改訂：2026 年 10 月 26 日

Cisco Nexus Hyperfabric：BGP の構成

Border Gateway Protocol（BGP）

BGP は、インターネット上のさまざまな自律システム（AS）間でルーティング情報を交換するためのダイナミック ルーティング プロトコルです。ネットワークが複数の外部ネットワークに接続する必要がある場合、または複雑でスケーラブルなルーティングをサポートする必要がある場合は、BGP を構成する必要があります。BGP は、自動ルート更新を可能にし、ネットワークの変更にすばやく適応するため、高可用性、冗長性、および柔軟性を必要とする中規模から大規模のネットワークには不可欠です。

デバイス間で BGP ピアリングが確立されると、デバイスは最初にルーティング テーブル全体を共有し、その後は変更されたルートの更新内容だけを交換します。BGP ポリシーを使用すると、アドバタイズされる、または受け入れられるルートを制御できるため、組織のニーズに応じてネットワーク トラフィックを管理できます。

静的ルーティングは単純ではあるものの拡張性がなく、手動更新が必要なのに対し、BGP は動的な拡張と信頼性をサポートする堅牢なソリューションです。

変更を設定して適用するには、編集モードであること、および変更をコミットしたことを確認してください。

BGP のポリシーのインポートおよびエクスポート

BGP のポリシーのインポートおよびエクスポートは、BGP ピア間のルーティング情報の選択、アドバタイズメント、および受け入れを制御するルールおよび構成のセットです。BGP のポリシーのインポートは、外部 BGP ピアから受信したルートに適用されます。BGP のポリシーのエクスポートは、外部 BGP ピアに送信されるルートに適用されます。各ポリシーには、最後に暗黙的なすべて拒否のルールがあります。

- デフォルトのインポートおよびエクスポート ポリシーは事前定義されており、変更できません。デフォルト ポリシーは、特定のルールを含むテンプレートとして機能します。
- デフォルトのインポート ポリシーとエクスポート ポリシーの両方を使用する場合、これらのルートは外部ピアにアドバタイズされません。
    - 外部学習ルート
    - デフォルト ルート
    - 内部エンドポイント IP アドレス

デフォルトのインポートまたはエクスポート ポリシーを表示するには、**[ファブリック（Fabrics）]** ページに移動します。**[アタッチメント（Attachments）]** エリアで、 **[BGP]** > **[ポリシーのインポート（Import policies）]**または**[BGP]** > **[ポリシーのエクスポート（Export policies）]**を選択します。

デフォルトのインポート ポリシー

表 *1:* デフォルトのインポート ポリシー

一致	セット	アクション
すべて	コミュニティ 64511:99	許可

デフォルトのエクスポート ポリシー

表 *2:* デフォルトのエクスポート ポリシー

一致	セット	アクション
コミュニティ 64511:99	-	拒否
ルート タグ ブラック	-	拒否
IPv4 プレフィックス 0.0.0.0/0（完全一致）	-	拒否
IPv6 プレフィックス ::/0（完全一致）	-	拒否
コミュニティ 64510:*	-	許可
IPv4 プレフィックス 0.0.0.0/0（完全一致か、それ以上）32	-	拒否
IPv6 プレフィックス ::/0（完全一致か、それ以上）128	-	拒否
すべて すべての条件が一致	-	許可

- スタティック ルートを追加すると、**[スタティック ルートの追加（Add Static Route）]** ページの **[破棄（Discard）]** オプションが、デフォルトのエクスポート ポリシーの **[一致ルート タグ黒、拒否（Match Route tag Black, Deny ）]** ルールと一致します。「スタティック ルートの追加」を参照してください。
- ルートタグ ルールは、レイヤ 3 論理ネットワーク、ルーテッド インターフェイス、ルーテッド サブインターフェイス、およびループバック IP ルートで設定されたタグとも照合できます。

- ルール **Community: 64510:*** は、1 つ以上の静的ルートを外部ネットワークにアドバタイズします。
- デフォルトのエクスポート ポリシーでは、これらのルールが、デフォルト ルートおよび内部エンドポイント IP アドレス（ホスト ルート）を外部ネットワークにアドバタイズしないようにします。
  - 0.0.0.0/0（完全一致）にマッチ、拒否（Deny）
  - Match ::/0（完全一致）にマッチ、拒否（Deny）
  - Match 0.0.0.0/0（完全一致か、それ以上）32、拒否（Deny）
  - Match ::/0（完全一致か、それ以上）128、拒否（Deny）
- 外部 BGP ピアからインポートされたルートには、デフォルトのインポート ポリシーによって設定されたルール **Community: 64511:99** があるため、デフォルトのエクスポート ポリシーの **Deny** ルールにより、ルートは BGP ピアにエクスポートされません。

ルート タグを使用して BGP ルートアドバタイズメントを制御する

ルートタグは、スタティックルート、またはレイヤ 3 論理ネットワーク（SVI）、ルーテッドインターフェイス、ルーテッド サブインターフェイス、ループバック インターフェイスの IP アドレスに適用される色ベースのメタデータです。Cisco Nexus HyperFabric は、タグを内部拡張コミュニティとしてルートに関連付けます。

BGP エクスポート ポリシーでは、一致タイプとして **Route-tag** を使用し、選択したタグを持つルートを許可または拒否します。たとえば、青ルートタグに一致するルールは、青タグ付きのすべての静的、SVI、ルーテッドインターフェイス、ルーテッド サブインターフェイス、およびループバック ルートを選択した BGP ピアにアドバタイズできます。

BGP インポート ポリシーの作成

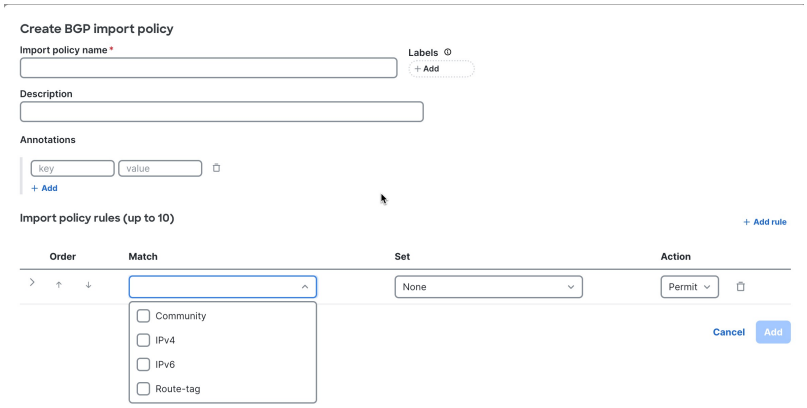
BGP インポート ポリシーを作成するには、次の手順を実行します。

ステップ 1 **[ファブリック（Fabrics）]** を選択してから、BGP インポート ポリシーを構成するファブリックを選択します。

ステップ 2 **[アタッチメント（Attachments）]** エリアで、**[BGP]** > **[ポリシーのインポート（Import policies）]** の順に選択します。

ステップ 3 **[+ 新しいポリシー（+New Policy）]** を選択します。

図 *1 :* 新しいポリシー



ステップ 4 BGP インポート ポリシーの詳細を入力します。

a) **[インポート ポリシー名（Import policy name）]** には、新しい BGP インポート ポリシーの名前を入力します。

b) **[ラベル（Labels）]** では、**[+ 追加（+ Add）]** を選択し、ポリシーの分類に役立つラベルを入力して、**Enter**を押します。

c) **[Description（説明）]** には、このBGP インポート ポリシーを説明するテキストを追加します。

d) **[注釈（Annotations）]** では、**[+ 追加（+ Add）]** を選択し、注釈の追加となるキーと値のペアを入力します。

ステップ 5 BGP インポート ポリシー ルールを入力します。

a) **[ポリシールールのインポート (最大 10 個) (Import policy rules (up to 10))]** エリアから、**[ルールの追加（+ Add rule）]** を選択して、最大 10 個のルールを追加します。

b) **[順序（Order）]** カラムで、矢印キーを使用してポリシー内のルールに順序を割り当てます。

c) **[一致（Match）]** 列で、ルールのタイプを選択します。

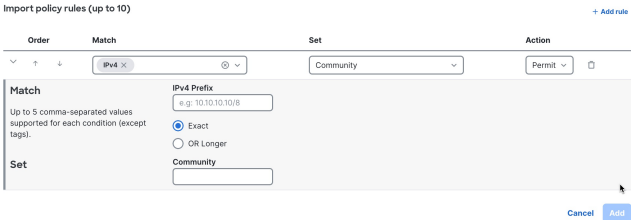
- **[コミュニティ（Community）]**：コミュニティ番号を指定します。ワイルドカードがサポートされます。
- **[IPv4]**：IPv4 プレフィックス、一致条件、およびルート起点を提供します。
- **[IPv6]**：IPv6 プレフィックス、一致条件、およびルート起点を提供します。
- **ブランク**：べてのルートに一致させるには、列を空白のままにします。この目的では「0.0.0.0/0 以上」または「::/0 以上」は入力できません。

d) **[設定（Set）]** カラムで、ドロップダウン リストから BGP 属性を選択します。

e) **[アクション（Action）]** カラムで、ドロップダウン リストから、ルールに一致するパケットに対して実行するアクション（許可または拒否）を選択します。

f) >を選択して、各ルールの一致値を追加します。各ルール（ルート タグを除く）に対して最大5つのカンマ区切り値を入力できます。

図 *2 : BGP* インポート ポリシー ルール



ステップ 6 [追加（**Add**）] を選択します。

BGP エクスポート ポリシーの作成

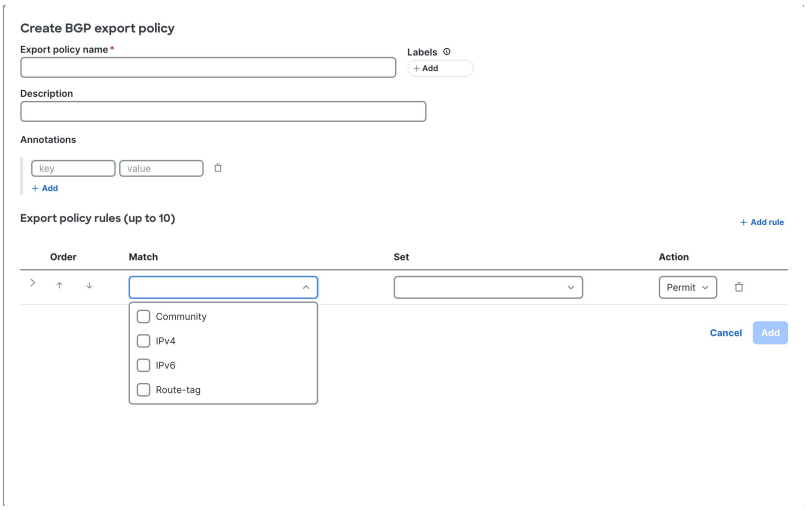
BGP エクスポート ポリシーを作成するには、次の手順を実行します。

ステップ 1 **[ファブリック（Fabrics）]** を選択してから、BGP エクスポート ポリシーを構成するファブリックを選択します。

ステップ 2 **[アタッチメント（Attachments）]** エリアで、**[BGP]** > **[ポリシーのエクスポート（Export policies）]** の順に選択します。

ステップ 3 **[+ 新しいポリシー（+New Policy）]** を選択します。

図 *3 :* 新しいポリシー



ステップ 4 BGP エクスポート ポリシーの詳細を入力します。

a) **[エクスポート ポリシー名（Export policy name）]** には、新しい BGP エクスポート ポリシーの名前を入力します。

b) **[ラベル（Labels）]** では、**[+ 追加（+ Add）]** を選択し、ポリシーの分類に役立つラベルを入力して、**Enter**を押します。

c) **[Description（説明）]** には、このBGP エクスポート ポリシーを説明するテキストを追加します。

d) **[注釈（Annotations）]** では、**[+ 追加（+ Add）]** を選択し、注釈の追加となるキーと値のペアを入力します。

ステップ 5 BGP エクスポート ポリシー ルールを入力します。

a) **[ポリシールールのエクスポート (最大 10 個) (Export policy rules (up to 10))]** エリアから、 **[ルールの追加（+ Add rule）]** を選択して、最大 10 個のルールを追加します。

b) **[順序（Order）]** カラムで、矢印キーを使用してポリシー内のルールに順序を割り当てます。

c) **[一致（Match）]** 列で、ルールのタイプを選択します。

- **[コミュニティ（Community）]**：コミュニティ番号を指定します。ワイルドカードがサポートされます。
- **[IPv4]**：IPv4 プレフィックス、一致条件、およびルート起点を提供します。
- **[IPv6]**：IPv6 プレフィックス、一致条件、およびルート起点を提供します。
- **[ルートタグ（Route-tag）]**：同じタグを持つルートを照合するためのカラー タグを選択します。ルートタグは、静的ルート、レイヤ3論理ネットワーク、ルーテッドインターフェイス、ルーテッドサブインターフェイス、およびループバックインターフェイスで設定できます。たとえば、**[許可（Permit）]**アクションと**青色**ルートタグ一致を使用して、青色で一致するタグ付きルートのみを BGP ピアにアドバタイズします。
- **ブランク**：べてのルートに一致させるには、列を空白のままにします。この目的では「0.0.0.0/0 以上」または「::/0 以上」は入力できません。

d) **[設定（Set）]** カラムで、ドロップダウン リストから BGP 属性を選択します。

- **[AS パス パッド（AS path pad）]**：AS パス リストを提供します。
- **[コミュニティ（Community）]**：コミュニティ番号を指定します。
- **[ネクストホップ IPv4（Next-hop IPv4）]**：ピア間の接続の IPv4 アドレスを指定します。
- **[ネクスト ホップ IPv6（Next-hop IPv6）]**：ピア間の接続の IPv6 アドレスを指定します。

e) **[アクション（Action）]** カラムで、ドロップダウン リストから、ルールに一致するパケットに対して実行するアクション（許可または拒否）を選択します。

f) 行を展開して、各ルールの一致値を追加します。

各ルール（ルート タグを除く）に対して最大 5 つのカンマ区切り値を入力できます。プレフィックスと完全に一致させるか、またはプレフィックス長が入力値以上（GE）以下か（LE）以下であるかに応じて一致させるかを選択できます。一致する動作の詳細と例については、ツールチップを参照してください。

図 *4 : BGP* エクスポート ポリシー ルール



ステップ 6 [追加（**Add**）] を選択します。

BGP ピアリング

BGP ピアリングは、Cisco Nexus HyperFabric 内で大まかに 2 つのタイプに分類できます。

- **ルーテッドインターフェイスからの BGP ピアリング**（ノースバウンドピアリング）：このピアリング タイプは、ルーテッドインターフェイスまたはルーテッドサブインターフェイスを使用して BGP セッションを確立します。通常、ネットワークファブリックを物理デバイスの背後にある外部ネットワークに接続します。
- **ホストインターフェイスからの BGP ピアリング**（サウスバウンドピアリング）：このピアリング タイプは、データセンターの論理ネットワーク サブネット内のネットワーク ファブリックとデバイス間で BGP セッションを確立します。このアプローチでは、一般的に仮想ルータ、仮想ファイアウォール、コンテナなどの仮想デバイスを使用します。個々のホストのトラフィックの移動に対するより良い制御とインサイトを提供します。

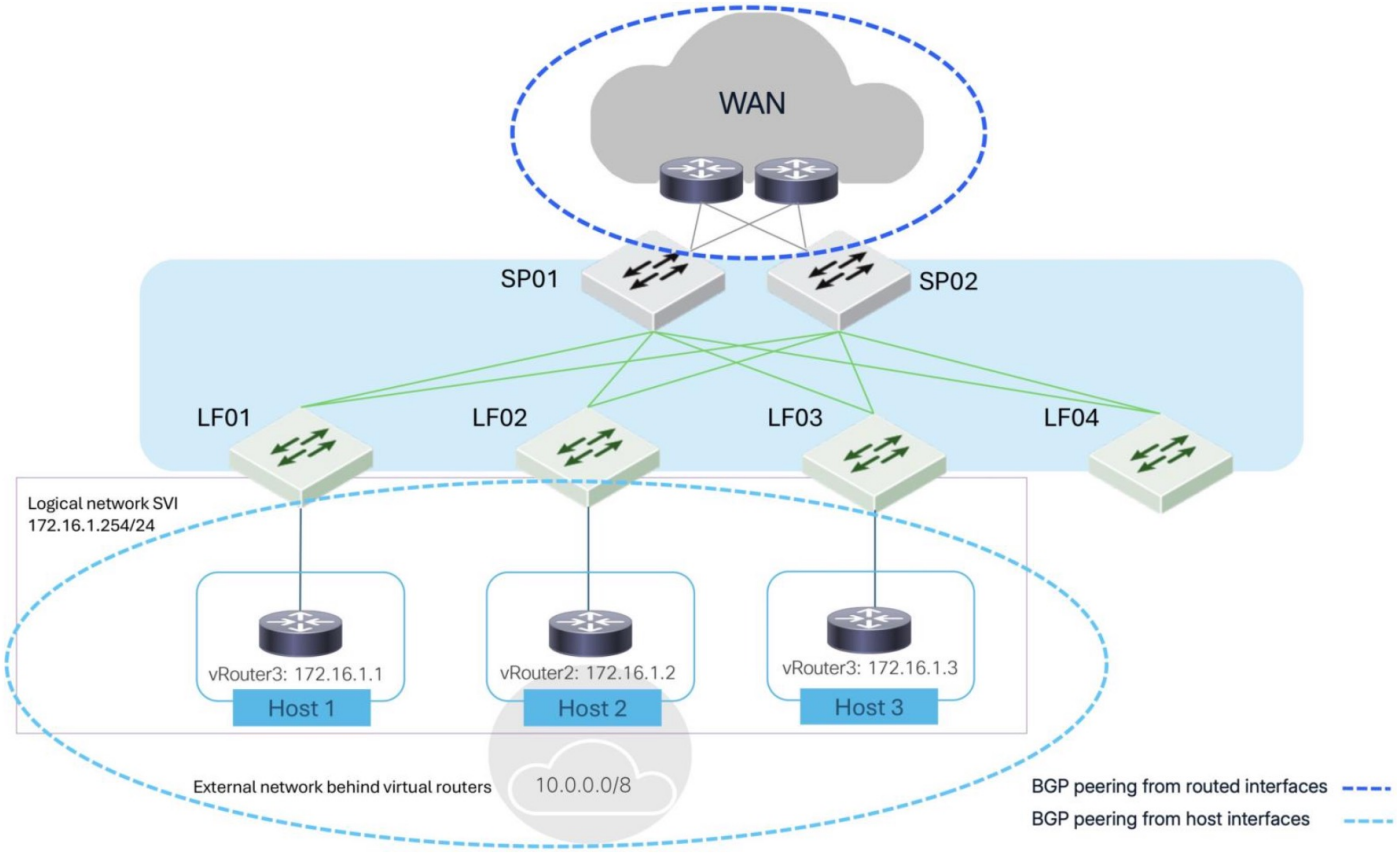
この図は、ネットワーク ファブリックを示しています。SP01 および SP02 はスパイン スイッチとして機能し、ワイド エリア ネットワーク（WAN）などのコア接続を提供します。リーフ スイッチ LF01、LF02、LF03、および LF04 は、冗長性とロード バランシングのために両方のスパインに接続します。ホスト 1、ホスト 2、およびホスト 3 を表す仮想ルータ（vRouter1、vRouter2、vRouter3）は、リーフ スイッチ LF01、LF02、および LF03 に接続します。

この図は、2 種類の BGP ピアリングを示しています。「ルーテッドインターフェイスからの BGP ピアリング」（青色の破線）は、仮想ルータを論理ネットワーク SVI（172.16.1.254/24）および外部ネットワーク（10.0.0.0/8）に接続します。「ホストインターフェイスからの BGP ピアリング」（水色の破線）は、仮想ルータをリーフ スイッチに直接接続します。この構成は、ファブリック内および外部ネットワークとの BGP ピアリング関係を示しています。

（注）

この図にはスパイン スイッチとリーフ スイッチが示されていますが、どちらのタイプの BGP ピアリングもスパイン スイッチやリーフ スイッチ以外のデバイスで発生する可能性があります。

図 5:

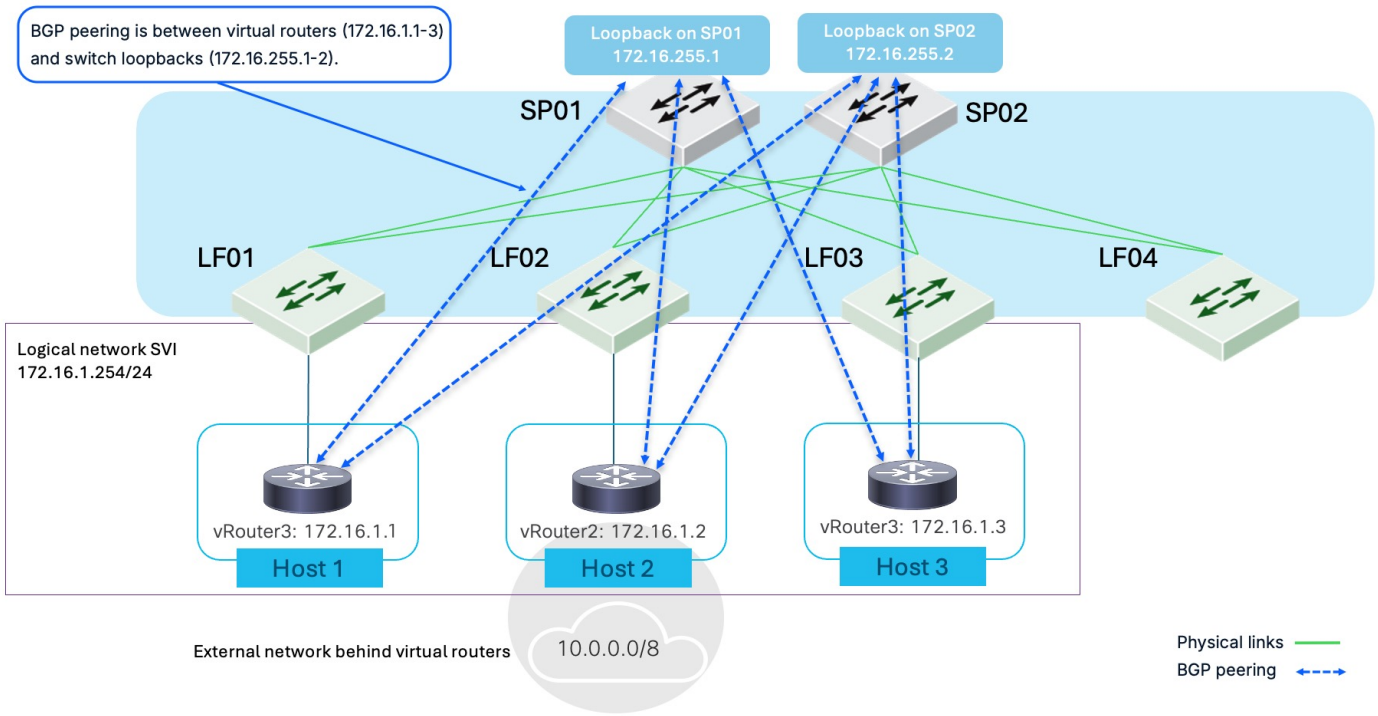


ホスト インターフェイスからの BGP ピアリングの例

これらの例は、ホスト インターフェイスからの BGP ピアリングの概念と復元力を示しています。

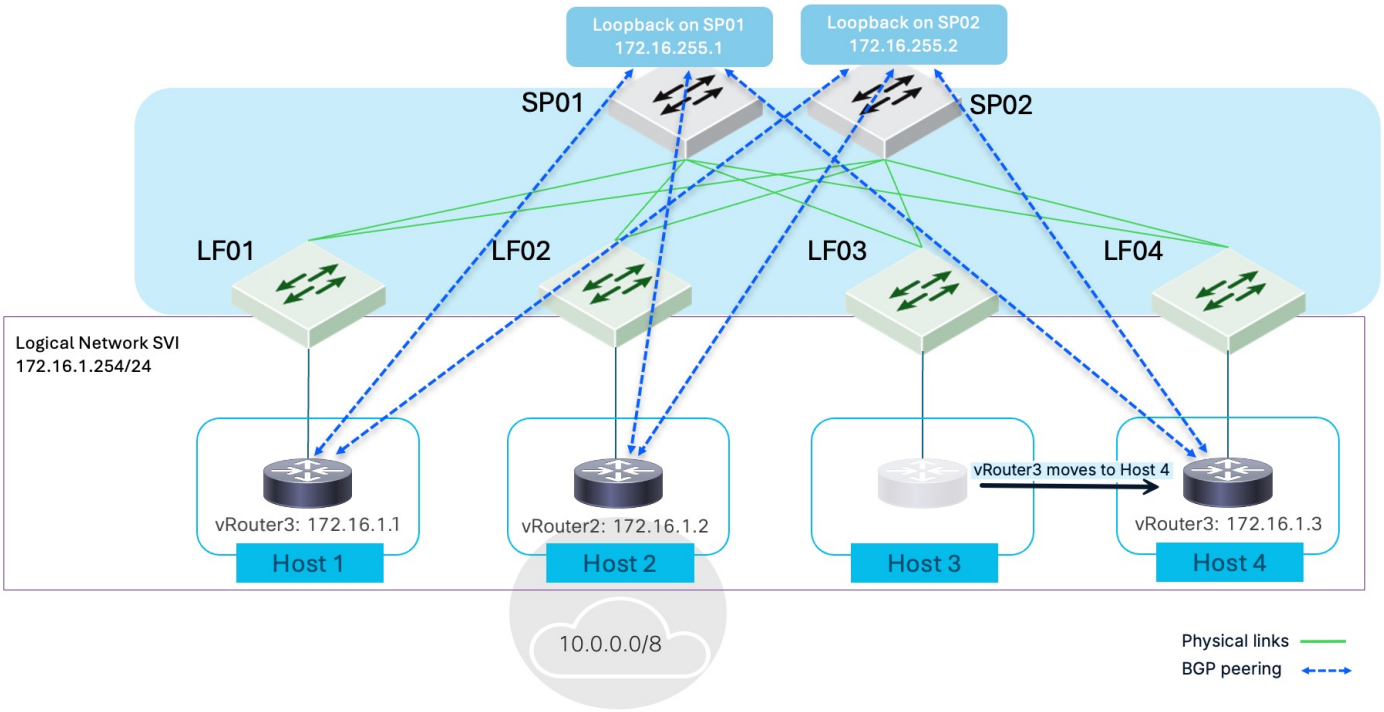
この例では、異なるホスト上の複数の仮想ルータ（vRouter1、vRouter2、vRouter3）が同じ論理ネットワーク内にあります。これらの仮想ルータは、ネットワーク ファブリックのコアを形成するスパイン スイッチ（SP01 および SP02）のループバック インターフェイスとの BGP ピアリングを確立します。これは、論理ネットワーク内の外部デバイスに接続されているホスト インターフェイスからの初期 BGP ピアリングを示しています。

図 *6*：ホスト インターフェイスからの ***BGP*** ピアリングの初期トポロジ



この例は、この設計の主な利点を強調しています。vRouter3 がホスト 3 からホスト 4 に移行し、ファブリック内の物理的な場所が変更されたことを示しています。BGP ピアリングは変更されず、ホスト インターフェイスからの BGP ピアリングの安定性とモビリティの利点が示されています。BGP セッションはアクティブなままで、仮想デバイスの物理再配置の影響を受けないため、サービスの継続的なルーティングと接続が確保されます。

図 *7:* ホスト インターフェイスからの安定した *BGP* ピアリングによるワークロードの移行



ルーテッド インターフェイスから BGP ピアリングを構成する

ルーテッドインターフェイスからの BGP ピアリング（ノースバウンド ピアリングとも呼ばれます）では、ルーテッド インターフェイスを使用してスイッチ間に BGP セッションを確立する必要があります。このタイプのピアリングは、ファブリックを外部ネットワークに接続します。ネットワークのトラフィックの入出力に使用されます。

ステップ 1 特定のルートテーブル（VRF）の BGP ピア エリアに移動します。

a) **[ファブリック（Fabrics）]**を選択し、設定するファブリックを選択します。

b) **[論理ネットワーク（Logical Networks）]** 領域で、**[ルート テーブル (VRF) (Route tables (VRF))]**をクリックします。

c) **[すべてのルート テーブル (VRF) (All route tables (VRFs))]** テーブルで、BGP ピアを構成するルート テーブルの名前を選択します。

d) **[構成（Configurations）]** エリアで、**[BGP ピア（BGP peers）]** を選択します。

ステップ 2 VRF のローカル自律システム（AS）番号を入力します。

a) **[BGP ピア（BGP peers）]** エリアで、を選択し、VRF のローカル AS を入力します。

b) **[保存（Save）]** を選択します。

デフォルトでは、ピアの構成時に、ローカル AS オーバーライドを構成しない限り、 VRF のローカル AS が BGP ピアに使用されます。

ステップ 3 **[+ BGP ピアの追加（+ Add BGP peer）]** > **[ホスト インターフェイスから（from host interface）]**を選択します。.

ステップ 4 **[ピア名（Peer name）]** には、新しい BGP ピアの名前を入力します。

ステップ 5 BGP ピア アドレスとインターフェイスの詳細を入力します。

a) **[ピア アドレスとインターフェイス（Peer address & interface）]** には、ピア IP アドレス（リモート BGP ネイバーの宛先 IP アドレス）を入力します。あるいは、パッシブ リスニング用のサブセットを入力することもできます。

（注） IPv4 と IPv6 の両方をサポートする BGP ピアの場合、アドレス ファミリごとに個別の BGP ピア構成を作成する必要があります。

b) **[使用可能なルーテッド インターフェイス テーブルの選択（Select an available routed interface table）]** で、BGP セッションの確立に使用されるローカルインターフェイスを選択します。

ステップ 6 BGP ピアリングの詳細を入力します。

a) **[タイプ（Type）]** では、BGP タイプを選択します。

- **[iBGP]**（内部 BGP）：この BGP タイプは、単一の自律システム（AS）内のルーティング情報の交換に使用されます。ピアは同じ AS 内に置かれます。
- **eBGP** (外部 BGP):この BGP タイプは、異なる AS 間でルーティング情報を交換するために使用されます。ピアは異なる AS にあります。

b) **[構成（Configuration）]** では、BGP タイプが eBGP の場合、 **[シングルホップ（single-hop）]** または **[マルチホップ（multi-hop）]** を選択します。

c) **[存続可能時間 (TTL) (Time to live (TTL))]** では、BGP タイプが eBGP でマルチホップの場合、ピアリング セッションで許可するホップ数（2 ~ 255）を入力します。

セキュリティ チェックとして、BGP は、受信した IP パケット ヘッダーの TTL 値がピアリング セッション用にここで設定された TTL 値以上の場合だけセッションを確立または維持します。

d) **[ピア AS（Peer AS）]** には、ピアの入力自律システム（AS）番号を入力します。

e) **[ローカル AS オーバーライド（Local AS override）]** 番号を入力します。

オーバーライド ローカル AS 番号を入力すると、スイッチは発信側スイッチの AS 番号を送信側 BGP スイッチの AS 番号に置き換えることができます。これにより、受信側スイッチは、受信側と同じ AS を持つ発信側からのパケットをドロップすることがなくなります。デフォルトでは、新しい値が指定されていない限り、VRF Local AS が使用されます。

ステップ 7 **[ポリシー（Policy）]**エリアでは、ドロップダウン リストから **[インポート ポリシー（Import policy）]** と **[エクスポート ポリシー（Export policy）]** を選択するか、デフォルトのままにします。

これらのポリシーは、BGP インポート ポリシーの作成 （3 ページ） および BGP エクスポート ポリシーの作成 （5 ページ） で定義します。

ステップ 8 （任意） **[セキュリティ（Security）]** エリアで、認証方法を選択し、ログイン情報を入力します。

ステップ 9 [保存（Save）] を選択します。

ホスト インターフェイスから BGP ピアリングを構成する

ホスト インターフェイスからの BGP ピアリングにより、ファブリックとエンドポイントの間に BGP セッションが確立されます。このピアリング タイプは、ループバックを使用して安定したセッションを維持します。ホストレベルのルーティングのきめ細かい制御と可視性を提供し、ネットワーク エッジでのトラフィックフローとポリシーの管理を支援します。

ホスト インターフェイスから BGP ピアを構成する前に、次の構成が存在することを確認します。

- BGP ピアを追加するVRF
- VRF 上のスイッチ仮想インターフェイス（SVI）を備えた論理ネットワーク
- BGP セッションをホストするスイッチ上のループバック インターフェイス
- ホスト ロールが割り当てられたポート、および
- 論理ネットワークのポート VLAN メンバーシップ。

ステップ 1 特定のルートテーブル（VRF）の **[BGP ピア（BGP peer）]** エリアに移動します。

a) **[ファブリック（Fabrics）]**を選択し、構成するファブリックをクリックします。
b) **[論理ネットワーク（Logical Networks）]** 領域で、**[ルート テーブル (VRF) (Route tables (VRF))]**をクリックします。
c) **[すべてのルート テーブル (VRF) (All route tables (VRFs))]** テーブルで、BGP ピアを構成するルートテーブルの名前を選択します。
d) **[構成（Configurations）]** エリアで、**[BGP ピア（BGP peers）]** を選択します。

ステップ 2 VRF のローカル AS を入力します。

a) **[BGP ピア（BGP peers）]** エリアで、を選択し、VRF のローカル AS を入力します。
b) **[保存（Save）]** を選択します。

デフォルトでは、ローカル AS オーバーライドを構成しない限り、 VRF のローカル AS が BGP ピアに使用されます。5.e を参照してください。

ステップ 3 **[+ BGP ピアの追加（+ Add BGP peer）]** > **[ホスト インターフェイスから（from host interface）]**を選択します。.

ステップ 4 BGP ピアリングの詳細を入力します。

a) **[ピア名（Peer name）]** には、新しい BGP ピアの名前を入力します。
b) **[ピアアドレスとインターフェイス（Peer address & interface）]** エリアで、以下のように設定します。

（注） IPv4 と IPv6 の両方をサポートする BGP ピアの場合、アドレス ファミリごとに個別の BGP ピア構成を作成する必要があります。

1. ピア IP アドレス（リモート BGP ネイバーの宛先 IP アドレス）を入力します。あるいは、パッシブ リスニング用のサブセットを入力できます。

2. **[ピア アドレスとインターフェイス（Peer address & interface）]** フィールドで指定された IP アドレスまたはサブネット内に含まれる IP アドレスまたはサブネットを持つホスト インターフェイスのみが必要な場合は、**[サブネット内の検索（Search within subnet）]** を有効にします。

3. **[使用可能な論理ネットワークの選択（Select an available logical network）]** エリアで、リモートピアとの BGP メッセージの送受信に使用するインターフェイスを選択します。

   ネットワークに使用されるIPアドレスのビット数を制限するために、**[ピア許可リストの編集(オプション) (Edit peer allow-list (optional))]** でネットワークプレフィックスを更新できます。たとえば 192.168.1.0/16 です。

4. **[ループバック インターフェイスの選択（Select a loopback interface）]** テーブルで、ループバック インターフェイスを選択して展開します。BGP ピアリング セッションの送信元として使用される、選択したループバック インターフェイスのスイッチ インスタンスを指定します。

   冗長性のために最大 4 つのスイッチ インスタンスを選択できます。各スイッチは最大 10 ピアを持つことができます。より多くのスイッチとピアが必要な場合は、同じ論理ネットワークを使用して、ホストインターフェイス構成から別の BGP ピアを作成できます。

ステップ 5 BGP ピアリング セッションを構成します。

a) **[タイプ（Type）]** では、BGP タイプを選択します。

- **[iBGP]**（内部 BGP）：この BGP タイプは、単一の自律システム（AS）内のルーティング情報の交換に使用されます。ピアは同じ AS 内に置かれます。
- **[eBGP]**（外部 BGP）：この BGP タイプは、異なる自律システム（AS）間でルーティング情報を交換するために使用されます。ピアは異なる AS にあります。

b) **[構成（Configuration）]** では、BGP タイプが eBGP の場合、**[マルチホップ（multi-hop）]** を選択します。

c) **[存続可能時間 (TTL) (Time to live (TTL))]** では、BGP タイプが eBGP でマルチホップの場合、ピアリング セッションで許可するホップ数（2 ~ 255）を入力します。

d) **[ピア AS（Peer AS）]** では、ピアの AS 番号を入力します。

e) **[ローカル AS オーバーライド（Local AS override）]** 番号を入力します。

   ローカル AS オーバーライド番号を入力すると、スイッチは発信元スイッチの AS 番号を送信元 BGP スイッチの AS 番号に置き換えます。このアクションにより、受信側スイッチは、受信者と同じ AS 番号を共有する送信側から送信されたパケットをドロップすることがなくなります。デフォルトでは、新しい値が指定されていない限り、VRF のローカル AS が使用されます。

ステップ 6 **[ポリシー（Policy）]**エリアでは、ドロップダウン リストから **[インポート ポリシー（Import policy）]** と **[エクスポート ポリシー（Export policy）]** を選択するか、デフォルトのままにします。

これらのポリシーは、BGP インポート ポリシーの作成 （3 ページ） および BGP エクスポート ポリシーの作成 （5 ページ） で定義します。

ステップ 7 **[セキュリティ（Security）]** エリアで、認証方法を選択し、ログイン情報を入力します。

ステップ 8 **[保存（Save）]** を選択します。

ファブリック内のすべての BGP セッションとポリシーを表示する

ファブリック全体の BGP ピアリング セッションとポリシー情報の詳細をすばやく見つけることができます。

- **ルーテッド インターフェイスからのピアリング セッション**（ノースバウンドピアリング）：これらの詳細を表示して、ルーテッド インターフェイスがファブリックとの BGP セッションを正常に確立していることを確認し、それらに関連付けられた VLAN と特定のスイッチの場所を確認します。このビューは、ダイナミック ルート ラーニングの確認、ルート アドバタイズの確認、および外部ネットワークとの接続のトラブルシューティングに不可欠です。
- **ポリシーのインポート**：これらの詳細に基づき、BGP ネイバーからファブリックのルーティング テーブルへのルートを把握し、確認します。これにより、必要なルートのみが学習され、ルーティング テーブルの汚染が防止され、セキュリティが適用され、着信トラフィックが正しく転送されます。
- **ポリシーのエクスポート**：これらの詳細に基づき、ファブリックが BGP ネイバーにアドバタイズしているルートを把握し、確認します。これは、外部で共有される情報を制御し、偶発的なルートリークを防止し、トラフィックをファブリックにルーティングする方法を管理するために重要です。

ステップ 1 **[ファブリック（Fabrics）]** を選択して、BGP ピアリング情報を表示するファブリックを選択します。

ステップ 2 **[アタッチメント（Attachments）]** エリアで、**[BGP]** を選択します。

ステップ 3 表示する情報のタイプを選択します。

BGP ピアの詳細の表示

BGP ピアの詳細を表示すると、ファブリックの BGP 動作のいくつかの重要な側面をアクティブにモニタできます。

- **[ピアの詳細（Peer details）]**：各 BGP セッションが確立され、スムーズに実行されているかどうかを確認します。これにより、BGP ピアとの接続を迅速に確認し、セッション確立に関する問題があればトラブルシュートできます。
- **[受信したルート（Received routes）]**：デバイスが BGP ピアから学習したルートを確認します。これらのルートには、AS パス、ネクスト ホップ、ローカル プリファレンスなどの重要な属性が含まれます。インポート ポリシーが適用される前にこれらの詳細を検査することにより、デバイスがネイバーからルートを正しく受信して処理することを確認できます。
- **[アドバタイズされたルート（Advertised routes）]**:：デバイスが BGP ピアにアドバタイズするルートを調べます。これは、異常なルートや不正なルートを検出するのに役立ちます。ルートリークやハイジャックの可能性を特定し、デバイスが共有するルートを制御してトラフィック フローを最適化できます。

これらの詳細をアクティブに確認することで、BGP 接続を検証し、ルーティングの問題を解決し、ファブリック全体で強力で効果的なルーティング ポリシーを維持できます。

この手順では、ファブリック レベルから BGP ピアの詳細に移動する方法について説明します。特定のVRFの BGP ピアを表示するには、**[論理ネットワーク（Logical Network）]** エリアで、**[ルート テーブル (VRF) (Route tables (VRF))]** > ***[vrf-name]*** > **[BGP ピア（BGP peers）]** > ***[bgp-peer-name]***を選択します。

ステップ 1 **[ファブリック（Fabrics）]** を選択して、BGP ピアリング情報を表示するファブリックを選択します。

ステップ 2 **[アタッチメント（Attachments）]** エリアで、**[BGP]** を選択します。

ステップ 3 **[BGP ピア（BGP peers）]** テーブルで、ピア名を選択します。

ステップ 4 表示する情報のタイプを選択します：**[ピアの詳細（Peer details）]**、**[受信したルート（Received routes）]**、または **[アドバタイズされたルート（Advertised routes）]**。

BGP ピアの管理

BGP ピアを編集または削除するには、次の手順に従います。

ステップ 1 編集または削除する BGP ピアのルート テーブルに移動します。

a) **[ファブリック（Fabrics）]**を選択し、構成するファブリックをクリックします。

b) **[論理ネットワーク（Logical Networks）]** 領域で、**[ルート テーブル（VRF）（Route tables (VRF)）]** をクリックします。

c) **[すべてのルート テーブル (VRF) (All route tables (VRFs))]** テーブルで、BGP ピアを含むルート テーブル名を選択します。

ステップ 2 BGP ピアの構成方法に応じて、**[ルーテッド インターフェイスから（from routed interface）]** または **[ホスト インターフェイスから（from host interface）]** を選択します。

ステップ 3 BGP ピアを編集します。

a) **[アクション（Action）]** カラムで、編集する BGP ピアのを選択します。

a) BGP ピアリングの詳細を編集します。

b) **[保存（Save）]** を選択します。

ステップ 4 BGP ピアを削除します。

a) **[アクション（Action）]** カラムで、編集する BGP ピアの  を選択します。

b) **[削除（Delete）]** を選択して削除を確認します。

終了して変更を確定する

変更内容を確認、確定、およびプッシュするまで、ファブリックに適用されません。

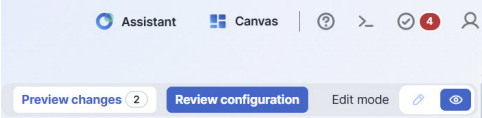
（注）

この手順の詳細な説明については、*Cisco Nexus Hyperfabric:Getting Started* の「Modify a fabric」を参照してください。

変更を終了して確定するには、次のステップに従います。

ステップ 1 **[構成のレビュー（Review configuration）]** を選択します。

図 *8 :* 構成のレビュー



ステップ 2 レビューリストで変更を確認します。

ステップ 3 **[コメントしてプッシュ（Comment and push）]** を選択します。

ステップ 4 **[構成を送信する前のコメント（Comments before sending configuration）]** ダイアログボックスに、変更の理由を入力します。

ステップ 5 **[構成のプッシュ（Push Configuration）]** を選択します。

よくあるトラブルシューティングのシナリオ

これらの質問では、BGP セッションの動作と設定のトラブルシューティングと理解に焦点を当てています。

Q：ホスト インターフェイス セッションから BGP を構成しましたが、BGP の状態が表示されません。完全に確立されていない場合、BGP セッションの状態が表示されないのはなぜですか。

A：ホスト インターフェイスから設定された BGP セッションは、パッシブ リッスン専用モードで動作します。したがって、セッションを開始しているネイバーによってアクティブに確立されたセッションの BGP セッションの状態のみが表示されます。

さらに、ホスト インターフェイスからの BGP は、特にコンテナ ネットワーク インターフェイス（CNI）の場合に、多数のネイバーに拡張できるように設計されています。このパッシブ モード構成により、BGP セットアップが簡素化され、 Cisco Nexus Hyperfabric 環境内でのメンテナンスが容易になります。

Q：ホストインターフェイス（仮想ファイアウォール）から BGP ネイバーを構成しました。ただし、仮想ファイアウォールからのアクティブな接続は確認されず、ファイアウォールには BGP の状態が IDLE と表示されます。なぜでしょうか。

A：Nexus HyperFabric は、ホスト インターフェイスから BGP を構成するときに、BGP インターフェイスとしてループバック インターフェイスを使用します。したがって、外部 BGP（eBGP）モードで実行している場合は、マルチホップの BGP ピアを構成する必要があります。

BGP ネイバーが IDLE 状態である場合、直接接続されていないために BGP ピアがセッションを確立できない可能性が高くなっています。デフォルトでは、eBGP のホップ制限は 1 です。この場合、BGP ピアで eBGP マルチホップ モードを有効にし、1 より大きいホップ カウントを指定してセッションを確立できるようにする必要があります。

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。