先ルートです。このフィールドで使用できる他のオプションとしては、一致プレフィックスおよびルーティング ポリシーで、RPC ルーティング ポリシーの宛先ルートと組み合わせることができます。

ステップ 10 [**コンテキスト（Contexts**）] 領域で、+ アイコンを展開して [**ルート制御コンテキストの作成（Create Route Control Context**）] ダイアログ ボックスを表示します。

ステップ 11 ルート制御のコンテキストの名前を入力し、各フィールドで必要なオプションを選択します。一致ルールで定義されている基準に一致するルートを拒否するには（次の手順で選択します）、アクション [**拒否（deny**）] を選択します。デフォルトのアクションは **permit** です。

ステップ 12 **Match Rule** フィールドで、前に作成したルールを選択します。

ステップ 13 **Set Rule** フィールドで、**Create Set Rules for a Route Map** を選択します。

通常は、ルート マップ/プロファイルで一致させることにより、プレフィックス リストに入出力を許可しますが、それに加えて何らかの属性をこれらのルートに設定し、その属性を持つルートをさらに一致させることもできます。

ステップ 14 **Create Set Rules for a Route Map** ダイアログボックスで、アクション ルールの名前を入力し、必要なチェック ボックスをオンにします。[完了（Finish）] をクリックします。

ステップ 15 **Create Route Control Context** ダイアログボックスで、**OK** をクリックします。[**インポートおよびエクスポート ルート制御向けのルート マップの作成（Create Route map for import and export route control**）] ダイアログ ボックスで、[**送信（Submit**）] をクリックします。

これで、ルート マップ/プロファイルの作成は完了です。ルート マップは、一致アクション ルールと設定アクション ルールの組み合わせです。ルート マップは、ユーザの必要に応じて、エクスポート プロファイルまたはインポート プロファイルまたは再配布可能プロファイルに関連付けられます。ルート マップのプロトコルを有効にすることができます。

ルート制御プロトコル

インポート制御とエクスポート制御を使用するルーティング制御プロトコルの設定について

このトピックでは、インポート制御とエクスポート制御を使用するルーティング制御プロトコルを設定する方法の典型的な例を示します。これは、外部 BGP を使用したネットワーク接続のレイヤ 3 が設定されていると仮定します。OSPF で設定されたネットワークの外部レイヤ 3 の次のタスクを実行することもできます。

GUI を使用した、インポート制御とエクスポート制御を使用するルート制御プロトコルの設定

この例では、ネットワーク接続 BGP を使用して外部レイヤ 3 が設定されていることを前提としています。OSPF を使用するように設定されたネットワークに対してもこれらのタスクを実行することができます。

このタスクでは、インポートポリシーとエクスポートポリシーの作成手順を示します。デフォルトでは、インポート制御は適用されていないため、インポート制御を手動で割り当てる必要があります。

始める前に

- テナント、プライベートネットワーク、およびブリッジドメインが作成されていること。
- テナント ネットワークのレイヤ 3 Outside が作成されていること。

手順

ステップ 1 メニュー バーで、**[テナント（TENANTS）] > [*Tenant_name*] > [ネットワーキング（Networking）] > [L3Out] > [*Layer3_Outside_name*]** の順にクリックします。

ステップ 2 [*Layer3_Outside_name*] を右クリックして、[**ルート制御のインポートおよびエクスポート向けルート マップの作成（Create Route map for import and export route control**）] をクリックします。

ステップ 3 [**ルート制御のインポートおよびエクスポート向けルート マップの作成（Create Route map for import and export route control**）] ダイアログ ボックスで、次のアクションを実行します。

a) [Name] フィールドのドロップダウン リストから、適切なルート プロファイルを選択します。
選択内容に応じて、特定の Outside でアドバタイズされている内容が自動的に使用されます。

b) **Type** フィールドで、**Match Prefix AND Routing Policy** を選択します。

c) [コンテキスト（Contexts）] 領域で、[+] をクリックして [ルート制御コンテキストの作成（Create Route Control Context）] ウィンドウを表示します。

ステップ 4 [Create Route Control Context] ダイアログボックスで、次の操作を実行します。

a) [Order] フィールドで、目的の順序の番号を選択します。

b) [Name] フィールドに、ルート制御プライベート ネットワークの名前を入力します。

c) **Match Rule** フィールドのドロップダウンリストで、**Create Match Rule For a Route Map** をクリックします。

d) **Create Match Rule** ダイアログボックスの **Name** フィールドに、一致ルールの名前を入力します。[Submit] をクリックします。`

必要に応じて、正規表現による一致コミュニティ条件および一致コミュニティ条件を指定します。一致コミュニティファクタでは、名前、コミュニティ、およびスコープを指定する必要があります。

e) [**セット ルール（Set Rule**）] ドロップダウン リストから、[**ルート マップのセット ルールの作成（Create Set Rules For a Route Map**）] を選択します。

f) **Create Set Rules For a Route Map** ダイアログボックスの **Name** フィールドに、ルールの名前を入力します。

g) 設定するルールのチェックボックスをオンにし、選択肢として表示されている適切な値を選択します。[完了（Finish）] をクリックします。
ポリシーが作成され、アクション ルールに関連付けられました。

h) [**ルート制御コンテキストの作成（Create Route Control Context**）] ダイアログボックスで、[**OK**] をクリックします。

i) [**インポートおよびエクスポート ルート制御向けのルート マップの作成（Create Route map for import and export route control**）] ダイアログ ボックスで、[**送信（Submit**）] をクリックします。

ステップ 5 [ナビゲーション（Navigation）] ペインで、**[ルート プロファイル（Route Profile）]** > **[*route_profile_name*]** > **[*route_control_private_network_name*]** の順に選択します。
[Work] ペインの [Properties] に、ルート プロファイル ポリシーと関連アクション ルール名が表示されます。

ステップ 6 [ナビゲーション（Navigation）] ペインで、[Layer3_Outside_name] をクリックし、[ポリシー/メイン（Policy/Main）] タブをクリックします。
Work ウィンドウに、**Properties** が表示されます。

ステップ 7 （任意） [**ルート制御の強化（Route Control Enforcement**）] フィールドのとなりの [**インポート（Import**）] チェック ボックスをオンにして、インポート ポリシーを有効にします。

インポート制御ポリシーはデフォルトで有効になっていませんが、ユーザが有効にすることができます。インポート制御ポリシーは BGP と OSPF でサポートされていますが、EIGRP ではサポートされていません。ユーザがサポートされていないプロトコルのインポート制御ポリシーを有効にしても、自動的に無視されます。エクスポート制御ポリシーは、BGP、EIGRP、および OSPF でサポートされます。

（注） BGP が OSPF 上で確立されると、インポート制御ポリシーは BGP にのみ適用され、OSPF は無視されます。

ステップ 8 カスタマイズされたエクスポート ポリシーを作成するには、[**ルート制御のインポートおよびエクスポートのルート マップ（Route Map for import and export rout control**）] を右クリックし、[**ルート制御のインポートおよびエクスポートのルート マップの作成（Create Route Map for import and export rout control**）] をクリックし、次のアクションを実行します。

a) [**ルート制御のインポートおよびエクスポート向けルート マップの作成（Create Route map for import and export route control**）] ダイアログ ボックスで、[**名前（Name**）] フィールドのドロップダウン リストから、エクスポート ポリシーを選択するか、名前を入力します。

b) [コンテキスト（Contexts）] 領域で、[+] をクリックして [ルート制御コンテキストの作成（Create Route Control Context）] ウィンドウを表示します。

c) [Create Route Control Context] ダイアログボックスの [Order] フィールドで、値を選択します。

d) [Name] フィールドに、ルート制御プライベート ネットワークの名前を入力します。

e) （任意） **Match Rule** フィールドのドロップダウンリストから **Create Match Rule For a Route Map** を選択し、必要に応じて一致ルール ポリシーを作成して、アタッチします。

f) [**セット ルール（Set Rule**）] フィールドのドロップダウン リストから、[**ルート マップのセット ルールの作成（Create Set Rules For a Route Map**）] を選択して、[**OK**] をクリックします。

または、必要に応じて既存の set アクションを選択し、**OK** をクリックします。

g) **Create Set Rules For A Route Map** ダイアログボックスの **Name** フィールドに名前を入力します。

h) 設定するルールのチェックボックスをオンにし、選択肢として表示されている適切な値を選択します。[完了（Finish）] をクリックします。
[Create Route Control Context] ダイアログ ボックスでは、ポリシーが作成されてアクション ルールに関連付けられています。

i) **OK** をクリックします。

j) [**インポートおよびエクスポート ルート制御向けのルート マップの作成（Create Route map for import and export route control**）] ダイアログ ボックスで、[**送信（Submit**）] をクリックします。

[Work] ペインに、エクスポート ポリシーが表示されます。

（注） エクスポート ポリシーを有効にするには、最初に適用する必要があります。この例では、このポリシーはネットワークのすべてのサブネットに適用されます。

ステップ 9 [**ナビゲーション（Navigation**）] ペインで **[L3Outs]** > **[*L3Out_name*]** > **[外部 EPG（External EPGs**）] > **[*externalEPG_name*]** の順に展開して、次のアクションを実行します。

a) **Route Control Profile** を展開します。

b) **Name** フィールドのドロップダウン リストから、前に作成したポリシーを選択します。

c) [**方向（Direction**）] フィールドのドロップダウン リストから、[**ルート エクスポート ポリシー（Route Export Policy**）] を選択します。[更新（Update）] をクリックします。

MP-BGP のインターリーク再配布

MP-BGP のインターリーク再配布の概要

このトピックでは、（）を使用して（）ファブリックでのインターリーク再配布を設定する方法について説明します。Cisco Application Centric InfrastructureACICisco Application Policy Infrastructure ControllerAPIC

Cisco ACI では、レイヤ 3 Outside（L3Out）が展開されている境界リーフ ノードが、L3Out ルートを BGP IPv4/IPv6 アドレス ファミリに再配布し、VRF 情報とともに MP-BGP VPNv4/VPNv6

アドレス ファミリに再配布して、L3Out ルートを配布します。境界リーフ ノードからスパイン ノードを介して他のリーフ ノードに移動します。Cisco ACI ファブリック内のインターリーク再配布は、BGP IPv4/IPv6 アドレス ファミリへの L3Out ルートのこの再配布を指します。デフォルトでは、BGP を介して学習されたルートを除き、ダイナミック ルーティング プロトコル、スタティック ルート、および L3Out インターフェイスの直接接続されたサブネットを介して学習されたルートなど、すべての L3Out ルートでインターリークが発生します。BGP を介して学習されたルートはすでに BGP IPv4/IPv6 テーブルにあり、インターリークなしで MP-BGP VPNv4/VPNv6 にエクスポートする準備ができています。

インターリーク再配布により、ユーザはルートマップを適用して L3Out ルートを選択的に BGP に再配布し、他のリーフ ノードに表示されるルートを制御したり、BGP コミュニティ、プリファレンス、メトリックなどの一部の属性をルートに設定したりできます。。この再配布により、入力境界リーフ ノードによって設定された属性に基づいて、または他のリーフ ノードがある境界リーフ ノードから別の境界リーフ ノードへのルートを優先できるように、別の境界リーフ ノードで選択的中継ルーティングを実行できます。

以前のリリースでは、OSPF および EIGRP ルートからのインターリーク再配布にルートマップを適用できました。

Cisco APIC 4.2(1) リリース以降では、スタティック ルートからのインターリーク再配布へのルートマップの適用がサポートされています。

Cisco APIC 5.1(4) リリース以降、直接サブネット（L3Out インターフェイス）からのインターリーク再配布へのルートマップの適用がサポートされています。この機能は、当初 Cisco APIC 4.2(6h) リリースで追加されましたが、5.1(4) リリースまではいずれの 5.x リリースでも使用できませんでした。

Cisco APIC 5.1(4) リリース以降では、スタティック ルートおよび直接サブネットのインターリーク再配布のために、ルートマップで**拒否**アクションを設定できます。この機能は、当初 Cisco APIC 4.2(6h) リリースで追加されましたが、5.1(4) リリースまではいずれの 5.x リリースでも使用できませんでした。

GUI を使用したインターリーク再配布のルート マップ の設定

インターリーク再配布のルート マップは、[テナント（Tenant）] [ポリシー（Policies）] [プロトコル（Protocol）] [ルート制御のルート マップ（Route Maps for Route Control）] で作成できます。 > > >

始める前に

テナントを作成します。

手順

ステップ 1 メニュー バーで、**[テナント]** をクリックします。

ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。

ステップ 3 [ナビゲーション（Navigation）] ペインで、[tenant_name Policies] [プロトコル（Protocol）] [ルート制御のルート マップ（Route Maps for Route Control）] を展開します。 > > >

ステップ 4 [ルート制御のルート マップ（Route Maps for Route Control）] を右クリックし、[ルート制御のルート マップの作成（Create Route Maps for Route Control）] をクリックします。[ルート制御のルート マップの作成（Create Route Maps for Route Control）] ダイアログボックスが表示されます。

ステップ 5 [名前（Name）] フィールドに、インターリーク（BGP への再配布）を制御するルート マップの名前を入力します。

ステップ 6 [コンテキスト（Contexts）] 領域で [+] サインをクリックして、**[ルート制御コンテキスト作成（Create Route Control Context）]** ダイアログ ボックスを表示し、次のアクションを実行します。

a) 必要に応じて、**[順序（Order）]** と **[名前（Name）]** フィールドに入力します。
b) **[アクション（Action）]** フィールドで **[許可（Permit）]** を選択します。
c) [一致ルール（Match Rule）] フィールドで、目的の一致ルールを選択するか、新しい一致ルールを作成します。
d) [セットルール（Set Rule）] フィールドで、目的のセットルールを選択するか、新しいセット ルールを作成します。
e) **[OK]** をクリックします。

作成する必要があるルート制御コンテキストごとに、この手順を繰り返します。

ステップ 7 **[ルート マップの作成（Create Route Map）]** ダイアログ ボックスで、**[送信（Submit）]** をクリックします。

GUI を使用したインターリーク再配布のルート マップの適用

特定の L3Out からのインターリーク再配布をカスタマイズするルートマップは、L3Out を介して適用する必要があります。

始める前に

テナント、VRF、および L3Out を作成します。

手順

ステップ 1 メニュー バーで、**[テナント]** をクリックします。

ステップ 2 [Work] ペインで、テナントの名前をダブルクリックします。

ステップ 3 **[ナビゲーション（Navigation）]** ペインで、**[*tenant_name*]** > **[ネットワーキング（Networking）]** > **[L3Outs]** > **[*L3Out_name*]** の順に展開します。

ステップ 4 [ポリシー メイン（Policy Main）] タブをクリックして、この L3Out の [プロパティ（Properties）] ウィンドウにアクセスします。 >

ステップ 5 OSPF または EIGRP ルートの場合は、次の操作を実行します。

a) [**インターリークのルート プロファイル（Route Profile for Interleak**）] フィールドで、ルート マップ/プロファイルを選択するか作成します。

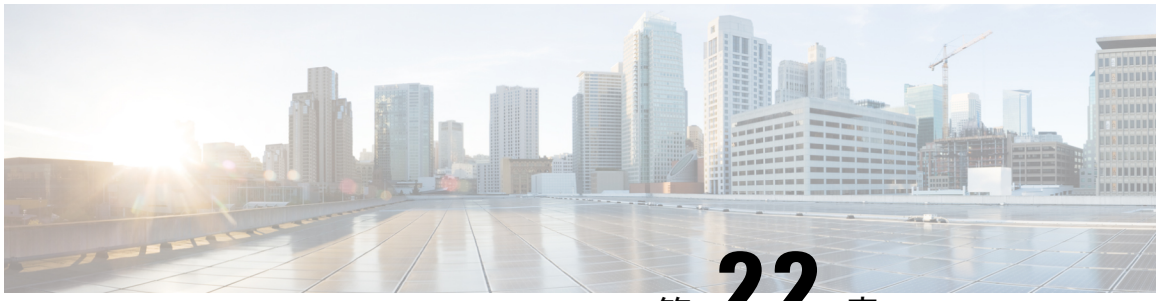
b) [ワーク（Work）] ペインで、[送信（Submit）] をクリックし、[変更の送信（Submit Changes）] をクリックします。

ステップ 6 スタティック ルートの場合は、次の操作を実行します。

a) [再配布のルート プロファイル（Route Profile for Redistribution）] フィールドで、[+] アイコンをクリックします。

b) [送信元（Source）] フィールドで、インターリーク再配布の送信元としてスタティック ルートのスタティックを選択します。

c) [更新（Update）] をクリックします。



第 22 章

ルーティングとサブネット範囲

この章は、次の内容で構成されています。

L3Out EPG スコープと制御パラメータ

サブネットの範囲と集約コントロール

次のセクションでは、サブネットを作成するときに利用できるいくつかの範囲と集約に関するオプションについて説明します:

Export Route Control Subnet: コントロールは、ファブリック外の特定の中継ルートをアドバタイズします。これは中継ルートにのみ影響するもので、内部ルートやブリッジドメインで設定されるデフォルトのゲートウェイには影響しません。

インポート ルート コントロール サブネット：このコントロールは、インポート ルート制御の強制が設定されている場合、ルートを Border Gateway Protocol（BGP）と Open Shortest Path First（OSPF） でファブリックにアドバタイズすることを可能にします。

External Subnets for the External EPG (セキュリティ インポート サブネットとも呼ばれる): このオプションは、ルーティング情報のファブリックへの出入りはコントロールしません。トラフィックがある外部 EPG から別の外部 EPG に、または内部 EPG に流れるようにするには、サブネットにはこのコントロールでマークを付ける必要があります。このコントロールを使用してサブネットにマークしなかった場合には、ある EPG から学習したルートが他の外部 EPG にもアドバタイズされますが、パケットはファブリックでドロップされます。パケットがドロップされるのは、APIC が許可済みリスト モデルで動作するからです。そのデフォルトの動作は、契約で明示的に許可されていない限り、EPG 間の全データ プレーン トラフィックをドロップするというものです。この許可済みリスト モデルは外部 EPG とアプリケーション EPG に適用されます。このオプションが設定されているセキュリティ ポリシーを使用する場合には、契約とセキュリティ プレフィックスを設定する必要があります。

Shared Route Control Subnet: VRF 間のリーキングの共有 L3Outs から学習されたサブネットは、他の VRF にアドバタイズされる前に、このコントロールでマークされる必要があります。APIC リリース 2.2(2e) 以降では、異なる VRF の共有 L3Outs は契約を使用して相互に通信できます。異なる VRF の共有 L3Outs 間の通信の詳細については、『*Cisco APIC* レイヤ *3* ネットワーキング構成定ガイド』を参照してください。

Shared Security Import Subnet: このコントロールは、共有 L3Out 学習ルートについては、[External Subnets for the External EPG] と同じです。トラフィックがある外部 EPG から別の外部 EPG に、または別の内部 EPG に流れるようにするには、サブネットにはこのコントロールでマークを付ける必要があります。このコントロールを使用してサブネットにマークしなかった場合には、ある EPG から学習したルートが他の外部 EPG にもアドバタイズされますが、パケットはファブリックでドロップされます。このオプションが設定されているセキュリティ ポリシーを使用する場合には、契約とセキュリティ プレフィックスを設定する必要があります。

Aggregate Export, Aggregate Import, and Aggregate Shared Routes: このオプションは、0.0.0.0/0 プレフィックスの前に 32 を追加します。現在、インポート/エクスポート ルート制御サブネットに集約できるのは、0.0.0.0/0 プレフィックスのみです。0.0.0.0/0 プレフィックスを集約すると、制御プロファイルを 0.0.0.0/0 ネットワークに適用することはできなくなります。

Aggregate Shared Route: このオプションは、共有ルート制御サブネットとしてマークされている任意のプレフィックスに使用できます。

Route Control Profile: ACI ファブリックは、ファブリックの内部と外部にアドバタイズされるルート用に、ルート マップの set 句もサポートします。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 プロファイルで設定されます。

セキュリティ インポート ポリシー

静的 L3Out EPG

本書で説明されているポリシーでは、ACI ファブリックの内外へのルーティング情報の交換、およびルートの制御とタグ付けに使用する方法を取り扱ってきました。ファブリックは許可リスト モデルで動作します。そのデフォルトの動作は、契約によって明示的に許可されていない限り、エンドポイント グループ間のすべてのデータプレーン トラフィックをドロップするというものです。この許可リスト モデルは外部 EPG とテナント EPG に適用されます。

中継トラフィックの場合、テナント トラフィックとは、セキュリティ ポリシーの設定方法と実装方法が少し異なります。

中継セキュリティ ポリシー

- プレフィックス フィルタリングを使用します。
- リリース 2.0(1m) 以降では、Ethertype、プロトコル、L4 ポート、および TCP フラグ フィルタのサポートが利用できるようになりました。
- セキュリティ インポート サブネット（プレフィックス）と外部 EPG で設定されたコントラクトを使用して実装されます。

テナント EPG セキュリティ ポリシー

- プレフィックス フィルタリングは使用しないでください。
- Ethertype、プロトコル、L4 ポート、および TCP フラグ フィルタをサポートします。
- テナント EPG←→EPG およびテナント EPG←→外部 EPG でサポートされます。

外部プレフィックス ベースの EPG 間に契約が存在しない場合、トラフィックはドロップされます。2 つの外部 Epg の間のトラフィックを許可するには、契約とセキュリティ プレフィックスを設定する必要があります。プレフィックスフィルタリングのみがサポートされるため、契約ではデフォルト フィルタを使用できます。

外部 L3Out 接続契約

L3Out 接続が展開されているすべてのリーフ ノードでは、L3Out 接続のプレフィックスの結合がプログラムされます。3 つ以上の L3Out 接続が展開されている場合、集約ルール 0.0.0.0/0 を使用すると、契約のない L3Out 接続間でもトラフィックのフローが許可されます。

L3Out インスタンス プロファイル (instP) で、プロバイダーとコンシューマの契約の関連づけとセキュリティ インポート サブネットを設定します。

セキュリティ インポート サブネットが設定されており、集約ルール、0.0.0.0/0 がサポートされている場合、セキュリティ インポート サブネットは ACL タイプのルールに従います。セキュリティ インポート サブネットのルール 10.0.0.0/8 は、 10.0.0.0～10.255.255.255 の範囲のすべてのアドレスに適合します。ルート制御サブネットで許可されているプレフィックスに対して正確なプレフィックス照合を設定する必要はありません。

3 つ以上の L3Out 接続が同じ VRF 内に設定されている場合は、ルールの結合が問題となるため、セキュリティ インポート サブネットを設定するときに注意する必要があります。

同じ L3Out で入出力する中継トラフィック フローは、0.0.0.0/0 セキュリティ インポート サブネットを設定すると、ポリシーによってドロップされます。この動作は、ダイナミックまたはスタティック ルーティングに当てはまります。この動作を防ぐためには、より詳細なサブネットを定義してください。

ダイナミック L3Out EPG 分類

Cisco APIC 5.2(4) リリースより前は、外部サブネットは外部 EPG の下で構成されていたため、外部サブネットの pcTag は外部 EPG の pcTag から派生していました。ルーティングが変更されると、外部サブネットは別の L3Out または外部 EPG から学習されました。 pcTag は、ルーティングが変更されても変更されません。

Cisco APIC 5.2(4) リリース以降、動的 L3Out EPG 分類 (DEC) 機能が導入され、ルーティングの変更に伴う pcTag の動的な変更が可能になりました。

この機能により、管理者はサブネットまたは BGP コミュニティを照合することにより、ルート マップを使用して外部 EPG を設定することもできます。外部 EPG 設定が設定されたルート マップは、デフォルト インポートを使用して L3Out に、またはルート制御プロファイルを使用して BGP ピアに適用できます。L3Out の外部 EPG および契約設定は以前と同じままです。

ルート マップに基づいて、特定の外部 EPG および関連する契約がプレフィックスに対して決定されます。

（注） ルート マップによる外部 EPG の選択は、L3Out で設定された外部 EPG サブネットよりも優先されます。たとえば、ルート マップ構成が 10.1.1.0/24 を外部 *EPG1* に関連付け、サブネット *10.1.1.0/24* が外部 *EPG2* に構成されている場合、外部 *EPG1* はルート マップによる外部 EPG 決定が優先されるため、*10.1.1.0/24* のハードウェアでプログラムされます。

DEC の注意事項と制限事項

- この機能は、BGP と OSPF のみをサポートします。
- DEC は、L3Out デフォルト インポート ルート マップまたは BGP ピア インポート ルート マップでのみサポートされます。
- 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。
- DEC は次の機能をサポートしていません。
  - サイト間
  - 浮動 L3Out との統合
  - スタティックルーティング
  - EIGRP
  - セグメント ルーティング
  - 午前
  - 浮動 L3Out を使用した BGP ネクストホップ伝達
  - Cisco ACI GOLF、SR-MPLS、およびフォールバック ルートとの共存

GUI を使用したダイナミック L3Out EPG 分類の設定

この手順では、ダイナミック L3Out EPG 分類（DEC）を構成し、BGP を使用してレイヤー 3 外部ネットワーク接続を構成していることを前提としています。OSPF を使用して設定された L3Out に対してこれらのタスクを実行することもできます。

このタスクでは、インポートポリシーとエクスポートポリシーの作成手順を示します。デフォルトでは、インポート制御は適用されていないため、インポート制御を手動で割り当てる必要があります。

始める前に

- テナント、プライベート ネットワーク、およびブリッジ ドメインが作成されていること。

- テナント ネットワークのレイヤ 3 Outside が作成されていること。

手順

ステップ 1 メニュー バーで、**[テナント（Tenants）] > > [すべてのテナント（ALL Tenants）]** の順に選択します。

ステップ 2 **[作業（Work）]** ペインで、テナント名をダブルクリックします。

ステップ 3 **[ナビゲーション（Navigation）]** ペインで、**[*tenant_name*]** > **[ネットワーキング（Networking）]** > **[L3Outs]** > ***[L3Out_name[*** の順に展開します。

ステップ 4 *[Layer3_Outside_name]* を右クリックして、**[ルート制御のインポートおよびエクスポート向けルート マップの作成（Create Route map for import and export route control）]** をクリックします。

ステップ 5 [**ルート制御のインポートおよびエクスポート向けルート マップの作成（Create Route map for import and export route control**）] ダイアログ ボックスで、次のアクションを実行します。

a) [**名前（Name**）] フィールドから、[**default-import**] を選択します。
選択内容に応じて、特定の L3Out でアドバタイズされている内容が自動的に使用されます。

b) **Type** フィールドで、**Match Prefix AND Routing Policy** を選択します。

c) **[コンテキスト（Contexts）]** 領域で、**[+]** をクリックして **[ルート制御コンテキストの作成（Create Route Control Context）]** ウィンドウを表示します。

ステップ 6 [Create Route Control Context] ダイアログボックスで、次の操作を実行します。

a) [Order] フィールドで、目的の順序の番号を選択します。

b) [Name] フィールドに、ルート制御プライベート ネットワークの名前を入力します。

c) **[関連する一致したルール（Associated Matched Rules）]** テーブルで、**[+]** をクリックします。

d) **[セット ルール（Set Rule）]** ドロップダウン リストから、**[ルート マップのセット ルールの作成（Create Set Rules For a Route Map）]** を選択します。

e) **[ルート マップの一致ルールの作成（Create Match Rule for Route Map）]** ダイアログボックスの **[名前（Name）]** フィールドに、一致ルールの名前を入力します。

f) 必要に応じて、正規表現による一致コミュニティ条件および一致コミュニティ条件を指定します。

一致コミュニティ ファクタでは、名前、コミュニティ、および範囲を指定する必要があります。

g) **[送信（Submit）]** をクリックします。

h) **[セット ルール（Set Rule）]** ドロップダウン リストから、**[ルート マップのセット ルールの作成（Create Set Rules For a Route Map）]** を選択します。

i) **[ルート マップのセット ルールの作成（Create Set Rules For a Route Map）]** ダイアログボックスの **[名前（Name）]** フィールドに、ルールの名前を入力します。

j) **[外部 EPG の設定（Set External EPG）]** チェックボックスをオンにして、**[外部 EPG（External EPG）]** ドロップダウン リストで EPG を選択して、**[完了（Finish）]** をクリックします。
ポリシーが作成され、アクション ルールに関連付けられました。

k) [**ルート制御コンテキストの作成（Create Route Control Context**）] ダイアログボックスで、[**OK**] をクリックします。

l) [**インポートおよびエクスポート ルート制御向けのルート マップの作成（Create Route map for import and export route control**）] ダイアログ ボックスで、[**送信（Submit**）] をクリックします。

ステップ 7 **[作業（Work）]** ペインで、**[ポリシー（Policy）]** > **[メイン（Main）]**タブを選択します。
Work ウィンドウに、**Properties** が表示されます。

ステップ 8 （任意） **[ルート制御の強化（Route Control Enforcement）]** フィールドのとなりの **[インポート（Import）]** チェック ボックスをオンにして、インポート ポリシーを有効にして **[送信（Submit）]** をクリックします。

インポート制御ポリシーはデフォルトで無効になっています。インポート制御ポリシーは BGP と OSPF でサポートされていますが、EIGRP ではサポートされていません。ユーザーがサポートされていないプロトコルのインポート制御ポリシーを有効にしても、プロトコルは自動的に無視されます。エクスポート制御ポリシーは、BGP、EIGRP、および OSPF でサポートされます。また、ネイバー インポート ルート マップごとに BGP を設定する場合は、インポート ポリシーの **[インポート（Import）]** チェックボックスをオンにする必要はありません。

（注） BGP が OSPF 上で確立されると、インポート制御ポリシーは BGP にのみ適用され、OSPF は無視されます。

ステップ 9 カスタマイズされたエクスポート ポリシーを作成するには、**[ナビゲーション（Navigation）]** ペインで、**[ルート制御のインポートおよびエクスポートのルート マップ（Route Map for import and export rout control）]** を右クリックし、**[ルート制御のインポートおよびエクスポートのルート マップの作成（Create Route Map for import and export rout control）]** をクリックし、次のアクションを実行します。

a) [**ルート制御のインポートおよびエクスポート向けルート マップの作成（Create Route map for import and export route control**）] ダイアログ ボックスで、[**名前（Name**）] ドロップダウン リストから、エクスポート ポリシーを選択するか、名前を入力します。

b) **[コンテキスト（Contexts）]** 領域で、**[+]** をクリックして **[ルート制御コンテキストの作成（Create Route Control Context）]** ダイアログを開きます。

c) **[ルート制御コンテキストの作成（Create Route Control Context）]** ダイアログボックスの **[注文（Order）]** フィールドに、値を入力します。

d) [Name] フィールドに、ルート制御プライベート ネットワークの名前を入力します。

e) （任意） **[関連する一致ルール（Associated Match Rules）]** テーブルで、**[+]** をクリックし、**[ルール名（Route Name）]** ドロップダウン リストから **[ルート マップの一致ルールを作成（Create Match Rule For a Route Map）]** を選択し、必要に応じてフィールドに入力して、**[送信（Submit）]** をクリックします。

f) [**セット ルール（Set Rule**）] ドロップダウン リストから、[**ルート マップのセット ルールの作成（Create Set Rules For a Route Map**）] を選択します。

または、既存のセット ルールを選択できます。

g) **[ルート マップのセット ルールの作成（Create Set Rules For a Route Map）]** を選択した場合は、**[ルート マップのセット ルールの作成（Create Set Rules For A Route Map）]** ダイアログ ボックスで、**[名前（Name）]** フィールドにセット ルールの名前を入力し、設定するルールのチェック ボックスをオンにして、次のように入力します。ルールに適切な値を入力し、**[完了（Finish）]** をクリックします。
[Create Route Control Context] ダイアログ ボックスでは、ポリシーが作成されてアクション ルールに関連付けられています。

h) **OK** をクリックします。

i) [**インポートおよびエクスポート ルート制御向けのルート マップの作成（Create Route map for import and export route control**）] ダイアログ ボックスで、[**送信（Submit**）] をクリックします。

[Work] ペインに、エクスポート ポリシーが表示されます。

（注） エクスポート ポリシーを有効にするには、最初に適用する必要があります。この例では、このポリシーはネットワークのすべてのサブネットに適用されます。

ステップ 10 **[ナビゲーション（Navigation）]** ペインで ***[tenant_name]*** > **[ネットワーキング（Networking）]** > **[L3Outs]** > ***[L3Out_name]*** > **[外部 EPG（External EPGs）]** > ***[external_EPG_name]*** の順に展開して、次のアクションを実行します。

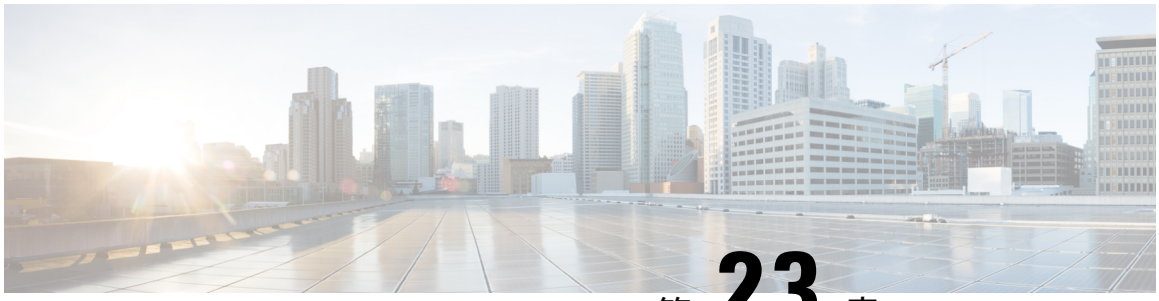
a) **ルート制御プロファイル** テーブルで、+ をクリックします。

b) **[名前（Name）]** フィールドのドロップダウン リストから、前に作成したポリシーを選択します。

c) **[方向（Direction）]** フィールドのドロップダウン リストから、**[ルート エクスポート ポリシー（Route Export Policy）]** を選択します。

d) **Update** をクリックします。

e) [Submit] をクリックします。



第 23 章

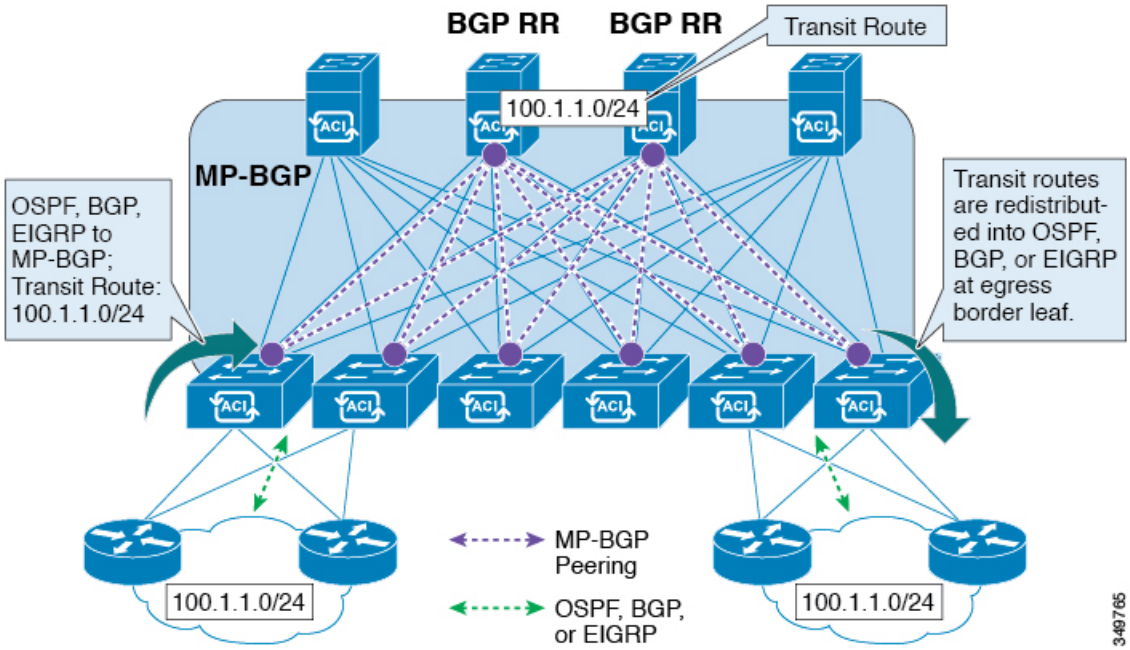
トランジット ルーティング

この章は、次の内容で構成されています。

中継 ACI ファブリックのルーティング

Cisco APIC ソフトウェアは、OSPF（NSSA）および iBGP を使用した外部レイヤ 3 接続をサポートします。ファブリックは、外部レイヤ3アウトサイド（l3out）接続の外部ルータにテナントブリッジドメインのサブネットをアドバタイズします。外部ルータから学習されたルートは、他の外部ルータにアドバタイズされません。ファブリックはスタブネットワークと同じように動作し、外部レイヤ 3 ドメイン間のトラフィックの伝送に使用できます。

図 *45 :* ファブリックでルーティング中継



中継のルーティングで1つのテナントとVRF内の複数のL3Out接続がサポートされているし、APIC は別の L3Out 接続を 1 つの L3Out 接続から学習したルートをアドバタイズします。外部レイヤ 3 ドメインは、境界リーフ スイッチの ファブリックとピアリングします。ファブリックはピア間の Multiprotocol-Border Gateway Protocol（MP-BGP）中継ドメインです。

外部L3Out接続の設定は、テナントとVRF レベルで実行されます。外部ピアから学習したルートは、VRF ごとに入力リーフの MP-BGP にインポートされます。L3Out 接続から学習したプレフィックスは、テナント VRF が存在するリーフ スイッチにのみエクスポートされます。

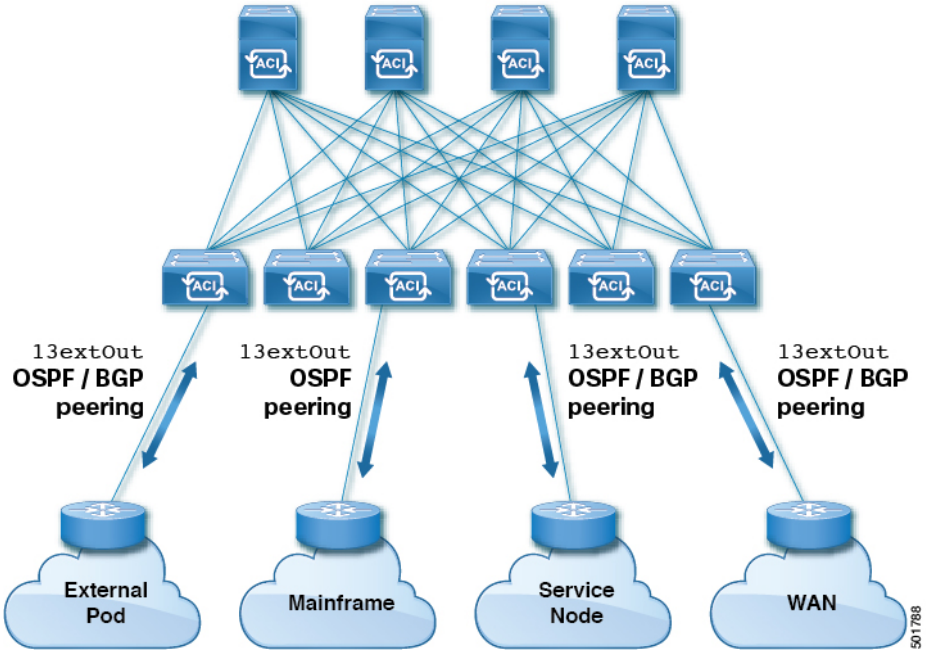
（注） 注意事項と中継ルーティングの設定のガイドラインは、次を参照してください。中継ルーティングのガイドライン （418 ページ）

トランジット ルーティングの使用例

レイヤ 3 ドメイン間のトランジット ルーティング

外部ポッド、メインフレーム、サービス ノード、WAN ルータなどの複数のレイヤ 3 ドメインがACIファブリックとピアリングして、それらの間のトランジット機能を提供することができます。

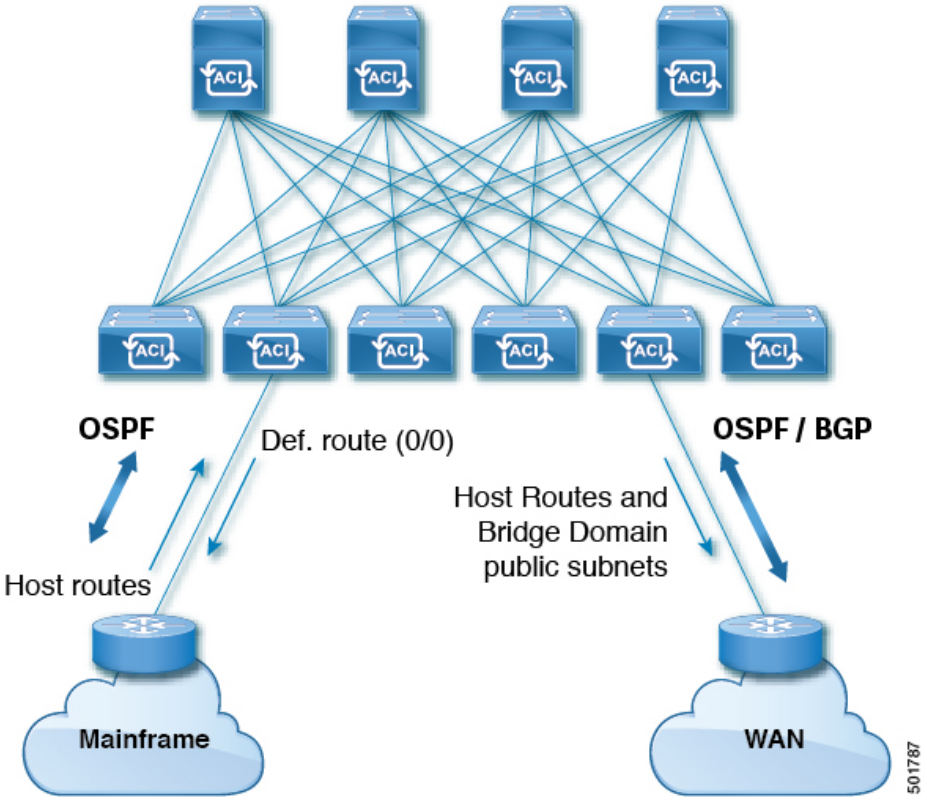
図 *46 :* レイヤ *3* ドメイン間のトランジット ルーティング



ACI ファブリックで中継されるメインフレーム トラフィック

メインフレームは、論理パーティション（LPAR）および仮想 IP アドレッシング（VIPA）の要件に対応する標準 IP ルーティング プロトコルを実行する IP サーバとして機能します。

図 *47 :* メインフレームのトランジット接続

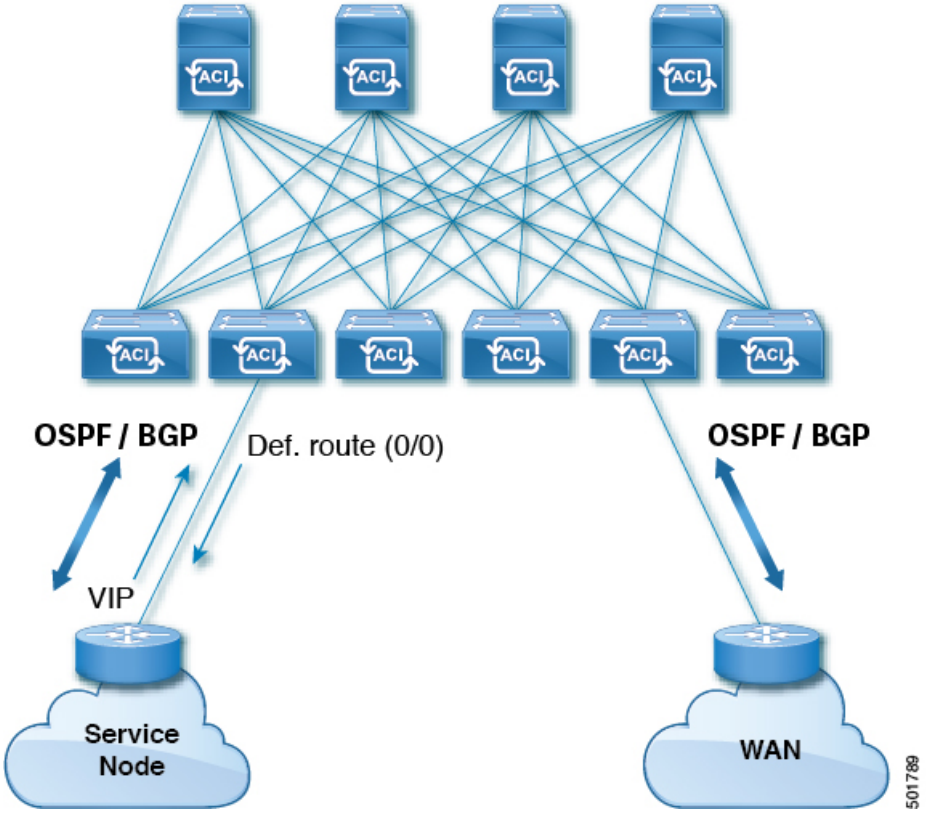


このトポロジにおいて、メインフレームは、ACI ファブリックが WAN ルータを経由して外部と接続するため、およびファブリック内の East-West トラフィックのための中継ドメインとなることを必要とします。これらは、ホストルートをファブリックにプッシュして、ファブリック内、および外部インターフェイスに再配布されるようにします。

サービス ノードのトランジット接続

サービス ノードは ACI ファブリックとピアリングし、外部 WAN インターフェイスに再配布される仮想 IP (VIP) ルートをアドバタイズすることができます。

図 *48 :* サービス ノードのトランジット接続

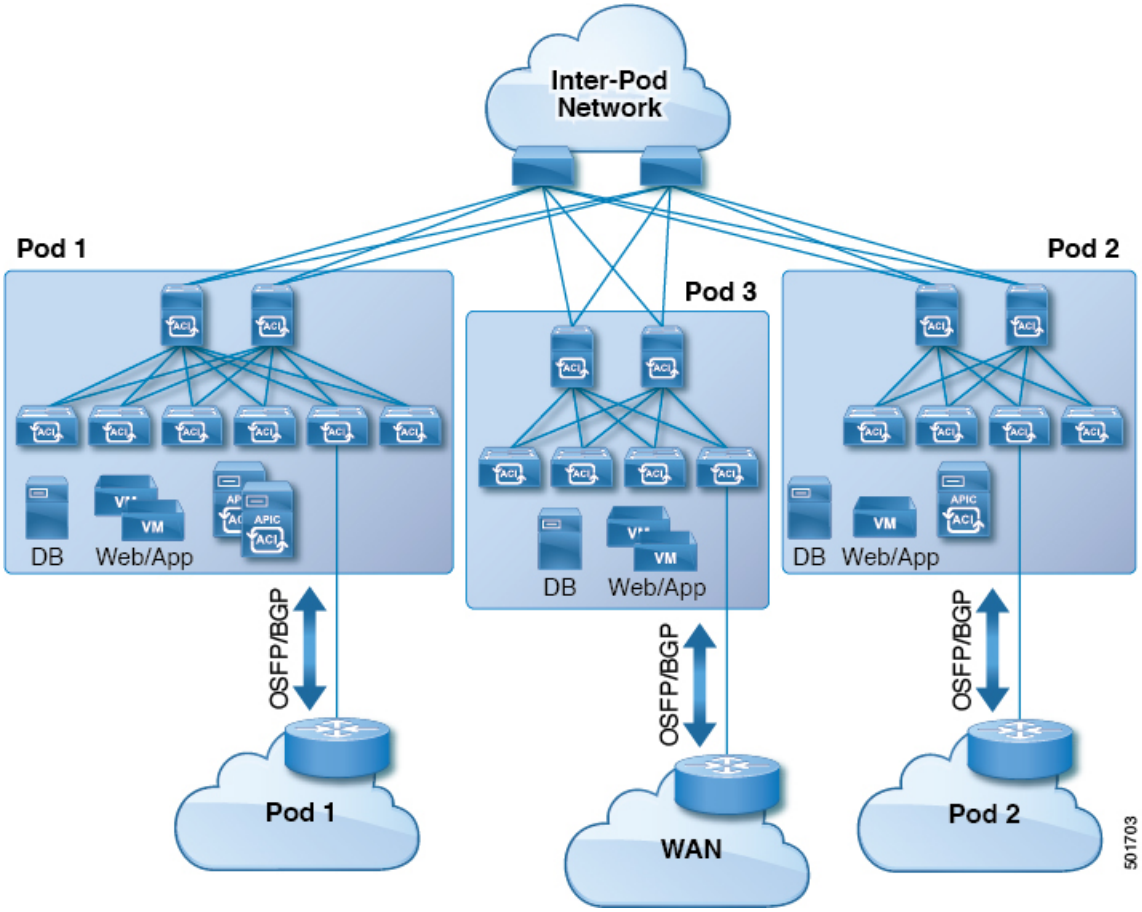


VIP は、特定のサイトやサービスの外部向けの IP アドレスです。VIP は、サービス ノードの背後にある 1 つ以上のサーバまたはノードに関連付けられています。

中継ルーティング設定でのマルチポッド

マルチポッド トポロジでは、ファブリックは、外部接続と複数のポッド間の相互接続の中継として機能します。クラウド プロバイダは、顧客データセンター内に管理対象のリソース ポッドを展開できます。責任分界点は、ファブリックとのピアリングを行っている OSPF または BGP を伴う L3Out にすることができます。

図 *49 :* 中継ルーティング設定における *L3Out* を伴う複数のポッド



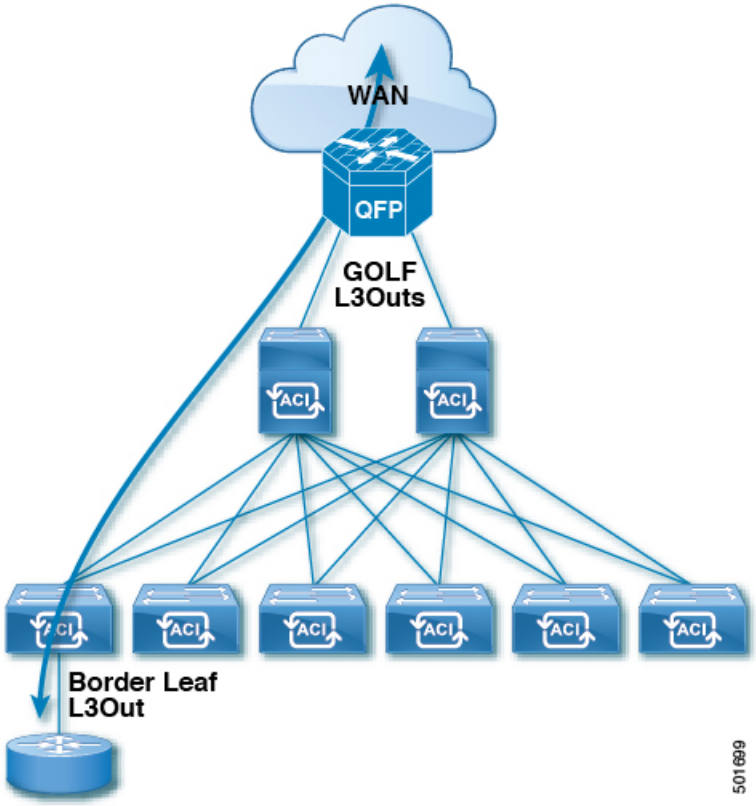
このようなシナリオでは、ポリシーは責任分界点で管理され、ACI ポリシーを設定する必要はありません。

レイヤ4 ～ レイヤ 7 ルート ピアリングはファブリックを中継として使用する特殊な使用例であり、ファブリックは複数ポッドに対する中継 OSPF または BGP ドメインの役目を果たします。ルート ピアリングは、接続されているリーフ ノードとルートを交換できるようにするため、レイヤ4 ～ レイヤ 7 サービス デバイス上で OSPF または BGP ピアリングを有効にするように設定します。ルート ピアリングの一般的な使用例として、SLB VIP が OSPF および iBGP を介して ファブリック外のクライアントにアドバタイズされる、ルート ヘルス インジェクションがあります。このシナリオの詳細については、『*L4-L7 Route Peering with Transit Fabric - Configuration Walkthrough*』を参照してください。

中継ルーティング設定での GOLF

APIC、リリース 2.0 以降では、Cisco ACI は、GOLF L3Out での中継ルーティング (BGP と OSPF) をサポートしています。 たとえば、次の図は、GOLF L3Out と境界リーフ L3Out を伴うファブリックで中継されるトラフィックを示しています。

図 *50* : 中継ルーティング設定での *GOLF L3Out* と境界リーフ *L3Out*



サポートされるトランジットの組み合わせのマトリックス

レイヤ 3 Outside 接続タイプ		OSPF	iBGP			eBGP			EIGRP v4	EIGRP v6	スタティックルート
			OSPF 上の iBGP	スタティックルート上の iBGP	直接接続上の iBGP	OSPF 上の eBGP	スタティックルート上の eBGP	直接接続上の eBGP			
OSPF		はい	はい*	はい	○*（APIC リリース 1.3 c でテスト）	はい	はい	はい	はい	○*（APIC リリース 1.2 g でテスト）	はい
iBGP	OSPF 上の iBGP	○*	X	X	X	○*（APIC リリース 1.3 c でテスト）	非対応	はい	はい	非対応	○
	スタティックルート上の iBGP	はい	X	X	X	○*（APIC リリース 1.2 g でテスト）	X	○*（APIC リリース 1.2 g でテスト）	はい	非対応	○
	直接接続上の iBGP	はい	X	X	X	-	X	○*（APIC リリース 1.2 g でテスト）	はい	非対応	○

レイヤ 3 Outside 接続タイプ		OSPF	iBGP			eBGP			EIGRP v4	EIGRP v6	スタティックルート
			OSPF 上の iBGP	スタティックルート上の iBGP	直接接続上の iBGP	OSPF 上の eBGP	スタティックルート上の eBGP	直接接続上の eBGP			
eBGP	OSPF 上の eBGP	はい	○*（APIC リリース 1.3 c でテスト）	○*（APIC リリース 1.3 c でテスト）	○*（APIC リリース 1.3 c でテスト）	はい	○*（APIC リリース 1.3 c でテスト）	○*（APIC リリース 1.3 c でテスト）	はい	非対応	○*（APIC リリース 1.3 c でテスト）
	スタティックルート上の eBGP	はい	X	X	X	○*（APIC リリース 1.2 g でテスト）	○（APIC リリース 3.0 でテスト）	○*（APIC リリース 1.2 g でテスト）	はい	非対応	○
	直接接続上の eBGP	はい	はい	はい	○*（APIC リリース 1.3 c でテスト）	○*（APIC リリース 1.3 c でテスト）	○*（APIC リリース 1.3 c でテスト）	はい	はい	非対応	○
EIGRPv4		はい	はい	はい	はい	はい	はい	はい	○（APIC リリース 1.3 c でテスト）	非対応	○

レイヤ 3 Outside 接続タイプ	OSPF	iBGP			eBGP			EIGRP v4	EIGRP v6	スタティック ルート
		OSPF 上の iBGP	スタティック ルート上の iBGP	直接接続上の iBGP	OSPF 上の eBGP	スタティック ルート上の eBGP	直接接続上の eBGP			
EIGRPv6	○ (APIC リリース 1.2 g でテスト)	X	X	X	X	X	X	X	○ (APIC リリース 1.3 c でテスト)	○ (APIC リリース 1.2 g でテスト)
スタティック ルート	はい	はい	はい	はい	○ (APIC リリース 1.3 c でテスト)	はい	はい	はい	○ (APIC リリース 1.2 g でテスト)	○

- 接続= 接続
- * = 同じリーフ スイッチではサポートされません
- × = サポートされていないかテストされていない組み合わせ

トランジット ルーティングの注意事項

中継ルーティングのガイドライン

作成し、中継ルーティング接続を維持する場合は、次のガイドラインを使用します。

トピック	注意またはガイドライン
複数の VRF 間のトランジット ルーティング時の ACI ファブリック iBGP への OSPF/EIGRP 再配布：ルート タグ	外部ルータを使用して複数の VRF 間のルーティングを行う中継ルーティング シナリオでは、デフォルト ルート タグ（4294967295）以外のエントリを使用して異なる VRF のポリシーを識別する場合に、1 つまたは複数の OSPF または EIGRP のテナント L3Out から取り消されたルートが存在する時にルーティングがループするリスクがあります。 これは想定されている動作です。EIGRP/OSPF が ACI ファブリックにルートを再配布すると、境界リーフ スイッチのデフォルトの iBGP アンチルーティング ループ メカニズムは、特定のデフォルト ルート タグ 4294967295 を使用するか、または [VRF/ポリシー（VRF/Policy）] ページの [トランジット ルート タグ ポリシー（Transit Route Tag Policy）] フィールドで割り当てられたものと同じタグを使用します。 VRF ごとに異なる固有の中継ルート タグを設定すると、デフォルトのアンチルーティング ループ メカニズムは機能しません。この状況を回避するには、すべての VRF で [トランジット ルート タグ ポリシー（Transit Route Tag Policy）] フィールドに同じ値を使用します。ルートマップとタグの使用に関する詳細については、「OSPF または EIGRP のバックツーバック設定」の行と、この表のルート制御プロファイル ポリシーに関するその他の情報を参照してください。 （注） ルート タグ ポリシーは、[ルート タグ ポリシーの作成（Create Route Tag Policy）] ページで設定します。このページには、[VRF /ポリシー（VRF / Policy）] ページの [トランジット ルート タグ ポリシー（Transit Route Tag Policy）] フィールドからアクセスします。 **[テナント（Tenants）] > [*tenant_name*] > [ネットワーキング（Networking）] > [VRFs] > [*VRF_name*]** の順にクリックします。

トピック	注意またはガイドライン
中継が1つのL3Outプロファイルを使用してルーティング	

トピック	注意またはガイドライン
	Cisco APIC リリース 2.3(1f) より前では、単一の L3Out プロファイル内での中継ルーティングはサポートされていませんでした。Cisco APIC リリース 2.3(1f) 以降では、単一の L3Out プロファイル内での中継ルーティングを構成できます。ただし次の制限があります。 • VRF インスタンスが強制されない場合、外部のサブネット 0.0.0.0/0（l3extSubnet）を使用して、同じレイヤ 3 EPG を共有するルータ間でのトラフィックを許可できます。 • VRF インスタンスが強制される場合、外部のデフォルト サブネット（0.0.0.0/0）を使用して、同じレイヤ 3 EPG 内のトラフィックで、送信元と接続先のプレフィックスの両方をマッチさせることはできません。同じレイヤ 3 EPG 内のすべてのトラフィックをマッチさせることを目的として、Cisco APIC は次のプレフィックスをサポートしています。 • **IPv4** • 0.0.0.0/1：外部 EPG 用の外部サブネット • 128.0.0.0/1：外部 EPG 用の外部サブネット • 0.0.0.0/0：インポート ルート制御サブネット、集約インポート • **IPv6** • 0::0/1：外部 EPG 用の外部サブネット • 8000::0/1：外部 EPG 用の外部サブネット • 0:0/0：インポートルート制御サブネット、集約インポート レイヤ 3 内 EPG 転送のコントラクトは必要ありません。 • または、少なくとも 1 つの他の EPG（アプリケーションまたは外部）を持つコントラクトと組み合わせて、単一のデフォルトサブネット（0.0.0.0/0）を使用することもできます。この EPG の代わりに vzAny を使用することはできません。ただし、他の EPG を展開する必要はありません。 たとえば、アプリケーション EPG の提供コントラクトと、レイヤ 3 EPG の消費コントラクトを使用す

トピック	注意またはガイドライン
	る場合（0.0.0.0/0でマッチング）や、アプリケーション EPG の消費コントラクトと、レイヤ 3 EPG の提供コントラクトを使用する場合（0.0.0.0/0 でマッチング）です。
ハードウェア サポートの違いを共有ルート:	第 2 世代のスイッチの VRF 機能間で正常にルートが共有されます（N9K-93108TC-EX など、スイッチ モデル名の最後やその後に「EX」や「FX」がつく Cisco Nexus N9K）。第 1 世代のスイッチですが、ルートを保存する物理的な 3 進コンテンツ対応メモリ（TCAM）にルートの解析を完全にサポートするだけの容量がないため、この設定のパケットは失敗する可能性があります。

トピック	注意またはガイドライン
背面に戻る設定で EIGRP や OSPF	Cisco APIC では、中継が、L3Out に設定されているエクスポートルート制御ポリシーのルーティングをサポートします。ルート(プレフィックス)を通過するこれらのポリシー制御は、L3Out でルーティングプロトコルに再配送されます。これらの中継ルートは、EIGRP や OSPF に再配布されたが、これらはルーティングループを防ぐためにタグ付けされた 4294967295 です。Cisco ACI ファブリックは、OSPF または EIGRP L3Out で学習すると、このタグに一致するルートを受け入れません。ただし、次の場合、この動作をオーバーライドする必要があります。 • EIGRP や OSPF を使用して、2 つの Cisco ACI ファブリックを接続します。 • EIGRP や OSPF を使用して、同じ Cisco ACI ファブリックで 2 つの異なる Vrf を接続します。 オーバーライドする必要がある場合には、APIC GUI の次の場所にある別のタグ ポリシーを使用して VRF を構成する必要があります：**[テナント（Tenant）]** > ***[Tenant_name]*** > **[ネットワーキング（Networking）]** > **[プロトコル ポリシー（Protocol Policies）]** > **[ルート タグ（Route Tag）]**。異なるタグを適用します。 新しいルートタグポリシーを作成するだけでなく、APIC GUI の次の場所でこのポリシーを使用する VRF を更新します。**[テナント（Tenant）]** > ***[Tenant_name]*** > **[ネットワーキング（Networking）]** > **[VRFs]** > ***[Tenant_VRF]*** VRF を作成したルート タグ ポリシーを適用します。 （注） 複数 L3Outs または同じ L3Out で複数のインターフェイスは同じリーフ スイッチに導入し、中継ルーティングに使用、(、IGP に再配布されません) IGP 内で、ルートをアドバタイズします。この状況では、ルート タグ ポリシーは適用されません。

トピック	注意またはガイドライン
BD サブネットをファブリック外にアドバタイズする	インポートおよびエクスポートのルート制御ポリシーは、中継ルート（他の外部ピアから学習したルート）およびスタティック ルートのみに適用されます。テナント BD サブネット上に設定されているファブリック内部のサブネットは、エクスポート ポリシー サブネットを使用して外部にアドバタイズされません。IP プレフィックス リストおよびルート マップを使用すると IP テナント サブネットは許可されますが、これらは別の設定手順を使用して実装されます。テナント サブネットをファブリックの外部にアドバタイズする場合は、次の設定手順を参照してください。 **1.** [subnet properties] ウィンドウで、テナント サブネットのスコープを [Public Subnet] として設定します。 **2.** オプション。[subnet properties] ウィンドウで、[Subnet Control] を [ND RA Prefix] として設定します。 **3.** テナント ブリッジ ドメイン（BD）を外部レイヤ 3 Outside に関連付けます (L3Out)。 **4.** テナント EPG と外部 EPG 間にコントラクト（プロバイダ/コンシューマ）の関連付けを作成します。 BD サブネットを Public 範囲に設定し、BD をレイヤ 3 Out に関連付けると、BD サブネット プレフィックスの境界リーフに IP プレフィックスおよびルート マップの連続エントリが作成されます。

トピック	注意またはガイドライン
デフォルト ルートのアドバタイズ	デフォルトルートのみを必要とするファブリックへの外部接続の場合、OSPF、EIGRP、および BGP の L3Out 接続をデフォルトルートの起点とすることがサポートされます。外部ピアからデフォルトルートが受信されると、この文書で説明されている中継エクスポートルート制御に従って、このルートを別のピアに再配布できます。 デフォルト ルートは、デフォルト ルート リーク ポリシーを使用してアドバタイズすることもできます。このポリシーは、デフォルト ルートがルーティング テーブル内にあるか、または常にデフォルトルートをアドバタイズすることがサポートされている場合、デフォルトルートのアドバタイズをサポートします。デフォルトルート リーク ポリシーは、L3Out 接続で設定されます。 デフォルト ルート リーク ポリシーを作成するときは、以下のガイドラインに従ってください: • BGP の場合、**Always** プロパティは適用されません。 • BGP の場合、**Scope** プロパティを設定するときには、**Outside** を選択します。 • OSPF の場合、範囲の値が **Context** だとタイプ 5 LSA が作成されるのに対し、**Outside** だとタイプ 7 LSA が作成されます。選択したは、L3Out で設定されたエリアのタイプによって異なります。エリア タイプが場合 **定期的な** 、範囲を設定します **コンテキスト** 。エリア タイプが場合 **NSSA** 、範囲を設定します **外部** 。 • EIGRP で、**Scope** プロパティを選択する場合には、**Context** を選択する必要があります。

トピック	注意またはガイドライン
MTU	Cisco ACI は、IP フラグメンテーションをサポートしていません。したがって、外部ルータへのレイヤ 3 Outside（L3Out）接続、または Inter-Pod Network（IPN）を介した multipod 接続を設定する場合は、MTU が両側で適切に設定されていることが重要です。ACI、Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定された MTU 値は IP ヘッダーを考慮に入れています（結果として、最大パケット サイズは、ACI で 9216 バイト、NX-OS および IOS で 9000 バイトに設定されます）。ただし、IOS XR などの他のプラットフォームは、パケット ヘッダーのを除く MTU 値を設定します（結果として最大パケット サイズは 8986 バイトになります）。 各プラットフォームの適切な MTU 値については、それぞれの設定ガイドを参照してください。 CLI ベースのコマンドを使用して MTU をテストすることを強く推奨します。たとえば、Cisco NX-OS CLI で `ping 1.1.1.1 df-bit packet-size 9000 source-interface ethernet 1/1` などのコマンドを使用します。

トランジット ルート制御

ルート トランジットは、インポートされるレイヤ 3 アウトサイド ネットワーク `L3extOut` プロファイル（`l3extInstP`）を通してトラフィックをインポートするために定義されます。異なるルート トランジットは、エクスポートされる別の `l3extInstP` を通してトラフィックをエクスポートするために定義されます。

ファブリック内の 1 つまたは複数のノードに複数の `l3extOut` ポリシーを配置できるので、プロトコルのさまざまな組み合わせがサポートされます。プロトコルの組み合わせはすべて、複数の `l3extOut` ポリシーを使用して 1 つのノードに配置することも、または複数の `l3extOut` ポリシーを使用して複数のノードに配置することも可能です。同じファブリック内の異なる `l3extOut` ポリシーに 3 つ以上のプロトコルを配置することもできます。

エクスポート ルートマップは、プレフィックス リストの一致から構成されます。各プレフィックス リストは、VRF 内のブリッジ ドメイン（BD）パブリック サブネット プレフィクスと、外部にアドバタイズする必要のあるエクスポート プレフィクストから構成されます。

ルート制御ポリシーは、`l3extOut` ポリシーで定義され、`l3extOut` に関連付けられたプロパティおよび関係によって制御されます。APIC は `l3extOut` の `enforceRtctrl` プロパティを使用して、ルート制御方向を適用します。デフォルトでは、エクスポートの制御を適用し、インポートのすべてを許可します。インポートおよびエクスポートされたルート（`l3extSubnets`）は、`l3extInstP` で定義されます。すべてのルートのデフォルト スコープはインポートです。これらは、プレフィックス ベースの EPG を形成するルートおよびプレフィックスです。

インポート ルート マップからのすべてのインポート ルートは、BGP および OSPF によってインポートを制御するために使用されます。エクスポート ルート マップからのすべてのエクスポート ルートは OSPF および BGP によってエクスポートを制御するために使用されます。

インポートとエクスポートのルート制御ポリシーは、異なるレベルで定義されます。IPv6 ではすべての IPv4 ポリシー レベルがサポートされます。`l3extInstP` および `l3extSubnet` MO で定義されている追加の関係でインポートを制御します。

デフォルト ルート リークは、`l3extOut` の下の `l3extDefaultRouteLeakP` MO の定義によって有効になります。

OSPF のエリアごと、BGP のピアごとに `l3extDefaultRouteLeakP` は Virtual Routing and Forwarding（VRF）範囲または `L3extOut` 範囲を有することができます。

次の設定ルールは、ルート制御を提供します。

- `rtctrlSetPref`
- `rtctrlSetRtMetric`
- `rtctrlSetRtMetricType`

`rtctrlSetComm` MO の追加構文には以下が含まれています。

- `no-advertise`
- `no-export`
- `no-peer`

BGP

ACI ファブリックは、外部ルータとの BGP ピアリングをサポートします。BGP ピアは `l3extOut` ポリシーに関連付けられており、`l3extOut` ごとに複数の BGP ピアを設定することができます。BGP は、`l3extOut` の下で `bgpExtP` MO を定義することにより `l3extOut` レベルで有効化できます。

（注） `l3extOut` ポリシーにルーティング プロトコル（たとえば、関連する VRF を含む BGP）が含まれる一方で、L3Out インターフェイスのプロファイルには必要な BGP インターフェイス設定の詳細が含まれます。いずれも BGP の有効化に必要です。

BGP ピアには、OSPF、EIGRP、接続されたインターフェイス、スタティック ルート、またはループバック経由で到達できます。外部ルータとのピアリングには iBGP または eBGP を使用できます。ファブリック内への外部ルートの配付には MP-BGP が使用されるため、外部ルータからの BGP ルート属性は保持されます。BGP は `l3extOut` に関連付けられた VRF に Ipv4 や IPv6 アドレス ファミリを有効にすることができます。スイッチ上で有効になるアドレス ファミリは、`bgpPeerP` ポリシーで `l3extOut` のために定義した IP アドレス タイプによって決まります。ポリシーは省略可能です。定義しない場合はデフォルトが使用されます。ポリシーはテナントに対して定義され、名前で参照される VRF によって使用できます。

ピア ポリシーを少なくとも 1 つのピアを定義して、境界リーフ（BL）の各スイッチでプロトコルを有効にする必要があります。ピア ポリシーは 2 つの場所で定義できます。

- `l3extRsPathL3OutAtt` の下：送信元インターフェイスとして物理インターフェイスが使用されます。
- `l3extLNodeP` の下：送信元インターフェイスとしてループバック インターフェイスが使用されます。

OSPF

接続を有効にして冗長性を提供するために、さまざまなホスト タイプが OSPF を必要とします。これらには、たとえばファブリック内および WAN へのレイヤ 3 中継として ACI ファブリックを使用するサービス ノード、外部ポッド、メインフレーム デバイスなどがあります。このような外部デバイスは、OSPF を実行している非境界リーフ スイッチを介してファブリックとピアリングします。デフォルト ルートは受信し、全域ルーティングには参加しないよう、OSPF エリアを NSSA（スタブ）エリアとして設定します。通常は、既存のルーティングの導入によって設定の変更が回避されるため、スタブ エリアの設定は必須ではありません。

`l3extOut` で `ospfExtP` 管理対象オブジェクトを設定して、OSPF を有効にします。BL スイッチ上で設定されている OSPF IP アドレス ファミリ バージョンは、OSPF インターフェイス IP アドレスに設定されているアドレス ファミリによって決まります。

（注） `l3extOut` ポリシーにルーティング プロトコル（たとえば、関連する VRF とエリア ID を含む OSPF）が含まれる一方で、レイヤ 3 外部インターフェイスのプロファイルには必要な OSPF インターフェイスの詳細が含まれます。いずれも OSPF のイネーブル化に必要です。

アドレス ファミリごとに設定可能な `fvRsCtxToOspfCtxPol` 関係を使用して、VRF レベルで OSPF ポリシーを設定します。設定していない場合、デフォルト パラメータが使用されます。

要求されるエリア プロパティ Ipv6 を公開する `ospfExtP` 管理対象オブジェクトで OSPF を設定します。

サブネットの範囲と集約コントロール

次のセクションでは、サブネットを作成するときに利用できるいくつかの範囲と集約に関するオプションについて説明します:

Export Route Control Subnet: コントロールは、ファブリック外の特定の中継ルートをアドバタイズします。これは中継ルートにのみ影響するもので、内部ルートやブリッジ ドメインで設定されるデフォルトのゲートウェイには影響しません。

インポート ルート コントロール サブネット：このコントロールは、インポート ルート制御の強制が設定されている場合、ルートを Border Gateway Protocol（BGP）と Open Shortest Path First（OSPF） でファブリックにアドバタイズすることを可能にします。

External Subnets for the External EPG (セキュリティ インポート サブネットとも呼ばれる): このオプションは、ルーティング情報のファブリックへの出入りはコントロールしません。トラ

フィックがある外部 EPG から別の外部 EPG に、または内部 EPG に流れるようにするには、サブネットにはこのコントロールでマークを付ける必要があります。このコントロールを使用してサブネットにマークしなかった場合には、ある EPG から学習したルートが他の外部 EPG にもアドバタイズされますが、パケットはファブリックでドロップされます。パケットがドロップされるのは、APIC が許可済みリスト モデルで動作するからです。そのデフォルトの動作は、契約で明示的に許可されていない限り、EPG 間の全データ プレーン トラフィックをドロップするというものです。この許可済みリスト モデルは外部 EPG とアプリケーション EPG に適用されます。このオプションが設定されているセキュリティ ポリシーを使用する場合には、契約とセキュリティ プレフィックスを設定する必要があります。

Shared Route Control Subnet: VRF 間のリーキングの共有 L3Outs から学習されたサブネットは、他の VRF にアドバタイズされる前に、このコントロールでマークされる必要があります。APIC リリース 2.2(2e) 以降では、異なる VRF の共有 L3Outs は契約を使用して相互に通信できます。異なる VRF の共有 L3Outs 間の通信の詳細については、『*Cisco APIC* レイヤ *3* ネットワー キング構成定ガイド』を参照してください。

Shared Security Import Subnet: このコントロールは、共有 L3Out 学習ルートについては、[External Subnets for the External EPG] と同じです。トラフィックがある外部 EPG から別の外部 EPG に、または別の内部 EPG に流れるようにするには、サブネットにはこのコントロールでマークを付ける必要があります。このコントロールを使用してサブネットにマークしなかった場合には、ある EPG から学習したルートが他の外部 EPG にもアドバタイズされますが、パケットはファブリックでドロップされます。このオプションが設定されているセキュリティ ポリシーを使用する場合には、契約とセキュリティ プレフィックスを設定する必要があります。

Aggregate Export, Aggregate Import, and Aggregate Shared Routes: このオプションは、0.0.0.0/0 プレフィックスの前に 32 を追加します。現在、インポート/エクスポート ルート制御サブネットに集約できるのは、0.0.0.0/0 プレフィクスのみです。0.0.0.0/0 プレフィックスを集約すると、制御プロファイルを 0.0.0.0/0 ネットワークに適用することはできなくなります。

Aggregate Shared Route: このオプションは、共有ルート制御サブネットとしてマークされている任意のプレフィックスに使用できます。

Route Control Profile: ACI ファブリックは、ファブリックの内部と外部にアドバタイズされるルート用に、ルート マップの set 句もサポートします。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 プロファイルで設定されます。

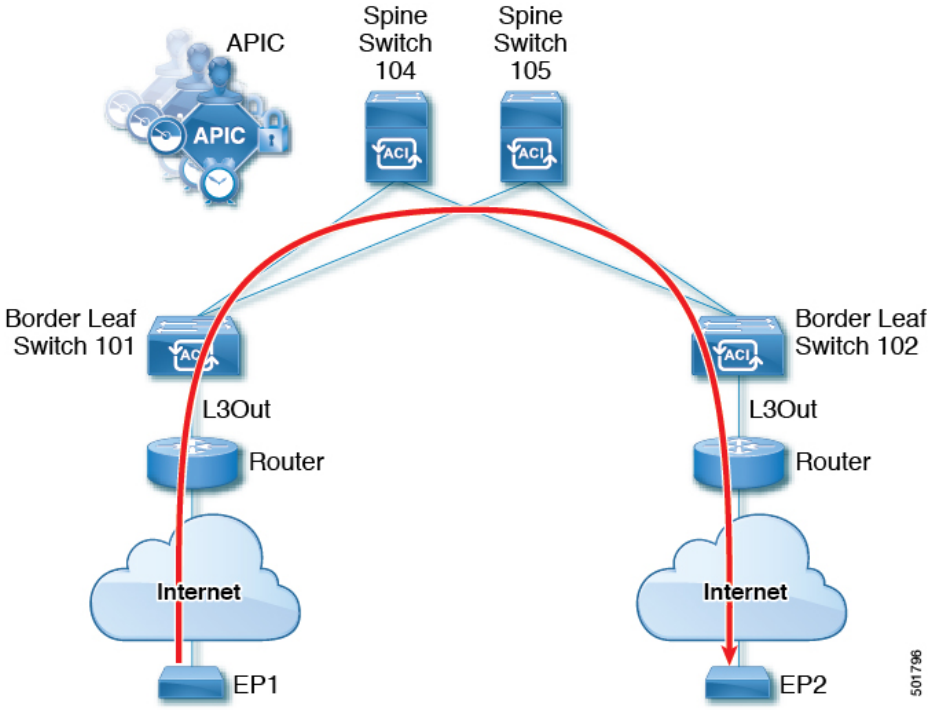
トランジット ルーティングの設定

トランジット ルーティングの概要

このトピックでは、CiscoAPIC を使用する際のトランジット ルーティングを設定する方法の一般的な例を説明します。

この章にある例では、次のトポロジを使用します。

図 *51 :*



この章の例では、Cisco ACI ファブリックには APIC クラスタによって制御される 2 個のリーフ スイッチと 2 個のスパイン スイッチがあります。境界リーフ スイッチ 101 と 102 には L3Out があり、2 t のルータに接続することでインターネットにも接続しています。この例の目標は、2 つの L3Out を通して、インターネット上の EP 1 から EP2 へ、ファブリック内外をトラフィックが行き来できるようにすることです。

この例では、両方の L3Out に関連付けられているテナントは、`t1` と、VRF がつく `v1` です。

L3Out を設定する前に、ノード、ポート、機能プロファイル、AEP、レイヤ 3 ドメインを設定します。BGP ルート リフレクタとして 104 と 105 スパイン スイッチを設定する必要があります。

トランジット ルーティングの設定には、次のコンポーネントの定義が含まれます。

1. テナントおよび VRF
2. リーフ 101 と 102 上のノードおよびインターフェイス
3. 各 L3Out のプライマリ ルーティング プロトコル（境界リーフ スイッチと外部ルータ間のルートの交換に使用。この例では BGP）
4. 各 L3Out のルーティング プロトコルの接続性（プライマリ プロトコルへの到達可能性情報の提供。この例では、OSPF）
5. 2 個の外部 EPG
6. 1 個のルート マップ

7. 少なくとも 1 つのフィルタと 1 つのコントラクト
8. 外部 EPG とコントラクトを関連付ける

（注） トランジット ルーティングの注意事項については、中継ルーティングのガイドライン （418 ページ） を参照してください。

次の表では、この章で使用される名前を一覧にしています。

プロパティ	ノード 101 の L3Out1 の名前	ノード 102 の L3Out2 の名前
テナント	t1	t1
VRF	v1	v1
ノード	ルータ ID 11.11.11.103 を持つ nodep1	ルータ ID 22.22.22.203 を持つ nodep2
OSPF インターフェイス	Eth/1/3 の ifp1	Eth/1/3 の ifp2
BPG ピア アドレス	15.15.15.2/24	25.25.25.2/24
外部 EPG	192.168.1.0/24 の extnw1	192.168.2.0/24 の extnw2
ルート マップ	Ctx1 を持つ rp1 とルートの宛先 192.168.1.0/24	ctx2 を持つ rp2 とルートの宛先 192.168.2.0/24
フィルタ	http-filter	http-filter
コントラクト	extnw1 によって提供される httpCtrct	extnw2 によって消費される httpCtrct

GUI を使用した中継ルーティングの設定

これらの手順は、テナントの中継ルーティングを設定する方法を示しています。この例では、2 つの L3Outs を、1 つの VRF 内、2 つの境界リーフ スイッチ上に展開します。スイッチは別々のルータに接続されています。

テナントと VRF を作成する手順を除き、これらの手順を 2 回繰り返して、同じテナントと VRF の下に 2 つの L3Out を作成します。

サンプルの名前については、中継 ACI ファブリックのルーティング （409 ページ）を参照してください。。

始める前に

- L3Out で使用されるインターフェイス（AAEP、VLAN プール、インターフェイス セレクタ）の L3 ドメインおよびファブリック アクセス ポリシーを設定します。

- ファブリック インフラ MPBGP の BGP ルート リフレクタ ポリシーを設定します。

手順

ステップ 1 テナントと VRF を作成するには、メニュー バーで、**Tenants** > **Add Tenant** を選択し、**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、テナント名を入力します。
b) In the **VRF Name** フィールドに、VRF 名を入力します。
c) **Submit** をクリックします。

（注） この手順の後の手順は 2 回実行して、中継ルーティングのための同じテナントと VRF に 2 つの L3Out を作成します。

ステップ 2 L3Out の作成を開始するには、[ナビゲーション（Navigation）] ペインで [テナント（Tenant）] [ネットワーキング（Networking）] を展開し、[L3Outs] を右クリックして [L3Out の作成（Create L3Out）] を選択します。

[**L3Out の作成（Create L3Out**）] ウィザードが表示されます。次の手順では、[**L3Out の作成（Create L3Out**）] ウィザードを使用した L3Out 設定例の手順を示します。

ステップ 3 [L3Out の作成（Create L3Out）] ウィザードの [識別（Identity）] ウィンドウに必要な情報を入力します。

a) **Name** フィールドに L3Out の名前を入力します。
b) **VRF** ドロップダウンリストから VRF を選択します。
c) [**L3 ドメイン（L3 Domain**）] ドロップダウン リストで、先ほど作成した、外部ルーテッド ドメインを選択します。
d) ルーテッドプロトコルのチェックボックスがある領域で、目的のプロトコル(BGP、OSPF、または EIGRP) をオンにします。

この章の例では、**BGP** および **OSPF** を選択します。

選択するプロトコルに応じて、設定する必要のあるプロパティに入力します。

e) OSPF を有効にした場合は、OSPF の詳細を入力します。

この章の例では、OSPF エリア **0** を使用し、**Regular area** に入力します。

f) [**次（Next**）] をクリックして [**ノードとインターフェイス（Nodes and Interfaces**）] ウィンドウに移動します。

ステップ 4 [L3Out の作成（Create L3Out）] ウィザードの [ノードとインターフェイス（Nodes and Interfaces）] ウィンドウに必要な情報を入力します。

a) 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。

[**デフォルトの使用（Use Defaults**）] フィールドで、デフォルトのノード プロファイル名およびインターフェイス プロファイル名を使用する場合は、チェックをオンにします。

- デフォルトのノードプロファイル名は *L3Out-name* _nodeProfile です。ここで、*L3Out-name* は [識別（Identity）] ページの [名前（Name）] フィールドに入力した名前です。
- 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。ここで、*L3Out-name* は、[識別（Identity）] ページの [名前（Name）] フィールドに入力した名前です。

b) [インターフェイス タイプ（Interface Types）] 領域で、[レイヤ 3（Layer 3）] および [レイヤ 2（Layer 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：
  - **ルーテッド**：ポート チャネルへのレイヤ 3 ルートを設定するには、このオプションを選択します。

    このオプションを選択すると、レイヤ 3 ルートは、このページの [**レイヤ 2（Layer 2）**] フィールドで選択された物理ポートまたはダイレクト ポート チャネルのいずれかになります。
  - **ルーテッド サブ**：ポート チャネルへのレイヤ 3 サブインターフェイス ルートを設定するには、このオプションを選択します。

    このオプションを選択すると、レイヤ 3 サブインターフェイスのルートは、このページの [**レイヤ 2（Layer 2）**] フィールドで選択された物理ポートまたはダイレクト ポート チャネルのいずれかになります。
  - **SVI**：ACI リーフ スイッチとルータ間に接続性を提供する Switch Virtual Interface（SVI）を設定するにはこのオプションを選択します。

    SVI は、物理ポート、直接ポート チャネル、仮想ポート チャネルのメンバーを持つことができ、このページの [**レイヤ 2（Layer 2）**] フィールドで選択します。
  - **フローティング SVI**：フローティング L3Out を設定するにはこのオプションを選択します。

    フローティング L3Out を使用すると、仮想ルータが 1 つのリーフ スイッチの下から別のリーフ スイッチに移動できるようにする L3Out を設定できます。この機能により、VM がホスト間を移動する際に、ルーティングを維持するために複数の L3Out インターフェイスを設定する必要がなくなります。
- レイヤ 2 ：（レイヤ 3 エリアで仮想 SVI を選択した場合は使用できません）
  - ポート
  - 仮想ポート チャネル（レイヤ 3 領域で [**SVI**] を選択した場合に使用可能）
  - ダイレクトポートチャネル(Direct Port Channel)

c) [**ノード ID**（**Node ID**）] フィールドのドロップダウン メニューで、L3Out のノードを選択します。

これらの例のトポロジでは、ノード 103 を使用します。

d) **Router ID** フィールドで、ルータ ID (L3Out に接続されているルータの IPv4 または IPv6 アドレス) を入力します。

e) （任意） 必要に応じて、ループバック アドレスに別の IP アドレスを設定できます。

[ルータ ID（Router ID）] フィールドに入力したエントリと同じ内容が [ループバック アドレス（Loopback Address）] フィールドに自動で入力されます。これは以前のビルドでの [ループバック アドレスのルータ ID の使用（Use Router ID for Loopback Address）] と同等です。ループバック アドレスにルータ ID を使用しない場合は、ループバック アドレスに別の IP アドレスを入力します。または、ループバック アドレスにルータ ID を使用しない場合は、このフィールドを空のままにします。

f) [ノードとインターフェイス（Nodes and Interfaces）] ウィンドウに追加の必要な情報を入力します。

このウィンドウに表示されるフィールドは、[レイヤ 3（Layer 3）] および [レイヤ 2（Layer 2）] 領域で選択したオプションによって異なります。

g) [ノードとインターフェイス（Nodes and Interfaces）] ウィンドウで残りの追加の情報を入力したら、[次（Next）] をクリックします。

[**プロトコル**（**Protocols**）] ウィンドウが表示されます。

ステップ 5 [L3Out の作成（Create L3Out）] ウィザードの [プロトコル（Protocols）] ウィンドウに必要な情報を入力します。

この例ではプロトコルとしてBGPとOSPFを使用しているため、次の手順でこれらのフィールドに情報を提供します。

a) [BGP ループバック ポリシー（BGP Loopback Policies）] および [BGP インターフェイス ポリシー（BGP Interface Policies）] 領域で、次の情報を入力します。

- **ピア アドレス**（**Peer Address**）：ピア IP アドレスを入力します
- **EBGP Multihop TTL**（**EBGP マルチホップ TTL**）：接続の存続可能時間（TTL）を入力します。範囲は 1 ー 255 ホップです。ゼロの場合、TTL は指定されません。デフォルトは 0 です。
- **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。

（注） ACI は asdot または asdot + 形式の AS 番号をサポートしていません。

b) [**OSPF**] 領域で、デフォルト OSPF ポリシー、以前に作成した OSPF ポリシー、または [**OSPF インターフェイス ポリシーの作成**（**Create OSPF Interface Policy**）] を選択します。

c) **[次へ（Next）]** をクリックします。

[**外部 EPG（External EPG**）] ウィンドウが表示されます。

ステップ 6 [L3Out の作成（Create L3Out）] ウィザードで [外部 EPG（External EPG）] ウィンドウに必要な情報を入力します。

a) **Name** フィールドに、外部ネットワークの名前を入力します。

b) [**提供済みコントラクト（Provided Contract**）] フィールドで、提供済みコントラクトの名前を入力します。

c) [**消費済みコントラクト（Consumed Contract**）] フィールドで、消費済みコントラクトの名前を入力します。

d) [すべての外部ネットワークのデフォルト EPG（Default EPG for all external network）] フィールドで、この L3Out 接続からのすべての中継ルートをアドバタイズしない場合はオフにします。

このボックスをオフにすると、[Subnets] 領域が表示されます。次の手順に従って、必要なサブネットとコントロールを指定します。

e) [+] アイコンをクリックして [サブネット（Subnet）] を展開し、[サブネットの作成（Create Subnet）] ダイアログ ボックスで次の操作を実行します。

f) **IP address** フィールドに、外部ネットワークの IP アドレスとサブネット マスクを入力します。

g) [**名前（Name**）] フィールドに、サブネットの名前を入力します。

h) **Scope** フィールドで、L3Out のプレフィックスのインポートとエクスポートを制御するための適切なチェック ボックスをオンにします。

（注） 範囲のオプションの詳細については、この **Create Subnet** パネルのオンライン ヘルプを参照してください。

i) （任意）[**ルート制御サブネットのエクスポート（Export Route Control Subnet**）] のチェック ボックスをオンにします。

[BGP ルート集約ポリシー（BGP Route Summarization Policy）] フィールドが使用可能になります。

j) [**BGP ルート集約ポリシー（BGP Route Summarization Policy**）] フィールドでは、ドロップダウン リストから既存のルート集約ポリシーを選択するか、必要に応じて新しいユーザーを作成します。

ルート集約ポリシーのタイプは、L3Out に対して有効になっているルーティング プロトコルに依存します。

k) [サブネットの作成（Create Subnet）] ウィンドウで必要な設定が完了したら、[OK] をクリックします。

l) （任意）より多くのサブネットを追加するにはこれを繰り返します。

m) [完了（Finish）] をクリックして、[L3Out の作成（Create L3Out）] ウィザードに必要な設定の入力を完了させます。

ステップ 7 作成した L3Out に移動し、[L3Out] を右クリックして、[ルート制御のインポートおよびエクスポートのルート マップの作成（Create Route map for import and export route control）] を選択します。

ステップ 8 [ルート制御のインポートおよびエクスポートのルート マップの作成（Create Route map for import and export route control）] ウィンドウで、次の操作を実行します。

a) **Name** フィールドに、ルート マップ名を入力します。

b) **Type** を選択します。

この例では、デフォルトの **Match Prefix AND Routing Policy** のままにします。

c) **+** アイコンをクリックして **Contexts** を展開し、ルート マップのルート コンテキストを作成します。

d) プロファイル コンテキストの順序と名前を入力します。

e) このコンテキストで実行するアクションとして **Deny** または **Permit** を選択します。

f) （任意） **Set Rule** フィールドで、**Create Set Rules for a Route Map** を選択します。

セット ルールのための名前を入力し、ルールで使用するオブジェクトをクリックし、**Finish** をクリックします。

g) [**一致ルール（Match Rule**）] フィールドで、[**ルート マップの一致ルールの作成（Create Match Rules for a Route Map**）] を選択します。

h) 一致ルールの名前を入力し、ルールで一致させる対象として **正規表現コミュニティ用語の一致（Match Regex Community Terms**）、**コミュニティ用語の一致（Match Community Terms**）、または **一致プレフィックス（Match Prefix**） を入力します。

i) [一致ルールの作成（Create Match Rule）] ウィンドウのフィールドへの入力が完了したら、[送信（Submit）] をクリックします。

j) **Create Route Control Context** ダイアログボックスで、**OK** をクリックします。

k) [**インポートおよびエクスポート ルート制御向けのルート マップの作成（Create Route map for import and export route control**）] ダイアログ ボックスで、[**送信（Submit**）] をクリックします。

ステップ 9 [ナビゲーション（Navigation）] ペインで **[L3Outs]** > **[*L3Out_name*]** > **[外部 EPG（External EPGs）]** > **[*externalEPG_name*]** の順に展開して、次のアクションを実行します。

a) **+** アイコンをクリックして **Route Control Profile** を展開します。

b) **Name** フィールドのドロップダウン リストから、前に作成したルート制御プロファイルを選択します。

c) **Direction** フィールドで、**Route Export Policy** を選択します。

d) **Update** をクリックします。

ステップ 10 作成した L3Out に移動し、[L3Out] を右クリックして、[ルート制御のインポートおよびエクスポートのルート マップの作成（Create Route map for import and export route control）] を選択します。

ステップ 11 [ルート制御のインポートおよびエクスポートのルート マップの作成（Create Route map for import and export route control）] ウィンドウで、次の操作を実行します。

（注） 受信ルートについて BGP、OSPF、または EIGRP の属性を設定するには、default-import ルート制御プロファイルを作成し、適切な set アクションと、 no match のアクションを作成します。

a) [**名前（Name**）] フィールドから、[**default-import**] を選択します。
b) [**タイプ（Type**）] フィールドでは、[**ルーティング ポリシーのみ一致（Match Routing Policy Only**）] をクリックする必要があります。
c) [**インポートおよびエクスポート ルート制御向けのルート マップの作成（Create Route map for import and export route control**）] ダイアログ ボックスで、[**送信（Submit**）] をクリックします。

ステップ 12 L3Out を使用していた EPG 間の通信を有効にするには、次の手順を使用して、少なくとも 1 つのフィルタと契約を作成します:

a) ナビゲーション ウィンドウの L3Out を使用するテナントの下で、**Contracts** を展開します。
b) **Filters** を右クリックして **Create Filter** を選択します。
c) **Name** フィールドに、フィルタのの名前を入力します。

フィルタは基本的にはアクセス コントロール リスト (ACL) です。

d) + アイコンをクリックして **Entries** を展開し、フィルタ エントリを追加します。
e) エントリ の詳細を追加します。。

たとえば、単純な Web フィルタの場合には、次のような条件を設定します:

- **EtherType—IP**
- **IP Protocol—tcp**
- **Destination Port Range From—Unspecified**
- **Destination Port Range To** to **https**

f) **Update** をクリックします。
g) **Create Filter** ダイアログボックスで、**Submit** をクリックします。

ステップ 13 契約を追加するには、次の手順を実行します:

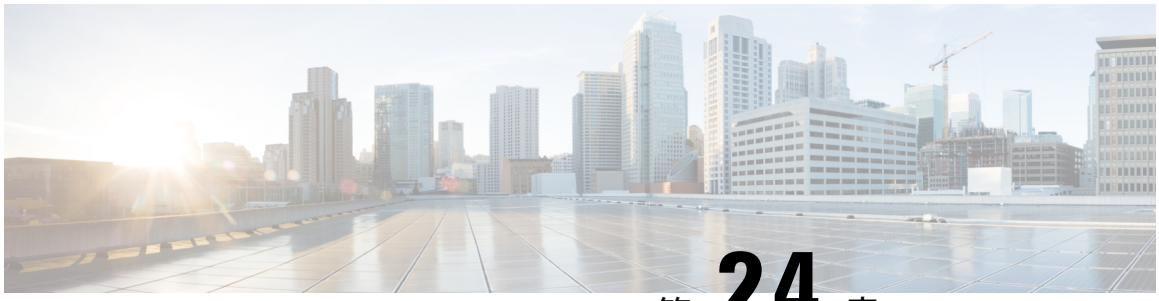
a) **Contracts** の下で、**Standard** を右クリックして、**Create Contract** を選択します。
b) 契約の名前を入力します。
c) + アイコンをクリックして **Subjects** を展開し、情報カテゴリを契約に追加します。
d) 情報カテゴリの名前を入力します。
e) [+]アイコンをクリックして [**フィルタ（Filters**）] を展開し、ドロップダウン リストから、前に作成したフィルタを選択します。
f) **Update** をクリックします。
g) **Create Contract Subject** ダイアログボックスで、**OK** をクリックします。
h) **Create Contract** ダイアログボックスで、**Submit**をクリックします。

ステップ 14 次の手順で、L3Out の EPGを契約に関連付けます:

最初の L3 外部 EPG（extnw1 が契約のプロバイダとなり、2 番目の外部 EPG、extnw2）がコンシューマとなります。

a) 契約をプロバイダとしての L3 外部 EPG に関連付けるには、テナントの下で [**ネットワーキング**（**Networking**）] をクリックし、[**L3Outs**] をクリックし、L3Out を展開します。
b) [**外部 EPG**（**External EPGs**）] を展開し、L3 外部 EPG をクリックし、[**コントラクト**（**Contracts**）] タブをクリックします。
c) + アイコンをクリックして **Provided Contracts** を展開します。

   2 番目の L3 外部 EPG で、+ アイコンをクリックして Consumed Contracts を展開します。
d) **Name** フィールドで、前に作成した契約をリストから選択します。
e) **Update** をクリックします。
f) [Submit] をクリックします。



第 24 章

共有サービス

この章は、次の内容で構成されています。

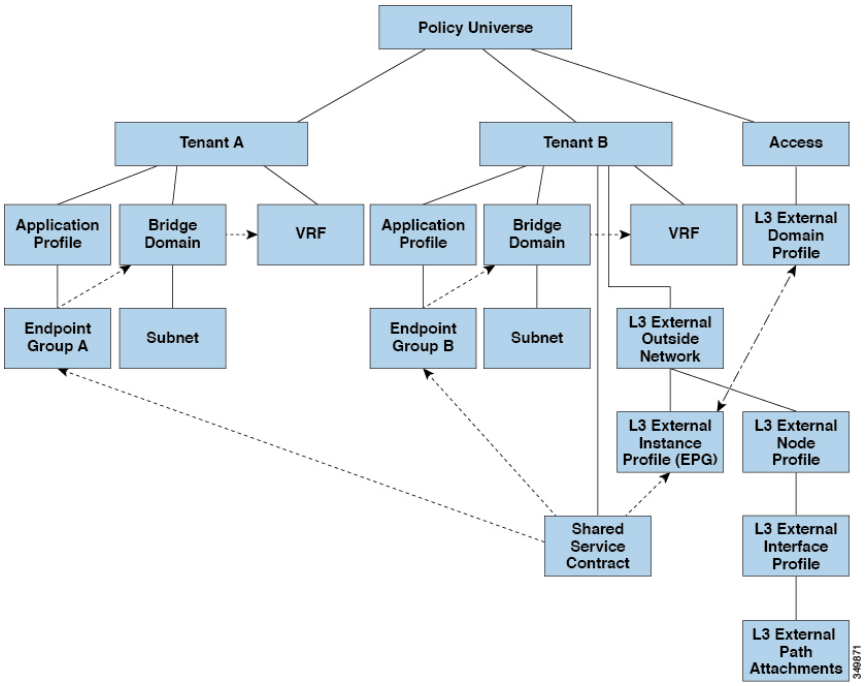
共有レイヤ 3 Out

共有レイヤ 3 アウトサイド（L3Out または `l3extOut`）構成は、外部ネットワークへのルーテッド接続を、VRF インスタンス間またはテナント間の共有サービスとして提供します。L3Out の外部 EPG インスタンス プロファイル（外部 EPG または `l3extInstP`）は、ルーティングの観点とコントラクトの観点の両方から共有できるルートを制御するための構成を提供します。外部 EPG 下のコントラクトは、これらのルートをリークする必要がある VRF インスタンスまたはテナントを決定します。

L3Out は、任意のテナント（*user*、`common`、`infra`、`mgmt`.）の共有サービスとしてプロビジョニングできます。任意のテナントの EPG は、外部 EPG がファブリック内のどこにプロビジョニングされているかには関係なく、共有サービス コントラクトを使用して、外部 EPG に接続できます。これにより、外部ネットワークへのルーテッド接続のプロビジョニングが簡単になります。複数のテナントが、外部ネットワークへのルーテッド接続用に単一の外部 EPG を共有できます。外部 EPG を共有すると、単一の共有外部 EPG を使用する EPG の数には関係なくスイッチ上で使用されるセッションは 1 つのみであるため、より効率的になります。

次の図は、共有外部 EPG 用に構成された主なポリシー モデル オブジェクトを示しています。

図 *52 :* 共有 *L3Out* ポリシー モデル



共有 L3Out ネットワーク設定については、以下の注意事項と制限事項に注意してください。

- テナント制限なし：テナント A と B は、任意の種類のテナント（*user*、`common`、`infra`、`mgmt`）です。共有外部 EPG が `common` テナントにある必要はありません。
- EPG の柔軟な配置：上の図の EPG A と EPG B は異なるテナントにあります。EPG A と EPG B で同じブリッジ ドメインと VRF インスタンスを使用することはできますが、それは必須ではありません。EPG A と EPG B は異なるブリッジ ドメインおよび異なる VRF インスタンスにありますが、同じ外部 EPG を共有しています。
- サブネットは、*private*、*public*、または *shared* です。L3Out のコンシューマまたはプロバイダ EPG にアドバタイズされるサブネットは、*shared* に設定されている必要があります。L3Out にエクスポートされるサブネットは *public* に設定される必要があります。
- 共有サービス コントラクトは、共有 L3Out ネットワーク サービスを提供する外部 EPG が含まれているテナントからエクスポートされます。共有サービス コントラクトは、共有サービスを使用する EPG が含まれているテナントにインポートされます。
- 共有 L3Out では禁止コントラクトを使用しないでください。この構成はサポートされません。
- 外部 EPG は、共有サービス プロバイダーとしてサポートされますが、非外部 EPG コンシューマと組み合わせる場合に限られます（L3Out EPG が外部 EPG と同じ）。
- トラフィック中断（フラップ）：外部 EPG を、外部サブネット 0.0.0.0/0 を使用して構成し、外部 EPG サブセットのスコープ プロパティを共有ルート制御（*shared-rctrl*）または共有セキュリティ（*shared-security*）に設定すると、VRF インスタンスはグローバル `pcTag`

を使用して再配置されます。これにより、その VRF インスタンス内のすべての外部トラフィックが中断されます（VRF インスタンスがグローバル pcTag を使用して再配置されるため）。

- 共有レイヤ L3Out のプレフィックスは一意である必要があります。同じ VRF インスタンスの同じプレフィックスを使用した、複数の共有 L3Out 構成は動作しません。VRF インスタンスにアドバタイズする外部サブネット（外部プレフィックス）が一意であることを確認してください（同じ外部サブネットが複数の外部 EPG に属することはできません）。プレフィックス prefix1 を使用した L3Out 構成（たとえば、L3Out1）と、同じくプレフィックス prefix1 を使用した 2 番目のレイヤ 3 アウトサイド構成（たとえば、L3Out2）を同じ VRF に所属させると、動作しません（導入される pcTag は 1 つのみであるため）。
- L3Out の異なる動作が、同じ VRF インスタンスの同じリーフ スイッチ上に構成される場合があります。考えられるシナリオは次の 2 つです。
  - シナリオ 1 は、SVI インターフェイスおよび 2 つのサブネット（10.10.10.0/24 および 0.0.0.0/0）が定義された L3Out がある場合です。L3Out ネットワーク上の入力トラフィックが、マッチング プレフィックス 10.10.10.0/24 を持っていると、入力トラフィックは外部 EPG pcTag を使用します。L3Out ネットワーク上の入力トラフィックが、マッチング デフォルト プレフィックス 0.0.0.0/0 を持っていると、入力トラフィックは外部ブリッジ pcTag を使用します。
  - シナリオ 2 は、2 つのサブネット（10.10.10.0/24 および 0.0.0.0/0）が定義されたルーテッドまたはルーテッドサブインターフェイスを使用する L3Out がある場合です。L3Out ネットワーク上の入力トラフィックが、マッチング プレフィックス 10.10.10.0/24 を持っていると、入力トラフィックは外部 EPG pcTag を使用します。L3Out ネットワーク上の入力トラフィックが、マッチング デフォルト プレフィックス 0.0.0.0/0 を持っていると、入力トラフィックは VRF インスタンス pcTag を使用します。
  - ここまでで説明した動作の結果として、同じ VRF インスタンスおよび同じリーフ スイッチに、SVI インターフェイスを使用する L3Out-A および L3Out-B が構成されている場合、次のユース ケースが考えられます。

    ケース 1 は L3Out-A 用です。この外部ネットワーク EPG には、10.10.10.0/24 および 0.0.0.0/1 という 2 つのサブネットが定義されています。L3Out-A 上の入力トラフィックがマッチング プレフィックス 10.10.10.0/24 を持っている場合、外部 EPG pcTag と contract-A を使用します。このコントラクトは L3Out-Aに関連付けられるものです。L3Out-A の出力トラフィックで特定のマッチが見つからない場合でも、0.0.0.0/1 との最大プレフィックス マッチがあるので、外部ブリッジ ドメイン pcTag と contract-A を使用します。

    ケース 2 は L3Out-B 用です。この外部 EPG では、1 つのサブネット 0.0.0.0/0 が定義されています。L3Out-B 上の入力トラフィックが、マッチング プレフィックス10.10.10.0/24（L3Out-A の下で定義されたもの）を持っている場合、L3Out-A および contract-A の EPG pcTag を使用します。このコントラクトは L3Out-A と結びつけられています。L3Out-Bと関連付けられている contract-B は使用しません。

- 許可されないトラフィック：無効な設定で、共有ルート制御（shared-rtctrl）に対する外部サブネットのスコープが、共有セキュリティ（shared-security）に設定されているサブネッ

トのサブセットとして設定されている場合、トラフィックは許可されません。たとえば、以下の設定は許可されません。

- *shared rtctrl*：10.1.1.0/24, 10.1.2.0/24
- *shared security*：10.1.0.0/16

この場合、10.1.1.0/24 および 10.1.2.0/24 の各プレフィックスがドロップ ルールを使用してインストールされているため、宛先 IP 10.1.1.1 を使用して非境界リーフの入力トラフィックはドロップされます。トラフィックは許可されません。そのようなトラフィックは、`shared-rtctrl` プレフィックスを shared-security プレフィックスとしても使用するように設定を修正することで、有効にすることができます。

- 不注意によるトラフィック フロー：次の設定シナリオを避けることで、不注意によるトラフィック フローを予防します。
  - **ケース 1** 設定の詳細：
    - VRF1 を使用する L3Out ネットワーク構成（例えば `L3Out-1`）を、`provider1` と呼ぶことにします。
    - VRF2 を使用する 2 番目の L3Out ネットワーク構成（例えば `L3Out-2`）を `provider2` と呼ぶことにします。
    - `L3Out-1` の VRF1 は、デフォルト ルート、0.0.0.0/0 をインターネットにアドバタイズします。これは *shared-rtctrl* および *shared-security* の両方を有効にします。
    - `L3Out-2` の VRF2 は特定のサブネット、192.0.0.0/8 を DNS および NTP にアドバタイズし、*shared-rtctrl* を有効にします。
    - `L3Out-2` の VRF2 には特定のサブネット、192.1.0.0/16 があります。これは *shared-security* を有効にします。
    - **バリエーション A**：EPG トラフィックは複数の VRF インスタンスに向かいます。
      - EPG1 と `L3Out-1` の間の通信は *allow_all* コントラクトによって制御されます。
      - EPG1 と `L3Out-2` の間の通信は *allow_all* コントラクトによって制御されます。

        結果：EPG1 から `L3Out-2` へのトラフィックも 192.2.x.x に向かいます。
    - **バリエーション B**：EPG は 2 番目の共有L3Out ネットワーク の *allow_all* コントラクトに従います。
      - EPG1 と `L3Out-1` の間の通信は *allow_all* コントラクトによって制御されます。
      - EPG1 と `L3Out-2` の間の通信は *allow_icmp* コントラクトによって制御されます。

        結果：EPG1 から `L3Out-2`、そして 192.2.x.x へのトラフィックは *allow_all* コントラクトに従います。
  - **ケース 2** 設定の詳細：

- 外部 EPG は、1 つの共有プレフィックスと、その他の非共有プレフィックスを持っています。
- `src = non-shared` で到達するトラフィックは、EPG に向かうことが許可されます。
  - **バリエーション A**：意図しないトラフィックが EPG を通過します。

    外部 EPG トラフィックは、次のプレフィックスを持つ L3Out を通過します。

    Unordered List bullet 5 `192.0.0.0/8 = import-security, shared-rtctrl`

    Unordered List bullet 5 `192.1.0.0/16 = shared-security`

    Unordered List bullet 5 EPG には `1.1.0.0/16 = shared` があります。

    結果：192.2.x.x からのトラフィックも EPG に向かいます。
  - **バリエーション B**：意図しないトラフィックが EPG を通過します。共有 L3Out に到達したトラフィックは EPG を通過できます。

    Unordered List bullet 5 -共有 L3Out VRF には、`pcTag = prov vrf` を持つ EPG と *allow_all* に設定されているコントラクトがあります。

    Unordered List bullet 5 EPG は `<subnet> = shared` となっています。

    結果：レイヤ 3 Out に到達するトラフィックは EPG を通過することができます。

レイヤ 3 アウトからレイヤ 3 アウト内部 VRF への漏洩

Cisco APIC リリース 2.2(2e) から、2 つの異なる VRF に 2 個のレイヤ 3 アウトがある場合、VRF 内部の漏洩がサポートされています。

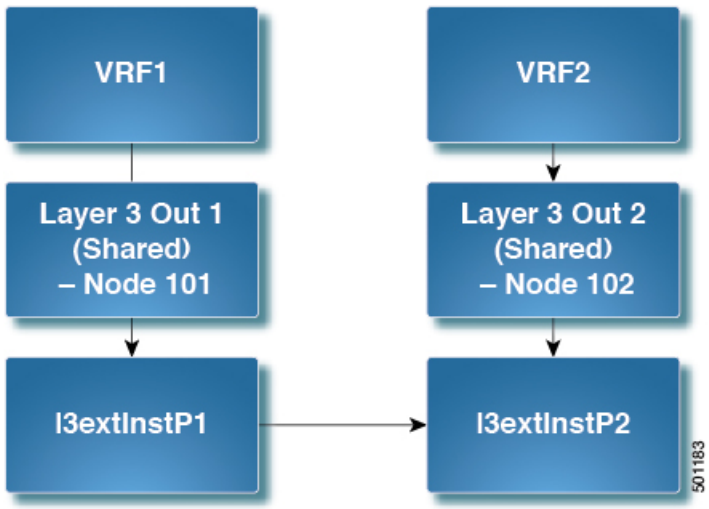
この機能を稼働するには、次の条件を満たす必要があります。

- 2 個のレイヤ 3 アウト間にはコントラクトが必要です。

- レイヤ 3 アウトの接続したり移行したりするサブネットのルートは、コントラクトを適用し（L3Out-L3Out および L3Out-EPG）、VRF 間の動的または静的ルートを漏洩させることなく漏洩します。
- 動的または静的ルートは、コントラクトを適用し（L3Out-L3Out および L3Out-EPG）、VRF 間で直接接続したり移行したりするルートをアドバタイズすることなく漏洩します。
- 異なる VRF の共有のレイヤ 3 アウトは相互に通信できます。
- ブリッジ ドメインに必要な関連付けられた L3Out はありません。VRF 間共有 L3Out を使用する場合は、テナント共通の L3Out にユーザ テナント ブリッジ ドメインを関連付ける必要はありません。テナント固有の L3Out がある場合、それぞれのテナントのブリッジ ドメインに関連付けられます。
- 2 個のレイヤ 3 アウトは異なる 2 個の VRF に存在し、正常にルートを交換できます。
- この強化は、アプリケーション EPG およびレイヤ 3 アウト内部 VRF 間の通信と同じです。唯一の違いは、アプリケーション EPG ではなく別のレイヤ 3 アウトが存在します。したがってこの状況では、コントラクトは 2 個のレイヤ 3 アウト間で記録されます。

次の図では、共有サブネットによる 2 個のレイヤ 3 アウトが存在します。両方の VRF でレイヤ 3 外部インスタンス プロファイル（l3extInstP）間のコントラクトがあります。この場合、VRF 1 の共有レイヤ 3 アウト は VRF 2 の共有レイヤ 3 と通信できます。

図 *53 : 2* 個の *VRF* 間で通信する共有レイヤ *3* アウト



拡張 GUI を使用した共有レイヤ 3 Out VRF 間リーキングの設定

始める前に

コンシューマとプロバイダーによって使用される契約ラベルがすでに作成されています。

手順

ステップ 1 メニュー バーで **Tenants** > **Add Tenant** を選択します。

ステップ 2 **Create Tenant** ダイアログボックスに、プロバイダーのテナント名を入力します。

ステップ 3 [**VRF 名（VRF Name**）] フィールドに、プロバイダの VRF 名を入力し、[**送信（Submit**）] をクリックしてテナントを作成します。

ステップ 4 [**ナビゲーション（Navigation**）] ペインの新しいテナント名の下で、[**L3Outs**] に移動します。

ステップ 5 [**L3Outs**] を右クリックし、[**L3Out の作成（Create L3Out**）] を選択します。

[**L3Out の作成（Create L3Out**）] ウィザードが表示されます。

ステップ 6 [**VRF の作成（Create VRF**）] ダイアログ ボックスで、次の操作を実行します。

a) **Name** フィールドに、L3Out の名前を入力します。
b) [**VRF**] フィールドで、前に作成した VRF を選択します。
c) [**L3 ドメイン（L3 Domain**）] フィールドで、L3 ドメインを選択します。
d) プロトコルに適切な選択を行い、[**次へ（Next**）] をクリックします。

ステップ 7 [**外部 EPG（External EPG**）] ウィンドウが表示されるまで、次のウィンドウで必要な選択を行います。

[識別（Identity）] ウィンドウで選択したプロトコルに応じて、[ノードとインターフェイス（Nodes and Interfaces）] ウィンドウと [プロトコル（Protocols）] ウィンドウが表示される場合があります。[L3Out の作成（Create L3Out）] ウィザードの最後のウィンドウは、[外部 EPG（External EPG）] ウィンドウです。

ステップ 8 [外部 EPG（External EPG）] ウィンドウで次のアクションを実行します。

a) **Name** フィールドに、外部ネットワーク名を入力します。
b) [すべての外部ネットワークのデフォルト EPG（Default EPG for all external network）] チェックボックスをオフにします。

[サブネット（Subnets）] フィールドが表示されます。

c) [サブネットの作成（Create Subnet）] ウィンドウにアクセスするには、[+] をクリックします。
d) [**サブネットの作成（Create Subnet**）] ダイアログ ボックスの [**IP アドレス（IP Address**）] フィールドに、マッチングを行う IP アドレスを入力します。**OK** をクリックします。
e) [L3Out の作成（Create L3Out）] ウィザードで [完了（Finish）] をクリックします。

ステップ 9 [ナビゲーション（Navigation）] ペインで、作成した [L3Out_name] [外部 EPG（External EPGs）] [ExternalEPG_name] に移動します。 > >

ステップ 10 **Work** ウィンドウの、外部ネットワークの **Properties** の下で、**Resolved VRF** フィールドに解決された VRF が表示されていることを確認します。

ステップ 11 外部サブネットの IP アドレスをダブルクリックして、[**サブネット（Subnet**）] ダイアログ ボックスを開きます。

ステップ 12 **Scope** フィールドで、必要なチェック ボックスをオンにして、**Submit** をクリックします。

このシナリオで、次のチェック ボックスをオンにします。

- [**外部 EPG の外部サブネット（External Subnets for the External EPG**）]
- **共有ルートコントロールサブネット**
- **共有セキュリティインポートサブネット**

ステップ 13 以前に作成した [**L3 Outside**] に移動します。

ステップ 14 [**プロバイダ ラベル（Provider Label**）] フィールドに、このタスクを開始するための前提条件として作成したプロバイダ名を入力します。**Submit** をクリックします。

ステップ 15 メニュー バーで、 **Tenants** > **Add Tenant** をクリックします。

ステップ 16 [**テナントの作成（Create Tenant**）] ダイアログ ボックスで、L3 コンシューマのためのテナント名を入力します。

ステップ 17 **VRF Name** フィールドに、コンシューマの VRF 名を入力します。

ステップ 18 [**ナビゲーション（Navigation**）] ペインの新しいテナント名の下で、コンシューマの [**L3Outs**] に移動します。

ステップ 19 [**L3Outs**] を右クリックし、[**L3Out の作成（Create L3Out**）] を選択します。

[**L3Out の作成（Create L3Out**）] ウィザードが表示されます。

ステップ 20 [**VRF の作成（Create VRF**）] ダイアログ ボックスで、次の操作を実行します。

a) **Name** フィールドに、L3Out の名前を入力します。
b) [**VRF**] フィールドで、ドロップダウン メニューから、コンシューマのために作成された VRF を選択します。
c) **Consumer Label** フィールドに、コンシューマ ラベルの名前を入力します。
d) [**L3 ドメイン（L3 Domain**）] フィールドで、L3 ドメインを選択します。
e) プロトコルに適切な選択を行い、[**次へ（Next**）] をクリックします。

ステップ 21 [**外部 EPG（External EPG**）] ウィンドウが表示されるまで、次のウィンドウで必要な選択を行います。

[識別（Identity）] ウィンドウで選択したプロトコルに応じて、[ノードとインターフェイス（Nodes and Interfaces）] ウィンドウと [プロトコル（Protocols）] ウィンドウが表示される場合があります。[L3Out の作成（Create L3Out）] ウィザードの最後のウィンドウは、[外部 EPG（External EPG）] ウィンドウです。

ステップ 22 [外部 EPG（External EPG）] ウィンドウで次のアクションを実行します。

a) **Name** フィールドに、外部ネットワーク名を入力します。
b) [すべての外部ネットワークのデフォルト EPG（Default EPG for all external network）] チェックボックスをオフにします。

[サブネット（Subnets）] フィールドが表示されます。

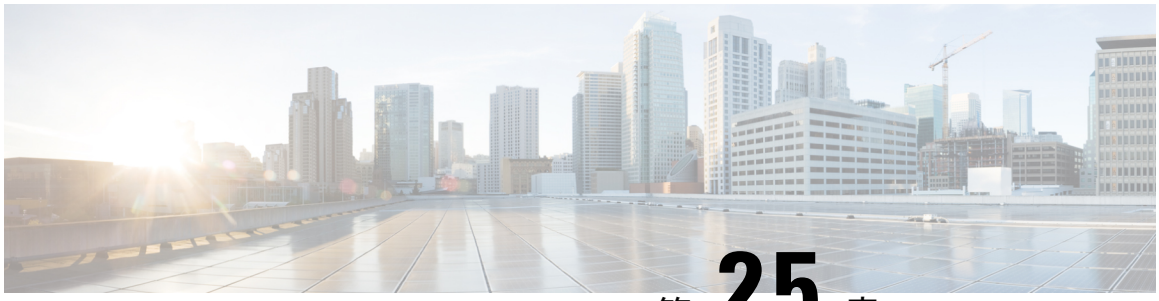
c) [サブネットの作成（Create Subnet）] ウィンドウにアクセスするには、[+] をクリックします。

d) [サブネットの作成（Create Subnet）] ダイアログ ボックスの [IP アドレス（IP Address）] フィールドに、マッチングを行う IP アドレスを入力します。**OK** をクリックします。
e) **Scope** フィールドで、必要なチェック ボックスをオンにして、**OK** をクリックします。

   このシナリオでは、**Shared Route Control Subnet** と **Shared Security Import Subnet** のチェック ボックスをオンにします。

f) [L3Out の作成（Create L3Out）] ウィザードで [完了（Finish）] をクリックします。

これで、共有レイヤ 3 Out VRF 間リーキングの設定は完了です。



第 25 章

L3Out の QoS

この章は、次の内容で構成されています。

L3Out QoS

L3Out QoS は、外部 EPG レベルで適用されるコントラクトを使用して設定できます。リリース 4.0(1) 以降、L3Out QoS は L3Out インターフェイスで直接設定することもできます。

（注） Cisco APICリリース 4.0(1) 以降を実行している場合は、L3Out に直接適用されるカスタム QoS ポリシーを使用して L3Out の QoS を設定することを推奨します。

パケットは入力 DSCP または CoS 値を使用して分類されるため、カスタム QoS ポリシーを使用して着信トラフィックを Cisco ACIQoS キューに分類できます。カスタム QoS ポリシーには、DSCP/CoS 値をユーザ キューまたは新しい DSCP/CoS 値（マーキングの場合）にマッピングするテーブルが含まれます。特定の DSCP/CoS 値のマッピングがない場合、ユーザ キューは入力 L3Out インターフェイスの QoS 優先度設定によって選択されます（設定されている場合）。

L3Out QoS ガイドラインと制約事項

L3Out の QoS 設定には次の注意事項が適用されます。

- カスタム QoS ポリシーは、Cisco Application Centric Infrastructure（ACI）ファブリックの外部から送信された（L3Out から受信した）レイヤ 3 マルチキャスト トラフィックではサポートされません。

- L3Out が存在する境界リーフ スイッチに適用するコントラクトを使用して QoS ポリシーを設定するには、VRFテーブルが出力モードである必要があります（ポリシー制御適用の方向は「出力」にする必要があります）。

  カスタム QoS 設定は L3Out で直接構成でき、境界リーフ スイッチからのトラフィックに適用できます。そのため、VRF テーブルは出力モードである必要はありません。

- 適用するQoSポリシーを有効にするには、VRFポリシー制御適用設定を「適用」にする必要があります。

- L3Outとその他のEPG間の通信を制御する契約を設定する際に、契約またはサブジェクトに QoS クラスまたはターゲット DSCP を含めます。

（注） 外部 EPG ではなく、契約の QoS クラスまたはターゲット DSCP のみ設定します（ `l3extInstP`）。

- 契約のサブジェクトを作成する際は、QoS 優先度レベルを選択する必要があります。[Unspecified] を選択することはできません。

（注） カスタム QoS ポリシーは QoS クラスが [**未指定**（**Unspecified**）] に設定されている場合でも DSCP/CoS 値を設定するため、カスタム QoS ポリシーは例外となります。QoS レベルが指定されていない場合、レベルはデフォルトで 3 として扱われます。

- 第 2 世代スイッチでは、QoS で、グローバル ポリシー、EPG、L3Out、カスタム QoS、および契約で設定された新しいレベル 4、5、6 をサポートします。次の制限が適用されます。
  - 厳密な優先順位を設定できるクラスの数は、5 つまで増加できます。
  - 3 つの新しいクラスは、第 1 世代スイッチでのみサポートされます。
  - 第1世代スイッチと、第2世代スイッチの間でトラフィックが流れる場合、トラフィックは QoS レベル 3 を使用します。
  - 新しいクラスでFEXと通信するため、トラフィックは値0のレイヤ2 Cosを伝送します。

  第 1 世代スイッチは、名の末尾に「EX」、「FX」、「FX2」、「GX」またはそれ以降のサフィックスがないことで識別できます。たとえば、N9K-9312TX という名前などです。第 1 世代以降のスイッチは、名の末尾に「EX」、「FX」、「FX2」、「GX」またはそれ以降のサフィックスが付いていることで識別できます。たとえば、N9K-93108TC-EX や N9K-9348GC-FXP という名前などです。

- QoSクラスを構成したり、L3Outインターフェイスに適用するカスタムQoSポリシーを作成できるようになりました。

GUI を使用して L3Out に QoS ディレクトリを設定する

この章では L3Out で QoS ディレクトリを設定する方法について説明します。これは、リリース 4.0(1) 以降の L3Out QoS の推奨設定方法です。Cisco APIC

手順

ステップ 1 メイン メニュー バーから **[テナント（Tenants）]** > **[<*tenant-name*>]** を選択します。

ステップ 2 左側の [ナビゲーション（Navigation）] ペインで、[テナント（Tenant） <tenant-name>] [ネットワーキング（Networking）] [L3Outs] [<routed-network-name>] [論理ノードプロファイル（Logical Node Profiles） [<node-profile-name>] [論理インターフェイス プロファイル（Logical Interface Profiles] [<interface-profile-name>] を展開します。 > > > > > > > >

存在しない場合は、新しいネットワーク、ノード プロファイル、およびインターフェイス プロファイルを作成する必要があります。

ステップ 3 メイン ウィンドウ ペインで、L3Out のカスタム QoS を設定します。

[QoS 優先順位（QoS Priority）] ドロップダウンリストを使用して、標準 QoS レベルの優先順位を設定できます。または、[カスタム QoS ポリシー（Custom QoS Policy）] ドロップダウンから既存のカスタム QoS ポリシーを設定するか、新しいカスタム QoS ポリシーを作成できます。

GUI を使用した L3Outs の QoS コントラクトの設定

この項では、コントラクトを使用して L3Out の QoS を設定する方法について説明します。

（注） リリース 4.0(1) 以降では、L3Out QoS 用にカスタム QoS ポリシーを使用することを推奨しています。GUI を使用して L3Out に QoS ディレクトリを設定する （451 ページ） で説明しています。

この項で説明するコントラクトを使用した QoS 分類の設定は、L3Out で直接設定された QoS ポリシーよりも優先されます。

手順

ステップ 1 L3Out により使用される境界リーフ スイッチに適用される QoS をサポートするために、L3Out を利用していたテナントの VRF インスタンスを設定します。

a) メイン メニュー バーから **[テナント（Tenants）]** > **[<*tenant-name*>]** を選択します。

b) **Navigation** ウィンドウで、**Networking** を展開し、**VRFs** を右クリックし、 **Create VRF** を選択します。
c) VRF の名前を入力します。
d) **Policy Control Enforcement Preference** フィールドで、**Enforced** を選択します。
e) [Policy Control Enforcement Dirction] で [Egress] を選択します

QoS 分類がコントラクトで実行される場合は、VRF の適用を強制を [出力（Egress）] に設定する必要があります。

f) L3Out の要件に従って VRF を設定します。

ステップ 2 L3Out を使用する EPG の間の通信を可能にするためにフィルタを設定するときには、QoS クラスまたはターゲット DSCP を含めて、L3Out を通して入力されるトラフィックにおける QoS の優先順位を適用します。

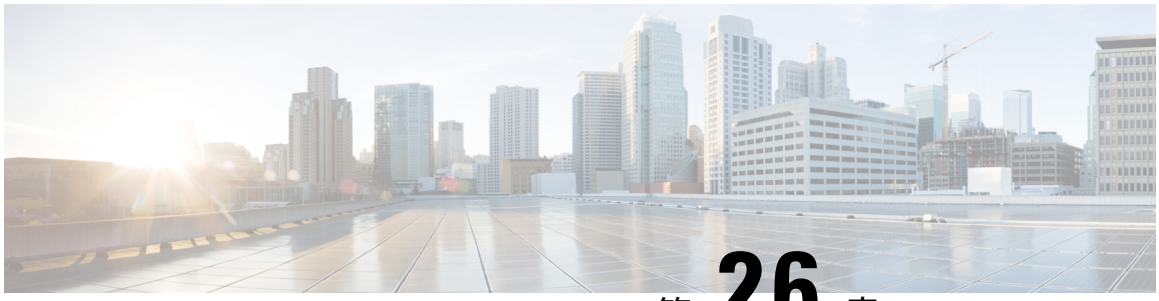
a) [Navigation] ウィンドウの L3Out を使用するテナントで、**Contracts** を展開し、**Filters** を右クリックし、**Create Filter** を選択します。
b) **Name** フィールドに、ファイルの名前を入力します。
c) [Entries] フィールドで、[+] をクリックしてフィルタ エントリを追加します。
d) エントリの詳細を追加し、**Update** をクリックし、**Submit** をクリックします。
e) 以前に作成したフィルタを展開し、フィルタ エントリをクリックします。
f) **Match DSCP** フィールドを、そのエントリで必要な DSCP レベルに設定します。たとえば **EF** にします。

ステップ 3 契約を追加します。

a) **Contracts** の下で、**Standard** を右クリックして、**Create Contract** を選択します。
b) 契約の名前を入力します。
c) **QoS Class** フィールドで、この契約で管理されるトラフィックの QoS 優先順位を選択します。または、**Target DSCP** の値を選択することもできます。

この項で説明するコントラクトを使用した QoS 分類の設定は、L3Out で直接設定された QoS ポリシーよりも優先されます

d) [Subjects] の [+] アイコンをクリックして、情報カテゴリを契約に追加します。
e) 情報カテゴリの名前を入力します。
f) [QoS Priority] フィールドで、必要な優先度レベルを選択します。[Unspecified] を選択することはできません。
g) [Filter Chain] の下で、[Filters] の [+] アイコンをクリックし、先ほど作成したフィルタをドロップダウンリストから選択します。
h) **Update** をクリックします。
i) **Create Contract Subject** ダイアログボックスで、**OK** をクリックします。



第 26 章

IP SLAs

この章は、次の内容で構成されています。

ACI IP SLA について

多くの企業ではビジネスのほとんどをオンラインで行い、サービスの損失は企業の収益性に影響を及ぼすことがあります。今では、インターネット サービス プロバイダ（ISP）や内部 IT 部門でさえも、定義済みのサービス レベル、サービス レベル契約（SLA）を提供して、お客様に一定の予測可能性を提供しています。

IP SLA トラッキングは、ネットワークの一般的な要件です。IP SLA トラッキングにより、ネットワーク管理者はネットワーク パフォーマンスに関する情報をリアルタイムで収集できます。Cisco ACI IP SLA では、ICMP および TCP プローブを使用して IP アドレスを追跡できます。トラッキング設定はルート テーブルに影響を与える可能性があり、トラッキング結果がネガティブになったときにルートを削除し、結果が再びポジティブになったときにルートをテーブルに戻すことができます。

ACI IP SLA は、次のものに使用できます。

- スタティック ルート：
  - ACI 4.1 の新機能
  - ルート テーブルからのスタティック ルートの自動削除または追加
  - ICMP および TCP プローブを使用してルートを追跡する
- ポリシーベース リダイレクト（PBR）トラッキング：
  - ACI 3.1 以降で使用可能
  - ネクスト ホップの自動削除または追加

- ICMP プローブと TCP プローブ、または L2Ping を使用した組み合わせを使用して、ネクストホップ IP アドレスを追跡します。
- ネクストホップの到達可能性に基づいて PBR ノードにトラフィックをリダイレクトする

PBR トラッキングの詳細については、『*Cisco APIC Layer 4 to Layer 7 Services Deployment Guide*』の「ポリシーベース リダイレクトの設定」を参照してください。

（注） いずれの機能でも、設定、API の使用、スクリプトの実行など、プローブの結果に基づいてネットワーク アクションを実行できます。

ACI IP SLA でサポートされるトポロジ

次の ACI ファブリック トポロジは IP SLA をサポートします。

- シングル ファブリック：IP SLA トラッキングは、L3out と EPG/BD の両方を介して到達可能な IP アドレスでサポートされます。
- マルチポッド
  - 異なるポッドで単一のオブジェクト トラッキング ポリシーを定義できます。
  - ワークロードは、あるポッドから別のポッドに移動できます。IP SLA ポリシーは引き続きアクセス可能性情報をチェックし、エンドポイントが移動したかどうかを検出します。
  - エンドポイントが別のポッドに移動すると、IP SLA トラッキングも他のポッドに移動されるため、トラッキング情報は IP ネットワークを通過しません。
- リモート リーフ
  - ACI メイン データ センターおよびリモート リーフ スイッチ全体で単一オブジェクト トラッキング ポリシーを定義できます。
  - リモート リーフ スイッチの IP SLA プローブは、IP ネットワークを使用せずに IP アドレスをローカルに追跡します。
  - ワークロードは、1 つのローカル リーフからリモート リーフに移動できます。IP SLA ポリシーは引き続きアクセス可能性情報をチェックし、エンドポイントが移動したかどうかを検出します。
  - IP SLA ポリシーは、エンドポイントの場所に基づいてリモート リーフ スイッチまたは ACI メイン データ センターに移動し、ローカル トラッキングを行うため、トラッキング トラフィックは IP ネットワークを通過しません。

Cisco ACI IP SLA のオペレーション

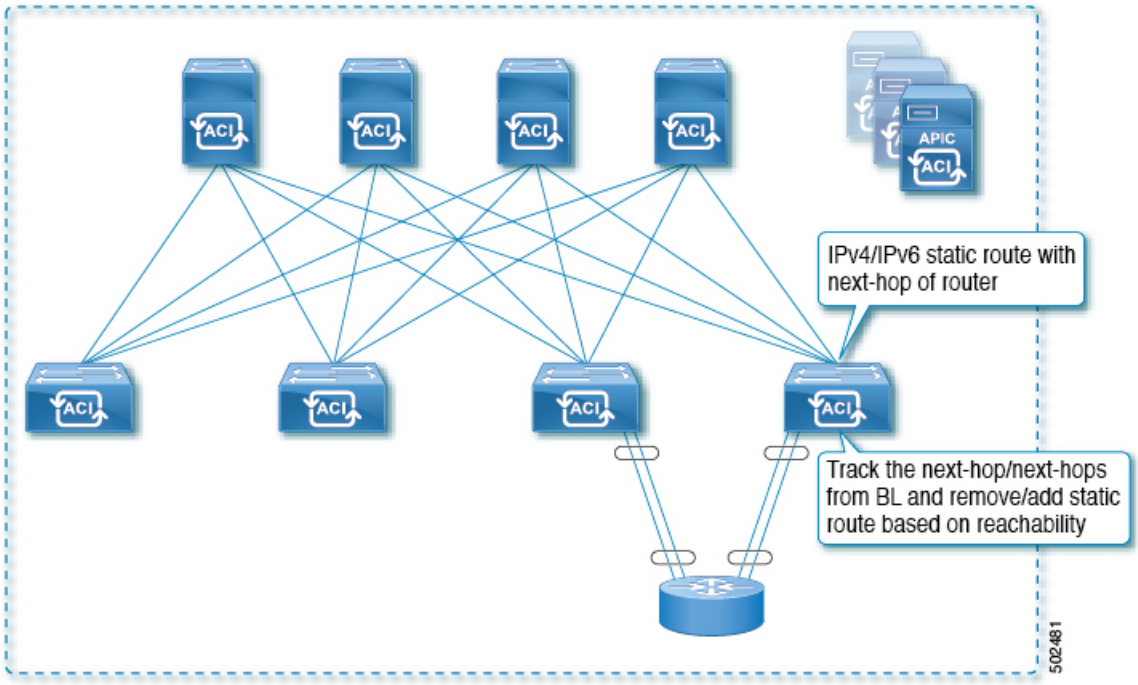
Cisco ACI IP SLA は、ACI ファブリック上でモニタリング機能を提供し、SLA プローブをデータ センター ネットワーク全体および外部ネットワークで実行できるようにします。これは、モニタリング中に使用されるプローブ タイプを定義する IP SLA モニタリング ポリシーを設定することによって実現されます。モニタリング ポリシーは、「トラック メンバー」と呼ばれるモニタリング プローブ プロファイルに関連付けられます。設定が完了すると、IP アドレス、関連付けられたモニタリング ポリシー、およびスコープ（ブリッジ ドメインまたは L3Out）によって、エンドポイントまたはネクストホップを定義します。1 つ以上のトラック メンバーを「トラック リスト」に割り当てることができます。トラックリストは、しきい値を設定します。これを超えると、トラック リストが使用可能（アップ）か使用不可（ダウン）かが決まります。

次の 4 つの例は、スタティック ルートでサポートされる ACI IP SLA の使用例を示しています。

例 1：ネクストホップのトラッキングによるスタティック ルートの可用性

次の図は、ネットワーク トポロジと、ルータのスタティック ルートの可用性を追跡する動作を示しています。

図 *54*：ネクストホップのトラッキングによるスタティック ルートの可用性



この使用ケースでは：

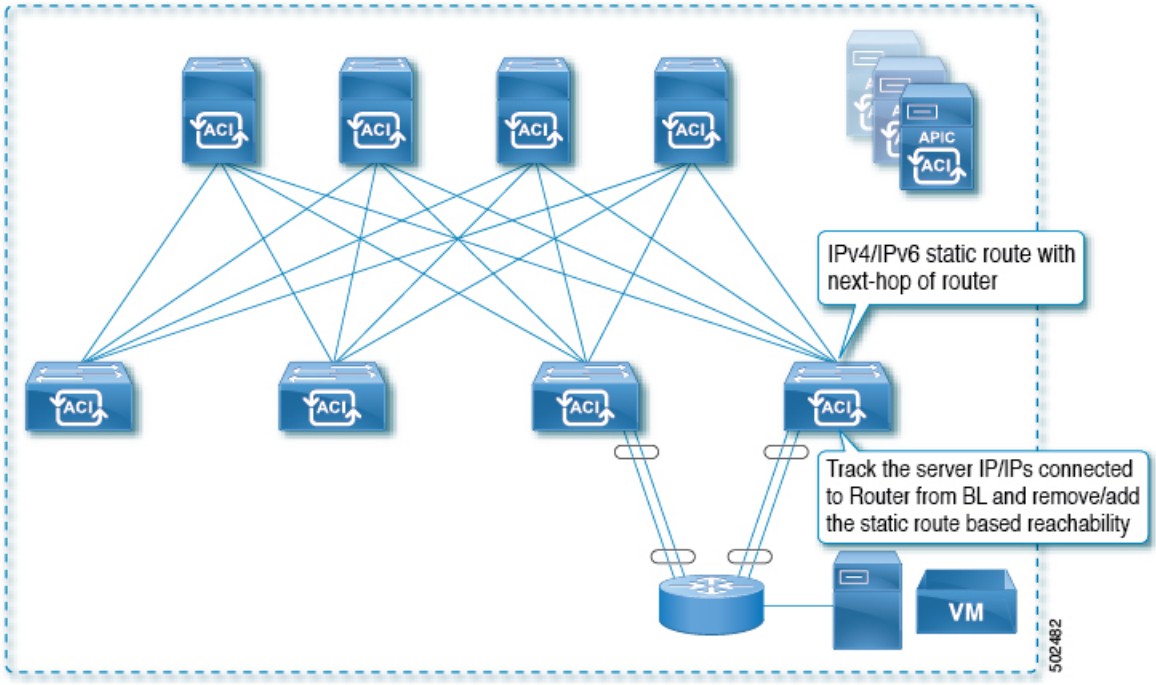
- ネクストホップは直接または間接のいずれかになります。つまり、ネクストホップはルータのループバック IP アドレスになります。
- ネクストホップには、物理インターフェイス、サブインターフェイス、ポート チャネル（PC）、PC サブインターフェイス、vPC、またはスイッチ仮想インターフェイス（SVI）を介してアクセスできます。

- スタティック ルートはL3out外部ネットワークの下で設定され、ネクストホップのアクセス可能性に基づいてルート テーブルから削除または追加できます。

例 2：L3Out を介した IP アドレスのトラッキングによるスタティック ルートの可用性

次の図は、L3Out外部ルートを介してサーバのスタティック ルートの可用性を追跡するためのネットワーク トポロジと動作を示しています。

図 *55 : L3Out* を介した *IP* アドレスの追跡によるスタティック ルートの可用性



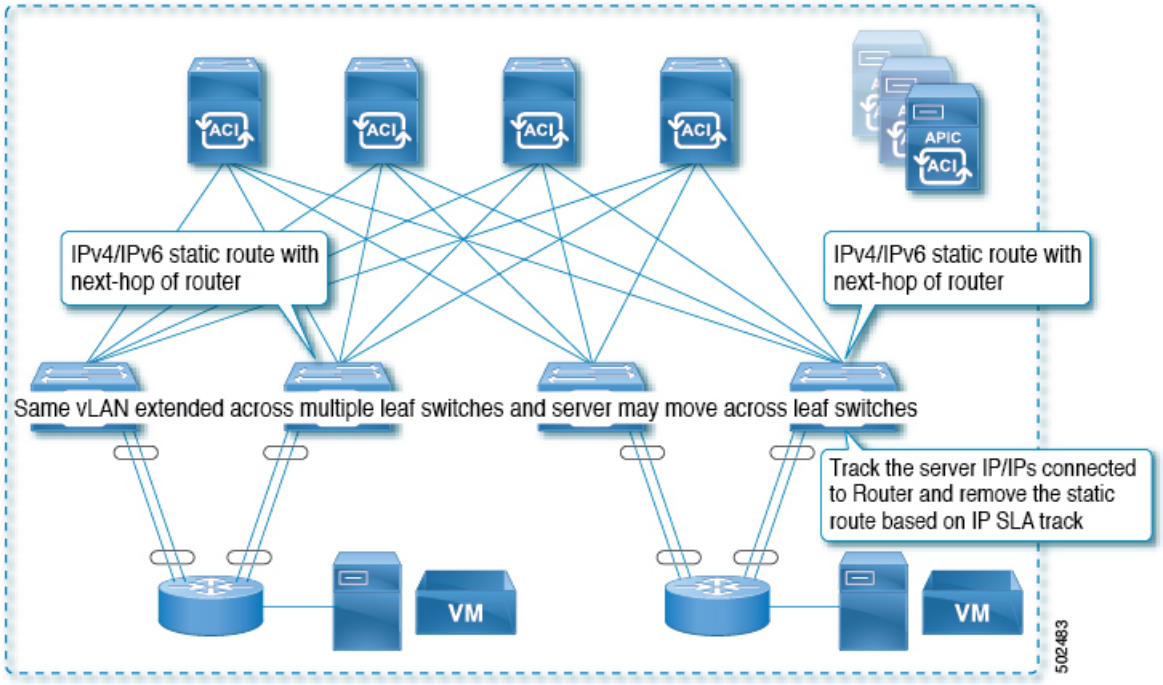
この使用ケースでは：

- ACI ファブリック（境界リーフ）からルータに接続されているサーバの IP アドレスを追跡し、サーバのアクセス可能性に基づいてスタティック ルートを削除または追加します。
- L3Out は、ポート チャネル（PC）、PC サブインターフェイス、vPC、スイッチ仮想インターフェイス（SVI）、L3 インターフェイス、または L3 サブインターフェイスを経由できます。
- スタティック ルートは L3Out で設定され、IP アドレスのアクセス可能性に基づいて削除または追加されます。

例 3：L3Out を介した IP アドレスのトラッキングによるスタティック ルートの削除

次の図は、L3Out外部ルートを介してサーバのスタティック ルートの可用性を追跡するためのネットワーク トポロジと動作を示しています。L3Out/VRFからアクセスできない場合、ルートは削除されます。

図 *56 : L3Out* を介した *IP* アドレスのトラッキングによるスタティック ルートの削除



この使用ケースでは：

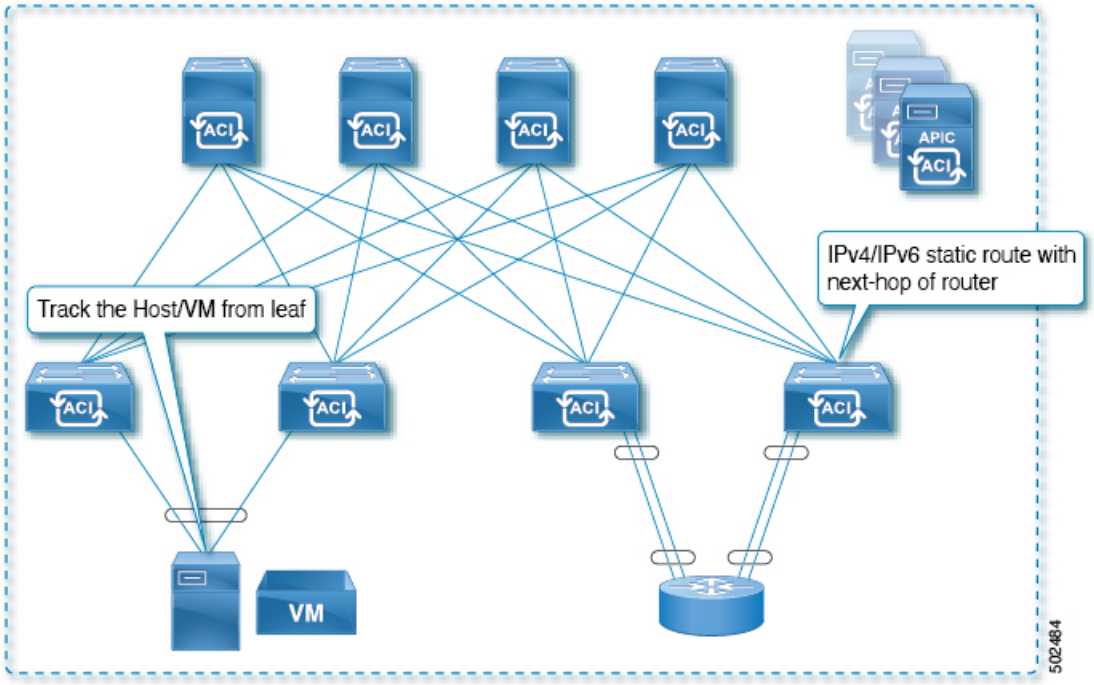
- L3Out は VLAN/SVI を介して設定され、その SVI は複数のリーフに拡張されます。
- L3Out を介してアクセス可能なサーバの IP アドレスは、リーフ間を移動できます。
- サーバの IP アドレスを追跡し、L3Out/VRF からアクセスできない場合は、ルート テーブルからスタティック ルートを削除します。
- サーバが再びアクセス可能になると、スタティック ルートがルート テーブルに戻されます。

例 4：ACI ファブリックの IP アドレスのトラッキングによるスタティック ルートの削除

前の例で示したように、ルートの IP SLA のプローブ IP は通常、ルートのネクストホップまたはルート経由で到達可能な外部 IP アドレスですが、エンドポイントが IP SLA の対象となるルートの背後に存在しない場合でも、プローブ IP として ACI BD でエンドポイント IP アドレスを使用することもできます。これは、ACI 内の特定のエンドポイントだけがスタティック ルートを使用する場合に役立ちます。このようなエンドポイントが存在しない場合、ルートは使用されません。

次の図は、ネットワーク トポロジと、ACI ファブリックの IP アドレスを追跡する動作を示しています。

図 *57 : ACI* ファブリックでの *IP* アドレスの追跡によるスタティック ルートの可用性



この使用ケースでは：

- EPG/BD 経由で接続されているエンドポイントの IP 到達可能性を追跡します。
- エンドポイントのアクセス可能性に基づいて、スタティック ルートが L3Out で削除または追加されます。
- エンドポイントがファブリック内のある場所から別の場所に移動しても、同じ BD からエンドポイントへの IP 到達可能性がある限り、IP SLA モニタリングはそれをアクセス可能と見なし、スタティック ルートの有効性に影響を与えません。

IP SLA モニタリングポリシー

IP Service Level Agreements（SLA）は、継続的で信頼性のある予測可能な方法でトラフィックを生成する、アクティブ トラフィック モニタリングを使用し、ネットワークのパフォーマンスを測定するために分析を行います。IP SLA モニタリング ポリシー動作による測定統計情報を、トラブルシューティング、問題分析、ネットワーク トポロジの設計に使用できます。

Cisco ACI では、IP SLA モニタリング ポリシーは次のものに関連付けられます。

- サービス リダイレクト ポリシー：サービス リダイレクト ポリシー下のすべての宛先は、モニタリング ポリシーで設定された設定とパラメータに基づいてモニタされます。
- スタティック ルート：IP SLA モニタリング ポリシーをトラック リストまたはトラック メンバーに追加し、スタティック ルートに関連付けることで、ルートのネクスト ホップ セグメントの可用性をモニタリングできます。

IP SLA モニタリング ポリシーは、プローブの頻度とタイプを識別します。

ACI IP SLA モニタリング動作プローブ タイプ

ACI IP SLA を使用して、コア、分散、エッジといったネットワークの任意の領域間のパフォーマンスをモニタできます。モニタリングは、物理的なプローブを展開しなくても、時間と場所を問わず実行できます。ACI IP SLA は、生成されたトラフィックを使用して、スイッチなどの 2 つのネットワーク デバイス間のネットワーク パフォーマンスを測定します。IP SLA 動作のタイプは次のとおりです。

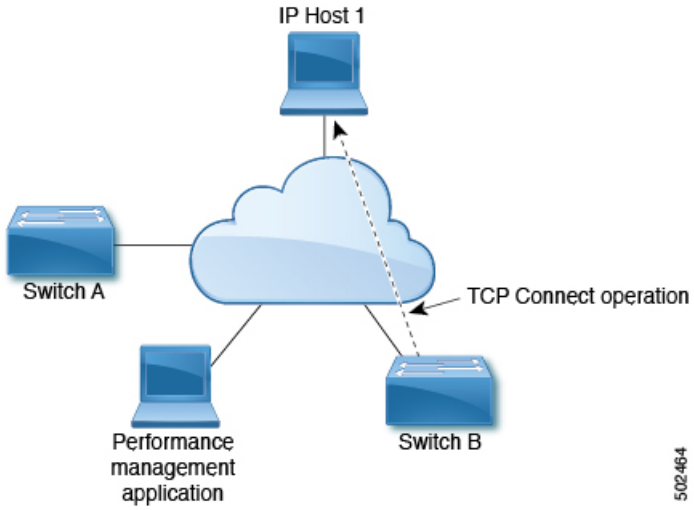
- ICMP： エコー プローブ
- TCP：プローブの接続

TCP 接続動作

IP SLA TCP 接続動作は、シスコ スイッチと IP デバイス間の TCP プローブの実行に要する応答時間を測定します。TCP は、信頼性の高い全二重データ伝送を行うトランスポート層（レイヤ 4）インターネットプロトコルです。宛先デバイスは、IP を使用する任意のデバイスになります。

次の図では、設定されたスタティック ルートに基づいて、スイッチ B が送信元 IP SLA デバイスとして設定されています。TCP接続動作は、IP SLA モニタリング ポリシー（スタティック ルートに関連付けられている）で、宛先デバイスを IP ホスト 1 として設定されます。

図 *58 : TCP* 接続の動作例



接続応答時間は、スイッチ B から IP ホスト 1 に TCP 要求メッセージを送信してから、IP ホスト 1 からの応答を受信するまでの時間を測定して算出されます。

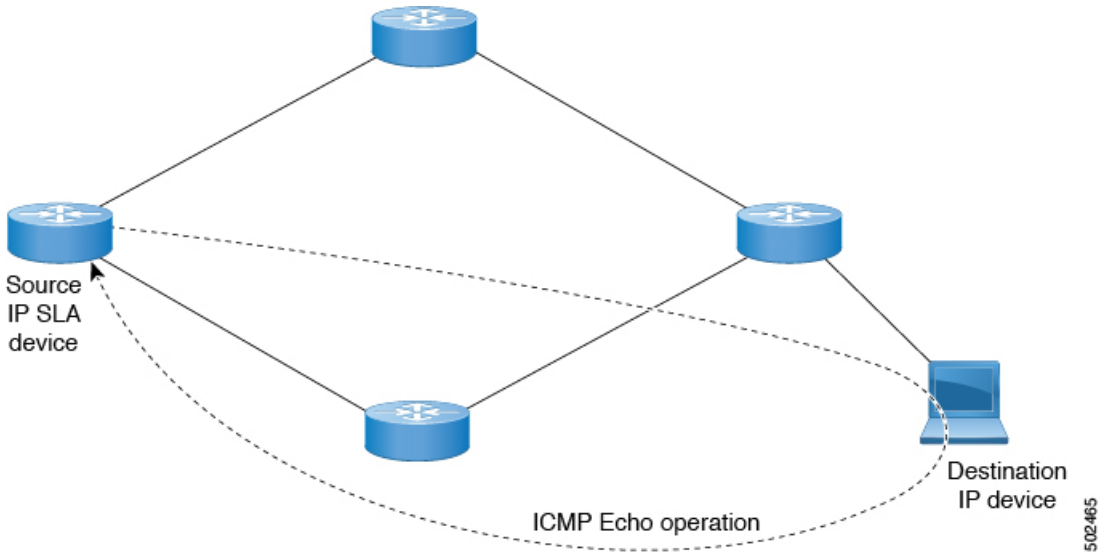
ICMP エコー動作

Internet Control Message Protocol（ICMP）エコー動作は、IPv4 または IPv6 を使用する 2 台のデバイス間のエンドツーエンド応答時間を測定します。応答時間は、ICMP エコー要求メッセー

ジを宛先に送信して応答を受信するまでの時間を測定して算出します。ICMP エコーは、ネットワーク接続問題のトラブルシューティングに役立ちます。ICMP エコー動作の結果を表示および分析することで、ネットワーク IP 接続の実況状況を判断できます。

次の図では、ICMP エコー動作は ping ベースのプローブを使用して送信元 IP SLA デバイスと宛先 IP デバイスの間の応答時間を測定します。多くのお客様が、応答時間の測定に IP SLA ICMP ベース動作、社内 ping テスト、または ping ベース専用プローブを使用しています。

図 *59 : ICMP* エコー動作の例



IP SLA ICMP エコー動作と ICMP ping テストは同じ IETF 仕様に準拠しているので、どちらの方法でも同じ応答時間が得られます。

IP SLA トラック メンバー

IP SLA トラック メンバーは、以下を識別します。

- 追跡対象の IP アドレス
- IP SLA モニタリング ポリシー（プローブの頻度とタイプ）
- スコープ（ブリッジ ドメインまたは L3Out）

IP SLA トラック リスト

IP SLA トラック リストは、モニタ対象のネットワーク セグメントを表す 1 つ以上の IP SLA トラック メンバーを集約します。トラック リストは、スタティック ルートを使用可能または使用不可と見なすために必要なトラック メンバーのパーセンテージまたは重みを決定します。しきい値のパーセンテージまたは重みに基づいてトラック リストが稼働している場合、スタティック ルートはルーティング テーブルに残ります。トラック リストがダウンしている場合、

スタティック ルートは、トラック リストが回復するまでルーティング テーブルから削除されます。

次に、しきい値パーセンテージ オプションを使用して、トラック リストに 4 つのトラック メンバーを設定する例を示します。

しきい値の設定：

- 「Percentage Up」パラメータを 100（パーセント）に設定します。
- 「Percentage Down」パラメータを 50（パーセント）に設定します。

このトラック リストでは、4 つのトラック メンバーのそれぞれに 25% が割り当てられます。トラック リストが到達不能（ダウン）になるには、4 つのトラック メンバーのうち 2 つが到達不能（50%）である必要があります。トラック リストが到達可能（アップ）に戻るには、4 つのトラック メンバーすべてが到達可能（100%）である必要があります。

（注） トラッキング リストがスタティック ルートに関連付けられ、トラッキング リストが到達不能（ダウン）になると、トラッキング リストが再び到達可能になるまで、スタティック ルートはルーティング テーブルから削除されます。

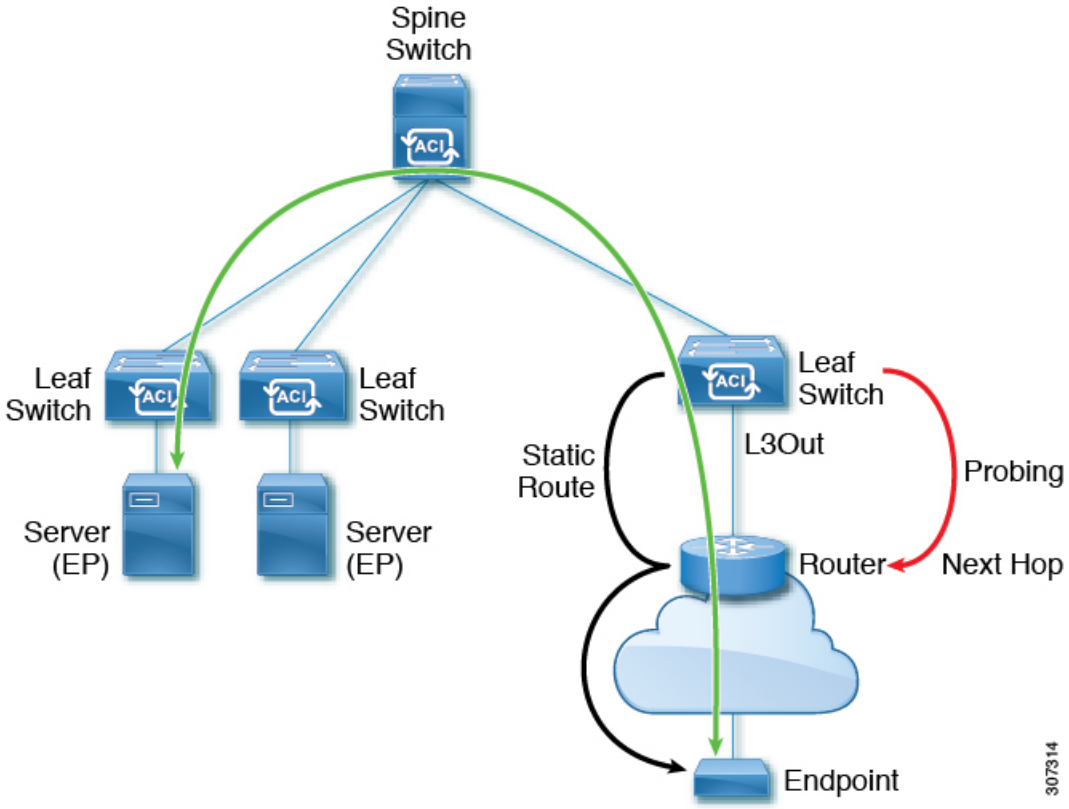
IP SLA 設定コンポーネントの関連付けの例

ACI IP SLA は、トラック メンバーとトラック リストに基づいて、送信するプローブのタイプと送信先を特定します。設定を計画すると、タスクを簡単かつ迅速に行うことができます。このセクションでは、IP SLA の設定方法を説明する例を使用します。

Cisco ACI IP SLA L3Out Example

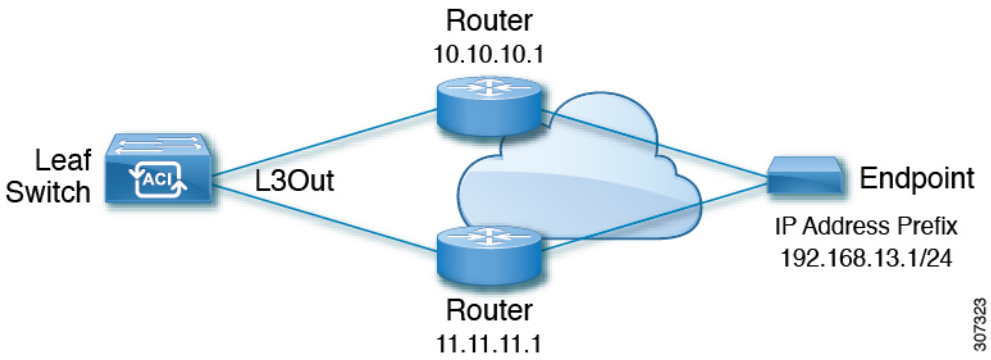
次の図は、ACI ファブリック内で外部エンドポイントを含む特定の設定済みスタティック ルートのモニタリング/プローブを提供する Cisco ACI IP SLA を示しています。

図 *60 :* 例：*ACI L3Out IP SLA*



次の図は、エンドポイント プレフィックス 192.168.13.1/24 のスタティック ルートを示しています。また、L3Out リーフ スイッチとコンシューマ エンドポイント間のスタティック ルートにあるルータのペアも示します。

図 *61 :* スタティックルートの例



上の図に基づいて ACI IP SLA を設定するには、ルータをモニタして、コンシューマ エンドポイントへの接続を確認する必要があります。これを行うには、スタティック ルート、トラック メンバー、およびトラック リストを作成します。

- ネクスト ホップ 10.10.10.1 および 11.11.11.1 の 192.168.13.1/24 のスタティック ルート

- トラック メンバー 1（TM-1）には、ルータの IP アドレス 10.10.10.1 が含まれています（これはネクスト ホップ プローブです）。
- トラック メンバー 2（TM-2）には、ルータの IP アドレス 11.11.11.1 が含まれています（これはネクスト ホップ プローブです）。
- TM-1 および TM-2 を含むトラック リスト 1（TL-1）（スタティック ルートに関連付けられたトラック リスト）。トラック リストには、設定されたプレフィックス エンドポイントに到達できるネクスト ホップのリストが含まれます。トラック リストが到達可能か到達不能かを決定するしきい値も設定されます）。
- TM-1 を含むトラック リスト 2（TL-2）（スタティック ルートに含まれるネクスト ホップ エントリに関連付けられる）
- TM-2 を含むトラック リスト 3（TL-3）（スタティック ルートに含まれるネクスト ホップ エントリに関連付けられる）

汎用スタティック ルートの場合、TL-1 をスタティック ルートに関連付け、TL-2 を 10.10.10.1 ネクスト ホップに関連付け、TL-3 を 11.11.11.1 ネクスト ホップに関連付けることができます。特定のスタティック ルートのペア（両方とも 192.168.13.1/24）では、一方の TL-2 と他方の TL-3 を関連付けることができます。また、ルータのネクスト ホップに TL-2 と TL-3 が関連付けられている必要があります。

これらのオプションを使用すると、1 台のルータで障害が発生しても、障害発生時にバックアップ ルートを提供できます。トラック メンバーとトラック リストの詳細については、次のセクションを参照してください。

IP SLA のガイドラインと制約事項

IP サービス レベル合意事項を計画および設定する場合は、次のガイドラインと制限事項を考慮してください。

- IP SLA は、IPv4 アドレスと IPv6 アドレスの両方をサポートします。
- IP SLA は、-EX および -FX シャーシを含むすべての Cisco Nexus 第 2 世代スイッチでサポートされます。
- Cisco Application Policy Infrastructure Controller（APIC）リリース 4.1(1) 以降、IP SLA モニタ ポリシーは IP SLA ポート値を検証します。検証のため、TCP が IP SLA タイプとして設定されている場合、Cisco APICは以前のリリースで許可されていた IP SLA ポート値 0 を受け入れなくなります。IP SLA ポート値が 0 である以前のリリースの IP SLA モニタ ポリシーは、Cisco APICがリリース 4.1(1) 以降にアップグレードされると無効になります。これにより、設定のインポートまたはスナップショットのロールバックが失敗します。

  回避策は、Cisco APICをアップグレードする前にゼロ以外の IP SLA ポート値を設定し、IP SLA ポートの変更後に取得されたスナップショットと設定のエクスポートを使用することです。

- IP SLA でリモート リーフ スイッチをサポートする場合は、グローバル GIPo を有効にする必要があります。
  1. メニュー バーで、[**システム（System**）] > [**システム設定（System Settings**）] を選択します。
  2. [システム設定（System Settings）] ナビゲーション ウィンドウで [**システム グローバル GIPo（System Global GIPo**）] をクリックします。
  3. [システム グローバル GIPo ポリシー（System Global GIPo Policy）] 作業ウィンドウで [**有効化（Enabled**）] をクリックします。
  4. [ポリシー使用警告（Policy Usage Warning）] ダイアログで、GIPo ポリシーを使用する可能性があるノードとポリシーを確認し、必要に応じて [**変更の送信（Submit Changes**）] をクリックします。

- [ファブリック（Fabric）]、[インベントリ（Inventory）]、[ポッド番号（Pod *number*）]、[リーフ ノード名（Leaf Node *name*）]、[プロトコル（Protocols）]、[IP SLA]、[ICMP エコー操作（ICMP Echo Operations）]、または [TCP 接続操作（TCP Connect Operations）] で表示される統計情報は、5 分間隔でのみ収集できます。間隔のデフォルトは [15 分] ですが、[5 分] に設定する必要があります。
- IP SLA ポリシーは、vPod 経由で接続されたエンドポイントではサポートされません。
- IP SLA は、単一のポッド、Cisco ACI Multi-Pod、およびリモート リーフ スイッチでサポートされます。
- 追跡対象の宛先 IP アドレスが接続されている場合、IP SLA はサポートされません。Cisco ACI マルチサイト
- ボーダー リーフ スイッチに、VRF の MP-BGP（マルチプロトコル ボーダー ゲートウェイ プロトコル）で再配布される静的ルートがある場合、MP-BGP ルートのアドミニストレーティブ ディスタンスは、次に示すように、静的ルートと同じになります。

```
leaf102# show ip route 10.10.10.10/32 vrf test:VRF-1
IP Route Table for VRF "test:VRF-1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.10.10.10/32, ubest/mbest: 1/0
*via 102.0.0.2, vlan45, [1/0], 01w00d, static
```

このルートは、VRF のファブリック MP-BGP ルートに挿入され、次に示すように、他のリモート リーフ スイッチによって iBGP ルートとして検出されます。

```
leaf103# show ip route 10.10.10.10/32 vrf test:VRF-1
IP Route Table for VRF "test:VRF-1"
'*' denotes best ucast next-hop
'**' denotes best mcast next-hop
'[x/y]' denotes [preference/metric]
'%<string>' in via output denotes VRF <string>

10.10.10.10/32, ubest/mbest: 1/0
```

```
*via 10.0.200.64%overlay-1, [1/0], 01w00d, bgp-65310, internal, tag 65310
recursive next hop: 10.0.200.64/32%overlay-1
```

ただし、iBGP ルートのアドミニストレーティブ ディスタンスは、iBGP AD のアドミニストレーティブ ディスタンスではなく、静的ルートのアドミニストレーティブ ディスタンスと同じです。

これは、APIC リリース 4.1(1) と APIC リリース 5.0(1) の両方で観察されました。

検証済み IP SLA 番号の詳細については、Cisco APIC のドキュメント ページで該当する『Cisco APIC の検証済みスケーラビリティ ガイド』を参照してください。https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

スタティック ルートの ACI IP SLA の設定および関連付け

ここでは、次の IP SLA ポリシーおよびプロファイルを設定および関連付けるために必要なタスクについて説明します。

- IP SLA モニターリング ポリシー
- IP SLA トラック メンバー
- IP SLA トラック リスト

前のコンポーネントは、スタティック ルートまたはネクスト ホップ プロファイルに適用されます。

GUI を使用した IP SLA モニタリング ポリシーの設定

GUI を使用して（）が特定の SLA タイプのモニタリング プローブを送信できるようにするには、次の手順を実行します。Cisco Application Policy Infrastructure ControllerAPICCisco APIC

手順

ステップ 1 メニュー バーで **[テナント（Tenant）]** > **[tenant_name]** をクリックします。[ナビゲーション（Navigation）] ペインで、**[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[IP SLA]**をクリックします。

ステップ 2 **IP SLA Monitoring Policies** を右クリックして、**Create IP SLA Monitoring Policy** をクリックします。

ステップ 3 **Create IP SLA Monitoring Policy** ダイアログボックスで、次の操作を実行します:

a) **[名前（Name）]** フィールドに、IP SLA モニタリング ポリシーの一意の名前を入力します。

b) **SLA Type** フィールドで、SLAタイプを選択します。

SLA タイプは、[TCP]、[ICMP]、[L2Ping]、または [HTTP] です。[**ICMP**] がデフォルト値です。

（注） [L2Ping] は、レイヤ 1/レイヤ 2 ポリシーベース リダイレクト（PBR）トラッキングでのみサポートされます。

c) SLA タイプに [HTTP] を選択した場合は、[HTTP バージョン（HTTP Version）] ボタンにバージョンを選択します。

d) SLA タイプに [HTTP] を選択した場合は、[HTTP URI] フィールドに、サービス ノード トラッキングに使用する HTTP URI を入力します。

URI は「/index.html」のように「/」で始まる必要があります。

e) SLA タイプに [TCP] を選択した場合は、[宛先 ポート（Destination Port）] フィールドにポート番号を入力します。

f) [SLA 頻度（SLA Frequency）] フィールドに、パケットを追跡するために設定された頻度を決定する値を秒単位で入力します。

範囲は、1 ～ 300 です。デフォルト値は 60 です。HTTP トラッキングの最小頻度は 5 秒です。

g) [検出乗数（Detect Multiplier）] フィールドに、失敗が検出されたか、またはトラックがダウンしていることを示す、失敗したプローブの数を行に入力します。

デフォルトでは、3 つのプローブが連続して検出されなかった場合に障害が検出されます。[検出乗数（Detect Multiplier）] フィールドの値を変更すると、行で検出されなかったプローブの数が変更されます。これにより、障害が検出されたタイミング、またはトラックがダウンしていると見なされるタイミングが決まります。

[SLA 頻度（SLA Frequency）] のエントリと組み合わせて使用すると、障害が検出されるタイミングを決定できます。たとえば、これらのフィールドに次のエントリを入力したとします。

- **SLA 頻度（秒）（SLA Frequency（sec））**: 5
- **検出乗数（Detect Multiplier）**: 30

この例のシナリオでは、約 150 秒で障害が検出されます（5 秒 x 30）。

h) [TCP] 以外の SLA タイプを選択した場合は、[データ サイズ（バイト）の要求（Request Data Size（bytes））] フィールドに、IP SLA 動作の要求パケットのペイロードに含まれるプロトコル データのサイズをバイト単位で入力します。

i) [サービスのタイプ（Type of Service）] フィールドに、IP SLA 動作の IPv4 ヘッダーのタイプ オブ サービス（ToS）を入力します。

j) [**処理タイムアウト（ミリ秒）（Operarion Timeout（milliseconds））**] フィールドに、要求パケットの応答に対する IP SLA 処理の待機時間をミリ秒単位で指定します。

k) **Threshold（milliseconds）** フィールドに、IP SLA 動作によって作成されるネットワーク モニターリング統計情報を計算するための上限しきい値を入力します。

l) [**トラフィック クラス値（Traffic Class Value）**] フィールドに、IPv6 ネットワークの IP SLA 動作の IPv6 ヘッダーのトラフィック クラス バイトを入力します。

m) **[送信（Submit）]** をクリックします。`

IP SLA モニタリング ポリシーが設定されます。

GUI を使用した IP SLA トラック メンバーの設定

このタスクを使用して、IP SLA トラック リストに追加された番号の 1 つである IP SLA トラック メンバーを作成します。トラッキング リストはスタティック ルートに適用され、定義されたネクスト ホップ間のパフォーマンスをモニタします。

始める前に

IP SLA モニタリング ポリシーを作成し、スタティック ルートでこのトラック メンバーが表すネクスト ホップの宛先 IP アドレスを知っている必要があります。

APIC GUI を使用して IP SLA トラック メンバーを設定するには、次の手順を実行します。

手順

ステップ 1 メニュー バーで、**[テナント（Tenants）]** > **[*tenant-name*]** をクリックします。

ステップ 2 [ナビゲーション（Navigation）] ペインで、[ポリシー（Policies）] を展開した後で、[プロトコル（Protocol）] を展開します。

ステップ 3 [IP SLA] を展開し、[トラック メンバー（Track Members）] を右クリックして [トラック メンバーの作成（Create Track Member）] を選択します。

ステップ 4 次のパラメータを設定します。

a) [名前（Name）] フィールドに、トラック メンバーの一意の名前を入力します。

b) [宛先 IP（Destination IP）] フィールドに、この設定が表すネクスト ホップの IP アドレスを入力します。

c) [トラックメンバーのスコープ（Scope of Track Member）] ドロップダウン リストで、このトラック メンバーが属する既存のブリッジ ドメインまたは外部ネットワークを選択します。

d) [IP SLA ポリシー（IP SLA Policy）] フィールドで、既存のを選択するか、モニタリング中に使用されるプローブを定義する新しい IP SLA モニタリング ポリシーを作成します。

ステップ 5 **[送信（Submit）]** をクリックします。`

次のタスク

上記の手順を繰り返して、モニタするスタティック ルートに必要な数のトラック メンバーを作成します。すべてのトラック メンバーを設定したら、トラック リストを作成して追加します。

GUI を使用した IP SLA トラック リストの設定

このタスクを使用して、スタティック ルートのネクスト ホップを表すトラック メンバーのグループを定義する IP SLA トラック リストを作成します。トラッキング リストはスタティック ルートに適用され、定義されたネクスト ホップ間のパフォーマンスをモニタします。

始める前に

1 つ以上の IP SLA トラック メンバーを作成しておく必要があります。

APIC GUI を使用して IP SLA トラック リストを設定するには、次の手順を実行します。

手順

ステップ 1 メニュー バーで、**[テナント（Tenants）]** > **[*tenant-name*]** をクリックします。

ステップ 2 [ナビゲーション（Navigation）] ペインで、[ポリシー（Policies）] を展開した後で、[プロトコル（Protocol）] を展開します。

ステップ 3 [IP SLA] を展開し、[トラック リスト（Track Lists）] を右クリックして [トラック リストの作成（Create Track List）] を選択します。

[**テナントの作成（Create Tenant**）] ダイアログ ボックスが表示されます。

ステップ 4 次のパラメータを設定します。

a) [名前（Name）] フィールドに、トラック リストの一意の名前を入力します。

b) ルートの可用性をアップまたはダウンしているトラック メンバーのパーセンテージに基づいて設定する場合は、[トラック リストのタイプ（Type of Track List）] フィールドで、[しきい値パーセンテージ（Threshold percentage）] を選択します。ルートの可用性が各トラック メンバーに割り当てられた重み値に基づいている場合は、[しきい値の重み（Threshold weight）] を選択します。

c) メンバー リストを追跡する [トラック メンバー関係のトラック リスト（Track list to track member relation）] テーブルで、テーブル ヘッドの [+] アイコンをクリックして、トラック メンバーをリストに追加します。既存のトラック メンバーを選択し、[トラック リストのタイプ（Type of Track List）] が [しきい値の重み（Threshold weight）] の場合は、重み値を割り当てます。

ステップ 5 **[送信（Submit）]** をクリックします。`

次のタスク

スタティック ルートまたはネクスト ホップ IP アドレスにトラック リストを関連付けます。

GUI を使用したスタティック ルートとトラック リストの関連付け

このタスクを使用して、トラック リストを設定済みのスタティック ルートに関連付け、システムが一連のネクスト ホップのパフォーマンスをモニタできるようにします。

（注） 次のタスクは、スタティック ルートのネクスト ホップ設定がすでに存在することを前提としています。

始める前に

スタティック ルートが設定されたルーテッド ネットワークが使用可能である必要があります。設定済みのトラック リストも使用できる必要があります。

APIC GUI を使用して IP SLA トラック リストをスタティック ルートに関連付けるには、次の手順を実行します。

手順

ステップ 1 メニュー バーで、**[テナント（Tenants）] > [*tenant-name*]** をクリックします。

ステップ 2 [ナビゲーション（Navigation）] ペインで、[**ネットワーキング（Networking**）]、[**L3Outs**] の順に展開します。

ステップ 3 設定済みのルーテッド ネットワーク（名前）、[論理ノード プロファイル（Logical Node Profiles）]、設定済みの論理ノードプロファイル（名前）、および[設定済みノード（Configured Nodes）] を展開します。

ステップ 4 設定済みのノード（名前）をクリックします。

[ノード関連付け（Node Association）] 作業ペインが表示されます。

ステップ 5 [スタティック ルート（Static Routes）] テーブルで、トラック リストを追加するルート エントリをダブルクリックします。

[**スタティック ルート（Static Route**）] ダイアログ ボックスが表示されます。

ステップ 6 [トラック ポリシー（Track Policy）] ドロップダウン リストで、このスタティック ルートに関連付ける IP SLA トラック リストを選択または作成します。

ステップ 7 **[送信（Submit）]** をクリックします。`

ステップ 8 [ポリシー使用の警告（Policy Usage Warning）] ダイアログが表示されます。

ステップ 9 この変更がこのスタティック ルートを使用する他のノードまたはポリシーに影響を与えないことを確認し、[変更の送信（Submit Changes）] をクリックします。

GUIを使用した、トラックリストとネクストホッププロファイルの関連付け

このタスクを使用して、トラック リストを設定済みのスタティック ルートのネクスト ホップ プロファイルに関連付けると、システムがネクストホップのパフォーマンスをモニタできるようにします。

始める前に

スタティック ルートとネクスト ホップ プロファイルが設定されたルーテッド ネットワークが使用可能である必要があります。

APIC GUI を使用して IP SLA トラック リストをネクスト ホップ プロファイルに関連付けるには、次の手順を実行します。

手順

ステップ 1 メニュー バーで、**[テナント（Tenants）]** > **[*tenant-name*]** をクリックします。

ステップ 2 [ナビゲーション（Navigation）] ペインで、[**ネットワーキング（Networking）**]、[**L3Outs**] の順に展開します。

ステップ 3 設定済みのルーテッド ネットワーク（名前）、[論理ノード プロファイル（Logical Node Profiles）]、設定済みの論理ノードプロファイル（名前）、および[設定済みノード（Configured Nodes）] を展開します。

ステップ 4 設定済みのノード（名前）をクリックします。

[ノード関連付け（Node Association）] 作業ペインが表示されます。

ステップ 5 [スタティック ルート（Static Routes）] テーブルで、トラック リストを追加するルート エントリをダブルクリックします。

[**スタティック ルート（Static Route**）] ダイアログ ボックスが表示されます。

ステップ 6 [ネクスト ホップ アドレス（Next Hop Addresses）] テーブルで、トラック リストを追加するネクスト ホップ エントリをダブルクリックします。

[ネクスト ホップ プロファイル（Next Hop Profile）] ダイアログが表示されます。

ステップ 7 [トラック ポリシー（Track Policy）] ドロップダウン リストで、このスタティック ルートに関連付ける IP SLA トラック リストを選択または作成します。

（注） IP SLA ポリシーをネクスト ホップ プロファイルに追加すると、トラック メンバーとトラック リストが自動的に作成され、プロファイルに関連付けられます。

ステップ 8 **[送信（Submit）]** をクリックします。`

ステップ 9 [ポリシー使用の警告（Policy Usage Warning）] ダイアログが表示されます。

ステップ 10 この変更がこのスタティック ルートを使用する他のノードまたはポリシーに影響を与えないことを確認し、[変更の送信（Submit Changes）] をクリックします。

ACI IP SLA モニタリング情報の確認

ここでは、IP SLA 統計情報、トラック リスト、トラック メンバー、および関連するスタティック ルートを表示するために必要なタスクについて説明します。

- GUI を使用した ACI IP SLA プローブ統計情報の表示
- CLI を使用したトラック リストおよびトラック メンバー ステータスの表示

GUI を使用した IP SLA プローブ統計情報の確認

ACI IP SLA は、次のリアルタイム統計情報を生成します。

ICMP

- ICMP エコー ラウンド トリップ時間（ミリ秒）
- 失敗した ICMP エコー プローブ（パケット）の数
- 成功した ICMP エコー プローブ（パケット）の数
- 伝送した ICMP エコー プローブ（パケット）の数

[TCP]

- 失敗した TCP 接続プローブ（パケット）の数
- 成功した TCP 接続プローブ（パケット）の数
- 伝送した TCP 接続プローブ（パケット）の数
- TCP 接続ラウンド トリップ時間（ミリ秒）

このタスクを使用して、現在スタティック ルートまたはネクスト ホップをモニタしている IP SLA トラック リストまたはメンバーの統計情報を表示します。

始める前に

統計情報を表示する前に、IP SLA トラック リストを作成し、スタティック ルートに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）]** > **[*tenant-name*]** をクリックします。

ステップ 2 [ナビゲーション（Navigation）] セクションで、[ポリシー（Policies）] を展開した後で、[プロトコル（Protocol）] を展開します。

ステップ 3 [IP SLA] を展開し、[トラック メンバー（Track Members）] または [トラック リスト（Track Lists）] を展開します。

ステップ 4 表示する既存のトラック メンバーまたはトラック リストをクリックします。

ステップ 5 [Stats] タブをクリックします。

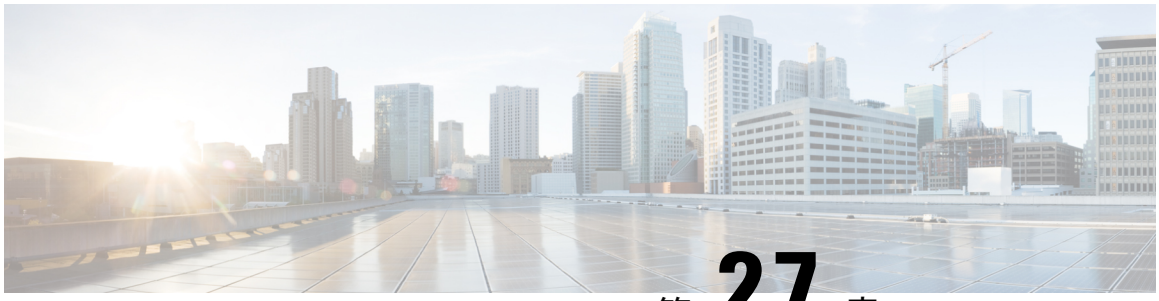
ステップ 6 [統計情報の選択（Select Stats）] アイコンをクリックして、表示するプローブ統計タイプを選択します。

ステップ 7 プローブ統計タイプを選択し（選択した統計タイプは青色で強調表示されます）、矢印アイコンで [使用可能（Available）] から [選択済み（Selected）] に移動します。反対の矢印アイコンを使用して、プローブ統計タイプを [選択済み（Selected）] から [使用可能（Available）] に戻すことができます。

ステップ 8 表示するプローブ統計タイプの選択が終了したら、[送信（Submit）] をクリックします。

次のタスク

このタスクで選択された統計情報は、グラフの上の凡例に表示されます。カウンタが累積し始めると、選択したプローブ統計タイプを表す線がグラフに表示されます。



第 27 章

HSRP

この章は、次の項で構成されています。

HSRP について

HSRP はファーストホップ冗長プロトコル（FHRP）であり、ファーストホップ IP ルータの透過的なフェールオーバーを可能にします。HSRP は、デフォルト ルータの IP アドレスを指定して設定された、イーサネット ネットワーク上の IP ホストにファーストホップ ルーティングの冗長性を提供します。ルータ グループでは HSRP を使用して、アクティブ ルータおよびスタンバイ ルータを選択します。ルータ グループでは、アクティブ ルータはパケットをルーティングするルータであり、スタンバイ ルータはアクティブ ルータに障害が発生したときや、プリセット条件に達したときに使用されるルータです。

大部分のホストの実装では、ダイナミックなルータ ディスカバリ メカニズムをサポートしていませんが、デフォルトのルータを設定することはできます。すべてのホスト上でダイナミックなルータ ディスカバリ メカニズムを実行するのは、管理上のオーバーヘッド、処理上のオーバーヘッド、セキュリティ上の問題など、さまざまな理由で現実的ではありません。HSRP は、そうしたホストにフェールオーバー サービスを提供します。

HSRP を使用するとき、ホストのデフォルト ルータとして HSRP 仮想 IP アドレスを設定します（実際のルータ IP アドレスの代わりに）。仮想 IP アドレスは、HSRP が動作するルータのグループで共有される IPv4 または IPv6 アドレスです。

ネットワーク セグメントに HSRP を設定する場合は、HSRP グループ用の仮想 MAC アドレスと仮想 IP アドレスを設定します。グループの各 HSRP 対応インターフェイス上で、同じ仮想アドレスを指定します。各インターフェイス上で、実アドレスとして機能する固有の IP アドレスおよび MAC アドレスも設定します。HSRP はこれらのインターフェイスのうちの 1 つを

アクティブ ルータにするために選択します。アクティブ ルータは、グループの仮想 MAC アドレス宛てのパケットを受信してルーティングします。

指定されたアクティブ ルータで障害が発生すると、HSRP によって検出されます。その時点で、選択されたスタンバイ ルータが HSRP グループの MAC アドレスおよび IP アドレスの制御を行うことになります。HSRP はこの時点で、新しいスタンバイ ルータの選択も行います。

HSRP ではプライオリティ指示子を使用して、デフォルトのアクティブ ルータにする HSRP 設定インターフェイスを決定します。アクティブ ルータとしてインターフェイスを設定するには、グループ内の他のすべての HSRP 設定インターフェイスよりも高いプライオリティを与えます。デフォルトのプライオリティは 100 なので、それよりもプライオリティが高いインターフェイスを 1 つ設定すると、そのインターフェイスがデフォルトのアクティブ ルータになります。

HSRP が動作するインターフェイスは、マルチキャスト ユーザ データグラム プロトコル（UDP）ベースの hello メッセージを送受信して、障害を検出し、アクティブおよびスタンバイ ルータを指定します。アクティブ ルータが設定された時間内に hello メッセージを送信できなかった場合は、最高のプライオリティのスタンバイ ルータがアクティブ ルータになります。アクティブ ルータとスタンバイ ルータ間のパケット フォワーディング機能の移動は、ネットワーク上のすべてのホストに対して完全に透過的です。

1 つのインターフェイス上で複数の HSRP グループを設定できます。仮想ルータは物理的には存在しませんが、相互にバックアップするように設定されたインターフェイスにとって、共通のデフォルト ルータになります。アクティブ ルータの IP アドレスを使用して、LAN 上でホストを設定する必要はありません。代わりに、仮想ルータの IP アドレス（仮想 IP アドレス）をホストのデフォルト ルータとして設定します。アクティブ ルータが設定時間内に hello メッセージを送信できなかった場合は、スタンバイ ルータが引き継いで仮想アドレスに応答し、アクティブ ルータになってアクティブ ルータの役割を引き受けます。ホストの観点からは、仮想ルータは同じままです。

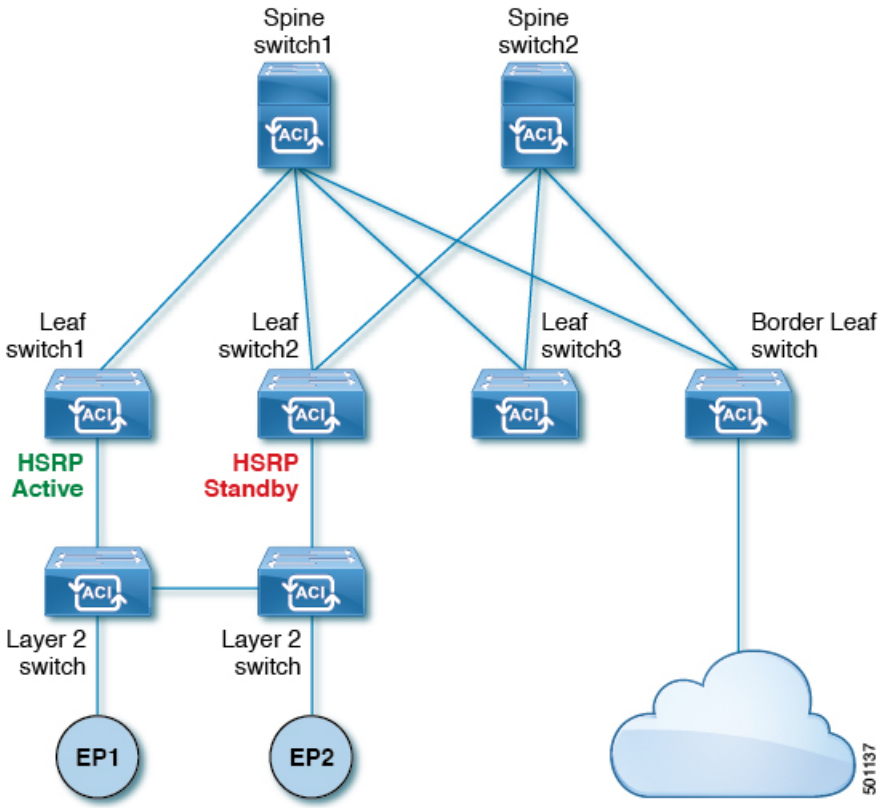
（注） ルーテッド ポートで受信した HSRP 仮想 IP アドレス宛のパケットは、ローカル ルータ上で終端します。そのルータがアクティブ HSRP ルータであるのかスタンバイ HSRP ルータであるのかは関係ありません。このプロセスには ping トラフィックと Telnet トラフィックが含まれます。レイヤ 2（VLAN）インターフェイスで受信した HSRP 仮想 IP アドレス宛のパケットは、アクティブ ルータ上で終端します。

Cisco APIC と HSRP について

Cisco ACI の HSRP は、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でのみサポートされます。したがって HSRP は、レイヤ 3 Out でのみ設定できます。レイヤ 2 接続は、HSRP を実行している ACI リーフ スイッチ間のレイヤ 2 スイッチなどの外部デバイスから提供される必要があります。HSRP は外部レイヤ 2 接続上で Hello メッセージを交換するリーフ スイッチ上で動作するからです。HSRP の hello メッセージは、スパイン スイッチではパス スルーされません。

次に示すのは、Cisco APIC での HSRP の導入のトポロジの例です。

図 *62 : HSRP* の配置トポロジ



HSRP のバージョン

Cisco APICは、デフォルトで HSRP バージョン 1 をサポートします。HSRP バージョン 2 を使用するようにインターフェイスを設定できます。

HSRP バージョン 2 では、HSRP バージョン 1 から次のように拡張されています。

- グループ番号の範囲が拡大されました。HSRP バージョン 1 がサポートするグループ番号は 0 ～ 255 です。HSRP バージョン 2 がサポートするグループ番号は 0 ～ 4095 です。
- IPv4 では、HSRP バージョン 1 で使用する IP マルチキャスト アドレス 224.0.0.2 の代わりに、IPv4 マルチキャスト アドレス 224.0.0.102 または IPv6 マルチキャスト アドレス FF02::66 を使用して hello パケットを送信します。
- IPv4 では 0000.0C9F.F000 ～ 0000.0C9F.FFFF、IPv6 アドレスでは 0005.73A0.0000 ～ 0005.73A0.0FFF の MAC アドレス範囲を使用します。HSRP バージョン 1 で使用する MAC アドレス範囲は、0000.0C07.AC00 ～ 0000.0C07.ACFF です。

注意事項と制約事項

次の注意事項と制約事項に従ってください。

- HSRP 状態は、HSRP IPv4 および IPv6 の両方で同じである必要があります。フェールオーバー後に同じ状態になるようにするには、プライオリティとプリエンプションを設定する必要があります。
- 現在、1 個の IPv4 と 1 個の IPv6 グループのみが Cisco ACI の同じサブインターフェイスでサポートされています。デュアル スタックが設定されている場合でも、仮想 MAC は IPv4 および IPv6 HSRP の設定で同じである必要があります。
- HSRP ピアに接続しているネットワークが純粋なレイヤ 2 ネットワークである場合、BFD IPv4 および IPv6 がサポートされています。リーフ スイッチでは、別のルータの MAC アドレスを設定する必要があります。BFD セッションは、リーフ インターフェイスで異なる MAC アドレスを設定する場合にのみアクティブになります。
- ユーザーは、デュアル スタック設定の IPv4 および IPv6 HSRP グループに同じ MAC アドレスを設定する必要があります。
- HSRP VIP はインターフェイス IP と同じサブネット内にある必要があります。
- HSRP 設定のインターフェイス遅延を設定することをお勧めします。
- HSRP は、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でのみサポートされます。HSRP は、VLAN インターフェイスおよびスイッチ済み仮想インターフェイス（SVI）ではサポートされていません。したがって、HSRP の VPC サポートは使用できません。
- HSRP のオブジェクト トラッキングはサポートされていません。
- SNMP の HSRP 管理情報ベース（MIB）はサポートされません。
- HSRP では、複数グループの最適化（MGO） はサポートされていません。
- ICMP IPv4 および IPv6 のリダイレクトはサポートされていません。
- Cold Standby および Non-Stop Forwarding（NSF）は、Cisco ACI 環境で再起動できないためサポートされていません。
- HSRP はリーフ スイッチでのみサポートされているため、拡張ホールドダウン タイマーのサポートはありません。HSRP はスパイン スイッチでサポートされていません。
- APIC 内では、HSRP のバージョン変更はサポートされていません。設定を削除し、新しいバージョンを再設定する必要があります。
- HSRP バージョン 2 は HSRP バージョン 1 と相互運用できません。どちらのバージョンも相互に排他的なので、インターフェイスはバージョン 1 およびバージョン 2 の両方を運用できません。しかし、同一ルータの異なる物理インターフェイス上であれば、異なるバージョンを実行できます。

- ルート セグメンテーションは、HSRP がインターフェイスでアクティブな場合、Cisco Nexus 93128TX、Cisco Nexus 9396PX、および Cisco Nexus 9396TX リーフ スイッチでプログラムされています。したがって、インターフェイスでルート パケットに実施する DMAC=router MAC チェックはありません。この制限は、Cisco Nexus 93180LC EX、Cisco Nexus 93180YC-EX、Cisco Nexus 93108TC EX リーフ スイッチには適用されません。
- HSRP 設定は、基本的な GUI モードではサポートされていません。APIC リリース 3.0 (1) 以降、基本的な GUI モードが廃止されました。
- ファブリックからレイヤ 3 アウト トラフィックは、状態に関係なく HSRP リーフ スイッチ全体で常にロード バランスします。HSRP リーフ スイッチが複数のポッドにわたる場合、ファブリックからアウト トラフィックは同じポッドで常にリーフ スイッチを使用します。
- この制限は、以前の Cisco Nexus 93128TX、Cisco Nexus 9396PX と Cisco Nexus 9396TX スイッチの一部に適用されます。HSRP を使用すると、レイヤ 2 の外部デバイスのフラッピングを防ぐため、ルーテッド インターフェイスまたはルーテッド サブインターフェイスの MAC アドレスを 1 個変更する必要があります。これは、インターフェイス論理プロファイルの下で論理インターフェイスごとに Cisco APIC が同じ MAC アドレス（00:22:BD:F8:19:FF）を割り当てるためです。

デフォルトの HSRP 設定

パラメータ	デフォルト値
Version	1
Delay	0
Reload Delay	0
Interface Control	No 使用-焼き込みアドレス (BIA)
Group ID	0
Group Af	IPv4
IP Obtain Mode	admin
プライオリティ	100
Hello Interval	3000 ミリ秒
Hold Interval	10000 ミリ秒
Group Control	プリエンプションは無効
Preempt Delay	0

パラメータ	デフォルト値
Authentication Type	プレーン テキスト
Authentication Key Timeout	0
VMAC	導出方法 (HSRP グループ Id)

GUI を使用した HSRP の設定

リーフ スイッチが設定されている場合、HSRP が有効になっています。

始める前に

- テナントと VRF が設定されています。
- VLAN プールは、適切な VLAN 範囲が定義され、レイヤ 3 ドメインが作成されて VLAN プールに接続されている状態で設定される必要があります。
- エンティティ プロファイルの接続も、レイヤ3 ドメインに関連付けられている必要があります。
- リーフ スイッチのインターフェイス プロファイルは必要に応じて設定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]** > **[Tenant-name]** をクリックします。**[ナビゲーション（Navigation）]** ペインで、**[ネットワーキング（Networking）]** > **L3Outs** > ***L3Out_name*** > **[論理ノード プロファイル（Logical Node Profiles）]** > **[論理インターフェイス プロファイル（Logical Interface Profile）]** をクリックします。

ここで、HSRP インターフェイス プロファイルが作成されます。

ステップ 2 論理インターフェイス プロファイルを選択し、**Create HSRP Interface Profile** をクリックします。

ステップ 3 **Create HSRPInterface Profile** ダイアログボックスで、次の操作を実行します。

a) **Version** フィールドで、該当するバージョンを選択します。
b) **HSRP Interface Policy** フィールドで、ドロップダウンから **Create HSRP Interface Policy** を選択します。
c) **Create HSRP Interface Policy** ダイアログボックスの **Name** フィールドに、ポリシーの名前を入力します。
d) **Control** フィールドで、該当するコントロールを選択します。

e) **Delay** フィールドと **Reload Delay** フィールドで、該当する値を設定します。**Submit** をクリックします。

HSRPインターフェイスポリシーが作成され、インターフェイスプロファイルに関連付けられます。

ステップ 4 **Create HSRP Interface Profile** ダイアログボックスで、 **HSRP Interface Groups** を展開します。

ステップ 5 **Create HSRP Group Profile** ダイアログボックスで、次の操作を実行します。

a) **Name**フィールドに、HSRP インターフェイスのグループ名を入力します。

b) **Group ID** フィールドで、適切な ID を選択します

使用可能な値は、HSRP バージョン 1 または 2 のバージョンのいずれがインターフェイスプロファイルに選択されたかに応じて異なります。

c) **IP** フィールドに、IP アドレスを入力します。

この IP アドレスはインターフェイスと同じサブネット内になければなりません。

d) **MAC Address** フィールドに、Mac アドレスを入力します。

（注） このフィールドを空白のままにすると、HSRP 仮想 MAC アドレスはグループ ID に基づいて自動的に計算されます。

e) [グループ名（Group Name）] フィールドにグループ名を入力します。

これは、HSRP MGO 機能の HSRP により、プロトコルで使用する名前です。

f) **Group Type** フィールドで、該当するタイプを選択します。

g) **IP Obtain Mode** フィールドで、該当するモードを選択します。

h) **HSRP Interface Policy** フィールドで、ドロップダウンから **Create HSRP Interface Policy** を選択します。

ステップ 6 **Create HSRP Group Policy** ダイアログボックスで、次の操作を実行します。

a) **Name** フィールドに、HSRP グループポリシーの名前を入力します。

b) **Key or Password** フィールドが自動的に設定されます。

認証タイプのデフォルト値はシンプルで、キーは、「cisco」です。これはユーザーが新規ポリシーを作成するときに、デフォルトで選択されます。

c) **Type** フィールドで、必要とするセキュリティのレベルを選択します。

d) **Priority** フィールドで、アクティブ ルータとスタンバイ ルータを定義する優先度を選択します。

e) 残りのフィールドで、該当する値を選択し、**Submit** をクリックします。
HSRP グループ ポリシーが作成されます。

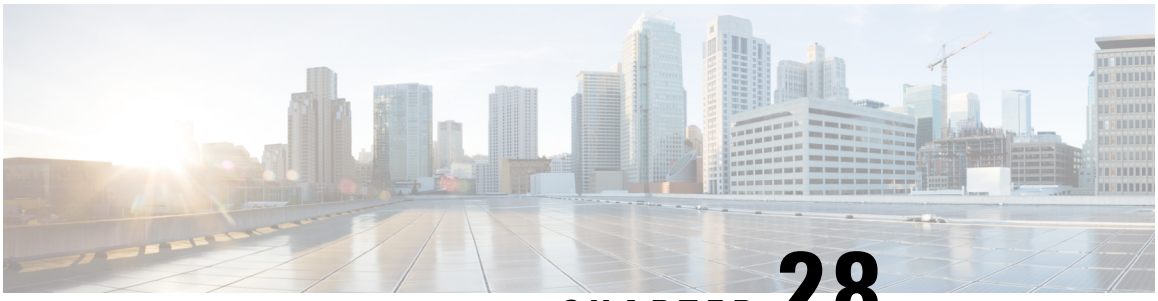
f) **Secondary Virtual IPs** フィールドに自動記入することにより、セカンダリ バーチャル IP を作成します。

これは、セカンダリ バーチャル IP で各サブインターフェイスで HSRP を有効にするために使用できます。また、ここで指定する IP アドレスは、インターフェイスのサブネットになければなりません。

g) **OK** をクリックします。

ステップ 7 **Create HSRP Interface Profile** ダイアログボックスで、**Submit** をクリックします。
これで HSRP の設定は完了です。

ステップ 8 [ナビゲーション]ペインで、作成した HSRP インターフェイスとグループ ポリシーを確認するには、**[ネットワーキング（Networking）]** > **[プロトコル ポリシー（Protocol Policies）]** > **[HSRP]** をクリックします。



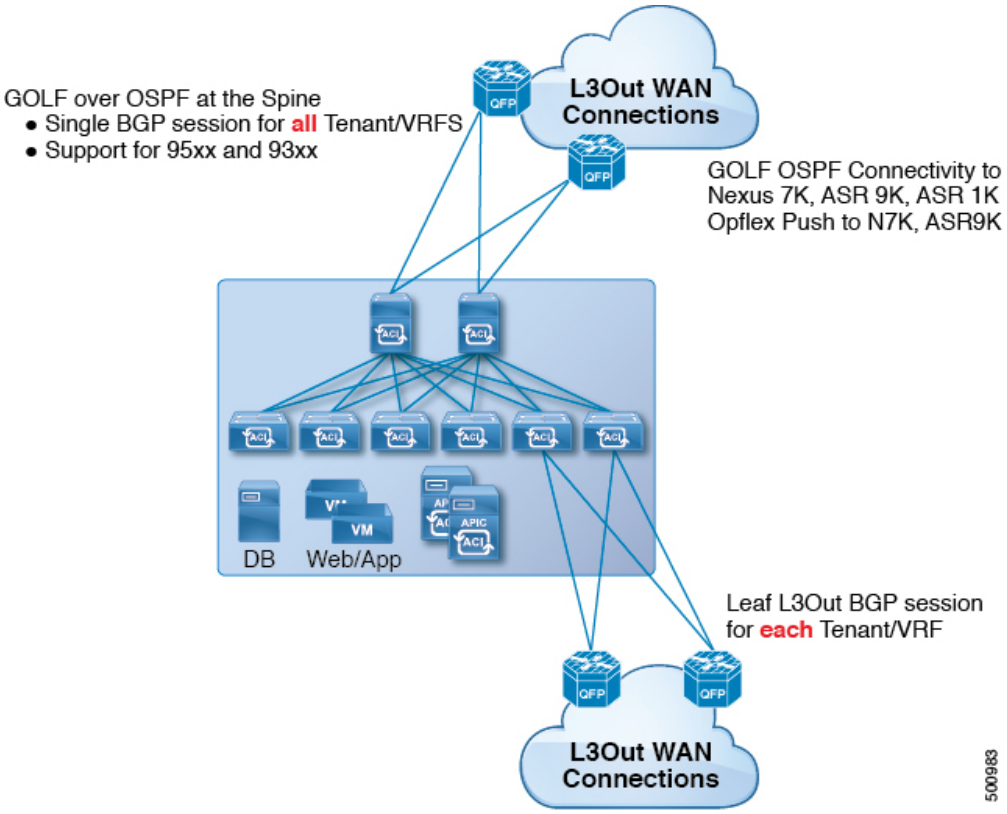
CHAPTER 28

Cisco ACI GOLF

Cisco ACI GOLF

Cisco ACI GOLF 機能 (ファブリック WAN のレイヤ 3 EVPN サービス機能とも呼ばれる) では、より効率的かつスケーラブルな ACI ファブリック WAN 接続が可能になります。スパイン スイッチに接続されている WAN に OSPF 経由で BGP EVPN プロトコルが使用されます。

図 *63 : Cisco ACI GOLF* のトポロジ



すべてのテナント WAN 接続が、WAN ルータが接続されたスパイン スイッチ上で単一のセッションを使用します。データセンター相互接続ゲートウェイ（DCIG）へのテナント BGP セッションのこの集約では、テナント BGP セッションの数と、それらすべてに必要な設定の量を低減することによって、コントロールプレーンのスケールが向上します。ネットワークは、スパイン ファブリック ポートに設定された レイヤ 3 サブインターフェイスを使用して拡張されます。GOLF を使用した、共有サービスを伴うトランジット ルーティングはサポートされていません。

スパイン スイッチでの GOLF 物理接続のためのレイヤ 3 外部外側ネットワーク (`L3extOut`) は、`infra` テナントの下で指定され、次のものを含みます:

- `LNodeP` (infra テナントの L3Out では、`l3extInstP` は必要ありません)。
- infra テナントの GOLF 用の `L3extOut` のプロバイダ ラベル。
- OSPF プロトコル ポリシー
- BGP プロトコル ポリシー

すべての通常テナントが、上記で定義した物理接続を使用します。通常のテナントで定義した `L3extOut` では、次が必要です:

- サブネットとコントラクトを持つ l3extInstP (EPG)。サブネットの範囲を使用して、ルート制御ポリシーとセキュリティポリシーのインポートまたはエクスポートを制御します。ブリッジドメインサブネットは外部的にアドバタイズするように設定される必要があり、アプリケーション EPG および GOLF L3Out EPG と同じ VRF に存在する必要があります。
- アプリケーション EPG と GOLF L3Out EPG の間の通信は、(契約優先グループではなく) 明示的な契約によって制御されます。
- l3extConsLbl コンシューマ ラベル。これは infra テナントの GOLF 用の L3Out の同じプロバイダ ラベルと一致している必要があります。ラベルを一致させることにより、他のテナント内のアプリケーション EPG が LNodeP 外部 L3Out EPG を利用することが可能になります。
- infra テナント内のマッチング プロバイダ L3extOut の BGP EVPN セッションは、この L3Out で定義されたテナント ルートをアドバタイズします。

に関する注意事項と制限事項 Cisco ACI GOLF

次に示す Cisco ACI GOLF のガイドラインおよび制限事項に従ってください。

- GOLF は共有サービスをサポートしていません。
- GOLF はトランジット ルーティングをサポートしていません。
- GOLF ルータは、トラフィックを受け入れるために少なくとも 1 つのルートを Cisco Application Centric Infrastructure（ACI）にアドバタイズする必要があります。Cisco ACI が外部ルータからルートを受信するまで、リーフ スイッチと外部ルータの間にトンネルは作成されません。
- すべての Cisco Nexus 9000 シリーズ Cisco ACI モードのスイッチと、すべての Cisco Nexus 9500 プラットフォーム Cisco ACI モード スイッチライン カードおよびファブリック モジュールが GOLF をサポートします。Cisco APIC、リリース 3.1(x) 以降では、これに N9K-C9364C スイッチが含まれます。
- 現時点では、ファブリック全体のスパイン スイッチインターフェイスに展開できるのは、単一の GOLF プロバイダ ポリシーだけです。
- Cisco APIC リリース 2.0(2) まで、GOLF は Cisco ACI マルチポッド でサポートされていません。リリース 2.0 (2) では、同じファブリックでの 2 つの機能を、スイッチ名の末尾に「EX」のない Cisco Nexus N9000K スイッチ上でのみサポートしています。たとえば N9K-9312TX です。2.1(1) リリース以降では、2 つの機能を、Cisco ACI マルチポッド およびEVPN トポロジで使用されているすべてのスイッチでともに展開できるようになりました。
- スパイン スイッチで GOLF を設定する場合、コントロール プレーンがコンバージするまでは、別のスパイン スイッチで GOLF の設定を行わないでください。
- スパイン スイッチは複数のプロバイダの GOLF 外側ネットワーク (GOLF L3Outs) に追加できますが、GOLF L3Out ごとのプロバイダ ラベルは異なっている必要があります。ま

た、この例では、OSPFエリアもL3extOutごとに異なっていて、異なるループバックアドレスを使用する必要があります。

- infraテナント内のマッチングプロバイダL3OutのBGP EVPNセッションは、このL3extOutで定義されたテナントルートをアドバタイズします。
- 3つのGOLF Outsを展開する場合、1つだけがGOLFのプロバイダ/コンシューマラベルを持っていて、どれも集約をエクスポートしないなら、Cisco APICはすべてのルートをエクスポートします。これは、テナントのリーフスイッチ上の既存のL3extOutと同じです。
- VRFインスタンスにSPAN接続先があるERSPANセッションがあり、VRFインスタンスでGOLFが有効になっており、ERSPAN送信元にスパインスイッチ上のインターフェイスがある場合、トランジットプレフィックスは非GOLF L3Outから間違ったBGPネクストホップでGOLFルータに送信されます。
- スパインスイッチとデータセンター相互接続（DCI）ルータ間に直接ピアリングがある場合、リーフスイッチからASRへのトランジットルートには、リーフスイッチのPTEPとして次のホップが存在することになります。この場合、そのCisco ACIポッドのTEP範囲に対してASRの静的ルートを定義します。また、DCIが同じポッドにデュアルホーム接続されている場合は、静的ルートの優先順位（管理距離）は、他のリンクを通じて受信するルートと同じである必要があります。
- デフォルトの bgpPeerPfxPol ポリシーは、ルートを20,000に制限しています。Cisco ACI WANインターコネクトピアの場合には、必要に応じてこれを増やしてください。
- 1つのスパインスイッチ上に2つのL3extOutが存在し、そのうちの一方のプロバイダラベルがprov1でDCI 1とピアリングしており、もう一方のL3extOutのプロバイダラベルがprov2でDCI 2とピアリングしているという、展開シナリオを考えます。テナントVRFインスタンスに、プロバイダラベルのいずれか一方(prov1またはprov2)をポイントしているコンシューマラベルがある場合、テナントルートはDCI 1とDCI 2の両方に送信されます。
- GOLF OpFlex VRFインスタンスを集約する場合、Cisco ACIファブリック内、またはGOLF OpFlex VRFインスタンスとシステム内のその他のVRFインスタンス間のGOLFデバイスでは、ルートのリーキングは発生しません。VRFリーキングのためには、(GOLFルータではなく)外部デバイスを使用する必要があります。

（注） Cisco ACI は IP フラグメンテーションをサポートしていません。したがって、外部ルータへのレイヤ 3 Outside（L3Out）接続、または Inter-Pod Network（IPN）を介した マルチポッド 接続を設定する場合は、インターフェイス MTU がリンクの両端で適切に設定されていることが推奨されます。Cisco ACI、 Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定可能な MTU 値はイーサネット ヘッダー (一致する IP MTU、14-18 イーサネット ヘッダー サイズを除く) を考慮していません。また、IOS XR などの他のプラットフォームには、設定された MTU 値にイーサネット ヘッダーが含まれています。設定された値が 9000 の場合、Cisco ACI、Cisco NX-OS Cisco IOS の最大 IP パケット サイズは 9000 バイトになりますが、IOS-XR のタグなしインターフェイスの最大 IP パケットサイズは 8986 バイトになります。

各プラットフォームの適切な MTU 値については、それぞれの設定ガイドを参照してください。

CLI ベースのコマンドを使用して MTU をテストすることを強く推奨します。たとえば、Cisco NX-OS CLI で `ping 1.1.1.1 df-bit packet-size 9000 source-interface ethernet 1/1` などのコマンドを使用します。

複数のサイトで共有 APIC ゴルフ接続

トポロジでは、複数のサイト、APIC サイトの拡大 Vrf は、ゴルフ接続を共有している場合、リスクのクロス VRF トラフィックの問題を回避する次のガイドラインに従います。

スパイン スイッチと、DCI の間でルート ターゲットの設定

ゴルフ Vrf の EVPN ルート ターゲット (RTs) を設定する 2 つの方法があります: 手動 RT と自動 RT. ルート ターゲットは、ACI 背表紙と OpFlex を介して DCIs の間で同期されます。ゴルフ Vrf の自動 RT は、形式に組み込まれて Fabric ID: – *ASN* : [*FabricID*] *VNID*

2 つのサイトには、次の図のように導入の Vrf がある、Vrf 間のトラフィックを混在させることができます。

サイト 1	サイト 2
ASN: 100、ファブリック ID: 1	ASN: 100、ファブリック ID: 1
VRF A：VNID 1000 インポート/エクスポート ルート ターゲット：100：[1] 1000	VRF A：VNID 2000 インポート/エクスポート ルート ターゲット：100：[1] 2000
VRF B：VNID 2000 インポート/エクスポート ルート ターゲット：100：[1] 2000	VRF B：VNID 1000 インポート/エクスポート ルート ターゲット：100：[1] 1000

Dci のために必要なルート マップ

トンネルは、中継ルートは、[DCI を介してリークとサイト間では作成されません、ため、コントロール プレーンの手間をも削減する必要があります。もう 1 つのサイトでゴルフ スパインに、DCI への 1 つのサイトでゴルフ スパインから送信される EVPN タイプ 5 およびタイプ 2 ルートを送信できませんする必要があります。これが発生スパイン スイッチに dci のために次のタイプの BGP セッションが必要がある場合。

Site1: IBGP--DCI--EBGP--サイト 2

Site1: EBGP--DCI--IBGP--サイト 2

Site1:--DCI--EBGP EBGP--サイト 2

Site1: IBGP RR クライアント--DCI (RR)----IBGP サイト 2

Dciのためにこの問題を避けるためには、ルートマップは、インバウンドおよびアウトバウンドのピア ポリシーのさまざまな BGP コミュニティで使用されます。

ルートを 1 つのサイト、もう 1 つのサイト フィルタ着信ピア ポリシーでコミュニティに基づくルートでゴルフ スパインへのアウト バウンド ピア ポリシー ゴルフ スパインから受信します。別のアウト バウンド ピア ポリシーは、WAN へコミュニティを取り除き。すべてのルート マップは、ピアのレベルでです。

GUI を使用した ACI GOLF の設定

次に、任意のテナント ネットワークが使用できるインフラ GOLF サービスを設定する手順について説明します。

手順

ステップ 1 メニュー バーで、をクリックして **テナント** 、] をクリックし、 **インフラ** を選択、テナントインフラ。

ステップ 2 [**ナビゲーション（Navigation**）] ペインで、**[ネットワー キング（Networking）]** オプションを展開し、次のアクションを行います。

a) [L3Outs] を右クリックし、[L3Out の作成（Create L3Out）] をクリックして、[L3Out の作成（Create L3Out）] ウィザードを開きます。

b) [名前（Name）]、[VRF]、および [L3 ドメイン（L3 Domain）] フィールドに必要な情報を入力します。

c) [用途：（Use For :）] フィールドで、[Golf] を選択します。

[プロバイダ ラベル（Provider Label）] フィールドと [ルート ターゲット（Route Target）] フィールドが表示されます。

d) [プロバイダ ラベル（Provider Label）]フィールドに、プロバイダ ラベル（たとえば、golf）を入力します。

e) **ルート ターゲット** フィールドで、自動または明示的なポリシーを持つ BGP ルート ターゲットをフィルタリング ポリシーを使用するかどうかを選択します。

- **自動** -自動 BGP ルート ターゲット Vrf でフィルタ リングは、これに関連付けられている実装は、外部設定をルーティングします。
- **明示的な** -ルート ターゲットの明示的にフィルタ リングの実装では、この設定の外部ルーティングに関連付けられている Vrf に BGP ルート ターゲット ポリシーが設定されています。

（注） 明示的なルート ターゲット ポリシーが設定されている、 **BGP ルート ターゲット プロファイル** テーブルで、 **BGP ページ** の **VRF ウィザードの作成** します。選択した場合、 **自動** オプションで **ルート ターゲット**] フィールドで明示ルート ターゲット ポリシーの設定、 **VRF ウィザードの作成** BGP ルーティングの中断を引き起こす可能性があります。

f) 残りのフィールドはそのままにして（BGP を選択するなど）、[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。

ステップ 3 [L3Out の作成（Create L3Out）] ウィザードの [ノードとインターフェイス（Nodes and Interfaces）] ウィンドウに必要な情報を入力します。

a) **[ノード ID]** ドロップダウン リストで、スパイン スイッチ ノード ID を選択します。
b) [Router ID] フィールドに、ルータ ID を入力します。
c) （任意） 必要に応じて、ループバック アドレスに別の IP アドレスを設定できます。

[ルータ ID（Router ID）] フィールドに入力したエントリと同じ内容が [ループバック アドレス（Loopback Address）] フィールドに自動で入力されます。これは以前のビルドでの [ループバック アドレスのルータ ID の使用（Use Router ID for Loopback Address）] と同等です。ループバックアドレスにルートIDを使用しない場合は、ループバックアドレスに別のIPアドレスを入力します。ループバック アドレスにルータ ID を使用しない場合は、このフィールドを空のままにします。

d) [外部コントロール ピア（External Control Peering）] フィールドはオンのままにします。
e) [ノードとインターフェイス（Nodes and Interfaces）] ウィンドウに追加の必要な情報を入力します。

このウィンドウに表示されるフィールドは、[レイヤ 3（Layer 3）] および [レイヤ 2（Layer 2）] 領域で選択したオプションによって異なります。

f) [ノードとインターフェイス（Nodes and Interfaces）] ウィンドウで残りの追加の情報を入力したら、[次（Next）] をクリックします。

[**プロトコル（Protocols**）] ウィンドウが表示されます。

ステップ 4 [L3Out の作成（Create L3Out）] ウィザードの [プロトコル（Protocols）] ウィンドウに必要な情報を入力します。

a) [BGP ループバック ポリシー（BGP Loopback Policies）] および [BGP インターフェイス ポリシー（BGP Interface Policies）] 領域で、次の情報を入力します。

- **ピア アドレス（Peer Address**）：ピア IP アドレスを入力します

- **EBGP Multihop TTL（EBGP マルチホップ TTL）**：接続の存続可能時間（TTL）を入力します。範囲は 1 ー 255 ホップです。ゼロの場合、TTL は指定されません。デフォルトは 0 です。
- **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、プレーン形式の 1 ー 4294967295 の 4 バイトにすることができます。

（注） ACI は asdot または asdot+ 形式の自律システム番号をサポートしません。

b) [**OSPF**] 領域で、デフォルト OSPF ポリシー、以前に作成した OSPF ポリシー、または [**OSPF インターフェイス ポリシーの作成（Create OSPF Interface Policy**）] を選択します。
c) **[次へ（Next）]** をクリックします。

[**外部 EPG（External EPG**）] ウィンドウが表示されます。

ステップ 5 [L3Out の作成（Create L3Out）] ウィザードで [外部 EPG（External EPG）] ウィンドウに必要な情報を入力します。

a) **Name** フィールドに、外部ネットワークの名前を入力します。
b) [**提供済みコントラクト（Provided Contract**）] フィールドで、提供済みコントラクトの名前を入力します。
c) [**消費済みコントラクト（Consumed Contract**）] フィールドで、消費済みコントラクトの名前を入力します。
d) [**すべてのサブネットを許可（Allow All Subnet**）] フィールドで、この L3Out 接続からのすべての中継ルートをアドバタイズしない場合はオフにします。

このボックスをオフにすると、[Subnets] 領域が表示されます。次の手順に従って、必要なサブネットとコントロールを指定します。

e) [完了（Finish）] をクリックして、[L3Out の作成（Create L3Out）] ウィザードに必要な設定の入力を完了させます。

ステップ 6 テナントの [**ナビゲーション（Navigation**）] ペインで、 ***tenant_name*** > **[ネットワー キング（Networking**）] > **L3Outs** を展開し、次のアクションを行います。

a) [L3Outs] を右クリックし、[L3Out の作成（Create L3Out）] をクリックしてウィザードを開きます。
b) [名前（Name）]、[VRF]、および [L3 ドメイン（L3 Domain）] フィールドに必要な情報を入力します。
c) [GOLF の使用（Use for GOLF）] フィールドの横にあるボックスをオンにします。
d) [ラベル（Label）] フィールドで、[コンシューマ（Consumer）] を選択します。
e) **[コンシューマ ラベル]** を割り当てます。この例では、（以前に作成した）*golf* を使用します。
f) [**次へ（Next**）] をクリックし、[**完了（Finish**）] をクリックします。

DCIG への BGP EVPN タイプ 2 ホスト ルートの分散化

DCIG への BGP EVPN タイプ 2 のホスト ルートの配信

APIC ではリリース 2.0(1f) まで、ファブリック コントロール プレーンは EVPN ホスト ルートを直接送信してはいませんでしたが、Data Center Interconnect Gateway（DCIG）にルーティングしている BGP EVPN タイプ 5（IP プレフィックス）形式のパブリック ドメイン（BD）サブネットをアドバタイズしていました。これにより、最適ではないトラフィックの転送となる可能性があります。転送を改善するため APIC リリース 2.1 x では、ファブリック スパインを有効にして、パブリック BD サブネットとともに DCIG に EVPN タイプ 2（MAC-IP）ホスト ルートを使用してホスト ルートをアドバタイズできます。

そのためには、次の手順を実行する必要があります。

1. BGP アドレス ファミリ コンテキスト ポリシーを設定する際に、ホスト ルート リークを有効にします。
2. GOLF セットアップで BGP EVPN へのホスト ルートをリークする場合：
    1. GOLF が有効になっている場合にホスト ルートを有効にするには、インフラストラクチャ テナント以外に、BPG アドレス ファミリ コンテキスト ポリシーがアプリケーション テナント（アプリケーション テナントはコンシューマ テナントであり、エンドポイントを BGP EVPN にリークします）で設定されている必要があります。
    2. 単一ポッド ファブリックについては、ホスト ルート機能は必要ありません。ホスト ルート機能は、マルチポッドファブリック セットアップで最適ではない転送を避けるために必要です。ただし、単一ポッドファブリックがセットアップされる場合、エンドポイントから BGP EVPN にリークするため、ファブリック外部接続ポリシーを設定し ETEP IP アドレスを提供する必要があります。そうしないと、ホスト ルートは、BGP EVPN にはリークされません。
3. VRF のプロパティを設定する場合：
    1. IPv4 および IPv6 の各アドレス ファミリの BGP コンテキストに BGP アドレス ファミリ コンテキスト ポリシーを追加します。
    2. VRF からインポートまたはエクスポート可能なルートを特定する BGP ルート ターゲット プロファイルを設定します。

GUI を使用して DCIG への BGP EVPN タイプ 2 のホスト ルートを分散する

次の手順で BGP EVPN タイプ 2 のホスト ルートの分散を有効にします。

始める前に

インフラ テナントでのACI の WAN 相互接続サービスをすでに設定しており、サービスを使用するテナントを設定している

手順

ステップ 1 メニュー バーで **[テナント（Tenants）]** > **[インフラ（infra）]** をクリックします。

ステップ 2 [ナビゲーション（Navigation）] ペインで、**[ポリシー（Policies）]** > **[プロトコル（Protocol）]** > **[BGP]**をクリックします。

ステップ 3 **BGP Address Family Context** を右クリックし、**Create BGP Address Family Context Policy** を選択し、次の手順を実行します:

a) ポリシーの名前を入力し、必要に応じて説明を追加します。

b) **Enable Host Route Leak** チェック ボックスをクリックします。

c) **Submit** をクリックします。

ステップ 4 **[テナント（Tenants）]** > **[tenant-name]**（BGP アドレス ファミリ コンテキスト ポリシーを使用するテナント）をクリックし、**[ネットワーキング（Networking）]** を展開します。

ステップ 5 **VRF** を展開し、分散するホスト ルートを含む VRF をクリックします。

ステップ 6 VRF のプロパティを設定するときには、**BGP Address Family Context Policy** を IPv4 と IPv6 の **BGP Context Per Address Families** に追加します。

ステップ 7 [Submit] をクリックします。

EVPN タイプ 2 ルート アドバタイズメントのトラブルシューティング

EVPN タイプ 2 ルート アドバタイズメントのトラブルシューティング

DCIG への EVPN タイプ 2 ルート配布のトラブルシューティング

EVPN トポロジでのトラフィック転送を最適化するために、ファブリック スパインを有効にして、BGP EVPN タイプ 5（IP プレフィックス）ルートの形式のパブリック BD サブネットとともに、EVPN タイプ 2（MAC-IP）ルートを使用してホスト ルートをデータセンター インターコネクト ゲートウェイ（DCIG）に配布できます。これは、HostLeak オブジェクトを使用して有効にします。ルート配布で問題が発生した場合は、このトピックの手順を使用してトラブルシューティングを行ってください。

手順

ステップ 1 スパイン スイッチ CLI で次のようなコマンドを入力して、問題の VRF-AF で HostLeak オブジェクトが有効になっていることを確認します。

例：

```
spine1# ls /mit/sys/bgp/inst/dom-apple/af-ipv4-ucast/
ctrl-l2vpn-evpn  ctrl-vpnv4-ucast  hostleak  summary
```

ステップ 2 スパイン スイッチ CLI で次のようなコマンドを入力して、config-MO が BGP によって正常に処理されたことを確認します。

例：

```
spine1# show bgp process vrf apple
```

出力は次のようになります。

```
 Information for address family IPv4 Unicast in VRF apple
    Table Id                  : 0
    Table state               : UP
    Table refcount            : 3
    Peers      Active-peers    Routes     Paths      Networks   Aggregates
    0          0               0          0          0          0

    Redistribution
        None

    Wait for IGP convergence is not configured
    GOLF EVPN MAC-IP route is enabled
    EVPN network next-hop 192.41.1.1
    EVPN network route-map map_pfxleakctrl_v4
    Import route-map rtctrlmap-apple-v4
    EVPN import route-map rtctrlmap-evpn-apple-v4
```

ステップ 3 パブリック BD サブネットが EVPN タイプ 5 ルートとして DCIG にアドバタイズされていることを確認します。

例：

```
spine1# show bgp l2vpn evpn 10.6.0.0 vrf overlay-1
Route Distinguisher: 192.41.1.5:4123    (L3VNI 2097154)
BGP routing table entry for [5]:[0]:[0]:[16]:[10.6.0.0]:[0.0.0.0]/224, version 2088
Paths: (1 available, best #1)
Flags: (0x000002 00000000) on xmit-list, is not in rib/evpn
Multipath: eBGP iBGP

  Advertised path-id 1
  Path type: local 0x4000008c 0x0 ref 1, path is valid, is best path
  AS-Path: NONE, path locally originated
    192.41.1.1 (metric 0) from 0.0.0.0 (192.41.1.5)
      Origin IGP, MED not set, localpref 100, weight 32768
      Received label 2097154
      Community: 1234:444
      Extcommunity:
          RT:1234:5101
          4BYTEAS-GENERIC:T:1234:444
```

```
  Path-id 1 advertised to peers:
    50.41.50.1
```

パス タイプ エントリで、**ref 1** は、1 つのルートが送信されたことを示します。

ステップ 4 EVPN ピアにアドバタイズされたホスト ルートが EVPN タイプ 2 MAC-IP ルートであったかどうかを確認します。

例：

```
spine1# show bgp l2vpn evpn 10.6.41.1 vrf overlay-1
Route Distinguisher: 10.10.41.2:100    (L2VNI 100)
BGP routing table entry for [2]:[0]:[2097154]:[48]:[0200.0000.0002]:[32]:[10.6.41
.1]/272, version 1146
Shared RD: 192.41.1.5:4123    (L3VNI 2097154)
Paths: (1 available, best #1)
Flags: (0x00010a 00000000) on xmit-list, is not in rib/evpn
Multipath: eBGP iBGP

  Advertised path-id 1
  Path type: local 0x4000008c 0x0 ref 0, path is valid, is best path
  AS-Path: NONE, path locally originated
  EVPN network: [5]:[0]:[0]:[16]:[10.6.0.0]:[0.0.0.0] (VRF apple)
    10.10.41.2 (metric 0) from 0.0.0.0 (192.41.1.5)
      Origin IGP, MED not set, localpref 100, weight 32768
      Received label 2097154 2097154
      Extcommunity:
          RT:1234:16777216

 Path-id 1 advertised to peers:
    50.41.50.1
```

共有 RD 行は、EVPN タイプ 2 ルートと BD サブネットによって共有される RD/VNI を示します。

EVPN ネットワーク行は、BD-Subnet の EVPN タイプ 5 ルートを示しています。

ピアにアドバタイズされたパス ID は、EVPN ピアにアドバタイズされたパスを示します。

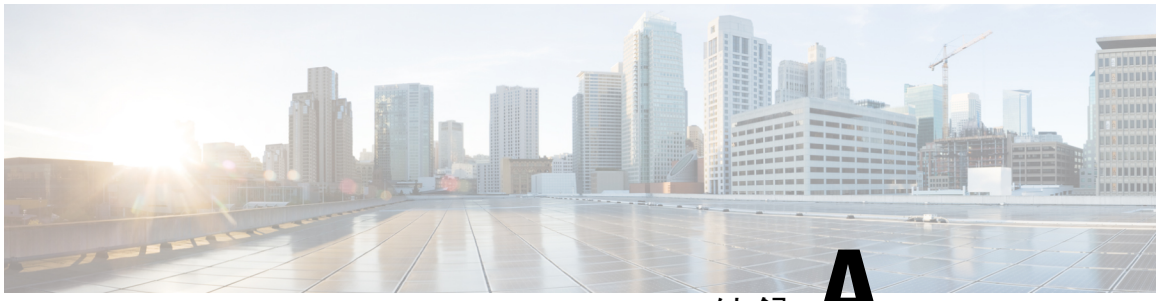
ステップ 5 DCIGデバイスで次のようなコマンドを入力して、EVPNピア（DCIG）が正しいタイプ2MAC-IPルートを受信し、ホスト ルートが特定の VRF に正常にインポートされたことを確認します（DCIG が以下の例の Cisco ASR 9000 スイッチ）：

例：

```
RP/0/RSP0/CPU0:asr9k#show bgp vrf apple-2887482362-8-1 10.6.41.1
Tue Sep  6 23:38:50.034 UTC
BGP routing table entry for 10.6.41.1/32, Route Distinguisher: 44.55.66.77:51
Versions:
  Process           bRIB/RIB  SendTblVer
  Speaker               2088        2088
Last Modified: Feb 21 08:30:36.850 for 28w2d
Paths: (1 available, best #1)
  Not advertised to any peer
  Path #1: Received by speaker 0
  Not advertised to any peer
  Local
    192.41.1.1 (metric 42) from 10.10.41.1 (192.41.1.5)
      Received Label 2097154
      Origin IGP, localpref 100, valid, internal, best, group-best, import-candidate,
imported
      Received Path ID 0, Local Path ID 1, version 2088
```

```
      Community: 1234:444
      Extended community: 0x0204:1234:444 Encapsulation Type:8 Router
MAC:0200.c029.0101 RT:1234:5101
      RIB RNH: table_id 0xe0000190, Encap 8, VNI 2097154, MAC Address: 0200.c029.0101,
IP Address: 192.41.1.1, IP table_id 0x00000000
      Source AFI: L2VPN EVPN, Source VRF: default,
Source Route Distinguisher: 192.41.1.5:4123
```

この出力では、受信した RD、ネクスト ホップ、および属性は、タイプ 2 ルートと BD サブネットで同じです。



付録 A

レイヤ 3 ネットワーキングの注意事項

レイヤ 3 ネットワーキングの注意事項

レイヤ 3 外部接続を作成し、維持する際には、次のガイドラインを使用してください。

トピック	注意またはガイドライン
vPC ペアの境界リーフ スイッチが、誤った VNID を持つ BGP パケットをピア上で学習したエンドポイントに転送する問題	設定に次の条件が存在する場合： • 2 つのリーフ スイッチが vPC ペアの一部である • L3Out の背後に接続されている 2 つのリーフ スイッチの場合、宛先エンドポイントは 2 番目（ピア）の境界リーフ スイッチに接続され、エンドポイントはそのリーフ スイッチで学習されたピアです。 ピアが学習したエンドポイント宛ての BGP パケットを受信する入力リーフ スイッチでエンドポイントが学習した場合、L3Out の背後にある最初のレイヤ 3 スイッチ間で中継 BGP 接続が確立できないという問題が発生する可能性があります。および vPC ペアの 2 番目のリーフ スイッチ上のピア上で学習されたエンドポイント。これは、ポート 179 を持つ中継 BGP パケットが VRF VNID ではなくブリッジ ドメイン VNID を使用して誤って転送されるために発生します。 この問題を解決するには、エンドポイントをファブリック内の他の非ピア リーフ スイッチに移動して、リーフ スイッチで学習されないようにします。

レイヤ 3 ネットワーキングの注意事項

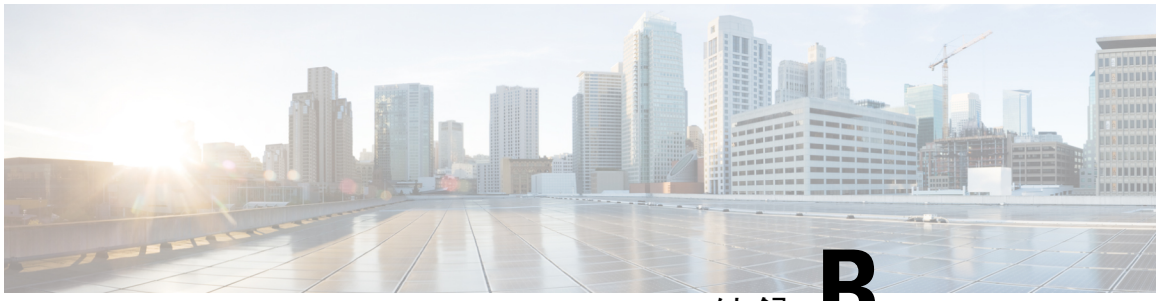
トピック	注意またはガイドライン
境界リーフ スイッチおよび GIR（メンテナンス）モード	境界リーフ スイッチに静的ルートがあり、GIR（Graceful Insertion and Removal）モード、またはメンテナンス モードがある場合、境界リーフ スイッチからのルートは ACI ファブリックにあるルーティング テーブルから削除されない可能性があり、ルーティングの問題が発生します。 この問題を回避するには、次のいずれかを実行します。 • その他の境界リーフ スイッチで同じ管理ディスタンスを持つ同じ静的ルートを設定するか、 • 静的ルートの次のホップへの到達性を追跡するため IP SLA または BFD を使用します
L3Out 集約統計情報は出力ドロップ カウンタをサポートしません	[テナント（Tenants）] [tenant_name] [ネットワーキング（Networking）] [L3Out] [L3Out_name] [統計情報（Stats）] を介して、[統計情報の選択（Select Stats）] ウィンドウにアクセスすると、L3Out 集約統計情報が出力ドロップ カウンタをサポートしていないことがわかります。＞＞＞＞＞これは、EPG VLAN からの出力ドロップを記録する ASIC に現在ハードウェア テーブルがないため、これらのカウンタに統計情報が入力されないためです。EPG VLAN の入力ドロップだけがあります。
CLI による更新	API または GUI で作成され CLI を通して更新されたレイヤ 3 外部ネットワークについては、プロトコルは API または GUI を通して外部ネットワークでグローバルに有効にする必要があり、CLI を介してさらに更新を行う前に、すべての参加ノードのノード プロファイルは API または GUI を通して追加される必要があります。
同じノード上のレイヤ 3 ネットワークのループバック	同じノードで 2 つのレイヤ 3 の外部ネットワークを設定するときに、ループバックはレイヤ 3 ネットワークに別々に設定されます。
入力ベース ポリシーの適用	Cisco APIC リリース 1.2(1) 以降、入力ベース ポリシーの適用により、出入力両方向でレイヤ 3 アウトサイド（L3Out）トラフィックにポリシー適用を定義できます。デフォルトでは入力になっています。リリース 1.2(1) 以降にアップグレード中、既存の L3Out 設定が出力に設定され、動作が既存の設定と一致します。特別なアップグレードのシーケンスは必要ありません。アップグレード後、グローバル プロパティ値を入力に変更します。変更されると、システムがルールとプレフィックス エントリを再プログラミングします。規則は出力リーフから削除され、入力リーフ上に既存の規則がない場合は、入力リーフ上にインストールされます。既存の設定がない場合、`Actrl` プレフィックス エントリが入力リーフ上にインストールされます。ダイレクト サーバ リターン（DSR）および属性 EPG には入力ベースのポリシー適用が必要です。vzAny と禁止コントラクトは、入力ベースのポリシー適用を契約無視します。入力には中継規則が適用されます。

レイヤ 3 ネットワーキングの注意事項

トピック	注意またはガイドライン
L3Outs によるブリッジ ドメイン	テナントのブリッジドメインには、共通テナントでプロビジョニングされている `l3extOut` によってアドバタイズされたパブリック サブネットを含めることができます。
OSPF と EIGRP のブリッジ ドメイン ルート アドバタイズメント	OSPF と EIGRP の両方があるノード上の同じ VRF で有効であり、ブリッジ ドメインのサブネットがいずれか 1 つの L3Out からアドバタイズされる場合、他の L3Out で有効になっているプロトコルからも同様にアドバタイズされます。 OSPF と EIGRP では、ブリッジ ドメイン ルート アドバタイズメントは VRF ごとに行われ、L3Out ごとには行われません。同じ VRF とノードで（複数エリアの）複数の OSPF L3Out が有効になっている場合、これと同じ動作が想定されます。この場合、ブリッジドメインのルートがいずれかの領域で有効になっていれば、すべての領域からアドバタイズされます。
BGP 最大プレフィックス制限	Cisco APICリリース 1.2（1x）以降、BGP `l3extOut` 接続のテナント ポリシーは、最大プレフィックス制限を使用して設定できます。これにより、ピアから受信されるルートプレフィックスの数をモニタし、制限することができます。最大プレフィックス制限を超えると、ログエントリが記録され、さらにプレフィックスが拒否されます。カウントが一定の間隔でしきい値を下回る場合、接続を再起動することができますが、そうしない場合接続がシャットダウンします。一度に1つのオプションだけを使用できます。デフォルト設定では20,000プレフィックスに制限され、その後は新しいプレフィックスは拒否されます。拒否オプションが導入されると、APIC でエラーが発生する前に BGP は設定されている制限よりも 1 つ多くプレフィックスを受け入れます。

レイヤ 3 ネットワーキングの注意事項

トピック	注意またはガイドライン
MTU	• Cisco ACI は IP フラグメンテーションをサポートしていません。したがって、外部ルータへのレイヤ 3 Outside（L3Out）接続、または Inter-Pod Network（IPN）を介したマルチポッド接続を設定する場合は、インターフェイス MTU がリンクの両端で適切に設定されていることが推奨されます。Cisco ACI、 Cisco NX-OS、Cisco IOS などの一部のプラットフォームでは、設定可能な MTU 値はイーサネット ヘッダー (一致する IP MTU、14-18 イーサネット ヘッダー サイズを除く) を考慮していません。また、IOS XR などの他のプラットフォームには、設定された MTU 値にイーサネット ヘッダーが含まれています。設定された値が 9000 の場合、Cisco ACI、Cisco NX-OS Cisco IOS の最大 IP パケット サイズは 9000 バイトになりますが、IOS-XR のタグなしインターフェイスの最大 IP パケットサイズは 8986 バイトになります。 • 物理インターフェイスの MTU 設定は次のように異なります。Cisco ACI • サブインターフェイスの場合、物理インターフェイスの MTU は固定され、リーフ スイッチの前面パネルポートでは 9216 に設定されます。 • SVI の場合、物理インターフェイス MTU はファブリック MTU ポリシーに基づいて設定されます。たとえば、ファブリック MTU ポリシーが 9000 に設定されている場合、SVI の物理インターフェイスは 9000 に設定されます。
L3Outs の QoS	L3Out 用の QoS ポリシーを設定し、L3Out が存在する BL スイッチで適用されるポリシーを有効にするには、次の注意事項に従ってください。 • VRF ポリシー制御の適用方向を **出力** に設定する必要があります。 • VRF ポリシー制御適用の優先度設定を **有効** に設定する必要があります。 • L3Out を使用して EPG 間の通信を制御するコントラクトを設定する際に、コントラクトまたはコントラクトの件名に QoS クラスまたはターゲット DSCP を含めます。
ICMP 設定	ICMP リダイレクトおよび ICMP 到達不能は、スイッチ CPU がこれらのパケットを生成しないように、デフォルトで無効になっています。Cisco ACI



付録 B

NX-OS スタイル CLI を使用したタスクの実行

Part I： レイヤ 3 の設定

NX-OS スタイルの CLI を使用した共通パーベイシブ ゲートウェイの設定

NX-OS スタイルの CLI を使用した共通パーベイシブ ゲートウェイの設定

始める前に

- テナント、VRF、およびブリッジ ドメインが作成されていること。

手順

共通パーベイシブ ゲートウェイを設定します。

例：

```
apic1#configure
apic1(config)#tenant demo
apic1(config-tenant)#bridge-domain test
apic1(config-tenant-bd)#l2-unknown-unicast flood
apic1(config-tenant-bd)#arp flooding
apic1(config-tenant-bd)#exit

apic1(config-tenant)#interface bridge-domain test
apic1(config-tenant-interface)#multi-site-mac-address 12:34:56:78:9a:bc
apic1(config-tenant-interface)#mac-address 00:CC:CC:CC:C1:01 (Should be unique for each
```

```
 ACI fabric)
apic1(config-tenant-interface)#ip address 192.168.10.1/24 multi-site
apic1(config-tenant-interface)#ip address 192.168.10.254/24 (Should be unique for each
ACI fabric)
```

NX-OS Style CLI を使用した IP エージングの設定

NX-OS スタイル CLI を使用した IP エージング ポリシーの設定

このセクションでは、CLI を使用した IP エージング ポリシーを有効および無効にする方法を説明します。

手順

ステップ 1 IP エージング ポリシーを有効にするには：

例：

```
ifc1(config)# endpoint ip aging
```

ステップ 2 IP エージング ポリシーを無効にするには：

例：

```
ifav9-ifc1(config)# no endpoint ip aging
```

次のタスク

エンドポイントの IP アドレスをトラッキングするために使用される間隔を指定するには、エンドポイント保持ポリシーを作成します。

NX-OS スタイル CLI を使用したブリッジ ドメイン上のスタティック ルートの設定

NX-OS スタイル CLI を使用したブリッジ ドメイン上のスタティック ルートの設定

パーベイシブ ブリッジ ドメイン (BD) でスタティック ルートを設定するには、NX-OS スタイルの次の CLI コマンドを使用します:

始める前に

テナント、VRF、BD および EPG が設定されています。

- スタティック ルートのサブネットを作成するには、epg (fvAEPg で fvSubnet オブジェクト)、普及 BD (fvBD) 自体 BD しないに関連付けられているように構成されます。

NX-OS スタイル CLI を使用したタスクの実行

- サブネットマスクが/32 にする必要があります (128/for IPv6) 1 つの IP アドレスまたは 1 つのエンドポイントをポイントします。これは、EPG に関連付けられている普及 BD で含まれています。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	コンフィギュレーション モードに入ります。
ステップ 2	**tenant** *tenant-name* 例： `apic1(config)# tenant t1`	テナントを作成するか、テナント設定モードに入ります。
ステップ 3	**application** *ap-name* 例： `apic1(config-tenant)# application ap1`	アプリケーション プロファイルを作成するか、アプリケーション プロファイル モードに入ります。

ステップ 4	**epg** *epg-name*
	例：
	`apic1(config-tenant-app)# epg ep1`
	`<> <A.B.C.D> [scope <scope>]`
		EPG を作成するか、EPG 設定モードに入ります。

ステップ 5	**endpoint ip***A.B.C.D/LEN* **next-hop** *A.B.C.D* [scope *scope*] 例： `apic1(config-tenant-app-epg)# endpoint ip 125.12.1.1/32 next-hop 26.0.14.101`	EPG の背後にエンドポイントを作成します。サブネットマスクは /32 で (IPv6 の場合は /128)、1 つの IP アドレスまたは1つのエンドポイントをポイントしている必要があります。

例

次の例は、EPG の背後にあるエンドポイントを設定するコマンドを示しています。

```
apic1# config
      apic1(config)# tenant t1
      apic1(config-tenant)# application ap1
      apic1(config-tenant-app)# epg ep1
      apic1(config-tenant-app-epg)# endpoint ip 125.12.1.1/32 next-hop 26.0.14.101
```

NX-OS Style CLI を使用した VRF ごとのデータプレーン IP ラーニングの設定

NX-OS-Style CLI を使用したデータプレーン IP ラーニングの設定

このセクションでは、NX-OS-Style CLI を使用してデータプレーン IP ラーニングを無効にする方法について説明します。

特定の VRF のデータプレーン IP ラーニングを無効にするには：

手順

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# config
```

ステップ 2 特定のテナントのテナント モードに入ります。

例：

```
apic1(config)# tenant name
```

ステップ 3 VRF のコンテキスト モードに入ります。

例：

```
apic1(config-tenant)# vrf context name
```

ステップ 4 VRF のデータプレーン IP ラーニングを無効にします。

例：

```
apic1(config-tenant-vrf)# ipdataplanelearning disabled
```

NX-OS Style CLI を使用した IPv6 ネイバー探索の設定

NX-OS スタイル CLI を使用したブリッジ ドメイン上の IPv6 ネイバー検索によるテナント、VRF、ブリッジ ドメインの設定

手順

ステップ 1 IPv6 ネイバー検索インターフェイス ポリシーを設定し、ブリッジ ドメインに割り当てます。

a) IPv6 ネイバー検索インターフェイス ポリシーを作成します。

例：

```
apic1(config)# tenant ExampleCorp
apic1(config-tenant)# template ipv6 nd policy NDPol001
apic1(config-tenant-template-ipv6-nd)# ipv6 nd mtu 1500
```

b) VRF およびブリッジ ドメインを作成します:

例：

```
apic1(config-tenant)# vrf context pvn1
apic1(config-tenant-vrf)# exit
apic1(config-tenant)# bridge-domain bd1
apic1(config-tenant-bd)# vrf member pvn1
apic1(config-tenant-bd)# exit
```

c) IPv6 ネイバー検索ポリシーをブリッジ ドメインに割り当てます。

例：

```
apic1(config-tenant)# interface bridge-domain bd1
apic1(config-tenant-interface)# ipv6 nd policy NDPol001
apic1(config-tenant-interface)#exit
```

ステップ 2 サブネット上で IPV6 ブリッジ ドメイン サブネットおよびネイバー検索プレフィックス ポリシーを作成します。

例：

```
apic1(config-tenant)# interface bridge-domain bd1
apic1(config-tenant-interface)# ipv6 address 34::1/64
apic1(config-tenant-interface)# ipv6 address 33::1/64
apic1(config-tenant-interface)# ipv6 nd prefix 34::1/64 1000 1000
apic1(config-tenant-interface)# ipv6 nd prefix 33::1/64 4294967295 4294967295
```

NX-OS スタイル CLI を使用したレイヤ 3 インターフェイス上の RA による IPv6 ネイバー探索インターフェイス ポリシーの設定

この例では、IPv6 ネイバー検索インターフェイス ポリシーを設定し、レイヤ 3 インターフェイスに割り当てます。次に、IPv6 レイヤ 3 アウトインターフェイス、ネイバー検索プレフィックス ポリシーを設定し、インターフェイスにネイバー検索ポリシーを関連付けます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	コンフィギュレーション モードに入ります。

NX-OS スタイル CLI を使用したタスクの実行

	コマンドまたはアクション	目的

ステップ 2	**tenant** *tenant_name*
	例：
	`apic1(config)# tenant ExampleCorp`
	`apic1(config-tenant)#`
		テナントを作成し、テナントモードを開始します。

ステップ 3	**template ipv6 nd policy** *policy_name* 例： `apic1(config-tenant)# template ipv6 nd policy NDPol001`	IPv6 ND ポリシーを作成します。

ステップ 4	**ipv6 nd mtu** *mtu value*
	例：
	`apic1(config-tenant-template-ipv6-nd)# ipv6 nd mtu 1500`
	`apic1(config-tenant-template-ipv6)# exit`
	`apic1(config-tenant-template)# exit`
	`apic1(config-tenant)#`
		IPv6 ND ポリシーに MTU 値を割り当てます。

ステップ 5	**vrf context** *VRF_name*
	例：
	`apic1(config-tenant)# vrf context pvn1`
	`apic1(config-tenant-vrf)# exit`
		VRF を作成します。

ステップ 6	**l3out** *VRF_name* 例： `apic1(config-tenant)# l3out l3extOut001`	レイヤ 3 アウト を作成します。

ステップ 7	**vrf member** *VRF_name*
	例：
	`apic1(config-tenant-l3out)# vrf member pvn1`
	`apic1(config-tenant-l3out)# exit`
		VRF をレイヤ 3 アウトインターフェイスに関連付けます。

ステップ 8	**external-l3 epg instp l3out** *l3extOut001* 例：	レイヤ 3 アウトおよび VRF をレイヤ 3 インターフェイスに割り当てます。

NX-OS スタイル CLI を使用したタスクの実行

	コマンドまたはアクション	目的
	apic1(config-tenant)# **external-l3 epg instp l3out l3extOut001** apic1(config-tenant-l3ext-epg)# **vrf member pvn1** apic1(config-tenant-l3ext-epg)# **exit**	
ステップ 9	**leaf** *2011* 例： apic1(config)# **leaf 2011**	リーフ スイッチ モードを開始します。
ステップ 10	**vrf context tenant** *ExampleCorp* **vrf** *pvn1* **l3out** *l3extOut001* 例： apic1(config-leaf)# **vrf context tenant ExampleCorp vrf pvn1 l3out l3extOut001** apic1(config-leaf-vrf)# **exit**	VRF をリーフ スイッチに関連付けます。
ステップ 11	**int** *eth 1/1* 例： apic1(config-leaf)# **int eth 1/1** apic1(config-leaf-if)#	インターフェイス モードに入ります。
ステップ 12	**vrf member tenant** *ExampleCorp* **vrf** *pvn1* **l3out** *l3extOut001* 例： apic1(config-leaf-if)# **vrf member tenant ExampleCorp vrf pvn1 l3out l3extOut001**	インターフェイスで関連付けられているテナント、VRF、レイヤ 3 Out を指定します。
ステップ 13	**ipv6 address** *2001:20:21:22::2/64* **preferred** 例： apic1(config-leaf-if)# **ipv6 address 2001:20:21:22::2/64 preferred**	プライマリまたは優先 Ipv6 アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 14	**ipv6 nd prefix** *2001:20:21:22::2/64 1000 1000* 例： `apic1(config-leaf-if)# ipv6 nd prefix 2001:20:21:22::2/64 1000 1000`	レイヤ 3 インターフェイス下で IPv6 ND プレフィックス ポリシーを設定します。

ステップ 15	**inherit ipv6 nd** *NDPol001*
	例：
	`apic1(config-leaf-if)# inherit ipv6 nd NDPol001`
	`apic1(config-leaf-if)# exit`
	`apic1(config-leaf)# exit`
		レイヤ 3 インターフェイス下で ND ポリシーを設定します。

設定が完了します。

NX-OS Style CLI を使用した Microsoft NLB の設定

NX-OS Style CLI を使用したユニキャスト モードでのMicrosoft NLB の設定

このタスクは、ブリッジ ドメインのすべてのポートに Microsoft NLB がフラッドするように設定します。

始める前に

これらの手順を進める前に次の使用可能な情報を準備してください。

- Microsoft NLB クラスタ VIP
- Microsoft NLB クラスタ MAC アドレス

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	コンフィギュレーション モードに入ります。
ステップ 2	**tenant** *tenant-name* 例： `apic1 (config)# tenant tenant1`	存在しない場合はテナントを作成します。または、テナント コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**application** *app-profile-name* 例： `apic1 (config-tenant)# application app1`	存在しない場合はアプリケーション プロファイルを作成します。または、アプリケーション プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**epg** *epg-name* 例： `apic1 (config-tenant-app)# epg epg1`	存在しない場合は EPG を作成します。または、EPG コンフィギュレーション モードを開始します。
ステップ 5	**[no] endpoint {ip | ipv6}** *ip-address* **epnlb mode mode-uc mac** *mac-address* 例： `apic1 (config-tenant-app-epg)# endpoint ip 192.0.2.2/32 epnlb mode mode-uc mac 03:BF:01:02:03:04`	Microsoft NLB をユニキャスト モードで設定します。 • *ip-address* はMicrosoft NLB クラスタ VIP です。 • *mac-address* は Microsoft NLB クラスタ MAC アドレスです。

NX-OS Style CLI を使用したマルチキャスト モードでのMicrosoft NLB の設定

このタスクは、ブリッジ ドメインの特定のポートでのみ Microsoft NLB がフラッドするように設定します。

始める前に

これらの手順を進める前に次の使用可能な情報を準備してください。

- Microsoft NLB クラスタ VIP
- Microsoft NLB クラスタ MAC アドレス

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	コンフィギュレーション モードに入ります。
ステップ 2	**tenant** *tenant-name* 例： `apic1 (config)# tenant tenant1`	存在しない場合はテナントを作成します。または、テナント コンフィギュレーション モードを開始します。
ステップ 3	**application** *app-profile-name* 例：	存在しない場合はアプリケーション プロファイルを作成します。または、アプ

	コマンドまたはアクション	目的
	`apic1 (config-tenant)# application app1`	リケーション プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**epg** *epg-name* 例： `apic1 (config-tenant-app)# epg epg1`	EPG 構成モードを開始します。まだ存在しない場合は EPG を作成します。
ステップ 5	**[no] endpoint {ip | ipv6}** *ip-address* **epnlb mode mode-mcast--static mac** *mac-address* 例： `apic1 (config-tenant-app-epg)# endpoint ip 192.0.2.2/32 epnlb mode mode-mcast--static mac 03:BF:01:02:03:04`	スタティック マルチキャスト モードで Microsoft NLB を設定します。 • *ip-address* はMicrosoft NLB クラスタ VIP です。 • *mac-address* は Microsoft NLB クラスタ MAC アドレスです。
ステップ 6	**[no] nlb static-group** *mac-address* **leaf** *leaf-num* **interface {ethernet** *slot/port* **| port-channel** *port-channel-name***} vlan** *portEncapVlan* 例： `apic1 (config-tenant-app-epg)# nlb static-group 03:BF:01:02:03:04 leaf 102 interface ethernet 1/12 vlan 19`	Microsoft NLB マルチキャスト VMAC を、Microsoft NLB サーバが接続されている EPG ポートに追加します。 • mac-address は、入力したMicrosoft NLBクラスタのMACアドレスです。ステップ 5 （508 ページ） • leaf-numは、追加または削除するインターフェイスを含むリーフスイッチです。 • port-channel-nameは、port-channel オプションを使用する場合のポートチャネルの名前です。 • portEncapVlanは、アプリケーション EPG のスタティック メンバのカプセル化 VLAN です。

NX-OS Style CLI を使用した IGMP モードでの Microsoft NLB の設定

このタスクは、ブリッジ ドメインの特定のポートでのみ Microsoft NLB がフラッドするように設定します。

始める前に

これらの手順を進める前に次の使用可能な情報を準備してください。

- Microsoft NLB クラスタ VIP
- Microsoft NLB クラスタ MAC アドレス

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	コンフィギュレーション モードに入ります。
ステップ 2	**tenant** *tenant-name* 例： `apic1 (config)# tenant tenant1`	存在しない場合はテナントを作成します。または、テナント コンフィギュレーション モードを開始します。
ステップ 3	**application** *app-profile-name* 例： `apic1 (config-tenant)# application app1`	存在しない場合はアプリケーション プロファイルを作成します。または、アプリケーション プロファイル コンフィギュレーション モードを開始します。
ステップ 4	**epg** *epg-name* 例： `apic1 (config-tenant-app)# epg epg1`	存在しない場合は EPG を作成します。または、EPG コンフィギュレーション モードを開始します。
ステップ 5	**[no] endpoint {ip | ipv6}** *ip-address* **epnlb mode mode-mcast-igmp group** *multicast-IP-address* 例： `apic1 (config-tenant-app-epg)# endpoint ip 192.0.2.2/32 epnlb mode mode-mcast-igmp group 1.3.5.7`	Microsoft NLB を IGMP モードで設定します。 • *ip-address* はMicrosoft NLB クラスタ VIP です。 • *multicast-IP-address* は、NLB エンドポイント グループのマルチキャスト IP です。

NX-OS Style CLI を使用した IGMP スヌーピングの設定

NX-OS スタイル CLI を使用した IGMP スヌーピング ポリシーの設定とブリッジ ドメインへの割り当て

始める前に

- IGMP スヌーピングのポリシーを消費するテナントを作成します。
- IGMP スヌーピング ポリシーを接続するテナントのブリッジ ドメインを作成します。

NX-OS スタイル CLI を使用したタスクの実行

手順

	コマンドまたはアクション	目的
ステップ 1	デフォルト値に基づいてスヌーピング ポリシーを作成します。 例： **apic1(config-tenant)# template ip igmp snooping policy cookieCut1** **apic1(config-tenant-template-ip-igmp-snooping)# show run all** # Command: show running -config all tenant foo template ip igmp snooping policy cookieCut1 # Time: Thu Oct 13 18:26:03 2016 tenant t_10 template ip igmp snooping policy cookieCut1 ip igmp snooping no ip igmp snooping fast-leave ip igmp snooping last-member-query-interval 1 no ip igmp snooping querier ip igmp snooping query-interval 125 ip igmp snooping query-max-response-time 10 ip igmp snooping stqrtup-query-count 2 ip igmp snooping startup-query-interval 31 no description exit exit apic1(config-tenant-template-ip-igmp-snooping)#	例の NX-OS スタイル CLI シーケンス： • デフォルト値を持つ cookieCut1 という名前の IGMP スヌーピング ポリシーを作成します。 • ポリシー cookieCut1 のデフォルト IGMP スヌーピングの値が表示されます。
ステップ 2	必要に応じてスヌーピング ポリシーを変更します。 例： **apic1(config-tenant-template-ip-igmp-snooping)# ip igmp snooping query-interval 300** **apic1(config-tenant-template-ip-igmp-snooping)# show run all** # Command: show running -config all tenant foo template ip igmp snooping policy cookieCut1 #Time: Thu Oct 13 18:26:03 2016 tenant foo template ip igmp snooping policy cookieCut1 ip igmp snooping no ip igmp snooping fast-leave ip igmp snooping	例の NX-OS スタイル CLI シーケンス： • cookieCut1 という名前の IGMP スヌーピング ポリシーのクエリ間隔値のカスタム値を指定します。 • ポリシー cookieCut1 の変更された IGMP スヌーピング値を確認します。

NX-OS スタイル CLI を使用したタスクの実行

	コマンドまたはアクション	目的
	last-member-query-interval 1 no ip igmp snooping querier ip igmp snooping query-interval 300 ip igmp snooping query-max-response-time 10 ip igmp snooping stqrtup-query-count 2 ip igmp snooping startup-query-interval 31 no description exit exit apic1(config-tenant-template-ip-igmp-snooping)# exit apic1(config--tenant)#	
ステップ 3	必要に応じてスヌーピング ポリシーを変更します。 **例**： apic1(config-tenant-template-ip-igmp-snooping)# ip igmp snooping ? <CR> fast-leave Enable IP IGMP Snooping fast leave processing last-member-query-interval Change the IP IGMP snooping last member query interval param querier Enable IP IGMP Snooping querier processing query-interval Change the IP IGMP snooping query interval param query-max-response-time Change the IP IGMP snooping max query response time startup-query-count Change the IP IGMP snooping number of initial queries to send startup-query-interval Change the IP IGMP snooping time for sending initial queries version Change the IP IGMP snooping version param apic1(config-tenant-template-ip-igmp-snooping)# ip igmp snooping version ? v2 version-2 v3 version-3 apic1(config-tenant)# show run # Command: show running-config tenant tenant1 # Time: Mon Jun 1 01:53:53 2020 tenant tenant1 <snipped> interface bridge-domain amit_bd ip address 10.175.31.30/24	例の NX-OS スタイル CLI シーケンス： • IGMP スヌーピング ポリシーのクエリ バージョンのカスタム値を指定します。 • ポリシーの変更された IGMP スヌーピング バージョンを確認します。

	コマンドまたはアクション	目的
	secondary ip address 100.175.31.1/32 secondary snooping-querier ip igmp snooping policy igmp_snoop_policy exit template ip igmp snooping policy igmp_snoop_policy ip igmp snooping fast-leave ip igmp snooping last-member-query-interval 2 ip igmp snooping querier v3 ip igmp snooping query-interval 100 ip igmp snooping startup-query-count 5 ip igmp snooping version v3 exit exit	
ステップ 4	ブリッジ ドメインにポリシーを割り当てます。 例： **apic1(config-tenant)# int bridge-domain bd3** **apic1(config-tenant-interface)# ip igmp snooping policy cookieCut1**	例の NX-OS スタイル CLI シーケンス： • ブリッジ ドメインの BD3 に移動します。IGMP スヌーピング ポリシーのクエリ間隔値は cookieCut1 という名前です。 • ポリシー cookieCut1 の変更された IGMP スヌーピングの値を持つ IGMP スヌーピングのポリシーを割り当てます。

次のタスク

複数のブリッジ ドメインに IGMP スヌーピングのポリシーを割り当てることができます。

NX-OS スタイル CLI によりスタティック ポートで IGMP スヌーピングおよびマルチキャストの有効化

EPGに静的に割り当てられたポートでIGMPスヌーピングおよびマルチキャストをイネーブルにできます。それらのポートで有効なIGMPスヌーピングおよびマルチキャストトラフィックへのアクセスを許可または拒否するアクセスユーザーのグループを作成および割り当てることができます。

このタスクで説明されている手順には、次のエンティティの事前設定を前提とします。

- テナント：tenant_A
- アプリケーション：application_A
- EPG：epg_A
- ブリッジ ドメイン：bridge_domain_A

NX-OS スタイル CLI を使用したタスクの実行

- vrf：vrf_A -- a member of bridge_domain_A
- VLAN ドメイン：vd_A（300 ～ 310 の範囲で設定される）
- リーフ スイッチ：101 およびインターフェイス 1/10

  スイッチ 101 のターゲット インターフェイス 1/10 が VLAN 305 に関連付けられており、enant_A、application_A、epg_A に静的にリンクされています。
- リーフ スイッチ：101 およびインターフェイス 1/11

  スイッチ 101 のターゲット インターフェイス 1/11 が VLAN 309 に関連付けられており、enant_A、application_A、epg_A に静的にリンクされています。

始める前に

EPG に IGMP スヌーピングおよびマルチキャストを有効にする前に、次のタスクを実行します。

- この機能を有効にして静的に EPG に割り当てるインターフェイスを特定する

（注） スタティック ポートの割り当てに関する詳細は、『*Cisco APIC* レイヤ *2* ネットワーキング設定ガイド』の「*NX-OS* スタイル *CLI* を使用した *APIC* で特定のポートの *EPG* を展開する」を参照してください。

- IGMP スヌーピング マルチキャスト トラフィックの受信者の IP アドレスを特定します。

手順

	コマンドまたはアクション	目的

ステップ 1	ターゲット インターフェイスで IGMP スヌーピングおよびレイヤ2マルチキャスティングを有効にします
	例：
	`apic1# conf t`
	`apic1(config)# tenant tenant_A`
	`apic1(config-tenant)# application application_A`
	`apic1(config-tenant-app)# epg epg_A`
	`apic1(config-tenant-app-epg)# ip igmp snooping static-group 225.1.1.1 leaf 101 interface ethernet 1/10 vlan 305`
	`apic1(config-tenant-app-epg)# end`
	
	`apic1# conf t`
	`apic1(config)# tenant tenant_A;`
	`application application_A; epg epg_A`
	`apic1(config-tenant-app-epg)# ip igmp`
		例のシーケンスでは次を有効にします。
		• 静的にリンクされているターゲット インターフェイス 1/10 の IGMP スヌーピング、そしてマルチキャスト IP アドレス、225.1.1.1 に関連付けます
		• 静的にリンクされているターゲット インターフェイス 1/11 の IGMP スヌーピング、そしてマルチキャスト IP アドレス、227.1.1.1 に関連付けます

	コマンドまたはアクション	目的
	snooping static-group 227.1.1.1 leaf 101 interface ethernet 1/11 vlan 309 apic1(config-tenant-app-epg)# exit apic1(config-tenant-app)# exit	

NX-OS スタイル CLI を使用した IGMP スヌーピングおよびマルチ キャスト グループへのアクセスの有効化

EPGに静的に割り当てられたポートでIGMPスヌーピングおよびマルチキャストを有効にした後、それらのポートで有効なIGMPスヌーピングおよびマルチキャスト トラフィックへのアクセスを許可または拒否するユーザーのアクセス グループを作成および割り当てできます。

このタスクで説明されている手順には、次のエンティティの事前設定を前提とします。

- テナント：tenant_A
- アプリケーション：application_A
- EPG：epg_A
- ブリッジ ドメイン：bridge_domain_A
- vrf：vrf_A -- a member of bridge_domain_A
- VLAN ドメイン：vd_A（300 ～ 310 の範囲で設定される）
- リーフ スイッチ：101 およびインターフェイス 1/10

  スイッチ 101 のターゲット インターフェイス 1/10 が VLAN 305 に関連付けられており、enant_A、application_A、epg_A に静的にリンクされています。
- リーフ スイッチ：101 およびインターフェイス 1/11

  スイッチ 101 のターゲット インターフェイス 1/11 が VLAN 309 に関連付けられており、enant_A、application_A、epg_A に静的にリンクされています。

（注） スタティック ポートの割り当てに関する詳細は、『*Cisco APIC* レイヤ *2* ネットワーキング設定ガイド』の「*NX-OS* スタイル *CLI* を使用した *APIC* で特定のポートの *EPG* を展開する」を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	route-map「アクセス グループ」を定義します。 例：	例のシーケンスを設定します。 • マルチキャスト グループ 225.1.1.1/24 にリンクされる

NX-OS スタイル CLI を使用したタスクの実行

	コマンドまたはアクション	目的
	apic1# conf t apic1(config)# tenant tenant_A; application application_A; epg epg_A apic1(config-tenant)# route-map fooBroker permit apic1(config-tenant-rtmap)# match ip multicast group 225.1.1.1/24 apic1(config-tenant-rtmap)# exit apic1(config-tenant)# route-map fooBroker deny apic1(config-tenant-rtmap)# match ip multicast group 227.1.1.1/24 apic1(config-tenant-rtmap)# exit	Route-map-access グループ「foobroker」のアクセスが許可されています。 • マルチキャスト グループ 225.1.1.1/24 にリンクされる Route-map-access グループ「foobroker」のアクセスが拒否されています。
ステップ 2	ルート マップ設定を確認します。 **例**： apic1(config-tenant)# show running-config tenant test route-map fooBroker # Command: show running-config tenant test route-map fooBroker # Time: Mon Aug 29 14:34:30 2016 tenant test route-map fooBroker permit 10 match ip multicast group 225.1.1.1/24 exit route-map fooBroker deny 20 match ip multicast group 227.1.1.1/24 exit exit	
ステップ 3	アクセス グループ接続パスを指定します。 **例**： apic1(config-tenant)# application application_A apic1(config-tenant-app)# epg epg_A apic1(config-tenant-app-epg)# ip igmp snooping access-group route-map fooBroker leaf 101 interface ethernet 1/10 vlan 305 apic1(config-tenant-app-epg)# ip igmp snooping access-group route-map newBroker leaf 101 interface ethernet 1/10 vlan 305	例のシーケンスを設定します。 • リーフ スイッチ 101、インターフェイス 1/10、VLAN 305 で接続されている Route-map-access グループ「foobroker」。 • リーフ スイッチ 101、インターフェイス 1/10、VLAN 305 で接続されている Route-map-access グループ「newbroker」。
ステップ 4	アクセスグループ接続を確認します。 **例**： apic1(config-tenant-app-epg)# show run # Command: show running-config tenant tenant_A application application_A epg epg_A # Time: Mon Aug 29 14:43:02 2016	

	コマンドまたはアクション	目的
	tenant tenent_A application application_A epg epg_A bridge-domain member bridge_domain_A ip igmp snooping access-group route-map fooBroker leaf 101 interface ethernet 1/10 vlan 305 ip igmp snooping access-group route-map fooBroker leaf 101 interface ethernet 1/11 vlan 309 ip igmp snooping access-group route-map newBroker leaf 101 interface ethernet 1/10 vlan 305 ip igmp snooping static-group 225.1.1.1 leaf 101 interface ethernet 1/10 vlan 305 ip igmp snooping static-group 225.1.1.1 leaf 101 interface ethernet 1/11 vlan 309 exit exit exit	

NX-OS Style CLI を使用した MLD スヌーピングの設定

NX-OS Style CLI を使用したブリッジ ドメインに対する MLD スヌーピング ポリシーの設定と割り当て

始める前に

- MLD スヌーピングのポリシーを消費するテナントを作成します。
- MLD スヌーピング ポリシーを接続するテナントのブリッジ ドメインを作成します。

手順

	コマンドまたはアクション	目的

ステップ 1	**configure terminal**
	例：
	`apic1# configure terminal`
	`apic1(config)#`
		コンフィギュレーションモードに入ります。

ステップ 2	**tenant** *tenant-name* 例：	テナントを作成するか、テナント設定モードに入ります。

NX-OS スタイル CLI を使用したタスクの実行

	コマンドまたはアクション	目的
	apic1(config)# **tenant tn1** apic1(config-tenant)#	
ステップ 3	**template ipv6 mld snooping policy** *policy-name* 例： apic1(config-tenant)# **template ipv6 mld snooping policy mldPolicy1** apic1(config-tenant-template-ip-mld-snooping)#	MLD スヌーピング ポリシーを作成します。例の NX-OS スタイルの CLI シーケンスは、mldPolicy1 という名前の MLD スヌーピング ポリシーを作成します。
ステップ 4	**[no] ipv6 mld snooping** 例： apic1(config-tenant-template-ip-mld-snooping)# **ipv6 mld snooping** apic1(config-tenant-template-ip-mld-snooping)# **no ipv6 mld snooping**	MLD スヌープ ポリシーの管理状態を有効または無効にします。デフォルトのステートはディセーブルです。
ステップ 5	**[no] ipv6 mld snooping fast-leave** 例： apic1(config-tenant-template-ip-mld-snooping)# **ipv6 mld snooping fast-leave** apic1(config-tenant-template-ip-mld-snooping)# **no ipv6 mld snooping fast-leave**	IPv6 MLD スヌーピング ファストリーブ処理を有効または無効にします。
ステップ 6	**[no] ipv6 mld snooping querier** 例： apic1(config-tenant-template-ip-mld-snooping)# **ipv6 mld snooping querier** apic1(config-tenant-template-ip-mld-snooping)# **no ipv6 mld snooping querier**	IPv6 MLD スヌーピング クエリア処理を有効または無効にします。有効にするクエリア オプションを割り当て済みのポリシーで効果的に有効にするには、ステップ 14 （519 ページ） で説明されているように、ポリシーを適用するブリッジ ドメインに割り当てられるサブネットでもクエリア オプションを有効にする必要があります。
ステップ 7	**ipv6 mld snooping last-member-query-interval** *parameter* 例： apic1(config-tenant-template-ip-mld-snooping)# **ipv6 mld snooping last-member-query-interval 25**	IPv6 MLD スヌーピングの最終メンバー クエリー間隔パラメータを変更します。NX-OS スタイルの CLI シーケンスの例では、IPv6 MLD スヌーピングの最後のメンバーのクエリー間隔パラメータが 25 秒に変更されます。有効なオプションは 1 ー 25 です。デフォルト値は 1 秒です。

NX-OS スタイル CLI を使用したタスクの実行

	コマンドまたはアクション	目的
ステップ 8	**ipv6 mld snooping query-interval** *parameter* 例： `apic1(config-tenant-template-ip-mld-snooping)# ipv6 mld snooping query-interval 300`	IPv6 MLD スヌーピング クエリー間隔パラメータを変更します。NX-OS スタイルの CLI シーケンス例では、IPv6 MLD スヌーピング クエリ間隔パラメータを 300 秒に変更します。有効なオプションは 1 ー 18000 です。デフォルト値は 125 秒です。
ステップ 9	**ipv6 mld snooping query-max-response-time** *parameter* 例： `apic1(config-tenant-template-ip-mld-snooping)# ipv6 mld snooping query-max-response-time 25`	IPv6 MLD スヌーピングの最大クエリー応答時間を変更します。NX-OS スタイルの CLI シーケンスの例では、IPv6 MLD スヌーピングの最大クエリ応答時間が 25 秒に変更されます。有効なオプションは 1 ー 25 です。デフォルトは 10 秒です。
ステップ 10	**ipv6 mld snooping startup-query-count** *parameter* 例： `apic1(config-tenant-template-ip-mld-snooping)# ipv6 mld snooping startup-query-count 10`	送信する初期クエリーの IPv6 MLD スヌーピング数を変更します。NX-OS スタイルの CLI シーケンスの例では、最初のクエリの IPv6 MLD スヌーピング数を 10 に変更します。有効なオプションは 1 ー 10 です。デフォルトは 2 です。
ステップ 11	**ipv6 mld snooping startup-query-interval** *parameter* 例： `apic1(config-tenant-template-ip-mld-snooping)# ipv6 mld snooping startup-query-interval 300`	初期クエリーを送信するための IPv6 MLD スヌーピング時間を変更します。NX-OS スタイルの CLI シーケンスの例では、最初のクエリを送信するための IPv6 MLD スヌーピング時間が 300 秒に変更されます。有効なオプションは 1 ー 18000 です。デフォルト値は 31 秒です。

ステップ 12	**exit**
	例：
	`apic1(config-tenant-template-ip-mld-snooping)# exit`
	`apic1(config-tenant)#`
		設定モードに戻ります。

ステップ 13	**interface bridge-domain** *bridge-domain-name* 例： `apic1(config-tenant)# interface`	インターフェイスブリッジ ドメインを設定します。例の NX-OS スタイルの CLI シーケンスは、bd1 という名前のインターフェイスブリッジ ドメインを設定します。

	コマンドまたはアクション	目的
	bridge-domain bd1 apic1(config-tenant-interface)#	
ステップ 14	**ipv6 address** *sub-bits/prefix-length* **snooping-querier** 例： apic1(config-tenant-interface)# **ipv6 address 2000::5/64 snooping-querier**	ブリッジドメインをスイッチクエリアとして設定します。これにより、ポリシーが適用されるブリッジドメインに割り当てられたサブネットでクエリアオプションが有効になります。
ステップ 15	**ipv6 mld snooping policy** *policy-name* 例： apic1(config-tenant-interface)# **ipv6 mld snooping policy mldPolicy1**	ブリッジドメインを MLD スヌーピング ポリシーに関連付けます。例の NX-OS スタイルの CLI シーケンスは、mldPolicy1 という名前の MLD スヌーピング ポリシーにブリッジドメインを関連付けます。
ステップ 16	**exit** 例： apic1(config-tenant-interface)# **exit** apic1(config-tenant)#	設定モードに戻ります。

NX-OS Style CLI を使用した IP マルチキャストの設定

NX-OS スタイルの CLI を使用したレイヤ 3 マルチキャストの設定

手順

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# configure
```

ステップ 2 テナントの設定モード、VRF の設定モードは、および PIM オプションの設定モードに入ります。

例：

```
apic1(config)# tenant tenant1
apic1(config-tenant)# vrf context tenant1_vrf
apic1(config-tenant-vrf)# ip pim
apic1(config-tenant-vrf)# ip pim fast-convergence
apic1(config-tenant-vrf)# ip pim bsr forward
```

ステップ 3 IGMP を設定し、VRF に適切な IGMP オプションを設定します。

NX-OS スタイル CLI を使用したタスクの実行

例：

```
apic1(config-tenant-vrf)# ip igmp
apic1(config-tenant-vrf)# exit
apic1(config-tenant)# interface bridge-domain tenant1_bd
apic1(config-tenant-interface)# ip multicast
apic1(config-tenant-interface)# ip igmp allow-v3-asm
apic1(config-tenant-interface)# ip igmp fast-leave
apic1(config-tenant-interface)# ip igmp inherit interface-policy igmp_intpol1
apic1(config-tenant-interface)# exit
```

ステップ 4 テナントの L3 Out モードに入り、PIM を有効にし、リーフ インターフェイス モードに入ります。このインターフェイスの PIM を設定します。

例：

```
apic1(config-tenant)# l3out tenant1_l3out
apic1(config-tenant-l3out)# ip pim
apic1(config-tenant-l3out)# exit
apic1(config-tenant)# exit
apic1(config)#
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/125
apic1(config-leaf-if) ip pim inherit interface-policy pim_intpol1
```

ステップ 5 IGMP コマンドを使用して、インターフェイスの IGMP を設定します。

例：

```
apic1(config-leaf-if)# ip igmp fast-leave
apic1(config-leaf-if)# ip igmp inherit interface-policy igmp_intpol1
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

ステップ 6 ファブリック RP を設定します。

例：

```
apic1(config)# tenant tenant1
apic1(config-tenant)# vrf context tenant1_vrf
apic1(config-tenant-vrf)# ip pim fabric-rp-address 20.1.15.1 route-map intervrf-ctx2
apic1(config-tenant-vrf)# ip pim fabric-rp-address 20.1.15.2 route-map intervrf-ctx1
apic1(config-tenant-vrf)# exit
```

ステップ 7 Inter-VRF マルチキャストを設定します。

例：

```
apic1(config-tenant)# vrf context tenant1_vrf
apic1(config-tenant-vrf)# ip pim inter-vrf-src ctx2 route-map intervrf-ctx2
apic1(config-tenant-vrf)# route-map intervrf-ctx2 permit 1
apic1(config-tenant-vrf)# match ip multicast group 226.20.0.0/24
apic1(config-tenant-vrf)#  exit
apic1(config-tenant)# exit
apic1(config)#
```

これにより、APIC のレイヤ 3 マルチキャストの設定を完了します。

NX-OS Style CLI を使用したレイヤ 3 IPv6 の設定

始める前に

- 目的の VRF、ブリッジ ドメイン、IPv6 アドレスを持つレイヤ 3 Out インターフェイスは、PIM6 が有効になるように設定する必要があります。レイヤ 3 Out の場合、IPv6 マルチキャストが機能するために、論理ノード プロファイルのノードに IPv6 ループバック アドレスが設定されます。
- 基本的なユニキャスト ネットワークを設定する必要があります。

手順

ステップ 1 VRF で PIM6 を有効にし、ランデブー ポイント（RP）を設定します。

例：

```
apic1(config)# tenant tenant1
apic1(config-tenant)# vrf context tenant1_vrf
apic1(config-tenant-vrf)# ipv6 pim
apic1(config-tenant-vrf)# ipv6 rp-address 2018::100:100:100:100 route-map ipv6_pim_routemap
```

ステップ 2 PIM6 インターフェイス ポリシーを設定し、レイヤ 3 Out に適用します。

例：

```
apic1(config-tenant)# l3out tenant1_l3out
apic1(config-tenant-l3out)# ipv6 pim
apic1(config-tenant-l3out)# exit
apic1(config-tenant)# exit
apic1(config)#
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/125
apic1(config-leaf-if) ipv6 pim inherit interface-policy pim6_intpol1
```

ステップ 3 BD で PIM6 を有効にします。

例：

```
apic1(config-tenant)# interface bridge-domain tenant1_bd
apic1(config-tenant-interface)# ipv6 multicast
apic1(config-tenant)# exit
apic1(config)#
```

PIM6 を使用したレイヤ 3 IPv6 マルチキャストが有効になります。

NX-OS スタイルの CLI を使用したマルチキャスト フィルタリングの構成

ブリッジ ドメイン レベルでマルチキャスト フィルタリングを設定します。このトピックの手順を使用して、ブリッジ ドメイン レベルで送信元フィルタリングまたは受信者フィルタリング、あるいはその両方を設定します。

始める前に

- マルチキャストフィルタリングを設定するブリッジ ドメインはすでに作成されています。
- ブリッジ ドメインは PIM 対応ブリッジ ドメインです。
- レイヤ 3 マルチキャストは VRF レベルで有効になります。

手順

ステップ 1 コンフィギュレーション モードを開始します。

```
apic1# configure
apic1(config)#
```

ステップ 2 テナントにアクセスし、PIM を有効にします。

```
apic1(config)# tenant tenant-name
apic1(config-tenant)# vrf context VRF-name
apic1(config-tenant-vrf)# ip pim
apic1(config-tenant-vrf)# exit
apic1(config-tenant)#
```

例：

```
apic1(config)# tenant t1
apic1(config-tenant)# vrf context v1
apic1(config-tenant-vrf)# ip pim
apic1(config-tenant-vrf)# exit
apic1(config-tenant)#
```

ステップ 3 マルチキャスト フィルタリングを構成するブリッジ ドメインにアクセスします。

```
apic1(config-tenant)# bridge-domain BD-name
apic1(config-tenant-bd)#
```

例：

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

ステップ 4 マルチキャスト *[送信元]* または *[受信者]* のフィルタリングを有効にするかどうかを決定します。

（注） 送信元フィルタリングと受信先フィルタリングの両方を同じブリッジドメインで有効にできます。

- このブリッジドメインでマルチキャスト送信元フィルタリングを有効にする場合は、次の例のように入力します。

```
apic1(config-tenant-bd)# src-filter source-route-map-policy
```

次に例を示します。

```
apic1(config-tenant-bd)# src-filter routemap-Mcast-src
```

- このブリッジドメインでマルチキャスト送信元フィルタリングを有効にする場合は、次の例のように入力します。

```
apic1(config-tenant-bd)# dst-filter destination-route-map-policy
```

次に例を示します。

```
apic1(config-tenant-bd)# dst-filter routemap-Mcast-dst
```

ステップ 5 IPv4 のマルチキャストを有効にします。

```
apic1(config-tenant-bd)# mcast-allow
apic1(config-tenant-bd)#
```

ステップ 6 VRF にブリッジ ドメインを関連付けます。

```
apic1(config-tenant-bd)# vrf member VRF-name
apic1(config-tenant-bd)# exit
apic1(config-tenant)#
```

例：

```
apic1(config-tenant-bd)# vrf member v1
apic1(config-tenant-bd)# exit
apic1(config-tenant)#
```

ステップ 7 ブリッジ ドメインでマルチキャストを有効にします。

```
apic1(config-tenant)# interface bridge-domain BD-name
apic1(config-tenant-interface)# ip multicast
apic1(config-tenant-interface)# exit
apic1(config-tenant)#
```

例：

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

```
apic1(config-tenant-interface)# ip multicast
apic1(config-tenant-interface)# exit
apic1(config-tenant)#
```

ステップ 8 ルート マップを設定します。

```
apic1(config-tenant)# route-map destination-route-map-policy <permit/deny> sequence_number
apic1(config-tenant-rtmap)# match ip multicast <source/group> IP_address_subnet
<source/group> IP_address_subnet
apic1(config-tenant-rtmap)# exit
apic1(config-tenant)# exit
apic1(config)#
```

例：

```
apic1(config-tenant)# route-map routemap-Mcast-src permit 1
apic1(config-tenant-rtmap)# match ip multicast source 10.10.1.1/24 group 192.1.1.1/32
apic1(config-tenant-rtmap)# exit
apic1(config-tenant)# route-map routemap-Mcast-dst permit 1
apic1(config-tenant-rtmap)# match ip multicast group 192.2.2.2/32
apic1(config-tenant-rtmap)# exit
apic1(config-tenant)# exit
apic1(config)#
```

NX-OS Style CLI を使用したマルチポッドの設定

NX-OS CLI を使用したマルチポッド ファブリックのセットアップ

始める前に

- ノード グループ ポリシーと L3Out ポリシーがすでに作成されています。

手順

ステップ 1 次の例に示すように、マルチポッドを設定します。

例：

```
ifav4-ifc1#  show run system
# Command: show running-config system
# Time: Mon Aug  1 21:32:03 2016
  system cluster-size 3
  system switch-id FOX2016G9DW 204 ifav4-spine4 pod 2
  system switch-id SAL1748H56D 201 ifav4-spine1 pod 1
  system switch-id SAL1803L25H 102 ifav4-leaf2 pod 1
  system switch-id SAL1819RXP4 101 ifav4-leaf1 pod 1
  system switch-id SAL1931LA3B 203 ifav4-spine2 pod 2
  system switch-id SAL1934MNY0 103 ifav4-leaf3 pod 1
  system switch-id SAL1934MNY3 104 ifav4-leaf4 pod 1
```

```
  system switch-id SAL1938P7A6 202 ifav4-spine3 pod 1
  system switch-id SAL1938PHBB 105 ifav4-leaf5 pod 2
  system switch-id SAL1942R857 106 ifav4-leaf6 pod 2
  system pod 1 tep-pool 10.0.0.0/16
  system pod 2 tep-pool 10.1.0.0/16
ifav4-ifc1#
```

ステップ 2 次の例のよ、VLAN ドメインを設定します。

例：

```
ifav4-ifc1# show running-config vlan-domain l3Dom
# Command: show running-config vlan-domain l3Dom
# Time: Mon Aug  1 21:32:31 2016
  vlan-domain l3Dom
    vlan 4
    exit
ifav4-ifc1#
```

ステップ 3 次の例のよ、ファブリックの外部接続を設定します。

例：

```
ifav4-ifc1# show running-config fabric-external
# Command: show running-config fabric-external
# Time: Mon Aug  1 21:34:17 2016
  fabric-external 1
    bgp evpn peering
    pod 1
      interpod data hardware-proxy 100.11.1.1/32
      bgp evpn peering
      exit
    pod 2
      interpod data hardware-proxy 200.11.1.1/32
      bgp evpn peering
      exit
    route-map interpod-import
      ip prefix-list default permit 0.0.0.0/0
      exit
    route-target extended 5:16
    exit
ifav4-ifc1#
```

ステップ 4 スパイン スイッチ インターフェイスと次の例のよの OSPF 設定を構成します。

例：

```
# Command: show running-config spine
# Time: Mon Aug  1 21:34:41 2016
  spine 201
    vrf context tenant infra vrf overlay-1
      router-id 201.201.201.201
      exit
    interface ethernet 1/1
      vlan-domain member l3Dom
      exit
    interface ethernet 1/1.4
      vrf member tenant infra vrf overlay-1
      ip address 201.1.1.1/30
      ip router ospf default area 1.1.1.1
      ip ospf cost 1
      exit
    interface ethernet 1/2
      vlan-domain member l3Dom
      exit
```

NX-OS スタイル CLI を使用したタスクの実行

```
  interface ethernet 1/2.4
    vrf member tenant infra vrf overlay-1
    ip address 201.2.1.1/30
    ip router ospf default area 1.1.1.1
    ip ospf cost 1
    exit
  router ospf default
    vrf member tenant infra vrf overlay-1
      area 1.1.1.1 loopback 201.201.201.201
      area 1.1.1.1 interpod peering
      exit
    exit
  exit
spine 202
  vrf context tenant infra vrf overlay-1
    router-id 202.202.202.202
    exit
  interface ethernet 1/2
    vlan-domain member l3Dom
    exit
  interface ethernet 1/2.4
        vrf member tenant infra vrf overlay-1
    ip address 202.1.1.1/30
    ip router ospf default area 1.1.1.1
    exit
  router ospf default
    vrf member tenant infra vrf overlay-1
      area 1.1.1.1 loopback 202.202.202.202
      area 1.1.1.1 interpod peering
      exit
    exit
  exit
spine 203
  vrf context tenant infra vrf overlay-1
    router-id 203.203.203.203
    exit
  interface ethernet 1/1
    vlan-domain member l3Dom
    exit
  interface ethernet 1/1.4
    vrf member tenant infra vrf overlay-1
    ip address 203.1.1.1/30
    ip router ospf default area 0.0.0.0
    ip ospf cost 1
    exit
  interface ethernet 1/2
    vlan-domain member l3Dom
    exit
  interface ethernet 1/2.4
    vrf member tenant infra vrf overlay-1
    ip address 203.2.1.1/30
    ip router ospf default area 0.0.0.0
    ip ospf cost 1
    exit
  router ospf default
    vrf member tenant infra vrf overlay-1
      area 0.0.0.0 loopback 203.203.203.203
      area 0.0.0.0 interpod peering
      exit
    exit
  exit
spine 204
  vrf context tenant infra vrf overlay-1
    router-id 204.204.204.204
```

```
    exit
  interface ethernet 1/31
    vlan-domain member l3Dom
    exit
  interface ethernet 1/31.4
    vrf member tenant infra vrf overlay-1
    ip address 204.1.1.1/30
    ip router ospf default area 0.0.0.0
    ip ospf cost 1
    exit
  router ospf default
    vrf member tenant infra vrf overlay-1
      area 0.0.0.0 loopback 204.204.204.204
      area 0.0.0.0 interpod peering
      exit
    exit
  exit
ifav4-ifc1#
```

NX-OS Style CLI を使用したリモート リーフ スイッチの設定

NX-OS スタイル CLI を使用したリモート リーフ スイッチの設定

この例では、リーフ スイッチがメインのファブリック ポッドと通信できるようにするため、スパイン スイッチとリモート リーフ スイッチを設定しています。

始める前に

- IPN ルータとリモート リーフ スイッチはアクティブで設定されています。WAN ルータとリモート リーフ スイッチ設定の注意事項 （154 ページ） を参照してください。
- リモート リーフ スイッチは、13.1.x 以降 (aci n9000 dk9.13.1.x.x.bin) のスイッチ イメージを実行しています。
- リモート リーフ スイッチを追加する予定のポッドが作成され、設定されています。

手順

ステップ 1 ポッド 2 のリモート ロケーション 5 で TEP プールを定義します。

ネットワーク マスクは /24 以下である必要があります。

次の新しいコマンドを使用します：**system remote-leaf-site** *site-id* **pod** *pod-id* **tep-pool** *ip-address-and-netmask*

例：

```
apic1(config)# system remote-leaf-site 5 pod 2 tep-pool 192.0.0.0/16
```

ステップ 2 ポッド 2 の、リモート リーフ サイト 5 にリモート リーフ スイッチを追加します。

NX-OS スタイル CLI を使用したタスクの実行

次のコマンドを使用します：**system switch-id** *serial-number node-id leaf-switch-name***pod** *pod-id* **remote-leaf-site** *remote-leaf-site-id* **node-type remote-leaf-wan**

例：

```
apic1(config)# system switch-id FDO210805SKD 109 ifav4-leaf9 pod 2
remote-leaf-site 5 node-type remote-leaf-wan
```

ステップ 3 VLAN 4 を含む VLAN で VLAN ドメインを設定します。

例：

```
apic1(config)# vlan-domain ospfDom
apic1(config-vlan)# vlan 4-5
apic1(config-vlan)# exit
```

ステップ 4 インフラ テナントに 2 つの L3Out を設定します。1 つはリモート リーフ接続のためで、もう 1 つはマルチポッド IPN のためです。

例：

```
apic1(config)# tenant infra
apic1(config-tenant)# l3out rl-wan
apic1(config-tenant-l3out)# vrf member overlay-1
apic1(config-tenant-l3out)# exit
apic1(config-tenant)# l3out ipn-multipodInternal
apic1(config-tenant-l3out)# vrf member overlay-1
apic1(config-tenant-l3out)# exit
apic1(config-tenant)# exit
apic1(config)#
```

ステップ 5 L3Out が使用する、スパイン スイッチ インターフェイスとサブインターフェイスを設定します。

例：

```
apic1(config)# spine 201
apic1(config-spine)# vrf context tenant infra vrf overlay-1 l3out rl-wan-test
apic1(config-spine-vrf)# exit
apic1(config-spine)# vrf context tenant infra vrf overlay-1 l3out ipn-multipodInternal
apic1(config-spine-vrf)# exit
apic1(config-spine)#
apic1(config-spine)# interface ethernet 8/36
apic1(config-spine-if)# vlan-domain member ospfDom
apic1(config-spine-if)# exit
apic1(config-spine)# router ospf default
apic1(config-spine-ospf)# vrf member tenant infra vrf overlay-1
apic1(config-spine-ospf-vrf)# area 5 l3out rl-wan-test
apic1(config-spine-ospf-vrf)# exit
apic1(config-spine-ospf)# exit
apic1(config-spine)#
apic1(config-spine)# interface ethernet 8/36.4
apic1(config-spine-if)# vrf member tenant infra vrf overlay-1 l3out rl-wan-test
apic1(config-spine-if)# ip router ospf default area 5
apic1(config-spine-if)# exit
apic1(config-spine)# router ospf multipod-internal
apic1(config-spine-ospf)# vrf member tenant infra vrf overlay-1
apic1(config-spine-ospf-vrf)# area 5 l3out ipn-multipodInternal
apic1(config-spine-ospf-vrf)# exit
apic1(config-spine-ospf)# exit
apic1(config-spine)#
apic1(config-spine)# interface ethernet 8/36.5
```

```
apic1(config-spine-if)# vrf member tenant infra vrf overlay-1 l3out ipn-multipodInternal
apic1(config-spine-if)# ip router ospf multipod-internal area 5
apic1(config-spine-if)# exit
apic1(config-spine)# exit
apic1(config)#
```

ステップ 6 メインのファブリック ポッドと通信するために使用するリモートのリーフ スイッチ インターフェイスとサブインターフェイスを設定します。

例：

```
(config)# leaf 101
apic1(config-leaf)# vrf context tenant infra vrf overlay-1 l3out rl-wan-test
apic1(config-leaf-vrf)# exit
apic1(config-leaf)#
apic1(config-leaf)# interface ethernet 1/49
apic1(config-leaf-if)# vlan-domain member ospfDom
apic1(config-leaf-if)# exit
apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant infra vrf overlay-1
apic1(config-leaf-ospf-vrf)# area 5 l3out rl-wan-test
apic1(config-leaf-ospf-vrf)# exit
apic1(config-leaf-ospf)# exit
apic1(config-leaf)#
apic1(config-leaf)# interface ethernet 1/49.4
apic1(config-leaf-if)# vrf member tenant infra vrf overlay-1 l3out rl-wan-test
apic1(config-leaf-if)# ip router ospf default area 5
apic1(config-leaf-if)# exit
```

例

次の例は、ダウンロード可能な設定を示しています:

```
apic1# configure
apic1(config)# system remote-leaf-site 5 pod 2 tep-pool 192.0.0.0/16
apic1(config)# system switch-id FDO210805SKD 109 ifav4-leaf9 pod 2
remote-leaf-site 5 node-type remote-leaf-wan
apic1(config)# vlan-domain ospfDom
apic1(config-vlan)# vlan 4-5
apic1(config-vlan)# exit
apic1(config)# tenant infra
apic1(config-tenant)# l3out rl-wan-test
apic1(config-tenant-l3out)# vrf member overlay-1
apic1(config-tenant-l3out)# exit
apic1(config-tenant)# l3out ipn-multipodInternal
apic1(config-tenant-l3out)# vrf member overlay-1
apic1(config-tenant-l3out)# exit
apic1(config-tenant)# exit
apic1(config)#
apic1(config)# spine 201
apic1(config-spine)# vrf context tenant infra vrf overlay-1 l3out rl-wan-test
apic1(config-spine-vrf)# exit
apic1(config-spine)# vrf context tenant infra vrf overlay-1 l3out ipn-multipodInternal
apic1(config-spine-vrf)# exit
apic1(config-spine)#
apic1(config-spine)# interface ethernet 8/36
apic1(config-spine-if)# vlan-domain member ospfDom
apic1(config-spine-if)# exit
apic1(config-spine)# router ospf default
apic1(config-spine-ospf)# vrf member tenant infra vrf overlay-1
```

```
apic1(config-spine-ospf-vrf)# area 5 l3out rl-wan-test
apic1(config-spine-ospf-vrf)# exit
apic1(config-spine-ospf)# exit
apic1(config-spine)#
apic1(config-spine)# interface ethernet 8/36.4
apic1(config-spine-if)# vrf member tenant infra vrf overlay-1 l3out rl-wan-test
apic1(config-spine-if)# ip router ospf default area 5
apic1(config-spine-if)# exit
apic1(config-spine)# router ospf multipod-internal
apic1(config-spine-ospf)# vrf member tenant infra vrf overlay-1
apic1(config-spine-ospf-vrf)# area 5 l3out ipn-multipodInternal
apic1(config-spine-ospf-vrf)# exit
apic1(config-spine-ospf)# exit
apic1(config-spine)#
apic1(config-spine)# interface ethernet 8/36.5
apic1(config-spine-if)# vrf member tenant infra vrf overlay-1 l3out ipn-multipodInternal
apic1(config-spine-if)# ip router ospf multipod-internal area 5
apic1(config-spine-if)# exit
apic1(config-spine)# exit
apic1(config)#
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant infra vrf overlay-1 l3out rl-wan-test
apic1(config-leaf-vrf)# exit
apic1(config-leaf)#
apic1(config-leaf)# interface ethernet 1/49
apic1(config-leaf-if)# vlan-domain member ospfDom
apic1(config-leaf-if)# exit
apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant infra vrf overlay-1
apic1(config-leaf-ospf-vrf)# area 5 l3out rl-wan-test
apic1(config-leaf-ospf-vrf)# exit
apic1(config-leaf-ospf)# exit
apic1(config-leaf)#
apic1(config-leaf)# interface ethernet 1/49.4
apic1(config-leaf-if)# vrf member tenant infra vrf overlay-1 l3out rl-wan-test
apic1(config-leaf-if)# ip router ospf default area 5
apic1(config-leaf-if)# exit
```

パートII：外部ルーティング（L3Out）の設定

外部ネットワークへのルーテッド接続

NX-OS Style CLI を使用した MP-BGP ルート リフレクタの設定

ACI ファブリックの MP-BGP ルート リフレクタの設定

ACI ファブリック内のルートを配布するために、MP-BGP プロセスを最初に実行し、スパインスイッチを BGP ルート リフレクタとして設定する必要があります。

次に、MP-BGP ルート リフレクタの設定例を示します。

（注） この例では、BGP ファブリック ASN は 100 です。スパイン スイッチ 104 と 105 が MP-BGP ルート リフレクタとして選択されます。

```
apic1(config)# bgp-fabric
apic1(config-bgp-fabric)# asn 100
apic1(config-bgp-fabric)# route-reflector spine 104,105
```

L3Out のノードとインターフェイス

NX-OS Style CLI を使用したレイヤ 3 ルーテッド ポート チャネルとサブインターフェイス ポート チャネルの設定

ポート チャネルの NX-OS は、CLI を使用してをルーテッド レイヤ 3 の設定

この手順では、レイヤ 3 ルーテッドポート チャネルを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**leaf** *node-id* 例： `apic1(config)# leaf 101`	リーフ スイッチまたはリーフ スイッチの設定を指定します。*Node-id* は形式 *node-id1-node-id2* の単一ノード ID または ID の範囲となる可能性があり、設定が適用されます。
ステップ 3	**interface port-channel** *channel-name* 例： `apic1(config-leaf)# interface port-channel po1`	指定したポート チャネルのインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**no switchport** 例： `apic1(config-leaf-if)# no switchport`	レイヤ 3 インターフェイスを可能になります。
ステップ 5	**vrf member** *vrf-name* **tenant** *tenant-name* 例： `apic1(config-leaf-if)# vrf member v1 tenant t1`	この仮想ルーティングおよび転送(VRF)インスタンスと L3 ポリシー、外部には、このポート チャネルを関連付けます場所。

NX-OS スタイル CLI を使用したタスクの実行

	コマンドまたはアクション	目的
		• *Vrf-name* は VRF 名です。32 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。 • テナント名 は、テナント名です。32 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。
ステップ 6	**vlan-domain member** *vlan-domain-name* 例： `apic1(config-leaf-if)# vlan-domain member dom1`	以前に設定された VLAN ドメインには、ポートチャネルのテンプレートを関連付けます。
ステップ 7	**ip address** *ip-address/subnet-mask* 例： `apic1(config-leaf-if)# ip address 10.1.1.1/24`	指定した インターフェイスの IP アドレスとサブネット マスクを設定します。
ステップ 8	**ipv6 address** *sub-bits/prefix-length* **preferred** 例： `apic1(config-leaf-if)# ipv6 address 2001::1/64 preferred`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスにおける IPv6 処理をイネーブルにします。場所： • *sub-bits* i引数は、prefix-name 引数で指定された一般的なプレフィックスによって提供されるプレフィックスに連結する、アドレスのサブプレフィックス ビットおよびホスト ビットです。sub-bits 引数は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16進数値を 16 ビット単位でコロンで区切って指定します。 • *Prefix-length* は IPv6 プレフィックスの長さです。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。

	コマンドまたはアクション	目的
ステップ 9	**ipv6 link-local** *ipv6-link-local-address* 例： `apic1(config-leaf-if)# ipv6 link-local fe80::1`	インターフェイスにIPv6リンクローカル アドレスを設定します。
ステップ 10	**mac-address** *mac-address* 例： `apic1(config-leaf-if)# mac-address 00:44:55:66:55::01`	インターフェイス MAC アドレスを手動で設定します。
ステップ 11	**mtu** *mtu-value* 例： `apic1(config-leaf-if)# mtu 1500`	このサービス クラスの MTU を設定します

例

この例では、基本レイヤ 3 ポート チャネルを設定する方法を示します。

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface port-channel po1
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vrf member v1 tenant t1
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# ip address 10.1.1.1/24
apic1(config-leaf-if)# ipv6 address 2001::1/64 preferred
apic1(config-leaf-if)# ipv6 link-local fe80::1
apic1(config-leaf-if)# mac-address 00:44:55:66:55::01
apic1(config-leaf-if)# mtu 1500
```

NX-OS CLI を使用したレイヤ 3 サブインターフェイス ポート チャネルの設定

この手順では、レイヤ 3 サブインターフェイス ポート チャネルを設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**leaf** *node-id* 例：	リーフ スイッチまたはリーフ スイッチの設定を指定します。*Node-id* は形式

NX-OS スタイル CLI を使用したタスクの実行

	コマンドまたはアクション	目的
	`apic1(config)# leaf 101`	*node-id1-node-id2* の単一ノード ID またはIDの範囲となる可能性があり、設定が適用されます。
ステップ 3	**vrf member** *vrf-name* **tenant** *tenant-name* 例： `apic1(config-leaf-if)# vrf member v1 tenant t1`	この仮想ルーティングおよび転送(VRF)インスタンスと L3 アウトサイド ポリシーにポート チャネルを関連付けます。場所： • *Vrf-name* は VRF 名です。32 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。 • テナント名 は、テナント名です。32 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。
ステップ 4	**vlan-domain member** *vlan-domain-name* 例： `apic1(config-leaf-if)# vlan-domain member dom1`	以前に設定された VLAN ドメインには、ポートチャネルのテンプレートを関連付けます。
ステップ 5	**ip address** *ip-address* / *subnet-mask* 例： `apic1(config-leaf-if)# ip address 10.1.1.1/24`	指定した インターフェイスの IP アドレスとサブネット マスクを設定します。
ステップ 6	**ipv6 address** *sub-bits* / *prefix-length* **preferred** 例： `apic1(config-leaf-if)# ipv6 address 2001::1/64 preferred`	IPv6 の一般的なプレフィックスに基づいてIPv6アドレスを設定し、インターフェイスにおけるIPv6処理をイネーブルにします。場所： • *sub-bits* i引数は、prefix-name 引数で指定された一般的なプレフィックスによって提供されるプレフィックスに連結する、アドレスのサブプレフィックス ビットおよびホスト ビットです。sub-bits 引数は、RFC 2373 に記載された形式で指定する必要があります。この形式では、アドレスは、16進数値を16ビット単位でコロンで区切って指定します。

NX-OS スタイル CLI を使用したタスクの実行

	コマンドまたはアクション	目的
		• *Prefix-length* は IPv6 プレフィックスの長さです。プレフィックス（アドレスのネットワーク部分）を構成するアドレスの上位連続ビット数を示す 10 進値です。10 進数値の前にスラッシュ記号が必要です。
ステップ 7	**ipv6 link-local** *ipv6-link-local-address* 例： `apic1(config-leaf-if)# ipv6 link-local fe80::1`	インターフェイスに IPv6 リンクローカル アドレスを設定します。
ステップ 8	**mac-address** *mac-address* 例： `apic1(config-leaf-if)# mac-address 00:44:55:66:55::01`	インターフェイス MAC アドレスを手動で設定します。
ステップ 9	**mtu** *mtu-value* 例： `apic1(config-leaf-if)# mtu 1500`	このサービス クラスの MTU を設定します
ステップ 10	exit 例： `apic1(config-leaf-if)# exit`	設定モードに戻ります。
ステップ 11	**interface port-channel** *channel-name* 例： `apic1(config-leaf)# interface port-channel po1`	指定したポート チャネルのインターフェイス コンフィギュレーション モードを開始します。
ステップ 12	**vlan-domain member** *vlan-domain-name* 例： `apic1(config-leaf-if)# vlan-domain member dom1`	以前に設定された VLAN ドメインには、ポートチャネルのテンプレートを関連付けます。
ステップ 13	exit 例： `apic1(config-leaf-if)# exit`	設定モードに戻ります。
ステップ 14	**interface port-channel** *channel-name.number* 例：	指定したサブインターフェイス ポート チャネルのインターフェイス設定モードを開始します。

NX-OS スタイル CLI を使用したタスクの実行

	コマンドまたはアクション	目的
	`apic1(config-leaf)# interface port-channel po1.2001`	
ステップ 15	**vrf member** *vrf-name* **tenant** *tenant-name* 例： `apic1(config-leaf-if)# vrf member v1 tenant t1`	この仮想ルーティングおよび転送(VRF)インスタンスと L3 アウトサイド ポリシーにポート チャネルを関連付けます。場所： • *Vrf-name* は VRF 名です。32 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。 • テナント名 は、テナント名です。32 文字以内の英数字のストリング（大文字と小文字を区別）で指定します。
ステップ 16	exit 例： `apic1(config-leaf-if)# exit`	設定モードに戻ります。

例

この例では、基本的なレイヤ 3 サブインターフェイス ポートチャネルを設定する方法を示します。

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface vlan 2001
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vrf member v1 tenant t1
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# ip address 10.1.1.1/24
apic1(config-leaf-if)# ipv6 address 2001::1/64 preferred
apic1(config-leaf-if)# ipv6 link-local fe80::1
apic1(config-leaf-if)# mac-address 00:44:55:66:55::01
apic1(config-leaf-if)# mtu 1500
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface port-channel po1
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface port-channel po1.2001
apic1(config-leaf-if)# vrf member v1 tenant t1
apic1(config-leaf-if)# exit
```

NX-OS CLI を使用したレイヤ 3 ポート チャネルにポートを追加する

この手順では、以前に設定したレイヤ 3 ポート チャネルにポートを追加します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**leaf** *node-id* 例： `apic1(config)# leaf 101`	リーフ スイッチまたはリーフ スイッチの設定を指定します。*Node-id* は形式 *node-id1-node-id2* の単一ノード ID または ID の範囲となる可能性があり、設定が適用されます。
ステップ 3	**interface Ethernet** *slot/port* 例： `apic1(config-leaf)# interface Ethernet 1/1-2`	設定するインターフェイスのインターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**channel-group** チャネル名 例： `apic1(config-leaf-if)# channel-group p01`	チャネル グループでポートを設定します。

例

この例では、ポートをレイヤ 3 にポートチャネルを追加する方法を示します。

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface Ethernet 1/1-2
apic1(config-leaf-if)# channel-group p01
```

NX-OS Style CLI を使用したスイッチ仮想インターフェイスの設定

NX-OS スタイル CLI を使用して、SVI インターフェイスのカプセル化スコープの設定

SVIインターフェイス カプセル化のスコープ設定を次の例表示する手順では、名前付きのレイヤ 3 アウト設定です。

手順

	コマンドまたはアクション	目的
ステップ 1	コンフィギュレーション モードを開始します。 例： `apic1# configure`	コンフィギュレーション モードを開始します。
ステップ 2	スイッチ モードを開始します。 例： `apic1(config)# leaf 104`	スイッチ モードを開始します。
ステップ 3	VLANインターフェイスを作成します。 例： `apic1(config-leaf)# interface vlan 2001`	VLANインターフェイスを作成します。VLAN の範囲は 1 ～ 4094 です。
ステップ 4	カプセル化の範囲を指定します。 例： `apic1(config-leaf-if)# encap scope vrf context`	カプセル化の範囲を指定します。
ステップ 5	インターフェイスモードを終了します。 例： `apic1(config-leaf-if)# exit`	インターフェイスモードを終了します。

NX-OS スタイル CLI を使用した SVI 自動状態の設定

始める前に

- テナントと VRF が設定されています。
- レイヤ3アウトが設定されており、レイヤ3アウトの論理ノードプロファイルと論理インターフェイス プロファイルが設定されています。

手順

	コマンドまたはアクション	目的
ステップ 1	コンフィギュレーション モードを開始します。 例： `apic1# configure`	コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	スイッチ モードを開始します。 例： `apic1(config)# leaf 104`	スイッチ モードを開始します。
ステップ 3	VLANインターフェイスを作成します。 例： `apic1(config-leaf)# interface vlan 2001`	VLANインターフェイスを作成します。VLAN の範囲は 1 ～ 4094 です。
ステップ 4	SVI 自動状態を有効にします。 例： `apic1(config-leaf-if)# autostate`	SVI 自動状態を有効にします。 デフォルトで、SVI 自動状態の値は有効ではありません。
ステップ 5	インターフェイスモードを終了します。 例： `apic1(config-leaf-if)# exit`	インターフェイスモードを終了します。

NX-OS Style CLI を使用したルーティング プロトコルの設定

NX-OS Style CLI を使用した BFD サポート付き BGP 外部ルーテッド ネットワークの設定

NX-OS スタイルの CLI を使用した BGP 外部ルーテッド ネットワークの設定

手順

ここでは、NX-OS CLI を使用して BGP 外部ルーテッド ネットワークを設定する方法を示します。

例：

```
apic1(config-leaf)# template route-profile damp_rp tenant t1
This template will be available on all leaves where tenant t1 has a VRF deployment
apic1(config-leaf-template-route-profile)# set dampening 15 750 2000 60
apic1(config-leaf-template-route-profile)# exit
apic1(config-leaf)#
apic1(config-leaf)# router bgp 100
apic1(config-bgp)# vrf member tenant t1 vrf ctx3
apic1(config-leaf-bgp-vrf)# neighbor 32.0.1.0/24 l3out l3out-bgp
apic1(config-leaf-bgp-vrf-neighbor)# update-source ethernet 1/16.401
apic1(config-leaf-bgp-vrf-neighbor)# address-family ipv4 unicast
apic1(config-leaf-bgp-vrf-neighbor-af)# weight 400
apic1(config-leaf-bgp-vrf-neighbor-af)# exit
apic1(config-leaf-bgp-vrf-neighbor)# remote-as 65001
apic1(config-leaf-bgp-vrf-neighbor)# private-as-control remove-exclusive
apic1(config-leaf-bgp-vrf-neighbor)# private-as-control remove-exclusive-all
apic1(config-leaf-bgp-vrf-neighbor)# private-as-control remove-exclusive-all-replace-as
```

```
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# address-family ipv4 unicast
apic1(config-leaf-bgp-vrf-af)# inherit bgp dampening damp_rp
This template will be inherited on all leaves where VRF ctx3 has been deployed
apic1(config-leaf-bgp-vrf-af)# exit
apic1(config-leaf-bgp-vrf)# address-family ipv6 unicast
apic1(config-leaf-bgp-vrf-af)# inherit bgp dampening damp_rp
This template will be inherited on all leaves where VRF ctx3 has been deployed
apic1(config-leaf-bgp-vrf-af)# exit
```

NX-OS スタイルの CLI を使用した BGP 最大パスの設定

始める前に

次のフィールドの許容値については、Cisco APIC ドキュメンテーション ページの 『Verified Scalability Guide for Cisco APIC』を参照してください。https://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

適切なテナントと BGP 外部ルーテッド ネットワークが作成され、使用可能になっています。

BGP にログインして、次のコマンドを使用します:

- eBGP パスのマルチパスを設定するためのコマンド：

  ```
  maximum-paths <value>
  ```

  ```
  no maximum-paths <value>
  ```

- iBGP パスのマルチパスを設定するためのコマンド：

  ```
  maximum-paths ibgp <value>
  ```

  ```
  no maximum-paths ibgp <value>
  ```

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# template bgp address-family newAf tenant t1
This template will be available on all nodes where tenant t1 has a VRF deployment
apic1(config-bgp-af)# maximum-paths ?
<1-64>  Number of parallel paths
ibgp  Configure multipath for IBGP paths
apic1(config-bgp-af)# maximum-paths 10
apic1(config-bgp-af)# maximum-paths ibgp 8
apic1(config-bgp-af)# end
apic1#
```

NX-OS スタイルの CLI を使用した AS パスのプリペンド

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、AS パスのプリペンド機能を実現する方法について説明します。

始める前に

構成済みのテナント

手順

境界ゲートウェイ プロトコル (BGP) ルートの自動システムパス (AS パス) を変更するには、`set as-path` コマンドを使用します。set as-path コマンドは、
`apic1(config-leaf-vrf-template-route-profile)# set as-path {'prepend as-num [ ,... as-num ] | prepend-last-as num}` の形式で実行します。

例：

```
apic1(config)# leaf 103
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# template route-profile rp1
apic1(config-leaf-vrf-template-route-profile)# set as-path ?
prepend Prepend to the AS-Path
prepend-last-as Prepend last AS to the as-path
apic1(config-leaf-vrf-template-route-profile)# set as-path prepend 100, 101, 102, 103
apic1(config-leaf-vrf-template-route-profile)# set as-path prepend-last-as 8
apic1(config-leaf-vrf-template-route-profile)# exit
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# exit
```

次のタスク

AS パスのプリペンドを無効にするには、示されているコマンドの no 形式を使用します:

```
apic1(config-leaf-vrf-template-route-profile)# [no] set
as-path { prepend as-num [ ,... as-num ] | prepend-last-as num}
```

NX-OS Style CLI を使用した BGP ネイバー シャットダウンの設定

NX-OS Style CLI を使用した *BGP* ネイバー シャットダウンの設定

次の手順では、NX-OS CLI を使用して BGP ネイバー シャットダウン機能を使用する方法について説明します。

手順

ステップ 1 L3Out のノードとインターフェイスを設定します。

この例では設定 VRF `v1` ノード 103 (border リーフ スイッチ) と呼ばれるで `nodep1` 、ルータ ID を `11.11.11.103` 。インターフェイスの設定も `eth1/3` ルーテッド インターフェイス (レイヤ 3 のポート)、IP アドレスとして `12.12.12.3/24` とレイヤ 3 ドメイン `dom1` 。

例：

```
apic1(config)# leaf 103
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# router-id 11.11.11.103
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# interface ethernet 1/3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vrf member tenant t1 vrf v1
apic1(config-leaf-if)# ip address 12.12.12.3/24
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

ステップ 2 BGP ルーティング プロトコルを設定します。

この例では、15.15.15.2 および ASN 100 の BGP ピア アドレスを使用して、プライマリのルーティング プロトコルとして BGP を設定します。

例：

```
apic1(config)# leaf 103
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 15.15.15.2
```

ステップ 3 BGPネイバーシャットダウン機能を使用します。

例：

```
apic1(config-leaf-bgp-vrf-neighbor)# shutdown
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# exit
```

NX-OS スタイル CLI を使用してノード BGP タイマー ポリシーあたりの VRF あたりを設定する

手順

	コマンドまたはアクション	目的

ステップ 1	タイマーポリシーを作成する前に、BGP ASN およびルート リフレクタを設定します。
	例：
	`apic1(config)#`
	`apic1(config)# bgp-fabric`
	`apic1(config-bgp-fabric)#`
	`route-reflector spine 102`
	`apic1(config-bgp-fabric)# asn 42`
	`apic1(config-bgp-fabric)# exit`
	`apic1(config)# exit`
	`apic1#`	

NX-OS スタイル CLI を使用したタスクの実行

	コマンドまたはアクション	目的

ステップ 2	タイマー ポリシーを作成します。
	例：
	`apic1# config`
	`apic1(config)# leaf 101`
	`apic1(config-leaf)# template bgp timers pol7 tenant tn1`
	`This template will be available on all nodes where tenant tn1 has a VRF deployment`
	`apic1(config-bgp-timers)# timers bgp 120 240`
	`apic1(config-bgp-timers)# graceful-restart stalepath-time 500`
	`apic1(config-bgp-timers)# maxas-limit 300`
	`apic1(config-bgp-timers)# exit`
	`apic1(config-leaf)# exit`
	`apic1(config)# exit`
	`apic1#`
		特定の値は、例としてのみ提供されます。

ステップ 3	設定された BGP ポリシーを表示します。
	例：
	`apic1# show run leaf 101 template bgp timers pol7`
	`# Command: show running-config leaf 101 template bgp timers pol7`
	`leaf 101`
	`template bgp timers pol7 tenant tn1`
	`timers bgp 120 240`
	`graceful-restart stalepath-time 500`
	`maxas-limit 300`
	`exit`
	`exit`	

ステップ 4	ノードで特定のポリシーを参照します。
	例：
	`apic1# config`
	`apic1(config)# leaf 101`
	`apic1(config-leaf)# router bgp 42`
	`apic1(config-leaf-bgp)# vrf member tenant tn1 vrf ctx1`
	`apic1(config-leaf-bgp-vrf)# inherit node-only bgp timer pol7`
	`apic1(config-leaf-bgp-vrf)# exit`
	`apic1(config-leaf-bgp)# exit`
	`apic1(config-leaf)# exit`
	`apic1(config)# exit`
	`apic1#`	

	コマンドまたはアクション	目的

ステップ 5	特定の BGP のタイマー ポリシーのノードが表示されます。
	例：
	`apic1# show run leaf 101 router bgp 42 vrf member tenant tn1 vrf ctx1`
	`# Command: show running-config leaf 101 router bgp 42 vrf member tenant tn1 vrf ctx1`
	`leaf 101`
	`router bgp 42`
	`vrf member tenant tn1 vrf ctx1`
	`inherit node-only bgp timer pol7`
	`exit`
	`exit`
	`exit`
	`apic1#`	

NX-OS スタイルの CLI を使用したセカンダリ IP アドレスでの双方向フォワーディング検出の設定

この手順では、NX-OS スタイルの CLI を使用して、セカンダリ IP アドレスに双方向転送検出 (BFD) を設定します。この例ではノード 103 (border リーフ スイッチ) で、ルータ ID を 11.11.11.103で VRF v1 を構成します。 また、インターフェイス eth1/3 をルーテッド インターフェイス（レイヤ 3 のポート）として構成し、IP アドレス 12.12.12.3/24 をプライマリ アドレスとして、6.11.1.224/24 をレイヤー 3 ドメイン dom1 のセカンダリ アドレスとして構成します。BFD は 99.99.99.14/32 で有効になっており、セカンダリ サブネット 6.11.1.0/24 を使用して到達可能です。

手順

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# configure terminal
```

ステップ 2 リーフ スイッチ 103 の構成モードを開始します。

例：

```
apic1(config)# leaf 103
```

ステップ 3 VRF インスタンスの構成モードを開始します。

例：

```
apic1(config-leaf)# vrf context tenant t1 vrf v1
```

ステップ 4 セカンダリ IP アドレスを構成します。

例：

```
apic1(config-leaf-vrf)# router-id 1.1.24.24
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# interface ethernet 1/3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vrf member tenant t1 vrf v1
apic1(config-leaf-if)# ip address 12.12.12.3/24
apic1(config-leaf-if)# ip address 6.11.1.224/24 secondary
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

ステップ 5 BFD を有効にします。

例：

```
apic1(config-leaf)# vrf context tenant t1 vrf v1 l3out Routed
apic1(config-leaf-vrf)#router-id 1.1.24.24
apic1(config-leaf-vrf)#ip route 95.95.95.95/32 12.12.12.4 bfd
apic1(config-leaf-vrf)#ip route 99.99.99.14/32 6.11.1.100 bfd
```

NX-OS スタイル CLI を使用したリーフ スイッチでの BFD のグローバルな設定

手順

ステップ 1 NX-OS CLI を使用して BFD IPV4 グローバル設定（bfdIpv4InstPol）を設定するには：

例：

```
apic1# configure
apic1(config)# template bfd ip bfd_ipv4_global_policy
apic1(config-bfd)# [no] echo-address 1.2.3.4
apic1(config-bfd)# [no] slow-timer 2500
apic1(config-bfd)# [no] min-tx 100
apic1(config-bfd)# [no] min-rx 70
apic1(config-bfd)# [no] multiplier 3
apic1(config-bfd)# [no] echo-rx-interval 500
apic1(config-bfd)# exit
```

ステップ 2 NX-OS CLI を使用して BFD IPV6 グローバル設定（bfdIpv6InstPol）を設定するには：

例：

```
apic1# configure
apic1(config)# template bfd ipv6 bfd_ipv6_global_policy
apic1(config-bfd)# [no] echo-address 34::1/64
apic1(config-bfd)# [no] slow-timer 2500
apic1(config-bfd)# [no] min-tx 100
apic1(config-bfd)# [no] min-rx 70
apic1(config-bfd)# [no] multiplier 3
apic1(config-bfd)# [no] echo-rx-interval 500
apic1(config-bfd)# exit
```

ステップ 3 NX-OS CLI を使用してアクセス リーフ ポリシー グループ (infraAccNodePGrp) を設定し、以前に作成した BFD グローバル ポリシーを継承するには:

例：

```
apic1# configure
apic1(config)# template leaf-policy-group test_leaf_policy_group
apic1(config-leaf-policy-group)# [no] inherit bfd ip bfd_ipv4_global_policy
apic1(config-leaf-policy-group)# [no] inherit bfd ipv6 bfd_ipv6_global_policy
apic1(config-leaf-policy-group)# exit
```

ステップ 4 NX-OS CLI を使用して以前に作成したリーフ ポリシー グループを リーフに関連付けるには:

例：

```
apic1(config)# leaf-profile test_leaf_profile
apic1(config-leaf-profile)# leaf-group test_leaf_group
apic1(config-leaf-group)# leaf-policy-group test_leaf_policy_group
apic1(config-leaf-group)# leaf 101-102
apic1(config-leaf-group)# exit
```

NX-OS スタイル CLI を使用したスパイン スイッチ上の BFD のグローバル設定

次の手順を使用して、NX-OS スタイル CLI を使用してスパイン スイッチの BFD をグローバルに設定します。

手順

ステップ 1 NX-OS CLI を使用して BFD IPV4 グローバル設定（bfdIpv4InstPol）を設定するには：

例：

```
apic1# configure
apic1(config)# template bfd ip bfd_ipv4_global_policy
apic1(config-bfd)# [no] echo-address 1.2.3.4
apic1(config-bfd)# [no] slow-timer 2500
apic1(config-bfd)# [no] min-tx 100
apic1(config-bfd)# [no] min-rx 70
apic1(config-bfd)# [no] multiplier 3
apic1(config-bfd)# [no] echo-rx-interval 500
apic1(config-bfd)# exit
```

ステップ 2 NX-OS CLI を使用して BFD IPV6 グローバル設定（bfdIpv6InstPol）を設定するには：

例：

```
apic1# configure
apic1(config)# template bfd ipv6 bfd_ipv6_global_policy
apic1(config-bfd)# [no] echo-address 34::1/64
apic1(config-bfd)# [no] slow-timer 2500
apic1(config-bfd)# [no] min-tx 100
apic1(config-bfd)# [no] min-rx 70
apic1(config-bfd)# [no] multiplier 3
apic1(config-bfd)# [no] echo-rx-interval 500
apic1(config-bfd)# exit
```

ステップ 3 NX-OS CLI を使用してスパイン ポリシー グループを設定し以前作成した BFD グローバル ポリシーを継承するには：

例：

```
apic1# configure
apic1(config)# template spine-policy-group test_spine_policy_group
apic1(config-spine-policy-group)# [no] inherit bfd ip bfd_ipv4_global_policy
apic1(config-spine-policy-group)# [no] inherit bfd ipv6 bfd_ipv6_global_policy
apic1(config-spine-policy-group)# exit
```

ステップ 4 NX-OS を使用して以前作成したスパイン ポリシー グループをスパイン スイッチに関連付けるには；

例：

```
apic1# configure
apic1(config)# spine-profile test_spine_profile
apic1(config-spine-profile)# spine-group test_spine_group
apic1(config-spine-group)# spine-policy-group test_spine_policy_group
apic1(config-spine-group)# spine 103-104
apic1(config-leaf-group)# exit
```

NX-OS スタイルの CLI を使用して BFD インターフェイスのオーバーライドを設定する

手順

ステップ 1 NX-OS CLI を使用して BFD インターフェイス ポリシー (bfdIfPol) を設定するには:

例：

```
apic1# configure
apic1(config)# tenant t0
apic1(config-tenant)# vrf context v0
apic1(config-tenant-vrf)# exit
apic1(config-tenant)# exit
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant t0 vrf v0
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# interface Ethernet 1/18
apic1(config-leaf-if)# vrf  member tenant t0 vrf v0
apic1(config-leaf-if)# exit
apic1(config-leaf)# template bfd bfdIfPol1 tenant t0
apic1(config-template-bfd-pol)# [no] echo-mode enable
apic1(config-template-bfd-pol)# [no] echo-rx-interval 500
apic1(config-template-bfd-pol)# [no] min-rx 70
apic1(config-template-bfd-pol)# [no] min-tx 100
apic1(config-template-bfd-pol)# [no] multiplier 5
apic1(config-template-bfd-pol)# [no] optimize subinterface
apic1(config-template-bfd-pol)# exit
```

ステップ 2 NX-OS CLI を使用して、以前に作成した BFD インターフェイス ポリシーを、IPv4 アドレスを持つ L3 インターフェイスに継承させるには:

例：

```
apic1# configure
apic1(config)# leaf 101
```

```
apic1(config-leaf)# interface Ethernet 1/15
apic1(config-leaf-if)# bfd ip tenant mode
apic1(config-leaf-if)# bfd ip inherit interface-policy bfdPol1
apic1(config-leaf-if)# bfd ip authentication keyed-sha1 key 10 key password
```

ステップ 3 NX-OS CLI を使用して、以前に作成した BFD インターフェイス ポリシーを、IPv6 アドレスを持つ L3 インターフェイスに継承させるには:

例：

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface Ethernet 1/15
apic1(config-leaf-if)# ipv6 address 2001::10:1/64 preferred
apic1(config-leaf-if)# bfd ipv6 tenant mode
apic1(config-leaf-if)# bfd ipv6 inherit interface-policy bfdPol1
apic1(config-leaf-if)# bfd ipv6 authentication keyed-sha1 key 10 key password
```

ステップ 4 NX-OS CLI を使用して、IPv4 アドレスを持つ VLAN インターフェイス上の BFD を設定するには:

例：

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface vlan 15
apic1(config-leaf-if)# vrf member tenant t0 vrf v0
apic1(config-leaf-if)# bfd ip tenant mode
apic1(config-leaf-if)# bfd ip inherit interface-policy bfdPol1
apic1(config-leaf-if)# bfd ip authentication keyed-sha1 key 10 key password
```

ステップ 5 NX-OS CLI を使用して、IPv6 アドレスを持つ VLAN インターフェイス上の BFD を設定するには:

例：

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface vlan 15
apic1(config-leaf-if)# ipv6 address 2001::10:1/64 preferred
apic1(config-leaf-if)# vrf member tenant t0 vrf v0
apic1(config-leaf-if)# bfd ipv6 tenant mode
apic1(config-leaf-if)# bfd ipv6 inherit interface-policy bfdPol1
apic1(config-leaf-if)# bfd ipv6 authentication keyed-sha1 key 10 key password
```

NX-OS スタイルの CLI を使用した BFD コンシューマ プロトコルの設定

手順

ステップ 1 NX-OS は、CLI を使用して、BGP コンシューマ プロトコルを BFD をイネーブルにします。

例：

```
apic1# configure
```

NX-OS スタイル CLI を使用したタスクの実行

```
apic1(config)# bgp-fabric
apic1(config-bgp-fabric)# asn 200
apic1(config-bgp-fabric)# exit
apic1(config)# leaf 101
apic1(config-leaf)# router bgp 200
apic1(config-bgp)# vrf member tenant t0 vrf v0
apic1(config-leaf-bgp-vrf)# neighbor 1.2.3.4
apic1(config-leaf-bgp-vrf-neighbor)# [no] bfd enable
```

ステップ 2 NX-OS は、CLI を使用して、EIGRP コンシューマ プロトコルを BFD をイネーブルにします。

例：

```
apic1(config-leaf-if)# [no] ip bfd eigrp enable
```

ステップ 3 NX-OS は、CLI を使用して、OSPF コンシューマ プロトコルを BFD をイネーブルにします。

例：

```
apic1(config-leaf-if)# [no] ip ospf bfd enable


apic1# configure
apic1(config)# spine 103
apic1(config-spine)# interface ethernet 5/3.4
apic1(config-spine-if)# [no] ip ospf bfd enable
```

ステップ 4 NX-OS は、CLI を使用して、スタティック ルート コンシューマ プロトコルを BFD をイネーブルにします。

例：

```
apic1(config-leaf-vrf)# [no] ip route 10.0.0.1/16 10.0.0.5 bfd


apic1(config)# spine 103
apic1(config-spine)# vrf context tenant infra vrf overlay-1
apic1(config-spine-vrf)# [no] ip route 21.1.1.1/32 32.1.1.1 bfd
```

ステップ 5 NX-OS は、CLI を使用して、IS-IS コンシューマ プロトコルを BFD をイネーブルにします。

例：

```
apic1(config)# leaf 101
apic1(config-spine)# interface ethernet 1/49
apic1(config-spine-if)# isis bfd enabled
apic1(config-spine-if)# exit
apic1(config-spine)# exit


apic1(config)# spine 103
apic1(config-spine)# interface ethernet 5/2
apic1(config-spine-if)# isis bfd enabled
apic1(config-spine-if)# exit
apic1(config-spine)# exit
```

NX-OS Style CLI を使用した OSPF 外部ルーテッド ネットワークの設定

NX-OS CLI を使用したテナントの OSPF 外部ルーテッド ネットワークの作成

外部ルーテッド ネットワーク接続の設定には、次のステップがあります。

1. テナントの下に VRF を作成します。
2. 外部ルーテッド ネットワークに接続された境界リーフ スイッチの VRF の L3 ネットワーキング構成を設定します。この設定には、インターフェイス、ルーティング プロトコル (BGP、OSPF、EIGRP) 、プロトコル パラメータ、ルートマップが含まれています。
3. テナントの下に外部 L3 EPG を作成してポリシーを設定し、これらの EPG を境界リーフ スイッチに導入します。ACI ファブリック内で同じポリシーを共有する VRF の外部ルーテッド サブネットが、1 つの「外部 L3 EPG」または 1 つの「プレフィクス EPG」を形成します。

設定は、2 つのモードで実現されます。

- テナント モード：VRF の作成および外部 L3 EPG 設定
- リーフ モード：L3 ネットワーキング構成と外部 L3 EPG の導入

次の手順は、テナントの OSPF 外部ルーテッド ネットワークを作成するためのものです。テナントの OSPF 外部ルーテッド ネットワークを作成するには、テナントを選択してからテナント用の VRF を作成する必要があります。

（注） この項の例では、テナント「exampleCorp」の「OnlineStore」アプリケーションの「web」epg に外部ルーテッド接続を提供する方法について説明します。

手順

ステップ 1 VLAN ドメインを設定します。

例：

```
apic1(config)# vlan-domain dom_exampleCorp
apic1(config-vlan)# vlan 5-1000
apic1(config-vlan)# exit
```

ステップ 2 テナント VRF を設定し、VRF のポリシーの適用を有効にします。

例：

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

NX-OS スタイル CLI を使用したタスクの実行

ステップ 3 テナント BD を設定し、ゲートウェイ IP を「public」としてマークします。エントリ「scope public」は、このゲートウェイ アドレスを外部 L3 ネットワークのルーティング プロトコルによるアドバタイズに使用できるようにします。

例：

```
apic1(config-tenant)# bridge-domain exampleCorp_b1
apic1(config-tenant-bd)# vrf member exampleCorp_v1
apic1(config-tenant-bd)# exit
apic1(config-tenant)# interface bridge-domain exampleCorp_b1
apic1(config-tenant-interface)# ip address 172.1.1.1/24 scope public
apic1(config-tenant-interface)# exit
```

ステップ 4 リーフの VRF を設定します。

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant exampleCorp vrf exampleCorp_v1
```

ステップ 5 OSPF エリアを設定し、ルート マップを追加します。

例：

```
apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant exampleCorp vrf exampleCorp_v1
apic1(config-leaf-ospf-vrf)# area 0.0.0.1 route-map map100 out
apic1(config-leaf-ospf-vrf)# exit
apic1(config-leaf-ospf)# exit
```

ステップ 6 VRF をインターフェイス (この例ではサブインターフェイス) に割り当て、OSPF エリアを有効にします。

例：

（注） サブインターフェイスの構成では、メイン インターフェイス (この例では、ethernet 1/11) は、「no switchport」によって L3 ポートに変換し、サブインターフェイスが使用するカプセル化 VLAN を含む vlan ドメイン (この例では dom_exampleCorp) を割り当てる必要があります。サブインターフェイス ethernet1/11.500 で、500 はカプセル化 VLAN です。

```
apic1(config-leaf)# interface ethernet 1/11
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vlan-domain member dom_exampleCorp
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface ethernet 1/11.500
apic1(config-leaf-if)# vrf member tenant exampleCorp vrf exampleCorp_v1
apic1(config-leaf-if)# ip address 157.10.1.1/24
apic1(config-leaf-if)# ip router ospf default area 0.0.0.1
```

ステップ 7 外部 L3 EPG ポリシーを設定します。これは、外部サブネットを特定し、epg「web」と接続する契約を消費するために一致させるサブネットが含まれます。

例：

```
apic1(config)# tenant t100
```

```
apic1(config-tenant)# external-l3 epg  l3epg100
apic1(config-tenant-l3ext-epg)# vrf member v100
apic1(config-tenant-l3ext-epg)# match ip 145.10.1.0/24
apic1(config-tenant-l3ext-epg)# contract consumer web
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)#exit
```

ステップ 8 リーフ スイッチの外部 L3 EPG を導入します。

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant t100 vrf v100
apic1(config-leaf-vrf)# external-l3 epg l3epg100
```

NX-OS Style CLI を使用した EIGRP 外部ルーテッド ネットワークの設定

NX-OS スタイルの CLI を使用したEIGRPの設定

手順

ステップ 1 ファブリックの Application Policy Infrastructure Controller (APIC) に SSH 接続します。

例：

```
# ssh admin@node_name
```

ステップ 2 設定モードを開始します。

例：

```
apic1# configure
```

ステップ 3 テナントの設定モードを入力します。

例：

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

ステップ 4 テナントでレイヤ 3 Outside を設定します:

例：

```
apic1(config-tenant)# show run
# Command: show running-config tenant tenant1
# Time: Tue Feb 16 09:44:09 2016
  tenant tenant1
    vrf context l3out
      exit
    l3out l3out-L1
      vrf member l3out
      exit
    l3out l3out-L3
      vrf member l3out
      exit
    external-l3 epg tenant1 l3out l3out-L3
      vrf member l3out
```

NX-OS スタイル CLI を使用したタスクの実行

```
    match ip 0.0.0.0/0
    match ip 3.100.0.0/16
    match ipv6 43:101::/48
    contract consumer default
    exit
  external-l3 epg tenant1 l3out l3out-L1
    vrf member l3out
    match ipv6 23:101::/48
    match ipv6 13:101::/48
    contract provider default
    exit
  exit
```

ステップ 5 リーフで EIGRP の VRF を設定します:

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant tenant1 vrf l3out l3out l3out-L1
apic1(config-leaf-vrf)# show run
# Command: show running-config leaf 101 vrf context tenant tenant1 vrf l3out l3out
l3out-L1
# Time: Tue Feb 16 09:44:45 2016
  leaf 101
    vrf context tenant tenant1 vrf l3out l3out l3out-L1
      router-id 3.1.1.1
      route-map l3out-L1_in
        scope global
        ip prefix-list tenant1 permit 1:102::/48
        match prefix-list tenant1
          exit
        exit
      route-map l3out-L1_out
        scope global
        ip prefix-list tenant1 permit 3.102.10.0/23
        ip prefix-list tenant1 permit 3.102.100.0/31
        ip prefix-list tenant1 permit 3.102.20.0/24
        ip prefix-list tenant1 permit 3.102.30.0/25
        ip prefix-list tenant1 permit 3.102.40.0/26
        ip prefix-list tenant1 permit 3.102.50.0/27
        ip prefix-list tenant1 permit 3.102.60.0/28
        ip prefix-list tenant1 permit 3.102.70.0/29
        ip prefix-list tenant1 permit 3.102.80.0/30
        ip prefix-list tenant1 permit 3.102.90.0/32
        <OUTPUT TRUNCATED>
        ip prefix-list tenant1 permit ::/0
        match prefix-list tenant1
          exit
        exit
      route-map l3out-L1_shared
        scope global
        exit
      exit
    exit
```

ステップ 6 EIGRP インターフェイス ポリシーを設定します:

例：

```
apic1(config-leaf)# template eigrp interface-policy tenant1 tenant tenant1
This template will be available on all leaves where tenant tenant1 has a VRF deployment
apic1(config-template-eigrp-if-pol)# show run
# Command: show running-config leaf 101 template eigrp interface-policy tenant1 tenant
tenant1
# Time: Tue Feb 16 09:45:50 2016
```

NX-OS スタイル CLI を使用したタスクの実行

```
  leaf 101
    template eigrp interface-policy tenant1 tenant tenant1
      ip hello-interval eigrp default 10
      ip hold-interval eigrp default 30
      ip throughput-delay eigrp default 20 tens-of-micro
      ip bandwidth eigrp default 20
      exit
    exit
```

ステップ 7 EIGRP の VRF ポリシーを設定します:

例：

```
apic1(config-leaf)# template eigrp vrf-policy tenant1 tenant tenant1
This template will be available on all leaves where tenant tenant1 has a VRF deployment
apic1(config-template-eigrp-vrf-pol)# show run
# Command: show running-config leaf 101 template eigrp vrf-policy tenant1 tenant tenant1
# Time: Tue Feb 16 09:46:31 2016
  leaf 101
    template eigrp vrf-policy tenant1 tenant tenant1
      metric version 64bit
      exit
    exit
```

ステップ 8 EIGRP VLAN インターフェイスを設定し、インターフェイスで EIGRP を有効にします:

例：

```
apic1(config-leaf)# interface vlan 1013
apic1(config-leaf-if)# show run
# Command: show running-config leaf 101 interface vlan 1013
# Time: Tue Feb 16 09:46:59 2016
  leaf 101
    interface vlan 1013
      vrf member tenant tenant1 vrf l3out
      ip address 101.13.1.2/24
      ip router eigrp default
      ipv6 address 101:13::1:2/112 preferred
      ipv6 router eigrp default
      ipv6 link-local fe80::101:13:1:2
      inherit eigrp ip interface-policy tenant1
      inherit eigrp ipv6 interface-policy tenant1
      exit
    exit
apic1(config-leaf-if)# ip summary-address ?
 eigrp  Configure route summarization for EIGRP
apic1(config-leaf-if)# ip summary-address eigrp default 11.11.0.0/16 ?
 <CR>
apic1(config-leaf-if)# ip summary-address eigrp default 11.11.0.0/16
apic1(config-leaf-if)# ip summary-address eigrp default 11:11:1::/48
apic1(config-leaf-if)# show run
# Command: show running-config leaf 101 interface vlan 1013
# Time: Tue Feb 16 09:47:34 2016
  leaf 101
    interface vlan 1013
      vrf member tenant tenant1 vrf l3out
      ip address 101.13.1.2/24
      ip router eigrp default
      ip summary-address eigrp default 11.11.0.0/16
      ip summary-address eigrp default 11:11:1::/48
      ipv6 address 101:13::1:2/112 preferred
      ipv6 router eigrp default
      ipv6 link-local fe80::101:13:1:2
      inherit eigrp ip interface-policy tenant1
```

NX-OS スタイル CLI を使用したタスクの実行

```
      inherit eigrp ipv6 interface-policy tenant1
      exit
    exit
```

ステップ 9 物理インターフェイスに VLAN を適用します:

例：

```
apic1(config-leaf)# interface ethernet 1/5
apic1(config-leaf-if)# show run
# Command: show running-config leaf 101 interface ethernet 1 / 5
# Time: Tue Feb 16 09:48:05 2016
  leaf 101
    interface ethernet 1/5
      vlan-domain member cli
      switchport trunk allowed vlan 1213 tenant tenant13 external-svi l3out l3out-L1
      switchport trunk allowed vlan 1613 tenant tenant17 external-svi l3out l3out-L1
      switchport trunk allowed vlan 1013 tenant tenant1 external-svi l3out l3out-L1
     switchport trunk allowed vlan 666 tenant ten_v6_cli external-svi l3out l3out_cli_L1

      switchport trunk allowed vlan 1513 tenant tenant16 external-svi l3out l3out-L1
      switchport trunk allowed vlan 1313 tenant tenant14 external-svi l3out l3out-L1
      switchport trunk allowed vlan 1413 tenant tenant15 external-svi l3out l3out-L1
      switchport trunk allowed vlan 1113 tenant tenant12 external-svi l3out l3out-L1
      switchport trunk allowed vlan 712 tenant mgmt external-svi l3out inband_l1
      switchport trunk allowed vlan 1913 tenant tenant10 external-svi l3out l3out-L1
      switchport trunk allowed vlan 300 tenant tenant1 external-svi l3out l3out-L1
      exit
    exit
```

ステップ 10 ルータ EIGRP を有効にします:

例：

```
apic1(config-eigrp-vrf)# show run
# Command: show running-config leaf 101 router eigrp default vrf member tenant tenant1
vrf l3out
# Time: Tue Feb 16 09:49:05 2016
  leaf 101
    router eigrp default
      exit
    router eigrp default
      exit
    router eigrp default
      exit
    router eigrp default
      vrf member tenant tenant1 vrf l3out
        autonomous-system 1001 l3out l3out-L1
        address-family ipv6 unicast
          inherit eigrp vrf-policy tenant1
          exit
        address-family ipv4 unicast
          inherit eigrp vrf-policy tenant1
          exit
        exit
      exit
```

NX-OS スタイル CLI を使用したルート集約の設定

NX-OS スタイル CLI を使用した BGP、OSPF、および EIGRP のルート集約の設定

手順

ステップ 1 NX-OS CLI を使用して次のように BGP ルート集約を設定します:

a) 次のように BGP を有効にします:

例：

```
apic1(config)# pod 1
apic1(config-pod)# bgp fabric
apic1(config-pod-bgp)# asn 10
apic1(config-pod)# exit
apic1(config)# leaf 101
apic1(config-leaf)# router bgp 10
```

b) 次のように 要約ルートを設定します:

例：

```
apic1(config-bgp)# vrf member tenant common vrf vrf1
apic1(config-leaf-bgp-vrf)# aggregate-address 10.0.0.0/8
```

ステップ 2 NX-OS CLI を使用して次のように OSPF 外部集約を設定します。

例：

```
apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant common vrf vrf1
apic1(config-leaf-ospf-vrf)# summary-address 10.0.0.0/8
```

ステップ 3 NX-OS CLI を使用して次のように OSPF エリア間集約を設定します。

```
apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant common vrf vrf1
apic1(config-leaf-ospf-vrf)# area 0.0.0.2 range 10.0.0.0/8 cost 20
```

ステップ 4 NX-OS CLI を使用して次のように EIGRP 集約を設定します。

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/31 (Or interface vlan <vlan-id>)
apic1(config-leaf-if)# ip summary-address eigrp default 10.0.0.0/8
```

（注） EIGRP を設定するルート集約ポリシーはありません。EIGRP の集約を有効にするために必要なだけの設定では、サマリー サブネット、InstP でです。

NX-OS スタイルの CLI を使用したルート マップとルート プロファイルによるルート制御の構成

NX-OS Style CLI を使用した BGP ピアごとのルート制御の設定

次の手順では、NX-OS CLI を使用して BGP ピア単位のルート制御を設定する方法について説明します。

手順

ステップ 1 ルート グループ テンプレートを作成し、ルート グループに IP プレフィックスを追加します。

この例では、テナント t1 のルート グループ match-rule1 を作成し、IP プレフィックス 200.3.2.0/24 をルート グループに追加します。

例：

```
apic1(config)# leaf 103
apic1(config-leaf)# template route group match-rule1 tenant t1
apic1(config-route-group)# ip prefix permit 200.3.2.0/24
apic1(config-route-group)# exit
apic1(config-leaf)#
```

ステップ 2 ノードのテナント VRF モードを開始します。

この例では、テナント t1 の VRF v1 のテナント VRF モードを開始します。

例：

```
apic1(config-leaf)# vrf context tenant t1 vrf v1
```

ステップ 3 ルートマップを作成し、ルートマップ コンフィギュレーション モードを開始します。すでに作成されているルート グループとマッチし、マッチ モードを開始してルートプロファイルを設定します。

この例では、ルートマップ rp1 を作成し、ルート グループ match-rule1 を順序番号 0 で照合します。

例：

```
apic1(config-leaf-vrf)# route-map rp1
apic1(config-leaf-vrf-route-map)# match route group match-rule1 order 0
apic1(config-leaf-vrf-route-map-match)# exit
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf)# exit
```

ステップ 4 BGP ルーティング プロトコルを設定します。

この例では、15.15.15.2 および ASN 100 の BGP ピア アドレスを使用して、プライマリのルーティング プロトコルとして BGP を設定します。

例：

```
apic1(config)# leaf 103
```

```
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 15.15.15.2
```

ステップ 5 BGP ピアごとのルート制御機能を設定します。

ここで、

- **in** は、ルート インポート ポリシー（ファブリックに許可されるルート）です。
- **out** は、ルート エクスポート ポリシー（外部ネットワークからアドバタイズされるルート）です。

例：

```
apic1(config-leaf-bgp-vrf-neighbor)# route-map rp1 in
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# exit
```

NX-OS スタイル CLI を使用して、明示的なプレフィックス リストでルート マップ/プロファイルの設定

始める前に

- テナントと VRF は、NX-OS CLI を介して設定する必要があります。
- NX-OS CLI を介してリーフ スイッチで VRF をイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	コンフィギュレーション モードに入ります。
ステップ 2	**leaf** *node-id* 例： `apic1(config)# leaf 101`	設定するリーフを指定します。
ステップ 3	**template route group** *group-name* **tenant** *tenant-name* 例：	ルート グループ テンプレートを作成します。

NX-OS スタイル CLI を使用したタスクの実行

	コマンドまたはアクション	目的
	apic1(config-leaf)# **template route group g1 tenant exampleCorp**	（注） ルート グループ (マッチ ルール) は、1 つ以上の IP プレフィックスと 1 つ以上のマッチ コミュニティ タームを持つことができます。マッチ タイプ全体では、AND フィルタがサポートされているため、ルート マッチ ルールが受け入れられるようにするために、ルート グループ内のすべての条件がマッチしている必要があります。ルート グループに複数の IP プレフィックスがある場合は、OR フィルタがサポートされます。マッチする場合は、いずれかのプレフィックスがルート タイプとして受け入れられます。
ステップ 4	**ip prefix permit** *prefix/masklen* [**le**{**32 | 128** }] 例： apic1(config-route-group)# **ip prefix permit 15.15.15.0/24**	ルート グループに IP プレフィックスを追加します。 （注） IP プレフィックスは、BD サブネットまたは外部ネットワークを示すことができます。集約プレフィックスが必要な場合は、IPv4 にはオプションの le 32 を、IPv6 には le 128 を使用してください。
ステップ 5	**community-list** [**standard | expanded**] *community-list-name expression* 例： apic1(config-route-group)# **community-list standard com1 65535:20**	これは任意のコマンドです。コミュニティーも IP プレフィックスと照合する必要がある場合は、コミュニティのマッチ基準を追加します。
ステップ 6	**exit** 例： apic1(config-route-group)# **exit** apic1(config-leaf)#	テンプレート モードを終了します。
ステップ 7	**vrf context tenant** *tenant-name* **vrf** *vrf-name* [**l3out** {**BGP | EIGRP | OSPF | STATIC** }]	ノードのテナント VRF モードを開始します。

NX-OS スタイル CLI を使用したタスクの実行

	コマンドまたはアクション	目的
	例： `apic1(config-leaf)# vrf context tenant exampleCorp vrf v1`	（注） オプションの l3out 文字列を入力する場合、L3Out は NX-OS CLI で設定した L3Out である必要があります。
ステップ 8	**template route-profile** *profile-name* [*route-control-context-name order-value*] 例： `apic1(config-leaf-vrf)# template route-profile rp1 ctxl 1`	マッチするルートに適用する必要のあるセットアクションを含むテンプレートを作成します。
ステップ 9	**set** *attribute value* 例： `apic1(config-leaf-vrf-template-route-profile)# set metric 128`	必要な属性 (アクションの設定) をテンプレートに追加します。

ステップ 10	**exit**
	例：
	`apic1(config-leaf-vrf-template-route-profile)# exit`
	`apic1(config-leaf-vrf)#`
		テンプレート モードを終了します。

ステップ 11	**route-map** *map-name* 例： `apic1(config-leaf-vrf)# route-map bgpMap`	ルートマップを作成し、ルートマップコンフィギュレーションモードを開始します。
ステップ 12	**match route group** *group-name* [**order** *number*] [**deny**] 例： `apic1(config-leaf-vrf-route-map)# match route group g1 order 1`	すでに作成されているルートグループとマッチし、マッチモードを開始してルートプロファイルを設定します。さらに、ルートグループで定義されているマッチ基準にマッチするルートを拒否する必要がある場合は、キーワード **[Deny]**を選択します。デフォルトの設定は **[Permit]** です。
ステップ 13	**inherit route-profile** *profile-name* 例： `apic1(config-leaf-vrf-route-map-match)# inherit route-profile rp1`	ルート プロファイルを継承します (アクションを設定します)。 （注） これらのアクションは、マッチしたルートに適用されます。または、ルートプロファイルを継承する代わりに、インラインで設定されたアクションを設定することもできます。

	コマンドまたはアクション	目的

ステップ 14	**exit**
	例：
	`apic1(config-leaf-vrf-route-map-match)# exit`
	`apic1(config-leaf-vrf-route-map)#`
		一致モードを終了します。

ステップ 15	**exit**
	例：
	`apic1(config-leaf-vrf-route-map)# exit`
	`apic1(config-leaf-vrf)#`
		ルートマップコンフィギュレーションモードを終了します。

ステップ 16	**exit**
	例：
	`apic1(config-leaf-vrf)# exit`
	`apic1(config-leaf)#`
		VRF コンフィギュレーションモードを終了します。

ステップ 17	**router bgp** *fabric-asn* 例： `apic1(config-leaf)# router bgp 100`	リーフ ノードを設定します。
ステップ 18	t1 v1 **vrf member tenant vrf** 例： `apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1`	BGP ポリシーの BGP の VRF メンバーシップとテナントを設定します。
ステップ 19	**neighbor** *IP-address-of-neighbor* 例： `apic1(config-leaf-bgp-vrf)# neighbor 15.15.15.2`	BGP ネイバーを設定します。
ステップ 20	**route-map** *map-name* {**in** | **out** } 例： `apic1(config-leaf-bgp-vrf-neighbor)# route-map bgpMap out`	BGP ネイバのルートマップを設定します。

NX-OS スタイルの CLI を使用した、インポート制御とエクスポート制御を使用するルート制御プロトコルの設定

この例では、ネットワーク接続 BGP を使用して外部レイヤ 3 が設定されていることを前提としています。OSPF を使用するように設定されたネットワークに対してもこれらのタスクを実行することができます。

ここでは、NX-OS CLI を使用してルート マップを作成する方法を説明します。

NX-OS スタイル CLI を使用したタスクの実行

始める前に

- テナント、プライベート ネットワーク、およびブリッジ ドメインが作成されていること。
- レイヤ 3 Outside テナント ネットワークが設定されていること。

手順

ステップ 1 一致コミュニティ、一致プレフィックス リストを使用したインポート ルート制御

例：

```
apic1# configure
apic1(config)# leaf 101
    # Create community-list
apic1(config-leaf)# template community-list standard CL_1 65536:20 tenant exampleCorp
apic1(config-leaf)# vrf context tenant exampleCorp vrf v1

     #Create Route-map and use it for BGP import control.
apic1(config-leaf-vrf)# route-map bgpMap
    # Match prefix-list and set route-profile actions for the match.
apic1(config-leaf-vrf-route-map)# ip prefix-list list1 permit 13.13.13.0/24
apic1(config-leaf-vrf-route-map)# ip prefix-list list1 permit 14.14.14.0/24
apic1(config-leaf-vrf-route-map)# match prefix-list list1
apic1(config-leaf-vrf-route-map-match)# set tag 200
apic1(config-leaf-vrf-route-map-match)# set local-preference 64
apic1(config-leaf)# router bgp 100
apic1(config-bgp)# vrf member tenant exampleCorp vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 3.3.3.3
apic1(config-leaf-bgp-vrf-neighbor)# route-map bgpMap in
```

ステップ 2 一致 BD、デフォルトのエクスポート ルート プロファイルを使用したエクスポート ルート制御

例：

```
# Create custom and "default-export" route-profiles
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant exampleCorp vrf v1
apic1(config-leaf-vrf)# template route-profile default-export
apic1(config-leaf-vrf-template-route-profile)# set metric 256
apic1(config-leaf-vrf)# template route-profile bd-rtctrl
apic1(config-leaf-vrf-template-route-profile)# set metric 128

#Create a Route-map and match on BD, prefix-list
apic1(config-leaf-vrf)# route-map bgpMap
apic1(config-leaf-vrf-route-map)# match bridge-domain bd1
apic1(config-leaf-vrf-route-map-match)#exit
apic1(config-leaf-vrf-route-map)# match prefix-list p1
apic1(config-leaf-vrf-route-map-match)#exit
apic1(config-leaf-vrf-route-map)# match bridge-domain bd2
apic1(config-leaf-vrf-route-map-match)# inherit route-profile bd-rtctrl
```

（注） この場合、bd1 のパブリック サブネットとプレフィックスリスト p1 を照合するプレフィックスが、ルート プロファイルの「default-export」を使用してエクスポートされ、bd2 のパブリック サブネットはルート プロファイルの「bd-rtctrl」を使用してエクスポートされます。

NX-OS Style CLI を使用したインターリーク再配布の設定

次の手順では、NX-OS スタイルの CLI を使用してインターリーク再配布を設定する方法について説明します。

始める前に

テナント、VRF および L3Out を作成します。

手順

ステップ 1 境界リーフ ノードのインターリーク再配布のルート マップを設定します。

例：

次の例では、[テナント（tenant）] [CLI_TEST] および [VRF] [VRF1] の IP プレフィックス リスト [CLI_PFX1] を使用してルート マップ [CLI_RP] を設定します。

```
apic1# conf t
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant CLI_TEST vrf VRF1
apic1(config-leaf-vrf)# route-map CLI_RP
apic1(config-leaf-vrf-route-map)# ip prefix-list CLI_PFX1 permit 192.168.1.0/24
apic1(config-leaf-vrf-route-map)# match prefix-list CLI_PFX1 [deny]
```

ステップ 2 設定されたルート マップを使用して、インターリーク再配布を設定します。

例：

次に、設定されたルート マップ [CLI_RP] を使用して OSPF ルートの再配布を設定する例を示します。

```
apic1# conf t
apic1(config)# leaf 101
apic1(config-leaf)# router bgp 65001
apic1(config-leaf-bgp)# vrf member tenant CLI_TEST vrf VRF1
apic1(config-leaf-bgp-vrf)# redistribute ospf route-map CLI_RP
```

NX-OS スタイル CLI を使用したトランジット ルーティングの設定

NX-OS スタイル CLI を使用したトランジット ルーティングの設定

次の手順では、テナントのトランジットルーティングを設定する方法を説明します。この例では、別々にルータに接続された 2 つの境界リーフ スイッチ上の 1 個の VRF で、2 個の L3Outs を展開します。

始める前に

- ノード、ポート、AEP、機能プロファイル、レイヤ 3 ドメインを設定します。
- 使用して VLAN ドメイン設定、 **vlan ドメイン** ドメイン および **vlan** *vlan* 範囲 コマンド。
- BGP ルート リフレクタ ポリシーを設定し、ファブリック内でルーテッドを伝達します。

手順

ステップ 1 テナントおよび VRF を設定します。

この例では VRF `v1` でテナント `t1` を設定します。VRF はまだ展開されていません。

例：

```
apic1# configure
apic1(config)# tenant t1
apic1(config-tenant)# vrf context v1
apic1(config-tenant-vrf)# exit
apic1(config-tenant)# exit
```

ステップ 2 ノードおよびインターフェイスを設定します。

この例では、2 つの境界リーフ スイッチでテナント t1 の 2 つの L3Outs を設定します。

- 最初の L3Out はノード 101 上にあり、`nodep1` という名前です。ノード 101 はルータ ID `11.11.11.103` で設定されます。ルーテッドインターフェイス `ifp1` が `eth1/3` にあり、IP アドレス `12.12.12.3/24` です。
- 2 番目の L3Out が ノード 102 上にあり、`nodep2` という名前です。ノード 102 はルータ ID `22.22.22.203` で設定されます。ルーテッドインターフェイス `ifp2` が `eth1/3` に存在し、IP アドレスは `23.23.23.1/24` です。

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# router-id 11.11.11.103
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# interface ethernet 1/3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vrf member tenant t1 vrf v1
```

NX-OS スタイル CLI を使用したタスクの実行

```
apic1(config-leaf-if)# ip address 12.12.12.3/24
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config)# leaf 102
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# router-id 22.22.22.203
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# interface ethernet 1/3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vrf member tenant t1 vrf v1
apic1(config-leaf-if)# ip address 23.23.23.3/24
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

ステップ 3 両方のリーフ スイッチのルーティング プロトコルを設定します。

この例では、両方の境界リーフ スイッチに対して、ASN 100 でプライマリ ルーティング プロトコルとしてBGPを設定します。BGP ピア `15.15.15.2` を持つノード101とBGP ピア `25.25.25.2` を持つノード102を設定します。

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 15.15.15.2
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# exit
apic1(config)# leaf 102
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 25.25.25.2
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# exit
```

ステップ 4 接続ルーティング プロトコルを設定します。

この例では、定期的なエリア ID `0.0.0.0` で両方の L3Outs に対して通信プロトコルとしてOSPFを設定します。

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant t1 vrf v1
apic1(config-leaf-ospf-vrf)# area 0.0.0.0 loopback 40.40.40.1
apic1(config-leaf-ospf-vrf)# exit
apic1(config-leaf-ospf)# exit
apic1(config-leaf)# exit
apic1(config)# leaf 102
apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant t1 vrf v1
apic1(config-leaf-ospf-vrf)# area 0.0.0.0 loopback 60.60.60.1
apic1(config-leaf-ospf-vrf)# exit
apic1(config-leaf-ospf)# exit
apic1(config-leaf)# exit
```

NX-OS スタイル CLI を使用したタスクの実行

ステップ 5 外部 EPG を設定します。

この例では、ネットワーク 192.168.1.0/24 をノード 101 上の外部ネットワーク extnw1 として、ネットワーク 192.168.2.0/24 をノード 102 上の外部ネットワーク extnw2 として設定します。

例：

```
apic1(config)# tenant t1
apic1(config-tenant)# external-l3 epg extnw1
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# match ip 192.168.1.0/24
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# external-l3 epg extnw2
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# match ip 192.168.2.0/24
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# exit
apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# external-l3 epg extnw1
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# exit
apic1(config)# leaf 102
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# external-l3 epg extnw2
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# exit
```

ステップ 6 オプション。ルート マップを設定します。

この例では、インバウンドおよびアウト バウンド方向で各 BGP ピアのルート マップを設定します。

例：

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# template route group match-rule1 tenant t1
apic1(config-route-group)# ip prefix permit 192.168.1.0/24
apic1(config-route-group)# exit
apic1(config-leaf)# template route group match-rule2 tenant t1
apic1(config-route-group)# ip prefix permit 192.168.2.0/24
apic1(config-route-group)# exit
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# route-map rp1
apic1(config-leaf-vrf-route-map)# match route group match-rule1 order 0
apic1(config-leaf-vrf-route-map-match)# exit
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf)# route-map rp2
apic1(config-leaf-vrf-route-map)# match route group match-rule2 order 0
apic1(config-leaf-vrf-route-map-match)# exit
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 15.15.15.2
apic1(config-leaf-bgp-vrf-neighbor)# route-map rp1 in
apic1(config-leaf-bgp-vrf-neighbor)# route-map rp2 out
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# exit
```

NX-OS スタイル CLI を使用したタスクの実行

```
apic1(config)# leaf 102
apic1(config-leaf)# template route group match-rule1 tenant t1
apic1(config-route-group)# ip prefix permit 192.168.1.0/24
apic1(config-route-group)# exit
apic1(config-leaf)# template route group match-rule2 tenant t1
apic1(config-route-group)# ip prefix permit 192.168.2.0/24
apic1(config-route-group)# exit
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# route-map rp1
apic1(config-leaf-vrf-route-map)# match route group match-rule2 order 0
apic1(config-leaf-vrf-route-map-match)# exit
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf)# route-map rp2
apic1(config-leaf-vrf-route-map)# match route group match-rule1 order 0
apic1(config-leaf-vrf-route-map-match)# exit
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 25.25.25.2
apic1(config-leaf-bgp-vrf-neighbor)# route-map rp2 in
apic1(config-leaf-bgp-vrf-neighbor)# route-map rp1 out
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# exit
```

ステップ 7 フィルタ（アクセス リスト）およびコントラクトを作成し、EPGが通信できるようにします。

例：

```
apic1(config)# tenant t1
apic1(config-tenant)# access-list http-filter
apic1(config-tenant-acl)# match ip
apic1(config-tenant-acl)# match tcp dest 80
apic1(config-tenant-acl)# exit
apic1(config-tenant)# contract httpCtrct
apic1(config-tenant-contract)# scope vrf
apic1(config-tenant-contract)# subject subj1
apic1(config-tenant-contract-subj)# access-group http-filter both
apic1(config-tenant-contract-subj)# exit
apic1(config-tenant-contract)# exit
apic1(config-tenant)# exit
```

ステップ 8 契約を設定し、Epg に関連付けます。

例：

```
apic1(config)# tenant t1
apic1(config-tenant)# external-l3 epg extnw1
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# contract provider httpCtrct
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# external-l3 epg extnw2
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# contract consumer httpCtrct
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# exit
apic1(config)#
```

例：中継ルーティング

この例では、中継ルーティングのマージされた設定を提供します。設定は別々のルータに接続されている 2 個の障壁リーフ スイッチで、2 つの L3Outs を持つ単一のテナントと VRF のためにあります。

```
apic1# configure
apic1(config)# tenant t1
apic1(config-tenant)# vrf context v1
apic1(config-tenant-vrf)# exit
apic1(config-tenant)# exit

apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# router-id 11.11.11.103
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# interface ethernet 1/3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vrf member tenant t1 vrf v1
apic1(config-leaf-if)# ip address 12.12.12.3/24
apic1(config-leaf-if)# exit
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 15.15.15.2
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant t1 vrf v1
apic1(config-leaf-ospf-vrf)# area 0.0.0.0 loopback 40.40.40.1
apic1(config-leaf-ospf-vrf)# exit
apic1(config-leaf-ospf)# exit
apic1(config-leaf)# exit

apic1(config)# leaf 102
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# router-id 22.22.22.203
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# interface ethernet 1/3
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# no switchport
apic1(config-leaf-if)# vrf member tenant t1 vrf v1
apic1(config-leaf-if)# ip address 23.23.23.3/24
apic1(config-leaf-if)# exit
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 25.25.25.2/24
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# router ospf default
apic1(config-leaf-ospf)# vrf member tenant t1 vrf v1
apic1(config-leaf-ospf-vrf)# area 0.0.0.0 loopback 60.60.60.3
apic1(config-leaf-ospf-vrf)# exit
apic1(config-leaf-ospf)# exit
apic1(config-leaf)# exit

apic1(config)# tenant t1
apic1(config-tenant)# external-l3 epg extnw1
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# match ip 192.168.1.0/24
apic1(config-tenant-l3ext-epg)# exit
```

NX-OS スタイル CLI を使用したタスクの実行

```
apic1(config-tenant)# external-l3 epg extnw2
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# match ip 192.168.2.0/24
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# exit

apic1(config)# leaf 101
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# external-l3 epg extnw1
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# exit
apic1(config)# leaf 102
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# external-l3 epg extnw2
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# exit

apic1(config)# leaf 101
apic1(config-leaf)# template route group match-rule1 tenant t1
apic1(config-route-group)# ip prefix permit 192.168.1.0/24
apic1(config-route-group)# exit
apic1(config-leaf)# template route group match-rule2 tenant t1
apic1(config-route-group)# ip prefix permit 192.168.2.0/24
apic1(config-route-group)# exit
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# route-map rp1
apic1(config-leaf-vrf-route-map)# match route group match-rule1 order 0
apic1(config-leaf-vrf-route-map-match)# exit
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf)# route-map rp2
apic1(config-leaf-vrf-route-map)# match route group match-rule2 order 0
apic1(config-leaf-vrf-route-map-match)# exit
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 15.15.15.2
apic1(config-leaf-bgp-vrf-neighbor)# route-map rp1 in
apic1(config-leaf-bgp-vrf-neighbor)# route-map rp2 out
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# exit

apic1(config)# leaf 102
apic1(config-leaf)# template route group match-rule1 tenant t1
apic1(config-route-group)# ip prefix permit 192.168.1.0/24
apic1(config-route-group)# exit
apic1(config-leaf)# template route group match-rule2 tenant t1
apic1(config-route-group)# ip prefix permit 192.168.2.0/24
apic1(config-route-group)# exit
apic1(config-leaf)# vrf context tenant t1 vrf v1
apic1(config-leaf-vrf)# route-map rp1
apic1(config-leaf-vrf-route-map)# match route group match-rule1 order 0
apic1(config-leaf-vrf-route-map-match)# exit
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf)# route-map rp2
apic1(config-leaf-vrf-route-map)# match route group match-rule2 order 0
apic1(config-leaf-vrf-route-map-match)# exit
apic1(config-leaf-vrf-route-map)# exit
apic1(config-leaf-vrf)# exit
apic1(config-leaf)# router bgp 100
apic1(config-leaf-bgp)# vrf member tenant t1 vrf v1
apic1(config-leaf-bgp-vrf)# neighbor 25.25.25.2
```

```
apic1(config-leaf-bgp-vrf-neighbor)# route-map rp2 in
apic1(config-leaf-bgp-vrf-neighbor)# route-map rp1 out
apic1(config-leaf-bgp-vrf-neighbor)# exit
apic1(config-leaf-bgp-vrf)# exit
apic1(config-leaf-bgp)# exit
apic1(config-leaf)# exit

apic1(config)# tenant t1
apic1(config-tenant)# access-list http-filter
apic1(config-tenant-acl)# match ip
apic1(config-tenant-acl)# match tcp dest 80
apic1(config-tenant-acl)# exit
apic1(config-tenant)# contract httpCtrct
apic1(config-tenant-contract)# scope vrf
apic1(config-tenant-contract)# subject http-subj
apic1(config-tenant-contract-subj)# access-group http-filter both
apic1(config-tenant-contract-subj)# exit
apic1(config-tenant-contract)# exit
apic1(config-tenant)# exit

apic1(config)# tenant t1
apic1(config-tenant)# external-l3 epg extnw1
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# contract provider httpCtrct
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# external-l3 epg extnw2
apic1(config-tenant-l3ext-epg)# vrf member v1
apic1(config-tenant-l3ext-epg)# contract consumer httpCtrct
apic1(config-tenant-l3ext-epg)# exit
apic1(config-tenant)# exit
apic1(config)#
```

NX-OS Style CLI を使用した共有サービスの設定

NX-OS スタイル CLI を使用して共有 レイヤ 3 VRF 内リークを設定する - 名前が付けられた例

手順

	コマンドまたはアクション	目的
ステップ 1	コンフィギュレーション モードを開始します。 例： `apic1# configure`	

ステップ 2	プロバイダー レイヤ 3 を設定します。
	例：
	`apic1(config)# tenant t1_provider`
	`apic1(config-tenant)# external-l3 epg l3extInstP-1 l3out T0-o1-L3OUT-1`
	`apic1(config-tenant-l3ext-epg)# vrf member VRF1`
	`apic1(config-tenant-l3ext-epg)# match`	

NX-OS スタイル CLI を使用したタスクの実行

	コマンドまたはアクション	目的
	ip 192.168.2.0/24 shared apic1(config-tenant-l3ext-epg)# **contract provider vzBrCP-1** apic1(config-tenant-l3ext-epg)# **exit** apic1(config-tenant)# **exit** apic1(config)# **leaf 101** apic1(config-leaf)# **vrf context tenant t1_provider vrf VRF1 l3out T0-o1-L3OUT-1** apic1(config-leaf-vrf)# **route-map T0-o1-L3OUT-1_shared** apic1(config-leaf-vrf-route-map)# **ip prefix-list l3extInstP-1 permit 192.168.2.0/24** apic1(config-leaf-vrf-route-map)# **match prefix-list l3extInstP-1** apic1(config-leaf-vrf-route-map-match)# **exit** apic1(config-leaf-vrf-route-map)# **exit** apic1(config-leaf-vrf)# **exit** apic1(config-leaf)# **exit**	
ステップ 3	レイヤ 3 Out コンシューマを設定します。 例： apic1(config)# **tenant t1_consumer** apic1(config-tenant)# **external-l3 epg l3extInstP-2 l3out T0-o1-L3OUT-1** apic1(config-tenant-l3ext-epg)# **vrf member VRF2** apic1(config-tenant-l3ext-epg)# **match ip 199.16.2.0/24 shared** apic1(config-tenant-l3ext-epg)# **contract consumer vzBrCP-1 imported** apic1(config-tenant-l3ext-epg)# **exit** apic1(config-tenant)# **exit** apic1(config)# **leaf 101** apic1(config-leaf)# **vrf context tenant t1_consumer vrf VRF2 l3out T0-o1-L3OUT-1** apic1(config-leaf-vrf)# **route-map T0-o1-L3OUT-1_shared** apic1(config-leaf-vrf-route-map)# **ip prefix-list l3extInstP-2 permit 199.16.2.0/24** apic1(config-leaf-vrf-route-map)# **match prefix-list l3extInstP-2** apic1(config-leaf-vrf-route-map-match)# **exit** apic1(config-leaf-vrf-route-map)# **exit** apic1(config-leaf-vrf)# **exit** apic1(config-leaf)# **exit** apic1(config)#	

NX-OS Style CLI を使用した共有レイヤ 3 VRF 間リークの設定：名前を付けた例

手順

	コマンドまたはアクション	目的
ステップ 1	コンフィギュレーション モードを開始します。 例： `apic1# configure`	

ステップ 2	プロバイダ テナントおよび VRF の設定
	例：
	`apic1(config)# tenant t1_provider`
	`apic1(config-tenant)# vrf context VRF1`
	`apic1(config-tenant-vrf)# exit`
	`apic1(config-tenant)# exit`	

ステップ 3	コンシューマ テナントおよび VRF の設定
	例：
	`apic1(config)# tenant t1_consumer`
	`apic1(config-tenant)# vrf context VRF2`
	`apic1(config-tenant-vrf)# exit`
	`apic1(config-tenant)# exit`	

ステップ 4	コントラクトの設定
	例：
	`apic1(config)# tenant t1_provider`
	`apic1(config-tenant)# contract vzBrCP-1 type permit`
	`apic1(config-tenant-contract)# scope exportable`
	`apic1(config-tenant-contract)# export to tenant t1_consumer`
	`apic1(config-tenant-contract)# exit`	

ステップ 5	プロバイダ外部レイヤ 3 EPG の設定
	例：
	`apic1(config-tenant)# external-l3 epg l3extInstP-1`
	`apic1(config-tenant-l3ext-epg)# vrf member VRF1`
	`apic1(config-tenant-l3ext-epg)# match ip 192.168.2.0/24 shared`
	`apic1(config-tenant-l3ext-epg)# contract provider vzBrCP-1`
	`apic1(config-tenant-l3ext-epg)# exit`
	`apic1(config-tenant)# exit`	

	コマンドまたはアクション	目的

ステップ 6	プロバイダ エクスポート マップの設定
	例：
	`apic1(config)# leaf 101`
	`apic1(config-leaf)# vrf context tenant t1_provider vrf VRF1`
	`apic1(config-leaf-vrf)# route-map map1`
	`apic1(config-leaf-vrf-route-map)# ip prefix-list p1 permit 192.168.2.0/24`
	`apic1(config-leaf-vrf-route-map)# match prefix-list p1`
	`apic1(config-leaf-vrf-route-map-match)# exit`
	`apic1(config-leaf-vrf-route-map)# exit`
	`apic1(config-leaf-vrf)# export map map1`
	`apic1(config-leaf-vrf)# exit`
	`apic1(config-leaf)# exit`	

ステップ 7	コンシューマ外部レイヤ 3 EPG の設定
	例：
	`apic1(config)# tenant t1_consumer`
	`apic1(config-tenant)# external-l3 epg l3extInstP-2`
	`apic1(config-tenant-l3ext-epg)# vrf member VRF2`
	`apic1(config-tenant-l3ext-epg)# match ip 199.16.2.0/24 shared`
	`apic1(config-tenant-l3ext-epg)# contract consumer vzBrCP-1 imported`
	`apic1(config-tenant-l3ext-epg)# exit`
	`apic1(config-tenant)# exit`	

ステップ 8	コンシューマ エクスポート マップの設定
	例：
	`apic1(config)# leaf 101`
	`apic1(config-leaf)# vrf context tenant t1_consumer vrf VRF2`
	`apic1(config-leaf-vrf)# route-map map2`
	`apic1(config-leaf-vrf-route-map)# ip prefix-list p2 permit 199.16.2.0/24`
	`apic1(config-leaf-vrf-route-map)# match prefix-list p2`
	`apic1(config-leaf-vrf-route-map-match)# exit`
	`apic1(config-leaf-vrf-route-map)# exit`
	`apic1(config-leaf-vrf)# export map map2`
	`apic1(config-leaf-vrf)# exit`
	`apic1(config-leaf)# exit`
	`apic1(config)#`	

NX-OS スタイルの CLI を使用した L3Out の QoS の設定

CLI を使用した L3Out での QoS の直接設定

この章では L3Out で QoS ディレクトリを設定する方法について説明します。これは、リリース 4.0(1) 以降の L3Out QoS の推奨設定方法です。Cisco APIC

次のオブジェクトの内の 1 つで L3Out の QoS を設定できます。

- Switch Virtual Interface（SVI）
- サブインターフェイス
- 外部ルーテッド

手順

ステップ 1 L3Out SVI に QoS プライオリティを設定します。

例：

```
interface vlan 19
    vrf member tenant DT vrf dt-vrf
    ip address 107.2.1.252/24
    description  'SVI19'
    service-policy type qos VrfQos006   // for custom QoS attachment
    set qos-class level6                // for set QoS priority
    exit
```

ステップ 2 サブインターフェイスに QoS プライオリティを設定します。

例：

```
interface ethernet 1/48.10
    vrf member tenant DT vrf inter-tentant-ctx2 l3out L4_E48_inter_tennant
    ip address 210.2.0.254/16
    service-policy type qos vrfQos002
    set qos-class level5
```

ステップ 3 外部ルーテッドに QoS プライオリティを設定します。

例：

```
interface ethernet 1/37
    no switchport
    vrf member tenant DT vrf dt-vrf l3out L2E37
    ip address 30.1.1.1/24
    service-policy type qos vrfQos002
    set qos-class level5
    exit
```

CLI を使用した L3Out の QoS コントラクトの設定

この項では、コントラクトを使用して L3Out の QoS を設定する方法について説明します。

NX-OS スタイル CLI を使用したタスクの実行

（注） リリース 4.0(1) 以降では、L3Out QoS 用にカスタム QoS ポリシーを使用することを推奨しています。CLI を使用した L3Out での QoS の直接設定 （574 ページ）で説明しています。

手順

ステップ 1 L3Out で QoS 優先順位の適用をサポートするために、出力モードの VRF を設定し、ポリシー適用を有効化します。

```
apic1# configure
apic1(config)# tenant t1
apic1(config-tenant)# vrf context v1
apic1(config-tenant-vrf)# contract enforce egress
apic1(config-tenant-vrf)# exit
apic1(congig-tenant)# exit
apic1(config)#
```

ステップ 2 QoS を設定します。

フィルタ (access-list) を作成するとき、ターゲット DSCP レベルの **match dscp** コマンドを含みます。

コントラクトを設定するとき、L3Out でのトラフィック出力の QoS クラスを含めます。または、ターゲット DSCP の値を定義することもできます。QoS ポリシーは、コントラクトまたはサブジェクトのいずれかでサポートされます。

L3out インターフェイスでの QoS またはカスタム QoS では VRF の適用は入力である必要があります。VRF の適用を出力にする必要があるのは、QOS 分類が EPG と L3out の間、または L3out から L3out へのトラフィックのコントラクトで実行される場合に限ります。

（注） QoS 分類がコントラクトで設定され、VRF の適用が出力である場合、コントラクト QoS 分類は L3out インターフェイス QoS またはカスタム QoS 分類をオーバーライドします。

```
apic1(config)# tenant t1
apic1(config-tenant)# access-list http-filter
apic1(config-tenant-acl)# match ip
apic1(config-tenant-acl)# match tcp dest 80
apic1(config-tenant-acl)# match dscp EF
apic1(config-tenant-acl)# exit
apic1(config-tenant)# contract httpCtrct
apic1(config-tenant-contract)# scope vrf
apic1(config-tenant-contract)# qos-class level1
apic1(config-tenant-contract)# subject http-subject
apic1(config-tenant-contract-subj)# access-group http-filter both
apic1(config-tenant-contract-subj)# exit
apic1(config-tenant-contract)# exit
apic1(config-tenant)# exit
apic1(config)#
```

NX-OS Style CLI を使用した ACI IP SLA の設定

NX-OS Style CLI を使用した IP SLA モニタリング ポリシーの設定

NX-OS スタイル CLI を使用して特定の SLA タイプのモニタリング プローブを送信するように Cisco Application Policy Infrastructure Controller（APIC）を設定するには、次の手順を実行します。

始める前に

テナントが設定されていることを確認します。

手順

ステップ 1 コンフィギュレーション モードを開始します。

例：

```
apic1# configure
```

ステップ 2 テナントを作成してテナント コンフィギュレーション モードを開始するか、既存のテナントのテナント コンフィギュレーション モードを開始します。

例：

```
apic1(config)# tenant t1
```

ステップ 3 IP SLA モニタリング ポリシーを作成し、IP SLA ポリシー コンフィギュレーション モードを開始します。

例：

```
apic1(config-tenant)# ipsla-pol ipsla-policy-3
```

ステップ 4 モニタリング頻度を秒単位で設定します。これはプローブの送信間隔です。

例：

```
apic1(config-ipsla-pol)# sla-frequency 40
```

ステップ 5 モニタリング プローブ タイプを設定します。

タイプに指定できる値は次のとおりです。

- `icmp`
- `l2ping`
- `tcp sla-port number`

スタティック ルートの IP SLA には ICMP と TCP のみが有効です。

例：

```
apic1(config-ipsla-pol)# sla-type tcp sla-port 90
```

次のタスク

作成した IP SLA モニタリング ポリシーを表示するには、次のように入力します。

show running-config all tenant *tenant-name* ipsla-pol

次の出力が表示されます。

```
# Command: show running-config all tenant 99 ipsla-pol
# Time: Tue Mar 19 19:01:06 2019
  tenant t1
    ipsla-pol ipsla-policy-3
      sla-detectmultiplier 3
      sla-frequency 40
      sla-type tcp sla-port 90
        sla-port 90
        exit
      exit
    exit
```

NX-OS Style CLI を使用した IP-SLA トラック メンバーの設定

NX-OS スタイルの CLI を使用して IP SLA トラック メンバーを設定するには、次の手順を実行します。

始める前に

テナントおよびテナントの下の IP SLA モニタリング ポリシーが設定されていることを確認します。

手順

ステップ 1 **configure**

コンフィギュレーション モードに入ります。

例：

```
apic1# configure
```

ステップ 2 **tenant** *tenant-name*

テナントを作成するか、テナント設定モードに入ります。

例：

```
apic1(config)# tenant t1
```

ステップ 3 name ipv4-or-ipv6-address name **track-member dst-IpAddr l3-out**

宛先 IP アドレスを持つトラック メンバーを作成し、トラック メンバー コンフィギュレーション モードを開始します。

例：

```
apic1(config-tenant)# )# track-member tm-1 dst-IpAddr 10.10.10.1 l3-out ext-l3-1
```

ステップ 4 **ipsla-monpol** *name*

トラック メンバーに IP SLA モニタリング ポリシーを割り当てます。

例：

```
apic1(config-track-member)# ipsla-monpol ipsla-policy-3
```

例

次の例は、IP SLA トラック メンバーを設定するコマンドを示しています。

```
apic1# configure
      apic1(config)# tenant t1
      apic1(config-tenant)# )# track-member tm-1 dst-IpAddr 10.10.10.1 l3-out ext-l3-1
      apic1(config-track-member)# ipsla-monpol ipsla-policy-3
```

次のタスク

作成したトラック メンバー設定を表示するには、次のように入力します。

show running-config all tenant *tenant-name* **track-member** *name*

次の出力が表示されます。

```
# Command: show running-config all tenant 99 track-member tm-1
# Time: Tue Mar 19 19:01:06 2019
  tenant t1
    track-member tm-1 10.10.10.1 l3-out ext-l3-1
      ipsla-monpol slaICMPProbe
      exit
    exit
```

NX-OS Style CLI を使用した IP-SLA トラック リストの設定

NX-OS スタイルの CLI を使用して IP SLA トラック リストを設定するには、次の手順を実行します。

始める前に

テナント、IP SLA モニタリング ポリシー、およびテナント下の少なくとも 1 つのトラック メンバーが設定されていることを確認します。

手順

ステップ 1 **configure**

コンフィギュレーション モードに入ります。

NX-OS スタイル CLI を使用したタスクの実行

例：

```
apic1# configure
```

ステップ 2 **tenant** *tenant-name*

テナントを作成するか、テナント設定モードに入ります。

例：

```
apic1(config)# tenant t1
```

ステップ 3 **track-list** *name* **{ percentage [percentage-down | percentage-up]** *number* **| weight [weight-down | weight-up** *number* **}**

パーセンテージまたは重みしきい値の設定でトラックリストを作成し、トラック リスト コンフィギュレーション モードを開始します。

例：

```
apic1(config-tenant)# )# track-list tl-1 percentage percentage-down 50 percentage-up 100
```

ステップ 4 **track-member** *name*

既存のトラック メンバーをトラック リストに割り当てます。

例：

```
apic1(config-track-list)# track-member tm-1
```

例

次の例は、IP SLA トラック リストを設定するコマンドを示しています。

```
apic1# configure
      apic1(config)# tenant t1
     apic1(config-tenant)# )# track-list tl-1 percentage percentage-down 50 percentage-up
 100
      apic1(config-track-list)# track-member tm1
```

次のタスク

作成したトラック メンバー設定を表示するには、次のように入力します。

show running-config all tenant *tenant-name* **track-member** *name*

次の出力が表示されます。

```
# Command: show running-config all tenant 99 track-list tl-1
# Time: Tue Mar 19 19:01:06 2019
  tenant t1
    track-list tl-1 percentage percentage-down 50 percentage-up 100
      track-member tm-1 weight 10
      exit
    exit
```

NX-OS Style CLI を使用したスタティック ルートとトラック リストの関連付け

NX-OS スタイル CLI を使用して IP SLA トラック リストをスタティック ルートに関連付けるには、次の手順を実行します。

始める前に

テナント、VRF およびテナントの下にあるトラック リストが設定されていることを確認してください。

手順

ステップ 1 **configure**

コンフィギュレーション モードに入ります。

例：

```
apic1# configure
```

ステップ 2 **leaf** *id* または *leaf-name*

リーフ スイッチを選択し、リーフ スイッチ コンフィギュレーション モードを開始します。

例：

```
apic1(config)# leaf 102
```

ステップ 3 **vrf context tenant** *name* **vrf** *name*

VRF コンテキストを選択し、VRF コンフィギュレーション モードを開始します。

例：

```
apic1(config-leaf)# )# vrf context tenant 99 vrf default
```

ステップ 4 **ip route** *ip-address next-hop-ip-address route-prefix* **bfd ip-trackList** *name*

既存のトラック リストをスタティック ルートに割り当てます。

例：

```
apic1(config-leaf-vrf)# ip route 10.10.10.1/4 20.20.20.8 10 bfd ip-trackList tl-1
```

例

次に、IP SLA トラック リストをスタティック ルートに関連付けるコマンドの例を示します。

```
apic1# configure
      apic1(config)# leaf 102
      apic1(config-leaf)# )# vrf context tenant 99 vrf default
      apic1(config-leaf-vrf)# ip route 10.10.10.1/4 20.20.20.8 10 bfd ip-trackList tl-1
```

NX-OS Style CLI を使用したトラック リストとネクスト ホップ プロファイルの関連付け

NX-OS スタイルの CLI を使用して IP SLA トラック リストをネクスト ホップ プロファイルに関連付けるには、次の手順を実行します。

始める前に

テナント、VRF およびテナントの下にあるトラック リストが設定されていることを確認してください。

手順

ステップ 1 **configure**

コンフィギュレーション モードに入ります。

例：

```
apic1# configure
```

ステップ 2 **leaf** *id* または *leaf-name*

リーフ スイッチを選択し、リーフ スイッチ コンフィギュレーション モードを開始します。

例：

```
apic1(config)# leaf 102
```

ステップ 3 **vrf context tenant** *name* **vrf** *name*

VRF コンテキストを選択し、VRF コンフィギュレーション モードを開始します。

例：

```
apic1(config-leaf)# )# vrf context tenant 99 vrf default
```

ステップ 4 **ip route** *ip-address next-hop-ip-address route-prefix* **bfd nh-ip-trackList** *name*

既存のトラック リストをネクスト ホップに割り当てます。

例：

```
apic1(config-leaf-vrf)# ip route 10.10.10.1/4 20.20.20.8 10 bfd nh-trackList tl-1
```

例

次に、IP SLA トラック リストをネクスト ホップ プロファイルに関連付けるコマンドの例を示します。

```
apic1# configure
      apic1(config)# leaf 102
      apic1(config-leaf)# )# vrf context tenant 99 vrf default
      apic1(config-leaf-vrf)# ip route 10.10.10.1/4 20.20.20.8 10 bfd nh-ip-trackList
tl-1
```

CLI を使用したトラック リストおよびトラック メンバー ステータスの表示

IP SLA トラック リストおよびトラック メンバー ステータスを表示できます。

手順

	コマンドまたはアクション	目的
ステップ 1	show track brief 例： `switch# show track brief`	すべてのトラック リストおよびトラック メンバーのステータスを表示します。

例

```
switch# show track brief
TrackId  Type     Instance    Parameter        State    Last Change
97       IP SLA   2034        reachability     up       2019-03-20T14:08:34.127-07:00
98       IP SLA   2160        reachability     up       2019-03-20T14:08:34.252-07:00
99       List     ---         percentage       up       2019-03-20T14:08:45.494-07:00
100      List     ---         percentage       down     2019-03-20T14:08:45.039-07:00
101      List     ---         percentage       down     2019-03-20T14:08:45.040-07:00
102      List     ---         percentage       up       2019-03-20T14:08:45.495-07:00
103      IP SLA   2040        reachability     up       2019-03-20T14:08:45.493-07:00
104      IP SLA   2887        reachability     down     2019-03-20T14:08:45.104-07:00
105      IP SLA   2821        reachability     up       2019-03-20T14:08:45.494-07:00
1        List     ---         percentage       up       2019-03-20T14:08:39.224-07:00
2        List     ---         weight           down     2019-03-20T14:08:33.521-07:00
3        IP SLA   2412        reachability     up       2019-03-20T14:08:33.983-07:00
26       IP SLA   2320        reachability     up       2019-03-20T14:08:33.988-07:00
27       IP SLA   2567        reachability     up       2019-03-20T14:08:33.987-07:00
28       IP SLA   2598        reachability     up       2019-03-20T14:08:33.990-07:00
29       IP SLA   2940        reachability     up       2019-03-20T14:08:33.986-07:00
30       IP SLA   2505        reachability     up       2019-03-20T14:08:38.915-07:00
31       IP SLA   2908        reachability     up       2019-03-20T14:08:33.990-07:00
32       IP SLA   2722        reachability     up       2019-03-20T14:08:33.992-07:00
33       IP SLA   2753        reachability     up       2019-03-20T14:08:38.941-07:00
34       IP SLA   2257        reachability     up       2019-03-20T14:08:33.993-07:00
```

CLI を使用したトラック リストとトラック メンバーの詳細の表示

IP SLA トラック リストおよびトラック メンバーの詳細を表示できます。

手順

	コマンドまたはアクション	目的
ステップ 1	show track [*number*] | more 例： `switch# show track | more`	すべてのトラック リストおよびトラック メンバーの詳細を表示します。

NX-OS スタイル CLI を使用したタスクの実行

例

```
switch# show track | more
Track 4
    IP SLA 2758
    reachability is down
    1 changes, last change 2019-03-12T21:41:34.729+00:00
    Tracked by:
        Track List 3
        Track List 5

Track 3
    List Threshold percentage
    Threshold percentage is down
    1 changes, last change 2019-03-12T21:41:34.700+00:00
    Threshold percentage up 1% down 0%
    Tracked List Members:
        Object 4 (50)% down
        Object 6 (50)% down
    Attached to:
        Route prefix 172.16.13.0/24

Track 5
    List Threshold percentage
    Threshold percentage is down
    1 changes, last change 2019-03-12T21:41:34.710+00:00
    Threshold percentage up 1% down 0%
    Tracked List Members:
        Object 4 (100)% down
    Attached to:
        Nexthop Addr 12.12.12.2/32

Track 6
    IP SLA 2788
    reachability is down
    1 changes, last change 2019-03-14T21:34:26.398+00:00
    Tracked by:
        Track List 3
        Track List 7

Track 20
    List Threshold percentage
    Threshold percentage is up
    4 changes, last change 2019-02-21T14:04:21.920-08:00
    Threshold percentage up 100% down 32%
    Tracked List Members:
    Object 4 (20)% up
    Object 5 (20)% up
    Object 6 (20)% up
    Object 3 (20)% up
    Object 9 (20)% up
    Attached to:
    Route prefix 88.88.88.0/24
    Route prefix 5000:8:1:14::/64
    Route prefix 5000:8:1:2::/64
    Route prefix 5000:8:1:1::/64
```

この例では、Track 4 は IP SLA ID と [Tracked by：] フィールドのトラック リストによって識別されるトラック メンバーです。

Track 3 は、しきい値情報と [トラック リスト メンバー（Track List Members）] フィールドのトラック メンバーによって識別されるトラック リストです。

トラック 20 は、現在到達可能（アップ）で、関連付けられているスタティック ルートを示すトラック リストです。

NX-OS Style CLI を使用した HSRP の設定

NX-OS スタイル CLI での Cisco APIC を使用してインライン パラメータで HSRP の設定

リーフ スイッチが設定されている場合、HSRP が有効になっています。

始める前に

- テナントと VRF が設定されています。
- VLAN プールは、適切な VLAN 範囲が定義され、レイヤ 3 ドメインが作成されて VLAN プールに接続されている状態で設定される必要があります。
- エンティティ プロファイルの接続も、レイヤ3 ドメインに関連付けられている必要があります。
- リーフ スイッチのインターフェイス プロファイルは必要に応じて設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	コンフィギュレーション モードに入ります。

ステップ 2	インライン パラメータを作成することにより、HSRP を設定します。
	例：
	`apic1(config)# leaf 101`
	`apic1(config-leaf)# interface ethernet 1/17`
	`apic1(config-leaf-if)# hsrp version 1`
	`apic1(config-leaf-if)# hsrp use-bia`
	`apic1(config-leaf-if)# hsrp delay minimum 30`
	`apic1(config-leaf-if)# hsrp delay reload 30`
	`apic1(config-leaf-if)# hsrp 10 ipv4`
	`apic1(config-if-hsrp)# ip 182.16.1.2`
	`apic1(config-if-hsrp)# ip 182.16.1.3 secondary`
	`apic1(config-if-hsrp)# ip 182.16.1.4 secondary`
	`apic1(config-if-hsrp)# mac-address 5000.1000.1060`	

	コマンドまたはアクション	目的
	apic1(config-if-hsrp)# **timers 5 18** apic1(config-if-hsrp)# **priority 100** apic1(config-if-hsrp)# **preempt** apic1(config-if-hsrp)# **preempt delay minimum 60** apic1(config-if-hsrp)# **preempt delay reload 60** apic1(config-if-hsrp)# **preempt delay sync 60** apic1(config-if-hsrp)# **authentication none** apic1(config-if-hsrp)# **authentication simple** apic1(config-if-hsrp)# **authentication md5** apic1(config-if-hsrp)# **authentication-key <mypassword>** apic1(config-if-hsrp)# **authentication-key-timeout <timeout>**	

NX-OS スタイル CLI のテンプレートとポリシーを使用した Cisco APIC の HSRP の設定

リーフ スイッチが設定されている場合、HSRP が有効になっています。

始める前に

- テナントと VRF が設定されています。
- VLAN プールは、適切な VLAN 範囲が定義され、レイヤ 3 ドメインが作成されて VLAN プールに接続されている状態で設定される必要があります。
- エンティティ プロファイルの接続も、レイヤ3ドメインに関連付けられている必要があります。
- リーフ スイッチのインターフェイス プロファイルは必要に応じて設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： apic1# **configure**	コンフィギュレーション モードに入ります。
ステップ 2	HSRP ポリシーテンプレートを設定します。 例： apic1(config)# **leaf 101**	

NX-OS スタイル CLI を使用したタスクの実行

	コマンドまたはアクション	目的
	apic1(config-leaf)# **template hsrp interface-policy hsrp-intfPol1 tenant t9** apic1(config-template-hsrp-if-pol)# **hsrp use-bia** apic1(config-template-hsrp-if-pol)# **hsrp delay minimum 30** apic1(config-template-hsrp-if-pol)# **hsrp delay reload 30** apic1(config)# **leaf 101** apic1(config-leaf)# **template hsrp group-policy hsrp-groupPol1 tenant t9** apic1(config-template-hsrp-group-pol)# **timers 5 18** apic1(config-template-hsrp-group-pol)# **priority 100** apic1(config-template-hsrp-group-pol)# **preempt** apic1(config-template-hsrp-group-pol)# **preempt delay minimum 60** apic1(config-template-hsrp-group-pol)# **preempt delay reload 60** apic1(config-template-hsrp-group-pol)# **preempt delay sync 60**	
ステップ 3	設定されているポリシー テンプレートを使用します。 例： apic1(config)# **leaf 101** apic1(config-leaf)# **interface ethernet 1/17** apic1(config-leaf-if)# **hsrp version 1** apic1(config-leaf-if)# **inherit hsrp interface-policy hsrp-intfPol1** apic1(config-leaf-if)# **hsrp 10 ipv4** apic1(config-if-hsrp)# **ip 182.16.1.2** apic1(config-if-hsrp)# **ip 182.16.1.3 secondary** apic1(config-if-hsrp)# **ip 182.16.1.4 secondary** apic1(config-if-hsrp)# **mac-address 5000.1000.1060** apic1(config-if-hsrp)# **inherit hsrp group-policy hsrp-groupPol1**	

NX-OS Style CLI を使用した Cisco ACI GOLF の設定

NX-OS スタイル CLI を使用した推奨される共有 GOLF 設定

マルチサイトで管理されている複数の APIC サイト間で、DCI による GOLF 接続を共有する場合、ルートマップと BPG を設定し VRF 間のトラフィックの問題を避けるために次の手順を使用します。

手順

ステップ 1 インバウンド ルート マップ

例：

```
Inbound peer policy to attach community:

 route-map multi-site-in permit 10

  set community 1:1 additive
```

ステップ 2 アウトバウンド ピア ポリシーを設定し、インバウンド ピア ポリシーのコミュニティに基づいてルートをフィルタします。

例：

```
ip community-list standard test-com permit 1:1

route-map multi-site-out deny 10

  match community test-com exact-match

route-map multi-site-out permit 11
```

ステップ 3 アウトバウンド ピア ポリシーを設定し、WAN へのコミュニティをフィルタします。

例：

```
ip community-list standard test-com permit 1:1

route-map multi-site-wan-out permit 11

  set comm-list test-com  delete
```

ステップ 4 BGP を設定します。

例：

```
router bgp 1

  address-family l2vpn evpn

  neighbor 11.11.11.11 remote-as 1

    update-source loopback0

    address-family l2vpn evpn

      send-community both
```

```
    route-map multi-site-in in

  neighbor 13.0.0.2 remote-as 2

    address-family l2vpn evpn

      send-community both

      route-map multi-site-out out
```

NX-OS スタイル CLI を使用した Cisco ACI GOLF 設定の例:

次の例を設定する CLI コマンドの show GOLF サービスで、OSPF over スパイン スイッチに接続されている WAN ルータの BGP EVPN プロトコルを使用します。

設定、BGP EVPN のテナント インフラ

次の例を設定する方法を示しています、インフラ VLAN ドメイン、VRF、インターフェイスの IP アドレッシングを含む、BGP EVPN および OSPF のテナントします。

```
configure
  vlan-domain evpn-dom dynamic
  exit
  spine 111
       # Configure  Tenant Infra VRF overlay-1 on the spine.
    vrf context tenant infra vrf overlay-1
        router-id 10.10.3.3
        exit

    interface ethernet 1/33
         vlan-domain member golf_dom
         exit
    interface ethernet 1/33.4
         vrf member tenant infra vrf overlay-1
         mtu 1500
         ip address 5.0.0.1/24
         ip router ospf default area 0.0.0.150
         exit
    interface ethernet 1/34
         vlan-domain member golf_dom
        exit
    interface ethernet 1/34.4
        vrf member tenant infra vrf overlay-1
        mtu 1500
        ip address 2.0.0.1/24
        ip router ospf default area 0.0.0.200
       exit

    router ospf default
       vrf member tenant infra vrf overlay-1
           area 0.0.0.150 loopback 10.10.5.3
           area 0.0.0.200 loopback 10.10.4.3
           exit
       exit
```

スパイン ノード上の BGP の設定

次の例では、BGP EVPN をサポートする BGP を設定する方法を示します。

```
    Configure
    spine 111
    router bgp 100
        vrf member tenant infra vrf overlay- 1
             neighbor 10.10.4.1 evpn
                 label golf_aci
                 update-source loopback 10.10.4.3
                 remote-as 100
                 exit
             neighbor 10.10.5.1 evpn
                 label golf_aci2
                 update-source loopback 10.10.5.3
                 remote-as 100
                 exit
        exit
    exit
```

BGP EVPN のテナントの設定

次の例では、BGP EVPN、BGP EVPN セッションで提供されるゲートウェイ サブネットを含むのテナントを設定する方法を示します。

```
configure
  tenant sky
    vrf context vrf_sky
      exit
    bridge-domain bd_sky
      vrf member vrf_sky
      exit
    interface bridge-domain bd_sky
      ip address 59.10.1.1/24
      exit
    bridge-domain bd_sky2
      vrf member vrf_sky
      exit
    interface bridge-domain bd_sky2
      ip address 59.11.1.1/24
      exit
    exit
```

BGP EVPN ルート ターゲット、ルート マップと、テナントのプレフィックス EPG の設定

次の例では、BGP EVPN を介してブリッジ ドメイン サブネットをアドバタイズするルートマップを設定する方法を示します。

```
configure
spine 111
    vrf context tenant sky vrf vrf_sky
        address-family ipv4 unicast
            route-target export 100:1
            route-target import 100:1
             exit

        route-map rmap
            ip prefix-list p1 permit 11.10.10.0/24
```

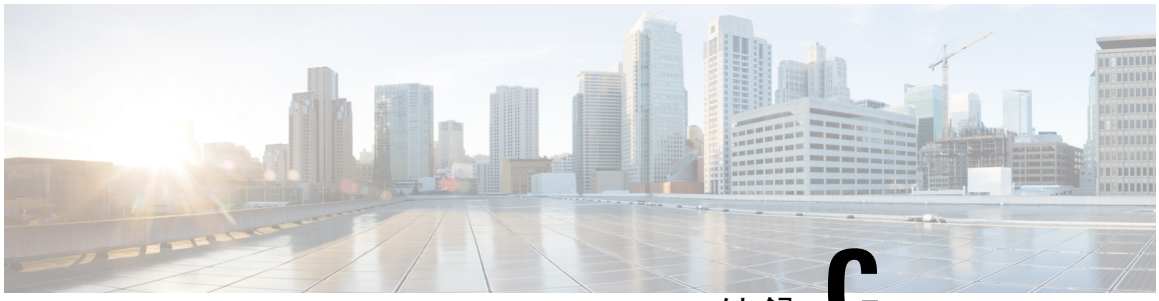
```
      match bridge-domain bd_sky
          exit
      match prefix-list p1
          exit

    evpn export map rmap label golf_aci

     route-map rmap2
      match bridge-domain bd_sky
          exit
      match prefix-list p1
         exit
     exit

    evpn export map rmap label golf_aci2

external-l3 epg l3_sky
  vrf member vrf_sky
  match ip 80.10.1.0/24
  exit
```

NX-OS スタイル CLI を使用して DCIG への配布の BGP EVPN タイプ 2 のホスト ルートの有効化

手順

	コマンドまたはアクション	目的

ステップ 1	BGP アドレス ファミリ configuration mode(設定モード、コンフィギュレーション モード) で、次のコマンドを DCIG に配布 EVPN タイプ 2 のホスト ルートを設定します。
	例：
	`apic1(config)# leaf 101`
	`apic1(config-leaf)# template bgp address-family bgpAf1 tenant bgp_t1`
	`apic1(config-bgp-af)# distance 250 240 230`
	`apic1(config-bgp-af)# host-rt-enable`
	`apic1(config-bgp-af)# exit`
		このテンプレートは、テナント bgp_t1 は VRF の導入を持つすべてのノードで利用可能になります。配布 EVPN タイプ 2 のホスト ルートを無効にするには、次のように入力します。、 **no ホスト -rt-enable** コマンド。



付録 C

REST API を使用してタスクを実行する

Part I： レイヤ 3 の設定

REST API を使用した共通パーベイシブ ゲートウェイの設定

REST API を使用した共通パーベイシブ ゲートウェイの設定

始める前に

- テナント、VRF、およびブリッジ ドメインが作成されていること。

手順

共通パーベイシブ ゲートウェイを設定します。

次の REST API XML の例では、太字のテキストは一般的なパーベイシブ ゲートウェイの設定に関連しています。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/policymgr/mo/.xml -->
<polUni>
  <fvTenant name="test">
    <fvCtx name="test"/>

    <fvBD name="test" vmac="12:34:56:78:9a:bc">
      <fvRsCtx tnFvCtxName="test"/>
      <!-- Primary address -->
      <fvSubnet ip="192.168.15.254/24" preferred="yes"/>
      <!-- Virtual address -->
```

```
      <fvSubnet ip="192.168.15.1/24" virtual="yes"/>
    </fvBD>

    <fvAp name="test">
      <fvAEPg name="web">
        <fvRsBd tnFvBDName="test"/>
        <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/3]" encap="vlan-1002"/>
      </fvAEPg>
    </fvAp>
  </fvTenant>
</polUni>
```

REST API を使用した IP エージングの設定

REST API を使用した IP エージングの設定

このセクションでは、REST API を使用した IP エージング ポリシーを有効および無効にする方法を説明します。

手順

ステップ 1 IP エージング ポリシーを有効にするには：

例：

```
<epIpAgingP adminSt="enabled" descr="" dn="uni/infra/ipAgingP-default" name="default"
ownerKey="" ownerTag=""/>
```

ステップ 2 IP エージング ポリシーを無効にするには：

例：

```
<epIpAgingP adminSt="disabled" descr="" dn="uni/infra/ipAgingP-default" name="default"
ownerKey="" ownerTag=""/>
```

次のタスク

エンドポイントの IP アドレスをトラッキングするために使用される間隔を指定するには、次の例のように XML で post を送信することによって、エンドポイント保持ポリシーを作成します。

```
<fvEpRetPol bounceAgeIntvl="630" bounceTrig="protocol"
holdIntvl="350" lcOwn="local" localEpAgeIntvl="900" moveFreq="256"
name="EndpointPol1" remoteEpAgeIntvl="350"/>
```

REST API を使用したブリッジ ドメインのスタティック ルートの設定

REST API を使用してブリッジ ドメインでのスタティック ルートの設定

- スタティック ルートのサブネットを作成するには、epg (fvAEPg で fvSubnet オブジェクト)、普及 BD (fvBD) 自体 BD しないに関連付けられているように構成されます。
- サブネットマスクが/32 にする必要があります (128/for IPv6) 1 つの IP アドレスまたは 1 つのエンドポイントをポイントします。これは、パーベイシブ BD に関連付けられている EPG に含まれます。

始める前に

テナント、VRF、BD、および EPG が作成されています。

手順

普及ゲートウェイで使用される BD のスタティック ルートを設定するには、次の例など post を入力します。

例：

```
       <fvAEPg name="ep1">
    <fvRsBd tnFvBDName="bd1"/>
           <fvSubnet ip="2002:0db8:85a3:0000:0000:8a2e:0370:7344/128"
ctrl="no-default-gateway"   >
               <fvEpReachability>
                   <ipNexthopEpP  nhAddr="2001:0db8:85a3:0000:0000:8a2e:0370:7343/128"
/>
               </fvEpReachability>
           </fvSubnet>
       </fvAEPg>
```

REST API を使用した IPv6 ネイバー 探索の設定

REST API を使用したブリッジ ドメインの IPv6 ネイバー探索対応のテナント、VRF、およびブリッジ ドメインの作成

手順

ネイバー探索インターフェイス ポリシーとネイバー探索プレフィックス ポリシーが適用された、テナント、VRF、ブリッジ ドメインを作成します。

例：

```
<fvTenant descr="" dn="uni/tn-ExampleCorp" name="ExampleCorp" ownerKey="" ownerTag="">
    <ndIfPol name="NDPol001" ctrl="managed-cfg”  descr="" hopLimit="64" mtu="1500"
nsIntvl="1000" nsRetries="3" ownerKey="" ownerTag="" raIntvl="600" raLifetime="1800"
reachableTime="0" retransTimer="0"/>
    <fvCtx descr="" knwMcastAct="permit" name="pvn1" ownerKey="" ownerTag=""
pcEnfPref="enforced">
    </fvCtx>
    <fvBD arpFlood="no" descr="" mac="00:22:BD:F8:19:FF" multiDstPktAct="bd-flood"
name="bd1" ownerKey="" ownerTag="" unicastRoute="yes" unkMacUcastAct="proxy"
unkMcastAct="flood">
        <fvRsBDToNdP tnNdIfPolName="NDPol001"/>
        <fvRsCtx tnFvCtxName="pvn1"/>
       <fvSubnet ctrl="nd" descr="" ip="34::1/64" name="" preferred="no" scope="private">

            <fvRsNdPfxPol tnNdPfxPolName="NDPfxPol001"/>
        </fvSubnet>
       <fvSubnet ctrl="nd" descr="" ip="33::1/64" name="" preferred="no" scope="private">

            <fvRsNdPfxPol tnNdPfxPolName="NDPfxPol002"/>
        </fvSubnet>
    </fvBD>
    <ndPfxPol ctrl="auto-cfg,on-link" descr="" lifetime="1000" name="NDPfxPol001"
ownerKey="" ownerTag="" prefLifetime="1000"/>
    <ndPfxPol ctrl="auto-cfg,on-link" descr="" lifetime="4294967295" name="NDPfxPol002"
 ownerKey="" ownerTag="" prefLifetime="4294967295"/>
</fvTenant>
```

（注） 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。

REST API を使用したレイヤ 3 インターフェイス上の RA による IPv6 ネイバー探索インターフェイス ポリシーの設定

手順

IPv6 ネイバー検索インターフェイス ポリシーを設定し、レイヤ 3 インターフェイスに関連付けます。

次の例では、非 VPC セットアップの設定が表示されます。

例：

```
<fvTenant dn="uni/tn-ExampleCorp" name="ExampleCorp">
  <ndIfPol name="NDPol001" ctrl="managed-cfg" hopLimit="64" mtu="1500" nsIntvl="1000"
nsRetries="3" raIntvl="600" raLifetime="1800" reachableTime="0" retransTimer="0"/>
  <fvCtx name="pvn1" pcEnfPref="enforced">
                    </fvCtx>
  <l3extOut enforceRtctrl="export" name="l3extOut001">
    <l3extRsEctx tnFvCtxName="pvn1"/>
    <l3extLNodeP name="lnodeP001">
      <l3extRsNodeL3OutAtt rtrId="11.11.205.1" rtrIdLoopBack="yes"
tDn="topology/pod-2/node-2011"/>
      <l3extLIfP name="lifP001">
```

```
        <l3extRsPathL3OutAtt addr="2001:20:21:22::2/64" ifInstT="l3-port" llAddr="::"
mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
tDn="topology/pod-2/paths-2011/pathep-[eth1/1]">
          <ndPfxP>
            <ndRsPfxPToNdPfxPol tnNdPfxPolName="NDPfxPol001"/>
          </ndPfxP>
        </l3extRsPathL3OutAtt>
        <l3extRsNdIfPol tnNdIfPolName="NDPol001"/>
      </l3extLIfP>
    </l3extLNodeP>
    <l3extInstP name="instp"/>
  </l3extOut>
  <ndPfxPol ctrl="auto-cfg,on-link" descr="" lifetime="1000" name="NDPfxPol001" ownerKey=""
 ownerTag="" prefLifetime="1000"/>
</fvTenant>
```

（注） VPC ポートについては、ndPfxP が l3extRsNodeL3OutAtt ではなく l3extMember の子である必要があります。次のコード スニペットは、VPC のセットアップでの設定を示します。

```
<l3extLNodeP name="lnodeP001">
<l3extRsNodeL3OutAtt rtrId="11.11.205.1" rtrIdLoopBack="yes"
tDn="topology/pod-2/node-2011"/>
<l3extRsNodeL3OutAtt rtrId="12.12.205.1" rtrIdLoopBack="yes"
tDn="topology/pod-2/node-2012"/>
  <l3extLIfP name="lifP002">
    <l3extRsPathL3OutAtt addr="0.0.0.0" encap="vlan-205" ifInstT="ext-svi"
llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
tDn="topology/pod-2/protpaths-2011-2012/pathep-[vpc7]" >
      <l3extMember addr="2001:20:25:1::1/64" descr="" llAddr="::" name=""
nameAlias="" side="A">
        <ndPfxP >
          <ndRsPfxPToNdPfxPol tnNdPfxPolName="NDPfxPol001"/>
        </ndPfxP>
      </l3extMember>
      <l3extMember addr="2001:20:25:1::2/64" descr="" llAddr="::" name=""
nameAlias="" side="B">
        <ndPfxP >
          <ndRsPfxPToNdPfxPol tnNdPfxPolName="NDPfxPol001"/>
        </ndPfxP>
      </l3extMember>
    </l3extRsPathL3OutAtt>
    <l3extRsNdIfPol tnNdIfPolName="NDPol001"/>    </l3extLIfP>
  </l3extLNodeP>
```

REST API を使用したネイバー探索重複アドレス検出の設定

手順

ステップ 1 サブネットの ipv6Dad エントリの値を **disabled** に変更することによって、サブネットのネイバー探索重複アドレス検出プロセスを無効にします。

次の例は、2001:DB8:A::11/64 サブネットのネイバー探索重複アドレス検出エントリを **disabled** に設定する方法を示しています:

（注） 次の REST API の例では、読みやすくなるように、長い行を \ 文字で分割しています。

例：

```
                <l3extRsPathL3OutAtt addr="2001:DB8:A::2/64" autostate="enabled" \
                 childAction="" descr="" encap="vlan-1035" encapScope="local" \
                 ifInstT="ext-svi" ipv6Dad="enabled" llAddr=": :" \
                 mac="00:22:BD:F8:19:DD"  mtu="inherit"  \
                 rn="rspathL3OutAtt-[topology/pod-1/paths-105/pathep-[eth1/1]]"  \
                 status=""  tDn="topology/pod-1/paths-105/pathep-[eth1/1]"  >
                    <l3extIp addr="2001:DB8:A::11/64" childAction="" descr="" \
                     ipv6Dad="disabled"  name="" nameAlias="" \
                     rn="addr-[2001:DB8:A::11/64]" status=""/>

                </l3extRsPathL3OutAtt>
            </l3extLIfP>
        </l3extLNodeP>
```

ステップ 2 リーフ スイッチで **show ipv6 int** コマンドを入力して、設定がリーフ スイッチに正しくプッシュされたか確認してください。例：

```
swtb23-leaf5# show ipv6 int vrf icmpv6:v1
IPv6 Interface Status for VRF "icmpv6:v1"(9)

vlan2, Interface status: protocol-up/link-up/admin-up, iod: 73
if_mode: ext
  IPv6 address:
    2001:DB8:A::2/64 [VALID] [PREFERRED]
    2001:DB8:A::11/64 [VALID] [dad-disabled]
  IPv6 subnet:  2001:DB8:A::/64
  IPv6 link-local address: fe80::863d:c6ff:fe9f:eb8b/10 (Default) [VALID]
```

REST API を使用した Microsoft NLB の設定

REST API を使用したユニキャスト モードでの Microsoft NLB の設定

手順

Microsoft NLB をユニキャスト モードで設定するには、次の例のように XML で POST を送信します。

例：

```
https://apic-ip-address/api/node/mo/uni/.xml
<polUni>
    <fvTenant name="tn2" >
        <fvCtx name="ctx1"/>
        <fvBD name="bd2">
            <fvRsCtx tnFvCtxName="ctx1" />
        </fvBD>
        <fvAp name = "ap1">
            <fvAEPg name = "ep1">
                <fvRsBd tnFvBDName = "bd2"/>
                <fvSubnet ip="10.0.1.1/32" scope="public" ctrl="no-default-gateway">
                    <fvEpNlb mac="12:21:21:35" mode="mode-uc"/>
                </fvSubnet>
            </fvAEPg>
        </fvAp>
    </fvTenant>
</polUni>
```

REST API を使用したマルチキャスト モードでの Microsoft NLB の設定

手順

Microsoft NLB をマルチキャスト モードで設定するには、次の例のように XML で POST を送信します。

例：

```
https://apic-ip-address/api/node/mo/uni/.xml
<polUni>
    <fvTenant name="tn2" >
        <fvCtx name="ctx1"/>
        <fvBD name="bd2">
            <fvRsCtx tnFvCtxName="ctx1" />
        </fvBD>
        <fvAp name = "ap1">
            <fvAEPg name = "ep1">
                <fvRsBd tnFvBDName = "bd2"/>
              <fvSubnet ip="2001:0db8:85a3:0000:0000:8a2e:0370:7344/128" scope="public"
 ctrl="no-default-gateway">
                    <fvEpNlb mac="03:21:21:35" mode="mode-mcast--static"/>
                </fvSubnet>
                <fvRsPathAtt tDn="topology/pod-1/paths-101/pathep-[eth1/6]"
encap="vlan-911" >
                    <fvNlbStaticGroup mac = "03:21:21:35"  />
                </fvRsPathAtt>
            </fvAEPg>
        </fvAp>
    </fvTenant>
</polUni>
```

REST API を使用した IGMP モードでの Microsoft NLB の設定

手順

Microsoft NLB を IGMP モードで設定するには、次の例のように XML で POST を送信します。

例：

```
https://apic-ip-address/api/node/mo/uni/.xml
<polUni>
    <fvTenant name="tn2" >
        <fvCtx name="ctx1"/>
        <fvBD name="bd2">
            <fvRsCtx tnFvCtxName="ctx1" />
        </fvBD>
        <fvAp name = "ap1">
            <fvAEPg name = "ep1">
                <fvRsBd tnFvBDName = "bd2"/>
                <fvSubnet ip="10.0.1.3/32" scope="public" ctrl="no-default-gateway">
                    <fvEpNlb group ="224.132.18.17" mode="mode-mcast-igmp" />
                </fvSubnet>
            </fvAEPg>
        </fvAp>
    </fvTenant>
</polUni>
```

REST API を使用した IGMP スヌーピングの設定

REST API を使用したブリッジ ドメインへの IGMP スヌーピング ポリシーの設定と割り当て

手順

IGMP スヌーピング ポリシーを設定してブリッジ ドメインに割り当てるには、次の例のように XML で POST を送信します。

例：

```
https://apic-ip-address/api/node/mo/uni/.xml
<fvTenant name="mcast_tenant1">
<!-- Create an IGMP snooping template, and provide the options -->
<igmpSnoopPol name="igmp_snp_bd_21"
ver="v2"
adminSt="enabled"
lastMbrIntvl="1"
queryIntvl="125"
rspIntvl="10"
startQueryCnt="2"
startQueryIntvl="31"
```

```
/>
<fvCtx name="ip_video"/>
<fvBD name="bd_21">
<fvRsCtx tnFvCtxName="ip_video"/>
<!-- Bind IGMP snooping to a BD -->
<fvRsIgmpsn tnIgmpSnoopPolName="igmp_snp_bd_21"/>
</fvBD></fvTenant>
```

この例では、次のプロパティで IGMP スヌーピング ポリシー、igmp_snp_bd_12 を作成および設定し、IGNPポリシー、igmp_snp_bd_12 をブリッジ ドメイン bd_21 にバインドします。

- 管理状態が有効です。
- 最後のメンバ クエリ間隔は、デフォルトでは、1 秒です。
- クエリ間隔は、デフォルトでは 125 です。
- クエリの応答間隔はデフォルトでは 10 秒です。
- クエリの開始カウントは、デフォルトでは 2 メッセージです。
- クエリの開始間隔は 31 秒です。
- クエリア バージョンを v2 に設定する。

REST API を使用した静的ポートでの IGMP スヌーピングとマルチキャストの有効化

EPG に静的に割り当てられているポートで、IGMP スヌーピングおよびマルチキャスト処理を有効にできます。それらのポートで有効な IGMP スヌープおよびマルチキャスト トラフィックへのアクセスを許可または拒否するアクセス ユーザーのグループを作成および割り当てることができます。

手順

スタティック ポートでアプリケーション EPG を設定するには、それらのポートを IGMP スヌーピングおよびマルチキャスト トラフィックを受信し処理するように有効にして、グループをアクセスに割り当てるかトラフィックへのアクセスを拒否するように割り当て、次の例のように XML で POST を送信します。

次の例では、IGMP スヌーピングが VLAN `202` 上の `leaf 102` インターフェイス `1/10` で有効になっています。マルチキャスト IP アドレス `224.1.1.1` および `225.1.1.` がこのポートに関連付けられます。

例：

```
https://apic-ip-address/api/node/mo/uni/.xml
<fvTenant name="tenant_A">
  <fvAp name="application">
    <fvAEPg name="epg_A">
      <fvRsPathAtt encap="vlan-202" instrImedcy="immediate" mode="regular"
tDn="topology/pod-1/paths-102/pathep-[eth1/10]">
        <!-- IGMP snooping static group case -->
```

```
        <igmpSnoopStaticGroup group="224.1.1.1" source="0.0.0.0"/>
        <igmpSnoopStaticGroup group="225.1.1.1" source="2.2.2.2"/>
      </fvRsPathAtt>
    </fvAEPg>
  </fvAp>
</fvTenant>
```

IGMP スヌーピングを REST API を使用するマルチ キャスト グループのアクセスを有効化

IGMP を有効にした後にスヌーピングおよび、EPG に静的に割り当てられているポートでマルチキャストすることができますし、作成を許可または IGMP スヌーピングへのアクセスを拒否するユーザのアクセスのグループを割り当てるおよびマルチキャスト トラフィックは、これらのポートで有効になっています。

手順

アクセスグループを定義する `F23broker` 、送信 XML で post このような次の例のよ。

例は、設定アクセスグループ `F23broker` tenant_A、Rmap_A、application_A、リーフ 102、1/10、インターフェイス VLAN 202 で、epg_A に関連付けられている。Rmap_A、アクセスグループとの関連付けによって `F23broker` マルチキャスト アドレス 226.1.1.1/24 で受信したマルチキャスト トラフィックへのアクセスがあり、マルチキャスト アドレス 227.1.1.1/24 で受信したトラフィックへのアクセスは拒否されます。

例：

```
<!-- api/node/mo/uni/.xml --> <fvTenant name="tenant_A"> <pimRouteMapPol name="Rmap_A">
<pimRouteMapEntry action="permit" grp="226.1.1.1/24" order="10"/> <pimRouteMapEntry action="deny"
grp="227.1.1.1/24" order="20"/> </pimRouteMapPol> <fvAp name="application_A"> <fvAEPg
name="epg_A"> <fvRsPathAtt encap="vlan-202" instrImedcy="immediate" mode="regular"
tDn="topology/pod-1/paths-102/pathep-[eth1/10]"> <!-- IGMP snooping access group case -->
<igmpSnoopAccessGroup name="F23broker"> <igmpRsSnoopAccessGroupFilterRMap
tnPimRouteMapPolName="Rmap_A"/> </igmpSnoopAccessGroup> </fvRsPathAtt> </fvAEPg> </fvAp>
</fvTenant>
```

REST API を使用した MLD スヌーピングの設定

REST API を使用した MLD スヌーピング ポリシーの設定とブリッジ ドメインへの割り当て

手順

MLD スヌーピング ポリシーを設定してブリッジ ドメインに割り当てるには、次の例のように XML で POST を送信します。

例：

```
https://apic-ip-address/api/node/mo/uni/.xml
<fvTenant name="mldsn">
    <mldSnoopPol adminSt="enabled" ctrl="fast-leave,querier"
name="mldsn-it-fabric-querier-policy" queryIntvl="125"
        rspIntvl="10" startQueryCnt="2" startQueryIntvl="31" status=""/>
    <fvBD name="mldsn-bd3">
        <fvRsMldsn status="" tnMldSnoopPolName="mldsn-it-policy"/>
    </fvBD>
</fvTenant>
```

この例では、MLD スヌーピング ポリシー [mldsn] を作成して次のプロパティを設定し、MLD ポリシー [mldsn-it-fabric-querier-policy] をブリッジ ドメイン [mldsn-bd3] にバインドします。

- 高速脱退処理が有効になっています
- クエリア処理が有効になっています
- クエリ間隔は 125 に設定されています
- 最大クエリ レスポンス タイムは 10 に設定されています
- 送信する初期クエリの数は 2 に設定されます
- 初期クエリの送信時間は 31 に設定されます

REST API を使用した IP マルチキャストの設定

REST API を使用したレイヤ 3 マルチキャストの設定

手順

ステップ 1 テナントと VRF を設定し、VRF のマルチキャストを有効にします。

例：

REST API を使用してタスクを実行する

```
<fvTenant dn="uni/tn-PIM_Tenant" name="PIM_Tenant">
   <fvCtx knwMcastAct="permit" name="ctx1">
       <pimCtxP mtu="1500">
       </pimCtxP>
   </fvCtx>
  </fvTenant>
```

ステップ 2 L3 アウトを設定し、L3 アウト上のマルチキャスト（PIM、IGMP）を有効にします。

例：

```
<l3extOut enforceRtctrl="export" name="l3out-pim_l3out1">
       <l3extRsEctx tnFvCtxName="ctx1"/>
       <l3extLNodeP configIssues="" name="bLeaf-CTX1-101">
         <l3extRsNodeL3OutAtt rtrId="200.0.0.1" rtrIdLoopBack="yes"
tDn="topology/pod-1/node-101"/>
         <l3extLIfP name="if-PIM_Tenant-CTX1" tag="yellow-green">
           <igmpIfP/>
           <pimIfP>
             <pimRsIfPol tDn="uni/tn-PIM_Tenant/pimifpol-pim_pol1"/>
           </pimIfP>
           <l3extRsPathL3OutAtt addr="131.1.1.1/24" ifInstT="l3-port" mode="regular"
mtu="1500" tDn="topology/pod-1/paths-101/pathep-[eth1/46]"/>
         </l3extLIfP>
       </l3extLNodeP>
       <l3extRsL3DomAtt tDn="uni/l3dom-l3outDom"/>
       <l3extInstP name="l3out-PIM_Tenant-CTX1-1topo" >
       </l3extInstP>
       <pimExtP enabledAf="ipv4-mcast" name="pim"/>
     </l3extOut>
```

ステップ 3 テナントで BD を設定して、BD のマルチキャストおよび IGMP を有効にします。

例：

```
<fvTenant dn="uni/tn-PIM_Tenant" name="PIM_Tenant">
   <fvBD arpFlood="yes" mcastAllow="yes" multiDstPktAct="bd-flood" name="bd2"
type="regular" unicastRoute="yes" unkMacUcastAct="flood" unkMcastAct="flood">
       <igmpIfP/>
       <fvRsBDToOut tnL3extOutName="l3out-pim_l3out1"/>
       <fvRsCtx tnFvCtxName="ctx1"/>
       <fvRsIgmpsn/>
      <fvSubnet ctrl="" ip="41.1.1.254/24" preferred="no" scope="private" virtual="no"/>

     </fvBD>
 </fvTenant>
```

ステップ 4 IGMP ポリシーを設定し、それを BD に割り当てます。

例：

```
<fvTenant dn="uni/tn-PIM_Tenant" name="PIM_Tenant">
     <igmpIfPol grpTimeout="260" lastMbrCnt="2" lastMbrRespTime="1" name="igmp_pol"
querierTimeout="255" queryIntvl="125" robustFac="2" rspIntvl="10" startQueryCnt="2"
startQueryIntvl="125" ver="v2">
     </igmpIfPol>
      <fvBD arpFlood="yes" mcastAllow="yes" name="bd2">
      <igmpIfP>
         <igmpRsIfPol tDn="uni/tn-PIM_Tenant/igmpIfPol-igmp_pol"/>
       </igmpIfP>
      </fvBD>
 </fvTenant>
```

ステップ 5 VRF のルート マップ、PIM、および RP ポリシーを設定します。

REST API を使用してタスクを実行する

（注） REST API を使用してファブリック RP を設定する場合、最初にスタティック RP を設定します。

例：

スタティック RP を設定しています：

```
<fvTenant dn="uni/tn-PIM_Tenant" name="PIM_Tenant">
     <pimRouteMapPol name="rootMap">
       <pimRouteMapEntry action="permit" grp="224.0.0.0/4" order="10" rp="0.0.0.0"
src="0.0.0.0/0"/>
     </pimRouteMapPol>
     <fvCtx knwMcastAct="permit" name="ctx1">
       <pimCtxP ctrl="" mtu="1500">
         <pimStaticRPPol>
           <pimStaticRPEntryPol rpIp="131.1.1.2">
             <pimRPGrpRangePol>
               <rtdmcRsFilterToRtMapPol tDn="uni/tn-PIM_Tenant/rtmap-rootMap"/>
             </pimRPGrpRangePol>
           </pimStaticRPEntryPol>
         </pimStaticRPPol>
       </pimCtxP>
   </fvCtx>
</fvTenant>
```

ファブリック RP を設定しています：

```
<fvTenant name="t0">
            <pimRouteMapPol name="fabricrp-rtmap">
               <pimRouteMapEntry grp="226.20.0.0/24" order="1"  />
            </pimRouteMapPol>
  <fvCtx name="ctx1">
         <pimCtxP ctrl="">
               <pimFabricRPPol status="">
                   <pimStaticRPEntryPol rpIp="6.6.6.6">
                       <pimRPGrpRangePol>
                          <rtdmcRsFilterToRtMapPol tDn="uni/tn-t0/rtmap-fabricrp-rtmap"
 />
                       </pimRPGrpRangePol>
                   </pimStaticRPEntryPol>
               </pimFabricRPPol>
            </pimCtxP>
  </fvCtx>
</fvTenant>
```

ステップ 6 PIM インターフェイス ポリシーを設定し、それを L3 アウトに適用します。

例：

```
<fvTenant dn="uni/tn-PIM_Tenant" name="PIM_Tenant">
  <pimIfPol authKey="" authT="none" ctrl="" drDelay="60" drPrio="1" helloItvl="30000"
itvl="60" name="pim_pol1"/>
  <l3extOut enforceRtctrl="export" name="l3out-pim_l3out1" targetDscp="unspecified">
       <l3extRsEctx tnFvCtxName="ctx1"/>
       <l3extLNodeP  name="bLeaf-CTX1-101">
         <l3extRsNodeL3OutAtt rtrId="200.0.0.1" rtrIdLoopBack="yes"
tDn="topology/pod-1/node-101"/>
         <l3extLIfP name="if-SIRI_VPC_src_recv-CTX1" tag="yellow-green">
           <pimIfP>
             <pimRsIfPol tDn="uni/tn-tn-PIM_Tenant/pimifpol-pim_pol1"/>
           </pimIfP>
         </l3extLIfP>
       </l3extLNodeP>
```

```
    </l3extOut>
 </fvTenant>
```

ステップ 7 Inter-VRF マルチキャストを設定します。

例：

```
<fvTenant name="t0">
            <pimRouteMapPol name="intervrf" status="">
               <pimRouteMapEntry grp="225.0.0.0/24" order="1" status=""/>
               <pimRouteMapEntry grp="226.0.0.0/24" order="2" status=""/>
               <pimRouteMapEntry grp="228.0.0.0/24" order="3" status="deleted"/>
            </pimRouteMapPol>
        <fvCtx name="ctx1">
            <pimCtxP ctrl="">
               <pimInterVRFPol status="">
                   <pimInterVRFEntryPol srcVrfDn="uni/tn-t0/ctx-stig_r_ctx" >
                    <rtdmcRsFilterToRtMapPol tDn="uni/tn-t0/rtmap-intervrf" />
                   </pimInterVRFEntryPol>
               </pimInterVRFPol>
            </pimCtxP>
        </fvCtx>
</fvTenant>
```

REST API を使用したレイヤ 3 IPv6 マルチキャストの設定

始める前に

- 目的の VRF、ブリッジドメイン、IPv6 アドレスを持つレイヤ 3 Out インターフェイスは、PIM6 が有効になるように設定する必要があります。レイヤ 3 Out の場合、IPv6 マルチキャストが機能するために、論理ノード プロファイルのノードに IPv6 ループバック アドレスが設定されます。
- 基本的なユニキャスト ネットワークを設定する必要があります。

手順

ステップ 1 VRF で PIM6 を有効にします。

例：

```
<fvTenant name="t0">
  <fvCtx name="ctx1" pcEnfPref="unenforced" >
    <pimIPV6CtxP ctrl=""  mtu="1500" />
  </fvCtx>
</fvTenant>
```

ステップ 2 レイヤ 3 Out で PIM6 を有効にします。

例：

```
<fvTenant dn="uni/tn-t0" name="t0">
  <l3extOut enforceRtctrl="export" name="bl_l3out_1">
```

REST API を使用してタスクを実行する

```
    <pimExtP enabledAf="ipv6-mcast" name="pim"/>
  </l3extOut>
</fvTenant>
```

ステップ 3 BD で PIM6 を有効にします。

例：

```
<fvTenant name="t0" >
  <fvBD name="BD_VPC5" ipv6McastAllow="yes" >
    <fvRsCtx tnFvCtxName="ctx1" />
    <fvSubnet ip="124:1::ffff:ffff:ffff:0/64" scope="public"/>
  </fvBD>
</fvTenant>
```

ステップ 4 スタティック ランデブー ポイントの設定

例：

```
<fvTenant name="t0">
  <pimRouteMapPol dn="uni/tn-t0/rtmap-static_101_ipv6" name="static_101_ipv6">
    <pimRouteMapEntry action="permit" grp="ff00::/8" order="1"
rp="2001:0:2001:2001:1:1:1:1/128" src="::"/>
  </pimRouteMapPol>
  <fvCtx name="ctx1" pcEnfPref="unenforced">
    <pimIPV6CtxP ctrl="" mtu="1500">
      <pimStaticRPPol>
        <pimStaticRPEntryPol rpIp="2001:0:2001:2001:1:1:1:1">
          <pimRPGrpRangePol>
            <rtdmcRsFilterToRtMapPol tDn="uni/tn-t0/rtmap-static_101_ipv6"/>
          </pimRPGrpRangePol>
        </pimStaticRPEntryPol>
      </pimStaticRPPol>
    </pimIPV6CtxP>
  </fvCtx>
</fvTenant>
```

ステップ 5 PIM6 インターフェイス ポリシーを設定し、レイヤ 3 Out に適用します。

例：

```
<fvTenant dn="uni/tn-t0" name="t0">
  <l3extOut enforceRtctrl="export" name="bl_l3out_1">
    <l3extLNodeP annotation="" configIssues="" descr="" name="common_np1" nameAlias=""
ownerKey="" ownerTag="" tag="yellow-green" targetDscp="unspecified">
       <l3extLIfP annotation="" descr="" name="common_intp1_v6" nameAlias="" ownerKey=""
 ownerTag="" prio="unspecified" tag="yellow-green">
            <pimIPV6IfP annotation="" descr="" name="" nameAlias="">
            <pimRsV6IfPol annotation="" tDn="uni/tn-common/pimifpol-pimv6_policy"/>
            </pimIPV6IfP>
       </l3extLIfP>
    </l3extLNodeP>
  </l3extOut>
</fvTenant>
```

PIM6 を使用したレイヤ 3 IPv6 マルチキャストが有効になります。

REST API を使用したマルチキャスト フィルタリングの設定

ブリッジ ドメイン レベルでマルチキャスト フィルタリングを設定します。このトピックの手順を使用して、ブリッジ ドメイン レベルで送信元フィルタリングまたは受信者フィルタリング、あるいはその両方を設定します。

始める前に

- マルチキャストフィルタリングを設定するブリッジ ドメインはすでに作成されています。
- ブリッジ ドメインは PIM 対応ブリッジ ドメインです。
- レイヤ 3 マルチキャストは VRF レベルで有効になります。

手順

ステップ 1 ブリッジ ドメインでマルチキャスト ソース フィルタリングを有効にする場合は、次の例のように XML で POST を送信します。

例：

```
<fvBD dn="uni/tn-filter/BD-BD1520" ipv6McastAllow="no" mcastAllow="yes">
 <pimBDP annotation="" descr="" name="" nameAlias="" ownerKey="" ownerTag="">
  <pimBDFilterPol annotation="" descr="" name="" nameAlias="">
   <pimBDSrcFilterPol annotation="" descr="" name="" nameAlias="">
    <rtdmcRsFilterToRtMapPol tDn="uni/tn-filter/rtmap-test_src_filter"/>
   </pimBDSrcFilterPol>
  </pimBDFilterPol>
 </pimBDP>
</fvBD>
```

ステップ 2 ブリッジ ドメインでマルチキャスト レシーバ フィルタリングを有効にする場合は、次の例のように XML で POST を送信します。

例：

```
<fvBD dn="uni/tn-filter/BD-BD1520" ipv6McastAllow="no" mcastAllow="yes">
 <pimBDP annotation="" descr="" name="" nameAlias="" ownerKey="" ownerTag="">
  <pimBDFilterPol annotation="" descr="" name="" nameAlias="">
   <pimBDDestFilterPol annotation="" descr="" name="" nameAlias="">
    <rtdmcRsFilterToRtMapPol tDn="uni/tn-filter/rtmap-Recv_filter"/>
   </pimBDDestFilterPol>
  </pimBDFilterPol>
 </pimBDP>
</fvBD>
```

（注） また、次の例のように XML で POST を送信することで、同じブリッジ ドメインで送信元と受信者の両方のフィルタリングを有効にすることもできます。

```
<fvBD dn="uni/tn-filter/BD-BD1520" ipv6McastAllow="no" mcastAllow="yes">
 <pimBDP annotation="" descr="" name="" nameAlias="" ownerKey="" ownerTag="">
  <pimBDFilterPol annotation="" descr="" name="" nameAlias="">
   <pimBDSrcFilterPol annotation="" descr="" name="" nameAlias="">
    <rtdmcRsFilterToRtMapPol tDn="uni/tn-filter/rtmap-test_src_filter"/>
   </pimBDSrcFilterPol>
   <pimBDDestFilterPol annotation="" descr="" name="" nameAlias="">
    <rtdmcRsFilterToRtMapPol tDn="uni/tn-filter/rtmap-Recv_filter"/>
   </pimBDDestFilterPol>
  </pimBDFilterPol>
 </pimBDP>
</fvBD>
```

REST API を使用したマルチポッドの設定

REST API を使用したマルチポッド ファブリックのセットアップ

手順

ステップ 1 Cisco APIC へのログイン：

例：

```
http://<apic-name/ip>:80/api/aaaLogin.xml

data: <aaaUser name="admin" pwd="ins3965!”/>
```

ステップ 2 TEP プールの設定：

例：

```
http://<apic-name/ip>:80/api/policymgr/mo/uni/controller.xml

<fabricSetupPol status=''>
    <fabricSetupP podId="1" tepPool="10.0.0.0/16" />
    <fabricSetupP podId="2" tepPool="10.1.0.0/16" status='' />
</fabricSetupPol>
```

ステップ 3 ノード ID ポリシーの設定：

例：

```
http://<apic-name/ip>:80/api/node/mo/uni/controller.xml

<fabricNodeIdentPol>
<fabricNodeIdentP serial="SAL1819RXP4" name="ifav4-leaf1" nodeId="101" podId="1"/>
<fabricNodeIdentP serial="SAL1803L25H" name="ifav4-leaf2" nodeId="102" podId="1"/>
<fabricNodeIdentP serial="SAL1934MNY0" name="ifav4-leaf3" nodeId="103" podId="1"/>
<fabricNodeIdentP serial="SAL1934MNY3" name="ifav4-leaf4" nodeId="104" podId="1"/>
<fabricNodeIdentP serial="SAL1748H56D" name="ifav4-spine1" nodeId="201" podId="1"/>
<fabricNodeIdentP serial="SAL1938P7A6" name="ifav4-spine3" nodeId="202" podId="1"/>
```

REST API を使用してタスクを実行する

```
<fabricNodeIdentP serial="SAL1938PHBB" name="ifav4-leaf5" nodeId="105" podId="2"/>
<fabricNodeIdentP serial="SAL1942R857" name="ifav4-leaf6" nodeId="106" podId="2"/>
<fabricNodeIdentP serial="SAL1931LA3B" name="ifav4-spine2" nodeId="203" podId="2"/>
<fabricNodeIdentP serial="FGE173400A9" name="ifav4-spine4" nodeId="204" podId="2"/>
</fabricNodeIdentPol>
```

ステップ 4 インフラ L3Out および外部接続プロファイルの設定：

例：

```
http://<apic-name/ip>:80/api/node/mo/uni.xml

<polUni>

<fvTenant descr="" dn="uni/tn-infra" name="infra" ownerKey="" ownerTag="">

   <l3extOut descr="" enforceRtctrl="export" name="multipod" ownerKey="" ownerTag=""
targetDscp="unspecified" status=''>
      <ospfExtP areaId='0' areaType='regular' status=''/>
      <l3extRsEctx tnFvCtxName="overlay-1"/>
     <l3extProvLbl descr="" name="prov_mp1" ownerKey="" ownerTag="" tag="yellow-green"/>


      <l3extLNodeP name="bSpine">
         <l3extRsNodeL3OutAtt rtrId="201.201.201.201" rtrIdLoopBack="no"
tDn="topology/pod-1/node-201">
            <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
            <l3extLoopBackIfP addr="201::201/128" descr="" name=""/>
            <l3extLoopBackIfP addr="201.201.201.201/32" descr="" name=""/>
         </l3extRsNodeL3OutAtt>

         <l3extRsNodeL3OutAtt rtrId="202.202.202.202" rtrIdLoopBack="no"
tDn="topology/pod-1/node-202">
            <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
            <l3extLoopBackIfP addr="202::202/128" descr="" name=""/>
            <l3extLoopBackIfP addr="202.202.202.202/32" descr="" name=""/>
         </l3extRsNodeL3OutAtt>

         <l3extRsNodeL3OutAtt rtrId="203.203.203.203" rtrIdLoopBack="no"
tDn="topology/pod-2/node-203">
            <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
            <l3extLoopBackIfP addr="203::203/128" descr="" name=""/>
            <l3extLoopBackIfP addr="203.203.203.203/32" descr="" name=""/>
         </l3extRsNodeL3OutAtt>

         <l3extRsNodeL3OutAtt rtrId="204.204.204.204" rtrIdLoopBack="no"
tDn="topology/pod-2/node-204">
            <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
            <l3extLoopBackIfP addr="204::204/128" descr="" name=""/>
            <l3extLoopBackIfP addr="204.204.204.204/32" descr="" name=""/>
         </l3extRsNodeL3OutAtt>

         <l3extLIfP name='portIf'>
          <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-1/paths-201/pathep-[eth1/1]"
 encap='vlan-4'  ifInstT='sub-interface' addr="201.1.1.1/30" />
          <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-1/paths-201/pathep-[eth1/2]"
 encap='vlan-4'  ifInstT='sub-interface' addr="201.2.1.1/30" />
          <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-1/paths-202/pathep-[eth1/2]"
 encap='vlan-4'  ifInstT='sub-interface' addr="202.1.1.1/30" />
          <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-2/paths-203/pathep-[eth1/1]"
 encap='vlan-4'  ifInstT='sub-interface' addr="203.1.1.1/30" />
          <l3extRsPathL3OutAtt descr='asr' tDn="topology/pod-2/paths-203/pathep-[eth1/2]"
 encap='vlan-4'  ifInstT='sub-interface' addr="203.2.1.1/30" />
           <l3extRsPathL3OutAtt descr='asr'
```

```
tDn="topology/pod-2/paths-204/pathep-[eth4/31]" encap='vlan-4'  ifInstT='sub-interface'
 addr="204.1.1.1/30" />

           <ospfIfP>
               <ospfRsIfPol tnOspfIfPolName='ospfIfPol'/>
           </ospfIfP>

         </l3extLIfP>
      </l3extLNodeP>

      <l3extInstP descr="" matchT="AtleastOne" name="instp1" prio="unspecified"
targetDscp="unspecified">
          <fvRsCustQosPol tnQosCustomPolName=""/>
      </l3extInstP>
   </l3extOut>

  <fvFabricExtConnP descr="" id="1" name="Fabric_Ext_Conn_Pol1" rt="extended:as2-nn4:5:16"
 status=''>
      <fvPodConnP descr="" id="1" name="">
         <fvIp addr="100.11.1.1/32"/>
      </fvPodConnP>
      <fvPodConnP descr="" id="2" name="">
         <fvIp addr="200.11.1.1/32"/>
      </fvPodConnP>
      <fvPeeringP descr="" name="" ownerKey="" ownerTag=""
type="automatic_with_full_mesh"/>
     <l3extFabricExtRoutingP descr="" name="ext_routing_prof_1" ownerKey="" ownerTag="">

         <l3extSubnet aggregate="" descr="" ip="100.0.0.0/8" name=""
scope="import-security"/>
         <l3extSubnet aggregate="" descr="" ip="200.0.0.0/8" name=""
scope="import-security"/>
         <l3extSubnet aggregate="" descr="" ip="201.1.0.0/16" name=""
scope="import-security"/>
         <l3extSubnet aggregate="" descr="" ip="201.2.0.0/16" name=""
scope="import-security"/>
         <l3extSubnet aggregate="" descr="" ip="202.1.0.0/16" name=""
scope="import-security"/>
         <l3extSubnet aggregate="" descr="" ip="203.1.0.0/16" name=""
scope="import-security"/>
         <l3extSubnet aggregate="" descr="" ip="203.2.0.0/16" name=""
scope="import-security"/>
         <l3extSubnet aggregate="" descr="" ip="204.1.0.0/16" name=""
scope="import-security"/>
      </l3extFabricExtRoutingP>
   </fvFabricExtConnP>
</fvTenant>
</polUni>
```

REST API を使用したリモート リーフ スイッチの設定

REST API を使用したリモート リーフ スイッチの設定

Cisco APIC を有効にして IPN ルータとリモートリーフ スイッチを検出し接続するには、このトピックの手順を実行します。

REST API を使用してタスクを実行する

この例では、マルチポッド トポロジで、ポッドにリモート リーフ スイッチが接続されていることを前提としています。VRF オーバーレイ 1 とともに、インフラ テナントに設定されている 2 個の L3Outs が含まれます。

- 1 個は VLAN 4 に設定され、リモート リーフ スイッチとスパイン スイッチ両方が WAN ルータに接続されている必要があります。
- 1 個はマルチポッド内部 L3Out が VLAN5 で設定されており、一緒に展開する場合はマルチポッドとリモート リーフ機能に必要です。

手順

ステップ 1 ポッドに接続されるように 2 個のリモート リーフ スイッチに TEP プールを定義するには、次の例のように XML で POST を送信します。

例：

```
<fabricSetupPol>
      <fabricSetupP tepPool="10.0.0.0/16" podId="1" >
           <fabricExtSetupP tepPool="30.0.128.0/20" extPoolId="1"/>
     </fabricSetupP>
     <fabricSetupP tepPool="10.1.0.0/16" podId="2" >
          <fabricExtSetupP tepPool="30.1.128.0/20" extPoolId="1"/>
     </fabricSetupP>
</fabricSetupPol>
```

ステップ 2 ノードのアイデンティティ ポリシーを定義するには、次の例のように XML で POST を送信します。

例：

```
<fabricNodeIdentPol>
     <fabricNodeIdentP serial="SAL17267Z7W" name="leaf1" nodeId="101" podId="1"
extPoolId="1" nodeType="remote-leaf-wan"/>
     <fabricNodeIdentP serial="SAL17267Z7X" name="leaf2" nodeId="102" podId="1"
extPoolId="1" nodeType="remote-leaf-wan"/>
     <fabricNodeIdentP serial="SAL17267Z7Y" name="leaf3" nodeId="201" podId="1"
extPoolId="1" nodeType="remote-leaf-wan"/>
     <fabricNodeIdentP serial="SAL17267Z7Z" name="leaf4" nodeId="201" podId="1"
extPoolId="1" nodeType="remote-leaf-wan"/>
</fabricNodeIdentPol>
```

ステップ 3 ファブリック外部接続プロファイルを設定するには、次の例のように XML で POST を送信します。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<imdata totalCount="1">
     <fvFabricExtConnP dn="uni/tn-infra/fabricExtConnP-1" id="1"
name="Fabric_Ext_Conn_Pol1" rt="extended:as2-nn4:5:16" siteId="0">
           <l3extFabricExtRoutingP name="test">
                <l3extSubnet ip="150.1.0.0/16" scope="import-security"/>
           </l3extFabricExtRoutingP>
          <l3extFabricExtRoutingP name="ext_routing_prof_1">
               <l3extSubnet ip="204.1.0.0/16" scope="import-security"/>
               <l3extSubnet ip="209.2.0.0/16" scope="import-security"/>
```

REST API を使用してタスクを実行する

```
                <l3extSubnet ip="202.1.0.0/16" scope="import-security"/>
                <l3extSubnet ip="207.1.0.0/16" scope="import-security"/>
                <l3extSubnet ip="200.0.0.0/8" scope="import-security"/>
                <l3extSubnet ip="201.2.0.0/16" scope="import-security"/>
                <l3extSubnet ip="210.2.0.0/16" scope="import-security"/>
                <l3extSubnet ip="209.1.0.0/16" scope="import-security"/>
                <l3extSubnet ip="203.2.0.0/16" scope="import-security"/>
                <l3extSubnet ip="208.1.0.0/16" scope="import-security"/>
                <l3extSubnet ip="207.2.0.0/16" scope="import-security"/>
                <l3extSubnet ip="100.0.0.0/8" scope="import-security"/>
                <l3extSubnet ip="201.1.0.0/16" scope="import-security"/>
                <l3extSubnet ip="210.1.0.0/16" scope="import-security"/>
                <l3extSubnet ip="203.1.0.0/16" scope="import-security"/>
                <l3extSubnet ip="208.2.0.0/16" scope="import-security"/>
            </l3extFabricExtRoutingP>
            <fvPodConnP id="1">
                  <fvIp addr="100.11.1.1/32"/>
            </fvPodConnP>
            <fvPodConnP id="2">
                  <fvIp addr="200.11.1.1/32"/>
            </fvPodConnP>
            <fvPeeringP type="automatic_with_full_mesh"/>
        </fvFabricExtConnP>
</imdata>
```

ステップ 4 VLAN 4 で L3Out を設定するには、リモート リーフ スイッチとスパイン スイッチ両方が WAN ルータに接続され、次の例のように XML を入力する必要があります。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<polUni>
<fvTenant name="infra">
  <l3extOut name="rleaf-wan-test">
    <ospfExtP areaId="0.0.0.5"/>
    <bgpExtP/>
    <l3extRsEctx tnFvCtxName="overlay-1"/>
    <l3extRsL3DomAtt tDn="uni/l3dom-l3extDom1"/>
    <l3extProvLbl descr="" name="prov_mp1" ownerKey="" ownerTag="" tag="yellow-green"/>
    <l3extLNodeP name="rleaf-101">
      <l3extRsNodeL3OutAtt rtrId="202.202.202.202" tDn="topology/pod-1/node-101">
      </l3extRsNodeL3OutAtt>
      <l3extLIfP name="portIf">
        <l3extRsPathL3OutAtt ifInstT="sub-interface"
tDn="topology/pod-1/paths-101/pathep-[eth1/49]" addr="202.1.1.2/30" mac="AA:11:22:33:44:66"
 encap='vlan-4'/>
        <ospfIfP>
          <ospfRsIfPol tnOspfIfPolName='ospfIfPol'/>
        </ospfIfP>
      </l3extLIfP>
    </l3extLNodeP>
    <l3extLNodeP name="rlSpine-201">
      <l3extRsNodeL3OutAtt rtrId="201.201.201.201" rtrIdLoopBack="no"
tDn="topology/pod-1/node-201">
        <!--
        <l3extLoopBackIfP addr="201::201/128" descr="" name=""/>
        <l3extLoopBackIfP addr="201.201.201.201/32" descr="" name=""/>
        -->
        <l3extLoopBackIfP addr="::" />
      </l3extRsNodeL3OutAtt>
      <l3extLIfP name="portIf">
        <l3extRsPathL3OutAtt ifInstT="sub-interface"
tDn="topology/pod-1/paths-201/pathep-[eth8/36]" addr="201.1.1.1/30" mac="00:11:22:33:77:55"
 encap='vlan-4'/>
```

REST API を使用してタスクを実行する

```
        <ospfIfP>
          <ospfRsIfPol tnOspfIfPolName='ospfIfPol'/>
        </ospfIfP>
      </l3extLIfP>
    </l3extLNodeP>
    <l3extInstP descr="" matchT="AtleastOne" name="instp1" prio="unspecified"
targetDscp="unspecified">
      <fvRsCustQosPol tnQosCustomPolName=""/>
    </l3extInstP>
  </l3extOut>
  <ospfIfPol name="ospfIfPol" nwT="bcast"/>
</fvTenant>
</polUni>
```

ステップ 5 リリース 4.1(2) 以前で、VLAN-5 でマルチポッド L3Out を設定するには、マルチポッドとリモート リーフ トポロジの両方と、次の例のように XML を送信する必要があります。

（注） リリース 4.1(2) 以降を実行している新しいリモート リーフ スイッチを導入し、それらのリモート リーフ スイッチで直接トラフィック転送をイネーブルにする場合は、この情報を入力しないでください。この場合、マルチポッドに VLAN-5 を使用して OSPF インスタンスを設定する必要はありません。

詳細については、ダイレクト トラフィック フォワーディングについて（170ページ）を参照してください。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<polUni>

  <fvTenant  name="infra" >
    <l3extOut name="ipn-multipodInternal">
      <ospfExtP areaCtrl="inherit-ipsec,redistribute,summary" areaId="0.0.0.5"
multipodInternal="yes" />
      <l3extRsEctx tnFvCtxName="overlay-1" />
      <l3extLNodeP name="bLeaf">
        <l3extRsNodeL3OutAtt rtrId="202.202.202.202" rtrIdLoopBack="no"
tDn="topology/pod-2/node-202">
           <l3extLoopBackIfP addr="202.202.202.212"/>
       </l3extRsNodeL3OutAtt>
        <l3extRsNodeL3OutAtt rtrId="102.102.102.102" rtrIdLoopBack="no"
tDn="topology/pod-1/node-102">
           <l3extLoopBackIfP addr="102.102.102.112"/>
       </l3extRsNodeL3OutAtt>
        <l3extLIfP name="portIf">
          <ospfIfP authKeyId="1" authType="none">
            <ospfRsIfPol tnOspfIfPolName="ospfIfPol" />
          </ospfIfP>
          <l3extRsPathL3OutAtt addr="10.0.254.233/30" encap="vlan-5"
ifInstT="sub-interface" tDn="topology/pod-2/paths-202/pathep-[eth5/2]"/>
          <l3extRsPathL3OutAtt addr="10.0.255.229/30" encap="vlan-5"
ifInstT="sub-interface" tDn="topology/pod-1/paths-102/pathep-[eth5/2]"/>
        </l3extLIfP>
      </l3extLNodeP>
      <l3extInstP matchT="AtleastOne" name="ipnInstP" />
    </l3extOut>
  </fvTenant>
</polUni>
```

REST API を使用した SR-MPLS ハンドオフの設定

REST API を使用した SR-MPLS インフラ L3Out の設定

- SR-MPLS インフラ L3Out は、境界リーフスイッチで設定され、SR-MPLS ハンドオフに必要なアンダーレイ BGP-LU およびオーバーレイ MP-BGP EVPN セッションを設定するために使用されます。
- SR-MPLS インフラ L3Out は、ポッドまたはリモート リーフ スイッチ サイトにスコープされます。
- 1 つの SR-MPLS インフラ L3Out 内の境界リーフ スイッチまたはリモート リーフ スイッチは、1 つ以上のルーティング ドメイン内の 1 つ以上のプロバイダー エッジ（PE）ルータに接続できます。
- ポッドまたはリモート リーフ スイッチ サイトには、1 つ以上の SR-MPLS インフラ L3Out を設定できます。
- 各 SR-MPLS インフラ L3Out には、一意のプロバイダー ラベルと 1 つのプロバイダー ラベルのみが必要です。各 SR-MPLS インフラ L3Out は、プロバイダー ラベルによって識別されます。

SR-MPLS インフラ L3Out を設定する場合は、次の項目を設定します。

- ノード
  - リーフ スイッチのみが SR-MPLS インフラ L3Out のノードとして設定できます（境界リーフ スイッチおよびリモート リーフ スイッチ）。
  - 各 SR-MPLS インフラ L3Out は、1 つのポッドからの境界リーフ スイッチまたは同じサイトからのリモート リーフ スイッチを持つことができます。
  - 各境界リーフ スイッチまたはリモート リーフ スイッチは、複数の SR-MPLS ドメインに接続する場合、複数の SR-MPLS インフラ L3Out で設定できます。
  - また、ノードの下にループバック インターフェイスを設定し、ループバック インターフェイスの下にノード SID ポリシーを設定します。
- インターフェイス
  - 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
    - ルーテッド ポートチャネルまたはポートチャネル サブインターフェイス

    サブインターフェイスでは、任意の VLAN タグがサポートされます。
  - また、SR-MPLS infra L3Out のインターフェイス エリアの下にアンダーレイ BGP ピア ポリシーを設定します。

REST API を使用してタスクを実行する

- **QoS ルール**
  - MPLS 入力ルールと MPLS 出力ルールは、SR-MPLS インフラ L3Out の MPLS QoS ポリシーを使用して設定できます。
  - MPLS QoS ポリシーを作成しない場合、入力 MPLS 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、SR-MPLS インフラ L3Out を使用してアンダーレイとオーバーレイを設定します。

- アンダーレイ：インターフェイス設定の一部としての BGP ピア IP（BGP LU ピア）設定。
- オーバーレイ：論理ノードプロファイル設定の一部としての MP-BGP EVPN リモート IPv4 アドレス（MP-BGP EVPN ピア）設定。

始める前に

- SR-MPLS のガイドラインおよび制限事項 （201 ページ） で提供されている SR-MPLS ガイドラインと制約事項を確認します。特に、SR-MPLS インフラ L3Out のガイドラインと制約事項 （202 ページ） で提供されているガイドラインと制約事項を確認してください。
- （任意）必要に応じて、の手順を使用して MPLS カスタム QoS ポリシーを設定します。REST API を使用した SR-MPLS カスタム QoS ポリシー （617 ページ）

手順

次のような情報が表示されます。

```
<polUni>
<fvTenant name="infra">
    <mplsIfPol name="default"/>
    <mplsLabelPol name="default" >
      <mplsSrgbLabelPol minSrgbLabel="16000" maxSrgbLabel="17000" localId="1" status=""/>

    </mplsLabelPol>

<l3extOut name="mplsOut" status="" descr="bl" mplsEnabled="yes">
    <l3extRsEctx tnFvCtxName="overlay-1"/>
    <l3extProvLbl name="mpls" />
    <mplsExtP status="" >
        <mplsRsLabelPol tDn="uni/tn-infra/mplslabelpol-default"/>
    </mplsExtP>
    <l3extLNodeP name="mplsLNP" status="">
        <l3extRsNodeL3OutAtt rtrId="100.1.1.1" rtrIdLoopBack="no"
tDn="topology/pod-1/node-101" status="">
            <l3extLoopBackIfP addr="10.10.10.11" status="">
                <mplsNodeSidP sidoffset="2" loopbackAddr="10.1.3.11" status=""/>
            </l3extLoopBackIfP>
        </l3extRsNodeL3OutAtt>

        <l3extLIfP name="mplsLIfP1" status="">
            <mplsIfP status="">
                <mplsRsIfPol tnMplsIfPolName="default" />
```

```
            </mplsIfP>
            <l3extRsPathL3OutAtt addr="34.1.2.3/30" ifInstT="l3-port"
tDn="topology/pod-1/paths-101/pathep-[eth1/8]">
                <bgpPeerP addr="9.9.9.7" addrTCtrl="af-ucast,af-label-ucast"
ctrl="send-ext-com" ttl="1" status="">
                    <bgpAsP asn="100"/>
                </bgpPeerP>
            </l3extRsPathL3OutAtt>
        </l3extLIfP>
        <bgpInfraPeerP addr="20.1.1.1" ctrl="send-com,send-ext-com" peerT="sr-mpls"
ttl="3" status="" >
            <bgpAsP asn="100"/>
        </bgpInfraPeerP>
    </l3extLNodeP>


    <l3extInstP name="mplsInstP">
        <l3extSubnet aggregate="" descr="" ip="11.11.11.0/24" name=""
scope="import-security"/>
    </l3extInstP>
    <bgpExtP/>
    <l3extRsL3DomAtt tDn="uni/l3dom-l3extDom1" />
</l3extOut>

</fvTenant>
</polUni>
```

REST API を使用した SR-MPLS VRF L3Out の設定

この項の手順を使用して、SR-MPLS VRF L3Out を設定します。これは、前の手順で設定した SR-MPLS インフラ L3Out からのトラフィックの転送に使用されます。

- ユーザ テナント VRF は SR-MPLS インフラ L3Out にマッピングされ、テナント ブリッジ ドメイン サブネットを DC-PE ルータにアドバタイズし、DC-PE から受信した MPLS VPN ルートをインポートします。
- 各 VRF の SR-MPLS VRF L3Out でルーティング ポリシーとセキュリティ ポリシーを指定する必要があります。これらのポリシーは、1 つ以上の SR-MPLS インフラ L3Out をポイントします。
- VRF ごとに 1 つの SR-MPLS VRF L3Out がサポートされます。
- 1 つの SR-MPLS VRF L3Out で複数のコンシューマ ラベルを設定でき、各コンシューマ ラベルで 1 つの SR-MPLS インフラ L3Out を識別できます。コンシューマ ラベルは、特定のポッドまたはリモート リーフ スイッチの特定の MPLS ドメインである 1 つの SR-MPLS VRF L3Out との間のトラフィックのエントリ ポイントと出口ポイントを識別します。

始める前に

- SR-MPLS のガイドラインおよび制限事項 （201 ページ） で提供されている SR-MPLS ガイドラインと制約事項を確認します。特に、SR-MPLS VRF L3Out のガイドラインと制約事項 （202 ページ） で提供されているガイドラインと制約事項を確認してください。

REST API を使用してタスクを実行する

- REST API を使用した SR-MPLS インフラ L3Out の設定 （613 ページ）の手順に従って、SR-MPLS インフラ L3Out を設定します。

手順

次のような情報が表示されます。

```
<polUni>
<fvTenant name="t1">
  <fvCtx name="v1">
    <!-- specify bgp evpn route-target -->
    <bgpRtTargetP af="ipv4-ucast">
      <bgpRtTarget rt="route-target:as4-nn2:100:1259" type="import"/>
      <bgpRtTarget rt="route-target:as4-nn2:100:1259" type="export"/>
    </bgpRtTargetP>
  </fvCtx>

  <!-- MPLS L3out -->
  <l3extOut name="out1" mplsEnabled="yes">
    <l3extRsEctx tnFvCtxName="v1" />

    <!-- MPLS consumer label -->
    <l3extConsLbl name="mpls1">
      <!-- route profile association -->
      <l3extRsLblToProfile tDn="uni/tn-t1/prof-rp1" direction="export" />
      <!-- InstP association -->
      <l3extRsLblToInstP tDn="uni/tn-t1/out-out1/instP-epgMpls1" />
    </l3extConsLbl>

    <!-- External-EPG -->
    <l3extInstP name="epgMpls1">
      <fvRsProv tnVzBrCPName="cp1"/>
      <l3extSubnet ip="55.1.1.1/28"/>
    </l3extInstP>
    <bgpExtP/>
  </l3extOut>

  <!-- route control profile -->
  <rtctrlProfile descr="" name="rp1" type="global" status="">
    <rtctrlCtxP action="permit" descr="" name="ctx1" order="0">
      <rtctrlRsCtxPToSubjP status="" tnRtctrlSubjPName="subj1"/>
    </rtctrlCtxP>
  </rtctrlProfile>
  <rtctrlSubjP descr="" name="subj1" status="" >
    <rtctrlMatchRtDest ip="101.1.1.1/32"/>
    <rtctrlMatchRtDest ip="102.1.1.0/24" aggregate="yes"/>
  </rtctrlSubjP>

  <!-- Filter and Contract (global) -->
  <vzBrCP name="cp1" scope="global">
    <vzSubj name="allow-all">
      <vzRsSubjFiltAtt action="permit" tnVzFilterName="default" />
    </vzSubj>
  </vzBrCP>
</fvTenant>
</polUni>
```

REST API を使用した SR-MPLS カスタム QoS ポリシー

SR MPLS カスタム QoS ポリシーは、MPLS QoS 出力 ポリシーで定義された着信 MPLS EXP 値に基づいて、SR-MPLS ネットワークから送信されるパケットのプライオリティを定義します。これらのパケットは、ACI ファブリック内にあります。また、MPLS QoS 出力ポリシーで定義された IPv4 DSCP 値に基づく MPLS インターフェイスを介して ACI ファブリックから離れるパケットの CoS 値および MPLS EXP 値をマーキングします。

カスタム出力ポリシーが定義されていない場合、デフォルトの Qos レベル（`Level3`）がファブリック内のパケットに割り当てられます。カスタム出力ポリシーが定義されていない場合、デフォルトの EXP 値（`0`）がファブリックから離れるパケットにマーキングされます。

手順

ステップ 1 SR-MPLS QoS ポリシーの作成

次のPOSTで、

- *customqos1*を、作成する SR-MPLS QoS ポリシーの名前に置き換えます。
- `qosMplsIngressRule`の場合：
  - from = "2" to = "3"を、ポリシーに一致させる EXP 範囲に置き換えます。
  - prio = "level5"を ACI ファブリック内にあるパケットの ACI QoS レベルに置き換えます。
  - target = "CS5" は、パケットが一致したときに設定する DSCP 値に置き換えます。
  - targetCos = "4" を、パケットが一致したときにパケットに設定する CoS 値に置き換えます。
- qosMplsEgressRule の場合：
  - from = "CS2" to = "CS4" を、ポリシーを照合する DSCP 範囲に置き換えます。
  - targetExp = "5" を、パケットがファブリックを離れるときに設定する EXP 値に置き換えます。
  - targetCos = "3" を、パケットがファブリックを離れるときに設定する CoS 値に置き換えます。

```
<polUni>
  <fvTenant name="infra">
    <qosMplsCustomPol descr="" dn="uni/tn-infra/qosmplscustom-customqos1" name="customqos1"
  status="" >
         <qosMplsIngressRule from="2" to="3" prio="level5" target="CS5" targetCos="4"
status="" />
         <qosMplsEgressRule from="CS2" to="CS4" targetExp="5" targetCos="3" status=""/>
    </qosMplsCustomPol>
  </fvTenant>
</polUni>
```

ステップ 2 SR-MPLS QoS ポリシーの作成

次の POST で、customqos1 を前の手順で作成した SR-MPLS QoS ポリシーの名前に置き換えます。

```
<polUni>
    <fvTenant name="infra">
        <l3extOut name="mplsOut" status="" descr="bl">
            <l3extLNodeP name="mplsLNP" status="">
              <l3extRsLNodePMplsCustQosPol  tDn="uni/tn-infra/qosmplscustom-customqos1"/>

            </l3extLNodeP>
        </l3extOut>
    </fvTenant>
</polUni>
```

パートII：外部ルーティング（L3Out）の設定

外部ネットワークへのルーテッド接続

REST API を使用した MP-BGP ルート リフレクタの設定

REST API を使用した MP-BGP ルート リフレクタの設定

手順

ステップ 1 スパイン スイッチをルート リフレクタとしてマークします。

例：

```
POST https://apic-ip-address/api/policymgr/mo/uni/fabric.xml

<bgpInstPol name="default">
  <bgpAsP asn="1" />
  <bgpRRP>
     <bgpRRNodePEp id="<spine_id1>”/>
     <bgpRRNodePEp id="<spine_id2>”/>
  </bgpRRP>
</bgpInstPol>
```

ステップ 2 次のポストを使用してポッド セレクタをセットアップします。

例：

FuncP セットアップの場合：

```
POST https://apic-ip-address/api/policymgr/mo/uni.xml

<fabricFuncP>
  <fabricPodPGrp name="bgpRRPodGrp”>
    <fabricRsPodPGrpBGPRRP tnBgpInstPolName="default" />
```

```
  </fabricPodPGrp>
</fabricFuncP>
```

例：

PodP セットアップの場合：

```
POST https://apic-ip-address/api/policymgr/mo/uni.xml

<fabricPodP name="default">
  <fabricPodS name="default" type="ALL">
    <fabricRsPodPGrp tDn="uni/fabric/funcprof/podpgrp-bgpRRPodGrp"/>
  </fabricPodS>
</fabricPodP>
```

REST API を使用したループ防止のための BGP ドメイン パス機能の設定

始める前に

ループ防止のための BGP ドメインパス機能について （237 ページ）に記載されている情報を使用して、BGP ドメイン パス機能に精通します。

手順

ステップ 1 ループ防止に BGP ドメイン パス機能を使用する場合は、グローバル `DomainIdBase` を設定します。

```
<polUni>
  <fabricInst>
   <bgpInstPol name="default">
    <bgpDomainIdBase  domainIdBase="12346" />
   </bgpInstPol>
  </fabricInst>
 </polUni>
```

ステップ 2 適切な L3Out で `send-domain-path` を有効にします。

```
<bgpPeerP addr="22.22.3.5" addrTCtrl="af-ucast" allowedSelfAsCnt="3" ttl="2"
 ctrlExt="send-domain-path" ctrl="send-ext-com">
</bgpPeerP>
```

L3Out のノードとインターフェイス

REST API を使用したレイヤ 3 ルーテッド ポート チャネルとサブインターフェイス ポート チャネルの設定

REST API を使用したレイヤ 3 ルーテッド ポート チャネルの設定

始める前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチが ACI ファブリックに登録され、使用可能であること。
- ポートチャネルは、L3Outインターフェイスにポートチャネルが使用される場合に設定されます。

（注） 次の REST API 例では、長い 1 行のテキストは \ で分けて読みやすくします。

手順

REST API を使用して以前作成したポート チャネルにレイヤ 3 ルートを設定するには、次のように XML で post を送信します。

例：

```
<polUni>
<fvTenant name=pep9>
    <l3extOut descr="" dn="uni/tn-pep9/out-routAccounting" enforceRtctrl="export" \
     name="routAccounting" nameAlias="" ownerKey="" ownerTag="" \
     targetDscp="unspecified">
        <l3extRsL3DomAtt tDn="uni/l3dom-Dom1"/>
        <l3extRsEctx tnFvCtxName="ctx9"/>
        <l3extLNodeP configIssues="" descr="" name="node101" nameAlias="" ownerKey="" \
         ownerTag="" tag="yellow-green" targetDscp="unspecified">
            <l3extRsNodeL3OutAtt rtrId="10.1.0.101" rtrIdLoopBack="yes" \
             tDn="topology/pod-1/node-101">
                <l3extInfraNodeP descr="" fabricExtCtrlPeering="no" \
                 fabricExtIntersiteCtrlPeering="no" name="" nameAlias="" spineRole=""/>
            </l3extRsNodeL3OutAtt>
            <l3extLIfP descr="" name="lifp17" nameAlias="" ownerKey="" ownerTag="" \
             tag="yellow-green">
                <ospfIfP authKeyId="1" authType="none" descr="" name="" nameAlias="">
                    <ospfRsIfPol tnOspfIfPolName=""/>
                </ospfIfP>
                <l3extRsPathL3OutAtt addr="10.1.5.3/24" autostate="disabled" descr="" \
                 encap="unknown" encapScope="local" ifInstT="l3-port" llAddr="::" \
```

```
                mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit" \
                tDn="topology/pod-1/paths-101/pathep-[po17_PolGrp]" \
                targetDscp="unspecified"/>
               <l3extRsNdIfPol tnNdIfPolName=""/>
               <l3extRsIngressQosDppPol tnQosDppPolName=""/>
               <l3extRsEgressQosDppPol tnQosDppPolName=""/>
           </l3extLIfP>
       </l3extLNodeP>
       <l3extInstP descr="" floodOnEncap="disabled" matchT="AtleastOne" \
        name="accountingInst" nameAlias="" prefGrMemb="exclude" prio="unspecified" \
        targetDscp="unspecified">
           <fvRsProv matchT="AtleastOne" prio="unspecified" tnVzBrCPName="webCtrct"/>
          <l3extSubnet aggregate="export-rtctrl,import-rtctrl" descr="" ip="0.0.0.0/0"
 \
            name="" nameAlias="" scope="export-rtctrl,import-rtctrl,import-security"/>
           <l3extSubnet aggregate="export-rtctrl,import-rtctrl" descr="" ip="::/0" \
            name="" nameAlias="" scope="export-rtctrl,import-rtctrl,import-security"/>
           <fvRsCustQosPol tnQosCustomPolName=""/>
       </l3extInstP>
       <l3extConsLbl descr="" name="golf" nameAlias="" owner="infra" ownerKey="" \
        ownerTag="" tag="yellow-green"/>
   </l3extOut>
</fvTenant>
</polUni>
```

REST API を使用して、レイヤ 3 サブインターフェイス ポート チャネルの設定

始める前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチが ACI ファブリックに登録され、使用可能であること。
- ポート チャネルは、「REST API を使用したポート チャネルの設定」の手順を使用して設定されます。

（注） 次の REST API 例では、1 つ以上の行のテキストはで区分するが、\ 読みやすさを改善する文字。

手順

REST API を使用して、以前に作成したポート チャネルをレイヤ 3 サブインターフェイス ルートを設定するには、次のようには、XML で post を送信します。

例：

```
<polUni>
<fvTenant name=pep9>
    <l3extOut descr="" dn="uni/tn-pep9/out-routAccounting" enforceRtctrl="export" \
     name="routAccounting" nameAlias="" ownerKey="" ownerTag="" targetDscp="unspecified">

        <l3extRsL3DomAtt tDn="uni/l3dom-Dom1"/>
        <l3extRsEctx tnFvCtxName="ctx9"/>
        <l3extLNodeP configIssues="" descr="" name="node101" nameAlias="" ownerKey="" \
         ownerTag="" tag="yellow-green" targetDscp="unspecified">
            <l3extRsNodeL3OutAtt rtrId="10.1.0.101" rtrIdLoopBack="yes" \
             tDn="topology/pod-1/node-101">
                <l3extInfraNodeP descr="" fabricExtCtrlPeering="no" \
                 fabricExtIntersiteCtrlPeering="no" name="" nameAlias="" spineRole=""/>
            </l3extRsNodeL3OutAtt>
            <l3extLIfP descr="" name="lifp27" nameAlias="" ownerKey="" ownerTag="" \
             tag="yellow-green">
                <ospfIfP authKeyId="1" authType="none" descr="" name="" nameAlias="">
                    <ospfRsIfPol tnOspfIfPolName=""/>
                </ospfIfP>
                <l3extRsPathL3OutAtt addr="11.1.5.3/24" autostate="disabled" descr="" \
                 encap="vlan-2001" encapScope="local" ifInstT="sub-interface" \
                 llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit" \
                 tDn="topology/pod-1/paths-101/pathep-[po27_PolGrp]" \
                 targetDscp="unspecified"/>
                <l3extRsNdIfPol tnNdIfPolName=""/>
                <l3extRsIngressQosDppPol tnQosDppPolName=""/>
                <l3extRsEgressQosDppPol tnQosDppPolName=""/>
            </l3extLIfP>
        </l3extLNodeP>
        <l3extInstP descr="" floodOnEncap="disabled" matchT="AtleastOne" \
         name="accountingInst" nameAlias="" prefGrMemb="exclude" prio="unspecified" \
         targetDscp="unspecified">
            <fvRsProv matchT="AtleastOne" prio="unspecified" tnVzBrCPName="webCtrct"/>
           <l3extSubnet aggregate="export-rtctrl,import-rtctrl" descr="" ip="0.0.0.0/0"
 \
             name="" nameAlias="" scope="export-rtctrl,import-rtctrl,import-security"/>
            <l3extSubnet aggregate="export-rtctrl,import-rtctrl" descr="" ip="::/0" \
             name="" nameAlias="" scope="export-rtctrl,import-rtctrl,import-security"/>
            <fvRsCustQosPol tnQosCustomPolName=""/>
        </l3extInstP>
        <l3extConsLbl descr="" name="golf" nameAlias="" owner="infra" ownerKey="" \
         ownerTag="" tag="yellow-green"/>
    </l3extOut>
</fvTenant>
</polUni>
```

REST API を使用したスイッチ仮想インターフェイスの設定

REST API を使用して、SVI インターフェイスのカプセル化スコープの設定

始める前に

インターフェイス セレクタが設定されます。

手順

SVI インターフェイスのカプセル化の範囲を設定します。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- /api/node/mo/.xml -->
<polUni>
 <fvTenant name="coke">
  <l3extOut descr="" dn="uni/tn-coke/out-l3out1" enforceRtctrl="export" name="l3out1"
nameAlias="" ownerKey="" ownerTag="" targetDscp="unspecified">
   <l3extRsL3DomAtt tDn="uni/l3dom-Dom1"/>
   <l3extRsEctx tnFvCtxName="vrf0"/>
   <l3extLNodeP configIssues="" descr="" name="__ui_node_101" nameAlias="" ownerKey=""
ownerTag="" tag="yellow-green" targetDscp="unspecified">
    <l3extRsNodeL3OutAtt rtrId="1.1.1.1" rtrIdLoopBack="no" tDn="topology/pod-1/node-101"/>

    <l3extLIfP descr="" name="int1_11" nameAlias="" ownerKey="" ownerTag=""
tag="yellow-green">
     <l3extRsPathL3OutAtt addr="1.2.3.4/24" descr="" encap="vlan-2001" encapScope="ctx"
 ifInstT="ext-svi" llAddr="0.0.0.0" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
 tDn="topology/pod-1/paths-101/pathep-[eth1/5]" targetDscp="unspecified"/>
     <l3extRsNdIfPol tnNdIfPolName=""/>
     <l3extRsIngressQosDppPol tnQosDppPolName=""/>
     <l3extRsEgressQosDppPol tnQosDppPolName=""/>
    </l3extLIfP>
   </l3extLNodeP>
  <l3extInstP descr="" matchT="AtleastOne" name="epg1" nameAlias="" prefGrMemb="exclude"
 prio="unspecified" targetDscp="unspecified">
    <l3extSubnet aggregate="" descr="" ip="101.10.10.1/24" name="" nameAlias=""
scope="import-security"/>
    <fvRsCustQosPol tnQosCustomPolName=""/>
   </l3extInstP>
  </l3extOut>
 </fvTenant>
</polUni>
```

REST API を使用した SVI 自動状態の設定

始める前に

- テナントと VRF が設定されています。
- レイヤ3アウトが設定されており、レイヤ3アウトの論理ノードプロファイルと論理インターフェイス プロファイルが設定されています。

手順

SVI の自動状態の値を有効にします。

例：

```
<fvTenant name="t1" >
   <l3extOut name="out1">
      <l3extLNodeP name="__ui_node_101" >
         <l3extLIfP descr="" name="__ui_eth1_10_vlan_99_af_ipv4" >
            <l3extRsPathL3OutAtt addr="19.1.1.1/24" autostate="enabled" descr=""
encap="vlan-100" encapScope="local" ifInstT="ext-svi" llAddr="::" mac="00:22:BD:F8:19:FF"
 mode="regular" mtu="inherit" tDn="topology/pod-1/paths-101/pathep-[eth1/10]"
targetDscp="unspecified" />
         </l3extLIfP>
      </l3extLNodeP>
   </l3extOut>
</fvTenant>
```

自動状態を無効にするには、上記の例では無効に値を変更する必要があります。例：
`autostate="disabled".`。

REST API を使用したルーティング プロトコルの設定

REST API を使用した BFD サポート付き BGP 外部ルーテッド ネットワークの設定

REST API を使用した BGP 外部ルーテッド ネットワークの設定

始める前に

外部ルーテッド ネットワークを設定するテナントがすでに作成されていること。

ここでは、REST API を使用して BGP 外部ルーテッド ネットワークを設定する方法を示します。

例：

手順

例：

```
<l3extOut descr="" dn="uni/tn-t1/out-l3out-bgp" enforceRtctrl="export" name="l3out-bgp"
 ownerKey="" ownerTag="" targetDscp="unspecified">
 <l3extRsEctx tnFvCtxName="ctx3"/>
 <l3extLNodeP configIssues="" descr="" name="l3extLNodeP_1" ownerKey="" ownerTag=""
tag="yellow-green" targetDscp="unspecified">
  <l3extRsNodeL3OutAtt rtrId="1.1.1.1" rtrIdLoopBack="no" tDn="topology/pod-1/node-101"/>

  <l3extLIfP descr="" name="l3extLIfP_2" ownerKey="" ownerTag="" tag="yellow-green">
   <l3extRsNdIfPol tnNdIfPolName=""/>
   <l3extRsIngressQosDppPol tnQosDppPolName=""/>
   <l3extRsEgressQosDppPol tnQosDppPolName=""/>
   <l3extRsPathL3OutAtt addr="3001::31:0:1:2/120" descr="" encap="vlan-3001"
encapScope="local" ifInstT="sub-interface" llAddr="::" mac="00:22:BD:F8:19:FF"
mode="regular" mtu="inherit" tDn="topology/pod-1/paths-101/pathep-[eth1/8]"
```

```
targetDscp="unspecified">
    <bgpPeerP addr="3001::31:0:1:0/120" allowedSelfAsCnt="3" ctrl="send-com,send-ext-com"
 descr="" name="" peerCtrl="bfd" privateASctrl="remove-all,remove-exclusive,replace-as"
 ttl="1" weight="1000">
     <bgpRsPeerPfxPol tnBgpPeerPfxPolName=""/>
     <bgpAsP asn="3001" descr="" name=""/>
    </bgpPeerP>
   </l3extRsPathL3OutAtt>
  </l3extLIfP>
  <l3extLIfP descr="" name="l3extLIfP_1" ownerKey="" ownerTag="" tag="yellow-green">
   <l3extRsNdIfPol tnNdIfPolName=""/>
   <l3extRsIngressQosDppPol tnQosDppPolName=""/>
   <l3extRsEgressQosDppPol tnQosDppPolName=""/>
  <l3extRsPathL3OutAtt addr="31.0.1.2/24" descr="" encap="vlan-3001" encapScope="local"
 ifInstT="sub-interface" llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
 tDn="topology/pod-1/paths-101/pathep-[eth1/8]" targetDscp="unspecified">
    <bgpPeerP addr="31.0.1.0/24" allowedSelfAsCnt="3" ctrl="send-com,send-ext-com"
descr="" name="" peerCtrl="" privateASctrl="remove-all,remove-exclusive,replace-as"
ttl="1" weight="100">
     <bgpRsPeerPfxPol tnBgpPeerPfxPolName=""/>
     <bgpLocalAsnP asnPropagate="none" descr="" localAsn="200" name=""/>
     <bgpAsP asn="3001" descr="" name=""/>
    </bgpPeerP>
   </l3extRsPathL3OutAtt>
  </l3extLIfP>
 </l3extLNodeP>
 <l3extRsL3DomAtt tDn="uni/l3dom-l3-dom"/>
 <l3extRsDampeningPol af="ipv6-ucast" tnRtctrlProfileName="damp_rp"/>
 <l3extRsDampeningPol af="ipv4-ucast" tnRtctrlProfileName="damp_rp"/>
 <l3extInstP descr="" matchT="AtleastOne" name="l3extInstP_1" prio="unspecified"
targetDscp="unspecified">
  <l3extSubnet aggregate="" descr="" ip="130.130.130.0/24" name=""
scope="import-rtctrl"></l3extSubnet>
  <l3extSubnet aggregate="" descr="" ip="130.130.131.0/24" name="" scope="import-rtctrl"/>

  <l3extSubnet aggregate="" descr="" ip="120.120.120.120/32" name=""
scope="export-rtctrl,import-security"/>
  <l3extSubnet aggregate="" descr="" ip="3001::130:130:130:100/120" name=""
scope="import-rtctrl"/>
 </l3extInstP>
 <bgpExtP descr=""/>
</l3extOut>
<rtctrlProfile descr="" dn="uni/tn-t1/prof-damp_rp" name="damp_rp" ownerKey="" ownerTag=""
 type="combinable">
 <rtctrlCtxP descr="" name="ipv4_rpc" order="0">
  <rtctrlScope descr="" name="">
   <rtctrlRsScopeToAttrP tnRtctrlAttrPName="act_rule"/>
  </rtctrlScope>
 </rtctrlCtxP>
</rtctrlProfile>
<rtctrlAttrP descr="" dn="uni/tn-t1/attr-act_rule" name="act_rule">
 <rtctrlSetDamp descr="" halfLife="15" maxSuppressTime="60" name="" reuse="750"
suppress="2000" type="dampening-pol"/>
</rtctrlAttrP>
```

REST API を使用した BGP パスの設定

次のフィールドの許容値については、Cisco APIC ドキュメンテーション ページの 『Verified Scalability Guide for Cisco APIC』を参照してください。https://www.cisco.com/c/en/us/support/

cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

さらに多くのパスを設定できるようにする 2 つのプロパティは、bgpCtxAfPol オブジェクトの maxEcmp と maxEcmpIbgp です。これら 2 つのプロパティを設定した後、実装の残り部分に反映されます。ECMP ポリシーは VRF レベルで適用されます。

次の例では、REST API を使用して BGP 最長パス機能を設定する方法の情報を提供します。

```
<fvTenant descr="" dn="uni/tn-t1" name="t1">
    <fvCtx name="v1">
        <fvRsCtxToBgpCtxAfPol af="ipv4-ucast" tnBgpCtxAfPolName="bgpCtxPol1"/>
    </fvCtx>
    <bgpCtxAfPol name="bgpCtxPol1" maxEcmp="64" maxEcmpIbgp="64"/>
</fvTenant>
```

REST API を使用した AS パス プリペンドの設定

次の例では、REST API を使用した AS パス プリペンド機能を設定する方法の情報を提供します。

```
<?xml version="1.0" encoding="UTF-8"?>
<fvTenant name="coke">
    <rtctrlAttrP name="attrp1">
        <rtctrlSetASPath criteria="prepend">
            <rtctrlSetASPathASN asn="100" order="1"/>
            <rtctrlSetASPathASN asn="200" order="10"/>
            <rtctrlSetASPathASN asn="300" order="5"/>
        <rtctrlSetASPath/>
        <rtctrlSetASPath criteria="prepend-last-as" lastnum=”9" />
    </rtctrlAttrP>

    <l3extOut name="out1">
        <rtctrlProfile name="rp1">
            <rtctrlCtxP name="ctxp1" order="1">
                <rtctrlScope>
                    <rtctrlRsScopeToAttrP tnRtctrlAttrPName="attrp1"/>
                </rtctrlScope>
            </rtctrlCtxP>
        </rtctrlProfile>
    </l3extOut>
</fvTenant>
```

REST API を使用した自律システム オーバーライド対応のネットワークのルーティング BGP 外部の設定

手順

自律型オーバーライドを有効にして、BGP 外部ルーテッド ネットワークを設定します。

（注） 太字で表示されているコードの行に設定の BGP AS オーバーライド部分が表示されます。この機能は Cisco APIC リリース 3.1(2m) で導入されました。

例：

REST API を使用してタスクを実行する

```
<fvTenant name="coke">

   <fvCtx name="coke" status="">
       <bgpRtTargetP af="ipv4-ucast">
           <bgpRtTarget type="import" rt="route-target:as4-nn2:1234:1300" />
           <bgpRtTarget type="export" rt="route-target:as4-nn2:1234:1300" />
       </bgpRtTargetP>
       <bgpRtTargetP af="ipv6-ucast">
           <bgpRtTarget type="import" rt="route-target:as4-nn2:1234:1300" />
           <bgpRtTarget type="export" rt="route-target:as4-nn2:1234:1300" />
       </bgpRtTargetP>
   </fvCtx>

   <fvBD name="cokeBD">
       <!-- Association from Bridge Doamin to Private Network -->
       <fvRsCtx tnFvCtxName="coke" />
       <fvRsBDToOut tnL3extOutName="routAccounting" />
       <!-- Subnet behind the bridge domain-->
       <fvSubnet ip="20.1.1.1/16" scope="public"/>
       <fvSubnet ip="2000:1::1/64" scope="public"/>
   </fvBD>
   <fvBD name="cokeBD2">
       <!-- Association from Bridge Doamin to Private Network -->
       <fvRsCtx tnFvCtxName="coke" />
       <fvRsBDToOut tnL3extOutName="routAccounting" />
       <!-- Subnet behind the bridge domain-->
       <fvSubnet ip="30.1.1.1/16" scope="public"/>

   </fvBD>
   <vzBrCP name="webCtrct" scope="global">
       <vzSubj name="http">
           <vzRsSubjFiltAtt tnVzFilterName="default"/>
       </vzSubj>
   </vzBrCP>

   <!-- GOLF L3Out -->
   <l3extOut name="routAccounting">
      <l3extConsLbl name="golf_transit" owner="infra" status=""/>
      <bgpExtP/>
      <l3extInstP name="accountingInst">
          <!--
          <l3extSubnet ip="192.2.2.0/24" scope="import-security,import-rtctrl" />
          <l3extSubnet ip="192.3.2.0/24" scope="export-rtctrl"/>
          <l3extSubnet ip="192.5.2.0/24" scope="export-rtctrl"/>
          <l3extSubnet ip="64:ff9b::c007:200/120" scope="export-rtctrl" />
          -->
          <l3extSubnet ip="0.0.0.0/0"
                               scope="export-rtctrl,import-security"
                               aggregate="export-rtctrl"

          />
          <fvRsProv tnVzBrCPName="webCtrct"/>
      </l3extInstP>

      <l3extRsEctx tnFvCtxName="coke"/>
   </l3extOut>

    <fvAp name="cokeAp">
      <fvAEPg name="cokeEPg" >
          <fvRsBd tnFvBDName="cokeBD" />
           <fvRsPathAtt tDn="topology/pod-1/paths-103/pathep-[eth1/20]" encap="vlan-100"
 instrImedcy="immediate" mode="regular"/>
```

REST API を使用してタスクを実行する

```
            <fvRsCons tnVzBrCPName="webCtrct"/>
        </fvAEPg>
        <fvAEPg name="cokeEPg2" >
            <fvRsBd tnFvBDName="cokeBD2" />
            <fvRsPathAtt tDn="topology/pod-1/paths-103/pathep-[eth1/20]" encap="vlan-110"
 instrImedcy="immediate" mode="regular"/>
            <fvRsCons tnVzBrCPName="webCtrct"/>
        </fvAEPg>
     </fvAp>

     <!-- Non GOLF L3Out-->
     <l3extOut name="NonGolfOut">
        <bgpExtP/>
        <l3extLNodeP name="bLeaf">
            <!--
            <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="20.1.13.1"/>
            -->
            <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="20.1.13.1">
            <l3extLoopBackIfP addr="1.1.1.1"/>

            <ipRouteP ip="2.2.2.2/32"  >
              <ipNexthopP nhAddr="20.1.12.3"/>
        </ipRouteP>


         </l3extRsNodeL3OutAtt>
            <l3extLIfP name='portIfV4'>
                <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/17]"
encap='vlan-1010' ifInstT='sub-interface' addr="20.1.12.2/24">

                </l3extRsPathL3OutAtt>
            </l3extLIfP>
            <l3extLIfP name='portIfV6'>
                <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/17]"
encap='vlan-1010' ifInstT='sub-interface' addr="64:ff9b::1401:302/120">
                    <bgpPeerP addr="64:ff9b::1401:d03" ctrl="send-com,send-ext-com" />
                </l3extRsPathL3OutAtt>
            </l3extLIfP>
            <bgpPeerP addr="2.2.2.2" ctrl="as-override,disable-peer-as-check,
send-com,send-ext-com" status=""/>
        </l3extLNodeP>
        <!--
         <bgpPeerP addr="2.2.2.2" ctrl="send-com,send-ext-com" status=""/>
         -->
        <l3extInstP name="accountingInst">
            <l3extSubnet ip="192.10.0.0/16" scope="import-security,import-rtctrl" />
            <l3extSubnet ip="192.3.3.0/24" scope="import-security,import-rtctrl" />
            <l3extSubnet ip="192.4.2.0/24" scope="import-security,import-rtctrl" />
           <l3extSubnet ip="64:ff9b::c007:200/120" scope="import-security,import-rtctrl"
 />
            <l3extSubnet ip="192.2.2.0/24" scope="export-rtctrl" />
            <l3extSubnet ip="0.0.0.0/0"
                                scope="export-rtctrl,import-rtctrl,import-security"
                                aggregate="export-rtctrl,import-rtctrl"

          />
        </l3extInstP>
       <l3extRsEctx tnFvCtxName="coke"/>
    </l3extOut>

</fvTenant>
```

REST API を使用した BGP ネイバー シャットダウンおよびソフト リセットの設定

REST API を使用した *BGP* ネイバー シャットダウンの設定

次の手順では、REST API を使用して BGP ネイバー シャットダウン機能を使用する方法について説明します。

手順

ステップ 1 ノードおよびインターフェイスを設定します。

この例では、ノード プロファイル、`nodep1`、ルータ ID `11.11.11.103` を持つノード 103（境界リーフ スイッチ）上で、VRF `v1` を設定します。. また、IP アドレス `12.12.12.1/24` およびレイヤ 3 ドメイン `dom1` で、ルーテッド インターフェイス（レイヤ 3 ポート）としてインターフェイス `eth1/3` を設定します。

例：

```
<l3extOut name="l3out1">
    <l3extRsEctx tnFvCtxName="v1"/>
    <l3extLNodeP name="nodep1">
        <l3extRsNodeL3OutAtt rtrId="11.11.11.103" tDn="topology/pod-1/node-103"/>
        <l3extLIfP name="ifp1"/>
         <l3extRsPathL3OutAtt addr="12.12.12.3/24" ifInstT="l3-port"
tDn="topology/pod-1/paths-103/pathep-[eth1/3]"/>
        </l3extLIfP>
    </l3extLNodeP>
    <l3extRsL3DomAtt tDn="uni/l3dom-dom1"/>
</l3extOut>
```

ステップ 2 BGP ルーティング プロトコルを設定し、BGP ネイバー シャットダウン機能を設定します。

この例では、IP アドレス、`15.15.15.2`、ASN 100 を持つ BGP ピアで、プライマリ ルーティング プロトコルとして BGP を設定します。

adminSt 変数は、次のいずれかに設定できます。

- enabled：BGP ネイバー シャットダウン機能をイネーブルにします。
- disabled：BGP ネイバー シャットダウン機能を無効にします。

次の例では、BGP ネイバー シャットダウン機能がイネーブルになっています。

例：

```
<l3extOut name="l3out1">
    <l3extLNodeP name="nodep1">
        <bgpPeerP addr="15.15.15.2"> adminSt="enabled"
            <bgpAsP asn="100"/>
        </bgpPeerP>
    </l3extLNodeP>
```

```
    <bgpExtP/>
</l3extOut>
```

REST API を使用した *BGP* ネイバー ソフト リセットの設定

次の手順では、REST API を使用して BGP ネイバー ソフト リセット機能を使用する方法について説明します。

手順

ステップ 1 ノードおよびインターフェイスを設定します。

この例では、ノード プロファイル、`nodep1`、ルータ ID `11.11.11.103` を持つノード 103（境界リーフ スイッチ）上で、VRF `v1` を設定します。. また、IP アドレス `12.12.12.1/24` およびレイヤ 3 ドメイン `dom1` で、ルーテッド インターフェイス（レイヤ 3 ポート）としてインターフェイス `eth1/3` を設定します。

例：

```
<l3extOut name="l3out1">
    <l3extRsEctx tnFvCtxName="v1"/>
    <l3extLNodeP name="nodep1">
        <l3extRsNodeL3OutAtt rtrId="11.11.11.103" tDn="topology/pod-1/node-103"/>
        <l3extLIfP name="ifp1"/>
         <l3extRsPathL3OutAtt addr="12.12.12.3/24" ifInstT="l3-port"
tDn="topology/pod-1/paths-103/pathep-[eth1/3]"/>
        </l3extLIfP>
    </l3extLNodeP>
    <l3extRsL3DomAtt tDn="uni/l3dom-dom1"/>
</l3extOut>
```

ステップ 2 BGP ルーティング プロトコルを設定し、BGP ネイバー ソフト リセット機能を設定します。

この例では、IP アドレス、`15.15.15.2`、ASN 100 を持つ BGP ピアで、プライマリ ルーティング プロトコルとして BGP を設定します。

dir 変数は、次のいずれかに設定できます。

- in：ソフト ダイナミック インバウンド リセットを有効にします。
- out：ソフト アウトバウンド リセットを有効にします。

次の例では、ソフト ダイナミック インバウンド リセットが有効になっています。

例：

```
<l3extOut name="l3out1">
    <l3extLNodeP name="nodep1">
        <bgpPeerP addr="15.15.15.2">
            <bgpAsP asn="100"/>
            <bgpPeerEntryClearPeerLTask>
                <attributes>
                    <mode>soft</mode>
                    <dir>in</dir>
```

```
                    <adminSt>start</adminSt>
                </attributes>
                <children/>
            </bgpPeerEntryClearPeerLTask>
        </bgpPeerP>
    </l3extLNodeP>
    <bgpExtP/>
</l3extOut>
```

REST API を使用した VRF ごと、ノード BGP ごとのタイマーの設定

次の例では、ノード内の VRF ごと、ノード BGP ごとのタイマーの設定方法を示します。`bgpProtP` (`l3extLNodeP` の下) を設定します。`bgpProtP` の下で、目的とする関係 (`bgpRsBgpNodeCtxPol`) を設定します。これは、BGP コンテキスト ポリシー (`bgpCtxPol`) に対するものです。

手順

`node1` でノード固有の BGP タイマー ポリシーを設定し、`node2` を、ノード固有ではない BGP タイマー ポリシーで設定します。

例：

```
POST https://apic-ip-address/mo.xml

<fvTenant name="tn1" >
    <bgpCtxPol name="pol1" staleIntvl="25" />
    <bgpCtxPol name="pol2" staleIntvl="35" />
    <fvCtx name="ctx1" >
      <fvRsBgpCtxPol tnBgpCtxPolName="pol1"/>
    </fvCtx>
     <l3extout name="out1" >
      <l3extRsEctx toFvCtxName="ctx1" />
      <l3extLNodeP name="node1" >
        <bgpProtP name="protp1" >
            <bgpRsBgpNodeCtxPol tnBgpCtxPolName="pol2" />
        </bgpProtP>
      </l3extLNodeP>
      <l3extLNodeP name="node2" >
      </l3extLNodeP>
```

この例では、`node1` は BGP タイマー値をポリシー `pol2` から取得し、`node2` は BGP タイマー値を `pol1` から取得します。タイマー値は `bgpDom` に適用されますが、これは VRF `tn1:ctx1` に対応しています。これは、「*VRF* ごと、ノード *BGP* ごとのタイマーの値」のセクションで説明したアルゴリズムに従って選択された、BGP タイマー ポリシーに基づきます。

削除するノード BGP タイマーが REST API を使用してごとの VRF あたり

次の例では、ノード内で既存の VRF ごとの各ノード BGP タイマーを削除する方法を示します。

手順

node1 で特定の BGP タイマー ポリシーのノードを削除します。

例：

```
POST https://apic-ip-address/mo.xml

<fvTenant name="tn1" >
    <bgpCtxPol name="pol1" staleIntvl="25" />
    <bgpCtxPol name="pol2" staleIntvl="35" />
    <fvCtx name="ctx1" >
      <fvRsBgpCtxPol tnBgpCtxPolName="pol1"/>
    </fvCtx>
     <l3extout name="out1" >
      <l3extRsEctx toFvCtxName="ctx1" />
      <l3extLNodeP name="node1" >
        <bgpProtP name="protp1" status="deleted" >
            <bgpRsBgpNodeCtxPol tnBgpCtxPolName="pol2" />
        </bgpProtP>
      </l3extLNodeP>
      <l3extLNodeP name="node2" >
      </l3extLNodeP>
```

上の例のコード フレーズ <bgpProtP name="protp1" status="deleted" > は、BGP タイマー ポリシーを削除します。削除後、node1 が node1 が関連付けられている VRF の BGP タイマー ポリシーのデフォルト設定になります。上の例では pol1 です。

REST API を使用したセカンダリ IP アドレスでの双方向フォワーディング検出の構成

次の例では、REST API を使用して、セカンダリ IP アドレスに Bidirectional Forwarding Detection（BFD）を構成します。

```
<l3extLIfP
  dn="uni/tn-sec-ip-bfd/out-secip-bfd-l3out/lnodep-secip-bfd-l3out_nodeProfile/
  lifp-secip-bfd-l3out_interfaceProfile" name="secip-bfd-l3out_interfaceProfile"
  prio="unspecified" tag="yellow-green" userdom=":all:">
    <l3extRsPathL3OutAtt addr="50.50.50.200/24" autostate="disabled"
      encap="vlan-2" encapScope="local" ifInstT="ext-svi" ipv6Dad="enabled"
      isMultiPodDirect="no" llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular"
      mtu="inherit" tDn="topology/pod-1/paths-101/pathep-[eth1/3]"
      targetDscp="unspecified" userdom=":all:">
        <l3extIp addr="9.9.9.1/24" ipv6Dad="enabled" userdom=":all:"/>
        <l3extIp addr="6.6.6.1/24" ipv6Dad="enabled" userdom=":all:"/>
    </l3extRsPathL3OutAtt>
    <l3extRsNdIfPol userdom="all"/>
    <l3extRsLIfPCustQosPol userdom="all"/>
    <l3extRsIngressQosDppPol userdom="all"/>
    <l3extRsEgressQosDppPol userdom="all"/>
    <l3extRsArpIfPol userdom="all"/>
</l3extLIfP>
<ipRouteP aggregate="no"
  dn="uni/tn-sec-ip-bfd/out-secip-bfd-l3out/lnodep-secip-bfd-l3out_nodeProfile/
  rsnodeL3OutAtt-[topology/pod-1/node-101]/rt-[6.0.0.1/24]"
  fromPfxLen="0" ip="6.0.0.1/24" pref="1" rtCtrl="bfd" toPfxLen="0" userdom=":all:">
```

```
    <ipNexthopP nhAddr="6.6.6.2" pref="unspecified" type="prefix" userdom=":all:"/>
</ipRouteP>
```

グローバル REST API を使用して BFD の設定

手順

次の REST API は、(BFD) を双方向フォワーディング検出のグローバル コンフィギュレーションを示します。

例：

```
<polUni>
 <infraInfra>
   <bfdIpv4InstPol name="default" echoSrcAddr="1.2.3.4" slowIntvl="1000" minTxIntvl="150"
 minRxIntvl="250" detectMult="5" echoRxIntvl="200"/>
   <bfdIpv6InstPol name="default" echoSrcAddr="34::1/64" slowIntvl="1000" minTxIntvl="150"
 minRxIntvl="250" detectMult="5" echoRxIntvl="200"/>
 </infraInfra>
</polUni>
```

REST API を使用した BFD インターフェイスのオーバーライドの設定

手順

次の REST API は、(BFD) を双方向フォワーディング検出のインターフェイスのオーバーライド コンフィギュレーションを示します。

例：

```
<fvTenant name="ExampleCorp">
  <bfdIfPol name="bfdIfPol" minTxIntvl="400" minRxIntvl="400" detectMult="5"
echoRxIntvl="400" echoAdminSt="disabled"/>
    <l3extOut name="l3-out">
        <l3extLNodeP name="leaf1">
            <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="2.2.2.2"/>

            <l3extLIfP name='portIpv4'>
                <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/11]"
ifInstT='l3-port' addr="10.0.0.1/24" mtu="1500"/>
                <bfdIfP type="sha1" key="password">
                    <bfdRsIfPol tnBfdIfPolName='bfdIfPol'/>
                </bfdIfP>
            </l3extLIfP>


        </l3extLNodeP>
    </l3extOut>
</fvTenant>
```

REST API を使用した BFD コンシューマ プロトコルの設定

手順

ステップ 1 次の例では、双方向の転送検出（BFD）のインターフェイス設定を示します。

例：

```
<fvTenant name="ExampleCorp">
  <bfdIfPol name="bfdIfPol" minTxIntvl="400" minRxIntvl="400" detectMult="5"
echoRxIntvl="400" echoAdminSt="disabled"/>
    <l3extOut name="l3-out">
        <l3extLNodeP name="leaf1">
            <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="2.2.2.2"/>

            <l3extLIfP name='portIpv4'>
                <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/11]"
ifInstT='l3-port' addr="10.0.0.1/24" mtu="1500"/>
                <bfdIfP type="sha1" key="password">
                    <bfdRsIfPol tnBfdIfPolName='bfdIfPol'/>
                </bfdIfP>
            </l3extLIfP>


        </l3extLNodeP>
    </l3extOut>
</fvTenant>
```

ステップ 2 次の例では、OSPF および EIGRP で BFD を有効にするためのインターフェイス設定を示します。

例：

リーフ スイッチ上の BFD

```
<fvTenant name="ExampleCorp">
      <ospfIfPol  name="ospf_intf_pol" cost="10" ctrl="bfd"/>
      <eigrpIfPol ctrl="nh-self,split-horizon,bfd"
dn="uni/tn-Coke/eigrpIfPol-eigrp_if_default"
</fvTenant>
```

例：

スパイン スイッチ上の BFD

```
<l3extLNodeP name="bSpine">

             <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-103" rtrId="192.3.1.8">
                 <l3extLoopBackIfP addr="10.10.3.1" />
                 <l3extInfraNodeP fabricExtCtrlPeering="false" />
             </l3extRsNodeL3OutAtt>

             <l3extLIfP name='portIf'>
                 <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-103/pathep-[eth5/10]"
encap='vlan-4' ifInstT='sub-interface' addr="20.3.10.1/24"/>
                 <ospfIfP>
                     <ospfRsIfPol tnOspfIfPolName='ospf_intf_pol'/>
                 </ospfIfP>
                 <bfdIfP name="test" type="sha1" key="hello" status="created,modified">
```

REST API を使用してタスクを実行する

```
                    <bfdRsIfPol tnBfdIfPolName='default' status="created,modified"/>
                </bfdIfP>
            </l3extLIfP>

        </l3extLNodeP>
```

ステップ 3 次の例では、BGP 上の BFD を有効にするためのインターフェイス設定を示します。

例：

```
<fvTenant name="ExampleCorp">
    <l3extOut name="l3-out">
        <l3extLNodeP name="leaf1">
            <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="2.2.2.2"/>

            <l3extLIfP name='portIpv4'>
                <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/11]"
ifInstT='l3-port' addr="10.0.0.1/24" mtu="1500">
                  <bgpPeerP addr="4.4.4.4/24" allowedSelfAsCnt="3" ctrl="bfd" descr=""
name="" peerCtrl="" ttl="1">
                    <bgpRsPeerPfxPol tnBgpPeerPfxPolName=""/>
                    <bgpAsP asn="3" descr="" name=""/>
                  </bgpPeerP>
                </l3extRsPathL3OutAtt>
            </l3extLIfP>


        </l3extLNodeP>
    </l3extOut>
</fvTenant>
```

ステップ 4 次の例では、スタティック ルートで BFD を有効にするためのインターフェイス設定を示します。

例：

リーフ スイッチ上の BFD

```
<fvTenant name="ExampleCorp">
    <l3extOut name="l3-out">
        <l3extLNodeP name="leaf1">
            <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="2.2.2.2">
              <ipRouteP ip="192.168.3.4" rtCtrl="bfd">
                <ipNexthopP nhAddr="192.168.62.2"/>
              </ipRouteP>
            </l3extRsNodeL3OutAtt>
            <l3extLIfP name='portIpv4'>
                <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/3]"
ifInstT='l3-port' addr="10.10.10.2/24" mtu="1500" status="created,modified" />

            </l3extLIfP>

        </l3extLNodeP>

    </l3extOut>
</fvTenant>
```

例：

スパイン スイッチ上の BFD

```
<l3extLNodeP name="bSpine">
```

REST API を使用してタスクを実行する

```
            <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-103" rtrId="192.3.1.8">
             <ipRouteP ip="0.0.0.0" rtCtrl="bfd">
               <ipNexthopP nhAddr="192.168.62.2"/>
             </ipRouteP>
            </l3extRsNodeL3OutAtt>

            <l3extLIfP name='portIf'>
                <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-103/pathep-[eth5/10]"
encap='vlan-4' ifInstT='sub-interface' addr="20.3.10.1/24"/>

                <bfdIfP name="test" type="sha1" key="hello" status="created,modified">
                   <bfdRsIfPol tnBfdIfPolName='default' status="created,modified"/>
                </bfdIfP>
            </l3extLIfP>

        </l3extLNodeP>
```

ステップ 5 次の例では、IS-IS で BFD を有効にするためのインターフェイス設定を示します。

例：

```
<fabricInst>
          <l3IfPol name="testL3IfPol" bfdIsis="enabled"/>
              <fabricLeafP name="LeNode" >
  <fabricRsLePortP tDn="uni/fabric/leportp-leaf_profile" />
 <fabricLeafS name="spsw" type="range">
 <fabricNodeBlk name="node101" to_="102" from_="101" />
 </fabricLeafS>
           </fabricLeafP>

          <fabricSpineP name="SpNode" >
 <fabricRsSpPortP tDn="uni/fabric/spportp-spine_profile" />
 <fabricSpineS name="spsw" type="range">
    <fabricNodeBlk name="node103" to_="103" from_="103" />
 </fabricSpineS>
        </fabricSpineP>

         <fabricLePortP name="leaf_profile">
 <fabricLFPortS name="leafIf" type="range">
<fabricPortBlk name="spBlk" fromCard="1" fromPort="49" toCard="1" toPort="49" />
       <fabricRsLePortPGrp tDn="uni/fabric/funcprof/leportgrp-LeTestPGrp" />
 </fabricLFPortS>
        </fabricLePortP>

      <fabricSpPortP name="spine_profile">
 <fabricSFPortS name="spineIf" type="range">
     <fabricPortBlk name="spBlk" fromCard="5" fromPort="1" toCard="5" toPort="2" />
     <fabricRsSpPortPGrp tDn="uni/fabric/funcprof/spportgrp-SpTestPGrp" />
 </fabricSFPortS>
    </fabricSpPortP>

 <fabricFuncP>
               <fabricLePortPGrp name = "LeTestPGrp">
 <fabricRsL3IfPol tnL3IfPolName="testL3IfPol"/>
              </fabricLePortPGrp>

           <fabricSpPortPGrp name = "SpTestPGrp">
 <fabricRsL3IfPol tnL3IfPolName="testL3IfPol"/>
          </fabricSpPortPGrp>

</fabricFuncP>
```

```
</fabricInst>
```

REST API を使用した OSPF 外部ルーテッド ネットワークの設定

REST API を使用した管理テナントの OSPF 外部ルーテッド ネットワークの作成

- ルータ ID と論理インターフェイス プロファイルの IP アドレスが異なっていて重複していないことを確認します。
- 次の手順は、管理テナントの OSPF 外部ルーテッド ネットワークを作成するためのものです。テナントの OSPF 外部ルーテッド ネットワークを作成するには、テナントを選択し、テナント用の VRF を作成する必要があります。
- 詳細については、『*Cisco APIC and Transit Routing*』を参照してください。

手順

管理テナントの OSPF 外部ルーテッド ネットワークを作成します。

例：

```
POST: https://apic-ip-address/api/mo/uni/tn-mgmt.xml

<fvTenant name="mgmt">
   <fvBD name="bd1">
      <fvRsBDToOut tnL3extOutName="RtdOut" />
      <fvSubnet ip="1.1.1.1/16" />
      <fvSubnet ip="1.2.1.1/16" />
      <fvSubnet ip="40.1.1.1/24" scope="public" />
      <fvRsCtx tnFvCtxName="inb" />
   </fvBD>
   <fvCtx name="inb" />

   <l3extOut name="RtdOut">
      <l3extRsL3DomAtt tDn="uni/l3dom-extdom"/>
      <l3extInstP name="extMgmt">
      </l3extInstP>
      <l3extLNodeP name="borderLeaf">
         <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="10.10.10.10"/>

         <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-102" rtrId="10.10.10.11"/>

         <l3extLIfP name='portProfile'>
           <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/40]"
ifInstT='l3-port' addr="192.168.62.1/24"/>
           <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-102/pathep-[eth1/40]"
ifInstT='l3-port' addr="192.168.62.5/24"/>
            <ospfIfP/>
                                 </l3extLIfP>
      </l3extLNodeP>
      <l3extRsEctx tnFvCtxName="inb"/>
      <ospfExtP areaId="57" />
```

```
   </l3extOut>
</fvTenant>
```

REST API を使用した EIGRP 外部ルーテッド ネットワークの設定

REST API を使用した EIGRP の設定

手順

ステップ 1 EIGRP コンテキスト ポリシーを設定します。

例：

```
<polUni>
    <fvTenant name="cisco_6">
        <eigrpCtxAfPol actIntvl="3" descr=""
dn="uni/tn-cisco_6/eigrpCtxAfP-eigrp_default_pol" extDist="170"
          intDist="90" maxPaths="8" metricStyle="narrow" name="eigrp_default_pol"
ownerKey="" ownerTag=""/>
    </fvTenant>
</polUni>
```

ステップ 2 EIGRP インターフェイス ポリシーを設定します。

例：

```
<polUni>
    <fvTenant name="cisco_6">
        <eigrpIfPol bw="10" ctrl="nh-self,split-horizon" delay="10"
delayUnit="tens-of-micro" descr="" dn="uni/tn-cisco_6/eigrpIfPol-eigrp_if_default"
         helloIntvl="5" holdIntvl="15" name="eigrp_if_default" ownerKey="" ownerTag=""/>

    </fvTenant>
</polUni>
```

ステップ 3 EIGRP VRF.を設定します。

例：

IPv4：

```
<polUni>
    <fvTenant name="cisco_6">
        <fvCtx name="dev">
          <fvRsCtxToEigrpCtxAfPol tnEigrpCtxAfPolName="eigrp_ctx_pol_v4" af="1"/>
        </fvCtx>
    </fvTenant>
</polUni>
```

IPv6

```
<polUni>
    <fvTenant name="cisco_6">
        <fvCtx name="dev">
         <fvRsCtxToEigrpCtxAfPol tnEigrpCtxAfPolName="eigrp_ctx_pol_v6" af="ipv6-ucast"/>

        </fvCtx>
```

REST API を使用してタスクを実行する

```
    </fvTenant>
</polUni>
```

ステップ 4 外部の EIGRP Layer3 を設定します。

例：

IPv4

```
<polUni>
    <fvTenant name="cisco_6">
        <l3extOut name="ext">
            <eigrpExtP asn="4001"/>
            <l3extLNodeP name="node1">
                <l3extLIfP name="intf_v4">
                    <l3extRsPathL3OutAtt addr="201.1.1.1/24" ifInstT="l3-port"
                      tDn="topology/pod-1/paths-101/pathep-[eth1/4]"/>
                    <eigrpIfP name="eigrp_ifp_v4">
                        <eigrpRsIfPol tnEigrpIfPolName="eigrp_if_pol_v4"/>
                    </eigrpIfP>
                </l3extLIfP>
            </l3extLNodeP>
        </l3extOut>
    </fvTenant>
</polUni>
```

IPv6

```
<polUni>
    <fvTenant name="cisco_6">
        <l3extOut name="ext">
            <eigrpExtP asn="4001"/>
            <l3extLNodeP name="node1">
                <l3extLIfP name="intf_v6">
                    <l3extRsPathL3OutAtt addr="2001::1/64" ifInstT="l3-port"
                      tDn="topology/pod-1/paths-101/pathep-[eth1/4]"/>
                    <eigrpIfP name="eigrp_ifp_v6">
                        <eigrpRsIfPol tnEigrpIfPolName="eigrp_if_pol_v6"/>
                    </eigrpIfP>
                </l3extLIfP>
            </l3extLNodeP>
        </l3extOut>
    </fvTenant>
</polUni>
```

IPv4 および IPv6

```
<polUni>
    <fvTenant name="cisco_6">
        <l3extOut name="ext">
            <eigrpExtP asn="4001"/>
            <l3extLNodeP name="node1">
                <l3extLIfP name="intf_v4">
                    <l3extRsPathL3OutAtt addr="201.1.1.1/24" ifInstT="l3-port"
                      tDn="topology/pod-1/paths-101/pathep-[eth1/4]"/>
                    <eigrpIfP name="eigrp_ifp_v4">
                        <eigrpRsIfPol tnEigrpIfPolName="eigrp_if_pol_v4"/>
                    </eigrpIfP>
                </l3extLIfP>

                <l3extLIfP name="intf_v6">
                    <l3extRsPathL3OutAtt addr="2001::1/64" ifInstT="l3-port"
                      tDn="topology/pod-1/paths-101/pathep-[eth1/4]"/>
                    <eigrpIfP name="eigrp_ifp_v6">
                        <eigrpRsIfPol tnEigrpIfPolName="eigrp_if_pol_v6"/>
```

```
                    </eigrpIfP>
                </l3extLIfP>
            </l3extLNodeP>
        </l3extOut>
    </fvTenant>
</polUni>
```

ステップ 5 （任意） インターフェイス ポリシー ノブを設定します。

例：

```
<polUni>
    <fvTenant name="cisco_6">
        <eigrpIfPol bw="1000000" ctrl="nh-self,split-horizon" delay="10"
          delayUnit="tens-of-micro" helloIntvl="5" holdIntvl="15" name="default"/>
    </fvTenant>
</polUni>
```

`Bandwidth（bw）属性は`（bw）属性は kbps で定義されています。`DelayUnit` 属性は、「1 万マイクロ」または「ピコ」です。

REST API を使用したルート集約の設定

BGP、OSPF、および REST API を使用して EIGRP のルート集約の設定

手順

ステップ 1 次のように、REST API を使用して BGP ルート集約を設定します。

例：

```
<fvTenant name="common">
           <fvCtx name="vrf1"/>
   <bgpRtSummPol name="bgp_rt_summ" cntrl='as-set'/>
   <l3extOut name="l3_ext_pol" >
             <l3extLNodeP name="bLeaf">
                <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="20.10.1.1"/>
              <l3extLIfP name='portIf'>
              <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/31]"
ifInstT='l3-port' addr="10.20.1.3/24/>
               </l3extLIfP>
             </l3extLNodeP>
         <bgpExtP />
           <l3extInstP name="InstP" >
         <l3extSubnet ip="10.0.0.0/8" scope="export-rtctrl">
           <l3extRsSubnetToRtSumm tDn="uni/tn-common/bgprtsum-bgp_rt_summ"/>
           <l3extRsSubnetToProfile tnRtctrlProfileName="rtprof"/>
         </l3extSubnet>
       </l3extInstP>
       <l3extRsEctx tnFvCtxName="vrf1"/>
   </l3extOut>
</fvTenant>
```

ステップ 2 次の REST API を使用して、OSPF のエリア間および外部の集約を設定します。

例：

```
<?xml version="1.0" encoding="utf-8"?>
<fvTenant name="t20">
  <!--Ospf Inter External route summarization Policy-->
  <ospfRtSummPol cost="unspecified" interAreaEnabled="no" name="ospfext"/>
  <!--Ospf Inter Area route summarization Policy-->
  <ospfRtSummPol cost="16777215" interAreaEnabled="yes" name="interArea"/>
  <fvCtx name="ctx0" pcEnfDir="ingress" pcEnfPref="enforced"/>
  <!-- L3OUT backbone Area-->
  <l3extOut enforceRtctrl="export" name="l3_1" ownerKey="" ownerTag=""
targetDscp="unspecified">
    <l3extRsEctx tnFvCtxName="ctx0"/>
    <l3extLNodeP name="node-101">
      <l3extRsNodeL3OutAtt rtrId="20.1.3.2" rtrIdLoopBack="no"
tDn="topology/pod-1/node-101"/>
      <l3extLIfP name="intf-1">
       <l3extRsPathL3OutAtt addr="20.1.5.2/24" encap="vlan-1001" ifInstT="sub-interface"
 tDn="topology/pod-1/paths-101/pathep-[eth1/33]"/>
      </l3extLIfP>
    </l3extLNodeP>
    <l3extInstP name="l3InstP1">
      <fvRsProv tnVzBrCPName="default"/>
      <!--Ospf External Area route summarization-->
      <l3extSubnet aggregate="" ip="193.0.0.0/8" name="" scope="export-rtctrl">
        <l3extRsSubnetToRtSumm tDn="uni/tn-t20/ospfrtsumm-ospfext"/>
      </l3extSubnet>
    </l3extInstP>
    <ospfExtP areaCost="1" areaCtrl="redistribute,summary" areaId="backbone"
areaType="regular"/>
  </l3extOut>
  <!-- L3OUT Regular Area-->
  <l3extOut enforceRtctrl="export" name="l3_2">
    <l3extRsEctx tnFvCtxName="ctx0"/>
    <l3extLNodeP name="node-101">
      <l3extRsNodeL3OutAtt rtrId="20.1.3.2" rtrIdLoopBack="no"
tDn="topology/pod-1/node-101"/>
      <l3extLIfP name="intf-2">
       <l3extRsPathL3OutAtt addr="20.1.2.2/24" encap="vlan-1014" ifInstT="sub-interface"
 tDn="topology/pod-1/paths-101/pathep-[eth1/11]"/>
      </l3extLIfP>
    </l3extLNodeP>
    <l3extInstP matchT="AtleastOne" name="l3InstP2">
      <fvRsCons tnVzBrCPName="default"/>
      <!--Ospf Inter Area route summarization-->
      <l3extSubnet aggregate="" ip="197.0.0.0/8" name="" scope="export-rtctrl">
        <l3extRsSubnetToRtSumm tDn="uni/tn-t20/ospfrtsumm-interArea"/>
      </l3extSubnet>
    </l3extInstP>
    <ospfExtP areaCost="1" areaCtrl="redistribute,summary" areaId="0.0.0.57"
areaType="regular"/>
  </l3extOut>
</fvTenant>
```

ステップ 3 次の REST API を使用して EIGRP の集約を設定します。

例：

```
<fvTenant name="exampleCorp">
  <l3extOut name="out1">
```

```
    <l3extInstP  name="eigrpSummInstp" >
      <l3extSubnet aggregate="" descr="" ip="197.0.0.0/8" name="" scope="export-rtctrl">

         <l3extRsSubnetToRtSumm/>
       </l3extSubnet>
    </l3extInstP>
  </l3extOut>
  <eigrpRtSummPol name="pol1" />
```

（注） EIGRP を設定するルート集約ポリシーはありません。EIGRP の集約を有効にするために必要なだけの設定では、サマリー サブネット、InstP でです。

REST API を使用したルート マップおよびルート プロファイルによるルート制御の設定

REST API を使用した BGP ピアごとのルート制御の設定

次の手順では、REST API を使用して BGP ピア単位のルート制御を設定する方法について説明します。

手順

BGP ピアごとのルート制御機能を設定します。

ここで、

- **direction="import"** は、ルート インポート ポリシー（ファブリックに許可されるルート）です。
- **direction="export"** は、ルート エクスポート ポリシー（外部ネットワークからアドバタイズされるルート）です。

例：

```
<polUni>
   <fvTenant name="t1">
       <fvCtx name="v1"/>
       <l3extOut name="l3out1">
           <l3extRsEctx tnFvCtxName="v1"/>
           <l3extLNodeP name="nodep1">
              <l3extRsNodeL3OutAtt rtrId="11.11.11.103" tDn="topology/pod-1/node-103"/>

               <l3extLIfP name="ifp1">
                   <l3extRsPathL3OutAtt addr="12.12.12.3/24" ifInstT="l3-port"
tDn="topology/pod-1/paths-103/pathep-[eth1/3]"/>
               </l3extLIfP>
               <bgpPeerP addr="15.15.15.2">
                   <bgpAsP asn="100"/>
                   <bgpRsPeerToProfile direction="export" tnRtctrlProfileName="rp1"/>
               </bgpPeerP>
```

```
            </l3extLNodeP>
            <l3extRsL3DomAtt tDn="uni/l3dom-dom1"/>
            <bgpExtP/>
            <ospfExtP areaId="0.0.0.0" areaType="regular"/>
            <l3extInstP name="extnw1" >
                <l3extSubnet ip="20.20.20.0/24" scope="import-security"/>
            </l3extInstP>
        </l3extOut>
        <rtctrlProfile name="rp1">
            <rtctrlCtxP name="ctxp1" action="permit" order="0">
                <rtctrlScope>
                    <rtctrlRsScopeToAttrP tnRtctrlAttrPName="attrp1"/>
                </rtctrlScope>
                <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule1"/>
            </rtctrlCtxP>
        </rtctrlProfile>
        <rtctrlSubjP name="match-rule1">
            <rtctrlMatchRtDest ip="200.3.2.0/24"/>
        </rtctrlSubjP>
        <rtctrlAttrP name="attrp1">
            <rtctrlSetASPath criteria="prepend">
                <rtctrlSetASPathASN asn="100" order="2"/>
                <rtctrlSetASPathASN asn="200" order="1"/>
            </rtctrlSetASPath>
        </rtctrlAttrP>
</fvTenant>
</polUni>
```

REST API を使用して、明示的なプレフィックス リストでルート マップ/プロファイルの設定

始める前に

- テナントと VRF を設定する必要があります。

手順

明示的なプレフィックス リストを使用してルート マップ/プロファイルを設定します。

（注） 以下の**太字**のエントリは、APIC リリース 4.2(3) 以降で使用可能な一致プレフィックスの拡張機能です。これらのフィールドの詳細については、一致プレフィックスの機能拡張 （385 ページ）を参照してください。

例：

```
<?xml version="1.0" encoding="UTF-8"?>
<fvTenant name="PM" status="">
   <rtctrlAttrP name="set_dest">
      <rtctrlSetComm community="regular:as2-nn2:5:24" />
   </rtctrlAttrP>
   <rtctrlSubjP name="allow_dest">
     <rtctrlMatchRtDest ip="192.169.0.0/24" aggregate="yes" fromPfxLen="26" toPfxLen="30"
 />
      <rtctrlMatchCommTerm name="term1">
```

```
            <rtctrlMatchCommFactor community="regular:as2-nn2:5:24" status="" />
            <rtctrlMatchCommFactor community="regular:as2-nn2:5:25" status="" />
         </rtctrlMatchCommTerm>
         <rtctrlMatchCommRegexTerm commType="regular" regex="200:*" status="" />
      </rtctrlSubjP>
      <rtctrlSubjP name="deny_dest">
         <rtctrlMatchRtDest ip="192.168.0.0/24" />
      </rtctrlSubjP>
      <fvCtx name="ctx" />
      <l3extOut name="L3Out_1" enforceRtctrl="import,export" status="">
         <l3extRsEctx tnFvCtxName="ctx" />
         <l3extLNodeP name="bLeaf">
            <l3extRsNodeL3OutAtt tDn="topology/pod-1/node-101" rtrId="1.2.3.4" />
            <l3extLIfP name="portIf">
               <l3extRsPathL3OutAtt tDn="topology/pod-1/paths-101/pathep-[eth1/25]"
ifInstT="sub-interface" encap="vlan-1503" addr="10.11.12.11/24" />
               <ospfIfP />
            </l3extLIfP>
            <bgpPeerP addr="5.16.57.18/32" ctrl="send-com" />
            <bgpPeerP addr="6.16.57.18/32" ctrl="send-com" />
         </l3extLNodeP>
         <bgpExtP />
         <ospfExtP areaId="0.0.0.59" areaType="nssa" status="" />
         <l3extInstP name="l3extInstP_1" status="">
            <l3extSubnet ip="17.11.1.11/24" scope="import-security" />
         </l3extInstP>
         <rtctrlProfile name="default-export" type="global" status="">
            <rtctrlCtxP name="ctx_deny" action="deny" order="1">
               <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="deny_dest" status="" />
            </rtctrlCtxP>
            <rtctrlCtxP name="ctx_allow" order="2">
               <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="allow_dest" status="" />
            </rtctrlCtxP>
            <rtctrlScope name="scope" status="">
               <rtctrlRsScopeToAttrP tnRtctrlAttrPName="set_dest" status="" />
            </rtctrlScope>
         </rtctrlProfile>
      </l3extOut>
      <fvBD name="testBD">
         <fvRsBDToOut tnL3extOutName="L3Out_1" />
         <fvRsCtx tnFvCtxName="ctx" />
         <fvSubnet ip="40.1.1.12/24" scope="public" />
         <fvSubnet ip="40.1.1.2/24" scope="private" />
         <fvSubnet ip="2003::4/64" scope="public" />
      </fvBD>
   </fvTenant>
```

REST API を使用した、インポート制御とエクスポート制御によるルーティング制御プロトコルの設定

この例では、ネットワーク接続 BGP を使用して外部レイヤ 3 が設定されていることを前提としています。OSPF を使用してネットワークを次のタスクを実行することもできます。

始める前に

- テナント、プライベート ネットワーク、およびブリッジドメインが作成されていること。
- レイヤ 3 Outside テナント ネットワークが設定されていること。

手順

インポート制御とエクスポート制御を使用するルート制御プロトコルを設定します。

例：

```
<l3extOut descr="" dn="uni/tn-Ten_ND/out-L3Out1" enforceRtctrl="export" name="L3Out1"
ownerKey="" ownerTag="" targetDscp="unspecified">
        <l3extLNodeP descr="" name="LNodeP1" ownerKey="" ownerTag="" tag="yellow-green"
 targetDscp="unspecified">
            <l3extRsNodeL3OutAtt rtrId="1.2.3.4" rtrIdLoopBack="yes"
tDn="topology/pod-1/node-101">
                <l3extLoopBackIfP addr="2000::3" descr="" name=""/>
            </l3extRsNodeL3OutAtt>
            <l3extLIfP descr="" name="IFP1" ownerKey="" ownerTag="" tag="yellow-green">
                <ospfIfP authKeyId="1" authType="none" descr="" name="">
                    <ospfRsIfPol tnOspfIfPolName=""/>
                </ospfIfP>
                <l3extRsNdIfPol tnNdIfPolName=""/>
                <l3extRsPathL3OutAtt addr="10.11.12.10/24" descr="" encap="unknown"
ifInstT="l3-port"
llAddr="::" mac="00:22:BD:F8:19:FF" mtu="1500"
tDn="topology/pod-1/paths-101/pathep-[eth1/17]" targetDscp="unspecified"/>
            </l3extLIfP>
        </l3extLNodeP>
        <l3extRsEctx tnFvCtxName="PVN1"/>
        <l3extInstP descr="" matchT="AtleastOne" name="InstP1" prio="unspecified"
targetDscp="unspecified">
            <fvRsCustQosPol tnQosCustomPolName=""/>
            <l3extSubnet aggregate="" descr="" ip="192.168.1.0/24" name="" scope=""/>
        </l3extInstP>
        <ospfExtP areaCost="1" areaCtrl="redistribute,summary" areaId="0.0.0.1"
areaType="nssa" descr=""/>
        <rtctrlProfile descr="" name="default-export" ownerKey="" ownerTag="">
            <rtctrlCtxP descr="" name="routecontrolpvtnw" order="3">
                <rtctrlScope descr="" name="">
                    <rtctrlRsScopeToAttrP tnRtctrlAttrPName="actionruleprofile2"/>
                </rtctrlScope>
            </rtctrlCtxP>
        </rtctrlProfile>
    </l3extOut>
```

REST API を使用したインターリーク再配布の設定

次の手順では、REST API を使用してインターリーク再配布を設定する方法について説明します。

始める前に

テナント、VRF、および L3Out を作成します。

REST API を使用してタスクを実行する

手順

ステップ 1 インターリーク再配布のルートマップを設定します。

例：

次の例では、2つのコンテキスト（ROUTES_A および ROUTES_ALL）を使用してルート マップ INTERLEAK_RP を設定します。最初のコンテキスト ROUTES_A は、IP プレフィックス リスト 10.0.0.0/24 le 32 と一致し、set rule COM_A を介してコミュニティ属性を設定します。2 番目のコンテキストは、すべてのルートと一致します。

```
POST: https://<APIC IP>/api/mo/uni.xml
BODY:
<fvTenant dn="uni/tn-SAMPLE">
    <!-- route map with two contexts (ROUTES_A and ROUTES_ALL)-->
    <rtctrlProfile type="global" name="INTERLEAK_RP">
        <rtctrlCtxP name="ROUTES_A" order="0" action="permit">
            <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="PFX_10-0-0-0_24"/>
            <rtctrlScope>
                <rtctrlRsScopeToAttrP tnRtctrlAttrPName="COM_A"/>
            </rtctrlScope>
        </rtctrlCtxP>
        <rtctrlCtxP name="ROUTES_ALL" order="9" action="permit">
            <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="ALL_PREFIX"/>
        </rtctrlCtxP>
    </rtctrlProfile>

    <!-- match rule with an IP prefix-list -->
    <rtctrlSubjP name="ALL_PREFIX">
        <rtctrlMatchRtDest ip="0.0.0.0/0" aggregate="yes"/>
    </rtctrlSubjP>

    <!-- match rule with an IP prefix-list -->
    <rtctrlSubjP name="PFX_10-0-0-0_24">
        <rtctrlMatchRtDest ip="10.0.0.0/24" aggregate="yes"/>
    </rtctrlSubjP>

    <!-- setu rule for community attribute -->
    <rtctrlAttrP name="COM_A">
        <rtctrlSetComm type="community" setCriteria="append"
community="regular:as2-nn2:100:200"/>
    </rtctrlAttrP>
</fvTenant>
```

ステップ 2 設定されたルートマップを L3Out に適用します。

次の例では、ステップ 1 のルート マップを L3Out `l3out1` に適用して、特定の L3Out からのルートのインターリーク再配布をカスタマイズします。

`L3extRsInterleakPol` は、特定の L3Out によって使用されるダイナミック ルーティング プロトコル（OSPF/EIGRP）ルートに適用されます。`L3extRsRedistributePol` は、`src` 属性（`static`）で指定されたスタティック ルートに適用されます。

例：

```
POST: https://<APIC IP>/api/mo/uni.xml
BODY:
<fvTenant dn="uni/tn-SAMPLE">
```

```
    <l3extOut name="l3out1">
        <!-- interleak redistribution for OSPF/EIGRP routes -->
        <l3extRsInterleakPol tnRtctrlProfileName="INTERLEAK_RP"/>
        <!-- interleak redistribution for static routes -->
        <l3extRsRedistributePol tnRtctrlProfileName="INTERLEAK_RP" src="static"/>
    </l3extOut>
</fvTenant>
```

REST API を使用したトランジット ルーティングの設定

REST API を使用したトランジット ルーティングの設定

次の手順では、テナントのトランジットルーティングを設定する方法を説明します。この例では、別のルータにそれぞれ接続された 2 つの境界リーフ スイッチで、1 つの VRF 内に 2 つの L3Out を展開します。

始める前に

- ノード、ポート、AEP、機能プロファイル、レイヤ 3 ドメインを設定します。
- 外部ルーテッド ドメインを作成し、L3Out のインターフェイスに関連付けます。
- ファブリック内でルートを伝播させるために、BGP ルート リフレクタ ポリシーを設定します。

手順

ステップ 1 テナントおよび VRF を設定します。

この例ではテナント `t1` および VRF `v1` を設定します。VRF はまだ展開されていません。

例：

```
<fvTenant  name="t1">
    <fvCtx name="v1"/>
</fvTenant>
```

ステップ 2 ノードおよびインターフェイスを設定します。

この例では、2 つの境界リーフ スイッチで、テナント t1 と VRF v1 に 2 つの L3Outs を設定します。VRF は、レイヤ 3 ドメイン `dom1` です。

- 最初の L3Out はノード 101 上にあり、`nodep1` という名前です。ノード 101 はルータ ID `11.11.11.103` で設定されます。ルーテッドインターフェイス `ifp1` が `eth1/3` にあり、IP アドレス `12.12.12.3/24` です。
- 2 番目の L3Out が ノード 102 上にあり、`nodep2` という名前です。ノード 102 はルータ ID `22.22.22.203` に設定されています。IP アドレス、`23.23.23.1/24` を持つ `eth1/3` でルーテッド インターフェイス `ifp2` があります。

REST API を使用してタスクを実行する

例：

```
<l3extOut name="l3out1">
    <l3extRsEctx tnFvCtxName="v1"/>
    <l3extLNodeP name="nodep1">
        <l3extRsNodeL3OutAtt rtrId="11.11.11.103" tDn="topology/pod-1/node-101"/>
        <l3extLIfP name="ifp1"/>
        <l3extRsPathL3OutAtt addr="12.12.12.3/24" ifInstT="l3-port"
tDn="topology/pod-1/paths-101/pathep-[eth1/3]"/>
        </l3extLIfP>
    </l3extLNodeP>
    <l3extRsL3DomAtt tDn="uni/l3dom-dom1"/>
</l3extOut>

<l3extOut name="l3out2">
    <l3extRsEctx tnFvCtxName="v1"/>
    <l3extLNodeP name="nodep2">
        <l3extRsNodeL3OutAtt rtrId="22.22.22.203" tDn="topology/pod-1/node-102"/>
        <l3extLIfP name="ifp2"/>
        <l3extRsPathL3OutAtt addr="23.23.23.3/24" ifInstT="l3-port"
tDn="topology/pod-1/paths-102/pathep-[eth1/3]"/>
        </l3extLIfP>
    </l3extLNodeP>
    <l3extRsL3DomAtt tDn="uni/l3dom-dom1"/>
</l3extOut>
```

ステップ 3 両方の境界リーフ スイッチのルーティング プロトコルを設定します。

この例では、両方の境界リーフ スイッチに対して、ASN 100 でプライマリ ルーティング プロトコルとしてBGPを設定します。BGPピア `15.15.15.2` を持つノード101とBGPピア `25.25.25.2` を持つノード102を設定します。

例：

```
<l3extOut name="l3out1">
    <l3extLNodeP name="nodep1">
        <bgpPeerP addr="15.15.15.2/24"
            <bgpAsP asn="100"/>
        </bgpPeerP>
    </l3extLNodeP>
</l3extOut>

<l3extOut name="l3out2">
    <l3extLNodeP name="nodep2">
        <bgpPeerP addr="25.25.25.2/24"
            <bgpAsP asn="100"/>
        </bgpPeerP>
    </l3extLNodeP>
</l3extOut>
```

ステップ 4 接続ルーティング プロトコルを設定します。

この例では、定期的なエリアID `0.0.0.0` で両方のL3Outsに対して通信プロトコルとしてOSPFを設定します。

例：

```
<l3extOut name="l3out1">
    <ospfExtP areaId="0.0.0.0" areaType="regular"/>
    <l3extLNodeP name="nodep1">
        <l3extLIfP name="ifp1">
            <ospfIfP/>
        <l3extIfP>
    <l3extLNodeP>
```

REST API を使用してタスクを実行する

```
</l3extOut>
<l3extOut name="l3out2">
    <ospfExtP areaId="0.0.0.0" areaType="regular"/>
    <l3extLNodeP name="nodep2">
        <l3extLIfP name="ifp2">
            <ospfIfP/>
        <l3extIfP>
    <l3extLNodeP>
</l3extOut>
```

ステップ 5 外部 EPG を設定します。

この例では、ノード 101 上の外部ネットワーク `extnw1` としてネットワーク `192.168.1.0/24` と、ノード 102 上の外部ネットワーク `extnw2` として `192.168.2.0/24` を設定します。また、ルート制御プロファイル `rp1` および `rp2`.と外部 EPG を関連付けます。

例：

```
<l3extOut name="l3out1">
     <l3extInstP name="extnw1">
          <l3extSubnet ip="192.168.1.0/24" scope="import-security"/>
          <l3extRsInstPToProfile direction="export" tnRtctrlProfileName="rp1"/>
    </l3extInstP>
</l3extOut>
<l3extOut name="l3out2">
     <l3extInstP name="extnw2">
          <l3extSubnet ip="192.168.2.0/24" scope="import-security"/>
          <l3extRsInstPToProfile direction="export" tnRtctrlProfileName="rp2"/>
    </l3extInstP>
</l3extOut>
```

ステップ 6 オプション。ルート マップを設定します。

この例では、インバウンドおよびアウトバウンド方向で各 BGP ピアのルート マップを設定します。`L3out1` では、ルート マップ `rp1` が `192.168.1.0/24` のインポート宛先に一致するルートに適用され、ルート マップ `rp2` が `192.168.2.0/24` のエクスポート宛先に一致するルートに適用されます。`L3out2` では、ルート マップの方向を反転します。

例：

```
<fvTenant name="t1">
    <rtctrlSubjP name="match-rule1">
        <rtctrlMatchRtDest ip="192.168.1.0/24" />
    </rtctrlSubjP>
    <rtctrlSubjP name="match-rule2">
        <rtctrlMatchRtDest ip="192.168.2.0/24" />
    </rtctrlSubjP>
    <l3extOut name="l3out1">
        <rtctrlProfile name="rp1">
            <rtctrlCtxP name="ctxp1" action="permit" order="0">
                <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule1" />
            </rtctrlCtxP>
        </rtctrlProfile>
        <rtctrlProfile name="rp2">
            <rtctrlCtxP name="ctxp1" action="permit" order="0">
                <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule2" />
            </rtctrlCtxP>
        </rtctrlProfile>
        <l3extInstP name="extnw1">
            <l3extRsInstPToProfile direction="import" tnRtctrlProfileName="rp1" />
            <l3extRsInstPToProfile direction="export" tnRtctrlProfileName="rp2" />
```

```
        </l3extInstP>
    </l3extOut>
    <l3extOut name="l3out2">
        <rtctrlProfile name="rp1">
            <rtctrlCtxP name="ctxp1" action="permit" order="0">
                <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule1" />
            </rtctrlCtxP>
        </rtctrlProfile>
        <rtctrlProfile name="rp2">
            <rtctrlCtxP name="ctxp1" action="permit" order="0">
                <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule2" />
            </rtctrlCtxP>
        </rtctrlProfile>
        <l3extInstP name="extnw2">
            <l3extRsInstPToProfile direction="import" tnRtctrlProfileName="rp2" />
            <l3extRsInstPToProfile direction="export" tnRtctrlProfileName="rp1" />
        </l3extInstP>
    </l3extOut>
</fvTenant>
```

ステップ 7 フィルタおよびコントラクトを作成し、EPG が通信できるようにします。

この例では、フィルタ `http-filter` とコントラクト `httpCtrct` を設定します。外部 EPG およびアプリケーション EPG は、それぞれプロバイダおよびコンシューマとして、すでにコントラクト `httpCtrct` と関連付けられています。

例：

```
<vzFilter name="http-filter">
    <vzEntry  name="http-e" etherT="ip" prot="tcp"/>
</vzFilter>
<vzBrCP name="httpCtrct" scope="context">
    <vzSubj name="subj1">
        <vzRsSubjFiltAtt tnVzFilterName="http-filter"/>
    </vzSubj>
</vzBrCP>
```

ステップ 8 コントラクトと外部 EPG を関連付けます。

この例では、外部 EPG `extnw1` をプロバイダとして、外部 EPG `extnw2` をコントラクト `httpCtrct` のコンシューマとして関連付けます。

```
 <l3extOut name="l3out1">
    <l3extInstP name="extnw1">
        <fvRsProv tnVzBrCPName="httpCtrct"/>
    </l3extInstP>
</l3extOut>
<l3extOut name="l3out2">
    <l3extInstP name="extnw2">
        <fvRsCons tnVzBrCPName="httpCtrct"/>
    </l3extInstP>
</l3extOut>
```

REST API の例: 中継ルーティング

次の例では、REST API を使用して、2 つの境界リーフ スイッチで 2 つの L3Outs を設定します。

REST API を使用してタスクを実行する

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- api/policymgr/mo/.xml -->
<polUni>
    <fvTenant name="t1">
        <fvCtx name="v1"/>
        <l3extOut name="l3out1">
            <l3extRsEctx tnFvCtxName="v1"/>
            <l3extLNodeP name="nodep1">
                <bgpPeerP addr="15.15.15.2/24">
                    <bgpAsP asn="100"/>
                </bgpPeerP>
              <l3extRsNodeL3OutAtt rtrId="11.11.11.103" tDn="topology/pod-1/node-101"/>

                <l3extLIfP name="ifp1">
                    <l3extRsPathL3OutAtt addr="12.12.12.3/24" ifInstT="l3-port"
tDn="topology/pod-1/paths-101/pathep-[eth1/3]" />
                    <ospfIfP/>
                </l3extLIfP>
            </l3extLNodeP>
            <l3extInstP name="extnw1">
                <l3extSubnet ip="192.168.1.0/24" scope="import-security"/>
                <l3extRsInstPToProfile direction="import" tnRtctrlProfileName="rp1"/>
                <l3extRsInstPToProfile direction="export" tnRtctrlProfileName="rp2"/>
                <fvRsProv tnVzBrCPName="httpCtrct"/>
            </l3extInstP>
            <bgpExtP/>
            <ospfExtP areaId="0.0.0.0" areaType="regular"/>
            <l3extRsL3DomAtt tDn="uni/l3dom-dom1"/>
            <rtctrlProfile name="rp1">
                <rtctrlCtxP name="ctxp1" action="permit" order="0">
                    <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule1"/>
                </rtctrlCtxP>
            </rtctrlProfile>
            <rtctrlProfile name="rp2">
                <rtctrlCtxP name="ctxp1" action="permit" order="0">
                    <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule2"/>
                </rtctrlCtxP>
            </rtctrlProfile>
        </l3extOut>
        <l3extOut name="l3out2">
            <l3extRsEctx tnFvCtxName="v1"/>
            <l3extLNodeP name="nodep2">
                <bgpPeerP addr="25.25.25.2/24">
                    <bgpAsP asn="100"/>
                </bgpPeerP>
                <l3extRsNodeL3OutAtt rtrId="22.22.22.203" tDn="topology/pod-1/node-102"
 />
                <l3extLIfP name="ifp2">
                    <l3extRsPathL3OutAtt addr="23.23.23.3/24" ifInstT="l3-port"
tDn="topology/pod-1/paths-102/pathep-[eth1/3]" />
                    <ospfIfP/>
                </l3extLIfP>
            </l3extLNodeP>
            <l3extInstP name="extnw2">
                <l3extSubnet ip="192.168.2.0/24" scope="import-security"/>
                <l3extRsInstPToProfile direction="import" tnRtctrlProfileName="rp2"/>
                <l3extRsInstPToProfile direction="export" tnRtctrlProfileName="rp1"/>
                <fvRsCons tnVzBrCPName="httpCtrct"/>
            </l3extInstP>
            <bgpExtP/>
            <ospfExtP areaId="0.0.0.0" areaType="regular"/>
            <l3extRsL3DomAtt tDn="uni/l3dom-dom1"/>
            <rtctrlProfile name="rp1">
                <rtctrlCtxP name="ctxp1" action="permit" order="0">
```

```
                    <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule1"/>
                </rtctrlCtxP>
            </rtctrlProfile>
            <rtctrlProfile name="rp2">
                <rtctrlCtxP name="ctxp1" action="permit" order="0">
                    <rtctrlRsCtxPToSubjP tnRtctrlSubjPName="match-rule2"/>
                </rtctrlCtxP>
            </rtctrlProfile>
        </l3extOut>
        <rtctrlSubjP name="match-rule1">
            <rtctrlMatchRtDest ip="192.168.1.0/24"/>
        </rtctrlSubjP>
        <rtctrlSubjP name="match-rule2">
            <rtctrlMatchRtDest ip="192.168.2.0/24"/>
        </rtctrlSubjP>
        <vzFilter name="http-filter">
            <vzEntry name="http-e" etherT="ip" prot="tcp"/>
        </vzFilter>
        <vzBrCP name="httpCtrct" scope="context">
            <vzSubj name="subj1">
                <vzRsSubjFiltAtt tnVzFilterName="http-filter"/>
            </vzSubj>
        </vzBrCP>
    </fvTenant>
</polUni>
```

共有 L3Out

REST API を使用した共有サービスの設定

共有設定の 2 つのレイヤ REST API を使用して 2 つの Vrf に 3 が記録されます。

2 つの方法が表示されますが、2 つの Vrf にレイヤ 3 が記録されるを共有する次の REST API の設定例は次の通信します。

手順

ステップ 1 プロバイダー レイヤ 3 を設定します。

例：

```
<tenant name="t1_provider">
<fvCtx name="VRF1">
<l3extOut name="T0-o1-L3OUT-1">
                <l3extRsEctx tnFvCtxName="o1"/>
                <ospfExtP areaId='60'/>
                <l3extInstP name="l3extInstP-1">
                <fvRsProv tnVzBrCPName="vzBrCP-1">
                </fvRsProv>
                <l3extSubnet ip="192.168.2.0/24" scope="shared-rtctrl, shared-security"
 aggregate=""/>
                </l3extInstP>
</l3extOut>
</tenant>
```

ステップ 2 レイヤ 3 Out コンシューマを設定します。

例：

```
<tenant name="t1_consumer">
<fvCtx name="VRF2">
<l3extOut name="T0-o1-L3OUT-1">
                <l3extRsEctx tnFvCtxName="o1"/>
                <ospfExtP areaId='70'/>
                <l3extInstP name="l3extInstP-2">
                <fvRsCons tnVzBrCPName="vzBrCP-1">
                </fvRsCons>
                <l3extSubnet ip="199.16.2.0/24" scope="shared-rtctrl, shared-security"
         aggregate=""/>
                </l3extInstP>
</l3extOut>
</tenant>
```

REST API を使用した L3Out の QoS の設定

REST API を使用した L3Out での QoS ディレクトリの設定

この章では L3Out で QoS ディレクトリを設定する方法について説明します。これは、リリース 4.0(1) 以降の L3Out QoS の推奨設定方法です。Cisco APIC

次のオブジェクトの内の 1 つで L3Out の QoS を設定できます。

- Switch Virtual Interface（SVI）
- サブインターフェイス
- 外部ルーテッド

手順

ステップ 1 L3Out SVI に QoS プライオリティを設定します。

例：

```
<l3extLIfP descr=""
dn="uni/tn-DT/out-L3_4_2_24_SVI17/lnodep-L3_4_E2_24/lifp-L3_4_E2_24_SVI_19"
           name="L3_4_E2_24_SVI_19" prio="level6" tag="yellow-green">
   <l3extRsPathL3OutAtt addr="0.0.0.0" autostate="disabled" descr="SVI19" encap="vlan-19"

                      encapScope="local" ifInstT="ext-svi" ipv6Dad="enabled" llAddr="::"

                         mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
                         tDn="topology/pod-1/protpaths-103-104/pathep-[V_L3_l4_2-24]"
                         targetDscp="unspecified">
       <l3extMember addr="107.2.1.253/24" ipv6Dad="enabled" llAddr="::" side="B"/>
       <l3extMember addr="107.2.1.252/24" ipv6Dad="enabled" llAddr="::" side="A"/>
    </l3extRsPathL3OutAtt>
    <l3extRsLIfPCustQosPol tnQosCustomPolName="VrfQos006"/>
</l3extLIfP>
```

ステップ 2 サブインターフェイスに QoS プライオリティを設定します。

例：

```
<l3extLIfP dn="uni/tn-DT/out-L4E48_inter_tenant/lnodep-L4E48_inter_tenant/lifp-L4E48"
           name="L4E48" prio="level4" tag="yellow-green">
    <l3extRsPathL3OutAtt addr="210.1.0.254/16" autostate="disabled" encap="vlan-20"
                         encapScope="local" ifInstT="sub-interface" ipv6Dad="enabled"
llAddr="::"
                         mac="00:22:BD:F8:19:FF" mode="regular" mtu="inherit"
                         tDn="topology/pod-1/paths-104/pathep-[eth1/48]"
targetDscp="unspecified"/>
    <l3extRsNdIfPol annotation="" tnNdIfPolName=""/>
    <l3extRsLIfPCustQosPol annotation="" tnQosCustomPolName=" vrfQos002"/>
</l3extLIfP>
```

ステップ 3 外部ルーテッドに QoS プライオリティを設定します。

例：

```
<l3extLIfP dn="uni/tn-DT/out-L2E37/lnodep-L2E37/lifp-L2E37OUT"
           name="L2E37OUT" prio="level5" tag="yellow-green">
    <l3extRsPathL3OutAtt addr="30.1.1.1/24" autostate="disabled" encap="unknown"
                         encapScope="local" ifInstT="l3-port" ipv6Dad="enabled"
                         llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular"
                         mtu="inherit" targetDscp="unspecified"
                         tDn="topology/pod-1/paths-102/pathep-[eth1/37]"/>
    <l3extRsNdIfPol annotation="" tnNdIfPolName=""/>
    <l3extRsLIfPCustQosPol tnQosCustomPolName="vrfQos002"/>
</l3extLIfP>
```

REST API を使用した L3Out の QoS コントラクトの設定

この項では、コントラクトを使用して L3Out の QoS を設定する方法について説明します。

（注） リリース 4.0(1) 以降では、L3Out QoS 用にカスタム QoS ポリシーを使用することを推奨しています。REST API を使用した L3Out での QoS ディレクトリの設定 （653 ページ）で説明しています。

手順

ステップ 1 テナント、VRF、ブリッジ ドメインを設定する場合、ポリシー適用が有効になっている状態で、出力モードに VRF を設定します（pcEnfDir="egress"）。次の例のように XML で post を送信します。

例：

```
<fvTenant  name="t1">
    <fvCtx name="v1" pcEnfPref="enforced" pcEnfDir="egress"/>
    <fvBD name="bd1">
        <fvRsCtx tnFvCtxName="v1"/>
        <fvSubnet ip="44.44.44.1/24" scope="public"/>
        <fvRsBDToOut tnL3extOutName="l3out1"/>
    </fvBD>"/>
</fvTenant>
```

ステップ 2 通信のため L3Out に参加して EPG を有効にする契約を作成するときは、優先順位の QoS を設定します。

この例のコントラクトには、L3Out で出力されるトラフィックの `level1` の QoS 優先順位を含みますまたは、ターゲットの DSCP 値を定義する可能性があります。QoS ポリシーは、契約またはサブジェクトのいずれかでサポートされます。

フィルタに `matchDscp =「Ef」` 条件があるため、このタグを持つトラフィックがコントラクト件名で指定されたキューを通して L3out プロセスにより受信できます。

（注） L3out インターフェイスでの QOS またはカスタム QOS では VRF の適用は入力とします。VRF の適用を出力にする必要があるのは、QOS 分類が EPG と L3out の間、または L3out から L3out へのトラフィックの契約で実行される場合に限ります。

（注） QOS 分類が契約で設定され、VRF の適用が出力である場合、契約 QOS 分類は L3out インターフェイス QOS またはカスタム QOS 分類をオーバーライドするため、これか新しいもののいずれかを設定する必要があります。

例：

```
<vzFilter name="http-filter">
    <vzEntry  name="http-e" etherT="ip" prot="tcp" matchDscp="EF"/>
</vzFilter>
<vzBrCP name="httpCtrct" prio="level1" scope="context">
    <vzSubj name="subj1">
        <vzRsSubjFiltAtt tnVzFilterName="http-filter"/>
    </vzSubj>
</vzBrCP>
```

REST API を使用した SR-MPLS カスタム QoS ポリシー

SR MPLS カスタム QoS ポリシーは、MPLS QoS 出力 ポリシーで定義された着信 MPLS EXP 値に基づいて、SR-MPLS ネットワークから送信されるパケットのプライオリティを定義します。これらのパケットは、ACI ファブリック内にあります。また、MPLS QoS 出力ポリシーで定義された IPv4 DSCP 値に基づく MPLS インターフェイスを介して ACI ファブリックから離れるパケットの CoS 値および MPLS EXP 値をマーキングします。

カスタム出力ポリシーが定義されていない場合、デフォルトの Qos レベル（`Level3`）がファブリック内のパケットに割り当てられます。カスタム出力ポリシーが定義されていない場合、デフォルトの EXP 値（`0`）がファブリックから離れるパケットにマーキングされます。

手順

ステップ 1 SR-MPLS QoS ポリシーの作成

次のPOSTで、

REST API を使用してタスクを実行する

- *customqos1*を、作成する SR-MPLS QoS ポリシーの名前に置き換えます。
- qosMplsIngressRuleの場合：
  - from = "2" to = "3"を、ポリシーに一致させる EXP 範囲に置き換えます。
  - prio = "level5"を ACI ファブリック内にあるパケットの ACI QoS レベルに置き換えます。
  - target = "CS5" は、パケットが一致したときに設定する DSCP 値に置き換えます。
  - targetCos = "4" を、パケットが一致したときにパケットに設定する CoS 値に置き換えます。
- qosMplsEgressRule の場合：
  - from = "CS2" to = "CS4" を、ポリシーを照合する DSCP 範囲に置き換えます。
  - targetExp = "5" を、パケットがファブリックを離れるときに設定する EXP 値に置き換えます。
  - targetCos = "3" を、パケットがファブリックを離れるときに設定する CoS 値に置き換えます。

```
<polUni>
  <fvTenant name="infra">
   <qosMplsCustomPol descr="" dn="uni/tn-infra/qosmplscustom-customqos1" name="customqos1"
  status="" >
        <qosMplsIngressRule from="2" to="3" prio="level5" target="CS5" targetCos="4"
status="" />
        <qosMplsEgressRule from="CS2" to="CS4" targetExp="5" targetCos="3" status=""/>
    </qosMplsCustomPol>
  </fvTenant>
</polUni>
```

ステップ 2 SR-MPLS QoS ポリシーの作成

次の POST で、customqos1 を前の手順で作成した SR-MPLS QoS ポリシーの名前に置き換えます。

```
<polUni>
    <fvTenant name="infra">
        <l3extOut name="mplsOut" status="" descr="bl">
            <l3extLNodeP name="mplsLNP" status="">
              <l3extRsLNodePMplsCustQosPol  tDn="uni/tn-infra/qosmplscustom-customqos1"/>

            </l3extLNodeP>
        </l3extOut>
    </fvTenant>
</polUni>
```

REST API を使用した ACI IP SLA の設定

REST API を使用した IP SLA モニタリング ポリシーの設定

REST API を使用して特定の SLA タイプのモニタリング プローブを送信できるようにするには、次の手順を実行します。Cisco APIC

手順

IP SLA モニタリング ポリシーの設定

例：

```
<?xml version="1.0" encoding="utf-8"?>
<imdata totalCount="1">
                <fvIPSLAMonitoringPol annotation="" descr=""
dn="uni/tn-t8/ipslaMonitoringPol-ICMP-Probe"
                 name="ICMP-Probe" nameAlias="" ownerKey="" ownerTag=""
slaDetectMultiplier="3" slaFrequency="5"
                 slaPort="0" slaType="icmp"/>
</imdata>
```

REST API を使用した IP-SLA トラック メンバーの設定

REST API を使用して IP SLA トラック メンバーを設定するには、次の手順を実行します。

手順

IP SLA トラック メンバーを設定します。

例：

```
<?xml version="1.0" encoding="utf-8"?>
<imdata totalCount="1">
             <fvTrackMember annotation="" descr="" dn="uni/tn-t8/trackmember-TM_pc_sub"

                dstIpAddr="52.52.52.1" name="TM_pc_sub" nameAlias="" ownerKey=""
ownerTag=""
                scopeDn="uni/tn-t8/out-t8_l3">
                        <fvRsIpslaMonPol annotation=""
tDn="uni/tn-t8/ipslaMonitoringPol-TCP-Telnet"/>
                </fvTrackMember>
</imdata>
```

REST API を使用した IP-SLA トラック リストの設定

REST API を使用して IP SLA トラック リストを設定するには、次の手順を実行します。

手順

IP SLA トラック リストを設定します。

例：

```
<?xml version="1.0" encoding="utf-8"?>
<imdata totalCount="1">
                <fvTrackList annotation="" descr="" dn="uni/tn-t8/tracklist-T8_pc_sub1"

              name="T8_pc_sub1" nameAlias="" ownerKey="" ownerTag="" percentageDown="0"

                percentageUp="1" type="weight" weightDown="5" weightUp="10">
                        <fvRsOtmListMember annotation=""
tDn="uni/tn-t8/trackmember-TM_pc_sub"
                        weight="10"/>
                </fvTrackList>
</imdata>
```

REST API を使用したスタティック ルートとトラック リストの関連付け

REST API を使用して IP SLA トラック リストをスタティック ルートに関連付けるには、次の手順を実行します。

手順

IP SLA トラック リストをスタティック ルートに関連付けます。

例：

```
<?xml version="1.0" encoding="utf-8"?>
<imdata totalCount="1">
                <ipRouteP aggregate="no" annotation="" descr=""

dn="uni/tn-t8/out-t8_l3/lnodep-t8_l3_vpc1/rsnodeL3OutAtt-[topology/pod-2/node-108]/rt-[88.88.88.2/24]"

                ip="88.88.88.2/24" name="" nameAlias="" pref="1" rtCtrl="">
                        <ipRsRouteTrack annotation=""
tDn="uni/tn-t8/tracklist-T8_TL1_Static"/>
                        <ipNexthopP annotation="" descr="" name="" nameAlias=""
nhAddr="23.23.2.3"
                        pref="1" type="prefix"/>
                </ipRouteP>
</imdata>
```

REST API を使用して ネクスト ホップ プロファイルのトラック リストに関連付けをする

REST API を使用して IP SLA トラック リストをネクスト ホップ プロファイルに関連付けるには、次の手順を実行します。

手順

IP SLA トラック リストをネクスト ホップ プロファイルに関連付けます。

例：

```
<?xml version="1.0" encoding="utf-8"?>
<imdata totalCount="1">
                <ipRouteP aggregate="no" annotation="" descr=""

dn="uni/tn-t8/out-t8_l3/lnodep-t8_l3_vpc1/rsnodeL3OutAtt-[topology/pod-2/node-109]/rt-[86.86.86.2/24]"

                ip="86.86.86.2/24" name="" nameAlias="" pref="1" rtCtrl="">
                        <ipNexthopP annotation="" descr="" name="" nameAlias=""
nhAddr="25.25.25.3" pref="1" type="prefix">
                                <ipRsNexthopRouteTrack annotation=""
tDn="uni/tn-t8/tracklist-ctx0_25.25.25.3"/>
                                <ipRsNHTrackMember annotation=""
tDn="uni/tn-t8/trackmember-ctx0_25.25.25.3"/>
                        </ipNexthopP>
                </ipRouteP>
</imdata>
```

REST API を使用した HSRP の設定

REST API を使用した APIC 内の HSRP の設定

リーフ スイッチが設定されている場合、HSRP が有効になっています。

始める前に

- テナントおよび VRF を設定する必要があります。
- VLAN プールは、適切な VLAN 範囲が定義され、レイヤ 3 ドメインが作成されて VLAN プールに接続されている状態で設定される必要があります。
- エンティティ プロファイルの接続も、レイヤ3ドメインに関連付けられている必要があります。
- リーフ スイッチのインターフェイス プロファイルは必要に応じて設定する必要があります。

手順

ステップ 1 ポート セレクタを作成します。

例：

REST API を使用してタスクを実行する

```
<polUni>
  <infraInfra dn="uni/infra">
    <infraNodeP name="TenantNode_101">
      <infraLeafS name="leafselector" type="range">
        <infraNodeBlk name="nodeblk" from_="101" to_="101">
            </infraNodeBlk>
      </infraLeafS>
      <infraRsAccPortP tDn="uni/infra/accportprof-TenantPorts_101"/>
    </infraNodeP>
    <infraAccPortP name="TenantPorts_101">
      <infraHPortS name="portselector" type="range">
        <infraPortBlk name="portblk" fromCard="1" toCard="1" fromPort="41" toPort="41">
            </infraPortBlk>
        <infraRsAccBaseGrp tDn="uni/infra/funcprof/accportgrp-TenantPortGrp_101"/>
      </infraHPortS>
    </infraAccPortP>
    <infraFuncP>
      <infraAccPortGrp name="TenantPortGrp_101">
        <infraRsAttEntP tDn="uni/infra/attentp-AttEntityProfTenant"/>
        <infraRsHIfPol tnFabricHIfPolName="default"/>
      </infraAccPortGrp>
    </infraFuncP>
  </infraInfra>
</polUni>
```

ステップ 2 テナント ポリシーを作成します。

例：

```
<polUni>
  <fvTenant name="t9" dn="uni/tn-t9" descr="">
    <fvCtx name="t9_ctx1" pcEnfPref="unenforced">
    </fvCtx>
    <fvBD name="t9_bd1" unkMacUcastAct="flood" arpFlood="yes">
      <fvRsCtx tnFvCtxName="t9_ctx1"/>
      <fvSubnet ip="101.9.1.1/24" scope="shared"/>
    </fvBD>
    <l3extOut dn="uni/tn-t9/out-l3extOut1" enforceRtctrl="export" name="l3extOut1">
      <l3extLNodeP name="Node101">
        <l3extRsNodeL3OutAtt rtrId="210.210.121.121" rtrIdLoopBack="no"
tDn="topology/pod-1/node-101"/>
      </l3extLNodeP>
      <l3extRsEctx tnFvCtxName="t9_ctx1"/>
      <l3extRsL3DomAtt tDn="uni/l3dom-dom1"/>
      <l3extInstP matchT="AtleastOne" name="extEpg" prio="unspecified"
targetDscp="unspecified">
        <l3extSubnet aggregate="" descr="" ip="176.21.21.21/21" name=""
scope="import-security"/>
      </l3extInstP>
    </l3extOut>
  </fvTenant>
</polUni>
```

ステップ 3 LLDP インターフェイス ポリシーを作成します。.

例：

```
<polUni>
  <fvTenant name="t9" dn="uni/tn-t9" descr="">
    <hsrpIfPol name="hsrpIfPol" ctrl="bfd" delay="4" reloadDelay="11"/>
  </fvTenant>
</polUni>
```

REST API を使用してタスクを実行する

ステップ 4 HSRP グループ ポリシーを作成します。.

例：

```
<polUni>
  <fvTenant name="t9" dn="uni/tn-t9" descr="">
    <hsrpIfPol name="hsrpIfPol" ctrl="bfd" delay="4" reloadDelay="11"/>
  </fvTenant>
</polUni>
```

ステップ 5 HSRP インターフェイス プロファイルおよび HSRP グループ プロファイルを作成します。

例：

```
<polUni>
  <fvTenant name="t9" dn="uni/tn-t9" descr="">
    <l3extOut dn="uni/tn-t9/out-l3extOut1" enforceRtctrl="export" name="l3extOut1">
      <l3extLNodeP name="Node101">
        <l3extLIfP name="eth1-41-v6" ownerKey="" ownerTag="" tag="yellow-green">
          <hsrpIfP name="eth1-41-v6" version="v2">
            <hsrpRsIfPol tnHsrpIfPolName="hsrpIfPol"/>
           <hsrpGroupP descr="" name="HSRPV6-2" groupId="330" groupAf="ipv6" ip="fe80::3"
 mac="00:00:0C:18:AC:01" ipObtainMode="admin">
              <hsrpRsGroupPol tnHsrpGroupPolName="G1"/>
            </hsrpGroupP>
          </hsrpIfP>
          <l3extRsPathL3OutAtt addr="2002::100/64" descr="" encap="unknown"
encapScope="local" ifInstT="l3-port" llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular"
 mtu="inherit" tDn="topology/pod-1/paths-101/pathep-[eth1/41]" targetDscp="unspecified">

            <l3extIp addr="2004::100/64"/>
          </l3extRsPathL3OutAtt>
        </l3extLIfP>
        <l3extLIfP name="eth1-41-v4" ownerKey="" ownerTag="" tag="yellow-green">
          <hsrpIfP name="eth1-41-v4" version="v1">
            <hsrpRsIfPol tnHsrpIfPolName="hsrpIfPol"/>
            <hsrpGroupP descr="" name="HSRPV4-2" groupId="51" groupAf="ipv4"
ip="177.21.21.21" mac="00:00:0C:18:AC:01" ipObtainMode="admin">
              <hsrpRsGroupPol tnHsrpGroupPolName="G1"/>
            </hsrpGroupP>
          </hsrpIfP>
          <l3extRsPathL3OutAtt addr="177.21.21.11/24" descr="" encap="unknown"
encapScope="local" ifInstT="l3-port" llAddr="::" mac="00:22:BD:F8:19:FF" mode="regular"
 mtu="inherit" tDn="topology/pod-1/paths-101/pathep-[eth1/41]" targetDscp="unspecified">

            <l3extIp addr="177.21.23.11/24"/>
          </l3extRsPathL3OutAtt>
        </l3extLIfP>
      </l3extLNodeP>
    </l3extOut>
  </fvTenant>
</polUni>
```

REST API を使用した Cisco ACI GOLF の設定

REST API を使用した GOLF の設定

手順

ステップ 1 次の例では、REST API を使用して GOLF のノードおよびスパイン スイッチ インターフェイスを展開する方法を示しています。

例：

```
POST
https://192.0.20.123/api/mo/uni/golf.xml
```

ステップ 2 次の XML で、スパイン スイッチ インターフェイスと GOLF サービスのインフラ テナント プロバイダを設定します。次の XML 構造を POST メッセージの本文に含めます。

例：

```
<l3extOut descr="" dn="uni/tn-infra/out-golf" enforceRtctrl="export,import"
    name="golf"
    ownerKey="" ownerTag="" targetDscp="unspecified">
    <l3extRsEctx tnFvCtxName="overlay-1"/>
    <l3extProvLbl descr="" name="golf"
         ownerKey="" ownerTag="" tag="yellow-green"/>
    <l3extLNodeP configIssues="" descr=""
         name="bLeaf" ownerKey="" ownerTag=""
         tag="yellow-green" targetDscp="unspecified">
         <l3extRsNodeL3OutAtt rtrId="10.10.3.3" rtrIdLoopBack="no"
             tDn="topology/pod-1/node-111">
             <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
             <l3extLoopBackIfP addr="10.10.3.3" descr="" name=""/>
         </l3extRsNodeL3OutAtt>
         <l3extRsNodeL3OutAtt rtrId="10.10.3.4" rtrIdLoopBack="no"
             tDn="topology/pod-1/node-112">
         <l3extInfraNodeP descr="" fabricExtCtrlPeering="yes" name=""/>
         <l3extLoopBackIfP addr="10.10.3.4" descr="" name=""/>
         </l3extRsNodeL3OutAtt>
         <l3extLIfP descr="" name="portIf-spine1-3"
             ownerKey="" ownerTag="" tag="yellow-green">
             <ospfIfP authKeyId="1" authType="none" descr="" name="">
               <ospfRsIfPol tnOspfIfPolName="ospfIfPol"/>
             </ospfIfP>
             <l3extRsNdIfPol tnNdIfPolName=""/>
             <l3extRsIngressQosDppPol tnQosDppPolName=""/>
             <l3extRsEgressQosDppPol tnQosDppPolName=""/>
             <l3extRsPathL3OutAtt addr="7.2.1.1/24" descr=""
                encap="vlan-4"
                encapScope="local"
                ifInstT="sub-interface"
                llAddr="::" mac="00:22:BD:F8:19:FF"
                mode="regular"
                mtu="1500"
                tDn="topology/pod-1/paths-111/pathep-[eth1/12]"
                targetDscp="unspecified"/>
          </l3extLIfP>
          <l3extLIfP descr="" name="portIf-spine2-1"
              ownerKey=""
```

REST API を使用してタスクを実行する

```
    ownerTag=""
    tag="yellow-green">
    <ospfIfP authKeyId="1"
         authType="none"
         descr=""
         name="">
         <ospfRsIfPol tnOspfIfPolName="ospfIfPol"/>
    </ospfIfP>
    <l3extRsNdIfPol tnNdIfPolName=""/>
    <l3extRsIngressQosDppPol tnQosDppPolName=""/>
    <l3extRsEgressQosDppPol tnQosDppPolName=""/>
    <l3extRsPathL3OutAtt addr="7.1.0.1/24" descr=""
         encap="vlan-4"
         encapScope="local"
         ifInstT="sub-interface"
         llAddr="::" mac="00:22:BD:F8:19:FF"
         mode="regular"
         mtu="9000"
         tDn="topology/pod-1/paths-112/pathep-[eth1/11]"
         targetDscp="unspecified"/>
</l3extLIfP>
<l3extLIfP descr="" name="portif-spine2-2"
    ownerKey=""
    ownerTag=""
    tag="yellow-green">
    <ospfIfP authKeyId="1"
         authType="none" descr=""
         name="">
         <ospfRsIfPol tnOspfIfPolName="ospfIfPol"/>
   </ospfIfP>
   <l3extRsNdIfPol tnNdIfPolName=""/>
   <l3extRsIngressQosDppPol tnQosDppPolName=""/>
   <l3extRsEgressQosDppPol tnQosDppPolName=""/>
   <l3extRsPathL3OutAtt addr="7.2.2.1/24" descr=""
         encap="vlan-4"
         encapScope="local"
         ifInstT="sub-interface"
                llAddr="::" mac="00:22:BD:F8:19:FF"
                mode="regular"
                mtu="1500"
                tDn="topology/pod-1/paths-112/pathep-[eth1/12]"
                targetDscp="unspecified"/>
   </l3extLIfP>
   <l3extLIfP descr="" name="portIf-spine1-2"
        ownerKey="" ownerTag="" tag="yellow-green">
        <ospfIfP authKeyId="1" authType="none" descr="" name="">
             <ospfRsIfPol tnOspfIfPolName="ospfIfPol"/>
        </ospfIfP>
        <l3extRsNdIfPol tnNdIfPolName=""/>
        <l3extRsIngressQosDppPol tnQosDppPolName=""/>
        <l3extRsEgressQosDppPol tnQosDppPolName=""/>
        <l3extRsPathL3OutAtt addr="9.0.0.1/24" descr=""
         encap="vlan-4"
         encapScope="local"
         ifInstT="sub-interface"
              llAddr="::" mac="00:22:BD:F8:19:FF"
              mode="regular"
              mtu="9000"
              tDn="topology/pod-1/paths-111/pathep-[eth1/11]"
              targetDscp="unspecified"/>
   </l3extLIfP>
   <l3extLIfP descr="" name="portIf-spine1-1"
         ownerKey="" ownerTag="" tag="yellow-green">
         <ospfIfP authKeyId="1" authType="none" descr="" name="">
```

REST API を使用してタスクを実行する

```
                        <ospfRsIfPol tnOspfIfPolName="ospfIfPol"/>
                    </ospfIfP>
                    <l3extRsNdIfPol tnNdIfPolName=""/>
                    <l3extRsIngressQosDppPol tnQosDppPolName=""/>
                    <l3extRsEgressQosDppPol tnQosDppPolName=""/>
                    <l3extRsPathL3OutAtt addr="7.0.0.1/24" descr=""
                      encap="vlan-4"
                      encapScope="local"
                      ifInstT="sub-interface"
                      llAddr="::" mac="00:22:BD:F8:19:FF"
                      mode="regular"
                      mtu="1500"
                      tDn="topology/pod-1/paths-111/pathep-[eth1/10]"
                           targetDscp="unspecified"/>
                </l3extLIfP>
                <bgpInfraPeerP addr="10.10.3.2"
                   allowedSelfAsCnt="3"
                   ctrl="send-com,send-ext-com"
                   descr="" name="" peerCtrl=""
                   peerT="wan"
                   privateASctrl="" ttl="2" weight="0">
                   <bgpRsPeerPfxPol tnBgpPeerPfxPolName=""/>
                   <bgpAsP asn="150" descr="" name="aspn"/>
                </bgpInfraPeerP>
                <bgpInfraPeerP addr="10.10.4.1"
                   allowedSelfAsCnt="3"
                   ctrl="send-com,send-ext-com" descr="" name="" peerCtrl=""
                   peerT="wan"
                   privateASctrl="" ttl="1" weight="0">
                   <bgpRsPeerPfxPol tnBgpPeerPfxPolName=""/>
                   <bgpAsP asn="100" descr="" name=""/>
                 </bgpInfraPeerP>
                 <bgpInfraPeerP addr="10.10.3.1"
                   allowedSelfAsCnt="3"
                   ctrl="send-com,send-ext-com" descr="" name="" peerCtrl=""
                   peerT="wan"
                   privateASctrl="" ttl="1" weight="0">
                   <bgpRsPeerPfxPol tnBgpPeerPfxPolName=""/>
                   <bgpAsP asn="100" descr="" name=""/>
                </bgpInfraPeerP>
            </l3extLNodeP>
           <bgpRtTargetInstrP descr="" name="" ownerKey="" ownerTag="" rtTargetT="explicit"/>

            <l3extRsL3DomAtt tDn="uni/l3dom-l3dom"/>
            <l3extInstP descr="" matchT="AtleastOne" name="golfInstP"
                      prio="unspecified"
                      targetDscp="unspecified">
                      <fvRsCustQosPol tnQosCustomPolName=""/>
             </l3extInstP>
             <bgpExtP descr=""/>
             <ospfExtP areaCost="1"
                    areaCtrl="redistribute,summary"
                    areaId="0.0.0.1"
                    areaType="regular" descr=""/>
</l3extOut>
```

ステップ 3 次の XML で、GOLF サービスのインフラ部分のテナント コンシューマを設定します。次の XML 構造を POST メッセージの本文に含めます。

例：

```
<fvTenant descr="" dn="uni/tn-pep6" name="pep6" ownerKey="" ownerTag="">
     <vzBrCP descr="" name="webCtrct"
```

REST API を使用してタスクを実行する

```
    ownerKey="" ownerTag="" prio="unspecified"
    scope="global" targetDscp="unspecified">
    <vzSubj consMatchT="AtleastOne" descr=""
         name="http" prio="unspecified" provMatchT="AtleastOne"
         revFltPorts="yes" targetDscp="unspecified">
         <vzRsSubjFiltAtt directives="" tnVzFilterName="default"/>
    </vzSubj>
</vzBrCP>
<vzBrCP descr="" name="webCtrct-pod2"
     ownerKey="" ownerTag="" prio="unspecified"
     scope="global" targetDscp="unspecified">
     <vzSubj consMatchT="AtleastOne" descr=""
          name="http" prio="unspecified"
          provMatchT="AtleastOne" revFltPorts="yes"
          targetDscp="unspecified">
          <vzRsSubjFiltAtt directives=""
                tnVzFilterName="default"/>
     </vzSubj>
 </vzBrCP>
 <fvCtx descr="" knwMcastAct="permit"
      name="ctx6" ownerKey="" ownerTag=""
      pcEnfDir="ingress" pcEnfPref="enforced">
      <bgpRtTargetP af="ipv6-ucast"
           descr="" name="" ownerKey="" ownerTag="">
           <bgpRtTarget descr="" name="" ownerKey="" ownerTag=""
           rt="route-target:as4-nn2:100:1256"
           type="export"/>
           <bgpRtTarget descr="" name="" ownerKey="" ownerTag=""
                rt="route-target:as4-nn2:100:1256"
                type="import"/>
      </bgpRtTargetP>
      <bgpRtTargetP af="ipv4-ucast"
           descr="" name="" ownerKey="" ownerTag="">
           <bgpRtTarget descr="" name="" ownerKey="" ownerTag=""
                rt="route-target:as4-nn2:100:1256"
                type="export"/>
           <bgpRtTarget descr="" name="" ownerKey="" ownerTag=""
                rt="route-target:as4-nn2:100:1256"
                type="import"/>
      </bgpRtTargetP>
      <fvRsCtxToExtRouteTagPol tnL3extRouteTagPolName=""/>
      <fvRsBgpCtxPol tnBgpCtxPolName=""/>
      <vzAny descr="" matchT="AtleastOne" name=""/>
      <fvRsOspfCtxPol tnOspfCtxPolName=""/>
      <fvRsCtxToEpRet tnFvEpRetPolName=""/>
      <l3extGlobalCtxName descr="" name="dci-pep6"/>
 </fvCtx>
 <fvBD arpFlood="no" descr="" epMoveDetectMode=""
      ipLearning="yes"
      limitIpLearnToSubnets="no"
      llAddr="::" mac="00:22:BD:F8:19:FF"
      mcastAllow="no"
      multiDstPktAct="bd-flood"
      name="bd107" ownerKey="" ownerTag="" type="regular"
      unicastRoute="yes"
      unkMacUcastAct="proxy"
      unkMcastAct="flood"
      vmac="not-applicable">
      <fvRsBDToNdP tnNdIfPolName=""/>
      <fvRsBDToOut tnL3extOutName="routAccounting-pod2"/>
      <fvRsCtx tnFvCtxName="ctx6"/>
      <fvRsIgmpsn tnIgmpSnoopPolName=""/>
      <fvSubnet ctrl="" descr="" ip="27.6.1.1/24"
           name="" preferred="no"
```

REST API を使用してタスクを実行する

```
                scope="public"
                virtual="no"/>
                <fvSubnet ctrl="nd" descr="" ip="2001:27:6:1::1/64"
                     name="" preferred="no"
                     scope="public"
                     virtual="no">
                     <fvRsNdPfxPol tnNdPfxPolName=""/>
                </fvSubnet>
                <fvRsBdToEpRet resolveAct="resolve" tnFvEpRetPolName=""/>
           </fvBD>
           <fvBD arpFlood="no" descr="" epMoveDetectMode=""
                ipLearning="yes"
                limitIpLearnToSubnets="no"
                llAddr="::" mac="00:22:BD:F8:19:FF"
                mcastAllow="no"
                multiDstPktAct="bd-flood"
                name="bd103" ownerKey="" ownerTag="" type="regular"
                unicastRoute="yes"
                unkMacUcastAct="proxy"
                unkMcastAct="flood"
                vmac="not-applicable">
                <fvRsBDToNdP tnNdIfPolName=""/>
                <fvRsBDToOut tnL3extOutName="routAccounting"/>
                <fvRsCtx tnFvCtxName="ctx6"/>
                <fvRsIgmpsn tnIgmpSnoopPolName=""/>
                <fvSubnet ctrl="" descr="" ip="23.6.1.1/24"
                     name="" preferred="no"
                     scope="public"
                     virtual="no"/>
                <fvSubnet ctrl="nd" descr="" ip="2001:23:6:1::1/64"
                     name="" preferred="no"
                     scope="public" virtual="no">
                     <fvRsNdPfxPol tnNdPfxPolName=""/>
                </fvSubnet>
                <fvRsBdToEpRet resolveAct="resolve" tnFvEpRetPolName=""/>
           </fvBD>
           <vnsSvcCont/>
           <fvRsTenantMonPol tnMonEPGPolName=""/>
           <fvAp descr="" name="AP1"
                ownerKey="" ownerTag="" prio="unspecified">
                <fvAEPg descr=""
                     isAttrBasedEPg="no"
                     matchT="AtleastOne"
                     name="epg107"
                     pcEnfPref="unenforced" prio="unspecified">
                     <fvRsCons prio="unspecified"
                          tnVzBrCPName="webCtrct-pod2"/>
                     <fvRsPathAtt descr=""
                          encap="vlan-1256"
                          instrImedcy="immediate"
                          mode="regular" primaryEncap="unknown"
                          tDn="topology/pod-2/paths-107/pathep-[eth1/48]"/>
                     <fvRsDomAtt classPref="encap" delimiter=""
                          encap="unknown"
                          instrImedcy="immediate"
                          primaryEncap="unknown"
                          resImedcy="lazy" tDn="uni/phys-phys"/>
                     <fvRsCustQosPol tnQosCustomPolName=""/>
                     <fvRsBd tnFvBDName="bd107"/>
                     <fvRsProv matchT="AtleastOne"
                          prio="unspecified"
                          tnVzBrCPName="default"/>
                </fvAEPg>
                <fvAEPg descr=""
```

REST API を使用してタスクを実行する

```
          isAttrBasedEPg="no"
          matchT="AtleastOne"
          name="epg103"
          pcEnfPref="unenforced" prio="unspecified">
          <fvRsCons prio="unspecified" tnVzBrCPName="default"/>
          <fvRsCons prio="unspecified" tnVzBrCPName="webCtrct"/>
          <fvRsPathAtt descr="" encap="vlan-1256"
               instrImedcy="immediate"
               mode="regular" primaryEncap="unknown"
               tDn="topology/pod-1/paths-103/pathep-[eth1/48]"/>
               <fvRsDomAtt classPref="encap" delimiter=""
                    encap="unknown"
                    instrImedcy="immediate"
                    primaryEncap="unknown"
                    resImedcy="lazy" tDn="uni/phys-phys"/>
               <fvRsCustQosPol tnQosCustomPolName=""/>
               <fvRsBd tnFvBDName="bd103"/>
     </fvAEPg>
</fvAp>
<l3extOut descr=""
     enforceRtctrl="export"
     name="routAccounting-pod2"
     ownerKey="" ownerTag="" targetDscp="unspecified">
     <l3extRsEctx tnFvCtxName="ctx6"/>
     <l3extInstP descr=""
          matchT="AtleastOne"
          name="accountingInst-pod2"
          prio="unspecified" targetDscp="unspecified">
     <l3extSubnet aggregate="export-rtctrl,import-rtctrl"
          descr="" ip="::/0" name=""
          scope="export-rtctrl,import-rtctrl,import-security"/>
     <l3extSubnet aggregate="export-rtctrl,import-rtctrl"
          descr=""
          ip="0.0.0.0/0" name=""
          scope="export-rtctrl,import-rtctrl,import-security"/>
     <fvRsCustQosPol tnQosCustomPolName=""/>
     <fvRsProv matchT="AtleastOne"
          prio="unspecified" tnVzBrCPName="webCtrct-pod2"/>
     </l3extInstP>
     <l3extConsLbl descr=""
          name="golf2"
          owner="infra"
          ownerKey="" ownerTag="" tag="yellow-green"/>
</l3extOut>
<l3extOut descr=""
     enforceRtctrl="export"
     name="routAccounting"
     ownerKey="" ownerTag="" targetDscp="unspecified">
     <l3extRsEctx tnFvCtxName="ctx6"/>
     <l3extInstP descr=""
          matchT="AtleastOne"
          name="accountingInst"
          prio="unspecified" targetDscp="unspecified">
     <l3extSubnet aggregate="export-rtctrl,import-rtctrl" descr=""
          ip="0.0.0.0/0" name=""
          scope="export-rtctrl,import-rtctrl,import-security"/>
     <fvRsCustQosPol tnQosCustomPolName=""/>
     <fvRsProv matchT="AtleastOne" prio="unspecified" tnVzBrCPName="webCtrct"/>
     </l3extInstP>
     <l3extConsLbl descr=""
          name="golf"
          owner="infra"
          ownerKey="" ownerTag="" tag="yellow-green"/>
</l3extOut>
```

```
</fvTenant>
```

REST API を使用した DCIG への BGP EVPN タイプ 2 ホスト ルート配信の有効化

次のように REST API を使用して、BGP EVPN タイプ 2 ホスト ルートの配信を有効にします。

始める前に

EVPN サービスを設定する必要があります。

手順

ステップ 1 次の例のように、XML が含まれている POST で、ホスト ルート リーク ポリシーを設定します。

例：

```
<bgpCtxAfPol descr="" ctrl="host-rt-leak" name="bgpCtxPol_0 status=""/>
```

ステップ 2 次の例のように、XML が含まれている POST を使用してアドレス ファミリの一方または両方の VRF BGP アドレス ファミリ コンテキスト ポリシーに、ポリシーを適用します。

例：

```
<fvCtx name="vni-10001">
<fvRsCtxToBgpCtxAfPol af="ipv4-ucast" tnBgpCtxAfPolName="bgpCtxPol_0"/>
<fvRsCtxToBgpCtxAfPol af="ipv6-ucast" tnBgpCtxAfPolName="bgpCtxPol_0"/>
</fvCtx>
```

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。