Cisco APIC レイヤ 2 ネットワーク設定ガイド、リリース 5.2(x)

最終更新：2025 年 5 月 26 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

© 2021–2024 Cisco Systems, Inc. All rights reserved.

Trademarks

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS REFERENCED IN THIS DOCUMENTATION ARE SUBJECT TO CHANGE WITHOUT NOTICE. EXCEPT AS MAY OTHERWISE BE AGREED BY CISCO IN WRITING, ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS DOCUMENTATION ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED.

The Cisco End User License Agreement and any supplemental license terms govern your use of any Cisco software, including this product documentation, and are located at: https://www.cisco.com/c/en/us/about/legal/cloud-and-software/software-terms.html. Cisco product warranty information is available at https://www.cisco.com/c/en/us/products/warranty-listing.html. US Federal Communications Commission Notices are found here https://www.cisco.com/c/en/us/products/us-fcc-notice.html.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any products and features described herein as in development or available at a future date remain in varying stages of development and will be offered on a when-and if-available basis. Any such product or feature roadmaps are subject to change at the sole discretion of Cisco and Cisco will have no liability for delay in the delivery or failure to deliver any products or feature roadmap items that may be set forth in this document.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

The documentation set for this product strives to use bias-free language. For the purposes of this documentation set, bias-free is defined as language that does not imply discrimination based on age, disability, gender, racial identity, ethnic identity, sexual orientation, socioeconomic status, and intersectionality. Exceptions may be present in the documentation due to language that is hardcoded in the user interfaces of the product software, language used based on RFP documentation, or language that is used by a referenced third-party product.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners.

The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

目 次

はじめに： **Trademarks** iii

第 1 章 **新機能および変更された機能** 1

新機能および変更された機能に関する情報 1

第 2 章 **Cisco ACI 転送** 3

ACI ファブリックは現代のデータ センター トラフィック フローを最適化する 3

ACI で VXLAN 4

サブネット間のテナント トラフィックの転送を促進するレイヤ 3 VNID 6

スパニング ツリー プロトコル BPDU の送信 8

第 3 章 **レイヤ 2 ネットワーク設定の前提条件** 11

レイヤ 2 の前提条件 11

第 4 章 **ネットワーク ドメイン** 13

ネットワーク ドメイン 13

関連資料 14

ブリッジ ドメイン 14

ブリッジ ドメインについて 14

VMM ドメイン 14

Virtual Machine Manager ドメインの主要コンポーネント 14

Virtual Machine Manager のドメイン 15

物理ドメイン設定 16

物理ドメインの設定 16

第 5 章 ブリッジング 19
外部ルータへのブリッジド インターフェイス 19
ブリッジ ドメインとサブネット 20
ブリッジ ドメイン オプション 23
GUI を使用したテナント、VRF およびブリッジ ドメインの作成 26
NX-OS CLI を使用した、テナント、VRF およびブリッジ ドメインの作成 29
適用されるブリッジ ドメインの設定 30
NX-OS スタイル CLI を使用した適用されるブリッジ ドメインの設定 31
カプセル化によるすべてのプロトコルおよびプロキシ ARP のカプセル化のフラッディングを設定する 33
カプセル化範囲限定のフラッディングの設定 38
Cisco APIC GUI を使用したカプセル化範囲限定のフラッディングの設定 39
NX-OS スタイル CLI を使用したカプセル化でのフラッディングの設定 40

第 6 章 EPG 41
エンドポイント グループについて 41
エンドポイント グループ 41
EPG シャットダウンでの ACI ポリシー設定 44
アクセス ポリシーによる VLAN から EPG への自動割り当て 44
ポート単位の VLAN 45
vPC に展開された EPG の VLAN ガイドライン 47
特定のポートに EPG を導入する 47
GUI を使用して特定のノードまたはポートへ EPG を導入する 47
NX-OS スタイルの CLI を使用した APIC の特定のポートへの EPG の導入 49
特定のポートに EPG を導入するためのドメイン、接続可能アクセス エンティティ プロファイル、および VLAN の作成 50
特定のポートに EPG を導入するためのドメイン、接続可能アクセス エンティティ プロファイル、および VLAN の作成 50
GUI を使用して特定のポートに EPG を展開するためのドメインおよび VLAN の作成 51
NX-OS スタイルの CLI を使用した、EPG を特定のポートに導入するための AEP、ドメイン、および VLAN の作成 53

重複する VLAN の検証 54
GUI を使用した重複 VLAN の検証 54
添付されているエンティティ プロファイルで複数のインターフェイスに EPG を導入する 55
AEP を使用してアプリケーション EPG を複数のポートに展開する 55
APIC GUI を使用した AEP による複数のインターフェイスへの EPG の導入 55
EPG 内の分離 58
EPG 内エンドポイント分離 58
ベア メタル サーバの EPG 内分離 58
ベア メタル サーバの EPG 内分離 58
GUI を使用したベア メタル サーバ の EPG 内分離の設定 59
NX-OS スタイルの CLI を使用したベア メタル サーバ の EPG 内分離の設定 60
VMware vDS の EPG 内分離 62
VMware VDS または Microsoft Hyper-V 仮想スイッチの EPG 分離 62
GUI を使用した VMware VDS または Microsoft Hyper-V の EPG 内分離の設定 66
NX-OS スタイル CLI を使用した VMware VDS または Microsoft Hyper-V の EPG 内分離の設定 67
Cisco ACI 仮想エッジの EPG 内分離の設定 69
Cisco ACI Virtual Edge での EPG 内分離の適用 69
GUI を使用した Cisco ACI Virtual Edge の EPG 内分離の設定 69
[Tenants] タブの下で、Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を選択する 71
[Tenents] タブの下で Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を表示する 71
[Virtual Networking] タブの下で、Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を選択する 72
[Virtual Networking] タブで Cisco ACI Virtual Edge の分離エンドポイント統計情報を表示する 72
NX-OS スタイルの CLI を使用した Cisco ACI Virtual Edge の EPG 内分離の設定 73
トラブルシューティング 74
エンドポイント接続のトラブルシューティング 74
エンドポイント ステータスの検査 75
トンネル インターフェイス ステータスの検査 76

エンドポイント 間での traceroute の実行 76
アトミック カウンタの構成 77
Cisco APIC GUI を使用したテナント SPAN セッションの設定 78
IP bエース EPG 構成の確認 79
GUI を使用した IP ベースの EPG 構成の確認 79
スイッチ コマンドを使用した IP-EPG 構成の確認 80

第 7 章 アクセス インターフェイス 83
アクセス インターフェイスについて 83
物理ポートの構成 86
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 87
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 89
GUI を使用したインターフェイス構成の変更 90
GUI を使用したインターフェイス構成の表示 91
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 91
ポート チャネル 95
PC ホスト ロード バランシング アルゴリズム 95
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 96
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 98
ポートチャネル ダイナミック ロードバランシング 105
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 107
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 108
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 108
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 109
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 110
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 111
Cisco ACI の仮想ポート チャネル 114
Cisco ACI 仮想ポートチャネルのワークフロー 116

GUI を使用した vPC の定義 117
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 119
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 119
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 121
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 123
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 125
リフレクティブ リレー (802.1Qbg) 130
GUI を使用したリフレクティブ リレーの有効化 131
NX-OS は、CLI を使用してリフレクティブ リレーの有効化 132
FEX デバイスへのポート、PC、および vPC 接続の設定 133
ACI FEX のガイドライン 134
FEX 仮想ポート チャネル 134
GUI を使用した ACI リーフ スイッチへの FEX 接続の構成 136
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 138
ポート プロファイルの設定 139
ポート プロファイルの設定のまとめ 145
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 152
NX-OS スタイル CLI を使用したポート プロファイルの設定 153
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 154
インターフェイス構成の編集 155

第 8 章 **FCoE 接続** 157
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 157
Fibre Channel over Ethernet のガイドラインと制限事項 160
Fibre Channel over Ethernet（FCoE）をサポートするハードウェア 160

APIC GUI を使用した FCoE の設定 161
FCoE GUI の設定 161
FCoE ポリシー、プロファイル、およびドメインの設定 161
APIC GUI を使用した FCoE vFC ポートの展開 164
APIC GUI を使用した vFC ポートへの EPG アクセスの展開 172
FCoE Initiation Protocol をサポートする EPG の導入 177
APIC GUI を使用した FCoE 接続のアンデプロイ 179
NX-OS スタイルの CLI を使用した FCoE の設定 181
FCoE NX-OS スタイル CLI 設定 181
NX-OS スタイル CLI を使用したポリシーまたはプロファイルのない FCoE 接続の設定 181
NX-OS スタイル CLI を使用したポリシーまたはプロファイルがある FCoE 接続の設定 185
NX-OS スタイル CLI を使用して FCoE オーバー FEX の設定 189
NX-OS スタイルの CLI を使用した FCoE 設定の検証 191
NX-OS スタイル CLI を使用した FCoE 要素の展開解除 192
vPC による SAN ブート 193
GUI を使用した vPC による SAN ブートの設定 195
CLI を使用した vPC による SAN ブートの設定 198

第 9 章
ファイバ チャネル NPV 201
ファイバ チャネル接続の概要 201
NPV トラフィック管理 204
自動アップリンク選択 204
トラフィック マップ 205
複数の NP リンクにまたがるサーバ ログインの破壊的自動ロード バランシング 205
FC NPV トラフィック管理のガイドライン 206
SAN A/B の分離 207
SAN ポート チャネル 207
ファイバ チャネル N ポート仮想化のガイドラインと制限事項 208
ファイバ チャネル N ポート仮想化でサポートされるハードウェア 210
ファイバ チャネル N ポート仮想化の相互運用性 210

ファイバ チャネル NPV GUI の設定 211
GUI を使用したネイティブ ファイバ チャネル ポート プロファイルの設定 211
GUI を使用したネイティブ FC ポート チャネル プロファイルの設定 213
ファイバ チャネル ポートの展開 215
ファイバ チャネル ポートのトラフィック マップの設定 218
ファイバ チャネル NPV NX-OS スタイル CLI の設定 219
CLI を使用したファイバ チャネル インターフェイスの設定 219
CLI を使用したファイバ チャネル NPV ポリシーの設定 221
CLI を使用した NPV トラフィック マップの設定 223
ファイバ チャネル NPV REST API の設定 223
REST API を使用した FC 接続の設定 223

第 10 章 **802.1 q トンネリング 229**
ACI 802.1 q トンネルについて 229
GUI を使用した802.1Q トンネルの設定 232
APIC GUI を使用した 802. 1 Q トンネル インターフェイスの設定 232
NX-OS スタイルの CLI を使用した 802.1Q トンネルの設定 234
NX-OS スタイル CLI を使用した802.1Q トンネルの設定 234
例：NX-OS スタイル CLI でポートを使用する 802.1Q トンネルを設定する 236
例：NX-OS スタイル CLI でポート チャネルを使用する 802.1Q トンネルを設定する 236
例：NX-OS スタイル CLI で仮想ポート チャネルを使用する 802.1Q トンネルを設定する 237

第 11 章 **Epg の Q-で-Q カプセル化のマッピング 239**
Epg の Q-で-Q カプセル化のマッピング 239
GUI を使用した EPG の Q-in-Q カプセル化マッピングの設定 240
GUI を使用して、特定のリーフ スイッチ インターフェイス上で Q-in-Q カプセル化を有効にします 240
GUI を使用したファブリック インターフェイス ポリシーでリーフ インターフェイスの Q-in-Q カプセル化の有効化 242
GUI を使用して EPG から Q-in-Q カプセル化が有効なインターフェイスにマッピングする 243

NX-OS スタイル CLI を使用した Q-in-Q カプセル化リーフ インターフェイスへの EPG のマッピング 244

第 12 章 ブレークアウト ポート 247

ブレークアウト ポートの設定 247

ダウンリンクのダイナミック ブレークアウト ポートの注意事項と制約事項 248

ファブリック リンクの自動ブレークアウト ポートの注意事項と制約事項 253

GUI を使用したプロファイルおよびセレクタによるブレークアウト ポートの構成 256

GUI を使用したプロファイルおよびセレクタによるブレークアウト ポートの構成 259

GUI を使用したインターフェイス コンフィギュレーションによるブレークアウト ポートの設定 262

NX-OS スタイルの CLI を使用したダイナミック ブレイクアウト ポートの設定 263

第 13 章 プロシキ ARP 269

プロキシ ARP について 269

注意事項と制約事項 276

プロキシ ARP がサポートされている組み合わせ 277

拡張 GUI を使用したプロキシ ARP の設定 277

プロキシ ARP は、Cisco NX-OS スタイル CLI を使用しての設定 278

第 14 章 トラフィック ストーム制御 281

トラフィック ストーム制御について 281

ストーム制御の注意事項と制約事項 282

GUI を使用したトラフィック ストーム制御ポリシーの設定 285

NX-OS スタイルの CLI を使用したトラフィック ストーム制御ポリシーの設定 287

ストーム制御 SNMP トラップの設定 288

ストーム トラップ 289

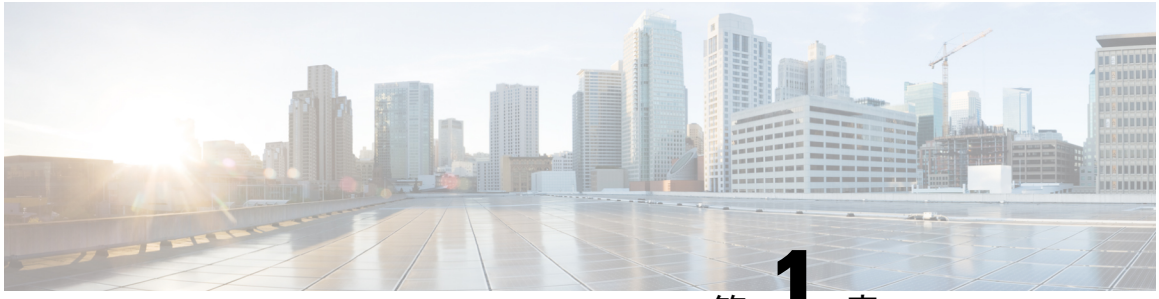
第 15 章 MACsec 291

MACsec について 291

スイッチ プロファイルの注意事項および制約事項 293

GUI を使用したファブリック リンクの MACsec の設定 297
GUI を使用したアクセス リンクの MACsec の設定 297
APIC GUI を使用した MACsec パラメータの設定 298
GUI を使用した MACsec キーチェーン ポリシーの設定 299
NX-OS スタイルの CLI を使用したMACsecの設定 300

第 16 章 ファブリック ポート トラッキング 303
ファブリック ポート トラッキングについて 303
GUI を使用したファブリック ポート トラッキングの設定 304



第 1 章

新機能および変更された機能

この章の内容は、次のとおりです。

- 新機能および変更された機能に関する情報 （1 ページ）

新機能および変更された機能に関する情報

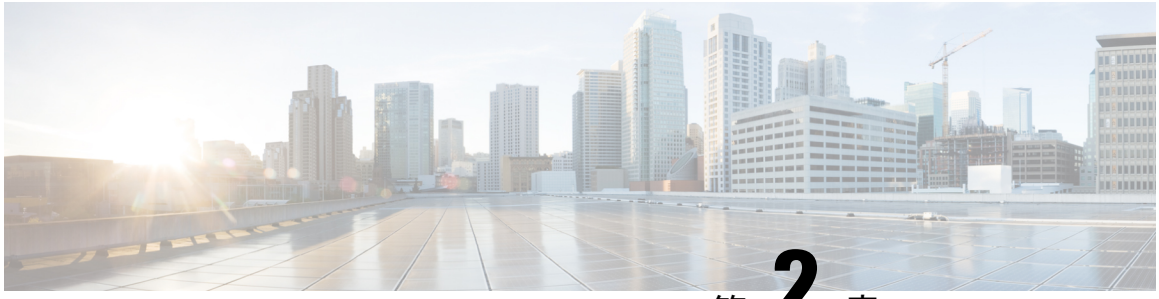
次の表に、本リリースに関するこのガイドでの重要な変更点の概要を示します。ただし、今リリースまでのガイドにおける変更点や新機能の一部は表に記載されていません。

表 *1 : Cisco APIC 6.1(2)* の新機能と変更点に関する情報

特長	説明	参照先
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。ポート チャネル DLB により、トラフィックが効率的に分散され、ネットワーク パフォーマンスが向上します。	ポートチャネル ダイナミックロードバランシング （105 ページ）

表 *2 : Cisco APIC 6.1*（*1*）の新機能および変更情報

特長	説明	参照先
該当なし	同様の LEM タイプを使用したポート プロファイルの構成に制限を追加しました。	ポート プロファイルの設定
該当なし	このドキュメントには、以前のリリースからの変更はありません。	N/A



第 2 章

Cisco ACI 転送

この章は、次の内容で構成されています。

- ACI ファブリックは現代のデータ センター トラフィック フローを最適化する （3 ページ）
- ACI で VXLAN （4 ページ）
- サブネット間のテナント トラフィックの転送を促進するレイヤ 3 VNID （6 ページ）
- スパニング ツリー プロトコル BPDU の送信 （8 ページ）

ACI ファブリックは現代のデータ センター トラフィック フローを最適化する

Cisco ACI アーキテクチャは、従来のデータセンター設計から来る制限を解放して、最新のデータセンターで増大する East-West トラフィックの需要に対応します。

今日のアプリケーション設計は、データセンターのアクセス レイヤを通る、サーバ間の East-West トラフィックを増大させています。このシフトを促進しているアプリケーションには、Hadoop のようなビッグデータの分散処理の設計 、VMware vMotion のようなライブの仮想マシンまたはワークロードの移行、サーバのクラスタ リング、および多層アプリケーションなどが含まれます。

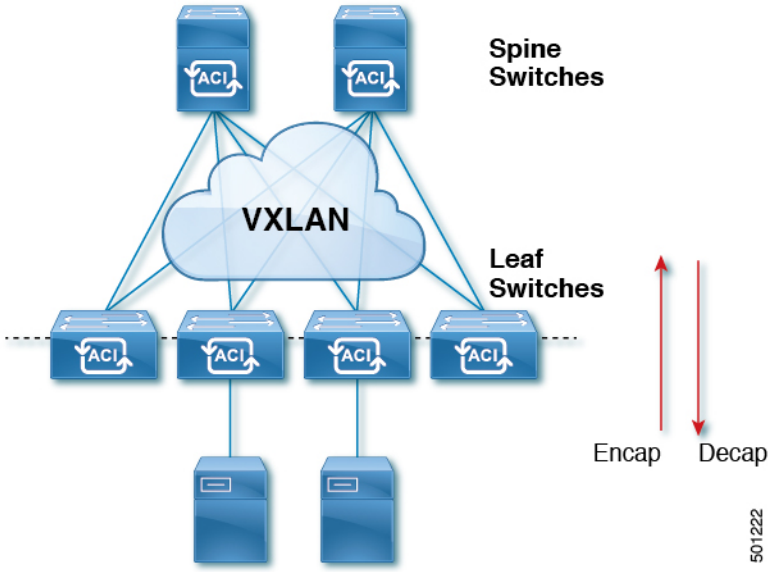
North-South トラフィックは、コア、集約、およびアクセス レイヤ、またはコラプスト コアとアクセス レイヤが重要となる、従来型のデータセンター設計を推進します。クライアントデータはWAN またはインターネットで受信され、サーバの処理を受けた後、データセンターを出ます。このような方式のため、WAN またはインターネットの帯域幅の制限により、デーセンターのハードウェアは過剰設備になりがちです。ただし、スパニング ツリー プロトコルが、ループをブロックするために要求されます。これは、ブロックされたリンクにより利用可能な帯域幅を制限し、トラフィックが準最適なパスを通るように強制する可能性があります。

従来のデータセンター設計においては、、IEEE 802.1Q VLAN がレイヤ 2 境界の論理セグメンテーションまたはまたはブロードキャスト ドメインを提供します。ただし、ネットワーク リンクの VLAN の使用は効率的ではありません。データセンター ネットワークでデバイスの配置要件は柔軟性に欠け、VLAN の最大値である 4094 の VLAN が制限となり得ます。IT 部門と

クラウドプロバイダが大規模なマルチテナントデータセンターを構築するようになるにつれ、VLAN の制限は問題となりつつあります。

スパイン リーフ アーキテクチャは、これらの制限に対処します。ACI ファブリックは、外界からは、ブリッジングとルーティングが可能な単一のスイッチに見えます。レイヤ 3 のルーティングをアクセス レイヤに移動すると、最新のアプリケーションが必要としている、レイヤ 2 の到達可能性が制限されます。仮想マシン ワークロード モビリティや一部のクラスタ リングのソフトウェアのようなアプリケーションは、送信元と宛先のサーバ間がレイヤ2で隣接していることを必要とします。アクセス レイヤでルーティングを行えば、トランク ダウンされた同じ VLAN の同じアクセス スイッチに接続したサーバだけが、レイヤ 2 で隣接します。ACI では、VXLAN が、基盤となるレイヤ 3 ネットワーク インフラストラクチャからレイヤ 2 のドメインを切り離すことにより、このジレンマを解決します。

図 *1: ACI* ファブリック



トラフィックがファブリックに入ると、ACI がカプセル化してポリシーを適用し、必要に応じてスパイン スイッチ (最大 2 ホップ) によってファブリックを通過させ、ファブリックを出るときにカプセル化を解除します。ファブリック内では、ACI はエンドポイント間通信でのすべての転送について、Intermediate System-to-Intermediate System プロトコル (IS-IS) および Council of Oracle Protocol (COOP) を使用します。これにより、すべての ACI リンクがアクティブで、ファブリック内での等コストマルチパス (ECMP) 転送と高速再コンバージョンが可能になります。ファブリック内と、ファブリックの外部のルータ内でのソフトウェア定義ネットワーク間のルーティング情報を伝播するために、 ACI はマルチプロトコル Border Gateway Protocol (MP-BGP) を使用します。

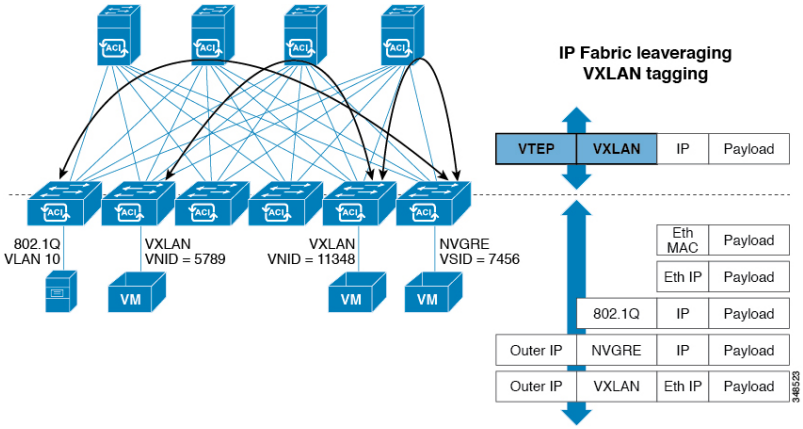
ACI で VXLAN

VXLAN は、レイヤ 2 オーバーレイの論理ネットワークを構築するレイヤ 3 のインフラストラクチャ上でレイヤ 2 のセグメントを拡張する業界標準プロトコルです。ACIインフラストラク

チャ レイヤ 2 ドメインが隔離ブロードキャストと障害ブリッジ ドメインをオーバーレイ内に存在します。このアプローチは大きすぎる、障害ドメインの作成のリスクなしで大きくなるデータセンター ネットワークを使用できます。

すべてのトラフィック、ACI ファブリックは VXLAN パケットとして正規化されます。入力で ACI VXLAN パケットで外部 VLAN、VXLAN、および NVGRE パケットをカプセル化します。次の図は、ACI カプセル化の正規化を示します。

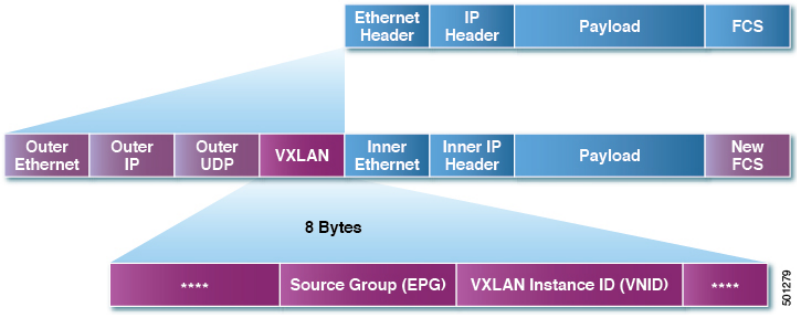
図 2 : ACI カプセル化の正規化



ACI ファブリックでの転送は、カプセル化のタイプまたはカプセル化のオーバーレイ ネットワークによって制限または制約されません。ACI ブリッジ ドメインのフォワーディング ポリシーは、必要な場合に標準の VLAN 動作を提供するために定義できます。

ファブリック内のすべてのパケットに ACI ポリシー属性が含まれているため、ACI は完全に分散された方法でポリシーを一貫して適用できます。ACI により、アプリケーション ポリシーの EPG ID が転送から分離されます。次の図に示すように、ACI VXLAN ヘッダーは、ファブリック内のアプリケーション ポリシーを特定します。

図 3 : ACI VXLAN のパケット形式



ACIVXLAN パケットには、レイヤ 2 の MAC アドレスとレイヤ 3 IP アドレスの送信元と宛先フィールド、ファブリック内の効率的なと拡張性の転送を有効にします。ACIVXLAN パケット ヘッダーの送信元グループ フィールドは、パケットが属するアプリケーション ポリシー エンドポイント グループ (EPG) を特定します。VXLAN インスタンス ID (VNID) は、テナントの仮想ルーティングおよび転送 (VRF) ドメイン ファブリック内で、パケットの転送を有効にし

ます。VXLAN ヘッダーで 24 ビット VNID フィールドでは、同じネットワークで一意レイヤ 2 のセグメントを最大 16 個の拡張アドレス空間を提供します。この拡張アドレス空間は、大規模なマルチテナント データセンターを構築する柔軟性 IT 部門とクラウド プロバイダーを提供します。

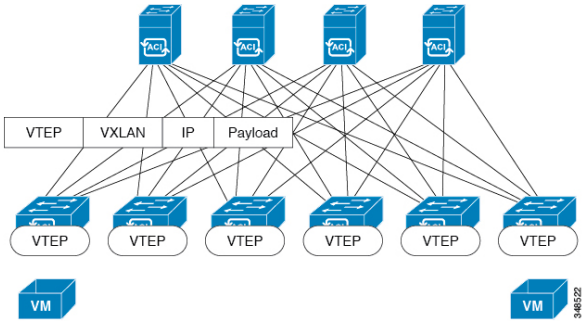
VXLAN を有効に ACI ファブリック全体にわたってスケールでの仮想ネットワーク インフラストラクチャのレイヤ 3 のアンダーレイ レイヤ 2 を展開します。アプリケーション エンドポイント ホスト柔軟に配置できます、アンダーレイ インフラストラクチャのレイヤ 3 バウンダリのリスクなしでデータセンター ネットワーク間をオーバーレイ ネットワーク、VXLAN でレイヤ 2 の隣接関係を維持します。

サブネット間のテナント トラフィックの転送を促進するレイヤ 3 VNID

ACI ファブリックは、ACI ファブリック VXLAN ネットワーク間のルーティングを実行するテナントのデフォルト ゲートウェイ機能を備えています。各テナントに対して、ファブリックはテナントに割り当てられたすべてのリーフ スイッチにまたがる仮想デフォルト ゲートウェイを提供します。これは、エンドポイントに接続された最初のリーフ スイッチの入力インターフェイスで提供されます。各入力インターフェイスはデフォルト ゲートウェイ インターフェイスをサポートします。ファブリック全体のすべての入力インターフェイスは、特定のテナント サブネットに対して同一のルータの IP アドレスと MAC アドレスを共有します。

ACI ファブリックは、エンドポイントのロケータまたは VXLAN トンネル エンドポイント (VTEP) アドレスで定義された場所から、テナント エンドポイント アドレスとその識別子を切り離します。ファブリック内の転送は VTEP 間で行われます。次の図は、ACI で切り離された ID と場所を示します。

図 *4: ACI* によって切り離された *ID* と場所



VXLAN は VTEP デバイスを使用してテナントのエンド デバイスを VXLAN セグメントにマッピングし、VXLAN のカプセル化およびカプセル化解除を実行します。各 VTEP 機能には、次の 2 つのインターフェイスがあります。

- ブリッジングを介したローカル エンドポイント通信をサポートするローカル LAN セグメントのスイッチ インターフェイス
- 転送 IP ネットワークへの IP インターフェイス

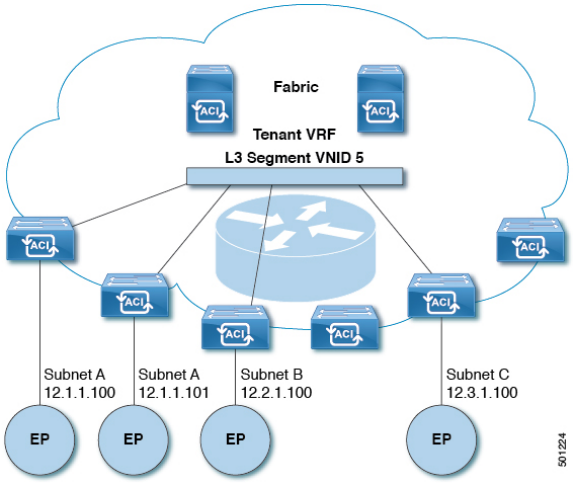
IP インターフェイスには一意の IP アドレスがあります。これは、インフラストラクチャ VLAN として知られる、転送 IP ネットワーク上の VTEP を識別します。VTEP デバイスはこの IP アドレスを使用してイーサネット フレームをカプセル化し、カプセル化されたパケットを、IP インターフェイスを介して転送ネットワークへ送信します。また、VTEP デバイスはリモート VTEP で VXLAN セグメントを検出し、IP インターフェイスを介してリモートの MAC Address-to-VTEP マッピングについて学習します。

ACI の VTEP は分散マッピング データベースを使用して、内部テナントの MAC アドレスまたは IP アドレスを特定の場所にマッピングします。VTEP はルックアップの完了後に、宛先リーフ スイッチ上の VTEP を宛先アドレスとして、VXLAN 内でカプセル化された元のデータ パケットを送信します。宛先リーフ スイッチはパケットをカプセル化解除して受信ホストに送信します。このモデルにより、ACI はスパニングツリー プロトコルを使用することなく、フルメッシュでシングル ホップのループフリー トポロジを使用してループを回避します。

VXLAN セグメントは基盤となるネットワーク トポロジに依存しません。逆に、VTEP 間の基盤となる IP ネットワークは、VXLAN オーバーレイに依存しません。これは送信元 IP アドレスとして開始 VTEP を持ち、宛先 IP アドレスとして終端 VTEP を持っており、外部 IP アドレス ヘッダーに基づいてパケットをカプセル化します。

次の図は、テナント内のルーティングがどのように行われるかを示します。

図 *5 : ACI* のサブネット間のテナント トラフィックを転送するレイヤ *3 VNID*



ACI はファブリックの各テナント VRF に単一の L3 VNID を割り当てます。ACI は、L3 VNID に従ってファブリック全体にトラフィックを転送します。出力リーフ スイッチでは、ACI によって L3 VNID からのパケットが出力サブネットの VNID にルーティングされます。

ACI のファブリック デフォルト ゲートウェイに送信されてファブリック入力に到達したトラフィックは、レイヤ 3 VNID にルーティングされます。これにより、テナント内でルーティングされるトラフィックはファブリックで非常に効率的に転送されます。このモデルを使用すると、たとえば同じ物理ホスト上の同じテナントに属し、サブネットが異なる 2 つの VM 間では、トラフィックが (最小パス コストを使用して) 正しい宛先にルーティングされる際に経由する必要があるは入力スイッチ インターフェイスのみです。

ACI ルート リフレクタは、ファブリック内での外部ルートの配布にマルチプロトコル BGP（MP-BGP）を使用します。ファブリック管理者は自律システム (AS) 番号を提供し、ルート リフレクタにするスパイン スイッチを指定します。

（注） Cisco ACI は IP フラグメンテーションをサポートしていません。したがって、外部ルータへのレイヤ 3 Outside（L3Out）接続、または Inter-Pod Network（IPN）を介したマルチポッド接続を設定する場合は、インターフェイス MTU がリンクの両端で適切に設定することを推奨します。

IGP プロトコル パケット（EIGRP、OSPFv3）は、インターフェイス MTU サイズに基づいてコンポーネントによって構築されます。 Cisco ACIでは、CPU MTU サイズがインターフェイス MTU サイズよりも小さく、構築されたパケットサイズが CPU MTU より大きい場合、パケットはカーネルによってドロップされます（特に IPv6）。このような制御パケットのドロップを回避するには、コントロールプレーンとインターフェイスの両方で常に同じ MTU 値を設定します。

Cisco ACI、Cisco NX-OS、および Cisco IOS などの一部のプラットフォームでは、設定可能な MTU 値はイーサネット ヘッダー (一致する IP MTU、14-18 イーサネット ヘッダー サイズを除く) を考慮していません。また、IOS XR などの他のプラットフォームには、設定された MTU 値にイーサネットヘッダーが含まれています。設定された値が 9000 の場合、Cisco ACI、Cisco NX-OS および Cisco IOS の最大 IP パケット サイズは 9000 バイトになりますが、IOS-XR のタグなしインターフェイスの最大 IP パケットサイズは 8986 バイトになります。

各プラットフォームの適切な MTU 値については、それぞれの設定ガイドを参照してください。

CLI ベースのコマンドを使用して MTU をテストすることを強く推奨します。たとえば、Cisco NX-OS CLI で、コマンド、ping 1.1.1.1 df-bit packet-size 9000 source-interface ethernet 1/1 を使用してください。

スパニング ツリー プロトコル BPDU の送信

スパニング ツリープロトコル（STP）を実行している 2 つ以上のスイッチが EPG の Cisco Application Centric Infrastructure（ACI）に接続されており、スタティックポートが次のように割り当てられている場合：

- EPG で静的に割り当てられたすべてのポートは、タグなしでアクセスされます。STP ブリッジ プロトコル データ ユニット（BPDU）はタグなしで送受信されます。
- スタティックに割り当てられたトランクポートとスタティックに割り当てられたアクセスタグなしポートが混在している場合：トランク ポートで受信された STP BPDU は、`dot1q` タグ付きのアクセス タグなしポートに送信されます。したがって、アクセス ポートは不整合状態になります。
- EPG で静的に割り当てられたトランク ポートと静的に割り当てられたアクセス ポートの組み合わせの場合、Cisco ACI は `dot1q` タグを使用してSTP BPDUを送信し、アクセスポートは `802.1p` アクセスを使用します。

この場合、タグ付き STP パケットを受信して処理するには、レイヤ 2 スイッチで 802.1p アクセスを使用する必要があります。

802.1p がレイヤ 2 スイッチで許可されていない場合は、トランク ポート アクセスを使用します。

- Cisco ACI は全二重ハブとして機能し、BPDU が受信されたカプセル化 VLAN に関連付けられた VxLAN VNID 内でスパニング ツリー BPDU をフラッディングします。Cisco ACI は全二重メディアであるため、高速スパニングツリー プロトコル（RSTP）または高速 VLAN 単位スパニングツリー（RPVST）のバージョンを実行する外部スイッチは、デフォルトでポイントツーポイント リンク タイプになります。その結果、STP を実行し、同じカプセル化 VLAN および EPG VNID に接続する 2 つ以上の外部スイッチがある場合、コンバージェンスと不安定性の問題を回避するために、外部スイッチインターフェイスでリンク タイプを「共有」に設定する必要があります。これらの問題は、スイッチがこのカプセル化に接続されているすべてのブリッジ（または STP 対応スイッチ）から BPDU を受信するために発生する可能性があります。

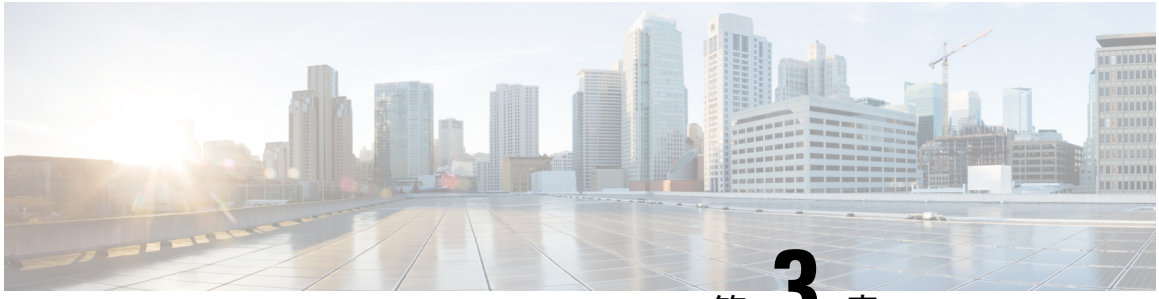
スパニング ツリー BPDU は、EPG パスで定義された特定の VLAN ID 内でフラッディングされます。このVLANは、リーフスイッチでは FD_VLAN と呼ばれます。リーフスイッチ間でFD_VLAN 内のトラフィックを転送するために、Cisco ACI は、fabric_encap と呼ばれる VXLAN VNID を割り当てます。fabric_encap は、VLAN プールに属する数値ベース識別子を取得し、VLAN プールから割り当てられた VLAN ID のインデックス値を追加することによって取得されます。たとえば、VXLAN VNID 9000 は、VLAN 範囲 10 ー 20 を含む VLAN プール A に割り当てられます。VLAN プール A の VLAN 10 には VNID 9000 が割り当てられ、VLAN 11 には VNID 9001 が割り当てられます。

このため、2 つの異なる EPG が同じ VLAN ID を使用しており、同じ VLAN プールからその VLAN ID を割り当てている場合は、異なるファブリックスイッチ上の 2 つの EPG に対して同じ fabric_encap VNID を導出できます。これにより、2 つの EPG 間でスパニング ツリー BPDU が意図せずフラッディングされる可能性があります。

この動作を回避するには、物理ドメインなどの個別の VLAN プールを持つ異なるドメインを各 EPG に割り当て、特定の VLAN ID を個別の VLAN プールから割り当てます。これにより、ベース ID が異なるようになるので、fabric_encap VNIDの重複が防止されます。

fabric_encap の値は、次のコマンドを使用して確認できます。また、特定の 802.1q VLAN ID のリーフ スイッチの出力の「Fabric_enc」列でも確認できます。

```
vsh_lc -c "show system internal eltmc info vlan br"
```



第 3 章

レイヤ 2 ネットワーク設定の前提条件

- レイヤ 2 の前提条件 （11 ページ）

レイヤ 2 の前提条件

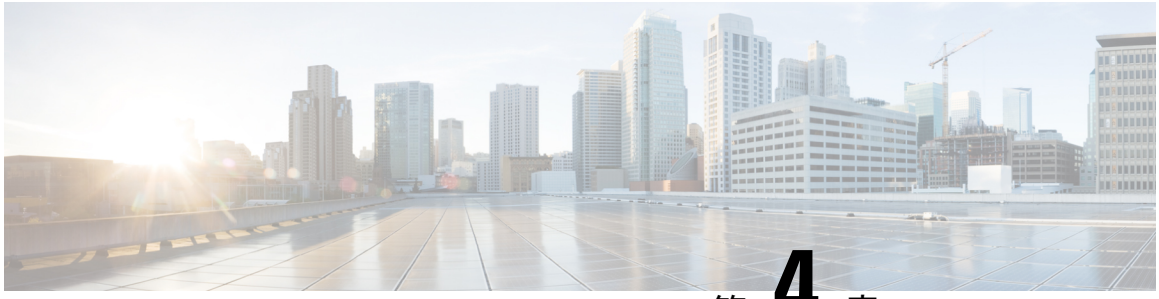
このガイドで説明するタスクを実行する前に、以下の事柄を完了しておいてください。

- ACI ファブリックをインストールして、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いて健全な状態であることを確認します。詳細については、『*Cisco APIC Getting Started Guide, Release 2.x*』を参照してください。
- レイヤ 2 ネットワークを設定する管理者のために、ファブリックの管理者アカウントを作成します。 詳細については、『*Cisco APIC Basic Configuration Guide*』の「*User Access, Authentication, and Accounting*」および「*Management*」の章を参照してください。
- ACI ファブリックにターゲット リーフ スイッチをインストールし、登録します。詳細については、『*Cisco APIC Getting Started Guide, Release 2.x*』を参照してください。

  仮想スイッチのインストールと登録の詳細については、『*Cisco ACI Virtualization Guide*』を参照してください。
- レイヤ 2 ネットワークを利用するテナント、VRF、および EPG を (アプリケーション プロファイルやコントラクトとともに) 設定します。詳細については、『*Cisco APIC Basic Configuration Guide*』の「*Basic User Tenant Configuration*」の章を参照してください。

⚠

注意 ファブリックのリーフ スイッチとスパイン スイッチの間に 1 ギガビット イーサネット (GE) または 10GE リンクを設置すると、帯域幅が不十分なために、パケットが転送されずにドロップされる可能性があります。これを避けるためには、リーフ スイッチとスパイン スイッチの間で 40GE または 100GE リンクを使用してください。



第 4 章

ネットワーク ドメイン

この章は、次の内容で構成されています。

- ネットワーク ドメイン （13 ページ）
- ブリッジ ドメイン （14 ページ）
- VMM ドメイン （14 ページ）
- 物理ドメイン設定 （16 ページ）

ネットワーク ドメイン

ファブリック管理者は、ポート、プロトコル、VLANプール、およびカプセル化を設定するドメインポリシーを作成します。これらのポリシーは、単一テナント専用にすることも、共有することもできます。ファブリック管理者がACIファブリック内にドメインを設定すると、テナント管理者はテナント エンドポイント グループ（EPG）をドメインに関連付けることができます。

以下のネットワーク ドメイン プロファイルを設定できます。

- VMM ドメイン プロファイル（`vmmDomP`）は、仮想マシンのハイパーバイザ統合のために必要です。
- 物理ドメイン プロファイル（`physDomP`）は、ベア メタル サーバ接続と管理アクセスに使用します。
- ブリッジド外部ネットワーク ドメイン プロファイル（`l2extDomP`）は通常、ACI ファブリックのリーフ スイッチにブリッジド外部ネットワーク トランク スイッチを接続するために使用されます。
- ルーテッド外部ネットワーク ドメイン プロファイル（`l3extDomP`）は、ACI ファブリックのリーフ スイッチにルータを接続するために使用されます。
- ファイバチャネル ドメイン プロファイル(`fcDomP`)は、ファイバチャネルの VLAN と VSAN を接続するために使用されます。

ドメインは VLAN プールに関連付けられるように設定されます。その後、EPG は、ドメインに関連付けられている VLAN を使用するように設定されます。

（注） EPG ポートと VLAN の設定は、EPG が関連付けられているドメイン インフラストラクチャ設定で指定されている設定に一致する必要があります。一致しない場合、APIC でエラーが発生します。そのようなエラーが発生した場合は、ドメインインフラストラクチャ設定が EPG ポートと VLAN の設定に一致していることを確認してください。

関連資料

レイヤ 3 のネットワー キングの詳細については、『*Cisco APIC Layer 3 Networking Configuration Guide*』を参照してください。

VMM ドメインの設定の詳細については、『*Cisco ACI Virtualization Guide*』の「*Cisco ACI Virtual Machine Networking*」を参照してください。

ブリッジ ドメイン

ブリッジ ドメインについて

ブリッジ ドメイン (BD) はファブリック内のレイヤ 2 フォワーディングの構造を表します。1 つ以上のエンドポイント グループ（EPG）を 1 つのブリッジ ドメインまたはサブネットと関連付けることができます。ブリッジ ドメインには1つまたは複数のサブネットを関連付けることができます。1 つまたは複数のブリッジ ドメインの組み合わせによってテナント ネットワークを形成します。2 つの EPG の間でのサービス機能を挿入するときには、それらの EPG は個別 BD の中になければなりません。2 つの EPG の間でのサービス機能を使用するには、これらの EPG は分離している必要があります。このことは、レイヤ 2 およびレイヤ 3 に基づく、レガシー サービス 挿入に従います。

VMM ドメイン

Virtual Machine Manager ドメインの主要コンポーネント

ACI ファブリック Virtual Machine Manager（VMM）ドメインにより、管理者は仮想マシン コントローラの接続ポリシーを設定できます。ACI VMM ドメイン ポリシーの基本的なコンポーネントは次のとおりです。

- **Virtual Machine Manager ドメイン プロファイル**：同様のネットワーキング ポリシー要件を持つ VM コントローラをグループ化します。たとえば、VM コントローラは VLAN プールとアプリケーション エンドポイント グループ（EPG）を共有できます。APIC はコントローラと通信し、のちに仮想ワークロードに適用されるポート グループなどのネットワー

ク設定を公開します。VMM ドメイン プロファイルには、次の基本コンポーネントが含まれます。

- **クレデンシャル**：有効な VM コントローラ ユーザ クレデンシャルを APIC VMM ドメインと関連付けます。
- **コントローラ**：ポリシーの適用ドメインの一部である VM コントローラへの接続方法を指定します。たとえば、コントローラは VMM ドメインの一部である VMware vCenter への接続を指定します。

（注） 1 つのドメインに VM コントローラの複数のインスタンスを含めることができますが、それらは同じベンダーのものである必要があります（VMware または Microsoft など）。

- **EPG の関連付け**：エンドポイント グループにより、エンドポイント間の接続と可視性が VMM ドメイン ポリシーの範囲内に規制されます。VMM ドメイン EPG は次のように動作します。
  - APIC は、これらの EPG をポート グループとして VM コントローラにプッシュします。
  - 1 つの EPG は、複数の VMM ドメインをカバーでき、1 つの VMM ドメインには複数の EPG を含めることができます。
- **接続可能エンティティ プロファイルの関連付け**：VMM ドメインを物理ネットワーク インフラストラクチャと関連付けます。接続可能エンティティ プロファイル（AEP）は、多数のリーフ スイッチ ポートで VM コントローラ ポリシーを展開するための、ネットワーク インターフェイス テンプレートです。AEP は、使用できるスイッチやポートおよびその設定方法を指定します。
- **VLAN プールの関連付け**：VLAN プールは、VMM ドメインが消費する VLAN カプセル化に使用する VLAN ID または範囲を指定します。

Virtual Machine Manager のドメイン

APIC VMM ドメイン プロファイルは、VMM ドメインを定義するポリシーです。VMM ドメイン ポリシーは APIC で作成され、リーフ スイッチにプッシュされます。

VMM ドメインは以下を提供します。

- 複数の VM コントローラ プラットフォームに対してスケーラブルな耐障害性サポートを可能にする、ACI ファブリックの共通レイヤ
- ACI ファブリック内の複数のテナントに対する VMM サポート

VMM ドメインには、VMware vCenter や Microsoft SCVMM Manager などの VM コントローラと、VM コントローラと対話するための ACI API に必要なクレデンシャルが含まれます。VMM ドメインはドメイン内の VM モビリティを実現できますが、ドメイン間は実現できません。単一の VMM ドメイン コントローラに VM コントローラの複数のインスタンスを含めることはできますが、同じタイプである必要があります。たとえば、1 つの VMM ドメインに、それぞれが複数の VM を実行する複数のコントローラを管理する多くの VMware vCenter を含めることができますが、SCVMM Manager も含めることはできません。VMM ドメインはコントローラ要素（pNIC、vNIC、VM 名など）をインベントリに含め、コントローラにポリシーをプッシュして、ポート グループなどの必要な要素を作成します。ACI VMM ドメインは VM モビリティなどのコントローラ イベントを監視し、状況に応じて応答します。

物理ドメイン設定

物理ドメインの設定

物理ドメインは、特定の VLAN ネームスペースが使用される範囲を制御します。物理ドメインと関連付けられた VLAN のネームスペースは、仮想サーバからのポート グループのスタティック マッピングに使用できますが、非仮想サーバを対象としています。物理デバイス タイプの物理ドメインを設定できます。

始める前に

- テナントを設定します。

手順

ステップ 1 メニュー バーで [Fabric] をクリックします。

ステップ 2 サブメニュー バーで [External Access Policies] をクリックします。

ステップ 3 [Navigation] ウィンドウで、[Physical and External Domains] を展開し、[Physical Domains] をクリックします。

ステップ 4 [Actions] ドロップダウン リストで [Create Physical Domain] を選択します。[Create Physical Domain] ダイアログボックスが表示されます。

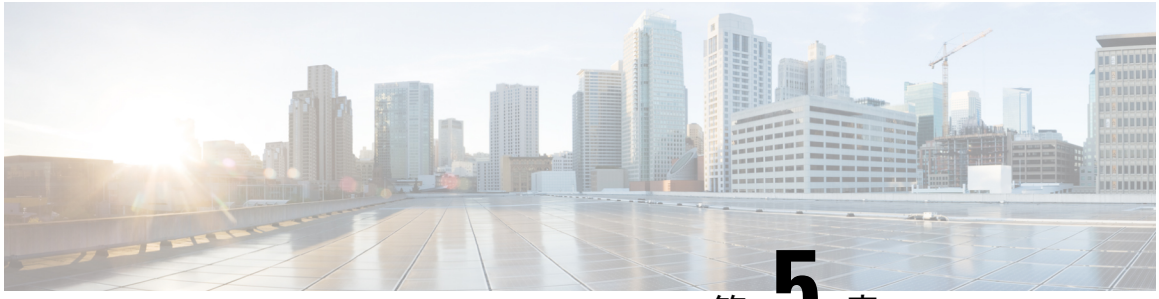
ステップ 5 次のフィールドに入力します。

名前	説明
[名前（Name）]	物理ドメイン プロファイルの名前。
Associate Attachable Entity Profiles	このドメインに関連付けられる、アタッチ可能なエンティティ プロファイルを選択します。
VLAN Pool	物理ドメインが使用する VLAN プール。VLAN プールは、APIC によってこの物理ドメインを使用しているサービス グループテン

名前	説明
	プレートに対して割り当てられる VLAN のプールの範囲を指定します。[Dynamic] または [Static] の割り当てをクリックします。

ステップ 6 （任意） AAA のセキュリティ ドメインを追加し、[Select] チェック ボックスをオンにします。

ステップ 7 [送信（Submit）] をクリックします。



第 5 章

ブリッジング

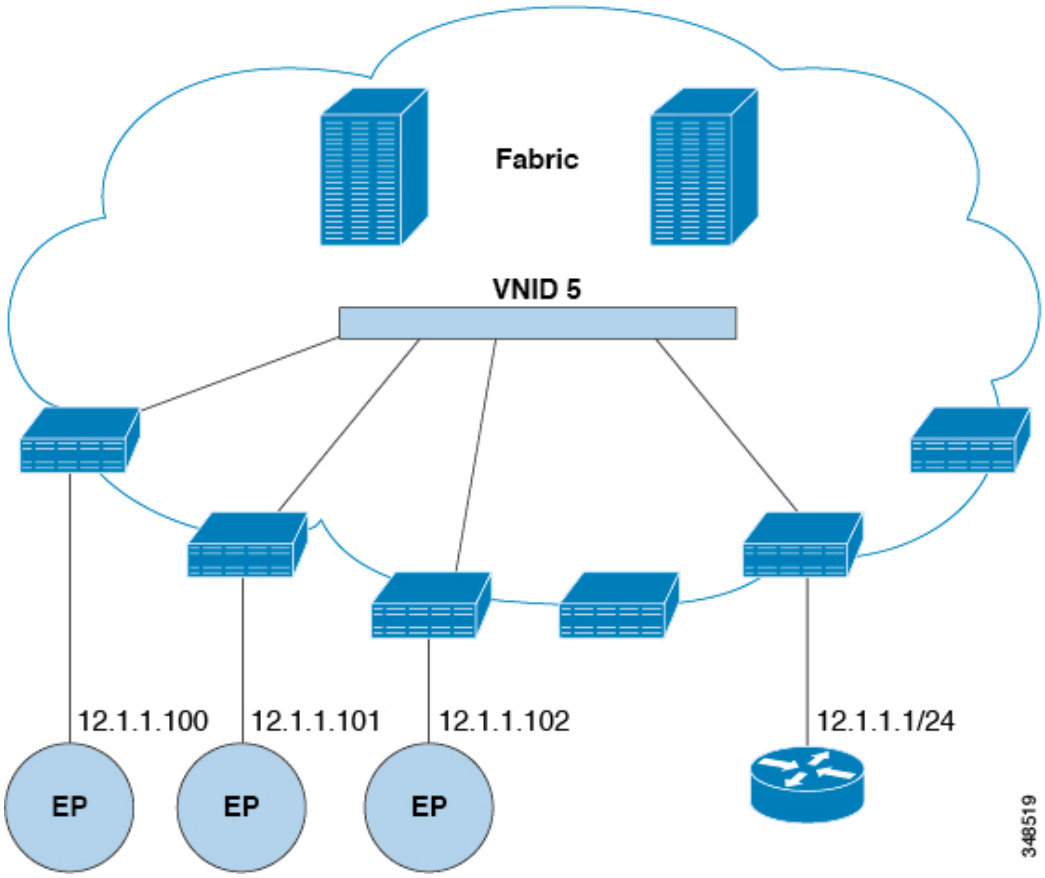
この章は、次の内容で構成されています。

- 外部ルータへのブリッジド インターフェイス （19 ページ）
- ブリッジ ドメインとサブネット （20 ページ）
- GUI を使用したテナント、VRF およびブリッジ ドメインの作成 （26 ページ）
- NX-OS CLI を使用した、テナント、VRF およびブリッジ ドメインの作成 （29 ページ）
- 適用されるブリッジ ドメインの設定 （30 ページ）
- カプセル化によるすべてのプロトコルおよびプロキシ ARP のカプセル化のフラッディングを設定する （33 ページ）

外部ルータへのブリッジド インターフェイス

次の図に示すように、リーフ スイッチのインターフェイスがブリッジド インターフェイスとして設定されている場合、テナント VNID のデフォルト ゲートウェイが外部ルータとなります。

図 *6:* ブリッジド外部ルータ

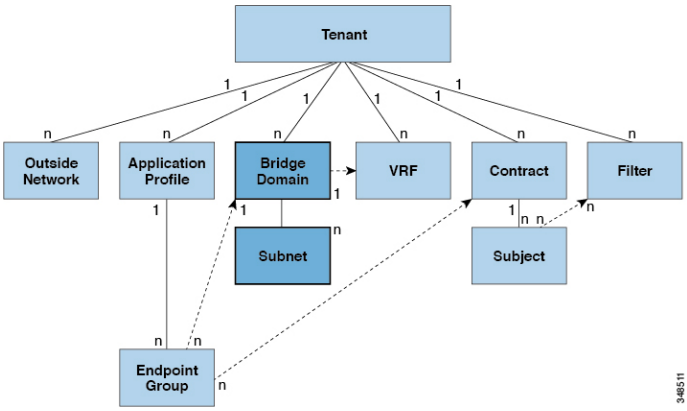


ACI ファブリックは、外部ルータの存在を認識せず、APIC はリーフ スイッチのインターフェイスを EPG に静的に割り当てます。

ブリッジ ドメインとサブネット

ブリッジ ドメイン（fvBD）は、ファブリック内のレイヤ 2 フォワーディングの構造を表します。次の図は、管理情報ツリー（MIT）内のブリッジ ドメインの場所とテナントの他のオブジェクトとの関係を示します。

図 7: ブリッジ ドメイン



ブリッジ ドメインは、VRF インスタンス（コンテキストまたはプライベート ネットワークとも呼ばれる）にリンクする必要があります。レイヤ 2 VLAN を除いて、少なくとも 1 つのサブネット（`fvSubnet`）が関連付けられている必要があります。フラッディングが有効な場合、ブリッジ ドメインは、一意のレイヤ 2 MAC アドレス空間とレイヤ 2 フラッド ドメインを定義します。VRF インスタンスが一意の IP アドレス空間を定義する一方で、そのアドレス空間は複数のサブネットで構成できます。これらのサブネットは、対応する VRF インスタンスを参照する 1 つ以上のブリッジ ドメインで定義されます。

ブリッジ ドメインまたは EPG の下のサブネットのオプションは次のとおりです。

- パブリック（*Public*）：サブネットをルーテッド接続にエクスポートできます。
- プライベート（*Private*）：サブネットはテナント内にのみ適用されます。
- 共有（*Shared*）：共有サービスの一部として、同じテナントまたは他のテナントにわたる複数の VRF インスタンスに対してサブネットの共有やエクスポートを行うことができます。共有サービスの例としては、異なるテナントの別の VRF インスタンスに存在する EPG へのルーテッド接続などがあります。これにより、トラフィックが VRF インスタンス間で双方向に移動することが可能になります。共有サービスを提供する EPG は、その EPG の下で（ブリッジ ドメインの下ではなく）サブネットを設定する必要があり、そのスコープは外部にアドバタイズするように設定し、VRF インスタンス間で共有する必要があります。

（注） 共有サブネットは、通信に含まれる VRF インスタンス全体で一意でなければなりません。EPG 下のサブネットがレイヤ 3 外部ネットワーク共有サービスを提供する場合、このようなサブネットは、Cisco Application Centric Infrastructure（ACI）ファブリック内全体でグローバルに一意である必要があります。

ブリッジ ドメイン パケットの動作は次の方法で制御できます。

パケット タイプ	モード
ARP	**ARP フラッディング** は有効または無効にできます。フラッディングを行わない場合、ARP パケットはユニキャストで送信されます。 （注） `limitIpLearnToSubnets` を `fvBD` で設定すると、ブリッジ ドメインの構成済みサブネット内または共有サービス プロバイダーである EPG サブネット内に IP アドレスが存在する場合のみ、エンドポイントの学習がブリッジ ドメインに限定されます。
未知のユニキャスト	**L2 Unknown Unicast** は、**Flood** または **Hardware Proxy** になり得ます。 （注） ブリッジ ドメインが **L2 Unknown Unicast** を持っており、それが **Flood** に設定されている場合、エンドポイントが削除されると、システムはそれを両方のローカル リーフ スイッチから削除します。そして、**Clear Remote MAC Entries** を選択すると、ブリッジ ドメインが展開されているリモートのリーフ スイッチからも削除されます。この機能を使用しない場合、リモート リーフは、タイマーが時間切れになるまで、学習したこのエンドポイントの情報を保持します。 **L2 Unknown Unicast** の設定を変更すると、このブリッジ ドメインに関連付けられた EPG にアタッチされているデバイスのインターフェイス上で、トラフィックがバウンスします (アップ ダウンします)。
未知の IP マルチキャスト	**L3 の不明なマルチキャスト フラッディング** **フラッド（Flood）**：パケットは入力および境界リーフ スイッチ ノードでのみフラッディングされます。N9K-93180YC-EX では、パケットは、ブリッジ ドメインが導入されているすべてのノードでフラッディングされます。 **最適化（Optimized）**：1 リーフあたり 50 のブリッジ ドメインのみサポートされます。この制限は N9K-93180YC-EX には該当しません。

パケット タイプ	モード
L2 マルチキャスト、ブロードキャスト、ユニキャスト	**マルチ宛先フラッディング**、次のいずれかになり得ます。 • **BD でフラッド（Flood in BD）**：ブリッジ ドメインにフラッドします。 • **カプセル化でフラッド（Flood in Encapsulation）**：カプセル化でフラッドします。 • **ドロップ（Drop）**：パケットをドロップします。

（注） Cisco APIC リリース 3.1(1) 以降では、Cisco Nexus 9000 シリーズ スイッチで (EX と FX で終わる名前を持つものとそれ以降)、次のプロトコルのカプセル化のフラッディングまたはブリッジ ドメインにフラッディングが可能です：OSPF/OSPFv3、BGP、EIGRP、LACP、ISIS、IGMP、PIM、ST-BPDU、ARP/GARP、RARP、および ND。

ブリッジ ドメインは複数のスイッチにまたがることができます。ブリッジ ドメインには複数のサブネットを含めることができますが、サブネットは単一のブリッジ ドメイン内に含まれます。ブリッジ ドメイン（fvBD）の `limitIPLearnToSubnets` プロパティが `yes` に設定されていると、ブリッジ ドメインの設定済みサブネットのいずれかの中に IP アドレスがあるとき、または EPG が共有サービス プロバイダーである場合には EPG サブネット内に IP アドレスがあるときのみ、ブリッジ ドメイン内でエンドポイントの学習が行われます。サブネットは複数の EPG にまたがることができ、1 つ以上の EPG を 1 つのブリッジ ドメインまたはサブネットに関連付けることができます。ハードウェアのプロキシ モードでは、異なるブリッジ ドメインのエンドポイントがレイヤ 3 のルックアップ動作の一部として学習されると、そのエンドポイントに ARP トラフィックが転送されます。

ブリッジ ドメイン オプション

ブリッジ ドメインは、不明なユニキャスト フレームのフラッド モードで、またはこれらのフレームのフラッディングを排除する最適化されたモードで動作するように設定できます。フラッディング モードで使用する場合、レイヤ 2 の不明なユニキャスト トラフィックはブリッジ ドメイン（GIP）のマルチキャスト ツリーでフラッディングされます。最適化されたモードでブリッジ ドメインを動作するようにするには、ハードウェア プロキシに設定する必要があります。この状況では、レイヤ 2 の不明なユニキャスト フレームはスパイン プロキシ エニーキャスト VTEP アドレスに送信されます。

注意 不明なユニキャスト フラッディング モードから hw プロキシ モードに変更すると、ブリッジ ドメイン内のトラフィックが停止します。

ブリッジ ドメインで IP ルーティングが有効になっている場合、マッピング データベースは、MAC アドレスだけでなく、エンドポイントの IP アドレスを学習します。

レイヤ 3 の設定 ブリッジ ドメイン ()] パネルのタブには次のパラメータを設定するには、管理者が使用できます。

- **ユニキャスト ルーティング** ：この設定が有効になっているサブネット アドレスが設定されている場合は、ファブリックはデフォルト ゲートウェイの機能を提供して、トラフィックをルーティングします。ユニキャストルーティングを有効にすると、マッピングデータベースがこのブリッジドメインのエンドポイントに付与された IP アドレスと VTEP の対応関係を学習します。IP 学習は、ブリッジドメイン内にサブネットが構成されているかどうかに左右されません。
- **サブネット アドレス** ：このオプションは、ブリッジ ドメインの SVI IP アドレス (デフォルト ゲートウェイ) を設定します。
- **制限のサブネット IP ラーニング** ：このオプションは、ユニキャスト リバース転送パス チェックに似ています。このオプションを選択すると、ファブリックはブリッジ ドメインに設定されている 1 以外のサブネットから IP アドレスを学習されません。

⚠

注意 有効化 **サブネットに制限 IP ラーニング** がブリッジ ドメイン内のトラフィックを停止します。

拡張 L2 専用モード：レガシーモード

Cisco Application Centric Infrastructure（ACI）では、VLAN が異なるリーフ ノードに展開されている限り、任意の目的で同じ VLAN ID を再利用できます。これにより、Cisco ACI ファブリックは、ファブリックとしての VLAN の理論上の最大数、4094 を超えることができます。ただし、これを実現するため、および基盤となる VxLAN 実装の複雑さを隠すために、個々のリーフノードに含めることのできる VLAN の数は少なくなります。このことは、リーフノードあたりの VLAN の密度が必要な場合に問題の原因となる可能性があります。このようなシナリオでは、ブリッジ ドメインで以前はレガシーモードと呼ばれていた、拡張 L2 専用モードを有効にできます。拡張 L2 専用モードのブリッジドメインでは、リーフノードごとに多数の VLAN を使用できます。ただし、このようなブリッジ ドメインにはいくつかの制限があります。

拡張 L2 専用モードとそれ以外のモードで、リーフ ノードごとにサポートされる VLAN またはブリッジ ドメインの数については、ご使用のリリースの Verified Scalability Guideを参照してください。

拡張 L2 専用モードの制限事項

レガシー モードまたは拡張 L2 専用モードの制限は次のとおりです。

- ブリッジ ドメインには、1 つの EPG と 1 つの VLAN のみを含めることができます。
- ユニキャスト ルーティングはサポートされていません。
- コントラクトはサポートされていません。

- VMM 統合のダイナミック VLAN 割り当てはサポートされていません。
- サービス グラフはサポートされていません。
- QoS ポリシーはサポートされていません。
- ブリッジ ドメインは、スタンドアロン Cisco NX-OS では基本的に VLAN として動作します。

拡張 L2 専用モードの設定

次に、拡張 L2 専用 モードでブリッジ ドメインを設定する際の考慮事項を示します。

- VLAN ID はブリッジドメインで設定されます。
- EPG で設定された VLAN ID は上書きされます。
- 既存のブリッジ ドメインで拡張 L2 専用モードの有効と無効を切り替えると、サービスに影響します。

  VLAN ID が変更前に使用されていたものと異なる場合、Cisco Application Policy Infrastructure Controller（APIC）は自動的にブリッジ ドメインの展開解除と再展開を行います。

  モード変更の前後で同じ VLAN ID が使用された場合、Cisco APIC はブリッジ ドメインの自動的な展開解除と再展開は行いません。手動でブリッジ ドメインを展開解除して再展開する必要があります。これは、 EPG で静的ポート設定を削除して再作成することで実行できます。
- 拡張 L2 専用モードの VLAN ID を変更する場合は、まずモードを無効にしてから、新しい VLAN ID で拡張 L2 専用モードを有効にする必要があります。

ブリッジ ドメインごとの IP 学習の無効化

ブリッジ ドメインの IP データプレーン学習は無効にできます。MAC 学習は引き続きハードウェアで行われますが、IP 学習は ARP/GARP/ND プロセスからのみ行われます。この機能は、Cisco APIC 3.1 リリースで主にサービス グラフ ポリシーベース リダイレクト（PBR）展開用に導入されましたが、VRF インスタンスごと（Cisco APIC リリース 4.0）ブリッジ ドメインサブネットごと、（Cisco APIC リリース 5.2）、および EPG ごと（Cisco APIC リリース 5.2）に IP データプレーン学習を無効にする機能に置き換えられました。ブリッジ ドメインごとに IP ラーニングを無効にすることは推奨されません。また、PBR で使用する場合を除き、サポートされません。

ブリッジ ドメインごとに IP 学習を無効化するには、次の注意事項と制限事項を参照してください。

- リモート リーフ スイッチで送信元 IP アドレスが S,G 情報を入力するように学習していないため、レイヤ 3 マルチキャストはサポートされていません。
- DL ビットが iVXLAN ヘッダーで設定されているため、MAC アドレスはリモート リーフ スイッチのデータ パスから学習されません。そのため、ブリッジ ドメインが展開されているファブリックで、リモート リーフ スイッチからすべてのリーフ スイッチに、不明な

ユニキャストトラフィックがフラッディングされることになります。エンドポイントデータプレーン学習が無効になっている場合は、この状況への対策として、プロキシモードでブリッジ ドメインを構成することをお勧めします。

- ARP がフラッド モードであり、GARP ベースの検出を有効にする必要があります。
- IP 学習を無効にすると、対応する VRF インスタンスでレイヤ 3 エンドポイントがフラッシュされません。同じリーフ スイッチを恒久的に指すエンドポイントになる可能性があります。この問題を解決するには、すべてのリーフ スイッチで、 この VRF 内のすべてのリモート IP エンドポイントをフラッシュします。

ブリッジドメインの構成を変更して、データプレーン学習を無効にしても、以前にローカルに学習したエンドポイントはフラッシュされません。これにより、既存のトラフィック フロー中断の影響は限られます。Cisco ACI リーフ スイッチが特定の送信元 MAC を持つトラフィックをエンド ポイント保持ポリシーよりも長く見ない場合、MAC が学習したエンドポイントは通常どおりエージングします。

（注） IP データプレーン学習を無効にすると、トラフィック転送の結果としてエンドポイントの IP 情報が更新されることはなくなりますが、Cisco ACI は ARP/ND を使用してエンドポイント IP 情報を更新できます。つまり、ローカルエンドポイントのエージング（設定変更前に学習されたか、設定変更後に学習されたか）は、通常のエージングとは若干異なり、[システム (System)] > [システム設定 (System Settings)] > [エンドポイント制御 (Endpoint Controls)] > [IPエージング (IP Aging)] にも依存します。

IP エージングが無効の場合、すでに学習されたエンドポイント MAC と一致する送信元 MAC からのトラフィックは、エンドポイントテーブルの MAC アドレス情報を更新し、その結果、IP 情報も更新します（これは IP データプレーンの学習が有効になっている場合と同じです）。

IP エージングが有効の場合、Cisco ACI はエンドポイント IP アドレスを個別にエージング アウトします（これは IP データプレーン学習が有効になっている場合と同じです）が、すでに学習したエンドポイントとマッチする既知の送信元 MAC および IP からのトラフィックにより、エンドポイント テーブルの MAC アドレス情報は更新されるのに対し、IP 情報は更新されないという点で、IP データプレーン学習を有効にした構成とは異なります。

GUI を使用したテナント、VRF およびブリッジ ドメインの作成

外部ルーテッドを設定するときにパブリック サブネットがある場合は、ブリッジ ドメインを外部設定と関連付ける必要があります。

手順

ステップ 1 メニュー バーで、**[テナント（Tenants）]** > **[テナントの追加（Add Tenant）]** を選択します。

ステップ 2 [Create Tenant] ダイアログボックスで、次のタスクを実行します。

a) [Name] フィールドに、名前を入力します。

b) **[セキュリティ ドメイン（Security Domains）]** セクションで、**[+]** をクリックして、**[セキュリティ ドメインの作成（Create Security Domain）]** ダイアログ ボックスを開きます。

c) **[名前（Name）]** フィールドに、セキュリティ ドメインの名前を入力し、**[送信（Submit）]** をクリックします。

d) **[テナントの作成（Create Tenant）]** ダイアログ ボックスで、作成したセキュリティ ドメインの **[更新（Update）]** をクリックします。

e) 必要に応じて他のフィールドに入力します。

f) [送信（Submit）] をクリックします。

テナント名 > **[ネットワーキング（Networking）]**画面が表示されます。

ステップ 3 **[作業（Work）]** ペインで、**[VRF]** アイコンをキャンバスにドラッグして **[Create VRF]** ダイアログボックスを開き、次の操作を実行します。

a) [Name] フィールドに、名前を入力します。

b) 必要に応じて他のフィールドに入力します。

c) **[送信（Submit）]** をクリックして VRF インスタンスの設定を完了します。

ステップ 4 **[作業（Work）]** ペインで、VRF インスタンスを囲む円内のキャンバスに **[ブリッジ ドメイン（Brdige Domain）]** アイコンをドラッグして、2 つを接続します。[Create Bridge Domain] ダイアログボックスが表示されたら、次のタスクを実行します。

a) [Name] フィールドに、名前を入力します。

b) 必要に応じて他のフィールドに入力します。

c) [次へ（Next）] をクリックします。

d) **[サブネット（Subnets）]** セクションで、**[+]** をクリックして、**[サブネットの作成（Create Subnet）]** ダイアログ ボックスを開きます。

e) **[ゲートウェイ IP**（Gateway IP）] フィールドに、IP アドレスとサブネット マスクを入力します。

f) 必要に応じて他のフィールドに入力します。

g) [OK] をクリックします。

h) **[ブリッジ ドメインの作成（Create Bridge Domain）]** ダイアログ ボックスに戻り、必要に応じて他のフィールドに入力します。

i) [次へ（Next）] をクリックします。

j) 必要に応じてフィールドに入力します。

k) **[OK]** をクリックしてブリッジ ドメインの設定を完了します。

ステップ 5 **[作業（Work）]** ペインで、VRF インスタンスを囲む円内のキャンバスに **[L3]** アイコンをドラッグして、2 つを接続します。[Create Routed Outside] ダイアログボックスが表示されたら、次のタスクを実行します。

a) [Name] フィールドに、名前を入力します。
b) **[ノードとインターフェイス プロトコル プロファイル（Nodes And Interfaces Protocol Profiles]** セクションで、**[+]** をクリックして **[ノード プロファイルの作成（Create Node Profile）]** ダイアログ ボックスを開きます。
c) [Name] フィールドに、名前を入力します。
d) **[ノード（Nodes）]** セクションで、**[+]** をクリックして **[ノードの選択（Select Node）]** ダイアログ ボックスを開きます。
e) **[ノード ID（Node ID）]** ドロップダウン リストから、ノードを選択します。
f) [Router ID] フィールドに、ルータ ID を入力します。
g) **[スタティック ルート（Static Routes）]** セクションで、**[+]** をクリックして**[スタティック ルートの作成（Create Static Routes）]** ダイアログ ボックスを開きます。
h) [Prefix] フィールドに、IPv4 アドレスまたは IPv6 アドレスを入力します。
i) **[ネクスト ホップ アドレス（Next Hop Addresses）]** セクションで、**[+]** をクリックして **[ネクスト ホップの作成（Create Next Hop）]** ダイアログ ボックスを開きます。
j) **[ネクスト ホップ アドレス（Next Hop Addresses）]** フィールドを展開し、IPv4 アドレスまたは IPv6 アドレスを入力します。
k) **[設定（Preference）]** フィールドに、数値を入力します。
l) 必要に応じて他のフィールドに入力します。
m) [OK] をクリックします。
n) **[静的ルートの作成（Create Static Route）]** ダイアログ ボックスで、必要に応じて他のフィールドに入力します。
o) [OK] をクリックします。
p) **[ノードの選択（Select Node）]** ダイアログ ボックスで、必要に応じて他のフィールドに入力します。
q) [OK] をクリックします。
r) **[ノード プロファイルの作成（Create Node Profile）]** ダイアログ ボックスで、必要に応じて他のフィールドに入力します。
s) [OK] をクリックします。
t) 必要に応じて **[BGP]**、**[OSPF]**、または **[EIGRP]** チェックボックスをオンにします。
u) 必要に応じて他のフィールドに入力します。
v) [次へ（Next）] をクリックします。
w) 必要に応じてフィールドに入力します。
x) **[OK]** をクリックしてレイヤ 3 の設定を完了します。

レイヤ 3 の設定を確認するには、**[ナビゲーション（Navigation）]** ペインで、**[ネットワーキング（Networking）]** > **[VRF]**の順に展開します。

NX-OS CLI を使用した、テナント、VRF およびブリッジ ドメインの作成

ここでは、テナント、VRF およびブリッジ ドメインを作成する方法を説明します。

（注） テナントの設定を作成する前に、vlan-domain コマンドを使用して VLAN ドメインを作成し、ポートを割り当てる必要があります。

手順

ステップ 1 次のように、VLAN ドメイン（一連のポートで許可される一連の VLAN を含む）を作成し、VLAN の入力を割り当てます。

例：

次の例（exampleCorp）では、VLAN 50 ～ 500 が割り当てられることに注意してください。

```
apic1# configure
apic1(config)# vlan-domain dom_exampleCorp
apic1(config-vlan)# vlan 50-500
apic1(config-vlan)# exit
```

ステップ 2 VLAN が割り当てられたら、これらの VLAN を使用できるリーフ（スイッチ）およびインターフェイスを指定します。次に、「vlan-domain member」と入力し、その後に作成したドメインの名前を入力します。

例：

次の例では、これらの VLAN（50 ～ 500）は、インターフェイス イーサネット 1/2 ～ 4（1/2、1/3、1/4 を含む 3 つのポート）上の leaf 101 で有効になっています。これは、このインターフェイスを使用すると、VLAN を使用できるあらゆるアプリケーションにこのポートの VLAN 50 ～ 500 を使用できることを意味します。

```
apic1(config-vlan)# leaf 101
apic1(config-vlan)# interface ethernet 1/2-4
apic1(config-leaf-if)# vlan-domain member dom_exampleCorp
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

ステップ 3 次の例に示すように、グローバル コンフィギュレーション モードでテナントを作成します。

例：

```
apic1(config)# tenant exampleCorp
```

ステップ 4 次の例に示すように、テナント コンフィギュレーション モードでプライベート ネットワーク（VRF とも呼ばれます）を作成します。

例：

```
apic1(config)# tenant exampleCorp
apic1(config-tenant)# vrf context exampleCorp_v1
apic1(config-tenant-vrf)# exit
```

ステップ 5 次の例に示すように、テナントの下にブリッジ ドメイン（BD）を作成します。

例：

```
apic1(config-tenant)# bridge-domain exampleCorp_b1
apic1(config-tenant-bd)# vrf member exampleCorp_v1
apic1(config-tenant-bd)# exit
```

（注）
この場合、VRF は「exampleCorp_v1」です。

ステップ 6 次の例に示すように、BD の IP アドレス（IP および ipv6）を割り当てます。

例：

```
apic1(config-tenant)# interface bridge-domain exampleCorp_b1
apic1(config-tenant-interface)# ip address 172.1.1.1/24
apic1(config-tenant-interface)# ipv6 address 2001:1:1::1/64
apic1(config-tenant-interface)# exit
```

次のタスク

次の項では、アプリケーション プロファイルを追加し、アプリケーション エンドポイント グループ（EPG）を作成し、EPG をブリッジ ドメインに関連付ける方法について説明します。

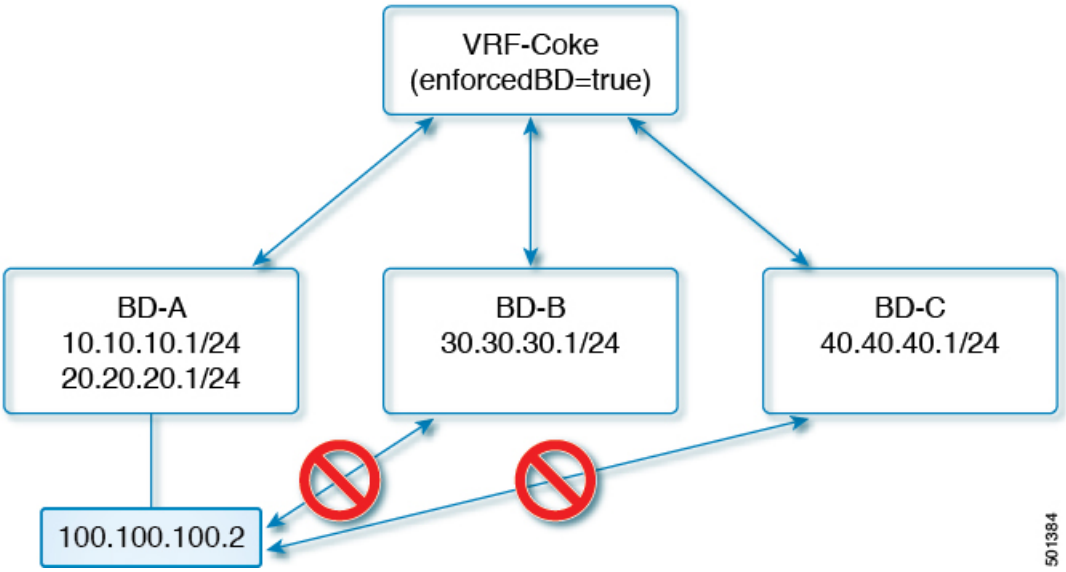
関連トピック

NX-OS スタイルの CLI を使用した VLAN ドメインの設定

適用されるブリッジ ドメインの設定

適用ブリッジ ドメインでは、関連付けられたブリッジ ドメイン内のサブネット ゲートウェイにしか ping を送信できない、対象のエンド ポイント グループ（EPG）内に、1 つのエンドポイントが作成されます。この設定を使用すると、任意のサブネットゲートウェイに ping を送信できる IP アドレスのグローバル例外リストを作成できます。

図 *8*: 適用されるブリッジ ドメイン



（注）

- 例外 IP アドレスは、すべての VRF インスタンスのすべてのブリッジ ドメイン ゲートウェイに ping を送信できます。
- L3Out 用に設定されたループバック インターフェイスでは、対象のループバック インターフェイスに合わせて設定された IP アドレスへの到達可能性は適用されません。
- eBGP ピアとなる IP アドレスが、L3Out インターフェイスのサブネットとは異なるサブネットに存在している場合には、許容例外サブネットにピア サブネットを追加する必要があります。そうしないと、送信元 IP アドレスが L3Out インターフェイスのサブネットとは異なるサブネットに存在するため、eBGP トラフィックがブロックされます。
- BGP プレフィックスベース ピアの場合は、許容例外サブネットのリストにピア サブネットを追加する必要があります。たとえば、20.1.1.0/24 が BGP プレフィックスベース ピアとして構成されている場合は、許容例外サブネットのリストに 20.1.1.0/24 を追加する必要があります。
- 適用ブリッジ ドメインは、VRFインスタンスがインバンドまたはアウトオブバンドであるかどうかにかかわらず、管理テナントではサポートされません。これらのVRFインスタンスへのトラフィックを制御するルールは、通常のコントラクトを使用して設定する必要があります。

NX-OS スタイル CLI を使用した適用されるブリッジ ドメインの設定

このセクションでは、NX-OS スタイル コマンドライン インターフェイス (CLI) を使用して、適用されるブリッジ ドメインを設定する方法について説明します。

手順

ステップ 1 テナントを作成し有効にします。

例：

次の例 (「cokeVrf」) が作成され有効になっています。

```
apic1(config-tenant)# vrf context cokeVrf
apic1(config-tenant-vrf)# bd-enforce enable
apic1(config-tenant-vrf)# exit
apic1(config-tenant)#exit
```

ステップ 2 例外リストに、サブネットを追加します。

例：

```
apic1(config)#bd-enf-exp-ip add1.2.3.4/24
apic1(config)#exit
```

適用されるブリッジ ドメインは次のようなコマンドを使用して動作可能かどうかを確認できます。

```
apic1# show running-config all | grep bd-enf
bd-enforce enable
bd-enf-exp-ip add 1.2.3.4/24
```

例

次のコマンドでは、除外リストからサブネットを削除します。

```
apic1(config)# no bd-enf-exp-ip 1.2.3.4/24
apic1(config)#tenant coke
apic1(config-tenant)#vrf context cokeVrf
```

次のタスク

適用されるブリッジ ドメインを無効にするには、次のコマンドを実行します。

```
apic1(config-tenant-vrf)# no bd-enforce enable
```

カプセル化によるすべてのプロトコルおよびプロキシ ARP のカプセル化のフラッディングを設定する

Cisco Application Centric Infrastructure（ACI）は、ブリッジ ドメインをレイヤ 2 ブロードキャスト境界として使用します。各ブリッジ ドメインには複数のエンドポイント グループ（EPG）を含めることができ、各 EPG は複数の仮想ドメインまたは物理ドメインにマッピングできます。各 EPG は、ドメインごとに異なる VLAN カプセル化プールを使用することもできます。各 EPG は、ドメインごとに異なる VLAN または VXLAN カプセル化プールを使用することもできます。

通常、ブリッジ ドメイン内に複数の EPG を配置すると、ブロードキャスト フラッディングはブリッジ ドメイン内のすべての EPG にトラフィックを送信します。EPG はエンドポイントをグループ化し、特定の機能を実行するためにトラフィックを管理するために使用されるものなので、ブリッジ ドメイン内のすべての EPG に同じトラフィックを送信することは必ずしも実用的ではありません。

カプセル化でのフラッディングは、ネットワーク内のブリッジ ドメインを統合するのに役立ちます。この機能は、EPG が関連付けられている仮想ドメインまたは物理ドメインのカプセル化に基づいて、ブリッジ ドメイン内のエンドポイントへのブロードキャスト フラッディングを制御できるようにするからです。

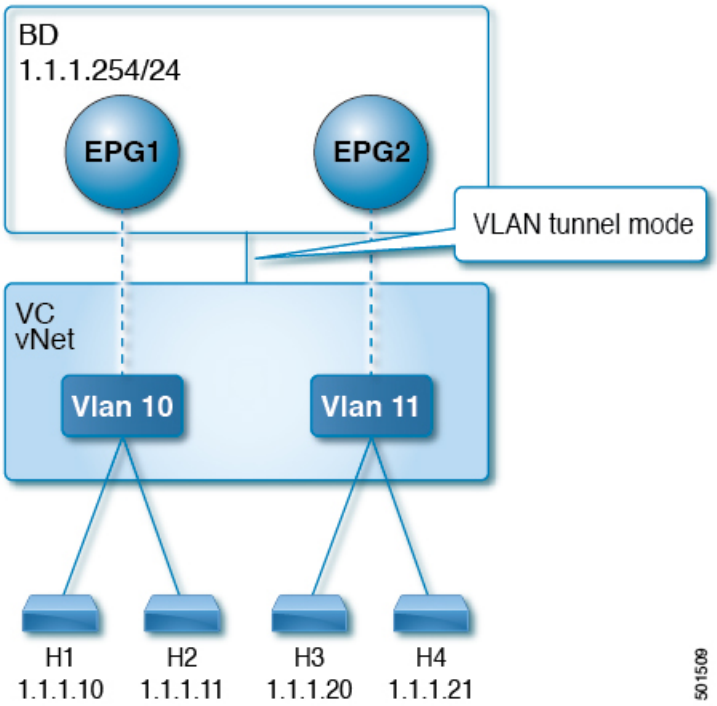
カプセル化でのフラッディングでは、同じブリッジ ドメインにおける異なる EPG のエンドポイント間の通信を許可するために、ブリッジ ドメインにサブネットと IP ルーティングを構成する必要があり、Cisco ACI がプロキシ ARP の役割を果たします。

VLAN カプセル化を使用したカプセル化でのフラッディングの使用例

カプセル化のフラッディングは、外部デバイスが VLAN に依存しない MAC 学習のために vNet ごとに 1 つの MAC アドレスが維持される仮想接続 トンネル モードを使用している場合によく用いられます。

トンネル モードで複数の VLAN を使用すると、いくつかの課題を導入できます。次の図に示すように、単一のトンネルでCisco ACIを使用する一般的な導入では、1 つのブリッジ ドメインの下に複数の EPG があります。この場合、特定のトラフィックがブリッジ ドメイン内（つまりすべての EPG 内）でフラッディングし、MACがあいまいになって転送エラーが発生するリスクがあります。

図 *9 : VLAN* トンネルモードの *Cisco ACI* の課題



このトポロジでは、ブレードスイッチ（この例では仮想接続）に、1つのアップリンクを使用してCisco ACIリーフノードに接続する単一のトンネルネットワークが定義されています。このリンクでは、2 人のユーザの VLAN、VLAN 10 と VLAN 11 が行われます。サーバーのゲートウェイがCisco ACIクラウドの外部にあるため、ブリッジ ドメインはフラッディング モードに設定されます。次のプロセスで ARP 交渉が発生します。

- サーバは、VLAN 10 ネットワーク経由で 1 つの ARP ブロードキャスト要求を送信します。
- ARP パケットは、外部のサーバに向かってトンネル ネットワークを通過し、そのダウンリンクから学習した送信元 MAC アドレスを記録します。
- その後、サーバーはアップリンクからCisco ACIリーフスイッチにパケットを転送します。
- Cisco ACIファブリックは、アクセスポート VLAN 10に着信する ARP ブロードキャスト パケットを確認し、EPG1 にマッピングします。
- ブリッジ ドメインは ARP パケットをフラッディングするように設定されているため、パケットはブリッジ ドメイン内でフラッディングされます。したがって、両方の EPG が同じブリッジ ドメイン内にあるため、これらのポートにフラッディングされます。
- 同じ ARP ブロードキャスト パケットは、同じアップリンクで復帰します。
- ブレード スイッチは、このアップリンクからの元の送信元 MAC アドレスを認識します。

結果：ブレード スイッチは、単一の MAC 転送テーブル内のダウンリンク ポートとアップリンク ポートの両方から学習した同じMACアドレスを持ち、トラフィックが中断します。

推奨される解決策

カプセル化オプションのフラッディングは、ブリッジドメイン内のフラッディング トラフィックを単一のカプセル化に制限するために使用されます。EPG1/VLAN X and EPG2/VLAN Y が同じブリッジドメインを共有し、カプセル化でのフラッディングが有効になっている時、カプセル化フラッディング トラフィックは他の EPG/VLAN に到達しません。

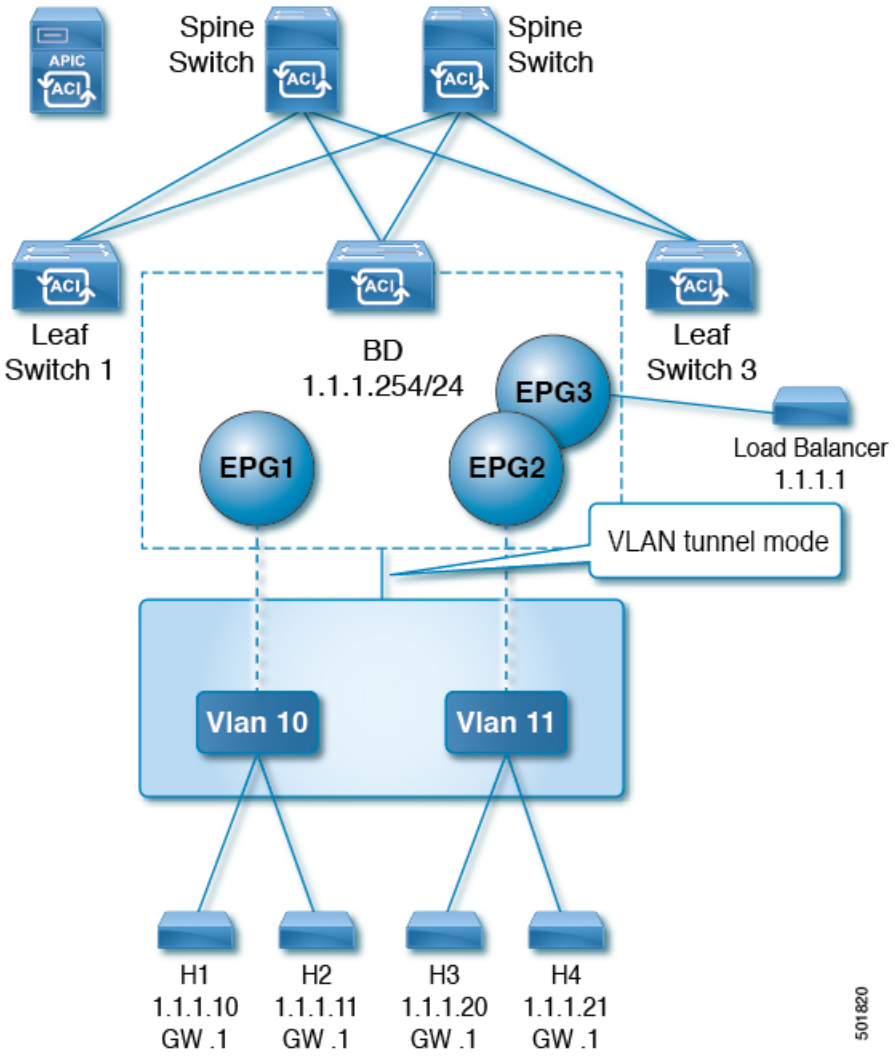
Cisco Application Policy Infrastructure Controller（APIC）リリース 3.1(1) 以降、Cisco Nexus 9000 シリーズスイッチ（名前の末尾が EX および FX 以降）では、すべてのプロトコルがカプセル化されます。また、VLAN 間のトラフィックのブリッジ ドメインでフラッディングが有効になっている場合、プロキシ ARP は MAC フラップの問題が発生しないようにします。また、すべてのフラッディング（ARP、GARP、およびBUM）をカプセル化に制限します。この制限は、有効になっているブリッジ ドメイン下のすべての EPG に適用されます。

（注） Cisco APIC APIC リリース 3.1 (1) より前のリリースでは、これらの機能はサポートされていません（カプセル内でフラッディングするとき含まれるプロキシ ARP およびすべてのプロトコル）。以前の Cisco APIC リリースまたは以前の世代のスイッチ（名前に EX または FX がない）では、カプセル化でフラッディングを有効にしても機能しません。情報障害は生成されませんが、Cisco APIC はヘルス スコアを 1 減らします。

（注） Cisco APIC リリース 3.2(5) 以降では、VXLAN カプセル化に関連付けられた EPG のカプセル化でフラッディングを設定できます。以前は、VLAN のみが仮想ドメインのカプセル化でのフラッディングでサポートされていました。ブリッジ ドメインまたは EPG を作成または変更するときに、カプセル化でのフラッディングを設定します。

推奨される解決策は、外部スイッチを追加して、1 つのブリッジ ドメインで複数の EPG をサポートすることです。外部のスイッチがある 1 つのブリッジ ドメイン下で複数の EPG を持つこの設計は、次の図に示されています。

図 *10*：外部のスイッチがある *1* つのブリッジ ドメイン下で複数の *EPG* を持つ設計



同じブリッジ ドメイン内では、一部の EPG をサービス ノードにすることができ、他の EPG にはカプセル化でのフラッディングを設定できます。ロード バランサは別の EPG に存在します。ロード バランサは EPG からパケットを受信し、その他の EPG に送信します（プロキシ ARP はなく、カプセル内のフラッディングは発生しません）。

マルチ宛先プロトコル トラフィック

EPG/ブリッジ ドメイン レベルのブロードキャスト セグメンテーションは、次のネットワーク制御プロトコルでサポートされます。

- OSPF
- EIGRP
- LACP
- IS-IS

- BGP
- IGMP
- PIM
- STP BPDU（EPG 内フラッディング）
- ARP/GARP（ARP プロキシによって制御）
- ND

カプセル化でのフラッディングの制限事項

すべてのプロトコルのカプセル化でのフラッディングには、次の制限が適用されます。

- カプセルのフラッディングは、ARP ユニキャスト モードでは機能しません。
- このリリースでは、ネイバー送信要求（プロキシ NS/ND）はサポートされていません。
- プロキシアドレス解決プロトコル（ARP）は暗黙的に有効にされるため、ARP トラフィックは異なるカプセル化間の通信のために CPU に送信できます。

  ARP トラフィックを処理するために異なるポートに均等に配信されるようにするには、ポート単位のコントロール プレーン ポリシング（CoPP）を有効にします。
- カプセル化でのフラッディングは、フラッド モードのブリッジ ドメインおよびフラッド モードの ARP でのみサポートされます。ブリッジ ドメイン スパイン プロキシ モードはサポートされていません。
- IPv4 レイヤ 3 マルチキャストはサポートされていません。
- カプセル化でのフラッディングが有効な場合でも、IPv6 NS/NDプロキシはサポートされません。その結果、同じ IPv6 サブネット下にあっても、カプセル化が異なる EPG に存在する 2 つのエンドポイント間の接続は、機能しないことがあります。
- 別の VLAN への仮想マシンの移行には、時間的な問題（60 秒）があります。別の VLAN または VXLAN への仮想マシンの移行には、時間的な問題（60 秒）があります。
- 仮想マシンの IP アドレスが、ファイアウォールの IP アドレスではなく、ゲートウェイの IP アドレスに変更された場合、ファイアウォールはバイパスされるため、ファイアウォールをゲートウェイにする仮想マシン間の通信セットアップは推奨されません。
- 以前のリリースではサポートされていません（以前と現在のリリース間の相互運用もサポートされていません）。
- 古い世代アプリケーション リーフ エンジン（ALE）とアプリケーション スパイン エンジン（ASE）を使用した混合モード トポロジは推奨されません。また、カプセル化でのフラッディングではサポートされません。同時に有効にすると、QoS の優先順位が適用されるのを防ぐことができます。
- 同じマルチサイト ドメインの一部であるCisco ACIファブリック全体に拡張された EPG とブリッジドメインでは、カプセル化でのフラッディングはサポートされません。ただし、

Cisco ACIファブリックでローカルに定義されたEPGとブリッジ ドメインでは、カプセル化でのフラッディングは引き続き機能し、完全にサポートされています。Cisco ACIファブリックと、そのファブリックに関連付けられたリモート リーフ スイッチ間でストレッチされるEPGまたはブリッジ ドメインにも、同じ考慮事項が適用されます。

- マイクロセグメンテーションがいずれかの形式で構成されているEPGでは、カプセル化でのフラッディングはサポートされません。これには、EPG内分離、VMMドメインでの「マイクロセグメンテーションを許可する」、マイクロセグメンテーションEPG、EPG内コントラクトが含まれます。
- 共通パーベイシブ ゲートウェイでは、カプセル化でのフラッディングはサポートされていません。Cisco APIC Layer 3 Networking Configuration Guideの「Common Pervasive Gateway」の章を参照してください。
- ブリッジ ドメインのすべてのEPGでカプセル化でのフラッディングを設定する場合は、ブリッジ ドメインでもカプセル化でのフラッディングを設定してください。
- IGMPスヌーピングは、カプセル化でのフラッディングではサポートされません。
- Cisco ACIにおいては、カプセル化でのフラッディングのために設定されたEPGで受信されるパケットのフラッディングを、（カプセル化ではなく）ブリッジ ドメインで生じさせる条件が存在します。これは、管理者がカプセル化でのフラッディングをEPGで直接設定したか、ブリッジ ドメインで設定したかに関係なく発生します。この転送動作の条件は、入力リーフ ノードに宛先MACアドレスのリモートエンドポイントがあり、出力リーフ ノードに対応するローカル エンドポイントがない場合です。これは、インターフェイスのフラッピング、STP TCNによるエンドポイント フラッシュ、過剰な移動のためにブリッジ ドメインで学習が無効になっているなどの理由で発生する可能性があります。

  4.2(6o)以降の4.2(6)リリース、4.2(7m)以降の4.2(7)リリース、および5.2(1g)以降のリリースでは、この動作が拡張されました。管理者が（EPGではなく）ブリッジ ドメインでカプセル化のフラッディングを有効にした場合、Cisco ACIは非入力（出力および中継）リーフ ノード上の外部デバイスに面したダウンリンクからのカプセル化で、このようなパケットを送信しません。この新しい動作により、パケットが予期しないカプセル化に漏洩することが防止されます。カプセル化でのフラッディングがEPGレベルでのみ有効になっている場合、非入力リーフ ノードは、カプセル化ではなくブリッジ ドメインでパケットをフラッディングする可能性があります。詳細については、拡張バグCSCvx83364を参照してください。
- レイヤ3ゲートウェイはCisco ACIファブリック内にある必要があります。

カプセル化範囲限定のフラッディングの設定

NX-OSスタイルのCLI、REST API、またはCisco Application Policy Infrastructure Controller（APIC）GUIを使用して、カプセル化でフラッディングを設定します。

EPGに設定されたカプセル化のフラッディングは、ブリッジド メイン（BD）に設定されたカプセル化のフラッディングよりも優先されます。BDとEPGの両方を設定すると、動作は次に説明したようになります。

表 *3 : BD* と *EPG* の両方が設定されているときの動作

設定	動作
EPG でのカプセルのフラッディングとブリッジ ドメインでのカプセルのフラッディング	カプセル化のフラッディングは、ブリッジ ドメインのすべての VLAN および VXLAN 上のトラフィックに対して発生します。
EPG でのカプセルのフラッディングが発生せずブリッジドメインでのカプセルのフラッディングが発生する	カプセル化のフラッディングは、ブリッジ ドメイン内のすべての VLAN および VXLAN のトラフィックに対して発生します。
EPG でのカプセルのフラッディングが発生しブリッジ ドメインでのカプセルのフラッディングが発生しない	カプセル化のフラッディングは、ブリッジ ドメインの EPG 内のその VLAN または VXLAN のトラフィックに対して発生します。
EPG でのカプセルのフラッディングが発生せずブリッジドメインでのカプセルのフラッディングも発生しない	ブリッジ ドメイン全体でフラッディングします。

Cisco APIC GUI を使用したカプセル化範囲限定のフラッディングの設定

ブリッジドメイン（BD）またはエンドポイントグループ（EPG）を作成または変更する場合は、Cisco Application Policy Infrastructure Controller（APIC）GUIを使用してカプセル化でフラッディングを設定します。

手順

ステップ 1 BD の作成時にカプセル化でフラッディングを設定するには、次の手順を実行します。

a) Cisco APIC にログインします。
b) **[Tenants]** > ***[tenant]*** > **[Networking]** > **[Bridge Domains]** を選択します。
c) **Bridge Domains** を右クリックして、**Create Bridge Domain** を選択します。
d) 手順 1 の **[Create Bridge Domain]** ダイアログ ボックスで、**[Multi Destination Flooding]** ドロップダウン リストから、[Flood in Encapsulation] を選択します。
e) 設定に応じてダイアログボックスの他のフィールドに入力し、**[Finish]** をクリックします。

ステップ 2 BD の変更時にカプセル化でフラッディングを設定するには、次の手順を実行します。

a) Cisco APIC にログインします。
b) **[Tenants]** > ***<tenan>]*** > **[Networking]** > **[Bridge Domains]** > ***<bridge domain>*** を選択します。
c) BD の作業ウィンドウで、**[Policy]** タブを選択し、**[General]** タブを選択します。
d) **[Multi Destination Flooding]** 領域で、**[Flood in Encapsulation]** を選択します。
e) **[送信（Submit）]** をクリックします。`

ステップ 3 EPG の作成時にカプセル化でフラッディングを設定するには、次の手順を実行します。

a) Cisco APIC にログインします。

b) **[Tenants]** > **<*tenant*>** > **[Application Profiles]** に移動します。
c) **[Application Profiles]** を右クリックし、**[Create Application EPG]** を選択します。
d) **[Create Application EPG]** ダイアログボックスの **[Flood in Encapsulation]** 領域で、**[Enabled]** を選択します。

   カプセル化のフラッディングはデフォルトで無効になっています。

e) 設定に応じてダイアログボックスの他のフィールドに入力し、**[Finish]** をクリックします。

ステップ 4 EPG の変更時にカプセル化でフラッディングを設定するには、次の手順を実行します。

a) **[Tenants]** > **<*tenant*>** > **[Application Profiles]** > **[Application EPG]** > **<*application EPG*>** に移動します。
b) EPG の作業ウィンドウで、**[Policy]** タブを選択し、**[General]** タブを選択します。
c) **[Flood in Encapsulation]** 領域で、**[Enabled]** を選択します。
d) [送信（Submit）] をクリックします。

NX-OS スタイル CLI を使用したカプセル化でのフラッディングの設定

NX-OS スタイル CLI を使用して選択したエンドポイント グループ（EPG）のみに対してカプセル化でフラッディングを追加する場合は、EPG 下で **flood-on-encapsulation enable** コマンドを入力します。

すべての EPG に対してカプセル化でフラッディングを追加する場合、ブリッジ ドメインに対して **multi-destination encap-flood** CLI コマンドを使用します。

手順

ステップ 1 ブリッジドメイン（BD）のカプセル化でフラッディングを設定します。

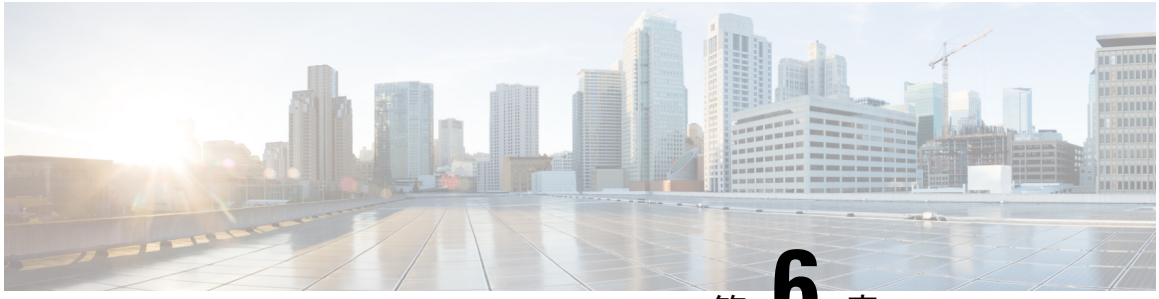
例：

```
APIC1#configure
APIC1(config)# tenant tenant
APIC1(config-tenant)# bridge-domain BD-name
APIC1(config-tenant-bd)# multi-destination encap-flood
APIC1(config-tenant)#exit
APIC1(config)#
```

ステップ 2 EPG のカプセル化でフラッディングを設定します。

例：

```
APIC1(config)# tenant tenant
APIC1(config-tenant)# application AP1
APIC1(config-tenant-app)# epg EPG-name
APIC1(config-tenant-app-epg)# flood-on-encapsulation
APIC1(config-tenant-app-epg)#no flood-on-encapsulation
```



第 6 章

EPG

この章は、次の内容で構成されています。

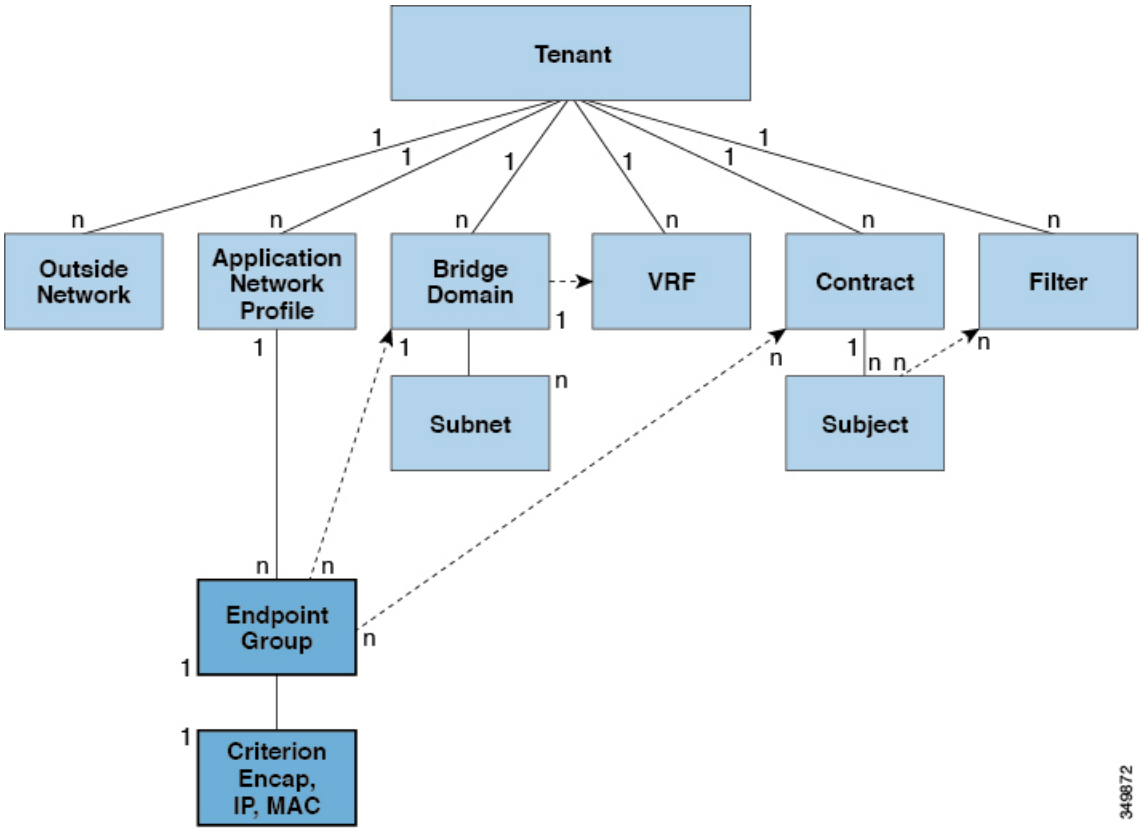
- エンドポイント グループについて （41 ページ）
- 特定のポートに EPG を導入する （47 ページ）
- 特定のポートに EPG を導入するためのドメイン、接続可能アクセス エンティティ プロファイル、および VLAN の作成 （50 ページ）
- 添付されているエンティティ プロファイルで複数のインターフェイスに EPG を導入する （55 ページ）
- EPG 内の分離 （58 ページ）
- Cisco ACI 仮想エッジの EPG 内分離の設定 （69 ページ）
- トラブルシューティング （74 ページ）
- エンドポイント接続のトラブルシューティング （74 ページ）
- IP bエース EPG 構成の確認 （79 ページ）

エンドポイント グループについて

エンドポイント グループ

エンドポイント グループ（EPG）は、ポリシー モデルの最も重要なオブジェクトです。次の図は、管理情報ツリー（MIT）内のアプリケーションEPGの場所とテナント内の他のオブジェクトとの関係を示します。

図 *11 :* エンドポイント グループ



EPGは、エンドポイントの集合を含む名前付き論理エンティティである管理対象オブジェクトです。エンドポイントは、ネットワークに直接的または間接的に接続されるデバイスです。エンドポイントには、アドレス（ID）、ロケーション、属性（バージョンやパッチ レベルなど）があり、物理または仮想にできます。エンドポイントのアドレスを知ることで、他のすべての ID の詳細にアクセスすることもできます。EPG は、物理および論理トポロジから完全に分離されます。エンドポイントの例には、インターネット上のサーバ、仮想マシン、ネットワーク接続ストレージ、またはクライアントが含まれます。EPG 内のエンドポイント メンバシップは、ダイナミックまたはスタティックにできます。

ACI ファブリックには、次のタイプの EPG を含めることができます。

- アプリケーション エンドポイント グループ（`fvAEPg`）
- レイヤ 2 外部外側ネットワーク インスタンスのエンドポイント グループ（`l2extInstP`）
- レイヤ 3 外部外側ネットワーク インスタンスのエンドポイント グループ（`l3extInstP`）
- アウトオブバンド（`mgmtOoB`）またはインバンド（`mgmtInB`）アクセス用の管理エンドポイント グループ。

EPGには、セキュリティ、仮想マシンのモビリティ（VMM）、QoS、レイヤ4～レイヤ7サービスなどの共通のポリシー要件を持つエンドポイントが含まれます。エンドポイントは個別に設定および管理されるのではなく、EPG 内に配置され、グループとして管理されます。

ポリシーは EPG に適用されます。個々のエンドポイントに適用されることは絶対にありません。EPG は、APIC において管理者により静的に設定されるか、vCenter または OpenStack などの自動システムによって動的に設定されます。

（注） EPG がスタティック バインディング パスを使用する場合、この EPG に関連付けられるカプセル化 VLAN はスタティック VLAN プールの一部である必要があります。IPv4/IPv6 デュアルスタック設定の場合、IP アドレスのプロパティは `fvStCEp` MO の `fvStIp` 子プロパティに含まれます。IPv4 および IPv6 アドレスをサポートする複数の `fvStIp` を 1 つの `fvStCEp` オブジェクト下に追加できます。ACI を、IPv4 のみのファームウェアから、IPv6 をサポートするバージョンのファームウェアにアップグレードすると、既存の IP プロパティが `fvStIp` MO にコピーされます。

EPG の設定内容にかかわらず、含まれるエンドポイントに EPG ポリシーが適用されます。

ファブリックへの WAN ルータ接続は、スタティック EPG を使用する設定の 1 つの例です。ファブリックへの WAN ルータ接続を設定するには、関連付けられている WAN サブネット内のエンドポイントを含む `l3extInstP` EPG を管理者が設定します。ファブリックは、エンドポイントの接続ライフサイクルが経過する間に、検出プロセスを通して EPG のエンドポイントについて学習します。エンドポイントを学習すると、ファブリックは、それに基づいて `l3extInstP` EPG ポリシーを適用します。たとえば、WAN 接続クライアントがアプリケーション（`fvAEPg`）EPG 内でサーバとの TCP セッションを開始すると、`l3extInstP` EPG は、`fvAEPg` EPG Web サーバとの通信が始まる前に、そのクライアント エンドポイントにポリシーを適用します。クライアント サーバ TCP セッションが終わり、クライアントとサーバの間の通信が終了すると、そのエンドポイントはもうファブリック内に存在しません。

（注） リーフ スイッチが EPG 下の *static binding (leaf switches)* 用に設定されている場合は、次の制限が適用されます。

- スタティック バインディングをスタティック パスで上書きすることはできません。
- そのスイッチのインターフェイスをルーテッド外部ネットワーク（L3out）設定に使用することはできません。
- そのスイッチのインターフェイスに IP アドレスを割り当てることはできません。

VMware vCenter への仮想マシン管理接続は、ダイナミック EPG を使用する設定の 1 つの例です。ファブリックで仮想マシン管理ドメインが設定されると、vCenter は、必要に応じて仮想マシン エンドポイントを開始、移動、シャットダウンさせることのできる EPG の動的設定をトリガーします。

EPG シャットダウンでの ACI ポリシー設定

EPG がシャットダウン モードの場合、EPG に関連する ACI ポリシー設定はすべてのスイッチから削除されます。EPG はすべてのスイッチから削除されます。EPG が ACI データ ストアに存在している間は、非アクティブ モードになります。APIC GUI で、EPG をサービスから削除するチェックボックスをオンにすることができます。

（注） シャットダウン モードの EPG に接続されているホストは、EPG との間で送受信できません。

アクセス ポリシーによる VLAN から EPG への自動割り当て

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 ポリシーと別に設定される一方で、テナント ポリシーの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。ファブリック アクセス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、またはファブリック エクステンダ (FEX) 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。

図 *12*：アクセス ポリシーとエンドポイント グループの関連付け

ポリシー モデルでは、vlan の Epg 緊密に結合されています。トラフィックが流れるようにするには、物理、VMM、L2out、L3out、またはファイバ チャネル ドメイン内に VLAN を持つリーフ ポートに EPG を展開する必要があります。詳細については、ネットワーク ドメイン（13 ページ）を参照してください。

ポリシー モデルでは、EPG に関連付けられているドメイン プロファイルには、VLAN インスタンス プロファイルが含まれています。ドメイン プロファイルには、両方の VLAN インスタンス プロファイル (VLAN プール) および attacheable アクセス エンティティ プロファイル (AEP) アプリケーション Epg に直接と関連付けられているが含まれています。AEP は、すべてのポートの [接続されている、および Vlan の割り当てのタスクを自動化するに関連付けられているアプリケーション Epg を展開します。大規模なデータセンター数千の Vlan の数百のプロビジョニング仮想マシンのアクティブなは簡単に、中に ACI ファブリックは VLAN プールから、VLAN Id を自動的に割り当てることができます。これは、膨大な従来データセンターで Vlan をトランキングと比較して、時間を節約できます。

VLAN の注意事項

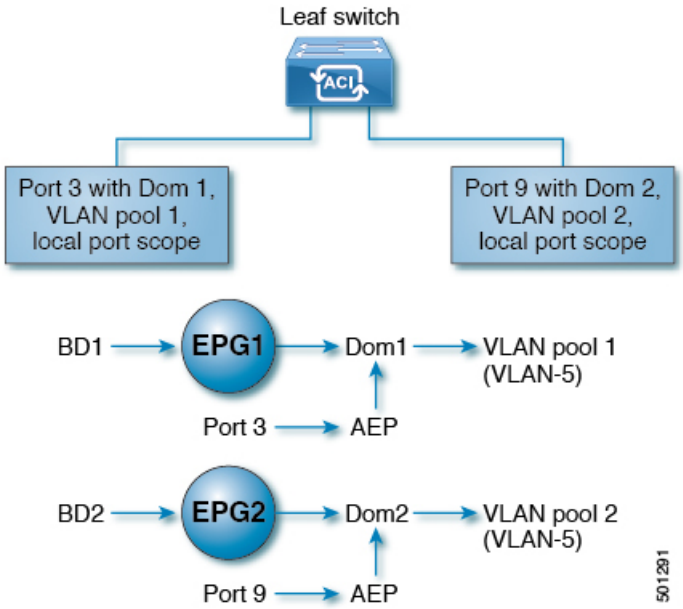
EPG トラフィックがフローは、Vlan の設定には次のガイドラインを使用します。

- 複数のドメインは、VLAN プールを共有できますが、1 つのドメインは、1 つの VLAN プールにのみ使用できます。
- 1 つのリーフ スイッチで同じ VLAN のカプセル化を複数の Epg を展開するを参照してください。 ポート単位の VLAN （45 ページ） 。

ポート単位の VLAN

v1.1 リリースより前の ACI バージョンでは、特定の VLAN カプセル化はリーフ スイッチ上の単一の EPG だけにマッピングされます。同じリーフ スイッチ上に同じ VLAN カプセル化を持つ第 2 の EPG があると、ACI でエラーが発生します。

v1.1 リリース以降では、次の図と同様、ポート単位の VLAN 設定で、特定のリーフ スイッチ (または FEX) 上に複数の EPG を同じ VLAN カプセル化で展開することができます。



単一のリーフ スイッチ上で、同じカプセル化番号を使用する複数の EPG の展開を有効にするには、次の注意事項に従ってください。

- EPG は、さまざまなブリッジ ドメインに関連付けられている必要があります。
- EPG は、さまざまなポートに展開する必要があります。
- ポートと EPG の両方が、VLAN 番号が含まれている VLAN プールに関連付けられている同じドメインに関連付けられている必要があります。
- ポートは `portLocal` VLAN スコープで設定されている必要があります。

たとえば、上の図の ポート 3 と 9 上に展開されている EPG のポート単位の VLAN で、両方が VLAN-5 を使用していれば、ポート 3 と EPG1 は Dom1 (プール 1) に、ポート 9 と EPG2 は Dom2 (プール 2) に関連付けられます。

ポート 3 からのトラフィックは EPG1 に関連付けられ、ポート 9 からのトラフィックは EPG2 に関連付けられます。

これは、外部レイヤ 3 外部接続用に設定されたポートには適用されません。

EPG に複数の物理ドメインがあり、VLAN プールが重複している場合は、EPG をポートに展開するために使用される AEP に複数のドメインを追加しないでください。これにより、トラフィック転送の問題が回避されます。

EPG に重複する VLAN プールを持つ物理ドメインが 1 つしかない場合、複数のドメインを単一の AEP に関連付けることができます。

入力および出力の両方向で個別の（ポート、VLAN）変換エントリの割り当てが可能なのは、`vlanScope` が `portlocal` に設定されているポートだけです。特定のポートで `vlanScope` が `portGlobal` (デフォルト) に設定されている場合には、EPG で使用される各 VLAN は、特定のリーフ スイッチ上で一意のものである必要があります。

（注） マルチ スパニング ツリー (MST) で設定されているインターフェイス上では、ポート単位の VLAN はサポートされていません。このツリーでは、VLAN ID が 1 つのリーフ スイッチ上で一意であること、そして VLAN の範囲がグローバルであることを必要とするからです。

同じリーフ スイッチで EPG に使用されていた VLAN 番号の再利用

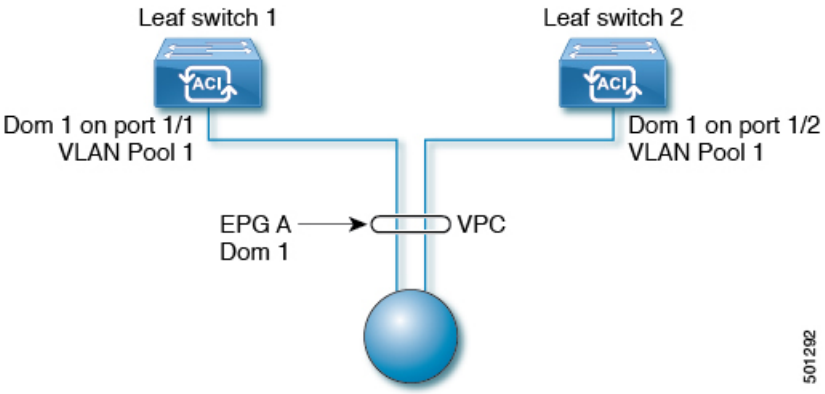
以前に、リーフ スイッチのポートに展開されている EPG 用に VLAN を設定していて、同じ VLAN 番号を同じリーフ スイッチの異なるポートの異なる EPG で再利用する場合には、中断なしでセットアップできるようにするため、次の例に示すようなプロセスに従ってください。

この例では、EPGは以前、9 ～ 100 の範囲の VLAN プールを含むドメインに関連付けられていたポートに展開されていました。ここで、9 ～ 20 からの VLAN カプセル化を使用する EPG を設定したいとします。

1. 異なるポート (たとえば、9 ～ 20 の範囲) で新しい VLAN プールを設定します。
2. ファイアウォールに接続されているリーフ ポートを含む新しい物理的なドメインを設定します。
3. ステップ 1 で設定した VLAN プールに物理的なドメインを関連付けます。
4. リーフ ポートの VLAN の範囲を `portLocal` として設定します。
5. 新しい EPG (この例ではファイアウォールが使用するもの) を、ステップ 2 で作成した物理ドメインに関連付けます。
6. リーフ ポートで EPG を展開します。

vPC に展開された EPG の VLAN ガイドライン

図 *13 : vPC の 2 つのレッグの VLAN*



EPG を vPC に展開する場合は、vPC の 2 つのレッグのリーフ スイッチ ポートに割り当てられた同じドメイン（同じ VLAN プール）に関連付ける必要があります。

この図では、EPG A は、リーフ スイッチ 1 およびリーフ スイッチ 2 のポートに展開されている vPC に展開されています。2 本のリーフ スイッチ ポートおよび EPG は、すべて同じ VLAN プールが含まれている同じドメインに関連付けられています。

特定のポートに EPG を導入する

GUI を使用して特定のノードまたはポートへ EPG を導入する

始める前に

EPG を導入するテナントがすでに作成されていること。

特定のノードまたはノードの特定のポートで、EPG を作成することができます。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 **[Tenants[** > ***[tenant]*** を選択します。

ステップ 3 左側のナビゲーション ウィンドウで、 ***tenant***、 **Application Profiles**、および ***application profile*** を展開します。

ステップ 4 **Application EPGs** を右クリックし、**Create Application EPG** を選択します。

ステップ 5 **Create Application EPG STEP 1 > Identity** ダイアログボックスで、次の操作を実行します:

a) **Name** フィールドに、EPG の名前を入力します。

b) **Bridge Domain** ドロップダウンリストから、ブリッジ ドメインを選択します。

c) [Statically Link with Leaves/Paths] チェックボックスをオンにします。

このチェック ボックスを使用して、どのポートに EPG を導入するかを指定できます。

d) [Next] をクリックします。

e) [Path] ドロップダウンリストから、宛先 EPG への静的パスを選択します。

ステップ 6 **Create Application EPG STEP 2 > Leaves/Paths** ダイアログボックスで、**Physical Domain** ドロップダウンリストから物理ドメインを選択します。

ステップ 7 次のいずれかの手順を実行します。

オプション	説明
次のものに EPG を展開する場合、	次を実行します。
ノード	**1.** **Leaves** エリアを展開します。 **2.** [Node] ドロップダウン リストから、ノードを選択します。 **3.** **Encap** フィールドで、適切な VLAN を入力します。 **4.** (オプション) **Deployment Immediacy** ドロップダウンリストで、デフォルトの **On Demand** のままにするか、**Immediate**を選択します。 **5.** (オプション) [Mode] ドロップダウンリストで、デフォルトの [Trunk] のままにするか、別のモードを選択します。
ノード上のポート	**1.** **Paths** エリアを展開します。 **2.** **Path** ドロップダウンリストから、適切なノードおよびポートを選択します。 **3.** (オプション) **Deployment Immediacy** フィールドのドロップダウンリストで、デフォルトの **On Demand** のままにするか、**Immediate** を選択します。 **4.** (オプション) [Mode] ドロップダウンリストで、デフォルトの [Trunk] のままにするか、別のモードを選択します。 **5.** **Port Encap** フィールドに、導入するセカンダリ VLAN を入力します。 **6.** (オプション) **Primary Encap** フィールドで、展開するプライマリ VLAN を入力します。

ステップ 8 **Update** をクリックし、**Finish** をクリックします。

ステップ 9 左側のナビゲーション ウィンドウで、作成した EPG を展開します。

ステップ 10 次のいずれかの操作を実行します:

- ノードで EPG を作成した場合は、**Static Leafs** をクリックし、作業ウィンドウで、静的バインド パスの詳細を表示します。

- ノードのポートでEPGを作成した場合は、**Static Ports** をクリックし、作業ウィンドウで、静的バインド パスの詳細を表示します。

NX-OS スタイルの CLI を使用した APIC の特定のポートへの EPG の導入

この手順では、NX-OS スタイルの CLI を使用し、Cisco Application Policy Infrastructure Controller（APIC）の特定のポートに EPG を展開します。

（注） Cisco APIC でインターフェイスごとの設定を行う際に、GUI と CLI を混在させないでください。GUI で実行した設定が、NX-OS スタイルの CLI では部分的にしか扱えない場合があります。

手順

ステップ 1 VLAN ドメインを設定します。

例：

```
apic1(config)# vlan-domain dom1
apic1(config-vlan)# vlan 10-100
```

ステップ 2 テナントを作成します。

例：

```
apic1# configure
apic1(config)# tenant t1
```

ステップ 3 プライベート ネットワーク/VRF を作成します。

例：

```
apic1(config-tenant)# vrf context ctx1
apic1(config-tenant-vrf)# exit
```

ステップ 4 ブリッジ ドメインを作成します。

例：

```
apic1(config-tenant)# bridge-domain bd1
apic1(config-tenant-bd)# vrf member ctx1
apic1(config-tenant-bd)# exit
```

ステップ 5 アプリケーション プロファイルおよびアプリケーション EPG を作成します。

例：

```
apic1(config-tenant)# application AP1
apic1(config-tenant-app)# epg EPG1
apic1(config-tenant-app-epg)# bridge-domain member bd1
apic1(config-tenant-app-epg)# exit
apic1(config-tenant-app)# exit
apic1(config-tenant)# exit
```

ステップ 6 EPG を特定のポートに関連付けます。

例：

```
apic1(config)# leaf 1017
apic1(config-leaf)# interface ethernet 1/13
apic1(config-leaf-if)# vlan-domain member dom1
apic1(config-leaf-if)# switchport trunk allowed vlan 20 tenant t1 application AP1 epg
EPG1
```

（注）
例に示した vlan-domain コマンドと vlan-domain member コマンドは、ポートに EPG を導入するための前提条件です。

特定のポートに EPG を導入するためのドメイン、接続可能アクセス エンティティ プロファイル、および VLAN の作成

特定のポートに EPG を導入するためのドメイン、接続可能アクセス エンティティ プロファイル、および VLAN の作成

このトピックでは、特定のポートに EPG を導入する場合に必須である物理ドメイン、接続可能アクセス エンティティ プロファイル（AEP）、および VLAN を作成する方法の典型的な例を示します。

すべてのエンドポイント グループ（EPG）にドメインが必要です。また、インターフェイス ポリシー グループを接続可能アクセス エンティティ プロファイル（AEP）に関連付ける必要があり、AEP と EPG が同じドメインに存在する必要がある場合は、AEP をドメインに関連付ける必要があります。EPG とドメイン、およびインターフェイス ポリシー グループとドメインの関連付けに基づいて、EPG が使用するポートと VLAN が検証されます。以下のドメインタイプが EPG に関連付けられます。

- アプリケーション EPG
- レイヤ 3 Outside 外部ネットワーク インスタンス EPG
- レイヤ 2 Outside 外部ネットワーク インスタンス EPG

- アウトオブバンドおよびインバンド アクセスの管理 EPG

APIC は、これらのドメイン タイプのうち 1 つまたは複数に EPG が関連付けられているかどうかを確認します。EPG が関連付けられていない場合、システムは設定を受け入れますが、エラーが発生します。ドメインの関連付けが有効でない場合、導入された設定が正しく機能しない可能性があります。たとえば、VLAN のカプセル化を EPG で使用することが有効でない場合、導入された設定が正しく機能しない可能性があります。

（注） スタティック バインディングを使用しない AEP との EPG アソシエーションは、一方のエンドポイントが同じ EPG の下でタギングをサポートし、もう一方のエンド ポイントが同じ EPG 内で VLAN タギングをサポートしないような AEP の下では、EPG を**トランク**として設定するシナリオで機能させることはできません。EPG で AEPを関連付ける際には、トランク、アクセス（タグ付き）、またはアクセス（タグなし）として設定できます。

GUI を使用して特定のポートに EPG を展開するためのドメインおよび VLAN の作成

始める前に

- EPG を導入するテナントがすでに作成されていること。
- EPG は特定のポートに静的に導入されます。

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（Navigation）]** ペインで、**[クイックスタート（Quick Start）]** をクリックします。

ステップ 3 **[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。

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。

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。

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）]** ダイアログの **[リンク レベル ポリシー（Link Level Policy）]** で、**[リンク レベル ポリシーの選択（Select Link Level Policy）]** をクリックします。

j) リンク レベル ポリシーを選択して **[選択（Select）]** を選択するか、**[リンク レベル ポリシーの作成（Create Link Level 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）]** をクリックします。

k) [保存（Save）] をクリックします。

ステップ 5 以下のアクションを実行して、ドメインと VLAN プールを作成します。

a) **[ナビゲーション（Navigation）]** ペインで、**[物理ドメインと外部ドメイン（Physical and External Domains）]** を展開します。

b) **[物理ドメイン（Physical Domains）]** を右クリックし、適切な**[物理ドメインの作成（Create Physical Domain）]** を選択します。

c) **[名前（Name）]** に、ドメインの名前を入力します。

d) **[VLAN プール（VLAN Pool）]**で、**[VLAN プールの作成（Create VLAN Pool）]** を選択し、必要に応じてフィールドに入力して、**[送信（Submit）]** をクリックします。

e) 目的に応じて、残りのフィールドに入力します。

f) [送信（Submit）] をクリックします。

ステップ 6 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。

ステップ 7 **[作業（Work）]** ペインで、目的のテナントをダブルクリックします。

ステップ 8 **[ナビゲーション（Navigation）]** ペインで、**テナント名** > **[アプリケーション プロファイル（Application Profiles）]** > **プロファイル名** > **[アプリケーション EPG（Application EPGs）]** > ***EPG* 名**を展開し、以下の操作を実行します。

a) **[ドメイン（Domains）（VM またはベアメタル）]** を右クリックし、**[物理ドメインの関連付けの追加（Add Physical Domain Association）]** をクリックします。

b) **[物理ドメインの関連付けの追加（Add Physical Domain Association）]** ダイアログで、**[物理ドメインのプロファイル（Physical Domain Profile）]** ドロップダウン リストから、前に作成したドメインを選択します。

c) [Submit] をクリックします。
AEP は、ノード上の特定のポート、およびドメインに関連付けられます。物理ドメインは VLAN プールに関連付けられ、テナントはこの物理ドメインに関連付けられます。

スイッチ プロファイルとインターフェイス プロファイルが作成されます。インターフェイス プロファイルのポート ブロックにポリシー グループが作成されます。AEP が自動的に作成され、ポート ブロックおよびドメインに関連付けられます。ドメインは VLAN プールに関連付けられ、テナントはドメインに関連付けられます。

NX-OS スタイルの CLI を使用した、EPG を特定のポートに導入するための AEP、ドメイン、および VLAN の作成

始める前に

- EPG を導入するテナントがすでに作成されていること。
- EPG は特定のポートに静的に導入されます。

手順

ステップ 1 VLAN ドメインを作成し、VLAN 範囲を割り当てます。

例：

```
apic1(config)# vlan-domain domP
apic1(config-vlan)# vlan 10
apic1(config-vlan)# vlan 25
apic1(config-vlan)# vlan 50-60
apic1(config-vlan)# exit
```

ステップ 2 インターフェイス ポリシー グループを作成し、そのポリシー グループに VLAN ドメインを割り当てます。

例：

```
apic1(config)# template policy-group PortGroup
apic1(config-pol-grp-if)# vlan-domain member domP
```

ステップ 3 リーフ インターフェイス プロファイルを作成し、そのプロファイルにインターフェイス ポリシー グループを割り当てて、そのプロファイルを適用するインターフェイス ID を割り当てます。

例：

```
apic1(config)# leaf-interface-profile InterfaceProfile1
apic1(config-leaf-if-profile)# leaf-interface-group range
apic1(config-leaf-if-group)# policy-group PortGroup
apic1(config-leaf-if-group)# interface ethernet 1/11-13
apic1(config-leaf-if-profile)# exit
```

ステップ 4 リーフ プロファイルを作成し、そのリーフ プロファイルにリーフ インターフェイス プロファイルを割り当てて、そのプロファイルを適用するリーフ ID を割り当てます。

例：

```
apic1(config)# leaf-profile SwitchProfile-1019
apic1(config-leaf-profile)# leaf-interface-profile InterfaceProfile1
apic1(config-leaf-profile)# leaf-group range
apic1(config-leaf-group)# leaf 1019
apic1(config-leaf-group)#
```

重複する VLAN の検証

このグローバル機能は、単一の EPG での重複する VLAN プールの関連付けを防止します。APIC のいずれかの EPG で重複するプールが割り当てられている場合、この機能は有効にできません（有効にしようとするとエラーが表示されます）。既存の重複プールが存在しない場合は、この機能を有効にできます。有効にすると、EPGにドメインを割り当てることを試行し、そのドメインに、EPG にすでに関連付けられている別のドメインと重複する VLAN プールが含まれていた場合、設定はブロックされます。

重複する VLAN プールが EPG の下に存在する場合、各スイッチによって EPG に割り当てられる FD VNID は非確定的になり、異なるスイッチが異なる VNID を割り当てる場合があります。これにより、vPC ドメイン内のリーフ間で EPM 同期が失敗する可能性が生じます（EPG 内のすべてのエンドポイントの接続が断続的になります）。また、ユーザーが EPG 間で STP を拡張している場合、FDVNIDの不一致によりスイッチ間でBPDUがドロップされるため、ブリッジング ループが発生する可能性もあります。

GUI を使用した重複 VLAN の検証

この手順では、APIC GUI を使用して VLAN のオーバーラップの検証を設定する例を示します。

手順

ステップ 1 メニュー バーで、**[システム（System）] > [システム設定（System Settings）]** を選択します。

ステップ 2 ナビゲーション ペインで、**[ファブリック ワイドの設定（Fabric Wide Setting）]** を選択します。

ステップ 3 作業ウィンドウで、**[EPG VLAN 検証の適用（Enforce EPG VLAN Validation）]** を見つけてオンにします。

（注）
重複する VLAN プールがすでに存在し、このパラメータがオンになっている場合、システムはエラーを返します。この機能を選択する前に、EPG に重複しない VLAN プールを割り当てる必要があります。

このパラメータをオンにして、重複する VLAN プールを EPG に追加しようとすると、エラーが返されます。

ステップ 4 [送信（Submit）] をクリックします。

添付されているエンティティ プロファイルで複数のインターフェイスに EPG を導入する

AEP を使用してアプリケーション EPG を複数のポートに展開する

APIC GUI と REST API を使用して、接続可能エンティティ プロファイルをアプリケーション EPG に直接関連付けることができます。これにより、単一の構成の接続可能エンティティ プロファイルに関連付けられたすべてのポートに、関連付けられたアプリケーション EPG を導入します。

APIC GUI を使用した AEP による複数のインターフェイスへの EPG の導入

アプリケーション EPG を接続可能アクセス エンティティ プロファイルに関連付けて、その接続可能アクセス エンティティ プロファイルに関連付けられたすべてのポートに EPG を導入することができます。

始める前に

- ターゲット アプリケーション EPG が作成されている。
- AEP での EPG 導入に使用する VLAN の範囲が含まれている VLAN プールが作成されている。
- 物理ドメインが作成され、VLAN プールと AEP にリンクされている。
- ターゲットの接続可能アクセス エンティティ プロファイルが作成され、アプリケーション EPG を導入するポートに関連付けられている。
- Cisco APIC 6.1(3) よりも前は、アクセス ポリシー階層を介してのみ、アプリケーションを接続可能アクセスエンティティプロファイルに関連付けることができました。Cisco APIC 6.1(3) 以降は、テナント階層またはアクセス ポリシー階層を介して、アプリケーションを接続可能アクセス エンティティ プロファイルに関連付けることができるようになりました。

（注） これらの特定の階層のいずれかを使用して AEP アタッチメントを作成する場合は、後続の変更操作も、作成された階層でのみ実行する必要があります。操作に重複がある場合、Cisco APIC はこの設定を拒否します。

手順

ステップ 1 次のいずれかの方法を使用して、アプリケーション EPG を接続可能アクセス エンティティ プロファイルに関連付けることができます。

a) 使用するアプリケーション EPG のページを開きます。GUI で、**[テナント（Tenant）]** > **[tenant_name]** > **[アプリケーション プロファイル（Application Profiles）]** > **[epg_name]** > **[静的 AAEP（Static AAEP）]**をクリックします。

b) **[静的 AAEP（Static AAEP）]** ウィンドウで、ターゲット接続可能アクセス エンティティ プロファイルをアプリケーション EPG に関連付けます。

フィールド	アクション（Action）
名前	AEP の名前を選択します。
Encap	ターゲット アプリケーション EPG の通信に使用される VLAN の ID を入力します。
Primary Encap	（オプション）アプリケーション EPG にプライマリ VLAN が必要な場合は、プライマリ VLAN の ID を入力します。
展開の緊急性	**[直ちに展開（Deployment Immediacy）]** フィールドのドロップダウンリストで、デフォルトの **[オンデマンド（On Demand）]** のままにするか、**[即座（Immediate）]** を選択します。
モード（Mode）	データを送信するモードを指定します： • **[トランク（Trunk）]**：ホストからのトラフィックに VLAN ID がタグ付けされている場合に選択します。 • **[トランク（ネイティブ）（Trunk（Native））]**：ホストからのトラフィックに 802.1p タグがタグ付けされている場合に選択します。 • **[アクセス（タグなし）（Access（Untagged））]**：ホストからのトラフィックがタグ付けされていない場合に選択します。

ステップ 2 または、この方法を使用して、アプリケーション EPG を接続エンティティ プロファイルに関連付けます。

a) 使用する接続可能アクセス エンティティ プロファイルのページを開きます。**[ファブリック（Fabric）]** > **[アクセス ポリシー（Access Policies）]** > **[ポリシー（Policies）]** > **[グローバル（Global）]** > **[接続可能アクセス エンティティ プロファイル（Attachable Access Entity Profiles）]**に移動します。

b) ターゲットの接続エンティティ プロファイルをクリックして、[接続可能アクセスエンティティ プロファイル（Attachable Access Entity Profiles）] ウィンドウを開きます。

c) **[使用方法を表示（Show Usage）]** ボタンをクリックして、この接続可能アクセスエンティティ プロファイルに関連付けられたリーフ スイッチとインターフェイスを表示します。

この接続エンティティ プロファイルに関連付けられたアプリケーション EPG が、この接続エンティティ プロファイルに関連付けられたすべてのスイッチ上のすべてのポートに展開されます。

d) **[アプリケーション EPG（Application EPGs）]** テーブルに基づき、この接続可能アクセスエンティティ プロファイルにターゲット アプリケーション EPG を関連付けます。アプリケーション EPG エントリを追加するには、[+] をクリックします。各エントリに次のフィールドがあります。

フィールド	アクション（Action）
Application EPG	ドロップダウンを使用して、関連付けられたテナント、アプリケーション プロファイル、およびターゲット アプリケーション EPG を選択します。
Encap	ターゲット アプリケーション EPG の通信に使用される VLAN ID の名前を入力します。
Primary Encap	（オプション）アプリケーション EPG にプライマリ VLAN が必要な場合は、プライマリ VLAN ID の名前を入力します。
モード	ドロップダウンを使用して、データを送信するモードを指定します。 • [Trunk]：ホストからのトラフィックに VLAN ID がタグ付けされている場合に選択します。 • **[トランク（ネイティブ）（Trunk（Native））]**：ホストからのトラフィックに 802.1p タグがタグ付けされている場合に選択します。 • **[アクセス（タグなし）（Access（Untagged））]**：ホストからのトラフィックがタグ付けされていない場合に選択します。

ステップ 3 [送信（Submit）] をクリックします。
この接続可能アクセス エンティティ プロファイルに関連付けられたアプリケーション EPG が、この接続可能アクセス エンティティ プロファイルに関連付けられたすべてのスイッチ上のすべてのポートに展開されます。

EPG 内の分離

EPG 内エンドポイント分離

EPG内エンドポイント分離ポリシーにより、仮想エンドポイントまたは物理エンドポイントが完全に分離されます。分離を適用した状態で稼働している EPG 内のエンドポイント間の通信は許可されません。分離を適用した EGP では、多くのクライアントが共通サービスにアクセスするときに必要な EPG カプセル化の数は低減しますが、相互間の通信は許可されません。

EPG の分離は、すべての Cisco Application Centric Infrastructure（ACI）ネットワーク ドメインに適用されるか、どれにも適用されないかの、どちらかになります。Cisco ACI ファブリックは接続エンドポイントに直接分離を実装しますが、ファブリックに接続されているスイッチはプライマリ VLAN（PVLAN）タグに従って分離規則を認識します。

（注） EPG 内エンドポイント分離を適用して EPG を設定した場合は、次の制限が適用されます。

- 分離を適用した EPG 全体のすべてのレイヤ 2 エンドポイント通信がブリッジ ドメイン内にドロップされます。
- 分離を適用した EPG 全体のすべてのレイヤ 3 エンドポイント通信が同じサブネット内にドロップされます。
- トラフィックが、分離が適用されている EPG から分離が適用されていない EPG に流れている場合、QoS CoS の優先順位設定の保持はサポートされません。

BPDU は、EPG 内分離が有効になっている EPG を介して転送されません。したがって、Cisco ACI 上の独立した EPG にマッピングされている VLAN でスパニング ツリーを実行する外部レイヤ 2 ネットワークを接続すると、Cisco ACI は外部ネットワークのスパニング ツリーがレイヤ2ループを検出できなくなる可能性があります。この問題を回避するには、これらの VLAN 内の Cisco ACI と外部ネットワーク間に単一の論理リンクのみを設定します。

ベア メタル サーバの EPG 内分離

ベア メタル サーバの EPG 内分離

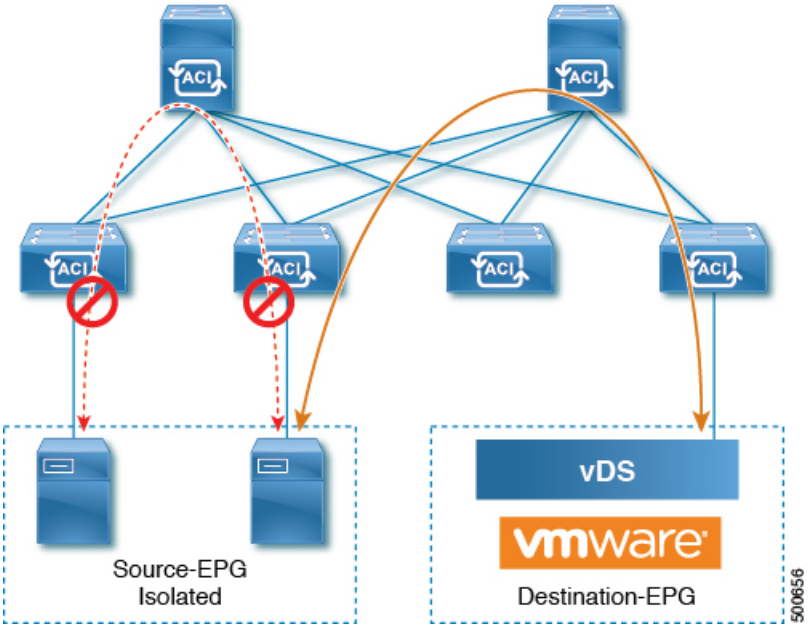
EPG 内エンドポイント分離のポリシーは、ベア メタル サーバなどの直接接続されているエンドポイントに適用できます。

次のような使用例があります。

- バックアップ クライアントは、バックアップ サービスにアクセスするための通信要件は同じですが、相互に通信する必要はありません。

- ロードバランサの背後にあるサーバの通信要件は同じですが、それらのサーバを相互に分離すると、不正アクセスや感染のあるサーバに対して保護されます。

図 *14*：ベア メタル サーバの *EPG* 内分離



ベア メタル の EPG 分離はリーフ スイッチで適用されます。ベア メタル サーバは VLAN カプセル化を使用します。ユニキャスト、マルチキャスト、およびブロードキャストのすべてのトラフィックが、分離が適用された EPG 内でドロップ（拒否）されます。ACI ブリッジ ドメインには、分離された EPG と通常の EPG を混在させることができます。分離された EPG それぞれには、VLAN 間トラフィックを拒否する複数の VLAN を指定できます。

GUI を使用したベア メタル サーバの EPG 内分離の設定

EPG が使用するポートは、リーフ スイッチにベア メタル サーバを直接接続するために使用する物理ドメイン内のベア メタル サーバと関連付ける必要があります。

手順

ステップ 1 テナントで、[Application Profile] を右クリックし、[Create Application EPG] ダイアログ ボックスを開いて次の操作を実行します。

a) [Name] フィールドに、EPG の名前（intra_EPG-deny）を追加します。
b) [Intra EPG Isolation] で、[Enforced] をクリックします。
c) [Bridge Domain] フィールドで、ドロップダウン リストからブリッジ ドメイン（bd1）を選択します。
d) [Statically Link with Leaves/Paths] チェックボックスをオンにします。
e) [Next] をクリックします。

ステップ 2 [Leaves/Paths] ダイアログボックスで、次の操作を実行します。

a) [Path] セクションで、ドロップダウン リストからトランク モードでのパス（Node-107/eth1/16）を選択します。

セカンダリ VLAN の [Port Encap]（vlan-102）を指定します。

（注）
ベア メタル サーバがリーフ スイッチに直接接続されている場合、Port Encap のセカンダリ VLAN のみが指定されます。

プライマリ VLAN の [Primary Encap]（vlan-103）を指定します。

b) [Update] をクリックします。

c) **[完了（Finish）]** をクリックします。

NX-OS スタイルの CLI を使用したベア メタル サーバの EPG 内分離の設定

手順

	コマンドまたはアクション	目的

ステップ 1	CLI で、EPG 内分離 EPG を作成します。
	例：
	以下に、VMM ケースを示します。
	`ifav19-ifc1(config)# tenant Test_Isolation`
	`ifav19-ifc1(config-tenant)# application PVLAN`
	`ifav19-ifc1(config-tenant-app)# epg EPG1`
	`ifav19-ifc1(config-tenant-app-epg)# show running-config`
	`# Command: show running-config`
	`tenant Test_Isolation`
	`application PVLAN epg EPG1`
	`tenant Test_Isolation`
	`application PVLAN`
	`epg EPG1`
	`bridge-domain member BD1`
	`contract consumer bare-metal`
	`contract consumer default`
	`contract provider Isolate_EPG`
	`isolation enforce <---- This enables EPG isolation mode.`
	`exit`
	`exit`
	`ifav19-ifc1(config)# leaf ifav19-leaf3`
	`ifav19-ifc1(config-leaf)# interface ethernet 1/16`
	`ifav19-ifc1(config-leaf-if)# show running-config`	

	コマンドまたはアクション	目的
	`ifav19-ifc1(config-leaf-if)# switchport trunk native vlan 101 tenant Test_Isolation application PVLAN epg StaticEPG primary-vlan 100` `exit`	

ステップ 2	設定を確認します。
	例：
	`show epg StaticEPG detail`
	`Application EPg Data:`
	`Tenant : Test_Isolation`
	`Application : PVLAN`
	`AEPg : StaticEPG`
	`BD : BD1`
	`uSeg EPG : no`
	`Intra EPG Isolation : enforced`
	`Vlan Domains : phys`
	`Consumed Contracts : bare-metal`
	`Provided Contracts : default,Isolate_EPG`
	`Denied Contracts :`
	`Qos Class : unspecified`
	`Tag List :`
	`VMM Domains:`
	`Domain Type Deployment Immediacy Resolution Immediacy State Encap Primary Encap`
	`--- --- --- --- --- --- --- ---`
	`DVS1 VMware On Demand immediate formed auto auto`
	
	`Static Leaves:`
	`Node Encap Deployment Immediacy Mode Modification Time`
	`--- --- --- --- --- --- --- ---`
	
	`Static Paths:`
	`Node Interface Encap Modification Time`
	`--- --- --- --- --- --- --- ---`
	`1018 eth101/1/1 vlan-100 2016-02-11T18:39:02.337-08:00`
	`1019 eth1/16`	

	コマンドまたはアクション	目的
	vlan-101 2016-02-11T18:39:02.337-08:00 Static Endpoints: Node Interface Encap End Point MAC End Point IP Address Modification Time ---------- ---------- ---------- ---------- ---------- ----------	

VMware vDS の EPG 内分離

VMware VDS または Microsoft Hyper-V 仮想スイッチの EPG 分離

EPG 内分離は、同じベース EPG またはマイクロセグメント（uSeg）EPG にある物理または仮想エンドポイントデバイスが相互に通信しないようにするオプションです。デフォルトでは、同じ EPG に含まれるエンドポイントデバイスは互いに通信することができます。しかし、EPG 内のエンドポイント デバイスの別のエンドポイント デバイスからの完全な分離が望ましい状況が存在します。たとえば、同じ EPG 内のエンドポイント VM が複数のテナントに属している場合、またはウイルスが広がるのを防ぐために、EPG 内の分離を実行することができます。

Cisco Application Centric Infrastructure（ACI）仮想マシン マネージャ（VMM）ドメインは、EPG 内分離が有効になっている EPG ごとに、VMware VDS または Microsoft Hyper-V 仮想スイッチで分離 PVLAN ポート グループを作成します。ファブリック管理者がプライマリ カプセル化を指定するか、または EPG と VMM ドメインの関連付け時にファブリックが動的にプライマリ カプセル化を指定します。ファブリック管理者が VLAN pri 値と VLAN-sec 値を静的に選択すると、VMM ドメインによって VLAN-pri と VLAN-sec がドメイン プール内のスタティック ブロックの一部であることが検証されます。

プライマリ カプセル化は、EPG VLAN ごとに定義されます。EPG 内分離にプライマリ カプセル化を使用するには、次のいずれかの方法で展開する必要があります。

- プライマリ VLAN とセカンダリ VLAN で定義されたポートを異なるスイッチに分離します。EPG VLAN はスイッチごとに作成されます。ポート カプセル化があり、EPG のスイッチ上のスタティック ポートのみの場合、プライマリ カプセル化は関連付けられません。
- ポート カプセル化のみを使用するスタティック ポートには別のカプセル化を使用します。これにより、プライマリカプセル化が関連付けられていない2番目のEPG VLANが作成されます。

次の例では、プライマリ VLAN-1103 を持つ 2 つのインターフェイス（Eth1/1、Eth1/3）の出力トラフィックを考慮します。Eth1/1ポート カプセル化が VLAN-1132 に（VLAN-1130 から）変更されたため、Eth1/3とセカンダリ VLAN を共有しません。

```
Port encap with VLAN-1130 on Eth1/1
Eth1/1: Port Encap only VLAN-1130
Eth1/6: Primary VLAN-1103 and Secondary VLAN-1130


fab2-leaf3# show vlan id 53 ext

VLAN Name                             Encap            Ports
---- -------------------------------- ---------------- ------------------------
53   JT:jt-ap:EPG1-1                  vlan-1130        Eth1/1, Eth1/3

module-1# show sys int eltmc info vlan access_encap_vlan 1130
            vlan_id:             53   :::           isEpg:              1
          bd_vlan_id:            52   :::         hwEpgId:          11278
      srcpolicyincom:             0   :::       data_mode:              0
        accencaptype:             0   :::    fabencaptype:              2
       accencapval:           1130   :::     fabencapval:          12192
             sclass:          49154   :::         sglabel:             12
          sclassprio:              1   :::     floodmetptr:             13
          maclearnen:              1   :::       iplearnen:              1
         sclasslrnen:              1   :::   bypselffwdchk:              0
            qosusetc:              0   :::       qosuseexp:              0
            isolated:              1   :::   primary_encap:           1103
           proxy_arp:              0   :::       qinq core:              0
           ivxlan_dl:              0   :::       dtag_mode:              0
      is_service_epg:              0


Port encap changed to VLAN-1132 on Eth1/1
fab2-leaf3# show vlan id 62 ext

VLAN Name                             Encap            Ports
---- -------------------------------- ---------------- ------------------------
62   JT:jt-ap:EPG1-1                  vlan-1132        Eth1/1

module-1# show sys int eltmc info vlan access_encap_vlan 1132
          [SDK Info]:
            vlan_id:             62   :::           isEpg:              1
          bd_vlan_id:            52   :::         hwEpgId:          11289
      srcpolicyincom:             0   :::       data_mode:              0
        accencaptype:             0   :::    fabencaptype:              2
        accencapval:           1132   :::     fabencapval:          11224
             sclass:          49154   :::         sglabel:             12
          sclassprio:              1   :::     floodmetptr:             13
          maclearnen:              1   :::       iplearnen:              1
         sclasslrnen:              1   :::   bypselffwdchk:              0
            qosusetc:              0   :::       qosuseexp:              0
            isolated:              1   :::   primary_encap:              0
           proxy_arp:              0   :::       qinq core:              0
           ivxlan_dl:              0   :::       dtag_mode:              0
      is_service_epg:              0

fab2-leaf3# show vlan id 53 ext

VLAN Name                             Encap            Ports
---- -------------------------------- ---------------- ------------------------
53   JT:jt-ap:EPG1-1                  vlan-1130        Eth1/3

module-1# show sys int eltmc info vlan access_encap_vlan 1130
          [SDK Info]:
```

```
        vlan_id:            53   :::          isEpg:             1
     bd_vlan_id:            52   :::        hwEpgId:         11278
srcpolicyincom:              0   :::      data_mode:             0
  accencaptype:              0   :::   fabencaptype:             2
  accencapval:            1130  :::    fabencapval:         12192
        sclass:           49154  :::        sglabel:            12
   sclassprio:               1   :::    floodmetptr:            13
   maclearnen:               1   :::      iplearnen:             1
  sclasslrnen:               1   :::  bypselffwdchk:             0
     qosusetc:               0   :::      qosuseexp:             0
     isolated:               1   :::  primary_encap:          1103
    proxy_arp:               0   :::      qinq core:             0
    ivxlan_dl:               0   :::      dtag_mode:             0
```

（注）

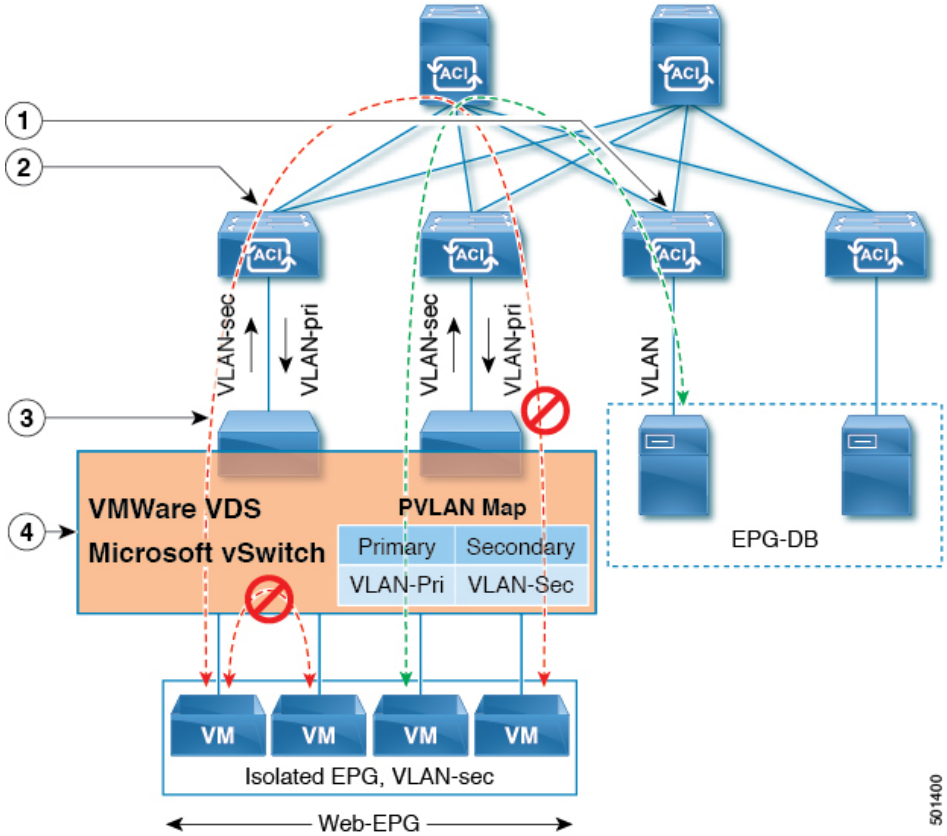
- イントラ EPG 隔離が強制されない場合、設定で指定されていても VLAN-pri 値は無視されます。
- EDM UCSM 統合を使用した VMware 分散仮想スイッチ（DVS）ドメインが失敗することがあります。ドメインに接続されているエンドポイント グループ（EPG）で EPG 内分離を設定し、プライベート VLAN をサポートしない UCSM Mini 6324 を使用すると、ドメインに障害が発生します。

BPDU は、EPG 内分離が有効になっている EPG を介して転送されません。したがって、Cisco ACI 上の独立した EPG にマッピングされている VLAN でスパニング ツリーを実行する外部レイヤ 2 ネットワークを接続すると、Cisco ACI は外部ネットワークのスパニング ツリーがレイヤ 2 ループを検出できなくなる可能性があります。この問題を回避するには、これらの VLAN 内の Cisco ACI と外部ネットワーク間に単一の論理リンクのみを設定します。

VMware VDS または Microsoft Hyper-V 仮想スイッチの VLAN-pri/VLAN-sec ペアは、EPG とドメインの関連付け中に VMM ドメインごとに選択されます。EPG 内隔離 EPG に作成されたポート グループは PVLAN に設定されたタイプでタグ付けされた VLAN-sec を使用します。VMware VDS または Microsoft Hyper-V 仮想スイッチおよびファブリックは、VLAN-pri/VLAN-sec カプセル化をスワップします。

- Cisco ACI ファブリックから VMware VDS または Microsoft Hyper-V 仮想スイッチへの通信は VLAN-pri を使用します。
- VMware VDS または Microsoft Hyper-V 仮想スイッチから Cisco ACI ファブリックへの通信は VLAN-sec を使用します。

図 *15 : VMware VDS* または *Microsoft Hyper-V* 仮想スイッチの *EPG* 分離



この図に関する次の詳細に注意してください。

1. EPG-DB は Cisco ACI リーフスイッチに VLAN トラフィックを送信します。Cisco ACI 出力リーフ スイッチは、プライマリ VLAN（PVLAN）タグを使用してトラフィックをカプセル化し、Web-EPG エンドポイントに転送します。

2. VMware VDS または Microsoft Hyper-V 仮想スイッチは、VLAN-sec を使用して Cisco ACI リーフ スイッチにトラフィックを送信します。 Web-EPG 内のすべての VLAN 内トラフィックに対して分離が適用されるため、Cisco ACI リーフ スイッチはすべての EPG 内トラフィックをドロップします。

3. Cisco ACI リーフ スイッチへの VMware VDS または Microsoft Hyper-V 仮想スイッチ VLAN-sec アップリンクが分離トランク モードです。Cisco ACI リーフ スイッチは、VMware VDS または Microsoft Hyper-V 仮想スイッチへのダウンリンク トラフィックに VLAN-pri を使用します。

4. PVLAN マップは、VMware VDS または Microsoft Hyper-V 仮想スイッチおよび Cisco ACI リーフ スイッチで設定されます。WEB-EPG からの VM トラフィックは VLAN-sec 内でカプセル化されます。VMware VDS または Microsoft Hyper-V 仮想スイッチは PVLAN タグに従ってローカルの WEB 内 EPG VM トラフィックを拒否します。すべての内部 ESXi ホストまたは Microsoft Hyper-V ホスト VM トラフィックは、VLAN-Sec を使用して Cisco ACI リーフ スイッチに送信されます。

GUI を使用した VMware VDS または Microsoft Hyper-V の EPG 内分離の設定

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 **Tenants** > ***tenant*** を選択します。

ステップ 3 左側のナビゲーション ウィンドウで、**[アプリケーション プロファイル]** フォルダと適切なアプリケーション プロファイルを展開します。

ステップ 4 **Application EPGs** フォルダを右クリックし、**Create Application EPG** を選択します。

ステップ 5 **Create Application EPG** ダイアログ ボックスで、次の手順を実行します:

a) **Name** フィールドに EPG 名を追加します。

b) **Intra EPG Isolation** エリアで、**Enforced** をクリックします。

c) **Bridge Domain** フィールドで、ドロップダウン リストからブリッジ ドメインを選択します。

d) EPG をベア メタル/物理ドメイン インターフェイスまたは VM ドメインに関連付けます。

- VM ドメインの場合、[Associate to VM Domain Profiles] チェックボックスをオンにします。
- ベア メタルの場合、[Statically Link with Leaves/Paths] チェックボックスをオンにします。

e) [Next] をクリックします。

f) **Associated VM Domain Profiles** エリアで、**+** アイコンをクリックします。

g) **Domain Profile** プロファイルのドロップダウン リストから、適切な VMM ドメインを選択します。

スタティックの場合、**Port Encap (or Secondary VLAN for Micro-Seg)** フィールドでセカンダリ VLAN を指定し、**Primary VLAN for Micro-Seg** フィールドで、プライマリ VLAN を指定します。Encap フィールドを空白のままにすると、値が動的に割り当てられます。

（注）
スタティックの場合、スタティック VLAN を VLAN プールで使用できる必要があります。

ステップ 6 **Update** をクリックし、**Finish** をクリックします。

NX-OS スタイル CLI を使用した VMware VDS または Microsoft Hyper-V の EPG 内分離の設定

手順

ステップ 1 CLI で、EPG 内分離 EPG を作成します。

例：

次の例は VMware VDSの場合です:

```
apic1(config)# tenant Test_Isolation
apic1(config-tenant)# application PVLAN
apic1(config-tenant-app)# epg EPG1
apic1(config-tenant-app-epg)# show running-config
# Command: show running-config tenant Tenant_VMM application Web epg intraEPGDeny
  tenant Tenant_VMM
    application Web
      epg intraEPGDeny
        bridge-domain member VMM_BD
       vmware-domain member PVLAN encap vlan-2001 primary-encap vlan-2002 push on-demand

        vmware-domain member mininet
          exit
        isolation enforce
        exit
      exit
    exit
apic1(config-tenant-app-epg)#
```

例：

次の例は、Microsoft Hyper-V 仮想スイッチを示します。

```
apic1(config)# tenant Test_Isolation
apic1(config-tenant)# application PVLAN
apic1(config-tenant-app)# epg EPG1
apic1(config-tenant-app-epg)# show running-config
# Command: show running-config tenant Tenant_VMM application Web epg intraEPGDeny
  tenant Tenant_VMM
    application Web
      epg intraEPGDeny
        bridge-domain member VMM_BD
        microsoft-domain member domain1 encap vlan-2003 primary-encap vlan-2004
        microsoft-domain member domain2
          exit
        isolation enforce
        exit
      exit
    exit
apic1(config-tenant-app-epg)#
```

ステップ 2 設定を確認します。

例：

```
 show epg StaticEPG detail
Application EPg Data:
Tenant              : Test_Isolation
```

```
Application         : PVLAN
AEPg                : StaticEPG
BD                  : VMM_BD
uSeg EPG            : no
Intra EPG Isolation : enforced
Vlan Domains        : VMM
Consumed Contracts  : VMware_vDS-Ext
Provided Contracts  : default,Isolate_EPG
Denied Contracts    :
Qos Class           : unspecified
Tag List            :
VMM Domains:
Domain                Type       Deployment Immediacy  Resolution Immediacy  State
      Encap       Primary
Encap
 --------------------  ---------  --------------------  --------------------
--------------  ----------  ----------
 DVS1                  VMware     On Demand             immediate             formed
       auto        auto

Static Leaves:
 Node        Encap             Deployment Immediacy  Mode                Modification
Time
----------  ----------------  --------------------  ------------------
------------------------------

Static Paths:
 Node        Interface                       Encap             Modification Time

 ----------  ------------------------------  ----------------
------------------------------
 1018        eth101/1/1                      vlan-100
2016-02-11T18:39:02.337-08:00
 1019        eth1/16                         vlan-101
2016-02-11T18:39:02.337-08:00

Static Endpoints:
 Node        Interface          Encap            End Point MAC      End Point IP Address
          Modification Time
 ----------  ------------------------------  ----------------  -----------------
------------------------------  ------------------------------

Dynamic Endpoints:
Encap: (P):Primary VLAN, (S):Secondary VLAN
 Node        Interface            Encap             End Point MAC      End Point IP
Address         Modification Time
 ----------  ------------------------------  ----------------  -----------------
------------------------------  ------------------------------
1017        eth1/3              vlan-943(P)       00:50:56:B3:64:C4  ---
         2016-02-17T18:35:32.224-08:00
                                 vlan-944(S)
```

Cisco ACI 仮想エッジの EPG 内分離の設定

Cisco ACI Virtual Edge での EPG 内分離の適用

デフォルトでは、EPGに属するエンドポイントは契約が設定されていなくても相互に通信できます。ただし、相互に、EPG 内のエンドポイントを特定できます。たとえば、EPG 内でウイルスや他の問題を持つ VM が EPG の他の VM に影響を及ぼすことがないように、エンドポイント分離を適用するのが望ましい場合があります。

アプリケーション内のすべてのエンドポイントに分離を設定することも、いずれにも設定しないこともできます。一部のエンドポイントに分離を設定し、他のエンドポイントに設定しない方法は使用できません。

EPG 内のエンドポイントを分離しても、エンドポイントが別の EPG 内のエンドポイントと通信できるようにするコントラクトには影響しません。

（注） VLAN モードで Cisco ACI Virtual Edge ドメインと関連付けられている EPG での EPG内分離の適用はサポートされていません。このような EPG で EPG 内の分離を適用しようとすると、エラーがトリガーされます。

（注） Cisco ACI Virtual Edge マイクロセグメント (uSeg) EPG で EPG 内分離を使用することは現在のところサポートされていません。

（注） VXLAN カプセル化を使用し、EPG 内分離が適用されている Cisco ACI Virtual Edge EPG では、プロキシ ARP はサポートされていません従って、Cisco ACI Virtual Edge EPG 間で契約が設定されていても、EPG 内分離された EPG 間でサブネット間通信を行うことはできません。(VXLAN)。

GUI を使用した Cisco ACI Virtual Edge の EPG 内分離の設定

この手順に従って、EPG のエンドポイントが相互に分離されている EPG を作成します。

EPG が使用するポートは VM マネージャ（VMM）のいずれかに属している必要があります。

（注） この手順は、EPG の作成時に EPG 内のエンドポイントを分離することを前提としています。既存の EPG 内のエンドポイントを分離するには、Cisco APIC 内の EPG を選択し、[Properties] ペインの [Intra EPG Isolation] 領域で [Enforced] を選択して [SUBMIT] をクリックします。

始める前に

VXLAN 関連の設定が Cisco ACI Virtual Edge VMM ドメインに存在すること、特に Cisco ACI Virtual Edge ファブリック全体のマルチキャスト アドレスとマルチキャスト アドレスのプール (EPG ごとに 1 つ) が存在することを確認します。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 [Tenants] を選択してテナントのフォルダを展開し、[Application Profiles] フォルダを展開します。

ステップ 3 アプリケーション プロファイルを右クリックし、[Create Application EPG] を選択します。

ステップ 4 [Create Application EPG] ダイアログボックスで、次の手順を実行します。

a) [Name] フィールドに EPG 名を入力します。

b) [Intra EPG Isolation] 領域で、[Enforced] をクリックします。

c) [Bridge Domain] ドロップダウン リストから、ブリッジ ドメインを選択します。

d) [Associate to VM Domain Profiles] チェックボックスをオンにします。

e) [Next] をクリックします。

f) **Associate VM Domain Profiles** エリアで、次の手順に従います:

- **+** (プラス) アイコンをクリックし、**Domain Profile** ドロップダウンリストから、対象とする Cisco ACI Virtual Edge VMM ドメインを選択します。
- **Switching Mode** ドロップダウンリストリストから、**AVE** を選択します。
- **Encap Mode** ドロップダウンリストから **VXLAN** または **Auto** を選択します。

  Auto を選択したら、Cisco ACI Virtual Edge VMM ドメインのカプセル化モードが VXLAN になっていることを確認します。
- (オプション) セットアップに適した他の設定オプションを選択します。

g) [Update] をクリックし、[Finish] をクリックします。

次のタスク

統計情報を選択して表示すると、エンドポイントが関与する問題の診断に役立ちます。このガイドの [Tenants] タブの下で、Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を選択する （71 ページ） と [Tenents] タブの下で Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を表示する （71 ページ） を参照してください。

[Tenants] タブの下で、Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を選択する

Cisco ACI Virtual Edge で EPG 内分離を設定した場合、拒否された接続数、受信パケット数、送信済みマルチキャストパケット数などのエンドポイントの統計情報を表示する前に、それらを選択する必要があります。その後、統計情報を表示できます。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 **[Tenants]** > ***[tenant]*** の順に選択します。

ステップ 3 テナントのナビゲーション ウィンドウで、**Application Profiles**、***profile***、および **Application EPGs** フォルダを展開し、表示するエンドポイント統計情報を含む EPG を選択します。

ステップ 4 EPG の [Properties] 作業ペインで、[Operational] タブをクリックして EPG 内のエンドポイントを表示します。

ステップ 5 エンドポイントをダブルクリックします。

ステップ 6 エンドポイントの [Properties] ダイアログボックスで、[Stats] タブをクリックし、チェック アイコンをクリックします。

ステップ 7 **Select Stats** ダイアログボックスの **Available** ペインで、エンドポイントについて表示する統計情報を選択し、右向き矢印を使用してそれらの情報を **Selected** ペインに移動します。

ステップ 8 [送信（Submit）] をクリックします。

[Tenents] タブの下で Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を表示する

Cisco ACI Virtual Edge で EPG 内分離を設定していた場合には、エンドポイントの統計情報を選択すると、確認することができるようになります。

始める前に

分離エンドポイントについて表示する統計情報を選択しておく必要があります。手順については、このガイドの [Tenants] タブの下で、Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を選択する （71 ページ） を参照してください。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 **[Tenants]** > ***[tenant]*** の順に選択します。

ステップ 3 テナントのナビゲーション ウィンドウで、**Application Profiles**、***profile***、および **Application EPGs** フォルダを展開し、表示の必要な統計情報があるエンドポイントを含んでいる EPG を選択します。

ステップ 4 EPG の [Properties] 作業ペインで、[Operational] タブをクリックして EPG 内のエンドポイントを表示します。

ステップ 5 統計情報を表示するエンドポイントをダブルクリックします。

ステップ 6 エンドポイントの **Properties** 作業ウィンドウで、**Stats** タブをクリックします。

作業ウィンドウに、先ほど選択した統計情報が表示されます。作業ウィンドウの左上で、テーブル ビュー アイコンやチャート ビュー アイコンをクリックして、ビューを変更できます。

[Virtual Networking] タブの下で、Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を選択する

Cisco ACI Virtual Edge で EPG 内分離を設定した場合、拒否された接続数、受信パケット数、送信済みマルチキャストパケット数などのエンドポイントの統計情報を表示する前に、それらを選択する必要があります。その後、統計情報を表示できます。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 **Virtual Networking** > **Inventory** > **VMM Domains** > **VMware** > ***VMM domain*** > **Controllers** > ***controller instance name*** > ***DVS-VMM name*** > **Portgroups** > ***EPG name*** > ***Learned Point MAC address (node)*** > を選択します。

ステップ 3 [Stats] タブをクリックします。

ステップ 4 チェック マークが付いたタブをクリックします。

ステップ 5 **Select Stats** ダイアログボックスで、表示する統計情報を **Available**ペインでクリックし、右向き矢印をクリックして、それらを **Selected** ペインに移動します。

ステップ 6 (オプション)サンプリング間隔を選択します。

ステップ 7 [送信（Submit）] をクリックします。

[Virtual Networking] タブで Cisco ACI Virtual Edge の分離エンドポイント統計情報を表示する

Cisco ACI Virtual Edge で EPG 内分離を設定していた場合には、エンドポイントの統計情報を選択すると、確認することができるようになります。

始める前に

分離エンドポイントについて表示する統計情報を選択しておく必要があります。手順については、このガイドの [Tenants] タブの下で、Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を選択する （71 ページ） を参照してください。

手順

ステップ 1 Cisco APIC にログインします。

ステップ 2 **Virtual Networking** > **Inventory** > **VMM Domains** > **VMware** > ***VMM name*** > **Controllers** > **controller instance name** > ***DVS-VMM name*** > **Portgroups** > ***EPG name*** > ***Learned Point MAC address (node)*** を選択します。

ステップ 3 [Stats] タブをクリックします。

中央のウィンドウに、先ほど選択した統計情報を表示します。作業ウィンドウの左上で、テーブル ビュー アイコンやチャート ビュー アイコンをクリックして、ビューを変更できます。

NX-OS スタイルの CLI を使用した Cisco ACI Virtual Edge の EPG 内分離の設定

始める前に

VXLAN に関連する設定に存在するかどうかを確認します Cisco ACI Virtual Edge VMM ドメイン、特に、 Cisco ACI Virtual Edge ファブリック全体のマルチキャスト アドレスと (EPG ごとに 1 つ) のマルチキャスト アドレスのプール。

手順

CLI で、EPG 内分離 EPG を作成します。

例：

```
# Command: show running-config tenant Tenant2 application AP-1 epg EPG-61
  tenant Tenant2
    application AP-1
      epg EPG-61
        bridge-domain member BD-61
        vmware-domain member D-AVE-SITE-2-3
          switching-mode AVE
          encap-mode vxlan
          exit
        isolation enforce            # This enables EPG into isolation mode.
        exit
      exit
    exit
```

次のタスク

統計情報を選択して表示すると、エンドポイントが関与する問題の診断に役立ちます。このガイドの [Tenants] タブの下で、Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を選択する （71 ページ） と [Tenents] タブの下で Cisco ACI Virtual Edge の分離されたエンドポイントの統計情報を表示する （71 ページ） を参照してください。

トラブルシューティング

エンドポイント接続のトラブルシューティング

手順

ステップ 1 各エンドポイントの動作ステータスを調べます。

動作ステータスにはエンドポイントのエラーや設定ミスが示されます。詳細は、

エンドポイント ステータスの検査 （75 ページ） を

ステップ 2 トンネル インターフェイスのステータスを調べます。

動作ステータスにはトンネルのエラーや設定ミスが示されます。「トンネルインターフェイス ステータスの検査 （76 ページ）」を参照してください。

ステップ 3 エンドポイント グループ（EPG）間で traceroute を実行します。

トレースルートでは、スパイン ノードなどの中間ノード、およびエンドポイント間の問題が明らかになります。「エンドポイント 間での traceroute の実行 （76 ページ）」を参照してください。

ステップ 4 エンドポイントのアトミック カウンタを構成します。

アトミック カウンタは、発信元エンドポイントがパケットを送信しているか、また送信先エンドポイントがパケットを受信しているか、そして受信されたパケット数が送信されたパケット数に等しいかどうかを確認します。「アトミック カウンタの構成 （77 ページ）」を参照してください。

ステップ 5 各 EPG でコントラクトを調べます。

各 EPG でのコントラクトを調べ、EPG 間でのトラフィックの流れが許可されているかを確認します。テストとして一時的にコントラクトを開き、無制限のトラフィックを許可することができます。

ステップ 6 発信元パケットをモニタリング ノードに転送するようにスパン ポリシーを構成します。

モニタリング ノードのパケット アナライザが誤ったアドレスやプロトコルなどのパケットの問題を示します。「Cisco APIC GUI を使用したテナント SPAN セッションの設定 （78 ページ）」を参照してください。

エンドポイント ステータスの検査

手順

ステップ 1 メニュー バーで、[Tenants] をクリックします。

ステップ 2 サブメニュー バーで、送信元エンドポイントを含むテナントをクリックします。

ステップ 3 **[ナビゲーション（Navigation）]** ペインでテナントを拡張し、**[アプリケーション プロファイル（Application Profiles）]** を拡張して、エンドポイントが含まれるアプリケーション プロファイルを拡張します。

ステップ 4 **[アプリケーション EPG（Application EPGs）]** を展開し、確認する EPG をクリックします。

ステップ 5 **[作業（Work）]** ペインで、**[エンドポイント（Endpoint）]** テーブルのエンドポイントのリストから送信元エンドポイントをダブルクリックし、**[クライアント エンド ポイント（Client End Point）]** ダイアログボックスを開きます。

ステップ 6 **[クライアント エンド ポイント（Client End Point）]** ダイアログボックスで、エンドポイントのプロパティを確認し、**[操作性（Operational）]** タブをクリックします。

ステップ 7 **[操作性（Operational）]** タブで、健全性、ステータスおよび障害情報を表示します。

[ステータス（Status）] テーブルで、変更、イベント、またはエラーなどのエントリがある項目をクリックします。

ステップ 8 **[クライアント エンド ポイント（Client End Point）]** ダイアログボックスを閉じます。

ステップ 9 **[エンドポイント（Endpoint）]** テーブルでエンドポイントの **[インターフェイス（Interface）]** エントリを表示し、ノードとトンネル ID をメモに記録します。

ステップ 10 送信先エンドポイントでこの手順を繰り返します。

（注）
ファブリック内の 2 つのリーフ スイッチの背後に展開された 2 つのマイクロセグメント EPG の IP アドレス間で、双方向のトラフィックが中断されることがあります。これは、マイクロセグメント EPG からベース EPG への構成変更により、IP アドレスが移行しているときに発生する可能性があります。または逆に、双方向トラフィックの実行中に 2 つの異なるリーフ スイッチで同時に発生する可能性があります。この場合、各リモートエンドポイントのポリシータグは引き続き以前の EPG を指します。

回避策：スイッチのリモート エンドポイントを手動でクリアするか、リモート エンドポイントが期限切れになるのを待ちます。エンドポイントをクリアするには、各スイッチの CLI にログオンし、適切なオプションを指定して **clear system internal epm endpoint** コマンドを入力します。たとえば、エンドポイントが IP アドレスに基づいている場合は、**clear system internal**

epm endpoint key vrf *vrf_name***{ip | ipv6}** *ip-address* と入力します。その後、エンドポイントは正しいポリシー タグで再学習されます。

トンネル インターフェイス ステータスの検査

この手順では、トンネル インターフェイスの動作ステータスを調べる方法を示します。

手順

ステップ 1 メニュー バーで、[Fabric] をクリックします。

ステップ 2 サブメニュー バーで、[Inventory] をクリックします。

ステップ 3 **[ナビゲーション（Navigation）]** ペインでポッドを拡張し、発信元エンドポイント インターフェイスのノード ID を拡張します。

ステップ 4 ノードの下で**[インターフェイス（Interfaces）]** を拡張し、**[トンネル インターフェイス（Tunnel Interfaces）]** を拡張して、発信元エンドポイント インターフェイス のトンネル ID をクリックします。

ステップ 5 **[作業（Work）]** ペインで、トンネル インターフェイスのプロパティを確認し、**[操作（Operational）]** タブをクリックします。

ステップ 6 **[操作性（Operational）]** タブで、健全性、ステータスおよび障害情報を表示します。

[ステータス（Status）] テーブルで、変更、イベント、またはエラーなどのエントリがある項目をクリックします。

ステップ 7 送信先エンドポイント インターフェイスでこの手順を繰り返します。

エンドポイント 間での traceroute の実行

手順

ステップ 1 メニュー バーで、[Tenants] をクリックします。

ステップ 2 サブメニュー バーで、送信元エンドポイントを含むテナントをクリックします。

ステップ 3 **[ナビゲーション]** ペインでテナントを展開し、**[ポリシー]** > **[トラブルシューティング]** を展開します。

ステップ 4 [Troubleshoot] で次のトレースルート ポリシーのいずれかを右クリックします。

- [Endpoint-to-Endpoint Traceroute Policies] を右クリックして [Create Endpoint-to-Endpoint Traceroute Policy] を選択する

- [Endpoint-to-External-IP Traceroute Policies] を右クリックして [Create Endpoint-to-External-IP Traceroute Policy] を選択する
- [External-IP-to-Endpoint Traceroute Policies] を右クリックして [Create External-IP-to-Endpoint Traceroute Policy] を選択する
- [External-IP-to-External-IP Traceroute Policies] を右クリックして [Create External-IP-to-External-IP Traceroute Policy] を選択する

ステップ 5 ダイアログボックスのフィールドに適切な値を入力し、[Submit] をクリックします。

（注）
フィールドの説明については、ダイアログボックスの右上隅にあるヘルプ アイコン（[?]）をクリックしてください。

ステップ 6 **[Navigation]** ペインまたは **[Traceroute Policies]** テーブルで、traceroute ポリシーをクリックします。

トレースルート ポリシーが [Work] ペインに表示されます。

ステップ 7 [Work] ペインで [Operational] タブをクリックし、[Source Endpoints] タブ、[Results] タブの順にクリックします。

ステップ 8 **[Traceroute Results]** テーブルで、追跡に使用された単数または複数のパスを確認します。

（注）
- 複数のパスが、送信元ノードから宛先ノードへの移動に使用されている場合があります。
- **[Name]** 列など、1 つまたは複数の列の幅を広げると確認しやすくなります。

アトミック カウンタの構成

手順

ステップ 1 メニュー バーで、[Tenants] をクリックします。

ステップ 2 サブメニュー バーで、必要なテナントをクリックします。

ステップ 3 **Navigation** ウィンドウで、テナントを展開し、**Policies** を展開し、それから **Troubleshoot** を展開します。

ステップ 4 **Troubleshoot** の下で、**Atomic Counter Policy** を展開し、トラフィック トポロジを選択します。

エンドポイントの組み合わせ、エンドポイント グループ、外部インターフェイスおよび IP アドレス間のトラフィックを測定できます。

ステップ 5 必要なトポロジを右クリックして、**Add** *topology* **Policy** を選択し、**Add Policy** ダイアログボックスを開きます。

ステップ 6 [Add Policy] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドにポリシーの名前を入力します。

b) トラフィックの送信元の識別情報を選択するか、入力します。

必要な識別情報のソース（エンドポイント、エンドポイントのグループ、外部インターフェイス、または IP アドレス）によって異なります。

c) トラフィックの宛先の識別情報を選択するか、入力します。

d) （任意）（任意）[Filters] テーブルで + アイコンをクリックし、カウントするトラフィックのフィルタリングを指定します。

表示される [Create Atomic Counter Filter] ダイアログボックスで、IP プロトコル番号（たとえば TCP=6）によるフィルタリング、および送信元と宛先の IP ポート番号によるフィルタリングを指定できます。

e) [Submit] をクリックし、アトミック カウンタ ポリシーを保存します。

ステップ 7 [Navigation] ペインで、選択したトポロジの下の新しいアトミック カウンタ ポリシーを選択します。

ポリシー設定が [Work] ペインに表示されます。

ステップ 8 [Work] ペインで [Operational] タブをクリックし、[Traffic] サブタブをクリックして、アトミック カウンタの統計情報を表示します。

Cisco APIC GUI を使用したテナント SPAN セッションの設定

SPAN は、スイッチまたはテナントで設定できます。このセクションでは、Cisco APIC GUI を使用して、複製された送信元パケットをリモート トラフィック アナライザに転送するようにテナントの SPAN ポリシーを設定する方法について説明します。設定手順では、1 つ以上の GUI ダイアログ ボックスのフィールドに値を入力する必要があります。フィールドを理解し、有効な値を決定するには、ダイアログ ボックスの右上隅にあるヘルプアイコン（**?**）をクリックしてヘルプ ファイルを表示します。

手順

ステップ 1 メニュー バーで、[Tenants] をクリックします。

ステップ 2 サブメニュー バーで、送信元エンドポイントを含むテナントをクリックします。

ステップ 3 **[ナビゲーション（Navigation）]** ペインでテナントを展開し、**[ポリシー（Policies）]** > **[トラブルシューティング（Troubleshooting）]** > を展開して、**[SPAN]** を展開します。

[SPAN] に表示される 2 つのノード：**[SPAN 宛先グループ（SPAN Destination Groups）]** と **[SPAN 送信元グループ（SPAN Source Groups）]**。

ステップ 4 **[ナビゲーション（Navigation）]**の下で **[SPAN 送信元グループ（SPAN Source Groups）]** を右クリックし、**[SPAN 送信元グループの作成（Create SPAN Source Group）]** を選択します。**[Create SPAN Source Group]** ダイアログが表示されます。

ステップ 5 **[SPAN 送信元グループの作成（Create SPAN Source Group）]** ダイアログ ボックスの必須フィールドに適切な値を入力します。

ステップ 6 **[送信元の作成（Create Sources）]** テーブルを展開し、**[SPAN 送信元の作成]** ダイアログ ボックスを開きます。

ステップ 7 **[SPAN 送信元の作成（Create SPAN Source）]** ダイアログ ボックスのフィールドに適切な値を入力します。

ステップ 8 SPAN送信元の作成が完了したら、**[OK]** をクリックします。

[SPAN 送信元グループの作成（Create VRF）] ダイアログ ボックスに戻ります。

ステップ 9 **[リモート場所の作成（Create Remote Location）]** ダイアログのフィールドに値を入力したら、**[送信（Submit）]** をクリックします。

次のタスク

SPAN 送信先のトラフィック アナライザを使用して、SPAN 送信元 EPGからのデータ パケットを観察し、パケット形式、アドレス、プロトコルおよびその他の情報を確認できます。

IP bエース EPG 構成の確認

作成できるエンドポイント グループ（EPG）には、アプリケーション EPG と IP ベースの EPG の 2 種類があります。IP ベースの EPG は、マイクロセグメント EPG であるという点で通常のアプリケーション EPG とは異なります。この章では、GUI またはスイッチ コマンドを使用して、IP ベースの EPG 構成が IP ベースとして正しく分類されていることを確認する方法について説明します。

この章は、次の項で構成されています。

GUI を使用した IP ベースの EPG 構成の確認

この手順では、GUI および Visore ツールを使用して IP ベースの EPG が正しく構成されていることを確認する方法について説明します。

手順

ステップ 1 作成した IP ベースの EPG が GUI の **uSeg EPGs** フォルダーの下に表示されていることを確認します（次のスクリーン キャプチャを参照）。
REST API を使用して作成された「IP」という名前の uSeg EPG の下にリストされている 1 つの IP ベースの EPG があることに注意してください。

ステップ 2 各 EPG IP（IP ベースの EPG）の EPG - IP プロパティ画面（右側のウィンドウ ペイン）で情報が正しいことを確認します。
画面の下部に表示される IP ベースの EPG と IP アドレスのリストに注意してください。

ステップ 3 Web ブラウザから、APIC の IP アドレスに続けて「/visore.html」を入力します。Visore は、EPG など、システム内のすべてのオブジェクトを表示できるツールです。Visore を使用して、IP ベースの EPG が正しく構成されていることを確認できます。Visore の詳細については、『アプリケーション ポリシー インフラストラクチャ コントローラ *Visore* ツールの紹介』を参照してください。

ステップ 4 ユーザー名とパスワードを入力し、**[ログイン（Login）]** をクリックします。

ステップ 5 **クラスまたは DN** の隣のフィールド（たとえば、「fvAEPg」）にクラスの名前を入力して、GUI で確認した IP ベースの EPG のクエリを実行します。

（注）
これは、APIC の観点からのビューです。上記の「示されるオブジェクトの総数（Total objects shown）」が「3」であることがわかります。これは、スイッチにダウンロードされた 3 つの EPG があることを意味します。以前 GUI に「IP」としてリストされていた IP ベースの EPG が、「dn」の隣に表示されていることがわかります。また、「isAttrBasedEPg」の横に「yes」と表示されていることにも注意してください。これは、これが IP ベースの EPG として適切に構成されたことを意味します。アプリケーション EPG と IP ベースの EPG の両方を含む、すべてのオブジェクトが Visore を使用して正常に設定されていることを確認できます。

ステップ 6 スイッチ側から見た図です。スイッチで、fvEpP クラスのクエリを実行して EPG を表示し、「crtrnEnabled」属性を確認できます。IP ベースの EPG の場合は「yes」に設定されます。
この EPG の下で、EPG の子が IP アドレスとともに表示されていることを確認して、適切な構成を確保します。構成された IP アドレスごとに、スイッチがトラフィックの分類に使用する 1 つのオブジェクト（「l3IpCktEp」という名前）があります。構成が完了すると、パケットが到着すると、スイッチはこれらのオブジェクトを使用して分類します。

ステップ 7 構成したすべてのエンドポイントと IP アドレスの pcTag が一致することを確認します。すべての EPG には pcTag があります。構成した IP アドレスと一致するすべてのエンドポイントは、この pcTag に分類されます。すべてのエンドポイントには、クラス クエリを実行できる IPアドレスがあります。トラブルシューティングを行うときは、これらのエンドポイント（サーバー）がこの IP ベースの EPG に正しく分類されているかどうかを確認する必要があります。（pcTags は IP ベースの EPG に一致する必要があります。）

スイッチ コマンドを使用した IP-EPG 構成の確認

この手順では、スイッチ コマンドを使用して IP-EPG (「IpCkt」)構成定を確認する方法について説明します。

手順

ステップ 1 リーフにログインします。

ステップ 2 /mit/sys ディレクトリに移動します。

ステップ 3 /mit/sys ディレクトリで、ctx（vrf コンテキスト ディレクトリ）を見つけます。

ステップ 4 VRF cts ディレクトリで、IpCkt が構成されている特定の BD ディレクトリに移動します。IpCkt が表示されます。

（注）
「IpCkt」と「IP-EPG」は、このドキュメントでは同じ意味で使用されます。

ステップ 5 ディレクトリに移動すると、「猫の概要」に IpCkt に関する情報が表示されます。

ステップ 6 サマリーの「operSt」に「サポートされていない」と表示されていないことを確認してください。

ステップ 7 IpCkt が構成されている BD に対応する VLAN ID を見つけます。

（注）
VLAN ID は、**show vlan internal bd-info** コマンドのいずれか、または **show system internal epm vlan all** コマンドで見つけることができます。

ステップ 8 BD の VLAN ID を見つけたら、**show system internal epm <vlan-id> detail** を発行します。ここで、特定の sclass で構成されたすべての IpCkts を表示できるはずです。（/mit/sys ディレクトリに表示されるものと一致する必要があります。）

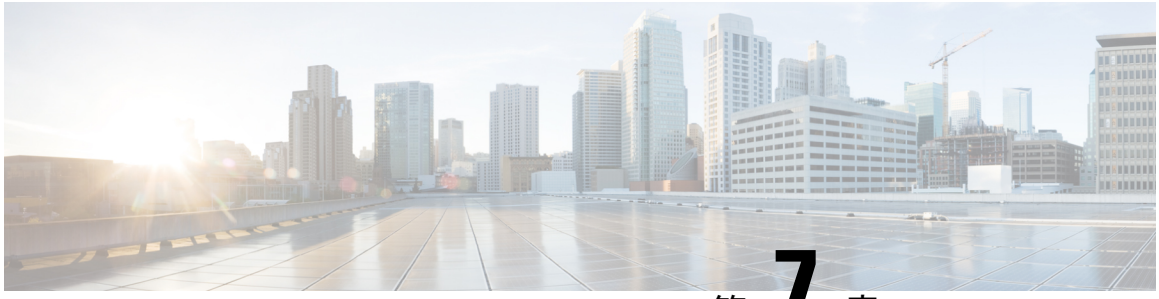
ステップ 9 vsh で実行した手順を vsh_lc に対して繰り返します。

ステップ 10 BD の IpCtk に一致する IP を使用して、**show system internal epm endp ip <a.b.c.d>** を介してトラフィックを送信します。学習した IP に「sclass」の IP フラグと特定の sclass 値があることを確認できます。

ステップ 11 vsh で実行した手順を vsh_lc に対して繰り返します。

この手順で使用するスイッチ トラブルシューティング コマンドのリスト:

```
Cd /mits/sys/ctx-vxlan…/bd-vxlan…
     - cat summary
Vsh -c “show system internal epm vlan all” or
Vsh -c “show vlan internal bd-info”
Vsh -c “show system internal epm vlan <vlan-id> detail”
Vsh -c “show system internal epm endp ip <a.b.c.d>"
Vsh_lc -c “show system internal epm vlan all” or
Vsh_lc -c “show vlan internal bd-info”
Vsh_lc -c “show system internal epm vlan <vlan-id> detail”
vsh_lc -c “show system internal epm endp ip <a.b.c.d>”
vsh_lc -c “show system internal epm epg”
```



第 7 章

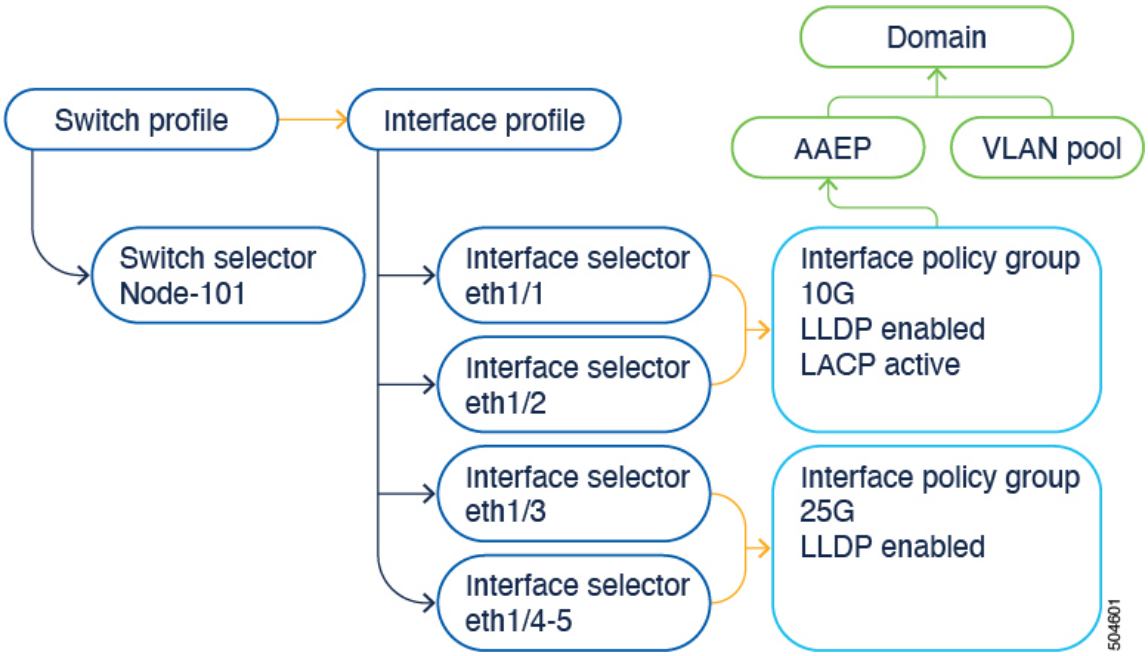
アクセス インターフェイス

- アクセス インターフェイスについて （83 ページ）
- 物理ポートの構成 （86 ページ）
- ポート チャネル （95 ページ）
- Cisco ACI の仮想ポート チャネル （114 ページ）
- リフレクティブ リレー (802.1Qbg) （130 ページ）
- FEX デバイスへのポート、PC、および vPC 接続の設定 （133 ページ）
- ポート プロファイルの設定 （139 ページ）
- インターフェイス構成の編集 （155 ページ）

アクセス インターフェイスについて

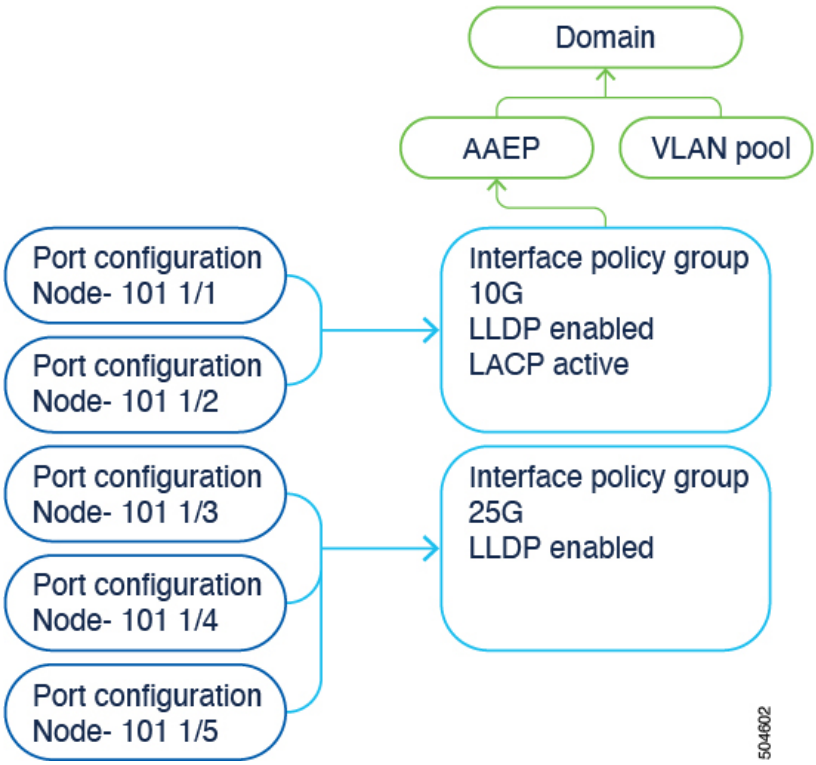
Cisco Application Centric Infrastructure（ACI）では、インターフェイス ポリシー グループ（インターフェイス速度やリンク層検出プロトコル（LLDP）などのインターフェイス ポリシーのグループ）をスイッチ ノード上のインターフェイスに関連付けることによって、インターフェイス構成を実行します。Cisco ACI は、4 つのオブジェクト（スイッチ プロファイル、スイッチ セレクタ、インターフェイス プロファイル、およびインターフェイス セレクタ）を使用して、特定のスイッチ ノード上の特定のインターフェイスを選択します。本書では、この動作モードを「プロファイ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 *16 :* 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 *17* : 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

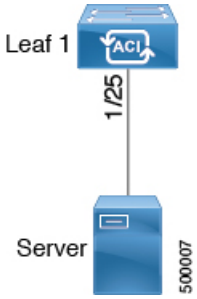
成オプションは、構成手順の数を 4 回から 1 回に減らすことで、構成ワークフローを簡素化します。

- **[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 *18 :* 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。

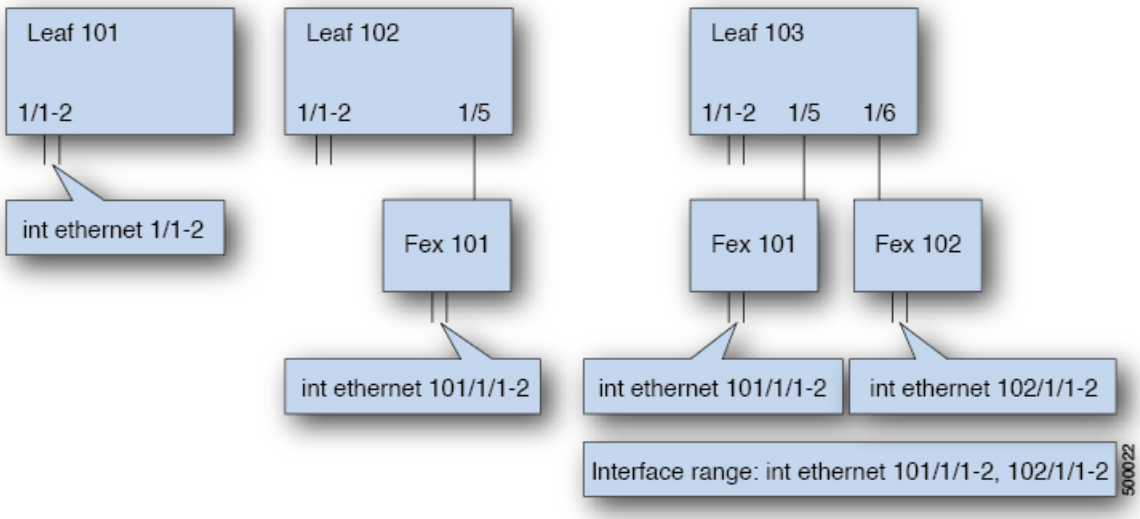
特定のインターフェイスのポリシー グループ名をクリックすると、802.1X 構成、アタッチ可能なエンティティ プロファイル、CDP 構成、LLDP 構成などのポリシー グループに関する情報が表示されます。

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 19 : Cisco ACI のリーフ ノード ポートと FEX ポートの例 （92 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 *19 : 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 *4 : 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。

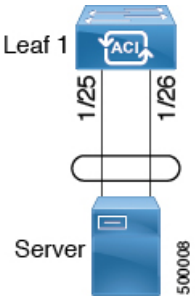
- Cisco Nexus 93128TX
- Cisco Nexus 9372PX
- Cisco Nexus 9372PX-E
- Cisco Nexus 9372TX
- Cisco Nexus 9372TX-E
- Cisco Nexus 9396PX
- Cisco Nexus 9396TX

（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 *20 :* 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。

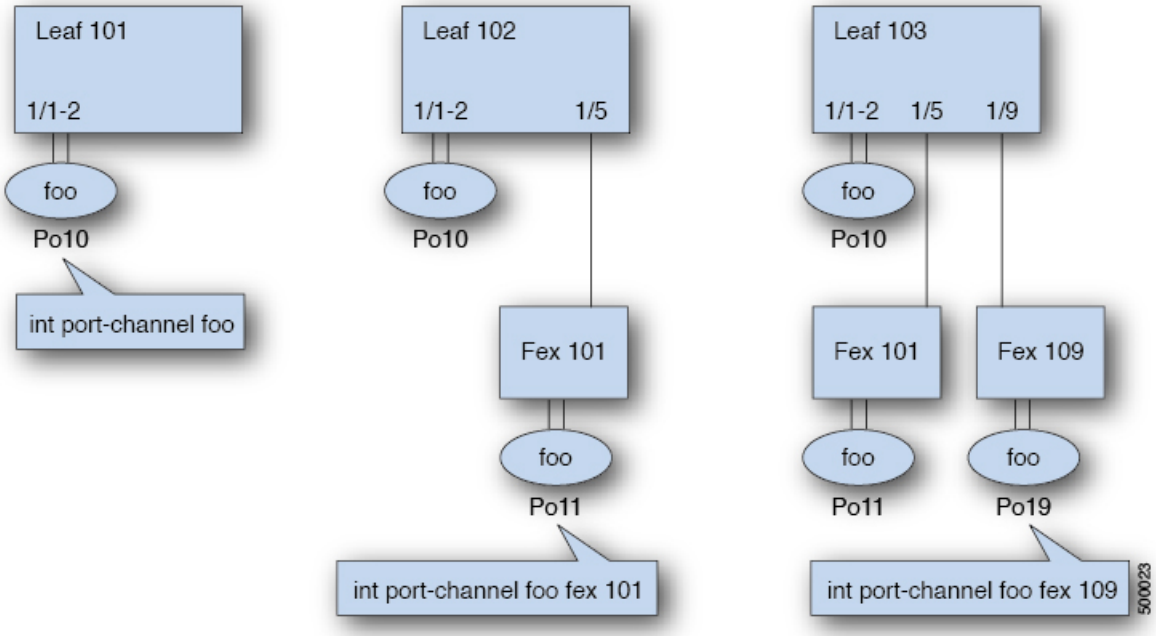
NX-OS CLI を使用したリーフ ノードおよび FEX デバイスのポートチャネルの設定

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 *21 :* 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 *5 : 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：

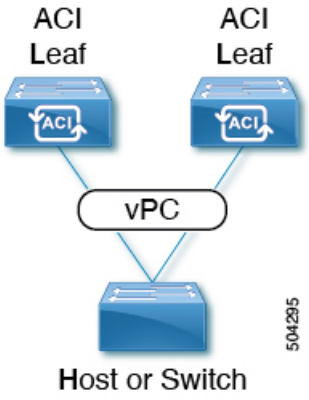
```
node# show dlb statistics
dlb statistics:
    Flowlet Hit          = 0
    Flowlet Create       = 156
    Flowlet Collision    = 0
    Flowlet DLB Rx pkts  = 3734297752
```

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 *22 : 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

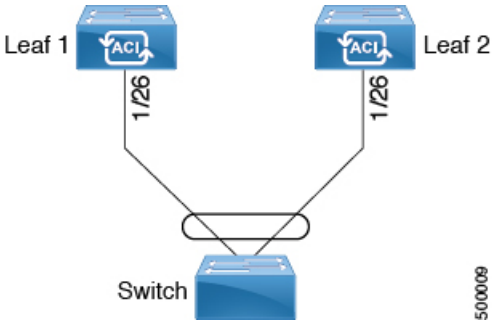
- ポート チャネルおよび仮想ポート チャネルは、LACP の有無にかかわらず構成できます。

  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 *23*：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 （114 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 （114 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。

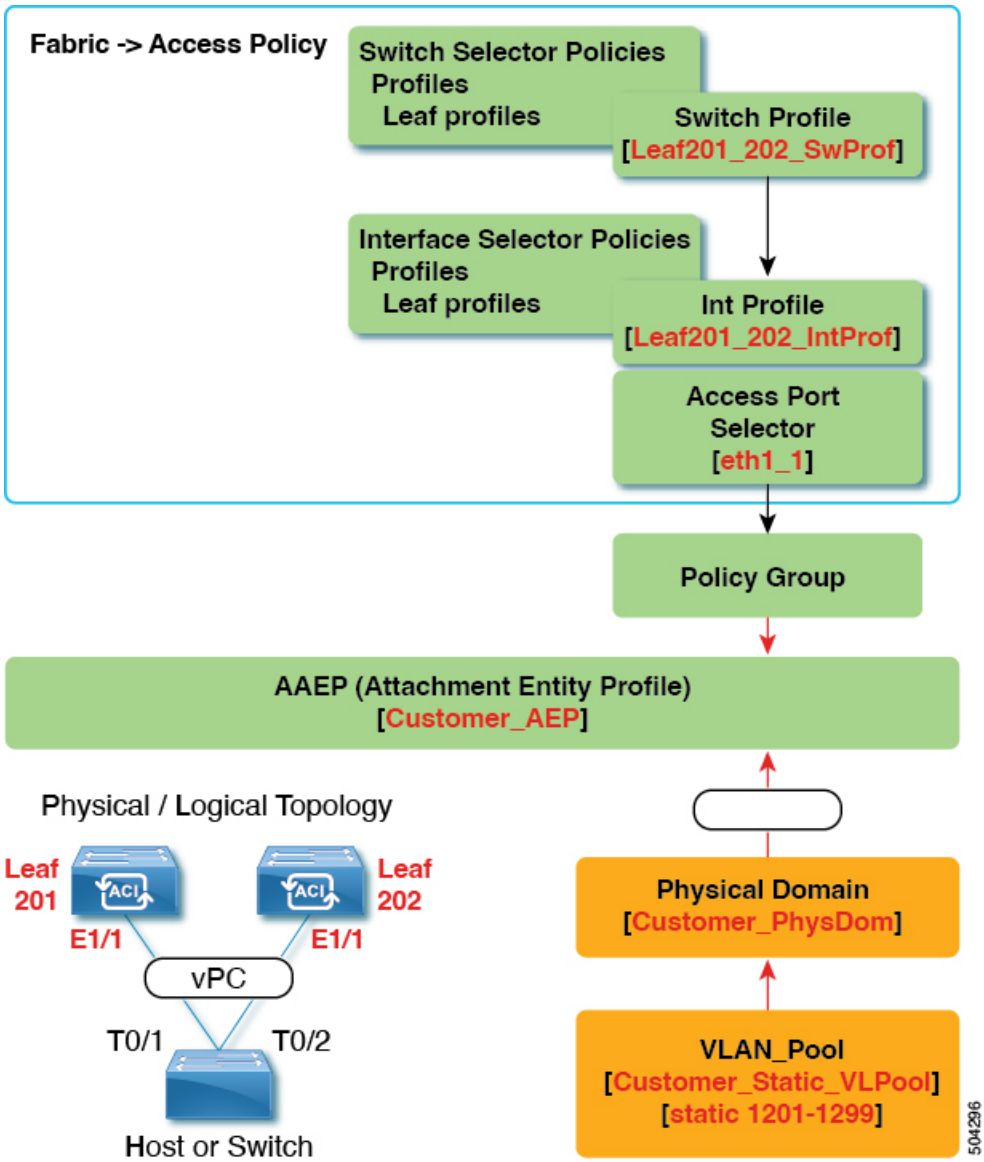
プロファイルとセレクタを使用したリーフ ノードおよび FEX デバイスでの仮想ポートチャネルの設定

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 *24*：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

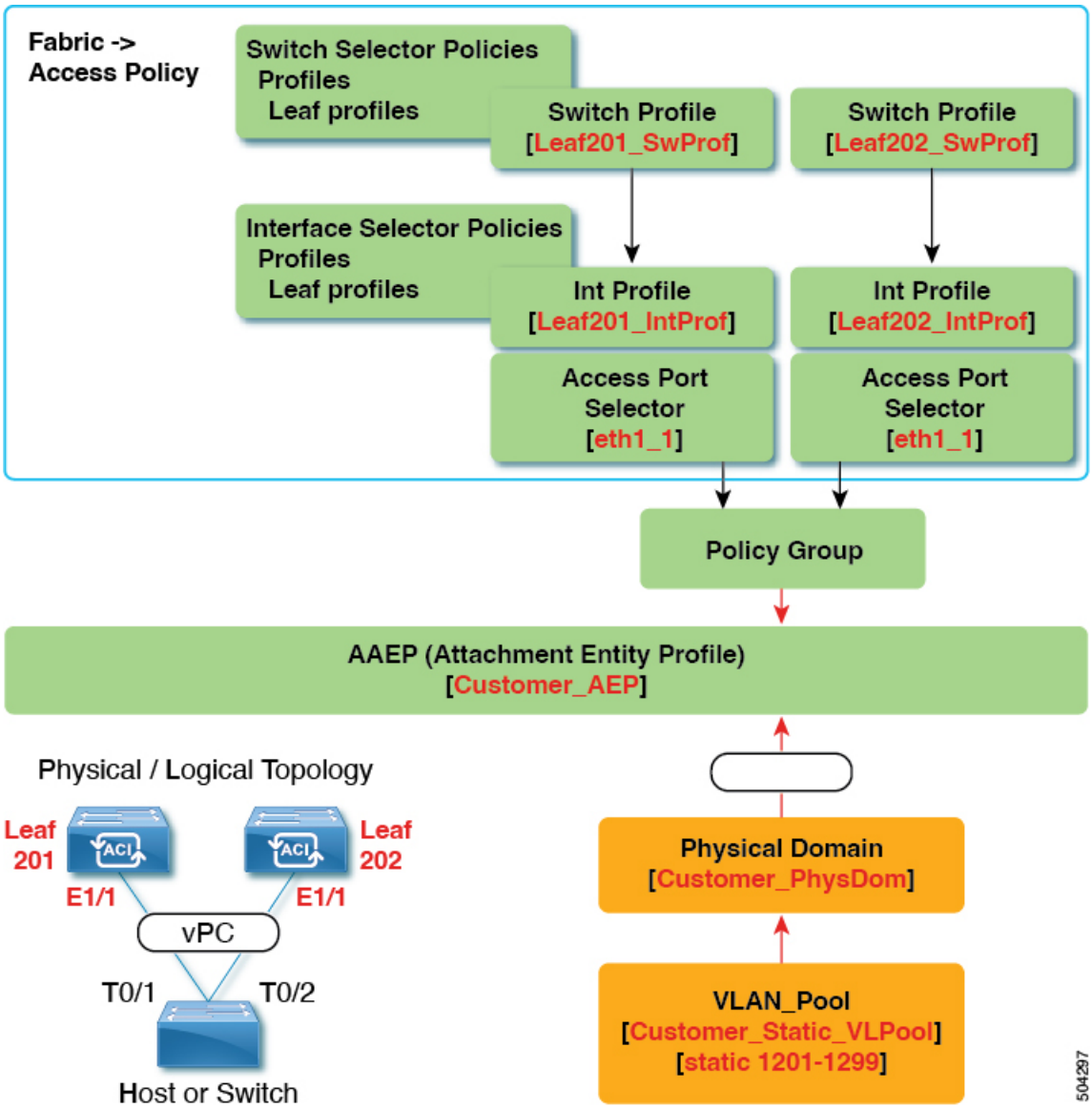
スイッチ/インターフェイス プロファイルを使用するための堅実なユース ケースになります。スイッチ、インターフェイス、アクセス ポート セレクタ、および vPC インターフェイス ポリシー グループを事前設定しておけば、最小限の労力で 48 のシャーシ タイプのサーバーを接続できるようにすることができます。

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 *25 :* 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

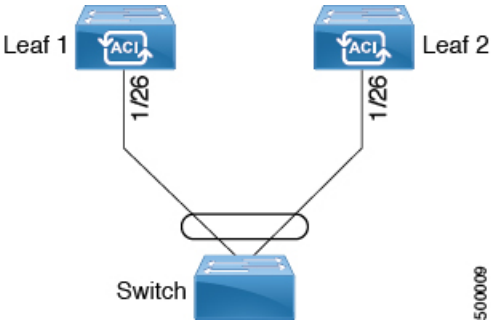
コンピューティング、サービス、または Cisco Application Policy Infrastructure Controller（APIC）などの混合ワークロードをサポートするリーフ スイッチがある場合は、この構成を使用しま

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 *26*：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 （114 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 （114 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 （86 ページ）
- ポート チャネル （95 ページ）
- Cisco ACI の仮想ポート チャネル （114 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。

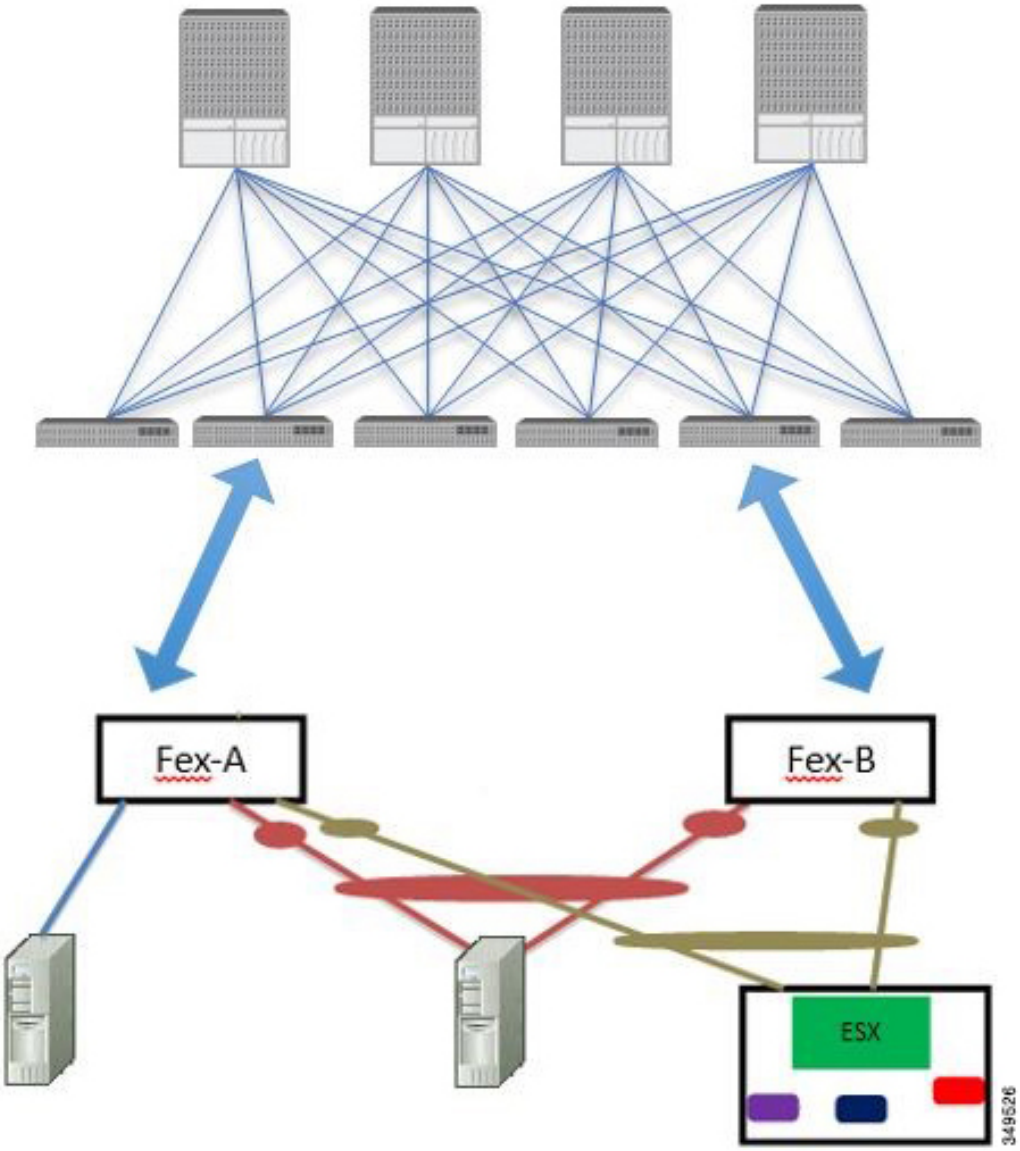
- リーフ スイッチ前面パネル ポートが EPG および VLAN を展開するように設定されていないと仮定して、最大 10,000 個のポート EPG が FEX を使用して展開することをサポートします。
- メンバーとして FEX ポートを含む各 FEX ポートまたは vPC では、各 VLAN で最大 20 個の EPG がサポートされます。
- FEX インターフェイスを備えた vPC は、ポート チャネル ポリシーで設定されたリンクの最小数と最大数を無視します。vPC は、リンク数が最小値を下回ったり、最大値を上回ったりしても、up 状態を維持します。
- 各 FEX LACP は、1 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 （114 ページ）を参照してください。

図 *27 :* 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。

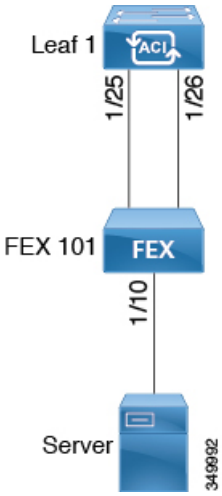
- FEX の背後にある VTEP および非 VTEP の両方のハイパーバイザ。
- ACI ファブリックに接続された 2 つの FEX に接続された仮想スイッチ（AVS や VDS など）（物理 FEX ポートに直接接続された vPC はサポートされません。vP Cはポート チャネルでのみサポートされます）。

（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 *28 :* 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 （145 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。

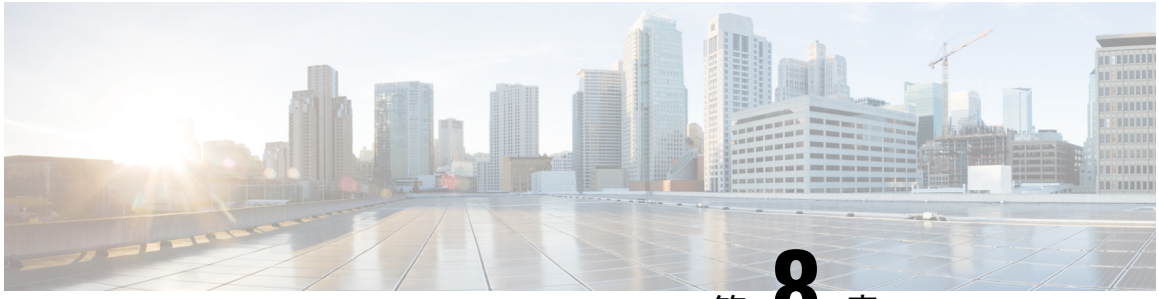
ステップ 2 ナビゲーション ペインで **[インターフェイスの構成（Interface Configuration）]** を選択します。

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。



第 8 章

FCoE 接続

この章は、次の内容で構成されています。

- 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 （157 ページ）
- Fibre Channel over Ethernet のガイドラインと制限事項 （160 ページ）
- Fibre Channel over Ethernet（FCoE）をサポートするハードウェア （160 ページ）
- APIC GUI を使用した FCoE の設定 （161 ページ）
- NX-OS スタイルの CLI を使用した FCoE の設定 （181 ページ）
- vPC による SAN ブート （193 ページ）

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。

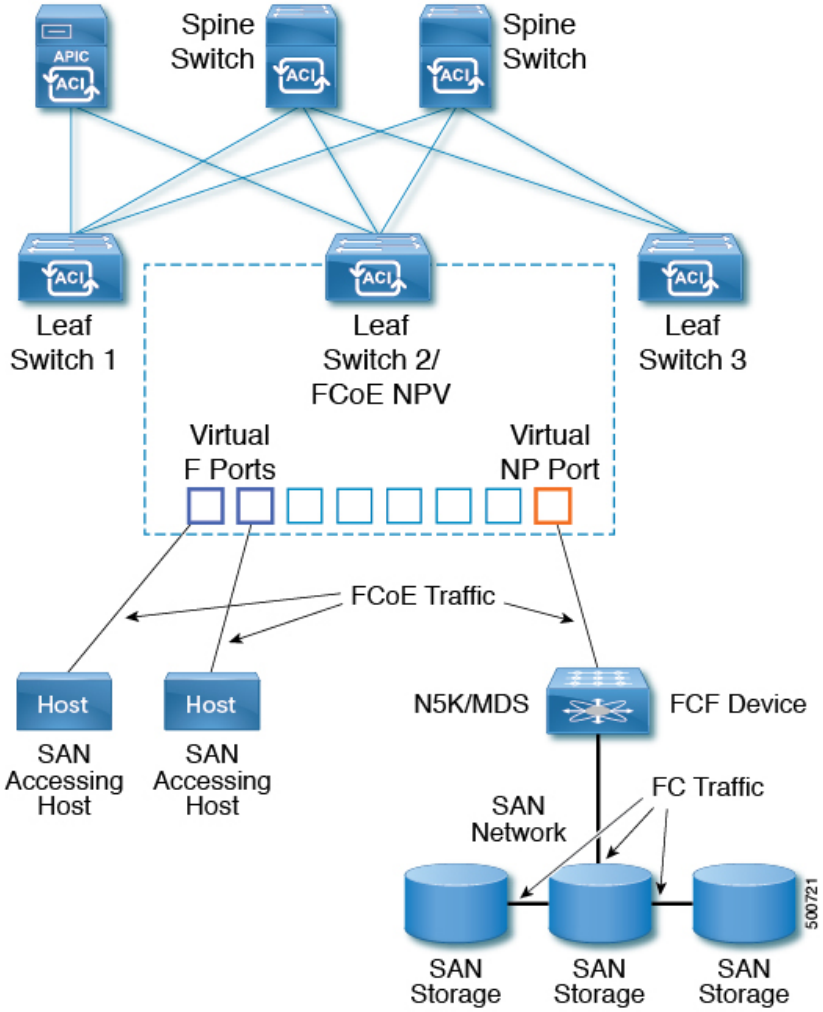
Cisco ACI ファブリックで FCoE プロトコルのサポートを標準実装することにより、イーサネットベースの Cisco ACI ファブリックに配置されているホストが、ファイバ チャネル ネットワークに配置されている SAN ストレージデバイスと通信できます。ホストは、Cisco ACI リーフスイッチに展開された仮想 F ポートを介して接続しています。SAN ストレージ デバイスとファイバ チャネル ネットワークは、ファイバチャネルフォワーディング（FCF）ブリッジおよび仮想 NP ポートを介して Cisco ACIファブリックに接続されます。このポートは、仮想 F ポートと同じ Cisco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

（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 *29 : 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。

Fibre Channel over Ethernet のガイドラインと制限事項

FCoE に使用する VLAN の vlanScope を `Global` に設定する必要があります。vlanScope を `portLocal` に設定することは、FCoE ではサポートされていません。値は、レイヤ 2 インターフェイス ポリシー（l2IfPol）を使用して設定されます。

Fibre Channel over Ethernet（FCoE）をサポートするハードウェア

FCoE は、次のスイッチでサポートされます。

- N9K-C93180LC-EX

  40 ギガビットイーサネット（GE）ポートが FCoE F または NP ポートとして有効になっている場合、40GE ポートブレークアウトを有効にすることはできません。FCoE は、ブレークアウト ポートではサポートされません。

- N9K-C93108TC-FX
- N9K-C93108TC-EX（FCoE NPVのみ）
- N9K-C93180YC-EX
- N9K-C93180LC-EX

  FEX ポートでの FCoE がサポートされます。

- N9K-C93180YC-FX

  サポート対象は、10/25G ポート（1〜48）、40G ポート（1/49〜54）、4x10G ブレークアウト ポート（1/49〜54）、および FEX ポート上の FCoE です。

FCoE は、次の Nexus FEX デバイスでサポートされます。

- 10 ギガ-ビット C2348UPQ N2K
- 10 ギガ-ビット C2348TQ N2K
- N2K-C2232PP-10GE
- N2K-B22DELL-P
- N2K-B22HP-P
- N2K-B22IBM-P
- N2K B22DELL P FI

APIC GUI を使用した FCoE の設定

FCoE GUI の設定

FCoE ポリシー、プロファイル、およびドメインの設定

[Fabric Access Policies] タブで APIC GUI を使用すれば、ポリシー、ポリシー グループ、およびプロファイルを設定して、ACI リーフ スイッチ上の F および NP ポートをサポートする FCoE のカスタマイズされ、スケールアウトした展開と割り当てを行うことが可能になります。次に、APIC の [Tenant] タブで、では、これらのポートへの EPG アクセスを設定できます。

ポリシーおよびポリシー グループ

FCoE のサポートのために作成または設定する APIC ポリシーとポリシー グループには、次のものが含まれます:

アクセス スイッチ ポリシー グループ

ACI リーフ スイッチを通して FCoE トラフィックをサポートする、スイッチ レベルのポリシーの組み合わせです。

このポリシー グループをリーフ プロファイルと関連付けて、指定された ACI リーフ スイッチでの FCoE サポートを有効にすることができます。

このポリシー グループは、次のポリシーで構成されています:

- **ファイバ チャネル SAN ポリシー**

  NPV リーフが使用する、EDTOV、RATOV、および MAC アドレス プレフィックス (FC マップとも呼ばれる) の値を指定します。

- **ファイバ チャネル ノード ポリシー**

  このポリシーグループに関連付けられる FCoE トラフィックに適用される、ロード バランス オプションと FIP キープ アライブ間隔を指定します。

インターフェイス ポリシー グループ

ACI リーフ スイッチのインターフェイスを通して FCoE トラフィックをサポートする、インターフェイス レベルのポリシーの組み合わせです。

このポリシー グループを FCoE のサポート的インターフェイス プロファイルと関連付けて、指定したインターフェイスでの FCoE サポートを有効にすることができます。

2 つのインターフェイス ポリシー グループを設定できます。F ポートの 1 つのポリシー グループと、 NP ポートの 1 つのポリシー グループです。

インターフェイスポリシーグループの以下のポリシーは、FCoEの有効化およびトラフィックに適用されます:

- **優先順位フロー制御ポリシー**

  このポリシー グループが適用されているインターフェイスの優先順位フロー制御(PFC)の状態を指定します。

  このポリシーは、どのような状況で QoS レベルの優先順位フロー制御が FCoE トラフィックに適用されるかを指定します。

- **Fibre Channel Interface Policy**

  このポリシー グループが適用されているインターフェイスが F ポートまたは NP ポートとして設定されるかどうかを指定します。

- **低速ドレイン ポリシー**

  ACI ファブリックでトラフィックの輻輳の原因となる FCoE パケットを処理するためのポリシーを指定します。

グローバル ポリシー

設定により、ACI ファブリックの FCoE トラフィックのパフォーマンス特性に影響を及ぼす APIC グローバル ポリシーです。

グローバル **QOS クラス ポリシー**（**Level1**、**Level2**、**Level4**、**Level5**、または**Level6** 接続に対応するもの）には、ACI ファブリック上の FCoE トラフィックに影響する次の設定が含まれます。

- **[PFC Admin State] は Auto に設定することが必要**

  FCoE トラフィックのこのレベルで優先順位フロー制御を有効にするかどうかを指定します (デフォルト値は false です)。

- **No Drop COS**

  特定のサービス クラス (CoS) レベルで指定された FCoE トラフィックのこのレベルに対し、no-drop ポリシーを有効にするかどうかを指定します。

  注: PFC および FCoE ノードロップに対して有効にされている QoS レベルは、CNA 上の PFC に対して有効にされている優先順位グループ ID と一致している必要があります。

  注: ノードロップおよび PFC に対して有効にできるのは、ただ 1 つの QoS レベルです。そして同じ QoS レベルが FCoE Epg に関連付けられている必要があります。

- QoS クラス — 優先順位フロー制御は、CoS レベルがファブリックに対してグローバルに有効にされていること、そしてFCoE トラフィックを生成するアプリケーションのプロファイルに割り当てられていることを必要とします。

  CoS保存も有効にする必要があります。**[ファブリック (Fabric)]** > **[アクセス ポリシー (Access Policies)]** > **[ポリシー (Policies)]** > **[グローバル (Global)]** > **[QoS クラス (QoS Class)]**荷移動して、**[COS Dot1P Preserve を保存 (Preserve COS Dot1p Preserve)]** を有効にします

（注） 一部のレガシー CNA も、**レベル 2** グローバル QoS ポリシーが、**ノードロップ** PFC、FCoE (Fibre Channel over Ethernet) QoS ポリシーで使用されていることを必要とする場合があります。使用しているコンバージドネットワークアダプタ （CNA） がファブリックにロギングしておらず、CNA から FCoE Initiation Protocol (FIP) フレームが送信されていないことがわかった場合には、 **レベル 2** を FCoE QoSポリシーとして有効にしてみてください。**Level2** ポリシーは、使用中の FCoE EPG にアタッチする必要があり、PFC no-drop に対して 1 つの QoS レベルのみを有効にできます。

プロファイル

FCoE をサポートするために作成または設定ができる APIC プロファイルとしては、次のものがあります:

リーフ プロファイル

FCoE トラフィックのサポートが構成される、ACI ファブリック リーフ スイッチを指定します。

アクセス スイッチ ポリシー グループに含まれるポリシーの組み合わせは、このプロファイルに含まれるリーフ スイッチに適用できます。

インターフェイス プロファイル

F ポートまたは NP ポートが展開される一連のインターフェイスを指定します。

少なくとも 2 つのリーフ インターフェイス プロファイルを設定します。一方は F ポートのインターフェイスプロファイルで、もう一方はNPポートのインターフェイスプロファイルです。

F ポートのインターフェイス ポリシー グループに含まれるポリシーの組み合わせは、F ポートのインターフェイスプロトコルに含まれている一連のインターフェイスに適用できます。

NP ポートのインターフェイス ポリシー グループに含まれるポリシーの組み合わせは、NP ポートのインターフェイスプロトコルに含まれている一連のインターフェイスに適用できます。

アタッチ エンティティ プロファイル

インターフェイス ポリシ - グループの設定をファイバチャネル ドメイン マッピングにバインドします。

ドメイン

FCoE をサポートするために作成または設定ができるドメインとしては、次のものがあります:

物理ドメイン

FCoE VLAN ディスカバリのための LANをサポートするため作成された仮想ドメイン。物理ドメインは、FCoE VLAN ディスカバリをサポートするための VLAN プールを指定します。

ファイバ チャネル ドメイン

FCoE 接続のための仮想 SAN をサポートするため作成された仮想ドメイン。

ファイバ チャネル ドメインは、FCoE トラフィックが搬送される VSAN プール、VLAN プールおよび VSAN 属性を指定します。

- **VSAN プール** - 既存の VLAN に関連付けられた仮想 SAN のセット。個々 の VSAN は、VLAN をイーサネット接続のためのインターフェイスに割り当てるのと同じ方法で、関連付けられた FCoE 対応のインターフェイスに割り当てることができます。
- **VLAN プール** - 個々 の VSAN に関連付けることができる VLAN のセット。
- **VSAN 属性** - VSAN から VLAN へのマッピング。

テナント エンティティ

[テナント] タブでは、ブリッジ ドメインおよび EPG エンティティを、FCoE ポートにアクセスし、FCoE トラフィックを交換するように設定します。

エンティティには、次のものがあります:

ブリッジ ドメイン (FCoE サポートのために設定されたもの)

テナントの下で、FCoE 接続を使用するアプリケーションのために FCoE トラフィックを送るように作成され、設定されたブリッジ ドメイン。

アプリケーション EPG

同じテナントの下で FCoE ブリッジ ドメインと関連付けられる EPG。

ファイバ チャネル パス

FCoE F ポートまたは NP ポートとして有効にされ、選択した EPG に関連付けられるインターフェイスを指定します。ファイバチャネルのパスを EPG に関連付けると、FCoE インターフェイスはが指定された VSAN に展開されます。

APIC GUI を使用した FCoE vFC ポートの展開

APIC GUI では、カスタマイズされたノード ポリシー グループ、リーフ プロファイル、インターフェイス ポリシー グループ、インターフェイス プロファイル、仮想 SAN ドメインを作成し、システム管理者が F ポートまたは NP ポートとして指定するすべてのインターフェイスを再利用して、整合性のある FCoE 関連ポリシーが適用されている FCoE トラフィックを処理できます。

始める前に

- ACI ファブリックがインストールされています。
- ポート チャネル (PC) トポロジ上で導入する場合、ポート チャネルは 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 （96 ページ）の説明に従ってセットアップします。
- 仮想ポートチャネル（vPC）トポロジを介して展開する場合は、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 （123 ページ）の説明に従って vPC が設定されます。

手順

ステップ 1 FCoE 補助スイッチ ポリシー グループを作成し、FCoE 設定をサポートするすべてのリーフ スイッチ ポリシーを指定して組み合わせます。

このポリシー グループは、NPV ホストとして機能するリーフ スイッチに適用されます。

a) APIC GUI で、APIC のメニュー バーから **[Fabric]** > **[Access Policies]** > **[Switches]** > **[Leaf Switches]** > **[Policy Groups]** の順にクリックします。

b) **Policy Groups** を右クリックして、**Create Access Switch Policy Group** をクリックします。

c) [Create Access Switch Policy Group] ダイアログボックスで、以下で説明する設定を指定して、[Submit] をクリックします。

ポリシー	説明
名前	スイッチ ポリシー グループを識別します。 このスイッチ ポリシー グループの FCoE 補助機能を示す名前を入力します。たとえば、 **`fcoe_switch_policy_grp`** のようにします。
ファイバ チャネル SAN ポリシー	次の SAN ポリシーの値を指定します: • FC プロトコルの EDTOV (デフォルト: 2000) • FC プロトコルの RATOV (デフォルト: 10000) • リーフ スイッチが使用する MAC アドレスのプレフィックス (FC マップとも呼ばれます)。この値は、同じポートに接続されているピア デバイスの値と一致する必要があります。通常、デフォルト値の OE:FC:00 が使用されます。 ドロップダウン オプション ボックスをクリックします。 • デフォルトの EDTOV、RATOV、および MAC アドレスのプレフィックス値を使用するには、**default** をクリックします。 • 既存のポリシーで指定した値を使用するには、そのポリシーをクリックします。

ポリシー	説明
	• カスタマイズした新しいMACアドレスプレフィックスを指定する新しいポリシーを作成するには、[Create Fibre Channel SAN Policy] をクリックして、プロンプトに従います。

ステップ 2 FCoE トラフィックをサポートするリーフ スイッチのリーフ プロファイルを作成します。

このプロファイルは、前の手順で設定されたスイッチ ポリシー グループを割り当てるスイッチまたはリーフスイッチの設定を指定します。この関連付けにより、事前定義されたポリシー設定で FCoE トラフィックをサポートするスイッチの設定を有効にします。

a) APIC メニュー バーから、**[Fabric]** > **[Access Policies]** > **[Switches]** > **[Leaf Switches]** > **[Profiles]** の順にクリックします。
b) **[リーフ プロファイル]** を右クリックし、**[リーフ プロファイルの作成]** をクリックします。
c) **[リーフ プロファイルの作成]** ダイアログで、リーフ プロファイルを作成し名前を付けます（例：NPV 1）
d) また、**Create Leaf Profile** ダイアログの **Leaf Selectors** テーブルで、**+** をクリックしてテーブルで新しい行を作成し、NPV デバイスとして動作するリーフ スイッチを指定します。
e) テーブルの新しい行で、リーフ名とブロックを選択し、前のステップで作成したスイッチ ポリシー グループを割り当てます。
f) **[Next（次へ）]** をクリックし、さらに **[Finish（終了）]** をクリックします。

ステップ 3 少なくとも 2 個の FCoE 補助インターフェイス ポリシー グループの作成：1 個は FCoE F ポート インターフェイスをサポートするすべてのポリシーを組み合わせ、1 個は FCoE NP ポートをサポートしているすべてのポリシーを組み合わせるためのものです。

これらのインターフェイス ポリシー グループは、F ポートおよび NP ポートとして使用されるインターフェイスに適用されるインターフェイスのプロファイルに適用します。

a) APIC メニュー バーで、**[Fabric]** > **[Access Policies]** > **[Interfaces]** > **[Leaf Interfaces]** > **[Policy Groups]** の順にクリックします。
b) **[Policy Groups]** を右クリックし、ポート アクセスの設定方法に応じて、**[Create Leaf Access Port Policy Group]**、**[Create PC Interface Port Policy]**、または **[Create vPC Interface Port Policy Group]** のいずれかのオプションをクリックします。

（注）
- PC インターフェイスで展開する場合、追加情報については 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 （96 ページ） を参照してください。
- vPC インターフェイスを介して展開する場合は、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 （123 ページ） で詳細を確認してください。

c) ポリシーグループ ダイアログで、設定するファイバチャネルインターフェイス ポリシー、低速ドレイン ポリシー、優先順位フロー制御ポリシーを含むように指定します。

ポリシー	説明
名前	このポリシー グループの名前。 このリーフアクセスポートのポリシーグループとポートタイプ（FまたはNP）の補助機能を示す、サポートを意図した名前を入力します。 **`fcoe_f_port_policy`** または **`fcoe_np_port_policy`**。
優先順位フロー制御ポリシー	このポリシー グループが適用されているインターフェイスの優先順位 フロー制御（PFC）の状態を指定します。 オプションには、次のものが含まれます。 • **[自動]**（デフォルト値）DCBXによってアドバタイズされ、ピアとの交渉が正常に行われた値を条件として、設定されている非ドロップ CoS のローカル ポートで、優先順位フロー制御（PFC）を有効にします。障害により、非ドロップ CoS 上で優先順位フロー制御が無効になります。 • **[オフ]** 機能によりあらゆる状況下で、ローカル ポートの FCoE 優先順位フロー制御を無効にします。 • **[オン]** 機能によりあらゆる状況下で、ローカル ポートの FCoE 優先順位フロー制御を有効にします。 ドロップダウン オプション ボックスをクリックします。 • デフォルト値を使用するには、**[デフォルト]** をクリックします。 • 既存のポリシーで指定した値を使用するには、そのポリシーをクリックします。 • 別の値を指定する新しいポリシーを作成するには、**[優先順位フロー制御ポリシーの作成]** をクリックし、指示に従います。 （注） PFC では、サービス クラス（CoS）レベルがファブリックに対してグローバルに有効になり、FCoE トラフィックを生成するアプリケーションのプロファイルに割り当てられている必要があります。また、CoS 保持が有効になっている必要があります。有効にするには、**[Fabric]** > **[Access Policies]** > **[Policies]** > **[Global]** > **[QoS Class]** に移動して、[Preserve COS Dot1p Preserve] を有効にします。
低速ドレイン ポリシー	ACI ファブリックでトラフィック輻輳を引き起こすFCoEパケットを処理する方法を指定します。オプションには、次のものが含まれます。 • 輻輳クリア アクション（デフォルト：無効） FCoE トラフィックの輻輳時に実行するアクション。次のオプションがあります。 • エラー：無効：ポートを無効にします。 • ログ：イベントログの輻輳を記録します。

ポリシー	説明
	• 無効：実行しません。 • 輻輳検出乗数（デフォルト：10） FCoE トラフィック輻輳に対処するため輻輳クリア アクションをトリガするポート上で受信した一時停止フレーム数。 • フラッシュ管理状態 • 有効：バッファをフラッシュします。 • 無効：バッファをフラッシュしません。 • フラッシュのタイムアウト（デフォルト：500 ミリ秒単位） 輻輳時にバッファのフラッシュをトリガするしきい値（ミリ秒）。 • デフォルト値を使用するには、**[デフォルト]** をクリックします。 • 既存のポリシーで指定した値を使用するには、そのポリシーをクリックします。 • 別の値を指定する新しいポリシーを作成するには、**[低速ドレイン ポリシーの作成]** をクリックしてプロンプトに従います。

ステップ 4 少なくとも 2 個のインターフェイス プロファイルの作成：1 個は F ポート接続をサポートするプロファイル、1 個は NP ポート接続をサポートするプロファイル、追加ポート ポリシーの変数に関連付けるオプションの追加プロファイル。

a) APIC バー メニューで、**[Fabric]** > **[Access Policies]** > **[Interfaces]** > **[Leaf Interfaces]** > **[Profiles]** をクリックします。

b) **Profiles** を右クリックし、**Create Leaf Interface Profile** を選択します。

c) [Create Leaf Interface Profile] ダイアログで、たとえば「FCoE_F_port_Interface_profile-1」など、プロファイルを説明する名前を入力します。

d) インターフェイスの [Interface Selectors] テーブルで、[+] をクリックして [Create Access Port Selector] ダイアログを表示します。このダイアログを使用すると、インターフェイスの範囲を表示し、次の表に記載されたフィールドに設定を適用できます。

オプション	説明
名前	このポート セレクタを説明する名前。
Interface IDs	この範囲が適用されるインターフェイスの設定を指定します。 • スイッチにすべてのインターフェイスを含むには、**[すべて]** を選択します。 • この範囲に個々のインターフェイスを含めるには、たとえば `1/20` など単一のインターフェイス ID を指定します。

オプション	説明
	• この範囲にインターフェイスの範囲を含めるには、たとえば **1/10 - 1/15** など、ハイフンで区切られた最低値と最大値を入力します。 （注） F ポートおよび NP ポートのインターフェイスのプロファイルを設定する際に、重複しない別の範囲をインターフェイスに指定します。
インターフェイス ポリシー グループ	前の手順で設定した F ポート インターフェイス ポリシー グループまたは NP ポート ポリシー グループの名前。 • F ポートとしてこのプロファイルに含まれるインターフェイスを指定するには、F ポート用に設定されているインターフェイスポリシーグループを選択します。 • NP ポートとしてプロファイルに含まれるインターフェイスを指定するには、NP ポート用に設定されているインターフェイス ポリシー グループを選択します。

ステップ 5 [Submit] をクリックします。前の手順を繰り返しすと、F ポートおよび NP ポートの両方にインターフェイス ポリシーを有することができます。

ステップ 6 FCoE トラフィックにグローバル QoS ポリシーを適用するかどうかを設定します。

さまざまなレベル（1、2、4，5、6）の FCoE トラフィックにさまざまな QoS ポリシーを指定することができます。

a) APIC バー メニューから、**[Fabric]** > **[Access Policies]** > **[Policies]** > **[Global]** > **[QoS Class]** の順にクリックし、[QoS Class] ペインで [Preserve CoS] フラグを有効にします。

b) **[QoS Class - Level 1]**、**[QoS Class - Level 2]**、**[QoS Class - Level 4]**、**[QoS Class - Level 5]**、または **[QoS Class - Level 6]** ダイアログで、次のフィールドを編集して PFC と no-drop CoS を指定します。それから **Submit.** をクリックします。

（注）
PFC とノードロップ CoS で設定できるのは 1 レベルだけです。

ポリシー	説明
PFC 管理状態	FCoE トラフィックのこのレベルに優先順位フロー制御を有効にするかどうか（デフォルト値は false です）。 優先順位フロー制御を有効にすると、FCoE トラフィックのこのレベルの [輻輳アルゴリズム] が [ノードロップ] に設定されます。
No-Drop-CoS	FCoE トラフィックの輻輳の場合でも FCoE パケット処理をドロップしない CoS レベル。

ステップ 7 ファイバ チャネル ドメインを定義します。仮想 SAN (VSAN) のセットを作成し、それらを既存の VLAN の設定にマップします。

a) APIC バー メニューで、**[Fabric]** > **[Access Policies]** > **[Physical and External Domains]** > **[Fibre Channel Domains]** の順にクリックします。

b) [Fibre Channel Domains] を右クリックし、[Create Fibre Channel Domain] をクリックします。

c) [Fibre Channel Domain] ダイアログで、次の設定を指定します。

オプション	説明/処理
Name	作成する VSAN ドメインに割り当てる名前またはラベルを指定します。(たとえば vsan-dom2 など)
VSAN Pool	このドメインに割り当てられる VSAN プール。 • 既存の VSAN プールを選択するには、ドロップダウンをクリックしてリストから選択します。変更する場合は、編集アイコンをクリックします。 • VSAN プールを作成するには、**Create a VSAN Pool** をクリックします。 VSAN プールを作成するダイアログで、プロンプトに従って以下を設定します: • FCoE をサポートするには、**静的**リソース割り当て方法が用いられます。 • FCoE F ポート インターフェイスと NP ポート インターフェイスを割り当てる際に利用できる VSAN の範囲です。 （注） 最小値は 1 です。最大値は 4078 です。 必要であれば、複数の範囲の VSAN を設定できます。
VLAN プール	VSAN プールのメンバーがマッピングで使用できる VLAN のプール。 VLAN プールは、このドメインの FCoE 接続をサポートする際に利用する、VLAN の数値範囲を指定します。指定した範囲内の VLAN が、VSAN がマップを行う際に利用できます。 • 既存の VLAN プールを選択するには、ドロップダウンをクリックしてリストから選択します。変更する場合は、編集アイコンをクリックします。 • VLAN プールを作成するには、**Create a VLAN Pool** をクリックします。 VLAN プールを作成するダイアログで、プロンプトに従って以下を設定します: • FCoE をサポートするには、**静的**リソース割り当て方法が用いられます。 • VSAN でマッピングを行う際に利用できる VLAN の範囲です。 （注） 最小値は 1 です。最大値は 4094 です。 必要であれば、複数の範囲の VLAN を設定できます。

オプション	説明/処理
VSAN Attr	このドメインの VSAN 属性マップ VSAN 属性は、VSAN プールの VSAN を VLAN プールの VLAN にマップします。 • 既存の VSAN 属性マップを選択するには、ドロップダウンをクリックしてリストから選択します。変更する場合は、編集アイコンをクリックします。 • VSAN 属性マップを作成するには、**Create VSAN Attributes** をクリックします。 VSAN 属性を構成するダイアログで、プロンプトに従って以下を設定します: • 適切なロード バランシング オプション (src-dst-ox-id or src-dst-id)。 • 個々 の VSAN から個々の VLAN へのマッピング。たとえば vsan-8 を vlan 10 にマッピングします （注） このドメインのために指定した範囲の VSAN と VLAN だけが、相互にマッピングできます。

ステップ 8 接続済みエンティティ プロファイルを作成し、ファイバ チャネル ドメインをインターフェイス ポリシー グループにバインドします。

a) APIC メニューバー で、**[Fabric]** > **[Access Policies]** > **[Interfaces]** > **[Leaf Interfaces]** > **[Policy Groups]** > ***[interface_policy_group_name]*** の順にクリックします。

この手順の *interface_policy_group_name* は、手順 3 で定義したインターフェイス ポリシ - グループです。

b) インターフェイス ポリシー グループのダイアログ ボックスで、[Attached Entity Profile] ドロップダウンをクリックし、既存のアタッチ エンティティ プロファイルを選択するか、**Create Attached Entity Profile** をクリックして、新しいものを作成します。

c) [Attached Entity Profile] ダイアログでは、以下の設定を指定します:

フィールド	説明
名前	この接続済みエンティティ プロファイルの名前
Domains To Be Associated To Interfaces	インターフェイスポリシーグループに関連付けられるドメインが一覧表示されます。 ここでは、手順 7 で設定したファイバ チャネル ドメインを選択します。 [Submit] をクリックします。

ステップ 9 リーフ プロファイルおよび F ポートと NP ポート インターフェイス プロファイルを関連付けます。

a) APIC メニュー バーから、**[Fabric]** > **[Access Policies]** > **[Switches]** > **[Leaf Switches]** > **[Profiles]** をクリックし、手順 2 で設定したリーフ プロファイルの名前をクリックします。

b) [Create Leaf Profile] ダイアログで、[Associated Interface Selector Profiles] 表を探し、[+] をクリックして新しい表の行を作成し、手順 4 で作成した F ポート インターフェイス プロファイルを選択します。

c) もう一度 **Associated Interface Selector Profiles** テーブルで、+をクリックしてテーブルの新しい行を作成し、手順 4 で作成した NP ポート インターフェイス プロファイルを選択します。

d) [Submit] をクリックします。

次のタスク

ACI ファブリックのインターフェイスに仮想 F ポートおよび NP ポートを正常に展開した後、次の手順でシステム管理者がこれらのインターフェイスを介して EGP アクセスと接続が可能になります。

詳細については、「APIC GUI を使用した vFC ポートへの EPG アクセスの展開 （172 ページ）」を参照してください。

APIC GUI を使用した vFC ポートへの EPG アクセスの展開

ACI ファブリック エンティティを、FCoE トラフィックおよび指定したインターフェイスの F ポートおよび NP ポートをサポートするように設定したら、次の手順はこれらのポートへの EPG アクセスを設定することです。

始める前に

- ACI ファブリックがインストールされていること。
- FC ネットワーク（SAN ストレージなど）に接続しているファイバ チャネル転送（FCF）スイッチは、イーサネットによって ACI リーフ スイッチポートに物理的に接続しています。
- FC ネットワークにアクセスする必要があるホスト アプリケーションは、同じ ACI リーフ スイッチのポートにイーサネットで物理的に接続されていること。
- リーフ ポリシー グループ、リーフ プロファイル、インターフェイス ポリシー グループ、インターフェイス プロファイルとファイバ チャネル ドメインのすべてが、FCoE トラフィックをサポートするように設定されていること。

手順

ステップ 1 適切なテナントの下で、既存のブリッジ ドメインを FCoE をサポートするように設定するか、FCoE をサポートするブリッジ ドメインを作成します。

オプション:	アクション:
FCoE の既存のブリッジ ドメインを設定するには	**1.** **Tenant** > ***tenant_name*** > **Networking** > **Bridge Domains** > ***bridge_domain_name*** をクリックします。 **2.** **タイプ** ブリッジ ドメインのフィールド **プロパティ** パネルにある、クリックして **fc** 。 **3.** [Submit] をクリックします。
FCoE の新しいブリッジ ドメインを作成するには	**1.** **Tenant** > ***tenant_name*** > **Networking** > **Bridge Domains** > **Actions** > **Create a Bridge Domain** をクリックします。 **2.** **Name** フィールド (**Specify Bridge Domain for the VRF** ダイアログ) で、ブリッジ ドメインの名前を入力します。 **3.** [Specify Bridge Domain for the VRF] ダイアログの [Type] フィールドで、[fc] をクリックします。 **4.** [VRF] フィールドで、ドロップダウンから VRF を選択するか、**Create VRF** をクリックし、新しい VRF を作成して設定します。 **5.** ブリッジ ドメインの設定を終了します。 **6.** [Submit] をクリックします。

ステップ 2 同じテナントでの下で、既存の EPG を設定するか、新しい EPG を作成して、FCoE が設定されたブリッジ ドメインと関連付けます。

オプション:	アクション:
既存の EPG を関連付ける	**1.** **[Tenant]** > ***[<テナント名>]*** > **[Application Profiles]** > ***[<アプリケーション プロファイル名>]*** > **[Application EPGs]** > ***[<EPG 名>]*** の順にクリックします。 **2.** **[QoS class]** フィールドで、このEPGによって生成されたトラフィックに割り当てる Quality of Service（**Level1**、**Level2**、**Level4**、**Level5**、または **Level6**）を選択します。 優先順位フロー制御のドロップ輻輳なしハンドリングで QoS レベルのいずれかを設定する場合、そしてドロップなしパケット優先順位で FCoE トラフィックを処理する必要がある場合には、この EPG にその QoS レベルを割り当てます。

オプション:	アクション:
	3. **Bridge Domain** フィールド (EPG の **Properties** パネル) で、ドロップダウンリストをクリックして、タイプに合わせて設定したドメインの名前を選択します。ここでは fcoe です。 **4.** [Submit] をクリックします。 （注） [Bridge Domain] フィールドを変更した場合には、変更後 30 ～ 35 秒待機する必要があります。[Bridge Domain] フィールドの変更を急ぎすぎると、NPV スイッチの vFC インターフェイスが障害を起こし、スイッチのリロードが必要になります。
新しい EPG を作成して関連付ける	**1.** **[Tenant]** > ***[<テナント名>]*** > **[Application Profiles]** > ***[<アプリケーション プロファイル名>]*** > **[Application EPGs]** の順にクリックします。 **2.** **Application EPGs** を右クリックし、**Create Application EPG** をクリックします。 **3.** **[QoS class]** フィールドで、このEPGによって生成されたトラフィックに割り当てる Quality of Service（**Level1**、**Level2**、**Level4**、**Level5**、または **Level6**）を選択します。 優先順位フロー制御のドロップ輻輳なしハンドリングで QoS レベルのいずれかを設定する場合、そしてドロップなしパケット優先順位で FCoE トラフィックを処理する必要がある場合には、この EPG にその QoS レベルを割り当てます。 **4.** **Bridge Domain** フィールド (**Specify the EPG Identity** ダイアログ) フィールドで、ドロップダウンリストをクリックして、タイプに合わせて設定したドメインの名前を選択します。ここでは fcoe です。 （注） [Bridge Domain] フィールドを変更した場合には、変更後 30 ～ 35 秒待機する必要があります。[Bridge Domain] フィールドの変更を急ぎすぎると、NPV スイッチの vFC インターフェイスが障害を起こし、スイッチのリロードが必要になります。 **5.** ブリッジ ドメインの設定を終了します。 **6.** **Finish** をクリックします。

ステップ 3 ファイバ チャネル ドメインと EPG の関連付けを追加します。

a) **[Tenant]** > ***[<テナント名>]*** > **[Application Profiles]** > ***[<アプリケーション プロファイル名>]*** > **[Application EPGs]** > ***[<EPG 名>]*** > **[Domains（VMs and Bare Metal）]** の順にクリックします。

b) [Domains（VMs and Bare Metal）] を右クリックし、[Add Fibre Channel Domain Association] をクリックします。
c) [Add Fibre Channel Domain Association] ダイアログで、[Fibre Channel Domain Profile] フィールドを探します。
d) ドロップダウンリスト をクリックし、以前に設定したファイバ チャネル ドメインの名前を選択します。
e) [Submit] をクリックします。

ステップ 4 関連する EPG の下で、ファイバ チャネルのパスを定義します。

ファイバ チャネルのパスでは、FCoE F ポートまたは NP ポートとして有効にされたインターフェイスを指定して、選択した EPG に関連付けます。

a) **[Tenant]** > ***[<テナント名>]*** > **[Application Profiles]** > ***[<アプリケーション プロファイル名>]*** > **[Application EPGs]** > ***[<EPG 名>]*** > **[Fibre Channel（Paths）]** の順にクリックします。
b) [Fibre Channel（Paths）] を右クリックし、[Deploy Fibre Channel] をクリックします。
c) [Deploy Fibre Channel] ダイアログで、次の設定を行います。

オプション:	アクション:
Path Type	FCoE トラフィックを送受信するためにアクセスされるインターフェイスのタイプです (ポート、ダイレクト ポート チャネル、または仮想ポート チャネル)。
Path	選択した EPG に関連付けられている FCoE トラフィックが流れるノードインターフェイスのパスです。 ドロップダウン リストをクリックして、リスト表示されたインターフェイスの中から選択します。。 （注） 以前に F ポートまたは NP ポートとして設定されているインターフェイスのみを選択します。設定されていないインターフェイスを選択すると、これらのインターフェイスにはデフォルト値だけが適用されます。 （注） FCoE over FEX を展開するには、以前に設定した FEX ポートを選択します。
VSAN	**Path** フィールドで選択したインターフェイスを使用する VSAN です。 （注） 指定する VSAN は、VSAN プールとして指定した VSAN の範囲になければなりません。 ほとんどの場合、この EPG がアクセスするために設定されているすべてのインターフェイスは、同じ VSAN に割り当てられている必要があります。ただし、仮想ポートチャネル (VPC) 接続上にファイバ チャネル パスを指定する場合を除きます。その場合には、2 つの VSAN を指定し、接続のレッグごとに 1 つを使用します。

オプション:	アクション:
VSAN Mode	選択した VSAN が選択したインターフェイスにアクセスするモードです (**Native** または **Regular**)。 FCoE サポート用に設定された各インターフェイスでは、ネイティブ モードに設定された VSAN が 1 つだけ必要です。同じインターフェイスに割り当てられる追加の VSAN は、通常モードでアクセスする必要があります。
Pinning label	(オプション) このオプションは、アクセスを F ポートへマッピングする場合にのみ適用されます。そしてこの F ポートは、特定のアップリンク NP ポートにバインドする必要があります。これは、ピニング ラベル (ピニング ラベル 1 またはピニング ラベル 2) を特定の NP ポートに関連付けます。それから、ピニング ラベルをターゲット F ポートに割り当てます。この関連づけを行うと、関連付けられた NP ポートは、すべての場合に、ターゲット F ポートへのアップリンク ポートとしての役割を果たします。 ピニング ラベルを選択し、それを NP ポートとして設定されたインターフェイスに関連付けます。 このオプションは、「トラフィック-マッピング」とも呼ばれるものを実装します。 （注） F ポートと、関連付けられているピニング ラベルの NP ポートは、同一のリーフ スイッチ上に存在する必要があります。

ステップ 5 [Submit] をクリックします。

ステップ 6 EPG アクセスをマッピングする、FCoE 対応のインターフェイスごとに、手順 4 と 5 を繰り返します。

ステップ 7 正常に導入できたかどうかは、次のように確認します。

a) **Fabric** > **Inventory** > ***Pod_name*** > ***leaf_name*** > **Interfaces** > **VFC interfaces** をクリックします。

ポートを展開したインターフェイスが、VFC インターフェイス下にリスト表示されます。

次のタスク

vFC インターフェイスへの EPG アクセスをセットアップした後の最後の手順は、FCoE 初期化プロトコル (FIP) をサポートするネットワークをセットアップすることです。これによって、それらのインターフェイスの検出が有効になります。

詳細については、「FCoE Initiation Protocol をサポートする EPG の導入 （177 ページ）」を参照してください。

FCoE Initiation Protocol をサポートする EPG の導入

FCoE EPG からサーバのポートへのアクセスを設定した後も、FCoE Initiation Protocol (FIP) をサポートするように EPG のアクセスを設定する必要があります。

始める前に

- ACI ファブリックがインストールされています。
- FC ネットワークにアクセスする必要があるホスト アプリケーションは、同じ ACI Leaf スイッチのポートにイーサネットで物理的に接続されます。
- リーフ ポリシー グループ、リーフ プロファイル、インターフェイス ポリシー グループ、インターフェイスのプロファイルとファイバ チャネル ドメインはすべて、APIC GUI を使用した vFC ポートへの EPG アクセスの展開 （172 ページ）のトピックで説明されているように、FCoE トラフィックをサポートするように設定されています。
- EPG から vFC ポートへのアクセスは、「APIC GUI を使用した vFC ポートへの EPG アクセスの展開 （172 ページ）」のトピックで説明しているように、有効になっています。

手順

ステップ 1 同じテナントの下で、FIP をサポートするように既存のブリッジ ドメインを設定するか、FIP をサポートする通常のブリッジ ドメインを作成します。

オプション:	アクション:
FCoE の既存のブリッジ ドメインを設定するには	**1.** **Tenant** > ***tenant_name*** > **Networking** > **Bridge Domains** > ***bridge_domain_name*** をクリックします。 **2.** **Type** フィールド (ブリッジ ドメインの **Properties** パネル) で、**Regular** をクリックします。 **3.** [Submit] をクリックします。
FCoE の新しいブリッジ ドメインを作成するには	**1.** **Tenant** > ***tenant_name*** > **Networking** > **Bridge Domains** > **Actions** > **Create a Bridge Domain** をクリックします。 **2.** **Name** フィールド (**Specify Bridge Domain for the VRF** ダイアログ) で、ブリッジ ドメインの名前を入力します。 **3.** [Specify Bridge Domain for the VRF] ダイアログの [Type] フィールドで、[Regular] をクリックします。 **4.** [VRF] フィールドで、ドロップダウンから VRF を選択するか、**Create VRF** をクリックし、新しい VRF を作成して設定します。 **5.** ブリッジ ドメインの設定を終了します。

オプション:	アクション:
	6. [Submit] をクリックします。

ステップ 2 同じテナントで、既存の EPG を設定するか、または通常型のブリッジ ドメインと関連付ける新しい EPG を作成します。

オプション:	アクション:
既存の EPG を関連付ける	**1.** **Tenant** > ***tenant_name*** > **Application Profiles** > **ap1** > **Application EPGs** > ***epg_name*** をクリックします。 **2.** **Bridge Domain** フィールド (EPG の **Properties** パネル) で、ドロップダウンリストをクリックして、先ほど FIP をサポートするように設定した通常型のブリッジ ドメインの名前を入力します。 **3.** [Submit] をクリックします。
新しい EPG を作成して関連付けるには、	**1.** **Tenant** > ***tenant_name*** > **Application Profiles** > **ap1** > **Application EPGs** をクリックします。 **2.** **Application EPGs** を右クリックし、**Create Application EPG** をクリックします。 **3.** **Bridge Domain** フィールド (**Specify the EPG Identity** ダイアログ) で、ドロップダウンリストをクリックして、先ほど FIP をサポートするように設定した通常型のブリッジ ドメインの名前を選択します。 **4.** ブリッジ ドメインの設定を終了します。 **5.** **Finish** をクリックします。

ステップ 3 EPG と物理ドメインの関連付けを追加します。

a) **Tenant** > ***tenant_name*** > **Application Profiles** > **ap1** > **Application EPGs** > ***epg_name*** > **Domains & Bare Metal** をクリックします。

b) **Domains & Bare Metal** を右クリックし、**Add Physical Domain Association** をクリックします。

c) **Add Physical Domain Association** ダイアログの [Physical Domain Profile Field] を操作します。

d) ドロップダウンリストをクリックし、FIP のサポートで使用する LAN を含む物理ドメインの名前を選択します。

e) [Submit] をクリックします。

ステップ 4 関連する EPG でパスを定義します。

FCoE F ポートまたは NP ポートとして有効にされ、選択した EPG に関連付けられるインターフェイスを指定します。

a) **[Tenant]** > ***[<テナント名>]*** > **[Application Profiles]** > **[ap1]** > **[Application EPGs]** > ***[<EPG 名>]*** > **[Static Ports]** の順にクリックします。
b) [Static Ports] を右クリックし、[Deploy Static EPG on PC, VPC, or Interface] をクリックします。
c) **Path Type** フィールドで、F モード vFC を展開するポートタイプ (ポート、直接ポートチャネル、または仮想ポート チャネル) を指定します。
d) **Path** フィールドで、F ポートを展開するすべてのパスを指定します。
e) FCoE VLAN ディスカバリとして、およびポート モードとして 802.1p (アクセス) のために使用する [VLAN Encap] を選択します。
f) [Submit] をクリックします。

FCoE コンポーネントは、FCoE ネットワークの動作を開始するために、ディスカバリ プロセスを開始します。

APIC GUI を使用した FCoE 接続のアンデプロイ

ACI ファブリック上のリーフ スイッチ インターフェイスの FCoE イネーブルメントを取り消すには、APIC GUI を使用した FCoE vFC ポートの展開 （164 ページ）で定義したファイバ チャネル パスとファイバ チャネル ドメインとその要素を削除します。

（注） クリーンアップ中に vFC ポートのイーサネット設定オブジェクト (infraHPortS) を削除した場合 (たとえば、GUI の **Leaf Interface Profiles** ページの **Interface Selector** テーブル)、デフォルトの vFC プロパティはそのインターフェイスに関連付けられたままになります。たとえば、vFC NP ポート 1/20 のインターフェイス設定が削除され、そのポートは vFCポート のままですが、デフォルト以外の NP ポート設定が適用されるのではなく、デフォルトの F ポート設定が使用されます。

始める前に

FCoE の展開中に指定した関連する VSAN プール、VLAN プール、および VSAN 属性マップを含む、ファイバ チャネル パスとファイバ チャネル ドメインの名前を知っている必要があります。

手順

ステップ 1 関連するファイバチャネルパスを削除して、この配置でパスが指定されたポート/vsan から vFC をアンデプロイします。

この操作では、この展開でパスが指定されたポート/vsan から vFC 展開が削除されます。

a) **[Tenant]** > ***[<テナント名>]*** > **[Application Profiles]** > ***[<アプリケーション プロファイル名>]*** > **[Application EPGs]** > ***[<アプリケーション EPG 名>]*** > **[Fibre Channel（Paths）]** の順にク

リックします。次に、ターゲットのファイバチャネルパスの名前を右クリックし、**[Delete]** を選択します。

b) [Yes] をクリックして削除を確定します。

ステップ 2 ファイバ チャネル ドメインを定義したときに設定した VLAN 対 VSAN マップを削除します。

この操作は、マップに定義されているすべての要素から vFC の展開を削除します。

a) **[Fabric]** > **[Access Policies]** > **[Pools]** > **[VSAN Attributes]** をクリックします。次に、ターゲット マップの名前を右クリックし、**[Delete]** を選択します。

b) **[Yes]** をクリックして削除を確定します。

ステップ 3 ファイバ チャネル ドメインを定義したときに定義した VLAN プールと VSAN プールを削除します。

これにより、ACI ファブリックからのすべての vFC 展開が不要になります。

a) **[Fabric]** > **[Access Policies]** > **[Pools]** > **[VSAN]** をクリックし、ターゲットVSANプール名を右クリックして、**[Delete]** を選択します。

b) [Yes] をクリックして削除を確定します。

c) **[Fabric]** > **[Access Policies]** > **[Pools]** > **[VLAN]** をクリックし、ターゲット VLAN プール名を右クリックして、**[Delete]** を選択します。

d) [Yes] をクリックして削除を確定します。

ステップ 4 削除したばかりの VSAN プール、VLAN プール、およびマップ エレメントを含むファイバ チャネル ドメインを削除します。

a) **[Tenants]** > **[<テナント名>]** > **[Application Profiles]** > **[Fibre Channel Domains]** をクリックします。次に、ターゲットのファイバ チャネル ドメインの名前を右クリックし、**[Delete]** を選択します。

b) **[Yes]** をクリックして削除を確定します。

ステップ 5 テナント/EPG/App とセレクタは、必要がない場合は削除できます。

オプション	Action
関連するアプリケーション EPG を削除するが、関連するテナントとアプリケーションプロファイルを保存する場合は、次のようにします。	**[Tenants]** > ***[tenant_name]*** > **[Application Profiles]** > ***[app_profile_name]*** > **[Application EPGs]** をクリックし、ターゲット アプリケーション EPG の名前を右クリックして **[Delete]** を選択し、**[Yes]** をクリックして削除を確認します。
関連するアプリケーションプロファイルを削除するが関連するテナントを保存する場合は、次のようにします。	**[Tenants]** > ***[tenant_name]*** > **[Application Profiles]** をクリックし、ターゲット アプリケーション プロファイルの名前を右クリックし、**[Delete]** を選択してから **[Yes]** をクリックして削除を確認します。

オプション	Action
関連するテナントを削除する場合:	**[Tenants]** > をクリックし、ターゲット テナントの名前を右クリックして**[Delete]**を選択し、**[Yes]** をクリックして削除を確認します。

NX-OS スタイルの CLI を使用した FCoE の設定

FCoE NX-OS スタイル CLI 設定

NX-OS スタイル CLI を使用したポリシーまたはプロファイルのない FCoE 接続の設定

次の例の NX-OS スタイル CLI シーケンス EPG の FCoE 接続を設定する **e1** テナントで **t1** 設定またはスイッチ レベルとインターフェイス レベル ポリシーとプロファイルを適用せず。

手順

	コマンドまたはアクション	目的

ステップ 1	ターゲットテナントの下には、FCoE トラフィックをサポートするブリッジ ドメインを設定します。
	例：
	`apic1(config)# tenant t1`
	`apic1(config-tenant)# vrf context v1`
	`apic1(config-tenant-vrf)# exit`
	`apic1(config-tenant)# bridge-domain b1`
	`apic1(config-tenant-bd)# fc`
	`apic1(config-tenant-bd)# vrf member v1`
	`apic1(config-tenant-bd)# exit`
	`apic1(config-tenant)# exit`
		サンプル コマンド シーケンスはブリッジ ドメインを作成 **b1** テナントで **t1** FCoE 接続をサポートするように設定します。

ステップ 2	同じのテナントの下には、FCoE に設定されたブリッジ ドメインとターゲット EPG を関連付けます。
	例：
	`apic1(config)# tenant t1`
	`apic1(config-tenant)# application a1`
	`apic1(config-tenant-app)# epg e1`
	`apic1(config-tenant-app-epg)# bridge-domain member b1`
	`apic1(config-tenant-app-epg)# exit`
	`apic1(config-tenant-app)# exit`
	`apic1(config-tenant)# exit`
		サンプル コマンド シーケンス作成 EPG **e1** し、FCoE に設定されたブリッジ ドメインにその EPG を関連付けます **b1**
		。

	コマンドまたはアクション	目的

ステップ 3	VLAN マッピングに VSAN ドメイン、VSAN プール、VLAN プール、VSAN を作成します。
	例：
	A
	`apic1(config)# vsan-domain dom1`
	`apic1(config-vsan)# vsan 1-10`
	`apic1(config-vsan)# vlan 1-10`
	`apic1(config-vsan)# fcoe vsan 1 vlan 1 loadbalancing src-dst-ox-id`
	`apic1(config-vsan)# fcoe vsan 2 vlan 2`
	例：
	B
	`apic1(config)# template vsan-attribute pol1`
	`apic1(config-vsan-attr)# fcoe vsan 2 vlan 12 loadbalancing src-dst-ox-id`
	`apic1(config-vsan-attr)# fcoe vsan 3 vlan 13 loadbalancing src-dst-ox-id`
	`apic1(config-vsan-attr)# exit`
	`apic1(config)# vsan-domain dom1`
	`apic1(config-vsan)# vsan 1-10`
	`apic1(config-vsan)# vlan 1-10`
	`apic1(config-vsan)# inherit vsan-attribute pol1`
	`apic1(config-vsan)# exit`
		例 A 、サンプル コマンド シーケンスは、VSAN ドメインを作成 **dom1** VSAN プールと VLAN プール、VSAN 1 を VLAN 1 にマッピングされ、VLAN 2 に VSAN 2 をマップ
		例 B 、代替サンプル コマンド シーケンスは再利用可能な VSAN 属性テンプレートを作成 **pol1** VSAN ドメインを作成し、 **dom1** 、そのテンプレートから属性とマッピングを継承します。

ステップ 4	FCoE Initialization (FIP) プロセスをサポートする物理ドメインを作成します。
	例：
	`apic1(config)# vlan-domain fipVlanDom`
	`apic1(config-vlan)# vlan 120`
	`apic1(config-vlan)# exit`
		例では、コマンド シーケンスは、通常の VLAN ドメインを作成 **fipVlanDom** 、VLAN を含む **120** FIP プロセスをサポートします。

ステップ 5	ターゲット テナントの下には、定期的なブリッジ ドメインを設定します。
	例：
	`apic1(config)# tenant t1`
	`apic1(config-tenant)# vrf context v2`
	`apic1(config-tenant-vrf)# exit`
	`apic1(config-tenant)# bridge-domain fip-bd`
	`apic1(config-tenant-bd)# vrf member v2`
	`apic1(config-tenant-bd)# exit`
	`apic1(config-tenant)# exit`
		コマンド シーケンスがブリッジ ドメインを作成例では、 **fip bd** 。

	コマンドまたはアクション	目的

ステップ 6	同じのテナントの下には、設定されている定期的なブリッジドメインでこのEPGを関連付けます。
	例：
	`apic1(config)# tenant t1`
	`apic1(config-tenant)# application a1`
	`apic1(config-tenant-app)# epg epg-fip`
	
	`apic1(config-tenant-app-epg)# bridge-domain member fip-bd`
	`apic1(config-tenant-app-epg)# exit`
	`apic1(config-tenant-app)# exit`
	`apic1(config-tenant)# exit`
		例では、コマンド シーケンス関連付けます EPG **epg fip** ブリッジ ドメインを **fip bd** 。

ステップ 7	VFC インターフェイスを F モードで設定します。
	例：
	A
	`apic1(config)# leaf 101`
	`apic1(config-leaf)# interface ethernet 1/2`
	`apic1(config-leaf-if)# vlan-domain member fipVlanDom`
	`apic1(config-leaf-if)# switchport trunk native vlan 120 tenant t1 application a1 epg epg-fip`
	`apic1(config-leaf-if)# exit`
	
	`apic1(config-leaf)# exit`
	`apic1(config-leaf)# interface vfc 1/2`
	`apic1(config-leaf-if)# switchport mode f`
	`apic1(config-leaf-if)# vsan-domain member dom1`
	`apic1(config-leaf-if)# switchport vsan 2 tenant t1 application a1 epg e1`
	`apic1(config-leaf-if)# switchport trunk allowed vsan 3 tenant t1 application a1 epg e2`
	`apic1(config-leaf-if)# exit`
	例：
	B
	`apic1(config)# vpc context leaf 101 102`
	`apic1(config-vpc)# interface vpc vpc1`
	`apic1(config-vpc-if)# vlan-domain member vfdom100`
	`apic1(config-vpc-if)# vsan-domain member dom1`
	`apic1(config-vpc-if)# #For FIP discovery`
	`apic1(config-vpc-if)# switchport trunk native vlan 120 tenant t1 application a1 epg epg-fip`
		例では **A** コマンド シーケンスは、インターフェイスを有効に **1/2** リーフ スイッチで **101** として機能する、 **F** ポートおよびインターフェイスの VSAN のドメインに関連 **dom1** 。
		ネイティブ モードで 1 つ (と 1 つだけ) の VSAN 対象のインターフェイスの各割り当てる必要があります。各インターフェイスには、通常モードで1つ以上の追加 Vsan を割り当てることができます。
		サンプル コマンド シーケンスは、対象のインターフェイスを関連付けます **1/2** と。
		• VLAN **120** FIP ディスカバリの EPG に関連付けます **epg fip** およびアプリケーション **a1** テナントで **t1** 。
		• VSAN **2** ネイティブ VSAN として、EPG に関連付けます **e1** およびアプリケーション **a1** テナントで **t1** 。
		• VSAN **3** 定期的な VSAN として。
		例 **B** では、コマンド シーケンスは、両方のレッグに同じ VSAN を持つ vPC を介して vFC を設定します。CLI からログごとに異なる Vsan を指定することはできません。代替設定は、GUI を高度な apic 内で実行できます。

	コマンドまたはアクション	目的

	`apic1(config-vpc-if)# switchport vsan 2 tenant t1 application a1 epg e1`
	`apic1(config-vpc-if)# exit`
	`apic1(config-vpc)# exit`
	`apic1(config)# leaf 101-102`
	`apic1(config-leaf)# interface ethernet 1/3`
	`apic1(config-leaf-if)# channel-group vpc1 vpc`
	`apic1(config-leaf-if)# exit`
	`apic1(config-leaf)# exit`
	例：
	C
	`apic1(config)# leaf 101`
	`apic1(config-leaf)# interface vfc-po pc1`
	`apic1(config-leaf-if)# vsan-domain member dom1`
	`apic1(config-leaf-if)# switchport vsan 2 tenant t1 application a1 epg e1`
	`apic1(config-leaf-if)# exit`
	`apic1(config-leaf)# interface ethernet 1/2`
	`apic1(config-leaf-if)# channel-group pc1`
	`apic1(config-leaf-if)# exit`
	`apic1(config-leaf)# exit`	

ステップ 8	VFC インターフェイスを NP モードで設定します。
	例：
	`apic1(config)# leaf 101`
	`apic1(config-leaf)# interface vfc 1/4`
	`apic1(config-leaf-if)# switchport mode np`
	`apic1(config-leaf-if)# vsan-domain member dom1`
		サンプル コマンド シーケンスは、インターフェイスを有効に **1/4** リーフ スイッチで **101** として機能する、 **NP** ポートおよびインターフェイスの VSAN のドメインに関連 **dom1** 。

ステップ 9	VSAN を対象となる FCoE 対応インターフェイスに割り当てます。
	例：
	`apic1(config-leaf-if)# switchport trunk allowed vsan 1 tenant t1 application a1 epg e1`
	`apic1(config-leaf-if)# switchport vsan 2 tenant t4 application a4 epg e4`
		ネイティブ モードで 1 つ (と 1 つだけ) の VSAN 対象のインターフェイスの各割り当てる必要があります。各インターフェイスには、通常モードで 1 つ以上の追加 Vsan を割り当てることができます。
		サンプル コマンド シーケンスは、ターゲット インターフェイスを VSAN **1** に割り当て、それを EPG **e1** とアプリケーション **a1** にテナント **t1** の下で関連付けます。「trunk allowed」は、VSAN 1 に通常モードのステータスを割り当てます。コマンド シーケンスも割り当てま

	コマンドまたはアクション	目的
		す、インターフェイス、必要な **ネイティブ モード** VSAN **2** 。次の例に示すは、同一のインターフェイスを異なるテナント アクセスで実行されているさまざまな Epg を提供するためにさまざまな Vsan の動作を渡します。

NX-OSスタイルCLIを使用したポリシーまたはプロファイルがあるFCoE接続の設定

次の例 NX-OS スタイル CLI のシーケンスを作成し、EPG の FCoE 接続を設定するポリシーを使用して **e1** テナントで **t1** 。

手順

	コマンドまたはアクション	目的

ステップ 1	ターゲット テナントの下には、FCoE トラフィックをサポートするブリッジ ドメインを設定します。
	例：
	`apic1# configure`
	`apic1(config)# tenant t1`
	`apic1(config-tenant)# vrf context v1`
	`apic1(config-tenant-vrf)# exit`
	`apic1(config-tenant)# bridge-domain b1`
	`apic1(config-tenant-bd)# fc`
	`apic1(config-tenant-bd)# vrf member v1`
	`apic1(config-tenant-bd)# exit`
	`apic1(config-tenant)# exit`
	`apic1(config)#`
		サンプル コマンド シーケンスはブリッジ ドメインを作成 **b1** テナントで **t1** FCoE 接続をサポートするように設定します。

ステップ 2	同じのテナントの下には、設定されている FCoE ブリッジ ドメインと、ターゲット EPG を関連付けます。
	例：
	`apic1(config)# tenant t1`
	`apic1(config-tenant)# application a1`
	
	`apic1(config-tenant-app)# epg e1`
	`apic1(config-tenant-app-epg)# bridge-domain member b1`
	`apic1(config-tenant-app-epg)# exit`
	`apic1(config-tenant-app)# exit`
	`apic1(config-tenant)# exit`
	`apic1(config)#`
		サンプル コマンド シーケンス作成 EPG **e1** その EPG の FCoE に設定されたブリッジ ドメイン関連付け **b1** 。

	コマンドまたはアクション	目的

ステップ 3	VLAN マッピングに VSAN ドメイン、VSAN プール、VLAN プール、VSAN を作成します。
	例：
	A
	`apic1(config)# vsan-domain dom1`
	`apic1(config-vsan)# vsan 1-10`
	`apic1(config-vsan)# vlan 1-10`
	`apic1(config-vsan)# fcoe vsan 1 vlan 1 loadbalancing src-dst-ox-id`
	`apic1(config-vsan)# fcoe vsan 2 vlan 2`
	例：
	B
	`apic1(config)# template vsan-attribute pol1`
	`apic1(config-vsan-attr)# fcoe vsan 2 vlan 12`
	`loadbalancing src-dst-ox-id`
	`apic1(config-vsan-attr)# fcoe vsan 3 vlan 13`
	`loadbalancing src-dst-ox-id`
	`apic1(config-vsan-attr)# exit`
	`apic1(config)# vsan-domain dom1`
	`apic1(config-vsan)# inherit vsan-attribute pol1`
	`apic1(config-vsan)# exit`
		例 **A** 、サンプル コマンド シーケンスは、VSAN ドメインを作成 **dom1** VSAN プールと VLAN プール、マップ VSAN 1 VLAN 1 と VLAN 2 に VSAN 2 をマップ
		例 **B** 、代替サンプル コマンド シーケンスは再利用可能な vsan 属性テンプレートを作成 **pol1** VSAN ドメインを作成し、 **dom1** 、そのテンプレートから属性とマッピングを継承します。

ステップ 4	FCoE Initialization (FIP) プロセスをサポートする物理ドメインを作成します。
	例：
	`apic1(config)# vlan-domain fipVlanDom`
	`apic1(config)# vlan-pool fipVlanPool`	

ステップ 5	ファイバ チャネル SAN ポリシーを設定します。
	例：
	`apic1#`
	`apic1# configure`
	`apic1(config)# template fc-fabric-policy ffp1`
	`apic1(config-fc-fabric-policy)# fctimer e-d-tov 1111`
	`apic1(config-fc-fabric-policy)# fctimer r-a-tov 2222`
	`apic1(config-fc-fabric-policy)# fcoe`
		サンプル コマンド シーケンスは、SAN のファイバ チャネル ポリシーを作成 **ffp1** の組み合わせを指定するエラー検出タイムアウト値 (EDTOV)、resource allocation(リソース割り当て、リソースの割り当て) タイムアウト値 (RATOV)、およびターゲット リーフ上の FCoE 対応のインターフェイスのデフォルト FC マップ値スイッチです。

	コマンドまたはアクション	目的
	`fcmap 0E:FC:01` `apic1(config-fc-fabric-policy)# exit`	

ステップ 6	ファイバ チャネル ノード ポリシーを作成します。
	例：
	`apic1(config)# template fc-leaf-policy flp1`
	`apic1(config-fc-leaf-policy)# fcoe fka-adv-period 44`
	`apic1(config-fc-leaf-policy)# exit`
		サンプル コマンド シーケンスは、ファイバチャネル ノードのポリシーを作成 **flp1** を中断のロード バランシングの有効化と FIP キープア ライブ値の組み合わせを指定します。これらの値は、ターゲット リーフ スイッチ上のすべての FCoE 対応インターフェイスにも適用されます。

ステップ 7	ノード ポリシー グループを作成します。
	例：
	`apic1(config)# template leaf-policy-group lpg1`
	`apic1(config-leaf-policy-group)# inherit fc-fabric-policy ffp1`
	`apic1(config-leaf-policy-group)# inherit fc-leaf-policy flp1`
	`apic1(config-leaf-policy-group)# exit`
	`apic1(config)# exit`
	`apic1#`
		サンプル コマンド シーケンスはノード ポリシー グループを作成 **lpg1** 、SAN のファイバ チャネル ポリシーの値を結合する **ffp1** とファイバ チャネル ノードのポリシー、 **flp1** 。このノード ポリシー グループの合計値は、後で設定されているノードのプロファイルに適用できます。

ステップ 8	ノード プロファイルを作成します。
	例：
	`apic1(config)# leaf-profile lp1`
	`apic1(config-leaf-profile)# leaf-group lg1`
	`apic1(config-leaf-group)# leaf 101`
	`apic1(config-leaf-group)# leaf-policy-group lpg1`
		サンプル コマンド シーケンスがノードのプロファイルを作成 **lp1** ノード ポリシー グループと関連付けます **lpg1** 、ノード グループ **lg1** 、およびリーフ スイッチ **101** 。

ステップ 9	F ポート インターフェイスのインターフェイス ポリシー グループを作成します。
	例：
	`apic1(config)# template policy-group ipg1`
	`apic1(config-pol-grp-if)# priority-flow-control mode auto`
	`apic1(config-pol-grp-if)# switchport mode f`
	`apic1(config-pol-grp-if)# slow-drain pause timeout 111`
	`apic1(config-pol-grp-if)# slow-drain congestion-timeout count 55`
	`apic1(config-pol-grp-if)# slow-drain congestion-timeout action log`
		サンプル コマンド シーケンスは、インターフェイス グループのポリシーを作成 **ipg1** し、プライオリティ フロー制御の有効化、F ポートの有効化、およびこのポリシー グループに適用されているすべてのインターフェイスに対して低速ドレイン ポリシーの値を決定する値の組み合わせを割り当てます。

	コマンドまたはアクション	目的

ステップ 10	NP ポートインターフェイスのインターフェイス ポリシー グループを作成します。
	例：
	`apic1(config)# template policy-group ipg2`
	`apic1(config-pol-grp-if)# priority-flow-control mode auto`
	`apic1(config-pol-grp-if)# switchport mode np`
	`apic1(config-pol-grp-if)# slow-drain pause timeout 111`
	`apic1(config-pol-grp-if)# slow-drain congestion-timeout count 55`
	`apic1(config-pol-grp-if)# slow-drain congestion-timeout action log`
		サンプル コマンド シーケンスは、インターフェイス グループ ポリシー **ipg2** を作成し、このポリシー グループに適用されているすべてのインターフェイスに対して、優先順位フロー制御の有効化、NP ポートの有効化、低速ドレイン ポリシーの値を決定する値の組み合わせを割り当てます。

ステップ 11	F ポート インターフェイスのインターフェイス プロファイルを作成します。
	例：
	`apic1# configure`
	`apic1(config)# leaf-interface-profile lip1`
	`apic1(config-leaf-if-profile)# description 'test description lip1'`
	`apic1(config-leaf-if-profile)# leaf-interface-group lig1`
	`apic1(config-leaf-if-group)# description 'test description lig1'`
	`apic1(config-leaf-if-group)# policy-group ipg1`
	`apic1(config-leaf-if-group)# interface ethernet 1/2-6, 1/9-13`
		サンプル コマンド シーケンスは、インターフェイス プロファイルを作成 **lip1** F ポートのインターフェイスの F ポートの特定のインターフェイス ポリシー グループ プロファイルを関連付けます **ipg1** 、このインターフェイスを指定しプロファイルとその関連するポリシー。適用されます。

ステップ 12	NP ポートインターフェイスのインターフェイス プロファイルを作成します。
	例：
	`apic1# configure`
	`apic1(config)# leaf-interface-profile lip2`
	`apic1(config-leaf-if-profile)# description 'test description lip2'`
	`apic1(config-leaf-if-profile)# leaf-interface-group lig2`
	`apic1(config-leaf-if-group)# description 'test description lig2'`
	`apic1(config-leaf-if-group)# policy-group ipg2`
	`apic1(config-leaf-if-group)# interface ethernet 1/14`
		サンプル コマンド シーケンスは、インターフェイス プロファイルを作成 **lip2** NP ポート インターフェイス、NP ポートの特定のインターフェイス ポリシー グループ プロファイルに関連付けます **ipg2** 、このインターフェイスを指定し、プロファイルとその関連するポリシー適用されます。

	コマンドまたはアクション	目的

ステップ 13	レベル 1 の QoS クラス ポリシーを設定します。
	例：
	`apic1(config)# qos parameters level1`
	`apic1(config-qos)# pause no-drop cos 3`
		サンプルコマンドシーケンスは、FCoE トラフィック プライオリティ フロー制御ポリシーを適用することがおよび非ドロップ パケットのクラスのサービス レベル 3 の処理を一時停止の QoS レベルを指定します。

NX-OS スタイル CLI を使用して FCoE オーバー FEX の設定

FEX ポートは、ポート Vsan として設定されます。

手順

ステップ 1 テナントと VSAN のドメインを設定します。

例：

```
apic1# configure
apic1(config)#  tenant t1
apic1(config-tenant)#   vrf context v1
apic1(config-tenant-vrf)#     exit
apic1(config-tenant)#   bridge-domain b1
apic1(config-tenant-bd)#       fc
apic1(config-tenant-bd)#       vrf member v1
apic1(config-tenant-bd)#       exit
apic1(config-tenant)#   application a1
apic1(config-tenant-app)#      epg e1
apic1(config-tenant-app-epg)# bridge-domain member b1
apic1(config-tenant-app-epg)# exit
apic1(config-tenant-app)#      exit
apic1(config-tenant)# exit

apic1(config)#  vsan-domain dom1
apic1(config-vsan)# vlan 1-100
apic1(config-vsan)# vsan 1-100
apic1(config-vsan)# fcoe vsan 2 vlan 2 loadbalancing src-dst-ox-id
apic1(config-vsan)# fcoe vsan 3 vlan 3 loadbalancing src-dst-ox-id
apic1(config-vsan)# fcoe vsan 5 vlan 5
apic1(config-vsan)# exit
```

ステップ 2 FEX をインターフェイスに関連付けます。

例：

```
apic1(config)#  leaf 101
apic1(config-leaf)#  interface ethernet 1/12
apic1(config-leaf-if)#  fex associate 111
apic1(config-leaf-if)#  exit
```

ステップ 3 ポート、ポート チャネル、および VPC あたり FEX を介して FCoE を設定します。

例：

```
apic1(config-leaf)#  interface vfc 111/1/2
apic1(config-leaf-if)#  vsan-domain member dom1
apic1(config-leaf-if)#  switchport vsan 2 tenant t1 application a1 epg e1
apic1(config-leaf-if)# exit

apic1(config-leaf)#  interface vfc-po pc1 fex 111
apic1(config-leaf-if)# vsan-domain member dom1
apic1(config-leaf-if)# switchport vsan 2 tenant t1 application a1 epg e1
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface ethernet 111/1/3
apic1(config-leaf-if)# channel-group pc1
apic1(config-leaf-if# exit
apic1(config-leaf)# exit

apic1(config)# vpc domain explicit 12 leaf 101 102
apic1(config-vpc)# exit
apic1(config)# vpc context leaf 101 102
apic1(config-vpc)#     interface vpc vpc1 fex 111 111
apic1(config-vpc-if)#       vsan-domain member dom1
apic1(config-vpc-if)#       switchport vsan 2 tenant t1 application a1 epg e1
apic1(config-vpc-if)#       exit
apic1(config-vpc)#     exit
apic1(config)# leaf 101-102
apic1(config-leaf)# interface ethernet 1/2
apic1(config-leaf-if)# fex associate 111
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface ethernet 111/1/2
apic1(config-leaf-if)# channel-group vpc1 vpc
apic1(config-leaf-if)# exit
```

ステップ 4 設定を確認するには、次のコマンドを実行します。

例：

```
apic1(config-vpc)# show vsan-domain detail
vsan-domain : dom1

vsan : 1-100

vlan : 1-100

Leaf          Interface         Vsan  Vlan  Vsan-Mode    Port-Mode  Usage
 Operational State
------------  ----------------  ----  ----  -----------  ---------
---------------------------------------
101           vfc111/1/2       2       2    Native                  Tenant: t1
  Deployed
                                                                     App: a1
                                                                     Epg: e1

101           PC:pc1           5       5    Native                Tenant: t1
  Deployed
                                                                     App: a1
                                                                     Epg: e1

101           vfc111/1/3       3       3    Native       F          Tenant: t1
  Deployed
                                                                     App: a1
                                                                     Epg: e1
```

NX-OS スタイルの CLI を使用した FCoE 設定の検証

次 **show** コマンドは、リーフ スイッチ ポートで FCoE の設定を確認します。

手順

使用して、 **vsan ドメインを表示** コマンドをターゲット スイッチで FCoE が有効になっていることを確認します。

コマンドの例では、FCoE がリストされているリーフ スイッチおよび接続の詳細を FCF で有効になっていることを確認します。

例：

```
ifav-isim8-ifc1# show vsan-domain detail
vsan-domain : iPostfcoeDomP1

vsan : 1-20  51-52  100-102  104-110  200  1999  3100-3101  3133
      2000

vlan : 1-20  51-52  100-102  104-110  200  1999  3100-3101  3133
      2000

                                  Vsan    Port                    Operational
 Leaf  Interface       Vsan  Vlan  Mode    Mode  Usage             State
 ----  ---------       ----  ----  ------- ----  ----------------  ------------
 101   vfc1/11         1     1     Regular  F    Tenant: iPost101  Deployed

                                                 App: iPost1

                                                 Epg: iPost1


 101   vfc1/12         1     1     Regular  NP   Tenant: iPost101  Deployed

                                                 App: iPost1

                                                 Epg: iPost1


 101   PC:infraAccBndl 4     4     Regular  NP   Tenant: iPost101  Deployed

          Grp_pc01                               App: iPost4

                                                 Epg: iPost4


 101   vfc1/30         2000        Native        Tenant: t1        Not deployed
                                                 App: a1           (invalid-path)

                                                 Epg: e1
```

NX-OS スタイル CLI を使用した FCoE 要素の展開解除

ACI ファブリックから FCoE 接続を導入解除に移動してもでは、いくつかのレベルで FCoE コンポーネントを削除することが必要です。

手順

ステップ 1 リーフ ポート インターフェイスの属性のリスト、そのモードの設定をデフォルトに設定し、その EPG の導入とドメインの関連付けを削除します。

インターフェイス vfc のポート モードの設定を設定する例 **1/2** のデフォルトに [EPG の導入を削除 **e1** と VSAN ドメインに関連付け **dom1** そのインターフェイスから。

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# interface vfc 1/2
apic1(config-leaf-if)# show run
# Command: show running-config leaf 101 interface vfc 1 / 2
# Time: Tue Jul 26 09:41:11 2016
  leaf 101
    interface vfc 1/2
      vsan-domain member dom1
      switchport vsan 2 tenant t1 application a1 epg e1
      exit
    exit
apic1(config-leaf-if)# no switchport mode
apic1(config-leaf-if)# no switchport vsan 2 tenant t1 application a1 epg e1
apic1(config-leaf-if)# no vsan-domain member dom1
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

ステップ 2 VSAN/VLAN マッピング、および VLAN と VSAN のプールを一覧表示して削除します。

この例では、**vsan 2** の VSAN/VLAN マッピング、VLAN プール **1-10**、および VSAN プール **1-10** を、VSAN ドメイン **dom1** から削除します。

例：

```
apic1(config)# vsan-domain dom1
apic1(config-vsan)# show run
# Command: show running-config vsan-domain dom1
# Time: Tue Jul 26 09:43:47 2016
  vsan-domain dom1
    vsan 1-10
    vlan 1-10
    fcoe vsan 2 vlan 2
    exit
apic1(config-vsan)# no fcoe vsan 2
apic1(config-vsan)# no vlan 1-10
apic1(config-vsan)# no vsan 1-10
apic1(config-vsan)# exit

################################################################################
NOTE: To remove a template-based VSAN to VLAN mapping use an alternate sequence:
################################################################################
```

```
apic1(config)# template vsan-attribute <template_name>
apic1(config-vsan-attr)# no fcoe vsan 2
```

ステップ 3 VSAN ドメインを削除します。

例は、ドメインの VSAN を削除する **dom1** 。

例：

```
apic1(config)# no vsan-domain dom1
```

ステップ 4 必要はないかどうかは、関連付けられているテナント、EPG、およびセレクタを削除できます。

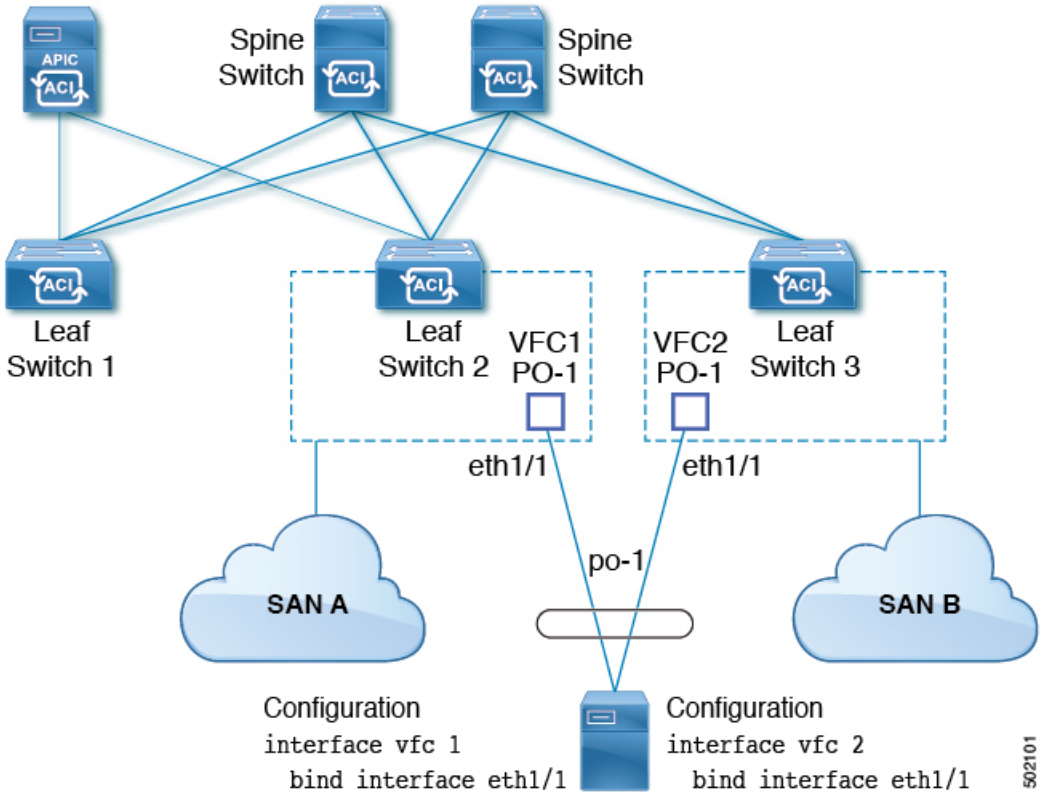
vPC による SAN ブート

Cisco ACI は、Link Aggregation Control Protocol（LACP）ベースの vPC におけるイニシエータの SAN ブートをサポートしています。この制限事項は、LACP ベースのポート チャネルに固有です。

通常のホスト-vPC トポロジでは、ホストに接続している vFC インターフェイスは vPC にバインドされており、vFC インターフェイスをアップする前に vPC を論理的にアップする必要があります。このトポロジでは、vPC で LACP が設定されている場合、ホストは SAN からブートできません。これは、ホストの LACP は通常はアダプタのファームウェアで実装されているのではなく、ホスト ドライバで実装されているためです。

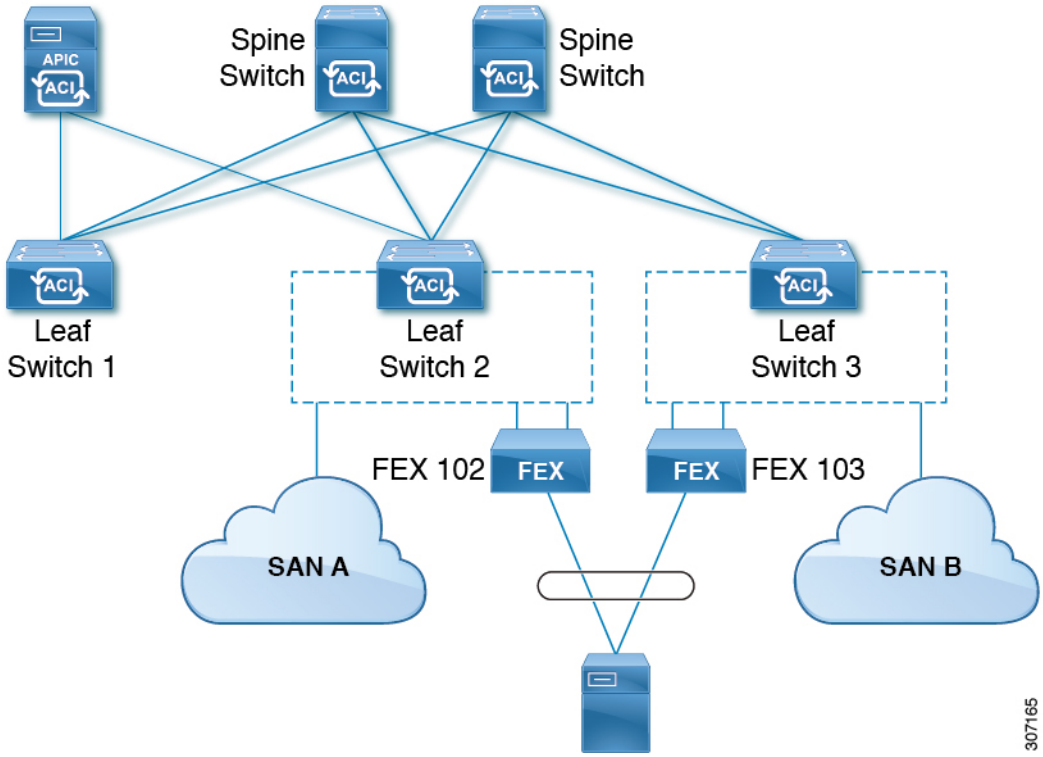
SAN ブートについては、ホストに接続している vFC インターフェイスは、 ポート チャネル自体ではなく、ポート チャネルのメンバーにバインドされています。このバインディングにより、最初の構成で LACP ベースのポート チャネルに依存することなく、CNA/ホスト バス アダプタ（HBA）のリンクがアップした時点で、SAN ブート中にホスト側の vFC がアップするようになります。

図 *30 : vPC* による *SAN* ブートのトポロジ



Cisco APIC リリース 4.0(2) 以降、次の図に示すように、SAN ブートは FEX ホストインターフェイス（HIF）ポート vPC を介してサポートされます。

図 *31 : FEX* ホストインターフェイス（*HIF*）ポート *vPC* を使用した *SAN* ブート トポロジ



vPC による SAN ブートのガイドラインと制約事項

- 複数のメンバーのポート チャネルはサポートされていません。
- vFC がメンバー ポートにバインドされている場合、ポート チャネルに複数のメンバーを持たせることはできません。
- vFC がポート チャネルにバインドされている場合、ポート チャネルには 1 つのメンバーポートしか持たせることはできません。

GUI を使用した vPC による SAN ブートの設定

設定を簡単に行うため、この手順では [Configure Interface, PC, and vPC] ウィザード（**[Fabric] > [Access Policies] > [Quickstart]**）を使用します。

始める前に

この手順では、次の項目がすでに設定済みであることを前提としています。

- VSAN Pool
- VLAN Pool
- VSAN の属性、 VSAN プール内の VSAN の VLAN へのマッピング

- ファイバ チャネル ドメイン（VSAN ドメイン）
- テナント、アプリケーション プロファイル
- アタッチ エンティティ プロファイル

手順

ステップ 1 APIC メニュー バーで、[Fabric] > [Access Policies] > [Quick Start] に移動し、[Configure an interface, PC, and VPC] をクリックします。

ステップ 2 [Configure an interface, PC, and VPC] 作業領域の [vPC Switch Pairs] ツールバーで、[+] をクリックしてスイッチ ペアを作成します。次のアクションを実行します。

a) [vPC Domain ID] テキスト ボックスで、スイッチ ペアを指定する番号を入力します。
b) [Switch 1] ドロップダウンリストで、リーフ スイッチを選択します。

同じ vPC ポリシー グループ内のインターフェイスを持つスイッチのみをペアリングできます。

c) [Switch 2] ドロップダウンリストで、リーフ スイッチを選択します。
d) [Save] をクリックしてこのスイッチ ペアを保存します。

ステップ 3 [Configure an interface, PC, and vPC] 作業領域で、緑色の大きい[+] をクリックし、スイッチを選択します。
[Select Switches To Configure Interfaces] 作業領域が開き、[Quick] オプションがデフォルトで選択されます。

ステップ 4 [Switches] ドロップダウンリストから 2 つのスイッチ ID を選択し、スイッチ プロファイルに名前を付けます。

ステップ 5 再び緑色の大きい [+] をクリックし、スイッチ インターフェイスを設定します。

ステップ 6 [Interface Type] コントロールで、[vPC] を選択します。

ステップ 7 [Interfaces] には、両方のスイッチでvPCメンバーとして使用される1つのポート番号（1/49 など）を入力します。

この操作によってインターフェイス セレクタ ポリシーが作成されます。[Interface Selector Name] テキスト ボックスで、ポリシーの名前を受け入れるか変更できます。

ステップ 8 [Interface Policy Group] コントロールで、[Create One] を選択します。

ステップ 9 [Fibre Channel Interface Policy] テキストボックスから、[Create Fibre Channel Interface Policy] を選択し、次の操作を実行します。

a) [Name] フィールドに、ファイバ チャネル インターフェイス ポリシーの名前を入力します。
b) [Port Mode] セレクタで、[F] を選択します。
c) [Trunk Mode] セレクタで、[trunk-on] を選択します。
d) [Submit] をクリックします。

ステップ 10 [Port Channel Policy] テキスト ボックスで、[Create Port Channel Policy] を選択し、次の操作を実行します。

a) [Name] フィールドに、ポート チャネル ポリシーの名前を入力します。
b) [Mode] ドロップダウンリストで、[LACP Active] を選択します。
c) [Control] セレクタから [Suspend Individual Port] を削除します。

[Suspend Individual Port] はポート チャネルから削除する必要があります。削除しないと、ホストからの LACP BPDU が受信されない場合に物理インターフェイスが中断されます。

d) [Submit] をクリックします。

ステップ 11 [Attached Device Type] ドロップダウンリストで、[Fibre Channel] を選択します。

ステップ 12 [Fibre Channel Domain] ドロップダウンリストで、ファイバ チャネル ドメイン（VSAN ドメイン）を選択します。

ステップ 13 [保存（Save）] をクリックして、この vPC 設定を保存します。

ステップ 14 [Save] をクリックして、このインターフェイス設定を保存します。

ステップ 15 [Submit] をクリックします。

ステップ 16 [Tenants] > [<テナント名>] > [Application Profiles] > [<名前>] > [Application EPGs] の順に展開します。

ステップ 17 [Application EPGs] を右クリックし、[Create Application EPG] を選択して、次の操作を実行します。

この EPG がネイティブ EPG になり、ネイティブ VLAN が設定されます。

a) [Name] フィールドに、EPG の名前を入力します。
b) [Bridge Domain] ドロップダウンリストで、[Create Bridge Domain] を選択します。
c) [Name] フィールドに、ブリッジ ドメインの名前を入力します。
d) [Type] コントロールで、[regular] を選択します。
e) [VRF] ドロップダウンリストで、テナント VRF を選択します。VRF がまだ存在しない場合は、[Create VRF] を選択し、VRF に名前を付けて、[Submit] をクリックします。
f) [Next]、[Next]、[Finish] の順にクリックして [Create Application EPG] に戻ります。
g) [Finish] をクリックします。

ステップ 18 前のステップで作成したネイティブ EPG を展開します。

ステップ 19 [Static Ports] を右クリックし、[Deploy Static EPG On PC, VPC, or Interface] をクリックして、次の操作を実行します。

a) [Path Type] コントロールで、[Virtual Port Channel] を選択します。
b) [Path] ドロップダウンリストから、vPC 用に作成されたポート チャネル ポリシーを選択します。
c) [Port Encap] ドロップダウンリストから [VLAN] を選択し、イーサネット VLAN の番号を入力します。
d) [Deployment Immediacy] コントロールで、[Immediate] を選択します。
e) [Mode] コントロールで、[Access（802.1P）] を選択します。
f) [Submit] をクリックします。

ステップ 20 [Application EPGs] を右クリックし、[Create Application EPG] を選択して、次の操作を実行します。

この EPG は、SAN ごとに 2 つの EPG のうちの 1 番目になります。

a) [Name] フィールドに、EPG の名前を入力します。
b) [Bridge Domain] ドロップダウンリストで、[Create Bridge Domain] を選択します。
c) [Name] フィールドに、ブリッジ ドメインの名前を入力します。
d) [Type] コントロールで、[fc] を選択します。
e) [VRF] ドロップダウンリストで、テナント VRF を選択します。VRF がまだ存在しない場合は、[Create VRF] を選択し、VRF に名前を付けて、[Submit] をクリックします。
f) [Next]、[Next]、[Finish] の順にクリックして [Create Application EPG] に戻ります。
g) [Finish] をクリックします。

ステップ 21 前の手順を繰り返して、2 番目のアプリケーション EPG を作成します。

この 2 番目の EPG は 2 番目の SAN に使用されます。

ステップ 22 2 つの SAN EPG のうちいずれか 1 つを展開し、[Fibre Channel（Paths）] を右クリックし、[Deploy Fibre Channel] を選択して、次の操作を実行します。

a) [Path Type] コントロールで、[Port] を選択します。
b) [Node] ドロップダウンリストで、スイッチ ペアの一方のリーフを選択します。
c) [Path] ドロップダウンリストで、VPC のイーサネット ポート番号を選択します。
d) [VSAN] テキスト ボックスで、「vsan-」で始まる VSAN 番号を入力します。

   たとえば、VSAN 番号が 300 の場合は「vsan-300」と入力します。

e) [VSAN Mode] コントロールで、[Native] を選択します。
f) [Submit] をクリックします。

ステップ 23 2 つの SAN EPG のうちもう一方を展開し、前の手順を繰り返してスイッチ ペアのもう一方のリーフを選択します。

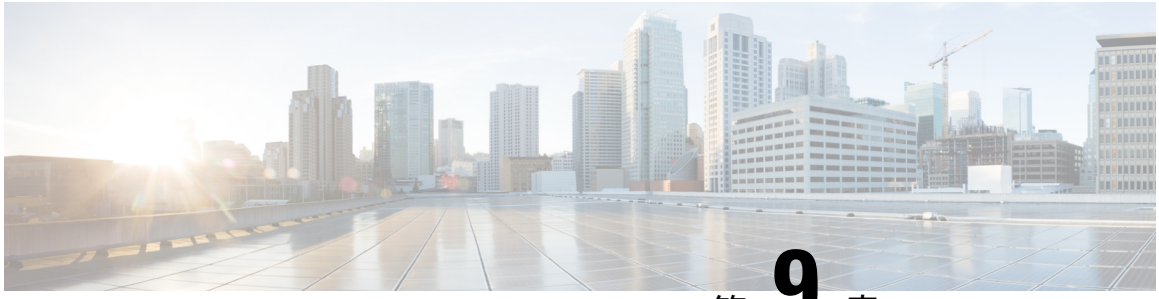
CLI を使用した vPC による SAN ブートの設定

この例では、次の項目がすでに設定されていると仮定しています。

- VLAN ドメイン
- テナント、アプリケーション プロファイル、アプリケーション EPG
- ポート チャネル テンプレート「Switch101-102_1-ports-49_PolGrp」

この例では、VSAN 200 はリーフ 101 上の物理イーサネット インターフェイス 1/49 にバインドされていて、VSAN 300 はリーフ 102 上の物理イーサネット インターフェイス 1/49 にバインドされています。2 つのインターフェイスは、仮想ポート チャネル Switch101-102_1-ports-49_PolGrp のメンバーです。

```
apic1(config-leaf)# show running-config
# Command: show running-config leaf 101
# Time: Sat Sep  1 12:51:23 2018
  leaf 101

    interface ethernet 1/49
      # channel-group Switch101-102_1-ports-49_PolGrp vpc
      switchport trunk native vlan 5 tenant newtenant application AP1 epg epgNative
      port-direction downlink
      exit

    # Port-Channel inherits configuration from "template port-channel
Switch101-102_1-ports-49_PolGrp"
    interface port-channel Switch101-102_1-ports-49_PolGrp
      exit

    interface vfc 1/49
      # Interface inherits configuration from "channel-group
Switch101-102_1-ports-49_PolGrp" applied to interface ethernet 1/49
      switchport vsan 200 tenant newtenant application AP1 epg epg200
      exit

apic1(config-leaf)# show running-config
# Command: show running-config leaf 102
# Time: Sat Sep  1 13:28:02 2018
  leaf 102
    interface ethernet 1/49
      # channel-group Switch101-102_1-ports-49_PolGrp vpc
      switchport trunk native vlan 1 tenant newtenant application AP1 epg epgNative
      port-direction downlink
      exit

    # Port-Channel inherits configuration from "template port-channel
Switch101-102_1-ports-49_PolGrp"
    interface port-channel Switch101-102_1-ports-49_PolGrp
      exit

    interface vfc 1/49
      # Interface inherits configuration from "channel-group
Switch101-102_1-ports-49_PolGrp" applied to interface ethernet 1/49
      switchport vsan 300 tenant newtenant application AP1 epg epg300
```



第 9 章

ファイバ チャネル NPV

この章は、次の内容で構成されています。

- ファイバ チャネル接続の概要 （201 ページ）
- NPV トラフィック管理 （204 ページ）
- SAN A/B の分離 （207 ページ）
- SAN ポート チャネル （207 ページ）
- ファイバ チャネル N ポート仮想化のガイドラインと制限事項 （208 ページ）
- ファイバ チャネル N ポート仮想化でサポートされるハードウェア （210 ページ）
- ファイバ チャネル N ポート仮想化の相互運用性 （210 ページ）
- ファイバ チャネル NPV GUI の設定 （211 ページ）
- ファイバ チャネル NPV NX-OS スタイル CLI の設定 （219 ページ）
- ファイバ チャネル NPV REST API の設定 （223 ページ）

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）アップリンクに集約して、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。

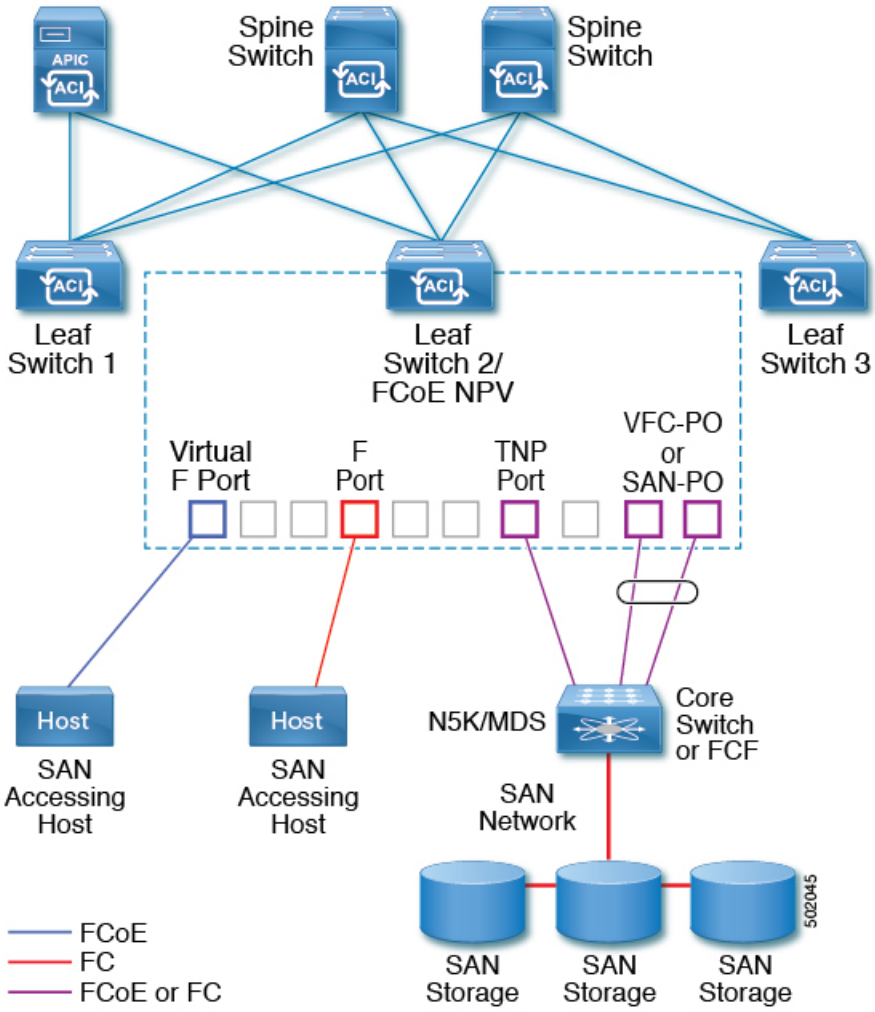
- ファブリックでドメイン ID を追加しなくても、ファブリックに接続するホスト数が増加します。NPV のコア スイッチのドメイン ID は、複数の NPV スイッチ間で共有されます。
- FC ホストと FCoE ホストは、ネイティブの FC インターフェイスを使用して SAN ファブリックに接続します。
- トラフィックの自動マッピングによるロード バランシング。NPV に接続しているサーバを新しく追加した場合に、トラフィックが現在のトラフィック負荷に基づいて、外部のアップリンク間で自動的に分散されます。
- トラフィックの静的マッピング。NPV に接続しているサーバを、外部のアップリンク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

NPV トラフィック管理

通常は、すべてのトラフィックにおいて、すべての使用可能なアップリンクの使用を許可することをお勧めします。NPV トラフィック管理は、自動トラフィック エンジニアリングがネットワーク要件を満たさない場合にだけ使用してください。

自動アップリンク選択

NPV は、外部 NP アップリンク インターフェイスの自動選択をサポートしています。サーバ（ホスト）インターフェイスがアップになると、サーバ インターフェイスと同じ VSAN 内で利用可能な外部インターフェイスから、負荷が最も少ない外部インターフェイスが選択されます。

新しい外部インターフェイスが動作可能になっても、新たに利用可能になったアップリンクを含めるために既存の負荷は自動的に再分散されません。外部インターフェイスが新しいアップリンクを選択できるようになってから、サーバ インターフェイスが動作します。

トラフィック マップ

FC NPV は、トラフィック マップをサポートしています。トラフィック マップにより、サーバ（ホスト）インターフェイスがコア スイッチに接続するために使用可能な外部（NP アップリンク）インターフェイスを指定できます。

Note FC NPV トラフィック マップがサーバインターフェイスに設定されると、サーバインターフェイスはそのトラフィック マップ内の外部インターフェイスからのみ選択する必要があります。指定された外部インターフェイスがいずれも動作していない場合、サーバは非動作状態のままになります。

FC NPV トラフィック マップ機能を使用すると、次のようなメリットが得られます。

- 特定のサーバインターフェイス（またはサーバインターフェイスの範囲）に外部インターフェイスの事前設定された設定を割り当てることによって、トラフィック エンジニアリングが容易になります。
- インターフェイスの再初期化またはスイッチの再起動後に、サーバインターフェイスは同じ トラフィック パスを提供することで、常に同じ外部インターフェイス（または指定された外部インターフェイスのセットのいずれか）に接続するので、永続的な FC ID 機能の適切な動作が確保されます。

複数の NP リンクにまたがるサーバ ログインの破壊的自動ロード バランシング

FC NPV は、サーバ ログインの中断的ロード バランシングをサポートしています。中断的ロード バランシングが有効の場合、新しい NP アップリンクが動作すると、FC NPV によって、サーバー インターフェイスがすべての利用可能な NP アップリンクにわたって再分配されます。サーバ インターフェイスを一方の NP アップリンクからの他方の NP アップリンクに移動するために、FC NPV はサーバインターフェイスを強制的に再初期化して、サーバがコア スイッチへのログインを新たに実行するようにします。

別のアップリンクに移されたサーバインターフェイスだけが再初期化されます。移されたサーバ インターフェイスごとにシステム メッセージが生成されます。

Note サーバ インターフェイスを再配布すると、接続されたエンド デバイスへのトラフィックが中断されます。既存のポート チャネルにメンバーを追加しても、中断的自動ロード バランシングはトリガーされません。

サーバ トラフィックの中断を避けるために、新しい NP アップリンクを追加してから、この機能をイネーブルし、サーバインターフェイスが再配布されてからこの機能を再度ディセーブルにしてください。

ディスラプティブ ロード バランシングがイネーブルでない場合、サーバ インターフェイスの一部またはすべてを手動で再初期化して、新しい NP アップリンク インターフェイスにサーバ トラフィックを分散することができます。

FC NPV トラフィック管理のガイドライン

FC NPV トラフィック管理を導入する際には、次の注意事項に従ってください。

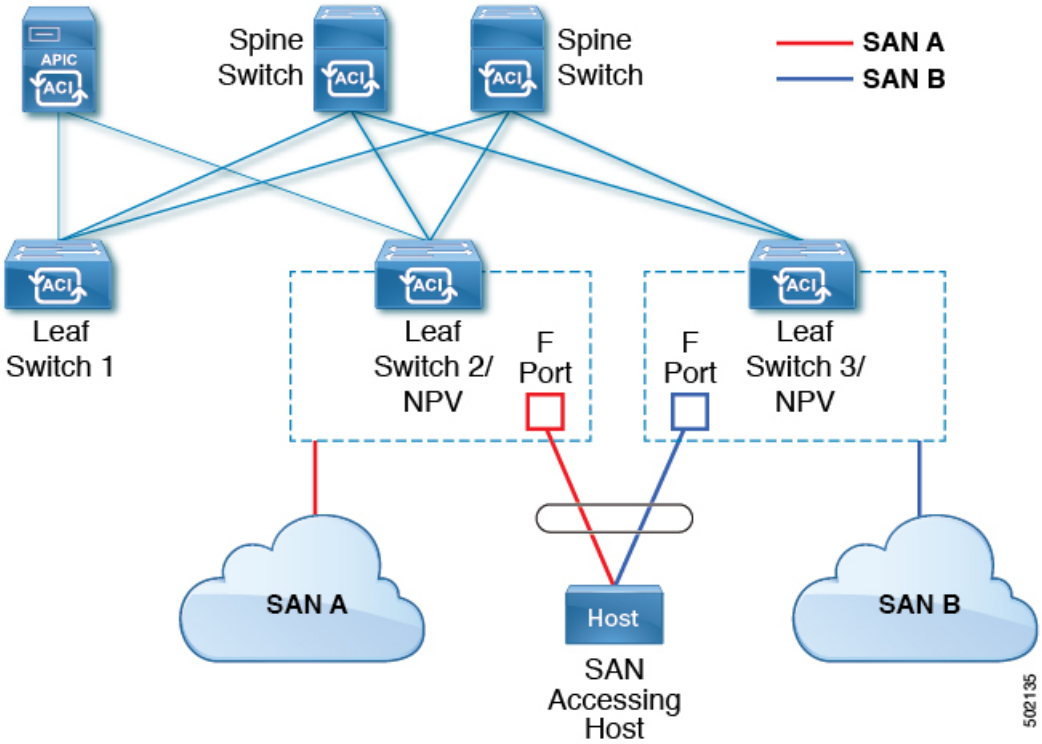
- NPV トラフィック管理は、自動トラフィック エンジニアリングがネットワーク要件を満たさない場合にだけ使用してください。
- すべてのサーバ インターフェイスにトラフィック マップを設定する必要はありません。FC NPV はデフォルトで自動トラフィック管理を使用します。
- NP アップリンク インターフェイスのセットを使用するように設定されたサーバ インターフェイスは、利用可能な NP アップリンク インターフェイスがなくても、他の利用可能な NP アップリンク インターフェイスを使用できません。
- ディスラプティブ ロード バランシングがイネーブルになると、サーバ インターフェイスは 1 つの NP アップリンクから別の NP アップリンクに移動される場合があります。NP アップリンク インターフェイス間を移動する場合、FC NPV ではコア スイッチに再度ログインする必要があり、トラフィックの中断が生じます。
- サーバのセットを特定のコア スイッチにリンクするには、サーバ インターフェイスを NP アップリンク インターフェイスのセット（すべてこのコア スイッチに接続されている）に関連付けてください。
- コア スイッチに永続的な FC ID を設定し、トラフィック マップ機能を使用してサーバ インターフェイスのトラフィックを NP アップリンクに送ります（すべてのアップリングが関連付けられたコア スイッチに接続しています）。
- トラフィック マップの固定を初めて設定する際は、最初のトラフィック マップを設定する前に、サーバのホスト ポートをシャットダウンする必要があります。
- トラフィックのマッピングを複数のアップリンクに設定していて、ホストへのログインに使用されるトラフィック マップを削除する場合は、先にホストをシャットダウンする必要があります。
- FEX の背後にある FCoE ホストのトラフィック マップを設定する場合、1 つのホストを複数の FCoE NP/アップリンク（VFC または VFC-PO）または単一のファイバ チャネル/SAN ポート チャネル NP/アップリンクにマッピングできます。

Note サーバが外部インターフェイスに静的にマッピングされている場合は、外部インターフェイスが何らかの理由でダウンする事態に備えて、サーバ トラフィックが再分配されません。

SAN A/B の分離

SAN A と SAN B の分離により、いずれかのファブリック コンポーネントが障害を起こしても SAN 接続が使用できることが保証されます。SAN A と SAN B の分離は、ファブリック全体で導入されている VSAN を分割することで、物理的または論理的に実現できます。

図 *32 : SAN A/B の分離*



SAN ポート チャネル

SAN ポート チャネルについて

- SAN ポート チャネルは、同じファイバ チャネル ノードに接続された一組の FC インターフェイスを結合して 1 つのリンクとして動作させる論理インターフェイスです。
- SAN ポート チャネルにより、帯域の利用率と可用性がサポートされます。

- Cisco ACI スイッチの SAN ポート チャネルは、FC コア スイッチに接続するため、そして VSAN のアップリンク間で最適な帯域幅利用と透過型のフェールオーバーを実現するために使用されます。

SAN ポート チャネルのガイドラインと制限事項

- Cisco ACI スイッチのアクティブ ポート チャネルの最大数（SAN ポート チャネルと VFC アップリンク/NP ポート チャネルの合計）は 7 です。追加で設定されたポート チャネルはすべて、既存のいずれかのアクティブ ポート チャネルをシャットダウンまたは削除するまで、 **errdisabled** 状態のままです。既存のアクティブ ポート チャネルをシャットダウンまたは削除してから、**errdisabled** のポート チャネルを shut/no shut してアップします。
- SAN ポート チャネルに結合できる FC インターフェイスの最大数は 16 個に制限されます。
- SAN ポート チャネルの Cisco ACI スイッチでのデフォルトのチャネル モードは**アクティブ**です。これは変更できません。
- SAN ポート チャネルがコア スイッチとして Cisco FC コア スイッチに接続されている場合は、アクティブなチャネル モードだけがサポートされます。Cisco FC コア スイッチでアクティブなチャネルモードを設定する必要があります。

SAN ポート チャネル モードについて

SAN ポート チャネルは、デフォルトではチャネル モードがアクティブの状態で設定されています。アクティブの場合、ピア ポートのチャネルグループ モードに関係なく、メンバー ポートはピア ポートとのポートチャネル プロトコルのネゴシエーションを開始します。チャネル グループで設定されているピア ポートがポートチャネル プロトコルをサポートしていない場合、またはネゴシエーション不可能を示すステータスを返す場合、ポート チャネルは無効になります。アクティブのポートチャネルモードでは、片側でポートチャネルメンバーのポートの有効化および無効化を明示的に行わなくても、自動回復が可能です。

ファイバチャネル N ポート仮想化のガイドラインと制限事項

ファイバ チャネル N ポート仮想化（NPV） を設定する場合、次の注意事項および制限事項に注意してください。

- ファイバ チャネル NP ポートはトランク モードをサポートしますが、ファイバ チャネル F ポートはサポートしません。
- トランク ファイバ チャネル ポートでは、最も高い VSAN により内部ログインが行われます。
- コア スイッチで次の機能を有効にする必要があります。

```
feature npiv
feature fport-channel-trunk
```

- 8G のアップリンク速度を使用する場合は、コア スイッチで IDLE フィル パターンを設定する必要があります。

（注） Cisco MDS スイッチでの IDLE フィル パターンの設定例を次に示します。

```
Switch(config)# int fc2/3
Switch(config)# switchport fill-pattern IDLE speed 8000
Switch(config)# show run int fc2/3

interface fc2/3
switchport speed 8000
switchport mode NP
switchport fill-pattern IDLE speed 8000
no shutdown
```

- ファイバ チャネル NPV のサポートは Cisco N9K-C93180YC-FX スイッチに限定されています。
- ファイバ チャネル設定にはポート 1 ー 48 を使用できます。ポート 49 ー 54 をファイバ チャネル ポートにすることはできません。
- ポートをイーサネットからファイバチャネルに、またはその逆に変換する場合は、スイッチをリロードする必要があります。Currently, you can convert only one contiguous range of ports to Fibre Channel ports, and this range must be a multiple of 4, ending with a port number that is a multiple of 4.現時点で変換できるのは、ファイバ チャネル ポートの連続した範囲のポートだけです。そしてこの範囲は 4 の倍数である必要があり、最後のポート番号は 4 の倍数になっている必要があります。たとえば、1 ～ 4、1 ～ 8、21 ～ 24 などです。
- Brocade ポート ブレード ファイバ チャネル 16 ～ 32 へのファイバ チャネル アップリンク（NP）接続は、Cisco N9K-93180YC-FX リーフ スイッチ ポートが 8G の速度で設定されている場合はサポートされません。
- 選択したポートの速度が SFP によってサポートされている必要があります。たとえば、32G の SFP は 8/16/32G をサポートするため、4G のポート速度には 8G または 16G の SFP が必要です。16G の SFP のサポートは 4/8/16G であるため、32G のポート速度には 32G の SFP が必要です。
- 速度の自動ネゴシエーションがサポートされています。デフォルトの速度は「auto」です。
- 40G およびブレークアウト ポートではファイバ チャネルを使用できません。
- FEX を FC ポートに直接接続することはできません。
- FEX HIF ポートを FC に変換することはできません。
- 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。

ファイバチャネルNポート仮想化でサポートされるハードウェア

ファイバ チャネル N ポート仮想化（FC NPV）は、次のスイッチでサポートされます。

- N9K-C93108TC-FX
- N9K-C93180YC-FX

次のファイバ チャネル Small Form-Factor Pluggable（SFP）トランシーバはサポートされています。

- DS-SFP-FC8G-SW：2/4/8G（2G の FC NPV ポート速度はサポート外）
- DS-SFP-FC16G-SW：4/8/16G（FC NPV ポート速度が 32G の場合は非互換）
- DS-SFP-FC32G-SW：8/16/32G（FC NPVポート速度が 4G の場合は非互換）

サポートされている NPIV コア スイッチは、Cisco Nexus 5000 シリーズ、Nexus 6000 シリーズ、Nexus 7000 シリーズ（FCoE）、および Cisco MDS 9000 シリーズ マルチレイヤ スイッチです。

ファイバ チャネル N ポート仮想化の相互運用性

次の表に、Cisco Application Policy Infrastructure Controller（APIC）のファイバ チャネル N ポート仮想化（FC NPV）機能の相互運用性がテストされたサード パーティ製品を示します。

表 *6 : FC NPV* でサポートされるサード パーティ製品

サード パーティ スイッチ ベンダー	Brocade
サード パーティ ハードウェア モデル	DS-6620B
サード パーティ ソフトウェア リリース	8.2.1a
Cisco NX-OS リリース	14.1(1) 以降
Cisco Nexus 9000 モデル	N9K-C93180YC-FX
相互運用性モード	NA（NPV）
Cisco SFP モジュール	DS-SFP-FC32G-SW
サード パーティ **SFP** モジュール	Brocade-32G

ファイバ チャネル NPV GUI の設定

GUI を使用したネイティブ ファイバ チャネル ポート プロファイルの設定

この手順では、ファイバチャネルのホスト（サーバなど）に接続するための一連のネイティブ ファイバ チャネル（FC）F ポートの設定を行います。

設定を簡単に行うため、この手順では **[Configure Interface, PC, and vPC]** ウィザードを使用します。

手順

ステップ 1 APIC メニュー バーで、**[Fabric] > [Access Policies] > [Quickstart]** に移動し、*[Configure an interface, PC, and vPC]* をクリックします。

ステップ 2 [Configured Switch Interfaces] ツールバーで、[+] をクリックしてスイッチ プロファイルを作成します。次のアクションを実行します。

このスイッチ プロファイルでは、サーバ ホスト ポートを設定します。別のスイッチ プロファイルでは、アップリンク ポートを設定します。

a) [Switches] ドロップダウンリストで、NPV リーフ スイッチを選択します。

この操作によって、自動的にリーフ スイッチ プロファイルが作成されます。[Switch Profile Name] テキスト ボックスで、リーフ スイッチ プロファイルの名前を受け入れるか変更できます。

b) さらにインターフェイス設定を開くには、ポートで大きな緑色の [+] をクリックします。

c) [Interface Type] で、[FC] を選択して、ファイバ チャネル ホスト インターフェイス ポート（F ポート）を指定します。

d) [Interfaces] で、FC ポートのポート範囲を入力します。

FC ポートに変換できるポートの連続範囲は 1 つだけです。この範囲は 4 の倍数にする必要があり、4 の倍数のポート番号で終わる必要があります（たとえば、1 ～ 4、1 ～ 8、21 ～ 24 は有効な範囲です）。

この操作によってインターフェイス セレクタ ポリシーが作成されます。[Interface Selector Name] テキスト ボックスで、ポリシーの名前を受け入れるか変更できます。

（注）
イーサネットから FC へのポートの変換には、スイッチのリロードが必要です。インターフェイス ポリシーを適用すると、スイッチをリロードするよう求める通知アラームが GUI に表示されます。スイッチのリロード中はスイッチへの通信が中断され、スイッチにアクセスしようとするとタイムアウトになります。

e) [Policy Group Name] ドロップダウンリストで、[Create FC Interface Policy Group] を選択します。

f) [Create FC Interface Policy Group] ダイアログボックスで、[Name] フィールドに名前を入力します。

g) [Fibre Channel Interface Policy] ドロップダウンリストで、[Create Fibre Channel Interface Policy] を選択します。

h) [Create Fibre Channel Interface Policy] ダイアログボックスで、[Name] フィールドに名前を入力し、次の設定を行います。

フィールド	設定
ポート モード	ホスト インターフェイスの場合、[F] を選択します。
Trunk Mode	ホストインターフェイスの場合、[trunk-off] を選択します。
速度	[auto]（デフォルト）を選択します。
[自動最大速度 (Auto Max Speed)]	Auto Max Speed設定は、速度が **auto** の場合にのみ適用されます。 [Auto Max Speed]は、速度が自動モードのときに最大速度を制限します。
Receive Buffer Credit	[64] を選択します。

i) [Submit]をクリックして、ファイバチャネルインターフェイスポリシーを保存し、[Create FC Interface PolicyGroup] ダイアログボックスに戻ります。

j) [Attached Entity Profile] ドロップダウンリストで、[Create Attachable Access Entity Profile] を選択します。

アタッチ可能なエンティティ プロファイルのオプションでは、リーフ アクセス ポートポリシーを展開するインターフェイスを指定します。

k) [Name] フィールドに、アタッチ可能なエンティティのポリシーの名前を入力します。

l) [Domains（VMM, Physical, or External）To Be Associated To Interfaces] ツールバーで、[+] をクリックしてドメイン プロファイルを追加します。

m) [Domain Profile] ドロップダウンリストで、[Create Fibre Channel Domain] を選択します。

n) [Name] フィールドに、ファイバ チャネル ドメインの名前を入力します。

o) [VSAN Pool] ドロップダウンリストで、[Create VSAN Pool] を選択します。

p) [Name] フィールドに、VSAN プールの名前を入力します。

q) [Encap Blocks] ツールバーで、[+] をクリックして VSAN 範囲を追加します。

r) [Create VSAN Ranges] ダイアログボックスで、[From] および [To] の VSAN 番号を入力します。

s) [Allocation Mode] で、[Static Allocation] を選択し、[OK] をクリックします。

t) [Create VSAN Ranges] ダイアログボックスで、[Submit] をクリックします。

u) [Create Fibre Channel Domain] ダイアログボックスで、[Submit] をクリックします。

（注）
ファイバチャネル ドメインでは、FCoE ではなくネイティブ FC ポートを使用する場合、VLAN プールや VSAN 属性を設定する必要はありません。

v) [Create Attachable Access Entity Profile] ダイアログボックスで、[Update] をクリックしてファイバ チャネル ドメイン プロファイルを選択し、[Submit] をクリックします。

w) [Create FC Policy Group] ダイアログボックスで、[Submit] をクリックします。

x) **[Configure Interface、PC、and vPC]** ダイアログ ボックスで、**[Save]** をクリックして、サーバー ホスト ポートのこのスイッチ プロファイルを保存します。

（注）
イーサネットから FC へのポートの変換には、スイッチのリロードが必要です。インターフェイス ポリシーを適用すると、スイッチをリロードするよう求める通知アラームが GUI に表示されます。スイッチのリロード中はスイッチへの通信が中断され、スイッチにアクセスしようとするとタイムアウトになります。

（注）
たとえば、アップリンクをダウンリンクとして再設定し、スイッチをリロードするなど、スイッチのポート プロファイルを変更すると、スイッチが Cisco APIC から設定を取得するまで、スイッチとの通信が中断されます。

[Fabric] > [Access Policies] > [Switches] > [Leaf Switches] > [Profiles] > [<名前>] で、[Leaf Profiles] 作業ペインの [Associated Interface Selector Profiles] リストにファイバ チャネル ポート プロファイルが表示されます。

次のタスク

- ファイバ チャネル アップリンク接続プロファイルを設定します。
- テナント内のサーバ ポートとアップリンク ポートを展開し、ファイバ チャネルのコア スイッチに接続します。

GUI を使用したネイティブ FC ポート チャネル プロファイルの設定

この手順では、ファイバ チャネルのコア スイッチへのアップリンク接続に使用するネイティブ ファイバ チャネル ポート チャネル（FC PC）プロファイルを設定します。

（注） この手順は、**[Configure Interface, PC, and vPC]** ウィザードを使用して実行することもできます。

始める前に

アタッチ可能なエンティティ プロファイルを含む、アップリンク接続を設定します。

手順

ステップ 1 [Fabric] > [Access Policies] > [Interfaces] > [Leaf Interfaces] > [Profiles] の順に展開します。

ステップ 2 [Profiles] を右クリックし、[Create Leaf Interface Profile] をクリックします。

ステップ 3 [Create Leaf Interface Profile] ダイアログボックスで、次の手順を実行します。

a) [Name] フィールドに、リーフ インターフェイス プロファイルの名前を入力します。

b) [Interface Selectors] ツールバーで、[+] をクリックして [Create Access Port Selector] ダイアログボックスを表示します。

c) [Name] フィールドに、ポート セレクタの名前を入力します。

d) [Interface IDs] フィールドで、FC PC ポートのポート範囲を入力します。

ポート チャネルには最大 16 個のポートを持たせることができます。

FC ポートに変換できるポートの連続範囲は 1 つだけです。この範囲は 4 の倍数にする必要があり、4 の倍数のポート番号で終わる必要があります（たとえば、1 ～ 4、1 ～ 8、21 ～ 24 は有効な範囲です）。

（注）
イーサネットから FC へのポートの変換には、スイッチのリロードが必要です。インターフェイス ポリシーを適用すると、スイッチを手動でリロードするよう求める通知アラームが GUI に表示されます。スイッチのリロード中はスイッチへの通信が中断され、スイッチにアクセスしようとするとタイムアウトになります。

e) [Interface Policy Group] ドロップダウンリストで、[Create FC PC Interface Policy Group] を選択します。

f) [Name] フィールドに、FC PC インターフェイス ポリシー グループの名前を入力します。

g) [Fibre Channel Interface Policy] ドロップダウンリストで、[Create Fibre Channel Interface Policy] を選択します。

h) [Name] フィールドに、FC PC インターフェイス ポリシーの名前を入力します。

i) [Create Interface FC Policy] ダイアログボックスで、[Name] フィールドに名前を入力し、次の設定を行います。

フィールド	設定
ポート モード	アップリンク インターフェイスの場合、[NP] を選択します。
Trunk Mode	アップリンク インターフェイスの場合、[trunk-on] を選択します。

j) [Submit] をクリックして、FC PC インターフェイス ポリシーを保存し、[Create FC PC Interface Policy Group] ダイアログボックスに戻ります。

k) **Port Channel Policy** ドロップで、**Create Port Channel Policy** を選択します。
l) [Name] フィールドに、ポート チャネル ポリシーの名前を入力します。

このメニューにある他の設定は無視できます。

m) [Submit] をクリックして、ポート チャネル ポリシーを保存し、[Create FC PC Interface Policy Group] ダイアログボックスに戻ります。
n) [Attached Entity Profile] ドロップダウンリストで、既存のアタッチ可能なエンティティ プロファイルを選択します。
o) [Submit] をクリックして [Create Access Port Selector] ダイアログボックスに戻ります。
p) [OK] をクリックして [Create Leaf Interface Profile] ダイアログボックスに戻ります。
q) [OK] をクリックして [Leaf Interfaces - Profiles] 作業ペインに戻ります。

ステップ 4 [Fabric] > [Access Policies] > [Switches] > [Leaf Switches] > [Profiles] の順に展開します。

ステップ 5 作成したリーフ スイッチ プロファイルを右クリックし、[Create Interface Profile] をクリックします。

ステップ 6 [Create Interface Profile] ダイアログボックスで、次の手順を実行します。

a) [Interface Select Profile] ドロップダウンリストで、ポート チャネル用に作成したリーフ インターフェイス プロファイルを選択します。
b) [Submit] をクリックして [Leaf Interfaces - Profiles] 作業ペインに戻ります。

（注）
イーサネットから FC へのポートの変換には、スイッチのリロードが必要です。インターフェイス ポリシーを適用すると、スイッチをリロードするよう求める通知アラームが GUI に表示されます。スイッチのリロード中はスイッチへの通信が中断され、スイッチにアクセスしようとするとタイムアウトになります。

[Fabric] > [Access Policies] > [Switches] > [Leaf Switches] > [Profiles] > [<名前>] で、作業ペインの [Associated Interface Selector Profiles] リストに FC ポート チャネル プロファイルが表示されます。

次のタスク

テナント内のサーバ ポートとアップリンク ポートを展開し、ファイバ チャネルのコア スイッチに接続します。

ファイバ チャネル ポートの展開

この手順では、ファイバ チャネル サーバ ホスト ポートとアップリンク ポートをアクティブにします。

始める前に

- ファイバ チャネル（FC）サーバ ホスト ポート プロファイル（F ポート）を設定します。
- FC アップリンク ポート プロファイル（NP または TNP ポート）を設定します。

- 関連付けられている 2 つのインターフェイス セレクタ プロファイル（1 つはホスト ポート用、1 つはアップリンク ポート用）を含むリーフ スイッチプロファイルを設定します。

手順

ステップ 1 [Tenants] > [<テナント名>] > [Application Profiles] の順に展開します。

テナントが存在しない場合は、テナントを作成する必要があります。

ステップ 2 [Application Profiles] を右クリックし、[Create Application Profile] をクリックして、次の操作を実行します。

a) [Name] フィールドに、アプリケーション プロファイルの名前を入力します。
b) [Submit] をクリックします。

ステップ 3 [Tenants] > [<テナント名>] > [Application Profiles] > [<名前>] > [Application EPGs] の順に展開します。

ステップ 4 [Application EPGs] を右クリックし、[Create Application EPG] をクリックして、次の操作を実行します。

ステップ 5 [Create Application EPG] ダイアログボックスで、次の操作を実行します。

a) [Name] フィールドに、アプリケーション EPG の名前を入力します。
b) 次を設定します。

フィールド	設定
Intra EPG Isolation	[Unenforced] を選択します。
Preferred Group Member	[Exclude] を選択します。
カプセル化のフラッディング	[Disabled] を選択します。

c) [Bridge Domain] ドロップダウンリストで、[Create Bridge Domain] を選択します。
d) [Name] フィールドに、ブリッジ ドメインの名前を入力します。
e) [Type] で、[fc] を選択してファイバ チャネル ブリッジ ドメインを指定します。
f) [VRF] ドロップダウンリストで、[Create VRF] を選択します。
g) [Name] フィールドに、VRF の名前を入力します。
h) [Submit] をクリックして [Create Bridge Domain] ダイアログボックスに戻ります。
i) [Next]、[Next]、[Finish] の順にクリックして [Create Application EPG] ダイアログボックスに戻ります。
j) [Finish] をクリックします。

ステップ 6 [Tenants] > [<テナント名>] > [Application Profiles] > [<名前>] > [Application EPGs] > [<名前>] > [Domains（VMs and Bare-Metals）] の順に展開します。

ステップ 7 [Domains（VMs and Bare-Metals）] を右クリックし、[Add Fibre Channel Domain Association] をクリックして、次の操作を実行します。

a) [Fibre Channel Domain Profile] ドロップダウンリストで、ホスト ポートの設定時に作成したファイバ チャネル ドメインを選択します。
b) [Submit] をクリックします。

ステップ 8 [Tenants] > [<テナント名>] > [Application Profiles] > [<名前>] > [Application EPGs] > [<名前>] > [Fibre Channel（Paths）] の順に展開し、次の操作を実行します。

このステップでは、サーバ ホスト ポートを展開します。

a) [Fibre Channel（Paths）] を右クリックし、[Deploy Fibre Channel] をクリックします。
b) [Path Type] コントロールで、[Port] をクリックします。
c) [Node] ドロップダウンリストで、リーフ スイッチを選択します。
d) [Path] ドロップダウンリストで、サーバ ホスト ポートとして設定されているリーフ スイッチ ポートを選択します。
e) [VSAN] フィールドに、ポートの VSAN を入力します。
f) [VSAN Mode] コントロールで、[Native] をクリックします。
g) [Type] が fcoe であることを確認します。
h) （オプション）トラフィック マップを必要とする場合は、[Pinning Label] ドロップダウンリストを使用します。

（注）
複数のアップリンク ポートが使用可能で、ホスト ポートにおいて常にその FLOGI を特定のアップリンクに送るようにする場合は、固定プロファイル（トラフィック マップ）を作成してホスト ポートをアップリンク ポートに関連付けることができます。そのようにしない場合は、使用可能なアップリンク ポート間でホストがロードバランスされます。

i) [Submit] をクリックします。
j) ファイバ チャネル ポート ホストごとに**ステップ a** から繰り返します。

ステップ 9 [Tenants] > [<テナント名>] > [Application Profiles] > [<名前>] > [Application EPGs] > [<名前>] > [Fibre Channel（Paths）] の順に展開し、次の操作を実行します。

このステップでは、アップリンク ポート チャネルを展開します。

a) [Fibre Channel（Paths）] を右クリックし、[Deploy Fibre Channel] をクリックします。
b) [Path Type] コントロールで、[Direct Port Channel] をクリックします。
c) [Port Type] ドロップダウンリストで、アップリンク ポートチャネルを選択します。
d) [VSAN] フィールドに、ポートのデフォルトの VSAN を入力します。
e) [VSAN Mode] コントロールで、ポートの VSAN の場合は [Native] をクリックし、トランクの VSAN の場合は [Regular] をクリックします。
f) [Type] が fcoe であることを確認します。
g) [Submit] をクリックします。`
h) ファイバ チャネル アップリンク ポートまたはポート チャネルごとに**ステップ a** から繰り返します。

ファイバ チャネル ポートのトラフィック マップの設定

複数のアップリンク ポートが使用可能なアプリケーションでは、デフォルトで、サーバ トラフィックが使用可能なアップリンク ポート間でロードバランスされます。場合によっては、1 つ以上の特定のアップリンク ポートまたはポート チャネルにログイン要求（FLOGI）を送信するようサーバを設定する必要があります。このような場合、固定プロファイル（トラフィック マップ）を作成して、それらのアップリンク ポートまたはポート チャネルにサーバ ポートを関連付けることができます。

この手順では、1 つ以上のサーバ ポートと 1 つ以上のアップリンク ポートまたはポート チャネルがすでに設定済みであると仮定します。サーバ ポートがすでに設定済みであるため、最初に、アップリンクにマッピングするすべてのサーバ ポートをシャットダウン（無効化）する必要があります。トラフィック マップを設定した後で、再度ポートを有効にします。

始める前に

この手順では、次の項目がすでに設定済みであることを前提としています。

- サーバ ポート（F ポート）およびアップリンク ポートまたはポート チャネル（NP ポート）
- テナント（アプリケーション プロファイルおよびアプリケーション EPG を含む）

（注） 固定プロファイル（トラフィック マップ）を作成する前に、アップリンクにマッピングするサーバ ポートをシャットダウンする必要があります。

手順

ステップ 1 [Fabric] > [Inventory] > [Pod <n>] > [Leaf <n>] > [Interfaces] > [FC Interfaces] 作業ウィンドウを選択し、アップリンクにマッピングするサーバ インターフェイス ポートを選択して無効にします。

ステップ 2 [Tenants] > [<テナント名>] > [Application Profiles] > [<アプリケーション プロファイル名>] > [Application EPGs] > [<EPG 名>] > [Fibre Channel（Paths）] の順に展開し、次の操作を実行します。

a) [Fibre Channel（Paths）] を右クリックし、[Deploy Fibre Channel] をクリックします。
b) [Path Type] コントロールで、[Port] をクリックします。
c) [Node] ドロップダウンリストで、リーフ スイッチを選択します。
d) [Path] ドロップダウンリストで、特定のアップリンク ポートにマッピングするサーバ ポートを選択します。
e) [VSAN] フィールドに、ポートのデフォルトの VSAN を入力します。
f) [VSAN Mode] コントロールで、[Native] をクリックします。
g) [Type] が fcoe であることを確認します。

h) [Pinning Label] ドロップダウンリストで、[Create Pinning Profile] を選択します。
i) [Name] フィールドに、トラフィック マップの名前を入力します。
j) [Path Type] コントロールで、[Port] をクリックして単一の NP アップリンク ポートに接続するか、[Direct Port Channel] をクリックして FC ポート チャネルに接続します。

パスの種類で [Port] を選択した場合は、表示される [Node] ドロップダウンリストでリーフ スイッチを選択する必要もあります。

パスの種類で [Direct Port Channel] を選択した場合は、インターフェイス ポリシー グループで定義した FC PC を選択する必要もあります。

k) [Path] ドロップダウンリストで、サーバ ポートをマッピングするアップリンク ポートまたはポート チャネルを選択します。
l) [Submit] をクリックして [Deploy Fibre Channel] ダイアログボックスに戻ります。
m) [Submit] をクリックします。`

ステップ 3 [Fabric] > [Inventory] > [Pod <n>] > [Leaf <n>] > [Interfaces] > [FC Interfaces] 作業ウィンドウを選択し、アップリンクにマッピングするサーバ インターフェイス ポートを選択して再び有効にします。

ファイバ チャネル NPV NX-OS スタイル CLI の設定

CLI を使用したファイバ チャネル インターフェイスの設定

NPV 対応リーフ スイッチでは、ユニバーサル ポートをファイバ チャネル（FC）ポートに変換することができます。FC ポートは F ポートまたは NP ポートのどちらかにすることができ、NP ポートではポート チャネルを形成できます。

手順

ステップ 1 ポートの範囲をイーサネットからファイバ チャネルに変換します。

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# slot 1
apic1(config-leaf-slot)# port 1 12 type fc
```

この例では、リーフ 101 のポート 1/1-12 をファイバ チャネル ポートに変換します。**[no]** 形式の **port type fc** コマンドで、ポートをファイバ チャネルから再びイーサネットに変換します。

（注）
ポートの変換はリーフ スイッチのリブート後にのみ行われます。

現在のところ、FC ポートに変換できるポートの連続範囲は 1 つだけです。この範囲は 4 の倍数にする必要があり、4 の倍数のポート番号で終わる必要があります（例：1 ～ 4、1 ～ 8、21 ～ 24）。

ステップ 2 すべてのファイバ チャネル インターフェイスを設定します。

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# interface fc 1/1
apic1(config-leaf-fc-if)# switchport mode [f | np]
apic1(config-leaf-fc-if)# switchport rxbbcredit <16-64>
apic1(config-leaf-fc-if)# switchport speed [16G | 32G | 4G | 8G | auto | unknown]
apic1(config-leaf-fc-if)# switchport trunk-mode [ auto | trunk-off | trunk-on | un-init]
apic1(config-leaf-fc-if)# switchport [trunk allowed] vsan <1-4093> tenant <name>  \
                              application <name> epg <name>
```

（注）
FC ホスト インターフェイス（F ポート）は、8Gbps の速度設定をサポートしていません。

FC インターフェイスは、アクセス モードまたはトランク モードで設定できます。FC ポートをアクセス モードに設定するには、次のコマンド形式を使用します。

例：

```
apic1(config-leaf-fc-if)# switchport vsan 2 tenant t1 application a1 epg e1
```

FC ポートをトランク モードに設定するには、次のコマンド形式を使用します。

例：

```
apic1(config-leaf-fc-if)# switchport trunk allowed vsan 4 tenant t1 application a1 epg
e1
```

FC ポート チャネルを設定するには、FC ポート インターフェイス テンプレートを設定し、FC ポートチャネルのメンバーになる FC インターフェイスに適用します。

ポート チャネルには最大 16 個のメンバーを持たせることができます。

例：

```
apic1(config)# template fc-port-channel my-fc-pc
apic1(config-fc-po-ch-if)# lacp max-links 4
apic1(config-fc-po-ch-if)# lacp min-links 1
apic1(config-fc-po-ch-if)# vsan-domain member dom1
apic1(config-fc-po-ch-if)# exit
apic1(config)# leaf 101
apic1(config-leaf)# interface fc 1/1-2
apic1(config-leaf-fc-if)# fc-channel-group my-fc-pc
apic1(config-leaf-fc-if)# exit
apic1(config-leaf)# interface fc-port-channel my-fc-pc
apic1(config-leaf-fc-pc)# switchport mode [f | np]
apic1(config-leaf-fc-pc)# switchport rxbbcredit <16-64>
```

```
apic1(config-leaf-fc-pc)# switchport speed [16G | 32G | 4G | 8G | auto | unknown]
apic1(config-leaf-fc-pc)# switchport trunkmode [ auto | trunk-off | trunk-on | un-init]
```

CLI を使用したファイバ チャネル NPV ポリシーの設定

始める前に

NPV アプリケーションで使用するリーフ スイッチ ポートをファイバ チャネル（FC）ポートに変換した。

手順

ステップ 1 ファイバ チャネル F ポート ポリシー グループのテンプレートを作成します。

例：

```
apic1(config)# template fc-policy-group my-fc-policy-group-f-ports
apic1(config-fc-pol-grp-if)# vsan-domain member dom1
apic1(config-fc-pol-grp-if)# switchport mode f
apic1(config-fc-pol-grp-if)# switchport trunk-mode trunk-off
```

速度など、他のスイッチ ポート設定を行うことができます。

ステップ 2 ファイバ チャネル NP ポート ポリシー グループのテンプレートを作成します。

例：

```
apic1(config)# template fc-policy-group my-fc-policy-group-np-ports
apic1(config-fc-pol-grp-if)# vsan-domain member dom1
apic1(config-fc-pol-grp-if)# switchport mode np
apic1(config-fc-pol-grp-if)# switchport trunk-mode trunk-on
```

速度など、他のスイッチ ポート設定を行うことができます。

ステップ 3 ファブリック全体のファイバ チャネル ポリシーを作成します。

例：

```
apic1(config)# template fc-fabric-policy my-fabric-fc-policy
apic1(config-fc-fabric-policy)# fctimer e-d-tov 1000
apic1(config-fc-fabric-policy)# fctimer r-a-tov 5000
apic1(config-fc-fabric-policy)# fcoe fcmap 0E:FC:01
```

ステップ 4 ファイバ チャネル ポート チャネル ポリシーを作成します。

例：

```
apic1(config)# template fc-port-channel my-fc-pc
```

```
apic1(config-fc-po-ch-if)# lacp max-links 4
apic1(config-fc-po-ch-if)# lacp min-links 1
apic1(config-fc-po-ch-if)# vsan-domain member dom1
```

ステップ 5 リーフ全体のファイバ チャネル ポリシー グループを作成します。

例：

```
apic1(config)# template fc-leaf-policy my-fc-leaf-policy
apic1(config-fc-leaf-policy)# npv auto-load-balance disruptive
apic1(config-fc-leaf-policy)# fcoe fka-adv-period 10
```

（注）
ここに示すポリシー コマンドは単なる例であり、必須の設定ではありません。

ステップ 6 リーフ ポリシー グループを作成します。

```
apic1(config)# template leaf-policy-group lpg1
apic1(config-leaf-policy-group)# inherit fc-fabric-policy my-fabric-fc-policy
apic1(config-leaf-policy-group)# inherit fc-leaf-policy my-fc-leaf-policy
```

FC 関連のポリシーを継承することによって、リーフ ポリシー グループが作成されます。

ステップ 7 リーフ プロファイルを作成し、リーフポリシーグループをリーフグループに適用します。

例：

```
apic1(config)# leaf-profile my-leaf-profile
apic1(config-leaf-profile)# leaf-group my-leaf-group
apic1(config-leaf-group)# leaf 101
apic1(config-leaf-group)# leaf-policy-group lpg1
```

この例では、リーフ ポリシー グループ lpg1 にグループ化された、ファブリック全体の FC ポリシーとリーフ全体の FC ポリシーを、リーフ 101 に適用します。

ステップ 8 リーフ インターフェイス プロファイルを作成し、fc ポリシーグループを一組の FC インターフェイスに適用します。

例：

```
apic1(config)# leaf-interface-profile my-leaf-interface-profile
apic1(config-leaf-if-profile)# leaf-interface-group my-leaf-interface-group
apic1(config-leaf-if-group)# fc-policy-group my-fc-policy-group-f-ports
apic1(config-leaf-if-group)# interface fc 1/1-10
```

CLI を使用した NPV トラフィック マップの設定

この手順では、FC/FCoE サーバ（ホスト）インターフェイスから NP モードに設定された FC/FCoE 外部（アップリンク）インターフェイスに送信されるトラフィックをマッピングします。

始める前に

すべてのサーバ インターフェイスが F ポートである必要があり、すべてのアップリンク インターフェイスが NP ポートである必要があります。

手順

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# npv traffic-map server-interface  \
    { vfc <slot/port> | vfc-po <po-name> |fc <slot/port> } \
    label <name> tenant <tn> app <ap> epg <ep>
apic1(config-leaf)# npv traffic-map external-interface \
    { vfc <slot/port> | vfc-po <po-name> |fc <slot/port> } \
    tenant <tn> label <name>
```

例：

```
apic1(config)# leaf 101
apic1(config-leaf)# npv traffic-map server-interface vfc 1/1 label serv1 tenant t1 app
ap1 epg epg1
apic1(config-leaf)# npv traffic-map external-interface vfc-po my-fc-pc tenant t1 label
ext1
```

ファイバ チャネル NPV REST API の設定

REST API を使用した FC 接続の設定

FC が有効なインターフェイスと Epg REST API を使用して、FC プロトコルを使用してこれらのインターフェイスへのアクセスを設定することができます。

手順

ステップ 1 VSAN プールを作成するには、次の例などと XML post を送信します。この例では、VSAN プール myVsanPool1 を作成し、vsan-50 から vsan-60 までを含むように VSAN の範囲を指定します。

例：

```
https://apic-ip-address/api/mo/uni/infra/vsanns-[myVsanPool1]-static.xml

<fvnsVsanInstP allocMode="static" name="myVsanPool1">
  <fvnsVsanEncapBlk from="vsan-50" name="encap" to="vsan-60"/>
</fvnsVsanInstP>
```

ステップ 2 ファイバ チャネル ドメインを作成するには、次の例のように XML で post を送信します。この例では、ファイバチャネル ドメイン（VSAN ドメイン）myFcDomain1 を作成し、VSAN プール myVsanPool1 に関連付けます。

例：

```
https://apic-ip-address/api/mo/uni/fc-myFcDomain1.xml

<fcDomP name="myFcDomain1">
  <fcRsVsanNs tDn="uni/infra/vsanns-[myVsanPool1]-static"/>
</fcDomP>
```

ステップ 3 FC ポートのアタッチ エンティティ ポリシー（AEP）を作成するには、次の例のように XML で POST を送信します。この例では、AEP myFcAEP1 を作成し、ファイバ チャネル ドメイン myFcDomain1 に関連付けます。

例：

```
https://apic-ip-address/api/mo/uni.xml

<polUni>
<infraInfra>
    <infraAttEntityP name="myFcAEP1">
        <infraRsDomP tDn="uni/fc-myFcDomain1"/>
    </infraAttEntityP>
</infraInfra>
</polUni>
```

ステップ 4 サーバ ホスト ポートの FC インターフェイス ポリシーとポリシー グループを作成するには、XML で POST を送信します。この例は次の要求を実行します。

- サーバ ホスト ポートの FC インターフェイス ポリシー myFcHostIfPolicy1 を作成します。これらは、トランキングのない F ポートです。
- FC ホスト インターフェイス ポリシー myFcHostIfPolicy1 を含む FC インターフェイス ポリシー グループ myFcHostPortGroup1 を作成します。
- ポリシー グループを FC インターフェイス ポリシーに関連付けて、これらのポートを FC ポートに変換します。

- ホスト ポート プロファイル myFcHostPortProfile を作成します。
- ポートを 5 ～ 8 の範囲で指定するポート セレクタ myFcHostSelector を作成します。
- リーフ ノード 104 を指定するノード セレクタ myFcNode1 を作成します。
- リーフ ノード 104 を指定するノード セレクタ myLeafSelector を作成します。
- ホスト ポートをリーフ ノードに関連付けます。

例：

```
https://apic-ip-address/api/mo/uni.xml

<polUni>
    <infraInfra>
       <fcIfPol name="myFcHostIfPolicy1" portMode="f" trunkMode="trunk-off" speed="auto"/>

        <infraFuncP>
            <infraFcAccPortGrp name="myFcHostPortGroup1">
                <infraRsFcL2IfPol tnFcIfPolName="myFcHostIfPolicy1" />
            </infraFcAccPortGrp>
        </infraFuncP>
        <infraAccPortP name="myFcHostPortProfile">
            <infraHPortS name="myFcHostSelector" type="range">
                <infraPortBlk name="myHostPorts" fromCard="1" toCard="1" fromPort="1"
toPort="8" />
              <infraRsAccBaseGrp tDn="uni/infra/funcprof/fcaccportgrp-myFcHostPortGroup1"
 />
            </infraHPortS>
        </infraAccPortP>
        <infraNodeP name="myFcNode1">
            <infraLeafS name="myLeafSelector" type="range">
                <infraNodeBlk name="myLeaf104" from_="104" to_="104" />
            </infraLeafS>
            <infraRsAccPortP tDn="uni/infra/accportprof-myHostPorts" />
        </infraNodeP>
    </infraInfra>
</polUni>
```

（注）
この設定を適用する場合は、ポートを FC ポートとしてアップするためにスイッチのリロードが必要になります。

現在のみ FC ポートに変換できるポートの 1 つの連続した範囲と、この範囲にする必要がありますが 4 の倍数で終わるポート番号 4 の倍数ことです。たとえば、1 ～ 4、1 ～ 8、21 ～ 24 などです。

ステップ 5 アップリンク ポート チャネルの FC アップリンク ポート インターフェイス ポリシーとポリシー グループを作成するには、XML で POST を送信します。この例は次の要求を実行します。

- アップリンク ポートの FC インターフェイス ポリシー myFcUplinkIfPolicy2 を作成します。これらは、トランキングが有効になっている NP ポートです。
- FC アップリンク インターフェイス ポリシー myFcUplinkIfPolicy2 を含む FC インターフェイス バンドル ポリシー グループ myFcUplinkBundleGroup2 を作成します。

- ポリシー グループを FC インターフェイス ポリシーに関連付けて、これらのポートを FC ポートに変換します。
- アップリンク ポート プロファイル myFcUplinkPortProfile を作成します。
- ポートを 1/9 ～ 12 の範囲で指定するポート セレクタ myFcUplinkSelector を作成します。
- ホスト ポートをリーフ ノード 104 に関連付けます。

例：

```
https://apic-ip-address/api/mo/uni.xml

<polUni>
    <infraInfra>
        <fcIfPol name="myFcUplinkIfPolicy2" portMode="np" trunkMode="trunk-on"
speed="auto"/>
        <infraFuncP>
            <infraFcAccBndlGrp name="myFcUplinkBundleGroup2">
                <infraRsFcL2IfPol tnFcIfPolName="myFcUplinkIfPolicy2" />
            </infraFcAccBndlGrp>
        </infraFuncP>
        <infraAccPortP name="myFcUplinkPortProfile">
            <infraHPortS name="myFcUplinkSelector" type="range">
                <infraPortBlk name="myUplinkPorts" fromCard="1" toCard="1" fromPort="9"
 toPort="12" />
                <infraRsAccBaseGrp
tDn="uni/infra/funcprof/fcaccportgrp-myFcUplinkBundleGroup2" />
            </infraHPortS>
        </infraAccPortP>
        <infraNodeP name="myFcNode1">
            <infraLeafS name="myLeafSelector" type="range">
                <infraNodeBlk name="myLeaf104" from_="104" to_="104" />
            </infraLeafS>
            <infraRsAccPortP tDn="uni/infra/accportprof-myUplinkPorts" />
        </infraNodeP>
    </infraInfra>
</polUni>
```

（注）
この設定を適用する場合は、ポートを FC ポートとしてアップするためにスイッチのリロードが必要になります。

現在のみ FC ポートに変換できるポートの 1 つの連続した範囲と、この範囲にする必要がありますが 4 の倍数で終わるポート番号 4 の倍数ことです。たとえば、1 ～ 4、1 ～ 8、21 ～ 24 などです。

ステップ 6 テナント、アプリケーションプロファイル、EPG を作成し、FC ブリッジ ドメインを EPG に関連付けるするには、次の例などと XML post を送信します。例では、FC およびアプリケーション EPG epg1 をサポートするように設定されたターゲット テナントの下に、ブリッジ ドメイン myFcBD1 を作成します。これにより、ファイバ チャネル ドメイン myFcDomain1 とファイバ チャネル パスが、リーフ スイッチ 104 のインターフェイス 1/7 に関連付けられます。各インターフェイスは、VSAN に関連付けられます。

例：

```
https://apic-ip-address/api/mo/uni/tn-tenant1.xml
```

```
<fvTenant name="tenant1">
  <fvCtx name="myFcVRF"/>
  <fvBD name="myFcBD1" type="fc">
    <fvRsCtx tnFvCtxName="myFcVRF"/>
  </fvBD>
  <fvAp name="app1">
    <fvAEPg name="epg1">
      <fvRsBd tnFvBDName="myFcBD1"/>
      <fvRsDomAtt tDn="uni/fc-myFcDomain1"/>
      <fvRsFcPathAtt tDn="topology/pod-1/paths-104/pathep-[fc1/1]" vsan="vsan-50"
vsanMode="native"/>
      <fvRsFcPathAtt tDn="topology/pod-1/paths-104/pathep-[fc1/2]" vsan="vsan-50"
vsanMode="native"/>
    </fvAEPg>
  </fvAp>
</fvTenant>
```

ステップ 7 サーバ ポートをアップリンク ポートに固定するトラフィック マップを作成するには、次の例のように XML で POST を送信します。この例では、サーバ ポート vFC 1/47 をアップリンク ポート FC 1/7 に固定するトラフィック マップを作成します。

例：

```
https://apic-ip-address/api/mo/uni/tn-tenant1.xml

<fvTenant name="tenant1">
  <fvAp name="app1">
    <fvAEPg name="epg1">
      <fvRsFcPathAtt tDn="topology/pod-1/paths-104/pathep-[eth1/47]" vsan="vsan-50"
vsanMode="native">
        <fcPinningLbl name="label1"/>
      </fvRsFcPathAtt>
    </fvAEPg>
  </fvAp>
</fvTenant>

https://apic-ip-address/api/mo/uni/tn-vfc_t1.xml

<fvTenant name="tenant1">
  <fcPinningP name="label1">
    <fcRsPinToPath tDn="topology/pod-1/paths-104/pathep-[fc1/7]"/>
  </fcPinningP>
</fvTenant>
```

（注）
トラフィック マップの固定を初めて設定する場合は、最初のトラフィック マップを設定する前にサーバ ホスト ポートをシャットダウンする必要があります。

第 10 章

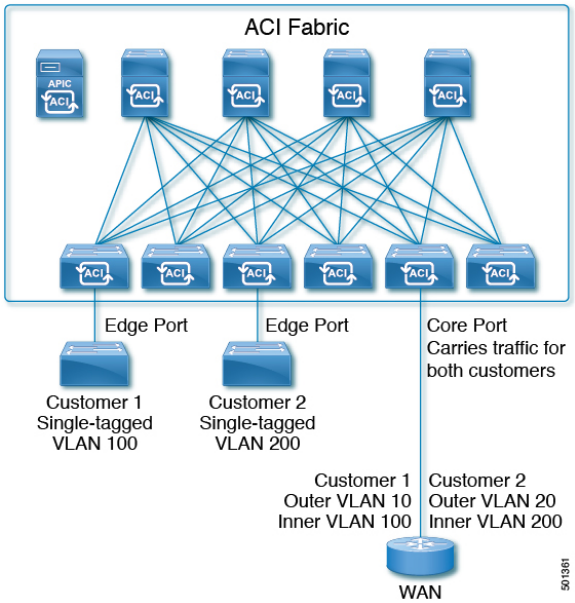
802.1 q トンネリング

この章は、次の内容で構成されています。

- ACI 802.1 q トンネルについて （229 ページ）
- GUI を使用した802.1Q トンネルの設定 （232 ページ）
- NX-OS スタイルの CLI を使用した 802.1Q トンネルの設定 （234 ページ）

ACI 802.1 q トンネルについて

図 *33 : 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 *7: 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 ドメインでフラッディングすることにより、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ディングします。
- 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。
- ブレークアウト ポートとして設定されているインターフェイスは、802.1 q をサポートしていません。
- 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。
- 802.1Q トンネルは、マルチポッド ファブリック全体でサポートされますが、マルチサイト全体ではサポートされません。

GUI を使用した802.1Q トンネルの設定

APIC GUI を使用した 802. 1 Q トンネル インターフェイスの設定

次の手順で、トンネルを使用するインターフェイスを設定します:

始める前に

トンネルを使用するテナントを作成します。

手順

ステップ 1 メニュー バーで、**[Fabric]** > **[Access Policies]** の順にクリックします。

ステップ 2 [ナビゲーション] バーで、**[ポリシー]** > **[インターフェイス]** > **[L2 インターフェイス]** をクリックします。

ステップ 3 **[L2 インターフェイス]** を右クリックし、**[L2 インターフェイス ポリシーの作成]** を選択して、次の操作を実行します。

a) **Name** フィールドに、レイヤ 2 インターフェイス ポリシーの名前を入力します。

b) オプション。ポリシーの説明を追加します。L2 インターフェイス ポリシーの目的を説明することをお勧めします。

c) **Dot1q トンネル**で、エッジ ポートとして使用するインターフェイスを有効にするインターフェイス ポリシーを作成するために、**QinQ** フィールドで、**edgePort** をクリックします。

d) **Dot1q トンネル**でコア ポートとして使用するインターフェイスを有効にするインターフェイス ポリシーを作成するために、**QinQ** フィールドで、**corePort** をクリックします。

ステップ 4 次の手順で、L2 インターフェイス ポリシーをポリシー グループに適用します。

a) **[ファブリック]** > **[アクセス ポリシー]** > **[インターフェイス]** > **[リーフ インターフェイス]**をクリックして、**[ポリシー グループ]** を展開します。

b) **[リーフ アクセス ポート]**、**[PC インターフェイス]** または **[VPC インターフェイス]** を右クリックし、トンネルに設定しているインターフェイスのタイプに応じて、次のいずれかを選択します。

- **リーフ アクセス ポート ポリシー グループの作成**
- **PC ポリシー グループの作成**
- **VPC ポリシー グループの作成**

c) 表示されるダイアログボックスで、以下のアクションを実行します:

- **Name** フィールドに、ポリシー グループの名前を入力します。

  オプション。ポリシー グループについての説明を追加します。ポリシー グループの目的を説明することをお勧めします。

- **L2 Interface Policy** フィールドで、下向き矢印をクリックし、前に作成した L2 インターフェイス ポリシーを選択します。
- CDP レイヤ 2 トンネリング プロトコルでトンネルを作成する場合は、[CDP Policy] 下向き矢印をクリックし、ポリシーダイアログボックスでポリシーの名前を追加し、管理状態を無効にして、[Submit] をクリックします。.
- LLDP レイヤ 2 トンネリング プロトコルでトンネルを作成する場合には、[LLDP Policy] 下向き矢印をクリックし、ポリシーダイアログボックスでポリシーの名前を追加し、送信状態を無効にして [submit] をクリックします。
- [Submit] をクリックします。

ステップ 5 次の手順に従ってリーフ インターフェイス プロファイルを作成します:

a) **[Fabric]** > **[Access Policies]** > **[Interfaces]** > **[Leaf Interfaces]** > **[Profiles]** をクリックします。

b) **Profiles** プロファイルを右クリックし、**Create Leaf Interface Profile** を選択し、次の手順に従います:

- **Name** フィールドに、**Leaf Interface Profile** の名前を入力します。

  オプション。説明を追加します。

- **Interface Selectors** フィールドで、**+** をクリックし、以下の情報を入力します:
  - **[名前]** フィールドに、インターフェイス セレクタの名前を入力します。

    オプション。説明を追加します。

  - **Interface IDs** フィールドに、このトンネルに含められる **Dot1q Tunnel** インターフェイス、または複数のインターフェイスの名前を入力します。
  - **Interface Policy Group** フィールドで、下向き矢印をクリックして、前に作成したインターフェイス ポリシー グループを選択します。

ステップ 6 トンネル設定のポートへのスタティック バインディングを作成するには、**[Tenant]** > **[Networking]** > **[Dot1Q Tunnels]** の順にクリックします。[Dot1Q Tunnels] を展開し、前に作成した **Dot1Q Tunnels <ポリシー名>** をクリックして、次の操作を実行します。

a) [Static Bindings] テーブルを展開して [Create Static Binding] ダイアログボックスを開きます。

b) [Port] フィールドで、ポートの種類を選択します。

c) [Node] フィールドで、ドロップダウンリストからノードを選択します。

d) [Path] フィールドで、ドロップダウンリストからインターフェイス パスを選択し、[Submit] をクリックします。

NX-OS スタイルの CLI を使用した 802.1Q トンネルの設定

NX-OS スタイル CLI を使用した802.1Q トンネルの設定

（注） **Dot1q トンネル** に含まれるインターフェイスのポート、ポート チャネル、仮想ポート チャネルを使用できます。手順の詳細にはポートの設定が含まれます。エッジおよびコア ポート チャネルと仮想ポート チャネルを設定するコマンドについては、下の例を参照してください。

次の手順で、**Dot1q トンネル** を作成し、NX-OS スタイル CLI を使用してトンネルで使用するインターフェイスを設定します。

（注） **Dot1q トンネル** には2 個以上のインターフェイスを含める必要があります。手順を繰り返し（または2個のインターフェイスをまとめて設定)、**Dot1q トンネル** で使用する各インターフェイスをマークします。この例で、2 個のインターフェイスは単一の顧客で使用されているエッジ スイッチ ポートとして設定されます。

次の手順を使用して、設定を次の手順を使用して、NX-OS スタイル CLI を使用して **Dot1q トンネル** を設定します。

1. トンネルで使用するインターフェイスを最低 2 個設定します。
2. **Dot1q トンネル** を作成します。
3. トンネルとすべてのインターフェイスを関連付けます。

始める前に

Dot1q トンネル を使用するテナントを設定します。

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`	コンフィギュレーションモードに入ります。
ステップ 2	次の手順により 802.1Q で使用するための 2 個のインターフェイスを設定します。	

	コマンドまたはアクション	目的
ステップ 3	**leaf** *ID* 例： `apic1(config)# leaf 101`	**Dot1q トンネル** のインターフェイスが配置されるリーフを特定します。
ステップ 4	**interface ethernet** *slot/port* 例： `apic1(config-leaf)# interface ethernet 1/13-14`	トンネルのポートとしてマークされるインターフェイスを特定します。

ステップ 5	**switchport mode dot1q-tunnel** {**edgePort** | **corePort**}
	例：
	`apic1(config-leaf-if)# switchport mode dot1q-tunnel edgePort`
	`apic1(config-leaf-if)# exit`
	`apic1(config-leaf)# exit`
	`apic1(config)# exit`
		802.1Q トンネルで使用するインターフェイスをマークして、設定モードをそのままにします。
		この例では、エッジポートを使用するためにいくつかのインターフェイス設定を示します。トンネルに複数のインターフェイスを設定するには、手順 3 ～ 5 を繰り返します。

ステップ 6	次の手順で 802.1q トンネルを作成します。	
ステップ 7	**leaf** *ID* 例： `apic1(config)# leaf 101`	インターフェイスが配置されているリーフに戻ります。
ステップ 8	**interface ethernet***slot/port* 例： `apic1(config-leaf)# interface ethernet 1/13-14`	トンネルに含まれるインターフェイスに戻ります。

ステップ 9	**switchport tenant***tenant-name***dot1q-tunnel** *tunnel-name*
	例：
	`apic1(config-leaf-if)# switchport tenant tenant64 dot1q-tunnel vrf64_edgetunnel`
	`apic1(config-leaf-if)# exit`
		トンネルにインターフェイスに関連付け、設定モードを終了します。

ステップ 10	トンネルとその他のインターフェイスを関連付けるには、ステップ 7 ～ 10 を繰り返します。	

例：NX-OS スタイル CLI でポートを使用する 802.1Q トンネルを設定する

この例では、2 つのポートを **Dot1q トンネル**で使用されるエッジ ポート インターフェイスとしてマークし、 さらに 2 つの ポートをコア ポート インターフェイスで使用されるものととしてマークし、トンネルを作成して、ポートをトンネルに関連付けます。

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/13-14
apic1(config-leaf-if)# switchport mode dot1q-tunnel edgePort
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config)leaf 102
apic1(config-leaf)# interface ethernet 1/10, 1/21
apic1(config-leaf-if)# switchport mode dot1q-tunnel corePort
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config)# tenant tenant64
apic1(config-tenant)# dot1q-tunnel vrf64_tunnel
apic1(config-tenant-tunnel)# l2protocol-tunnel cdp
apic1(config-tenant-tunnel)# l2protocol-tunnel lldp
apic1(config-tenant-tunnel)#  access-encap 200
apic1(config-tenant-tunnel)# mac-learning disable
apic1(config-tenant-tunnel)# exit
apic1(config-tenant)# exit
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/13-14
apic1(config-leaf-if)# switchport tenant tenant64 dot1q-tunnel vrf64_tunnel
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config)# leaf 102
apic1(config-leaf)# interface ethernet 1/10, 1/21
apic1(config-leaf-if)# switchport tenant tenant64 dot1q-tunnel vrf64_tunnel
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
```

例：NX-OS スタイル CLI でポート チャネルを使用する 802.1Q トンネルを設定する

例では、このエッジ ポート 8021 q インターフェイスとして 2 つのポート チャネルにマークし、2 つ以上のポート チャネルをコア ポート 802.1 q インターフェイスとしてマークして、**Dotq トンネル** を作成し、トンネルとポート チャネルを関連付けます。

```
apic1# configure
apic1(config)# tenant tenant64
apic1(config-tenant)# dot1q-tunnel vrf64_tunnel
apic1(config-tenant-tunnel)# l2protocol-tunnel cdp
apic1(config-tenant-tunnel)# l2protocol-tunnel lldp
apic1(config-tenant-tunnel)#  access-encap 200
apic1(config-tenant-tunnel)# mac-learning disable
apic1(config-tenant-tunnel)# exit
```

```
apic1(config-tenant)# exit
apic1(config)# leaf 101
apic1(config-leaf)# interface port-channel pc1
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface ethernet 1/2-3
apic1(config-leaf-if)# channel-group pc1
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface port-channel pc1
apic1(config-leaf-if)# switchport mode dot1q-tunnel edgePort
apic1(config-leaf-if)# switchport tenant tenant64 dot1q-tunnel vrf64_tunnel
apic1(config-tenant-tunnel)# exit
apic1(config-tenant)# exit
apic1(config)# leaf 102
apic1(config-leaf)# interface port-channel pc2
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface ethernet 1/4-5
apic1(config-leaf-if)# channel-group pc2
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface port-channel pc2
apic1(config-leaf-if)# switchport mode dot1q-tunnel corePort
apic1(config-leaf-if)# switchport tenant tenant64 dot1q-tunnel vrf64_tunnel
```

例：NX-OS スタイル CLI で仮想ポート チャネルを使用する 802.1Q トンネルを設定する

この例では、2 つの仮想ポート チャネル (vPC) を **Dot1q トンネル**の エッジポート 802.1Q インターフェイスとしてマークし、さらに2つのVPCをトンネルのためのコアポートインターフェイスとしてマークし、トンネルを作成して、仮想ポートチャネルをトンネルに関連付けています。

```
apic1# configure
apic1(config)# vpc domain explicit 1 leaf 101 102
apic1(config)# vpc context leaf 101 102
apic1(config-vpc)# interface vpc vpc1
apic1(config-vpc-if)# switchport mode dot1q-tunnel edgePort
apic1(config-vpc-if)# exit
apic1(config-vpc)# exit
apic1(config)# vpc domain explicit 1 leaf 103 104
apic1(config)# vpc context leaf 103 104
apic1(config-vpc)# interface vpc vpc2
apic1(config-vpc-if)# switchport mode dot1q-tunnel corePort
apic1(config-vpc-if)# exit
apic1(config-vpc)# exit
apic1(config)# tenant tenant64
apic1(config-tenant)# dot1q-tunnel vrf64_tunnel
apic1(config-tenant-tunnel)# l2protocol-tunnel cdp
apic1(config-tenant-tunnel)# l2protocol-tunnel lldp
apic1(config-tenant-tunnel)#  access-encap 200
apic1(config-tenant-tunnel)# mac-learning disable
apic1(config-tenant-tunnel)# exit
apic1(config-tenant)# exit
apic1(config)# leaf 103
apic1(config-leaf)# interface ethernet 1/6
apic1(config-leaf-if)# channel-group vpc1 vpc
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config)# leaf 104
```

例：NX-OS スタイル CLI で仮想ポート チャネルを使用する 802.1Q トンネルを設定する

```
apic1(config-leaf)# interface ethernet 1/6
apic1(config-leaf-if)# channel-group vpc1 vpc
apic1(config-leaf-if)# exit
apic1(config-leaf)# exit
apic1(config-vpc)# interface vpc vpc1
apic1(config-vpc-if)# switchport tenant tenant64 dot1q-tunnel vrf64_tunnel
apic1(config-vpc-if)# exit
```

第 11 章

Epg の Q-で-Q カプセル化のマッピング

- Epg の Q-で-Q カプセル化のマッピング （239 ページ）
- GUI を使用した EPG の Q-in-Q カプセル化マッピングの設定 （240 ページ）
- NX-OS スタイル CLI を使用した Q-in-Q カプセル化リーフ インターフェイスへの EPG のマッピング （244 ページ）

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、9300-FX2、および 9300-FX3 プラットフォーム スイッチでサポートされます。
- 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ディング」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

GUI を使用した EPG の Q-in-Q カプセル化マッピングの設定

GUI を使用して、特定のリーフ スイッチ インターフェイス上で Q-in-Q カプセル化を有効にします

リーフスイッチポート、PC、または vPC は、APIC GUI の次のいずれかの場所の **[インターフェイス (Interface)]** タブで Q-in-Q カプセル化モードを有効にします。

- **[Fabric]** > **[Inventory]** > **[Topology]**
- **[Fabric]** > **[Inventory]** > **[Pod]**
- **[Fabric]** > **[Inventory]** > **[Pod]** > ***[leaf-name]***

[Topology] タブまたは **[Pod Interface]** タブで **VPC** を設定します。

始める前に

Q-in-Q モードに設定されたインターフェイスでマッピングされるテナント、アプリケーションプロファイル、およびアプリケーション EPG を作成する必要があります。

手順

ステップ 1 メニューバーで **[Fabric** > **Inventory]** を選択し、**[Topology]**、**[Pod]** をクリックするか、**[Pod]** を展開してリーフを選択します。

ステップ 2 [Topology] タブ、または [Pod] パネルの [Interface] タブを選択します。

ステップ 3 **[Operation/Configuration]** トグル ボタンをクリックして、設定パネルを表示します。

ステップ 4 **[+]** をクリックしてリーフスイッチの図を追加し、1 つ以上のスイッチを選択して**[Add Selected]** をクリックします。

[<リーフ名>] パネルの [Interface] タブで、[Operation]/[Configuration] トグルボタンをクリックすると、自動的にスイッチのダイアグラムが表示されます。

ステップ 5 Q-in-Q カプセル化モードを有効にするインターフェイスをクリックします。

ステップ 6 ポートを設定するには、次の手順を実行します。

a) 左上の **L2** をクリックします。

b) L2 タブの **[L2 QinQ State]** フィールドで **[Double Q Tag Port]** をクリックし、**[Submit]** をクリックします。

ステップ 7 PCを設定するには、次の手順を実行します。

a) 左上の **PC** をクリックします。

b) **[Physical Interface]** タブで、**[Policy Group Name]** を入力します。

c) L2 タブの **[L2 QinQ State]** フィールドで **[Double Q Tag Port]** をクリックし、**[Submit]** をクリックします。

ステップ 8 vPC を設定するには、次のステップを実行します。

a) 2 つのリーフ スイッチ ダイアグラムで、VPC の 2 つのレッグのインターフェイスをクリックします。

b) **[vPC]** をクリックします。

c) **[Physical Interface]** タブで、**[Logical Pair ID]** (自動保護グループの識別子) を入力します。各保護グループには、固有の ID があります。ID は1～1000 の範囲です) および **[Policy Group Name]**。

d) L2 タブの **[L2 QinQ State]** フィールドで **[Double Q Tag Port]** をクリックし、**[Submit]** をクリックします。

GUI を使用したファブリック インターフェイス ポリシーでリーフ インターフェイスの Q-in-Q カプセル化の有効化

リーフ インターフェイス プロファイルを使用して、Q-in-Q カプセル化のリーフ インターフェイス、PC、および vPC を有効にします。

始める前に

Q-in-Q モードに設定されたインターフェイスでマッピングされるテナント、アプリケーション プロファイル、およびアプリケーション EPG を作成する必要があります。

手順

ステップ 1 メニュー バーで、**Fabric** > **External Access Policies** を選択します。

ステップ 2 [ナビゲーション] バーで、**[ポリシー]** > **[インターフェイス]** > **[L2 インターフェイス]** をクリックします。

ステップ 3 **[L2 インターフェイス]** を右クリックし、**[L2 インターフェイス ポリシーの作成]** を選択して、次の操作を実行します。

a) **[名前 }** フィールドに、レイヤ 2 インターフェイス ポリシーの名前を入力します。

b) オプション。ポリシーの説明を追加します。L2 インターフェイス ポリシーの目的を説明することをお勧めします。

c) Q-in-Q カプセル化を有効にするインターフェイス ポリシーを作成するには、**[QinQ]** フィールドで **[doubleQtagPort]** をクリックします。

d) [Submit] をクリックします。

ステップ 4 次の手順で、ポリシー グループに L2 インターフェイス ポリシーを適用されます。

a) **[ファブリック]** > **[外部アクセス ポリシー]** > **[インターフェイス]** > **[リーフ インターフェイス]** をクリックし、**[ポリシー グループ]** を展開します。

b) **[リーフ アクセス ポート]**、**[PC インターフェイス]**、または **[vPC インターフェイス]** を右クリックし、トンネルに設定するインターフェイスのタイプに応じて、次のいずれかを選択します。

- **リーフ アクセス ポート ポリシー グループの作成**
- **PC ポリシー グループの作成**
- **vPC ポリシー グループの作成**

c) 結果のダイアログボックスでポリシー グループ名を入力し、以前作成した L2 インターフェイス ポリシーを選択し、**[送信]** をクリックします。

ステップ 5 次の手順で、リーフ インターフェイス プロファイルを作成します。

a) **[ファブリック]** > **[外部アクセス ポリシー]** > **[インターフェイス]** > **[リーフ インターフェイス]** > **[プロファイル]** の順にクリックします。

b) **[リーフ プロファイル]** を右クリックして、**[リーフ インターフェイス ポリシーの作成]** を選択し、次の手順を実行します。

- **Name** フィールドに、**Leaf Interface Profile** の名前を入力します。

  オプション。説明を追加します。

- **[インターフェイス セレクタ]** フィールドで、**[+]** をクリックし、次の情報を入力します。

  - **[名前]** フィールドに、インターフェイス セレクタの名前を入力します。

    オプション。説明を追加します。

  - セレクタの名前とし、任意で説明を入力します。
  - インターフェイス ID フィールドに、プロファイルに含む単一または複数のインターフェイスを入力します。
  - **[インターフェイス ポリシー グループ]** フィールドで、以前作成したインターフェイス ポリシー グループを選択します。

GUI を使用して EPG から Q-in-Q カプセル化が有効なインターフェイスにマッピングする

EPF は、次のモデルのいずれかで Q-in-Q カプセルが有効なインターフェイスに関連付けることができます:

- 特定の Q-in-Q カプセル化が有効なインターフェイス上に静的な EPG を展開します。
- EPG を Q-in-Q カプセル化が有効なリーフ スイッチに静的にリンクします。
- EPG を Q-in-Q カプセル化が有効なエンドポイント (スタティック MAC アドレスを持つもの) に関連付けます

APIC GUI の同じエリアに 3 つすべてのタスクが実行されます。

始める前に

- Q-in-Q モードで構成されたインターフェイスにマッピングされるテナント、アプリケーション プロファイル、おおびアプリケーション EPG を作成します。
- ターゲット インターフェイスは Q-in-Q カプセル化で構成されている必要があります。

手順

ステップ 1 メニュー バーで、**Tenants** > ***tenant-name*** の順にクリックします。

ステップ 2 ナビゲーション ウィンドウで、**Application Profiles** > > ***application-profile-name*** > **Application EPGs** > ***application-EPG-name*** を展開します。

ステップ 3 Q-in-Q モードが有効になっているインターフェイス、PC、または vPC にスタティック EPG を展開するには、次の手順を実行します。

a) アプリケーション EPG の下で、**[スタティック ポート (Static Ports)]** を右クリックし、**[スタティック EPG を PC、vPC、またはインターフェイスに展開 (Deploy Static EPG on PC, vPC, or Interface)]** を選択します。

b) パスのタイプ、ノード、および Q-in-Q が有効になっているインターフェイスのパスを選択します。

c) **Port Encap (or Secondary VLAN for Micro-Seg)** フィールドで、 **QinQ** を選択し、EPG にマップされるトラフィックの外部および内部 VLAN タグを入力します。

d) [Submit] をクリックします。

ステップ 4 EPG をQ-in-Q モードが有効なノードに静的にリンクするには、次の手順を実行します:

a) アプリケーション EPG で、**Static Leafs** を右クリックして、**Statically Link With Node** を選択します。

b) [Node] フィールドで、リストから Q-in-Q が有効なスイッチを選択します。

c) [Encap] フィールドで、 **QinQ** を選択し、EPG の外部および内部 VLAN タグを入力します。

d) [Submit] をクリックします。

ステップ 5 EPG と静的エンドポイントを関連付けるには、次の手順を実行します:

a) アプリケーション EPG で、**Static EndPoints** を右クリックし、**Create Static EndPoint** を選択します。

b) インターフェイスの MAC アドレスを入力します。

c) パスのタイプ、ノード、および Q-in-Q カプセル化が有効になっているインターフェイスのパスを選択します。

d) オプション。エンドポイントの IP アドレスを追加します。

e) **Encap** フィールドで、**QinQ** を選択し、外部および内部 VLAN タグを入力します。

f) [送信（Submit）] をクリックします。

NX-OS スタイル CLI を使用した Q-in-Q カプセル化リーフ インターフェイスへの EPG のマッピング

Q-in-Q カプセル化のインターフェイスを有効にし、EPG にインターフェイスを関連付けます。

始める前に

Q-in-Q モードに設定されているインターフェイスでマッピングされるテナント、アプリケーション プロファイル、アプリケーション EPG を作成します。

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	**leaf** *number* 例： apic1(config)# leaf 101	設定するリーフを指定します。
ステップ 3	**interface ethernet***slot/port* 例： `apic1 (config-leaf)# interface ethernet 1/25`	設定するインターフェイスを指定します。
ステップ 4	**switchport mode dot1q-tunnel** doubleQtagPort 例： `apic1(config-leaf-if)# switchport mode dot1q-tunnel doubleQtagPort`	Q-in-Q カプセル化のインターフェイスを有効にします。
ステップ 5	**switchport trunkqinq outer-vlan***vlan-number* **inner-vlan** *vlan-number* **tenant** *tenant-name* **application** *application-name* **epg** *epg-name* 例： `apic1(config-leaf-if)# switchport trunk qinq outer-vlan 202 inner-vlan 203 tenant tenant64 application AP64 epg EPG64`	インターフェイスを EPG に関連付けます。

例

次の例では、リーフ インターフェイス 101/1/25 で Q-in-Q カプセル化を有効にして（VLAN ID 201 外部および VLAN ID 203 内部）、EPG64 にインターフェイスを関連付けます。

```
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/25
apic1(config-leaf-if)#switchport mode dot1q-tunnel doubleQtagPort
apic1(config-leaf-if)# switchport trunk qinq outer-vlan 202 inner-vlan 203 tenant tenant64
 application AP64 epg EPG64
```

第 12 章

ブレークアウト ポート

この章は、次の項で構成されています。

- ブレークアウト ポートの設定 （247 ページ）
- ダウンリンクのダイナミック ブレークアウト ポートの注意事項と制約事項 （248 ページ）
- ファブリック リンクの自動ブレークアウト ポートの注意事項と制約事項 （253 ページ）
- GUI を使用したプロファイルおよびセレクタによるブレークアウト ポートの構成 （256 ページ）
- GUI を使用したプロファイルおよびセレクタによるブレークアウト ポートの構成 （259 ページ）
- GUI を使用したインターフェイス コンフィギュレーションによるブレークアウト ポートの設定 （262 ページ）
- NX-OS スタイルの CLI を使用したダイナミック ブレイクアウト ポートの設定 （263 ページ）

ブレークアウト ポートの設定

ブレークアウト 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。ブレークアウトでは、40 ギガビット（Gb）ポートを 4 つの独立した論理 10 Gb ポートに分割すること、100Gb ポートを 4 つの独立した論理 25Gb ポートに分割するころ、または 400Gb ポートを 4 つの独立した論理 100Gb ポートに分割することができます。

スイッチのダウンリンク（アクセス側ポートまたはダウンリンク ポートとも呼ばれます）およびファブリック リンクにブレークアウトを設定します。ファブリック リンクは、リーフ スイッチとスパイン スイッチ間の接続、またはマルチティア トポロジのティア 1 リーフ スイッチとティア 2 リーフ スイッチ間の接続を形成します。

ブレークアウト ポートは、次の方法で構成できます。

- ポート プロファイルとセレクタを使用できます。この方法では、リーフ インターフェイス プロファイルでブレークアウト リーフ ポートを構成し、プロファイルとスイッチを関連付け、サブポートを構成します。

- Cisco Application Policy Infrastructure Controller（APIC）6.0(1) リリース以降では、**[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）]**ワークフローを使用できます。
- **[ファブリック（Fabric）]** > **[インベントリ（Inventory）]** > ***pod*** > ***leaf_name*** ワークフローを使用できます。Cisco APIC 6.0(1) 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。

ダウンリンクのダイナミック ブレークアウトポートの注意事項と制約事項

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
- N9K-C93180YC-FX3
- N9K-C93600CD-GX
- N9K-C9364C-GX
- N9K-C9408（6.0（2）リリース以降）
- N9K-C9348D-GX2A（6.0（3）リリース以降）
- N9K-C9364D-GX2A（6.0（3）リリース以降）
- N9K-C9332D-GX2B（6.0（3）リリース以降）

100Gb から 25Gb へのブレークアウト機能は、次のスイッチのアクセスポートでサポートされます。

- N9K-C93180LC-EX
- N9K-C9336C-FX2
- N9K-C93180YC-FX
- N9K-C93360YC-FX2
- N9K-C93216TC-FX2
- N9K-C93108TC-FX3P

- N9K-C93180YC-FX3
- N9K-C93600CD-GX
- N9K-C9364C-GX
- N9K-C9408（6.0（2）リリース以降）
- N9K-C9348D-GX2A（6.0（3）リリース以降）
- N9K-C9364D-GX2A（6.0（3）リリース以降）
- N9K-C9332D-GX2B（6.0（3）リリース以降）

400Gb から 100Gb へのブレークアウト機能は、次のスイッチのアクセスポートでサポートされます。

- N9K-C9348D-GX2A
- N9K-C9364D-GX2A
- N9K-C9332D-GX2B
- N9K-C93600CD-GX
- N9K-C9316D-GX
- N9K-C9408（6.0(2) リリース以降）
- 6.0(2) リリース以降、QDD-400G-SR4.2-BD 光ファイバは 400Gb ポートでサポートされます。100Gb 速度のピアノードは、QSFP-100G-SR1.2 光ファイバを使用する必要があります。
- 6.0(3) リリース以降、任意の長さの QDD-4ZQ100 ケーブルを使用した 400Gb-100Gb ブレークアウトは、以下のプラットフォームでのみサポートされます。
  - N9K-C9332D-GX2B、N9K-C9348D-GX2A、N9K-C9364D-GX2A、N9K-C9316D-GX、および N9K-C93600CD-GX リーフおよびスパイン スイッチ
  - N9K-X9716D-GX ライン カード
- N9K-C9400-SW-GX2A スイッチは、N9K-X9400-8D ライン カード拡張モジュールを持つ 400Gb ブレークアウトをサポートし、ピア 100G-PCC は、N9K-X9400-8D および N9K-X9400-16W ライン カード拡張モジュールでサポートされます。
- QDD-400G-DR4-S、QDD-4X100G-FR-S、QDD-4X100G-LR-S 光ファイバは 400Gb ポートでサポートされます。100Gb 速度のピア ノードは、次のオプティクスを使用できます。
  - QSFP-100G-DR-S
  - QSFP-100G-FR-S
  - QSFP-100G-LR-S

ブレークアウト ポートを設定する前に、次のいずれかのケーブルを使用して、40Gb ポートを 4 つの 10Gb ポートに、100Gb ポートを 4 つの 25 Gb ポートに、または 400Gb ポートを 4 つの 100Gb ポートに接続します。

- Cisco QSFP-4SFP10G

  6.0（3）リリース以降、GX2 スイッチはこの直接接続ケーブルをサポートしています。

- Cisco QSFP-4SFP25G

  6.0（3）リリース以降、GX2 スイッチはこの直接接続ケーブルをサポートしています。

- Cisco QSFP-4X10G-AOC

  6.0（3）リリース以降、GX2 スイッチはこの直接接続ケーブルをサポートしています。

- Cisco QDD-4ZQ100-CU（1M、2M、2.5M、および 3M）（6.0（3）リリース以降）
- MPO から、両端に QSFP-40G-SR4 および 4 X SFP-10G-SR を備えたブレークアウト 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 を備えたブレークアウト スプリッタ ケーブルへ
- MPO から、両端に QDD-400G-DR4-S、QDD-4X100G-FR-S、または QDD-4X100G-LR-S、および 4 x QSFP-100G-DR-S、4 x QSFP-100G-FR-S、または 4 x QSFP-100G-LR-S を備えたブレークアウト スプリッタ ケーブルへ
- MPO から、両端に QDD-400G-SR4.2-BD および 4 x QSFP-100G-SR1.2 を備えたブレークアウト 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/

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。

- ブレークアウトポートは、ダウンリンクと変換ダウンリンクの両方でサポートされます。
- 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 ー 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 ー 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

  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

  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 ー 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-C9400-SW-GX2A と Cisco N9K-X9400-16W ラインカード

  奇数番号のプロファイリングされた QSFP ポートで、ブレークアウトを構成できます。

- 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。
- スパイン スイッチ インターフェイスでのダイナミック ブレークアウト構成はサポートされていません。
- 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。
- ポートでダイナミック ブレークアウトが有効になっている場合、親ポート上の他のポリシー（モニタリング ポリシーを除く）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。
- Cisco APIC ポリシーを使用して構成された、ダイナミック ブレークアウトまたは 400Gb ポートの 100Gb ポート x 4 への ブレークアウトは、QDD-4X100G-FR-S および QDD-4X100G-LR-S オプティクスでサポートされています。
- ブレイクアウト 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。

- すでにブレークアウトされているポートでポート プロファイル ポリシーを削除すると、ブレークアウト設定がクリーンアップされ、スイッチのリロード時にポートがネイティブ方向に戻ります。
- 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 ー 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 ー 4 または1/5 ー 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 ー 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 ー 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 ー 4 または 1/5 ー 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 ー 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。
  - ポート 1/25 ー 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 がブレー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（ブレークアウト）+ 10 x 4 ポート 10/25G（ブレークアウト）= 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。

ファブリック リンクの自動ブレークアウトポートの注意事項と制約事項

ブレークアウトがサポートされているライン カードにトランシーバを挿入すると、ポートは自動的にブレークアウトします。ブレークアウトを手動で設定する必要はありません。

400Gb から 100Gbへのブレークアウト機能は、次のライン カードのファブリック ポートでサポートされます。

- QDD-4X100G-FR-S、QDD-4X100G-LR-S、または QDD-400G-SR4.2-BD トランシーバを搭載した N9K-X9716D-GX

400Gb から 100Gb へのブレークアウト機能は、次のスイッチのファブリック ポートでサポートされます。

- N9K-C9348D-GX2A
- N9K-C9364D-GX2A
- N9K-C9332D-GX2B
- N9K-C93600CD-GX
- N9K-C9316D-GX
- N9K-C9408（6.0(2) リリース以降）

- 6.0(2) リリース以降、QDD-400G-SR4.2-BD 光ファイバは 400Gb ポートでサポートされます。100Gb 速度のピアノードは、QSFP-100G-SR1.2 光ファイバを使用する必要があります。
- 6.0(3) リリース以降、任意の長さの QDD-4ZQ100 ケーブルを使用した 400Gb-100Gb ブレークアウトは、以下のプラットフォームでのみサポートされます。
  - N9K-C9332D-GX2B、N9K-C9348D-GX2A、N9K-C9364D-GX2A、N9K-C9316D-GX、および N9K-C93600CD-GX リーフおよびスパイン スイッチ
  - N9K-X9716D-GX ライン カード
- N9K-C9400-SW-GX2A スイッチは、N9K-X9400-8D ライン カード拡張モジュールを持つ 400Gb ブレークアウトをサポートし、ピア 100G-PCC は、N9K-X9400-8D および N9K-X9400-16W ライン カード拡張モジュールでサポートされます。
- QDD-4X100G-FR-S および QDD-4X100G-LR-S オプティクスは、400Gb ポートでサポートされます。100Gb 速度のピア ノードは、次のオプティクスを使用できます。
  - QSFP-100G-DR-S
  - QSFP-100G-FR-S
  - QSFP-100G-LR-S

次のいずれかのケーブルを使用してポートを接続します。

- Cisco QDD-4ZQ100-CU（1M、2M、2.5M、および 3M）（6.0(3) リリース以降）
- MPO から、両端に QDD-4X100G-FR-S または QDD-4X100G-LR-S および 4 x QSFP-100G-DR-S、4 x QSFP-100G-FR-S、または 4 x QSFP-100G-LR-S を備えた 4xLC ブレークアウト スプリッタ ケーブル
- MPO から、両端に QDD-400G-SR4.2-BD および 4 x QSFP-100G-SR1.2 を備えたブレークアウト スプリッタ ケーブルへ

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。

- すでにブレークアウトされているポートでポート プロファイル ポリシーを削除すると、ブレークアウト設定がクリーンアップされ、スイッチのリロード時にポートがネイティブ方向に戻ります。

ファブリック リンクでの 400G から 4x100G へのブレイクアウトに関する次のガイドラインと制限事項に従ってください。

- QDD-400G-SR4.2-BD 光ファイバを備えたファブリックポートを非ブレークアウトからブレークアウトに変更するには、トランシーバを取り外し、ブレークアウトケーブルをトランシーバに接続してから、トランシーバを再度挿入する必要があります。
- GX2 スイッチは、次のスイッチからスイッチへの接続をサポートします。
  - スパイン スイッチからリーフ スイッチ

  - リーフ スイッチからスパイン スイッチ
  - リーフスイッチからリーフスイッチ（多層）

- GX ライン カードは、次のスイッチからスイッチへの接続をサポートします。
  - スパインスイッチからリーフスイッチへ

- スパインスイッチからスパインスイッチのブレークアウトはサポートされていません。
- スパイン スイッチから IPN または ISN ブレークアウトは、スパイン スイッチの QDD-4X100G-FR-S または QDD-4X100G-LR-S オプティックでサポートされます。
- スパイン スイッチから IPN または ISN ブレークアウトは、スパイン スイッチの QDD-400G-SR4.2-BD 光ファイバと IPN または ISN 側の QSFP-100G-SR1.2 光ファイバでサポートされます。
- 両側（スパイン スイッチおよび IPN/ISN 側）の QDD-400G-SR4.2-BD 光ファイバを使用したスパイン スイッチから IPN または ISN の場合、リンクは起動しません。
- 特定のハードウェアおよびポートのブレークアウトをサポートしていないリリースにダウングレードすると、ブレークアウトポートはブレークアウトされず、リンクがダウンします。スパインとリーフスイッチ間のすべての接続がブレークアウトのみの場合、ブレークアウトをサポートしていないリリースにダウングレードすると、リンクはダウンし、ノードはファブリック外になります。
- スイッチから SFP トランシーバを取り外した場合、トランシーバを再度追加する前に、少なくとも 15 秒待つ必要があります。
- Cisco Nexus 9300 GX2 シリーズまたは Cisco N9K-X9716D-GX ライン カードでは、ラインカードの電源がオフの状態で光ファイバを交換しても、ポートは起動しません。次に例を示します。

  1. スロット 4 に Cisco N9K-X9716D-GX ラインカードがあり、4x100-FR-S トランシーバがポート（たとえば、ポート 8）に挿入されている。ポート 8は、4x100-FR-S トランシーバが挿入されたときに自動的にアクティブになる自動ブレークアウト機能により、4 つのポート（Eth4/8/1-4）に分割されます。
  2. スロット 4 のラインカードの電源をオフにします。
  3. ラインカードの電源がオフになっている間に、ポート 8 から 4x100G-FR-S 光ファイバを取り外し、4x100G-FR-S 以外の光ファイバを挿入します。
  4. スロット 4 のラインカードの電源をオンにします。ポート Eth4/8は、ピア エンドで互換性のあるポートとトランシーバの組み合わせに接続した後でも起動しません。

GUIを使用したプロファイルおよびセレクタによるブレークアウト ポートの構成

この手順では、ポート プロファイルとセレクタを使用して、ブレークアウト ポートを構成します。リーフ インターフェイス プロファイルでブレークアウト リーフ ポートを構成し、プロファイルとスイッチを関連付け、サブポートを構成します。

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。
- ブレークアウト ポートを設定できる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。
- 40GE または 100GE リーフ スイッチ ポートは、ダウンリンク ポートに Cisco ブレイク アウト ケーブルを接続します。

手順

ステップ 1 メニュー バーで、**[Fabric]** > **[Access Policies]** の順に選択します。

ステップ 2 ナビゲーション ウィンドウで、**Interfaces** および **Leaf Interfaces** および **Profiles** を展開します。

ステップ 3 **Profiles** を右クリックして **Create Leaf Interface Profile** を選択します。

ステップ 4 名前と説明 (オプション) を入力して、**Interface Selectors** の [+] 記号をクリックします。

ステップ 5 次の手順を実行します。

a) **Access Port Selector** の名前と説明（オプション）を入力します。

b) **Interface IDs** フィールドで、ブレイクアウト ポートのスロットとポートを入力します。

c) **Interface Policy Group** フィールドで、下矢印をクリックして **Create Leaf Breakout Port Group** を選択します。

d) **Leaf Breakout Port Group** の名前 (およびオプションとして説明) を入力します。

e) **Breakout Map** フィールドで、**10g-4x** または **25g-4x** を選択します。

ブレークアウトをサポートするスイッチのリストについては、ブレークアウト ポートの設定 （247 ページ） を参照してください。

f) [Submit] をクリックします。

ステップ 6 ブレークアウト ポートを EPG に割り当てるには、次の手順を実行します。

メニュー バーで、**[Tenant]** > **[Application Profiles]** > **[Application EPG]** の順に選択します。[Application EPGs] を右クリックして [Create Application EPG] ダイアログボックスを開き、次の手順を実行します。

a) [Statically Link with Leaves/Paths] チェックボックスをオンにして、ダイアログボックスの [Leaves/Paths] タブにアクセスします。

b) 次のいずれかの手順を実行します。

オプション	説明
次のものに EPG を展開する場合、	次を実行します。
ノード	**1.** **Leaves** エリアを展開します。 **2.** [Node] ドロップダウン リストから、ノードを選択します。 **3.** **Encap** フィールドで、適切な VLAN を入力します。 **4.** (オプション) **Deployment Immediacy** ドロップダウンリストで、デフォルトの **On Demand** のままにするか、**Immediate**を選択します。 **5.** (オプション) [Mode] ドロップダウンリストで、デフォルトの [Trunk] のままにするか、別のモードを選択します。
ノード上のポート	**1.** **Paths** エリアを展開します。 **2.** **Path** ドロップダウンリストから、適切なノードおよびポートを選択します。 **3.** (オプション) **Deployment Immediacy** フィールドのドロップダウンリストで、デフォルトの **On Demand** のままにするか、**Immediate** を選択します。 **4.** (オプション) [Mode] ドロップダウンリストで、デフォルトの [Trunk] のままにするか、別のモードを選択します。 **5.** **Port Encap** フィールドに、導入するセカンダリ VLAN を入力します。 **6.** (オプション) **Primary Encap** フィールドで、展開するプライマリ VLAN を入力します。

ステップ 7 リーフ インターフェイス プロファイルをリーフ スイッチに関連付けるため、次の手順に従います。

a) **Switches** と **Leaf Switches**、および **Profiles** を展開します。

b) **Profiles** を右クリックして **Create Leaf Profiles** を選択します。

c) リーフ プロファイルの名前と、オプションとして説明を入力します。

d) **+** 記号 (**Leaf Selectors** エリア) をクリックします。

e) リーフ セレクタの名前と、オプションとして説明を入力します。

f) **Blocks** フィールドの下向き矢印をクリックして、ブレイクアウト インターフェイス プロファイルと関連付けるスイッチを選択します。
g) **Policy Group** フィールドの下向き矢印をクリックし、**Create Access Switch Policy Group** を選択します。
h) アクセス スイッチ ポリシー グループの名前と、オプションとして説明を入力します。
i) オプション。その他のポリシーを有効にします。
j) [Submit] をクリックします。
k) **Update** をクリックします。
l) [Next] をクリックします。
m) **Associations Interface Selector Profiles** エリアで、ブレイクアウト ポート用に以前に作成したインターフェイス セレクタ プロファイルを選択します。
n) **Finish** をクリックします。

ステップ 8 ブレイクアウト ポートが 4 つのサブ ポートに分割されたことを確認するために、次の手順に従います:

a) メニュー バーで、**Fabric** > **Inventory** をクリックします。
b) ナビゲーションバーで、ブレイクアウトポートがあるポッドとリーフをクリックします。
c) **Interfaces** および **Physical Interfaces** を展開します。
ブレイクアウト ポートが設定された場所に 4 つのポートが表示されます。たとえば、1/10 をブレイクアウト ポートとして設定した場合、次のように表示されます:

- **eth1/10/1**
- **eth1/10/2**
- **eth1/10/3**
- **eth1/10/4**

ステップ 9 サブ ポートを設定するには、次の手順を実行します:

a) メニュー バーで、**[Fabric]** > **[Access Policies]** をクリックします。
b) ナビゲーションバーで、**Interfaces**、**Leaf Interfaces**、**Profiles**、および前に作成したブレイクアウト リーフ インターフェイス プロファイルを展開します。

ブレークアウトケーブルが付属するポートのセレクタが表示されます。既存のポートのセレクタでサブポート ブロックを定義する代わりに、新しいアクセス ポート セレクタで定義する必要があります。

c) ナビゲーションバーで、上位レベルのインターフェイス プロファイルを右クリックし、**[Create Access Port Selector]** を選択します。
d) **[Name]** フィールドで、サブ ポートの名前を入力します。
e) **Interface IDs** フィールドに、4 つのサブ ポートの ID を、`1/10/1-4` のフォーマットで入力します。
f) **[Interface Policy Group]** フィールドで、**[Create Leaf Access Port Policy Group]** を選択します。
g) **[送信（Submit）]** をクリックします。`

ステップ 10 AAEP をポートにリンクする個々のインターフェイスにポリシーグループを適用するには、次の手順を実行します。

a) **[Name]** フィールドに、リーフ アクセス ポートのグループ ポリシー名を入力します。
b) **[Link Level Policy]** フィールドで、**[link-level_auto]** を選択します。
c) **[CDP Policy]** フィールドで、**[cdp_enabled]** を選択します。
d) **[LLDP Policy]** フィールドで、**[default]** を選択します。
e) **[Attached Entity Profile]** フィールドで、ポリシー グループにアタッチする AAEP プロファイルを選択します。
f) [送信（Submit）] をクリックします。

GUI を使用したプロファイルおよびセレクタによるブレークアウト ポートの構成

この手順では、ポート プロファイルとセレクタを使用して、ブレークアウト ポートを構成します。リーフ インターフェイス プロファイルでブレークアウト リーフ ポートを構成し、プロファイルとスイッチを関連付け、サブポートを構成します。

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。
- ブレークアウト ポートを設定できる 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。
- 40GE または 100GE リーフ スイッチ ポートは、ダウンリンク ポートに Cisco ブレイク アウト ケーブルを接続します。

手順

ステップ 1 メニュー バーで、**[Fabric]** > **[Access Policies]** の順に選択します。

ステップ 2 ナビゲーション ウィンドウで、**Interfaces** および **Leaf Interfaces** および **Profiles** を展開します。

ステップ 3 **Profiles** を右クリックして **Create Leaf Interface Profile** を選択します。

ステップ 4 名前と説明 (オプション) を入力して、**Interface Selectors** の [+] 記号をクリックします。

ステップ 5 次の手順を実行します。

a) **Access Port Selector** の名前と説明（オプション）を入力します。

b) **Interface IDs** フィールドで、ブレイクアウト ポートのスロットとポートを入力します。
c) **Interface Policy Group** フィールドで、下矢印をクリックして **Create Leaf Breakout Port Group** を選択します。
d) **Leaf Breakout Port Group** の名前 (およびオプションとして説明) を入力します。
e) **Breakout Map** フィールドで、**10g-4x** または **25g-4x** を選択します。

ブレークアウトをサポートするスイッチのリストについては、ブレークアウト ポートの設定 （247 ページ） を参照してください。

f) [Submit] をクリックします。

ステップ 6 ブレークアウト ポートを EPG に割り当てるには、次の手順を実行します。

メニュー バーで、**[Tenant]** > **[Application Profiles]** > **[Application EPG]** の順に選択します。[Application EPGs] を右クリックして [Create Application EPG] ダイアログボックスを開き、次の手順を実行します。

a) [Statically Link with Leaves/Paths] チェックボックスをオンにして、ダイアログボックスの [Leaves/Paths] タブにアクセスします。
b) 次のいずれかの手順を実行します。

オプション	説明
次のものに EPG を展開する場合、	次を実行します。
ノード	**1.** **Leaves** エリアを展開します。 **2.** [Node] ドロップダウン リストから、ノードを選択します。 **3.** **Encap** フィールドで、適切な VLAN を入力します。 **4.** (オプション) **Deployment Immediacy** ドロップダウンリストで、デフォルトの **On Demand** のままにするか、**Immediate**を選択します。 **5.** (オプション) [Mode] ドロップダウンリストで、デフォルトの [Trunk] のままにするか、別のモードを選択します。
ノード上のポート	**1.** **Paths** エリアを展開します。 **2.** **Path** ドロップダウンリストから、適切なノードおよびポートを選択します。 **3.** (オプション) **Deployment Immediacy** フィールドのドロップダウンリストで、デフォルトの **On Demand** のままにするか、**Immediate** を選択します。 **4.** (オプション) [Mode] ドロップダウンリストで、デフォルトの [Trunk] のままにするか、別のモードを選択します。 **5.** **Port Encap** フィールドに、導入するセカンダリ VLAN を入力します。

オプション	説明
	6. (オプション) **Primary Encap** フィールドで、展開するプライマリ VLAN を入力します。

ステップ 7 リーフ インターフェイス プロファイルをリーフ スイッチに関連付けるため、次の手順に従います。

a) **Switches** と **Leaf Switches**、および **Profiles** を展開します。
b) **Profiles** を右クリックして **Create Leaf Profiles** を選択します。
c) リーフ プロファイルの名前と、オプションとして説明を入力します。
d) **+** 記号 (**Leaf Selectors** エリア) をクリックします。
e) リーフ セレクタの名前と、オプションとして説明を入力します。
f) **Blocks** フィールドの下向き矢印をクリックして、ブレイクアウト インターフェイス プロファイルと関連付けるスイッチを選択します。
g) **Policy Group** フィールドの下向き矢印をクリックし、**Create Access Switch Policy Group** を選択します。
h) アクセス スイッチ ポリシー グループの名前と、オプションとして説明を入力します。
i) オプション。その他のポリシーを有効にします。
j) [Submit] をクリックします。
k) **Update** をクリックします。
l) [Next] をクリックします。
m) **Associations Interface Selector Profiles** エリアで、ブレイクアウト ポート用に以前に作成したインターフェイス セレクタ プロファイルを選択します。
n) **Finish** をクリックします。

ステップ 8 ブレイクアウト ポートが 4 つのサブ ポートに分割されたことを確認するために、次の手順に従います:

a) メニュー バーで、**Fabric** > **Inventory** をクリックします。
b) ナビゲーション バーで、ブレイクアウト ポートがあるポッドとリーフをクリックします。
c) **Interfaces** および **Physical Interfaces** を展開します。
ブレイクアウト ポートが設定された場所に 4 つのポートが表示されます。たとえば、1/10 をブレイクアウト ポートとして設定した場合、次のように表示されます:

- **eth1/10/1**
- **eth1/10/2**
- **eth1/10/3**
- **eth1/10/4**

ステップ 9 サブ ポートを設定するには、次の手順を実行します:

a) メニュー バーで、**[Fabric]** > **[Access Policies]** をクリックします。
b) ナビゲーションバーで、**Interfaces**、**Leaf Interfaces**、**Profiles**、および前に作成したブレイクアウト リーフ インターフェイス プロファイルを展開します。

ブレークアウト ケーブルが付属するポートのセレクタが表示されます。既存のポートのセレクタでサブポート ブロックを定義する代わりに、新しいアクセス ポート セレクタで定義する必要があります。

c) ナビゲーションバーで、上位レベルのインターフェイス プロファイルを右クリックし、**[Create Access Port Selector]** を選択します。
d) **[Name]** フィールドで、サブ ポートの名前を入力します。
e) **Interface IDs** フィールドに、4 つのサブ ポートの ID を、`1/10/1-4` のフォーマットで入力します。
f) **[Interface Policy Group]** フィールドで、**[Create Leaf Access Port Policy Group]** を選択します。
g) **[送信（Submit）]** をクリックします。`

ステップ 10 AAEP をポートにリンクする個々のインターフェイスにポリシーグループを適用するには、次の手順を実行します。

a) **[Name]** フィールドに、リーフ アクセス ポートのグループ ポリシー名を入力します。
b) **[Link Level Policy]** フィールドで、**[link-level_auto]** を選択します。
c) **[CDP Policy]** フィールドで、**[cdp_enabled]** を選択します。
d) **[LLDP Policy]** フィールドで、**[default]** を選択します。
e) **[Attached Entity Profile]** フィールドで、ポリシー グループにアタッチする AAEP プロファイルを選択します。
f) [送信（Submit）] をクリックします。

GUI を使用したインターフェイス コンフィギュレーションによるブレークアウト ポートの設定

（）6.0(1) リリース以降では、ファブリック アクセス ポリシー インターフェイス設定ワークフローを使用して、ブレークアウト ポートを設定できます。Cisco Application Policy Infrastructure ControllerAPIC > >

始める前に

- Cisco Application Centric Infrastructure（ACI）ファブリックが設置され、Cisco 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。
- ブレークアウト ポートを設定できる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。
- 40GE または 100GE リーフ スイッチ ポートは、ダウンリンク ポートに Cisco ブレイク アウト ケーブルを接続します。

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）]** > **[削除（Delete）]**の順に選択します。

ステップ 4 **[ブレークアウト（Breakout）]** ページで、次のサブ手順を実行します。

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。

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) **[ブレークアウト マップ（Breakout Map）]** で、目的のブレークアウト タイプを選択します。

d) [保存（Save）] をクリックします。

NX-OS スタイルの CLI を使用したダイナミック ブレイクアウト ポートの設定

ブレークアウトポートを設定、設定を確認および NX-OS スタイル CLI を使用してサブ ポートで、EPG を設定するには、次の手順を使用します。

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。
- 40GE または 100GE リーフ スイッチ ポートは、ダウンリンク ポートに Cisco ブレイク アウト ケーブルを接続します。

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`	コンフィギュレーションモードに入ります。
ステップ 2	**leaf** *ID* 例： `apic1(config)# leaf 101`	ブレークアウトポートが配置され、リーフ configuration mode(設定モード、コンフィギュレーション モード) を開始リーフ スイッチを選択します。
ステップ 3	**interface ethernet***slot/port* 例： `apic1(config-leaf)# interface ethernet 1/16`	40 ギガビット イーサネット (GE) ブレークアウトポートとして有効にするインターフェイスを識別します。
ステップ 4	**breakout10g-4x|25g-4x** 例： `apic1(config-leaf-if)# breakout 10g-4x`	ブレイク アウトを選択したインターフェイスを有効にします。 （注） ダイナミック ブレイク アウト ポート機能は、スイッチのサポートを参照してください。 ブレークアウト ポートの設定 （247 ページ） 。

ステップ 5	**show run**
	例：
	`apic1(config-leaf-if)# show run`
	`# Command: show running-config leaf 101 interface ethernet 1 / 16`
	`# Time: Fri Dec  2 18:13:39 2016`
	`  leaf 101`
	`    interface ethernet 1/16`
	`      breakout 10g-4x`
	`apic1(config-leaf-if)# exit`
	`apic1(config-leaf)# exit`
		インターフェイスの実行コンフィギュレーションを表示することによって、設定を確認し、グローバル コンフィギュレーション モードに戻ります。

ステップ 6	**tenant** *tenant-name* 例： `apic1(config)# tenant tenant64`	選択またはブレイク アウト ポートで消費され、テナント configuration mode(設定モード、コンフィギュレーション モード)を開始するテナントを作成します。
ステップ 7	**vrf context** *vrf-name* 例：	作成またはテナントに関連付けられている Virtual Routing and Forwarding (VRF) インスタンスを識別し、

	コマンドまたはアクション	目的
	`apic1(config-tenant)# vrf context vrf64` `apic1(config-tenant-vrf)# exit`	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。
ステップ 8	**bridge-domain** *bridge-domain-name* 例： `apic1(config-tenant)# bridge-domain bd64`	作成またはテナントに関連付けられているブリッジ ドメインを識別し、BD configuration mode(設定モード、コンフィギュレーション モード) を開始します。

ステップ 9	**vrf member** *vrf-name*
	例：
	`apic1(config-tenant-bd)# vrf member vrf64`
	`apic1(config-tenant-bd)# exit`
		ブリッジ ドメイン、VRF の関連付け、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。

ステップ 10	**application** *application-profile-name* 例： `apic1(config-tenant)# application app64`	作成またはテナントと EPG に関連付けられているアプリケーションプロファイルを識別します。
ステップ 11	**epg** *epg-name* 例： `apic1(config-tenant)# epg epg64`	作成または EPG を識別し、EPG configuration mode(設定モード、コンフィギュレーション モード) に入力します。

ステップ 12	**bridge-domain member** *bridge-domain-name*
	例：
	`apic1(config-tenant-app-epg)# bridge-domain member bd64`
	`apic1(config-tenant-app-epg)# exit`
	`apic1(config-tenant-app)# exit`
	`apic1(config-tenant)# exit`
		EPG をブリッジ ドメインに関連付け、グローバル設定モードをに戻ります。
		たとえば、必要に応じて、サブ ポートを設定コマンドを使用して、速度リーフインターフェイス モードでサブ ポートを設定します。

ステップ 13	**leaf** *leaf-name*
	例：
	`apic1(config)# leaf 1017`
	`apic1(config-leaf)# interface ethernet 1/13`
	`apic1(config-leaf-if)# vlan-domain member dom1`
	`apic1(config-leaf-if)# switchport trunk allowed vlan 20 tenant t1 application AP1 epg EPG1`
	（注）
		EPG をブレークアウト ポートに関連付けます。

	コマンドまたはアクション	目的
	上の例に示した vlan-domain コマンドと vlan-domain member コマンドは、ポートに EPG を導入するための前提条件です。	

ステップ 14	**speed** *interface-speed*
	例：
	`apic1(config)# leaf 101`
	`apic1(config-leaf)# interface ethernet 1/16/1`
	`apic1(config-leaf-if)# speed 10G`
	`apic1(config-leaf-if)# exit`
		リーフインターフェイスモードを開始し、[インターフェイスの速度を設定 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。

ステップ 15	**show run** 例： `apic1(config-leaf)# show run`	サブ ポートを設定した後にリーフ configuration mode(設定モード、コンフィギュレーション モード) で次のコマンドを入力して、サブポートの詳細が表示されます。

サブ ポート 1/16/1、2/1/16、1/16/3 および 4/1/16 ブレイク アウトを有効になっているリーフ インターフェイス 1/16 で 101 上のポートを確認します。

例

この例では、ブレイク アウト ポートで設定します。

```
apic1# configure
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/16
apic1(config-leaf-if)# breakout 10g-4x
```

この例では、サブインターフェイス ポートの EPG で設定します。

```
apic1(config)# tenant tenant64
apic1(config-tenant)# vrf context vrf64
apic1(config-tenant-vrf)# exit
apic1(config-tenant)# bridge-domain bd64
apic1(config-tenant-bd)# vrf member vrf64
apic1(config-tenant-bd)# exit
apic1(config-tenant)# application app64
apic1(config-tenant-app)# epg epg64
apic1(config-tenant-app-epg)# bridge-domain member bd64
apic1(config-tenant-app-epg)# end
```

この例では、10 G に、ブレイク アウトの速度サブ ポートを設定します。

```
apic1(config)# leaf 101
apic1(config-leaf)# interface ethernet 1/16/1
apic1(config-leaf-if)# speed 10G
apic1(config-leaf-if)# exit

apic1(config-leaf)# interface ethernet 1/16/2
apic1(config-leaf-if)# speed 10G
```

```
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface ethernet 1/16/3
apic1(config-leaf-if)# speed 10G
apic1(config-leaf-if)# exit
apic1(config-leaf)# interface ethernet 1/16/4
apic1(config-leaf-if)# speed 10G
apic1(config-leaf-if)# exit
```

この例では、リーフ 101、インターフェイス 1/16 に接続されている、4 つのアシスタント的なポートを示します。

```
apic1#(config-leaf)# show run
# Command: show running-config leaf 101
# Time: Fri Dec  2 00:51:08 2016
  leaf 101
    interface ethernet 1/16/1
      speed 10G
      negotiate auto
      link debounce time 100
      exit
    interface ethernet 1/16/2
      speed 10G
      negotiate auto
      link debounce time 100
      exit
    interface ethernet 1/16/3
      speed 10G
      negotiate auto
      link debounce time 100
      exit
    interface ethernet 1/16/4
      speed 10G
      negotiate auto
      link debounce time 100
      exit
    interface ethernet 1/16
      breakout 10g-4x
      exit
    interface vfc 1/16
```

第 13 章

プロシキ ARP

この章は、次の内容で構成されています。

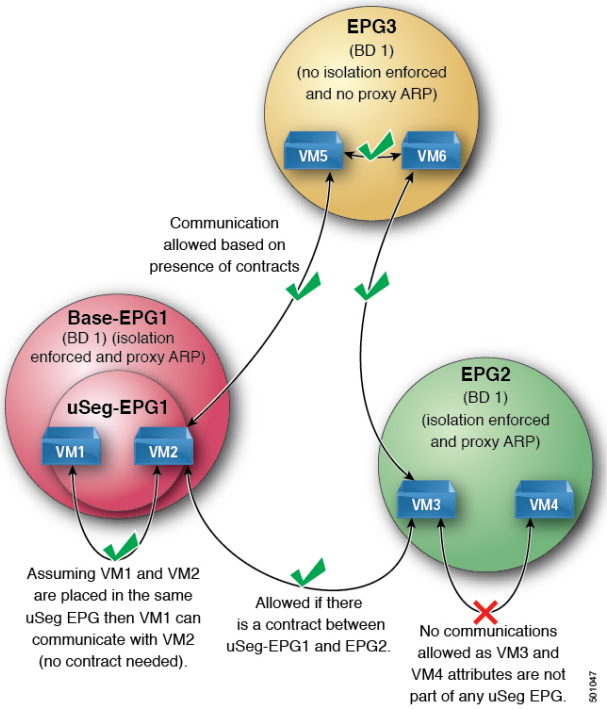
- プロキシ ARP について （269 ページ）
- 注意事項と制約事項 （276 ページ）
- プロキシ ARP がサポートされている組み合わせ （277 ページ）
- 拡張 GUI を使用したプロキシ ARP の設定 （277 ページ）
- プロキシ ARP は、Cisco NX-OS スタイル CLI を使用しての設定 （278 ページ）

プロキシ ARP について

Cisco ACI のプロキシ ARP は、ネットワークまたはサブネット内のエンドポイントが、別のエンドポイントの MAC アドレスを知らなくても、そのエンドポイントと通信できるようにします。プロキシ ARP はトラフィックの宛先場所を知っており、代わりに、最終的な宛先として自身の MAC アドレスを提供します。

プロキシ ARP を有効にするには、EPG 内エンドポイント分離を EPG で有効にする必要があります。詳細については、次の図を参照してください。EPG 内エンドポイント分離と Cisco ACI の詳細については、「*Cisco ACI* 仮想化ガイド」を参照してください。

図 *34 :* プロキシ *ARP* および *Cisco APIC*



Cisco ACI ファブリック内のプロキシ ARP は従来のプロキシ ARP とは異なります。通信プロセスの例として、プロキシ ARP が EPG で有効になっているとき、エンドポイント A が ARP 要求をエンドポイント B に送信し、エンドポイント B がファブリック内で学習される場合、エンドポイント A はブリッジ ドメイン（BD）MAC からプロキシ ARP 応答を受信します。エンドポイント A が B、エンドポイントの ARP 要求を送信し、エンドポイント B はすでに ACI ファブリック内で学習しない場合は、ファブリックはプロキシ ARP の BD 内で要求を送信します。エンドポイント B は、ファブリックに戻る要求、このプロキシ ARP に応答します。この時点では、ファブリックはプロキシ ARP エンドポイント A への応答を送信しませんが、エンドポイント B は、ファブリック内で学習します。エンドポイント A は、エンドポイント B に別の ARP 要求を送信する場合、ファブリックはプロキシ ARP 応答から送信 BD mac です。

次の例ではプロキシ ARP 解像度がクライアント VM1 と VM2 間の通信の手順します。

1. VM2 通信を VM1 が必要です。

図 *35 : VM2* 通信を *VM1* が必要です。

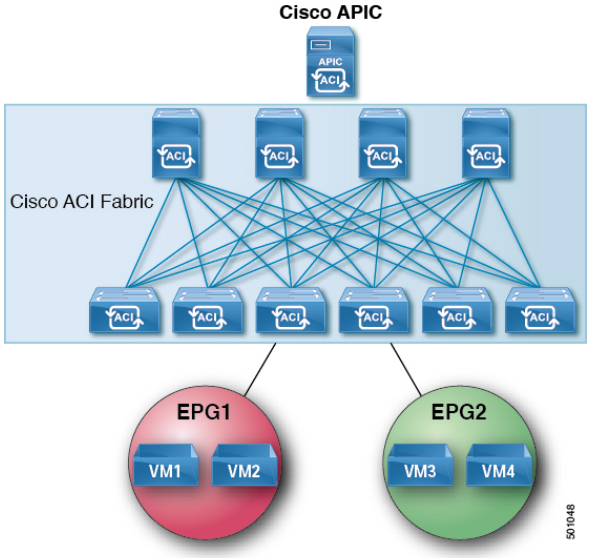


表 *8 : ARP* 表の説明

デバイス	状態
VM1	IP = * MAC = *
ACI ファブリック	IP = * MAC = *
VM2	IP = * MAC = *

2. VM1 は、ブロードキャスト MAC アドレスとともに ARP 要求を VM2 に送信します。

図 *36 : VM1* はブロードキャスト *MAC* アドレスとともに *ARP* 要求を *VM2* に送信します

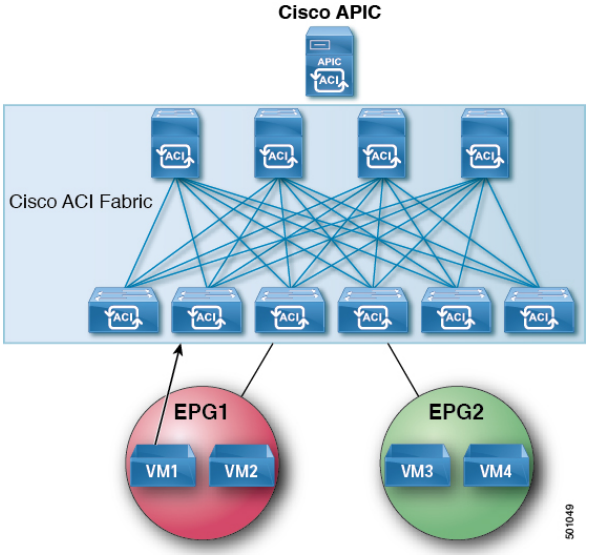


表 *9 : ARP* 表の説明

デバイス	状態
VM1	IP = VM2 IP; MAC = ?
ACI ファブリック	IP = VM1 IP; MAC = VM1 MAC
VM2	IP = * MAC = *

3. ACI ファブリックは、ブリッジ ドメイン（BD）内のプロキシ ARP 要求をフラッディングします。

図 *37 : ACI* ファブリックは *BD* 内のプロキシ *ARP* 要求をフラッディングします

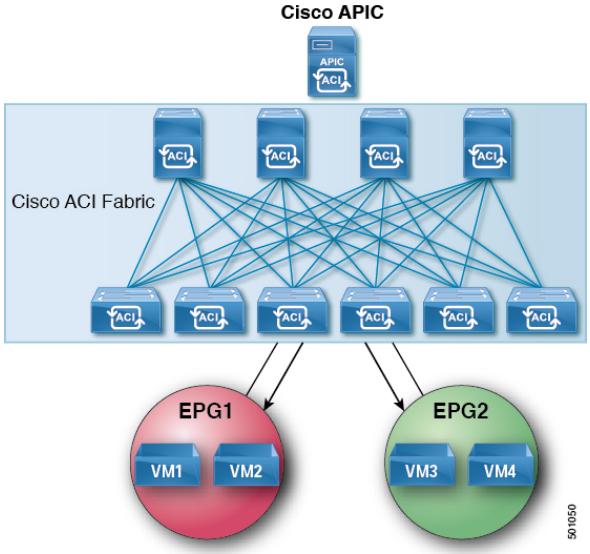


表 *10 : ARP* 表の説明

デバイス	状態
VM1	IP = VM2 IP; MAC = ?
ACI ファブリック	IP = VM1 IP; MAC = VM1 MAC
VM2	IP = VM1 IP; MAC = BD MAC

4. VM2 は、ARP 応答を ACI ファブリックに送信します。

図 *38 : VM2* は *ARP* 応答を *ACI* ファブリックに送信します

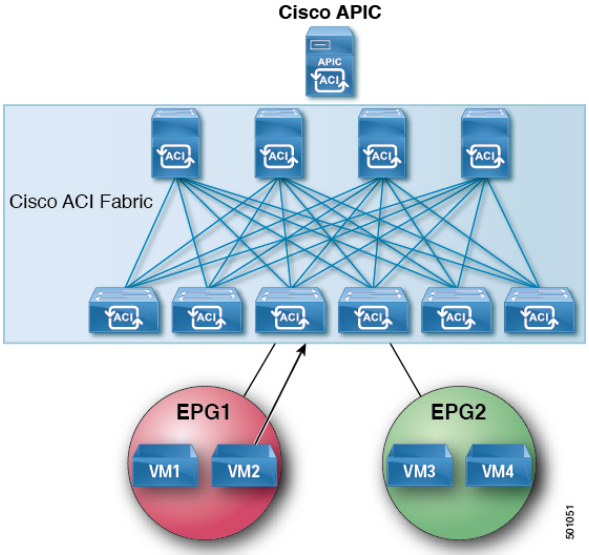


表 *11 : ARP* 表の説明

デバイス	状態
VM1	IP = VM2 IP; MAC = ?
ACI ファブリック	IP = VM1 IP; MAC = VM1 MAC
VM2	IP = VM1 IP; MAC = BD MAC

5. VM2 が学習されます。

図 *39 : VM2* が学習されます

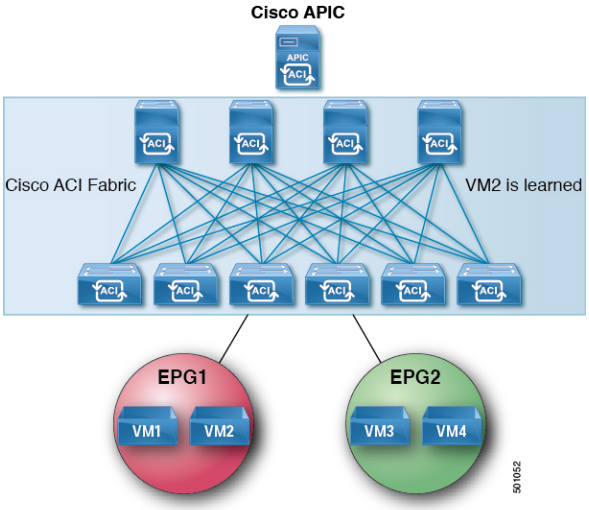


表 *12 : ARP* 表の説明

デバイス	状態
VM1	IP = VM2 IP; MAC = ?
ACI ファブリック	IP = VM1 IP; MAC = VM1 MAC IP = VM2 IP; MAC = VM2 MAC
VM2	IP = VM1 IP; MAC = BD MAC

6. VM1 は、ブロードキャスト MAC アドレスとともに ARP 要求を VM2 に送信します。

図 *40 : VM1* はブロードキャスト *MAC* アドレスとともに *ARP* 要求を *VM2* に送信します

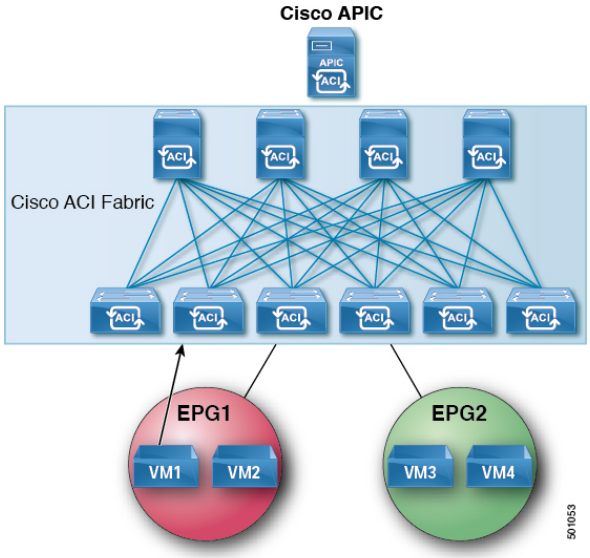


表 *13 : ARP* 表の説明

デバイス	状態
VM1	IP = VM2 IP MAC = ?
ACI ファブリック	IP = VM1 IP; MAC = VM1 MAC IP = VM2 IP; MAC = VM2 MAC
VM2	IP = VM1 IP; MAC = BD MAC

7. ACI ファブリックは、プロキシ ARP VM1 への応答を送信します。

図 *41 : ACI* ファブリック *VM1* にプロキシ *ARP* 応答を送信します。

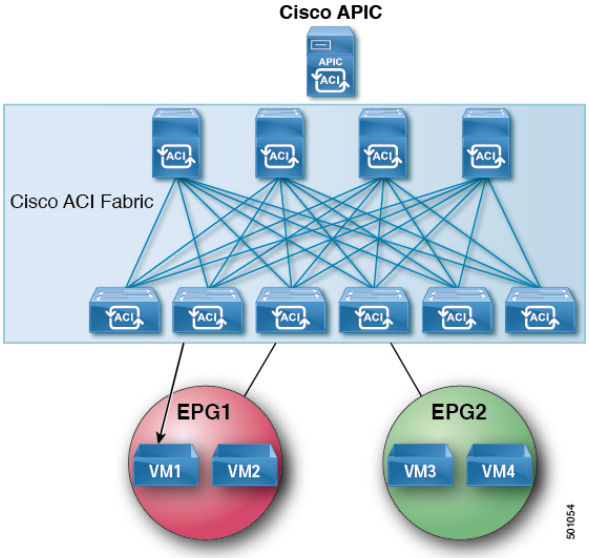


表 *14 : ARP* 表の説明

デバイス	状態
VM1	IP = VM2 IP;MAC = BD MAC
ACI ファブリック	IP = VM1 IP; MAC = VM1 MAC IP = VM2 IP; MAC = VM2 MAC
VM2	IP = VM1 IP; MAC = BD MAC

注意事項と制約事項

プロキシ ARP を使用すると、次のガイドラインと制限事項を考慮してください。

- プロキシ ARP は、隔離 Epg でのみサポートされます。EPG が隔離ではない場合、障害が発生します。プロキシ ARP が有効になっていると隔離 Epg 内で発生する通信では、uSeg Epg を設定する必要があります。たとえば、隔離の EPG 内で別の IP アドレスを持つ複数の Vm がある可能性があり、これらの Vm の IP address range(IP アドレス範囲、IP アドレスの範囲) に一致する IP の属性を持つ uSeg EPG を設定することができます。
- 隔離されたエンドポイントを通常のエンドポイントと、定期的なエンドポイントを隔離のエンドポイントからの ARP 要求には、プロキシ ARP は使用しないでください。このような場合は、エンドポイントは、接続先の Vm の実際の MAC アドレスを使用して通信します。

プロキシ ARP がサポートされている組み合わせ

次のプロキシ ARP 表では、サポートされている組み合わせを示します。

ARP 送信元/宛先	定期的な EPG	プロキシ ARP に適用される EPG の隔離
定期的な EPG	ARP	ARP
プロキシ ARP に適用される EPG の隔離	ARP	プロシキ ARP

拡張 GUI を使用したプロキシ ARP の設定

始める前に

- 適切なテナント、VRF、ブリッジ ドメイン、アプリケーションプロファイルおよび EPG を作成する必要があります。
- プロキシ ARP が有効にするのにが EPG で内通 EPG の分離を有効にする必要があります。

手順

ステップ 1 メニュー バーで、**Tenant** > **Tenant_name** をクリックします。

ステップ 2 **ナビゲーション**] ペインで、展開、 **Tenant_name** > **アプリケーション プロファイル** > **Application_Profile_name** > **アプリケーション Epg** 、右クリックして **アプリケーション EPG の作成** を実行するダイアログボックス、次のアクションに、 **アプリケーション EPG の作成** ダイアログボックス:

a) **Name** フィールドに EPG 名を追加します。

ステップ 3 **Intra EPG Isolation** フィールドで、**Enforced** を選択します。
内通 EPG 分離が適用されるときに、 **転送制御** フィールドは使用可能になります。

ステップ 4 **Forwarding Control** フィールドで、**proxy-arp** チェック ボックスをオンにします。
proxy-arp が有効になります。

ステップ 5 **Bridge Domain** フィールドで、ドロップダウン リストから、関連付ける適切なブリッジ ドメインを選択します。

ステップ 6 必要に応じて、ダイアログボックスの残りのフィールドを選択し、をクリックして **終了** 。

プロキシ ARP は、Cisco NX-OS スタイル CLI を使用しての設定

始める前に

- 適切なテナント、VRF、ブリッジ ドメイン、アプリケーションプロファイルおよび EPG を作成する必要があります。
- プロキシ ARP が有効にするのにが EPG で内通 EPG の分離を有効にする必要があります。

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`	コンフィギュレーション モードに入ります。
ステップ 2	**tenant** *tenant-name* 例： `apic1(config)# tenant Tenant1`	テナント コンフィギュレーション モードを開始します。
ステップ 3	**application** *application-profile-name* 例： `apic1(config-tenant)# application Tenant1-App`	アプリケーション プロファイルを作成し、アプリケーション モードを開始します。
ステップ 4	**epg** *application-profile-EPG-name* 例： `apic1(config-tenant-app)# epg Tenant1-epg1`	EPG を作成し、EPG モードに入ります。
ステップ 5	**proxy-arp enable** 例： `apic1(config-tenant-app-epg)# proxy-arp enable`	プロキシ ARP を有効にします。 （注） プロキシ arp をディセーブルにできます、 **no プロキシ arp** コマンド。
ステップ 6	**exit** 例： `apic1(config-tenant-app-epg)# exit`	ポート アプリケーション 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 7	**exit** 例： `apic1(config-tenant-app)# exit`	テナント コンフィギュレーション モードに戻ります。
ステップ 8	**exit** 例： `apic1(config-tenant)# 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

次に、プロキシ ARP を設定する例を示します。

```
apic1# conf t
apic1(config)# tenant Tenant1
apic1(config-tenant)# application Tenant1-App
apic1(config-tenant-app)# epg Tenant1-epg1
apic1(config-tenant-app-epg)# proxy-arp enable
apic1(config-tenant-app-epg)#
apic1(config-tenant)#
```

第 14 章

トラフィック ストーム制御

この章は、次の項で構成されています。

- トラフィック ストーム制御について （281 ページ）
- ストーム制御の注意事項と制約事項 （282 ページ）
- GUI を使用したトラフィック ストーム制御ポリシーの設定 （285 ページ）
- NX-OS スタイルの CLI を使用したトラフィック ストーム制御ポリシーの設定 （287 ページ）
- ストーム制御 SNMP トラップの設定 （288 ページ）

トラフィック ストーム制御について

トラフィック ストームは、パケットが LAN でフラッディングする場合に発生するもので、過剰なトラフィックを生成し、ネットワークのパフォーマンスを低下させます。トラフィック ストーム制御ポリシーを使用すると、物理インターフェイス上におけるブロードキャスト、未知のマルチキャスト、または未知のユニキャストのトラフィック ストームによって、レイヤ 2 ポート経由の通信が妨害されるのを防ぐことができます。

デフォルトでは、ストーム制御はACIファブリックでは有効になっていません。ACIブリッジドメイン（BD）レイヤ 2 の未知のユニキャストのフラッディングは BD 内でデフォルトで有効になっていますが、管理者が無効にすることができます。その場合、ストーム制御ポリシーはブロードキャストと未知のマルチキャストのトラフィックにのみ適用されます。レイヤ2の未知のユニキャストのフラッディングが BD で有効になっている場合、ストーム制御ポリシーは、ブロードキャストと未知のマルチキャストのトラフィックに加えて、レイヤ2の未知のユニキャストのフラッディングに適用されます。

トラフィック ストーム制御（トラフィック抑制ともいいます）を使用すると、着信するブロードキャスト、マルチキャスト、未知のユニキャストのトラフィックのレベルを1秒間隔でモニタできます。この間に、トラフィック レベル（ポートで使用可能な合計帯域幅のパーセンテージ、または特定のポートで許可される1秒あたりの最大パケット数として表されます）が、設定したトラフィック ストーム制御レベルと比較されます。入力トラフィックが、ポートに設定したトラフィック ストーム制御レベルに到達すると、トラフィック ストーム制御機能によってそのインターバルが終了するまでトラフィックがドロップされます。管理者は、ストーム制御しきい値を超えたときにエラーを発生させるようにモニタリング ポリシーを設定できます。

ストーム制御の注意事項と制約事項

以下のガイドラインと制約事項に従って、トラフィック ストーム制御レベルを設定してください。

- 通常、ファブリック管理者は以下のインターフェイスのファブリック アクセス ポリシーでストーム制御を設定します。
  - 標準トランク インターフェイス。
  - 単一リーフ スイッチ上のダイレクト ポート チャネル。
  - バーチャル ポート チャネル（2 つのリーフ スイッチ上のポート チャネル）。
- リリース 4.2(1) 以降では、ストーム制御のしきい値に達した場合に、次の制約事項に従って、SNMP トラップをCisco Application Centric Infrastructure（ACI）からトリガーできるようになりました。
  - ストーム制御に関連するアクションには、ドロップとシャットダウンの 2 つがあります。シャットダウン アクションでは、インターフェイス トラップが発生しますが、ストームがアクティブまたはクリアであることを示すためのストーム制御トラップは、シャットダウンアクションによっては決定されません。したがって、ポリシーでシャットダウンアクションが設定されているストーム制御トラップは無視する必要があります。
  - ストーム制御ポリシーがオンの状態でポートがフラップすると、統計情報の収集時にクリア トラップとアクティブ トラップが一緒に表示されます。通常、クリア トラップとアクティブ トラップは一緒に表示されませんが、この場合は予期される動作です。
- ポート チャネルおよびバーチャル ポート チャネルでは、ストーム制御値（1 秒あたりのパケット数またはパーセンテージ）はポートチャネルのすべての個別メンバーに適用されます。

（注） Cisco Application Policy Infrastructure Controller（APIC）リリース 1.3(1) およびスイッチ リリース 11.3(1) 以降のスイッチ ハードウェアの場合、ポートチャネル設では、集約ポートのトラフィック抑制は設定値の最大 2 倍になることがあります。新しいハードウェア ポートは slice-0 と slice-1 の 2 つのグループに内部的にさらに分割されています。スライスマップを確認するには、`vsh_lc` コマンドの `show platform internal hal l2 port gpd` を使用して、`Sl` カラムで `slice 0` または `slice 1` を探します。ポート チャネル メンバーがスライス 0 とスライス 1 の両方に該当する場合、式は各スライスに基づいて計算されるため、許可されるストーム制御トラフィックが設定値の 2 倍になることがあります。

- 使用可能な帯域幅のパーセンテージで設定する場合、値100はトラフィック ストーム制御を行わないことを意味し、値 0.01 はすべてのトラフィックを抑制します。
- ハードウェアの制限およびさまざまなサイズのパケットのカウント方式が原因で、レベルのパーセンテージは概数になります。着信トラフィックを構成するフレームのサイズに応じて、実際に適用されるパーセンテージ レベルと設定したパーセンテージ レベルの間には、数パーセントの誤差がある可能性があります。1 秒あたりのパケット数（PPS）の値は、256 バイトに基づいてパーセンテージに変換されます。
- 最大バーストは、通過するトラフィックがないときに許可されるレートの最大累積です。トラフィックが開始されると、最初の間隔では累積レートまでのすべてのトラフィックが許可されます。後続の間隔では、トラフィックは設定されたレートまでのみ許可されます。サポートされる最大数は65535 KBです。設定されたレートがこの値を超えると、PPSとパーセンテージの両方についてこの値で制限されます。
- 累積可能な最大バーストは 512 MB です。
- 最適化されたマルチキャストフラッディング（OMF）モードの出力リーフスイッチでは、トラフィック ストーム制御は適用されません。
- OMF モードではない出力リーフ スイッチでは、トラフィック ストーム制御が適用されます。
- ストーム制御は、スパニング ツリープロトコル（STP）と OSPF トラフィックをポリシングしません。
- FEX のリーフ スイッチでは、ホスト側インターフェイスにはトラフィック ストーム制御を使用できません。
- Cisco Nexus C93128TX、C9396PX、C9396TX、C93120TX、C9332PQ、C9372PX、C9372TX、C9372PX-E、C9372TX-E の各スイッチでは、トラフィック ストーム制御のユニキャスト/マルチキャストの差別化がサポートされていません。
- Cisco Nexus C93128TX、C9396PX、C9396TX、C93120TX、C9332PQ、C9372PX、C9372TX、C9372PX-E、C9372TX-E の各スイッチでは、トラフィック ストーム制御の SNMP トラップがサポートされていません。
- Cisco Nexus C93128TX、C9396PX、C9396TX、C93120TX、C9332PQ、C9372PX、C9372TX、C9372PX-E、C9372TX-E の各スイッチでは、トラフィック ストーム制御トラップがサポートされていません。
- ストーム制御アクションは、物理イーサネット インターフェイスおよびポート チャネル インターフェイスでのみサポートされます。

  リリース4.1(1)以降では、ストーム制御**シャットダウン**オプションがサポートされています。デフォルトの Soak Instance Count を持つインターフェイスに対して**シャットダウン** アクションが選択されると、しきい値を超えるパケットは 3 秒間ドロップされ、ポートは 3 秒間シャットダウンされます。デフォルトのアクションは、**ドロップ**です。**シャットダウン**アクションを選択すると、ユーザーはソーキング間隔を指定するオプションを使用できます。デフォルトのソーキング間隔は 3 秒です。設定可能な範囲は 3 ～ 10 秒です。

- インターフェイスに設定されたデータ プレーン ポリシング（DPP）ポリサーの値がストーム ポリサーの値よりも低い場合、DPP ポリサーが優先されます。DPPポリサーとストーム ポリサーの間に設定されている低い方の値が、設定されたインターフェイスで適用されます。
- リリース 4.2(6) 以降、ストーム ポリサーは、DHCP、ARP、ND、HSRP、PIM、IGMP、および EIGRP プロトコルに対応する、リーフ スイッチのすべての転送制御トラフィックに強制されます。このことは、ブリッジ ドメインが**BD でのフラッディング**または**カプセル化でのフラッディング**のどちらに設定されているかには関係しません。この動作の変更は、EX 以降のリーフスイッチにのみ適用されます。
  - EX スイッチでは、プロトコルの 1 つに対し、スーパーバイザ ポリサーとストーム ポリサーの両方を設定できます。この場合、サーバーが設定されたスーパーバイザ ポリサー レート（制御プレーン ポリシング、CoPP）よりも高いレートでトラフィックを送信すると、ストーム ポリサーはストーム ポリサー レートとして設定されているよりも多くのトラフィックを許可します。着信トラフィック レートがスーパーバイザ ポリサー レート以下の場合、ストーム ポリサーは設定されたストーム トラフィック レートを正しく許可します。この動作は、設定されたスーパーバイザ ポリサーおよびストーム ポリサーのレートに関係なく適用されます。
  - ストーム ポリサーが、指定されたプロトコルのリーフ スイッチで転送されるすべての制御トラフィックに適用されるようになった結果、リーフ スイッチで転送される制御トラフィックがストーム ポリサー ドロップの対象になります。以前のリリースでは、この動作の変更の影響を受けるプロトコルでは、このようなストーム ポリサーのドロップは発生しません。
- トラフィック ストーム制御は、PIM が有効になっているブリッジ ドメインまたは VRF インスタンスのマルチキャスト トラフィックをポリシングできません。
- ストーム コントロール ポリサーがポートチャネル インターフェイスに適用されている場合、許可されるレートが設定されているレートを超えることがあります。ポートチャネルのメンバー リンクが複数のスライスにまたがる場合、許可されるトラフィック レートは、構成されたレートにメンバー リンクがまたがるスライスの数を掛けたものに等しくなります。

  ポートからスライスへのマッピングは、スイッチ モデルによって異なります。

  例として、ストーム ポリサー レートが 10Mbps のメンバー リンク port1、port2、および port3 を持つポートチャネルがあるとします。
  - port1、port2、port3 が slice1 に属している場合、トラフィックは 10Mbps にポリシングされます。
  - port1 と port2 が slice1 に属し、port3 が slice2 に属している場合、トラフィックは 20Mbps にポリシングされます。
  - port1 が slice1 に属し、port2が slice2 に属し、port3 が slice3 に属している場合、トラフィックは 30Mbps にポリシングされます。

GUI を使用したトラフィック ストーム制御ポリシーの設定

手順

ステップ 1 メニュー バーで、[Fabric] をクリックします。

ステップ 2 サブメニュー バーで、[Access Policies] をクリックします。

ステップ 3 **Navigation** ウィンドウで **Policies** を展開します。

ステップ 4 **Interface** を展開します。

ステップ 5 [Storm Control] を右クリックし、[Create Storm Control Interface Policy] を選択します。

ステップ 6 [Create Storm Control Interface Policy] ダイアログボックスで、[Name] フィールドにポリシーの名前を入力します。

ステップ 7 **Configure Storm Control** フィールドで、**All Types** または **Unicast, Broadcast, Multicast** のいずれかのオプション ボタンをクリックします。

（注）
Unicast, Broadcast, Multicast オプション ボタンを選択すると、それぞれのトラフィック タイプで個別にストーム制御を設定することができます。

ステップ 8 [Specify Policy In] フィールドで、[Percentage] または [Packets Per Second] いずれかのオプション ボタンをクリックします。

ステップ 9 [Percentage] を選択した場合は、次の手順を実行します。

a) [Rate] フィールドに、トラフィック レートのパーセンテージを入力します。

ポートで使用可能な合計帯域幅のパーセンテージを指定する 0 ～ 100 の数値を入力します。1 秒の間隔中に入力トラフィックがこのレベルに達するか、それを超えると、トラフィック ストーム制御により、その間隔の残りのトラフィックはドロップされます。値 100 は、トラフィック ストーム制御を行わないことを意味します。値 0 の場合、すべてのトラフィックが抑制されます。

b) [Max Burst Rate] フィールドに、バースト トラフィック レートのパーセンテージを入力します。

ポートで使用可能な合計帯域幅のパーセンテージを指定する 0 ～ 100 の数値を入力します。入力トラフィックがこれ以上になると、トラフィック ストーム制御が開始してトラフィックをドロップされるようになります。

（注）
Max Burst Rate は、**Rate** の値以上でなければなりません。

ステップ 10 [Packets Per Second] を選択した場合は、次の手順を実行します。

a) [Rate] フィールドに、トラフィック レートを 1 秒あたりのパケット数で入力します。

この間、トラフィック レベル（1 秒あたりにポートを通過するパケット数として表される）が、設定したトラフィック ストーム制御レベルと比較されます。入力トラフィックが、ポートに設定したトラフィック ストーム制御レベルに達するかそれを超えると、トラフィック ストーム制御機能によってそのインターバルが終了するまでトラフィックがドロップされます。

b) [Max Burst Rate] フィールドに、バースト トラフィック レートを 1 秒あたりのパケット数で入力します。

この間、トラフィック レベル（1 秒あたりにポートを通過するパケット数として表される）が、設定したバースト トラフィック ストーム制御レベルと比較されます。入力トラフィックが、ポートに設定したトラフィック ストーム制御レベルに達するかそれを超えると、トラフィック ストーム制御機能によってそのインターバルが終了するまでトラフィックがドロップされます。

ステップ 11 **[Storm Control Action]** で [shutdown]を選択し、**[Storm Control Soak Count]** フィールドでデフォルトを調整することで、ポリシー アクションをデフォルトから変更できます。

（注）
デフォルトの Soak Instance Count を持つインターフェイスに対して**シャットダウン** アクションが選択されると、しきい値を超えるパケットは 3 秒間ドロップされ、ポートは 3 秒間シャットダウンされます。

ステップ 12 [Submit] をクリックします。

ステップ 13 ストーム制御インターフェイス ポリシーをインターフェイス ポートに適用します。

a) メニュー バーで、[Fabric] をクリックします。
b) サブメニュー バーで、[Access Policies] をクリックします。
c) **Navigation** ウィンドウで **Interfaces** を展開します。
d) **Leaf Interfaces** を展開します。
e) **Policy Groups** を展開します。
f) **Leaf Policy Groups** を選択します。

（注）
APIC バージョンが 2.x よりも前の場合は、**[Policy Groups]** を選択します。

g) リーフ アクセス ポート ポリシー グループ、PC インターフェイス ポリシー グループ、vPC インターフェイス ポリシー グループ、またはストーム制御ポリシーを適用する PC/vPC オーバーライド ポリシー グループを選択します。
h) [Work] ペインで、[Storm Control Interface Policy] のドロップダウンをクリックし、作成したトラフィック ストーム制御ポリシーを選択します。
i) [送信（Submit）] をクリックします。

NX-OS スタイルの CLI を使用したトラフィック ストーム制御ポリシーの設定

手順

	コマンドまたはアクション	目的

ステップ 1	次のコマンドを入力して PPS ポリシーを作成します。
	例：
	`(config)# template policy-group pg1`
	`(config-pol-grp-if)# storm-control pps 10000 burst-rate 10000`	

ステップ 2	次のコマンドを入力してパーセント ポリシーを作成します。
	例：
	`(config)# template policy-group pg2`
	`(config-pol-grp-if)# storm-control level 50 burst-rate 60`	

ステップ 3	物理ポート、ポート チャネルまたは仮想ポート チャネルでストーム制御を設定します。
	例：
	`[no] storm-control [unicast|multicast|broadcast] level <percentage> [burst-rate <percentage>]`
	`[no] storm-control [unicast|multicast|broadcast] pps <packet-per-second> [burst-rate <packet-per-second>]`
	
	`sd-tb2-ifc1# configure terminal`
	
	`sd-tb2-ifc1(config)# leaf 102`
	
	`sd-tb2-ifc1(config-leaf)# interface ethernet 1/19`
	`sd-tb2-ifc1(config-leaf-if)# storm-control unicast level 35 burst-rate 45`
	`sd-tb2-ifc1(config-leaf-if)# storm-control broadcast level 36 burst-rate 36`
	`sd-tb2-ifc1(config-leaf-if)# storm-control broadcast level 37 burst-rate 38`
	`sd-tb2-ifc1(config-leaf-if)#`	

	コマンドまたはアクション	目的

	`sd-tb2-ifc1# configure terminal`
	
	`sd-tb2-ifc1(config)# leaf 102`
	
	`sd-tb2-ifc1(config-leaf)# interface ethernet 1/19`
	`sd-tb2-ifc1(config-leaf-if)# storm-control broadcast pps 5000 burst-rate 6000`
	`sd-tb2-ifc1(config-leaf-if)# storm-control unicast pps 7000 burst-rate 7000`
	`sd-tb2-ifc1(config-leaf-if)# storm-control unicast pps 8000 burst-rate 10000`
	`sd-tb2-ifc1(config-leaf-if)#`	

ステップ 4	ポリシー アクションを変更するには、次の手順を実行します。
	
	例：
	
	`apic1(config-leaf-if)# storm-control action ?`
	` drop  drop`
	` shutdown  shutdown`	

ステップ 5	ポート **シャットダウン** アクションにのみ適用される soak-instance カウントを設定します。
	
	例：
	
	`apic-ifc1(config-leaf)# int eth 1/27`
	`apic-ifc1(config-leaf-if)# storm-control soak-instance-count ?`
	`<3-10> Storm Control SI-Count Instances`	

ストーム制御 SNMP トラップの設定

ここでは、リーフ スイッチでトラフィック ストーム制御 SNMP トラップを設定する方法について説明します。

MIB 定義のトラップ名を使用して、SNMP トラップのストーム制御を設定することができます。インターフェイスの MIB イベントと、いつストームが検出されてクリアされたかにより、同じリーフのトラップをフィルタリングして、ストームを設定します。ストームは次の 2 つの方法で設定できます。

- 詳細な設定：ユニキャスト、マルチキャスト、ブロードキャストなどのトラフィックのタイプを設定します。
- 詳細でない設定：すべてのタイプのトラフィックを設定します。

ストーム制御のしきい値に達した場合に Cisco ACI から SNMP トラップをトリガーする際の制限の詳細については、ストーム制御の注意事項と制約事項（282ページ）を参照してください。トラフィック ストーム制御トラップでサポートされていない Cisco Nexus スイッチの詳細については、ストーム制御のガイドラインを参照してください。

ストーム トラップ

ストーム トラップは、イベントが発生し、ストームがアクティブまたはクリアされるたびにトリガーされます。

```
cpscEventRev1 NOTIFICATION-TYPE
        OBJECTS   { cpscStatus }
        STATUS     current
        DESCRIPTION
```

実装では、特定のトラフィック タイプに関してインターフェイスでストーム イベントが発生したときに、この通知を送信することになります。

ストーム ステータスは、それぞれブロードキャスト、ユニキャスト、マルチキャスト、および非詳細ラフィック タイプのフィールドである [bcDropIncreased]、[uucDropIncreased]、[mcDropIncreased]、および [dropIncreased] で更新されます。これらは dbgIfStorm MO のフィールドです。詳細設定と非詳細設定では、フラグを使用してストームを設定します。ストームがアクティブな場合、フラグは 1 に設定され、ストームがクリアされると、フラグは 2 に設定されます。次のコマンドのフラグにより、SNMP トラップ トリガーに必要なイベントが生成されます。

```
cat / mit / sys / phys-\ [eth--1 \] / dbgIfStorm / summary
```

```
# Interface Storm Drop Couters
bcDropBytes   :0
bcDropIncreased   :2
childAction    :
dn        :sys/phys-[eth/1]/dbgIfStorm
dropBytes      :0
dropIncreased  :2
mcDropBytes    :0
mcDropIncreased :2
modTs           :never
monPoIDn        :uni/infra/moninfra-default
m               :dbgIfStorm
status          :
uucDropBytes    :0
uucDropIncreased :2
```

第 15 章

MACsec

この章は、次の内容で構成されています。

- MACsec について （291 ページ）
- スイッチ プロファイルの注意事項および制約事項 （293 ページ）
- GUI を使用したファブリック リンクの MACsec の設定 （297 ページ）
- GUI を使用したアクセス リンクの MACsec の設定 （297 ページ）
- APIC GUI を使用した MACsec パラメータの設定 （298 ページ）
- GUI を使用した MACsec キーチェーン ポリシーの設定 （299 ページ）
- NX-OS スタイルの CLI を使用したMACsecの設定 （300 ページ）

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に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 はまたは責任を負う 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。

スイッチ プロファイルの注意事項および制約事項

MACsec は次のスイッチでサポートされます。

- N9K-C93108TC-FX3P
- N9K-C93108TC-FX3（6.0(5) リリース以降）
- N9K-C93108TC-FX
- N9K-C93180YC-FX3
- N9K-C93180YC-FX
- N9K-C93216TC-FX2
- N9K-C93240YC-FX2
- N9K-C9332C
- N9K-C93360YC-FX2
- N9K-C9336C-FX2
- N9K-C9348GC-FXP、10G +のみ
- N9K-C9364C
- N9K-C9364D-GX2A
- N9K-C9348D-GX2A
- N9K-C9332D-GX2B
- N9K-C9408（6.0(2) リリース以降）

MACsec は次のライン カードでサポートされます。

- N9K-X9716D-GX
- N9K-X9736C-FX

次の注意事項および制約事項に従って、スイッチで MACsec を設定します。

- MACsec は10G QSA モジュールではサポートされていません。
- MACsec は Cisco ACI リーフ スイッチの 1G の速度ではサポートされていません。
- Cisco ACI リーフ スイッチとコンピュータホスト間の MACsec は、シスコによって検証されていません。スイッチ間モードは検証され、サポートされています。
- MACsec は、ブレークアウト ポートでサポートされています。
- MACsec はリモート リーフ スイッチでサポートされていません。

- 銅線ポートを使用する場合、銅線ケーブルは 10G モードでピア デバイス（スタンドアロン N9k）に直接接続する必要があります。
- ピアの 10G 銅線 SFP モジュールはサポートされません。
- FEX ポートは MACsec ではサポートされません。
- **must-secure** モードは、ポッド レベルではサポートされていません。
- 「default」という名前の MACsec ポリシーはサポートされていません。
- 自動キー生成は、ファブリック ポートのポッド レベルでのみサポートされます。
- そのノードのファブリック ポートが **[必須セキュア]** モードの MACsec で実行されている場合、ノードの再起動をクリアしないでください。
- MACsec を実行しているポッドに新しいノードを追加する、またはポッド内のノードのステートレス リブートを行うには、ノードをポッドに参加させるために、**must-secure** モードを **should-secure** に変更する必要があります。
- ファブリック リンクが **should-secure** モードである場合にのみ、アップグレードまたはダウングレードを開始します。アップグレードまたはダウングレードが完了したら、モードを **must-secure** に変更できます。**must-secure** モードでアップグレードまたはダウングレードすると、ノードがファブリックへの接続を失います。失われた接続を回復するには、**should-secure** モードで、Cisco Application Policy Infrastructure Controller（APIC）に表示されるノードのファブリック リンクを構成する必要があります。ファブリックが MACsec をサポートしていないバージョンにダウングレードされた場合、ファブリック外のノードが クリーン リブートされる必要があります。
- PC または vPC インターフェイスの場合、MACsec は PC または vPC インターフェイスごとのポリシー グループを使用して展開できます。ポートセレクタは、特定のポートのセットにポリシーを展開するために使用されます。したがって、L3Out インターフェイスに対応する正しいポート セレクタを作成する必要があります。
- 設定をエクスポートする前に、**should-secure** モードで MACsec ポリシーを設定することを推奨します。
- スパイン スイッチ上のすべてのリンクは、ファブリック リンクと見なされます。ただし、スパイン スイッチ リンクを IPN 接続のために使用している場合、そのリンクはアクセス リンクとして扱われます。これらのリンクで MACsec を展開するには、MACsec アクセス ポリシーを使用する必要があります。
- 5.2(3) リリースでは、 マルチポッド スパイン バックツーバックのサポートが追加されました。マルチポッド スパイン バックツーバック での MACsec には、次の注意事項および制約事項が適用されます。
  - バックツーバック リンクはファブリック リンクとして扱われます。スパイン バックツーバック リンクで MACsec を有効にする場合は、MACsec ファブリック ポリシーを作成する必要があります。

MACsec ファブリックポリシーの作成については、 *Cisco APIC* レイヤ *2* ネットワーク設定ガイドの「Configuring MACsec for Fabric Links Using the GUI」の手順を参照してください。

- 両方のバックツーバック リンクで同じ MACsec ポリシーを使用する必要があります。ポッド ポリシーを使用した場合は、両方のポッドで同じ MACsec ポリシーを展開する必要があります。

- リモート リーフ ファブリック リンクを IPN 接続に使用する場合、そのリンクはアクセスリンクとして扱われます。これらのリンクで MACsec を展開するには、MACsec アクセスポリシーを使用する必要があります。
- リモート リーフ スイッチのファブリック リンクに **must-secure** モードを不適切に導入すると、ファブリックへの接続が失われる可能性があります。こうした問題を防ぐため、「must-secure モードの展開 （296 ページ）」で説明している手順に従ってください。
- 新しいキーが空のキーチェーンに追加されるか、アクティブなキーがキーチェーンから削除された場合、MACsec セッションの形成または切断に最大で 1 分かかります。
- スパインスイッチのラインカードまたはファブリックモジュールをリロードする前に、すべての **must-secure** リンクを **should-secure** モードに変更する必要があります。リロードが完了し、セッションが **should-secure** モードになったら、モードを **must-secure** に変更します。
- 暗号スイート AES 128 または Extended Packet Numbering（XPN）のない AES 256 を選択する場合は、Security Association Key（SAK）の有効期限を明示的に指定する必要があります。SAK の有効期限値をデフォルト（「無効」）のままにすると、インターフェイスがランダムにアウトオブサービスになる可能性があります。
- フレームの順序が変更されるプロバイダーネットワーク上で MACsec の使用をサポートするには、リプレイウィンドウが必要です。ウィンドウ内のフレームは順不同で受信できますが、リプレイ保護されません。デフォルトのウィンドウ サイズは 64 です。Cisco APIC GUI または CLI を使用する場合、リプレイ ウィンドウのサイズは、0 ー 2^{32}- 1 の範囲で設定できます。XPN 暗号スイートの場合、最大リプレイ ウィンドウ サイズは 2^{30}-1 です。これより大きなウィンドウ サイズを設定しても、ウィンドウ サイズは 2^{30}-1 に制限されます。暗号スイートを非 XPN 暗号スイートに変更した場合、制限はなく、設定されたウィンドウ サイズが使用されます。
- 5.2(2) リリース以降で Cisco N9K-X9716D-GX ライン カード ファブリック ポートで MACsec を使用していて、それを 5.2(2) より前のリリースにダウングレードした場合、そのような以前のリリースではこのラインカードで MACsec はサポートされません。ただし、MACsec がサポートされていないことによる障害は発生しません。このシナリオでは、ピア リーフ スイッチが MACsec をサポートしている場合、セッションはセキュアな状態で起動します。ただし、スパイン側では、セッションが保留中として表示されます。
- リンク レベル フロー制御（LLFC）およびプライオリティ フロー制御（PFC）は、MACsec ではサポートされません。

- Cisco APIC は、クライアントのインフラストラクチャを介した MACsec の受け渡しをサポートしていません。

must-secure モードの展開

must-secure モードに設定されているポリシーを誤って展開すると、接続が失われる可能性があります。そのような問題を避けるため次の手順に従う必要があります。

- MACsec **must-secure** モードを有効にする前に、各リンク ペアにキーチェーンがあることを確認する必要があります。確実を期すため、ポリシーを **should-secure** モードで展開し、MACsec セッションが想定されるリンクでアクティブになったら、モードを **must-secure** に変更することをお勧めします。
- **[必須セキュア]** に設定されている MACsec ポリシーでキーチェーンの交換を試行すると、リンクがダウンする原因となる可能性があります。この場合は、次の手順に従います。
  1. 新しいキーチェーンを使用している MACsec ポリシーを **[should-secure]** モードに変更します。
  2. 影響を受けるインターフェイスが **[should-secure]** モードを使用しているか確認します。
  3. 新しいキーチェーンを使用するように MACsec ポリシーを更新します。
  4. アクティブな MACsec セッションと関連するインターフェイスが新しいキーチェーンを使用していることを確認します。
  5. MACsec ポリシーを **[必須セキュア]** モードに変更します。
- **must-secure** モードで展開された MACsec ポリシーを無効化/削除するには、次の手順を実行します。
  1. MACsec ポリシーを **[should-secure]** に変更します。
  2. 影響を受けるインターフェイスが **[should-secure]** モードを使用しているか確認します。
  3. MACsec ポリシーを無効/削除します。

キーチェーンの定義

- 開始時刻が **[現在]** のキーチェーンに 1 個のキーが存在します。**must-secure** を、即座にアクティブになるキーを持たないキーチェーンで展開した場合、キーの時刻が来て MACsec セッションが開始されるまで、トラフィックはリンク上でブロックされます。**should-secure** モードが使用されている場合、キーが現在になり、MACsec セッションが開始されるまでトラフィックが暗号化されます。
- 終了時刻が **infinite** のキーチェーンに 1 個のキーが存在する必要があります。キーチェーンの期限が切れると、**must-secure** モードに設定されている影響を受けるインターフェイ

スでトラフィックがブロックされます。設定されたインターフェイス **はセキュア** モード暗号化されていないトラフィック送信します。

- 終了時刻のオーバーラップし、キーの間に移行すると、MACsecセッションを順番に使用されるキーの開始時刻が残っています。

GUI を使用したファブリック リンクの MACsec の設定

手順

ステップ 1 メニュー バーで、**Fabric** > **Fabric Policies** > **Policies** > **MACsec** > **Interfaces** をクリックします。**Navigation** ウィンドウで、**Interfaces** を右クリックして **Create MACsec Fabric Interface Policy** を開き、次の手順を実行します:

a) **Name** フィールドに、MACsec ファブリック インターフェイス ポリシーの名前を入力します。

b) **MACsec Parameters** フィールドで、以前に設定した MACsec パラメータ ポリシーを選択するか、新しいものを作成します。

c) **MACsec Keychain Policy** フィールドで、以前に設定した MACsec パラメータ ポリシーを選択するか、新しいものを作成して、**Submit** を作成します。

MACsec Keychain Policy を作成するには、GUI を使用した MACsec キーチェーン ポリシーの設定 （299 ページ）を参照してください。

ステップ 2 **MACsec Fabric Interface Policy** をファブリック リーフまたはスパイン ポート ポリシー グループに適用するには、**Interfaces** > ***Leaf/Spine*** **Interfaces** > **Policy Groups** > ***Spine/Leaf*** **Port Policy Group_*name*** をクリックします。**Work** ウィンドウで、今作成した **MACsec Fabric Interface Policy** を選択します。

ステップ 3 **MACsec Fabric Interface Policy** をポッド ポリシー グループに適用するには、ナビゲーション ウィンドウで **Pods** > **Policy Groups** > **Pod Policy Group_*name*** をクリックします。**Work** ウィンドウで、今作成した **MACsec Fabric Interface Policy** を選択します。

GUI を使用したアクセス リンクの MACsec の設定

手順

ステップ 1 メニュー バーで、**[ファブリック]** > **[外部アクセス ポリシー]** をクリックします。**Navigation** ウィンドウで、**Policies** > **Interface** > **MACsec** > **Interfaces** をクリックし、**Interfaces** を右クリックして **Create MACsec Fabric Interface Policy** を開き、次の手順を実行します:

a) **Name** フィールドに、MACsec アクセス インターフェイス ポリシーの名前を入力します。
b) **MACsec Parameters** フィールドで、以前に設定した MACsec パラメータ ポリシーを選択するか、新しいものを作成します。
c) **MACsec Keychain Policy** フィールドで、以前に設定した MACsec パラメータ ポリシーを選択するか、新しいものを作成して、**Submit** を作成します。

MACsec Keychain Policy を作成するには、GUI を使用した MACsec キーチェーン ポリシーの設定 （299 ページ）を参照してください。

ステップ 2 **MACsec Access Interface Policy** をファブリック リーフまたはスパイン ポート ポリシー グループに適用するには、**Interfaces** > ***Leaf/Spine*** **Interfaces** > **Policy Groups** > ***Spine/Leaf*** **Policy Group_*name*** をクリックします。**Work** ウィンドウで、今作成した **MACsec Fabric Interface Policy** を選択します。

APIC GUI を使用した MACsec パラメータの設定

手順

ステップ 1 メニュー バーで、**[Fabric]** > **[Access Policies]** の順にクリックします。**ナビゲーション**] ペインで、[をクリックする **インターフェイス ポリシー** > **ポリシー**] を右クリックし、 **MACsec ポリシー** を開く **MACsec アクセス パラメータ ポリシーの作成** し、次のアクションを実行します。

a) **Name** フィールドに、MACsec アクセス パラメータ ポリシーの名前を入力します。
b) **セキュリティ ポリシー** フィールドで、暗号化されたトラフィックのモードを選択し、をクリックして **Submit** 。

（注）
MACsec を展開する前に **セキュア モードをする必要があります** キーチェーンは、影響を受けるインターフェイスに導入する必要があります、またはインターフェイスがダウンします。

ステップ 2 適用する、 **MACsec アクセス パラメータ ポリシー** リーフまたはナビゲーション ペインで、スパイン ポートのポリシー グループをクリックして **インターフェイス ポリシー** > **ポリシー グループ** > **スパイン リーフ/ポリシー Group_ 名** 。**作業**] ペインで、[、 **MACsec アクセス インターフェイス ポリシー** だけを作成します。

GUI を使用した MACsec キーチェーン ポリシーの設定

手順

ステップ 1 メニュー バーで **Fabric** > **Fabric Policies** > **Policies** > **MACsec** > **KeyChains** をクリックします。**Navigation** ウィンドウで、**KeyChains** を右クリックして **Create MACsec Keychain Policy** を開き、次の手順を実行します:

a) **Name** フィールドに、MACsec ファブリック インターフェイス ポリシーの名前を入力します。

b) **MACsec キー ポリシー** テーブルを展開して、キー ポリシーを作成します。

ステップ 2 **MACsec Policy** ダイアログボックスで次の操作を実行します。

a) **Name** フィールドに、MACsec キー ポリシーの名前を入力します。

b) **Key Name** フィールドにキーの名前を入力します (64 文字までの 16 進数)。

（注）
キーチェーンあたり最大 64 のキーがサポートされています。

c) **Pre-shared Key** フィールドに、事前共有キーの情報を入力します。

（注）
- 128 ビットの暗号スイートでは、32 文字の PSK だけが許可されます。
- 256 ビットの暗号スイートでは、64 文字の PSK だけが許可されます。

d) **Start Time** フィールドで、キーが有効になる日付を選択します。

e) **End Time** フィールドで、キーの有効期限が切れる日付を選択します。**Ok** と **Submit** をクリックします。

（注）
キーチェーンで複数のキーを定義する場合には、古いキーから新しいキーへのスムーズな移行を確実にするために、キーの有効期間をオーバーラップさせて定義する必要があります。古いキーの endTime と新しいキーの startTime をオーバー ラップさせてください。

アクセス ポリシーでキーチェーン ポリシーを設定するには、メニュー バーで **Fabric** > **External Access Policies** をクリックします。**Navigation** ウィンドウで **Policies** > **Interface** > **MACsec** > **MACsec KeyChain Policies** をクリックし、**Create MACsec Keychain Policy** を右クリックして開き、上記の手順を実行します。

NX-OS スタイルの CLI を使用したMACsecの設定

手順

ステップ 1 アクセス インターフェイスの MACsec セキュリティ ポリシーの設定

例：

```
apic1# configure
apic1(config)#   template macsec access security-policy accmacsecpol1
apic1(config-macsec-param)#     cipher-suite gcm-aes-128
apic1(config-macsec-param)#     conf-offset offset-30
apic1(config-macsec-param)#     description 'description for mac sec parameters'
apic1(config-macsec-param)#     key-server-priority 1
apic1(config-macsec-param)#     sak-expiry-time 110
apic1(config-macsec-param)#     security-mode must-secure
aapic1(config-macsec-param)#     window-size 1
apic1(config-macsec-param)#     exit
apic1(config)#
```

ステップ 2 アクセス インターフェイスの MACsec キー チェーンを設定します。

PSK は、2 通りの方法で設定できます:

（注）

- 下のキー 12ab に示すように、**psk-string** コマンドを使用してインラインで設定します。PSK は、ログに記録され、公開されるため、安全ではありません。
- キー ab12 で示すように、新しいコマンド **Enter PSK string** を **psk-string** コマンドの後で使用し、個別に入力して設定します。ローカルにエコーされるだけで、ログには記録されないため、PSK は安全です。

例：

```
apic1# configure
apic1(config)#   template macsec access keychain acckeychainpol1
apic1(config-macsec-keychain)#     description 'macsec key chain kc1'
apic1(config-macsec-keychain)#     key 12ab
apic1(config-macsec-keychain-key)#       life-time start 2017-09-19T12:03:15 end
2017-12-19T12:03:15
apic1(config-macsec-keychain-key)#       psk-string 123456789a223456789a323456789abc
apic1(config-macsec-keychain-key)#       exit
apic1(config-macsec-keychain)#     key ab12
apic1(config-macsec-keychain-key)#       life-time start now end infinite
apic1(config-macsec-keychain-key)#       life-time start now end infinite
apic1(config-macsec-keychain-key)# psk-string
Enter PSK string: 123456789a223456789a323456789abc
apic1(config-macsec-keychain-key)# exit
apic1(config-macsec-keychain)# exit
apic1(config)#
```

ステップ 3 アクセス インターフェイスの MACsec インターフェイス ポリシーを設定します:

例：

```
apic1# configure
apic1(config)#   template macsec access interface-policy accmacsecifpol1
apic1(config-macsec-if-policy)#     inherit macsec security-policy accmacsecpol1 keychain
 acckeychainpol1
apic1(config-macsec-if-policy)#     exit
apic1(config)#
```

ステップ 4 MACsec インターフェイス ポリシーをリーフ (またはスパイン) 上のアクセス ンターフェイスに関連付けます:

例：

```
apic1# configure
apic1(config)#   template macsec access interface-policy accmacsecifpol1
apic1(config-macsec-if-policy)#     inherit macsec security-policy accmacsecpol1 keychain
 acckeychainpol1
apic1(config-macsec-if-policy)#     exit
apic1(config)
```

ステップ 5 ファブリック インターフェイス用に MACsec セキュリティ ポリシーを設定します:

例：

```
apic1# configure
apic1(config)#   template macsec fabric security-policy fabmacsecpol1
apic1(config-macsec-param)#     cipher-suite gcm-aes-xpn-128
apic1(config-macsec-param)#     description 'description for mac sec parameters'
apic1(config-macsec-param)#     window-size 1
apic1(config-macsec-param)#     sak-expiry-time 100
apic1(config-macsec-param)#     security-mode must-secure
apic1(config-macsec-param)#     exit
apic1(config)#
```

ステップ 6 ファブリック インターフェイス用に MACsec キー チェーンを設定します:

PSK は、2 通りの方法で設定できます:

（注）

- 下のキー 12ab に示すように、**psk-string** コマンドを使用してインラインで設定します。PSK は、ログに記録され、公開されるため、安全ではありません。
- キー ab12 で示すように、新しいコマンド **Enter PSK string** を **psk-string** コマンドの後で使用し、個別に入力して設定します。ローカルにエコーされるだけで、ログには記録されないため、PSK は安全です。

例：

```
apic1# configure
apic1(config)#   template macsec fabric security-policy fabmacsecpol1
apic1(config-macsec-param)#     cipher-suite gcm-aes-xpn-128
apic1(config-macsec-param)#     description 'description for mac sec parameters'
apic1(config-macsec-param)#     window-size 1
apic1(config-macsec-param)#     sak-expiry-time 100
apic1(config-macsec-param)#     security-mode must-secure
apic1(config-macsec-param)#     exit
apic1(config)#   template macsec fabric keychain fabkeychainpol1
apic1(config-macsec-keychain)#     description 'macsec key chain kc1'
apic1(config-macsec-keychain)#     key 12ab
apic1(config-macsec-keychain-key)#       psk-string 123456789a223456789a323456789abc
apic1(config-macsec-keychain-key)#       life-time start 2016-09-19T12:03:15 end
2017-09-19T12:03:15
```

```
apic1(config-macsec-keychain-key)#       exit
apic1(config-macsec-keychain)#     key cd78
apic1(config-macsec-keychain-key)# psk-string
Enter PSK string: 123456789a223456789a323456789abc
apic1(config-macsec-keychain-key)# life-time start now end infinite
apic1(config-macsec-keychain-key)# exit
apic1(config-macsec-keychain)# exit
apic1(config)#
```

ステップ 7 MACsec インターフェイス ポリシーをリーフ (またはスパイン) 上のファブリック ンターフェイスに関連付けます:

例：

```
apic1# configure
apic1(config)#   leaf 101
apic1(config-leaf)#     fabric-interface ethernet 1/52-53
apic1(config-leaf-if)#       inherit macsec interface-policy fabmacsecifpol2
apic1(config-leaf-if)#       exit
apic1(config-leaf)#
```

第 16 章

ファブリック ポート トラッキング

- ファブリック ポート トラッキングについて （303 ページ）
- GUI を使用したファブリック ポート トラッキングの設定 （304 ページ）

ファブリック ポート トラッキングについて

ポート トラッキング機能は、ファブリック ポートのステータスに基づいて、各リーフ ノードのダウンリンクポートのステータスを管理します。ファブリック ポートはリーフとスパイン ノード間のリンクです。多層トポロジ内の階層 1 と階層 2 のリーフ ノード間のリンク、およびリモート リーフ ノード間のリンク（バックツーバック リンク）も、ファブリック リンクと見なされます。

この機能が有効にされていて、特定のリーフ ノードで動作しているファブリック ポートの数が設定されたしきい値以下になると、外部ノードが他の正常なリーフ ノードにスイッチ オーバーできるように、リーフ ノードのダウンリンク ポートはダウンにされます。動作中のファブリック ポートの数が設定されたしきい値を超えて回復すると、ダウンリンク ポートは回復します。この時点で、ダウンリンク ポートの起動を遅延させるための待機時間が設定されています。リーフ ノードが vPC ピアの一部であり、インフラ ISIS の隣接関係がない場合（ノードが他の vPC ピア リーフ ノードと通信できない場合）、すべてのファブリック ポートがダウンした場合など、ポート トラッキングがトリガーされた場合、ステータスの復元後に vPC ダウンリンク ポートが起動するまでの時間は、vPC 遅延タイマーまたはポート トラッキングで設定された遅延のいずれか長い方になります。非 vPC ダウンリンクポートは、常にポート トラッキングで設定された遅延タイマーに従います。

Cisco Application Centric Infrastructure（ACI）スイッチ リリース 14.2(1) 以降、ファブリック インフラ ISIS 隣接のステータス（`aggFabAdjOperSt` で表されます。これは管理対象オブジェクト クラス `isisDom` の属性 です）も、ダウンリンク ポートのシャットダウンをトリガーするための代替条件としてチェックされます。このチェックは、特定のリーフ スイッチのファブリック ポートがアップしているもののが、別の理由でリーフ ノードが他の Cisco ACI ノードへの到達可能性を失った場合を考慮に入れて、行われます。この条件は、動作可能なファブリック ポートの最小数などの他のパラメータに関係なく、機能が有効になっている場合は常にチェックされます。ただし、これはリモート リーフ ノードには適用できません。そのようなノードはファブリック インフラの到達可能性について ISIS に依存していないためです。

Cisco ACI スイッチ リリース 15.0(1) 以降、[APIC ポートを含める（Include APIC ports）] オプションがサポートされています。このオプションは、デフォルトで無効です。このオプションが無効になっている場合、ポート トラッキングは、ユーザー トラフィック用に設定されたダウンリンク ポート （つまり、EPG または L3Out によって使用されているポート）のみをダウン状態にしますが、Cisco Application Policy Infrastructure Controller（APIC）に接続されているダウンリンク ポートまたは未使用のポートはダウン状態にしません。このオプションを有効にすると、ポート トラッキングによってリーフ ノードのすべてのダウンリンク ポートがダウン状態にされます。リリース 15.0(1) より前のリリースでは、ユーザー トラフィック用に構成されたダウンリンク ポートは、Cisco APIC に接続されたポートがダウン状態になっていなかったときにダウン状態にされます。ポート トラッキングを構成して、Cisco APIC に接続されたポートをダウン状態にすることはできませんでした。

（注） ポート トラッキングは、各リーフノードでポートを停止または起動する条件をチェックします。

FEX ファブリック ポート（FEX と FEX の親リーフノードを接続するネットワーク インターフェイス、NIF）は、ポート トラッキングの影響を受けません。

GUI を使用したファブリック ポート トラッキングの設定

この手順では、Cisco Application Policy Infrastructure Controller（APIC）GUIを使用してポートトラック機能を設定します。

手順

ステップ 1 メニュー バーで、**[システム（System）]** > **[システム設定（System Settings）]** 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、**[ポート トラッキング（Port Tracking）]** を選択します。

ステップ 3 **[ポート トラッキングの状態（Port tracking state）]** パラメータで **[on]** を選択して、ファブリック ポート トラッキングを有効にします。

ステップ 4 **[遅延復元タイマー（Delay restore timer）]** パラメータには、時間を秒単位で指定します。

このパラメータは、ファブリック ポートの状態とインフラ ISIS 隣接関係が復元された後、リーフノードがダウンリンク ポートを起動するまでの時間を決定します。

ステップ 5 **[ポートトラッキングをトリガーするアクティブなファブリック ポートの数（Number of active fabric ports that triggers port tracking）]** パラメータを設定します。

リーフ ノード上の動作可能なファブリック ポートの数が設定された数以下になると、リーフノードはダウンリンク ポートをダウンさせます。

ステップ 6 （任意） [Include APIC ports when port tracking is trigger]チェックボックスをオンにします。

このパラメータを有効にすると、ポート トラッキングがトリガーされたときに Cisco APIC に接続されているダウンリンク ポートとユーザー トラフィックのダウンリンク ポートがダウンします。このオプションは、Cisco APIC が高可用性のために 2 つの異なるリーフ ノードに接続されている場合を除き、オンにしないでください。

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。