



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 \(1 ページ\)](#)
- [SD-Access の新しい自動化 \(4 ページ\)](#)
- [ファブリックサイトの追加 \(5 ページ\)](#)
- [ファブリックサイトのデバイスの構成 \(6 ページ\)](#)
- [ファブリックへのデバイスの追加 \(7 ページ\)](#)
- [ボーダーノードとしてのデバイスの追加 \(9 ページ\)](#)
- [LISP Pub/Sub の設定 \(11 ページ\)](#)
- [IP のトランジット ネットワークの作成 \(12 ページ\)](#)
- [SD-Access トランジットネットワークの作成 \(12 ページ\)](#)
- [認証テンプレートの選択 \(13 ページ\)](#)
- [ファブリックサイト内のポートの設定 \(14 ページ\)](#)
- [ファブリックネットワークのワイヤレス SSID の設定 \(15 ページ\)](#)
- [仮想ネットワーク \(16 ページ\)](#)
- [ファブリックゾーンの設定 \(20 ページ\)](#)
- [拡張ノードデバイスの設定 \(25 ページ\)](#)
- [サブリカントベースの拡張ノードの設定 \(33 ページ\)](#)
- [ポートチャネルの設定 \(41 ページ\)](#)
- [マルチキャスト \(43 ページ\)](#)

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

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

Software-Defined Access ファブリックネットワークは、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。ファブリックサイトの全体的な集約は、多数のエンドポイントに対応し、モジュール方式で（または水平方向に）拡張します。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相互接続されます。

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。IP トランジットは、従来型の IP ベース（VRF-LITE、MPLS）ネットワークを利用します。これには、サイト間での VRF と SGT の再マッピングが必要です。
- **SD-Access 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。SD-Access 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。SD-Access 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。

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：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。

SD-Access の新しい自動化

強化された Cisco SD-Access ユーザーインターフェイス（UX）では、シンプルさ、柔軟性、豊富で直感的なコンテキストが統合されています。Cisco SD-Access UX のベータ版は、ユーザーエクスペリエンスを強化し、次の機能を提供します。

- 仮想ネットワークやファブリックサイトなどのファブリック要素間の関連付けの明確化
- 強化されたワークフロー
- ファブリック要素とその属性の簡潔なビュー

拡張 Cisco SD-Access UX は、次のもので構成されています。

- 仮想ネットワーク、ファブリックサイト、およびトランジットネットワークごとの概要ページ
- [Virtual Networks] の概要ビューには、次の 4 つのセクションがあります。
 - 最初のセクションには、さまざまな段階のタスクの数、レイヤ3仮想ネットワークとエニーキャストゲートウェイの数、エニーキャストゲートウェイ、レイヤ2仮想ネットワークとそれらの VLAN の数が表示されます。
 - 2 番目のセクションには、仮想ネットワークタスクがグラフィカルに表示されます。
 - 3 番目のセクションには、保存されたヒントのリストが表示されます。
 - 最後のセクションには、提供されるさまざまなワークフローのカードベースのビューが表示されます。
- [Fabric Sites] ページには、[Summary] ビュー、[Map] ビュー、および [Table] ビューの 3 つのビューがあります。

[Summary] ビューには、ヒントとインサイト、および進行中のワークフローが表示されます。また、ファブリックサイト、ファブリックゾーン、ファブリックデバイス、コントロールプレーン、およびボーダーノードの数の概要も提供します。

- [Transits] ページには、SD-Access トランジット、SDWAN トランジット、および IP ベースのトランジットの数の概要が表示されます。このページには、トランジットネットワークを作成するオプションもあります。

Cisco DNA Center メニューバーの [Preview New SD-Access] トグルボタンを使用して、古い Cisco SD-Access UX と拡張 Cisco SD-Access UX を切り替えます。



(注) この章で説明するすべてのタスクは、拡張 Cisco SD-Access UX に関連しています。

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、ファブリックサイトを作成できます。

- ステップ 1** メニューアイコン (☰) をクリックして、[Provision] > [Fabric Sites]。
- ステップ 2** [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。
- ステップ 3** [Create Fabric Sites and Fabric Zones] をクリックします。
または、最初の 3 つの手順の代わりに、メニューアイコン (☰) をクリックして、[Workflow] > [Create Fabric Sites] の順に選択します。
- ステップ 4** [Create Fabric Sites and Fabric Zones] ウィンドウで、[Let's Do it] をクリックして、ワークフローに直接移動します。
- ステップ 5** [Fabric Site Location] ウィンドウで、ファブリックゾーンとして追加するエリア、建物、またはフロアを選択します。
- ステップ 6** [Wired Endpoint Data Collection] ウィンドウで、[Monitor wired clients] 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。
- ステップ 7** [Authentication Template] ウィンドウで、次の手順を実行します。
 - ファブリックサイトの認証テンプレートを選択します。
 - [Closed Authentication] : 認証前のすべてのトラフィック (DHCP、DNS、ARP など) が廃棄されます。
 - 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。

- [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。

- None

b) (オプション) [Closed Authentication]、[Open Authentication]、または [Low Impact] を選択した場合は、[Edit] をクリックして認証設定を編集します。

- [First Authentication Method] : [802.1x] または [MAC Authentication Bypass (MAB)] を選択します
- [802.1x Timeout (in seconds)] : スライダを使用して、802.1x タイムアウトを秒単位で指定します。
- [Wake on LAN] : [Yes] または [No] を選択します。
- [Number of Hosts] : [Unlimited] または [Single] を選択します。
- [BPDU Guard] : このチェックボックスを使用して、すべての [Closed Authentication] ポートでブリッジプロトコルデータユニット (BPDU) ガードを有効または無効にします。
- [Pre-Authentication Access Control List] : トグルボタンを有効にして、[Low Impact] 認証の事前認証制御を構成します。[Implicit Action] ドロップダウンリストから、暗黙的なアクションを選択します。ルールの説明を入力します。アクセスコントラクトを追加するには、[Add Contract Action] をクリックし、ルールを選択して、[Apply Table] をクリックします。

ステップ 8 [Fabric Zones] ウィンドウで、次のいずれかのオプションを選択します。

- ファブリックゾーンを指定し、範囲指定されたサブネットを作成するには、[Setup Fabric Zones Now] をクリックし、表示されたネットワーク階層からファブリックサイトを選択します。
- 後でファブリックゾーンを指定するには、[Setup Fabric Zones Later] をクリックします。

ステップ 9 [Summary] ウィンドウで、ファブリックサイトの設定を確認します。

ここでファブリックサイトまたはゾーン設定を編集できます。

ステップ 10 [Deploy] をクリックします。

サイトとゾーンがプロビジョニングされるまでに数秒かかります。サイトの作成が成功すると、「Success!Your fabric site is created」 というメッセージが表示されます。

ファブリックサイトのデバイスの構成

次のタブを使用して、ファブリックサイトのデバイスを構成できます。

- [Fabric Infrastructure] タブ : デバイスをファブリックロールに割り当てます。
- [Authentication Template] 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。

- [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：ファブリックサイト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。

ファブリックへのデバイスの追加

ファブリックサイトを作成すると、そのファブリックサイトにデバイスを追加できます。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も指定できます。

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)
- ファブリックサイト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。それらのロールがないデバイスもあります。ただし、各ファブリックサイトには、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）。

- **[Provision] > [Network Devices] > [Inventory]** ウィンドウに、検出されたデバイスが表示されます。
- 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。
- 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。
- 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 メニューアイコン (☰) をクリックして、 **[Provision] > [Fabric Sites]**。

ステップ 2 **[SUMMARY]** で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 デバイスを追加するファブリック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 **[Fabric Infrastructure]** タブの **[List]** ビューで、デバイスをクリックします。スライドインペインには、次の **[Fabric]** オプションが表示されます。

オプション	説明
エッジノード	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ボタンをトグルします。
ボーダー ノード	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ボタンをトグルします。
コントロールプレーンノード	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ボタンをトグルします。

デバイスをファブリックインボックスとして設定するには、 **[Control Plane Node]**、 **[Border Node]**、および **[Edge Node]** 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 Node]** と **[Border Node]** 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 \(7 ページ\)](#) 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 メニューアイコン (☰) をクリックして、[Provision] > [Fabric Sites]。
- ステップ2 [Fabric Sites] タブの [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。
- ステップ3 ボーダーノードを設定するファブリック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 [Fabric Infrastructure] タブの [List] ビューで、デバイスをクリックします。
- ステップ5 スライドインペインで、[Border Node] トグルボタンを有効にします。
- ステップ6 表示されたスライドインペインで、[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 ボーダーノードの優先度を設定するには、[Modify Border Priority] チェックボックスをオンにして、優先度の値を入力します。
優先度の範囲は、1 ~ 10 です。値が小さいほど、ボーダーの優先度が高くなります。(1 は最高の優先度を示します。10 は最も低い優先度を示します) デフォルトでは、ボーダーの優先度の値は10に設定されています。
ネットワークに2つ以上のボーダーが設定されている場合、トラフィックは優先度の高いボーダーを介してルーティングされます。優先順位が設定されていない場合、トラフィックはボーダーノード間で負荷分散されます。

ステップ 10 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、外部ルートをインポートせずに、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イン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ル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] および [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] および [Do not import external routes] の両方のチェックボックスをオフにします。
- 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 11 [Add Transit Site] にカーソルを合わせ、ボーダーデバイスで有効にするトランジットネットワークを選択します。

a) [IP:BGP IP TRANSIT] の場合、IP インターフェイスを構成します。

- [Add External Interface] 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. [External Interface] を選択します。
 2. [Remote AS Number] は、選択したトランジットまたはピアネットワークから自動的に導出されます。
 3. [Interface Description] に説明を入力します。
 4. (オプション) [Actions] ドロップダウンリストにカーソルを合わせて、[Enable All] または [Disable All] を選択します。
 5. 目的の仮想ネットワークの [Enable Layer-3 Handoff] ボタンを切り替えます。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。
 6. 選択した仮想ネットワークの VLAN ID を入力します。
 7. [Save] をクリックします。
- [Select IP Pool] ドロップダウンリストから、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。

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。

仮想ネットワークに存在する IP アドレスプールのリストと、ファブリック以外のデバイスを接続できるインターフェイスのリストが表示されます。

- b) [External Interface] を選択してください。
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。

LISP Pub/Sub の設定

最初のコントロールプレーンをファブリックに追加する場合にのみ、ファブリックサイトで LISP Pub/Sub を設定できます。

始める前に

ファブリックデバイスが Cisco IOS XE リリース 17.6.1 以降で動作することを確認します。

ステップ 1 メニューアイコン (☰) をクリックして、[Provision] > [Fabric Sites]。

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 デバイスを追加するファブリック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 [Fabric Infrastructure] タブの [List] ビューで、コントロールプレーンとして設定するデバイスをクリックします。

ステップ 5 スライドインペインで、[Control Plane Node] トグルボタンを有効にして、このプレーンを設定します。

ステップ 6 [Configure Control Plane] スライドインペインで、[LISP PubSub] ルート配布プロトコルを選択し、[Add] をクリックします。

ステップ 7 [Add] をクリックします。

ステップ 8 [展開 (Deploy)] をクリックします。

ステップ9 [Modify Fabric] ウィンドウで、操作をスケジュールし、[Apply] をクリックします。

ファブリックサイトの LISP Pub/Sub の設定を確認するには、[SITE SUMMARY] ウィンドウで LISP Pub/Sub のステータスを確認します。

IP のトランジット ネットワークの作成

ステップ1 メニューアイコン (☰) をクリックして、[Provision] > [Transits].

ステップ2 [Create Transit] をクリックします。

ステップ3 [Transit] スライドインペインで、トランジットネットワークの名前を入力します。

ステップ4 [IP-Based] 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5 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6 [Save] をクリックします。

SD-Access トランジットネットワークの作成

SD-Access 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 メニューアイコン (☰) をクリックして、[Provision] > [Transits].

ステップ2 [Create Transit] をクリックします。

ステップ3 [Transit] スライドインペインで、トランジットネットワークの名前を入力します。

ステップ4 SD-Access の [Transit Type] を選択します。

LISP Pub/Sub コントロールプレーンのないファブリックサイトのトランジットを設定する場合は、[SD-Access (LISP/BGP)] を選択してください。

LISP Pub/Sub コントロールプレーンのあるファブリックサイトのトランジットを設定する場合は、[SD-Access (LISP PubSub)] を選択してください。

[SD-Access (LISP PubSub)] トランジットを他の Cisco DNA Center クラスタと共有する場合は、[Yes, Share] を選択してください。共有しない場合は、[No, keep it local] を選択してください。

(注) [Yes, Share] オプションは、複数の Cisco DNA Center パッケージがすべての Cisco DNA Center クラスタにインストールされている場合にのみ表示されます。

ステップ5 ドロップダウンリストから [Transit Control Plane Node Site] を選択します。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6 ドロップダウンリストからトランジットネットワークの [Transit Control Plane Node] を選択します。

ステップ7 (オプション) 追加のマップサーバーを構成するには、プラスアイコン (+) をクリックし、**ステップ5 (12 ページ)** と **ステップ6 (13 ページ)** を繰り返します。

ステップ8 [Save] をクリックします。

トランジットネットワークを作成すると、[Transits] ウィンドウに、新しく作成されたトランジットとその属性が表示されます。

(注) LISP/BGP コントロールプレーンを使用するファブリックサイトに [SD-Access (LISP PubSub)] トランジットを追加することはできません。LISP Pub/Sub コントロールプレーンを使用するファブリックサイトに [SD-Access (LISP/BGP)] トランジットを追加することはできません。

次のタスク

ファブリックサイトを SD-Access トランジットと相互接続するには、トランジットをボーダーノードに追加します。

認証テンプレートの選択

ファブリックサイト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設定できます。

ステップ1 メニューアイコン (☰) をクリックして、[Provision] > [Fabric Sites].

ステップ2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ3 ファブリックサイトを選択します。

ステップ4 [Authentication Template] タブをクリックします。

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

- **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。
- **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。
- **None**

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 Autoconf を使用してアクセスポイント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。

- a) スライドインペインで、次の手順を実行します。
- [First Authentication Method] : [802.1x] または [MAC Authentication Bypass (MAB)] を選択します
 - [802.1x Timeout (in seconds)] : スライダを使用して、802.1x タイムアウトを秒単位で指定します。
 - [Wake on LAN] : [Yes] または [No] を選択します。
 - [Number of Hosts] : [Unlimited] または [Single] を選択します。
- (注) [Number of Hosts] は、1つの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。
- [Pre-Authentication Access Control List] : トグルボタンを有効にして、[Low Impact] 認証の事前認証制御を構成します。[Implicit Action] ドロップダウンリストから、暗黙的なアクションを選択します。ルールの説明を入力します。アクセスコントラクトを追加するには、[Add Contract Action] をクリックし、ルールを選択して、[Apply Table] をクリックします。
- b) **[Save]** をクリックします。
- 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。

ファブリックサイト内のポートの設定

[Port Assignment] タブで、ファブリックサイト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。

- ステップ1** メニューアイコン (☰) をクリックして、**[Provision] > [Fabric Sites]**。
- ステップ2** [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。
- ステップ3** ファブリックサイトを選択します。
- ステップ4** [Port Assignment] タブをクリックします。
- ステップ5** ファブリックデバイスのリストから、構成するデバイスのドロップダウンを展開します。
 デバイスで利用可能なポートが表示されます。
- ステップ6** デバイスのポートのチェックボックスをオンにします。
- ステップ7** [Configure] にカーソルを合わせ、[Assign Ports] を選択します。
- ステップ8** slide-in pane 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
[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。

オプション	説明
アクセス ポイント (AP)	アクセスポイントに接続するポートを設定します。
トランク	ポートをトランク ポートとして設定します。
サブリカントベースの拡張ノード	サブリカントベースの拡張ノードを受信するようにポートを設定します。

- 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 (Data)] ドロップダウンリストからデータの VLAN 名を選択します。
 2. [Security Group] ドロップダウンリストからセキュリティグループを選択します。
セキュリティグループは、[None] 認証テンプレートでのみサポートされます。
 3. [VLAN Name (Voice)] ドロップダウンリストから音声の VLAN 名を選択します。
 4. [Authentication Template] ドロップダウンリストから認証タイプを選択します。
 5. コネクテッドデバイスに関する [Description] を入力します。
- 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 (Data)] ドロップダウンリストから VLAN 名を選択します。
 2. [Authentication Template] 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。
- サブリカントベースの拡張ノードデバイスを接続するには、[Supplicant-Based Extended Node] を選択します。
- トランクポートを接続するには、[Trunk] を選択し、ポートの説明を [Description] に入力します。

ステップ 9 [更新 (Update)] をクリックします。

ファブリックネットワークのワイヤレス SSID の設定

始める前に

ワイヤレスデバイスをファブリックサイトに追加してください。

ステップ 1 メニューアイコン (☰) をクリックして、[Provision] > [Fabric Sites].

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

- ステップ3** ファブリックサイトを選択します。
- ステップ4** [Wireless SSID] タブをクリックし、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5** [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6** [Assign SGT] ドロップダウンリストから、SSID のセキュリティグループを選択します。
- ステップ7** 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。

仮想ネットワーク

仮想ネットワークは、共通物理ネットワークインフラストラクチャ内でトラフィックをセグメント化するために使用されるオーバーレイです。これは「マクロセグメンテーション」とも呼ばれます。レイヤ2 仮想ネットワークはスイッチドトラフィックをセグメント化し、レイヤ3 仮想ネットワークはルーテッドトラフィックをセグメント化します。Cisco SD-Access ファブリックに接続されている各エンドポイントは、静的エッジポート設定または Identity Service Engine からの動的ポリシーに基づいて、特定の仮想ネットワークに割り当てられます。仮想ネットワークのエンドポイントは、マイクロセグメンテーションポリシーによって明示的にブロックされていないかぎり、相互に通信できます。異なる仮想ネットワークにまたがるエンドポイントは、デフォルトでは、相互に通信できません。仮想ネットワーク間トラフィックの場合は、接続ポリシーを Cisco SD-Access ファブリックの外部（フュージョンデバイス上など）で実装する必要があります。

仮想ネットワークの一般的な使用例は、社内エンドポイントとビルディング管理システムの両方を含むオフィスビルです。社内エンドポイントは、照明、暖房、換気、空調などのビルディングシステムとは別にセグメント化する必要があります。この場合、ネットワーク管理者は、2 つ以上の仮想ネットワークを使用して社内エンドポイントとビルディングシステムをマクロセグメント化することにより、ビルディングシステムと社内エンドポイントの間の不正アクセスをブロックすることができます。

レイヤ3 仮想ネットワークは、複数のファブリックサイトやネットワークドメイン（ワイヤレス LAN、キャンパス LAN、および WAN）にまたがる場合があります。レイヤ2 仮想ネットワークは、単一のファブリックサイト内に存在します。

レイヤ3 仮想ネットワークの作成

- ステップ1** メニューアイコン（☰）をクリックして、[Workflows] > [Create Layer 3 Virtual Networks] の順に選択します。
- または、[Provision] > [Virtual Networks] で [Layer 3] タブに移動し、[Create Layer 3 Virtual Networks] をクリックすることもできます。
- ステップ2** タスクの概要ウィンドウが開いたら、[Let's Do it] をクリックして、ワークフローに直接移動します。

- ステップ3** [Choose your creation process] ウィンドウで、作成するレイヤ3仮想ネットワークの数を入力します。
- ステップ4** [Create your Layer 3 virtual networks] ウィンドウで、レイヤ3仮想ネットワークの名前を入力します。
- ステップ5** [Select your Fabric Sites] ウィンドウで、次のいずれかをクリックします。
- [By Layer 3 Virtual Network] タブ：レイヤ3仮想ネットワークを複数のファブリックサイトに関連付けるには、対応するドロップダウンリストからレイヤ3仮想ネットワークとファブリックサイトを選択します。仮想ネットワークは複数のファブリックサイトに割り当てることができます。作成したすべてのレイヤ3仮想ネットワークについて、この関連付けを繰り返します。
 - [By Fabric Site] タブ：複数のレイヤ3仮想ネットワークをファブリックサイトに割り当てるには、対応するドロップダウンリストからファブリックサイトとレイヤ3仮想ネットワークを選択します。複数のレイヤ3仮想ネットワークを1つのファブリックサイトに割り当てることができます。必要なすべてのファブリックサイトについて、この関連付けを繰り返します。
- ステップ6** [Configuring traffic exit behavior] ウィンドウで、この仮想ネットワークが複数のファブリックサイトに関連付けられている場合のトラフィックの出口動作を設定します。
- デフォルトでは、[Local Exit] が選択されています。このオプションにより、関連付けられている各ファブリックサイトのローカルボーダーを通過してトラフィックが出るようになります。
 - 仮想ネットワークを位置指定し、指定された境界でトラフィックが出られるようにするには、[Anchor (Multisite Remote Border)] を選択します。
- 関連付けられているファブリックサイトのリストから、この仮想ネットワークにおけるすべてのトラフィックに関して出口として機能するボーダーを持つサイトを選択します。関連付けられている他のファブリックサイトは、この仮想ネットワークを継承します。
- ステップ7** [Summary] ウィンドウで、レイヤ3仮想ネットワークの設定を確認します。
- ステップ8** [Let's begin deploying your Layer 3 virtual network] ウィンドウで、[Create] をクリックして仮想ネットワークのコンテキストを作成します。
- ステップ9** 選択したサイトに仮想ネットワークを割り当てるには、[Deploy] をクリックします。
- ステップ10** 仮想ネットワークの作成を確認するには、[View All Virtual Networks] をクリックします。
- [Virtual Networks] ウィンドウに、ファブリックに含まれるすべてのレイヤ3仮想ネットワークの詳細情報が表示されます。

レイヤ2仮想ネットワークの作成

- ステップ1** メニューアイコン (☰) をクリックして、[Workflows] > [Create Layer 2 Virtual Networks] の順に選択します。
- または、[Provision] > [Virtual Networks] で [Layer 2] タブに移動し、[Create Layer 2 Virtual Networks] をクリックすることもできます。

- ステップ2** タスクの概要ウィンドウが開いたら、[Let's Do it] をクリックして、ワークフローに直接移動します。
- ステップ3** [Configure VLANs] ウィンドウで、ファブリックに接続する VLAN の数を入力するには、次の手順を実行します。
- 各 VLAN の **VLAN 名** とオプションの **VLAN ID** を入力します。
 - [Traffic Type] ドロップダウンリストで、[Data] または [Voice] を選択します。
レイヤ2仮想ネットワークではフラッドリングがデフォルトで有効になっています。
 - (オプション) [Wireless] ボタンを切り替えてワイヤレスを有効にします。
- ステップ4** [Select a fabric site for each Layer 2 virtual network] ウィンドウで、レイヤ2仮想ネットワークのファブリックサイトを選択します。
- 必要に応じて、このレイヤ2仮想ネットワークに関連付けるレイヤ3仮想ネットワークを選択できます。
- (注) [L3VN Name] ドロップダウンでレイヤ3仮想ネットワークを選択しないことで、純粋なレイヤ2仮想ネットワークを作成できます。
- ステップ5** [Summary] ウィンドウで、レイヤ2仮想ネットワークの設定を確認して、[Create] をクリックします。
- ステップ6** レイヤ2仮想ネットワークのプロビジョニングを確認するために、[Submit] をクリックします。
- レイヤ2仮想ネットワークがプロビジョニングされると、成功メッセージが表示されます。
- ステップ7** レイヤ2仮想ネットワークの作成を確認するには、[Virtual Network Overview] をクリックします。[Virtual Networks] ウィンドウの [Layer 2] タブには、ファブリックに含まれるすべてのレイヤ2仮想ネットワークの詳細情報が表示されます。

ファブリックサイトへのレイヤ3仮想ネットワークの追加

- ステップ1** メニューアイコン (☰) をクリックして、[Provision] > [Virtual Networks]。
- ステップ2** [NETWORK OBJECTS] で、[Layer 3 Virtual Networks] の数を示す数字をクリックします。
- 表示されるウィンドウに、グローバルレベルで作成されたすべてのレイヤ3仮想ネットワークが示されます。
- ステップ3** [Layer 3] タブの、目的のレイヤ3仮想ネットワークの [Actions] 列で、カーソルを省略記号アイコン (⋮) の上に置き、[Add to Fabric Site] を選択します。
- ステップ4** [Select Fabric Site] スライドインペインで、サイトを選択し、[Select] をクリックします。
-

エニーキャストゲートウェイの作成

始める前に

レイヤ3仮想ネットワークが作成されていることを確認します。

ステップ 1 メニューアイコン (☰) をクリックして、**[Provision] > [Virtual Networks]**。

ステップ 2 **[LAYER 2]** で、**[Anycast Gateways]** の数を示す数字をクリックします。

ステップ 3 **[Anycast Gateway]** タブで、**[Create Anycast Gateway]** をクリックします。

または、**[Layer 3]** タブで、レイヤ 3 仮想ネットワークの**[Actions]** 列の下にある省略記号アイコン (⋮) の上にカーソルを置き、**[Create Anycast Gateways]** を選択して**ステップ 6 (19 ページ)** へスキップします。

ステップ 4 **[Let's Do it]** をクリックします。

ステップ 5 **[Select Layer 3 Virtual Networks to configure]** ウィンドウで、ゲートウェイを追加する 1 つ以上の仮想ネットワークを選択します。

ステップ 6 **[Add IP Pools and VLANs]** ウィンドウの左側のペインで、ゲートウェイを作成するレイヤ 3 仮想ネットワークを選択し、次の手順を実行します。

- a) ドロップダウンリストから **[IP Pool]** を選択します。
- b) **INFRA_VN** に対して、次の手順を実行します。
 - **[Pool Type]** ドロップダウンリストから **[AP]** または **[Extended Node]** を選択します。
 - **[VLAN Name]** に有効な VLAN 名を入力するか、**[Auto generate VLAN name]** チェックボックスをオンにします。
 - **[VLAN ID]** に仮想ネットワークのカスタム VLAN ID を入力します。
 - サプリカントベースの拡張ノードをオンボードするには、**[Supplicant-Based Extended Node Onboarding]** チェックボックスをオンにします。

(注) このチェックボックスは、**[Extended Node]** プールタイプを選択した場合にのみ表示されます。
- c) IP ダイレクトブロードキャスト機能を有効にするには、**[Directed Broadcast]** トグルボタンをクリックします。

(注)

 - 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 フラッドイングを有効にします。
 - ルータおよび Nexus 7000 シリーズ スイッチは、ダイレクトブロードキャストをサポートしていません。
 - ダイレクトブロードキャストを有効にする前に、アンダーレイマルチキャストが有効になっていることを確認してください。
- d) **[VLAN Name]** に有効な VLAN 名を入力するか、**[Auto generate VLAN name]** チェックボックスをオンにします。
- e) **[VLAN ID]** に仮想ネットワークのカスタム VLAN ID を入力します。

- (注)
- 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。


- f) [Traffic Type] ドロップダウンリストから、[Data] または [Voice] を選択します。
- g) ドロップダウンリストから [Security Group] を選択します。
- h) 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 VLAN] トグルボタンをクリックします。

認証サーバーを使用できない場合、クリティカルプールが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。

- i) レイヤ 2 仮想ネットワークを有効にするには、[Enable] トグルボタンをクリックします。
- j) レイヤ 2 フラッディングを有効にするには、[Flooding] トグルボタンをクリックします。
- (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。

- k) 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] トグルボタンをクリックします。
- l) ファブリック対応のワイヤレスネットワークに接続されているブリッジモードの仮想マシンのオンボーディングを有効にするには、[Bridge Mode VM] トグルボタンをクリックします。

(注) [Bridge-Network Virtual Machine] トグルボタンは、ワイヤレストグルボタンを有効にした場合にのみ表示されます。

- m) 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 7 [Summary] ウィンドウで、エンドポイントの接続設定を確認します。

ステップ 8 [Let's begin creating your Gateway] ウィンドウで、[Create] をクリックします。

ステップ 9 成功メッセージが表示された後にゲートウェイの作成を確認するには、[View All Virtual Networks] をクリックします。

ファブリックゾーンの設定

ファブリックサイト（親サイト）は、ネットワークを簡単に管理できるように、より小さなサブネットによるファブリックゾーンに分割できます。ファブリックゾーンは、独自のエッジノードと拡張ノードを持つことができますが、コントロールプレーンとボーダーのために親サイトに接続します。以前の Cisco DNA Center のリリースから現在のリリースに移行した場合は、既存のファブリックサイトにファブリックゾーンを作成することができます。このファブリックゾーンは、親サイトのすべてのプロパティを継承します。

はじめる前に

- ネットワーク階層がグローバルサイトの下に作成されていることを確認します。
- 階層の最下位に位置していない親サイトを選択します。

次に、ファブリックゾーンを設定するためのワークフローの概要を示します。

1. 次のいずれかの方法でファブリックゾーンを作成します。
 - **[Create a Fabric Site]** ワークフローを使用して、ファブリックサイトとそのゾーンを作成します。詳細については、[ファブリックサイトおよびそのファブリックゾーンの作成 \(21 ページ\)](#) を参照してください。
 - 既存のファブリックサイトを編集して、ファブリックゾーンを追加します。詳細については、[ファブリックサイト内のファブリックゾーンの作成 \(23 ページ\)](#) を参照してください。
2. ファブリックゾーンにエッジノードと拡張ノードを追加します。詳細については、[ファブリックへのデバイスの追加 \(7 ページ\)](#) を参照してください。
3. ファブリックゾーンにレイヤ 3 仮想ネットワークとセグメントを割り当てます。詳細については、[ファブリックゾーンへのレイヤ 3 仮想ネットワークの追加 \(23 ページ\)](#) を参照してください。



(注) ファブリックゾーンで使用できるのは親サイトの仮想ネットワークとセグメントのみです。



(注) ファブリックゾーンに追加されたセグメントは、親サイトでは更新できません。
親サイトのファブリックゾーンのエッジノードおよび拡張ノードは編集できません。
ファブリックゾーンのエッジノードは、親サイトのコントロールプレーンまたはボーダーとして設定できます。

ファブリックサイトおよびそのファブリックゾーンの作成

ステップ 1 メニューアイコン (☰) をクリックして、**[Provision] > [Fabric Sites]**。

ステップ 2 **[Create Fabric Site]** をクリックします。

または、メニューアイコンをクリックして**[Workflows] > [Create Fabric Site]**の順に選択します。

ステップ 3 タスクの概要ウィンドウが表示されたら、**[Let's Do It]** をクリックして、ワークフローに直接移動します。

ステップ 4 **[Fabric Site Location]** ウィンドウで、ファブリックゾーンとして追加するエリア、建物、またはフロアを選択します。

ステップ 5 [Wired Endpoint Data Collection] ウィンドウで、[Monitor wired clients] 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。

ステップ 6 [Authentication Template] ウィンドウで、次の手順を実行します。

a) ファブリックサイトの認証テンプレートを選択します。

- [Closed Authentication] : 認証前のすべてのトラフィック (DHCP、DNS、ARP など) が廃棄されません。
- **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。
- [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。
- **None**

b) (オプション) [Closed Authentication]、[Open Authentication]、または [Low Impact] を選択した場合は、[Edit] をクリックして認証設定を編集します。

- [First Authentication Method] : [802.1x] または [MAC Authentication Bypass (MAB)] を選択します
- [802.1x Timeout (in seconds)] : スライダーを使用して、802.1x タイムアウトを秒単位で指定します。
- [Wake on LAN] : [Yes] または [No] を選択します。
- [Number of Hosts] : [Unlimited] または [Single] を選択します。
- [BPDU Guard] : このチェックボックスを使用して、すべての [Closed Authentication] ポートでブリッジプロトコルデータユニット (BPDU) ガードを有効または無効にします。
- [Pre-Authentication Access Control List] : トグルボタンを有効にして、[Low Impact] 認証の事前認証制御を構成します。[Implicit Action] ドロップダウンリストから、暗黙的なアクションを選択します。ルールの説明を入力します。アクセスコントラクトを追加するには、[Add Contract Action] をクリックし、ルールを選択して、[Apply Table] をクリックします。

ステップ 7 [Fabric Zones] ウィンドウで、ファブリックゾーンを指定し、範囲指定されたサブネットを作成するには、[Setup Fabric Zones Now] をクリックします。

ファブリックゾーンを有効にするには、ネットワーク階層でファブリックサイトを選択します。

ステップ 8 [Summary] ウィンドウで、ファブリックサイトの設定を確認します。

ここでファブリックサイトまたはゾーン設定を編集できます。

ステップ 9 [Deploy] をクリックします。

サイトとゾーンがプロビジョニングされるまでに数秒かかります。サイトの作成が成功すると、「Success! Your fabric site is created」というメッセージが表示されます。

サイト階層ペインでは、新しく作成されたファブリックゾーンに「FZ」というタグが付けられます。

ファブリックサイト内のファブリックゾーンの作成

ステップ1 メニューアイコン (☰) をクリックして、[Provision] > [Fabric Sites]。

ステップ2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ3 ファブリックゾーンを指定するファブリックサイトの[Actions]列で、省略記号アイコン (⋮) の上にカーソルを置き、[Edit Fabric Zone] を選択します。

ステップ4 [Fabric Zones] ウィンドウで、エリア、建物、またはフロアを選択します。

ステップ5 [Next] をクリックします。

ステップ6 [Summary] ウィンドウに表示されるファブリックサイトの設定を確認します。

ここでファブリックサイトまたはゾーン設定を編集できます。

ステップ7 [Deploy] をクリックします。

サイトとゾーンがプロビジョニングされるまでに数秒かかります。「**Success!**Your fabric site is created」というメッセージが表示されます。

サイト階層ペインでは、新しく作成されたファブリックゾーンに「FZ」というタグが付けられます。

次のタスク

- 新しく作成したファブリックゾーンにエッジノードデバイスと拡張ノードデバイスのみを追加します。

ファブリックゾーンに割り当てられたデバイスを親サイトに割り当てることはできません。ただし、ファブリックゾーンに割り当てられたエッジノードデバイスを親サイトのコントロールプレーンまたはボーダーノードとして設定することは引き続き可能です。

- ファブリックゾーンに IP プールと仮想ネットワークを割り当てます。

ファブリックゾーンへのレイヤ3仮想ネットワークの追加

始める前に

ファブリックゾーンが作成されていることを確認します。



(注) ファブリックゾーンに追加できるのは親サイトのレイヤ3仮想ネットワークのみです。

-
- ステップ1** メニューアイコン (☰) をクリックして、**[Provision] > [Virtual Networks]**。
- ステップ2** **[NETWORK OBJECTS]** で、**[Layer 3 Virtual Networks]** の数を示す数字をクリックします。
表示されるウィンドウに、グローバルレベルのすべてのレイヤ3仮想ネットワークが示されます。
- ステップ3** **[Global]** ファブリックサイトをクリックします。
- ステップ4** **[Select Fabric Site]** スライドインペインで、ファブリックゾーンを選択し、**[Select]** をクリックします。
- ステップ5** **[Layer 3]** タブで、**[Add Layer 3 VN]** をクリックします。
- ステップ6** **[Add Virtual Network]** スライドインペインで、ファブリックゾーンに追加する仮想ネットワークを選択します。**[更新 (Update)]** をクリックします。
-

ファブリックゾーンへのレイヤ2仮想ネットワークの追加

始める前に



(注) ファブリックゾーンに追加されたゲートウェイは、親サイトでは更新できません。

-
- ステップ1** メニューアイコン (☰) をクリックして、**[Provision] > [Virtual Networks]**。
- ステップ2** **[LAYER 2]** で、**[Layer 2 Virtual Networks]** の数を示す数字をクリックします。
表示されるウィンドウに、グローバルレベルのすべてのレイヤ2仮想ネットワークが示されます。
- ステップ3** **[Global]** ファブリックサイトをクリックします。
- ステップ4** **[Select Fabric Site]** スライドインペインで、ファブリックゾーンを選択し、**[Select]** をクリックします。
- ステップ5** **[Layer 2]** タブで、**[Add Layer 2 Virtual Network]** をクリックします。
- ステップ6** **[Select L2VNs]** スライドインペインで、レイヤ2仮想ネットワークを選択します。
- ステップ7** **[Add]** をクリックします。
-

ファブリックゾーンへのエニーキャストゲートウェイの追加

始める前に

ファブリックゾーンが作成されていることを確認します。



(注) 親サイトのエニーキャストゲートウェイのみをファブリックゾーンに追加できます。

ファブリックゾーンに追加されたエニーキャストゲートウェイは、親サイトでは更新できません。

ステップ 1 メニューアイコン (☰) をクリックして、[Provision] > [Virtual Networks]。

ステップ 2 [LAYER 2] で、[Anycast Gateways] の数を示す数字をクリックします。

表示されるウィンドウに、グローバルレベルのすべてのエニーキャストゲートウェイが示されます。

ステップ 3 [Global] ファブリックサイトをクリックします。

ステップ 4 [Select Fabric Site] スライドインペインで、ファブリックゾーンを選択し、[Select] をクリックします。

ステップ 5 [Anycast Gateway] タブで、[Add Anycast Gateway] をクリックします。

ステップ 6 [Select Anycast Gateway(s)] スライドインペインで、レイヤ 3 仮想ネットワークを選択し、[Next] をクリックします。

ステップ 7 追加するエニーキャストゲートウェイを選択します。

ステップ 8 [Add] 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、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トポロジビューに表示されます。[Port Assignment] タブを使用して、拡張ノードにポートを割り当てることができます。



(注) 拡張ノードは、GUI ベ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。

デバイスは、拡張ノードネイバーの Cisco DNA ライセンスおよびデバイスの Cisco DNA ライセンスに応じてオンボードされます。

- ネイバーが Cisco DNA Essentials ライセンスで動作している場合、デバイスは、その Cisco DNA ライセンスに関係なく、標準の拡張ノードとしてオンボードされます。
- ネイバーが Cisco DNA Advantage ライセンスで動作している場合、デバイスは、Cisco DNA Essentials ライセンスがあれば、標準の拡張ノードとしてオンボードされます。
- ネイバーが Cisco DNA Advantage ライセンスで動作している場合、デバイスは、Cisco DNA Advantage ライセンスがあれば、ポリシー拡張ノードとしてオンボードされます。
- デバイ스에複数のネイバーがあり、それらのネイバーに異なる Cisco DNA ライセンスレベルがある場合、デバイスは Cisco DNA ライセンスに関係なく、標準の拡張ノードとしてオンボードされます。

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。

ポリシー拡張ノードデバイスには、Cisco IOS XE リリース 17.1.1s 以降を実行している Cisco Catalyst Industrial Ethernet (IE) 3400、IE 3400 Heavy Duty シリーズ スイッチ、および Cisco Catalyst 9000 シリーズ スイッチがあります。

シスコ 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 Industrial Ethernet 4000、4010、5000 シリーズ スイッチは、ポリシー拡張ノードとして構成することはできません。

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。



(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)
IP サービスライセンスがある場合は、Switch Database Management (SDM) テンプレートを `dual-ipv4-and-ipv6 default` に手動で変更する必要があります。
- Cisco Catalyst IE 3400、3400 Heavy Duty (X-coded および D-coded) シリーズ スイッチ：Cisco IOS XE リリース 17.1.1s。
- Cisco Catalyst IE 3300 シリーズ スイッチ：Cisco IOS XE リリース 16.12.1s。
- Cisco Digital Building シリーズ スイッチ、Cisco Catalyst 3560-CX スイッチ：リリース 15.2(7)E0s。

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ノードデバイスに必要な最小ソフトウェアバージョンは Cisco IOS XE リリース 17.1.1 s です。

次の設定手順は、標準の拡張ノードとポリシー拡張ノードの両方に適用されます。

始める前に

ポリシー拡張ノードとしてデバイスを設定するには、デバイスとそれをサポートするエッジノードの両方で、Network Advantage と Cisco 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INFRA_VNに割り当てます。[エニーキャストゲートウェイの作成 \(18 ページ\)](#)を参照してください。[Pool Type]として[Extended Node]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。リングまたはダイジェーション内の後続の拡張ノードに関して、それが接続している、前の拡張ノードでポートチャネルを作成します。

(注) この手順は、ファブリックのグローバル認証モードが[Open Authentication]、[Low Impact]、または[Closed Authentication]の場合にのみ完了してください。ファブリックサイトが[None]認証モードに設定されている場合、ポートチャネルは、プラグアンドプレイプロビジョニングを使用した拡張ノードのオンボーディング中に自動的に作成されます。

ポートチャネルを作成するには、次の手順を実行します。

- a) メニューアイコン (☰) をクリックして、[Provision] > [Fabric Sites]。
- b) [Fabric Sites] タブで、ファブリックサイトの数を示す数字をクリックします。
- c) ファブリックサイトを選択します。
- d) [Fabric Infrastructure] タブで、ファブリックエッジノード (または接続に応じて拡張ノード) を選択します。
- e) スライドインペインの [Port Channel] タブで、[Create Port Channel] をクリックします。
- f) 次の手順を実行します。

- [Connected Device Type] ドロップダウンリストから [Extended Node] を選択します。
- 説明を入力します。
- [Port Aggregation Protocol (PAgP Desirable)] 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 リリース 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。

(注) 拡張ノードのオンボーディングでは Link Aggregation Control Protocol (LACP) は機能しません。

- 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。

g) [Done] をクリックします。

これで、ファブリックエッジノード（または拡張ノード）にポートチャネルが作成され、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。

拡張ノードのポリシー拡張ノードへのアップグレード

Cisco SD-Access の自動化は、Cisco DNA Essentials ライセンスを持つポリシー拡張ノード対応デバイスを拡張ノードとしてオンボーディングします。ライセンスを Cisco DNA Advantage にアップグレードすることにより、この拡張ノードデバイスをポリシー拡張ノードに変換できます。

デジチェーンでは、アップストリームデバイスが拡張ノードである場合、拡張ノードをポリシー拡張ノードにアップグレードすることはできません。

リングでは、隣接するノードが両方とも拡張ノードである場合、拡張ノードをポリシー拡張ノードにアップグレードすることはできません。

ポリシー拡張ノードにアップグレードされたノードを、拡張ノードとして再構成することはできません。

拡張ノードをポリシー拡張ノードに変換するには、次の手順を実行します。

始める前に

- 拡張ノードがすでにオンボーディングされていることを確認してください。
- Cisco DNA Center でスマートライセンス認証情報を更新します。

ステップ 1 Cisco DNA Center ライセンスマネージャを使用して、デバイスでのライセンスレベルを Cisco DNA Essentials から Cisco DNA Advantage に変更します。

a) メニューアイコン (☰) をクリックして、[Tools] > [License Manager] の順に選択します。

- b) [Devices] タブで、デバイスを選択します。
 - c) [Actions] > [Change License] > [Change DNA License] を選択します。
 - d) [Change DNA License Level] ウィンドウで、[Advantage] をクリックします。
 - e) [Confirm] をクリックします。
 - f) [Success] メッセージウィンドウで、[OK] をクリックします。
- デバイスがリロードします。

ステップ 2 ノードが [Reachable] になり、[Managed] 状態になるのを待ちます。

[Provision] > [Network Devices] > [Inventory] ウィンドウに、すべてのデバイスの到達可能性ステータスが表示されます。

ステップ 3 「Netconf Connection Refused」エラーが表示された場合は、デバイスを再同期します。エラーがなくなるまで、再同期プロセスを繰り返します。

- a) [Provision] > [Network Devices] > [Inventory] ウィンドウで、デバイスを選択します。
- b) [Actions] > [Inventory] > [Resync Device] の順に選択します。

ステップ 4 ポリシー拡張ノードへアップグレードします。

- a) [Provision] > [Fabric Sites] ウィンドウで、デバイスがオンボーディングされているサイトを選択します。
- b) [Fabric Infrastructure] タブで、デバイスをクリックしてその属性を編集します。
- c) [Fabric] タブで、[Extended Node Attributes] の下の [Policy] ボタンを切り替えます。
- d) 表示される [Policy Extended Node Upgrade] ウィンドウで、[Upgrade] をクリックします。

拡張ノードの削除

このタスクでは、拡張ノード、ポリシー拡張ノード、および認証済み拡張ノードを削除する手順について説明します。

ステップ 1 ファブリックから拡張ノードデバイスを削除します。

- a) メニューアイコン (☰) をクリックして、[Provision] > [Fabric Sites]。
- b) [Fabric Sites] タブで、ファブリックサイトの数を示す数字をクリックします。
- c) 拡張ノードデバイスを含むファブリックサイトを選択します。
- d) [Fabric Infrastructure] タブで、拡張ノードデバイスをクリックします。
- e) スライドインペインで、[Remove From Fabric] をクリックします。
- f) [Add] をクリックします。

ステップ 2 デバイスを [Inventory] から削除します。

インベントリからデバイスを削除する手順については、[ネットワーク デバイスの削除](#)を参照してください。

ステップ3 サブリカントベースの拡張ノードデバイスの場合、ファブリックエッジノードまたは FIAB でポート割り当て設定を削除します。

拡張ノードおよびポリシー拡張ノードの REP リングトポロジの設定

拡張ノードによってネットワーク障害の回復時間が 50 ms 未満となる冗長性を実現するには、ファブリックサイトの Resilient Ethernet Protocol (REP) リングを設定します。

特に明記されていないかぎり、「拡張ノード」という用語はポリシー拡張ノードも表します。

REP リングでは、次のデバイスを設定できます。

- 拡張ノード：

Cisco IOS 15.2(7)E3 以降のリリースが動作する Cisco Industrial Ethernet (IE) 4000、4010、5000 シリーズ スイッチ。

Cisco IOS XE 17.3.3 以降のリリースが動作する Cisco Catalyst IE3300 シリーズ スイッチ。

- ポリシー拡張ノード：

Cisco IOS XE 17.3.3 以降のリリースが動作する Cisco Catalyst IE3400、IE3400H シリーズ スイッチ。

REP リングの制約事項

- 拡張ノードを既存の REP リングに追加するには、最初に REP リングを削除します。REP リングを削除すると、Per VLAN Spanning Tree Protocol (PVSTP) が有効になり、レイヤ 2 ループが回避されます。次に、新しい拡張ノードをファブリックに追加し、REP リングを再度作成して、新しい拡張ノードを含めます。
- 特定の REP リング内の複数のリングおよびリングのリングはサポートされていません。
- REP リング内のノードには、ダイジーチェーン方式で他のノードを接続できます。ただし、ダイジーチェーンのノードには、ノードのリングを接続することはできません。
- REP リングまたはダイジーチェーンでは、拡張ノードとポリシー拡張ノードを混在させることはできません。REP リングまたはダイジーチェーンは、拡張ノードのみで、またはポリシー拡張ノードのみで構成されている必要があります。
- デフォルトでは、1 つの REP リングに最大 18 台のデバイスをオンボードできます。19 台以上のデバイスをオンボードするには、**spanning-tree vlan infra VN VLAN max-age 40** コマンドを使用して BPDU タイマーを増やします。このコマンドを設定するには、Cisco DNA Center のテンプレートを使用します。

リングの最後の 2 つのノードが同時にオンボードを試みると、まれに、これらのノード間にポートチャンネルが作成されない場合があることに注意してください。REP リングが作成されると、リングの最後の 2 つのノード間にポートチャンネルが確立されます。

特に明記されていないかぎり、次の手順は拡張ノードとポリシー拡張ノードの両方に適用されます。

始める前に

ファブリックエッジノードと拡張ノードがオンボードされていることを確認します。

REP リングの終端となっているファブリックエッジノードとそのインターフェイスを特定します。



(注) REP リング設定手順により、ネットワークトラフィックが短時間中断される可能性があります。

-
- ステップ 1** メニューアイコン (☰) をクリックして、[Workflows] > [Configure REP Ring] の順に選択します。
- または、ファブリックサイトトポロジビューに移動して、REP リングを作成するファブリックエッジノードまたは FIAB ノードを選択し、[REP Rings] タブで [Create REP Ring] をクリックすることもできます。
- ステップ 2** タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローに直接移動します。
- ステップ 3** [Select a fabric site] ウィンドウで、エッジノードと拡張ノードの両方があるサイトを選択します。
- ステップ 4** [Select a fabric edge node] ウィンドウで、ファブリックエッジノードを選択します。
- ステップ 5** [Select Extended Nodes connected to Fabric Edge] ウィンドウで、ファブリックエッジノードに接続する拡張ノードを選択します。
- ファブリックエッジノードに接続する 2 つの拡張ノードを選択できます。
- ステップ 6** ファブリックサイト、エッジノード、および拡張ノードの選択を確認し、必要に応じて編集します。
- ステップ 7** REP リングの設定を開始するには、[Provision] をクリックします。
- [REP Ring Configuration Status] ウィンドウで、設定の進捗状況の詳細なステータスを確認できます。
- ステップ 8** [REP Ring Summary] ウィンドウに、作成された REP リングの詳細情報が、検出されたデバイスとともに表示されます。
- ステップ 9** REP リングの作成後、成功メッセージが表示されます。
- REP リングの作成を確認するには、ファブリックサイトウィンドウに移動し、ファブリックエッジノードをクリックします。
- スライドインウィンドウの [REP Ring] タブで、そのエッジノードに存在するすべての REP リングのリストを確認できます。
- リスト内の REP リング名をクリックすると、リングに存在するデバイス、リングに接続する各デバイスのポートなどの詳細情報が表示されます。
-

REP リングステータスの表示

REP リング内のデバイスのステータスを表示するには、次の手順を実行します。

ステップ 1 Cisco DNA Center GUI でメニューアイコン (☰) をクリックして、**[Provision] > [Fabric Sites]**。

ステップ 2 **[Fabric Sites]** タブで、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 すべてのファブリックサイトを表示するリストからファブリックサイトを選択します。

ステップ 4 **[Fabric Infrastructure]** タブで、ファブリックエッジノードまたは FIAB をクリックします。

スライドインウィンドウに、選択したファブリックエッジノードまたは FIAB の詳細が表示されます。

ステップ 5 **[REP Rings]** タブで、**[View]** をクリックして **[REP Ring Topology Status]** を表示します。

[REP Topology Status] セクションには、REP リング内のすべてのデバイスの現在の状態が表示されます。**[Role]** 列に表示される状態は、**[Open]**、**[Fail]**、または **[Alt]** です。

[Open] は、デバイスリンクが稼働していて、トラフィックを転送していることを示します。

[Fail] は、デバイスリンクがダウンしていることを示します。

[Alt] は、デバイスリンクがアップしているが、ポートがトラフィックを転送できないことを示します。

REP リングの削除

ステップ 1 メニューアイコン (☰) をクリックして、**[Provision] > [Fabric Sites]**。

ステップ 2 **[Fabric Infrastructure]** タブで、REP リングを終了するファブリックエッジノードをクリックします。

スライドインウィンドウに、選択したファブリックエッジノードの詳細が表示されます。

ステップ 3 **[REP Rings]** タブで、目的の REP リングの **[Actions (...)] > [Delete]** をクリックします。

これにより、REP リングが削除されます。

REP リングからのノードの削除

このタスクでは、REP リングから1つまたは複数の拡張ノードを削除する手順について説明します。



(注) 拡張ノードが削除された後、ダウンサイジングされた REP リングは既存のインターフェイスを使用して隣接デバイスへのリンクを作成する必要があります。

始める前に

ノードが属する REP リングが不完全でないことを確認してください。

ステップ 1 拡張ノードデバイスをネットワークから手動で削除します。

または、REP リング内のデバイスがダウンすると、[Fabric Infrastructure] ウィンドウに通知が表示されません。

ステップ 2 メニューアイコン (☰) をクリックして、[Provision] > [Fabric Sites]。

ステップ 3 [Fabric Infrastructure] タブで、REP リングを終了するファブリックエッジノードをクリックします。

slide-in paneに、選択したファブリックエッジノードの詳細が表示されます。

ステップ 4 [REP Rings] タブで、目的の REP リングについて、[Actions (...)] > [Rediscover]を選択します。

REP リングから拡張ノードデバイスが削除され、REP リングの表示が更新されます。

サブリカントベースの拡張ノードの設定

Authenticated Extended Node (AEN) とも呼ばれるサブリカントベースの拡張ノードは、IEEE 802.1x (Dot1x) サブリカント設定を受け取り、完全な認証と承認の後にのみ SD-Access ネットワークにオンボードされる拡張ノードデバイスです。サブリカントベースの拡張ノードデバイスをオンボードするには、ファブリックエッジのオーセンティケータポートをクロズド認証テンプレートで設定する必要があります。

次のプラットフォームは、サブリカントベースの拡張ノードオンボーディングをサポートしています。

ファブリックエッジまたは FIAB :

Cisco Catalyst 9000 シリーズ : Cisco IOS XE 17.7.1 以降で動作する C9300、C9400、C9500、および C9500H スイッチ。

サブリカントベースの拡張ノード :

Cisco Catalyst 9000 シリーズ : Cisco IOS XE 17.7.1 以降で動作する C9200、C9300、C9400、C9500、および C9500H スイッチ。

サブリカントベースの拡張ノードの設定手順

始める前に

- Cisco ISE を構成して、リリース 3.1 以降で動作することを確認します。「[サブリカントベースの拡張ノードをオンボードするための Cisco Identity Services Engine の設定 \(36 ページ\)](#)」を参照してください。

- ファブリックエッジノードまたは FIAB デバイスをファブリックに追加し、それが Cisco IOS XE 17.7.1 以降で動作することを確認します。
- ファブリックエッジノードと Cisco ISE の間のパスに適切なパス MTU を設定します。値は 9100 をお勧めします。パス MTU は、LAN 自動化中、またはアンダーレイの構成時に、ファブリック内のすべてのデバイスに設定されることに注意してください。

ステップ 1 Cisco DNA Center で AAA サーバー設定を構成します。

- a) **[System] > [Settings] > [External Services] > [Authentication and Policy Servers]** ウィンドウで、デバイス認証用の AAA サーバーとして Cisco ISE を定義します。
詳細な手順については、『[Cisco DNA Center Administrator Guide](#)』の「Configure Authentication and Policy Servers」を参照してください。
- b) Cisco ISE サーバーをグローバルサイトに追加します。詳細については、[Cisco ISE またはその他の AAA サーバーの追加](#)を参照してください。

ステップ 2 (オプション) オンボーディング前にデバイスを認証するように Cisco DNA Center を構成します。

- a) メニューアイコン (☰) をクリックして、**[System] > [Settings] > [Device Settings] > [PnP Device Authorization]** の順に選択します。
- b) **[Device Authorization]** チェックボックスをオンにしてデバイスで許可を有効にします。
- c) **[Save]** をクリックします。

ステップ 3 PKI 証明書を管理するように Cisco DNA Center アプライアンスを構成します。

- a) メニューアイコン (☰) をクリックして、**[System] > [Settings] > [Trust & Privacy] > [PKI Certificates]** の順に選択します。
- b) **[PKI Certificates]** ウィンドウで、**[Use Cisco DNA Center]** をクリックします。
- c) **[CA Management]** タブで、**[Download CA Certificate]** をクリックします。
- d) Cisco ISE の信頼できる証明書ストアに証明書を追加します。詳細については、『[Cisco Identity Services Engine Administrator Guide](#)』を参照してください。<https://www.cisco.com/c/en/us/support/security/identity-services-engine/products-installation-and-configuration-guides-list.html>

外部証明書を使用する場合は、その証明書を Cisco ISE の信頼できる証明書ストアに追加します。

ステップ 4 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。

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 5 ファブリックサイトで **[Closed Authentication]** を有効にし、ブリッジプロトコルデータユニット (BPDU) ガードを無効にします。

デフォルトでは、**[Closed Authentication]** を選択すると、すべてのダウンリンクアクセスポートに BPDU ガード設定がプッシュされます。拡張ノードのようなりモートスイッチが接続されている場合、BPDU ガードはポートをエラーディセーブルモードにプッシュします。BPDU ガードを無効にするには、クローズド認証の設定時に、**[Enable BPDU Guard]** チェックボックスをオフにします。

詳細については、「[認証テンプレートの選択](#)」を参照してください。

ステップ6 エニーキャストゲートウェイの作成 (18 ページ) に記載されているように、拡張 IP アドレスプールを INFRA_VN に割り当てます。

[Create Anycast Gateways] ワークフローで、[Pool Type] として [Extended Node] を選択し、[Supplicant-Based Extended Node Onboarding] チェックボックスをオンにします。

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。

(注) 拡張 IP アドレスプールは、ファブリックエッジデバイスが Cisco IOS XE 17.7.1 以降で動作している場合にのみ正常に割り当てられます。Cisco DNA Center の以前のリリースからアップグレードした場合は、拡張 IP アドレスプールを構成する前に、サブリカントベースの拡張ノードの移行を完了する必要があります。

ステップ7 ファブリックエッジデバイスまたは FIAB に拡張ノードデバイスを接続します。

オンボーディングの前にデバイスを認証することを選択した場合 (ステップ 2)、電源をオンにした後、拡張ノードデバイスは [Pending Authorization] 状態になります。[Provision] > [Plug and Play] ウィンドウでデバイスのステータスを確認できます。

ステップ8 (オプション) デバイスを認証します。

この手順は、デバイスが [Pending Authorization] 状態の場合にのみ実行してください。

- a) メニューアイコン (☰) をクリックして、[Provision] > [Plug and Play]。
- b) [Plug and Play] ウィンドウで、サブリカントベースの拡張ノードデバイスを選択し、[Actions] > [Authorize] の順に選択します。

認証プロセスは、Cisco ISE で証明書ベースの EAP-TLS 認証を完了するために、サブリカントベースの拡張ノードデバイスをプロビジョニングします。認証後、Cisco ISE はサブリカントベースの拡張ノードデバイスに完全なアクセスを許可します。サブリカントベースの拡張ノードデバイスは、SD-Access ファブリックに完全にオンボードされます。

サブリカントベースの拡張ノードデバイスがファブリックにオンボードされた後は、ファブリック エッジサブリカント ポートへのアクセスは認証ステータスのみに基づきます。デバイスまたはポートがダウンすると、認証セッションがクリアされ、ポートでトラフィックが許可されなくなります。ポートが再び起動すると、IEEE 802.1x (Dot1x) 認証プロセスを経て、SD-Access ネットワークへのアクセスが回復します。

障害のあるポートの交換

オーセンティケータ (ファブリックエッジまたは FIAB) ポートとサブリカントポート間のリンクがダウンした場合、障害のあるポートを交換し、[Port Assignment] メニューから新しいポートを設定できます。

ステップ1 サブリカントポートを交換するには、次の手順に従います。

- a) 新しいサブリカントポートの設定をクリアします。
- b) 既存の設定を現在のサブリカントポートから新しいサブリカントポートにコピーして、802.1X 認証を可能にします。

ステップ 2 オーセンティケータポートを交換するには、次の手順に従います。

- a) サブリカントポートをオーセンティケータの新しいインターフェイスに割り当てます。ポートの割り当てについては、「[ファブリックサイト内のポートの設定](#)」を参照してください。[Connected Device Type] として [Supplicant-Based Extended Node] を選択します。
- b) オーセンティケータの古いインターフェイスの既存のポート割り当てをクリアします。

ステップ 3 オーセンティケータとサブリカントの古いポート間の物理接続を切断します。オーセンティケータとサブリカントの新しいポート間をケーブルで接続します。このリンクを確立します。

ステップ 4 オーセンティケータとサブリカントの新しいポート間のリンクが確立したら、次の手順を実行します。

- a) オーセンティケータとサブリカントの両方に対して **[Inventory] > [Resync Device]** を実行して、Cisco DNA Center のデバイス情報を再同期します。「[デバイス情報の再同期](#)」を参照してください。
- b) 新しいサブリカントポートをオーセンティケータに割り当てます。ポートの割り当てについては、「[ファブリックサイト内のポートの設定](#)」を参照してください。[Connected Device Type] として [Authenticator Switch] を選択します。
- c) 古いサブリカントポートのポート割り当てをクリアします。

サブリカントベースの拡張ノードをオンボードするための Cisco Identity Services Engine の設定

このタスクでは、Cisco Identity Services Engine (ISE) でサブリカントベースの拡張ノード (SBEN) デバイスをプロファイリングする方法について説明します。以下にリストされている手順は、Cisco ISE 設定手順の一部です。詳細については、『[Cisco Identity Services Engine Administrator Guide](#)』を参照してください。

始める前に

Cisco DNA Center から CA 証明書をダウンロードします。

ステップ 1 CA 証明書を Cisco ISE にインポートします。

Cisco ISE ホームページから、**[Administration] > [System] > [Certificates] > [System Certificate] > [Import]** を選択します。[Import] ウィンドウで、[Trust for client authentication and Syslog] 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。詳細については、『[Cisco Identity Services Engine Administrator Guide](#)』の「Import the Root Certificates to the Trusted Certificate Store」セクションを参照してください。

ステップ 2 RADIUS 属性を使用して、次の認証プロファイルを設定します。

Cisco ISE メインメニューから、**[Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles]** を選択します。

次のプロファイルを構成します。

SBEN-DHCP:

Access Type = ACCESS_ACCEPT
Filter-ID = **SBEN_DHCP_ACL.in**

SBEN_LIMITED_ACCESS_AUTHZ:

Access Type = ACCESS_ACCEPT
Filter-ID = **SBEN_MAB_ACL.in**
cisco-av-pair = interface-template-name=**SWITCH_SBEN_MAB_TEMPLATE**

SBEN_FULL_ACCESS_AUTHZ :

Access Type = ACCESS_ACCEPT
cisco-av-pair = interface-template-name=**SWITCH_SBEN_FULL_ACCESS_TEMPLATE**

ステップ 3 [Profiling Policies] ウィンドウでデバイス プロファイリング ポリシーを定義します。

- a) Cisco ISE のメインメニューから、**[Policy] > [Profiling] > [Profiling Policies]**を選択します。
- b) [Profiling Policies] ウィンドウで、[Cisco-Device] : [Cisco-Switch] ポリシーの新しい [DHCP-v-i-vendor-class] 条件を追加します。

サブリカントベースの拡張ノードをオンボードするための Cisco Identity Services Engine の設定

* Name Description

Policy Enabled

* Minimum Certainty Factor (Valid Range 1 to 65535)

* Exception Action

* Network Scan (NMAP) Action

Create an Identity Group for the policy Yes, create matching Identity Group
 No, use existing Identity Group hierarchy

Parent Policy

* Associated CoA Type

System Type

Rules

If	Condition	<input type="text" value="Cisco-IOS-NMAPOSCheck"/>	Then	<input type="text" value="Certainty Factor Increases"/>	<input type="text" value="10"/>	<input type="text"/>
If	Condition	<input type="text" value="CDP_cdpCachePlatform_CONTAINS_9200..."/>	Then	<input type="text" value="Certainty Factor Increases"/>	<input type="text" value="20"/>	<input type="text"/>
If	Condition	<input type="text" value="DHCP_v-i-vendor-class_CONTAINS_9200..."/>	Then	<input type="text" value="Certainty Factor Increases"/>	<input type="text" value="20"/>	<input type="text"/>
If	Condition	<input type="text"/>	OR	<input type="text"/>	<input type="text"/>	<input type="text"/>
If	Condition	<input type="text"/>	<input type="text" value="DHCP:v-i-ven..."/>	<input type="text" value="CONTAIN"/>	<input type="text" value="9200"/>	<input type="text"/>
If	Condition	<input type="text"/>	<input type="text" value="DHCP:v-i-ven..."/>	<input type="text" value="CONTAIN"/>	<input type="text" value="9300"/>	OR
If	Condition	<input type="text"/>	<input type="text" value="DHCP:v-i-ven..."/>	<input type="text" value="CONTAIN"/>	<input type="text" value="9500"/>	OR

- c) サブリカントデバイスの新しい子ポリシーを [Cisco-Switch] の下に作成し、[CdpCachePlatform] および [V-I-Vendor-Class] 条件を適用します。

子ポリシーの [Minimum Certainty Factor] の値が親ポリシーの値よりも高いことを確認してください。

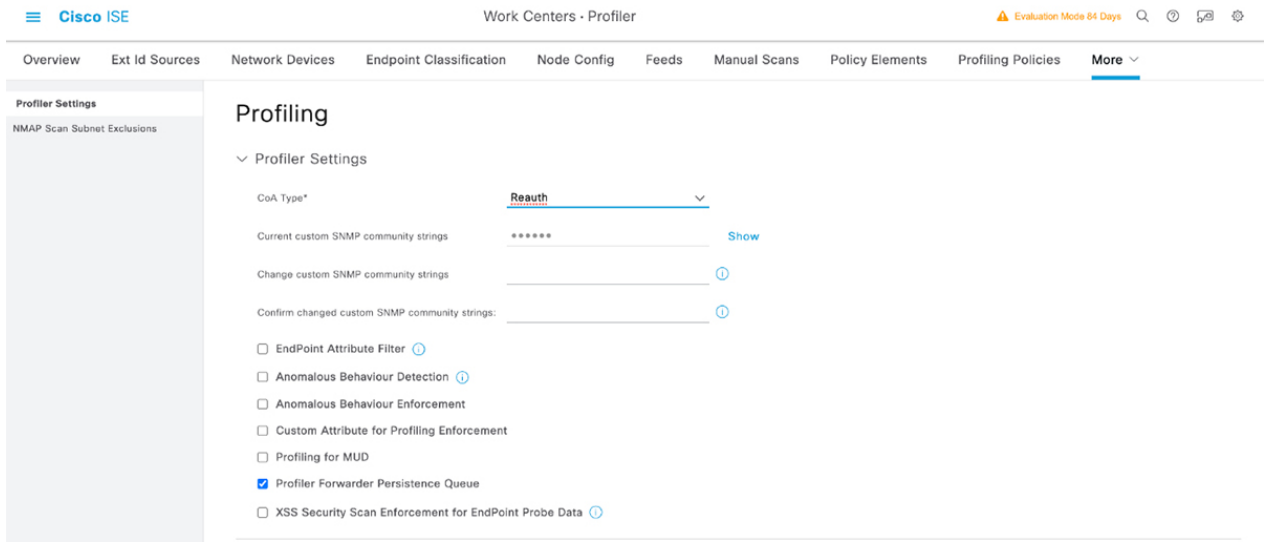
* Name	CAT9K_EN	Description	<input type="text"/>
Policy Enabled	<input checked="" type="checkbox"/>		
* Minimum Certainty Factor	30	(Valid Range 1 to 65535)	
* Exception Action	NONE	▼	
* Network Scan (NMAP) Action	NONE	▼	
Create an Identity Group for the policy	<input checked="" type="radio"/> Yes, create matching Identity Group <input type="radio"/> No, use existing Identity Group hierarchy		
* Parent Policy	Cisco-Switch	▼	
* Associated CoA Type	Global Settings	▼	
System Type	Administrator Created		
Rules			
If Condition	CDP_odpCachePlatform_CONTAINS_C92...	▼	Then Certainty Factor Increases ▼ 30
If Condition	DHCP_v-i-vendor-class_CONTAINS_C920...	▼	Then Certainty Factor Increases ▼ 30

ステップ 4 グローバル認可変更 (CoA) タイプを [Reauth] に設定します。

[CoA Type] を設定するには、Cisco ISE ホームページから、[Work Centers] > [Profiler] > [Settings]の順に移動します。

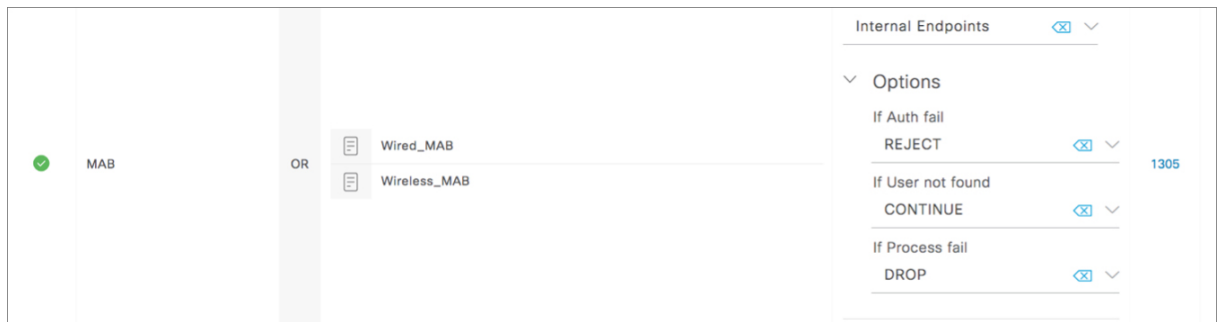
[CoA Type] ドロップダウンリストから [Reauth] を選択します。

サブリカントベースの拡張ノードをオンボードするための Cisco Identity Services Engine の設定

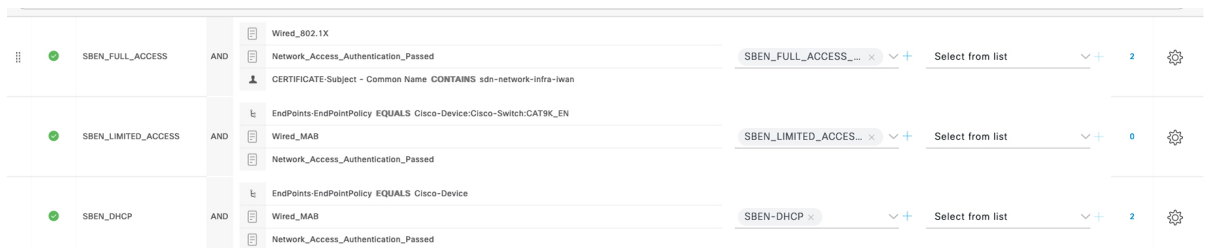


ステップ 5 [Authorization Policy] ウィンドウで認証ポリシーを定義します。

- Cisco ISE ホームページから、[Policy] > [Policy Sets] > [Default] > [Authorization Policy]を選択します。
- デフォルト MAB ポリシーの [If User not found] フィールドが [CONTINUE] オプションに設定されていることを確認します。



- [Authorization Policy] ウィンドウで、サブリカントデバイスの認証ポリシーを構成し、ポリシーを以前に作成した認証プロファイル (SBEN-DHCP、SBEN_LIMITED_ACCESS_AUTHZ、SBEN_FULL_ACCESS_AUTHZ) に関連付けます。



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 [Closed Authentication] の場合にのみ、次の手順を実行します。



(注) 他の認証モードでは、次の手順は自動化されています。

- ステップ1 メニューアイコン (☰) をクリックして、**[Provision] > [Fabric Sites]**。
- ステップ2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。
- ステップ3 ファブリックサイトを選択します。
- ステップ4 [Fabric Infrastructure] タブで、ファブリックエッジノードをクリックします。
- ステップ5 スライドインペインの [Port Channel] タブで、**[Create Port Channel]** をクリックします。
- ステップ6 [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7 新しいポートチャネルの説明を [Description] に入力します。
- ステップ8 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9 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 10 [Done] をクリックします。

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 メニューアイコン (☰) をクリックして、[Provision] > [Fabric Sites]。

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 ファブリックサイトを選択します。

ステップ 4 [Fabric Infrastructure] タブで、ファブリックエッジノードをクリックします。

ステップ 5 スライドインペインで、[Port Channel] タブをクリックします。

ステップ 6 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クリックします。

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 7 ポートチャネルを更新します。

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 8 [Done] をクリックします。

ポートチャネルの削除

ステップ 1 メニューアイコン (☰) をクリックして、[Provision] > [Fabric Sites]。

ステップ 2 [SUMMARY] で、ファブリックサイトの数を示す数字をクリックします。

ステップ 3 ファブリックサイトを選択します。

ステップ 4 [Fabric Infrastructure] タブで、ファブリックエッジノードをクリックします。

ステップ 5 スライドインペインで、[Port Channel] タブをクリックします。

[Port Channel] ビューには、既存のポートチャネルがすべて一覧表示されます。

ステップ6 ポートチャネルのチェックボックスをオンにして、[Delete] をクリックします。

ステップ7 プロンプトで [Yes] をクリックします。

マルチキャスト

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) 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にのみ展開されます。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ノード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 メニューアイコン (☰) をクリックして、[Workflows] > [Configure Multicast] の順に選択します。

ステップ2 タスクの概要ウィンドウが表示されたら、[Let's Do It] をクリックして、ワークフローに直接移動します。

ステップ3 [Select a site to enable multicast] ウィンドウで、ドロップダウンリストから [Site] を選択します。

ステップ4 [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を次の中から選択します。

- **Native Multicast**
- **Head-end replication**

- ステップ 5** [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。
- (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 6** [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。
- ステップ 7** [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 8** 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。
- b) [ASM] の選択時に、RP のタイプ (内部または外部) を選択します。
- ステップ 9** 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。
- 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。
- ステップ 10** 設定を送信する前に、[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。
-

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。