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 （1 ページ）
- SR-MPLS ハンドオフの ACI 実装について （7 ページ）
- SR-MPLS 設定モデルについて （16 ページ）
- 注意事項と制約事項 （21 ページ）
- GUI を使用した SR-MPLS インフラ L3Out の設定 （28 ページ）
- GUI を使用した SR-MPLS VRF L3Out の設定 （37 ページ）
- GUI を使用した SR-MPLS カスタム QoS ポリシーの作成 （40 ページ）
- MPLS 統計情報の表示 （42 ページ）
- SR-MPLS グローバル ブロック（GB）の設定 （45 ページ）
- IP ハンドオフ設定から SR ハンドオフ設定への移行 （47 ページ）
- ループ防止のための BGP ドメインパス機能について （55 ページ）

ACI ハンドオフについて

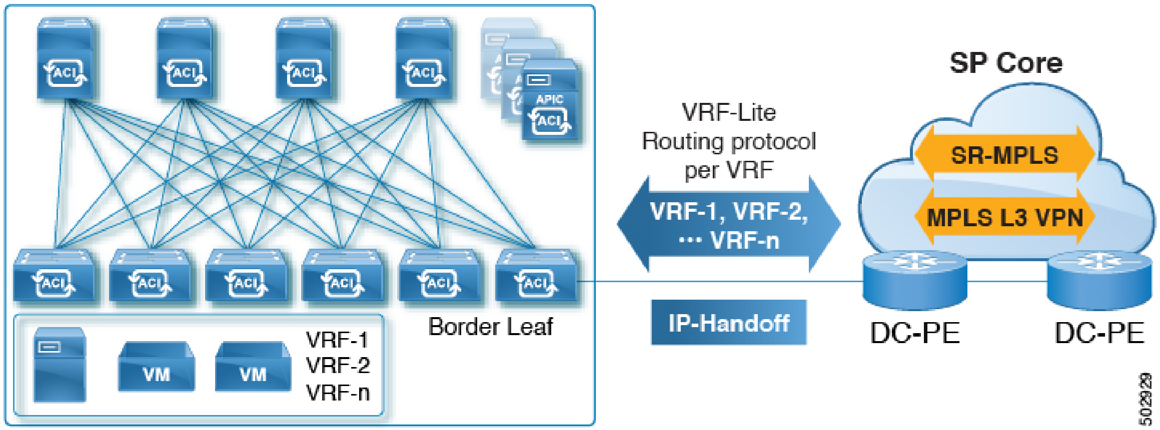
ここでは、IP ハンドオフを使用したリリース 5.0(1) より前のリリースでの ACI ハンドオフの処理方法と、リリース 5.0(1) 以降の SR-MPLS ハンドオフを使用した処理方法について説明します。Cisco APICCisco APIC

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 1 : *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。

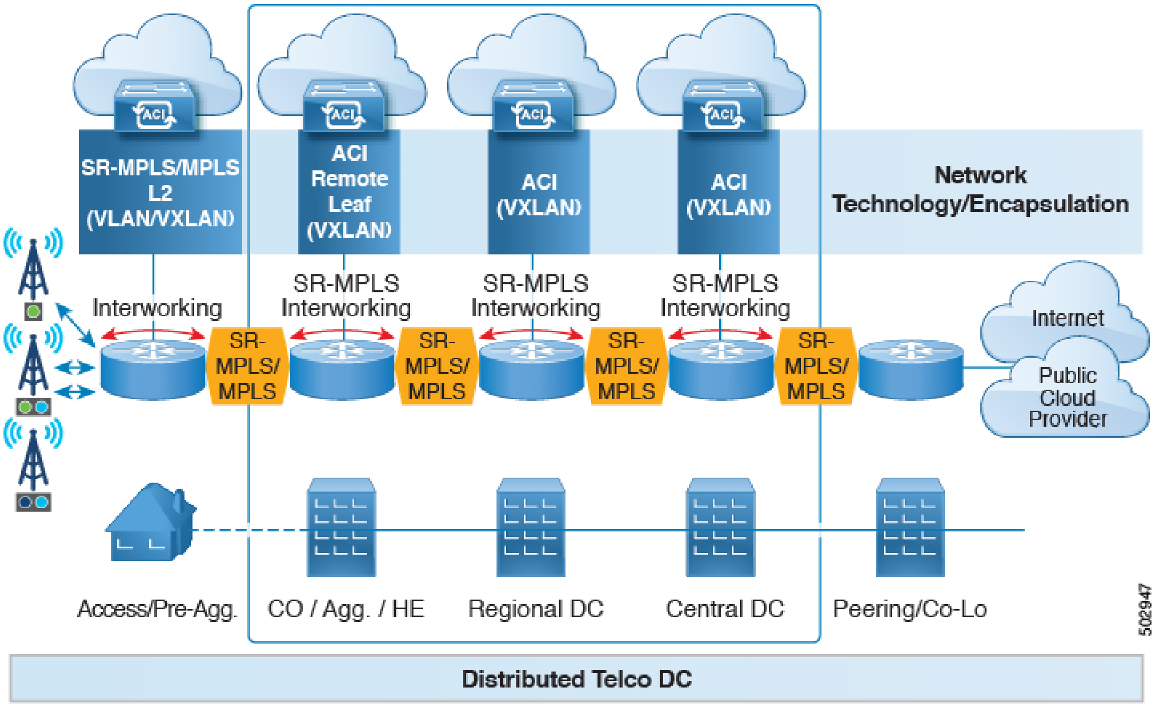
次のシナリオは、SR-MPLS を使用した DC-PE への ACI ハンドオフの設定がどのように役立つかを示しています。

- 統合セグメント ルーティングの転送 （3 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 （3 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 （4 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 （5 ページ）
• SR または MPLS による DC およびトランスポート QoS （6 ページ）

統合セグメント ルーティングの転送

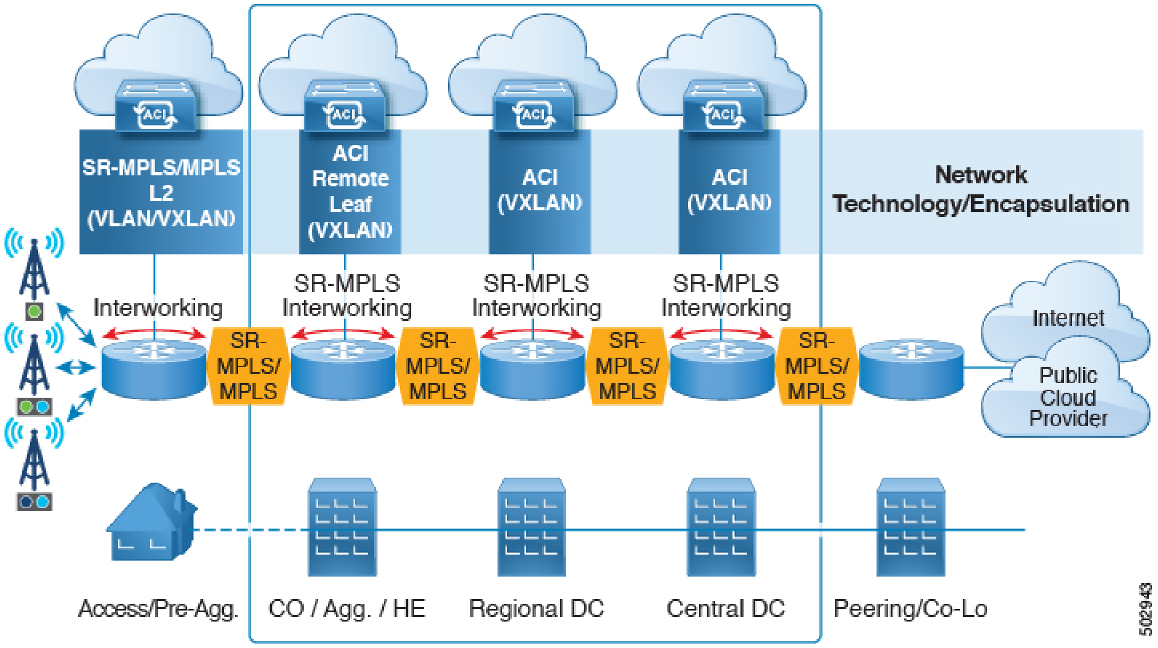
次のシナリオでは、異なる ACI DC ネットワークを相互接続するための統合 SR または MPLS トランスポート ネットワークの導入について説明します。VXLAN から SR-MPLS へのハンドオフは、ACI ネットワークと DC-PE ルータ間の各ロケーションで活用されます。



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

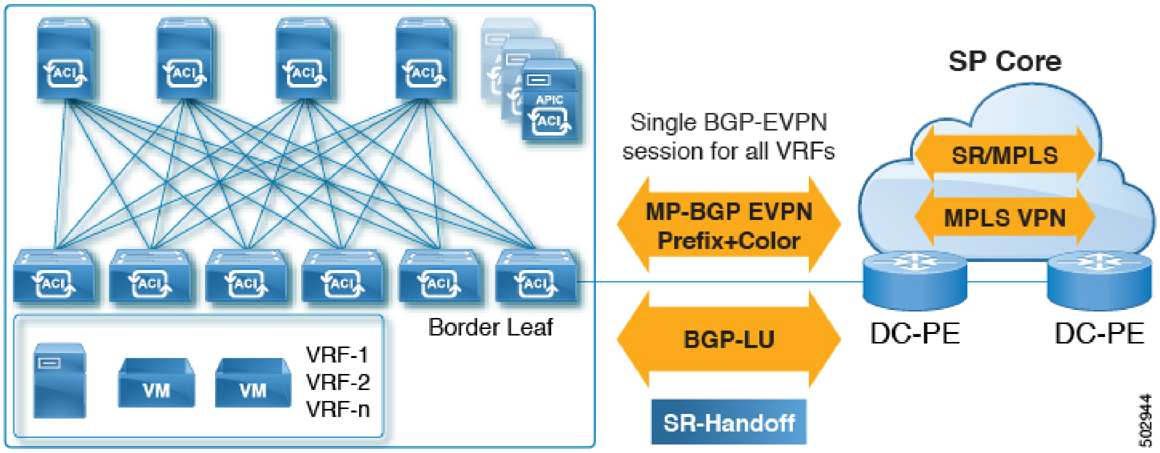
次のシナリオでは、DC-to-DC フローは VXLAN ではなくセグメント ルーティングを使用してカプセル化されます。



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。

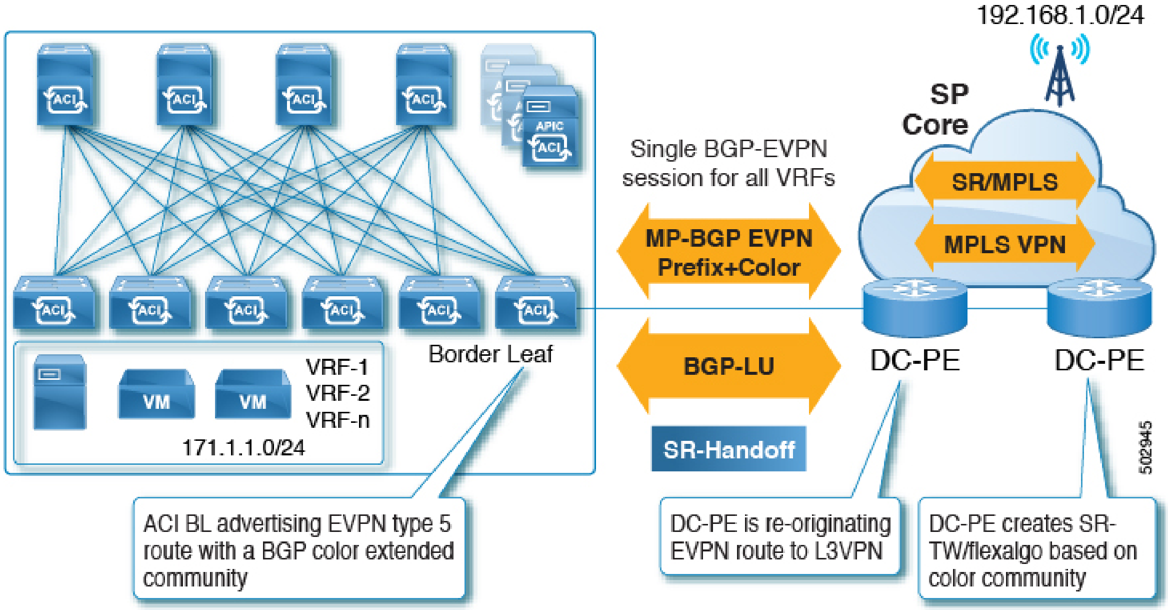


SR ハンドオフでは、VRF 単位のコントロール プレーンおよびデータ プレーン セッションの代わりに単一のコントロール プレーンおよびデータ プレーン セッションが使用され、Cisco ACI ファブリックから SP コアへの統合 SR トランスポートが使用されます。BGP ラベル ユニ

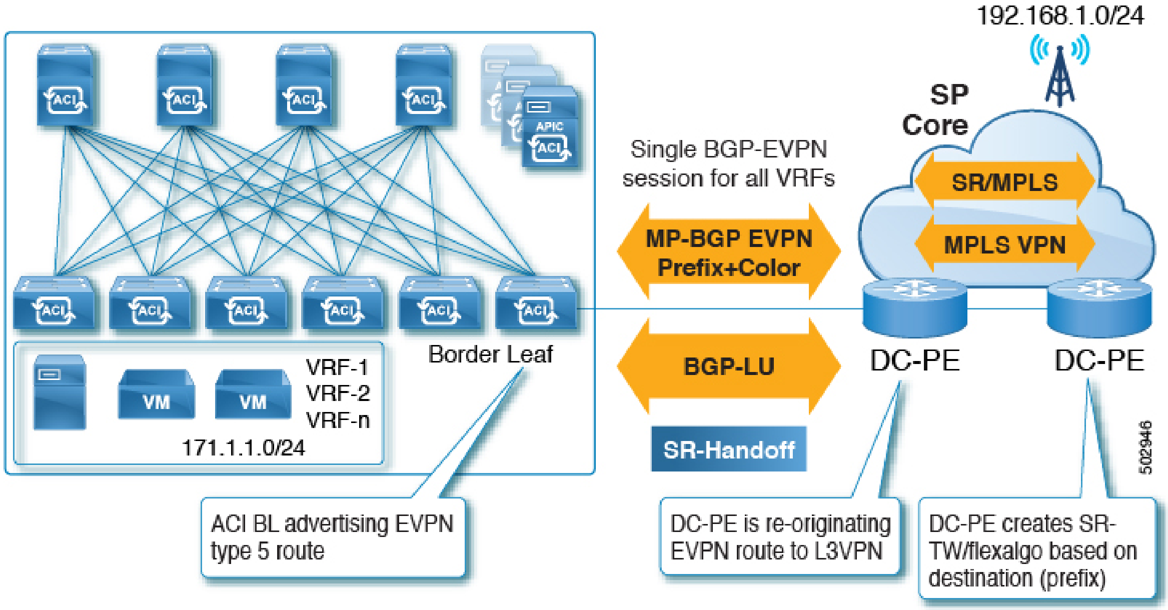
キャスト（BGP LU）アドレスファミリは、アンダーレイ ラベル交換に使用されます。MP-BGP EVPN アドレス ファミリは、VRF 情報ごとにプレフィックスと MPLS ラベルを伝送します。

[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。



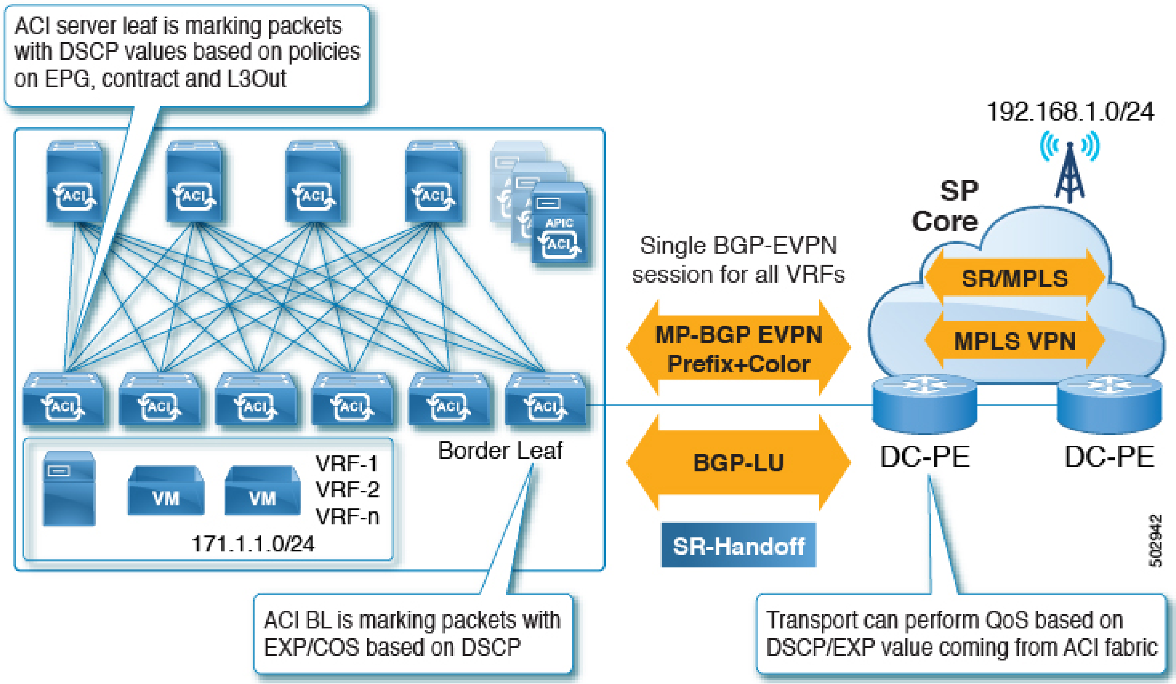
同様に、次の図に示すように、ACI 境界リーフ スイッチから EVPN タイプ 5 プレフィックスをアドバタイズでき、DC-PE は宛先プレフィックスに基づいて SR-TE または Flex Algo ルーティング ポリシーを作成できます。



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。

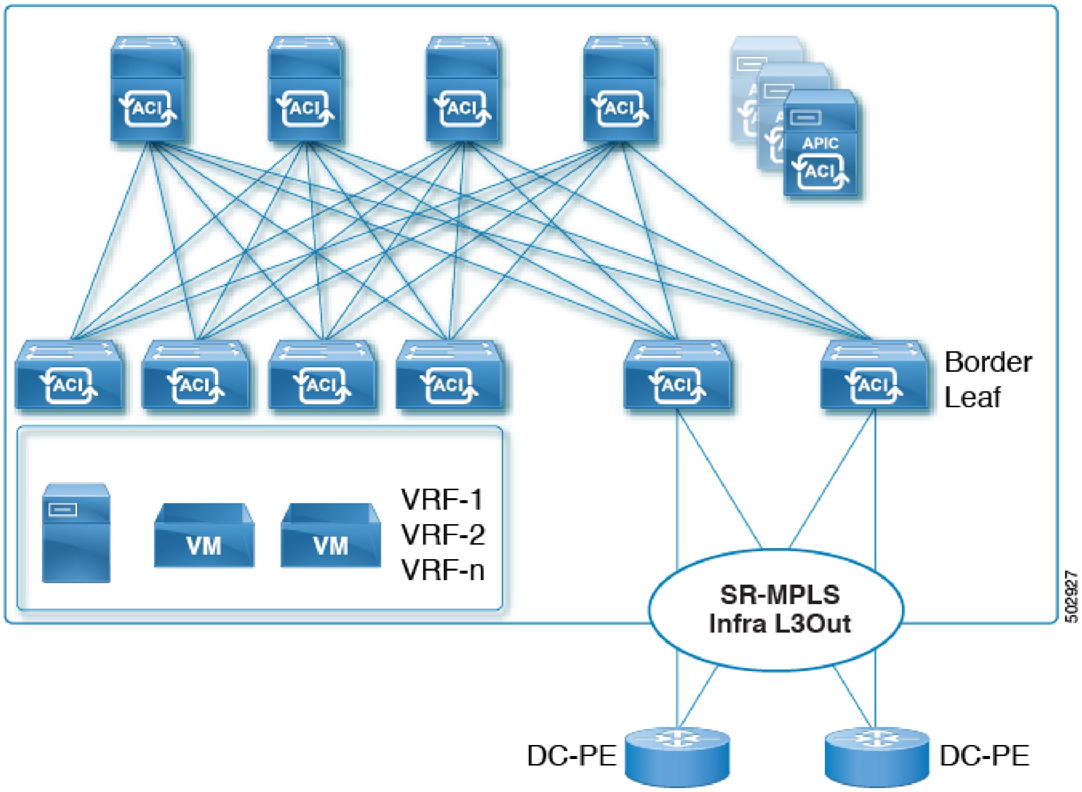
SR-MPLS ハンドオフの ACI 実装について

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 は 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 2 : *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。

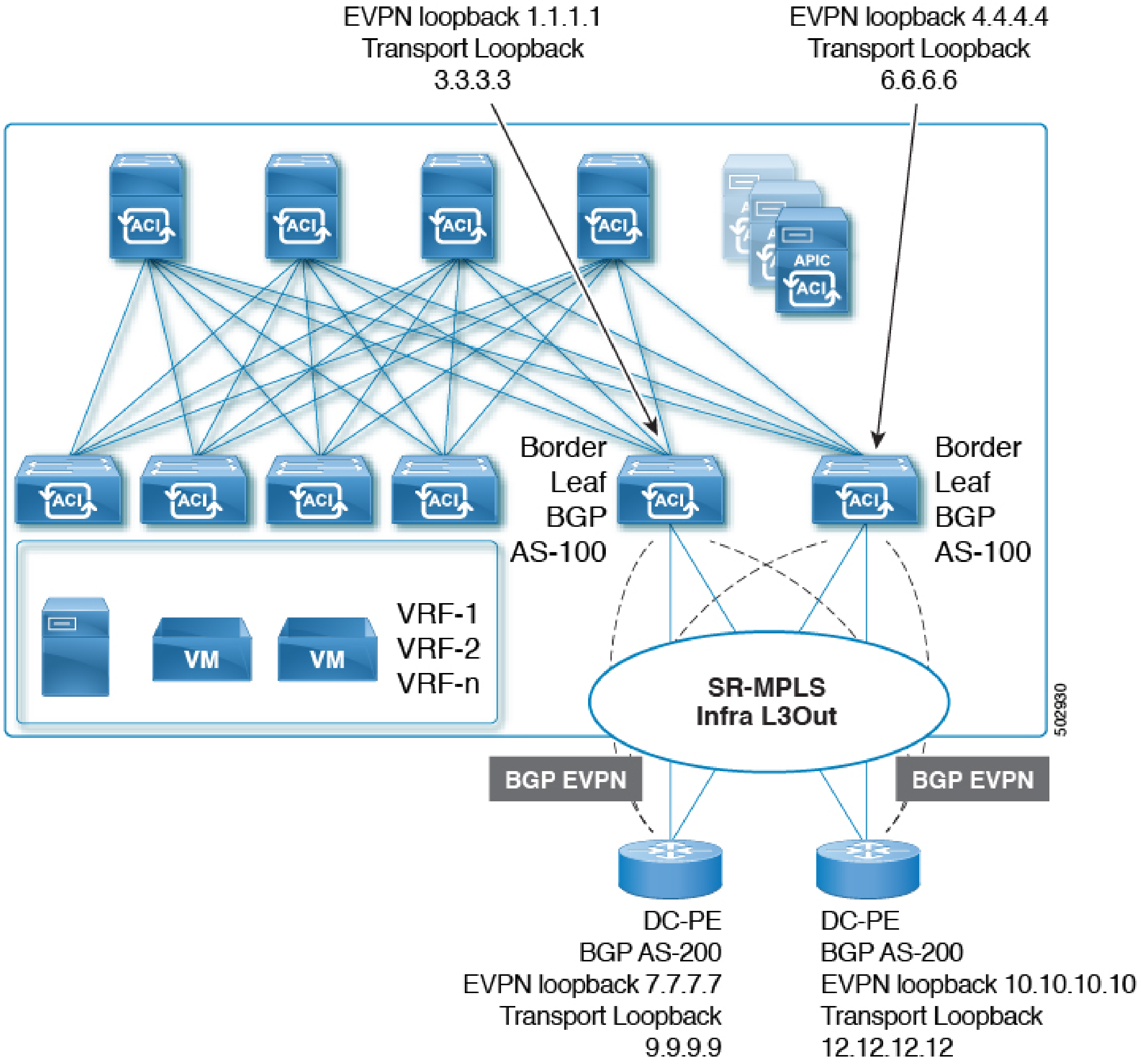
SR-MPLS インフラ L3Out の設定手順については、GUI を使用した SR-MPLS インフラ L3Out の設定 （28 ページ）を参照してください。

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。

- ACI 境界リーフ スイッチと DC-PE 間の MP-BGP EVPN セッション （8 ページ）
- BGP EVPN セッションのマルチホップ BFD （10 ページ）
- 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） （10 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 （11 ページ）

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。

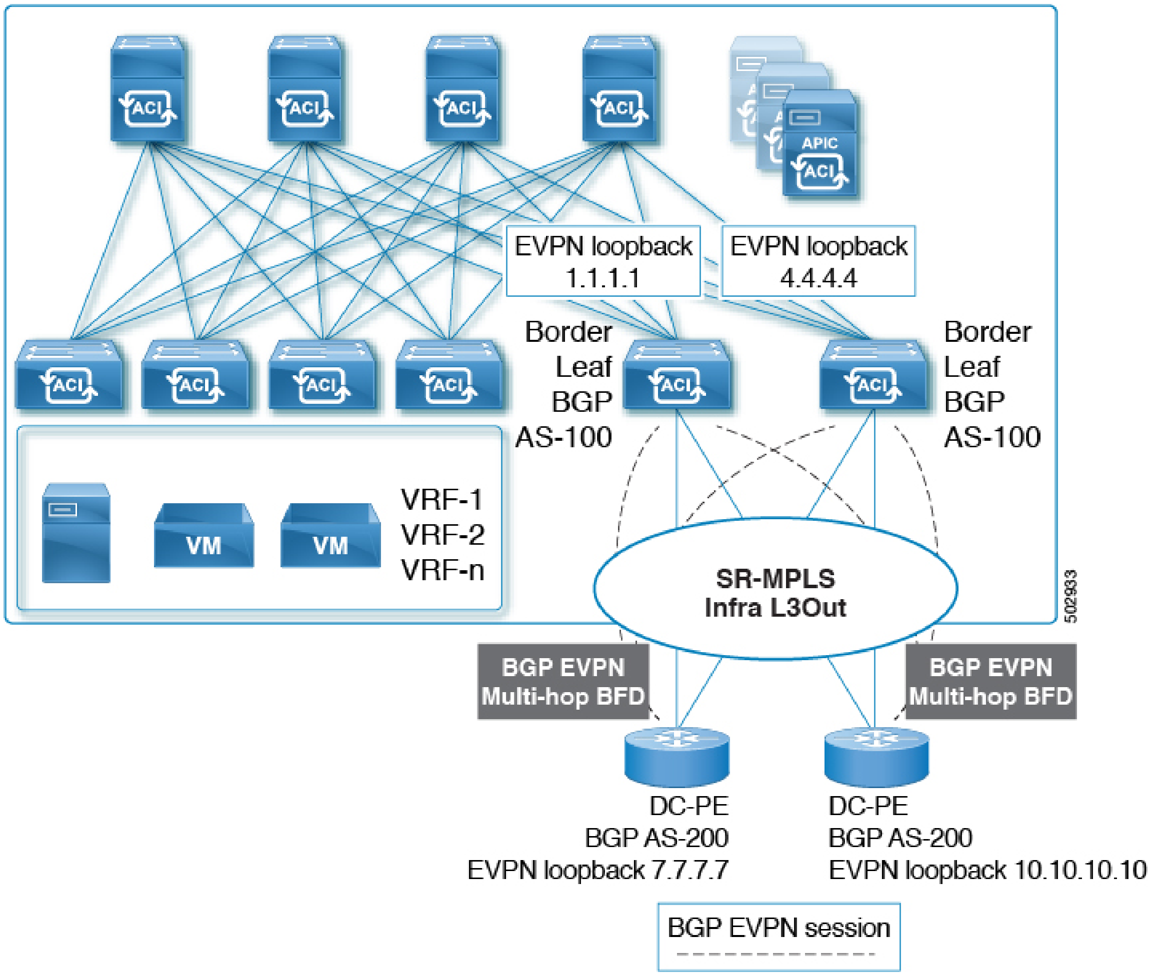
- BGP ラベル付きユニキャスト アドレス ファミリを使用したトランスポート ループバックのラベル アドバタイズメント。
- SR-MPLS インフラ VRF の境界リーフ スイッチ上の一意のルータ ID。
- ルータ ID は、BGP-EVPN ループバックおよびトランスポート ループバック アドレスとは異なる必要があります。

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 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ることに注意してください。

BGP EVPN セッションのマルチホップ BFD

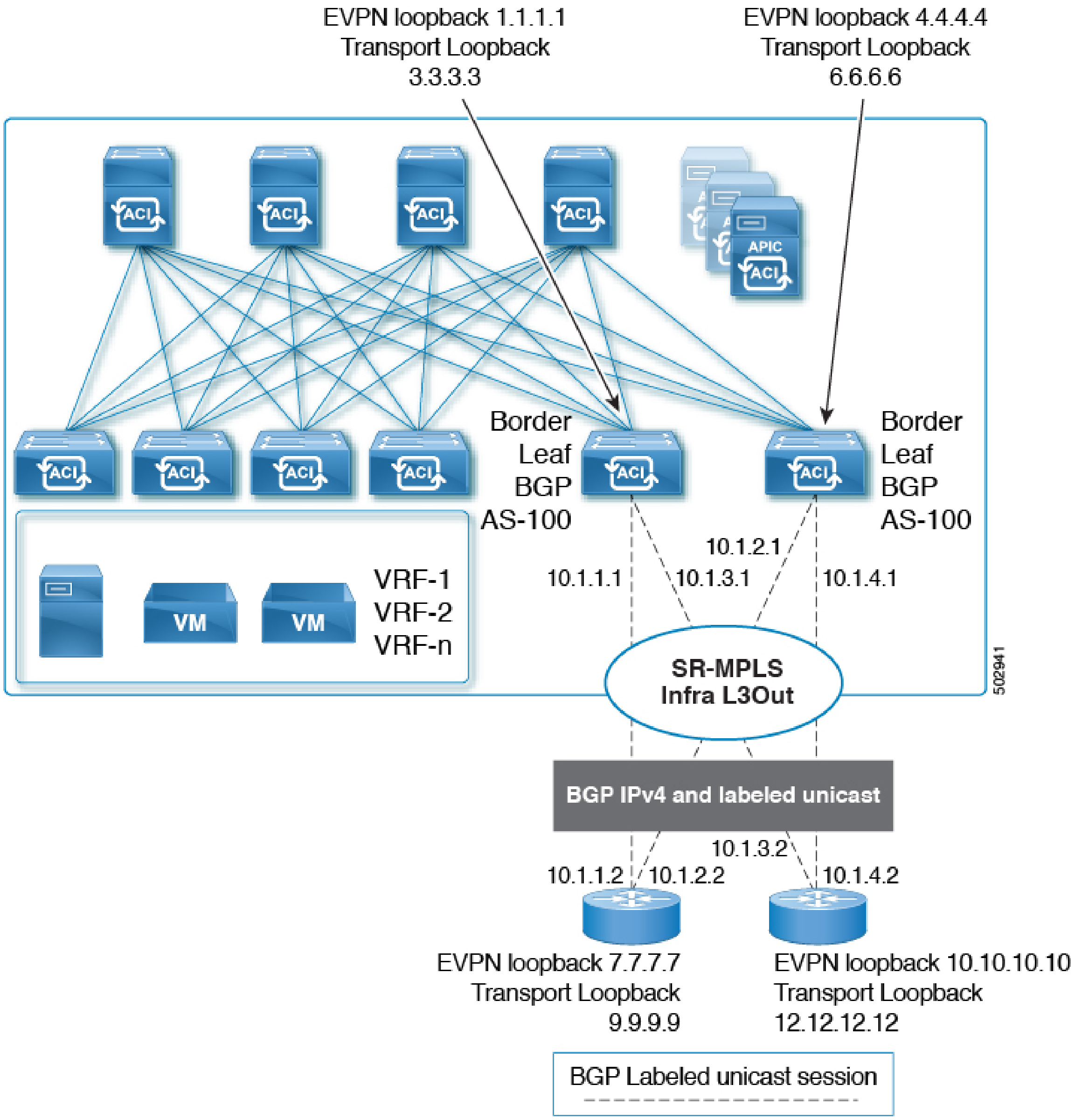
リリース5.0(1) から、次の図に示すように、マルチホップ BFD のサポートが可能になりました。この場合、EVPN ループバック間にマルチホップ BFD EVPN セッションを設定できます。



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を変更できることに注意してください。

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、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。

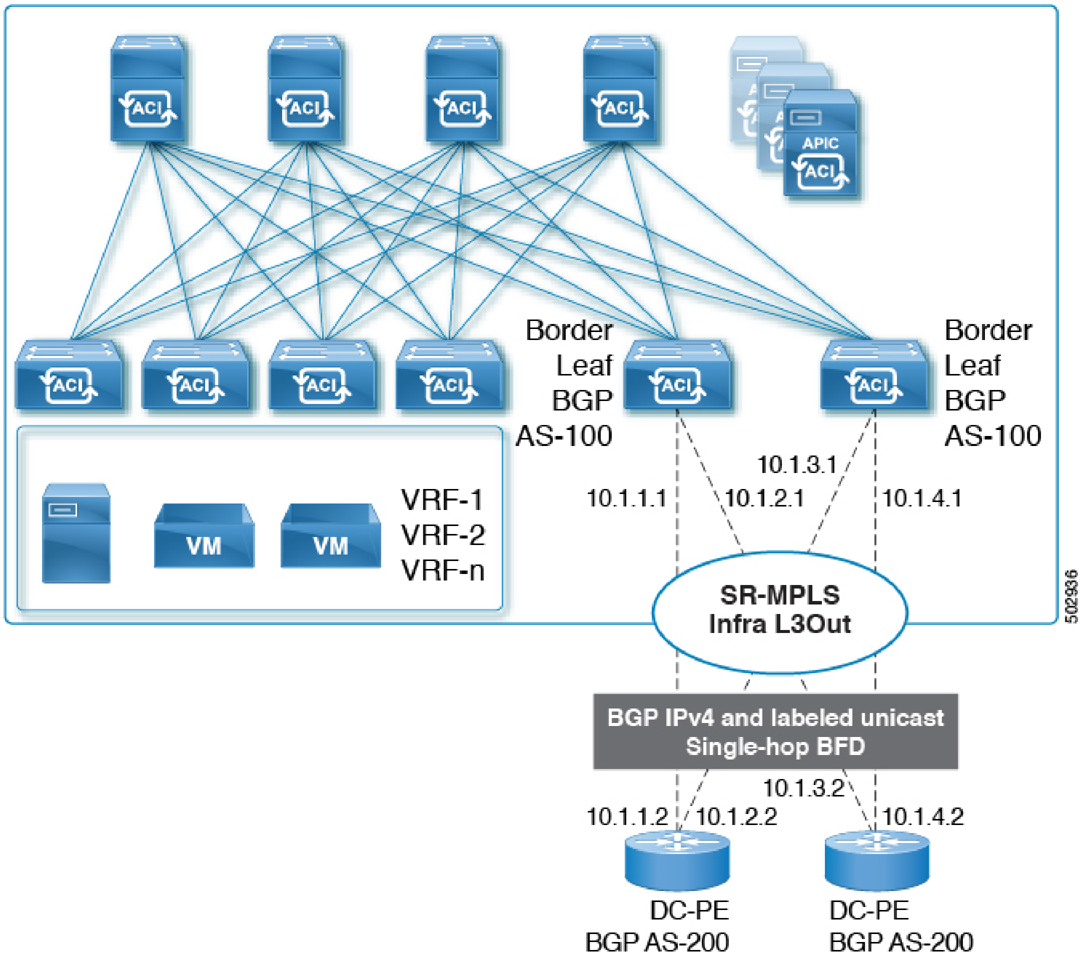


BGP IPv4アドレス ファミリは EVPN ループバックを自動的にアドバタイズし、BGP ラベル付きユニキャスト アドレス ファミリは SR-MPLS ラベルを使用して SR トランスポート ループバックを自動的にアドバタイズします。

繰り返しますが、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。

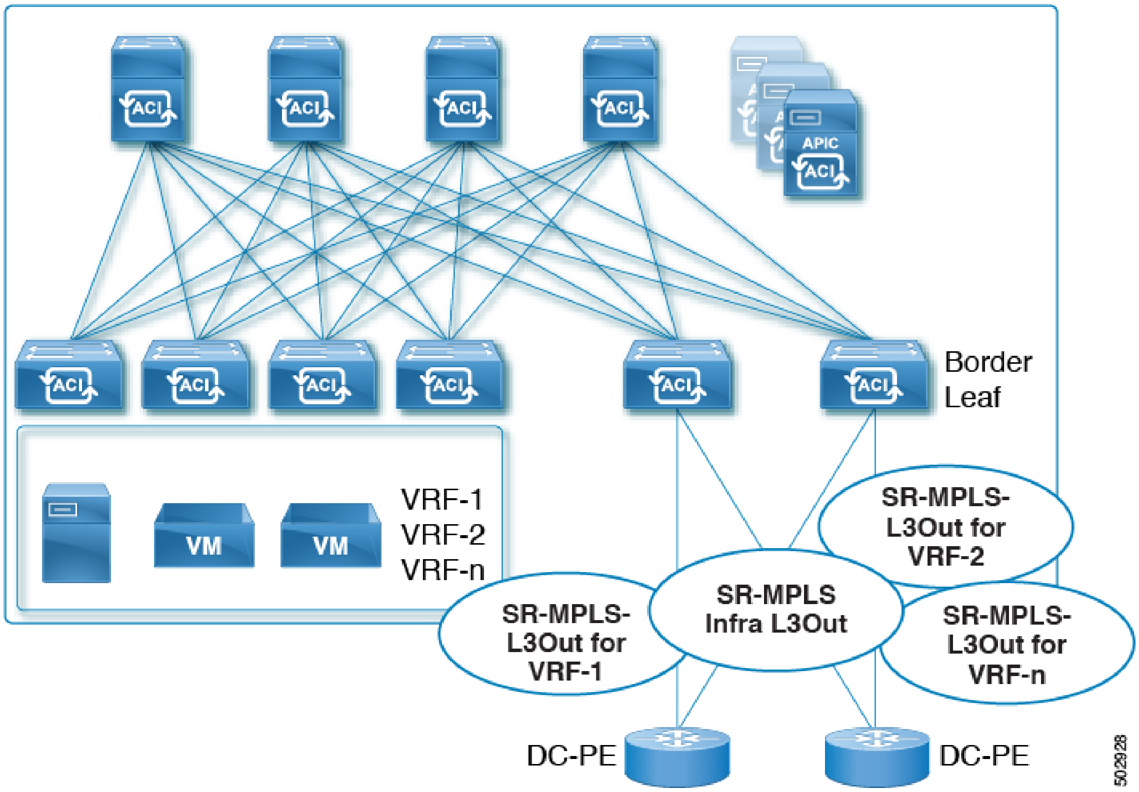


ACI 境界リーフ スイッチと DC-PE 間の BGP EVPN セッションでは、最小タイマーが 50 ミリ秒、検出乗数が 3 のシングルホップ BFD がサポートされます。要件に基づいてこのタイマー値を変更できることに注意してください。

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 3 : *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 （37 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 4 : 入力 *QoS*

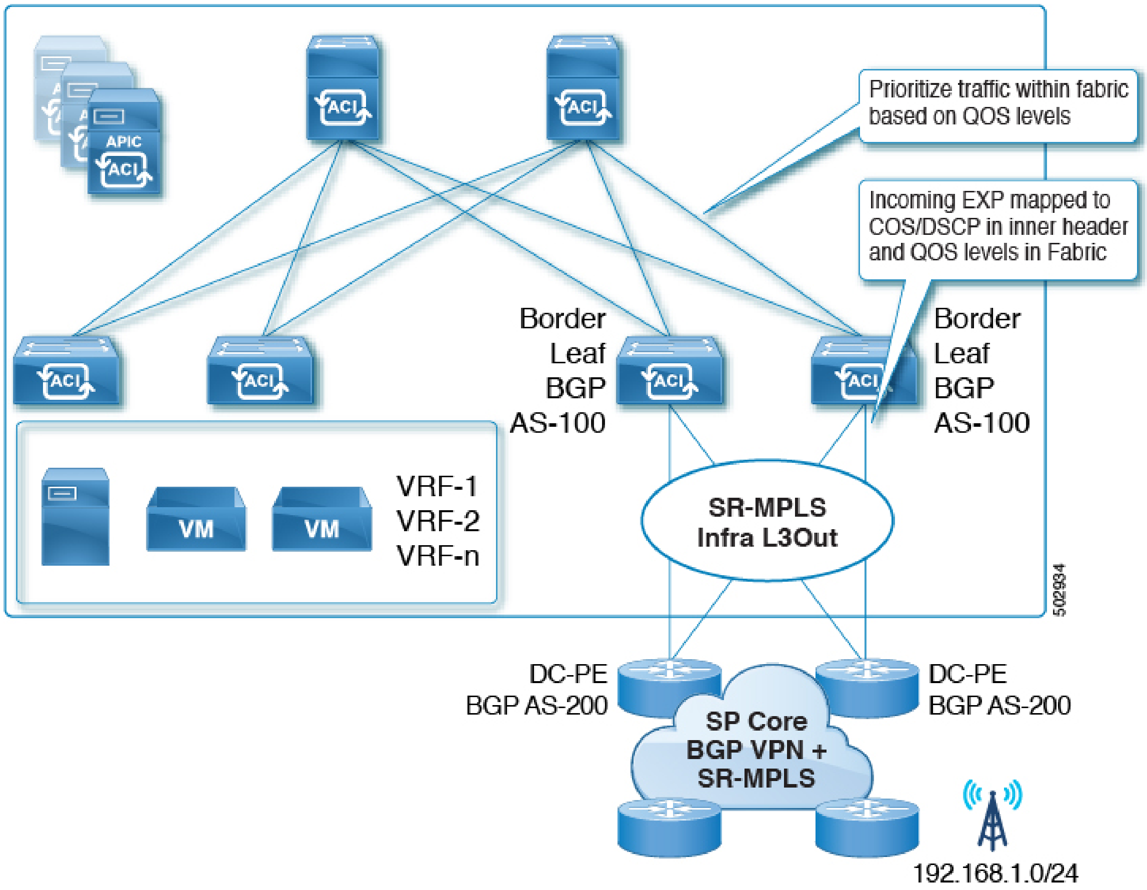
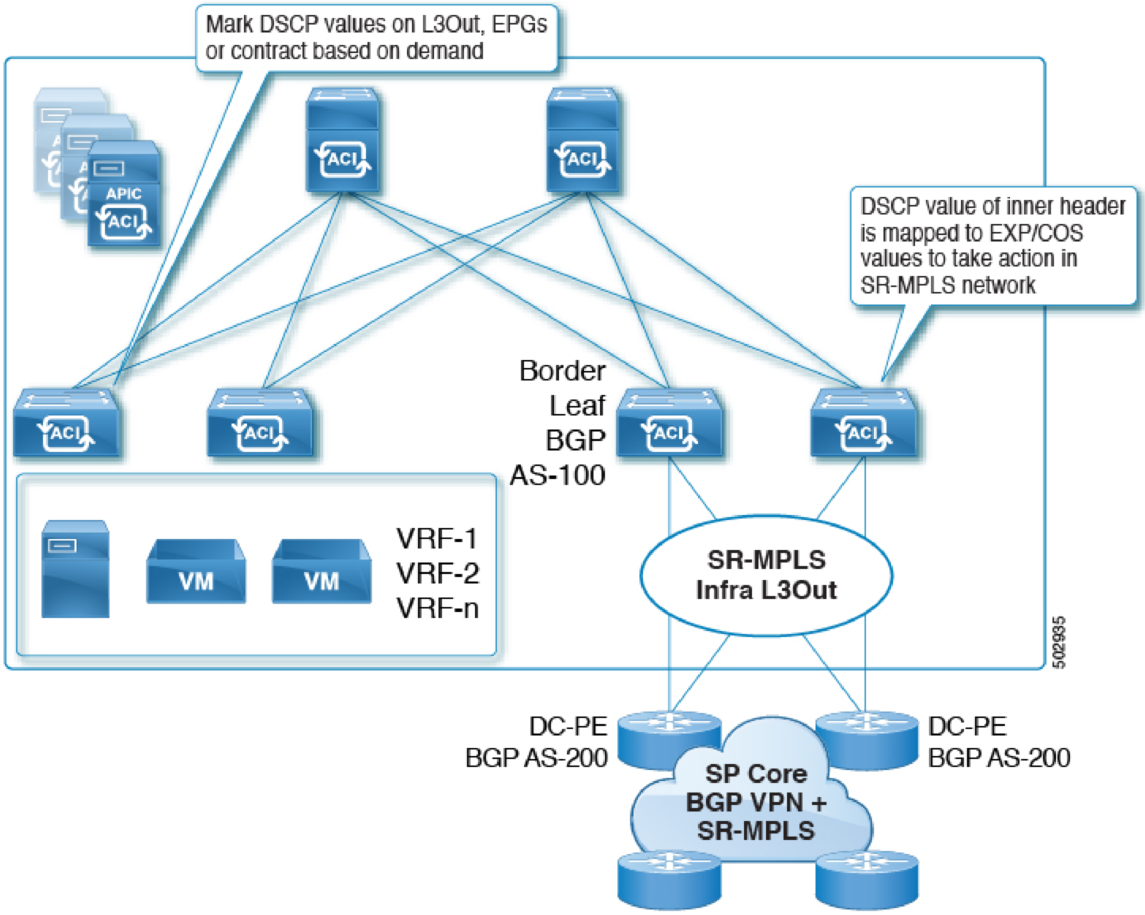

APIC
ACI
Prioritize traffic within fabric based on QOS levels
Incoming EXP mapped to COS/DSCP in inner header and QOS levels in Fabric
Border Leaf BGP AS-100
Border Leaf BGP AS-100
VM
VM
VRF-1
VRF-2
VRF-n
SR-MPLS Infra L3Out
DC-PE BGP AS-200
DC-PE BGP AS-200
SP Core BGP VPN + SR-MPLS
192.168.1.0/24
502934

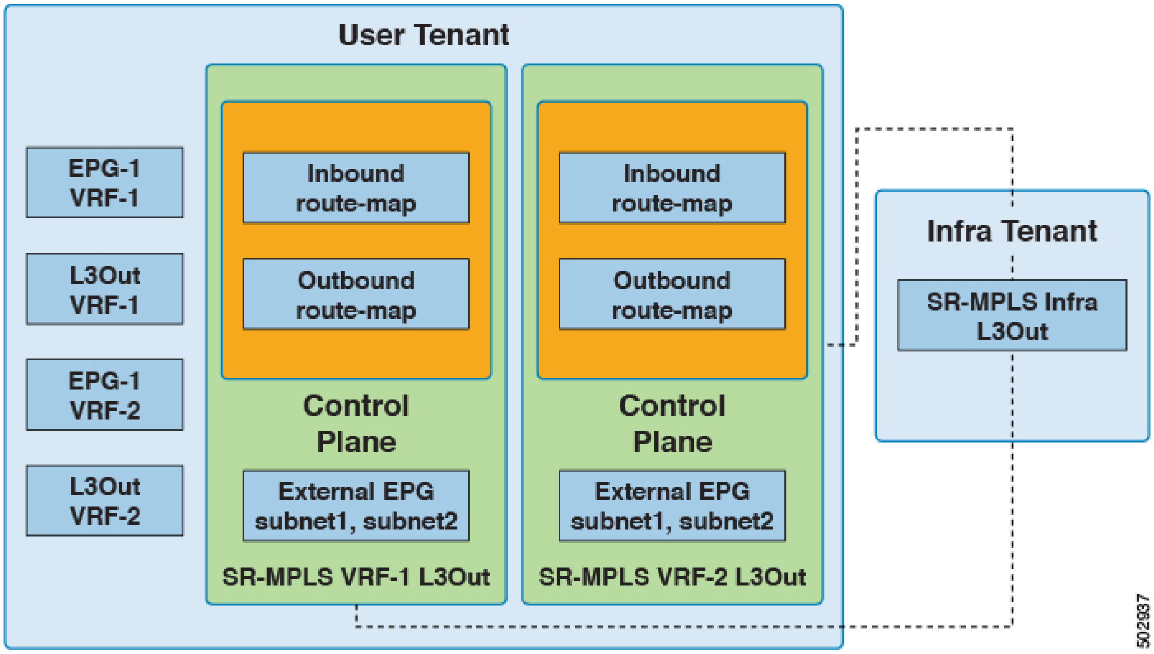
図 5 : 入力 *QoS*



GUI を使用した SR-MPLS カスタム QoS ポリシーの作成（40 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 （7 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 （12 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。

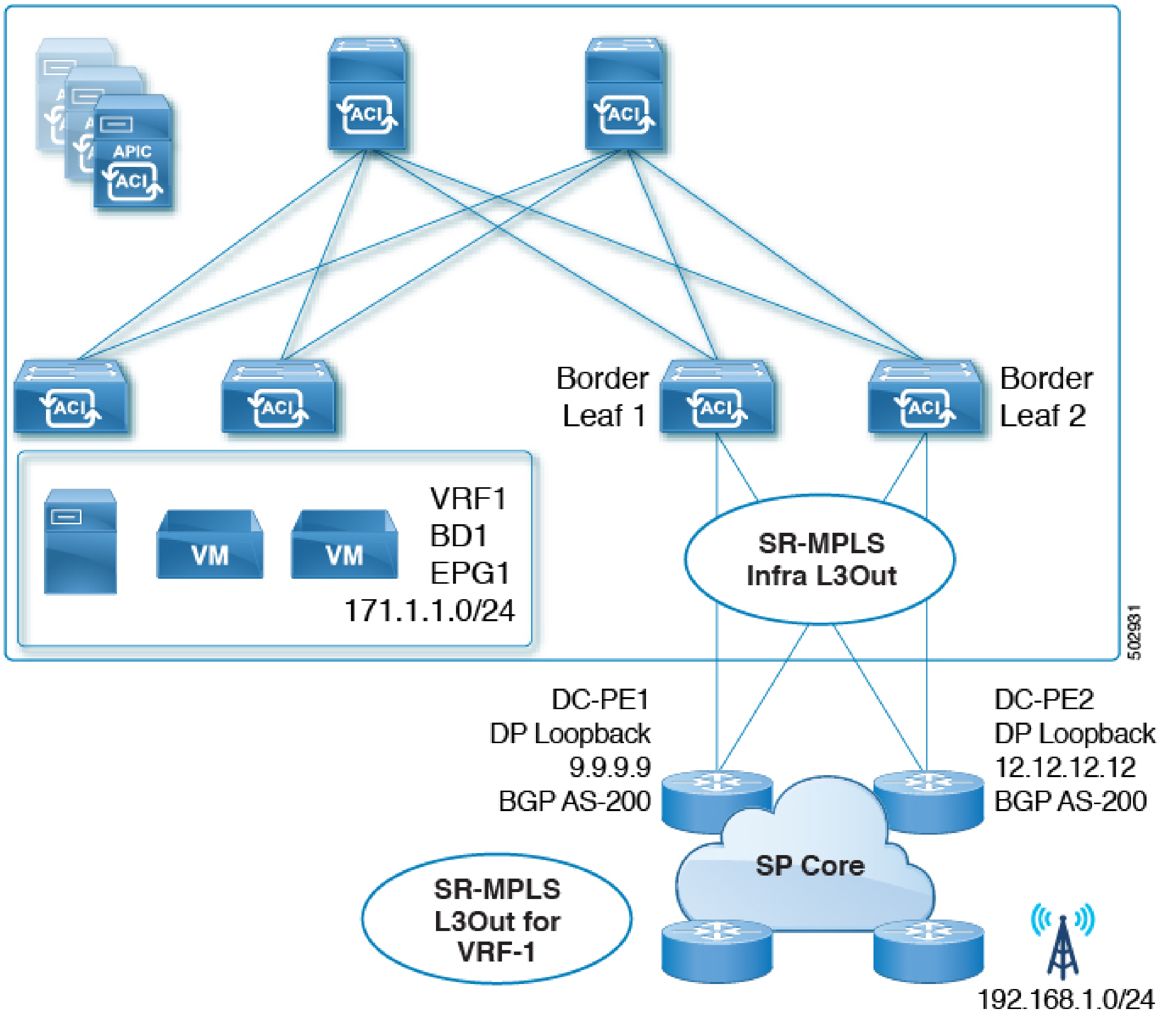
SR-MPLS VRF L3Out 内で、外部 EPG と、データ プレーンに使用される該当の外部 EPG 内のサブネットも設定します。これらのサブネットは、ACI セキュリティ ポリシーを適用するために使用されます。外部 EPG サブネットは、フラグを使用して別の VRF のプレフィックスをリークするためにも使用されます。外部 EPG サブネットでルート リークとセキュリティ フラグを有効にすると、そのサブネットは別の VRF にリークされる可能性があります。集約フラグを使用して外部 EPG サブネットを設定し、プレフィックスを別の VRF にリークすることもできます。この場合、リーフ スイッチ 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。

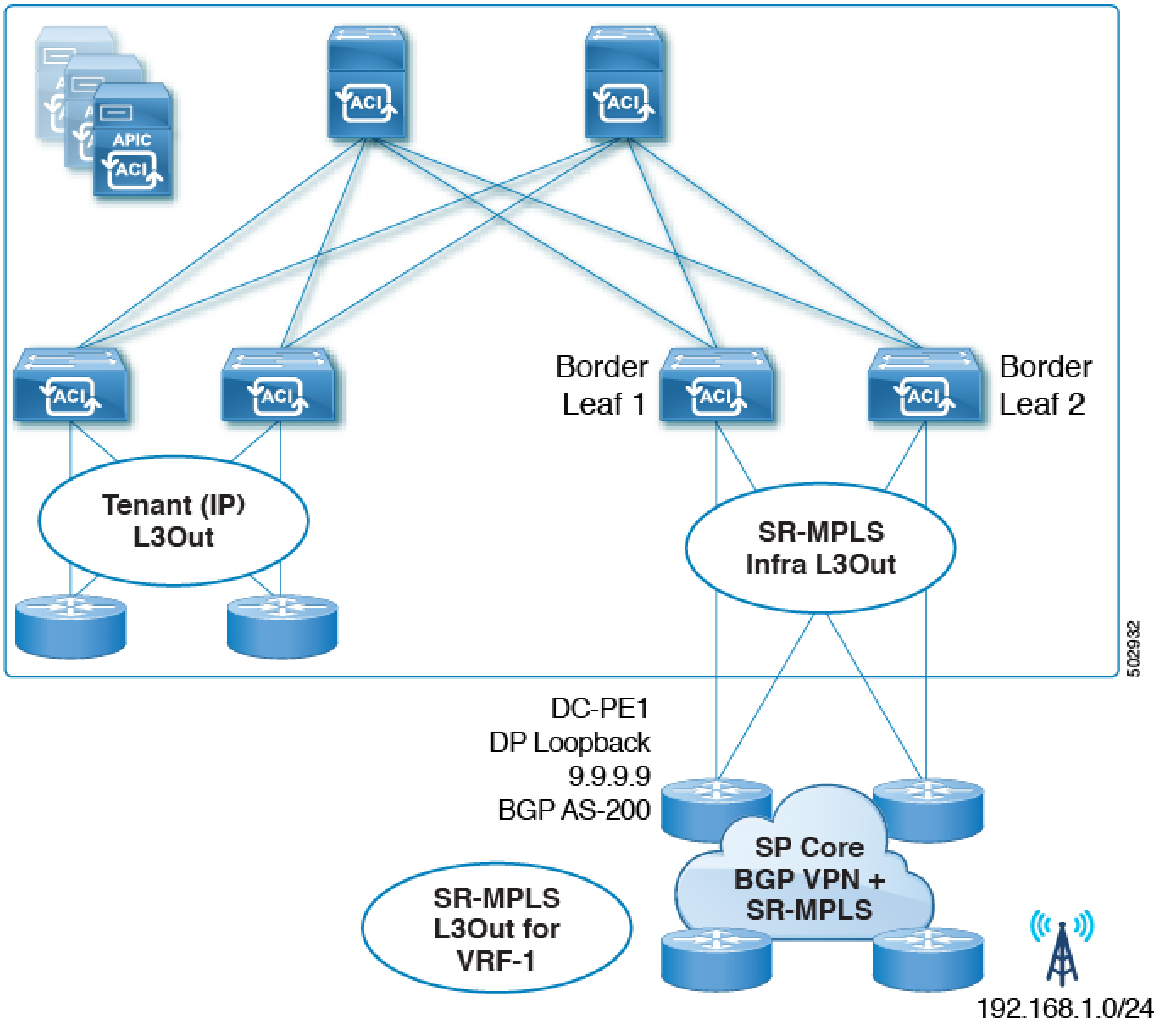


このシナリオでは、次の設定を行います。

- 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。

注意事項と制約事項

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。

- 対応プラットフォーム （21 ページ）
- プラットフォームでの制限 （21 ページ）
- SR-MPLS インフラ L3Out のガイドラインと制約事項 （22 ページ）
- SR-MPLS VRF L3Out のガイドラインと制約事項 （22 ページ）
- MPLS スイッチングに関するガイドラインと制限事項 （27 ページ）
- SR-MPLS 統計情報のガイドラインと制約事項 （28 ページ）

対応プラットフォーム

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

プラットフォームでの制限

- 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 ACI ファブリックを使用できます。

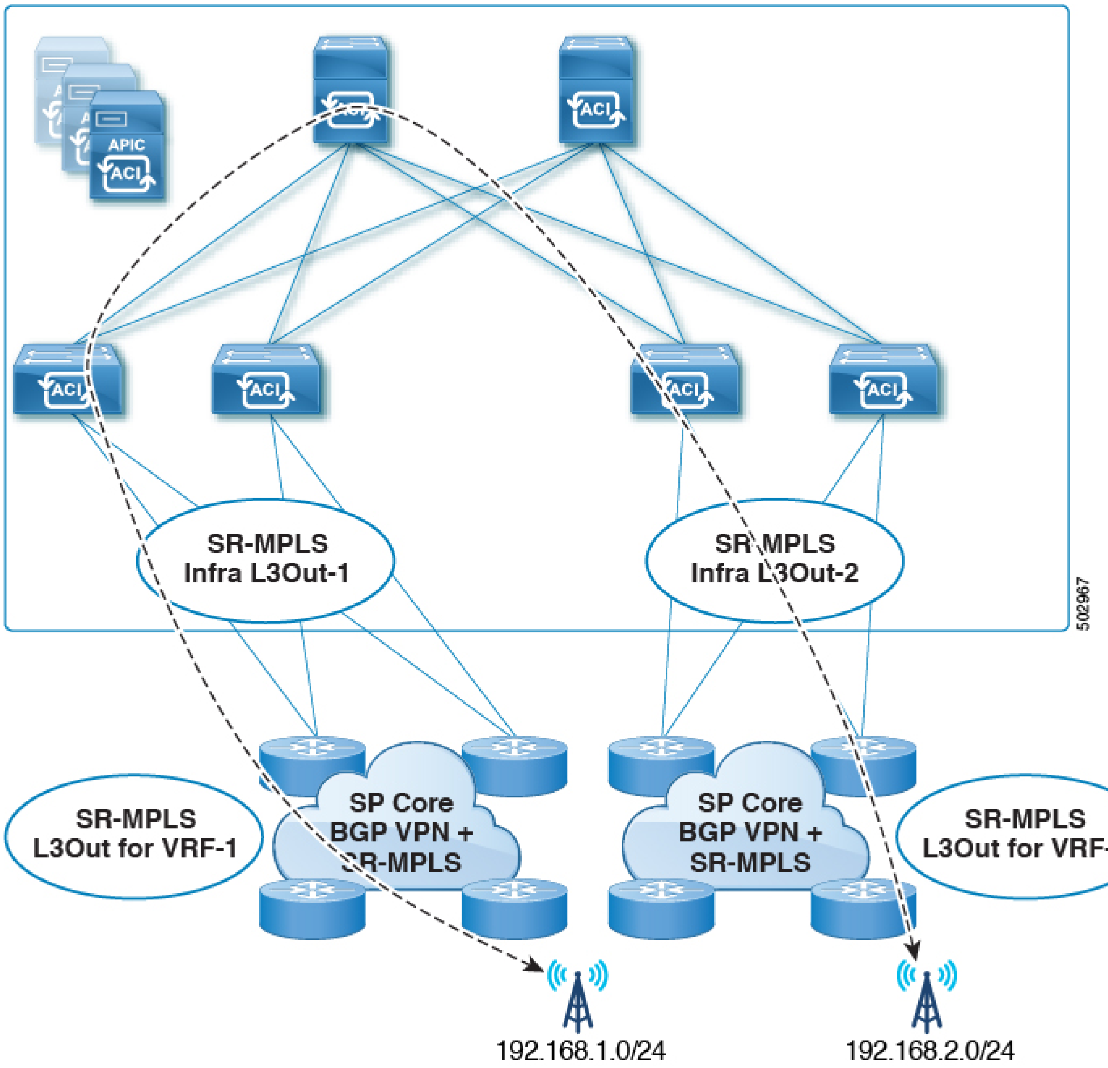
SR-MPLS インフラ L3Out のガイドラインと制約事項

- 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。

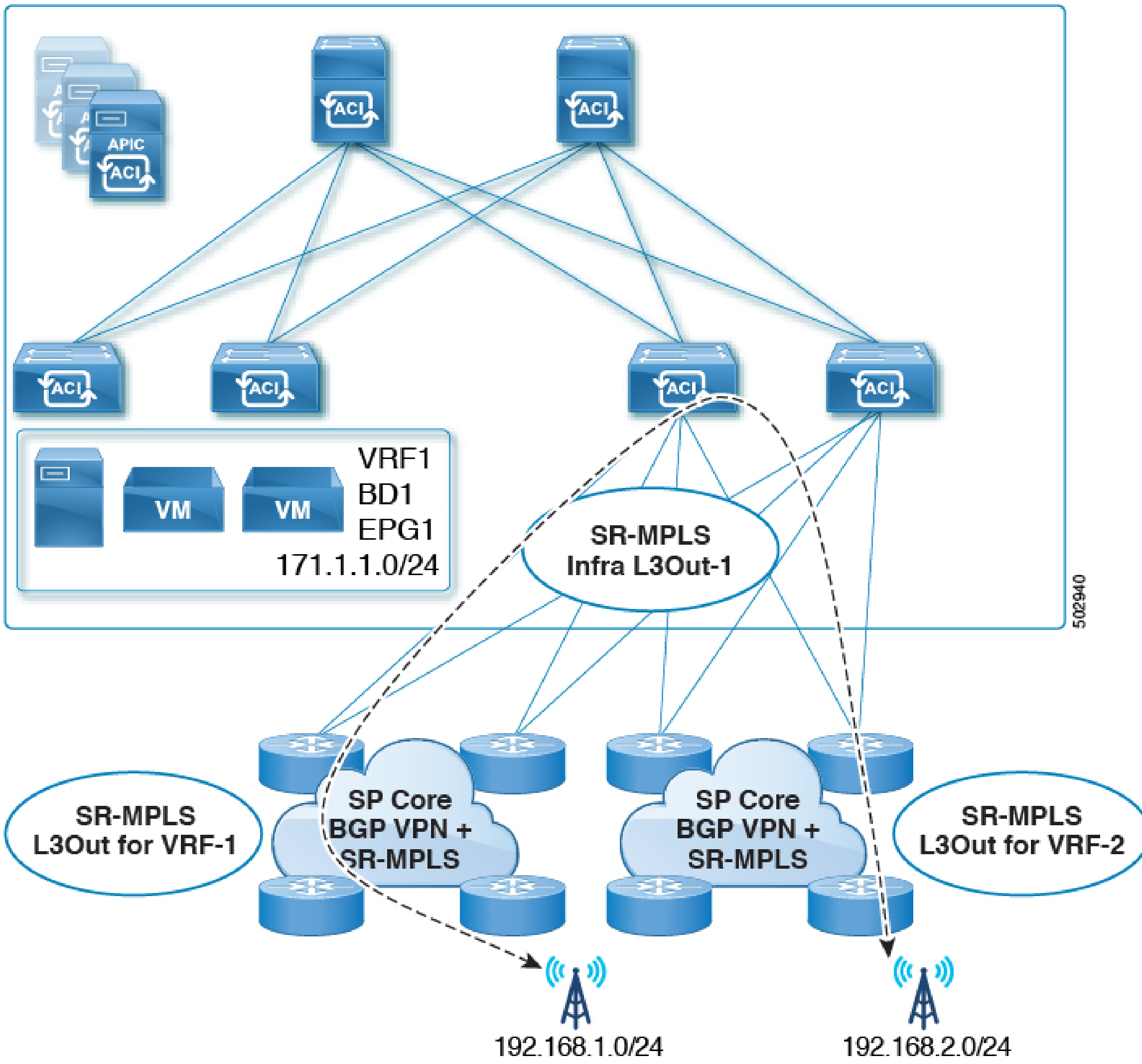
SR-MPLS VRF L3Out のガイドラインと制約事項

Routing Policy

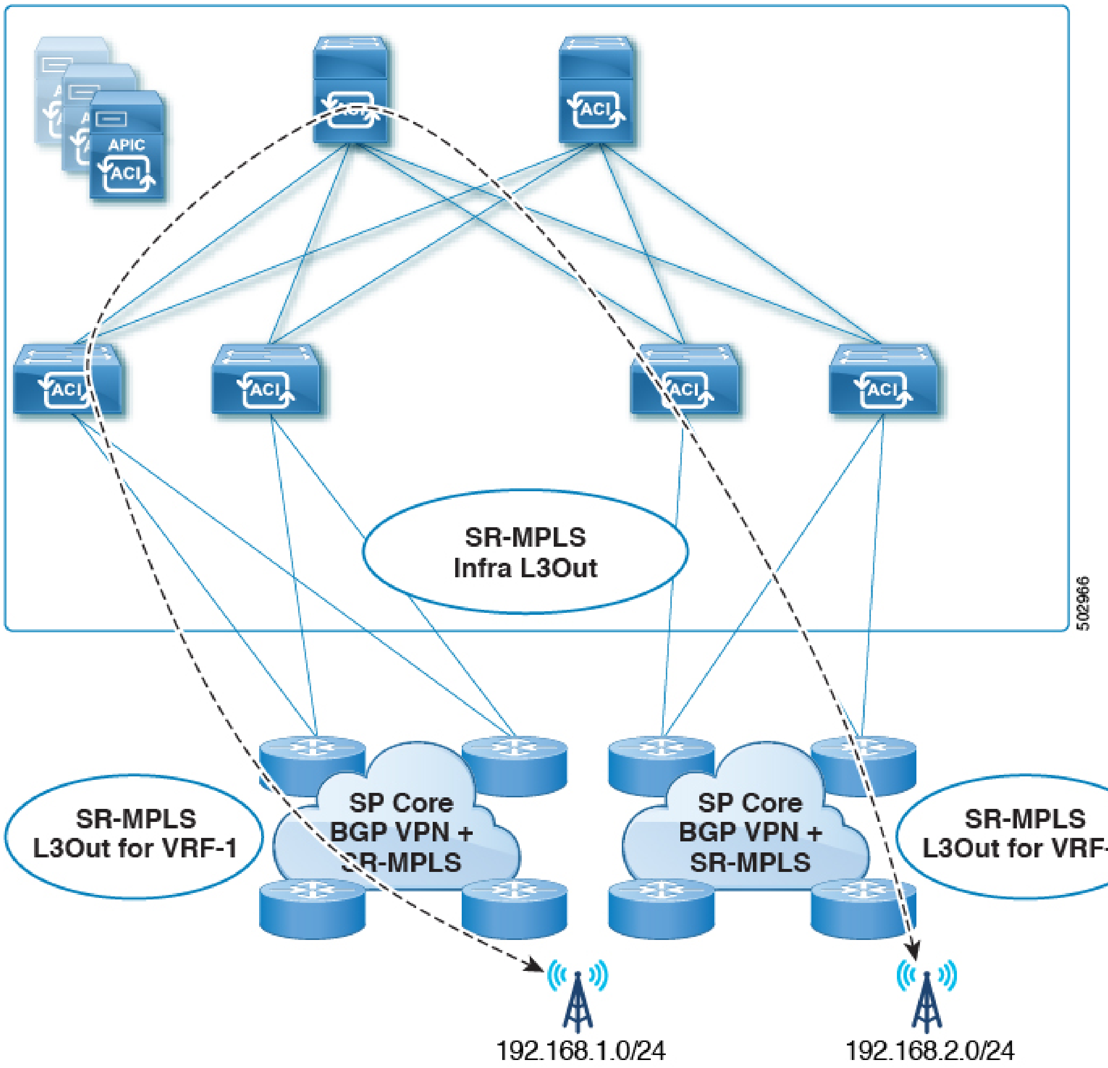
- 各 SR-MPLS VRF L3Out 内では、アウトバウンド ルート マップ（エクスポート ルーティング ポリシー）の定義は必須ですが、インバウンド ルート マップ（インポート ルーティング ポリシー）の定義はオプションです。
- SR-MPLS VRF L3Out に関連付けられているルーティング ポリシーは、グローバル タイプである必要があります。つまり、ブリッジ ドメイン サブネットを含むすべてのルートを明示的に追加する必要があります。
- ホストベース ルーティングは SR-MPLS ではサポートされません。
- 移行ルーティングがサポートされますが、一部の制約があります。
  - 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）。



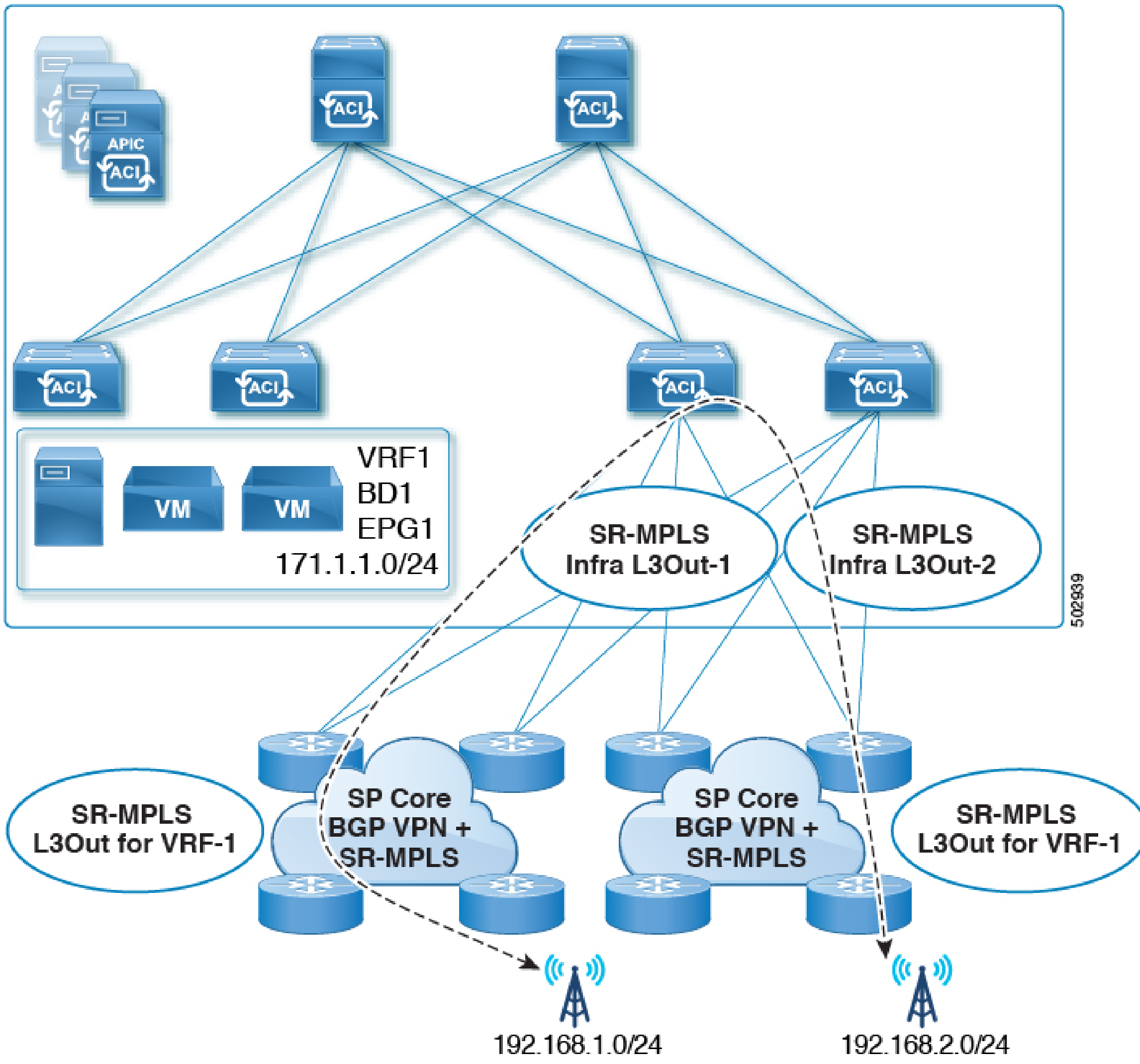
- サポート対象：次の図に示すように、同じ境界リーフ ペアと異なる VRF を持つ SR-MPLS トラフィック。



- 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。

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 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。

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。

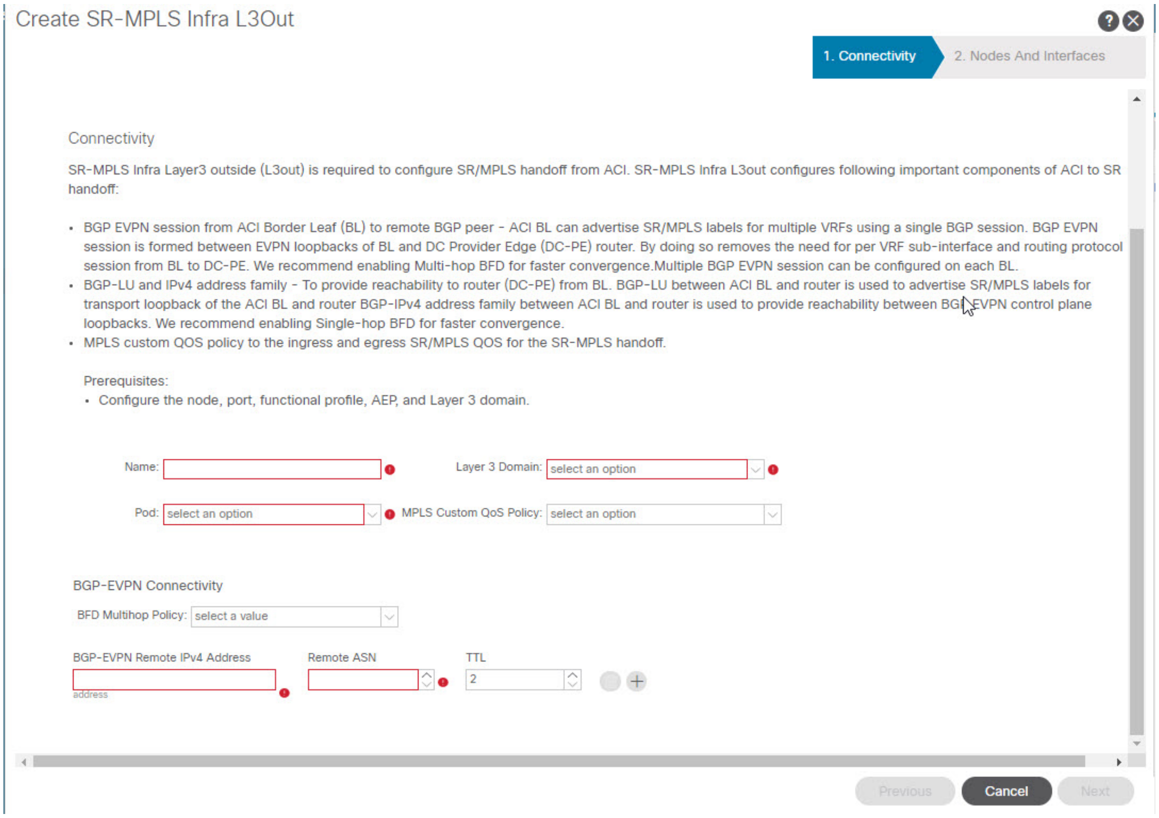
始める前に

- 注意事項と制約事項 （21 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 （22 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 （40 ページ）

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 （40 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 （10 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。

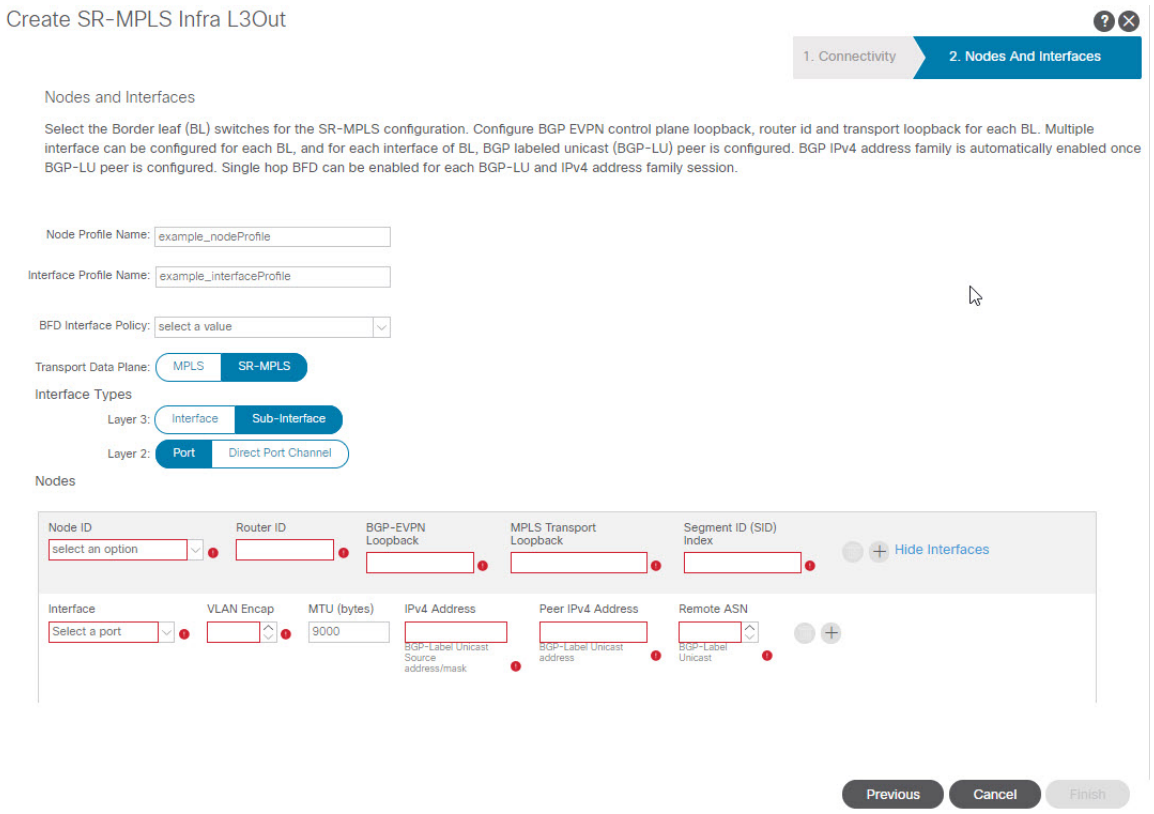
（注） ACI は asdot または asdot + 形式の AS 番号をサポートしていません。asdot または asdot + 形式の AS 番号の詳細については、『Explaining 4-Byte Autonomous System（AS）ASPLAIN and ASDOT Notation for Cisco IOS』を参照してください。https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/border-gateway-protocol-bgp/white_paper_c11_516829.html

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（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（34 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（34 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（34 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（33 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（33 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、「ACI 境界リーフ スイッチと DC-PE 間の MP-BGP EVPN セッション （8 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 ～ 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 ～ 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 （36 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 （36 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 （37 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

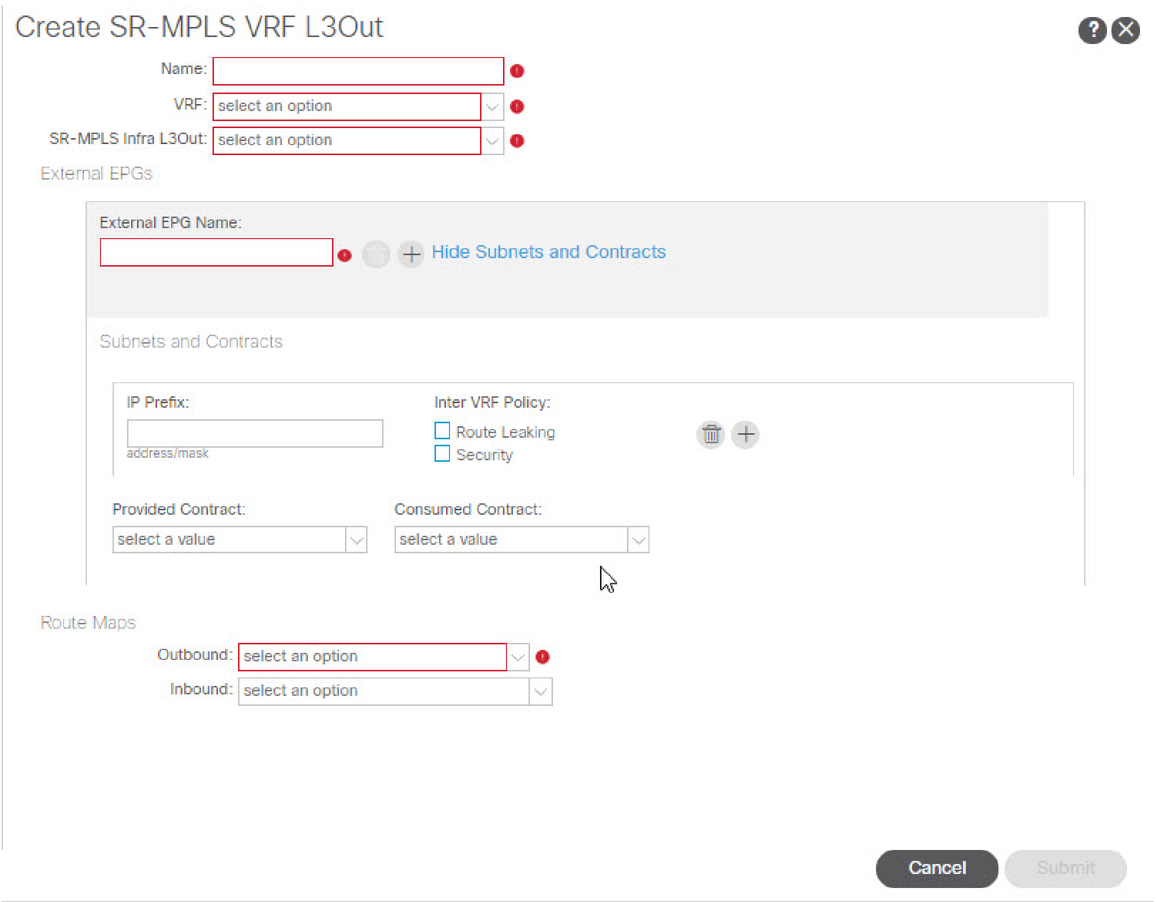
- 注意事項と制約事項 （21 ページ） で提供されている SR-MPLS ガイドラインと制約事項を確認します。特に、SR-MPLS VRF L3Out のガイドラインと制約事項 （22 ページ） で提供されているガイドラインと制約事項を確認してください。
- GUI を使用した SR-MPLS インフラ L3Out の設定 （28 ページ） の手順に従って、SR-MPLS インフラ L3Out を設定します。

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 *6 : 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 （28 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 （39 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 （39 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 （40 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。

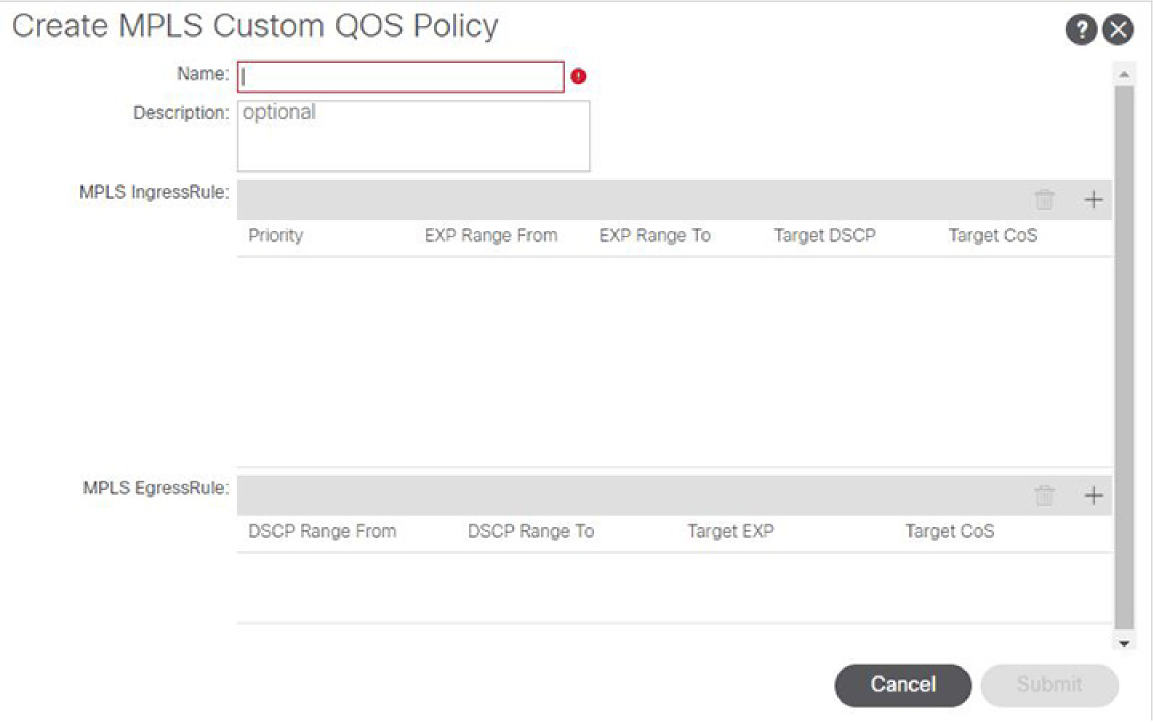
カスタム出力ポリシーが定義されていない場合、デフォルトの Qos レベル（`Level3`）がファブリック内のパケットに割り当てられます。カスタム出力ポリシーが定義されていない場合、デフォルトの EXP 値（`0`）がファブリックから離れるパケットにマーキングされます。

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。 > > >

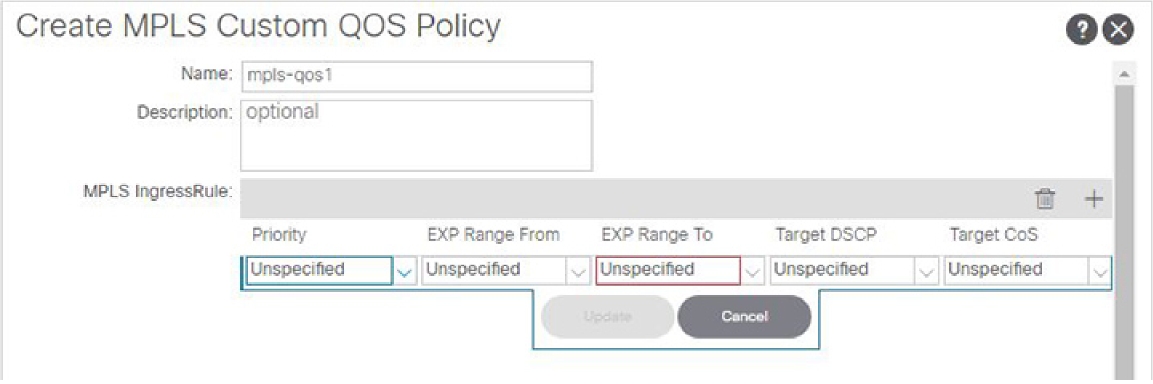
ステップ 3　[MPLS カスタム QoS （MPLS Custom QoS）] フォルダを右クリックし、[MPLS カスタム QoS ポリシーの作成（Create MPLS Custom QoS Policy）] を選択します。

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 （43 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 （44 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 （43 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 （44 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。

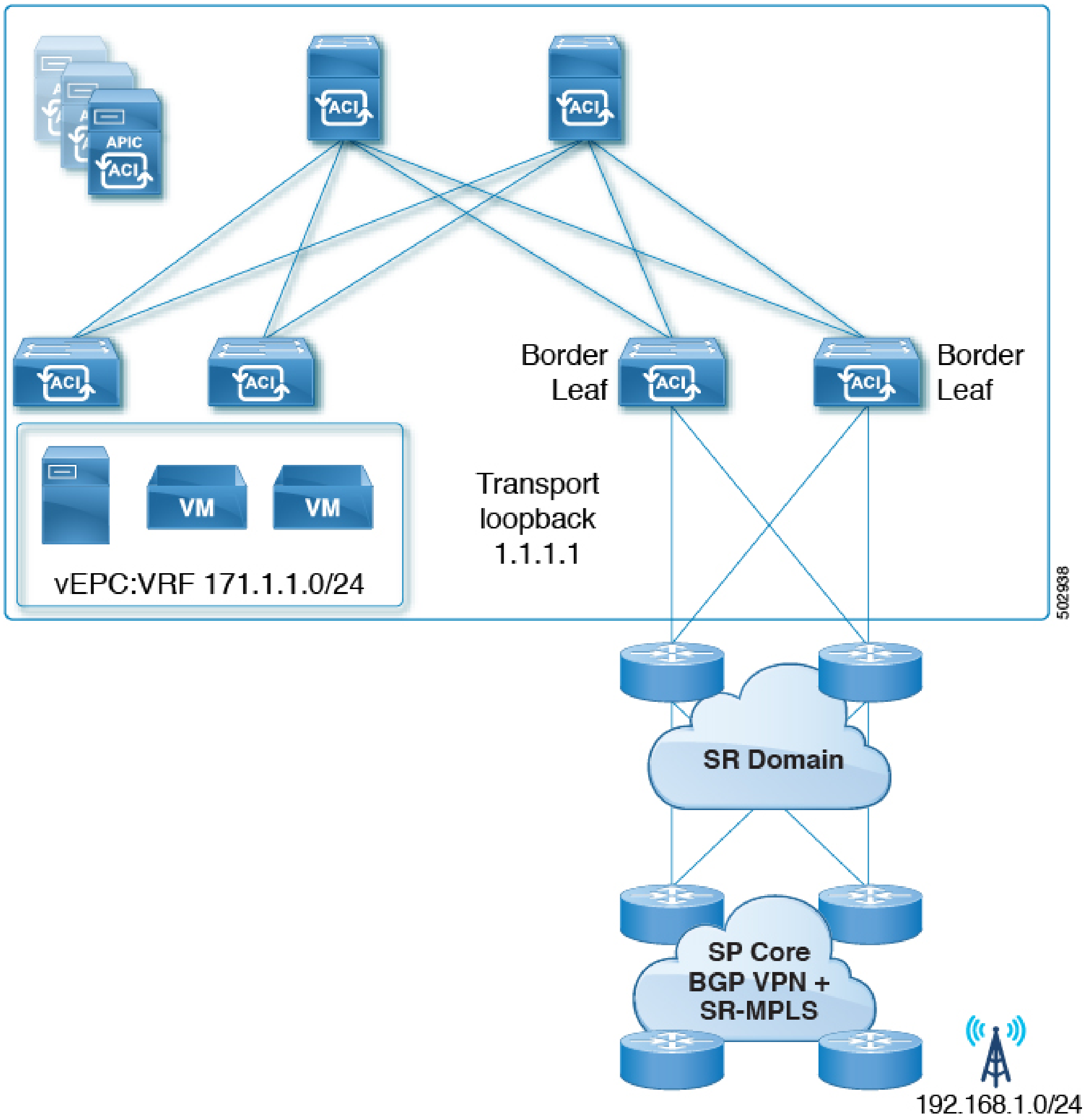
- 特定のリーフ スイッチの VRF 統計情報を表示するには、そのリーフ スイッチの VRF コンテキストに移動します。

  [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。

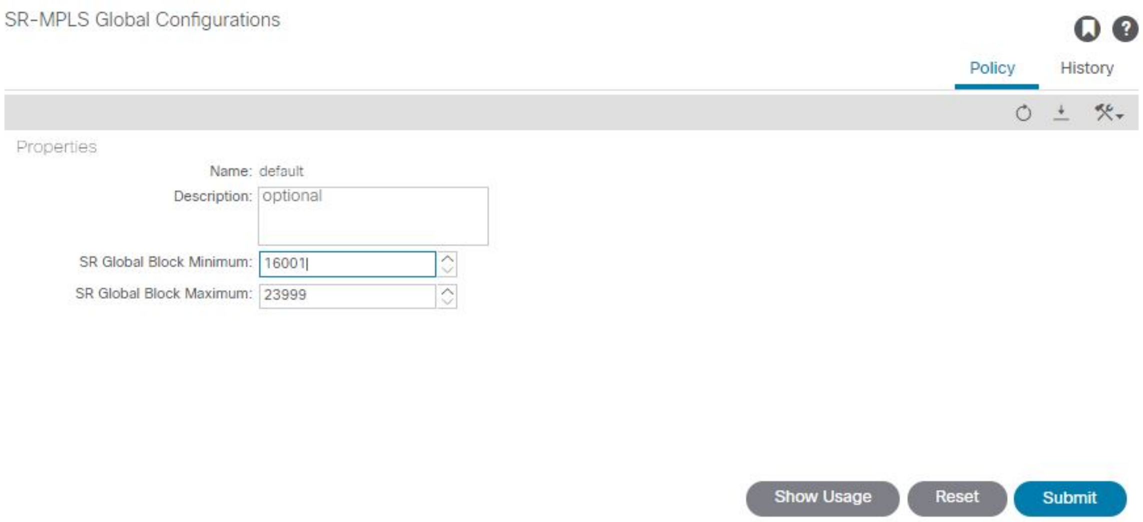
- 設定可能な SR-GB の範囲は 16000 ー 471804 です。
- ACI ファブリックのデフォルトの SR-GB 範囲は 16000 ～ 23999 です。
- ACI は、アンダーレイ ラベルに対して常にヌルをアドバタイズします（トランスポート ループバック）。

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 [送信（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 （1 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 （1 ページ） リリース 5.0(1) での ACI ハンドオフ：SR ハンドオフ （2 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 （47 ページ）に記載の情報について、確認してください。

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 （28 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 （37 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 （47 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 （50 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 （47 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 （48 ページ）

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 （52 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 （54 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 （47 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 （48 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 （50 ページ）

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 （47 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 （47 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。

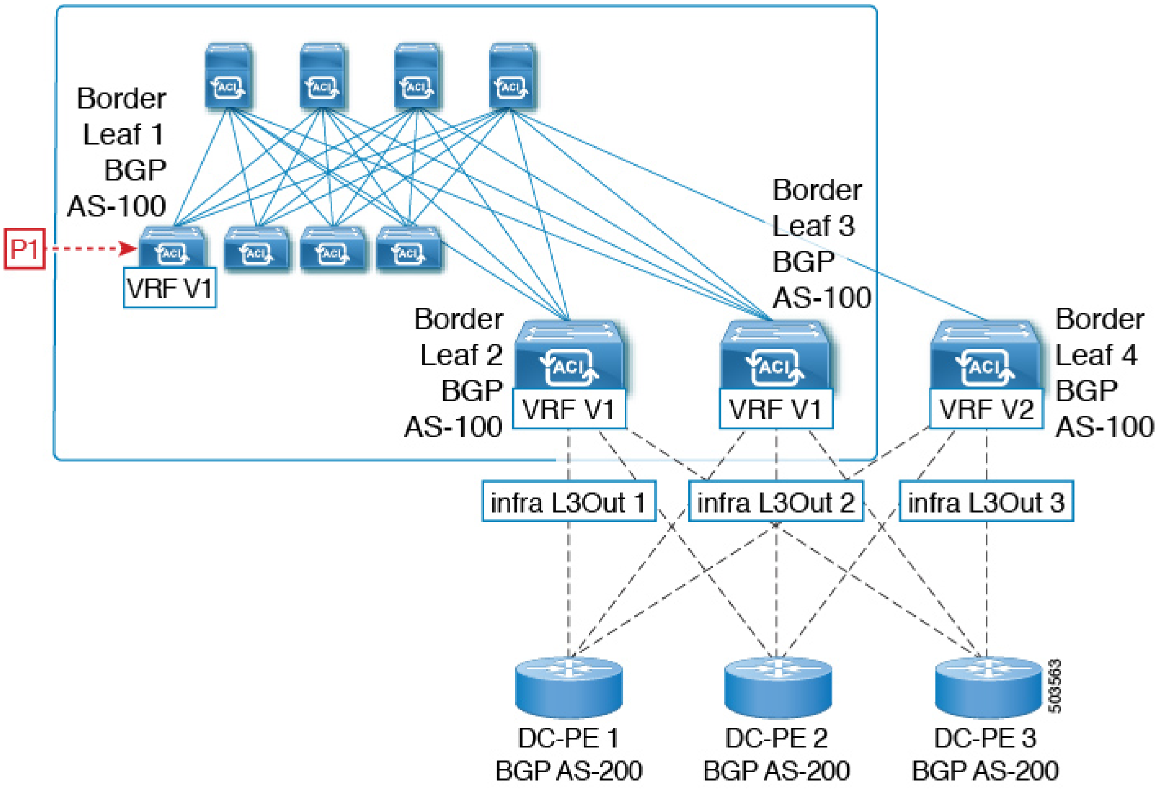
ループ防止のための BGP ドメインパス機能について

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。

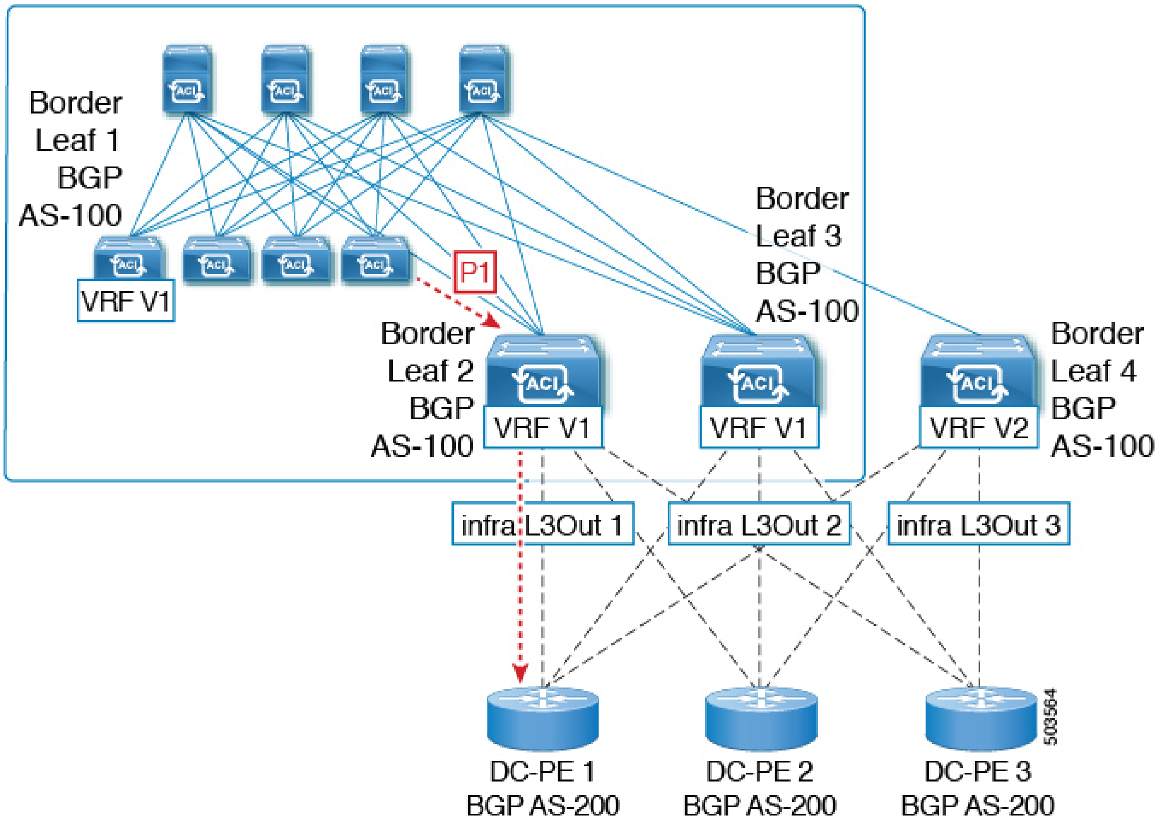
- AS パス チェックなどの既存の BGP ループ防止メカニズムの意図的な無効化
- 異なる VRF または VPN 間のルート リーク

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。

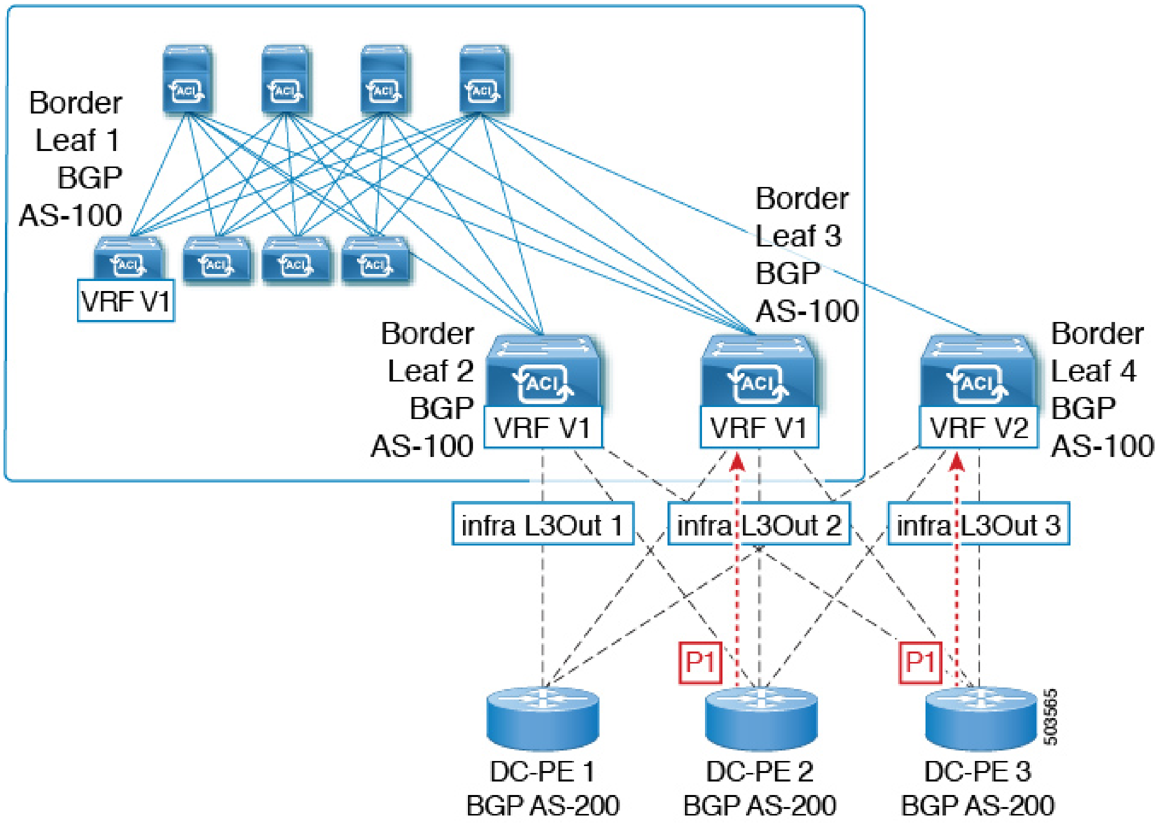
1. BGP IP L3Out ピアから受信したプレフィックス P1 は、Multiprotocol Border Gateway Protocol（MP-BGP）を使用して ACI ファブリックでアドバタイズされます。



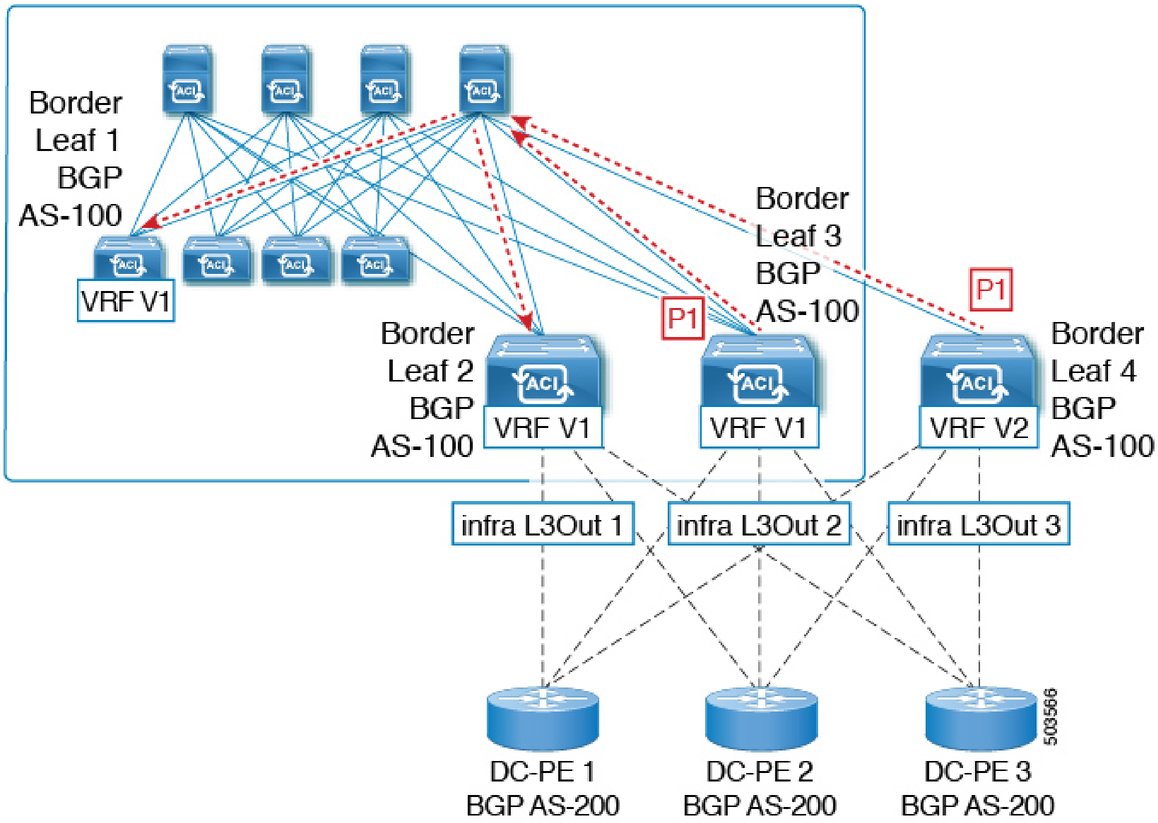
2. 中継のケースとして、このプレフィックスは SR-MPLS インフラ L3Out を介して外部にアドバタイズできます。



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 （55 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。

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 （62 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（61 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（61 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。 > > > >

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。