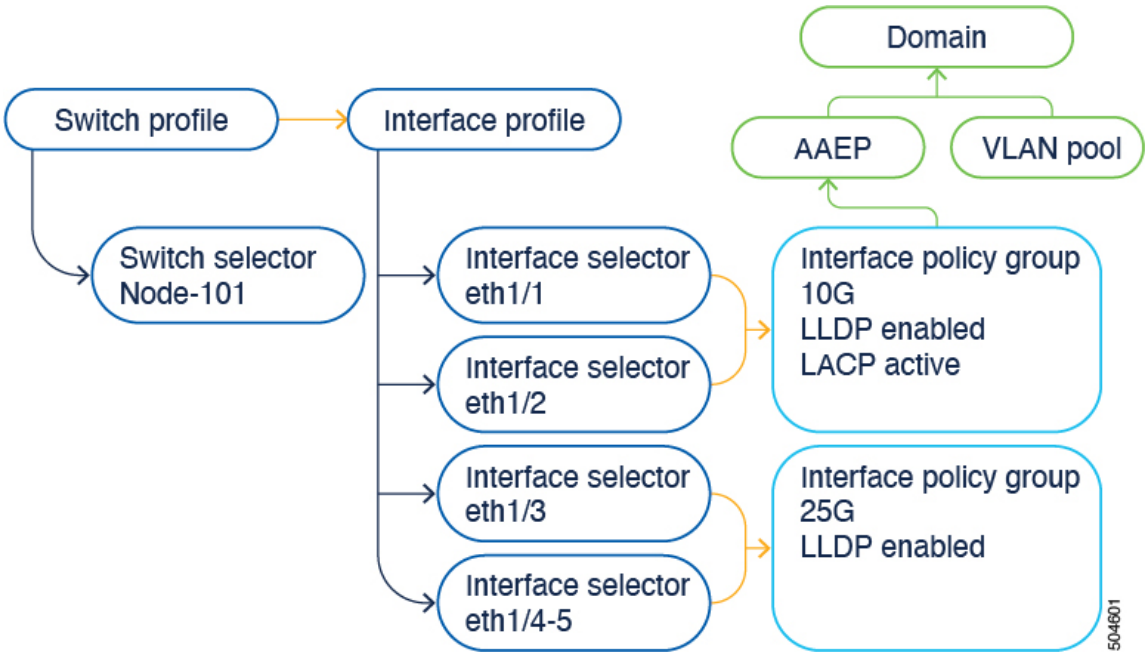
アクセス インターフェイス

- アクセス インターフェイスについて （1 ページ）
- 物理ポートの構成 （4 ページ）
- ポート チャネル （13 ページ）
- Cisco ACI の仮想ポート チャネル （32 ページ）
- リフレクティブ リレー (802.1Qbg) （48 ページ）
- FEX デバイスへのポート、PC、および vPC 接続の設定 （51 ページ）
- ポート プロファイルの設定 （57 ページ）
- インターフェイス構成の編集 （73 ページ）

アクセス インターフェイスについて

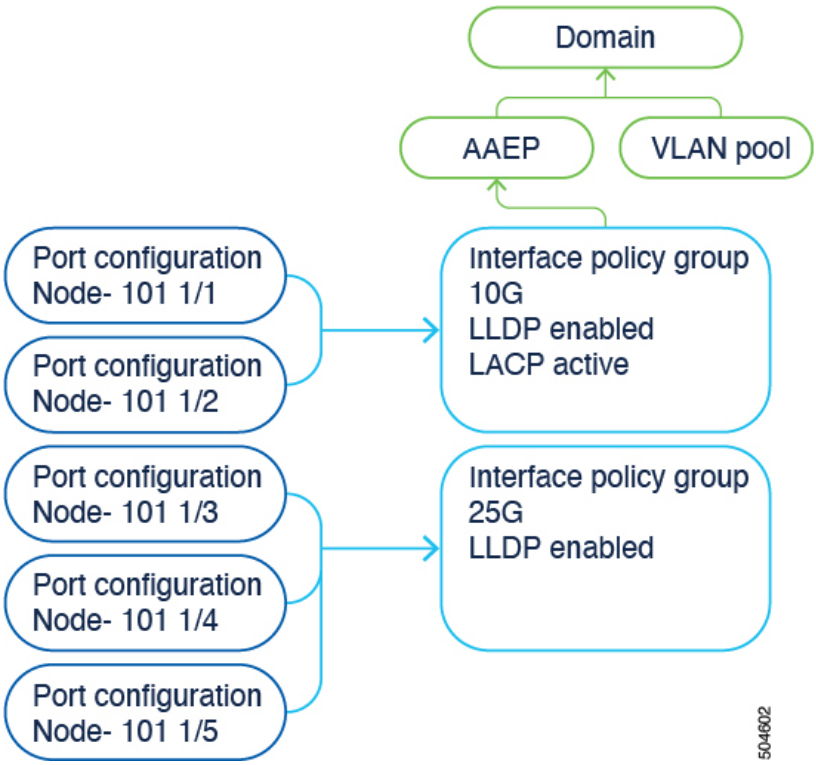
Cisco Application Centric Infrastructure（ACI）では、インターフェイス ポリシー グループ（インターフェイス速度やリンク層検出プロトコル（LLDP）などのインターフェイス ポリシーのグループ）をスイッチ ノード上のインターフェイスに関連付けることによって、インターフェイス構成を実行します。Cisco ACI は、4 つのオブジェクト（スイッチ プロファイル、スイッチ セレクタ、インターフェイス プロファイル、およびインターフェイス セレクタ）を使用して、特定のスイッチ ノード上の特定のインターフェイスを選択します。本書では、この動作モードを「プロファイルとセレクタの構成」と呼びます。次の図で、この構成について説明します：

図 *1:* プロファイルとセレクタに基づくインターフェイス構成



Cisco ACI 6.0（1）リリースでは、インターフェイス構成を簡素化する「ポート単位の構成」構成オプション（「インターフェイス構成」または `infraPortConfig` とも呼ばれます。後者がこの構成のオブジェクト名です）が追加されています。このオプションは、4 つのオブジェクトを 1 つのオブジェクトとして表示し、このオブジェクトでスイッチノード上のインターフェイスを指定します。その結果、スイッチ プロファイル、スイッチ セレクタ、インターフェイス プロファイル、およびインターフェイスセレクタを個別に使用したり、維持したりする必要はありません。

図 *2 :* ポート単位の構成



Cisco Application Policy Infrastructure Controller（APIC）GUI で次の方法でポート単位の設定にアクセスできます。

- **[ファブリック（Fablic）] > [アクセスポリシー（Access Policies）] > [インターフェイスの構成（Interfaces Configuration）]**
- **[ファブリック（Fablic）] > [アクセスポリシー（Access Policies）] > [クイック スタート（Quick Start）] > [インターフェイスの構成（Interfaces Configuration）]**
- **[ファブリック（Fabric）] > [インベントリ（Inventory）] >** ***[pod_ID]*** **>** ***[switch_name]*** **> [インターフェイス（Interface）]タブ > [インターフェイスの構成（Configure Interfaces）]**

Cisco APIC GUI の以前と同じ場所で、スイッチプロファイルとセレクタ、およびインターフェイス プロファイルとセレクタを使用してスイッチを構成できます：

- **[ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）] > [スイッチ（Switches）] > [リーフ スイッチ（Leaf Switches）] > [プロファイル（Profiles）]**
- **[ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）] > [スイッチ（Switches）] > [スパイン スイッチ（Spine Switches）] > [プロファイル（Profiles）]**
- **[ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）] > [インターフェイス（Interfaces）]> [リーフ インターフェイス（Leaf Interfaces）]> [プロファイル（Profiles）]**
- **[ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）] > [インターフェイス（Interfaces）] > [スパイン インターフェイス（Spine Interfaces）] > [プロファイル（Profiles）]**

ただし、ポート単位の構成を使用することを推奨します。

インターフェイス構成オプションを使用する場合、Cisco APIC は、できるだけ少ない読み取り専用のオブジェクトで済ませられるような方法で、スイッチプロファイルとセレクタ、およびインターフェイスプロファイルとセレクタを作成して維持します。たとえば、2 つの連続するポートを同じように構成すると、Cisco APIC は構成内に範囲を自動的に作成します。ポートは個別に構成するため、これらの最適化について心配する必要はありません。Cisco APIC が適切に処理します。Cisco APIC が自動的に作成するこれらのオブジェクトは「システム生成プロファイル」と呼ばれます。ユーザーが管理する必要はありません。

システムによって生成されたプロファイルは、GUI の**[ファブリック（Fabric）]** > **[アクセス ポリシー（Access Policies）]** > **[インターフェイス（Interfaces）]** > **[{リーフ | スパイン} {スイッチ | インターフェイス}（{Leaf | Spine} {Switches | Interfaces}）]** > **[Profiles（プロファイル）]**の下に、ユーザー定義プロファイルとともに表示されます。

インターフェイス構成オプションを使用してインターフェイスを構成するとき、以前にプロファイルとセレクタを使用してインターフェイスを設定していた場合には、 Cisco APIC は既存のプロファイルからインターフェイスを自動的に削除し、インターフェイスをシステム生成プロファイルにシームレスに移動します。既存のスイッチおよびインターフェイスプロファイルに他のインターフェイスが含まれている場合、Cisco APIC はそれらを削除しません。従来の方法でそれらを使用し続けることができます。既存のプロファイルにインターフェイスが含まれていない場合、Cisco APIC は不要になったプロファイルを自動的に削除します。

マルチノードセレクタを使用してインターフェイスをすでに構成していた場合、つまり、複数のリーフ スイッチを持つプロファイルにポートセレクタを割り当てていた場合は、Cisco APIC のマルチノードセレクタに属する各ノードに同じインターフェイスを同時に構成して、それらのノードを既存のプロファイルから自動的に削除する必要があります。そうしないと、検証の失敗によって移行がブロックされます。

物理ポートの構成

Cisco Application Centric Infrastructure（ACI）リーフ スイッチ インターフェイスを構成するには、複数の方法があります：

- セレクタとプロファイルベースの構成モデルを使用します。**[ファブリック（Fabric）]** > **[アクセス ポリシー（Access Policies）]** > **[スイッチ（Switches）]** > **[リーフ スイッチ（Leaf Switches）]** > **[プロファイル（Profiles）]**から、リーフ ノードを選択するためのリーフ セレクタおよび関連付けられたインターフェイス プロファイルを構成できます。これにより、インターフェイス プロファイル（**[ファブリック（Fabric）]** > **[アクセス ポリシー（Access Policies）]** > **[インターフェイス（Interfaces）]** > **[リーフ インターフェイス（Leaf Interfaces）]** > **[プロファイル（Profiles）]**）を選択します。そしてこれは、1 つ以上のインターフェイスを選択して、インターフェイス ポリシー グループに関連付けます。

- Cisco Application Policy Infrastructure Controller（APIC）5.2(7) リリース以降のインターフェイス構成を使用して行います。**[ファブリック（Fablic）]** > **[アクセスポリシー（Access Policies）]** > **[インターフェイスの構成（Interfaces Configuration）]** に移動します。この構

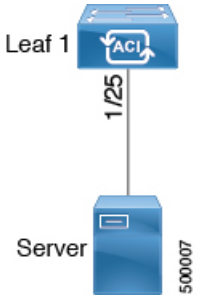
成オプションは、構成手順の数を 4 回から 1 回に減らすことで、構成ワークフローを簡素化します。

- **[ファブリック（Fabric）] > [インベントリ（Inventory）] > *[pod_ID]* > *[switch_name]***からのインベントリ ビューを用いて行います。Cisco APIC 5.2(7) リリース以降、インベントリ ビューの構成でもインターフェイスの構成を使用します。
- **[ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）] > [クイック スタート（Quick Start）]**ウィザードを用いて行います。Cisco APIC 5.2(7) リリース以降、インベントリ ビューの構成でもインターフェイスの構成を使用します。

リリース 5.2(7) 以降の GUI を使用したインターフェイス設定モデルを使用したリーフ スイッチ物理ポートの設定

リリース 5.2(7) 以降において、**[ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）] > [クイック スタート（Quick Start）] > [インターフェイスの構成（Configure Interfaces）]**または**[ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）] > [インターフェイスの構成（Interface Configuration）]**ページのいずれかで、サーバーを、ポートチャネルを持つCisco Application Centric Infrastructure（ACI）リーフ スイッチ インターフェイスに接続します。手順は、Cisco ACI リーフ スイッチ インターフェイスに他の種類のデバイスを接続する場合と同じになります。

図 *3*: ベア メタル サーバのスイッチ インターフェイス設定



始める前に

- Cisco ACI ファブリックが設置され、Cisco Application Policy Infrastructure Controller（APIC）がオンラインになっており、Cisco APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ構成を作成できる Cisco APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチが Cisco ACI ファブリックに登録され、使用可能であること。

手順

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）]** > **[アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 **ナビゲーション** ペインで **[クイック スタート（Quick Start）] [インターフェイスの構成（Interface Configuration）]** を選択します。

ステップ 3 **作業**ペインで、[クイックスタート（Quick Start）] ウィザードの **[インターフェイスの構成（Configure Interfaces）]** をクリックし、**[インターフェイスの構成（Configure Interfaces）]** をクリックするか、または **[インターフェイス構成（Interface Configuration ）]** の **作業**ペインで、**[アクション（Actions）]** > **[インターフェイスの構成（Configure Interfaces）]**をクリックします。

ステップ 4 **[インターフェイスの設定（Configure Interfaces）]** ダイアログで、以下のアクションを実行します。

a) **[ノード タイプ（Node Type）]** で、**[リーフ（Leaf）]** をクリックします。

b) **[ポート タイプ（Port Type）]** で、**[アクセス（Access）]** をクリックします。

c) **[インターフェイス タイプ（Interface Type）]** で、目的のタイプを選択します。

d) **[インターフェイス集約タイプ（Interface Aggregation Type）]** で、**[個別（Individual）]** を選択します。

e) **[ノード（Node）]**で、**[ノードの選択（Select Node）]** をクリックし、目的のスイッチ（ノード）のボックスにチェックを入れ、**[OK]** をクリックします。複数のスイッチを選択できます。

f) **[すべてのスイッチのインターフェイス（Interfaces For All Switches）]** で、目的のインターフェイスの範囲を入力します。

g) **[リーフ アクセス ポート ポリシー グループ（Leaf Access Port Policy Group）]** の場合は、**[リーフ アクセス ポート ポリシー グループの選択（Select Leaf Access Port Policy Group）]** をクリックします。

h) **[リーフ アクセス ポート ポリシー グループの選択（Select Leaf Access Port Policy Group）]** ダイアログで、**[リーフ アクセス ポート ポリシー グループの作成（Create Leaf Access Port Policy Group）]** をクリックします。

   インターフェイス ポリシー グループは、選択したスイッチのインターフェイスに適用するインターフェイス ポリシーのグループを指定する名前付きポリシーです。インターフェイス ポリシーの例は、リンクレベルのポリシー（たとえば、1 gbit のポート速度）、ストーム制御インターフェイス ポリシーなどです。

i) **[リーフ アクセス ポート ポリシー グループの作成（Create Leaf Access Port Policy Group）]** ダイアログで、目的のポリシーを選択または作成します。

j) [保存（Save）] をクリックします。

次のタスク

これで、基本リーフ スイッチ インターフェイスの設定手順は完了しました。

（注） この設定はハードウェア接続を有効にしますが、このハードウェア設定に関連付けられた有効なアプリケーション プロファイル、EPG、およびコントラクトがないと、データ トラフィックはフローできません。

セレクタおよびプロファイルからのインターフェイスから GUI を使用したインターフェイス構成への移行

この手順を使用して、既存のインターフェイスの構成を、セレクタベースおよびプロファイルベースのモデルから、インターフェイス構成モデルに変換できます。

（注） Cisco Application Policy Infrastructure Controller（APIC）は、アクティブなポリシー グループ オーバーライドの設定されたインターフェイスを自動的に移行しません。これらのポートは手動で移行する必要があります。

手順

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）]** > **[アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 **ナビゲーション** ペインで **[インターフェイスの設定（Interface Configuration）]** を選択します。

ステップ 3 テーブルで、移行するインターフェイスを選択し、右側にある 3 つのドットをクリックします。

ステップ 4 ポップアップ メニューで、**[インターフェイス構成の編集（Edit Interface Configuration）]** を選択します。

次のメッセージが表示されます。

このインターフェイスは、インターフェイス セレクタを使用して構成されています。インターフェイスを構成する新しい方法に移行することをお勧めします。［保存（Save）］ をクリックすると、このインターフェイスは移行されます。

ステップ 5 [保存（Save）] をクリックします。

Cisco APIC は、インターフェイスを新しい構成モデルに変換します。

ステップ 6 Cisco APIC のリリースと目的に応じて、次のサブステップのセットのいずれかを実行します。

単一のインターフェイスを移行するには、次の手順を実行します。

a) テーブルで、移行するインターフェイスを選択し、右側にある 3 つのドットをクリックします。

b) ポップアップ メニューで、**[インターフェイス構成の編集（Edit Interface Configuration）]** を選択します。

次のメッセージが表示されます。

このインターフェイスは、インターフェイス セレクタを使用して構成されています。インターフェイスを構成する新しい方法に移行することをお勧めします。[保存（Save）] をクリックすると、このインターフェイスは移行されます。

c) [保存（Save）] をクリックします。

Cisco APIC は、インターフェイスを新しい構成モデルに変換します。

6.0(2) 以降のリリースでは、 は、セレクタベースおよびプロファイルベースのモデルに基づく既存の設定をインターフェイス設定モデルに移行するタスクを簡素化します。Cisco APIC複数のノードを選択することで、ノードのすべてのポートのセレクタベースの構成を移行できます。この機能は、セレクタが複数のノードにまたがる場合に役立ちます。複数のインターフェイスを移行するには、次の手順を実行します。

a) テーブルで、移行するインターフェイスを選択します。
b) **[アクション（Actions）]** > **[インターフェイスの構成（Configure Interfaces）]**をクリックします。

次のメッセージが表示されます。

このインターフェイスは、インターフェイス セレクタを使用して構成されています。インターフェイスを構成する新しい方法に移行することをお勧めします。[保存（Save）] をクリックすると、このインターフェイスは移行されます。

c) [保存（Save）] をクリックします。

Cisco APIC は、インターフェイスを新しい構成モデルに変換します。

GUI を使用したインターフェイス構成の変更

インターフェイスの構成は、次のように変更できます。

手順

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）]** > **[アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 **ナビゲーション** ペインで **[インターフェイスの設定（Interface Configuration）]** を選択します。

ステップ 3 テーブルで、移行するインターフェイスを選択し、右側にある 3 つのドットをクリックします。

ステップ 4 ポップアップ メニューで、**[インターフェイス構成の編集（Edit Interface Configuration）]** を選択します。

このインターフェイスに関連付けられているポリシー グループを示すウィンドウが表示されます。

ステップ 5 既存のポリシー グループがある場合は、グループの横にある **x** をクリックして削除できます。

ステップ 6 **[リーフ アクセス ポート ポリシー グループの選択（Select Leaf Access Port Policy Group）]** をクリックして、新しいポリシー グループを割り当てます。

ステップ 7 既存のポリシー グループを選択するか、**[リーフ アクセス ポート ポリシー グループの作成（Create Leaf Access Port Policy Group）]** をクリックして新しいポリシー グループを作成します。

ステップ 8 [保存（Save）] をクリックします。

GUI を使用したインターフェイス構成の表示

Cisco Application Policy Infrastructure Controller（APIC）GUI は、インターフェイスがセレクタとプロファイルモデルを使用して構成されているか、インターフェイス構成モデルを使用して構成されているかに関係なく、インターフェイス構成の統合ビューを表示します。

[ファブリック（Fabric）] > **[アクセス ポリシー（Access Policies）]** > **[インターフェイス構成（Interface Configuration）]**を選択し、右側のテーブルに移動して、すべてのリーフ ノードとインターフェイスを表示します。

リーフ ノードをクリックすると、管理状態、TEP の IP アドレス、ID 番号、ハードウェア モデル、シリアル番号、ソフトウェア バージョンなどのリーフ ノードの情報が表示されます。

インターフェイスをクリックすると、インターフェイスの情報が表示されます。このビューは「インフラ ポート サマリー」と呼ばれます。右上の中央のアイコンをクリックすると、インターフェイスの情報が全画面表示されます。全画面表示には、**[概要（Overview）]**、**[操作（Operational）]**、**[展開済み EPG（Deployed EPGs）]**、**[VLAN（VLANs）]**、**[統計（Statistics）]**、**[QoS 統計（QoS stats）]**、および **[イベント分析（Event Analytics）]** という追加情報を表示するタブが含まれています。この全画面表示を閉じるには、右上の **[x]** をクリックします。

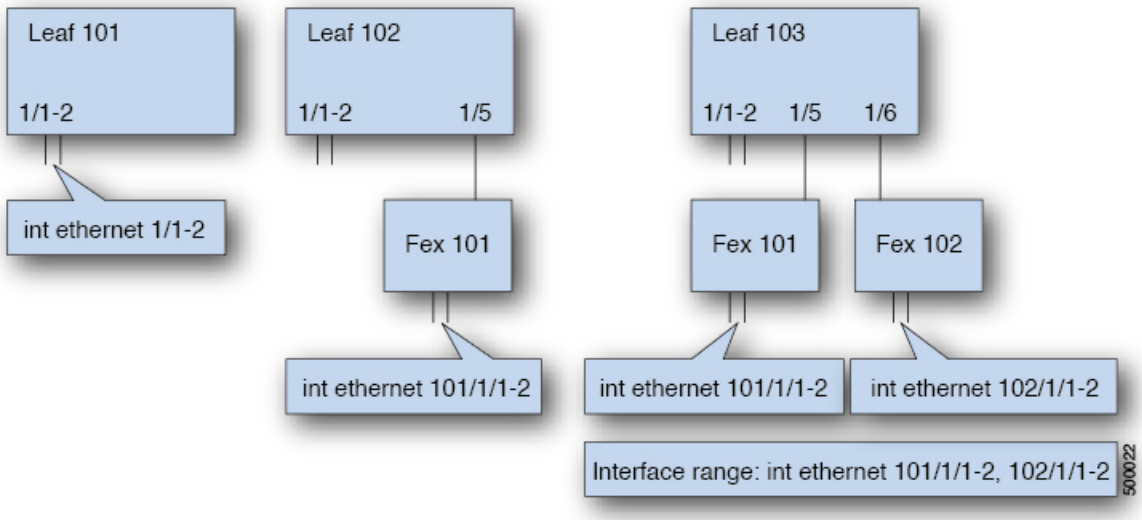
特定のインターフェイスのポリシー グループ名をクリックすると、802.1X 構成、アタッチ可能なエンティティ プロファイル、CDP 構成、LLDP 構成などのポリシー グループに関する情報が表示されます。

NX-OS CLI を使用したリーフ ノードおよび FEX デバイス上の物理ポートの設定

次の例のコマンドは、REST API/SDK および GUI と完全な互換性がある Cisco Application Centric Infrastructure（ACI）ポリシー モデルで、多数の管理対象オブジェクトを作成します。いずれにせよ、CLI ユーザーは Cisco ACI モデル内部ではなく、意図したネットワーク設定に注力できます。

図 4 : Cisco ACI のリーフ ノード ポートと FEX ポートの例 （10 ページ） に、リーフ ノードに直接接続されたイーサネット ポート、またはリーフ ノードに接続された FEX モジュールの例と、CLI でそれぞれがどのように表示されるのかを示します。FEX ポートでは、*fex-id* はポート自体の名前に **ethernet 101/1/1** として含まれます。インターフェイス範囲を記述する際は、**ethernet** キーワードを NX-OS で繰り返す必要はありません。例：**interface ethernet 101/1/1-2, 102/1/1-2**。

図 *4 : Cisco ACI* のリーフ ノード ポートと *FEX* ポートの例



- リーフ ノードの ID 番号はグローバルです。
- *fex-id* 番号は各リーフ ノードでローカルです。
- キーワード **ethernet** の後のスペースに注意してください。

手順

ステップ 1 **configure**

グローバル コンフィギュレーション モードを開始します。

例：

```
apic1# configure
```

ステップ 2 **leaf** *node-id*

構成するリーフ ノードを指定します。*node-id* には、設定の適用対象となる単一のノード ID、または ID の範囲を *node-id1–node-id2* という形式で指定できます。

例：

```
apic1(config)# leaf 102
```

ステップ 3 **interface** *type*

設定するインターフェイスを指定します。インターフェイス タイプと ID を指定できます。イーサネット ポートの場合は、「ethernet slot / port」を使用します。

例：

```
apic1(config-leaf)# interface ethernet 1/2
```

ステップ 4 （任意） **fex associate** *node-id*

設定するインターフェイスが FEX インターフェイスの場合、このコマンドを使用して、設定前に FEX モジュールをリーフ ノードに接続する必要があります。

（注）
この手順は、FEX ポートを使用してポートチャネルを作成する前に行う必要があります。

例：

```
apic1(config-leaf-if)# fex associate 101
```

ステップ 5 **speed** *speed*

ここでの速度設定は一例です。ここでは、以下の表に示す任意のインターフェイス設定を設定できます。

例：

```
apic1(config-leaf-if)# speed 10G
```

次の表に、この時点で構成できるインターフェイス設定を示します。

コマンド	目的
[no] shut	物理インターフェイスをシャットダウンします
[no] speed *speedValue*	物理インターフェイスの速度を設定します
[no] link debounce time *time*	リンク でバウンスを設定します
[no] negotiate auto	ネゴシエートを設定します
[no] cdp enable	Cisco Discovery Protocol（CDP）を無効または有効にします
[no] mcp enable	Mis-Cabling Protocol（MCP）を無効または有効にします
[no] lldp transmit	物理インターフェイスの送信を設定します
[no] lldp receive	物理インターフェイスの LLDP 受信を設定します

コマンド	目的
spanning-tree {bpduguard | bpdufilter} {enable | disable}	スパニング ツリー BPDU を設定します
[no] storm-control level *percentage* [burst-rate *percentage*]	ストーム制御（パーセント）を設定します
[no] storm-control pps *packets-per-second* burst-rate *packets-per-second*	ストーム制御（秒当たりのパケット）を設定します

例

リーフ ノードに 1 つのポートを設定します。次に、プロパティ speed、cdp、および admin state についてリーフ 101 のインターフェイス eth1/2 を設定する例を示します。

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/2
apic1(config-leaf-if)# speed 10G
apic1(config-leaf-if)# cdp enable
apic1(config-leaf-if)# no shut
```

複数のリーフ ノードの複数のポートを設定します。次に、リーフ ノード 101 ～ 103 のそれぞれのインターフェイス eth1/1-10 での速度設定の例を示します。

```
apic1(config)# leaf 101-103
apic1(config-leaf)# interface eth 1/1-10
apic1(config-leaf-if)# speed 10G
```

リーフ ノードに FEX を接続します。次に、リーフ ノードに FEX モジュールを接続する例を示します。NX-OS とは異なり、リーフ ノード ポート Eth1/5 は暗黙的にファブリック ポートとして構成され、FEX ファブリック ポートチャネルは FEX アップリンク ポートで内部的に作成されます。Cisco ACI では、FEX ファブリック ポートチャネルはデフォルト構成を使用します。ユーザー構成は使用できません。

（注） 次の例に示すように、この手順はFEXポートを使用してポートチャネルを作成する前に行う必要があります。

```
apic1(config)# leaf 102
apic1(config-leaf)# interface eth 1/5
apic1(config-leaf-if)# fex associate 101
```

リーフ ノードに接続した FEX ポートを設定します。次に、リーフ ノード 102 ～ 103 のそれぞれに接続した FEX モジュール 101 のインターフェイス eth1/1-10 での速度設定の例を示します。FEX ID 101 はポート ID に含まれています。FEX ID は 101 から始まり、リーフ ノードに対してローカルです。

```
apic1(config)# leaf 102-103
apic1(config-leaf)# interface eth 101/1/1-10
apic1(config-leaf-if)# speed 1G
```

ポート チャネル

PC ホスト ロード バランシング アルゴリズム

次の表に、Cisco Application Centric Infrastructure（ACI）リーフ ノード ダウンリンクにわたるポートチャネル ロード バランシングで使用されるデフォルトのハッシュアルゴリズムと対称ハッシュ アルゴリズム オプションを示します。対称ハッシュ アルゴリズム オプションは、Cisco Application Policy Infrastructure Controller（APIC）リリース 2.3(1e) で導入されました。

表 *1 : PC* ホスト ロード バランシング アルゴリズム

Traffic Type	データ ポイントのハッシュ
エンド ホスト PC（デフォルト）	**レイヤ 2 トラフィック用**： • 送信元 MAC アドレス • 宛先 MAC アドレス • セグメント ID（VXLAN VNID）または VLAN ID **IP トラフィックの場合**： • 送信元 MAC アドレス • 宛先 MAC アドレス • 送信元 IP アドレス • 宛先 IP アドレス • プロトコル タイプ • 送信元レイヤ 4 ポート • 宛先レイヤ 4 ポート • セグメント ID（VXLAN VNID）または VLAN ID
PC 対称ハッシュ（構成可能）	**オプションを選択する**： • 送信元 IP アドレス • 宛先 IP アドレス • 送信元レイヤ 4 ポート • 宛先レイヤ 4 ポート

Po1 や Po2 などのリーフ スイッチに複数のポート チャネルがある場合、次のシナリオがサポートされます。

- Po1：SIP のみで対称ハッシュを有効にします。
- Po2：対称ハッシュを有効にしません。デフォルトのハッシュを使用します。

ただし、次のシナリオは、2 番目のポート チャネル Po2 のハッシュ パラメータが異なることになるため、サポートされません。

- Po1：SIP のみで対称ハッシュを有効にします。
- Po2：DIP のみで対称ハッシュを有効にします。

つまり、単一のリーフ スイッチでは、対称ハッシュを必要とするすべてのポートチャネルが同じハッシュ ポリシー/パラメータを使用するか、デフォルトのハッシュを使用する必要があります。

対称ハッシュは、次のスイッチではサポートされていません。

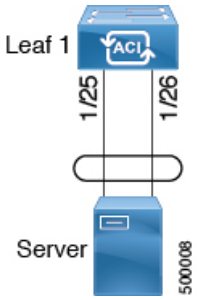
- Cisco Nexus 93128TX
- Cisco Nexus 9372PX
- Cisco Nexus 9372PX-E
- Cisco Nexus 9372TX
- Cisco Nexus 9372TX-E
- Cisco Nexus 9396PX
- Cisco Nexus 9396TX

（注） ポート チャネル ハッシュ アルゴリズムは、個々のリーフ ノードに個別に適用されます。アルゴリズムは、vPC ペアのリーフ ノードへのロード バランシングなど、ファブリック内のロード バランシングには影響しません。したがって、対称ハッシュは vPC ではサポートされません。

GUI を使用した ACI リーフ スイッチのポート チャネルの構成

この手順では、**[ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）] > [クイック スタート（Quick Start）] > [インターフェイスの構成（Interface Configuration）]**または**[ファブリック（Fabric）] > [アクセス ポリシー（Access Policies）] > [インターフェイス構成（Interface Configuration）]**ページを使用して、ポート チャネルを使用してCisco Application Centric Infrastructure（ACI）リーフ スイッチ インターフェイスにサーバーを接続します。 手順は、Cisco ACI リーフ スイッチ インターフェイスに他の種類のデバイスを接続する場合と同じになります。

図 *5:* スイッチ ポート チャネル設定



始める前に

- Cisco ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチが Cisco ACI ファブリックに登録され、使用可能であること。
- Cisco APIC 6.1(3) 以降では、ポート チャネルごとに 32 のメンバーを構成できます。**lacp min-links** の値は LACP ポート チャネルで使用されるもので、ポート チャネルをアクティブにするためにアクティブになる必要のある最小リンク数を定義します。これが 32 に拡張されました。FEX および SAN ポート チャネルは引き続き 16 個のメンバーのみをサポートします。

手順

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）]** > **[アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 次のいずれかの方法を使用して、**[インターフェイスの構成（Configure Interfaces）]** ダイアログを開きます。

方法 1：

a) **[ナビゲーション（Navigation）]** ペインで、**[クイックスタート（Quick Start）]** をクリックします。

b) **[作業（Work）]** ペインで、**[インターフェイスの設定（Configure Interfaces）]** をクリックします。

方法 2：

a) **ナビゲーション** ペインで **[インターフェイスの設定（Interface Configuration）]** を選択します。

b) **作業**ペインで、**[アクション（Actions）]** > **[インターフェイスの設定（Configure Interfaces）]** をクリックします。

ステップ 3 **[インターフェイスの設定（Configure Interfaces）]** ダイアログで、以下のアクションを実行します。

a) **[ノード タイプ（Node Type）]** で、**[リーフ（Leaf）]** をクリックします。
b) **[ポート タイプ（Port Type）]** で、**[アクセス（Access）]** をクリックします。
c) **[インターフェイス タイプ（Interface Type）]** で、目的のタイプを選択します。
d) **[インターフェイス集約タイプ（Interface Aggregation Type）]** で、**[PC]** を選択します。
e) **[ノード（Node）]**で、**[ノードの選択（Select Node）]** をクリックし、目的のスイッチ（ノード）のボックスにチェックを入れ、**[OK]** をクリックします。
f) **[すべてのスイッチのインターフェイス（Interfaces For All Switches）]** で、目的のインターフェイスの範囲を入力します。
g) **[PC/vPC インターフェイス ポリシー グループ（PC/vPC Interface Policy Group）]** で、**[PC/vPC インターフェイス ポリシー グループの選択（Select PC/vPC Interface Policy Group）]** をクリックし、既存のポートチャネル ポリシー グループを選択するか、新規に作成します。
h) **[ポートチャネル メンバー ポリシー（Port Channel Member Policy）]** で、**[ポートチャネル メンバー ポリシーの選択（Select Port Channel Member Policy）]** をクリックし、既存のポートチャネル メンバー ポリシーを選択するか、新規に作成します。
i) **[PC/vPC インターフェイス ポリシー グループの選択（Select PC/vPC Interface Policy Group）]** ダイアログで、既存のポリシー グループを選択するか、**[PC/vPC インターフェイス ポリシー グループの作成（Create PC/vPC Interface Policy Group）]** をクリックして新しいポリシー グループを作成します。
j) [保存（Save）] をクリックします。

次のタスク

これで、ポート チャネルの設定手順は完了しました。

（注） この設定はハードウェア接続を有効にしますが、このハードウェア設定に関連付けられた有効なアプリケーション プロファイル、EPG、およびコントラクトがないと、データ トラフィックはフローできません。

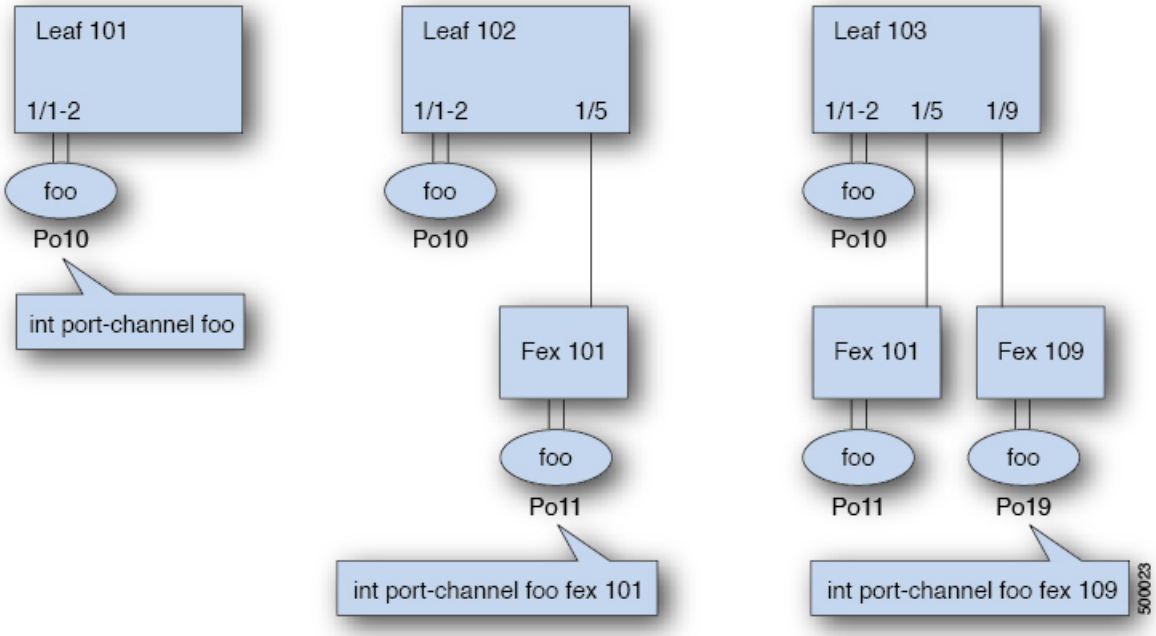
NX-OS CLI を使用したリーフ ノードおよび FEX デバイスのポートチャネルの設定

ポート チャネルは NX-OS の論理インターフェイスです。これは、複数の物理ポートのために帯域幅を集約するとともに、リンク障害時の冗長性を確保する目的でも使用されます。NX-OS におけるポート チャネル インターフェイスは、ノード内では一意となる、1 ～ 4096 の範囲でユーザが指定した番号によって識別されます。ポートチャネルインターフェイスは、（**interface port-channel** コマンドを使用して） 明示的に構成するか、または（**channel-group** コマンドを使用して）暗黙的に作成します。ポート チャネル インターフェイスの構成は、ポート チャネ

ルのすべてのメンバーポートに適用されます。特定の互換性パラメータ（速度など）は、メンバー ポートでは設定できません。

ACI モデルでは、ポート チャネルは論理エンティティとして設定され、1 つ以上のリーフ ノードでポート セットに割り当てられるポリシーのコレクションを表す名前によって識別されます。このような割り当てによって各リーフ ノードにポート チャネル インターフェイスが 1 個作成されます。これは、リーフ ノード内の 1 ～ 4096 の範囲で自動生成される番号によって識別されます。同じポートチャネル名を持つノード間で、番号を同じにすることも、別にすることもできます。これらのポートチャネルのメンバーシップは、同じでも異なっていてもかまいません。FEX ポート上にポート チャネルを作成するときには、同じポート チャネル名を使用して、リーフ ノードに接続されている各 FEX デバイスに対して 1 つのポート チャネル インターフェイスを作成することができます。したがって、N 個の FEX モジュールに接続されている各リーフ ノードには最大で N+1 個の一意のポート チャネル インターフェイス（自動生成されるポート チャネル番号で識別される）を作成できます。これは以下の例で説明します。FEX ポートのポートチャネルは、*fex-id* とポートチャネル名を指定することによって識別されます（例：**interface port-channel foo fex 101**）。

図 *6 :* リーフ スイッチと *FEX* ポートのポート チャネルの例



- 各リーフが N 個の FEX ノードに接続されているときは、ポート チャネル foo のリーフごとに N+1 個のインスタンスが可能です。
- リーフ ポートおよび FEX ポートを同じポート チャネル インスタンスの一部にすることはできません。
- 各 FEX ノードはポート チャネル foo のインスタンスを 1 つだけ持つことができます。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure** 例： `apic1# configure`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**template port-channel** *channel-name* 例： `apic1(config)# template port-channel foo`	新しいポート チャネルを作成するか、既存のポートチャネルを構成します（グローバル構成）。
ステップ 3	[**no**] **switchport access vlan** *vlan-id* **tenant** *tenant-name* **application** *application-name* **epg** *epg-name* 例： `apic1(config-po-ch-if)# switchport access vlan 4 tenant ExampleCorp application Web epg webEpg`	ポート チャネルが関連付けられるすべてのポート上に VLAN を持つ EPG を展開します。

ステップ 4	**channel-mode active**
	例：
	`apic1(config-po-ch-if)# channel-mode active`
	（注）
	対称ハッシュを有効にするには、**lacp symmetric-hash** コマンドを入力します。
	`apic1(config-po-ch-if)# lacp symmetric-hash`
		（注）
		channel-mode コマンドは、NX-OS の channel-group コマンドの mode オプションに相当します。ただし、ACI ではこれは（メンバー ポートではなく）ポート チャネルでサポートされます。
		対称ハッシュは、次のスイッチではサポートされていません。
		• Cisco Nexus 93128TX
		• Cisco Nexus 9372PX
		• Cisco Nexus 9372PX-E
		• Cisco Nexus 9372TX
		• Cisco Nexus 9372TX-E
		• Cisco Nexus 9396PX
		• Cisco Nexus 9396TX

ステップ 5	**exit** 例： `apic1(config-po-ch-if)# exit`	設定モードに戻ります。

	コマンドまたはアクション	目的
ステップ 6	**leaf** *node-id* 例： `apic1(config)# leaf 101`	設定するリーフスイッチを指定します。*node-id* には、設定の適用対象となる単一のノード ID、または ID の範囲を *node-id1–node-id2* という形式で指定できます。
ステップ 7	**interface** *type* 例： `apic1(config-leaf)# interface ethernet 1/1-2`	ポートチャネルに構成するインターフェイスまたはインターフェイスの範囲を指定します。
ステップ 8	[**no**] **channel-group** *channel-name* 例： `apic1(config-leaf-if)# channel-group foo`	インターフェイスまたはインターフェイスの範囲をポート チャネルに割り当てます。ポートチャネルからインターフェイスを削除するには、キーワード **no** を使用します。インターフェイス上からポート チャネルの割り当てを変更する場合は、以前のポート チャネルからインターフェイスを先に削除しなくても、**channel-group** コマンドを入力することができます。

ステップ 9	（任意） **lacp port-priority** *priority*
	例：
	`apic1(config-leaf-if)# lacp port-priority 1000`
	`apic1(config-leaf-if)# lacp rate fast`
		この設定とその他のポート単位の LACP プロパティは、この時点でポート チャネルのメンバーポートに適用できます。
		（注）
		ACI モデルでは、これらのコマンドはポートがポート チャネルのメンバーになった後でのみ使用できます。ポートがポート チャネルから削除された場合、これらのポート単位のプロパティの設定も削除されます。

次の表に、ACI モデルでポート チャネル プロパティのグローバル コンフィギュレーションを行うためのさまざまなコマンドを示します。これらのコマンドは、（config-leaf-if）CLI モードで特定のリーフのポートチャネルのオーバーライドを設定するためにも使用できます。ポートチャネル上から行った構成は、すべてのメンバー ポートに適用されます。

CLI 構文	機能
[no] speed <speedValue>	ポート チャネルの速度の設定
[no] link debounce time <time>	ポート チャネルのリンク デバウンスの設定

CLI 構文	機能
[no] negotiate auto	ポート チャネルのネゴシエートの構成
[no] cdp enable	ポートチャネルのCDPの無効化または有効化
[no] mcp enable	ポート チャネルの MCP の無効化または有効化
[no] lldp transmit	ポート チャネルの送信の設定
[no] lldp receive	ポート チャネルの LLDP 受信の設定
spanning-tree <bpduguard | bpdufilter> <enable | disable>	スパニング ツリー BPDU を設定します
[no] storm-control level <percentage> [burst-rate <percentage>]	ストーム制御（パーセント）を設定します
[no] storm-control pps <packet-per-second> burst-rate <packets-per-second>	ストーム制御（秒当たりのパケット）を設定します
[no] channel-mode { active | passive | on| mac-pinning }	ポート チャネルのリンクの LACP モード |
[no] lacp min-links <value>	リンクの最小数を設定します
[no] lacp max-links <value>	リンクの最大数を設定します
[no] lacp fast-select-hot-standby	ホット スタンバイ ポートの LACP 高速セレクトを設定します
[no] lacp graceful-convergence	LACP グレースフル コンバージェンスを設定します
[no] lacp load-defer	LACP ロード遅延メンバー ポートを設定します
[no] lacp suspend-individual	LACP 個別ポートの中断を設定します
[no] lacp port-priority	LACP ポート プライオリティ
[no] lacp rate	LACP レートを設定します

例

ポート チャネル（グローバル コンフィギュレーション）を設定します。速度およびチャネル モードの 2 つの設定を含むポリシーのコレクションを表す論理エンティティ「foo」を作成します。必要に応じてより多くのプロパティを設定できます。

（注） channel mode コマンドは、NX-OS の channel group コマンドの mode オプションに相当します。ただし、ACI ではこれは（メンバー ポートではなく）ポート チャネルでサポートされます。

```
apic1(config)# template port-channel foo
apic1(config-po-ch-if)# switchport access vlan 4 tenant ExampleCorp application Web epg
 webEpg
apic1(config-po-ch-if)# speed 10G
apic1(config-po-ch-if)# channel-mode active
```

FEX のポート チャネルにポートを構成します。この例では、ポート チャネル foo はリーフ ノード 102 に接続されている FEX 101 のポート イーサネット 1/1-2 に割り当てられ、ポート チャネル foo のインスタンスを作成します。リーフ ノードは番号（例えば 1002）を自動生成し、スイッチのポート チャネルを識別します。このポート チャネル番号は、作成されたポート チャネル foo のインスタンス数とは無関係で、リーフ ノード 102 に固有のものです。

（注） リーフ ノードにFEXモジュールを接続する設定は、FEXポートを使用してポートチャネルを作成する前に実行する必要があります。

```
apic1(config)# leaf 102
apic1(config-leaf)# interface ethernet 101/1/1-2
apic1(config-leaf-if)# channel-group foo
```

リーフ 102 では、このポート チャネル インターフェイスを interface port channel foo FEX 101 と呼ぶこともできます。

```
apic1(config)# leaf 102
apic1(config-leaf)# interface port-channel foo fex 101
apic1(config-leaf)# shut
```

複数のリーフ ノードでポートチャネルにポートを設定します。この例におけるポートチャネル foo は、101 ～ 103 の各リーフ ノード内にあるイーサネット 1/1-2 ポートに割り当てられます。リーフ ノードは各ノードで固有の番号（ノード間で同一にする、または分けられる）を自動生成し、これがポート チャネル インターフェイスを表します。

```
apic1(config)# leaf 101-103
apic1(config-leaf)# interface ethernet 1/1-2
apic1(config-leaf-if)# channel-group foo
```

ポートチャネルにメンバーを追加します。この例では、各リーフ ノードのポートチャネルに 2 つのメンバー eth1/3-4 を追加し、各ノードのポート チャネル foo がメンバー eth 1/1-4 を持つようにします。

```
apic1(config)# leaf 101-103
apic1(config-leaf)# interface ethernet 1/3-4
apic1(config-leaf-if)# channel-group foo
```

ポート チャネルからメンバーを削除します。この例は、各リーフ ノードでポート チャネル foo から 2 つのメンバー eth1/2、eth1/4 を削除し、各ノードのポート チャネル foo がメンバー eth 1/1、eth1/3 を持つようにします。

```
apic1(config)# leaf 101-103
apic1(config-leaf)# interface eth 1/2,1/4
apic1(config-leaf-if)# no channel-group foo
```

複数のリーフ ノードで異なるメンバーを持つポート チャネルを設定します。次に、同じポート チャネル foo ポリシーを使用して、リーフごとにメンバー ポートが異なる複数のリーフ ノードでポートチャネルインターフェイスを作成する例を示します。リーフ ノードのポート チャネル番号は、同じポート チャネル foo に対して同じでも異なっていてもかまいません。ただし CLI では、構成は interface port-channel foo で参照されます。FEX ポートにポート チャネルが構成されている場合は、interface port-channel foo fex <fex-id> で参照されます。

```
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/1-2
apic1(config-leaf-if)# channel-group foo
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config)# leaf 102
apic1(config-leaf)# interface ethernet 1/3-4
apic1(config-leaf-if)# channel-group foo
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config)# leaf 103
apic1(config-leaf)# interface ethernet 1/5-8
apic1(config-leaf-if)# channel-group foo
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface ethernet 101/1/1-2
apic1(config-leaf-if)# channel-group foo
```

LACP のポート単位のプロパティを設定します。次に、LACP のポート単位のプロパティについてポート チャネルのメンバー ポートを構成する例を示します。

（注） ACI モデルでは、これらのコマンドはポートがポート チャネルのメンバーになった後でのみ使用できます。ポートがポート チャネルから削除された場合、これらポート単位のプロパティ設定も削除されます。

```
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/1-2
apic1(config-leaf-if)# channel-group foo
apic1(config-leaf-if)# lacp port-priority 1000
apic1(config-leaf-if)# lacp rate fast
```

ポート チャネルの管理状態を設定します。この例におけるポート チャネル foo は、channel-group コマンドを使用することで、101 ～ 103 の各リーフ ノードに対して構成されます。ポート チャネルの管理状態は、ポート チャネル インターフェイスを使用して各リーフで設定できます。ACI モデルでは、ポート チャネルの管理状態をグローバル スコープで構成することはできません。

```
// create port-channel foo in each leaf
apic1(config)# leaf 101-103
```

```
apic1(config-leaf)# interface ethernet 1/3-4
apic1(config-leaf-if)# channel-group foo

// configure admin state in specific leaf
apic1(config)# leaf 101
apic1(config-leaf)# interface port-channel foo
apic1(config-leaf-if)# shut
```

オーバーライド構成は、他のプロパティを共有しながら各リーフのポートチャネルインターフェイスに特定の VLAN ドメインを割り当てる場合などにとても便利です。

```
// configure a port channel global config
apic1(config)# interface port-channel foo
apic1(config-if)# speed 1G
apic1(config-if)# channel-mode active

// create port-channel foo in each leaf
apic1(config)# leaf 101-103
apic1(config-leaf)# interface ethernet 1/1-2
apic1(config-leaf-if)# channel-group foo

// override port-channel foo in leaf 102
apic1(config)# leaf 102
apic1(config-leaf)# interface port-channel foo
apic1(config-leaf-if)#  speed 10G
apic1(config-leaf-if)#  channel-mode on
apic1(config-leaf-if)#  vlan-domain dom-foo
```

次の例では、channel-group コマンドを使用することで、ポートのポート チャネル割り当てを変更します。他のポートチャネルに割り当てる前にポートチャネルのメンバーシップを削除する必要はありません。

```
apic1(config)# leaf 101-103
apic1(config-leaf)# interface ethernet 1/3-4
apic1(config-leaf-if)# channel-group foo
apic1(config-leaf-if)# channel-group bar
```

ポートチャネル ダイナミック ロードバランシング

ポートチャネル スタティック ロードバランシング

スイッチが複数のバンドルリンクを持つポートチャネルを介してサーバーまたは別のスイッチにパケットを転送する場合、スイッチはハッシュアルゴリズムを使用してそのパケットのリンクを選択します。ハッシュ アルゴリズムでは、送信元と宛先の IP アドレス、送信元と宛先のポート番号、場合によってはプロトコルタイプなどのパラメータが考慮されます。

ポート チャネルのスタティック ロード バランシングでは、トラフィックは各リンクの負荷に関係なく、ポート チャネル内の同じリンクに一貫してハッシュされます。出力メンバー リンクは、5 タプル ハッシュに基づいて静的に選択されます。

ポート チャネルのスタティック ロード バランシングの欠点

ポート チャネル スタティック ロード バランシング アプローチを使用すると、ポート チャネルのリンク上でトラフィックが均等に分散され、一部のリンクはあまり使用されず、他のリンクは十分に活用されないままとなることがあります。

ポート チャネル ダイナミック ロードバランシング

ポート チャネル ダイナミック ロード バランシング（DLB）は、各リンクの負荷に基づいてポートチャネル内の複数のリンクにトラフィックを分散するネットワーキング技術です。ポートチャネル DLB は、リンクの現在の負荷に基づいてポートチャネルのリンク上のトラフィック分散を調整します。スイッチは各リンクの出力トラフィック負荷を監視し、使用率が最も低いリンクを選択してトラフィックを分散します。

フローレット

フローレットは、同じフロー内の連続するパケットのグループ、つまりバーストで、アイドル間隔で区切られます。各フローレットは、パケットの順序変更を引き起こすことなく個別に転送できます。

フローレットのエージング タイム

フローレットテーブルは、フローレットに関する情報を保持し、エージングを使用してフローレット ギャップを特定し、パケットの順序変更を防止します。たとえば、フローレットのエージング タイムを x マイクロ秒に設定したとします。既存のフローレットのトラフィックが x マイクロ秒間受信されない場合、フローレットエントリは削除対象としてマークされます。さらに x マイクロ秒経過すると、このフローレット エントリは完全に削除されます。

バーストギャップが、構成されたフローレットエージングタイムよりも小さい場合、パケットは、フローレット テーブルにフローレット エントリがまだ存在しているのと同じ、そのリンクで送信されます。バースト ギャップが構成されたフローレット エージング タイムを超えると、これらのパケットのフローレットエントリが削除されるため、パケットは異なるリンクで送信されます。

ポートチャネルのダイナミック ロード バランシングの利点

ポートチャネル DLB には次の利点があります。

- 効率的なトラフィック分散：リアルタイムのリンク使用率に基づいてトラフィックのバランスをとり、ネットワークの輻輳を防止します。
- ネットワーク パフォーマンスの向上：ネットワークの輻輳への長時間のバーストフローの影響を軽減します。
- コンバージェンスの高速化：ソフトウェアの介入を必要とせずに、ポートステータスの変化に適応します。

ポートチャネル ダイナミック ロード バランシングの制限事項

ポートチャネル DLB には次のような制限があります。

- ポートチャネル DLB は、レイヤ 2 ポート チャネルとして設定された前面パネル ポートにのみ適用できます。
- L3Out SVI VLAN のレイヤ 2 ポートチャネルのポート チャネル DLB は認定されていないため、サポートされていません。

- FEX HIF、NIF、および FC ポートはサポートされていません。
- SAN およびファイバ チャネル ポート チャネルはサポートされていません。
- DLB がサポートされるポート チャネルのメンバー ポートの数は、スライスごとに 32、スイッチごとに 64 です。

（注） **アップリンク ポートの高速リンク フェールオーバー**が有効になっているファブリック リンクの数も、各スイッチの最大ポート容量である 64 に含まれています。

（注） スイッチは、1 つまたは複数のスライスで構成されます。各スライスは自己完結型のスイッチング サブシステムです。スイッチのポートは、スライスに分散されます。

- BUM（ブロードキャスト、不明なユニキャスト、およびマルチキャストトラフィック）はサポートされていません。
- Cisco Nexus 9400 などの LEM ベースのシャーシはサポートされていません。

GUI を使用してポート チャネルのダイナミック ロード バランシング ポリシーを作成する

GUI を使用してポート チャネルのダイナミック ロード バランシング ポリシーを作成するには、次の手順に従います。

手順

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）]** > **[アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 [ナビゲーション（Navigation）] ペインで、**[ポリシー（Policies）]** > **[スイッチ（Switch）]** を展開し、**[ダイナミック ロード バランシング（Dynamic Load Balancing）]** を右クリックして、**[ダイナミック ロード バランシング ポリシーの作成（Create Dynamic Load Balancing Policy）]** を選択します。

[ダイナミック ロード バランシング ポリシーの作成（Create Dynamic Load Balancing Policy）] ダイアログボックスが表示されます。

ステップ 3 ポリシーの名前と説明を入力します。

ステップ 4 **[フローレット エージング時間（Flowlet Aging Time）]** フィールドに、エージング時間をマイクロ秒単位で入力します。

[フローレット エージング時間（Flowlet Aging Time）] で指定できる範囲は 1 ～2000000 マイクロ秒です。デフォルト値は500マイクロ秒です。推奨値は、トラフィック フローで観察された最大ラウンドトリップ時間（RTT）の 2 倍です。

ステップ 5 [送信（Submit）] をクリックします。

GUI を使用して、ポート チャネルのダイナミック ロード バランシング ポリシーをスイッチ ポリシー グループに関連付ける

GUI を使用してポート チャネルのダイナミック ロード バランシング ポリシーをスイッチ ポリシー グループに関連付けるには、次の手順に従います。

手順

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）]** > **[アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 [ナビゲーション（Navigation）] ペインで、**[スイッチ（Switches）]** > **[リーフスイッチ（Leaf Switches）]** > **[ポリシーグループ（Policy Groups）]** を展開し、スイッチ ポリシー グループを選択します。

[アクセス スイッチ ポリシー グループ（Access Switch Policy Group）] ペインが表示されます。

ステップ 3 **[ダイナミック ロード バランシング ポリシー（Dynamic Load Balancing Policy）]** ドロップダウンリストで、DLB ポリシーを選択します。

ステップ 4 [送信（Submit）] をクリックします。

GUI を使用して、ポート チャネルのダイナミック ロード バランシングを有効にする

GUI を使用してポート チャネルでダイナミック ロード バランシングを有効にするには、次の手順を実行します。

手順

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）]** > **[アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 ナビゲーション ペインで、**[インターフェイス（Interfaces）]**>**[リーフ インターフェイス（Leaf Interfaces）]** > **[プロファイル（Profiles）]**を展開し、アクセス プロファイルを展開します。

ステップ 3 アクセス プロファイルからポートチャネルを選択します。

[アクセス ポート セレクタ（Access Port Selector）] ペインが表示されます。

ステップ 4 **[ポリシー グループ（Policy Group）]** ドロップダウン リストで、次のいずれかを実行します。

- 既存のポリシー グループを選択し、**[ポリシー グループ（Policy Group）]** ドロップダウン リストの横にある アイコンをクリックします。**[PC/vPC インターフェイス ポリシー グループ（PC/vPC Interface Policy Group）]** ダイアログボックスが表示されます。
- **[PC インターフェイス ポリシー グループの作成（Create PC Interface Policy Group）]** を選択します。**[PC インターフェイス ポリシー グループの作成（Create PC Interface Policy Group）]** ダイアログボックスが表示されます。ポリシー グループの名前を入力します。
- **[VPC インターフェイス ポリシー グループの作成（Create VPC Interface Policy Group）]** を選択します。**[VPC インターフェイス ポリシー グループの作成（Create VPC Interface Policy Group）]** ダイアログボックスが表示されます。ポリシー グループの名前を入力します。

ステップ 5 **[ポート チャネル ポリシー （Port Channel Policy）]** ドロップダウン リストで、次のいずれかを実行します。

- 既存のポート チャネル ポリシーを選択し、 **[ポート チャネル ポリシー（Port Channel Policy）]** ドロップダウン リストの横にあるアイコンをクリックします。**[ポート チャネル ポリシー（Port Channel Policy）]** ダイアログボックスが表示されます。
- **Create Port Channel Policy** を選択します。**[ポート チャネル ポリシーの作成（Create Port Channel Policy）]** ダイアログボックスが表示されます。ポート チャネル ポリシーの名前を入力します。

ステップ 6 **[ポート チャネル ポリシー（Port Channel Policy）]** ダイアログボックスまたは **[ポート チャネル ポリシーの作成（Create Port Channel Policy）]** ダイアログボックスで、**[ダイナミック（Dynamic）]** トグル ボタンをクリックして、ポート チャネルでのダイナミック ロード バランシングを有効にします。

ステップ 7 [送信（Submit）] をクリックします。

GUI を使用してポート チャネルのダイナミック ロード バランシング構成を表示する

GUI を使用してポート チャネルのダイナミック ロード バランシング構成を表示するには、次の手順に従います。

手順

ステップ 1 メニュー バーで、 **[Fabric]** > **[Inventory]** を選択します。

ステップ 2 [ナビゲーション（Navigation）] ペインで、**[ポッド（Pod）]**>**[リーフ（Leaf）]** を展開します。

ステップ 3 **[Dynamic Load Balancing]** と **[Fast Link Failover]** を選択します。

[ポートチャネル ダイナミック ロード バランシングとアップリンク ポート高速リンクフェールオーバー（Port-Channel Dynamic Load Balancing and Uplink Port Fast Link Failover）] ペインが表示されます。

ステップ 4 **[ポリシー（Policy）**] タブをクリックして、ポート チャネル DLB ポリシーのフローレット エージング タイムを表示します。

ステップ 5 **[動作（Operational）]** > **[スイッチごとの使用状況（Per Switch Usage）]**タブをクリックして、DLB またはアップリンク ポートの高速リンク フェールオーバーを現在使用しているポートの数と、スイッチ レベルでサポートされているポートの最大数を表示します。

DLB またはアップリンク ポート高速リンク フェールオーバーでアクティブ化されるポートの数は、スイッチのキャパシティを超えてはなりません。

ステップ 6 **[動作（Operational）]** > **[スライスごとの使用状況（DLB のみ）（Per Slice Usage （DLB Only）**]タブをクリックして、DLB を現在使用しているポートの数と、スライス レベルでサポートされているポートの最大数を表示します。

DLB でアクティブ化される各スライスのポート数は、スライスのキャパシティを超えてはなりません。

ステップ 7 [ナビゲーション（Navigation）] ペインで **[ポッド（Pod）]** > **[ノード（Node）]** を展開し、**[サマリー（Summary）]** > **[DLB インターフェイス（DLB Interfaces）]** ペインをクリックして、現在 DLB またはアップリンク ポート高速リンク フェイルオーバーを使用しているポートの数と、ノード レベルでサポートされているポートの最大数を表示します。

GUI を使用したダイナミック ロード バランシング統計の表示

GUI を使用してポート チャネルのダイナミック ロード バランシング統計情報を表示するには、次の手順に従います。

手順

ステップ 1 メニュー バーで、 **[Fabric]** > **[Inventory]** を選択します。

ステップ 2 [ナビゲーション（Navigation）]ペインで、**[ポッド（Pod）]**>**[リーフ（Leaf）]** を展開します。

ステップ 3 **[Dynamic Load Balancing]** と **[Fast Link Failover]** を選択します。

[ポートチャネル ダイナミック ロード バランシングとアップリンク ポート高速リンクフェールオーバー（Port-Channel Dynamic Load Balancing and Uplink Port Fast Link Failover）] ペインが表示されます。

ステップ 4 DLB 統計情報を表示するには、**[統計情報（Statistics）]** タブをクリックします。

表 *2 : DLB* 統計情報の説明

DLB 統計情報	説明
DLB 入力パケットの総数	DLB が受信したパケット数の合計
コリジョンを伴うフローレットの総数	フローレット衝突の発生回数
作成済みフローレットの合計	作成された新しいフローレット エントリの数
ヒットしたフローレットの総数	着信パケットが既存のフローレット エントリと一致した回数

CLI を使用したポート チャネルのダイナミック ロード バランシング構成の確認

CLI を使用してポート チャネルのダイナミック ロード バランシング設定を確認するには、次の手順を実行します。

手順

ステップ 1 **show port-channel dlb usage** コマンドを実行して、すべてのポート チャネルで使用される DLB リソースを確認します。

例：

```
node# show port-channel dlb usage
Dynamic load balancing resource usage for port-channel1

                    Interface         Configured                 Operational
    State
    Port-channel:   port-channel1     dynamic                    dynamic
    (SU)
    Members:        Ethernet1/31      dynamic                    dynamic
    (up)
                    Ethernet1/32      dynamic                    dynamic
    (up)
                    Ethernet1/33      dynamic                    dynamic
    (up)
                    Ethernet1/34      dynamic                    dynamic
    (up)
                    Ethernet1/35      dynamic                    dynamic
    (up)

DLB resources utilized by port-channel1: 5

Dynamic load balancing resource usage for port-channel2

                    Interface         Configured                 Operational
    State
    Port-channel:   port-channel2     static                     static
```

```
    (SU)
    Members:        Ethernet1/1       static                    static
    (up)

DLB resources utilized by port-channel2: 0

Dynamic load balancing resource usage for port-channel3

                    Interface         Configured                Operational
    State
    Port-channel:   port-channel3     static                    static
    (SU)
    Members:        Ethernet1/3       static                    static
    (up)

DLB resources utilized by port-channel3: 0

Dynamic load balancing resource usage for port-channel4

                    Interface         Configured                Operational
    State
    Port-channel:   port-channel4     dynamic                   dynamic
    (SU)
    Members:        Ethernet1/7       dynamic                   dynamic
    (up)
                    Ethernet1/8       dynamic                   dynamic
    (up)
                    Ethernet1/9       dynamic                   dynamic
    (up)
                    Ethernet1/10      dynamic                   dynamic
    (up)

DLB resources utilized by port-channel4: 4

Dynamic load balancing resource usage for port-channel5

                    Interface         Configured                Operational
    State
    Port-channel:   port-channel5     static                    static
    (RU)
    Members:        Ethernet1/4       static                    static
    (up)
                    Ethernet1/5       static                    static
    (up)

DLB resources utilized by port-channel5: 0

Dynamic Load Balance Resource Summary for above port-channels

Total DLB configured port-channels:                2
Total DLB operational port-channels:               2
Total DLB non operational port-channels:           0
Total DLB not supported port-channels:             0
Total DLB resources utilized by port-channels:     9
```

ステップ 2 **show port-channel dlb usage interface port-channel** コマンドを実行して、特定のポート チャネルで使用される DLB リソースを確認します。

例：

```
node# show port-channel dlb usage interface port-channel 4
Dynamic load balancing resource usage for port-channel4

                    Interface         Configured                Operational
```

```
    State
    Port-channel:   port-channel4     dynamic                    dynamic
    (SU)
    Members:        Ethernet1/7       dynamic                    dynamic
    (up)
                    Ethernet1/8       dynamic                    dynamic
    (up)
                    Ethernet1/9       dynamic                    dynamic
    (up)
                    Ethernet1/10      dynamic                    dynamic
    (up)

DLB resources utilized by port-channel4: 4

Dynamic Load Balance Resource Summary for above port-channels

Total DLB configured port-channels:                1
Total DLB operational port-channels:               1
Total DLB non operational port-channels:           0
Total DLB not supported port-channels:             0
Total DLB resources utilized by port-channels:     4
```

ステップ 3 **show port-channel internal info** コマンドを実行して、ポート チャネルのポートの DLB ステータスを確認します。

例：

```
node# show port-channel internal info interface port-channel 4

port-channel4
channel    : 4
bundle     : 65535
ifindex    : 0x16000003
admin mode : active
oper mode  : active
nports     : 4
active     : 4
pre cfg    : 0
ltl        : 0x2006 (8198)
lif        : 0x0
iod        : 0x150 (336)
global id  : 4
flag       : 0
lock count : 0
num. of SIs: 0
ac mbrs    : 0 0
lacp graceful conv disable   : 0
lacp suspend indiv disable   : 0
pc min-links                 : 1
pc max-bundle                : 16
pc max active members        : 16
pc is-suspend-minlinks       : 0
port load defer enable       : 0
port-channel bfd config enabled     : 0
port-channel bfd config complete: 0
port-channel bfd destination: null
port-channel bfd start timeout: 0
port-channel bfd distinguished name (dn):

port-channel dlb admin mode: dynamic
port-channel dlb operational mode: dynamic
lacp fast-select-hot-standby disable   : 0
port-channel port hash-distribution    : adaptive
ethpm bundle lock count : 0
```

```
Members:
Ethernet1/7 [bundle_no = 0]     is_ltl_programmed = 1
    is_pixm_ltl_programmed = 1
Port BFD session state: 5 (none)
dlb operational mode: dynamic
Ethernet1/8 [bundle_no = 1]     is_ltl_programmed = 1
    is_pixm_ltl_programmed = 1
Port BFD session state: 5 (none)

dlb operational mode: dynamic
Ethernet1/9 [bundle_no = 2]     is_ltl_programmed = 1
    is_pixm_ltl_programmed = 1
Port BFD session state: 5 (none)

dlb operational mode: dynamic

Ethernet1/10 [bundle_no = 3]     is_ltl_programmed = 1
    is_pixm_ltl_programmed = 1
Port BFD session state: 5 (none)

dlb operational mode: dynamic
port-channel external lock:
Lock Info: resource [eth-port-channel 4]
  type[0] p_gwrap[(nil)]
      FREE @ 2024-10-14T17:07:22.364638000+05:30
  type[1] p_gwrap[(nil)]
      FREE @ 2024-10-14T17:10:05.142954000+05:30
  type[2] p_gwrap[(nil)]
      FREE @ 2024-10-14T17:10:04.493453000+05:30
0x16000003
internal (ethpm bundle) lock:
Lock Info: resource [eth-port-channel 4]
  type[0] p_gwrap[(nil)]
      FREE @ 2024-10-14T17:07:22.364616000+05:30
  type[1] p_gwrap[(nil)]
      FREE @ 2024-10-14T17:10:11.300577000+05:30
  type[2] p_gwrap[(nil)]
      FREE @ 2024-10-14T17:10:11.300369000+05:30
0x16000003
```

ステップ 4 **show dlb statistics** コマンドを実行して DLB 統計情報を確認します。

例：

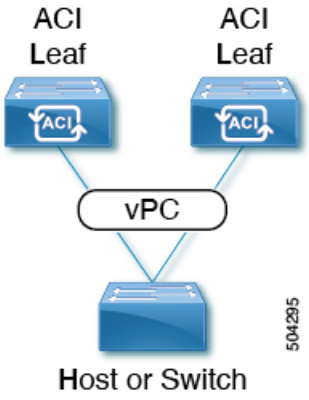
```
node# show dlb statistics
dlb statistics:
    Flowlet Hit          = 0
    Flowlet Create       = 156
    Flowlet Collision    = 0
    Flowlet DLB Rx pkts  = 3734297752
```

Cisco ACI の仮想ポート チャネル

仮想ポートチャネル（vPC）によって、2 つの異なるCisco Application Centric Infrastructure（ACI）リーフ ノードに物理的に接続されたリンクを、リンク集約テクノロジーをサポートするネットワーク スイッチ、サーバー、他のネットワークデバイスなどから単一のポートチャネル（PC）に見えるようにすることができます。vPC は、vPC のピア スイッチとして指定された 2 台の

Cisco ACI リーフ スイッチから構成されます。Of the vPC peers, one is primary and one is secondary. The system formed by the switches is referred to as a vPC domain.

図 *7: vPC* ドメイン



次の動作は、Cisco ACI vPC 実装に固有です。

- vPC ピア間に専用ピア リンクはありません。代わりに、ファブリック自体がマルチシャーシ トランキング（MCT）として機能します。
- ピア到達可能性プロトコル：Cisco ACI は、Cisco Fabric Services（CFS）の代わりに Zero Message Queue（ZMQ）を使用します。
  - ZMQ は、トランスポートとして TCP を使用するオープンソースの高性能メッセージング ライブラリです。
  - このライブラリは、スイッチ上では libzmq としてパッケージ化されており、vPC ピアと通信する必要がある各アプリケーションにリンクされています。
- ピアの到達可能性は、物理ピア リンクを使用して処理されません。代わりに、ルーティング トリガーを使用してピアの到達可能性を検出します。
  - vPC マネージャは、ピア ルート通知のためにユニキャスト ルーティング情報ベース（URIB）に登録します。
  - IS-IS がピアへのルートを検出すると、URIB は vPC マネージャに通知します。vPC マネージャは、ピアとの ZMQ ソケットを開こうとします。
  - ピア ルートが IS-IS によって取り消されると、URIB は vPC マネージャに再び通知し、vPC マネージャは MCT リンクをダウンします。
- 2 つのリーフ スイッチ間に vPC ドメインを作成する場合は、以下のハードウェア モデルの制限が適用されます。
  - 第 1 世代のスイッチは、第 1 世代の他のスイッチとのみ互換性があります。これらのスイッチ モデルは、スイッチ名の末尾に「EX」、「FX」、「FX2」、「GX」またはそれ以降のサフィックスがないことで識別できます。たとえば、N9K-9312TX という名前などです。

- 第 2 世代以降のスイッチは、vPC ドメインで混在させることができます。これらのスイッチモデルは、スイッチ名の末尾に「EX」、「FX」、「FX2」、「GX」またはそれ以降のサフィックスが付いていることで識別できます。たとえば、N9K-93108TC-EX や N9K-9348GC-FXP という名前などです。

互換性のある vPC スイッチ ペアの例：

- N9K-C9312TX および N9K-C9312TX
- N9K-C93108TC-EX および N9K-C9348GC-FXP
- N9K-C93180TC-FX and N9K-C93180YC-FX
- N9K-C93180YC-FX および N9K-C93180YC-FX

互換性のない vPC スイッチ ペアの例：

- N9K-C9312TX および N9K-C93108TC-EX
- N9K-C9312TX および N9K-C93180YC-FX

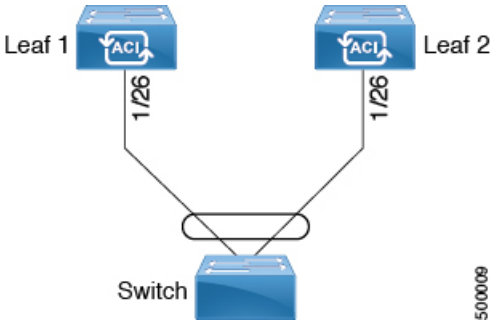
- ポートチャネルおよび仮想ポートチャネルは、LACP の有無にかかわらず構成できます。

  ポートを LACP 付きで構成したのに、ポートがピアから LACP PDU を受信しなかった場合、LACP はポートを中断状態に設定します。これによって、サーバーの中には起動に失敗するものがあります。LACP がポートを論理的 up 状態にすることを必要としているからです。**LACP suspend individual** を無効にして、動作を個々の使用に合わせて調整できます。そのためには、vPC ポリシー グループでポート チャネル ポリシーを作成し、モードを LACP アクティブに設定してから、**Suspend Individual Port** を削除します。これ以後、vPC 内のポートはアクティブなまま、LACP パケットを送信し続けます。

- ARP ネゴシエーションに基づく、仮想ポート チャネル間での適応型ロード バランシング（ALB）は、Cisco ACI ではサポートされていません。

Cisco ACI 仮想ポートチャネルのワークフロー

図 *8*: バーチャル ポート チャネルの設定



仮想ポート チャネル（vPC）の構成ワークフローは次のとおりです。

始める前に

- インフラ セキュリティ ドメインに読み取り/書き込みアクセス権限があることを確認します。
- 必要なインターフェイスを持つターゲット リーフ スイッチが使用できることを確認します。
- 同じ vPC ペアの一部になる 2 つのリーフ スイッチのハードウェアに互換性があることを確認します。詳細については、Cisco ACI の仮想ポート チャネル （32 ページ）を参照してください。

手順

ステップ 1 vPC タイプの VLAN プール、ドメイン、AAEP、アクセス リーフ ポート ポリシー グループを構成します。

ステップ 2 vPC スイッチ ペアを構成します。

ステップ 3 vPC インターフェイスを構成します。

ステップ 4 アプリケーション プロファイルを設定します。

a) メニュー バーで、**[テナント（Tenants）]** > **[すべてのテナント（ALL Tenants）]** の順に選択します。

b) [作業（Work）] ペインで、テナントをダブルクリックします。

c) [ナビゲーション（Navigation）] ペインで、**テナント名** > **[クイックスタート（Quick Start）]** を選択します。

d) エンドポイント グループ（EPG）、コントラクト、ブリッジ ドメイン、サブネット、およびコンテキストを設定します。

e) 以前に作成した仮想ポートチャネル スイッチのプロファイルにアプリケーションプロファイル EPG を関連付けます。

GUI を使用した vPC の定義

この手順では、GUI を使用して vPC を定義します。次の例に示すように、リーフ スイッチ ピア グループ名は単純にすることをお勧めします。

- Leaf201_202
- Leaf203_204
- Leaf205_206

名前付けと番号付けのベスト プラクティスについては、*Cisco ACI* オブジェクトの名前付けと番号付け： ベスト プラクティスドキュメントを参照してください。

https://www.cisco.com/c/en/us/td/docs/switches/datacenter/aci/apic/sw/kb/b-Cisco-ACI-Naming-and-Numbering.html

始める前に

同じ vPC ペアの一部になる 2 つのリーフ スイッチのハードウェアに互換性があることを確認します。詳細については、Cisco ACI の仮想ポート チャネル （32 ページ）を参照してください。

手順

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）]** > **[アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 ナビゲーション ペインで、**[ポリシー（Policies）]** > **[スイッチ（Switch）]** > **[仮想ポートチャネルのデフォルト（Virtual Port Channel default）]**を選択します。

ステップ 3 **[明示的な vPC 保護グループ（Explicit vPC Protection Groups）]** テーブルで、**[+]** をクリックし、次のようにフィールドに入力します。

a) **[名前（Name）]** フィールドに、vPC ペアの名前を入力します。

名前の例：`Leaf201_202`。この例のような名前を使用すると、どの 2 つのファブリック ノードが vPC ピアであるかを簡単に識別できます。

b) **[ID]** フィールドに、vPC ペアの ID（論理ピア ID） を入力します。

ID の例：`201`。この例では、ペアの最初のノード ID 番号を使用して、ID を vPC ペアと関連付けやすくしています。

c) **[Switch 1]** および **[Switch 2]** フィールドで、vPC スイッチ ペアのリーフスイッチを選択します。

d) [送信（Submit）] をクリックします。

vPC ペアは、**[明示的な vPC 保護グループ（Explicit vPC Protection Groups）]** テーブルに追加されます。**[仮想 IP（Virtual IP）]** 値は、システム トンネル エンドポイント （TEP）プールから自動生成された IP アドレスであり、vPC スイッチ ペアの仮想共有（エニーキャスト）TEP を表します。つまり、vPC ペアの vPC 接続エンドポイント宛てのパケットは、このエニーキャスト VTEP を使用してパケットを送信します。

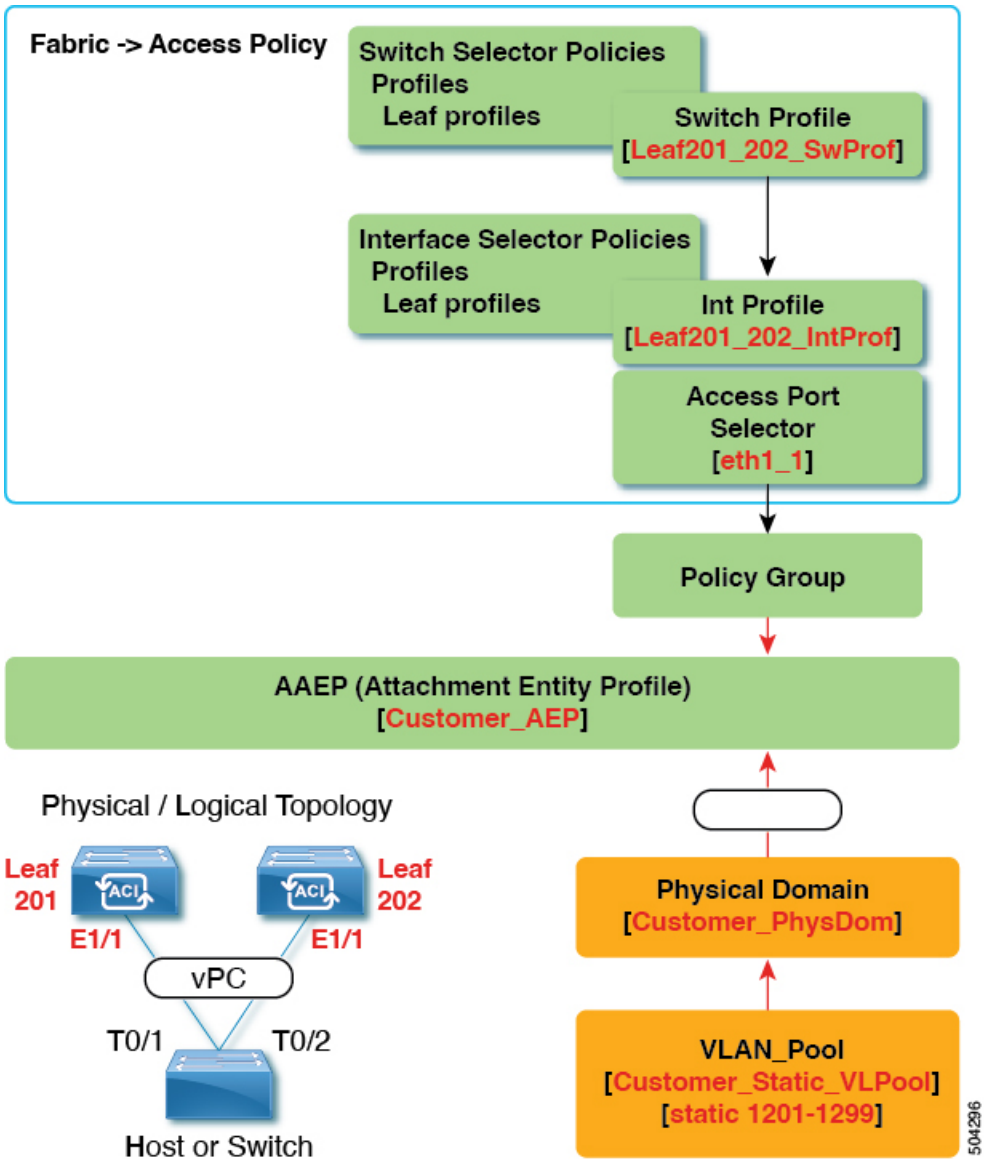
プロファイルとセレクタを使用したリーフ ノードおよび FEX デバイスでの仮想ポートチャネルの設定

結合プロファイルを持ち、2台のリーフスイッチ間で同じリーフスイッチインターフェイスを持つ vPC

このユース ケースの例では、次のことを定義します。

- `Leaf201_202_SwProf` と呼ばれる結合スイッチプロファイル（ノード 201 およびノード 202）
- `Leaf201_202_IntProf` と呼ばれる結合インターフェースプロファイル（ノード 201 およびノード 202）
- `Eth1_1` と呼ばれるアクセス ポート セレクタ（`Leaf201_202` インターフェイス プロファイルの下）は、vPC インターフェイス ポリシー グループを指しています。
- vPC インターフェイス ポリシー グループは、`Customer_AEP` と呼ばれる AAEP を指しています。
- AEP（`Customer_AEP`）には、`Customer_PhysDom` との関連付けがあります。
- `Customer_PhysDom` には、`Customer_Static_VLPool` と呼ばれる VLAN プールとの関連付けがあります。

図 *9:* 結合プロファイルを持ち、*2* 台のリーフ スイッチ間で同じリーフ スイッチ インターフェイスを持つ *vPC*



この構成の機能

スイッチ `Leaf201` および `Leaf202` で、ポート Eth1/1 を vPC の一部として設定します。この vPC インターフェイスは、VLAN 1201 ～ 1299 にアクセスできます。インターフェイス ポリシー グループに応じて、LACP アクティブおよびその他のインターフェイス固有のポリシー設定を有効にすることができます。

この構成をいつ使用するか

たとえば、vPC 接続されたサーバーのみを備えたコンピューティング リーフ スイッチの専用ペアがある場合、これは、それらのスイッチのファブリック アクセス ポリシーの下で、結合

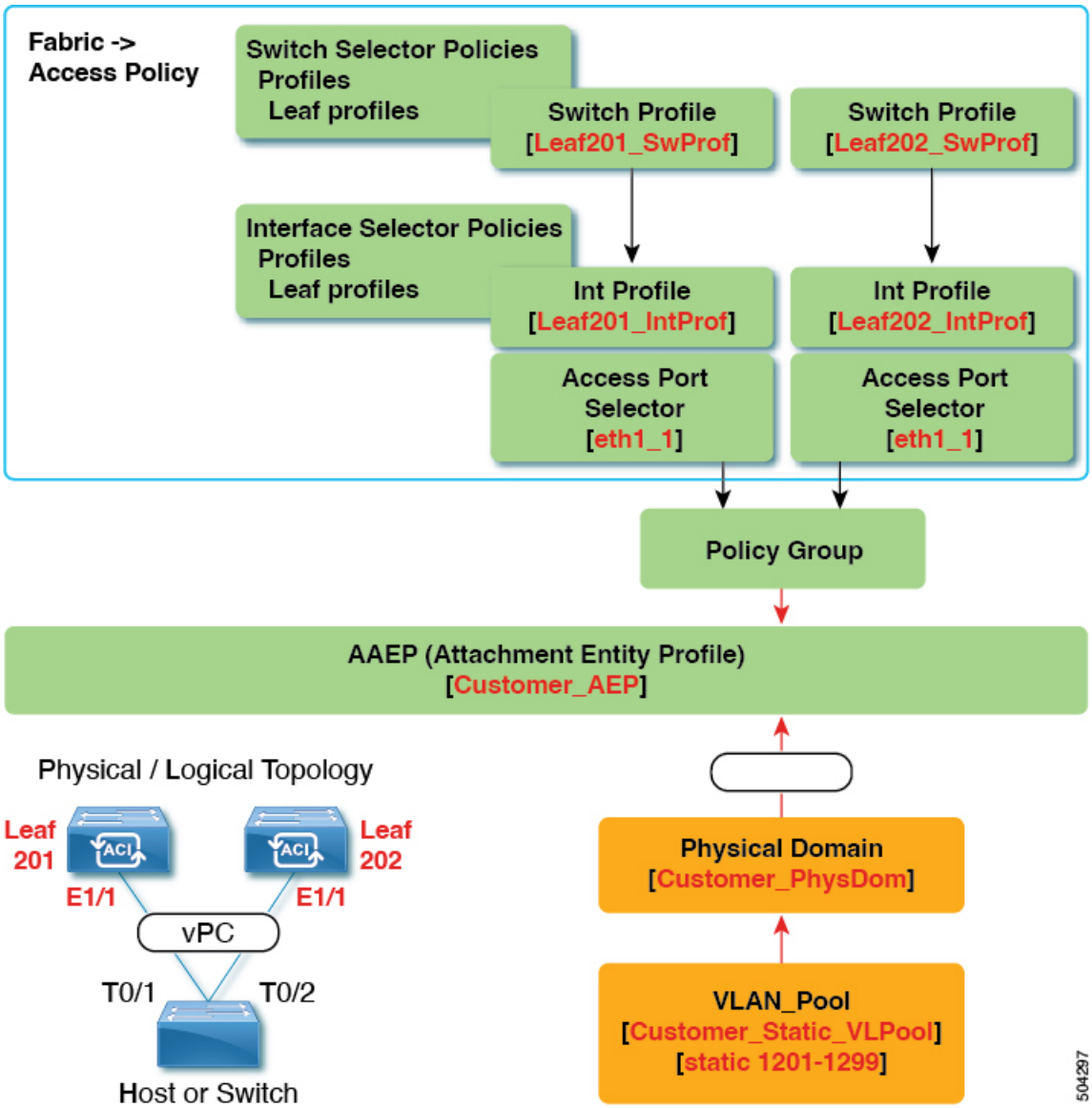
スイッチ/インターフェイス プロファイルを使用するための堅実なユース ケースになります。スイッチ、インターフェイス、アクセス ポート セレクタ、および vPC インターフェイス ポリシー グループを事前設定しておけば、最小限の労力で 48 のシャーシ タイプのサーバーを接続できるようにすることができます。

個別のプロファイルを持つ2台のリーフスイッチ間で同じリーフスイッチインターフェイスを持つ vPC

このユース ケースの例では、次のことを定義します。

- `Leaf201_SwProf` および `Leaf202_SwProf` と呼ばれる個々のスイッチ プロファイル（ノード 201 およびノード 202）。
- `Leaf201_IntProf` および `Leaf202_IntProf` と呼ばれる個々のインターフェース プロファイル（ノード 201 およびノード 202）
- Eth1_1 と呼ばれるアクセス ポート セレクタ（Leaf201 および Leaf202 インターフェイス プロファイルの下）は、同じ vPC インターフェイス ポリシー グループを指しています。
- vPC インターフェイス ポリシー グループは、`Customer_AEP` と呼ばれる AAEP を指しています。
- AEP（`Customer_AEP`）には、`Customer_PhysDom` との関連付けがあります。
- `Customer_PhysDom` には、`Customer_Static_VLPool` と呼ばれる VLAN プールとの関連付けがあります。

図 *10 :* 個別のプロファイルを持つ *2* 台のリーフ スイッチ間で同じリーフ スイッチ インターフェイスを持つ *vPC*



この構成の機能

スイッチ `Leaf201` および `Leaf202` で、ポート Eth1/1 を vPC の一部として設定します。この vPC インターフェイスは、VLAN 1201 ～ 1299 にアクセスできます。インターフェイス ポリシー グループに応じて、LACP アクティブおよびその他のインターフェイス固有のポリシー設定を有効にすることができます。

この構成をいつ使用するか

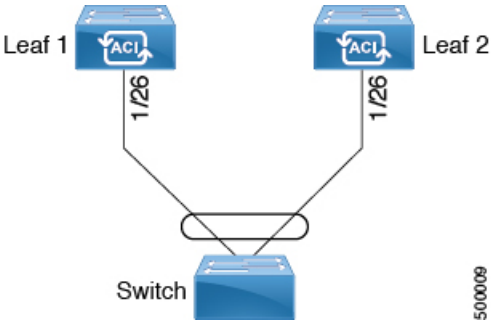
コンピューティング、サービス、または Cisco Application Policy Infrastructure Controller（APIC）などの混合ワークロードをサポートするリーフ スイッチがある場合は、この構成を使用しま

す。この場合、個別のインターフェイスプロファイルを使用すると、最大限の柔軟性が得られると同時に、**ファブリック** > **アクセス ポリシー**の設定を可能な限りクリーンで管理しやすい状態に保つことができます。

GUI を使用したインターフェイス構成モデルによる ACI リーフ スイッチ仮想ポートチャネルの構成

この手順では、「インターフェイス構成」方式を使用して、トランク スイッチを Cisco Application Centric Infrastructure（ACI）リーフ スイッチの仮想ポート チャネルに接続します。手順は、Cisco ACI リーフ スイッチ インターフェイスに他の種類のデバイスを接続する場合と同じになります。

図 *11*：スイッチ バーチャル ポート チャネル設定



始める前に

- Cisco ACIファブリックが設置され、Cisco Application Policy Infrastructure Controller（APIC）がオンラインになっており、Cisco APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ構成を作成できる Cisco APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチが Cisco ACI ファブリックに登録され、使用可能であること。

（注） 2 つのリーフ スイッチ間に vPC ドメインを作成する場合は、同じ vPC ペアの一部になる 2 つのリーフ スイッチのハードウェアに互換性があることを確認します。詳細については、Cisco ACI の仮想ポート チャネル （32 ページ）を参照してください。

手順

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）]** > **[アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 次のいずれかの方法を使用して、**[インターフェイスの構成（Configure Interfaces）]** ダイアログを開きます。

方法 1：

a) **[ナビゲーション（Navigation）]** ペインで、**[クイックスタート（Quick Start）]** をクリックします。

b) **[作業（Work）]** ペインで、**[インターフェイスの設定（Configure Interfaces）]** をクリックします。

方法 2：

a) **ナビゲーション** ペインで **[インターフェイスの設定（Interface Configuration）]** を選択します。

b) **作業**ペインで、**[アクション（Actions）]**> **[インターフェイスの設定（Configure Interfaces）]** をクリックします。

ステップ 3 **[インターフェイスの設定（Configure Interfaces）]** ダイアログで、以下のアクションを実行します。

a) **[ノード タイプ（Node Type）]** で、**[リーフ（Leaf）]** をクリックします。

b) **[ポート タイプ（Port Type）]** で、**[アクセス（Access）]** をクリックします。

c) **[インターフェイス タイプ（Interface Type）]** で、**[イーサネット（Ethernet）]** をクリックします。

d) **[インターフェイスの集約タイプ（Interface Aggregation Type）]**で、**[vPC]** を選択します。

e) **[vPC リーフ スイッチ ペア（vPC Leaf Switch Pair）]** の場合は、**[vPC リーフ スイッチ ペアの選択（Select vPC Leaf Switch Pair）]** をクリックし、目的のスイッチ ペアのボックスにチェックを入れて、**[選択（Select）]**をクリックします。複数のスイッチを選択できます。オプションとして、**[vPC リーフ スイッチ ペアの作成（Create vPC Leaf Switch Pair）]**をクリックし、必要に応じてフィールドに入力し、ペアを選択して**[選択（Select）]** をクリックします。

f) **[すべてのスイッチのインターフェイス（Interfaces For All Switches）]** で、目的のインターフェイスの範囲を入力します。

g) **[PC/vPC インターフェイス ポリシー グループ（PC/vPC Interface Policy Group）]** の場合は、**[PC/vPC インターフェイス ポリシー グループの選択（Select PC/vPC Interface Policy Group）]** をクリックします。

h) **[PC/vPC インターフェイス ポリシー グループの選択（Select PC/vPC Interface Policy Group）]** ダイアログで、既存の vPC ポリシー グループを選択し、**[選択（Select）]** をクリックします。オプションとして、**[PC/vPC インターフェイス ポリシー グループの作成（Create PC/vPC Interface Policy Group）]** をクリックして新しい vPC ポリシー グループを作成し、フィールドに入力して **[保存（Save）]**をクリックし、そのポリシー グループを選択して **[選択（Select）]** をクリックします。

i) **[ポート チャネル メンバー ポリシー（Port Channel Member Policy）]** で、**[ポート チャネル メンバー ポリシーの選択（Select Port Channel Member Policy）]**、をクリックし、ポリシーを選択して **[選択（Select）]** をクリックします。オプションとして、**[ポート チャネル メンバー ポリシーの作成（Create Port Channel Member Policy）]** をクリック

し、必要に応じてフィールドに入力して **[保存（Save）]** をクリックし、そのポリシーを選択して **[選択（Select）]** をクリックします。

j) [保存（Save）] をクリックします。

確認：vPC が適切に設定されていることを確認するには、外部スイッチがアタッチされているリーフ スイッチ上で、CLI コマンド **show int** を使用します。

次のタスク

これで、スイッチ バーチャル ポート チャネルの設定手順は完了しました。

（注） この設定はハードウェア接続を有効にしますが、このハードウェア設定に関連付けられた有効なアプリケーション プロファイル、EPG、およびコントラクトがないと、データ トラフィックはフローできません。

NX-OS CLI を使用したリーフ ノードおよび FEX デバイスの仮想ポート チャネルの設定

仮想 ポート チャネル（vPC）は、ホストまたはスイッチを 2 つのアップストリーム リーフ ノードに接続して帯域幅の使用率と可用性を向上させる、ポート チャネルの拡張機能です。NX-OS では、vPC 設定は 2 つのアップストリーム スイッチのそれぞれで行われ、スイッチ間のピア リンクを使用して設定が同期されます。

Cisco Application Centric Infrastructure（ACI）モデルでは、ピア リンクは必要なく、vPC 設定は両方のアップストリーム リーフ ノードに対してグローバルに実行できます。**vpc context** と呼ばれるグローバル コンフィギュレーション モードが Cisco ACI では導入されており、vPC インターフェイスは、両方のリーフノードにグローバルコンフィギュレーションを適用可能にする **interface vpc** というタイプを使用して表されます。

Cisco ACI モデルの vPC では、リーフポートを使用する vPC と FPC ポートを介した vPC の 2 つの異なるトポロジがサポートされます。リーフノードのペア間には多数の vPC インターフェイスを作成することができます。同様に、ストレート トポロジのリーフノード ペアに接続された FEX モジュールのペア間にも、多数の vPC インターフェイスを作成できます。

vPV に関する検討事項としては、以下のようなものがあります。

- 使用される vPC 名は、リーフノードペア間で一意です。たとえば、「corp」という vPC を作成する場合、FEX の有無にかかわらず、各リーフペアで作成できるのは 1 つだけです。
- リーフポートと FEX ポートを同じ vPC に含めることはできません。
- 各 FEX モジュールは、vPC corp の 1 つのインスタンスにのみ含めることができます。
- 設定を可能にする vPC コンテキスト

- vPC コンテキストモードでは、特定のリーフペアのすべての vPC を設定できます。vPC over FEX の場合、次の 2 つの代替例に示すように、vPC コンテキスト用に、または vPC インターフェイスとともに *fex-id* ペアを指定する必要があります。

```
(config)# vpc context leaf 101 102
(config-vpc)# interface vpc Reg fex 101 101
```

または

```
(config)# vpc context leaf 101 102 fex 101 101
(config-vpc)# interface vpc Reg
```

Cisco ACIモデルでは、vPC の設定は次の手順で行います（次の例に示します）。

（注） VLAN ドメインは、VLAN の範囲で必要です。ポート チャネルのテンプレートに関連付けられている必要があります。

1. VLAN の範囲で VLAN ドメイン構成 (グローバル設定)
2. vPC ドメイン設定（グローバル設定）
3. ポート チャネルのテンプレートの設定 (グローバル設定)
4. ポート チャネルのテンプレートを VLAN ドメインに関連付ける
5. vPC ポート チャネル設定（グローバル設定）
6. ポートをリーフノードの vPC に設定する
7. レイヤ 2、レイヤ 3を vPC コンテキストの vPC に設定する

始める前に

同じ vPC ペアの一部になる 2 つのリーフ スイッチのハードウェアに互換性があることを確認します。詳細については、Cisco ACI の仮想ポート チャネル （32 ページ）を参照してください。

手順

ステップ 1 **configure**

グローバル コンフィギュレーション モードを開始します。

例：

```
apic1# configure
```

ステップ 2 **vlan-domain***name*[**dynamic**] [**type** *domain-type*]

仮想ポート チャネルの VLAN ドメインの設定 (ポート チャネルのテンプレートとここ)。

例：

```
apic1(config)# vlan-domain dom1 dynamic
```

ステップ 3 **vlan***range*

VLAN ドメインの VLAN の範囲を設定し、configuration mode(設定モード、コンフィギュレーション モード) を終了します。単一の VLAN または複数の VLAN 範囲を設定できます。

例：

```
apic1(config-vlan)# vlan 1000-1999
apic1(config-vlan)# exit
```

ステップ 4 **vpc domain explicit** *domain-id* **leaf** *node-id1 node-id2*

vPC ドメインをリーフノードのペア間に設定します。リーフ ノード ペアとともに明示モードで vPC ドメイン ID を指定できます。

vPC ドメインを設定するための代替コマンドは次のとおりです。

- **vpc domain** [**consecutive** | **reciprocal**]

  連続オプションおよび相互オプションを使用すると、Cisco ACI ファブリック内のすべてのリーフ ノードで vPC ドメインを自動設定できます。

- **vpc domain consecutive** *domain-start* **leaf** *start-node end-node*

  このコマンドは、リーフ ノード ペアの選択されたセットに対して連続して vPC ドメインを設定します。

例：

```
apic1(config)# vpc domain explicit 1 leaf 101 102
```

ステップ 5 **peer-dead-interval** *interval*

リーフ スイッチは、ピアから応答を受信する前に、vPC を復元するまで待機する時間の遅延を設定します。この時間内ピアから応答を受信するはないとリーフ スイッチ、ピアを停止するいると見なすをマスターとしての役割を持つ vPC 始動します。ピアから応答を受信するとその時点で、vPC を復元します。範囲は 5 ～ 600 秒です。デフォルトは 200 秒です。

例：

```
apic1(config-vpc)# peer-dead-interval 10
```

ステップ 6 **exit**

グローバル コンフィギュレーション モードに戻ります。

例：

```
apic1(config-vpc)# exit
```

ステップ 7 **template port-channel** *channel-name*

新しいポートチャネルを作成するか、既存のポートチャネルを設定します（グローバル コンフィギュレーション）。

すべての vPC は、各リーフ ペアのポートチャネルとして設定されます。同じ vPC のリーフ ペアでは、同じポートチャネル名を使用する必要があります。このポートチャネルは、リーフ

ノードの 1 つ以上のペア間で vPC を作成するために使用できます。各リーフ ノードには、この vPC のインスタンスが 1 つだけあります。

例：

```
apic1(config)# template port-channel corp
```

ステップ 8 **vlan-domain member***vlan-domain-name*

以前に設定された VLAN ドメインには、ポート チャネルのテンプレートを関連付けます。

例：

```
vlan-domain member dom1
```

ステップ 9 **switchport access vlan** *vlan-id* **tenant** *tenant-name* **application** *application-name* **epg** *epg-name*

ポート チャネルを関連付けるすべてのポート上に VLAN を持つ EPG を導入します。

例：

```
apic1(config-po-ch-if)# switchport access vlan 4 tenant ExampleCorp application Web epg
 webEpg
```

ステップ 10 **channel-mode active**

（注）
vPC のポートチャネルはアクティブ チャネルモードである必要があります。

例：

```
apic1(config-po-ch-if)# channel-mode active
```

ステップ 11 **exit**

設定モードに戻ります。

例：

```
apic1(config-po-ch-if)# exit
```

ステップ 12 **leaf** *node-id1 node-id2*

設定するリーフ スイッチのペアを指定します。

例：

```
apic1(config)# leaf 101-102
```

ステップ 13 **interface** *typeleaf/interface-range*

ポート チャネルに設定するインターフェイスまたはインターフェイスの範囲を指定します。

例：

```
apic1(config-leaf)# interface ethernet 1/3-4
```

ステップ 14 [**no**] **channel-group** *channel-name* **vpc**

インターフェイスまたはインターフェイスの範囲をポートチャネルに割り当てます。ポートチャネルからインターフェイスを削除するには、キーワード **no** を使用します。インターフェ

イス上からポートチャネルの割り当てを変更する場合は、以前のポートチャネルからインターフェイスを最初に削除することなく **channel-group** コマンドを入力することができます。

（注）
このコマンドの **vpc** キーワードは、ポートチャネルを vPC にします。vPC がまだ存在しない場合は、vPC ID が自動的に生成され、すべてのメンバー リーフ ノードに適用されます。

例：

```
apic1(config-leaf-if)# channel-group corp vpc
```

ステップ 15 **exit**

例：

```
apic1(config-leaf-if)# exit
```

ステップ 16 **exit**

例：

```
apic1(config-leaf)# exit
```

ステップ 17 **vpc context leaf** *node-id1 node-id2*

vPC コンテキスト モードでは、vPC の設定を両方のリーフ ノード ペアに適用できます。

例：

```
apic1(config)# vpc context leaf 101 102
```

ステップ 18 **interface vpc** *channel-name*

例：

```
apic1(config-vpc)# interface vpc blue fex 102 102
```

ステップ 19 （任意） [**no**] **shutdown**

vPC コンテキストでの管理状態の設定では、両方のリーフ ノードに対して 1 つのコマンドで vPC の管理状態を変更できます。

例：

```
apic1(config-vpc-if)# no shut
```

例

次に、基本的な vPC を設定する例を示します。

```
apic1# configure
apic1(config)# vlan-domain dom1 dynamic
apic1(config-vlan)# vlan 1000-1999
apic1(config-vlan)# exit
apic1(config)# vpc domain explicit 1 leaf 101 102
apic1(config-vpc)# peer-dead-interval 10
apic1(config-vpc)# exit
apic1(config)# template port-channel corp
apic1(config-po-ch-if)# vlan-domain member dom1
```

```
apic1(config-po-ch-if)# channel-mode active
apic1(config-po-ch-if)# exit
apic1(config)# leaf 101-102
apic1(config-leaf)# interface ethernet 1/3-4
apic1(config-leaf-if)# channel-group corp vpc
apic1(config-leaf-if)# exit
apic1(config)# vpc context leaf 101 102
```

次に、FEX ポートを使用して vPC を設定する例を示します。

```
apic1(config-leaf)# interface ethernet 101/1/1-2
apic1(config-leaf-if)# channel-group Reg vpc
apic1(config)# vpc context leaf 101 102
apic1(config-vpc)# interface vpc corp
apic1(config-vpc-if)# exit
apic1(config-vpc)# interface vpc red fex 101 101
apic1(config-vpc-if)# switchport
apic1(config-vpc-if)# exit
apic1(config-vpc)# interface vpc blue fex 102 102
apic1(config-vpc-if)# shut
```

リフレクティブ リレー (802.1Qbg)

リフレクティブ リレーでは、Cisco APIC リリース 2.3(1) でスイッチング オプションの開始時刻です。リフレクティブ リレー: IEEE 標準 802.1Qbg のタグのないアプローチ: ポリシーを適用し、必要に応じて、宛先またはターゲット VM サーバ上にトラフィックを送信する外部のスイッチへのすべてのトラフィックを転送します。ローカルスイッチングはありません。ブロードキャストまたはマルチキャスト トラフィックは、リフレクティブ リレーは、各 VM サーバでローカルにパケットのレプリケーションを提供します。

リフレクティブ リレーの利点の 1 つは、スイッチング機能および管理機能、Vm をサポートするサーバ リソースを解放するための外部スイッチを活用しています。リフレクティブ リレーでは、ポリシー、同じサーバ上の Vm の間のトラフィックに適用する Cisco APIC で設定することもできます。

Cisco ACI、入ってきたの同じポートからオンに戻すにトラフィックを許可する、リフレクティブ リレーを有効にできます。APIC GUI、NX-OS CLI または REST API を使用して、レイヤ 2 インターフェイス ポリシーとして individual ports(個々のポート、個別ポート)、ポート チャネルまたは仮想ポート チャネルでリフレクティブ リレーを有効にすることができます。この機能はデフォルトではディセーブルになっています。

用語 仮想イーサネット ポートのためのアグリゲータ 802.1Qbg を説明する (VEPA) が使用されるも機能します。

リフレクティブ リレーのサポート

リフレクティブ リレーには、次のサポートされています。

- IEEE 標準 802.1Qbg タグのないアプローチ、リフレクティブ リレーとも呼ばれます。

  Cisco APIC 2.3(1) リリースのリリースは IEE 標準 802.1Qbg をサポートしていませんマルチチャネル テクノロジーと S タグ付きアプローチです。

- 物理ドメイン。

  仮想ドメインはサポートしていません。

- 物理ポート、ポート チャネル（Pc）と仮想ポートチャネル（vPC）

  シスコ ファブリック エクステンダ (FEX) とブレード サーバはサポートされていません。リフレクティブ リレーはサポートされていないインターフェイスで有効になっていると、障害が発生すると、最後の有効な設定が保持されます。ポートでリフレクティブ リレーを無効にすると、障害をクリアします。

- Cisco Nexus 9000 シリーズのスイッチと *EX* または *FX* 、モデル名の最後にします。

GUI を使用したリフレクティブ リレーの有効化

; By default(デフォルトで、デフォルトでは) リフレクティブ リレーが無効になっていますただし、スイッチのレイヤ 2 インターフェイス ポリシーとして、ポート、またはポート チャネルまたは仮想ポート チャネルでこれを有効にできます。最初にポリシーを設定し、ポリシー グループとポリシーを関連付けます。

始める前に

この手順では、Cisco Application Centric Infrastructure（ACI）ファブリックをセットアップし、物理スイッチを設置してあることを前提としています。

手順

ステップ 1 **[ファブリック]** > **[外部アクセス ポリシー]** > > **[インターフェイス ポリシー]** を選択し、**[ポリシー]** フォルダを開きます。

ステップ 2 **[L2 インターフェイス]** フォルダを右クリックして、**[L2 インターフェイス ポリシーの作成]** を選択します。

ステップ 3 **[L2 インターフェイス ポリシーの作成]** ダイアログ ボックスで、**[名前]** フィールドに名前を入力します。

ステップ 4 **[リフレクティブ リレー （802.1Qbg)]** エリアで、**[有効]** をクリックします。

ステップ 5 必要に応じて、ダイアログ ボックスのその他のオプションを選択します。

ステップ 6 [Submit] をクリックします。

ステップ 7 **[ポリシー]** ナビゲーション ペインで、**[ポリシー グループ]** フォルダを開いて、**[リーフ ポリシー グループ]** フォルダをクリックします。

ステップ 8 **[リーフ ポリシー グループ]** 中央ペインで、**[ACTIONS]** ドロップダウン リストを展開し、**[Create Leaf Access Port Policy Group]**、**[Create PC Interface Policy Group]**、**[Create vPC Interface Policy Group]**、または **[Create PC/vPC Override Policy Group]** を選択します。

ステップ 9 ポリシーグループ ダイアログ ボックスで、**[Name field]** フィールドに名前を入力します。

ステップ 10 **[L2 インターフェイス ポリシー]** ドロップダウン リストで、リフレクティブ リレーを有効にするために作成したポリシーを選択します。

ステップ 11 [送信（Submit）] をクリックします。

NX-OS は、CLI を使用してリフレクティブ リレーの有効化

; By default(デフォルトで、デフォルトでは) リフレクティブ リレーが無効になっていますただし、スイッチのレイヤ 2 インターフェイス ポリシーとして、ポート、またはポート チャネルまたは仮想ポート チャネルでこれを有効にできます。CLI では、NX-OS テンプレートを使用して、複数のポートでリフレクティブ リレーの有効化または individual ports(個々のポート、個別ポート) で有効にすることができます。

始める前に

この手順では、Cisco Application Centric Infrastructure（ACI）ファブリックを設定し、物理スイッチをインストールしてあることを前提としています。

手順

リフレクティブ リレー 1 つまたは複数のポートで有効にします。

例：

この例では、1 つのポートでリフレクティブ リレーが有効にします。

```
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/2
apic1(config-leaf-if)# switchport vepa enabled
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

例：

この例では、リフレクティブ リレー、テンプレートを使用して複数のポートで有効にします。

```
apic1(config)# template policy-group grp1
apic1(config-pol-grp-if)# switchport vepa enabled
apic1(config-pol-grp-if)# exit
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/2-4
apic1(config-leaf-if)# policy-group grp1
```

例：

この例では、ポート チャネルでリフレクティブ リレーが有効にします。

```
apic1(config)# leaf 101
apic1(config-leaf)# interface port-channel po2
apic1(config-leaf-if)# switchport vepa enabled
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config)#
```

例：

この例では、複数のポート チャネルでリフレクティブ リレーが有効にします。

```
apic1(config)# template port-channel po1
apic1(config-if)# switchport vepa enabled
apic1(config-if)# exit
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/3-4
apic1(config-leaf-if)# channel-group po1
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

例：

この例では、仮想ポート チャネルでリフレクティブ リレーが有効にします。

```
apic1(config)# vpc domain explicit 1 leaf 101 102
apic1(config-vpc)# exit
apic1(config)# template port-channel po4
apic1(config-if)# exit
apic1(config)# leaf 101-102
apic1(config-leaf)# interface eth 1/11-12
apic1(config-leaf-if)# channel-group po4 vpc
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config)# vpc context leaf 101 102
apic1(config-vpc)# interface vpc po4
apic1(config-vpc-if)# switchport vepa enabled
```

FEX デバイスへのポート、PC、および vPC 接続の設定

FEX 接続とそれらの構成に使用されるプロファイルは、GUI、NX-OS スタイルの CLI、または REST API を使用して作成できます。Cisco Application Policy Infrastructure Controller（APIC）3.0（1k）リリース以降では、FEX 接続構成のインターフェイス プロファイルがサポートされています。

構成には、2 つの主要な手順があります。

- FEX と Cisco Application Centric Infrastructure（ACI）リーフ スイッチ間の接続の定義
- サーバーに接続されている FEX ポートの構成

Cisco ACI リーフ スイッチへの FEX 接続を構成した後の、FEX ホスト側ポートの構成は、個々のインターフェイス、ポートチャネル、または vPC としての Cisco ACI リーフ スイッチ ポートの構成と変わりません。

GUI、NX-OS スタイルの CLI、または REST API を使用してポート、PC、および vPC を構成する方法については、次の項を参照してください。

- 物理ポートの構成 （4 ページ）
- ポート チャネル （13 ページ）
- Cisco ACI の仮想ポート チャネル （32 ページ）

ACI FEX のガイドライン

FEX を展開するときは、次のガイドラインに従ってください。

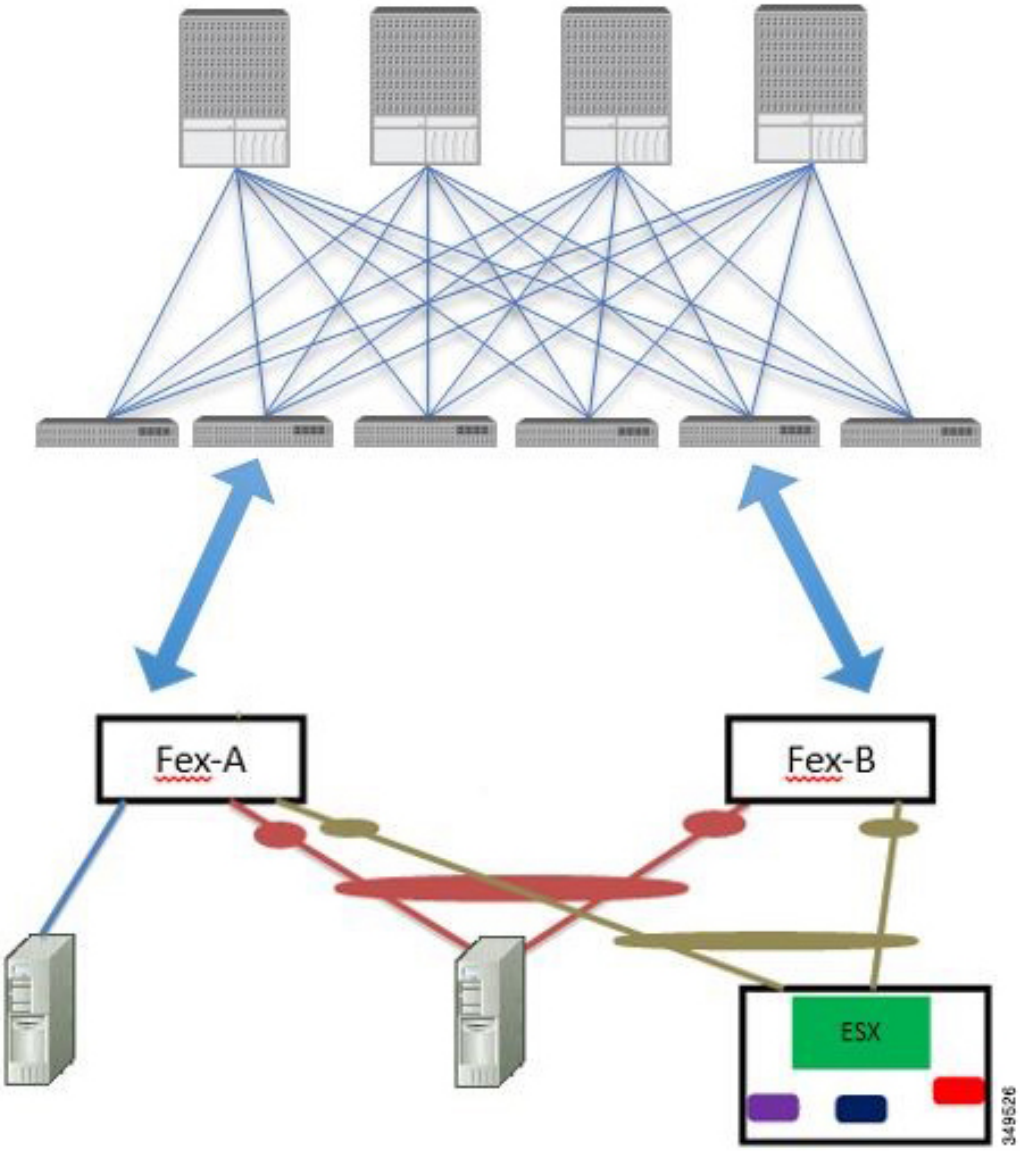
- リーフ スイッチ前面パネル ポートが EPG および VLAN を展開するように設定されていないと仮定して、最大 10,000 個のポート EPG が FEX を使用して展開することをサポートします。
- メンバーとして FEX ポートを含む各 FEX ポートまたは vPC では、各 VLAN で最大 20 個の EPG がサポートされます。
- FEX インターフェイスを備えた vPC は、ポート チャネル ポリシーで設定されたリンクの最小数と最大数を無視します。vPC は、リンク数が最小値を下回ったり、最大値を上回ったりしても、up 状態を維持します。
- 各 FEX LACP は、1 つのポート チャネルで最大 8 つのアクティブ メンバー ポートをサポートします。同じポート チャネルに、ホット スタンバイとして 8 つのポートを追加できます。
- APIC からの LACP min-link/max-link 設定はサポートされていません。FEX は、**max-link** パラメータとして常に 8 を使用します。

FEX 仮想ポート チャネル

ACI ファブリックは、FEX ストレート vPC とも呼ばれる Cisco Fabric Extender（FEX）サーバ側仮想ポート チャネル（vPC）をサポートします。

（注） 2 つのリーフ スイッチ間に vPC ドメインを作成する場合は、同じ vPC ペアの一部になる 2 つのリーフ スイッチのハードウェアに互換性があることを確認します。詳細については、Cisco ACI の仮想ポート チャネル （32 ページ）を参照してください。

図 *12 :* サポートされる *FEX vPC* トポロジ



サポートされる FEX vPC ポート チャネル トポロジは次のとおりです。

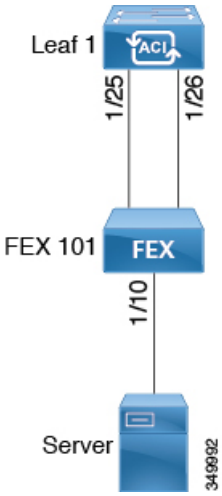
- FEX の背後にある VTEP および非 VTEP の両方のハイパーバイザ。
- ACI ファブリックに接続された 2 つの FEX に接続された仮想スイッチ（AVS や VDS など）（物理 FEX ポートに直接接続された vPC はサポートされません。vP Cはポート チャネルでのみサポートされます）。

（注） GARP を、同じ FEX 上の異なるインターフェイスで IP から MAC バインディングへ変更する際の通知プロトコルとして使用する場合、ブリッジ ドメインは **[ARP フラッディング (ARP Flooding)]** に設定し、**[EP 移動検出モード (EP Mode Detection Mode)]** : **[GARP ベースの検出 (GARP-based Detection)]** を、ブリッジ ドメイン ウィザードの **[L3 構成 (L3 Configuration)]** ページで有効にする必要があります。この回避策は、のみ生成 1 スイッチで必要です。第 2 世代のスイッチで、または以降では、この問題ではありません。

GUI を使用した ACI リーフ スイッチへの FEX 接続の構成

この手順では、FEX にサーバを接続する手順を示します。手順は、Cisco Application Centric Infrastructure（ACI）が接続された FEX にデバイスを接続する場合と同じになります。

図 *13 :* 基本的な *FEX* 設定



（注） FEX ID 165 ～ 199 の FEX 接続の設定は、APIC GUI ではサポートされていません。これらの FEX ID のいずれかを使用するには、NX-OS スタイル CLI を使用してプロファイルを設定します。詳細については、「*NX-OS* スタイル *CLI* のインターフェイス プロファイルを使用して *FEX* 接続を設定する」を参照してください。

始める前に

- Cisco ACI ファブリックが設置され、Cisco Application Policy Infrastructure Controller（APIC）がオンラインになっており、Cisco APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成できる Cisco APIC ファブリック管理者アカウントが使用可能であること。

- ターゲット リーフ スイッチ、インターフェイス、およびプロトコルが設定されており、使用可能であること。
- FEX に電源が入っていて、ターゲット リーフ スイッチのインターフェイスに接続されていること。

（注） FEXに接続されているファブリックポートチャネルでは、最大8つのメンバーがサポートされます。

手順

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）]** > **[アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 **ナビゲーション** ペインで **[インターフェイスの設定（Interface Configuration）]** を選択します。

ステップ 3 **作業** ペインで、**[アクション（Actions）]** > **[ファブリック エクステンダ（Fabric Extender）]** をクリックします。

ステップ 4 **[ファブリック エクステンダ（Fabric Extender）]** ダイアログボックスで、次の操作を実行します。

a) **[ノード（Node）]** で、**[ノードの選択（Select Node）]** をクリックし、目的のノードのボックスにチェックを入れて、**[OK]** をクリックします。複数のノードを選択できます。

b) **[すべてのスイッチのインターフェイス（Interfaces For All Switches）]** で、目的のインターフェイスの範囲を入力します。

c) **[接続先 FEX の ID（Connected FEX ID）]** には、FEX の ID を入力します。

NX-OS スタイル CLI を使用して、FEX ID 165 ～ 199 を構成する必要があります。『*Configuring FEX Connections Using Interface Profiles with the NX-OS Style CLI*』を参照してください。

d) [保存（Save）] をクリックします。
Cisco APIC は、必要な FEX プロファイル（`switch-policy-name_FexPFEX-ID`）とセレクタ（`switch-policy-name_ifselctor`）を自動的に生成します。

確認：FEX がオンラインであることを確認するには、FEX が接続されているスイッチに対して CLI コマンド show fex を使用します。

ステップ 5 通常の Cisco ACI リーフ スイッチ インターフェイスなどの FEX インターフェイスを、**[ファブリック（Fabric）]** > **[ファブリック アクセス（Fabric Access）]** > **[インターフェイス構成（Interface Configuration）]** によって構成できるようになりました。

次のタスク

（注） この設定はハードウェア接続を有効にしますが、このハードウェア設定に関連付けられた有効なアプリケーション プロファイル、EPG、およびコントラクトがないと、データ トラフィックはフローできません。

プロファイルと NX-OS スタイル CLI を使用した ACI リーフ スイッチへのFEX 接続の構成

NX-OS スタイル CLI を使用してリーフ ノードへの接続を FEX を設定するには、次の手順を使用します。

（注） FEX ID 165〜199 の FEX 接続の構成は、Cisco Application Policy Infrastructure Controller（APIC）GUI ではサポートされていません。これらの FEX Id のいずれかを使用するには、次のコマンドを使用して、プロファイルを設定します。

手順

ステップ 1 **configure**

グローバル コンフィギュレーション モードを開始します。

例：

```
apic1# configure
```

ステップ 2 **leaf-interface-profile** *name*

設定するリーフ インターフェイス プロファイルを指定します。

例：

```
apic1(config)# leaf-interface-profile fexIntProf1
```

ステップ 3 **leaf-interface-group** *name*

設定するインターフェイス グループを指定します。

例：

```
apic1(config-leaf-if-profile)# leaf-interface-group leafIntGrp1
```

ステップ 4 **fex associate** *fex-id* [**template** *template-typefex-template-name*]

リーフ ノードにFEXモジュールを接続します。使用するテンプレートを指定するのにオプションのテンプレートのキーワードを使用します。存在しない場合、システムは、名前とタイプが指定したで、テンプレートを作成します。

例：

```
apic1(config-leaf-if-group)# fex associate 101
```

例

このマージの例では、ID 101 で FEX 接続のリーフ インターフェイス プロファイルを設定します。

```
apic1# configure
apic1(config)# leaf-interface-profile fexIntProf1
apic1(config-leaf-if-profile)# leaf-interface-group leafIntGrp1
apic1(config-leaf-if-group)# fex associate 101
```

ポート プロファイルの設定

アップリンクおよびダウンリンク変換は、名前の末尾が EX か FX、またはそれ以降の Cisco Nexus 9000 シリーズ スイッチでサポートされます（たとえば、N9K-C9348GC-FXP または N9K-C93240YC-FX2）。変換後のダウンリンクに接続されている FEX もサポートされています。

サポートされているサポート対象の Cisco スイッチについては、『ポート プロファイルの設定のまとめ （63 ページ）』を参照してください。

アップリンクポートがダウンリンクポートに変換されると、他のダウンリンクポートと同じ機能を持つようになります。

制約事項

- FAST リンク フェールオーバー ポリシーとポート プロファイルは、同じポートではサポートされていません。ポート プロファイルが有効になっている場合、FAST リンク フェールオーバーを有効にすることはできません。その逆も同様です。
- サポートされているリーフ スイッチの最後の 2 つのアップリンク ポートは、ダウンリンク ポートに変換することはできません（これらはアップリンク接続用に予約されています）。
- ダイナミック ブレークアウト（100Gbと40Gbの両方）は、N9K-C93180YC-FX スイッチのプロファイルされた QSFP ポートでサポートされます。ブレイクアウトおよびポート プロファイルでは、ポート 49-52 でアップリンクからダウンリンクへの変換が一緒にサポートされています。ブレークアウト（**10g-4x** オプションと **25g-4x** オプションの両方）は、ダウンリンク プロファイル ポートでサポートされます。
- N9K-C9348GC-FXP は FEX をサポートしていません。
- ブレークアウトはダウンリンク ポートでのみサポートされます。他のスイッチに接続されているファブリック ポートではサポートされません。

- Cisco ACI リーフスイッチは、56 を超えるファブリック リンクを持つことはできません。
- スイッチのポート プロファイル構成を変更した後にスイッチをリロードすると、データプレーンを通過するトラフィックが中断されます。
- ポート プロファイルがいずれかの LEM タイプで構成されており、その LEM を交換する場合は、交換する LEM タイプが、取り外した LEM タイプと一致している必要があります。

ガイドライン

アップリンクをダウンリンクに変換したり、ダウンリンクをアップリンクに変換したりする際は、次の注意事項にご注意ください。

サブジェクト	ガイドライン
N9K-X9400-8D のポート プロファイルの注意事項	この LEM には、次の注意事項が適用されます。 • この LEM には 8 つのポートがあり、デフォルトでは 4 つのダウンリンクと 4 つのアップリンクがあります。 • ポート プロファイルの変換は、最初の 6 つのポートでサポートされます。 • この LEM には、ポート グループの依存関係はありません。
N9K-X9400-16W のポート プロファイルの注意事項	この LEM には、次の注意事項が適用されます。 • この LEM には 16 個のポートがあり、デフォルトは 12 個のダウンリンクと 4 個のアップリンクです。 • ポート プロファイルの変換は、最初の 6 つのポートでサポートされます。 • この LEM には、ポート プロファイル変換用の 2 ポートのポート グループ依存関係があります。つまり、ポート 1 ～ 2、3 ～ 4、および 5 ～ 6 にはポート グループの依存関係があります。たとえば、ポート 2 をアップリンクとして変換する場合は、ポート 1 もアップリンクに変換する必要があります。

サブジェクト	ガイドライン
N9K-X9400-22L のポート プロファイルの注意事項	6.1(2) リリースでは、この LEM のサポートが追加されています。以下の注意事項が適用されます。 • この LEM には 22 個のポートがあり、デフォルトでは 14 個のダウンリンクと 8 個のアップリンクがあります。 • ポート プロファイルの変換は、最初の 18 個のポートでサポートされます。 • この LEM には、ポート 9 と 10 を除くポート プロファイル変換用の 4 つのポートのポート グループ依存関係があります。これは、ポート 1 ～ 4、5 ～ 8、11 ～ 14、および 15 ～ 18 がポート グループの一部であることを意味します。たとえば、ポート 2 をアップリンクに変換する場合は、ポート 1 ～ 4 をすべて変換する必要があります。 • ポート 9 および 10 は 2 のポート グループです。ポート 10 をアップリンクとして変換する場合は、ポート 9 もアップリンクにする必要があります。
LEM の不一致	N9K-C9400-SUP-A で、ポート 7 ～ 18 にポート プロファイルが構成された N9K-X9400-22L LEM があり、N9K-X9400-8D や N9K-X9400 などの別の LEM タイプと交換する場合-16W の場合、8D または 16W モジュールはモジュール ステータスを表示します。 **LEM タイプの不一致**。この障害は、ポートプロファイルの変換が一致しないために発生します。8D および 16W モジュールの場合、ポート プロファイルの変換はポート 1 ～ 6 のみです。 8D または 16W LEM を不一致から回復するには、以前の LEM（つまり、N9K-X9400-22L LEM）のすべてのポートに存在するポート プロファイル構成を削除します。ポートプロファイルを構成しないでください。このプロセスの後、クリーン リロードを実行して LEM を回復します。

サブジェクト	ガイドライン
ポート プロファイルを使用したノードのデコミッション	デコミッションされたノードがポートプロファイル機能を展開している場合、ポート変換はノードのデコミッション後も削除されません。 ポートをデフォルト状態に戻すには、デコミッション後に手動で設定を削除する必要があります。これを行うには、スイッチにログオンし、`setup-clean-config.sh` スクリプトを実行して、実行されるまで待ちます。それから、`リロード` コマンドを入力します。 オプションとして、`-k` を `setup-clean-config.sh` スクリプトで指定することができます。ポートプロファイルの設定がリロード後も維持され、追加のリブートが不要になります。 6.0(5) 以降では、オプション `-k` または `--keep-port-profile` を指定せずに `setup-clean-config.sh` スクリプトを実行すると、リロード後もポートプロファイル設定が保持されます。構成を手動で削除するには、 `-d` または `--delete-profiles` を指定して `setup-clean-config.sh`スクリプトを実行します。
最大アップリンク ポートの制限	最大アップリンク ポートの制限に達し、ポート 25 および 27 がアップリンクからダウンリンクへ返還されるとき、Cisco 93180LC EX スイッチのアップリンクに戻ります。 Cisco N9K-93180LC-EX スイッチでは、ポート 25 および 27 がオリジナルのアップリンク ポートです。ポート プロファイルを使用して、ポート 25 および 27 をダウンリンク ポートに変換する場合でも、ポート 29、30、31、および 32 は引き続き 4 つの元のアップリンク ポートとして使用できます。変換可能なポート数のしきい値のため（最大 12 ポート）、8 個以上のダウンリンク ポートをアップリンク ポートに変換できます。たとえば、ポート 1、3、5、7、9、13、15、17 はアップリンク ポートに変換されます。ポート 29、30、31、および 32 は、4 つの元からのアップリンク ポートです（Cisco 93180LC-EX スイッチでの最大アップリンク ポートの制限）。 スイッチがこの状態でポート プロファイル設定がポート 25 および 27 で削除される場合、ポート 25 および 27 はアップリンク ポートへ再度変換されますが、前述したようにスイッチにはすでに 12 個のアップリンク ポートがあります。ポート 25 および 27 をアップリンク ポートとして適用するため、ポート範囲 1、3、5、7、9、13、15、17 からランダムで 2 個のポートがアップリンクへの変換を拒否されます。この状況はユーザにより制御することはできません。 そのため、リーフ ノードをリロードする前にすべての障害を消去し、ポートタイプに関する予期しない問題を回避することが必須です。ポートプロファイルの障害を消去せずにノードをリロードすると、特に制限超過に関する障害の場合、ポートは予想される動作状態になることに注意する必要があります。

ブレークアウト制限

スイッチ	リリース	制限事項
N9K-C93180LC-EX	Cisco APIC 3.1(1) 以降	• 40 Gb と 100 Gb のダイナミック ブレークアウトは、ポート 1 ~ 24 の奇数ポート上でサポートされます。 • 上位ポート（奇数ポート）ブレークアウトされると、下部ポート（偶数ポート）はエラーが無効になります。 • ポート プロファイルおよびブレークアウトは、同じポートでサポートされていません。ただし、ポート プロファイルを適用してファブリック ポートをダウンリンクに変換してからであれば、ブレークアウト設定を適用できます。
N9K-C9336C-FX2-E	Cisco APIC 5.2(4) 以降	• 40Gb および 100Gb のダイナミック ブレークア ウトは、ポート 1 ー 34 でサポートされます。 • ポート プロファイルは、ブレークアウトが有効になっているポートには適用できません。ただし、ポート プロファイルを適用してファブリック ポートをダウンリンクに変換してからであれば、ブレークアウト設定を適用できます。 • 34 ポートすべてをブレークアウトポートとして設定できます。 • 34 のポートにブレークアウト設定を適用する場合は、34 のダウンリンク ポートを持つようにポートのポート プロファイルを設定してから、リーフ スイッチをリブートする必要があります。 • 複数のポートのリーフ スイッチにブレークアウト設定を同時に適用する場合、34 ポートのハードウェアがプログラムされるまでに最大 10 分かかります。プログラミングが完了するまで、ポートはダウンしたままになります。新しい設定の場合、クリーン リブート後、またはスイッチの検出中に遅延が発生する可能性があります。

スイッチ	リリース	制限事項
N9K-C9336C-FX2	Cisco APIC 4.2(4) 以降	• 40Gb および 100Gb のダイナミック ブレークア ウトは、ポート 1 ー 34 でサポートされます。 • ポート プロファイルは、ブレークアウトが有効になっているポートには適用できません。ただし、ポート プロファイルを適用してファブリック ポートをダウンリンクに変換してからであれば、ブレークアウト設定を適用できます。 • 34 ポートすべてをブレークアウトポートとして設定できます。 • 34 のポートにブレークアウト設定を適用する場合は、34 のダウンリンク ポートを持つようにポートのポート プロファイルを設定してから、リーフ スイッチをリブートする必要があります。 • 複数のポートのリーフ スイッチにブレークアウト設定を同時に適用する場合、34 ポートのハードウェアがプログラムされるまでに最大 10 分かかります。プログラミングが完了するまで、ポートはダウンしたままになります。新しい設定の場合、クリーン リブート後、またはスイッチの検出中に遅延が発生する可能性があります。
N9K-C9336C-FX2	Cisco APIC 3.2(1) 以降、ただし 4.2(4) は含まない	• ポート 1 ~ 30 では、40 Gb と 100 Gb のダイナミック ブレークがサポートされています。 • ポート プロファイルおよびブレークアウトは、同じポートでサポートされていません。ただし、ポート プロファイルを適用してファブリック ポートをダウンリンクに変換してからであれば、ブレークアウト設定を適用できます。 • 最大20のポートをブレークアウトポートとして設定できます。

スイッチ	リリース	制限事項

N9K-C93180YC-FX	Cisco APIC 3.2(1) 以降	• 40 Gb と 100 Gb のダイナミック ブレークは、52、上にあるときにプロファイリング QSFP ポートがポート 49 でサポートされます。ダイナミック ブレークアウトを使用するには、次のステップを実行します。
		  • ポート 49～52 を前面パネル ポート（ダウンリンク）に変換します。
		  • 次の方法のいずれかを使用して、ポート プロファイルのリロードを実行します。
		  • Cisco APIC GUI で、**[ファブリック（Fabric）]**>**[インベントリ（Inventory）]** > **[ポッド（Pod）]**>**[リーフ（Leaf）]**に移動し、**[シャーシ（Chassis）]** を右クリックして、**[リロード（Reload）]** を選択します。
		  • iBash CLI で、**reload** コマンドを入力します。
		  • プロファイルされたポート 49 - 52 のブレーク アウトを適用します。
		• ポート 53 および 54 では、ポート プロファイルまたはブレークアウトをサポートしていません。

N9K-C93240YC-FX2	Cisco APIC 4.0(1) 以降	ブレークアウトは変換後のダウンリンクではサポートされていません。

ポート プロファイルの設定のまとめ

次の表に、アップリンクからダウンリンク、およびダウンリンクからアップリンクへのポートプロファイル変換をサポートするスイッチでサポートされるアップリンクおよびダウンリンクをまとめます。

スイッチ モデル	デフォルト リンク	最大アップリンク (ファブリック ポート)	最大ダウンリンク (サーバのポート)	サポートされているリリース
N9K-C9348GC-FXP[1] N9K-C9348GC-FX3	48 x 100 M/1 G BASE-T ダウンリンク 4 x 10/25 Gbps SFP28 ダウンリンク 2 x 40/100 Gbps QSFP28 アップリンク	48 x 100 M/1 G BASE-T ダウンリンク 4 x 10/25 Gbps SFP28 アップリンク 2 x 40/100 Gbps QSFP28 アップリンク	デフォルトのポート設定と同じ	3.1(1) 6.0(5)
N9K-C93180LC-EX	24 x 40 Gbps QSFP28 ダウンリンク（ポート 1ー24） 2 x 40/100 Gbps QSFP28 アップリンク（ポート 25、27） 4 x 40/100 Gbps QSFP28 アップリンク（ポート 29ー32） または 12 X 100 Gbps QSFP28 ダウンリンク（1ー24 の奇数番号ポート） 2 x 40/100 Gbps QSFP28 アップリンク（ポート 25、27） 4 x 40/100 Gbps QSFP28 アップリンク（ポート 29ー32）	18 X 40 Gbps QSFP28 ダウンリンク（1 ー 24） 6 X 40 Gbps QSFP28 アップリンク（1ー24） 2 x 40/100 Gbps QSFP28 アップリンク（25、27） 4 x 40/100 Gbps QSFP28 アップリンク（29 ー 32） または 6 x 100 Gbps QSFP28 ダウンリンク（1ー24 の範囲の奇数） 6 x 100 Gbps QSFP28 アップリンク（1ー24 の範囲の奇数） 2 x 40/100 Gbps QSFP28 アップリンク（25、27） 4 x 40/100 Gbps QSFP28 アップリンク（29 ー 32）	24 X 40 Gbps QSFP28 ダウンリンク（1 ー 24） 2 x 40/100 Gbps QSFP28 ダウンリンク（25、27） 4 x 40/100 Gbps QSFP28 アップリンク（29 ー 32） または 12 X 100 Gbps QSFP28 ダウンリンク（1 ー 24 の範囲の奇数） 2 x 40/100 Gbps QSFP28 ダウンリンク（25、27） 4 x 40/100 Gbps QSFP28 アップリンク（29 ー 32）	3.1(1)

スイッチ モデル	デフォルト リンク	最大アップリンク (ファブリック ポート)	最大ダウンリンク (サーバのポート)	サポートされているリリース
N9K-C93180YC-EX N9K-C93180YC-FX N9K-C93180YC-FX3	48 x 10/25 Gbps ファイバ ダウンリンク 6 x 40/100 Gbps QSFP28 アップリンク	デフォルトのポート設定と同じ	48 x 10/25 Gbps ファイバ ダウンリンク 4 x 40/100 Gbps QSFP28 ダウンリンク 2 x 40/100 Gbps QSFP28 アップリンク	3.1(1)
		48 X 10/25 Gbps ファイバ アップリンク 6 x 40/100 Gbps QSFP28 アップリンク		4.0(1) 5.1(3)
N9K-C93108TC-EX[2] N9K-C93108TC-FX[2] N9K-C93108TC-FX3	48 x 10GBASE T ダウンリンク 6 x 40/100 Gbps QSFP28 アップリンク	デフォルトのポート設定と同じ	48 x 10/25 Gbps ファイバ ダウンリンク 4 x 40/100 Gbps QSFP28 ダウンリンク 2 x 40/100 Gbps QSFP28 アップリンク	3.1(1) 4.0(1) 5.1(3)

スイッチ モデル	デフォルト リンク	最大アップリンク (ファブリック ポート)	最大ダウンリンク (サーバのポート)	サポートされているリリース
N9K-C9336C-FX2	30 x 40/100 Gbps QSFP28 ダウンリンク 6 x 40/100 Gbps QSFP28 アップリンク	18 x 40/100 Gbps QSFP28 ダウンリンク 18 x 40/100 Gbps QSFP28 アップリンク	デフォルトのポート設定と同じ	3.2(1)
		18 x 40/100 Gbps QSFP28 ダウンリンク 18 x 40/100 Gbps QSFP28 アップリンク	34 X 40/100 Gbps QSFP28 ダウンリンク 2 x 40/100 Gbps QSFP28 アップリンク	3.2(3)
		36 x 40/100-Gbps QSFP28 アップリンク	34 X 40/100 Gbps QSFP28 ダウンリンク 2 x 40/100 Gbps QSFP28 アップリンク	4.1(1)
N9K-C9336C-FX2-E	30 x 40/100 Gbps QSFP28 ダウンリンク 6 x 40/100 Gbps QSFP28 アップリンク	36 x 40/100-Gbps QSFP28 アップリンク	34 X 40/100 Gbps QSFP28 ダウンリンク 2 x 40/100 Gbps QSFP28 アップリンク	5.2(4)
N9K-93240YC-FX2	48 x 10/25 Gbps ファイバ ダウンリンク 12 x 40 / 100Gbps QSFP28 アップリンク	デフォルトのポート設定と同じ	48 x 10/25 Gbps ファイバ ダウンリンク 10 X 40/100 Gbps QSFP28 ダウンリンク 2 x 40/100 Gbps QSFP28 アップリンク	4.0(1)
		48 X 10/25 Gbps ファイバ アップリンク 12 x 40 / 100Gbps QSFP28 アップリンク		4.1(1)

スイッチ モデル	デフォルト リンク	最大アップリンク (ファブリック ポート)	最大ダウンリンク (サーバのポート)	サポートされているリリース
N9K-C93216TC-FX2	96 X 10G BASE-T ダウンリンク 12 x 40 / 100Gbps QSFP28 アップリンク	デフォルトのポート設定と同じ	96 X 10G BASE-T ダウンリンク 10 X 40/100 Gbps QSFP28 ダウンリンク 2 x 40/100 Gbps QSFP28 アップリンク	4.1(2)
N9K-C93360YC-FX2	96 X 10/25 Gbps SFP28 ダウンリンク 12 x 40 / 100Gbps QSFP28 アップリンク	44 x 10 / 25Gbps SFP28 ダウンリンク 52 x 10 / 25Gbps SFP28 アップリンク 12 x 40 / 100Gbps QSFP28 アップリンク	96 X 10/25 Gbps SFP28 ダウンリンク 10 X 40/100 Gbps QSFP28 ダウンリンク 2 x 40/100 Gbps QSFP28 アップリンク	4.1(2)
N9K-C93600CD-GX	28 x 40/100 Gbps QSFP28 ダウンリンク（ポート 1～28） 8 x 40/100/400 Gbps QSFP-DD アップリンク（ポート 29～36）	28 X 40/100 Gbps QSFP28 アップリンク 8 x 40/100/400 Gbps QSFP-DD アップリンク	28 X 40/100 Gbps QSFP28 ダウンリンク 6 X 40/100/400 Gbps QSFP-DD ダウンリンク 2 x 40/100/400 Gbps QSFP-DD アップリンク	4.2(2)
N9K-C9364C-GX	48 x 40/100 Gbps QSFP28 ダウンリンク（ポート 1～48） 16 x 40/100 Gbps QSFP28 アップリンク（ポート 49～64）	56 x 40/100 Gbps QSFP28 アップリンク	62 X 40/100 Gbps QSFP28 ダウンリンク 2 x 40/100 Gbps QSFP28 アップリンク	4.2(3)

スイッチ モデル	デフォルト リンク	最大アップリンク (ファブリック ポート)	最大ダウンリンク (サーバのポート)	サポートされているリリース
N9K-C9316D-GX	12 x 40/100/400 Gbps QSFP-DD ダウンリンク（ポート 1～12） 4 x 40/100/400 Gbps QSFP-DD アップリンク（ポート 13～16）	16 X 40/100/400 Gbps QSFP-DD アップリンク	14 x 40/100/400 Gbps QSFP-DD ダウンリンク	5.1(4)
N9K-C9332D-GX2B	2 x 1/10 Gbps SFP+ ダウンリンク（ポート 33～34） 24 x 40/100/400 Gbps QSFP-DD ダウンリンク（ポート 1～24） 8 x 40/100/400 Gbps QSFP-DD アップリンク（ポート 25～32）	2 X 1/10 Gbps SFP+ ダウンリンク 32 X 40/100/400 Gbps QSFP-DD アップリンク	2 X 1/10 Gbps SFP+ ダウンリンク 30 X 40/100/400 Gbps QSFP-DD ダウンリンク 2 x 40/100/400 Gbps QSFP-DD アップリンク	5.2(3)
N9K-C9348D-GX2A	2 x 1/10 Gbps SFP+ ダウンリンク（ポート 49～50） 36 x 40/100/400 Gbps QSFP-DD ダウンリンク（ポート 1～36） 12 x 40/100/400 Gbps QSFP-DD アップリンク（ポート 37～48）	2 X 1/10 Gbps SFP+ ダウンリンク 48 x 40/100/400 Gbps QSFP-DD アップリンク	2 X 1/10 Gbps SFP+ ダウンリンク 46 X 40/100/400 Gbps QSFP-DD ダウンリンク 2 x 40/100/400 Gbps QSFP-DD アップリンク	5.2(5)

スイッチ モデル	デフォルト リンク	最大アップリンク (ファブリック ポート)	最大ダウンリンク (サーバのポート)	サポートされているリリース
N9K-C9364D-GX2A	2 x 1/10 Gbps SFP+ ダウンリンク（ポート 65～66） 48 x 40/100/400 Gbps QSFP-DD ダウンリンク（ポート 1～48） 16 x 40/100/400 Gbps QSFP-DD アップリンク（ポート 49～64）	2 X 1/10 Gbps SFP+ ダウンリンク 56 X 40/100/400 Gbps QSFP-DD アップリンク	2 X 1/10 Gbps SFP+ ダウンリンク 62 X 40/100/400 Gbps QSFP-DD ダウンリンク 2 x 40/100/400 Gbps QSFP-DD アップリンク	5.2(5)
N9K-C9408（N9K-X9400-8D 搭載）[3]	6 X 40/100/400 Gbps QSFP-DD ダウンリンク 2 x 40/100/400 Gbps QSFP-DD アップリンク	8 x 40/100/400 Gbps QSFP-DD アップリンク	デフォルトのポート設定と同じ	6.0(2)
N9K-C9408（N9K-X9400-16W 搭載）[3]	12 x 100/200 Gbps QSFP56 ダウンリンク 4 x 100/200 Gbps QSFP56 アップリンク	6 x 100/200 Gbps QSFP56 アップリンク（ポート 1～6） 6 x 100/200 Gbps QSFP56 ダウンリンク（ポート 7～12） 4 x 100/200 Gbps QSFP56 アップリンク（ポート 13～16）	デフォルトのポート設定と同じ	6.0(2)[4]

1 FEX をサポートしていません。

2 アップリンクからダウンリンクへの変換のみがサポートされています。

3 ポート 1～6 のみがポート プロファイルの変換をサポートします。

4 6.0(2) リリースは 200 Gbps をサポートしていません。

GUI を使用したアップリンクからダウンリンクまたはダウンリンクからアップリンクへの変更

この手順では、ポート タイプ (アップリンクまたはダウンリンク) を決定するポート プロファイルを設定する方法について説明します。**[ファブリック（Fabric）]** > **[アクセス ポリシー（Access Policies）]** > **[インターフェイスの構成（Interface Configuration）]** > **[アクション（Actions）]** > **[インターフェイスの変換（Convert Interfaces）]**を使用して、ポートをアップリンクまたはダウンリンクとして設定できます。**[ファブリック（Fabric）]** > **[インベントリ（Inventory）]** > **[トポロジ（Topology）]** > **[インターフェイスの変換（Convert Interfaces）]**. を使用することもできます。2 つの方法は同じワークフローを提供します。

始める前に

- Cisco Application Centric Infrastructure（ACI）ファブリックが設置され、Cisco Application Policy Infrastructure Controller（APIC）がオンラインになっており、 Cisco APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成または変更できる Cisco APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチが Cisco ACI ファブリックに登録され、使用可能であること。

手順

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）]** > **[アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 ナビゲーション ペインで **[インターフェイスの構成（Interface Configuration）]** を選択します。

ステップ 3 作業ペインで、**[アクション（Actions）]** > **[インターフェイスの変換（Convert Interfaces）]**をクリックします。

ステップ 4 **[インターフェイス構成サポート タイプ（Interface Configuration Support Type）]** ドロップダウン リストで、**[アップリンクへの変換（Convert to Uplink）]** または **[ダウンリンクへの変換（Convert to Downlink）]** を選択します。

ステップ 5 **[ノード（Node）]** フィールドで、**[ノードの選択（Select Node）]** をクリックし、ノードを選択します。

ステップ 6 **[すべてのスイッチのインターフェイス（Interfaces for All Switches）]** フィールドで、目的のインターフェイスを入力します。

ダウンリンクをアップリンクに、またはアップリンクをダウンリンクに変換した後、GUI または CLI の `reload` コマンドを使用してスイッチをリロードする必要があります。スイッチの電源の再投入では不十分です。

NX-OS スタイル CLI を使用したポート プロファイルの設定

NX-OS スタイルの CLI を使用したポート プロファイルの設定をするには、次の手順を実行します。

始める前に

- ACI ファブリックが設置され、APIC コントローラがオンラインになっており、APIC クラスタが形成されて正常に動作していること。
- 必要なファブリック インフラストラクチャ設定を作成または変更できる APIC ファブリック管理者アカウントが使用可能であること。
- ターゲット リーフ スイッチが ACI ファブリックに登録され、使用可能であること。

手順

ステップ 1 **configure**

グローバル コンフィギュレーション モードを開始します。

例：

```
apic1# configure
```

ステップ 2 **leaf** *node-id*

設定するリーフまたはリーフ スイッチを指定します。

例：

```
apic1(config)# leaf 102
```

ステップ 3 **interface** *type*

設定するインターフェイスを指定します。インターフェイス タイプと ID を指定できます。イーサネット ポートの場合は、ethernet *slot* / *port* を使用します。

例：

```
apic1(config-leaf)# interface ethernet 1/2
```

ステップ 4 **port-direction** {**uplink** | **downlink**}

ポートの方向を決定するか変更します。この例ではダウンリンクにポートを設定します。

（注）
N9K-C9336C-FX スイッチでは、アップリンクからダウンリンクへの変更はサポートされていません。

例：

```
apic1(config-leaf-if)# port-direction downlink
```

ステップ 5 ポートがあるリーフ スイッチにログインし、**reload** コマンドを入力します。

NX-OS スタイル CLI を使用したポート プロファイルの設定と変換の確認

show interface brief CLI コマンドを使用して、ポートの設定と変換を確認することができます。

（注） ポート プロファイルは、Cisco N9K-C93180LC EX スイッチのトップ ポートにのみ展開されます。たとえば、1、3、5、7、9、11、13、15、17、19、21、および23となります。ポートプロファイルを使用してトップ ポートを変換すると、ボトム ポートはハードウェア的に無効になります。たとえば、ポート プロファイルを使用して Eth 1/1 を変換すると、Eth 1/2 はハードウェア的に無効になります。

手順

ステップ 1 この例では、アップリンク ポートをダウンリンク ポートに変換する場合の出力を示しています。アップリンク ポートをダウンリンク ポートに変換変換する前に、この例での出力が表示されます。**routed** というキーワードは、ポートがアップリンク ポートであることを示しています。

例：

```
switch# show interface brief
<snip>
Eth1/49          --      eth  routed  down   sfp-missing              100G(D)   --
Eth1/50          --      eth  routed  down   sfp-missing              100G(D)   --
<snip>
```

ステップ 2 ポートプロファイルを設定して、スイッチのリロード、後に、例では、出力が表示されます。キーワード **トランク** ダウンリンク ポートとしてポートを示します。

例：

```
switch# show interface brief
<snip>
Eth1/49          0       eth  trunk   down   sfp-missing              100G(D)   --
Eth1/50          0       eth  trunk   down   sfp-missing              100G(D)   --
<snip>
```

インターフェイス構成の編集

この手順では、以前に構成したインターフェイスの構成を編集する方法について説明します。これにより、インターフェイスのポート ポリシー グループまたは説明を変更できます。

始める前に

少なくとも 1 つのインターフェイスを構成する必要があります。

手順

ステップ 1 メニュー バーで、**[ファブリック（FABRIC）]** > **[アクセス ポリシー（Access Policies）]** の順に選択します。

ステップ 2 ナビゲーション ペインで **[インターフェイスの構成（Interface Configuration）]** を選択します。

ステップ 3 作業ウィンドウで、構成を編集するインターフェイスの行の右端にある **[...]** をクリックし、**[インターフェイス構成の編集（Edit Interface Configuration）]** を選択します。

ステップ 4 **[インターフェイス名ポリシーグループの編集（Edit Policy Group for interface-name）]** ダイアログで、必要に応じて構成を変更します。

ステップ 5 [保存（Save）] をクリックします。

（注）
ノードまたはポートプロファイルを使用して行われた既存の構成については、APIC REST API の構成手順を使用して FEX 構成全体を移行できます。

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。