



ファブリックネットワークのプロビジョニング

- [ファブリックネットワークについて \(1 ページ\)](#)
- [ファブリック ドメインの設定 \(5 ページ\)](#)

ファブリックネットワークについて

ファブリックネットワークは、1つまたは複数の場所で単一のエンティティとして管理されるデバイスの論理グループです。ファブリックネットワークを使用すると、仮想ネットワークやユーザーおよびデバイスグループの作成、高度なレポート作成などが可能になります。その他の機能には、アプリケーション認識、トラフィック分析、トラフィックの優先順位付け、最適なパフォーマンスと運用効率のためのステアリングのインテリジェントサービスがあります。

Cisco DNA Center では、デバイスをファブリックネットワークに追加できます。これらのデバイスは、ファブリックネットワーク内のコントロールプレーン、ボーダーデバイスまたはエッジデバイスとして機能するように設定できます。

ファブリック サイトとファブリック ドメイン

ファブリックサイトは、コントロールプレーン、ボーダー、エッジ、ワイヤレスコントローラ、ISE PSN のネットワークデバイスの固有のセットを持つ独立したファブリック領域です。異なるレベルの冗長性とスケールは、DHCP、AAA、DNS、インターネットなどのローカルリソースを含むことにより、サイトごとに設計することができます。

ファブリックサイトは、単一の物理的ロケーション、複数のロケーション、またはロケーションのサブセットのみをカバーすることができます。

- 単一の場所: ブランチ、キャンパスまたはメトロ キャンパス
- 複数の場所: メトロ キャンパス + 複数ブランチ
- ロケーションのサブセット: キャンパス内での構築または領域

ファブリックドメインは、1つ以上のファブリックサイトとトランジットサイトで構成できます。複数のファブリックサイトは、トランジットサイトを使用して互いに接続されます。¥トランジットサイトには2つのタイプがあります。

- **SD-Access トランジット**: サイト間通信のためのドメイン全体のコントロールプレーンノードでネイティブ SD-Access (LISP、VXLAN、CTS) ファブリックを有効にします。
- **IP ベース トランジット**: 従来型の IP ベース (VRF-LITE、MPLS) ネットワークを利用します。これは、サイト間で VRF と SGT のマッピングを必要とします。

マルチサイトファブリックドメイン

マルチサイトファブリックドメインは、トランジットサイト経由で相互接続されたファブリックサイトの集合体です。ファブリックサイトは、コントロールプレーンノード、ボーダーノード、およびエッジノードの独自のセットを持つファブリックの一部です。指定されたファブリックサイトもまた、ファブリック WLC と AP、および関連するサイト指定の ISE PSN も含みます。単一のファブリックドメインに含まれる複数のファブリックサイトは、トランジットサイトを使用して相互接続されます。

Software-Defined Access (SDA) ファブリックは、複数のサイトで構成されることがあります。各サイトは、優れた拡張性、復元力、生存性、およびモビリティを備えます。サイトの全体的な集約 (すなわち、ファブリックドメイン) には、非常に多くのエンドポイントに対応できることや、各サイト内に含まれるサイトを集約することによってモジュール方式で (または水平方向に) 拡張できることも要求されます。

トランジットサイト

トランジットサイトとは、2つ以上のファブリックサイトを相互に接続したり、ファブリックサイトと外部ネットワーク (インターネット、データセンターなど) を接続するサイトです。トランジットネットワークには2つのタイプがあります。

- **IP トランジット**: 通常の IP ネットワークを使用して、外部ネットワークに接続するか2つ以上のファブリックサイトを接続します。
- **SDA トランジット**: LISP/VxLAN のカプセル化を使用して2つのファブリックサイトを接続します。SDA トランジットエリアは、独自のコントロールプレーンノードを持つがエッジノードやボーダーノードはないファブリックの一部として定義できます。ただし、外部ボーダーを持つファブリックを使用することもできます。SDA トランジットを使用すると、エンドツーエンドポリシープレーンは SGT グループタグを使用して維持されます。

IP のトランジットネットワークの作成

新しい IP トランジットネットワークを追加するには、次の手順に従います。

ステップ 1 Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [Fabric] の順に選択します。

- ステップ2 [Add Fabric or Transit/Peer Network] にマウスポインタを合わせます。
- ステップ3 ドロップダウンリストで [Transit/Peer Network] をクリックします。
- ステップ4 ネットワークのトランジットの名前を入力します。
- ステップ5 トランジットタイプとして、**IP ベース** を選択します。
ルーティングプロトコルが BGP にデフォルトとして設定されます。
- ステップ6 トランジットネットワークの自律システム番号 (ASN) を入力します。
- ステップ7 [Save] をクリックします。

SDA トランジット ネットワークの作成

新しい SDA トランジット ネットワークを追加するには、次の手順に従います。

- ステップ1 Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [Fabric] の順に選択します。
- ステップ2 [Add Fabric or Transit/Peer Network] にマウスポインタを合わせます。
- ステップ3 ドロップダウンメニューで [Transit/Peer Network] をクリックします。
- ステップ4 ネットワークのトランジットの名前を入力します。
- ステップ5 トランジットタイプとして [SD-Access] を選択します。
- ステップ6 このトランジットネットワークのトランジット コントロール プレーンのサイトを入力します。少なくとも1つのトランジットマップサーバーを選択します。
- ステップ7 このトランジットネットワークのトランジット コントロール プレーンを入力します。
- ステップ8 2番目のマップサーバーを追加するには、手順7と手順8を繰り返します。
- ステップ9 [Save] をクリックします。

次のタスク

SDA トランジットの作成後、ファブリックサイトに移動し、SDA トランジットを接続するサイトに接続します。[Provision] > [Fabric] > [Fabric Site] の順に移動します。作成したファブリックサイトを選択します。[Fabric Site] > [Border] > [Edit Border] > [Transit] の順にクリックします。ドロップダウンリストで SDA トランジットサイトをポイントし、[Add] をクリックします。

ファブリック ドメインの作成

Cisco DNA Center では、デフォルト LAN ファブリックと呼ばれるデフォルトのファブリックドメインが作成されます。

始める前に

ネットワークが設計されていること、ポリシーが Cisco Integrated Services Engine (ISE) から取得されているか Cisco DNA Center で作成されていること、デバイスがインベントリに登録され、サイトに追加されていることを確認してください。

-
- ステップ 1 Cisco DNA Center GUI で、[Menu] アイコン (≡) をクリックし、[Provision]>[Fabric] の順に選択します。
 - ステップ 2 [Add Fabric or Transit/Peer Network] にマウスポインタを合わせます。
 - ステップ 3 ポップアップから、[Add Fabric] をクリックします。
 - ステップ 4 ファブリック名を入力します。
 - ステップ 5 ファブリック サイトの 1 つを選択します。
 - ステップ 6 [Add] をクリックします。
-

ファブリックの準備状況とコンプライアンスのチェック

ファブリックの準備状況チェック

ファブリックの準備状況チェックは、デバイスがファブリックに追加される準備が整っていることを確認するために、デバイス上で実行される事前プロビジョニングチェックのセットです。ファブリックの準備状況チェックは、デバイスのプロビジョニング時に自動的に実行されるようになりました。インターフェイス VLAN とマルチ VRF の設定チェックは、ファブリックの準備状況チェックの一環としては行われません。

ファブリックの準備状況チェックには、次の項目が含まれます。

- 接続チェック：エッジノードからマップサーバーへの接続、エッジノードからボーダーへの接続など、デバイス間で必要な接続を確認します。
- 既存の設定チェック（ブラウフィールドチェック）：SD-Access を介してプッシュされる設定と競合する設定がデバイスにあり、それが後でエラーになる可能性がないかを確認します。
- ハードウェアバージョン：デバイスのハードウェアバージョンがサポートされているかどうかを確認します。
- イメージタイプ：サポートされているイメージタイプ（IOS XE、IOS、NXOS、Cisco Controller）を使用してデバイスが実行されているかどうかを確認します。
- ループバック インターフェイス：デバイス上のループバック インターフェイスの設定を確認します。SDA アプリケーションを使用するには、デバイスにループバック インターフェイスが設定されている必要があります。
- ソフトウェアライセンス：デバイスが適切なソフトウェアライセンスを使用して実行されているかどうかを確認します。

- ソフトウェアバージョン：デバイスが適切なソフトウェアイメージを使用して実行されているかどうかを確認します。

サポートされているソフトウェアバージョンの詳細については、「[Cisco SD-Access Hardware and Software Compatibility Matrix](#)」を参照してください。

ファブリックの準備状況チェックの実行中にエラーが検出された場合、エラー通知が[[topology](#)] エリアに表示されます。問題を修正し、デバイスのプロビジョニングワークフローを続行できます。

ファブリック コンプライアンス チェック

ファブリック コンプライアンスとは、ファブリック プロビジョニング中に設定されたユーザー インテントに従って動作するデバイスの状態です。ファブリック コンプライアンス チェックは、次の条件に基づいてトリガーされます。

- 有線デバイスの場合は 24 時間ごと、ワイヤレスデバイスの場合は 6 時間ごと。
- 有線デバイスで設定が変更された場合。

有線デバイスの設定変更によって SNMP トラップがトリガーされ、それによってコンプライアンスチェックがトリガーされます。Cisco DNA Center サーバーが SNMP サーバーとして設定されていることを確認します。

次のコンプライアンスチェックを実行し、デバイスがファブリックに準拠していることを確認します。

- 仮想ネットワーク：Cisco DNA Center 上の仮想ネットワークのユーザー インテントの現在の状態に準拠するように、必要な VRF がデバイスに設定されているかどうかを確認します。
- ファブリック ロール：デバイスの設定が Cisco DNA Center のファブリック ロールのユーザー インテントに準拠しているかどうかを確認します。
- セグメント：セグメントの VLAN 設定と SVI 設定を確認します。
- ポートの割り当て：VLAN および認証プロファイルのインターフェイス設定を確認します。

ファブリック ドメインの設定

デバイスをサイトに追加し、それらのデバイス（ボーダー、コントロールプレーン、またはエッジ）にロールを割り当てることができます。また、IP アドレスプールを設定してホスト間の通信を有効にできます。

ファブリックサイトの追加

始める前に

IP デバイストラッキング (IPDT) がすでにサイトに設定されている場合にのみ、新しいファブリックサイトを作成できます。つまり、サイトのテレメトリ設定を構成するときには、[Monitor wired clients] を有効にしておく必要があります。

-
- ステップ1 Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [Fabric] の順に選択します。
 - ステップ2 [Add Fabric or Transit/Peer Network] にマウスポインタを合わせます。
 - ステップ3 ドロップダウンリストから、[Fabric] をクリックします。
 - ステップ4 スライド表示された [Add Fabric Site] ペインで、サイトリストから表示する [Site] を選択します。
 - ステップ5 [Next] をクリックします。
 - ステップ6 ファブリックサイトに追加する仮想ネットワークを選択します。
 - ステップ7 [Finish] をクリックします。

サイトで IPDT がまだ有効になっていない場合 (ネットワークテレメトリ設定時に [Monitor Wire Clients] が選択されていない場合)、ファブリックサイトは追加されません。

ファブリックへのデバイスの追加

ファブリック ドメインを作成した後にファブリック サイトを追加してから、このファブリックサイトにデバイスを追加できます。また、デバイスがコントロールプレーンノード、エッジノード、またはボーダーノードとして機能する必要があるかどうかを指定することもできます。

IP デバイストラッキング (IPDT) がファブリックサイトに設定されている場合にのみ、新しいデバイスをファブリックサイトに追加できます。

アクセスロールが割り当てられ、サイトで IPDT を有効にする前にプロビジョニングされたデバイスは、ファブリックに追加できません。このようなデバイスは、ファブリックサイトに追加する前に再プロビジョニングしてください。プロビジョニングワークフローを調べて、デバイスでの [Deployment of IPDT] のステータスを確認します。



- (注)
- ファブリック ドメイン内のデバイスをコントロールプレーン ノードまたはボーダー ノードとして指定する手順はオプションです。それらの役割がないデバイスもあります。ただし、各ファブリック ドメインには、少なくとも1つのコントロールプレーン ノードデバイスと1つのボーダー ノードデバイスが存在する必要があります。有線ファブリックの現在のリリースでは、冗長性を確保するために最大6つのコントロールプレーン ノードを追加できます。
 - 現在、シスコ ワイヤレス コントローラは2つのコントロールプレーンノードとのみ通信します。

始める前に

デバイスをプロビジョニングします（まだプロビジョニングしていない場合）。

1. Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します **[Provision] > [Devices] > [Inventory]**。
2. [Inventory] ウィンドウに、検出されたデバイスが表示されます。
3. ファブリックの準備状況チェックに合格し、プロビジョニングする準備が整ったら、トポロジビューにデバイスがグレー色で表示されます。
4. ファブリックの準備状況チェックの実行中にエラーが検出された場合、エラー通知が [topology] エリアに表示されます。[See more details] をクリックして、結果のウィンドウに一覧表示された問題のあるエリアを確認します。問題を修正し、[Re-check] をクリックして問題が解決されていることを確認します。
5. 問題解決の一環としてデバイスの設定を更新する場合は、デバイスで **[Inventory] > [Resync]** を実行して、デバイス情報を再同期してください。



- (注) ファブリックの準備状況チェックに失敗しても、デバイスのプロビジョニングを続行できます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン（☰）をクリックして選択します **[Provision] > [Fabric]** の順に選択します。

すべてのプロビジョニングされたファブリック ドメインがウィンドウに表示されます。

ステップ 2 ファブリック ドメインのリストから、ファブリックを選択します。

結果の画面に、そのファブリック ドメイン内のすべてのサイトが表示されます。

ステップ 3 サイトを選択します。

インベントリされたネットワーク内のすべてのデバイスがトポロジビューに表示されます。ファブリックに追加されたデバイスは青色で表示されます。

ステップ 4 リストビューでデバイスをクリックします。スライドインウィンドウにデバイスの詳細が表示され、次の [Fabric] オプションが表示されます。

オプション	説明
エッジ	選択したデバイスをエッジノードとして有効にするには、このオプションの横にあるトグルボタンをクリックします。
ボーダー	選択したデバイスをボーダーノードとして有効にするには、このオプションの横にあるトグルボタンをクリックします。
コントロールプレーン	選択したデバイスをコントロールプレーンノードとして有効にするには、このオプションの横にあるトグルボタンをクリックします。

デバイスを一体型ファブリックとして設定するには、[Control Plane]、[Border]、および [Edge] オプションを選択します。

デバイスをコントロールプレーンおよびボーダーノードとして設定するには、[Control Plane] と [Border] の両方を選択します。

ステップ 5 [Add] をクリックします。

次のタスク

デバイスがファブリックに追加されると、ファブリック コンプライアンス チェックが自動的に実行され、デバイスがファブリックに準拠していることが確認されます。トポロジには、ファブリック コンプライアンス チェックに失敗したデバイスが青色で、横に十字マークが付いた状態で表示されます。エラー通知の [詳細の表示 (See more details)] をクリックして問題領域を特定し、修正します。

ボーダーノードとしてのデバイスの追加

ファブリックにデバイスを追加する場合、[ファブリックへのデバイスの追加 \(6 ページ\)](#) で説明したように、コントロールプレーン、ボーダーノード、またはエッジノードとして動作するようにさまざまな組み合わせで追加できます。

ボーダーノードとしてデバイスを追加するには、次の手順を実行します。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [Provision] > [Fabric] の順に選択します。

プロビジョニングされたすべてのファブリック ドメインのリストが表示されます。

ステップ 2 ファブリック ドメインのリストから、ファブリックを選択します。

すべてのファブリックサイトのリストが表示されます。

ステップ 3 ファブリックサイトのリストから、サイトを選択します。インベントリされたネットワーク内のすべてのデバイスが結果のトポロジビューに表示されます。トポロジ表示では、ファブリックに追加されるすべてのデバイスは青です。

- ステップ 4** デバイスをクリックします。
- ステップ 5** 表示されるスライドインウィンドウで、[Border] トグルボタンをクリックします。
- ステップ 6** 表示されたウィンドウで、[Layer 3 Handoff] タブをクリックします。
- ステップ 7** [Enable Layer-3 Handoff] チェックボックスを選択します。
- ステップ 8** デバイスの [ローカル自律番号 (Local Autonomous Number)] を入力します。
- ローカル自律番号がデバイスですでに設定されている場合は、その番号が表示され、このフィールドは無効になります。デバイスですでに設定されているローカル自律番号を変更することはできません。
- ステップ 9** [Select IP Pool] ドロップダウンリストから、IP アドレスプールを選択します。
- IP プールは IP トランジットネットワークを追加する場合にのみ選択します。
- ステップ 10** ボーダーデバイスで有効になっているトランジットネットワークを選択します。
- a) ボーダーで SDA トランジットを有効にするには、[Select Transit/Peer Network] ドロップダウンリストからユーザーが作成した SDA トランジットドメインを選択します。
- [Add] をクリックします。
- b) ボーダーで IP トランジットを有効にするには、[Select Transit/Peer Network] ドロップダウンリストからユーザーが作成した IP トランジットドメインを選択します。
- [Add] をクリックします。
- 表示されるウィンドウで、次の手順を実行します。
1. デザイン階層から IP プールを選択します。選択したプールは、ボーダーノードと IP ピア間で IP ルーティングを自動化するために使用されます。
 2. [インターフェイスの追加 (Add Interface)] をクリックして、次の画面でインターフェイスの詳細を入力します。
 3. ドロップダウンリストから [外部インターフェイス (External Interface)] を選択します。
 4. [Interface Description] で、インターフェイスのカスタム説明を入力します。
 5. [リモートAS番号 (Remote AS Number)] を入力します。
 6. リストで [仮想ネットワーク (Virtual Network)] をチェックします。この仮想ネットワークは、ボーダーによってリモートピアにアダプタイズされます。1つ、複数、またはすべての仮想ネットワークを選択できます。
 7. [Save] をクリックします。
- ステップ 11** デフォルトでは、ボーダーは外部ボーダーとして指定され、外部ルートを実ポートせずに、すべての不明なトラフィックへのゲートウェイとして機能します。ボーダーを内部ボーダーとして設定すると、既知のトラフィックへのゲートウェイとして、特定の外部ルートを実ポートするように設定できます。ボーダーには、内部ボーダーおよび外部ボーダーを組み合わせたロールを設定することもできます。
- ボーダーを外部ボーダーとして指定し、不明なネットワークへの接続を提供するには、[Default to all Virtual Networks] と [Do not Import External Routes] の両方のチェックボックスをオンにします。

- ボーダーを内部ボーダーとして指定し、特定のネットワークアドレスのゲートウェイとして動作させるには、[Default to all Virtual Networks] と [Do not Import External Routes] の両方のチェックボックスをオンにしないでください。
- このボーダーノードを内部および外部ボーダーとして指定するには、[Default to all Virtual Networks] チェックボックスをオンにします。これは、エッジノードから送信されたすべての既知のトラフィックおよび不明なトラフィックへのゲートウェイとして機能します。（[Do not Import External Routes] チェックボックスはオンにしないでください）。

ステップ 12 (オプション) ファブリックネットワークに非ファブリックネットワークを接続している場合、または従来のネットワークから SDA ネットワークに移行する場合にのみ、この手順を実行します。[Layer 2 Handoff] タブをクリックします。仮想ネットワークのリストと、各仮想ネットワークの IP プールの数が表示されます。

- a) ハンドオフする仮想ネットワークをクリックします。

仮想ネットワークを選択すると、仮想ネットワークに存在する IP アドレスプールのリストが表示されます。非ファブリックデバイスを接続できるインターフェイスのリストも表示されます。

- b) [External Interface] を選択してください。

Cisco DNA Center リリース 2.1.2.6 では、レイヤ 2 ハンドオフを実行できる複数のインターフェイスを選択できます。

- c) [Interface Description] に説明を入力します。

- d) ファブリックを拡張する必要がある [External VLAN] 番号を入力します。

Cisco DNA Center 2.1.2.6 より前のリリースでは、仮想ネットワークは 1 つのインターフェイスでのみハンドオフできます。複数のインターフェイス経由で同じ仮想ネットワークを処理することはできません。

Cisco DNA Center リリース 2.1.2.6 以降のリリースでは、仮想ネットワークは単一のインターフェイスまたは複数のインターフェイスでハンドオフできます。セグメントのレイヤ 2 ハンドオフを 2 つの異なるデバイスで実行することもできます。いずれの場合も、ネットワークにループが形成されていないことを確認します。

- e) [Save] をクリックします。

ステップ 13 [Add] をクリックします。

ホスト オンボーディングの設定

[Host Onboarding] タブでは、ファブリック ドメインにアクセスできる各種デバイスまたはホストの設定を指定することができます。

[Host Onboarding] タブには次のサブタブがあります。

- [Authentication] タブ：ファブリック用の認証テンプレートを選択します。認証テンプレートは、Cisco ISE から取得される一連の定義済みの設定です。認証テンプレートを選択したら、[Save] をクリックします。

- [Virtual Networks] タブ：IP アドレスプールを仮想ネットワーク（デフォルト、ゲスト、またはユーザー定義）に関連付け、[Update] をクリックします。表示される IP アドレスプールは、サイト固有のプールのみです。
- [Wireless SSIDs] タブ：ホストがアクセスできるネットワーク内のワイヤレス SSID を指定します。ゲスト SSID またはエンタープライズ SSID を選択してアドレスプールを割り当て、[保存 (Save)] をクリックできます。
- [Port Assignment] タブ：ファブリックドメインに接続するデバイスのタイプに応じて、各ポートに固有の設定を適用します。これを行うには、固有の割り当てが必要なポートを選択し、[Assign] をクリックして、ドロップダウンリストからポートタイプを選択します。

次の制約事項に注意してください。

- Cisco SD-Access 展開環境では、AP、拡張ノード、およびユーザーデバイス（単一のコンピュータまたは単一のコンピュータと電話機など）と、トランクポートを必要とするデバイス（単一サーバーなど）のみがサポートされます。
- 内部スイッチまたは仮想スイッチを備えたサーバーはサポートされていません。
- その他のネットワーキング機器（ハブ、ルータ、スイッチなど）はサポートされていません。

認証テンプレートの選択

ファブリックドメイン内のすべてのデバイスに適用される認証テンプレートを選択できます。

ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (≡) をクリックして選択します [Provision] > [Fabric] の順に選択します。

ステップ 2 表示されたウィンドウで、ファブリックをクリックします。

ステップ 3 [Fabric Sites] ペインで、サイトを選択します。

ステップ 4 [Host Onboarding] タブをクリックします。

ステップ 5 [Authentication] タブで、サイトの認証テンプレートを選択します。

- **クローズ認証 (Closed Authentication)**：認証前のすべてのトラフィック (DHCP、DNS、ARP を含む) は廃棄されます。
- **[Low Impact]**：スイッチポートに ACL を適用することでセキュリティを追加して、認証前に非常に制限されたネットワークアクセスを許可します。ホストが正常に認証されると、追加のネットワークアクセスが許可されます。
- **認証なし**
- **オープン認証 (Open Authentication)**：ホストには、802.1X 認証を受ける必要なくネットワークアクセスが許可されます。

選択した認証テンプレートの設定を編集して、サイト固有の認証要件に対応することができます。

サイトレベルの認証を変更する前に、マクロまたは自動設定を使用して AP がオンボーディングされ、かつまだ定期的な再同期が行われていないファブリックデバイスがあれば再同期する必要があります。

ステップ 6 (オプション) 選択した認証方式の設定を編集するには、[Edit] をクリックします。

ウィンドウがスライドし、選択した認証方式のパラメータが表示されます：[First Authentication Order]、[802.1x to MAB Fallback]、[Wake on LAN]、[Number of hosts]。

(注) [Number of hosts] は、ポートに接続できるデータホストの数を指定します。[Single] の場合、ポートでは 1 つのデータクライアントのみを保持できます。[Unlimited] の場合、ポートで複数のデータクライアントと 1 つの音声クライアントを保持できます。

必要な変更を行って、[保存 (Save)] をクリックします。

編集ウィンドウが閉じます。保存された変更は、認証テンプレートが編集されているサイトにのみ適用されます。

ステップ 7 [展開 (Deploy)] をクリックします。

ヒットレス認証変更機能を使用すると、ファブリックからデバイスを削除することなく、1 つの認証方式から別の認証方式に切り替えることができます。

ファブリック ドメインへの仮想ネットワークの関連付け


IP アドレス プールにより、ホスト デバイスはファブリック ドメイン内で通信できるようになります。

IP アドレス プールを設定すると、Cisco DNA Center はすぐに各ノードに接続し、ホストが通信できるように適切なスイッチ仮想インターフェイス (SVI) を作成します。

IP アドレス プールを追加することはできませんが、リストされているものからプールを設定できます。ここにリストされている IP アドレス プールは、ネットワークの設計時に作成されたものです。

この手順を使用して、仮想ネットワークの次の機能を設定できます。

- 共通 IP アドレス プール
- ワイヤレス IP アドレス プール
- 重要な IP アドレス プール
- IP Directed Broadcast
- カスタム VLAN ID
- レイヤ 2 フラッドイング
- 位置指定された仮想ネットワーク

- ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Provision] > [Fabric] の順に選択します。
- ステップ 2 表示されたウィンドウで、ファブリックをクリックします。
- ステップ 3 [Fabric Sites] ペインで、サイトを選択します。
- ステップ 4 [Host Onboarding] タブで、[Virtual Networks] をクリックします。
- ステップ 5 選択したファブリックサイトに1つ以上の仮想ネットワークを関連付けるには、 アイコン ([Add Virtual Network]) をクリックします。
 - a) [Add Virtual Network] スライドインペインで、ファブリックサイトに追加する仮想ネットワークを選択します。
 - b) [更新 (Update)] をクリックします。
- ステップ 6 仮想ネットワークを編集するには、[Virtual Networks] タブで仮想ネットワークをクリックします。
- ステップ 7 [Edit Virtual Networks] スライドインペインで次のフィールドを確認します。

フィールド	説明
IP Pool Name	仮想ネットワークに関連付けられている IP アドレスプール。
VLAN	仮想ネットワークに関連付けられている VLAN の ID。
VLAN 名	仮想ネットワークに関連付けられている VLAN の名前。
Traffic Type	仮想ネットワーク上で有効になっているトラフィックのタイプ。
スケラブルグループ	IP プールが属しているグループ。
共通プール	選択した IP プールはファブリック内の複数のサイトで共有されています。 共通プールを有効または無効にするには、[Actions] > [Enable Common Pool]/[Disable Common Pool] の順に選択します。
Wireless Pool	選択した IP プールはワイヤレスプールとして有効になっています。 選択した IP プールをワイヤレスプールとして有効または無効にするには、[Actions] > [Enable Wireless Pool]/[Disable Wireless Pool] の順に選択します。 有効にすると、ファブリックのワイヤレス SSID を設定するときに、定義済みのワイヤレスプールからのみ選択できます。
Layer-2 Only	選択した IP プールはレイヤ 2 セグメントとしてのみ使用されています。
IP Directed Broadcast	選択した IP プールの IP ダイレクトブロードキャスト設定。この設定を有効にするには、チェックボックスをオンにします。ディセーブルにするには、このチェックボックスをオフにします。
Layer-2 Flooding	選択した IP プールのレイヤ 2 フラッディング設定。この設定を有効にするには、チェックボックスをオンにします。ディセーブルにするには、この

フィールド	説明
	チェックボックスをオフにします。レイヤ2フラッディングはデフォルトで無効になっています。

ステップ 8 選択した仮想ネットワークに1つ以上のIPアドレスプールを関連付けるには、[Add]をクリックします。
[Edit Virtual Network] スライドインペインで、次の手順を実行します。

- a) [IP Address Pool] ドロップダウンリストからプールを選択します。
- b) [VLAN Name] に有効な名前を入力します。
- c) 仮想ネットワークのカスタム **VLAN** 番号を入力します。

次の点に注意してください。


- VLAN ID 1、1002 ~ 1005、2046、および 4095 は予約済みで、使用できません。
- カスタム VLAN ID を指定しない場合は、Cisco DNA Center が 1021 ~ 2020 の範囲の VLAN ID を生成します。

- d) [Scalable Group] ドロップダウンリストからグループを選択します。
- e) [Traffic] ドロップダウンリストからトラフィックのタイプを選択します。
仮想ネットワークを介して送信するトラフィックとして、音声またはデータを選択できます。
- f) レイヤ2フラッディングを有効にするには、[Layer-2 Flooding] チェックボックスをオンにします。
(注) レイヤ2フラッディングにはアンダーレイマルチキャストが必要であり、これは LAN 自動化中に設定されます。LAN 自動化でアンダーレイをプロビジョニングしない場合は、アンダーレイマルチキャストを手動で設定します。
- g) この IP プールをクリティカル IP アドレスプールに含めるには、[Critical Pool] チェックボックスをオンにします。
クリティカルプールは、認証サーバーを使用できない場合に、クローズド認証プロファイルに使用されます。認証サーバーがない場合、クリティカルプールにクリティカルVLANが割り当てられ、未認証のすべてのホストがそのクリティカルVLANに配置されます。
- h) この IP プールをファブリック内の複数のサイトで共有するには、[Common Pool] チェックボックスをオンにします。
サイト間のレイヤ2ハンドオフ機能では、ファブリック内の複数のサイトで IP プールを共有できます。
- i) この IP プールをワイヤレス IP アドレスプールとして有効にするには、[Wireless Pool] チェックボックスをオンにします。
- j) IP ダイレクトブロードキャスト機能を有効にするには、[IP Directed Broadcast] チェックボックスをオンにします。

- (注)
- IP ダイレクトブロードキャストを有効にする前に、レイヤ 2 フラッディングを有効にします。
 - サイト間のレイヤ 2 ハンドオフが有効になっているセグメントでは、IP ダイレクトブロードキャスト機能を有効にできません。
 - ルータおよび Nexus 7000 シリーズ スイッチは、IP ダイレクトブロードキャスト機能をサポートしていません。

k) [Add] をクリックして設定を保存します。

ここで指定した設定は、仮想ネットワークのすべてのデバイスに展開されます。

l) IP プールをさらに関連付けるには、 アイコンをクリックして上記の手順を繰り返します。

ステップ 9 この仮想ネットワークを位置指定し、この仮想ネットワークを通過するすべてのトラフィックの共通ボーダーとしてそのボーダーを有効にするには、[Use Border/CP for this site to be common for the Virtual Network] チェックボックスをオンにします。

位置指定された仮想ネットワークを他のファブリックサイトに追加して、マルチサイトゲストの共通のボーダーへのアクセスを有効にすることができます。

位置指定された仮想ネットワークは、その横にアンカータグが付いた状態で表示されます。

- (注)
- セグメントが含まれている場合、仮想ネットワークを位置指定することはできません。
 - 仮想ネットワークを位置指定する前に、すべてのコントロールプレーンと境界デバイスがプロビジョニングされていることを確認します。
 - 位置指定された仮想ネットワークでマルチキャストを有効にすると、継承された仮想ネットワークにセグメントが設定されている場合は、継承された仮想ネットワークのエッジデバイスにマルチキャストが設定されます。継承された仮想ネットワークにセグメントがない場合、マルチキャストは、最初のセグメントが作成された後にのみ展開されます。

ステップ 10 すべての仮想ネットワークに IP プールを関連付けた後、[Save] をクリックします。

ファブリック ドメインのワイヤレス SSID の設定

ステップ 1 [Wireless SSID] セクションで、ホストがアクセス可能なネットワーク内のワイヤレス SSID を指定します。

ステップ 2 [Choose Pool] をクリックし、SSID の IP プール予約を選択します。

ステップ 3 [Assign SGT] ドロップダウンリストから、SSID のスケーラブルなグループを選択します。

ステップ 4 SSID でワイヤレスマルチキャストを有効にするには、[Enable Wireless Multicast] チェックボックスをオンにします。

ファブリックサイト内のポートの設定

[Port Assignment] タブで、ファブリックドメインの各アクセスデバイスを設定できます。デバイスの各ポートのネットワーク動作設定を指定できます。



(注) ここで行うポートの設定は、[仮想ネットワーク (Virtual Networks)] セクションで行ったデバイスの一般設定をオーバーライドします。

- ステップ 1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Provision] > [Fabric] の順に選択します。
- ステップ 2 表示されたウィンドウで、ファブリックをクリックします。
- ステップ 3 [Fabric Sites] ペインで、サイトを選択します。
- ステップ 4 [Host Onboarding] タブで、[Port Assignment] タブをクリックします。
- ステップ 5 左側のペインに表示されるファブリックデバイスのリストから、設定するデバイスを選択します。デバイスで使用可能なポートが右側のペインに表示されます。
- ステップ 6 右側のペインで、デバイスのポートを選択し、[Assign] をクリックします。
- ステップ 7 スライドする [Port Assignment] ペインで、ドロップダウンリストの次のオプションから [Connected Device Type] を選択します。

オプション	説明
トランク	ポートをトランクポートとして設定します。
[Access Point(AP)]	アクセスポイントに接続するポートを設定します。
[User Devices (ip-phone, computer, laptop)]	ホストデバイスに接続するポートを設定します。

- a) トランクポートを接続するには、[Trunk] を選択し、このポートの [Description] を入力します。
- b) アクセスポイントを接続するには、[Access Point(AP)] を選択し、次の手順を実行します。
 1. [VLAN Name / IP Address Pool (Data)] ドロップダウンリストから VLAN と IP アドレスを選択します。
 2. [Authentication] ドロップダウンリストから認証タイプを選択します。
 3. コネクテッドデバイスに関する [Description] を入力します。
- c) ホストデバイスを接続するには、[User Devices (ip-phone, computer, laptop)] を選択し、次の手順を実行します。
 1. [VLAN Name / IP Address Pool (Data)] ドロップダウンリストからデータの IP アドレスプールを選択します。
 2. プロビジョニングされているグループである [Scalable Groups] を選択します。

スケーラブルグループは、[No Authentication] プロファイルでのみサポートされます。

3. [VLAN Name / IP Address Pool (Voice)] ドロップダウンリストから音声の IP アドレスプールを選択します。
4. [Authentication] ドロップダウンリストから認証テンプレートを選択します。
5. コネクテッドデバイスに関する [Description] を入力します。

d) [更新 (Update)] をクリックします。

ステップ 8 すべてのポートの割り当てが完了したら、[Deploy] をクリックします。

拡張ノードデバイスの設定

拡張ノードはレイヤ2スイッチモードで動作するデバイスで、ファブリックテクノロジーをネイティブにはサポートしていません。拡張ノードは、自動化されたワークフローによって設定されます。設定後、拡張ノードデバイスがファブリックポロジビューに表示されます。拡張ノードでの [Port Assignment] は、[Host Onboarding] ウィンドウで実行できます。



- (注) 拡張ノードは、ユーザー インターフェイススペースのプロビジョニング ワークフローではオンボードできません。拡張ノードをオンボードするには、デバイス設定を工場出荷時の初期状態にリセットし、デバイスの電源をオンにした後に、SD-Access 自動化ワークフローを使用する必要があります。

拡張ノードデバイスは、マルチキャストトラフィックをサポートします。

ポリシー拡張ノードは、仮想ネットワーク内のセキュリティポリシーをサポートする拡張ノードです。ポリシー拡張ノードのポート割り当て時に、[Group] を選択できます。

Cisco IOS XE 17.1.1s 以降のリリースのソフトウェアを実行している Cisco Catalyst 産業用イーサネット (IE) 3400、IE 3400 Heavy Duty シリーズスイッチ、および Cisco Catalyst 9000 シリーズスイッチは、ポリシー拡張ノードデバイスです。

Cisco デジタルビルディングシリーズスイッチ、Cisco Catalyst 3560-CX スイッチ、および Cisco 産業用イーサネット 4000、4010、5000 シリーズスイッチは、ポリシー拡張ノードデバイスではありません。ポート割り当て時の [Cisco TrustSec] と [Group] の選択はサポートされていません。

拡張ノードの設定手順

Cisco Catalyst 9300、Cisco Catalyst 9400、および Cisco Catalyst 9500 シリーズスイッチは、ファブリックエッジとして設定されたときに拡張ノードをサポートします。

ポリシー拡張ノードをサポートするエッジノードでサポートされているソフトウェアの最小バージョンは Cisco IOS XE 17.1.1 s です。



(注) ファブリックエッジノードとして設定されている Cisco Catalyst 9200 シリーズスイッチは、拡張ノードデバイスをサポートしていません。

以下に、拡張ノードでサポートされている最小ソフトウェアバージョンを示します。

- Cisco Industrial Ethernet 4000、4010、5000 シリーズ スイッチ : 15.2(7)E0s (LAN ベースライセンスが有効になっている)
- Cisco Catalyst IE 3400、3400 Heavy Duty (X-coded および D-coded) シリーズスイッチ : IOS XE 17.1.1s
- Cisco Catalyst IE 3300 シリーズスイッチ : IOS XE 16.12.1s
- Cisco Digital Building シリーズスイッチ、Cisco Catalyst 3560-CX スイッチ : 15.2(7)E0s

ポリシー拡張ノードを設定する前に、次のことを確認してください。

- ポリシー拡張ノードデバイス、およびポリシー拡張ノードをサポートするエッジデバイスで必要な最小ソフトウェアバージョンは Cisco IOS XE 17.1.1 s です。
- ポリシー拡張ノードとそれをサポートするエッジノードの両方で、Network Advantage と DNA Advantage のライセンスレベルが有効になっている必要があります。

ステップ 1 拡張ノードのネットワーク範囲を設定します。[IP アドレスプールを設定する](#) を参照してください。この手順では、IP アドレスプールを追加し、サイトレベルで IP プールを予約します。CLI および SNMP クレデンシャルが設定されていることを確認します。

ステップ 2 拡張 IP アドレス プールを、[Fabric] > [Host Onboarding] タブの下にある INFRA_VN に割り当てます。プールタイプとして **拡張ノード** を選択します。

Cisco DNA Center Cisco DNA Center は、サポートされているファブリックエッジデバイスで拡張 IP アドレスプールと VLAN を設定します。これにより、拡張ノードのオンボーディングが有効になります。

ステップ 3 拡張 IP アドレスプールとオプション 43 を使用して DHCP サーバーを設定します。拡張 IP アドレスプールが Cisco DNA Center から到達可能であることを確認します。

(注) オプション 43 の詳細については、[DHCP コントローラ ディスカバリ](#) を参照してください。

ステップ 4 ファブリックエッジデバイスに拡張ノードデバイスを接続します。拡張ノードデバイスからファブリックエッジへ複数のリンクを設定できます。

ステップ 5 拡張ノードに接続されているファブリックエッジノードでポートチャネルを作成します。

この手順は、ファブリックのグローバル認証モードが [No Authentication] ではない場合にのみ実行します。認証モードは **Open**、**Low Impact**、または **Closed** のいずれかです。

ポートチャネルを作成するには、次の手順を実行します。

- [Provision] > [Fabric] > [Fabric Infrastructure] に移動し、ファブリックエッジノードを選択します。タイトルにデバイス名の付いたウィンドウがスライド表示されます。

- b) [Port Channel] タブで、[Create Port Channel] をクリックします。
- c) ペインのすべてのフィールドに入力します。

- [Connected Device Type] ドロップダウンから [Extended Node] を選択します。
- [Port Aggregation Protocol (PAgP)] を選択します。

Cisco IOS XE リリース 17.1.1s 以降、IE 3300 および IE 3400 デバイスは PAgP をサポートしていません。

- Cisco IOS XE 17.1.1s よりも前のバージョンを実行している場合は、IE 3300 および IE 3400 デバイスの [On] を選択します。
- 拡張ノードのオンボーディングでは Link Aggregation Control Protocol (LACP) は機能しないことに注意してください。
- ポートチャネルとしてバンドルするポートを選択します。

- d) [Done] をクリックします。

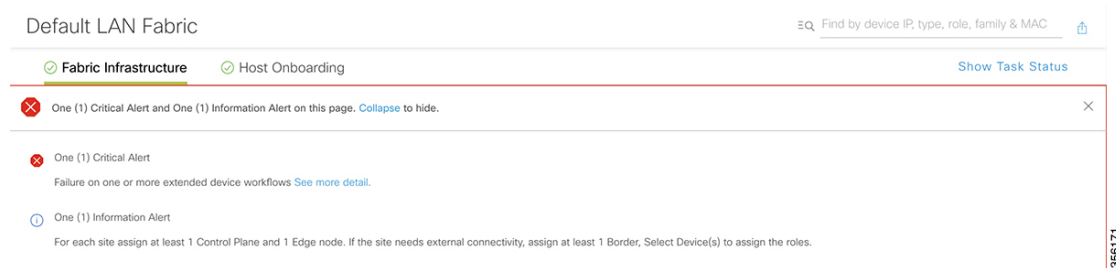
これで、ファブリックエッジノードにポートチャネルが作成されて、拡張デバイスがオンボードされます。

ステップ 6 以前の設定がない場合は、拡張ノードデバイスの電源をオンにします。拡張ノードデバイスに設定がある場合は、以前の設定の書き込み消去を実行して、拡張ノードデバイスをリロードします。

Cisco DNA Center Cisco DNA Center では、拡張ノードデバイスをインベントリに追加し、同じサイトをファブリックエッジとして割り当てます。次に、拡張ノードデバイスがファブリックに追加されます。これで、拡張ノードデバイスがオンボードされ、管理できるようになりました。

設定が完了すると、拡張ノードがファブリックトポロジに、拡張ノードであることを示すタグ (X) とともに表示されます。

拡張ノードの設定中にワークフローでエラーが発生した場合は、[Topology] ウィンドウにバナーでエラー通知が表示されます。



[See more details] をクリックしてエラーを確認します。

[Task Monitor] ウィンドウがスライド表示され、拡張ノード設定タスクのステータスが表示されます。

[See Details] をクリックして、エラーの原因および考えられるソリューションを確認します。

ポートチャネルの設定

単一のエンティティとして機能するようにバンドルされたポートのグループは、ポートチャネルと呼ばれます。ファブリックエッジと、拡張ノードやサーバーなどリモート接続されたデバイスとの間のポートチャネルでは、接続の復元力と帯域幅が増加します。

ポートチャネルの作成

認証がクローズド認証の場合にのみ、次の手順を実行します。他の認証モードでは、次の手順が自動化されていることに注意してください。

-
- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Provision] > [Fabric] の順に選択します。
- ステップ 2** 表示されたウィンドウで、ファブリックをクリックします。
- ステップ 3** [Fabric Sites] ペインで、サイトを選択します。
- ステップ 4** [Fabric Infrastructure] タブをクリックすると、すべてのファブリックデバイスが表示されます。
- ステップ 5** ファブリックエッジノードをクリックします。
タイトルにデバイス名の付いたウィンドウがスライド表示されます。
- ステップ 6** [Port Channel] タブで、[Create Port Channel] をクリックします。
- ステップ 7** [Connected Device Type] ドロップダウンから、接続済みのデバイスのタイプを選択します。
- ファブリックエッジノードと拡張ノードの間または2つの拡張ノードの間にポートチャネルを作成する場合は、[Extended Node] を選択します。
 - 片側にファブリックエッジノードまたは拡張ノードがあり、反対側にサードパーティデバイスまたはサーバーポートがあるポートチャネルを作成するには、[Trunk] を選択します。
- ステップ 8** 新しいポートチャネルの適切な説明を [Description] に入力します。
- ステップ 9** 適切なプロトコルを選択します。
- Cisco IOS XE リリース 16.12.1s および以前のリリースを実行する拡張ノードの場合は、プロトコルとして [On] を選択します。
 - Cisco IOS XE リリース 17.1.1s および以降のリリースを実行する拡張ノードの場合は、プロトコルとして [Port Aggregation Protocol (PAgP)] を選択します。
 - **Link Aggregation Control Protocol (LACP)** を拡張ノードのプロトコルとして選択しないでください。LACP モードでは、トランクポートまたはサーバーポートのみを接続できます。
- ステップ 10** 表示されたポートの一覧から、バンドルするポートを選択します。

- (注) LACP モードで接続されたポートチャネルには、16 を超えるメンバーを含めることはできません。
- PAgP モードで接続されたポートチャネルには8つを超えるメンバーを含めることはできません。

- ステップ 11** [Done] をクリックします。
- 作成した新しいポートチャネルがウィンドウに表示されます。

ポートチャネルの更新

始める前に

ポートチャネルを更新する前に、少なくとも1つのメンバーインターフェイスが存在することを確認します。

-
- ステップ 1** Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します[Provision] > [Fabric] の順に選択します。
- ステップ 2** 表示されたウィンドウで、ファブリックをクリックします。
- ステップ 3** [Fabric Sites] ペインで、サイトを選択します。
- ステップ 4** [Fabric Infrastructure] タブをクリックすると、すべてのファブリックデバイスが表示されます。
- ステップ 5** ファブリックエッジノードをクリックします。
- タイトルにデバイス名の付いたウィンドウがスライド表示されます。
- ステップ 6** [Port Channel] タブを選択します。
- ステップ 7** 表示されるポートチャネルのリストから、更新するポートチャネルを選択します。
- 結果のウィンドウに、選択したポートチャネルのすべてのインターフェイスとステータスが表示されます。
- ステップ 8** ポートチャネルで必要な更新を実行します。
- ポートチャネルにインターフェイスを追加したり、ポートチャネルの既存のインターフェイスを削除したりできます。
- ステップ 9** [Done] をクリックします。

ポートチャネルの削除

-
- ステップ 1** Cisco DNA Center GUI で、[Menu] アイコン (☰) をクリックし、[Provision] > [Fabric] > [Fabric Infrastructure] の順に選択します。
- ステップ 2** ポートチャネルを削除するデバイスをクリックします。

デバイス名の付いたウィンドウがスライド表示されます。

ステップ3 [Port Channel] タブをクリックします。

開いた [Port Channel] ビューには、既存のポートチャンネルがすべて表示されます。

ステップ4 ポートチャンネルを選択し、[Delete] をクリックします。

ステップ5 プロンプトで [Yes] をクリックします。

マルチキャスト概要

マルチキャストトラフィックは、次のような異なる方法で転送されます。

- ランデブーポイントを使用した共有ツリー経由。この場合、PIM SM が使用されます。
- 最短パス ツリー (SPT) 経由。PIM Source Specific Multicast (SSM) では SPT だけが使用されます。PIM SM は、受信側が接続しているエッジルータで送信元が認識されると SPT に切り替わります。

『[IP マルチキャストルーティングテクノロジーの概要 \(IP Multicast Technology Overview\)](#)』を参照してください。

マルチキャストの設定

Cisco DNA Center には、仮想ネットワークでグループ通信またはマルチキャストトラフィックを有効にするためのワークフローが用意されています。このワークフローでは、ネットワークでのマルチキャスト実装 (ネイティブマルチキャストまたはヘッドエンドレプリケーション) を選択することもできます。



- (注) Cisco DNA Center リリース 2.2.2.4 以降では、ボーダーがマルチサイトリモートボーダーとして機能する仮想ネットワークでマルチキャストを有効にすることができます。このような仮想ネットワークでマルチキャストを設定すると、継承された仮想ネットワークにすでにセグメントが含まれている場合は、継承された仮想ネットワークのデバイスにもマルチキャストが設定されます。継承された仮想ネットワークにセグメントがない場合、マルチキャストは、最初のセグメントが作成された後のみ展開されます。仮想ネットワークとその継承ネットワークが同じタイプのマルチキャスト実装を展開していることを確認してください。継承された仮想ネットワークのエッジデバイスをランデブーポイント (RP) として設定することはできません。

ステップ1 Cisco DNA Center GUI で [Menu] アイコン (☰) をクリックして選択します [Provision]。すべてのプロビジョニングされたファブリックドメインがウィンドウに表示されます。

- ステップ 2** ファブリック ドメインのリストから、ファブリックを選択します。ファブリックに設定されているすべてのサイトが表示されます。マルチキャストを設定するサイトを選択します。
- ステップ 3** [Fabric Sites] ペインで、選択したサイトの横にある歯車アイコンをクリックします。
- ステップ 4** ドロップダウンリストから [Configure Multicast] を選択します。
マルチキャスト構成のワークフローの最初のウィンドウが表示されます。
- ステップ 5** [Enabling Multicast] ウィンドウで、ネットワークのマルチキャスト実装方式 ([Native Multicast] または [Head-end replication]) を選択し、[Next] をクリックします。
- ステップ 6** [Virtual Networks] ウィンドウで、マルチキャストを設定する仮想ネットワークを選択します。[Next] をクリックします。
(注) 継承された仮想ネットワークを選択してマルチキャストを設定することはできません。
- ステップ 7** [Multicast pool mapping] ウィンドウで、[IP Pools] ドロップダウンリストから IP アドレスプールを選択します。選択した IP アドレスプールは、選択した仮想ネットワークに関連付けられます。[Next] をクリックします。
- ステップ 8** [Select multicast type] ウィンドウで、実装するマルチキャストのタイプを選択し、[Next] をクリックします。
- **SSM** (送信元特定マルチキャスト)
 - **ASM** (任意の固有のマルチキャスト)
- ステップ 9** 次の手順を実行します。
- a) [SSM] を選択した場合は、仮想ネットワークごとに IP グループの範囲を追加して、SSM リストを設定します。仮想ネットワークに複数の IP グループ範囲を追加できます。
 1. 225.0.0.0 ~ 239.255.255.255 の IP グループ範囲を選択します。
 2. IP グループの [Wildcard Mask] を入力します。
 3. [Next] をクリックします。
 - b) [ASM] を選択した場合は、ランデブーポイント (RP) のタイプを選択します。
 - **内部 RP**
 - **外部 RP**[次へ (Next)] をクリックします。
- ステップ 10** ランデブーポイントを設定するには、次の手順を実行します。
内部ランデブーポイントを設定する場合は、次のようにします。
- a) 内部ランデブーポイントとして設定する必要があるデバイスを選択します。選択した 2 番目のランデブーポイントは、冗長ランデブーポイントになります。[次へ (Next)] をクリックします。
 - b) 一覧表示されている各仮想ネットワークに内部ランデブーポイントを割り当てます。[Next] をクリックします。

外部ランデブーポイントを設定する場合は、次のようにします。

- a) [Setup your External RP] ウィンドウで、外部ランデブーポイントの IPv4 または IPv6 アドレスを入力します。
(オプション) 2 番目の IPv4 または IPv6 アドレスのセットを入力できます。
[Next] をクリックします。
- b) [Select which RP IP Address(es) to utilize] ウィンドウで、各仮想ネットワークの IP アドレスを選択します。
[Next] をクリックします。

ステップ 11 構成を送信する前に、[Summary] ウィンドウに表示されているマルチキャスト設定を確認し、必要に応じて変更します。

[Finish] をクリックして、マルチキャストの設定を完了します。

サイト間レイヤ2のハンドオフ

サイト間のレイヤ2ハンドオフ機能を使用すると、ファブリック内の複数のサイトにわたって IP サブネットを拡張できます。同じ IP サブネットがファブリック内のサイト間で共存します。

次の制約事項に注意してください。

- 一体型ファブリックまたはボーダーとエッジとして設定されたデバイスは、サイト間のレイヤ2ハンドオフには使用できません。
- サイト間のレイヤ2ハンドオフと SDA トランジットはサポートされていません。
- Wake on LAN 機能は、サイト間のレイヤ2ハンドオフが有効になっているセグメントではサポートされません。

始める前に

- すべてのデバイスが検出され、プロビジョニングされており、IP プールが共有されるサイトでその IP プールが予約されていることを確認します。
- IP プールを共有するサイトがアンダーレイ接続されていることを確認します。ボーダー間にこの接続がないと、共通サブネット上の IP アドレスの取得を試みるホストで DHCP が機能しない可能性があります。
- アンダーレイマルチキャストが設定されていることを確認します。これは、レイヤ2のフラディングが機能するために必要です。アンダーレイマルチキャストは、LAN 自動化ワークフロー中に設定されます。

ステップ1 ファブリック ドメインへの仮想ネットワークの関連付け。[Layer-2 Flooding] チェックボックスと [Common Pool] チェックボックスがオンになっていることを確認します。

[Layer-2 Flooding] と [Common Pool] が有効になっている場合、IP プールは他のサイトへ拡張できるようになります。

ステップ2 ボーダーにレイヤ2 ハンドオフを設定します。

- a) [Provision] > [Fabric] > [Fabric Infrastructure] タブで、サイト間のレイヤ2 ハンドオフを設定するボーダーデバイスを選択します。
- b) [L2 Handoff] セクションで、共通 IP プールが関連付けられている仮想ネットワークを選択します。
- c) サイト間で他のボーダーに接続するボーダーの外部インターフェイスを設定します。
- d) [Extend the subnet to other site] チェックボックスをオンにして、外部 VLAN 番号を共通 IP プールに割り当てます。

ステップ3 IP プールを共有する他のサイトに対して、上記の手順を繰り返します。

すべての相互接続されたボーダーで同じ外部 VLAN 番号を指定していることを確認します。

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。