



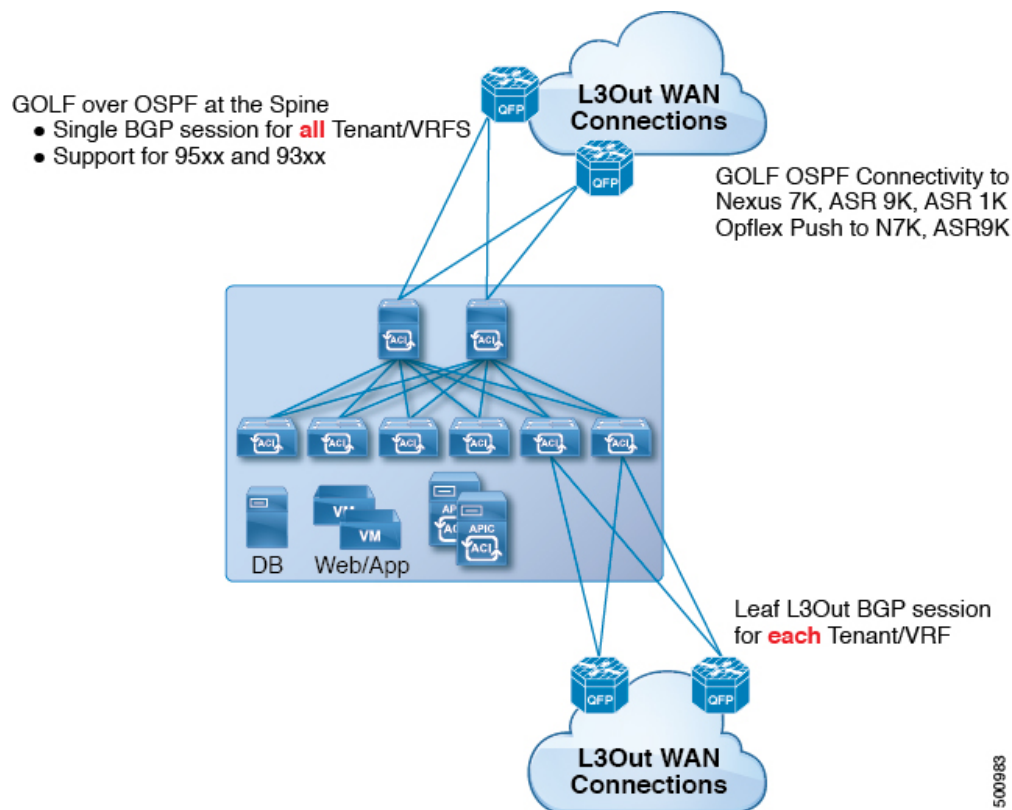
[Cisco ACI GOLF]

- [\[Cisco ACI GOLF\] \(1 ページ\)](#)
- [DCIG への BGP EVPN タイプ 2 ホスト ルートの分散化, on page 17](#)

[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 1 : [Cisco ACI GOLF] 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。

レイヤ 3 外部アウトサイド ネットワーク (L3extOut) [GOLF] は、infra テナントの下で指定されています。このネットワークは、スパインスイッチの物理接続です。そして次のものが含まれます：

- LNodeP (infra テナントの L3Out では、l3extInstP は、必要ありません。)
- 次のプロバイダー ラベル。L3extOut これは、インフラ テナント内にある [GOLF] のプロバイダー ラベルです。
- 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ます。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 ラベルです。これは、L3Out の同じプロバイダー ラベルと一致している必要があります。この L3Out は、[GOLF] 用であり、`infra` テナント内にあります。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。
- 一致するプロバイダー `L3extOut` (`infra` テナント内) の BGP EVPN セッションは、この L3Out で定義されてるテナント ルートをアドバタイズします。

次の注意事項と制限事項 [Cisco ACI GOLF]

次の [Cisco ACI GOLF] 注意事項と制約事項を確認します：

- 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 アプリケーションセントリックインフラストラクチャ (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]：モードスイッチおよびすべての 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は 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、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 (Cisco ACI Multi-Pod)]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 (Cisco ACI Multi-Pod)] および EVPN トポロジで使用されているすべてのスイッチと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] を構成する場合、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] の構成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ー [GOLF] 外部ネットワーク ([GOLF] L3Out) に追加できます。ただし [GOLF] 各 L3Out に違うプロバイダー ラベルが必要です。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。
- 一致するプロバイダー L3Out (infra テナント内) 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 を展開する時、[GOLF] に 1 つだけがプロバイダー/利用者ラベル、および 0/0 エクスポート集約を持たない場合、[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 スイッチ上にある既存の 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。
- 2 つの L3extOut が存在するデプロイメントシナリオでは、1 つのスパインスイッチ上に、そのうちの 1 つにプロバイダ ラベル prov1 があり DCI 1 とピアリングし、2 番目の L3extOut は、プロバイダー ラベル prov2 を持つ DCI 2 とピアリングします。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、ルートのリークは、[Cisco ACI] ファブリックまたは、GOLF OpFlex VRF インスタンスとシステム内の他の VRF インスタンス間の GOLF デバイス上では発生しません。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 外部 (L3Out) 接続を構成する場合、または Inter-Pod Network (IPN) を介した [マルチポッド (Multi-Pod)] 接続を構成する場合は、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。[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、構成可能な 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、構成された MTU 値にイーサネットヘッダーが含まれています。構成された値が 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。

Multi-Site サイト間の共有 GOLF 接続を使用する

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、ピアのレベルです。

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
```

ACI の構成 [GOLF] GUI の使用

次の手順は、すべてのテナントネットワークが利用できるインフラ [GOLF] サービスを構成する方法を説明します。

手順

ステップ 1 メニュー バーで、[テナント (Tenants)] をクリックし、その後にインフラ テナントを選択するために [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、[ネットワーキング (Networking)] オプションを展開して、次のアクションを実行します :

- [L3Out (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。
- [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。
- [使用目的 : (Use For:)] フィールドで、[ゴルフ (Golf)] を選択します。

[プロバイダー ラベル (Provider Label)] および [ルートターゲット (Route Target)] フィールドが表示されます。

- d) [プロバイダー ラベル (Provider Label)] フィールドに、プロバイダー ラベルを入力します(たとえば、[ゴルフ (Golf)])。
- e) [ルートターゲット (Route Target)] 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 (Automatic)] : 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 (Explicit)] : 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 ポリシーは、[BGP ルート ターゲット プロファイル (BGP Route Target Profile)] テーブルで構成されます。これは、[BGP ページ (BGP Page)] ([VRF ウィザードの作成 (Create VRF Wizard)] 内) にあります。[自動 (Automatic)] オプション [ルート ターゲット (Route Target)] フィールドで選択した場合、[VRF ウィザードの作成 (Create VRF Wizard)] 内で明示ルート ターゲット ポリシーの構成は、BGP ルーティング中断の原因となる可能性があります。

- 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 [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。これは、[L3Outの作成 (Create L3Out)] ウィザードにあります。

- a) [ノード ID (Node 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) [ルータ ID (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。

次の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。[ルータ ID (Router ID)] フィールド。これは、以前に構築した [ループバック アドレスとしてのユーザー ルータ ID (Use Router ID for Loopback Address)] オプションと同等です。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) [外部制御ピアリング (External Control Peering)] フィールドを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)] エリア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)] 上に構築できます。

[プロトコル (Protocols)] ウィンドウが表示されます。

ステップ 4 [プロトコル (Protocols)] ウィンドウで必要な情報を入力します。これは、[L3Outの作成 (Create L3Out)] ウィザードにあります。

- 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)] エリアで、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
 - [EBGP マルチホップ TTL (EBGP Multihop TTL)] を入力します : 接続の存続可能時間 (TTL) を入力します。範囲は 1 ～ 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 ～ 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] エリアで、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 [外部 EPG (External EPG)] ウィンドウの必要な情報を、次に入力します。これは、[L3Outの作成 (Create L3Out)] ウィザードにあります。

- a) [名前 (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) [提供されたコントラクト (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、サブネットエリアが表示されます。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) [終了 (Finish)] をクリックして [L3Outの作成 (Create L3Out)] ウィザードで必要な構成を完了します。

ステップ 6 任意のテナントの [ナビゲーション (Navigation)] ペインで、[tenant_name] > [ネットワーキング (Networking)] > [L3Out (L3Outs)] を展開して、次のアクションを実行します :

- a) [L3Out (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 に活用 (Use for GOLF)] フィールドの横にあるチェック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 (Consumer Label)] を割り当てます。この例では、[ゴルフ (Golf)] (以前に作成済み) を作成します。
- f) [次へ (Next)] をクリックし、[終了 (Finish)] をクリックします。

[Cisco ACI GOLF] NX-OS スタイル CLI を使用した 構成の例

次の例を構成する CLI コマンドの [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。

BGP EVPN のテナント インフラの構成

次の例を構成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 の構成

次の例では、BGP EVPN をサポートする BGP を構成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 のテナントの構成

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構成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
  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 の構成

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 マップを構成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

```

構成 [GOLF] REST API の使用

手順の概要

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、REST API を使用：
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構成します。次の XML 構造を POST メッセージの本文に含めます。
3. 次の XML で、[GOLF] サービスのインフラ部分のテナント コンシューマを構成します。次の XML 構造を POST メッセージの本文に含めます。

手順の詳細

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、REST API を使用：

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構成します。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>
    <l3extLIIfP 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"/>
    </l3extLIIfP>
    <l3extLIIfP descr="" name="portIf-spine2-1" ownerKey=""
ownerTag="" tag="yellow-green">
    <ospfIfP authKeyId="1" authType="none" descr=""
name="">
    <ospfRsIfPol tnOspfIfPolName="ospfIfPol"/>
    </ospfIfP>
    <l3extRsNdIfPol tnNdIfPolName=""/>
    <l3extRsIngressQosDppPol tnQosDppPolName=""/>
    <l3extRsEgressQosDppPol tnQosDppPolName=""/>
    <l3extRsPathL3OutAtt addr="7.1.0.1/24" 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"/>
    </l3extLIIfP>
    <l3extLIIfP 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"/>
    </l3extLIIfP>
    <l3extLIIfP 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="">
        <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 コンシューマを構成します。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="webCtct" 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="webCtct-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="dc1-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"
      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="" 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>
  <l3extConsLbl1 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>

```

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、BGP 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構成およびサービスを使用するテナントを構成している必要があります。

手順

-
- ステップ 1 メニュー バーで、[テナント (Tenants)] > [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 ウィンドウで [ポリシー (Policies)] > [プロトコル (Protocol)] > [BGP] へ移動します。
 - ステップ 3 次を右クリックします。[BGP アドレス ファミリ コンテキスト (BGP Address Family Context)]、次を選択します [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)] および次のステップを実行します：
 - 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) [ホストルートリークを有効化 (Enable Host Route Leak)] チェックボックスをオンにします。
 - c) [送信 (Submit)] をクリックします。
 - ステップ 4 登録手続きを開始するには、[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 のプロパティを構成する場合、IPv4 および IPv6 のために [BGP アドレス ファミリー コンテキスト ポリシー (BGP Address Family Context Policy)] を [アドレス ファミリごとの BGP コンテキストの追加 (BGP Context Per Address Families)] へ追加します。
 - ステップ 7 [送信 (Submit)] をクリックします。
-

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	<p>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。</p> <p>例 :</p> <pre>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</pre>	<p>このテンプレートは、テナント <code>bgp_t1</code> 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、<code>no host-rt-enable</code> コマンドを使用します。</p>

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。