



# ファブリック プロビジョニング

---

この章は、次の内容で構成されています。

- [ファブリック プロビジョニング \(2 ページ\)](#)
- [スタートアップ検出と構成 \(2 ページ\)](#)
- [ファブリック インベントリ \(4 ページ\)](#)
- [プロビジョニング \(6 ページ\)](#)
- [多層アーキテクチャ \(6 ページ\)](#)
- [APIC クラスタの管理 \(7 ページ\)](#)
- [メンテナンス モード \(10 ページ\)](#)
- [ストレッチ ACI ファブリックの設計の概要 \(12 ページ\)](#)
- [ストレッチ ACI ファブリック関連ドキュメント \(13 ページ\)](#)
- [ファブリック ポリシーの概要 \(13 ページ\)](#)
- [ファブリック ポリシーの構成 \(14 ページ\)](#)
- [アクセスポリシーの概要 \(16 ページ\)](#)
- [アクセス ポリシーの構成 \(17 ページ\)](#)
- [ポートチャネルと仮想ポートチャネルアクセス \(19 ページ\)](#)
- [FEX 仮想ポート チャネル \(19 ページ\)](#)
- [ファイバチャネル、または FCoE \(21 ページ\)](#)
- [802.1Q トンネル \(27 ページ\)](#)
- [ダイナミック ブレイクアウト ポート \(29 ページ\)](#)
- [ポートプロファイルの設定 \(33 ページ\)](#)
- [ポートプロファイルの設定のまとめ \(38 ページ\)](#)
- [ファブリック ポートの障害検出のためのポート トラッキング ポリシー \(42 ページ\)](#)
- [Epg の Q-で-Q カプセル化のマッピング \(43 ページ\)](#)
- [レイヤ 2 マルチキャスト \(45 ページ\)](#)
- [ファブリック セキュア モード \(50 ページ\)](#)
- [FAST リンク フェールオーバー ポリシーの構成 \(50 ページ\)](#)
- [ポートセキュリティと ACI について \(51 ページ\)](#)
- [ファースト ホップセキュリティについて \(53 ページ\)](#)
- [MACsec について \(54 ページ\)](#)

- データ プレーン ポリシング (55 ページ)
- スケジューラ (56 ページ)
- ファームウェア アップグレード (57 ページ)
- 設定ゾーン (60 ページ)
- 位置情報 (61 ページ)

## ファブリック プロビジョニング

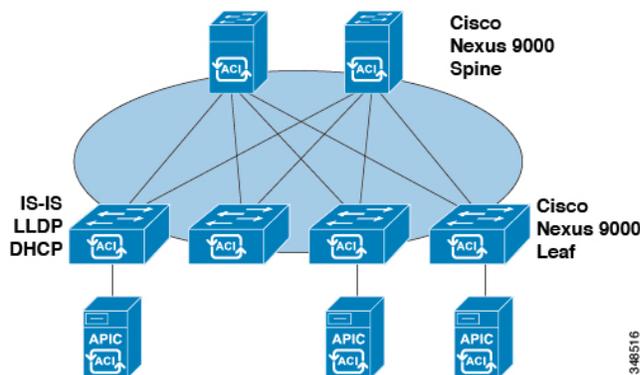
Cisco Application Centric Infrastructure (ACI) の自動化とセルフプロビジョニングにより、従来のスイッチング インフラストラクチャに勝るこれらの操作上のメリットがもたらされます。

- クラスタ化され論理的に一元化されたが物理的に分散されている APIC では、ファブリック全体にポリシー、ブートストラップおよびイメージ管理が提供されます。
- APIC 起動トポロジの自動検出、自動構成、およびインフラストラクチャ アドレッシングでは、次の業界標準のプロトコルが使用されます。Intermediate System-to-Intermediate System (IS-IS)、Link Layer Discovery Protocol (LLDP)、Dynamic Host Configuration Protocol (DHCP)。
- APIC では、シンプルで自動化されたポリシーベースのプロビジョニングとアップグレードのプロセス、および自動イメージ管理が提供されます。
- APIC では、スケーラブルな構成管理が提供されます。ACI のデータセンターは非常に規模が大きい場合があるため、スイッチまたはインターフェイスを個別に構成すると、スクリプトを使用しても十分に拡張しません。APIC ポッド、コントローラ、スイッチ、モジュール、およびインターフェイスセレクタ (すべて、範囲、特定のインスタンス) により、ファブリック全体の対称構成が可能になります。対称構成を適用するには、管理者がインターフェイス構成を単一のポリシー グループに関連付けるスイッチ プロファイルを定義します。その後、個別に構成する必要なく、そのプロファイル内のすべてのインターフェイスに迅速に展開されます。

## スタートアップ検出と構成

クラスタ化された APIC コントローラでは、ファブリックに DHCP、ブートストラップ構成およびイメージ管理が提供され、自動化されたスタートアップおよびアップグレードが可能になります。次の図は、スタートアップ検出を示します。

図 1: スタートアップ検出の構成



Cisco Nexus ACI ファブリック ソフトウェアは ISO イメージとしてバンドルされており、Cisco Integrated Management Controller (CIMC) の KVM インターフェイスを介して Cisco APIC サーバにインストールできます。Cisco Nexus ACI Software ISO には、Cisco APIC イメージ、リーフノードのファームウェア イメージ、スパイン ノードのファームウェア イメージ、デフォルトのファブリック インフラストラクチャポリシー、運用に必要なプロトコルが含まれています。

ACI ファブリックのブートストラップシーケンスは、すべてのスイッチにインストールされている工場出荷時のイメージによってファブリックがブートすると開始されます。ACI ファームウェアと APIC を実行する Cisco Nexus 9000 シリーズスイッチは、ブートプロセスに予約済みのオーバーレイを使用します。このインフラストラクチャスペースはスイッチ上でハードコードされています。APIC はデフォルトのオーバーレイを通じてリーフに接続できます。または、ローカルで有効な ID を使うことができます。

ACI ファブリックはインフラストラクチャスペースを使用します。インフラストラクチャスペースはファブリック内でセキュアに隔離され、ここですべてのトポロジ検出、ファブリック管理、インフラストラクチャアドレッシングが行われます。ファブリック内の ACI ファブリック管理コミュニケーションは、内部のプライベート IP アドレスを通じてインフラストラクチャスペース内で行われます。このアドレッシング方式によって、APIC はクラスタ内のファブリック ノードおよび他の Cisco APIC コントローラとの通信を行えます。APIC は、Link Layer Discovery Protocol (LLDP) ベースの検出プロセスを使用してクラスタ内の他の Cisco APIC コントローラの IP アドレスとノード情報を検出します。

次に、APIC クラスタ検出プロセスについて説明します。

- Cisco ACI の各 APIC は、内部のプライベート IP アドレスを使用してクラスタ内の ACI ノードおよび他の APIC と通信します。APIC は、LLDP ベースの検出プロセスを通じてクラスタ内の他の APIC コントローラの IP アドレスを検出します。
- APIC は、APIC ID から APIC IP アドレスと APIC の汎用一意識別子 (UUID) にマッピングを提供するアプライアンス ベクトル (AV) を維持します。最初に、各 APIC がローカルの IP アドレスで満たされた AV から開始し、他のすべての APIC スロットが不明としてマークされます。
- スwitchの再起動後、リーフのポリシー要素 (PE) が APIC からその AV を取得します。スイッチはその後、この AV をすべてのネイバーにアドバタイズし、ローカル AV とネイバーの AV 間の不一致をローカル AV のすべての APIC にレポートします。

このプロセスを使用して、APIC はスイッチを介して ACI の他の APIC コントローラについて学習します。クラスタ内のこれらの新しく検出された APIC コントローラを検証した後、APIC コントローラはローカル AV を更新して、スイッチを新しい AV でプログラミングします。その後、スイッチはこの新しい AV のアドバタイズを開始します。このプロセスは、すべてのスイッチが同一の AV を持ち、すべての APIC コントローラが他のすべての APIC コントローラの IP アドレスを認識するまで続きます。



- (注) クラスタへの変更を開始する前に、必ずその状態を確認してください。クラスタに対して計画した変更を実行するときは、クラスタ内のすべてのコントローラが正常である必要があります。クラスタ内の 1 つ以上の APIC コントローラが正常でない場合は、先に進む前にそのクラスタに変更を加えてその状況を修復してください。また、APIC に追加されたクラスタ コントローラが APIC クラスタ内の他のコントローラと同じファームウェアバージョンを実行しているか確認してください。APIC クラスタを正常に変更するために従う必要があるガイドラインについては、「[KB: Cisco ACI APIC クラスタ管理](#)」の記事を参照してください。

ACI ファブリックは、APIC に直接接続されているリーフノードから順に段階的に起動されます。LLDP およびコントロールプレーン IS-IS コンバージェンスは、このブートプロセスと並行して行われます。ACI ファブリックは LLDP および DHCP ベースのファブリック検出機能を使用して、ファブリック スイッチ ノードの検出、インフラストラクチャの VXLAN トンネル エンドポイント (VTEP) アドレスの割り当て、スイッチへのファームウェアのインストールを自動的に行います。この自動プロセスの前に、Cisco APIC コントローラ上で最小限のブートストラップ構成を行う必要があります。APIC コントローラが接続され、IP アドレスが割り当てられると、Web ブラウザに APIC コントローラのアドレスを入力して APIC GUI にアクセスできます。APIC GUI は HTML5 を実行し、Java をローカルにインストールする必要がなくなります。

## ファブリック インベントリ

ポリシーモデルには、すべてのノードおよびインターフェイスを含むファブリックの完全なリアルタイムインベントリが含まれます。このインベントリ機能により、プロビジョニング、トラブルシューティング、監査、およびモニタリングを自動化できます。

Cisco ACI のファブリック スイッチの場合は、ファブリック メンバーシップのノードインベントリに、ノード ID、シリアル番号および名前を識別するポリシーが含まれます。サードパーティのノードは、管理対象外のファブリック ノードとして記録されます。Cisco ACI のスイッチは自動的に検出することができ、またはポリシー情報をインポートできます。ポリシーモデルは、ファブリック メンバー ノードのステータス情報も保持します。

ノードのステータス	条件
不明	ポリシーが存在しません。すべてのノードにはポリシーが必要で、ポリシーがない場合はメンバー ノードのステータスは不明となります。

ノードのステータス	条件
検出中 (Discovering)	ノードが検出され、ホスト トラフィックの応答待ちであることを示す一時的な状態です。
未検出	ノードにはポリシーがありますが、ファブリックで提示されたことはありません。
Unsupported	ノードは Cisco のスイッチですが、サポートされていません。たとえば、ファームウェアのバージョンが ACI のファブリックと互換性がありません。
廃止	ノードはポリシーとして検出されましたが、ユーザがこれを無効にしました。ノードを再び有効化することができます。  (注) リーフスイッチを廃止するときにワイプ オプションを指定すると、APIC はリーフスイッチと APIC の両方のリーフスイッチ構成すべての削除を試みます。リーフスイッチに到達できない場合は、APIC のみがクリーニングされます。この場合、ユーザはリーフスイッチをリセットして手動でワイプする必要があります。
非アクティブ	ノードが到達不能です。検出されましたが、現在アクセスできません。たとえば、電源がオフになっているか、ケーブルが切断されている可能性があります。
アクティブ	ノードはファブリックのアクティブ メンバーです。

無効のインターフェイスは、管理者によってブラックリスト化されたものや、APIC が異常を検出するため取り除かれたものである可能性があります。リンク ステート異常の例を次に示します。

- スパインに接続されているスパイン、リーフに接続されているリーフ、リーフ アクセスポートに接続されているスパイン、非 ACI ノードに接続されているスパイン、または非 ACI デバイスに接続されているリーフ ファブリック ポートなどの配線の不一致。
- ファブリック名の不一致。ファブリック名は各 ACI ノードに保存されます。工場出荷時のデフォルト状態に戻して再設定されることなくノードが別のファブリックに移動される場合、ファブリック名が保持されます。
- UUID の不一致によって APIC がノードを無効化します。

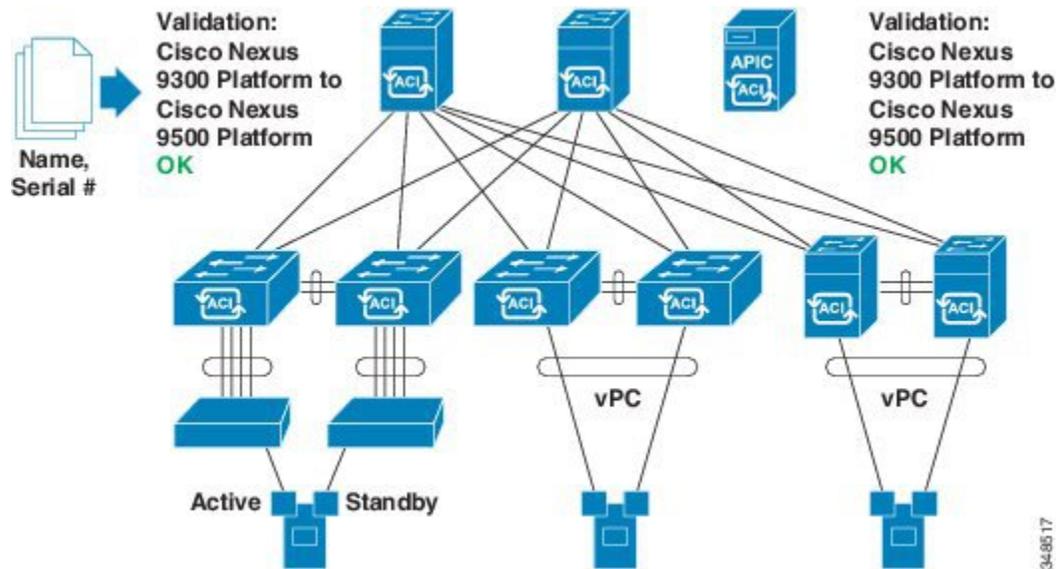


(注) 管理者が APIC を使用してスパインのすべてのリーフ ノードを無効化する場合、スパインへのアクセスを回復するためにスパインの再起動が必要です。

# プロビジョニング

APIC プロビジョニング方式により、適切な接続を通じて ACI ファブリックが自動的に起動します。次の図は、ファブリックのプロビジョニングを示します。

図 2: ファブリック プロビジョニング



Link Layer Discovery Protocol (LLDP) ディスカバリが隣接するすべての接続を動的に学習した後、これらの接続は緩やかなルールに照らし合わせて検証できます。たとえば、「LEAF can connect to only SPINE-L1-\*」または「SPINE-L1-\* can connect to SPINE-L2-\* or LEAF」などと指定できます。ルールの不一致が発生すると、障害が発生し、リーフが別のリーフまたはスパインに接続されたスパインに接続できないため、接続がブロックされます。また、接続に注意が必要であることを示すアラームが作成されます。Cisco ACI ファブリックの管理者は、テキストファイルからすべてのファブリック ノードの名前とシリアル番号を APIC にインポートすることができ、または APIC GUI、コマンドライン インターフェイス (CLI) または API を使用してシリアル番号を自動的に検出し、名前をノードに割り当てることをファブリックに許可できます。APIC は、SNMP 経由で検出可能です。次の `asysobjectId` があります。

```
ciscoACIController OBJECT IDENTIFIER ::= { ciscoProducts 2238 }
```

## 多層アーキテクチャ

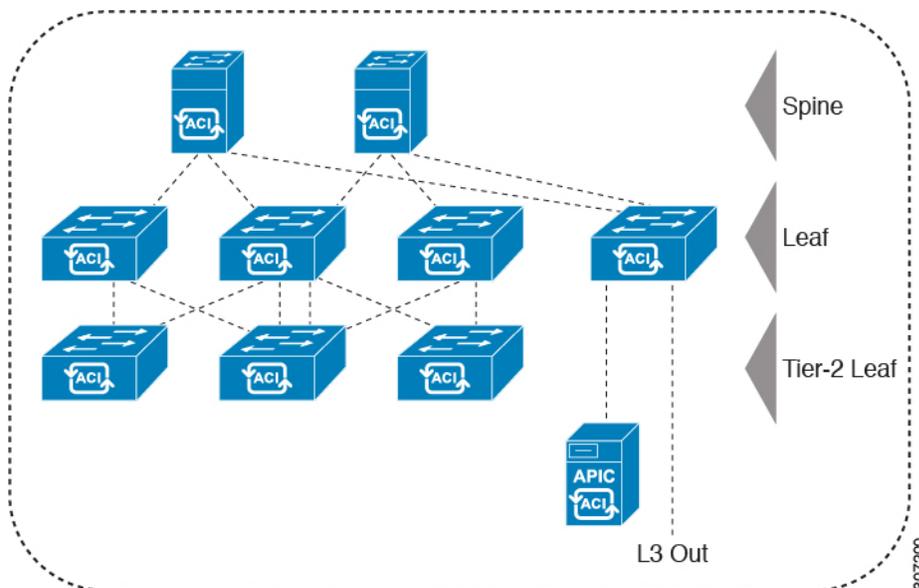
3 階層コア集約アクセス アーキテクチャは、データ センター ネットワーク トポロジで共通です。Cisco APIC リリース 4.1(1) 時点で、コア集約アクセス アーキテクチャに対応するマルチ階層 ACI ファブリック トポロジを作成するため、ラックスペースや配線などコストが高いコンポーネントのアップグレードの必要性を軽減できます。階層 2 リーフ レイヤーを追加することで、このトポロジが可能になります。階層 2 リーフ レイヤーは、ダウンリンク ポート上のホ

ストまたはサーバへの接続、およびアップリンク ポート上のリーフ レイヤー (集約) への接続をサポートします。

マルチ階層トポロジでは、リーフ スイッチには最初にスパイン スイッチへのアップリンク接続と、階層 2 リーフ スイッチへのダウンリンク接続があります。トポロジ全体を ACI ファブリックにするには、階層 2 リーフ ファブリック ポートに接続されているリーフ スイッチ上のすべてのポートが、ファブリック ポートとして設定されている必要があります (まだデフォルトのファブリック ポートを使用していない場合)。APIC が階層 2 リーフ スイッチを検出した後、階層 2 リーフ 上のダウンリンク ポートをファブリック ポートに変更し、中間レイヤリーフ 上のアップリンク ポートに接続できます。

次の図は、マルチ階層ファブリック トポロジの例を示します。

図 3: マルチ階層ファブリック トポロジ例



上の図のトポロジがリーフ集約レイヤに接続している Cisco APIC および L3Out/EPG を示しており、階層 2 リーフ アクセス レイヤは APIC および L3Out/EPG への接続もサポートしています。

## APIC クラスタの管理

### クラスタ管理の注意事項

Cisco Application Policy Infrastructure Controller (APIC) クラスタは複数の Cisco APIC コントローラで構成され、ACI ファブリックに対する統合されたリアルタイム モニタリング、診断および構成管理機能がオペレータに提供されます。最適なシステム パフォーマンスが得られるように、Cisco APIC クラスタを変更する場合は次のガイドラインに従ってください。



- (注) クラスタへの変更を開始する前に、必ずその状態を確認してください。クラスタに対して計画した変更を実行するときは、クラスタ内のすべてのコントローラが正常である必要があります。クラスタ内の1つ以上の Cisco APIC のヘルス ステータスが「十分に正常」でない場合は、先に進む前にその状況を修復してください。また、Cisco APIC に追加されたクラスタコントローラが Cisco APIC クラスタ内の他のコントローラと同じファームウェアバージョンを実行しているか確認してください。

クラスタを管理する場合、次の一般的ガイドラインに従ってください。

- クラスタ内には少なくとも3つのアクティブな Cisco APIC を追加のスタンバイ Cisco APIC とともに使用することを推奨します。ほとんどの場合、3、5、または7の Cisco APIC のクラスタサイズにすることをお勧めします。80~200のリーフスイッチの2つのサイトのマルチポッドファブリックには4つの Cisco APIC を推奨します。
- 現在クラスタにない Cisco APIC からのクラスタ情報は無視します。正確なクラスタ情報ではありません。
- クラスタ スロットには Cisco APIC ChassisID を含みます。スロットを設定すると、割り当てられたシャーシ ID の Cisco APIC を解放するまでそのスロットは使用できません。
- Cisco APIC ファームウェア アップグレードが進行中の場合は、それが完了し、クラスタが完全に適合するまでクラスタへの他の変更はしないでください。
- Cisco APIC を移動する際は、最初に正常なクラスタがあることを確認します。Cisco APIC クラスタの状態を確認するには、後にシャットダウンする Cisco APIC を選択します。Cisco APIC をシャットダウンした後、Cisco APIC に移動し、再接続して、電源を入れます。GUI から、クラスタ内のすべてのコントローラが完全に適合状態に戻すことを確認します。



- (注) 一度に1つの Cisco APIC のみ移動します。

- Cisco APIC クラスタが2つ以上のグループに分割されると、ノードの ID が変更され、その変更はすべての Cisco APIC で同期されません。これにより、Cisco APIC との間のノード ID で不整合が発生する可能性があります。また、影響を受けるリーフ ノードも Cisco APIC GUI のインベントリに表示されないことがあります。Cisco APIC クラスタを分割すると、Cisco APIC からの影響を受けるリーフ ノードの使用停止し、ここでも登録するため、ノード ID の矛盾が解決されると、クラスタ内の APIC のヘルス ステータスが完全に適合状態ではしまず。
- Cisco APIC クラスタを設定する前に、すべての Cisco APIC のパフォーマンスが同じファームウェアバージョンを実行していることを確認します。異なるバージョンを実行して Cisco APIC のパフォーマンスの最初のクラスタ リングはサポートされていない動作し、クラスタ内の問題が発生する可能性があります。

ここでは、次の内容について説明します。

## Cold Standby について (Cisco APIC クラスタ用)

Cold Standby 機能 Cisco Application Policy Infrastructure Controller (APIC クラスタ用) を使用すれば、クラスタ内の Cisco APIC をアクティブ/スタンバイモードで運用できます。Cisco APIC クラスタでは、指定されたアクティブ状態の Cisco APIC は負荷を共有し、指定されたスタンバイ状態の Cisco APIC はアクティブなクラスタ内の任意の Cisco APIC の置き換えとして動作することができます。

管理者ユーザーとして、Cisco APIC が初めて起動したときに Cold Standby 機能をセットアップできます。クラスタ内には少なくとも 3 基のアクティブ状態の Cisco APIC があり、1 基以上のスタンバイ状態の Cisco APIC があるようにすることを推奨します。管理者ユーザーとして、アクティブな Cisco APIC をスタンバイ状態の Cisco APIC で置き換えるには、切り替えを開始できます。

### 特記事項

- スタンバイ Cisco APIC を追加するには 3 つのアクティブ Cisco APIC が必要です。
- スタンバイ Cisco APIC は、初期セットアップ中にスタンバイ Cisco APIC がクラスタに参加するときに、クラスタの同じファームウェアバージョンで実行する必要があります。
- アップグレードプロセス中に、Cisco APIC のすべてのアクティブなパフォーマンスをアップグレードすると、スタンバイ Cisco APIC もありますが自動的にアップグレードします。
- 初期設定時に、スタンバイ Cisco APIC に ID が割り当てられます。スタンバイ Cisco APIC がアクティブ Cisco APIC に切り替えられた後、スタンバイ Cisco APIC (新しくアクティブになった) は、置き換えられた (前にアクティブだった) Cisco APIC の ID の使用を開始します。
- 管理者ログインはスタンバイ Cisco APIC で有効ではありません。Cold Standby Cisco APIC をトラブルシューティングをするには、*rescue-user* として SSH を使用して、スタンバイにログインする必要があります。
- 切り替え中、置き換えられたアクティブ Cisco APIC は、置き換えられた Cisco APIC への接続を防ぐため、電源オフにする必要があります。
- 次の条件が失敗する経路でスイッチします。
  - スタンバイ Cisco APIC に接続がない場合。
  - スタンバイ Cisco APIC のファームウェアのバージョンがアクティブ クラスタと同じではない場合。
- スタンバイ Cisco APIC をアクティブに切り替えた後、必要に応じて別のスタンバイ Cisco APIC をセットアップできます。
- **[スタンバイ (新しいアクティブ) の OOB IP アドレスを保持する (Retain OOB IP address for Standby (new active)) ]** がオンになっている場合、スタンバイ (新しいアクティブ) APIC は元のスタンバイ OOB 管理 IP アドレスを保持します。

- [スタンバイ (新しいアクティブ) の OOB IP アドレスを保持する (Retain OOB IP address for Standby (new active))] がオンでない場合：
  - アクティブな APIC が 1 つだけダウンしている場合: スタンバイ (新しいアクティブ) Cisco APIC は、古いアクティブ Cisco APIC の OOB 管理 IP アドレスを使用します。
  - 複数のアクティブ Cisco APIC がダウンしている場合：スタンバイ (新しいアクティブ) Cisco APIC は、アクティブな APIC の OOB 管理 IP アドレスを使用しようとしませんが、アクティブな APIC の OOB 管理 IP アドレス構成のシャードがマイノリティ状態にある場合は失敗する可能性があります。
- Cisco ACI マルチポッドについては、古いアクティブ Cisco APIC とスタンバイ Cisco APIC が異なる OOB 管理 IP サブネットを使用している場合、スタンバイ (新しいアクティブ) では、Cisco APIC が元のスタンバイ OOB 管理 IP アドレスを保持するオプションをオンにする必要があります。そうしないと、スタンバイ (新しいアクティブ) Cisco APIC への OOB 管理 IP 接続が失われます。この状況は、古いアクティブ Cisco APIC とスタンバイ Cisco APIC が異なるポッドにある場合に発生する可能性があります。
 

この理由で OOB 管理 IP 接続が失われた場合、または複数のアクティブ Cisco APIC がダウンしている場合は、新しい静的ノード管理 OOB IP アドレスを作成して、新しいアクティブ (以前はスタンバイ) APIC OOB 管理 IP アドレスを変更する必要があります。構成を変更するには、クラスタのマイノリティ状態を解除する必要があることに注意してください。
- スタンバイ Cisco APIC はポリシー設定または管理で関係しません。
- 管理者クレデンシャルを持っている場合でも、スタンバイ Cisco APIC に情報が複製されることはありません。

## メンテナンス モード

メンテナンス モードを使用する際に理解に役立つ用語を紹介します。

- **グレースフル挿入と削除 (GIR)** : ユーザー トラフィックからスイッチを分離するために使用される操作。
- **メンテナンス モード** : デバッグ目的でユーザー トラフィックからスイッチを分離するために使用されます。APIC GUI の [ファブリック メンバーシップ] ページの [メンテナンス (GIR)] フィールドを有効にすることにより、メンテナンス モードにスイッチを入れることができます。これは、[ファブリック]>[インベントリ]>[ファブリック メンバーシップ] (スイッチを右クリックして、[メンテナンス (GIR)] を選択する) にあります。

スイッチをメンテナンス モードにすると、そのスイッチは動作可能な ACI ファブリック インフラストラクチャの一部とは見なされず、通常の APIC 通信は受け入れられません。したがって、この状態にあるスイッチのファームウェアアップグレードを実行しようとすると、障害が発生したり、不完全なステータスで無限にスタックしたりする可能性があるため、この状態のスイッチに対するファームウェアアップグレードの実行はサポートされていません。

メンテナンスモードでは、最小限のサービスの中断でネットワークからのスイッチを分離できます。メンテナンスモードでトラフィックに影響を与えることなくリアルタイムのデバッグを実行することができます。

メンテナンスモードを使用してスイッチを正常に取り出し、そのスイッチをネットワークから分離して、デバッグ操作を実行することができます。スイッチは、最小限のトラフィックの中断だけで、通常の転送パスから取り外されます。

正常に削除、外部のすべてのプロトコルが適切に電源を切るファブリック プロトコル (IS-IS) を除くと、スイッチは、ネットワークから切り離します。メンテナンスモード時に、最大メトリックは IS-IS 内でアダプタイズ、Cisco Application Centric Infrastructure ( Cisco ACI ) ファブリックおよびそのため、メンテナンス モードがスパインスイッチからのトラフィックをひく点されません。さらに、スイッチの前面パネルのすべてのインターフェイスが、スイッチファブリック インターフェイスを除いてシャット ダウンされます。デバッグ操作後にスイッチを完全動作 (通常) モードに戻すには、スイッチをリコミッショニングさせる必要があります。この操作により、スイッチのステートレス リロードがトリガーされます。

グレースフルの挿入で、スイッチは自動的にデコミッショニング、再起動、およびリコミッショニングされます。リコミッショニングが完了したら、外部のすべてのプロトコルを復元し、IS-IS で最大のメトリックは 10 分後にリセットされます。

次のプロトコルがサポートされています。

- Border Gateway Protocol (BGP)
- Enhanced Interior Gateway Routing Protocol (EIGRP)
- Intermediate System-to-Intermediate System (IS-IS)
- Open Shortest Path First (OSPF)
- リンク集約制御プロトコル (LACP)

プロトコルに依存しないマルチキャスト (PIM) はサポートされていません。

### 特記事項

- 境界リーフ スイッチに静的ルートがあり、メンテナンス モードがある場合、境界リーフ スイッチからのルートは ACI ファブリックにあるルーティング テーブルから削除されない可能性があり、ルーティングの問題が発生します。

この問題を回避するには、次のいずれかを実行します。

- その他の境界リーフ スイッチで同じ管理ディスタンスを持つ同じ静的ルートを設定するか、
  - 静的ルートの次のホップへの到達性を追跡するため IP SLA または BFD を使用します
- アップグレードまたはダウン グレード メンテナンス モードでスイッチがサポートされていません。

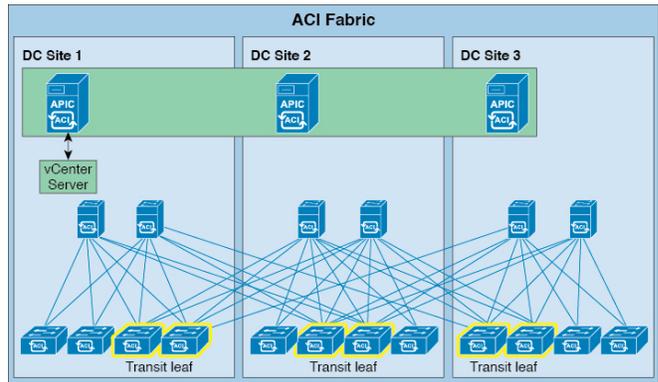
- イーサネット ポート モジュールでは、インターフェイスを増殖停止、スイッチは、メンテナンスモードでは、通知に関連します。その結果、リモートスイッチを再起動するか、またはこの時間中にファブリック リンクかを調べますは、ファブリック リンクはありません確立した後で、スイッチがリブート手動でない限り (を使用して、 **acidiag タッチ クリーン** コマンド)、廃棄、および recommissioned。
- スイッチがメンテナンスモード中の場合、スイッチの CLI 「show」 コマンドでは、前面パネル ポートがアップ状態であり、BGP プロトコルがアップ状態かつ実行中であることを示します。インターフェイスは実際にシャットダウンされ、BGP のその他すべての隣接関係がダウンしますが、表示されているアクティブ状態でデバッグが可能です。
- 複数のポッドの 再配布されたルートのメトリックを IS-IS 63 未満に設定する必要があります。設定を 再配布されたルートのメトリックを IS-IS 、選択 ファブリック > ファブリック ポリシー > ポッド ポリシー > IS-IS ポリシー 。
- 既存の登場させには、すべてのレイヤ3トラフィック迂回がサポートされています。LACP でレイヤ2のすべてのトラフィックは、冗長ノードを迂回も。ノードは、メンテナンスモードに入ります、されるとすぐに、ノードで実行されている LACP は、不要になった集約できるようにポートチャネルの一部としてネイバーを通知します。すべてのトラフィックは vPC ピア ノードを迂回します。

## ストレッチ ACI ファブリックの設計の概要

ストレッチ ACI ファブリックは、複数の場所に分散された ACI リーフおよびスパイン スイッチを接続する部分的にメッシュ化された設計です。通常、ACI ファブリックの実装は、フルメッシュ設計がファブリック内の各リーフスイッチを各スパインスイッチに接続する単一のサイトであり、最高のスループットとコンバージェンスが得られます。マルチサイトのシナリオでは、フルメッシュ接続が不可能であるか、コストがかかりすぎる可能性があります。複数のサイト、建物、または部屋が、十分なファイバ接続ではサービスを提供できない距離にまたがる場合や、サイト全体の各リーフスイッチを各スパインスイッチに接続するにはコストがかかりすぎる場合があります。

次の図にストレッチ ファブリック トポロジを示します。

図 4: ACI ストレッチ ファブリック トポロジ



ストレッチ ファブリックは単一の ACI ファブリックです。サイトには 1 つの管理ドメインおよび 1 つの可用性ゾーンがあります。管理者は、サイトを 1 つのエンティティとして管理できます。APIC コントローラ ノードで行われた構成変更は、サイト全体のデバイスに適用されます。ストレッチされた ACI ファブリックは、サイト間でのライブ VM 移行機能を保持します。ACI ストレッチ ファブリックの設計は検証されており、相互接続された最大 3 つのサイトでサポートされています。

ACI ストレッチ ファブリックは、基本的に、さまざまな場所に広がる「ストレッチ ポッド」を表します。ACI マルチポッドアーキテクチャを備えた ACI リリース 2.0(1) 以降、さまざまな場所に分散して ACI ファブリックを展開するための、より堅牢で回復力のある（推奨される）方法が提供されています。詳細については、次のホワイトペーパーを参照してください。

<https://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/application-centric-infrastructure/white-paper-c11-737855.html>

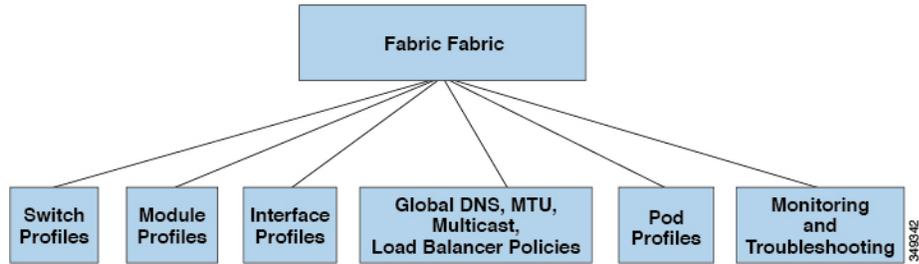
## ストレッチ ACI ファブリック 関連ドキュメント

KB ストレッチ ACI ファブリック 設計の概要 テクニカルノートは、トラフィックフロー、APIC クラスターの冗長性、および複数のサイトにまたがる ACI ファブリックを実装するための運用上の考慮事項に関する設計ガイドラインを提供します。

## ファブリック ポリシーの概要

ファブリック ポリシーは、内部のファブリック インターフェイスの操作を管理し、スパイン およびリーフスイッチを接続するさまざまな機能、プロトコル、およびインターフェイスの構成を可能にします。ファブリックの管理者権限を持つ管理者は、要件に応じて新しいファブリック ポリシーを作成できます。APIC では、管理者はファブリック ポリシーを適用するポッド、スイッチおよびインターフェイスを選択できます。次の図は、ファブリックのポリシーモデルの概要を示します。

図 5: ファブリック ポリシーの概要



ファブリック ポリシーは、次のカテゴリにグループ化されます。

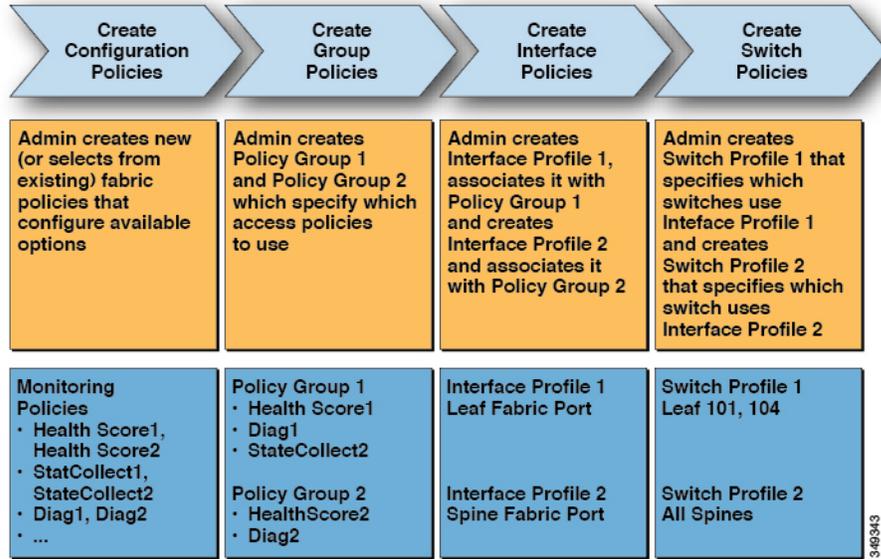
- スイッチプロファイルは、構成するスイッチとスイッチの構成ポリシーを指定します。
- モジュールプロファイルは、構成するスパインスイッチモジュールとスパインスイッチの構成ポリシーを指定します。
- インターフェイスプロファイルは、構成するファブリック インターフェイスとインターフェイスの構成ポリシーを指定します。
- グローバルポリシーは、DNS、ファブリック MTU のデフォルト、マルチキャストツリー、およびファブリック全体で使用するロードバランサの構成を指定します。
- ポッドプロファイルは、日付と時刻、SNMP、Council of Oracle Protocol (COOP)、IS-IS、および Border Gateway Protocol (BGP) ルートリフレクタポリシーを指定します。
- モニタリングおよびトラブルシューティングのポリシーは、モニタする対象、しきい値、障害とログの処理方法、および診断方法を指定します。

## ファブリック ポリシーの構成

ファブリック ポリシーは、スパインおよびリーフスイッチに接続するインターフェイスを構成します。ファブリックポリシーは、モニタリング（統計の収集および統計のエクスポート）、トラブルシューティング（オンデマンド診断とSPAN）、IS-IS、Council of Oracle Protocol (COOP)、SNMP、境界ゲートウェイプロトコル (BGP) のルートリフレクタ、DNS、またはネットワークタイムプロトコル (NTP) などの機能を有効にできます。

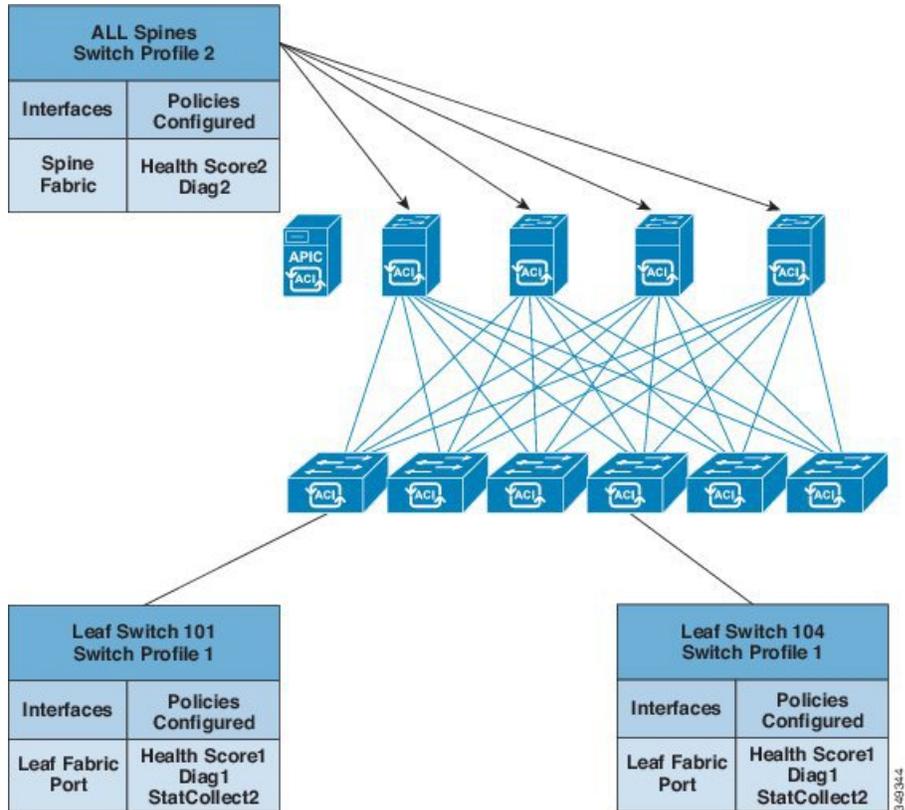
ファブリック全体で構成を適用するには、管理者がポリシーの定義済みグループをスイッチ上のインターフェイスに単一段階で関連付けます。このようにして、ファブリック上の多数のインターフェイスを一度に構成できます。1 個のポートを一度に構成することはスケーラブルではありません。次の図は、ACIファブリックを構成するプロセスがどのように動作するかを示します。

図 6: ファブリック ポリシーの構成プロセス



次の図は、ACI ファブリックにスイッチ プロファイル 1 およびスイッチ プロファイル 2 を適用した結果を示します。

図 7: ファブリック スイッチ ポリシーの適用



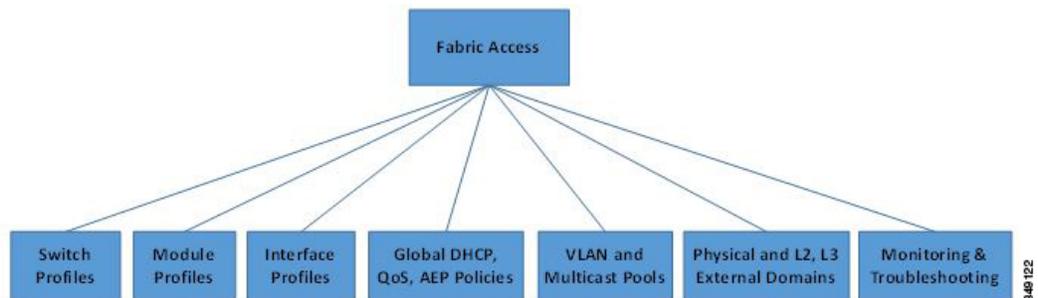
インフラストラクチャと範囲を組み合わせることにより、管理者はスケーラブルな方法でファブリック構成を管理することができます。これらの設定は、REST API、CLI、または GUI を使用して実行できます。GUI 内の [クイック スタート インターフェイス (Quick Start Interface)] 構成ウィザードでは、そのようなポリシーの実行に必要な基盤となるオブジェクトが自動的に作成されます。

## アクセスポリシーの概要

アクセスポリシーは、仮想マシンコントローラおよびハイパーバイザなどのデバイスに接続する外向きインターフェイス、ホスト、ネットワーク接続ストレージ、ルータ、またはファブリックエクステンダ (FEX) インターフェイスを構成します。アクセスポリシーにより、ポートチャネルおよび仮想ポートチャネル、Link Layer Discovery Protocol (LLDP)、Cisco Discovery Protocol (CDP)、または Link Aggregation Control Protocol (LACP) などのプロトコル、および統計収集、監視、および診断などの機能の構成が可能になります。

次の図は、アクセスポリシー モデルの概要を示します。

図 8: アクセスポリシー モデルの概要



アクセスポリシーは、次のカテゴリにグループ化されます。

- スイッチ プロファイルは、構成するスイッチとスイッチの構成ポリシーを指定します。
- モジュール プロファイルは、構成するリーフスイッチのアクセスカードおよびアクセスモジュールとリーフスイッチの構成ポリシーを指定します。
- インターフェイス プロファイルは、構成するアクセス インターフェイスとインターフェイスの構成ポリシーを指定します。
- グローバルポリシーにより、ファブリック全体に使用できる DHCP、QoS、および接続可能アクセス エンティティ (AEP) のプロファイル機能の構成が可能になります。AEP プロファイルは、リーフポートの大規模セットでハイパーバイザポリシーを展開するためのテンプレートを提供し、仮想マシン管理 (VMM) のドメインと物理ネットワークインフラストラクチャを関連付けます。また、レイヤ2およびレイヤ3の外部ネットワークの接続にも必要となります。
- プールは、VLAN、VXLAN およびマルチキャストアドレスプールを指定します。プールは共有リソースで、VMMなどの複数のドメインおよびレイヤ4～レイヤ7のサービスで

消費できます。プールは、さまざまなトラフィックのカプセル化 ID を表します（たとえば、VLAN ID、VNID、マルチキャストアドレスなど）。

- 物理および外部ドメイン ポリシーには、次のものが含まれます。
  - 外部ブリッジドメインのレイヤ2 ドメインプロファイルには、ファブリックに接続されたブリッジレイヤ2 ネットワークが使用するポートおよび VLAN の仕様が含まれます。
  - 外部ルーテッドドメインのレイヤ3 ドメインプロファイルには、ファブリックに接続されたルーテッドレイヤ3 ネットワークが使用するポートおよび VLAN の仕様が含まれます。
  - 物理ドメイン ポリシーには、テナントまたはエンドポイント グループで使用されるポートや VLAN などの物理インフラストラクチャの仕様が含まれます。
- モニタリングおよびトラブルシューティングのポリシーは、モニタする対象、しきい値、障害とログの処理方法、および診断方法を指定します。

## アクセス ポリシーの構成

アクセスポリシーは、スパインスイッチに接続していない外向きインターフェイスを構成します。外向きインターフェイスは、仮想マシンコントローラなどの外部デバイス、ハイパーバイザ、ホスト、ルータ、または Fabric Extender (FEX; ファブリックエクステンダ) と接続します。アクセスポリシーにより、管理者はポートチャネルおよび仮想ポートチャネル、LLDP、CDP、LACP などのプロトコル、モニタリングや診断などの機能を設定することができます。

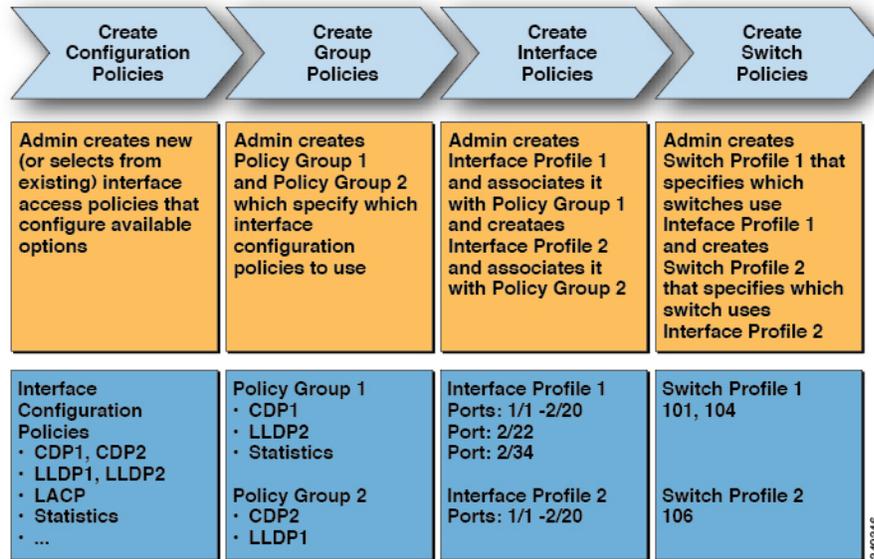
スイッチインターフェイス用のサンプル XML ポリシー、ポートチャネル、仮想ポートチャネル、およびインターフェイスの変更のスピードについては、『Cisco APIC Rest API 構成ガイド』に記載されています。



- (注) テナント ネットワーク ポリシーがファブリックのアクセスポリシーと別に構成される一方で、依存する基盤となるアクセスポリシーが整わないとテナント ポリシーはアクティブ化されません。

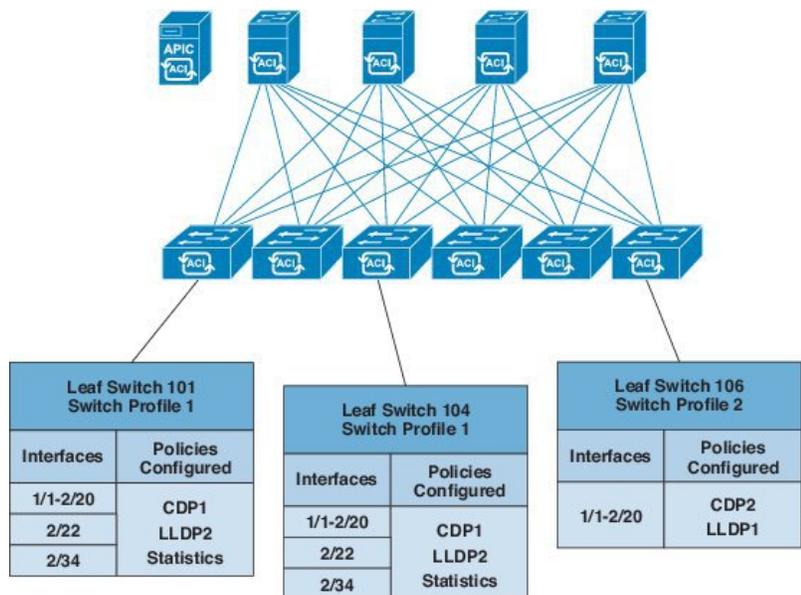
潜在的に多数のスイッチ間で構成を適用するためには、管理者は、単一のポリシーグループのインターフェイス構成を関連付けるスイッチプロファイルを定義します。このようにして、ファブリック上の多数のインターフェイスを一度に構成できます。スイッチプロファイルには、複数のスイッチに対する対称構成や一意の特殊用途構成を含めることができます。次の図は、ACI ファブリックへのアクセス構成のプロセスを示します。

図 9: アクセス ポリシーの構成プロセス



次の図は、ACI ファブリックにスイッチ プロファイル 1 およびスイッチ プロファイル 2 を適用した結果を示します。

図 10: アクセススイッチ ポリシーの適用



インフラストラクチャと範囲を組み合わせることにより、管理者はスケーラブルな方法でファブリック構成を管理することができます。これらの設定は、REST API、CLI、または GUI を使用して実行できます。GUI 内の [クイック スタート インターフェイス (Quick Start Interface)]、[PC]、[VPC 構成 (VPC Configuration)] ウィザードでは、そのようなポリシーの実行に必要な基盤となるオブジェクトが自動的に作成されます。

## ポートチャネルと仮想ポートチャネル アクセス

アクセスポリシーにより、管理者はポートチャネルと仮想ポートチャネルを構成できます。スイッチ インターフェイス用のサンプル XML ポリシー、ポートチャネル、仮想ポートチャネル、およびインターフェイスの変更のスピードについては、『Cisco APIC Rest API 構成ガイド』に記載されています。

## 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。

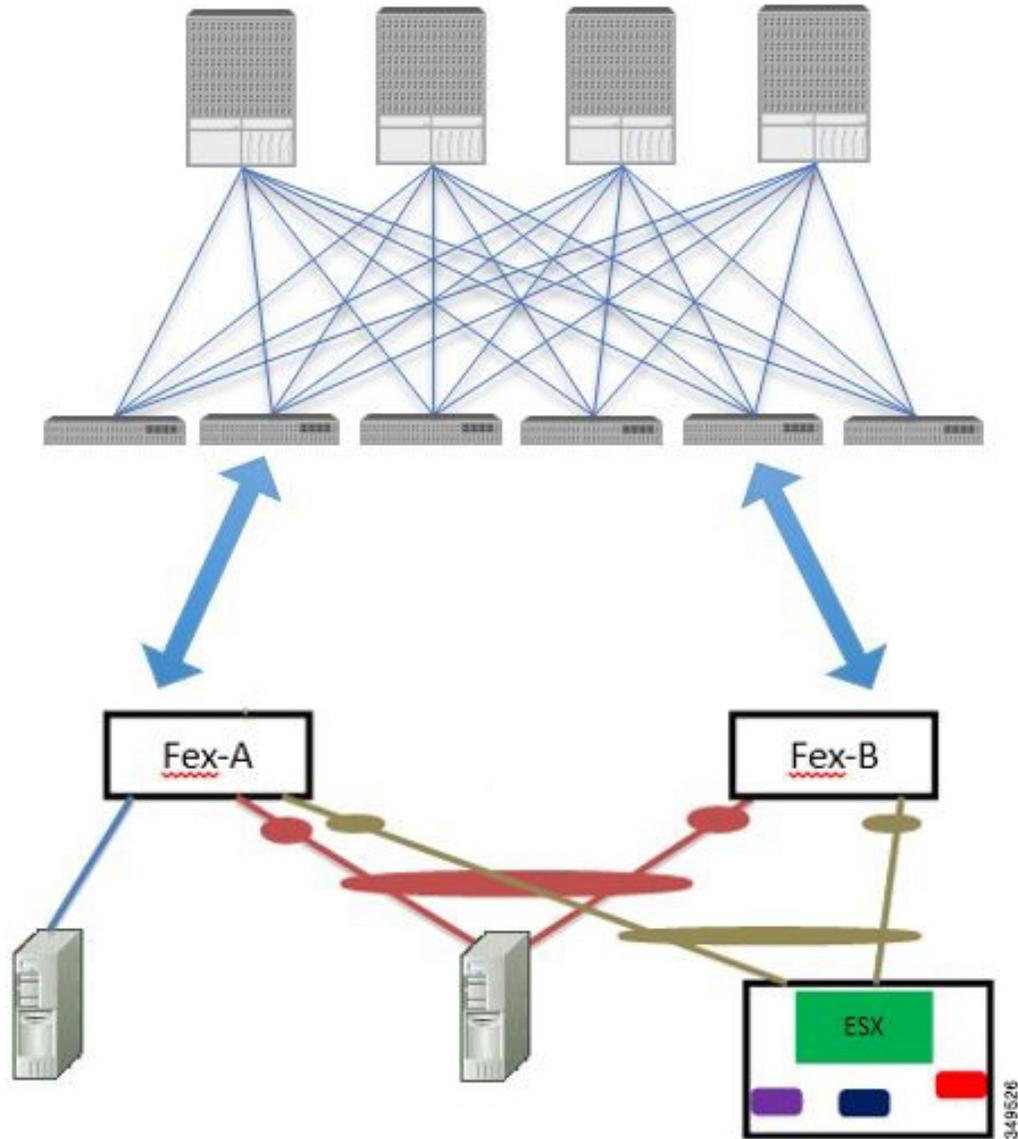


(注) 2 台のリーフ スイッチ間で vPC ドメインを作成する場合、以下のいずれかの方法によって、両スイッチの世代を一致させる必要があります。

- 1: なしで Cisco Nexus N9K スイッチの生成」EX」または「FX」、スイッチ名前末尾にたとえば、N9K 9312TX
- 2: Cisco Nexus N9K スイッチ間での生成」EX」または「FX」スイッチ モデルの名前の末尾にたとえば、N9K-93108TC-EX

これら 2 つのスイッチは互換性のある vPC ピアではありません。代わりに、同じ世代のスイッチを使用してください。

図 11: 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 チャンネル 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。vPC はポートチャンネルでのみサポートされます)。



- (注) GAAP 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 n.jpy への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 (GRAP-based Detection)] を、ブリッジドメインウィザードの [L3 設定 (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。

## ファイバチャネル、または FCoE

ファイバチャネルおよび FCoE 構成情報については、『Cisco APIC Layer 2 Networking Configuration Guide』を参照してください。

## Cisco ACI ファブリックでの Fibre Channel over Ethernet トラフィックのサポート

Cisco Application Centric Infrastructure (ACI) では、Cisco ACI ファブリック上の Fibre Channel over Ethernet (FCoE) に対するサポートを設定して、管理することができます。

FCoE は、ファイバチャネルパケットをイーサネットパケット内にカプセル化するプロトコルです。これにより、ストレージトラフィックをファイバチャネル SAN とイーサネットネットワーク間でシームレスに移動できます。

Cisco ACI ファブリックで FCoE プロトコルのサポートを標準実装することにより、イーサネットベースの Cisco ACI ファブリックに配置されているホストが、ファイバチャネルネットワークに配置されている SAN ストレージデバイスと通信できます。ホストは、Cisco ACI リーフスイッチに展開された仮想 F ポートを介して接続しています。SAN ストレージデバイスとファイバチャネルネットワークは、ファイバチャネルフォワーディング (FCF) ブリッジおよび仮想 NP ポートを介して Cisco ACI ファブリックに接続されます。このポートは、仮想 F ポートと同じ Cisco ACI リーフスイッチに導入されます。仮想 NP ポートおよび仮想 F ポートも汎用的に仮想ファイバチャネル (vFC) ポートと呼ばれます。

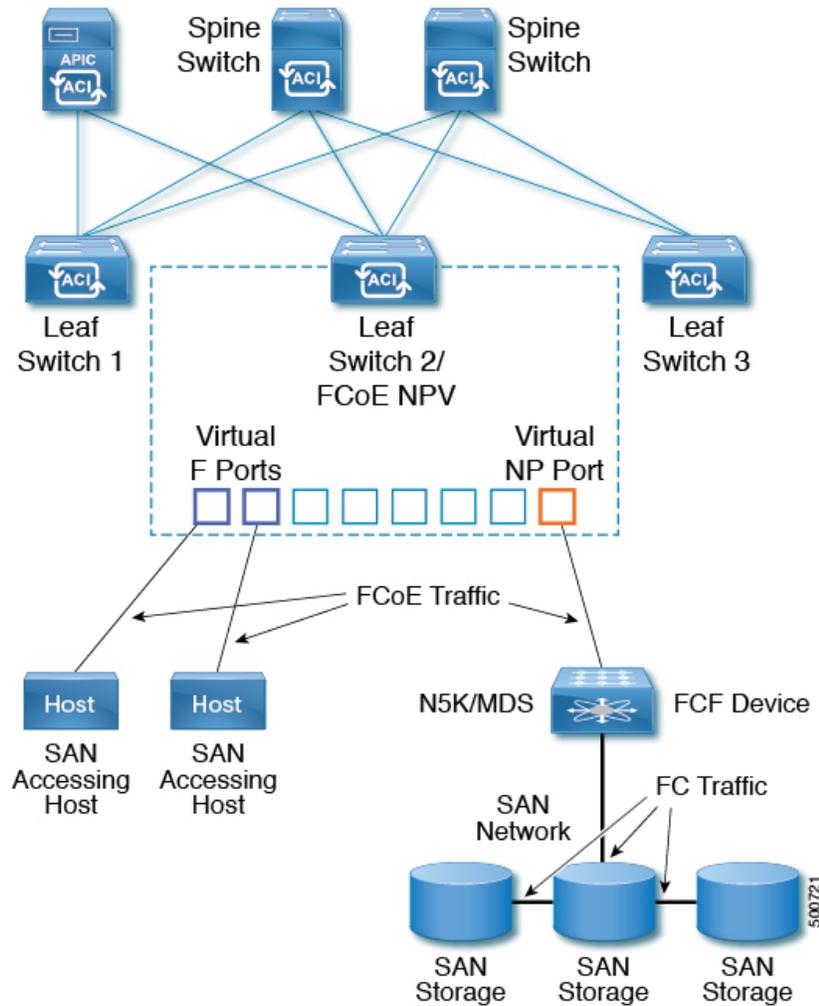


- (注) FCoE トポロジにおける Cisco ACI リーフスイッチの役割は、ローカル接続された SAN ホストとローカル接続された FCF デバイスの間で、FCoE トラフィックのパスを提供することです。リーフスイッチでは SAN ホスト間のローカルスイッチングは行われず、FCoE トラフィックはスパインスイッチに転送されません。

### Cisco ACI を介した FCoE トラフィックをサポートするトポロジ

Cisco ACIファブリック経由のFCoEトラフィックをサポートする一般的な設定のトポロジは、次のコンポーネントで構成されます。

図 12: Cisco ACI FCoE トラフィックをサポートするトポロジ



- NPV バックボーンとして機能するようにファイバチャネル SAN ポリシーを通して設定されている 1 つ以上の Cisco ACI リーフ スイッチ。
- 仮想 F ポートとして機能するように設定された NPV 設定リーフ スイッチ上で選択された インターフェイス。SAN 管理アプリケーションまたは SAN を使用しているアプリケーションを実行しているホストとの間を往来する FCoE トラフィックの調整を行います。
- 仮想 NP ポートとして機能するように設定された NPV 設定リーフ スイッチ上で選択された インターフェイス。ファイバチャネル転送 (FCF) ブリッジとの間を往来する FCoE トラフィックの調整を行います。

FCFブリッジは、通常 SAN ストレージデバイスを接続しているファイバチャネルリンクからファイバチャネルトラフィックを受信し、ファイバチャネルパケットを FCoE フレームにカプセル化して、Cisco ACI ファブリック経由で SAN 管理ホストまたは SAN データ消費ホストに送信します。FCoE トラフィックを受信し、ファイバチャネルに再パッケージしてファイバチャネル ネットワーク経由で伝送します。



- (注) 前掲の Cisco ACI トポロジでは、FCoE トラフィックのサポートには、ホストと仮想 F ポート間の直接接続、および、FCF デバイスと仮想 NP ポート間の直接接続が必要です。

Cisco Application Policy Infrastructure Controller (APIC) サーバーは、Cisco APIC GUI、NX-OS スタイルの CLI、または REST API へのアプリケーションコールを使用して、FCoE トラフィックを設定およびモニタできます。

### FCoE の初期化をサポートするトポロジ

FCoE トラフィックフローが説明の通り機能するためには、別の VLAN 接続を設定する必要があります。SAN ホストはこの接続を経由して、FCoE 初期化プロトコル (FIP) パケットをブロードキャストし、F ポートとして有効にされているインターフェイスを検出します。

### vFC インターフェイス設定ルール

Cisco APIC GUI、NX-OS スタイル CLI、または REST API のいずれを使用して vFC ネットワークと EPG の導入を設定する場合でも、次の一般的なルールがプラットフォーム全体に適用されます。

- F ポートモードは、vFC ポートのデフォルトモードです。NP ポートモードは、インターフェイスポリシーで具体的に設定する必要があります。
- デフォルトのロードバランシングモードはリーフスイッチ、またはインターフェイスレベル vFC 設定が `src dst ox id`。
- ブリッジドメインごとに 1 つの VSAN 割り当てがサポートされます。
- VSAN プールおよび VLAN プールの割り当てモードは、常にスタティックである必要があります。
- vFC ポートでは、VLAN にマッピングされている VSAN を含む VSAN ドメイン (ファイバチャネルドメインとも呼ばれます) との関連付けが必要です。

## ファイバチャネル接続の概要

Cisco ACI では、N ポート仮想化 (NPV) モードを使用したリーフスイッチでのファイバチャネル (FC) 接続がサポートされています。NPV により、スイッチにおいて、ローカル接続されたホストポート (N ポート) からの FC トラフィックをノードプロキシ (NP ポート) アプリックに集約して、コアスイッチに送ることができます。

スイッチは、NPV を有効にした後はNPV モードになります。NPV モードはスイッチ全体に適用されます。NPV モードのスイッチに接続するエンド デバイスはそれぞれ、この機能を使用するためにNポートとしてログインする必要があります（ループ接続デバイスはサポートされていません）。（NPV モードの）エッジスイッチからNPV コアスイッチへのすべてのリンクは、（Eポートではなく）NPポートとして確立されます。このポートは、通常のスイッチ間リンクに使用されます。



- (注) FC NPV アプリケーションにおける ACI リーフ スイッチの役割は、ローカル接続された SAN ホストとローカル接続されたコアスイッチ間のFCトラフィックのパスを提供することです。リーフ スイッチでは SAN ホスト間のローカル スイッチングは行われず、FC トラフィックはスパイン スイッチに転送されません。

### FC NPV の利点

FC NPV では次の機能を提供します。

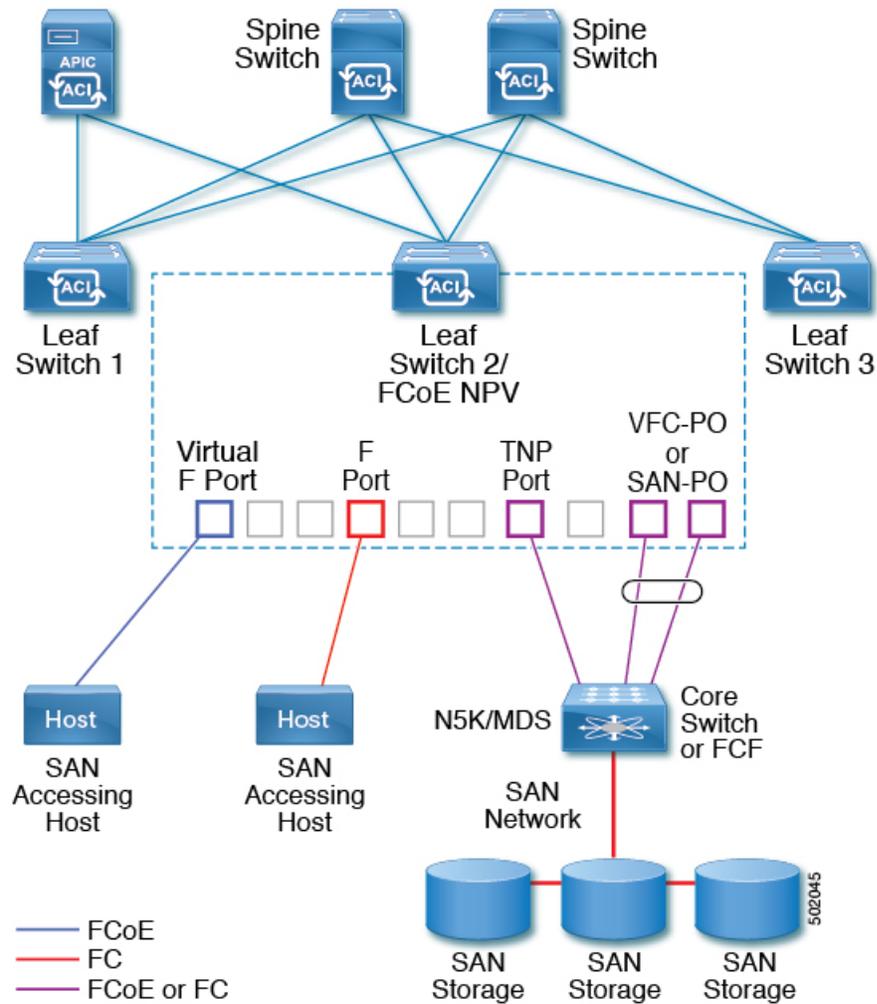
- ファブリックでドメイン ID を追加しなくても、ファブリックに接続するホスト数が増加します。NPV のコアスイッチのドメイン ID は、複数の NPV スイッチ間で共有されます。
- FC ホストと FCoE ホストは、ネイティブの FC インターフェイスを使用して SAN ファブリックに接続します。
- トラフィックの自動マッピングによるロード バランシング。NPV に接続しているサーバを新しく追加した場合に、トラフィックが現在のトラフィック負荷に基づいて、外部のアップリンク間で自動的に分散されます。
- トラフィックの静的マッピング。NPV に接続しているサーバを、外部のアップリンクに静的にマッピングすることができます。

### FC NPV モード

ACI の Feature-set fcoe-npv は、最初に FCoE/FC 設定がプッシュされるときに、デフォルトで自動的に有効になります。

### FC トポロジ

ACI ファブリック経由の FC トラフィックをサポートするさまざまな設定のトポロジを、次の図に示します。



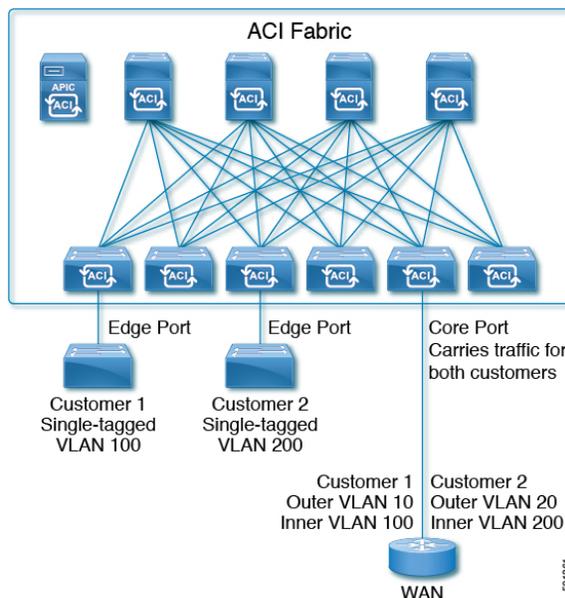
- ACI リーフスイッチ上のサーバー/ストレージホストインターフェイスは、ネイティブの FC ポートか仮想 FC (FCoE) ポートのどちらかとして機能するように設定できます。
- FC コアスイッチへのアップリンクインターフェイスは、次のいずれかのポートタイプとして設定できます。
  - ネイティブ FC NP ポート
  - SAN-PO NP ポート
- FCF スイッチへのアップリンク インターフェイスは、次のいずれかのポートタイプとして設定できます。
  - 仮想 (vFC) NP ポート
  - vFC-PO NP ポート

- N ポート ID 仮想化 (NPIV) がサポートされており、デフォルトで有効になっています。そのため、単一のリンクを経由して N ポートに複数の N ポート ID またはファイバチャネル ID (FCID) を割り当てるのが可能です。
- コアスイッチへの NP ポートでは、トランキングを有効にすることができます。トランキングにより、ポートで複数の VSAN をサポートできます。トランク モードが有効になった NP ポートのことを、TNP ポートと呼びます。
- 複数の FC NP ポートを結合してコアスイッチへの SAN ポートチャネル (SAN-PO) とすることができます。トランキングは SAN ポートチャネルでサポートされます。
- FCF ポートでは 4/16/32 Gbps および自動速度設定がサポートされますが、ホストインターフェイスでは 8Gbps はサポートされません。デフォルトの速度は「auto」です。
- FC NP ポートでは、4/8/16/32 Gbps および自動速度設定がサポートされます。デフォルトの速度は「auto」です。
- Flogi に続く複数の FDISC (ネスト NPIV) は、FC/FCoE ホストと FC/FCoE NP リンクによってサポートされます。
- FEX の背後にある FCoE ホストは、FCoE NP/アップリンクを介してサポートされます。
- APIC 4.1(1) リリース以降、FEX の背後にある FCoE ホストは、ファイバチャネル NP/アップリンクを介してサポートされます。
- 1 つの FEX の背後にあるすべての FCoE ホストは、複数の vFC および vFC-PO アップリンク間、または単一のファイバチャネル/SAN ポートチャネルアップリンクを通じてロードバランシングできます。
- SAN ブートは、FEX で FCoE アップリンク経由でサポートされます。
- APIC 4.1(1) リリース以降、SAN ブートは FC/SAN-PO アップリンクでもサポートされます。
- SAN ブートは、FEX を介して接続された FCoE ホストの vPC を介してサポートされます。

# 802.1Q トンネル

## ACI 802.1 q トンネルについて

図 13: ACI 802.1 q トンネル



エッジ（トンネル）ポートで 802.1Q トンネルを設定して、Quality of Service（QoS）の優先順位設定とともに、ファブリックのイーサネットフレームの point-to-multi-point トンネリングを有効にできます。Dot1q トンネルは、タグなし、802.1Q タグ付き、802.1ad 二重タグ付きフレームを、ファブリックでそのまま送信します。各トンネルでは、単一の顧客からのトラフィックを伝送し、単一のブリッジドメインに関連付けられています。Cisco Application Centric Infrastructure（ACI）の前面パネルポートは、Dot1q トンネルの一部とすることができます。レイヤ 2 スイッチングは宛先 MAC（DMAC）に基づいて行われ、通常の MAC ラーニングはトンネルで行われます。エッジポート Dot1q トンネルは、スイッチモデル名の最後に「EX」またはそれ以降のサフィックスが付く、Cisco Nexus 9000 シリーズスイッチでサポートされます。

同じコアポートで複数の 802.1Q トンネルを設定することができ、複数の顧客からの二重タグ付きトラフィックを伝送できます。それぞれは、802.1Q トンネルごとに設定されたアクセスのカプセル化で識別されます。802.1Q トンネルでは、MAC アドレス学習を無効にすることもできます。エッジポートとコアポートの両方を、アクセスカプセル化が設定され、MAC アドレス学習が無効にされた 802.1Q トンネルに所属させることができます。エッジポートとコアポートの Dot1q トンネルは、スイッチモデル名の最後に「FX」またはそれ以降のサフィックスが付く、Cisco Nexus 9000 シリーズスイッチでサポートされます。

IGMP および MLD パケットは、802.1Q トンネルを介して転送できます。

このドキュメントで使用する用語は、Cisco Nexus 9000 シリーズのドキュメントとは異なっている場合があります。

表 1: 802.1Q トンネルの用語

ACI のドキュメント	Cisco Nexus 9000 シリーズのドキュメント
エッジポート	トンネルポート
コアポート	トランクポート

次の注意事項および制約事項が適用されます:

- VTP、CDP、LACP、LLDP、および STP プロトコルのレイヤ 2 トンネリングは、次の制限付きでサポートされます。
  - リンク集約制御プロトコル (LACP) トンネリングは、個々のリーフ インターフェイスを使用する、ポイントツーポイントトンネルでのみ、予想通りに機能します。ポートチャネル (PC) または仮想ポートチャネル (vPC) ではサポートされていません。
  - PC または vPC を持つ CDP および LLDP トンネリングは確定的ではありません。これは、トラフィックの宛先として選択するリンクによって異なります。
  - レイヤ 2 プロトコル トンネリングに VTP を使用するには、CDP をトンネル上で有効にする必要があります。
  - レイヤ 2 プロトコルのトンネリングが有効になっており、Dot1q トンネルのコアポートにブリッジドメインが展開されている場合、STP は 802.1Q トンネルブリッジドメインではサポートされません。
  - Cisco ACI リーフスイッチは、トンネルブリッジドメインのエンドポイントでフラッシングを行い、ブリッジドメインでフラッドिंगすることにより、STP TCN パケットに反応します。
  - 2 個上のインターフェイスを持つ CDP および LLDP トンネリングが、すべてのインターフェイスでパケットをフラッドिंगします。
  - エッジポートからコアポートにトンネリングしているレイヤ 2 プロトコルパケットの宛先 MAC アドレスは、01-00-0c-cd-cd-d0 に書き換えられ、コアポートからエッジポートにトンネリングしているレイヤ 2 プロトコルパケットの宛先 MAC アドレスは、プロトコルに対して標準のデフォルト MAC アドレスに書き換えられます。
- PC または vPC が Dot1q Tunnel 内の唯一のインターフェイスであり、削除してから再設定した場合には、PC/VPC の Dot1q トンネルへの関連付けを削除して、再設定してください。
- 製品 ID に EX が含まれるスイッチに導入された 802.1Q トンネルでは、最初の 2 つの VLAN タグの 0x8100 + 0x8100、0x8100 + 0x88a8、0x88a8 + 0x88a8 の Ethertype の組み合わせはサポートされません。

トンネルが EX と FX またはそれ以降のスイッチの組み合わせに導入されている場合は、この制限が適用されます。

製品 ID に FX 以降が含まれるスイッチにのみトンネルが導入されている場合、この制限は適用されません。

- コア ポートについては、二重タグつきフレームのイーサタイプは、0x8100 の後に 0x8100 が続く必要があります。
- 複数のエッジ ポートおよびコア ポートを（リーフ スイッチ上のものであっても）Dot1q トンネルに含めることができます。
- エッジ ポートは 1 つのトンネルの一部にのみ属することが可能ですが、コア ポートは複数の Dot1q トンネルに属することができます。
- 通常の EPG を 802.1Q で使用されるコア ポートに展開できます。
- L3Outs は、Dot1q トンネルで有効になっているインターフェイスではサポートされていません。
- FEX インターフェイスは Dot1q トンネル のメンバーとしてはサポートされていません。
- インターフェイス レベルの統計情報は Dot1q トンネル のインターフェイスでサポートされていますが、トンネル レベルの統計情報はサポートされていません。

## ダイナミック ブレイクアウト ポート

### ダイナミック ブレイクアウト ポートの設定

ブレイクアウトケーブルは非常に短いリンクに適しており、コスト効率の良いラック内および隣接ラック間を接続する方法を提供します。

ブレイクアウトでは、40 ギガビット (Gb) ポートを独立して 4 分割し、10Gb または 100Gb ポートを独立した状態で論理 25 Gb ポートに 4 分割できます。

ブレイクアウト ポートを設定する前に、次のケーブルのいずれかを使用して 40 Gb ポートを 4 つの 10 Gb ポートまたは 100 Gb ポートを 4 つの 25 Gb ポートに接続します。

- Cisco QSFP-4SFP10G
- Cisco QSFP-4SFP25G
- Cisco QSFP-4X10G-AOC
- MPO から、両端に QSFP-40G-SR4 および 4 X SFP-10G-SR を備えたブレイクアウト スプリッタ ケーブルへ
- MPO から、両端に QSFP-100G-SR4-S と 4 X SFP-25G-SR-S を備えたブレイクアウト スプリッタ ケーブルへ



(注) サポートされている光ファイバとケーブルについては、『Cisco Optics-to-Device Compatibility Matrix』を参照してください。

<https://tmgmatrix.cisco.com/>

40Gb から 10Gb へのダイナミック ブレークアウト機能は、次のスイッチのアクセス側ポートでサポートされます。

- N9K-C93180LC-EX
- N9K-C93180YC-FX
- N9K-C9336C-FX2
- N9K-C93360YC-FX2
- N9K-C93216TC-FX2
- N9K-C93108TC-FX3P (5.1(3) リリース以降)
- N9K-C93180YC-FX3 (5.1(3) リリース以降)
- N9K-C93600CD-GX (5.1(3) リリース以降)
- N9K-C9364C-GX (5.1(3) リリース以降)

100 Gb から 25 Gb までのブレークアウト機能は、次のスイッチのポートが面しているアクセスでサポートされています。

- N9K-C93180LC-EX
- N9K-C9336C-FX2
- N9K-C93180YC-FX
- N9K-C93360YC-FX2
- N9K-C93216TC-FX2
- N9K-C93108TC-FX3P (5.1(3) リリース以降)
- N9K-C93180YC-FX3 (5.1(3) リリース以降)
- N9K-C93600CD-GX (5.1(3) リリース以降)
- N9K-C9364C-GX (5.1(3) リリース以降)

次に示すガイドラインおよび制限事項に従ってください。

- ブレイクアウトポートは、ダウンリンクと変換されたダウンリンクでのみサポートされません。
- 次のスイッチは、プロファイルされた QSFP ポートでダイナミックブレークアウト（100Gb と 40Gb の両方）をサポートします。

- Cisco N9K-C93180YC-FX
- Cisco N9K-C93216TC-FX2
- Cisco N9K-C93360YC-FX2
- Cisco N9K-C93600CD-GX

これは、ポート 1/25 ～ 34 にのみ適用されます。ポートをダウンリンクに変換する場合、ポート 1/29 ～ 34 はダイナミック ブレークアウトに使用できます。

- Cisco N9K-C9336C-FX2

最大 34 のダイナミック ブレークアウトを構成できます。

- Cisco N9K-C9364C-GX (5.1(3) リリース以降)

1/1 ～ 59 の奇数番号のプロファイリングされた QSFP ポートで、最大 30 のダイナミック ブレークアウトを設定できます。

- Cisco N9K-93600CD-GX (5.1(3) リリース以降)

40/100G ポート x 24 から最大 12 のダイナミック ブレークアウトを設定でき、ポート 25 ～ 34 から最大 10 のダイナミック ブレークアウトを設定できます。ポートをダウンリンクに変換する場合、ポート 29 ～ 34 はダイナミック ブレークアウトに使用できます。最後の 2 つのポート (ポート 35 と 36) は、ファブリック リンク用に予約されています。

- Cisco N9K-C9336C-FX2 スイッチは、ブレークアウト サブポートで LACP fast hello をサポートします。
- ブレークアウト ポートは Cisco Application Policy Infrastructure Controller (APIC) 接続には使用できません。
- ファスト リンク フェールオーバー ポリシーは、ダイナミック ブレークアウト機能と同一ポートではサポートされていません。
- ブレークアウトのサポートは、ポリシー モデルが使用されているその他のポート タイプと同じ方法で使用できます。
- ポートがダイナミック ブレークアウトに対して有効になっている場合、親ポートのその他のポート (モニタリング ポリシー以外) は無効になります。
- ポートがダイナミック ブレークアウトに対して有効になっている場合、親ポートのその他の EPG 展開が無効になります。
- ブレークアウト サブポートは、ブレークアウト ポリシー グループを使用してもこれ以上分割することはできません。
- ブレークアウト サブポートは LACP をサポートします。デフォルトでは、「デフォルト」ポート チャネル メンバー ポリシーで定義された LACP 送信レート設定が使用されます。LACP 送信レートは、「デフォルト」ポート チャネル メンバー ポリシーを変更するか、各 PC/vPC インターフェイス ポリシー グループでのオーバーライド ポリシー グループを使用すれば、変更できます。

- ブレイクアウト サブポートを持つポート チャネルの LACP 送信レートを変更する必要がある場合、ブレークアウト サブポートを含むすべてのポート チャネルで同じ LACP 送信レート設定を使用することが必要です。オーバーライドポリシーを設定して、次のように送信レートを設定できます。
  1. デフォルトのポート チャネル メンバー ポリシーを設定/変更して、Fast Transmit Rate を含めます ([Fabric] > [Access Policies] > [Policies] > [Interface] > [Port Channel Member]) 。
  2. すべての PC/vPC インターフェイス ポリシー グループを設定して、上記のデフォルトポート チャネル メンバー ポリシーをオーバーライドポリシー グループに含めます ([Fabric] > [Access Policies] > [Interfaces] > [Leaf Interfaces] > [Policy Groups] > [PC/vPC Interface]) 。
- 次の注意事項および制約事項が Cisco N9K-C9364C-GX スイッチに適用されます。
  - 奇数番号のポート (行 1 および行 3) は、ブレークアウトをサポートします。隣接する偶数ポート (行 2 または行 4) は無効になります (「hw-disabled」)。これは、ポート 1/1 ~ 60 に適用されます。
  - 最後の 2 つのポート (1/63 と 64) は、ファブリック リンク用に予約されています。
  - ポート 1/61 と 62 はダウンリンク ポートに変換できますが、ブレークアウトはサポートされていません。ブレークアウトポートと 40/100G の非ブレークアウトポートは、1/1 ~ 4 または 1/5 ~ 8 など、1/1 から始まる 4 つのポートのセットに混在させることはできません。  
たとえば、ポート 1/1 がブレークアウト対応の場合、ポート 1/3 はブレークアウト対応またはネイティブ 10G で使用できます。ポート 1/3 が 40/100G の場合、error-disabled 状態になります。
  - ダウンリンクの最大数は、30 x 4ポート 10/25 (ブレークアウト) + 2 ポート (1/61 と 62) = 122ポートです。ポート 1/63 および 64 はファブリック リンク用に予約されており、1/2 ~ 60の偶数番号のポートは error-disabled になっています。
  - このスイッチは、すべてのポートで 10G with QSA をサポートします。ネイティブ 10G には QSA が必要です。
- 次の注意事項および制約事項が Cisco N9K-93600CD-GX スイッチに適用されます。
  - 奇数番号のポート (行 1 のすべてのポート) はブレークアウトをサポートします。行 2 の偶数番号のポートは無効になります (「hw-disabled」)。これは、ポート 1 ~ 24 にのみ適用されます。
  - ブレークアウトと 40/100G 非ブレークアウトは、1/1 ~ 4 または 1/5 ~ 8 など、1/1 から 1/24 までの 4 つのポートのセットに混在させることはできません。次に例を示します。
    - ポート 1/1 ~ 24 の場合、セットごとに 4 つのポートを使用できます。

たとえば、ポート 1/1 がブレイクアウト対応の場合、ポート 1/3 はブレイクアウト対応またはネイティブ 10Gで使用できます。ポート 1/3 が 40/100G の場合、`error-disabled` 状態になります。

- ポート 1/25 ~ 28 では、セットごとに 2 つのポートを使用できます。

たとえば、ポート 1/25 がブレイクアウト対応の場合でも、ポート 1/27 は 40/100G で使用できます。

- ダウンリンクの最大数は、12 x 4 ポート 10/25G (ブレイクアウト) + 10 x 4 ポート 10/25G (ブレイクアウト) = 88 ポートです。ポート 35 および 36 はファブリックリンク用に予約されており、12 個のポートは無効になっています。
- このスイッチは、すべてのポートで 10G with QSA をサポートします。ネイティブ 10G には QSA が必要です。

## 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 \(38 ページ\)](#) 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 ブレイクアウト (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。ブレイクアウト (**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。

### 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、次のガイドラインにご注意ください。

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、スイッチにログインし、 <code>setup-clean-config.sh -k</code> スクリプトを実行して、実行完了を待ちます。それから、リロードコマンドを入力します。 <code>-k</code> スクリプトオプションを使用すると、ポートプロファイルの設定がリロード後も維持され、追加のリポートが不要になります。

サブジェクト	ガイドライン
<p>最大アップリンク ポートの制限</p>	<p>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。</p> <p>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）。</p> <p>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。</p> <p>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。</p>

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	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> </ul>
N9K-C9336C-FX2-E	Cisco APIC 5.2(4) 以降	<ul style="list-style-type: none"> <li>• 40Gb および 100Gb のダイナミック ブレークアウトは、ポート 1 ~ 34 でサポートされます。</li> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> </ul>

スイッチ	リリース	制限事項
N9K-C9336C-FX2	Cisco APIC 4.2(4) 以降	<ul style="list-style-type: none"> <li>• 40Gb および 100Gb のダイナミック ブレークアウトは、ポート 1 ~ 34 でサポートされます。</li> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> </ul>
N9K-C9336C-FX2	Cisco APIC 3.2(1) 以降、ただし 4.2(4) は含まない	<ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。</li> <li>• 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。</li> </ul>

スイッチ	リリース	制限事項
N9K-C93180YC-FX	Cisco APIC 3.2(1) 以降	<ul style="list-style-type: none"> <li>• 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、次の手順を実行します。 <ul style="list-style-type: none"> <li>• 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。</li> <li>• 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。 <ul style="list-style-type: none"> <li>• APIC GUI で、[ファブリック]&gt; [インベントリ]&gt; [ポッド]&gt; [リーフ] に移動し、[シャーシ] クリックしてから [リロード] を選択します。</li> <li>• NX-OS スタイル CLI で、<b>setup-clean-config.sh -k</b> スクリプトを入力し、実行を待機し、<b>reload</b> コマンドを入力します。</li> </ul> </li> <li>• 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。</li> </ul> </li> <li>• 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。</li> </ul>
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

次の表では、アップリンクからダウンリンク、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の変換をサポートしているスイッチで、サポートされているアップリンクおよびダウンリンクをまとめています。

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 <sup>1</sup>	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(i)
N9K-C93180LC-EX	24 X 40 Gbps QSFP28 ダウンリンク (1-24)  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 (29-32)  または 12 X 100 Gbps QSFP28 ダウンリンク (1-24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 (29-32)	18 X 40 Gbps QSFP28 ダウンリンク (1-24)  6 X 40 Gbps QSFP28 アップリンク (1-24)  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 (29-32)  または 6 x 100 Gbps QSFP28 ダウンリンク (1-24の奇数)  6 x 100 Gbps QSFP28 アップリンク (1-24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 (29-32)	24 X 40 Gbps QSFP28 ダウンリンク (1-24)  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 (29-32)  または 12 X 100 Gbps QSFP28 ダウンリンク (1-24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 (29-32)	3.1(i)

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	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	3.1(1i)
		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 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)
N9K-C93108TC-EX <sup>2</sup> N9K-C93108TC-FX <sup>2</sup>	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

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	デフォルトのポート設定と同じ	3.2(i)
		18 x 40/100 Gbps QSFP28 アップリンク	34 X 40/100 Gbps QSFP28 ダウンリンク	3.2(3i)
		18 x 40/100 Gbps QSFP28 アップリンク	2 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	4.1
N9K-93240YC-FX2	48 x 10/25 Gbps ファイバ ダウンリンク  12 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	4.0(1)
		48 X 10/25 Gbps ファイバ アップリンク  12 X 40/100 Gbps QSFP28 アップリンク	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
N9K-C93216TC-FX2	96 X 10G BASE-T ダウンリンク  12 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	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

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-C93360YC-FX2	96 X 10/25 Gbps SFP28 ダウンリンク  12 X 40/100 Gbps 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  8 X 40/100/400 Gbps QSFP-DD アップリンク	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(2e)
N9K-C9364C-GX	48/40/100 Gbps QSFP28 ダウンリンク  16 X 40/100 Gbps QSFP28 アップリンク	64 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(3j)

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。

## ファブリック ポートの障害検出のためのポート トラッキング ポリシー

ファブリック ポートの障害検出は、ポート トラッキング システム設定で有効にすることができます。ポート トラッキング ポリシーは、リーフスイッチとスパインスイッチ間のファブリック ポート、およびティア1リーフスイッチとティア2リーフスイッチ間のポートのステータス

を監視します。有効なポートトラッキングポリシーがトリガーされると、リーフスイッチは、EPGによって導入されたスイッチ上のすべてのアクセスインターフェイスをダウンさせます。

[ポートトラッキングがトリガーされたときに APIC ポートを含める (**Include APIC ports when port tracking is triggered**)] オプションを有効にした場合、リーフスイッチがすべてのファブリックポートへの接続を失うと (つまり、ファブリックポートが 0 になると)、ポートトラッキングは Cisco Application Policy Infrastructure Controller (APIC) ポートを無効にします。Cisco APIC がファブリックに対してデュアルまたはマルチホームの場合にのみ、この機能を有効にします。Cisco APIC ポートを停止すると、デュアルホームの Cisco APIC の場合にセカンダリポートに切り替えるのに役立ちます。



(注) ポートトラッキングの設定は、[システム (System)] >> [システム設定 (System Settings)] >> [ポートトラッキング (Port Tracking)] で行えます。

ポートトラッキングポリシーは、ポリシーをトリガーするファブリックポート接続の数と、指定されたファブリックポートの数を超えた後にリーフスイッチアクセスポートをバックアップするための遅延タイマーを指定します。

次の例は、ポートトラッキングポリシーの動作を示しています。

- ポートトラッキングポリシーは、ポリシーをトリガーする各リーフスイッチのアクティブなファブリックポート接続のしきい値が 2 であることを指定します。
- ポートトラッキングポリシーは、リーフスイッチからスパインスイッチへのアクティブなファブリックポート接続の数が 2 に低下したときにトリガーされます。
- 各リーフスイッチは、そのファブリックポート接続を監視し、ポリシーで指定されたしきい値に従ってポートトラッキングポリシーをトリガーします。
- ファブリックポート接続が復旧すると、リーフスイッチは遅延タイマーが期限切れになるのを待ってから、アクセスポートを復旧します。これにより、トラフィックがリーフスイッチアクセスポートで再開可能になる前に、ファブリックが再コンバージェンスする時間が与えられます。大規模ファブリックでは、遅延タイマーをより長い時間に設定する必要がある場合があります。



(注) このポリシーを構成するときは注意が必要です。ポートトラッキングをトリガーするアクティブなスパインポートの数のポートトラッキング設定が高すぎる場合、すべてのリーフスイッチアクセスポートがダウンします。

## Epg の Q-で-Q カプセル化のマッピング

Cisco Application Policy Infrastructure Controller (APIC) を使用すれば、通常のインターフェイス、PC、または vPC で入力される二重タグ付き VLAN トラフィックを EPG にマッピングでき

ます。この機能が有効で、二重タグ付きトラフィックが EPG のネットワークに入ると、両方のタグがファブリック内で個別に処理され、Cisco Application Centric Infrastructure (ACI) スイッチの出力時に二重タグに復元されます。単一タグおよびタグなしのトラフィックの入力はドロップします。

次の注意事項および制約事項が適用されます。

- この機能は、Cisco Nexus 9300-FX プラットフォーム スイッチでのみサポートされています。
- 外側と内側の両方のタグは、EtherType 0x8100 である必要があります。
- MAC ラーニングとルーティングは、アクセスのカプセル化ではなく、EPG ポート、sclass、および VRF インスタンスに基づいています。
- QoS 優先度設定がサポートされ、入力の外側のタグから派生し、出力の両方のタグに書き換えられます。
- EPG はリーフ スイッチの他のインターフェイスに同時に関連付けることができ、単一タグの VLAN に設定されます。
- サービス グラフは、Q-in-Q カプセル化したインターフェイスにマッピングされているプロバイダとコンシューマ EPG をサポートしています。サービス ノードの入力および出力トラフィックが単一タグのカプセル化フレームにある限り、サービス グラフを挿入することができます。
- vPC ポートが Q-in-Q カプセル化モードに対して有効になっている場合、VLAN 整合性チェックは実行されません。

この機能では、次の機能とオプションがサポートされていません。

- ポート単位の VLAN 機能
- FEX 接続
- Mixed mode
 

たとえば、Q-in-Q カプセル化モードのインターフェイスでは、通常の VLAN のカプセル化ではなく、二重タグ付きカプセルのみを持つ EPG にバインディングされている静的パスを有します。
- STP と「カプセル化でのフラッドイング」オプション
- タグなしおよび 802.1p モード
- マルチポッドと複数サイト
- レガシブリッジ ドメイン
- L2Out および L3Out 接続
- VMM の統合
- ポート モードをルーテッドから Q-in-Q カプセル化モードに変更する

- Q-in-Q カプセル化モードのポートでの VLAN 単位の誤配線プロトコル

## レイヤ2 マルチキャスト

### Cisco APIC および IGMP スヌーピングについて

IGMP スヌーピングは、Internet Group Management Protocol (IGMP) ネットワーク トラフィックをリスニングするプロセスです。この機能により、ネットワーク スイッチはホストとルータ間の IGMP 対話をリスニングして、必要ないマルチキャストリンクをフィルタでき、特定のマルチキャスト トラフィックを受け取るポートを制御することができます。

Cisco APIC は、N9000 スタンドアロンなどの従来のスイッチに含まれる完全な IGMP スヌーピング機能をサポートします。

- ブリッジドメインごとのポリシーベースの IGMP スヌーピング構成

APICを使用すると、ブリッジドメインごとにIGMPスヌーピングのプロパティを有効化、無効化、またはカスタマイズするポリシーを構成できます。その後、そのポリシーを1つまたは複数のブリッジドメインに適用できます。

- 静的ポート グループの導入

スイッチ ポートが IGMP マルチキャスト トラフィックを受信および処理しているため、IGMP 静的ポートのグループ化によりすでにアプリケーション EPG に静的に割り当てられた事前プロビジョニングは有効です。この事前プロビジョニングは、通常 IGMP スヌーピング スタックがポートを動的に学習するときに発生する参加遅延を防止します。

静的グループ メンバーシップは、アプリケーション EPG に割り当てられている静的ポート (*static-binding ports* と呼ばれます) でのみ事前プロビジョニングできます。

- アプリケーション EPG のアクセス グループ構成

「アクセス-グループ」ができるストリームを制御するために使用任意ポート背後に参加します。

実際に所属するするポートの設定を適用できることを確認するには、アプリケーション EPG に静的に割り当てられているインターフェイスでアクセス グループ設定を適用できる EPG。

ルート マップ ベースのアクセス グループのみが許可されます。



- (注) **vzAny** を使用して、VRF 内のすべての EPG に対して IGMP スヌーピングなどのプロトコルを有効にすることができます。**vzAny** について詳細は、「[vzAny を使用して VRF 内のすべての EPG に通信ルールを自動的に適用する](#)」を参照してください。

**vzAny** を使用するには、[テナント (Tenants) ]>>[tenant-name]>>[ネットワーク (Networking) ]>>[VRFs]> >[vrf-name]>>[VRF 向けの EPG 収集 (EPG Collection for VRF) ] の順に移動します。

## ACI ファブリックに IGMP スヌーピングを実装するには



- (注) ブリッジ ドメインで IGMP スヌーピングをディセーブルにしないことを推奨します。IGMP スヌーピングをディセーブルにすると、ブリッジ ドメインで不正なフラッディングが過度に発生し、マルチキャストのパフォーマンスが低下する場合があります。

IGMP スヌーピング ソフトウェアは、ブリッジ ドメイン内の IP マルチキャスト トラフィックを調べて、該当する受信側が常駐するポートを検出します。IGMP スヌーピングではポート情報を利用することにより、マルチアクセスブリッジドメイン環境における帯域幅消費量を削減し、ブリッジドメイン全体へのフラッディングを回避します。デフォルトでは、IGMP スヌーピングがブリッジドメインでイネーブルにされています。

この図は、ホストへの接続を持つ ACI リーフ スイッチに含まれる IGMP ルーティング機能と IGMP スヌーピング機能を示しています。IGMP スヌーピング機能は、IGMP メンバーシップ レポートをスヌーピングし、メッセージを残し、必要な場合にのみ IGMP ルータ機能に転送します。



その結果、ACI ファブリックは送信元 IP アドレス 0.0.0.0 の IGMP レポートを送信します。



(注) IGMP スヌーピングの詳細については、RFC 4541 を参照してください。

## 仮想化のサポート

IGMP スヌーピングに対して、複数の仮想ルーティングおよび転送（VRF）インスタンスを定義できます。

リーフスイッチでは、**show** コマンドに VRF 引数を指定して実行すると、表示される情報のコンテキストを確認できます。VRF 引数を指定しない場合は、デフォルト VRF が使用されます。

## APIC IGMP スヌーピング機能、IGMPv1、IGMPv2、および高速リーブ機能

IGMPv1 と IGMPv2 は両方とも、メンバーシップレポート抑制をサポートします。つまり、同一サブネット上の2つのホストが同一グループのマルチキャストデータを受信する場合、他方のホストからメンバーレポートを受信するホストは、そのレポートを送信しません。メンバーシップレポート抑制は、同じポートを共有しているホスト間で発生します。

各スイッチポートに接続されているホストが1つしかない場合は、IGMPv2 の高速脱退機能を設定できます。高速脱退機能を使用すると、最終メンバーのクエリーメッセージがホストに送信されません。APIC は、IGMP 脱退メッセージを受信すると、ただちに該当するポートへのマルチキャスト データ転送を停止します。

IGMPv1 では、明示的な IGMP 脱退メッセージが存在しないため、APIC の IGMP スヌーピング機能は、特定のグループについてマルチキャストデータを要求するホストが存続しないことを示すために、メンバーシップメッセージタイムアウトを使用する必要があります。



(注) 高速脱退機能がイネーブルになっている場合、他のホストの存在は確認されないため、IGMP スヌーピング機能は、最終メンバーのクエリーインターバル設定を無視します。

## APIC IGMP スヌーピング ファンクション キーと IGMPv3

APIC での IGMPv3 スヌーピング ファンクションでは、完全な IGMPv3 スヌーピングがサポートされています。これにより、IGMPv3 レポートの（S、G）情報に基づいて、抑制されたフラグディングが提供されます。この送信元ベースのフィルタリングにより、デバイスは対象のマルチキャストグループにトラフィックを送信する送信元に基づいて、マルチキャストトラフィックの宛先ポートを制限できます。

デフォルトでは、IGMP スヌーピング機能は、ブリッジドメインでは、各 VLAN ポート上のホストを追跡します。この明示的なトラッキング機能は、高速脱退メカニズムをサポートして

います。IGMPv3 ではすべてのホストがメンバーシップ レポートを送信するため、レポート抑制機能を利用すると、デバイスから他のマルチキャスト対応ルータに送信されるトラフィック量を制限できます。レポート抑制を有効にしても、IGMPv1 または IGMPv2 ホストが同じグループをリクエストしなかった場合、IGMP スヌーピング機能はプロキシレポートを作成します。プロキシ機能により、ダウンストリーム ホストが送信するメンバーシップ レポートからグループ ステートが構築され、アップストリーム クエリアからのクエリーに応答するためにメンバーシップ レポートが生成されます。

IGMPv3 メンバーシップ レポートにはブリッジ ドメインのグループ メンバの一覧が含まれていますが、最終ホストが脱退すると、ソフトウェアはメンバーシップ クエリーを送信します。最終メンバーのクエリー インターバルについてパラメータを設定すると、タイムアウトまでにどのホストからも応答がなかった場合、IGMP スヌーピングはグループ ステートを削除します。

## Cisco APIC および IGMP スヌーピング クエリア関数

マルチキャスト トラフィックをルーティングする必要がないために、Protocol-Independent Multicast (PIM) がインターフェイス上でディセーブルになっている場合は、メンバーシップ クエリーを送信するように IGMP スヌーピング クエリア機能を設定する必要があります。APIC、IGMP スヌープ ポリシー内で定義マルチキャストのソースとレシーバが含まれているブリッジ ドメインでクエリアがないその他のアクティブなクエリアします。

Cisco ACI はデフォルトで、IGMP スヌーピングが有効になっています。さらに、ブリッジ ドメイン サブネット制御は、「クエリア IP」を選択、リーフ スイッチによって、クエリアとして動作およびクエリ パケット送信を開始します。セグメントは、明示的なマルチキャスト ルータ (PIM が有効になっていません) があるときに ACI Leaf スイッチでクエリアを有効にする必要があります。ブリッジ ドメインで、クエリアが設定されている、使用される IP アドレス マルチキャストのホストが設定されている同じサブネットからにする必要があります。



- (注) クエリアの IP アドレスは、ブロードキャスト IP アドレス、マルチキャスト IP アドレス、または 0 (0.0.0.0) にしないでください。

IGMP スヌーピング クエリアがイネーブルな場合は、定期的に IGMP クエリーが送信されるため、IP マルチキャスト トラフィックを要求するホストから IGMP レポート メッセージが発信されます。IGMP スヌーピングはこれらの IGMP レポートを待ち受けて、適切な転送を確立します。

IGMP スヌーピング クエリアは、RFC 2236 に記述されているようにクエリア選択を実行します。クエリア選択は、次の構成で発生します。

- 異なるスイッチ上の同じ VLAN に同じサブネットに複数のスイッチ クエリアが設定されている場合。
- 設定されたスイッチ クエリアが他のレイヤ 3 SVI クエリアと同じサブネットにある場合。

## ファブリック セキュアモード

ファブリック セキュアモードは、ファブリック機器に物理的にアクセスできる関係者が、管理者による手動の承認なしに、スイッチまたは APIC コントローラをファブリックに追加できないようにします。リリース 1.2(1x) 以降、ファームウェアは、ファブリック内のスイッチとコントローラに、有効な Cisco のデジタル署名付き証明書に関連付けられた有効なシリアル番号があることを確認します。この検証は、このリリースへのアップグレード時またはファブリックの初期インストール時に実行されます。この機能のデフォルト設定は **permissive** モードです。既存のファブリックは、リリース 1.2(1) 以降へのアップグレード後もそのまま実行されます。ファブリック全体のアクセス権を持つ管理者は、**strict** モードを有効にする必要があります。次の表は、2つの動作モードの自動要約です。

Permissive モード (デフォルト)	Strict モード
1つ以上のスイッチに無効な証明書がある場合でも、既存のファブリックが正常に動作できるようにします。	有効な Cisco シリアル番号と SSL 証明書を持つスイッチのみが許可されます。
シリアル番号ベースの認証を強制しません。	シリアル番号認証を強制します。
自動検出されたコントローラとスイッチが、シリアル番号認証を強制せずにファブリックに参加できるようにします。	管理者がコントローラとスイッチを手動で承認してファブリックに参加させる必要があります。

## FAST リンク フェールオーバー ポリシーの構成

FAST リンク フェールオーバー ポリシーは、-EX、-FX、および -FX2 サフィックスが付いたスイッチモデルのアップリンクに適用されます。アップリンク MAC ステータスに基づいてトラフィックを効率的に負荷分散します。この機能により、スイッチはレイヤ 2 またはレイヤ 3 ルックアップを実行し、アップリンク ステータスを考慮して、パケットハッシュ アルゴリズムに基づいて出力レイヤ 2 インターフェイス (アップリンク) を提供します。この機能により、データ トラフィックのコンバージェンスが 200 ミリ秒未満に短縮されます。

FAST リンク フェールオーバーの構成に関する次の制限事項を参照してください。

- FAST リンク フェールオーバ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。
- リモートリーフの構成は、FAST リンク フェールオーバーでは機能しません。この場合、FAST リンク フェールオーバー ポリシーは機能せず、障害は生成されません。
- FAST リンク フェールオーバーポリシーが有効になっている場合、個々のアップリンクでの SPAN の構成は機能しません。個々のアップリンクで SPAN を有効にしようとしても障

害は生成されませんが、FAST リンク フェールオーバー ポリシーはすべてのアップリンクと一緒に有効にすることも、個々のダウンリンクで有効にすることもできます。



(注) FAST リンク フェールオーバーは、[ファブリック (Fabric)] > [アクセス ポリシー (Access Policies)] > [ポリシー (Policies)] > [スイッチ (Switch)] > [FAST リンク フェールオーバー (Fast Link Failover)] の下にあります。

## ポート セキュリティと ACI について

ポート セキュリティ機能は、ポートごとに取得される MAC アドレスの数を制限することによって、不明な MAC アドレスでフラグディングしないように ACI ファブリックを保護します。ポート セキュリティ機能のサポートは、物理ポート、ポート チャネル、および仮想ポート チャネルで使用できます。

## ポート セキュリティおよびラーニング動作

非 vPC ポートまたはポート チャネルでは、新しいエンドポイントに対して学習イベントが発生し、新しい学習が許可されているか確認する検証が行われます。対応するインターフェイスに設定されていない、または無効なポート セキュリティ ポリシーが存在する場合、エンドポイント ラーニング動作はサポートされているものから変更されません。ポリシーが有効になっており制限に到達している場合、現在のサポートされているアクションは次の通りです。

- エンドポイントを学習し、ドロップアクションのハードウェアにインストールします。
- サイレントに学習を破棄します。

制限に到達していない場合、エンドポイントが学習され、この新しいエンドポイントが発生したため制限に達しているかどうか確認する検証が行われます。制限に到達しており、学習の無効化アクションが設定されている場合、インターフェイス上のハードウェアでラーニングが無効になります（物理インターフェイスまたはポートチャネルまたはvPC）。制限に到達しており、学習の無効化アクションが設定されていない場合、エンドポイントはドロップアクションでハードウェアにインストールされます。このようなエンドポイントは、他のエンドポイントのように通常期限切れです。

初めて制限に達したとき、ポート セキュリティ ポリシー オブジェクトの動作状態がそれを反映して更新されます。スタティックルールは、ユーザーに警告ができるように、障害の発生と定義されます。制限に到達すると、Syslog も発生します。

vPC の場合、MAC 制限に到達するとピア リーフ スイッチにも通知されるため、ラーニングがピアで無効になる可能性があります。vPC ピアはいつでも再起動でき、vPC レッグが動作不能になるか再起動できるため、この状態はピアと調和して vPC ピアはこの状態に同期されません。同期しない場合は、1 個のレッグでラーニングが有効になり、他のレッグで無効になる状況が発生する可能性があります。

デフォルトでは、制限に到達してラーニングが無効になると、60 秒のデフォルト タイムアウト値の後、自動的に再度有効になります。

## 保護モード

保護モードはセキュリティ違反が発生している以上に増やさないようにします。MAC の制限がポートで設定されている最大値を超えると、超過した MAC アドレスからすべてのトラフィックはドロップされ、さらにラーニングが無効になります。

## ポート レベルでのポート セキュリティ

APIC では、ユーザがスイッチポートのポートセキュリティを設定できます。ポート上で MAC が制限の最大設定値を超過すると、超過した MAC アドレスからすべてのトラフィックが転送されます。次の属性がサポートされます。

- **ポート セキュリティのタイムアウト**：現在サポートされているタイムアウト値は、60 ~ 3600 秒の範囲でサポートされています。
- **違反行為**：違反行為は保護モードで使用できます。保護モードでは、MAC の取得が無効になるため、MAC アドレスは CAM テーブルに追加されません。Mac ラーニングが設定されているタイムアウト値の後に再度有効になります。
- **最大エンドポイント**：現在のサポートされている最大のエンドポイント設定値は、0 ~ 12000 の範囲でサポートされています。最大エンドポイント値が 0 の場合、そのポートではポートセキュリティ ポリシーが無効になります。

## ポート セキュリティに関するガイドラインと制約事項

次のようなガイドラインと制約事項があります。

- ポートセキュリティは、ポートごとに使用できます。
- ポートセキュリティは、物理ポート、ポートチャネル、および仮想ポートチャネル (vPC) でサポートされています。
- スタティック MAC アドレスとダイナミック MAC アドレスがサポートされています。
- セキュアなポートからセキュアでないポートへと、セキュアでないポートからセキュアなポートへの MAC アドレスの移動がサポートされています。
- MAC アドレスの制限は、MAC アドレスにのみ適用され、MAC と IP によるアドレスには実行されません。
- ポートセキュリティは、ファブリック エクステンダ (FEX) ではサポートされていません。

## ファーストホップセキュリティについて

ファーストホップセキュリティ (FHS) 機能では、レイヤ2リンク上でより優れたIPv4とIPv6のリンクセキュリティおよび管理が可能になります。サービスプロバイダ環境で、これらの機能は重複アドレス検出 (DAD) とアドレス解像度 (AR) などのアドレス割り当てや派生操作が、より緊密に制御可能です。

次のサポートされている FHS 機能はプロトコルをセキュアにして、ファブリック リーフスイッチにセキュアなエンドポイントデータベースを構築するのに役立ち、MIM 攻撃や IP の盗難などのセキュリティ盗難を軽減するために使用されます。

- **ARP 検査**：ネットワーク管理者は、無効な MAC アドレスから IP アドレスへのバインディングがある ARP パケットを代行受信、記録、およびドロップすることができます。
- **ND 検査**：レイヤ2 ネイバー テーブルでステートレス自動設定アドレスのバインディングを学習し、保護します。
- **DHCP 検査**：信頼できない送信元からの DHCP メッセージを検証し、無効なメッセージをフィルタ処理して除外します。
- **RA ガード**：ネットワーク管理者は、不要または不正なルータアドバタイズメント (RA) ガードメッセージをブロックまたは拒否できます。
- **IPv4 および IPv6 ソース ガード**—不明なソースからのデータトラフィックをすべてブロックします。
- **信頼制御**：信頼できる送信元はその企業の管理制御下にあるデバイスです。これらのデバイスには、ファブリック内のスイッチ、ルータ、およびサーバが含まれます。ファイアウォールを越えるデバイスやネットワーク外のデバイスは信頼できない送信元です。一般的に、ホストポートは信頼できない送信元として扱われます。

FHS 機能は、次のセキュリティ対策を提供します。

- **ロールの適用**：信頼できない主催者が、そのロールの有効範囲を超えるメッセージを送信することを防ぎます。
- **バインディングの適用**：アドレスの盗難を防止します。
- **DoS 攻撃の軽減対策**：悪意あるエンドポイントを防ぎ、データベースが操作サービスを提供することを停止するポイントにエンドポイントデータベースを成長させます。
- **プロキシサービス**：アドレス解決の効率を高めるため一部のプロキシサービスを提供します。

FHS 機能は、テナントブリッジドメイン (BD) ごとに有効になっています。ブリッジドメインとして、単一または複数のリーフスイッチで展開可能で、FHS 脅威の制御と軽減のメカニズムは単一のスイッチと複数のスイッチのシナリオにも対応できます。

## MACsec について

MACsec は、IEEE 802.1AE 規格ベースのレイヤ 2 ホップバイホップ暗号化であり、これにより、メディア アクセス非依存プロトコルに対してデータの機密性と完全性を確保できます。

MACsec は、暗号化キーにアウトオブバンド方式を使用して、有線ネットワーク上で MAC レイヤの暗号化を提供します。MACsec Key Agreement (MKA) プロトコルでは、必要なセッションキーを提供し、必要な暗号化キーを管理します。

802.1 ae MKA と暗号化はリンク、つまり、リンク (ネットワーク アクセス デバイスと、PC か IP 電話機などのエンドポイント デバイス間のリンク) が直面しているホストのすべてのタイプでサポートされますか。リンクが接続されている他のスイッチまたはルータ。

MACsec は、イーサネット パケットの送信元および宛先 MAC アドレスを除くすべてのデータを暗号化します。ユーザは、送信元と宛先の MAC アドレスの後に最大 50 バイトの暗号化をスキップするオプションもあります。

WAN またはメトロイーサネット上に MACsec サービスを提供するために、サービスプロバイダーは、Ethernet over Multiprotocol Label Switching (EoMPLS) および L2TPv3 などのさまざまなトランスポート レイヤ プロトコルを使用して、E-Line や E-LAN などのレイヤ 2 透過サービスを提供しています。

EAP-over-LAN (EAPOL) プロトコルデータユニット (PDU) のパケット本体は、MACsec Key Agreement PDU (MKPDU) と呼ばれます。3 回のハートビート後 (各ハートビートは 2 秒) に参加者から MKPDU を受信しなかった場合、ピアはライブ ピア リストから削除されます。たとえば、クライアントが接続を解除した場合、スイッチ上の参加者はクライアントから最後の MKPDU を受信した後、3 回のハートビートが経過するまで MKA の動作を継続します。

### APIC ファブリック MACsec

APIC はまた責任を負う MACsec キーチェーン ディストリビューションのポッド内のすべてのノードに特定のポートのノードになります。サポートされている MACsec キーチェーンし、apic 内でサポートされている MACsec ポリシー ディストリビューションのとおりです。

- 単一ユーザ提供キーチェーンと 1 ポッドあたりポリシー
- ユーザが提供されるキーチェーンとファブリック インターフェイスごとのユーザが提供されるポリシー
- 自動生成されたキーチェーンおよび 1 ポッドあたりのユーザが提供されるポリシー

ノードは、複数のポリシーは、複数のファブリックリンクの導入を持つことができます。これが発生すると、ファブリック インターフェイスごとキーチェーンおよびポリシーが優先して指定の影響を受けるインターフェイス。自動生成されたキーチェーンと関連付けられている MACsec ポリシーでは、最も優先度から提供されます。

APIC MACsec では、2 つのセキュリティ モードをサポートしています。MACsec **セキュリティで保護する必要があります** 中に、リンクの暗号化されたトラフィックのみを許可する **セキュリティで保護する必要があります** により、両方のクリアし、リンク上のトラフィックを暗号

化します。MACsec を展開する前に **セキュリティで保護する必要があります** モードでのキーチェーンは影響を受けるリンクで展開する必要がありますまたはリンクがダウンします。たとえば、ポートをオンにできますで MACsec **セキュリティで保護する必要があります** モードがピアがしているリンクでのキーチェーンを受信する前にします。MACsec を導入することが推奨されて、この問題に対処する **セキュリティで保護する必要があります** モードとリンクの 1 回すべてにセキュリティ モードを変更 **セキュリティで保護する必要があります** 。



(注) MACsec インターフェイスの設定変更は、パケットのドロップになります。

MACsec ポリシー定義のキーチェーンの定義に固有の設定と機能の機能に関連する設定で構成されています。キーチェーン定義と機能の機能の定義は、別のポリシーに配置されます。MACsec 1 ポッドあたりまたはインターフェイスごとの有効化には、キーチェーン ポリシーおよび MACsec 機能のポリシーを組み合わせることが含まれます。



(注) 内部を使用して生成キーチェーンは、ユーザのキーチェーンを指定する必要はありません。

#### APIC アクセス MACsec

MACsec はリーフ スイッチ L3out インターフェイスと外部のデバイス間のリンクを保護するために使用します。APIC GUI および CLI のユーザを許可するで、MACsec キーとファブリック L3Out インターフェイスの設定を MacSec をプログラムを提供する物理/pc/vpc インターフェイスごと。ピアの外部デバイスが正しい MacSec 情報を使用してプログラムすることを確認するには、ユーザの責任です。

## データ プレーン ポリシング

データ プレーン ポリシング (DPP) を使用して、ACI ファブリック アクセス インターフェイスの帯域幅使用量を管理します。DPP ポリシーは出力トラフィック、入力トラフィック、またはその両方に適用できます。DPP は特定のインターフェイスのデータ レートを監視します。データ レートがユーザ設定値を超えると、ただちにパケットのマーキングまたはドロップが発生します。ポリシングではトラフィックがバッファリングされないため、伝搬遅延への影響はありません。トラフィックがデータ レートを超えた場合、ACI ファブリックは、パケットのドロップか、パケット内 QoS フィールドのマーキングのどちらかを実行できます。



(注) 出力データプレーンポリサーは、スイッチ仮想インターフェイス (SVI) ではサポートされていません。

DPP ポリシーは、シングルレート、デュアルレート、カラー対応のいずれかになります。シングルレートポリシーは、トラフィックの認定情報レート (CIR) を監視します。デュアルレ

ト ポリサーは、CIR と最大情報レート (PIR) の両方を監視します。また、システムは、関連するバースト サイズもモニタします。指定したデータ レート パラメータに応じて、適合 (グリーン)、超過 (イエロー)、違反 (レッド) の3つのカラー、つまり条件が、パケットごとにポリサーによって決定されます。

通常、DPP ポリシーは、サーバやハイパーバイザなどの仮想または物理デバイスへの物理または仮想レイヤ2 接続に適用されます。ルータについてはレイヤ3 接続で適用されます。リーフスイッチアクセスポートに適用される DPP ポリシーは、ACI ファブリックのファブリックアクセス (infraInfra) 部分で構成され、ファブリック管理者が構成する必要があります。境界リーフスイッチアクセスポート (l3extOut または l2extOut) のインターフェイスに適用される DPP ポリシーは、ACI ファブリックのテナント (fvTenant) 部分で構成され、テナント管理者が構成できます。

各状況に設定できるアクションは1 つだけです。たとえば、DPP ポリシーを最大 200 ミリ秒のバーストで、256,000 bps のデータ レートに適合させることが可能です。この場合、システムは、このレートの範囲内のトラフィックに対して適合アクションを適用し、このレートを超えるトラフィックに対して違反アクションを適用します。カラー対応ポリシーは、トラフィックが以前にカラーによってすでにマーキングされているものと見なします。次に、このタイプのポリサーが実行するアクションの中で、その情報が使用されます。

## スケジューラ

スケジュールにより、設定のインポート/エクスポートまたはテクニカル サポートの収集などの操作を1 つ以上の指定した時間帯に発生させることができます。

スケジュールには、一連のタイムウィンドウ (オカレンス) が含まれます。これらのウィンドウは、1 回だけ発生させるか、または毎週指定した日時に繰り返し発生させることができます。期間や実行するタスクの最大数などのウィンドウで定義されているオプションにより、スケジュール設定されたタスクの実行時期が決定されます。たとえば、最大時間長またはタスク数に達したため特定のメンテナンス時間帯に変更を展開できない場合、この展開は次のメンテナンス時間に持ち越されます。

各スケジュールは、APIC が1 つまたは複数のメンテナンス時間帯に入っているかどうか、定期的に確認します。入っている場合、スケジュールはメンテナンスポリシーで指定された制限に対し適切な展開を実行します。

スケジュールには、スケジュールに関連付けられたメンテナンス時間を決定する1 つ以上のオカレンスが含まれています。オカレンスは次のいずれかになります。

- **[One-time]** ウィンドウ：一度だけ行うスケジュールを定義します。これらの時間帯は、その時間帯の最大時間長まで、または時間帯の中で実行可能なタスクの最大数に達するまで継続されます。
- **[Recurring]** ウィンドウ：繰り返すスケジュールを定義します。この時間帯は、タスクの最大数に達するまで、または時間帯に指定された日の終わりに達するまで継続します。

スケジュールを構成すると、構成中に次のエクスポートポリシーとファームウェアポリシーを選択して適用できます。

- テクニカル サポート エクスポート ポリシー
- 構成エクスポートポリシー：日次自動バックアップ
- ファームウェアダウンロード

## ファームウェア アップグレード

APIC 上のポリシーは、ファームウェア アップグレード プロセスの次の項目を管理します。

- 使用するファームウェアのバージョン。
- シスコから APIC リポジトリへのファームウェア イメージのダウンロード。
- 互換性の適用。
- アップグレードするもの：
  - スイッチ
  - 結果を表示するための APIC
  - 互換性カタログ
- アップグレードを実行する時期。
- 障害の処理方法（再試行、一時停止、無視など）。

各ファームウェア イメージには、サポートされるタイプおよびスイッチ モデルを識別する互換性カタログが含まれます。APIC は、ファームウェア イメージ、スイッチタイプ、およびそのファームウェア イメージを使用することを許可されるモデルのカタログを保持しています。デフォルトの設定では、互換性カタログに適合しない場合、ファームウェアの更新が拒否されます。

イメージ管理を実行する APIC には、互換性カタログ、APIC コントローラのファームウェア イメージおよびスイッチ イメージのイメージリポジトリがあります。管理者は、イメージソース ポリシーを作成することで外部 HTTP サーバまたは SCP サーバから新しいファームウェア イメージを APIC イメージリポジトリにダウンロードできます。

APIC 上のファームウェア グループポリシーは、必要なファームウェア バージョンを定義します。

メンテナンスグループポリシーは、ファームウェアをアップグレードする時期、アップグレードするノード、および障害の処理方法を定義します。また、メンテナンスグループポリシーは、同時にアップグレードできるノードのグループを定義して、それらのメンテナンスグループをスケジュールに割り当てます。ノードグループオプションには、すべてのリーフノード、すべてのスパインノード、またはファブリックの一部であるノードのセットが含まれます。

APIC コントローラのファームウェア アップグレードポリシーは、クラスタ内のすべてのノードに常に適用されますが、アップグレードは常に一度に 1 つのノードに実行されます。APIC

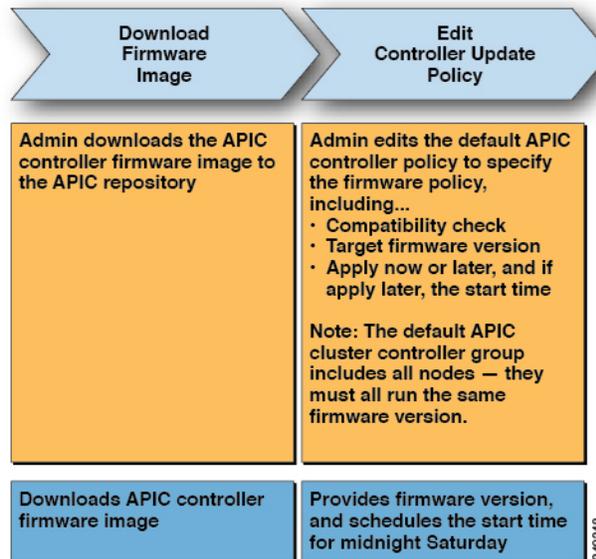
GUIにより、ファームウェア アップグレードに関するリアルタイムのステータス情報が提供されます。



(注) 定期的アップグレードまたは1度だけのアップグレードのスケジュールに過去の日時が設定されている場合、スケジューラはただちにアップグレードをトリガーします。

次の図は、APIC クラスタ ノードのファームウェア アップグレードのプロセスを示します。

図 15: APIC クラスタ コントローラのファームウェア アップグレードのプロセス



APICは、次のようにこのコントローラのファームウェアアップグレードポリシーを適用します。

- 管理者が土曜日の午前0時にコントローラ アップデート ポリシーを構成したため、APICは土曜日の午前0時にアップグレードを開始します。
- システムは、既存のファームウェアの互換性を確認し、新しいファームウェアイメージで提供される互換性カタログに従って、新しいバージョンにアップグレードします。
- アップグレードは、クラスタ内のすべてのノードがアップグレードされるまで、一度に1個のノードずつ行われます。



(注) APIC はノードの複製クラスタであるため、中断は最小限に抑えるべきです。管理者は、APIC のアップグレードのスケジュールを検討する際にシステムの負荷を認識し、メンテナンス期間中にアップグレードを計画する必要があります。

- APIC を含む ACI ファブリックは、アップグレードが進行中でも動作し続けます。

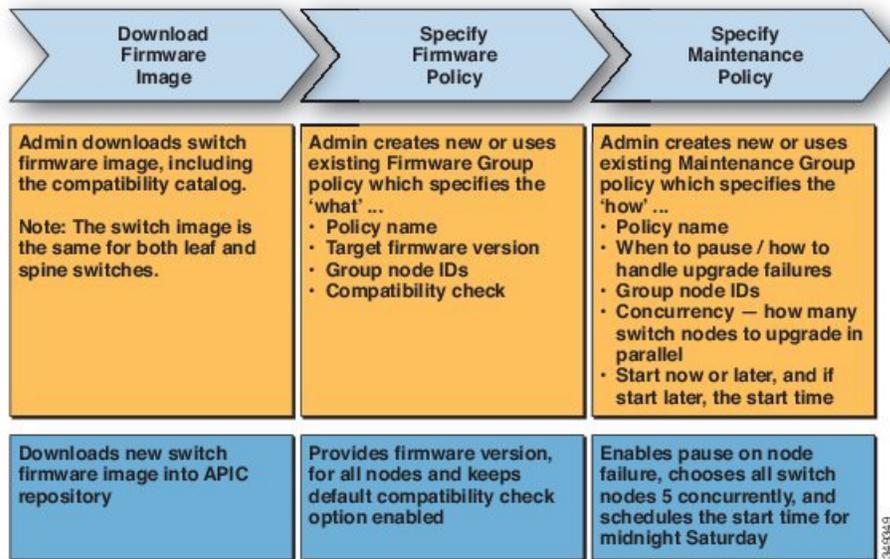


(注) コントローラのアップグレードはランダムに行われます。各 APIC コントローラはアップグレードに約10分かかります。コントローラのイメージがアップグレードされると、クラスタからドロップし、新しいバージョンで再起動します。その間、クラスタ内の他の APIC コントローラは動作しています。コントローラが再起動すると、クラスタに再び参加します。その後、クラスタが収束し、次のコントローラのイメージのアップグレードを開始します。クラスタがすぐに収束せず、完全な適合状態にならないければ、その後のアップグレードは、クラスタが収束して完全な適合状態になるまで待機状態になります。この期間中、「Waiting for Cluster Convergence」メッセージが表示されます。

- コントローラノードのアップグレードが失敗すると、アップグレードが一時停止し、手動による介入が行われるまで待機します。

次の図は、すべての ACI ファブリック スイッチ ノードのファームウェアをアップグレードするプロセスがどのように動作するかを示します。

図 16: スイッチ ファームウェアのアップグレードプロセス



APIC は、次のようにこのスイッチ アップグレード ポリシーを適用します。

- 管理者が土曜日の午前 0 時にコントローラ アップデート ポリシーを構成したため、APIC は土曜日の午前 0 時にアップグレードを開始します。
- システムは、既存のファームウェアの互換性を確認し、新しいファームウェアイメージで提供される互換性カタログに従って、新しいバージョンにアップグレードします。

- アップグレードは、すべての指定されたノードがアップグレードされるまで、一度に5個のノードずつ行われます。



(注) ファームウェアのアップグレードにより、スイッチがリブートします。リブートにより数分間スイッチの操作が中断される場合があります。メンテナンス期間中にファームウェアのアップグレードをスケジュールします。

- スイッチノードのアップグレードが失敗すると、アップグレードが一時停止し、手動による介入が行われるまで待機します。

ファームウェア アップグレードを実行するための詳細な手順については、『*Cisco APIC Management, Installation, Upgrade, and Downgrade Guide*』を参照してください。

## 設定ゾーン

構成ゾーンは、ACIファブリックをさまざまなゾーンに分割します。これらのゾーンは、異なる時間で構成変更を使用して更新できます。これにより、トラフィックを中断させたり、ファブリックをダウンさせたりする可能性のある、欠陥のあるファブリック全体の構成を展開するリスクを制限できます。管理者は、クリティカルでないゾーンに構成を展開し、それが適切であると判断した後でクリティカルなゾーンに展開することが可能です。

次のポリシーは、構成ゾーンのアクションを指定します。

- `infrazone:ZoneP` は、システムアップグレード時に自動的に作成されます。削除することも変更することもできません。
- `infrazone:Zone` には、1つ以上のポッドグループ (PodGrp) または1つ以上のノードグループ (NodeGrp) が含まれます。



(注) PodGrp または NodeGrp のいずれかのみを選択できます。両方は選べません。

ノードは1つのゾーン (`infrazone:Zone`) のみに属することができます。NodeGrp には、名前と展開モードの2つのプロパティがあります。展開モードのプロパティは次のとおりです。

- `enabled` : 保留中の更新がすぐに送信されます。
- `disabled` : 新しい更新は延期されます。



- (注)
- 無効な構成ゾーンでノードをアップグレード、ダウングレード、コミッション、またはデコミッションしないでください。
  - 無効な構成ゾーンでノードのクリーンリロードまたはアップリンク/ダウンリンクポート変換リロードを実行しないでください。

- `triggered` : 保留中の更新はすぐに送信され、展開モードは変更が `triggered` 以前の値に自動的にリセットされます。

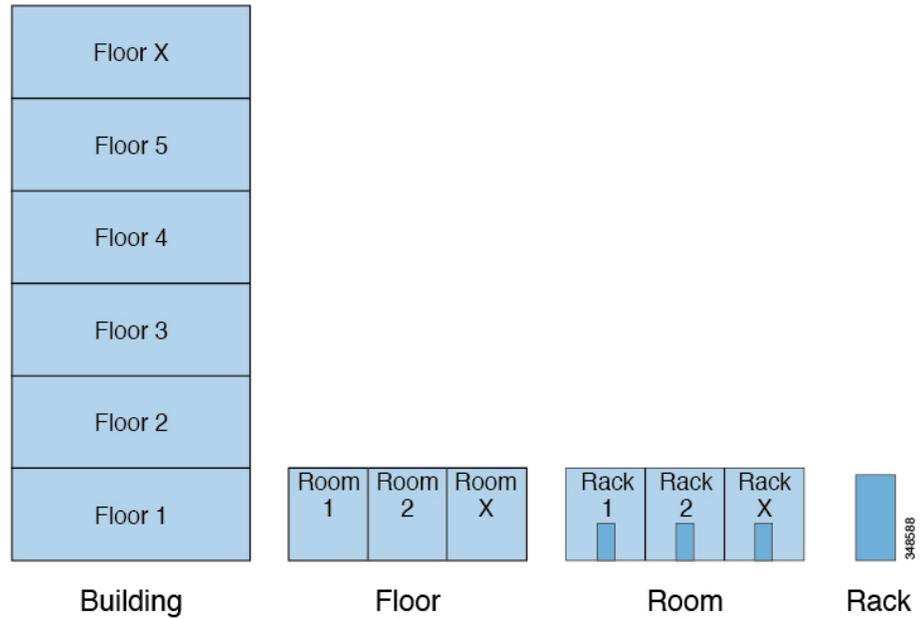
特定のノードセットでポリシーが作成、変更、または削除されると、ポリシーが展開されている各ノードに更新が送信されます。ポリシークラスと `infraczone` の構成に基づいて、次のことが起こります。

- `infraczone` 構成に従わないポリシーの場合、APIC はすべてのファブリック ノードに更新をすぐに送信します。
- `infraczone` 構成に従うポリシーの場合、更新は `infraczone` 構成に従って進行します。
  - ノードが `infraczone:Zone` の一部である場合、ゾーンの展開モードが有効に設定されている場合、更新はすぐに送信されます。それ以外の場合、更新は延期されます。
  - ノードが `infraczone:Zone` の一部でない場合、更新はすぐに実行されます。これは、ACI ファブリックのデフォルトの動作です。

## 位置情報

管理者は、位置情報ポリシーを使用して、データセンター施設内の ACI ファブリック ノードの物理ロケーションをマッピングします。次の図は、地理位置情報マッピング機能の例を示します。

図 17: 位置情報 (GeoLocation)



たとえば、単一の部屋でのファブリック展開の場合は、管理者がデフォルトのルームオブジェクトを使用して、スイッチの物理ロケーションに一致する1つ以上のラックを作成します。大規模な展開の場合、管理者は1つ以上のサイトオブジェクトを作成できます。各サイトには、1つ以上の建物を含めることができます。各建物には、1つ以上のフロアがあります。各フロアには1つ以上の部屋があり、各部屋には1つ以上のラックがあります。最後に、各ラックは1つ以上のスイッチに関連付けることができます。

## 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。