eBGP ルーテッド ファブリックの管理

BGP ベースのルーテッド ファブリックの管理

この章では、選択したルーティング プロトコルとして eBGP を使用して、典型的なスパイン リーフ ベースのルーテッド ファブリックを構成する方法について説明します。これは、大規模なスケーラブル データ センター（MSDC）ネットワークに推奨される展開の選択肢です。Same-Tier-AS オプションと Multi-AS オプションの両方がサポートされています。ルーテッド ファブリックには、リーフ間のレイヤ 2 ストレッチまたはサブネット ストレッチはありません。つまり、ネットワークはリーフのペアまたはラックに配置され、リーフは直接接続されたサーバー ワークロードのデフォルト ゲートウェイをホストします。ラック全体のサブネット アドバタイズメントは、スパインを介して eBGP 経由で通信されるため、ルーテッド ファブリック内での Any-to-Any の到達可能性が実現されます。ルーテッド ファブリックは、IPv4 または IPv6 ベースにすることができます。IPv6 ルーテッド ファブリックは IPv6 を使用して、ファブリック内接続とルート アドバタイズメントを構築します。IPv6 ルーテッド ファブリックは、ファブリック内リンクにリンク ローカル アドレスを割り当て、RFC 5549 をサポートして、IPv6 ネクスト ホップを使用した IPv4 ルート アドバタイジングを可能にします。スイッチ ロール リーフ、スパイン、ボーダー、スーパー スパイン、およびボーダー スーパー スパインがサポートされています。

eBGP ベースのファブリックの作成

1. **[LAN]** > **[ファブリック（Fabrics）]** を選択します。
2. **[アクション（Actions）]** ドロップダウンリストから、**[ファブリックの作成（Create Fabric）]** を選択します。

   [ファブリックの作成（Create Fabric）] ウィンドウが表示されます。

   フィールドについて説明します。

   [ファブリック名（Fabric Name）]：ファブリックの名前を入力します。

[ファブリックのテンプレート（Fabric Template）]：**Easy_Fabric_eBGP** ファブリック テンプレートを選択するには、これをクリックします。スタンドアロン ファブリックを作成するためのファブリック設定が表示されます。[選択（Select）] をクリックします。

3. デフォルトでは、**[全般パラメータ（General Parameters）]** タブが表示されます。

4. **[一般パラメータ（General Parameters）]** タブには以下のフィールドがあります。

   [スパインの BGP ASN（BGP ASN for Spines）]：ファブリックのスパイン スイッチの BGP AS 番号を入力します。

   [BGP AS モード（BGP AS Mode）]：**Multi-AS** または **Same-Tier-AS** を選択します。

   Multi-AS ファブリックでは、スパイン スイッチには一意の BGP AS 番号があり、各リーフ スイッチには一意の AS 番号があります。2 つのリーフ スイッチが vPC スイッチ ペアを形成している場合、それらは同じ AS 番号を持ちます。

   Same-Tier-AS ファブリックでは、スパイン スイッチには一意の BGP AS 番号があり、リーフ スイッチには一意の AS 番号があり、ボーダーは 1 つの AS を共有します。同じ役割を持つリーフ スイッチまたはボーダー スイッチは、異なる AS を持つことはできません。

   リーフとボーダーは、同じ AS を持つことも、異なる AS を持つこともできます。

   ファブリックは、スパイン スイッチの AS 番号によって識別されます。

   [手動アンダーレイ IP アドレス割り当て（Manual Underlay IP Address Allocation）]：**[手動アンダーレイ IP アドレス割り当て（Manual Underlay IP Address Allocation）]** チェックボックスをオンにして、動的アンダーレイ IP アドレス割り当てを無効にします。

5. **[EVPN]** をクリックします。[EVPN VXLAN オーバーレイを有効にする（Enable EVPN VXLAN Overlay）] オプションを明示的に無効にする必要があります。このチェックボックスはデフォルトで有効になっていることに注意してください。このオプションは、顧客が eBGP アンダーレイ/オーバーレイ ベースの VXLAN EVPN ファブリックを構築することを望むユースケースでのみ有効にします。

   [ルーテッド ファブリック（Routed Fabric）]：ルーテッド ファブリックでは、スパイン リーフ ネットワーク間の IP 到達可能性が確立されると、選択したファースト ホップ ルーティング プロトコル （FHRP）として HSRP または VRRP を使用し、リーフ上にネットワークを簡単に作成して展開することができます。

   eBGP ルーテッド ファブリックを作成すると、ファブリックは eBGP をコントロール プレーンとして使用して、ファブリック内接続を構築します。スパイン スイッチとリーフ スイッチ間のリンクは、eBGP ピアリングがその上に構築される、ポイント ツー ポイント（p2p）番号付き IP アドレスで自動構成されます。

   Routed_Network_Universal テンプレートは、ルーテッド ファブリックにのみ適用されることに注意してください。

   [ファースト ホップ冗長性プロトコル（First Hop Redundancy Protocol）]：FHRP プロトコルを指定します。**hsrp** または **vrrp** のいずれかを選択します。このフィールドは、ルーテッド ファブリックにのみ適用されます。

Note

- ネットワークの作成後に、このファブリック設定を変更することはできません。変更する場合は、すべてのネットワークを削除してから、FHRP 設定を変更する必要があります。
- [EVPN] タブ セクションの残りのフィールドは、EVPN VXLAN オーバーレイを有効にする場合にのみ適用されます。

6. **[vPC]** をクリックします。このタブのフィールドは次のとおりです。

   [vPC ピア リンク VLAN（vPC Peer Link VLAN）]：vPC ピア リンク SVI に使用される VLAN です。

   [vPC ピア リンク VLAN をネイティブ VLAN とする（Make vPC Peer Link VLAN as Native VLAN）]：vPC ピア リンク VLAN をネイティブ VLAN として有効にします。

   [vPC ピア キープアライブ オプション（vPC Peer Keep Alive option）]：管理またはループバック オプションを選択します。管理ポートおよび管理 VRF に割り当てられた IP アドレスを使用する場合は、[管理（management）] を選択します。ループバック インターフェイス（および非管理 VRF）に割り当てられた IP アドレスを使用する場合は、ループバックを選択します。IPv6 アドレスを使用する場合は、ループバック ID を使用する必要があります。

   [vPC 自動回復時間（vPC Auto Recovery Time）]：vPC 自動回復タイムアウト時間を秒単位で指定します。

   [vPC 遅延復元時間（vPC Delay Restore Time）]：vPC 遅延復元時間を秒単位で指定します。

   [vPC ピア リンク ポート チャネル番号（vPC Peer Link Port Channel Number）]：vPC ピア リンクのポート チャネル ID を指定します。デフォルトでは、このフィールドの値は 500 です。

   [vPC IPv6 ND 同期（vPC IPv6 ND Synchronize）]：vPC スイッチ間の IPv6 ネイバー探索同期を有効にします。チェック ボックスはデフォルトでオンになっています。この機能を無効にするには、チェック ボックスをオフにします。

   [vPC advertise-pip]：アドバタイズ PIP 機能を有効にするには、**[vPC advertise-pip]** チェックボックスをオンにします。

   特定の vPC で アドバタイズ PIP 機能をイネーブルにすることもできます。

   [すべての vPC ペアで同じ vPC ドメイン ID を有効にする（Enable the same vPC Domain Id for all vPC Pairs）]：**[すべての vPC ペアで同じ vPC ドメイン ID を有効にする（Enable the same vPC Domain Id for all vPC Pairs）]** チェックボックスをオンにします。このフィールドを選択すると、**[vPC ドメイン ID（vPC Domain Id）]** フィールドが編集可能になります。

   [vPC ドメイン ID（vPC Domain Id）]：すべての vPC ペアで使用される vPC ドメイン ID を指定します。

[vPC ドメイン ID の範囲（vPC Domain Id Range）]：新しいペアリングに使用する vPC ドメイン ID の範囲を指定します。

[ファブリック vPC ピアリングの QoS を有効にする（Enable QoS for Fabric vPC-Peering）]：スパインの QoS を有効にして、vPC ファブリック ピアリング通信の配信を保証します。

Note ファブリック設定の vPC ファブリック ピアリングとキューイング ポリシーの QoS オプションは相互に排他的です。

[QoS ポリシー名（QoS Policy Name）]：すべてのファブリック vPC ピアリング スパインで同じにする必要がある QoS ポリシー名を指定します。

デフォルト名は [spine_qos_for_fabric_vpc_peering] です。

7. **[プロトコル（Protocols）]**をクリックします。このタブのフィールドは次のとおりです。

[ルーティング ループバック ID（Routing Loopback Id）]：ループバック インターフェイス ID は、デフォルトで 0 として設定されます。BGP ルータ ID として使用されます。

[BGP 最大パス（BGP Maximum Paths）]：BGP 最大パスを指定します。

[BGP 認証を有効にする（Enable BGP Authentication）]：**[BGP 認証を有効にする（Enable BGP Authentication）]**チェックボックスをオンにして BGP 認証を有効にします。チェックボックスをオフにして無効にします。このフィールドを有効にすると、[BGP 認証キー暗号化タイプ（BGP Authentication Key Encryption Type）] および [BGP 認証キー（BGP Authentication Key）] フィールドが有効になります。

[BGP 認証キー暗号化タイプ（BGP Authentication Key Encryption Type）]：3DES 暗号化タイプの場合は 3、Cisco 暗号化タイプの場合は 7 を選択します。

[BGP 認証キー（BGP Authentication Key）]：暗号化タイプに基づいて暗号化キーを入力します。

Note プレーン テキスト パスワードはサポートされていません。スイッチにログインし、暗号化されたキーを取得して、[BGP 認証キー（BGP Authentication Key）] フィールドに入力します。詳細については、「認証キーの取得」の項を参照してください。

[BFD の有効化（Enable BFD）]：**[BFD の有効化（Enable BFD）]**チェックボックスは、ファブリック内のすべてのスイッチで**機能 bfd** を有効にする場合にオンにします。この機能は、IPv4 アンダーレイでのみ有効で、範囲はファブリック内にあります。

NDFC は、ファブリック内の BFD をサポートします。ファブリック設定では、BFD 機能はデフォルトで無効になっています。有効にすると、デフォルト設定のアンダーレイ プロトコルに対して BFD が有効になります。カスタムの必須 BFD 構成は、スイッチごとの自由形式またはインターフェイスごとの自由形式ポリシーを使用して展開する必要があります。

[BFD の有効化（Enable BFD）] チェックボックスをオンにすると、次の構成がプッシュされます。

```
feature bfd
```

Note BFD が有効になっている NDFC では、次の構成がすべての P2P ファブリック インターフェイスにプッシュされます。

```
no ip redirects
no ipv6 redirects
```

BFD機能の互換性については、それぞれのプラットフォームのマニュアルを参照してください。サポートされているソフトウェアイメージについては、*Compatibility Matrix for Cisco*を参照してください。

[BGP 向け BFD を有効にする（Enable BFD for BGP）]：**[BGP 向け BFD を有効にする（Enable BFD for BGP）]** チェックボックスをオンにして、BGP ネイバーの BFD を有効にします。このオプションは、デフォルトで無効です。

[BFD 認証を有効にする（Enable BFD Authentication）]：**[BFD 認証を有効にする（Enable BFD Authentication）]** チェックボックスをオンにして、BFD 認証を有効にします。このフィールドを有効にすると、[BFD 認証キー ID（BFD Authentication Key ID）] フィールドと [BFD 認証キー（BFD Authentication Key）] フィールドが編集可能になります。

[BFD 認証キー ID（BFD Authentication Key ID）]：インターフェイス認証の BFD 認証キー ID を指定します。

[BFD 認証キー（BFD Authentication Key）]：BFD 認証キーを指定します。

BFD認証パラメータを取得する方法については、『*Cisco NDFC* ファブリック コントローラ構成ガイド』の「暗号化された *BFD* 認証キーの取得」を参照してください。

8. [詳細設定（Advanced）] をクリックします。このタブのフィールドは次のとおりです。

[ファブリック内インターフェイス MTU（Intra Fabric Interface MTU）]：ファブリック内インターフェイスの MTU を指定します。この値は偶数にする必要があります。

[レイヤ 2 ホスト インターフェイス MTU（Layer 2 Host Interface MTU）]：レイヤ 2 ホスト インターフェイスの MTU を指定します。この値は偶数にする必要があります。

電源モード（Power Supply Mode）：適切な電源モードを選択します。

[CoPP プロファイル（CoPP Profile）]：ファブリックの適切なコントロール プレーン ポリシング（CoPP）プロファイル ポリシーを選択します。デフォルトでは、strict オプションが入力されます。

[VRF Lite サブネット IP 範囲（VRF Lite Subnet IP Range）] および **[VRF Lite サブネット マスク（VRF Lite Subnet Mask）]**：これらのフィールドには、DCI サブネットの詳細が入力されます。必要に応じて、次のフィールドを更新します。

[ブートストラップスイッチの CDP を有効にする（Enable CDP for Bootstrapped Switch）]：**[ブートストラップスイッチの CDP を有効にする（Enable CDP for Bootstrapped Switch）]** チェックボックスをオンにして、ブートストラップスイッチの CDP を有効にします。

[NX-API の有効化（Enable NX-API）]：HTTPS での NX-API の有効化を指定します。このチェックボックスは、デフォルトでオンになっています。

[HTTP での NX-API の有効化（Enable NX-API on HTTP）]：HTTP での NX-API の有効化を指定します。HTTP を使用するには、**[HTTP での NX-API の有効化（Enable NX-API on HTTP）]** チェックボックスと **[NX-API の有効化（Enable NX-API）]** チェックボックスをオンにします。このチェックボックスは、デフォルトでオンになっています。このチェックボックスをオフにすると、エンドポイント ロケータ（EPL）、レイヤ 4〜レイヤ 7 サービス（L4ーL7 サービス）、VXLAN OAM など、NX-API を使用し、Cisco がサポートするアプリケーションは、HTTP ではなく HTTPS を使用するようになります。

Note **[NX-API の有効化（Enable NX-API）]** と **[HTTP での NX-API の有効化（Enable NX-API on HTTP）]** チェックボックスをオンにすると、アプリケーションは HTTP を使用します。

[厳密な構成コンプライアンスの有効化（Enable Strict Config Compliance）]：**[厳密な構成コンプライアンスの有効化（Enable Strict Config Compliance）]** チェックボックスをオンにして、この機能を有効にします。

厳密な構成コンプライアンスについては、*Enhanced Monitoring and Monitoring Fabrics Guide*を参照してください。

Note ファブリックで厳密な構成コンプライアンスが有効になっている場合、Cisco NDFC のリソースで Network Insights を展開することはできません。

[AAA IP 認証の有効化（Enable AAA IP Authorization）]：AAA サーバーで IP 認証が有効になっている場合に、AAA IP 認証を有効にします。

[DCNM をトラップ ホストとして有効にする（Enable DCNM as Trap Host）]：**[DCNM をトラップ ホストとして有効にする（Enable DCNM as Trap Host）]** チェックボックスをオンにして、NDFC をトラップ ホストとして有効にします。

[TCAM 割り当ての有効化（Enable TCAM Allocation）]：TCAM コマンドは、有効にすると VXLAN および vPC ファブリック ピアリングに対して自動的に生成されます。

[グリーンフィールド クリーンアップ オプション（Greenfield Cleanup Option）]：スイッチをリロードせずにスイッチのグリーンフィールド クリーンアップ オプションを有効にします。このオプションは、通常、Cisco Nexus 9000v スイッチを使用するデータセンター環境でのみ推奨されます。

[デフォルト キューイング ポリシーの有効化（Enable Default Queuing Policies）]：**[デフォルト キューイング ポリシーの有効化（Enable Default Queuing Policies）]** チェックボックスをオンにして、このファブリック内のすべてのスイッチにQoSポリシーを適用します。すべてのスイッチに適用したQoSポリシーを削除するには、このチェックボックスをオフにし、すべての設定を更新してポリシーへの参照を削除し、保存して展開します。さまざまなCisco Nexus 9000シリーズ スイッチに使用できる定義済みのQoS設定が含まれています。このチェックボックスをオンにすると、適切なQoS設定がファブリック内のスイッチにプッシュされます。システムキューイングは、設定がスイッチに展開されると更新されます。インターフェイスごと自由形式ブロックに必要な設定を追加することにより、必要に応じて、定義されたキューイング ポリシーを使用してインターフェイス マーキングを実行できます。

テンプレート エディタでポリシー ファイルを開いて、実際のキューイング ポリシーを確認します。Cisco NDFC Web UIから、**[操作（Operations）]** > **[テンプレート（Templates）]**の順に選択します。ポリシー ファイル名でキューイング ポリシーを検索します（例：[queuing_policy_default_8q_cloudscale]）。ファイルを選択し、**[テンプレートの変更/表示（Modify/View template）]** アイコンをクリックしてポリシーを編集します。

プラットフォーム特有の詳細については、『*Cisco Nexus 9000 Series NX-OS Quality of Service* コンフィグレーション ガイド』を参照してください。

[N9K クラウド スケール プラットフォームのキューイング ポリシー（N9K Cloud Scale Platform Queuing Policy）]：ファブリック内のEX、FX、およびFX2で終わるすべてのCisco Nexus 9200シリーズスイッチおよびCisco Nexus 9000シリーズスイッチに適用するキューイング ポリシーをドロップダウン リストから選択します。有効な値は[queuing_policy_default_4q_cloudscale]および[queuing_policy_default_8q_cloudscale]です。FEXには[queuing_policy_default_4q_cloudscale]ポリシーを使用します。FEXがオフラインの場合にのみ、[queuing_policy_default_4q_cloudscale]ポリシーから[queuing_policy_default_8q_cloudscale]ポリシーに変更できます。

[N9K R シリーズ プラットフォーム キューイング ポリシー（N9K R-Series Platform Queuing Policy）]：ドロップダウンリストから、ファブリック内のRで終わるすべてのCisco Nexusスイッチに適用するキューイング ポリシーを選択します。有効な値は[queuing_policy_default_r_series]です。

[その他の N9K プラットフォーム キューイング ポリシー（Other N9K Platform Queuing Policy）]：ドロップダウンリストからキューイングポリシーを選択し、ファブリック内にある、上記2つのオプションで説明したスイッチ以外の他のすべてのスイッチに適用します。有効な値は[queuing_policy_default_other]です。

[MACsecの有効化（Enable MACsec）]：ファブリックのMACsecを有効にします。詳細については、Easy ファブリックおよび eBGP ファブリックでの MACsec サポートを参照してください。

[リーフの自由形式の構成（Leaf Freeform Config）]：リーフ、ボーダー、およびボーダーゲートウェイのロールを持つスイッチに追加するCLIです。

[スパインの自由形式の構成（Spine Freeform Config）]：スパイン、ボーダー スパイン、ボーダー ゲートウェイ スパイン、およびスーパー スパインのロールを持つスイッチに追加する CLI です。

[ファブリック内リンクの追加構成（Intra-fabric Links Additional Config）]：ファブリック内リンクに追加する CLI です。

9. **[管理性（Manageability）]** をクリックします。このタブのフィールドは次のとおりです。

   [DNS サーバー IP（DNS Server IPs）]：DNS サーバーの IP アドレス（v4/v6）のカンマ区切りリストを指定します。

   [DNS サーバー VRF（DNS Server VRFs）]：すべての DNS サーバーに 1 つの VRF を指定するか、DNS サーバーごとに 1 つの VRF を、カンマ区切りリストで指定します。

   [NTP サーバー IP（NTP Server IPs）]：NTP サーバーの IP アドレス（v4/v6）のカンマ区切りリストを指定します。

   [NTP サーバー VRF（NTP Server VRFs）]：すべての NTP サーバーに 1 つの VRF を指定するか、NTP サーバーごとに 1 つの VRF を、カンマ区切りリストで指定します。

   [Syslog サーバー IP（Syslog Server IPs）]：syslog サーバーの IP アドレスのカンマ区切りリスト（v4/v6）を指定します（使用する場合）。

   [Syslog サーバーのシビラティ（重大度）（Syslog Server Severity）]：syslog サーバーごとに、1 つの syslog シビラティ（重大度）値のカンマ区切りリストを指定します。最小値は 0 で、最大値は 7 です。高い重大度を指定するには、大きい数値を入力します。

   [Syslog サーバー VRF（Syslog Server VRFs）]：すべての syslog サーバーに 1 つの VRF を指定するか、syslog サーバーごとに 1 つの VRF を指定します。

   [AAA 自由形式の構成（AAA Freeform Config）]：AAA 自由形式の構成を指定します。

   ファブリック設定で AAA 構成が指定されている場合は、**switch_freeform** PTI で、ソースが **UNDERLAY_AAA**、説明が **AAA Configurations** であるものが作成されます。

10. **[ブートストラップ（Bootstrap）]** タブをクリックします。このタブのフィールドは次のとおりです。

    [ブートストラップを有効にする（Enable Bootstrap）]：**[ブートストラップを有効にする（Enable Bootstrap）]** チェックボックスをオンにして、ブートストラップ機能を有効にします。

    ブートストラップをイネーブルにした後、次のいずれかの方法を使用して、DHCP サーバで IP アドレスの自動割り当てをイネーブルにできます。

    - 外部 DHCP サーバ（External DHCP Server）：[スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）] および [スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）] フィールドに外部 DHCP サーバに関する情報を入力します。

- ローカル DHCPサーバー（Local DHCP Server）：**[ローカル DHCP サーバー（Local DHCP Server）]**チェックボックスをオンにして、残りの必須フィールドに詳細を入力します。

[ローカル DHCP サーバーを有効にする（Enable Local DHCP Server）]：ローカルDHCPサーバーを介した自動 IP アドレス割り当ての有効化を開始するには、**[ローカル DHCP サーバーを有効にする（Enable Local DHCP Server）]** チェックボックスをオンにします。このチェックボックスをオンにすると、**[DHCP スコープ開始アドレス（DHCP Scope Start Address）]** および **[DHCP スコープ終了アドレス（DHCP Scope End Address）]** フィールドが編集可能になります。

このチェックボックスをオンにしない場合、NDFC は自動 IP アドレス割り当てにリモートまたは外部の DHCP サーバーを使用します。

[DHCP バージョン（DHCP Version）]：このドロップダウンリストから [DHCPv4] または [DHCPv6] を選択します。DHCPv4 を選択すると、**[スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）]** フィールドが無効になります。DHCPv6 を選択すると、**[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]** は無効になります。

Note Cisco IPv6 POAP は、Cisco Nexus 7000 シリーズ スイッチではサポートされていません。Cisco Nexus 9000 および 3000 シリーズ スイッチは、スイッチが L2 隣接（eth1 またはアウトオブバンド サブネットは /64 が必須）、またはスイッチがいくつかの IPv6 /64 サブネット内に存在する L3 隣接である場合にのみ、IPv6 POAP をサポートします。/64 以外のサブネット プレフィックスはサポートされません。

[DHCP スコープ開始アドレス（DHCP Scope Start Address）] および **[DHCP スコープ終了アドレス（DHCP Scope End Address）]**：スイッチ アウトオブバンド POAP に使用される IP アドレス範囲の最初と最後の IP アドレスを指定します。

[スイッチ管理デフォルト ゲートウェイ（Switch Mgmt Default Gateway）]：スイッチの管理 VRF のデフォルト ゲートウェイを指定します。

[スイッチ管理 IP サブネット プレフィックス（Switch Mgmt IP Subnet Prefix）]：スイッチの Mgmt0 インターフェイスのプレフィックスを指定します。プレフィックスは 8 ～ 30 の間である必要があります。

DHCP スコープおよび管理デフォルト ゲートウェイ *IP* アドレスの仕様（*DHCP scope and management default gateway IP address specification*）：管理デフォルト ゲートウェイ IP アドレスを 10.0.1.1 に、サブネット マスクを 24 に指定した場合、DHCP スコープが指定したサブネット、10.0.1.2～10.0.1.254 の範囲内であることを確認してください。

スイッチ管理 IPv6 サブネット プレフィックス（Switch Mgmt IPv6 Subnet Prefix）：スイッチの Mgmt0 インターフェイスの IPv6 プレフィックスを指定します。プレフィックスは 112 ー 126 の範囲で指定する必要があります。このフィールドは DHCP の IPv6 が有効な場合に編集できます。

[AAA 構成を有効にする（Enable AAA Config）]：**[AAA 構成を有効にする（Enable AAA Config）]**チェックボックスをオンにして、デバイスの起動時に**[管理性（Manageability）]**タブからの AAA 構成が含められるようにします。

[ブートストラップ フリーフォームの設定（Bootstrap Freeform Config）]：（オプション）必要に応じて追加のコマンドを入力します。たとえば、AAA またはリモート認証関連の構成を使用している場合は、このフィールドにこれらの構成を追加してインテントを保存する必要があります。デバイスが起動すると、[Bootstrap Freeform Config]フィールドで定義されたインテントが含まれます。

NX-OSスイッチの実行コンフィギュレーションに示されているように、running-configを正しいインデントで自由形式の設定フィールドにコピーアンドペーストします。freeform config は running config と一致する必要があります。詳細については、スイッチでのフリーフォーム構成エラーの解決を参照してください。ファブリック スイッチでのフリーフォーム構成の有効化に記されています。

DHCPv4/DHCPv6 マルチ サブネット スコープ（DHCPv4/DHCPv6 Multi Subnet Scope）：1行に1つのサブネット スコープを入力して、フィールドを指定します。**[ローカル DHCP サーバーの有効化（Enable Local DHCP Server）]**チェックボックスをオンにした後で、このフィールドは編集可能になります。

スコープの形式は次の順で定義する必要があります。

[DHCP スコープ開始アドレス、DHCP スコープ終了アドレス、スイッチ管理デフォルト ゲートウェイ、スイッチ管理サブネット プレフィックス（DHCP Scope Start Address, DHCP Scope End Address, Switch Management Default Gateway, Switch Management Subnet Prefix）]

例：10.6.0.2、10.6.0.9、16.0.0.1、24

11. **[構成のバックアップ（Configuration Backup）]**をクリックします。このタブのフィールドは次のとおりです。

    [毎時ファブリック バックアップ（Hourly Fabric Backup）]：**[毎時ファブリック バックアップ（Hourly Fabric Backup）]**チェックボックスをオンにして、ファブリック構成とインテントの 1 時間ごとのバックアップを有効にします。

    新しいファブリック設定とインテントの1時間ごとのバックアップを有効にできます。前の時間に設定のプッシュがあった場合、NDFC はバックアップを取ります。

    インテントとは、NDFC に保存されているものの、まだスイッチにプロビジョニングされていない構成を指します。

    [スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）]：**[スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）]**チェックボックスをオンにして、毎日のバックアップを有効にします。このバックアップは、構成のコンプライアンスによって追跡されないファブリック デバイスの実行構成の変更を追跡します。

    [スケジュール済みの時間（Scheduled Time）]：スケジュールされたバックアップ時間を 24 時間形式で指定します。[スケジュール済みファブリック バックアップ（Scheduled Fabric Backup）]チェックボックスをオンにすると、このフィールドが有効になります。

    両方のチェックボックスをオンにして、両方のバックアップ プロセスを有効にします。

[保存（Save）]をクリックすると、バックアップ プロセスが開始されます。

Note 1 時間ごと、およびスケジュールされたバックアップ プロセスは、次の定期的な構成コンプライアンス アクティビティ中にのみ発生し、最大 1 時間の遅延が発生する可能性があります。即時バックアップをトリガーするには、次の手順を実行します。

a. **[LAN]** > **[トポロジ（Topology）]**を選択します。

b. 特定のファブリック ボックス内をクリックします。[ファブリック トポロジ (fabric topology)] 画面が表示されます。

c. 画面左側の [アクション（Actions）] ペインで、[ファブリックの再同期（Re-Sync Fabric）] をクリックします。

ファブリック トポロジ ウィンドウでファブリック バックアップを開始することもできます。[アクション（Actions）] ペインで [今すぐバックアップ（Backup Now）] をクリックします。

関連情報を入力して更新したら、**[保存（Save）]** をクリックします。

12. **[フロー モニタ（Flow Monitor）]** をクリックします。このタブのフィールドは次のとおりです。

[Netflow を有効にする（Enable Netflow）]：**[Netflow を有効にする（Enable Netflow）]** チェックボックスをオンにして、このファブリックの VTEP で Netflow を有効にします。デフォルトでは、Netflow は無効になっています。有効にすると、NetFlow 設定は、NetFlow をサポートするすべての VTEPS に適用されます。

Note ファブリックで Netflow が有効になっている場合、ダミーの no_netflow PTI を使用して、特定のスイッチで Netflow を使用しないように選択することができます。

netflow がファブリック レベルで有効になっていない場合、インターフェイス、ネットワーク、または vrf レベルで netflow を有効にすると、エラー メッセージが生成されます。Cisco NDFC の Netflow サポートについては、Netflow サポート を参照してください。

[Netflow エクスポータ（Netflow Exporter）] 領域で、**[アクション（Actions）]** > **[追加（Add）]**の順にクリックして、1 つ以上の Netflow エクスポータを追加します。このエクスポータは、Netflow データの受信側です。このタブのフィールドは次のとおりです。

- **[エクスポータ名（Exporter Name）]**：エクスポータの名前を指定します。
- **[IP]**：エクスポータの IP アドレスを指定します。
- **[VRF]**：エクスポータがルーティングされる VRF を指定します。
- **[送信元インターフェイス（Source Interface）]**：送信元インターフェイス名を入力します。

- **[UDP ポート（UDP Port）]**：Netflow データがエクスポートされる UDP ポートを指定します。

[保存（Save）] をクリックしてエクスポータを構成します。**[キャンセル（Cancel）]** をクリックして破棄します。既存のエクスポータを選択し、**[アクション（Actions）]**>**[編集（Edit）]**または**[アクション（Actions）]**>**[削除（Delete）]**を選択して、関連するアクションを実行することもできます。

[Netflow レコード（Netflow Record）] 領域で、**[アクション（Actions）]**>**[追加（Add）]** をクリックして、1 つ以上の Netflow レコードを追加します。この画面のフィールドは次のとおりです。

- **[レコード名（Record Name）]**：レコードの名前を指定します。
- **[レコード テンプレート（Record Template）]**：レコードのテンプレートを指定します。レコード テンプレート名の 1 つを入力します。リリース 12.0.2 では、次の 2 つのレコード テンプレートを使用できます。カスタム Netflow レコード テンプレートを作成できます。テンプレート ライブラリに保存されているカスタム レコード テンプレートは、ここで使用できます。
  - **netflow_ipv4_record**：IPv4 レコード テンプレートを使用します。
  - **netflow_l2_record**：レイヤ 2 レコード テンプレートを使用します。
- **[レイヤ 2 レコード（Is Layer2 Record）]**：レコードがレイヤ 2 Netflow の場合は、**[レイヤ 2 レコード（Is Layer2 Record）]** チェック ボックスをオンにします。

[保存（Save）]をクリックしてレポートを構成します。**[キャンセル（Cancel）]**をクリックして破棄します。既存のレコードを選択し、**[アクション（Actions）]**>**[編集（Edit）]** または**[アクション（Actions）]**>**[削除（Delete）]**を選択して、関連するアクションを実行することもできます。

[Netflow モニタ（Netflow Monitor）] 領域で、**[アクション（Actions）]** > **[追加（Add）]** の順にクリックして、1 つ以上の Netflow モニタを追加します。この画面のフィールドは次のとおりです。

- **[モニタ名（Monitor Name）]**：モニタの名前を指定します。
- **[レコード名（Record Name）]**：モニタのレコードの名前を指定します。
- **[エクスポータ 1 の名前（Exporter1 Name）]**：Netflow モニタのエクスポータの名前を指定します。
- **[エクスポータ 2 の名前（Exporter2 Name）]**：（オプション）Netflow モニタの副次的なエクスポータの名前を指定します。

各 netflow モニタで参照されるレコード名とエクスポータは、「**Netflow レコード（Netflow Record）**」と「**Netflow エクスポータ（Netflow Exporter）**」で定義する必要があります。

[保存（Save）]をクリックして、モニタを構成します。**[キャンセル（Cancel）]**をクリックして破棄します。既存のモニタを選択し、**[アクション（Actions）]**>**[編集（Edit）]**または**[アクション（Actions）]**>**[削除（Delete）]**を選択して、関連するアクションを実行することもできます。

13. [ファブリック（Fabric）] をクリックして、スライドイン ペインに概要を表示します。[起動（Launch）] アイコンをクリックして、[ファブリックの概要（Fabric Overview）] を表示します。

特筆すべき点

- ブラウンフィールド移行は、eBGP ファブリックではサポートされていません。
- リーフスイッチの AS 番号は、作成後に**再計算と展開（Recalculate & Deploy）**操作を実行した後は変更できません。変更が必要になった場合は、**leaf_bgp_asn** ポリシーを削除し、**再計算と展開（Recalculate & Deploy）**操作を実行して、この AS に関連する BGP 構成を削除する必要があります。次に、新しい AS 番号を使用して、leaf_bgp_asn ポリシーを追加できます。
- Multi-AS モードと Same-Tier-AS モードを切り替える場合は、モードを変更する前に、手動で追加されたすべての BGP ポリシー（リーフ スイッチの Leaf_bgp_asn および ebgp オーバーレイ ポリシーを含む）を削除し、**再計算と展開（Recalculate & Deploy）**操作を実行します。
- サポートされているロールは、リーフ、スパイン、スーパー スパイン、ボーダー リーフ、およびボーダー スーパー スパインです。
- ボーダーおよびスーパー スパイン ボーダー デバイスでは、VRF-Lite が手動モードでサポートされます

ファブリックへのスイッチの追加

各ファブリックのスイッチは一意であるため、各スイッチは1つのファブリックにのみ追加できます。ファブリックへのスイッチの追加 を参照してください。

ファブリック アンダーレイ eBGP ポリシーの展開

NDFC では、**Easy_Fabric_eBGP** テンプレートを持つファブリックが作成されます。1 つのスパイン スイッチと 3 つのリーフ スイッチがインポートされます。

ファブリックには次の 2 種類があります。

- **マルチ AS モード ファブリックの作成**：マルチ AS モード ファブリックでは、スパイン スイッチには共通の BGP AS 番号があり、各リーフ スイッチには一意の BGP AS 番号があります。Same-Tier-AS から Multi-AS モードへのファブリック変換にも同じ手順を使用します。

- **Same-Tier-AS モード ファブリックの作成**：Same-Tier-AS モード ファブリックの作成については、別の手順が説明されています。Multi-AS から Same-Tier-AS モードへのファブリック変換にも同じ手順を使用します。

  Same-Tier-AS ファブリックでは、すべてのスパイン スイッチには共通の BGP AS 番号があり、すべてのリーフ スイッチには共通の BGP AS 番号があります（スパイン スイッチの BGP AS 番号とは異なります）。次のセクションで説明するように、ポリシーを展開する必要があります。

ファブリック アンダーレイ eBGP ポリシーを展開するには、各リーフ スイッチに **leaf_bgp_asn** ポリシーを手動で追加して、スイッチで使用される BGP AS 番号を指定する必要があります。後ほど**再計算と展開**操作を実施すると、リーフ スイッチとスパイン スイッチ間の物理インターフェイス上に eBGP ピアリングが生成され、アンダーレイの到達可能性情報が交換されます。

必要なスイッチにポリシーを追加するには、ポリシーの追加およびポリシーの表示と編集を参照してください。

eBGP ベースのファブリックでのネットワークの展開

ルーテッド ファブリックのネットワークの概要

NDFC を使用して、ルーテッド ファブリックのトップダウン ネットワーク構成を作成できます。ルーテッド ファブリックは、1 つの VRF で実行されます。これがデフォルトの VRF です。ルーテッド ファブリックでは、VRF の手動作成は無効になっていることに注意してください。ファブリックは IPv4 ファブリックであるため、ネットワーク内の IPv6 アドレスはサポートされていません。ルーテッドファブリックでは、レイヤ 2 のみのネットワークでない限り、ネットワークは 1 つのデバイスまたは vPC デバイスのペアにのみアタッチできます。

Note ルーテッド ファブリック ネットワークの構成は、config-profile の下に置かれません。

eBGP ファブリックがルーテッド ファブリック（EVPN が無効）として構成されている場合、ファブリック レベルで、ホストトラフィックのファーストホップ冗長性プロトコル（FHRP）として HSRP または VRRP のいずれかを選択できます。HSRP がデフォルト値です。

vPC ペアの場合、NDFC はファブリック設定に基づいてネットワーク レベルで HSRP または VRRP 設定を生成します。HSRP を選択した場合、各ネットワークは 1 つの HSRP グループと HSRP VIP アドレスを持つように構成されます。デフォルトでは、すべてのネットワークは NDFC によって割り当てられた同じ HSRP グループ番号を共有しますが、これはネットワークごとに上書きできます。VRRP サポートは HSRP に似ています。

ガイドライン

- HSRP 認証または VRRP 認証はサポートされていません。認証を使用する場合は、ネットワークの自由形式構成に適切なコマンドを入力できます。

- vPC ピア ゲートウェイを使用すると、一部のサードパーティ デバイスが HSRP 仮想 MAC を無視し、ARP 学習に ARP パケット送信元 MAC を使用している場合に、ピア リンクの使用を最小限に抑えることができます。ルーテッド ファブリック モードでは、NDFC は VPC デバイスの vPC ピア ゲートウェイ コマンドを生成します。
- eBGP ファブリックで、ネットワークと VRF が存在する場合、ルーテッド ファブリック タイプと EVPN ファブリック タイプの間、または HSRP と VRRP の間で変更することはできません。ファブリック タイプまたは FHRP を変更する場合には、これらのネットワークと VRF を展開解除して削除する必要があります。詳細については、スタンドアロン ファブリックのネットワークの展開解除およびスタンドアロン ファブリックの *VRF* の展開解除を参照してください。
- ファブリックが以前にルーテッドファブリック モードで実行されていた場合、FHRP プロトコルやネットワーク VLAN 範囲などのデフォルトのファブリック値は、ルーテッドファブリックに対して内部的に設定されます。異なる値を構成する場合は、ファブリック設定を編集する必要があります。ネットワーク構成を展開する前に、FHRP プロトコル ファブリック設定を更新し、**[再計算して展開（Recalculate & Deploy）]** をクリックする必要があります。

ルーテッド ファブリックでのネットワークの作成と展開

この手順は、ルーテッド ファブリックでネットワークを作成して展開する方法を示しています。

Before you begin

ルーテッド ファブリックを作成し、必要なリーフおよびスパイン ポリシーを展開します。

Procedure

ステップ 1 次のナビゲーションパスのいずれかを選択します。

- **[LAN] > [ファブリック（Fabrics）]** を選択します。ファブリックをクリックして、**[ファブリック（Fabric）]** スライドイン ペインを開きます。**[起動（Launch）]** アイコンをクリックします。**[ファブリックの概要（Fabric Overview）] > [ネットワーク（Networks）]** を選択します。
- **[LAN] > [ファブリック（Fabrics）]** を選択します。ファブリックをダブルクリックして、**[ファブリック概要（Fabric Overview）] > [ネットワーク（Networks）]** を開きます。

ステップ 2 **[アクション（Actions）]** ドロップダウン リストから、**[作成（Create）]** を選択します。

[ネットワークの作成（Create Networks）] ウィンドウが表示されます。このウィンドウのフィールドは次のとおりです。

[ネットワーク名（Network Name）]：ネットワークの名前を指定します。ネットワーク名には、アンダースコア（_）とハイフン（-）以外の空白や特殊文字は使用できません。

[レイヤ 2 のみ（Layer 2 Only）]：（オプション）ネットワークがレイヤ 2 のみであるかどうかを指定します。FHRP 構成は、レイヤ 2 のみのネットワークでは生成されません。

Note L3 ネットワーク テンプレートがスタンドアロン デバイスにアタッチされている場合、FHRP 構成は生成されません。

[ネットワーク テンプレート（Network Template）]：**Routed_Network_Universal** テンプレートを選択します。

VLAN ID：（オプション）ネットワークの対応するテナント VLAN ID を指定します。

[ネットワーク プロファイル（Network Profile）] セクションには、[一般パラメータ（General Parameters）] タブと [詳細（Advanced）] タブがあります。

[一般パラメータ（General Parameters）] タブで、必要な詳細を指定します。

[アクティブ時のインターフェイス IPv4 アドレス（Intf IPv4 addr on active）]：vPC ペアのアクティブ デバイスの IPv4 インターフェイス アドレスを指定します。このフィールドは、デバイスの vPC ペア用にネットワークを作成して展開する場合にのみ適用されます。

[スタンバイ時のインターフェイス IPv4 アドレス（Intf IPv4 addr on standby）]：vPC ペアのスタンバイ/バックアップ デバイスの IPv4 インターフェイス アドレスを指定します。このフィールドは、デバイスの vPC ペア用にネットワークを作成して展開する場合にのみ適用されます。

[IPv4 ゲートウェイ/ネットマスク（IPv4 Gateway/NetMask）]：IPv4 ゲートウェイ アドレスとサブネットを指定します。

[アクティブ時のインターフェイス IPv6 アドレス（Interface IPv6 addr on active）]: vPC ペアのアクティブ デバイスの IPv6 インターフェイス アドレスを指定します。このフィールドは、デバイスの vPC ペア用にネットワークを作成して展開する場合にのみ適用されます。

[スタンバイ時のインターフェイス IPv6 アドレス（Interface IPv6 addr on standby）]：vPC ペアのスタンバイ/バックアップ デバイスの IPv6 インターフェイス アドレスを指定します。このフィールドは、デバイスの vPC ペア用にネットワークを作成して展開する場合にのみ適用されます。

[IPv6 リンク ローカル アドレス（IPv6 Link Local address）]：IPv6 リンク ローカル アドレスを指定します。このフィールドは、デバイスの vPC ペア用のネットワークを作成、展開しており、VRRP が FHRP プロトコルとして選択されている場合にのみ適用されます。

Note IPv4 ゲートウェイ アドレスとインターフェイス アドレスは同じサブネットになければなりません。

[一般パラメータ（General Parameters）] タブの次のフィールドはオプションです。

[Vlan 名（Vlan Name）]：VLAN 名を指定します。

[インターフェイスの説明 (Interface Description)]：インターフェイスの説明を指定します。

[スタンバイ インターフェイスの説明（Standby Intf Description）]：vPC ペアのスタンバイ インターフェイスの説明を指定します。

[L3 インターフェイスの MTU（MTU for L3 interface）]：レイヤ 3 インターフェイスの MTU を入力します。

[ルーティング タグ（Routing Tag）]：各ゲートウェイの IP アドレス プレフィックスに関連付けられているルーティング タグを指定します。

[詳細（Advanced）] タブ：このタブは、デバイスの vPC ペア用にネットワークを作成、展開している場合にのみ適用されます。

[ファースト ホップ冗長性プロトコル（First Hop Redundancy Protocol）]：ファブリック設定で選択された FHRP を指定する読み取り専用フィールド。

[アクティブ/マスター スイッチの優先度（Active/master Switch Priority）]：アクティブまたはマスター デバイスの優先度を指定します。

[スタンバイ/バックアップ スイッチの優先度（Standby/backup Switch Priority）]：スタンバイまたはバックアップデバイスの優先度を指定します。デフォルト値は 100 です。展開前にネットワーク構成をプレビューしても、このデフォルト値は表示されないことに注意してください。

[プリエンプトを有効にする（Enable Preempt）]：スタンバイ/バックアップ デバイスがアクティブ デバイスをプリエンプトできるかどうかを指定します。

[HSRP/VRRP グループ（HSRP/VRRP Group）]：HSRP または VRRP グループ番号を指定します。デフォルトでは、HSRP グループ番号は 1 です。

[仮想 MAC アドレス（Virtual MAC Address）]：オプション。仮想 MAC アドレスを指定します。デフォルトでは、VMAC は HSRP グループ番号（0000.0c9f.f000 + グループ番号）に基づいて内部的に生成されます。仮想 MAC アドレスは、ファブリック設定で **hsrp** が選択されている場合にのみ適用されます。

[HSRP バージョン（HSRP Version）]：HSRP バージョンを指定します。デフォルト値は 1 です。**[HSRP バージョン（HSRP Version）]** フィールドは、HSRP にのみ適用されます。

ステップ 3 [ネットワークの作成（Create Network）] をクリックします。詳細については、ネットワークを参照してください。

ステップ 4 **[ネットワーク アタッチメント（Network Attachment）]** ウィンドウで、vPC ペアに対し、デバイスにアクティブ状態を割り当てます。

アクティブ デバイスの場合は **[isActive]** チェックボックスをオンにし、スタンバイ デバイスの場合は **[isActive]** チェックボックスをオフにします。

[保存（Save）] をクリックします。

Note ルーテッドファブリックで、展開されたネットワークを編集し、変更を加えずに保存すると、ネットワークのステータスが **[保留中（Pending）]** に変わります。同様に、展開されたネットワークに対して **[ネットワーク アタッチメント（Network Attachment）]** ウィンドウを開き、変更せずに保存すると、ネットワークのステータスが **[保留中（Pending）]** に変わります。このような場合は、**[プレビュー（Preview）]** アイコンをクリックして構成をプレビューします。このアクションにより、ネットワーク ステータスが **展開済み（Deployed）** に戻ります。

ステップ 5 （オプション）**[プレビュー（Preview）]** アイコンをクリックして、デバイスに展開された構成をプレビューします。

[構成のプレビュー（Preview Configuration）] ウィンドウが表示されます。

ステップ 6 [展開（Deploy）] をクリックします。

[ファブリックの概要（Fabric Overview）] ウィンドウに移動し、**[展開（Deploy）]** ボタンをクリックして、ネットワークを展開することもできます。

ルーテッド ファブリックと外部ファブリック間のファブリック間リンクの作成

ファブリック間リンクを使用して、ルート ファブリックをエッジ ルータに接続できます。このリンクは、物理インターフェイスで IP アドレスを構成し、デフォルトの vrf でエッジ ルーターとの eBGP ピアリングを確立します。BGP 構成には、リーフ スイッチへのデフォルト ルートのアドバタイズが含まれます。

Note 外部ファブリック設定の **[ファブリック モニター モード（Fabric Monitor Mode）]** チェックボックスはオフにすることができます。**[ファブリック モニター モード（Fabric Monitor Mode）]** チェックボックスをオフにすると、NDFC が設定を外部ファブリックに展開できるようになります。詳細については、外部ファブリックの作成を参照してください。

Procedure

ステップ 1 **[LAN] > [ファブリック（Fabrics）]** を選択します。ルーティングされたファブリックをダブルクリックします。

[ファブリックの概要（Fabric Overview）] ウィンドウが表示されます。

ステップ 2 **[リンク（Links）]** タブで、**[アクション（Actions）] > [作成（Create）]** をクリックします。

[リンク管理 - リンクの作成（Link Management-Create Link）] ウィンドウが表示されます。

[リンク タイプ（Link Type）] : **[ファブリック間（Inter-Fabric）]** を選択して、2 つのファブリック間のボーダー スイッチを介するファブリック間接続を作成します。

[リンク サブタイプ（Link Sub-Type）] : このフィールドは IFC タイプを入力します。ドロップダウン リストから **[ROUTED_FABRIC]** プロファイルを選択します。

[リンク テンプレート（Link Template）] : リンク テンプレートが入力されます。テンプレートには、選択内容に基づいて、対応するパッケージ済みのデフォルトテンプレートが自動的に設定されます。ルーテッドファブリックの場合、**ext_routed_fabric** テンプレートが読み込まれます。

[送信元ファブリック（Source Fabric）] : このフィールドには、送信元ファブリック名が事前に入力されます。

[宛先ファブリック（Destination Fabric）] : このドロップダウンボックスから宛先ファブリックを選択します。

[送信元デバイス（Source Device）] と **[送信元インターフェイス（Source Interface）]**：宛先デバイスに接続する送信元デバイスとイーサネット インターフェイスまたはポート チャネル インターフェイスを選択します。ボーダーのロールを持つデバイスのみを選択できます。

[宛先デバイス（Destination Device）] と **[宛先インターフェイス（Destination Interface）]**：送信元デバイスに接続する宛先デバイスとイーサネット インターフェイスまたはポート チャネル インターフェイスを選択します。

送信元デバイスと送信元インターフェイスの選択に基づき、Cisco 検出プロトコル情報（使用可能な場合）に基づいて宛先情報が自動入力されます。宛先外部デバイスが宛先ファブリックの一部であることを確認するために、追加の検証が実行されます。

[一般パラメータ（General Parameters）] タブには、次のフィールドが含まれています。

[送信元 BGP ASN（Source BGP ASN）]：このフィールドには、**leaf_bgp_asn** ポリシーを作成して適用した場合、リーフの AS 番号が自動入力されます。

[送信元 IPv4 アドレス/マスク（Source IPv4 Address/Mask）]：宛先デバイスに接続する送信元インターフェイスの IP アドレスをこのフィールドに入力します。

[宛先 IPv4（Destination IPv4）]：このフィールドに宛先インターフェイスの IPv4 アドレスを入力します

[宛先 BGP ASN（Destination BGP ASN）]：このフィールドには、宛先デバイスの AS 番号が自動入力されます。

[送信元 IPv6 アドレス/マスク（Source IPv6 Address/Mask）]：宛先デバイスに接続する送信元インターフェイスの IP アドレスをこのフィールドに入力します。

[宛先 IPv6（Destination IPv6）]：このフィールドに宛先インターフェイスの IPv6 アドレスを入力します

[BGP の最大パス（BGP Maximum Paths）]：サポートされる最大の BGP パスを指定します。

[リンク MTU（Link MTU）]：このフィールドにインターフェイス MTU を入力します。

[デフォルト ルート構成を無効にする（Disable Default Route Config）]：**[デフォルト ルート構成を無効にする（Disable Default Route Config）]** チェック ボックスをオンにします。

[詳細設定（Advanced）] タブには、次のオプションのフィールドが含まれています。

[送信元インターフェイスの説明（Source Interface Description）] および **[宛先インターフェイスの説明（Destination Interface Description）]**：後で使用するためのリンクについて説明します。**保存して展開**すると、この説明が実行構成に反映されます。

[送信元インターフェイス フリーフォーム CLI（Source Interface Freeform CLIs）] および **[宛先インターフェイス フリーフォーム CLI（Destination Interface Freeform CLIs）]**：送信元と宛先インターフェイスに固有のフリーフォーム構成を入力します。スイッチの実行構成に表示されている設定を、インデントなしで追加する必要があります。詳細については、ファブリック スイッチでのフリーフォーム設定の有効化を参照してください。

ステップ 3 [保存（Save）] をクリックします。

ステップ 4 外部ファブリックのエッジ ルータに接続しているデバイスをダブルクリックし、**[アクション（Actions）] > [再計算と展開（Recalculate & Deploy）]** をクリックします。

ステップ 5 **[構成の展開（Deploy Configuration）]** ウィンドウで構成の展開が完了したら、**[閉じる（Close）]** をクリックします。

ステップ 6 **[LAN ファブリック（LAN Fabric）]** ウィンドウで外部ファブリックに移動し、ファブリックをダブルクリックします。

ステップ 7 **[リンク（Links）]** タブをクリックして、外部ファブリックのすべてのリンクを表示します。

作成されたファブリック間リンクが表示されます。

Note 外部ファブリックが監視モードでない場合、ファブリック間リンクが作成されます。

ステップ 8 **[LAN ファブリック（LAN Fabric）]** ウィンドウに移動します。

ステップ 9 ルーテッド ファブリックに接続している外部ファブリックをダブルクリックし、**[アクション（Actions）] > [再計算と展開（Recalculate & Deploy）]** をクリックします。

ステップ 10 **[構成の展開（Deploy Configuration）]** ウィンドウで構成の展開が完了したら、**[閉じる（Close）]** をクリックします。

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。