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 （1 ページ）
- OSPF インターフェイス プロファイルの作成 （3 ページ）
- L3Out の SVI のカスタマイズ （9 ページ）
- Cisco フローティング L3Out について （21 ページ）

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。オプションとして、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。

障害（Fault）

次のようなシナリオでは障害が発生し、OSPF セッションがダウンします。

- KeyChain ポリシーの「Key」で提供されることになっているキー（キー文字列）で、事前共有キーが提供されていない

- KeyChain ポリシーでキー（キー文字列）が構成されていない
- 3DES や AES などのサポートされていない暗号化アルゴリズムを指定した。これらのアルゴリズムは、認証ではサポートされています。

キーの送信/受け入れライフタイムが期限切れになり、現用系のキーがなくなったためにOSPFセッションがダウンしても、障害は発生しません。OSPF インターフェイスの KeyChain の状態は「not-ready」（準備ができていない）状態になります。

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 MD5 または簡易認証を使用して OSPF インターフェイスプロファイルを構成するには、次の手順を実行します。

a) **[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）]）。

b) **[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。

c) **[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。

d) [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。
- **[簡易（Simple）]**：以前に指定した認証キーである **OSPFv2 認証キー**を指定する必要があります。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。
- **[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 8 KeyChain 認証を使用して OSPF インターフェイスプロファイルを構成するには、次の手順を実行します。

a) **[OSPFv2 キーチェーン ポリシー（OSPFv2 KeyChain Policy）]** フィールドで、OSPFv2 KeyChain 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。

（注）
認証は、従来の方法（*OSPFv2* 認証タイプ - *MD5*認証/簡易認証 ）を指定するか、 *OSPFv2* キーチェーンポリシーを指定して、構成できます。

キーチェーンポリシーを構成すると、選択済みの認証タイプは上書きされます。

ステップ 9 （OSPFv3 にのみ適用可能） **[OSPFv3 IPsec ポリシー（OSPFv3 IPsec Policy）]**：OSPFv3 IPsec ポリシーを L3Out インターフェイスに関連付けるには、ドロップダウン リストから IPsec ポリシーを選択します。OSPFv3 IPsec ポリシーの作成については、「OSPF IPsec ポリシーの作成」の手順を参照してください。

次のタスク

OSPFv2 KeyChain のローテーションを指定するには、キー ポリシーの作成 （6 ページ） を参照してください。

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 （3 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（Tenant）] > [すべてのテナント（All Tenants）]** をクリックします。

ステップ 2 [作業（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、 **[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 4 **[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間（**Key acceptライフタイムの開始時間**）] フィールドで、 **YYYY-MM--DD-HH-MM-SS** 形式で開始時間を指定します。

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。

このフィールドは、OSPFv3 IPSec ポリシーでは適用されません。

（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。

このフィールドは、OSPFv3 IPSec ポリシーでは適用されません。

ステップ 5 [Submit] をクリックします。

OSPF IPsec ポリシーの作成

Cisco APIC リリース 6.1(2) 以降では、OSPFv3 セッションの暗号化と認証がサポートされています。使用する手順

（注） OSPFv3 はインフラ テナントではサポートされていません。 OSPF IPSec ポリシーのサポートは、ユーザ テナントのみを対象としています。

始める前に

キーチェーン ポリシーを作成します。

手順

ステップ 1 メニュー バーで、**[テナント（Tenants）]**> テナント名 をクリックします。

ステップ 2 左側の[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 IPSec]**をクリックします。

ステップ 3 **[IPSec 認証ポリシーの作成（Create IPSec Authentication Policy）**] ウィンドウで、次の詳細を入力します。

- [名前（Name）] : IPSec ポリシーの名前。

- [説明（Description）]：この IPSec ポリシーの説明。
- [IP セキュリティ プロトコル（IP Security Protocol）]：認証ヘッダー（AH）またはカプセル化セキュリティ ペイロード（ESP）のいずれかを選択します。

  [認証ヘッダー（Authentication Header）] を選択した場合は、認証のみがサポートされます。[ESP] を選択した場合、使用可能なオプションは認証、暗号化、または両方（認証と暗号化）です。

  サポートされているキーチェーンアルゴリズム：

  - 認証ヘッダー：MD5（デフォルト）、HMAC-SHA1。
  - カプセル化セキュリティ プロトコル：認証用：HMAC-SHA1。暗号化の場合：3DES（デフォルト）、AES。

    （注）
    アルゴリズムを選択しないか、サポートされていないアルゴリズムを選択すると、デフォルトが自動的に選択されます。

- [セキュリティ パラメータ インデックス（Security Parameter Index）]：IPSec プロトコルを作成するための一意の値。ドロップダウン リストから値を選択します。サポートされている範囲は 256 ～ 4294967295 です。
- [OSPFv3 認証キーチェーン（OSPFv3 Authentication Keychain）]：ドロップダウン リストからキーチェーン値を選択します。[IP セキュリティ プロトコル（IP Security Protocol）] フィールドで AH オプションを選択した場合、このフィールドは必須です。フィールドを空白のままにすると、障害が生じます。

  障害が実際に生じたかを確認するには、[OSPF インターフェイス プロファイル（OSPF Interface Profile）] 画面に移動し、**[障害（Faults）]** タブをクリックします。

- [OSPFv3 暗号化キーチェーン（OSPFv3 Encryption Keychain）]：ドロップダウン リストからキーチェーン値を選択します。**[IP セキュリティ プロトコル（IP Security Protocol）]** フィールドで [AH] オプションを選択した場合、このフィールドは適用外になります。[IP セキュリティ プロトコル（IP Security Protocol）] フィールドで [ESP] オプションを選択した場合は、**[認証キーチェーン（Authentication Keychain）]** フィールドまたは**[暗号化キーチェーン（Encryption Keychain）]** フィールドに値を入力する必要があります。

ステップ 4 **[送信（Submit）]** をクリックします。

SSH またはコンソール セッション上のスイッチで **show ipv6 ospfv3 interface** *interface-id* コマンドを使用すれば、作成された IPSec ポリシーを確認できます。

ステップ 5 作成した OSPFv3 IPSec ポリシーを L3Out インターフェイスに関連付けるには、OSPF インターフェイス プロファイルの作成の手順のステップ 9 を参照してください。

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 *1 :* ローカル範囲のカプセル化と *1* 個のレイヤ *3* アウト

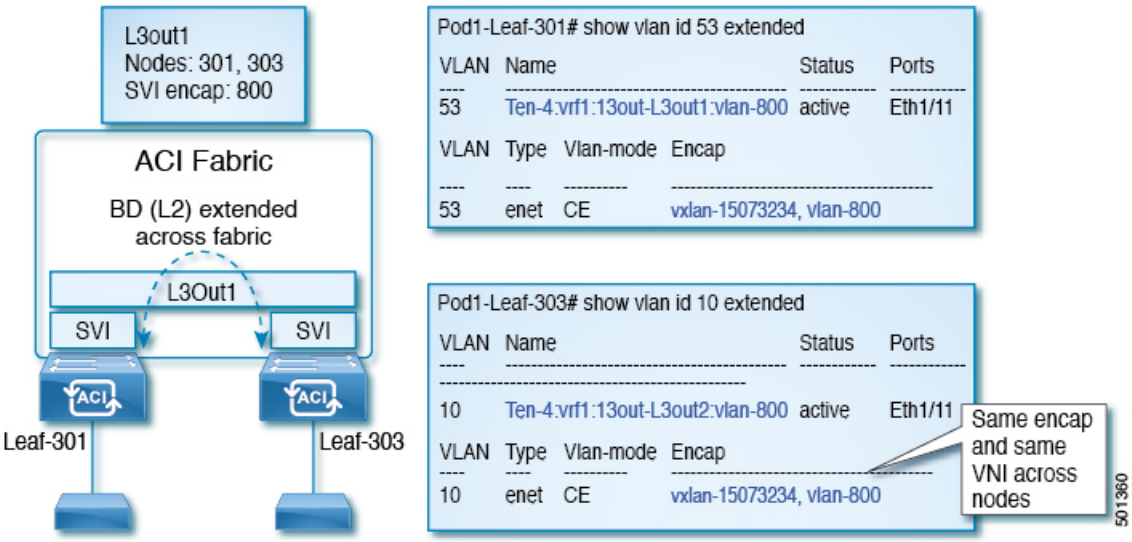
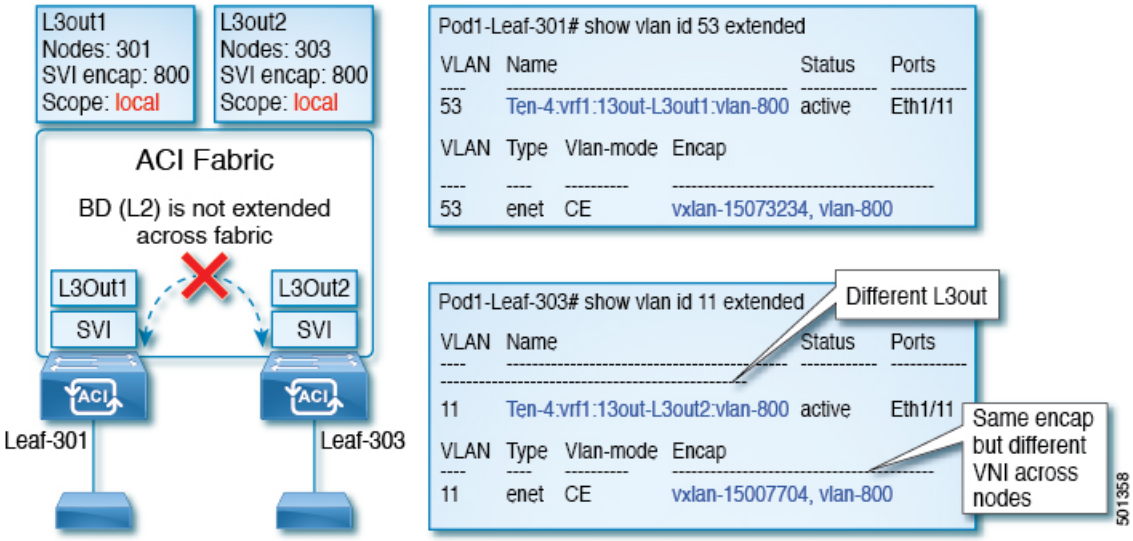


図 *2*: ローカル範囲のカプセル化と *2* 個のレイヤ *3* アウト

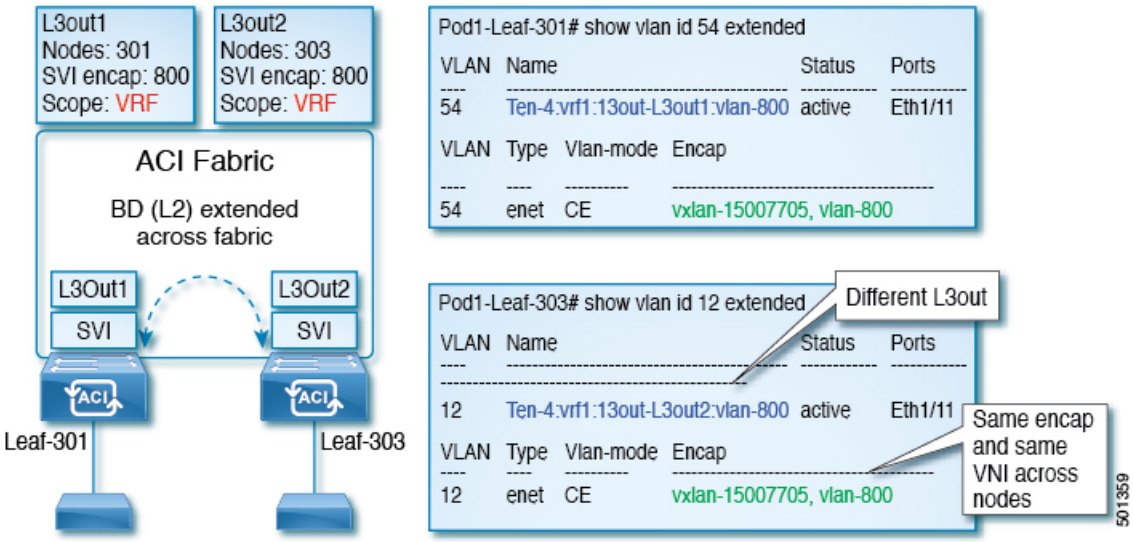


Cisco APIC リリース 2.3 以降、同じ外部カプセル化（SVI）を使用して、2 個以上のレイヤ 3 アウトを展開する場合の動作を選択できるようになりました。

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 *3*: *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 *1*: 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。

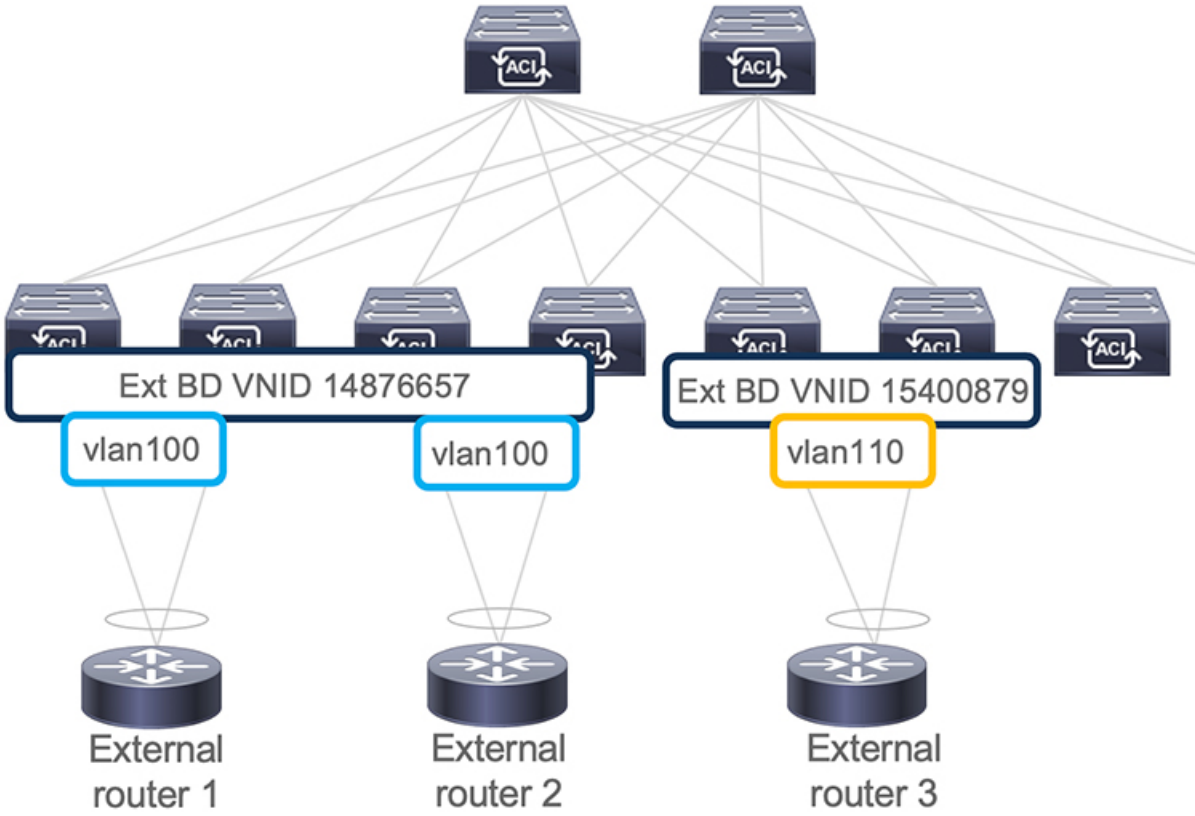
デフォルト値は **Local** です。

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

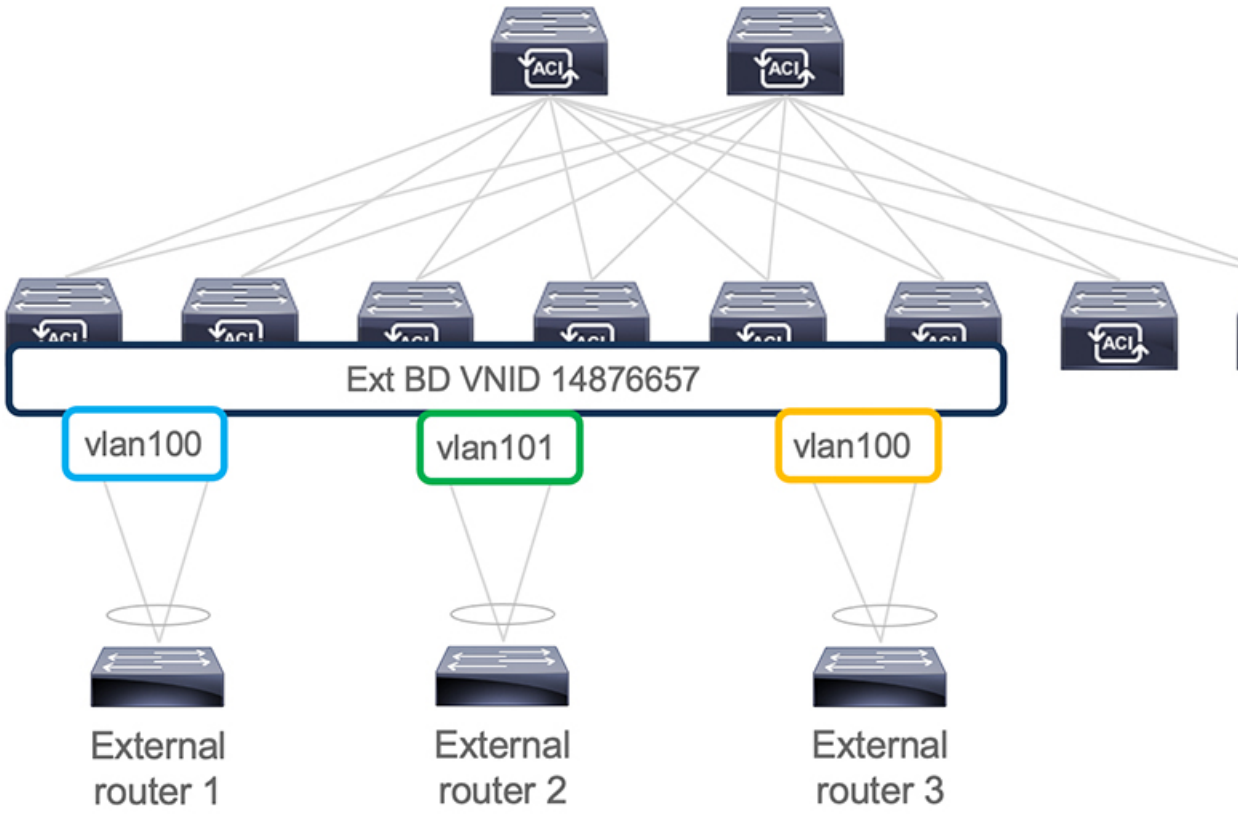
同じカプセル化 VLAN を使用する異なるリーフ スイッチ上の SVI インターフェイスで L3Out が設定されている場合、SVI VLAN は同じ VXLAN ネットワーク識別子（VNID）にマッピングされます。これにより、ファブリック全体に単一のブリッジ ドメイン（外部ブリッジ ドメイン）とブロードキャスト ドメインが形成されます。次の図に示すように、異なる VLAN で設定された SVI インターフェイスは、別個の外部ブリッジ ドメインを形成します。リリース 5.2(3) より前は、異なるスイッチ上に異なるカプセル化 VLAN を持つ単一の外部ブリッジ ドメインを作成することはできませんでした。

図 *4 :* 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。

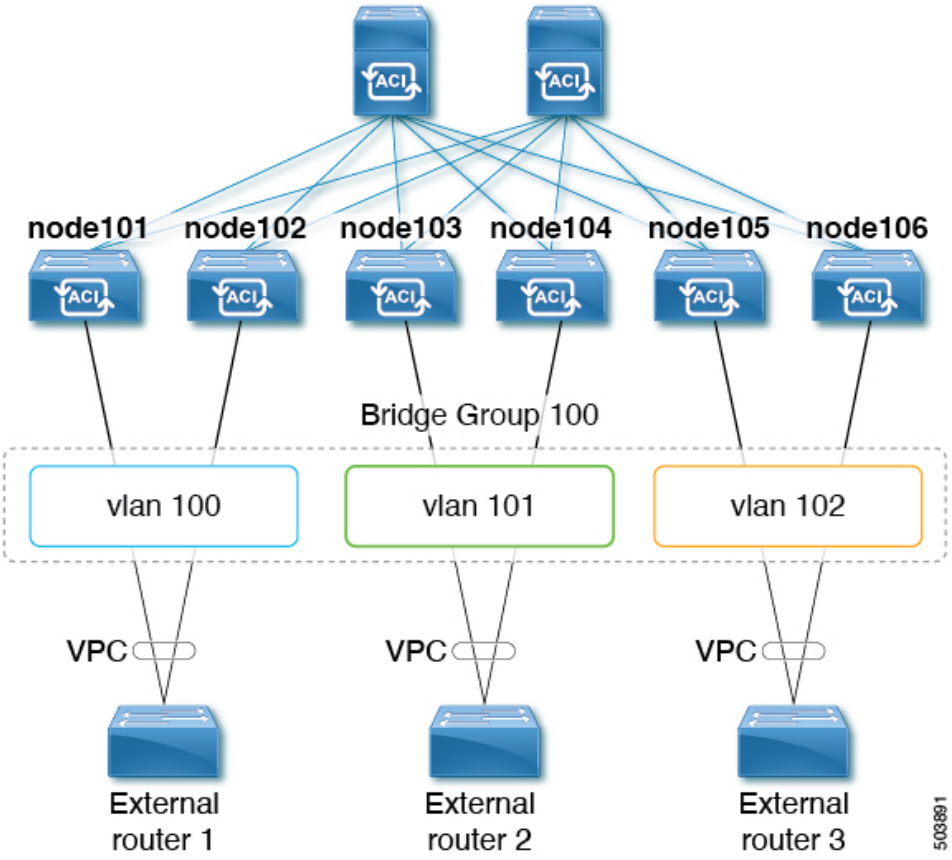
図 *5*：異なるカプセル化で外部ブリッジ ドメインに関連付けられた単一の *VNID*（*ACI 5.2(3)* 以降のリリース）。



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 （11 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 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 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 *2: 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

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。