Cisco Nexus 5000 シリーズ NX-OS FCoE オペレーション ガイド リリース 5.1(3)N1(1)

Cisco Nexus 5000 プラットフォーム スイッチ用
および Cisco Nexus 5500 プラットフォーム スイッチ用

2011 年 12 月 5 日

Text Part Number: OL-28440-01-J

【注意】シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。

本書は、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。

また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

Cisco Nexus 5000 シリーズ NX-OS FCoE オペレーション ガイド リリース 5.1(3)N1(1)

CONTENTS

はじめに

ここでは、『*Cisco Nexus 5000 シリーズ NX-OS FCoE オペレーション ガイド リリース 5.1(3)N1(1)*』の対象読者、構成、および表記法について説明します。また、関連マニュアルの入手方法についても説明します。

この章では、次の事項について説明します。

対象読者

このマニュアルは、Cisco Nexus 5000 プラットフォーム スイッチおよび Cisco Nexus 5500 プラットフォーム スイッチの設定および保守を担当する、経験豊富なネットワーク管理者を対象にしています。

表記法

コマンドの説明には、次のような表記法が使用されます。

表記法	説明
bold	太字の文字は、表示どおりにユーザが入力するコマンドおよびキーワードです。
italic	イタリック体の文字は、ユーザが値を入力する引数です。
[x]	角カッコで囲まれているものは、省略可能な要素（キーワードまたは引数）です。
[x | y]	いずれか 1 つを選択できる省略可能なキーワードや引数は、角カッコで囲み、縦棒で区切って示しています。
{x | y}	必ずいずれか 1 つを選択しなければならない必須キーワードや引数は、波カッコで囲み、縦棒で区切って示しています。

[x {y | z}]	角カッコまたは波カッコが入れ子になっている箇所は、任意または必須の要素内の任意または必須の選択肢であることを表します。角カッコ内の波カッコと縦棒は、省略可能な要素内で選択すべき必須の要素を示しています。
variable	ユーザが値を入力する変数であることを表します。イタリック体が使用できない場合に使用されます。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。

出力例では、次の表記法を使用しています。

表記法	説明
screen フォント	スイッチが表示する端末セッションおよび情報は、screen フォントで示しています。
太字の screen フォント	ユーザが入力しなければならない情報は、太字の screen フォントで示しています。
イタリック体の screen フォント	ユーザが値を指定する引数は、イタリック体の screen フォントで示しています。
< >	パスワードのように出力されない文字は、山カッコ（< >）で囲んで示しています。
[ ]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!、#	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「*注釈*」です。役立つ情報やこのマニュアルに記載されていない参照資料を紹介しています。

注意 「*要注意*」の意味です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。

関連資料

Cisco Nexus 5000 シリーズ スイッチおよび Cisco Nexus 2000 シリーズ ファブリック エクステンダのマニュアルは、次の URL から入手できます。

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、次の URL で、毎月更新される『*What's New in Cisco Product Documentation*』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

新機能および変更された機能に関する情報

この章では、『Cisco Nexus 5000 シリーズ NX-OS FCoE オペレーション ガイド リリース 5.1(3)N1(1)』の新機能および変更された機能に関するリリース固有の情報を示します。このマニュアルの最新バージョンは、次のシスコ Web サイトから入手できます。

http://www.cisco.com/en/US/products/ps9670/products_installation_and_configuration_guides_list.html

Cisco NX-OS Release 5.x に関するその他の情報については、次のシスコ Web サイトから入手できる『*Cisco Nexus 5000 Series Switch NX-OS Release Notes*』を参照してください。

http://www.cisco.com/en/US/products/ps9670/prod_release_notes_list.html

表 1 に、Cisco Nexus 5000 シリーズ NX-OS FCoE オペレーション ガイド リリース 5.1(3)N1(1) に記載されている新機能と変更された機能を示します。

表 1　　Release 5.1(3)N1(1) の新機能および変更された機能

機能	説明	変更されたリリース	参照先
FCoE NPV	この機能が導入されました。	5.1(3)N1(1)	第 6 章「FCoE NPV の使用」

CHAPTER 1

Fibre Channel Over Ethernet の動作

この章の内容は、次のとおりです。

概要

Cisco Nexus 5000 シリーズ スイッチでは 2009 年から FCoE をサポートしています。データセンターでの FCoE の採用が増えて、必要になった設計および運用上の考慮事項があります。このマニュアルでは、これらの考慮事項について説明し、Cisco Nexus 5000 シリーズ スイッチを使用した FCoE ソリューションの導入方法および実装方法に関するガイドラインを示します。

FCoE の考慮事項

この項では、次のトピックについて取り上げます。

SAN ファブリック分離の維持

ハイ アベイラビリティ（HA）は、すべてのデータセンター設計で必要です。これは、ポート レベル、スーパーバイザ レベル、さらには物理ネットワーク レベルのいずれで HA を使用して実現するのかを問いません。ファイバ チャネル ストレージ エリア ネットワーク（FC SAN）では、一般に SAN A および SAN B（またはファブリック A およびファブリック B）と呼ばれる、物理的に異なりながら完全に一致する 2 つのネットワークを構築することによってハイ アベイラビリティを実現します。これらのネットワークでは、データセンターの LAN ネットワークとは異なり、互いに完全に物理的に独立しており、互いを認識しません。ストレージ トラフィックに適切なサービスを提供するために、ホストのオペレーティング システムとドライバに応じて、2 系統の独立したネットワーク間でアプリケーション側からトラフィックをロード バランシング、つまり「複数パス化」できます。この必須の分離は、データセンターのイーサネット LAN と並んで、FCoE ネットワーク構築の重要な要素です。

この項では、次のトピックについて取り上げます。

ファブリックごとに異なる FC-MAP の維持

FC-MAP は、スイッチが属しているファブリックを識別する FCoE スイッチの特性です。たとえば、ファブリック A の FC-MAP と、これとは異なるファブリック B の FC-MAP が存在する可能性があります。FCoE スイッチの具体的な FC-MAP 値を設定すると、さまざまなファブリックに属するように特定のスイッチを指定できます。

FCoE 環境でファブリックの分離を維持するには、SAN ファブリックごとに異なる FC-MAP 値を使用することを推奨します。Cisco Nexus 5000 シリーズ スイッチの FC-MAP 値は FCoE 対応デバイスのアドレス指定に使用されるため、FC-MAP 値を変更する処理により、スイッチにログインしているすべてのホストに中断が発生します。この中断があるため、FC-MAP はスイッチの初期設定の一部として設定することを推奨します。

デフォルトでは、**feature fcoe** コマンドを使用して Cisco Nexus 5000 シリーズ スイッチで FCoE をイネーブルにすると、デフォルトの FC-MAP がスイッチに割り当てられます。イーサネット ファブリックで FCoE がイネーブルのスイッチ間の SAN A と B SAN の分離を確保する最も簡単な方法は、ファブリック B に属するすべてのスイッチの FC-MAP 値をデフォルト以外の値に変更することです。これにより、FCoE スイッチは誤ったファブリックに加入できなくなり、FC および FCoE トラフィックの要件である SAN の分離を行いやすくなります。

スイッチの FC-MAP を変更するには、次の手順を実行します。

```
switch# configure terminal
switch(config)# fcoe fcmap 0e.fc.2a
```

（注）　スイッチの FC-MAP 値を変更する処理は、接続されているすべての FCoE ホストを中断させ、ホストはファブリックに再度ログインする必要があります。したがって、スイッチを設置して初期設定するときか、メンテナンス ウィンドウの間で、FC-MAP を変更することを推奨します。

（注）　Cisco Nexus 5000 シリーズ スイッチの FC-MAP のデフォルト値は、0E.FC.00 です。FC-MAP の設定可能な値の範囲は OE.FC.00 ～ 0E.FC.FF です。

VLAN から VSAN への番号付け

FCoE のファブリックを設定する場合、最初の手順は、1 つの VSAN の FC トラフィックがイーサネット ネットワークを通過できるようにする､VLAN から VSAN へのマッピングの作成です。 ストレージ トラフィックを他のすべてのイーサネット VLAN から切り離すために、FCoE トラフィック専用 VLAN を設けることがベスト プラクティスです。また、VLAN 1、VSAN 1 または設定されたネイティブ VLAN を FCoE ネットワークに割り当てないことをお勧めします。一般的にこれらの VLAN/VSAN は管理トラフィックに使用されるか、他に VLAN または VSAN が割り当てられていないデバイスに使用されます。FCoE VLAN としての VLAN 1 の使用は、Cisco NX-OS Release 5.0(1)N1(2) 以降のリリースを実行している Cisco Nexus 5000 シリーズ スイッチではサポートされません。

VLAN から VSAN へのマッピングは、1 対 1 の関係です。単一 VLAN インスタンスに対する複数 VSAN のマッピングはサポートされていません。FCoE VLAN/VSAN マッピングの VLAN インスタンスと VSAN インスタンスは、いずれも、ハードウェア VLAN リソースを消費することに注意してください。現在、Cisco Nexus 5000 シリーズ スイッチでは、最大 31 個のサポート対象 VLAN/VSAN マッピングを持つことができます。VLAN と VSAN の番号は 1 ～ 4096 の範囲で指定できます。

FCoE VLAN は、何といってもストレージ トラフィックのコンテナである点が、一般的なイーサネット VLAN とは異なります。MAC ラーニング、ブロードキャスト、フラッディングは発生せず、サブネットにマッピングされません。FCoE VLAN は、単に、指定された FC VSAN のトラフィックを伝送し、ネットワークを通過する可能性のある他のイーサネット VLAN からの分離を維持するために使用されます。

設定ミスのあったときの混乱やサービスの中断を避けるために、SAN A と SAN B のいずれにも、異なる FCoE VLAN 番号および VSAN 番号を設定することをお勧めします。2 個のファブリック間で同じ VLAN または VSAN の番号を使用すると、設定ミスまたはケーブル配線ミスの場合に、両方の SAN ファブリックをマージするおそれがあります。SAN A スイッチには SAN A VLAN のみを定義する（逆も同様）こともベスト プラクティスです。

ホスト側 FCoE ポートは、ネイティブ VLAN、FCoE VLAN、およびホスト アプリケーションに必要なその他のすべてのイーサネット VLAN を伝送するトランク ポートとして設定する必要があります。ホスト側ポートは、**spanning-tree port type edge** [**trunk**] インターフェイス レベル コマンドを使用して、スパニングツリー エッジ ポートとして設定する必要もあります。

（注）
- FCoE Initialization Protocol（FIP）はネイティブ VLAN を使用するため、すべての FCoE リンクは、FCoE VLAN およびネイティブ VLAN を伝送するようにトランキングする必要があります。
- FCoE VSAN は、VLAN にマッピングする前に、設定されている必要があり、Cisco Nexus 5000 シリーズ スイッチの VSAN データベースに存在する必要があります
- VLAN 1 では FCoE をイネーブルにできません

FCoE およびスパニングツリー プロトコルの考慮事項

ネイティブ FC にはループされた環境の概念がないため、イーサネット環境でスパニングツリー プロトコル（STP）に似たプロトコルは必要ありません。一方、イーサネット ファブリックに FCoE を配置する場合、STP はロスレス イーサネット クラウド越しにホストに接続する FCoE VLAN（VF ポート）で動作します。このロスレス クラウドは、通常は、DCB ブリッジまたは FIP スヌーピングのデバイスで構成されます。このため、FCoE を展開する場合に従う必要がある STP の設定に関するいくつかの推奨事項があります。目的は、SAN A、SAN B、およびイーサネット ファブリック間に独立した STP トポロジを実装することです。これにより、イーサネット トポロジの変更がストレージ トラフィックに影響を与えなくなります。

（注）　STP は 2 台の FCF 間の VE ポート接続の FCoE VLAN では実行されません。

（注）　Cisco Nexus 5000 シリーズ スイッチの Cisco NXOS Release 5.0(1)N1(1) 以降では、STP は、接続されたホストに直接接続する VF ポートの FCoE VLAN で STP は実行されません（Cisco Nexus 2232 ファブリック エクステンダへのホスト接続を含む）。STP は、DCB クラウドまたは FIP スヌーピング デバイス経由でホストに接続する VF ポートで引き続き実行されます。

（注）　Cisco NXOS Release 4.2(1)N2（1a）以前のリリースでは、STP は、すべての VF ポート接続用の FCoE VLAN で動作します（直接接続されているホストまたは DCB クラウドを介して接続されたホスト）。このため、スパニングツリー ポート タイプ エッジ トランクとして VF ポートを設定する必要があります

この項では、次のトピックについて取り上げます。

- 「デュアル ファブリック FCoE 導入のための MST インスタンス」（P.1-4）
- 「デュアル ファブリック FCoE 導入のための PVST+」（P.1-5）

デュアル ファブリック FCoE 導入のための MST インスタンス

イーサネット環境で複数インスタンス STP を実行する場合、同じ MST 領域内のすべてのスイッチは、同じインスタンスへの VLAN マッピングを持つ必要があります。このために、すべての VLAN をすべてのスイッチに定義する必要はありません。MST を使用している環境で FCoE を実行するときは、SAN A に属する FCoE VLAN 専用の MST インスタンスと、SAN B に属する FCoE VLAN 専用の MST インスタンスを持つことを推奨します。これらのインスタンスは、通常のイーサネット VLAN を含むすべてのインスタンスと分離する必要があります。この例では、ファブリック A の FCoE VLAN が VLAN 20 ～ 29 で、ファブリック B の FCoE VLAN が VLAN 30 ～ 39 であることを示します。

スパニングツリー MST 設定

- name FCoE-Fabric
- revision 5
- instance 5 vlan 1-19,40-3967,4048-4093
- instance 10 vlan 20-29
- instance 15 vlan 30-39

上記の設定では、インスタンス 5 はネイティブ イーサネット VLAN にマッピングし、インスタンス 10 はファブリック A（20-29）の VLAN にマッピングし、インスタンス 15 はファブリック B（30-39）の VLAN にマッピングします。

MST の設定要件のために、同じ MST 領域内のすべてのスイッチは、SAN A と B SAN の両方のインスタンスを含む、同じ MST 設定を持つ必要があります。つまり、SAN A に参加しているスイッチは、SAN B VLAN 用の別のインスタンスを使用した MST 設定も含むことになります。ただし、SAN A のスイッチでは、これらの SAN B VLAN を定義しません。

デュアル ファブリック FCoE 導入のための PVST+

PVST を実行している場合は、各 VLAN にすでに独自のスパニングツリー トポロジが存在しています。各 SAN ファブリックの FCoE トラフィックは異なる個別 VLAN によって定義されているため、PVST+ は SAN A、SAN B、およびイーサネット ファブリックに含まれる VLAN のスパニングツリー ドメインを自動的に分離します。

FCoE および仮想ポート チャネル（vPC）の考慮事項

仮想ポート チャネル（vPC）は、1 つのデバイスが複数のアップストリーム デバイスに接続し、イーサネット ループによるスパニングツリー ブロッキング パスの影響なしですべての使用可能なリンクを転送できるイーサネット機能です。vPC は 3 通りの状況で役立ちます。

1. 2 台のアップストリーム スイッチにサーバを接続
2. 2 台のアップストリーム Nexus 5X00 に FEX を接続
3. 2 台のアップストリーム スイッチにスイッチを接続

いずれのシナリオでも、アップストリーム スイッチは、仮想ポート チャネル機能をサポートする必要があります。ダウンストリーム デバイスは、vPC を認識せず、単に、標準イーサネット ポート チャネルとして接続を認識します。

ネイティブ FC における SAN A と SAN B の物理的分離の要件が原因で、vPC 上では FCoE トラフィックを実行できませんが、ホストからファーストホップ FCoE デバイスに対して、同じ物理インフラストラクチャで FCoE および vPC を並列で実行することはできます。このトポロジを設定するには、次の事項を考慮する必要があります。

- ホストは、ファブリック A の Cisco Nexus 5000 シリーズ スイッチに接続するリンクと、ファブリック B の Cisco Nexus 5000 シリーズ スイッチに接続するリンクの 2 個の 10G リンクだけを使用してアップストリーム Cisco Nexus 5000 シリーズ vPC ペア スイッチに接続する必要があります。ポート 1 個だけが各スイッチに向かうため、一般に *シングル ポート vPC* と呼ばれます。
- vPC トポロジをサポートするためには、ホストに第 2 世代 CNA が必要です。

（注）

- FCoE および vPC は、単一ポートによってホスト接続された vPC でのみ並列実行できます。FCoE と、FEX および Cisco Nexus 5000 シリーズ スイッチの間またはスイッチの 2 レイヤ間の vPC はサポートされません。
- 各アクセス デバイスへのリンクを複数含む FCoE および vPC はサポートされません。FCoE と共存する vPC は各 vPC ピア デバイスへのリンクを 1 つだけ含む必要があります。
- 同じ SAN ファブリック内のスイッチ（FCF）をまたがる vPC はサポートされません。各 vPC ピアは、異なるファブリックに含まれる必要があります。つまり、SAN A に 1 つのピア、SAN B に 1 つのピアです。

この項では、次のトピックについて取り上げます。

CNA を使用する vPC の必須チーミング ドライバ

ホストをアップストリームの vPC スイッチ ペアに接続する場合、ホスト側からの唯一の要件は、NIC インターフェイスでリンク集約をサポートすることです。これは、Link Aggregation Control Protocol（LACP）または動作に対する標準 802.3ad *ポート チャネル モード*を使用して実現できます。ホスト オペレーティング システムまたはネイティブ CNA ハードウェアで、これらのオプションの 1 つをサポートしていることを確認することが重要です。

第 2 世代 CNA の要件

vPC に設定されたアップストリーム Cisco Nexus 5000 シリーズ スイッチに、CNA を搭載したホストを接続するときは、Emulex と QLogic の両方から提供されている、第 2 世代 CNA が必要です。これは、ホスト接続に FCoE トラフィックが含まれるかどうかには関係ありません。これらの第 2 世代 CNA は、vPC（イーサネットのみ）、FCoE、または FCoE+vPC の設定を持つ Cisco Nexus 2232 ファブリック エクステンダにホスト接続から接続する場合にも必要です。

CNA を介したイーサネット トラフィックおよび FC トラフィックの表示

現在、CNA では、イーサネット NIC とファイバ チャネル HBA の 2 種類のアダプタをホスト オペレーティング システムに提示します。これらのアダプタは CNA の同じ 10GE ポートに対応しますが、オペレーティング システムに対しては、完全にわかれた物理的に独立した 2 個のインターフェイスとして表示されます。このアダプタ ポート バーチャライゼーションがあるため、NIC を使用するイーサネット ファブリックのトポロジと、HBA を使用する FC ファブリックのトポロジの 2 種類のトポロジを、トラフィック タイプに基づいて作成できます。

FCoE および vPC をホストから並列実行する場合、たとえば、提示される NIC インターフェイスにポート チャネルを設定し、CNA から OS に提示される FC HBA に SAN マルチパスまたはその他の SAN HA メカニズムを設定します。現在、同じネットワークで FCoE を実行するときは、ホスト側の vPC ポート チャネルで 2X10GE リンクだけを使用する必要があります。各 10GE リンクがアップストリーム vPC スイッチへの単一の接続を提供するために使用されます。

図 1-1　CNA を使用したイーサネットおよび FC トラフィック

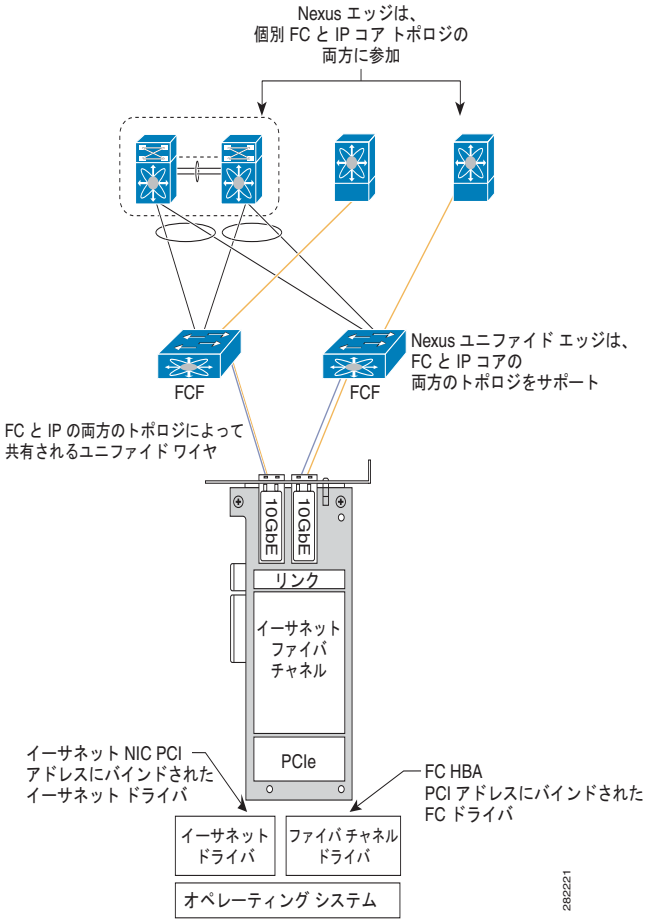


図 1-2　アダプタのコントロール パネル表示

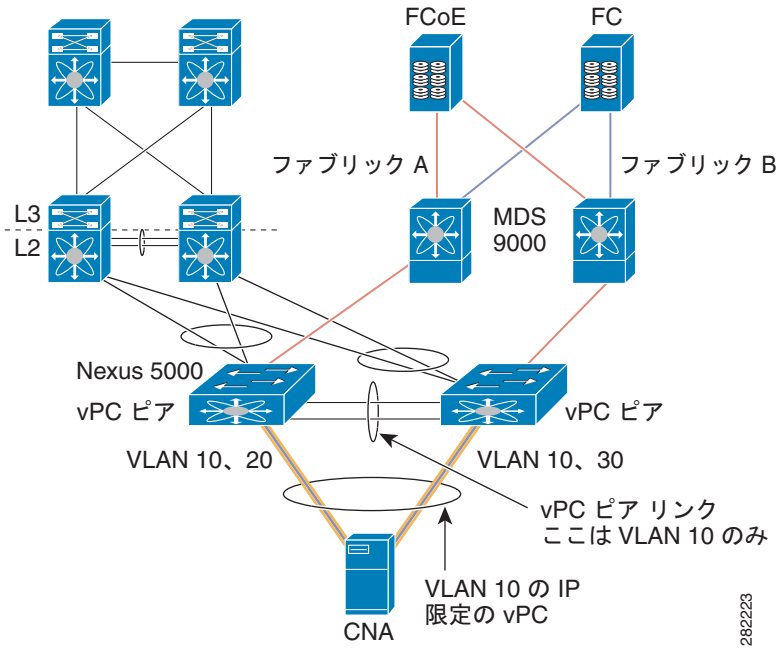
（注）

- ホストからの統合ネットワークを介した VPC + FCoE では、ホストがポート チャネル機能をサポートする必要があります（LACP または「ポート チャネル モード ON」）。サポート マトリクスについては、個々の CNA および OS のベンダーに確認してください。
- 統合ネットワークを介した VPC + FCoE は、ホストとファースト ホップ Nexus 5000 または Nexus 5000/2232 ペアの間でだけサポートされます。統合されたネットワークの VPC および FCoE は、アクセス レイヤ越しや、Nexus 7000 プラットフォームに接続されたホストではサポートされません。
- vPC および FCoE は、ファースト ホップ アクセス デバイスを超えて同じネットワーク上で共存できません。

vPC での FCoE VLAN 設定

通常、同じポート チャネルに属するインターフェイスには同じポート設定を定義する必要があります。これには、VLAN 設定が含まれます。ただし、vPC の接続と並んでファブリックの分離を維持するためには、1 個のアップリンクに SAN A の FCoE VLAN を宣言し、もう 1 個のアップリンクに SAN B の FCoE VLAN を宣言する必要があります。これは推奨されるベスト プラクティス設定です。図 1-3 に、vPC および FCoE を同時に実行する Cisco Nexus 5000 シリーズ スイッチに接続されたホストを示します。

図 1-3　vPC トポロジでの FCoE VLAN 設定



長距離 FCoE に合わせたバッファ割り当ての変更

Cisco Nexus 5000 シリーズ スイッチの Cisco NXOS Release 5.0(1)N1(1) 以降では、VE ポート間の距離の延長をサポートするためにポート バッファの割り当ておよび xon と xoff しきい値を調整できます。FCoE トラフィック（または任意の「no-drop」トラフィック）を伝送するよう設定されている場合、各ポートに設定されるデフォルトの距離は、300 m です。このサポート距離は、ダウンストリーム デバイスに向けて PAUSE が開始される時刻と、このダウンストリーム デバイスがこの PAUSE フレームを処理してフレームの送信を停止する時刻の間に、通過中にフレームを取り込むために割り当てられる利用可能なバッファ スペースの量に基づきます。このポートごとのバッファ割り当ておよび設定は、リンクの両端の 2 ポートの間で一致している必要があります（ホスト CNA ポートも含む）。これは、バッファ間クレジットがネイティブ FC 環境の 2 台のデバイス間で初期化される方法と似ています。

FCoE に現在割り当てられている Xon のしきい値およびバッファ サイズは、buffer-size - xon = 300 m の FCoE フレームに相当します。Nexus 5000 シリーズ スイッチの class-fcoe（すべての no-drop クラス）のデフォルト設定パラメータを次に示します。

- qos-group 1
- q-size: 76800, HW MTU: 2400 (2240 configured)
- drop-type: no-drop, xon: 128, xoff: 240

2 台の FCoE 対応スイッチ（VE ポートで 2 台の FCF を接続）の間の FCoE トラフィックのために 3000 m の距離をサポートするには、FCoE サービス クラス class-fcoe のバッファ割り当ておよび xon と xoff の値を変更する必要があります。これは、Quality of Service 設定を編集することで実現できます。この設定の例は、『Nexus 5000 Configuration Guide』の「Configuring NO-Drop Buffer Threshold」セクションで参照できます。

http://www.cisco.com/en/US/docs/switches/datacenter/nexus5000/sw/qos/502_n1_1/Cisco_Nexus_5000_Series_NX-OS_Quality_of_Service_Configuration_Guide_Rel_502_N1_1.pdf

3000 m までの no-drop サービスをサポートするために必要なしきい値を次の表に示します。

3000 m no-drop クラス用の設定	バッファ サイズ	一時停止しきい値（XOFF）	復帰しきい値（XON）
Nexus 5000 シリーズ	143680 バイト	58860 バイト	38400 バイト
Nexus 5500 プラットフォーム	152000 バイト	103360 バイト	83520 バイト

FCoE の統合リンクおよび専用リンク

FCoE は転送にイーサネット ファブリックを使用するため、同じインフラストラクチャにイーサネット LAN トラフィックと SAN ストレージ トラフィックの両方を統合することが可能です。統合は複数のレベルがあります。ネットワークの統合とデバイスの統合の 2 レベルが最も一般的であり、以下に説明します。

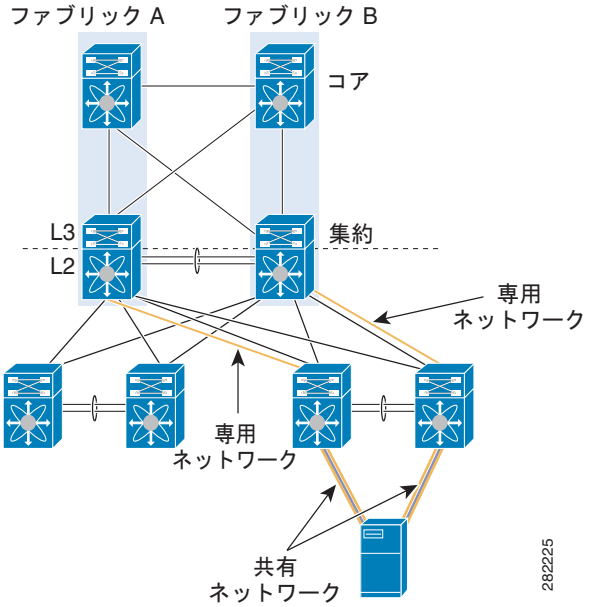
リンク統合は、イーサネット LAN トラフィックおよび SAN ストレージ トラフィックで、ホストとスイッチ間または 2 台のスイッチ間で同じ物理ネットワークを共有している場合を指します。

デバイスの統合は、イーサネット LAN トラフィックとストレージ SAN トラフィックが同じスイッチング デバイスを通過する一方で、専用のネットワークまたはスイッチ ポートを使用して分離が維持されている場合を指します。

このマニュアルに記載されているトポロジでは、FCoE トラフィックのスコープを説明する 2 つの用語を使用します。FCoE とネイティブ イーサネット トラフィックが同時に同じリンクを使用する「統合リンク」と、FCoE およびネイティブ イーサネット トラフィックで 2 個の分離された DCB イーサネット リンクを使用する「専用リンク」です。ここでは、統合リンクおよび専用リンクが妥当な、データセンター ネットワークのさまざまな場所について説明します。

図 1-4 に、専用リンクと統合リンクの例を示します。ホストからアクセス デバイスに接続されているネットワークは、イーサネット トラフィックと FCoE トラフィックの両方を伝送する統合リンクです。アクセスから集約への移動には専用リンクがあります。イーサネット トラフィック専用の青いネットワークと、FCoE トラフィック専用のオレンジ色のネットワークです。

図 1-4　統合リンクおよび専用リンク



この項では、次のトピックについて取り上げます。

- 「統合リンクが妥当なケース」（P.1-11）
- 「専用ネットワークが妥当なケース」（P.1-12）

統合リンクが妥当なケース

アクセス レイヤの FCoE の利点の 1 つが同じ物理ネットワークおよび同じ物理デバイスに FC SAN とイーサネット LAN を統合する機能です。この統合により、データセンターで LAN および SAN ネットワークの両方を実行するために必要なアクセス スイッチ、ホスト アダプタ、ケーブル、および光カードの数が減ることにより、設備支出が大幅に節約されます。この統合は、サーバへの 10GE が大量の帯域幅を提供できることによって可能になります。現在のデータセンターでは、イーサネット トラフィック専用の 10 ギガビット イーサネットを転送しているサーバはわずかであるため、ホスト アプリケーションのパフォーマンスに影響を及ぼすことなく、これらの共通ネットワークを共有する追加のストレージ トラフィックを収容する余裕があります。

また、CNA の動作と、LAN および SAN ネットワークの両方に対応する異なる物理デバイスをホスト アプリケーションに提示する機能により、ホスト レベルで FC HA から Ethernet HA を分離できます。これは、HBA で別々の FC マルチパスのオプションを使用しながら、NIC で別々のイーサネット チーミング オプションを使用することによって実現されます。これらのチーミング オプションは、使用しているオペレーティング システムおよび CNA によって異なります。

アクセス レイヤを越えて移動するとき、オーバーサブスクライブ比率とイーサネットの帯域幅プロビジョニングによって、使用可能な超過帯域幅の量およびデータセンター内で統合リンクを実行する場合と専用リンク実行する場合のメリットが決まります。

専用ネットワークが妥当なケース

LAN と SAN ネットワークのハイ アベイラビリティ要件は大きく異なります。イーサネットでは、互いへのマルチホーミング デバイスによって HA を実現し（部分/完全メッシュ）ファイバ チャネル（および FCoE）では、2 系統の物理的に独立したネットワークを構築することによって HA を実現します。この両方の要件は、FCoE とイーサネットを組み合わせるネットワークで満たされている必要があります。

イーサネット HA モデルでは、スパニングツリー プロトコルに関する一部の課題を解決することによってイーサネット データセンターの設計を改善する、複数の拡張が行われています。一例として、Nexus 製品スイートに搭載されている仮想ポート チャネリング機能があります。vPC の特質は、すべてのアップリンクをブロックするスパニングツリーなしで、複数のアップストリーム デバイスに複数のパスを転送できることです。これは、イーサネット トラフィックには役立ちますが、FC/FCoE に必要な SAN A/SAN B の分離は失われます。

したがって、多くの場合、イーサネット トラフィックとストレージ トラフィックで個別に専用ネットワークを使用することが推奨されます。専用ネットワークを使用すると、vPC などの拡張イーサネット機能を利用するようにイーサネット リンクを設定でき、ファブリックの分離の要件に基づいてストレージ リンクを設定できます。これは、アップストリーム LAN アグリゲーションまたは SAN コア デバイスにアクセス スイッチを接続する場合に、特に一般的です。

Cisco Nexus 5000 シリーズ スイッチ FCoE の考慮事項

Cisco Nexus 5000 シリーズ スイッチには、複数の 10 ギガビット イーサネット ポートの転送の決定およびバッファ リングの処理を担当する、ユニファイド ポート コントローラ（UPC）ASIC が組み込まれています。

- Cisco Nexus 5000 プラットフォーム スイッチ（Cisco Nexus 5010 スイッチおよび Cisco Nexus 5020 スイッチ）には、第 1 世代 UPC ASIC が組み込まれています。
- Cisco Nexus 5500 プラットフォーム スイッチ（Cisco Nexus 5548P スイッチ、Nexus 5548UP スイッチ、および Nexus 5596UP スイッチ）には、第 2 世代 UPC ASIC が組み込まれています。

ここでは、FCoE 設定およびサポートされるトポロジに関連する、第 1 世代と第 2 世代のアーキテクチャの違いについて説明します。

この項では、次のトピックについて取り上げます。

- 「VLAN の拡張性」（P.1-12）
- 「FCoE QoS 設定」（P.1-13）
- 「ユニファイド ポートのオプション」（P.1-13）

VLAN の拡張性

第 1 世代と第 2 世代の ASIC の違いの 1 つは、使用可能な VLAN リソースの数です。第 1 世代 ASIC では、最大 512 個の VLAN をサポートします（507 個がユーザ設定可能）。第 2 世代 ASIC では、使用可能な VLAN 数が 512 から 4096 に増えました。現在、両方の世代で、FCoE VLAN/VSAN のマッピングでは、31 個の VLAN と 31 個の VSAN がサポートされています。

（注）　FCoE VLAN/VSAN マッピングの VLAN および VSAN はハードウェア VLAN リソースを消費します。

FCoE QoS 設定

Nexus 5000 シリーズ スイッチは、FCoE トラフィック用にいくらかのバッファ スペースを常に予約します。Nexus 5000 シリーズ スイッチで FCoE 機能をイネーブルにすると、Nexus は予約済みバッファを使用して、必要な QoS ポリシーとバッファ割り当てを自動的に設定します。

Nexus 5500 シリーズ スイッチでは、トラフィック ニーズに基づいてすべての利用可能なポート バッファを設定できます。これにより、利用可能なすべてのバッファを使用できる、カスタム FCoE ポリシーを作成できます。

Nexus 5500 シリーズ スイッチで FCoE をイネーブルにすると、システムはカスタム QoS ポリシーを検索します。見つからない場合は、次に示すデフォルト QoS 設定が自動的に使用されます。

```
switch(config-sys-qos)# service-policy type qos input fcoe-default-in-policy
switch(config-sys-qos)# service-policy type queuing input fcoe-default-in-policy
switch(config-sys-qos)# service-policy type queuing output fcoe-default-out-policy
switch(config-sys-qos)# service-policy type network-qosfcoe-default-nq-policy
```

詳細については、次の URL にある『Cisco Nexus 5000 Series NX-OS Quality of Service Configuration Guide』を参照してください。

http://www.cisco.com/en/US/products/ps9670/products_installation_and_configuration_guides_list.html

ユニファイド ポートのオプション

ユニファイド ポートでは、1 および 10 ギガビット イーサネット ポート、1、2、および 4 ギガビットまたは 2、4、および 8 ギガビット FC（使用するトランシーバによる）を稼働できるため設定の柔軟性が増します。ユニファイド ポートにより、拡張モジュールを使用して一定数の FC ポートを購入する必要がなくなります。ユニファイド ポートは、Cisco Nexus 5548P スイッチと Nexus 5548UP プラットフォームの拡張モジュールおよび Cisco Nexus 5596UP スイッチのすべてのベース ポートで使用できます。ユニファイド ポートを使用する場合、慎重に従う必要のある設定要件があります。

イーサネットまたは FC という、同様なタイプのポートは、連続した順序で設定する必要があります。ポート タイプを変更すると、ユニファイド ポートの設定場所に応じて、スイッチまたは拡張モジュールのリブートが必要です。したがって、スイッチの初期設定時には慎重な計画が必要です。シスコでは、ベスト プラクティスとして、プラットフォームの一方の端からイーサネット ポートの設定を開始し（Eth1/1 からカウントアップ）、プラットフォームのもう一方の端から必要なファイバ チャネル ポートを設定する（Eth 1/48 からカウントダウン）ことをお勧めします。

ユニファイド ポートの設定の詳細については、『*Unified Port Configurations on Cisco Nexus 5500 Platform Switches*』マニュアルを参照してください。

プライオリティ フロー制御と Enhanced Transmission Selection に関する考慮事項

プライオリティ フロー制御（PFC）および Enhanced Transmission Selection（ETS）は、いずれも、標準化の最終段階にある IEEE 802.1Q Enhance Ethernet 標準の一部です。PFC および ETS の両方が、すべての Cisco Nexus 5000 シリーズ スイッチでサポートされています。PFC は、特定の CoS 値に割り当てられている FCoE トラフィックで、FC プロトコルに必要なロスレス品質を保持できるようにする、サービス クラス（CoS）ベースの PAUSE です。ETS は 10 ギガビット イーサネット リンクを CoS 値に基づいて複数のレーンに分割し、輻輳があるときに維持される必要な帯域幅要件を割り当てるためのメカニズムです。ETS は、デフォルト トラフィックが高優先順位のトラフィックと干渉することを防ぎます。

PFC および ETS は、現在の FCoE ネットワークで、FCoE トラフィックにロスレス トランスポートと専用帯域幅を提供するためによく使用されます。ただし、FCoE に固有のものではなく、特定のトラフィック クラスに特定のサービスのレベルを提供するために、FCoE 環境の外で多くの用途があります。

この項では、次のトピックについて取り上げます。

PFC および ETS のデフォルト設定

PFC と ETS の両方が、トラフィック タイプを分類するためにサービス クラス（CoS）ビットを使用します。イーサネット フレームの IEEE 802.1Q 標準トランキング ヘッダーには、8 個の CoS 値があります。Cisco Nexus 5000 シリーズ スイッチでは、6 個のクラスを手動で設定できます。6 個のユーザ設定可能なクラスの 4 個までは、no-drop サービス クラスとして指定できます。no-drop クラスに属するトラフィックは、ポートの輻輳時にパケットのドロップを避けるために一時停止されることを意味します。

デフォルトでは、Nexus 5000 プラットフォームおよび他のベンダーの FCoE 製品の FCoE トラフィック用 CoS 値は 3 に決定されています。FCoE が Cisco Nexus 5000 シリーズ スイッチでイネーブルの場合、COS 3 は no-drop サービス（PFC 設定）および輻輳時の帯域幅の 50 % 保証（ETS の設定）に自動的に設定されます。FCoE トラフィックは、「no-drop」クラスとしてサポートするというベンダー間の合意があるため、デフォルトの CoS 値 3 のままにすることがベスト プラクティスです。

CoS 値 3 を使用する他のトラフィックがネットワークにすでに存在するか、FCoE トラフィックを COS 3 から移動する別の理由がある場合は、Quality Of Service の設定を介して変更できます。

PFC および ETS の設定の変更

PFC および ETS の設定は、Nexus 5000 シリーズ スイッチ上の Quality of Service 設定で設定および変更します。次に、FCoE no-drop サービス クラスを COS 4 に変更しながら、FCoE 用に予約された帯域幅を 10 ギガビット イーサネット リンクの 20 % に変更する QoS 設定の例を示します。

ステップ 1　ポリシーマップ タイプ qos を定義および適用することにより、まず分類ルールを作成します。

```
N5k(config)# class-map type qos class-lossless
N5k(config-cmap-qos)# match cos 4
N5k(config-cmap-qos)# policy-map type qos policy-lossless
N5k(config-pmap-qos)# class type qos class-lossless
N5k(config-pmap-c-qos)# set qos-group 7
N5k(config-pmap-uf)# system qos
N5k(config-sys-qos)# service-policy type qos input policy-lossless
```

ステップ 2　ポリシーマップ タイプ network を定義して適用します。

```
N5k(config-pmap-qos)# class type network-qos policy-lossless
N5k(config-cmap-uf)# match qos-group 7
N5k(config-cmap-uf)# policy-map type network-qos policy-lossless
N5k(config-pmap-uf)# class type network-qos class-lossless
N5k(config-pmap-uf-c)# pause no-drop
N5k(config-pmap-uf)# system qos
N5k(config-sys-qos)# service-policy type network-qos policy-lossless
```

ステップ 3　ポリシーマップ タイプ qos を定義および適用することにより、まず分類ルールを作成します。

```
N5k(config)# class-map type queuing class-voice
N5k(config-cmap-que)# match qos-group 2
N5k(config-cmap-que)# class-map type queuing class-high
N5k(config-cmap-que)# match qos-group 3
N5k(config-cmap-que)# class-map type queuing class-low
N5k(config-cmap-que)# match qos-group 7
N5k(config-cmap-que)# exit
```

ステップ 4　各クラスの分類ルールを作成します。

```
N5k(config)# policy-map type queuing policy-BW
N5k(config-pmap-que)# class type queuing class-voice
N5k(config-pmap-c-que)# priority
N5k(config-pmap-c-que)# class type queuing class-voice
N5k(config-pmap-c-que)# bandwidth percent 20
N5k(config-pmap-c-que)# class type queuing class-high
N5k(config-pmap-c-que)# bandwidth percent 40
N5k(config-pmap-c-que)# class type queuing class-low
N5k(config-pmap-c-que)# bandwidth percent 10
N5k(config-pmap-c-que)# class type queuing class-fcoe
N5k(config-pmap-c-que)# bandwidth percent 30
N5k(config-pmap-c-que)# class type queuing class-default
N5k(config-pmap-c-que)# bandwidth percent 0
N5k(config-pmap-c-que)# system qos
N5k(config-sys-qos)# service-policy type queuing output policy-BW
```

PFC および ETS の設定を変更するときのホスト側の問題

Data Center Bridging Exchange（DCBX）プロトコルは、イーサネット標準化檀代によって現在検討中の IEEE 802.1Q Data Center Bridging（DCB）標準の別の部分です。DCBX は、PFC および ETS の設定を DCB ピア間で矛盾のないように構成するために DCB 対応デバイス間で実行されるプロトコルです。DCB は、中央のスイッチングの場所から DCB ピア デバイスを設定する方法としても使用できます。DCB *willing* をサポートする CNA は、アップストリーム DCB スイッチング デバイスの DCB 設定（PFC および ETS の設定を含む）を受信するように設定されます。これにより、DCB および FCoE デバイスの管理および設定が大幅に簡素化されます。

Cisco Nexus 5000 シリーズ スイッチで FCoE トラフィックのデフォルト設定を変更する場合、スイッチでは DCBX プロトコルを使用して、接続されているすべての CNA にこれらの設定変更をリレーできます。これを実施するには、CNA ベンダーおよびプラットフォームが *willing* モードの DCBX をサポートしている必要があります。ネットワーク デバイスの DCBX の設定の受け入れをサポートするかどうかは、個々の CNA ベンダーに確認してください。

CNA が DCB willing 方式をサポートしていない場合、デフォルトの PFC および ETS の設定から変更するためには、手動で Nexus 5000 シリーズおよびダウンストリーム CNA デバイスの設定を変更して一致させる必要があります。CNA によっては、これらの設定を変更するために、異なるツールやコマンドが使用されます。

（注）　DCBX ネゴシエーションがホストとスイッチまたはスイッチとスイッチの間で失敗した場合、PFC の設定は、Nexus 5000 シリーズ スイッチに設定されず、DCB の設定が一致するまで vFC インターフェイスは停止したままになります。

（注）　DCBX 標準には、可能な no-drop レーンは 8 個あると示されていますが、CNA ベンダーが FCoE および no-drop サービスに現在サポートしている CoS 値の数は異なっています。サポートされている FCoE および no-drop クラスの正しい数については、CNA ベンダーに問い合わせてください。

Cisco Nexus の相互運用性

相互運用性については、『*Cisco Data Center Interoperability Support Matrix*』を参照してください。

FCoE でサポートされるトポロジ

この項では、次のトピックについて取り上げます。

シングル ホップ FCoE 配置トポロジ

Cisco Nexus 5000 シリーズ スイッチと Cisco Nexus 2000 シリーズ ファブリック エクステンダを使用した FCoE を展開するときに可能なシングル ホップのソリューションは 2 通りあります。1 つ目のソリューションは、ファースト ホップ統合アクセス スイッチにホストを直接接続する「直接接続」です。2 つ目のシングル ホップ ソリューションでは、サーバとファースト ホップ スイッチの間に FEX を導入します。FEX は親スイッチへのリモート ラインカードとして機能し、ローカル スイッチング機能を持たないため、イーサネットまたはストレージのトポロジでは、ホップと見なされません。次に、スイッチおよび FEX を含む、現在サポートされている設定と現在のシングル ホップ導入オプションについて詳細に説明します。

この項では、次のトピックについて取り上げます。

スイッチ モードおよび NPV モード

Cisco Nexus 5000 シリーズ スイッチには、ストレージ トラフィックの転送に関して、スイッチ モードと N ポート バーチャライザ（NPV）モードの 2 つの動作モードがあります。これは、シスコ マルチプロトコル ディレクタ シリーズ（MDS）ファイバ チャネル スイッチで使用可能な動作モードと同じです。両方のプラットフォームのデフォルト モードは「スイッチ」モードです。以下のトポロジでは、Cisco Nexus 5000 シリーズ スイッチは、スイッチまたは NPV モードのいずれでもかまいません。NPV モードの Cisco Nexus 5000 シリーズ スイッチの唯一の要件は、アップストリーム デバイスが標準の N ポート ID バーチャライゼーション（NPIV）機能をサポートすることです。

Cisco Nexus 5000 シリーズ スイッチがスイッチ モードで動作しているときは、FSPF、ゾーン分割、DNS などのすべてのファブリック サービスは、アクセス デバイスでネイティブです。これは、すべての転送の決定が、スイッチ上で動作する FSPF によって実施されることを意味します。このモードは、スイッチがファイバ チャネル ファブリック内のドメイン ID を使用することも意味します。1 つのファブリック内でサポートされるドメイン ID の数に関連する制限があります。具体的なドメイン ID の制限は、ストレージ ベンダーおよび OSM パートナーによって定義されます。

NPV は、FLOGI および転送の決定の両方に対するプロキシとして動作するファイバ チャネル スイッチの機能を定義し、この動作をアップストリーム デバイスに渡します。このアップストリーム デバイスは、複数 FCID に単一の FC ポートを渡すことができる FC 標準である NPIV を実行できる必要があります。FC ネットワークの NPV デバイスの利点は、ドメイン ID が排除され、したがって、サポートされるドメイン ID 制限を超えないで、より多くの FC スイッチをファブリック追加できる点です。

Cisco Nexus 5000 シリーズ スイッチは、NPV モードでも動作できます。NPV がスイッチでイネーブルになっている場合、FC ファブリック サービスはプラットフォームでローカルに実行されません。転送サービスおよびゾーン分割サービスは、代わりに、アップストリーム NPIV デバイスで処理されます。Cisco SAN 以外のコア スイッチにスイッチを接続する場合の相互運用性の課題を回避するために、シスコでは、NPV モードでスイッチを設定することをお勧めします。

スイッチで NPV をイネーブルにする処理は中断を伴うため、ファブリックの中断を回避するために初期設定時に実施する必要があります。NPV をイネーブルにするにはスイッチのリブートが必要であり、現在の実行コンフィギュレーションが消去されるため、スイッチの初期設定後に NPV をイネーブルにする場合は、リブート後に再適用できるように、現在の実行コンフィギュレーションを外部のテキストファイルに保存してください。

スイッチ モードと NPV モードの間の切り替えは、次のコマンドを使用して実行できます。

NPV モードをイネーブルにするには、次のコマンドを使用します。

```
switch# feature npv
```

NPV モードを無効にするには、次のコマンドを使用します（スイッチ モードに戻ります）。

```
switch# no feature npv
```

（注）　スイッチで NPV を実行するには、アップストリームに接続されたデバイスで NPIV 機能がイネーブルである必要があります

（注）　NPV の同一スイッチに接続されている FC または FCoE ストレージ デバイスと通信する FC または FCoE ホストはサポートされません。

vPC およびアクティブ/スタンバイ

Nexus 5000 シリーズ スイッチのホスト側インターフェイスでは、単一の接続ホスト用の単一接続された NIC、デュアルホーム接続サーバ用のアクティブ スタンバイ NIC チーミング、デュアルホーム接続サーバ用の vPC という、さまざまな方法によるサーバへの接続を提供できます。FC では、ストレージへの独立した 2 個のパス、つまり、ファブリック A とファブリック B を必要とするため、このマニュアルではデュアルホーム接続サーバ オプションを重点的に扱います。

アクティブ/スタンバイ接続は、イーサネット LAN にデュアルホーム接続されている一方で、1 個のリンクのみをアクティブに転送するサーバを示します。2 個目のリンクは、障害が発生した場合のバックアップとして使用されますが、障害が発生しない限りアクティブにトラフィックを転送しません。vPC は、デュアルホーム接続されたサーバで両方のイーサネット リンクを同時にアクティブに転送で

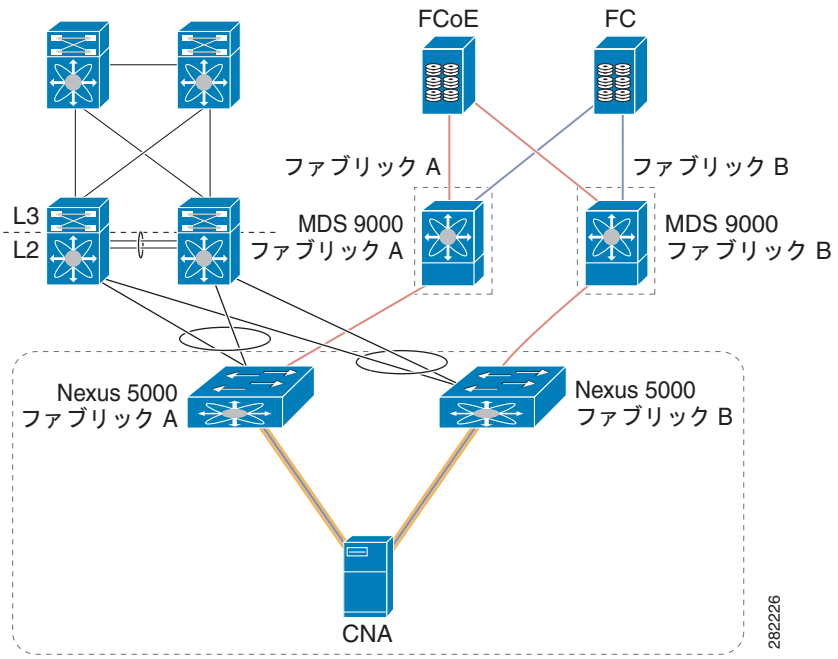
きる、Cisco Nexus 製品で導入されたテクノロジーです。vPC の利点は、アクティブ / スタンバイ設定の倍の帯域幅を持つアクセスをサーバに提供することおよび障害が発生した場合にスパニングツリーよりも高速なコンバージェンス能力もあることです。

LAN 管理者は、イーサネットのハイ アベイラビリティの要件に基づいて、アクティブ / スタンバイ接続または vPC 接続を使用したサーバの接続を選択できます。サーバをデュアルホーム接続するために使用する方式にかかわらず、FCoE は、この両方のトポロジと共存できます。

アクティブ/スタンバイ イーサネットのトポロジを使用した直接接続された CNA

図 1-5 に、アクティブ / スタンバイ設定で、デュアル ポートの CNA が 2 台のスイッチに接続するトポロジを示します。イーサネット トラフィックはこの設定の 1 個のリンクだけを通過しますが、FCoE トラフィックは両方のパスでファブリックに転送されます。これは、CNA では、イーサネットの NIC アダプタと FC/FCoE の FC アダプタを区別できるためです。CNA によるイーサネット NIC とストレージ HBA の見え方に関する詳細については、「CNA を介したイーサネット トラフィックおよび FC トラフィックの表示」（P.1-6）を参照してください。

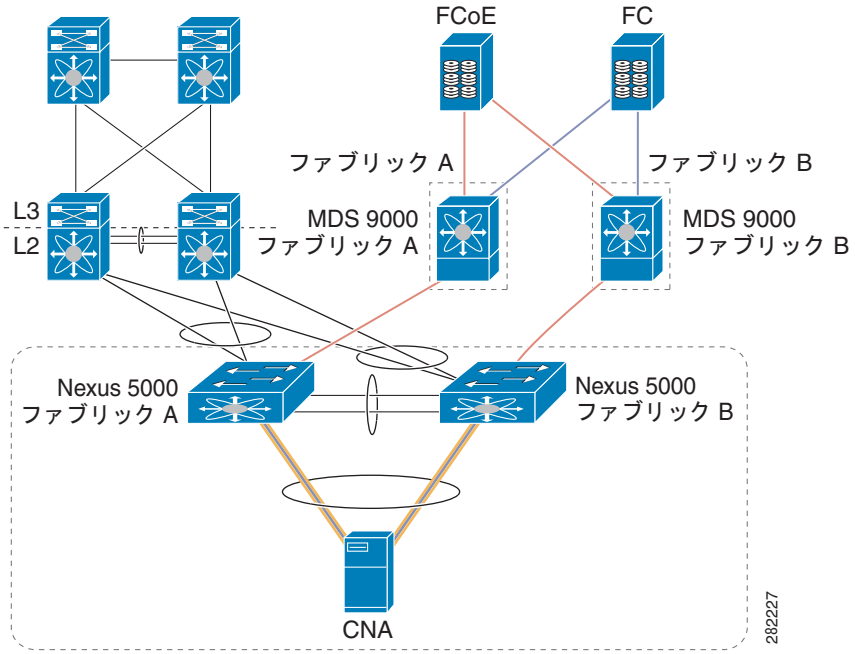
図 1-5　アクティブ/スタンバイ トポロジの 2 台の Cisco Nexus 5000 シリーズのスイッチに接続するデュアル ポート CNA



vPC イーサネットのトポロジを使用した直接接続された CNA

図 1-6 に、1 つのポートだけが CNA を各スイッチに接続する vPC 設定で、デュアル ポート CNA が 2 台のスイッチに接続するトポロジを示します。オペレーティング システムでは、イーサネット トラフィックがサーバから出る、これら 2 つの物理ポートおよびポート チャネルのイーサネットの側面を認識できます。FC トラフィックは、まだ各リンクに個別にマッピングされます。つまり、ファブリック A のトラフィックを転送する 1 個の 10 ギガビット リンクとファブリック B のトラフィックを転送するもう 1 つの 10 ギガビット リンクです。CNA によるイーサネット NIC とストレージ HBA の見え方に関する詳細については、「CNA を介したイーサネット トラフィックおよび FC トラフィックの表示」（P.1-6）を参照してください。

図 1-6　vPC トポロジの 2 台の Cisco Nexus 5000 シリーズにスイッチに接続するデュアル ポート CNA



（注）　直接接続 FCoE（Cisco Nexus 5000 シリーズ スイッチのスイッチポートに直接接続されている CNA）は、複数のメンバー ポートを持つように設定されたポート チャネル インターフェイスではサポートされません。直接接続 FCoE デバイスは、各 CNA ポート チャネルからの単一リンクが各アップストリーム スイッチまたはファブリック エクステンダに接続するときに通過する、仮想ポート チャネルを介してサポートされます。

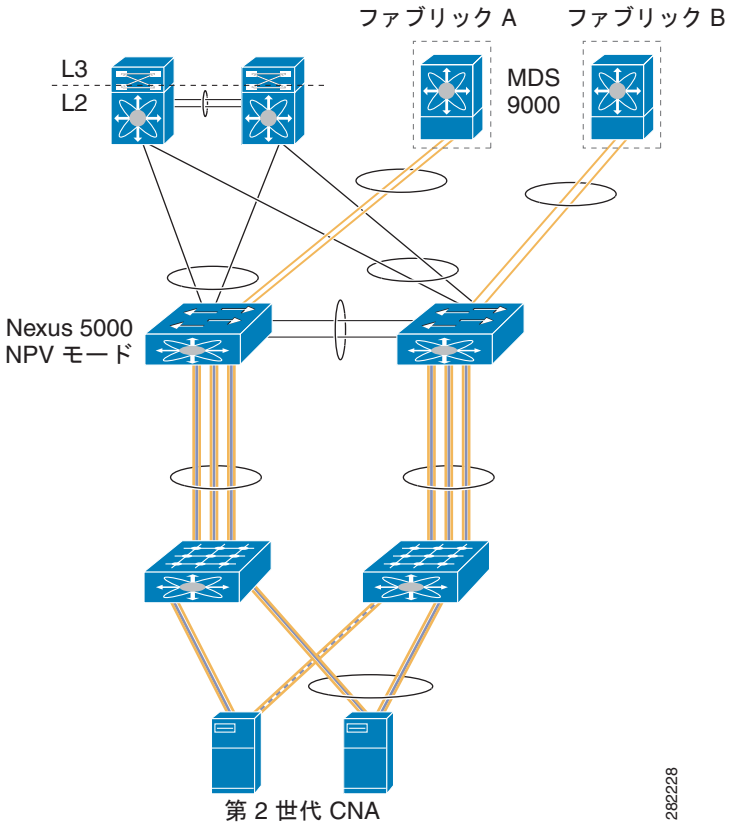
Cisco Nexus 5000 シリーズ スイッチと Cisco Nexus 2000 ファブリック エクステンダのトポロジ

Nexus 2232 ファブリック エクステンダは、親の Cisco Nexus 5000 シリーズ スイッチへのリモート ラインカードとして機能します。Nexus 2232 ファブリック エクステンダには、いずれもロスレス イーサネットおよび FCoE をサポートする、ホスト側の 32 個の 10 ギガビット イーサネット インターフェイスがあります。Cisco Nexus 5000 シリーズ スイッチおよび FEX トポロジを介した FCoE のサポートには、次の要件があります。

- FCoE を実行している Nexus 2232 ファブリック エクステンダは、各アップストリームの親スイッチにシングルホーム接続されている必要があります。
- Cisco Nexus 2232 ファブリック エクステンダ ホスト インターフェイスへのホスト接続には、第 2 世代（FIP 対応）CNA が必要です。

Cisco Nexus 2232 ファブリック エクステンダを FCoE トポロジに追加しても、サポートされる設定は変わりません。ホストは、アクティブ/スタンバイ イーサネット接続を使用するか、vPC 接続を介して Cisco Nexus 2232 ファブリック エクステンダに接続できます。図 1-7 にサポートされているトポロジを示します。

図 1-7　アクティブ/スタンバイ イーサネット接続を使用するか vPC 接続を介して Cisco Nexus 2232 ファブリック エクステンダ接続されたホスト



（注）　FEX アクティブ-アクティブ トポロジに属する 2 台のスイッチに FEX が接続されている場合、FEX インターフェイスおよびポート チャネル インターフェイス上では、FCoE はサポートされていません。

FIP スヌーピング ブリッジ

FIP スヌーピング ブリッジ（FSB）は、CNA と FCF の間の FIP 通信を監視できるロスレス イーサネット ブリッジです。FC/FCoE 転送ロジック機能はありませんが、代わりに FIP パケットを「スヌープ」し、CNA と FCF の間で行われる、FLOGI/LOGIN などの FIP 通信を監視します。特定の FCF を介した FC/FCoE ファブリックへの CNA ログインを検出した FIP スヌーピング ブリッジは、この CNA と FCF の間の通信がポイントツーポイントのままであることを保証するために、アクセス リストを動的に作成します。FIP スヌーピングは、不正なデバイスがデータセンターのネットワークに入り込んで、FCF を偽装できないようにするために、ロスレス イーサネット ブリッジを通過ときに使用するセキュリティ対策の 1 つです。

FSB は、ファブリック内で検出される FIP 通信に基づいて ACL を動的に作成するために拡張されたレイヤ 2 ロスレス イーサネット ブリッジであることに注意してください。FSB は FC/FCoE プロトコルおよびサービスを認識せず、FSPF に基づいて FCoE トラフィックを転送しません。代わりに、すべてのトラフィックはレイヤ 2 プロトコル（STP）によって伝送され、MAC アドレスに基づいてスイッチングされます。

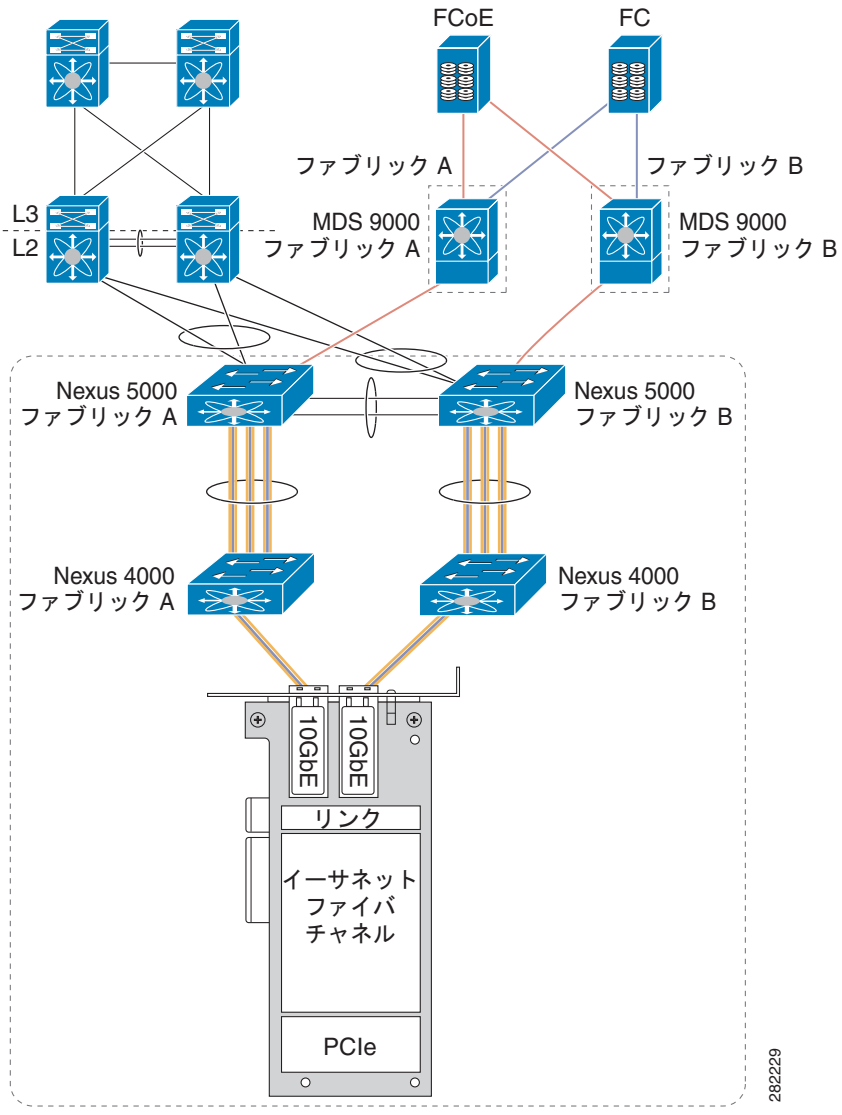
Cisco Nexus 4000 シリーズ スイッチは、IBM ブレード シャーシの FIP スヌーピング デバイスであり、通過する FCoE フレームをサポートするには、Cisco Nexus 5000 シリーズ FCF スイッチに接続する必要があります。Cisco Nexus 4000 シリーズ スイッチには、14 台のブレード サーバのそれぞれに接続さ

れる 14 個のダウン側 10 ギガビット ポートと Cisco Nexus 5000 シリーズ スイッチに接続するために使用される 6 個の 10 ギガビット イーサネット アップリンク ポートがあります。図 1-8 および図 1-9 に、Cisco Nexus 4000 シリーズ スイッチ FIP スヌーピング ブリッジを Cisco Nexus 5000 シリーズ FCF スイッチに接続するときにサポートされている 2 通りの設定を示します。

統合リンクを使用した Cisco Nexus 5000 シリーズ スイッチから Cisco Nexus 4000 シリーズ スイッチ FCoE への接続

図 1-8 に、FCoE およびイーサネット トラフィックの両方が同じリンクを同時に使用している統合リンクを使用して、Cisco Nexus 5000 シリーズ スイッチに接続された Cisco Nexus 4000 シリーズ スイッチを示します。FCoE ではファブリックの分離が必要なため、イーサネット トラフィックは 1 つのパスだけを通る必要があり、vPC などの他の Ethernet HA テクノロジーを利用できません。

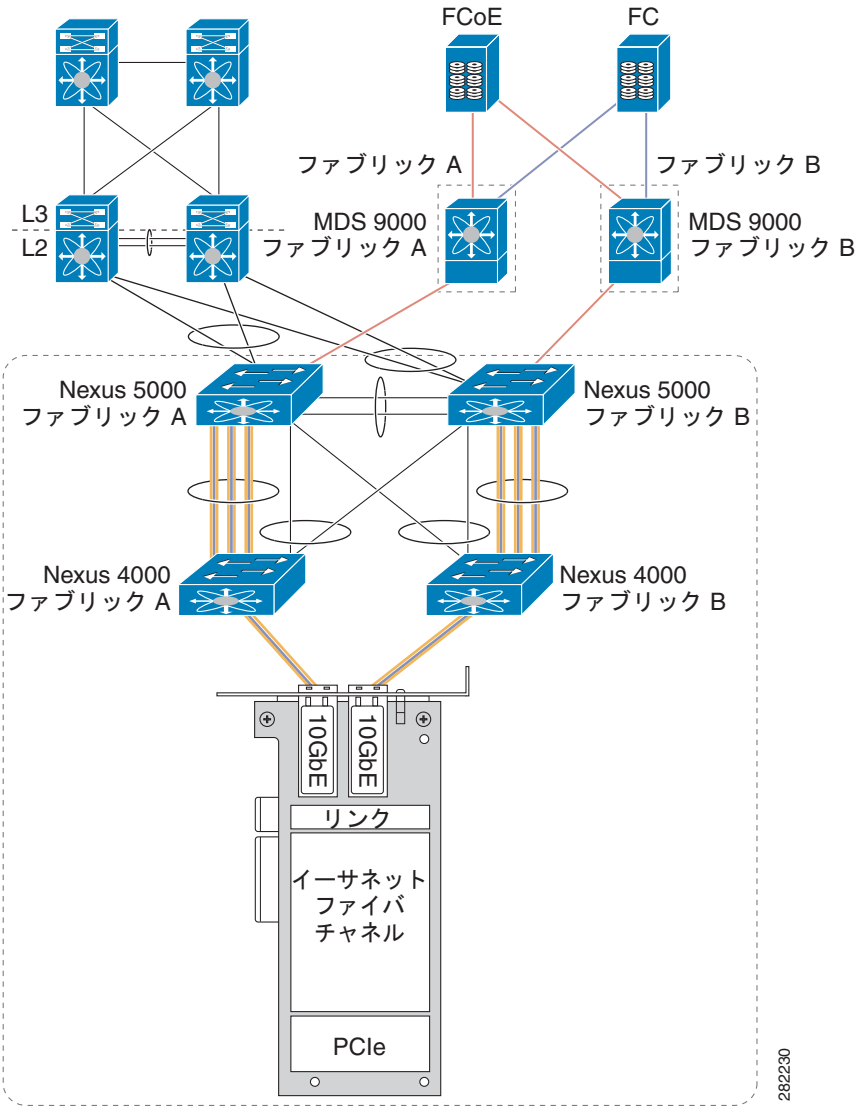
図 1-8　統合リンクを使用して Cisco Nexus 4000 シリーズ スイッチ FCoE に接続された Cisco Nexus 5000 シリーズ スイッチ



専用ネットワークを使用して Cisco Nexus 4000 シリーズ スイッチ FCoE に接続された Cisco Nexus 5000 シリーズ スイッチ

図 1-9 に、専用リンクを使用して Cisco Nexus 5000 シリーズ スイッチに接続する Cisco Nexus 4000 シリーズ スイッチを示します。青色のリンクはイーサネット専用リンクであり、ピンクと青のリンクは FCoE 専用リンクです。図 1-9 には、統合リンクは示されていません。このトポロジの Cisco Nexus 4000 シリーズ スイッチと Cisco Nexus 5000 シリーズ スイッチの間で専用リンクを実行する利点は、ストレージとイーサネット トラフィックの両方がそれぞれの HA モデルを活用できる点です。イーサネット トラフィックは、アップストリーム スイッチにマルチホーム接続されており、vPC を使用してすべての使用可能なパスを転送する一方で、FCoE はイーサネット ネットワークを介してファブリックの分離を維持します。

図 1-9　専用ネットワークを使用して Cisco Nexus 4000 シリーズ スイッチ FCoE に接続された Cisco Nexus 5000 シリーズ スイッチ

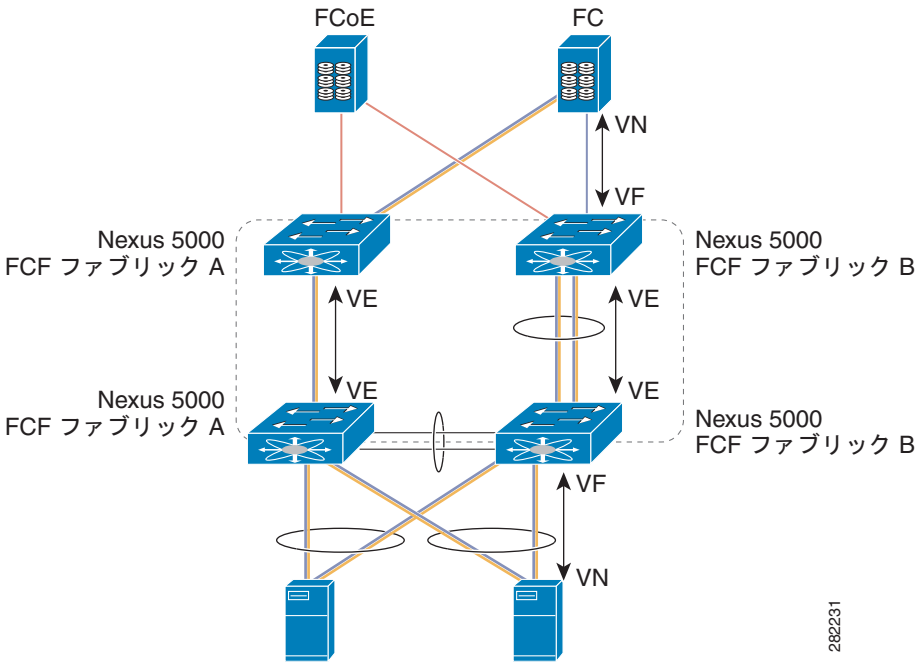


マルチ ホップ FCoE ソリューション

マルチ ホップ FCoE は、2 台の FCF を接続する仮想 E ポート（VE ポート）のサポートによって実現されます。ネイティブ FC での E_Ports と同様に、VE ポートは FCoE ファブリックを拡張するために使用されます。VE ポートは NXOS Release 5.0(1)N2(2) 以降の Nexus 5000 シリーズ スイッチでサポートされています。VE ポートを使用して Nexus 5000 シリーズ スイッチを接続する方法は、単一リンクの使用とポート チャネル経由の 2 通りあります。VE ポートの設定例は、第 3 章「FCoE ポートの設定例」を参照してください。

ファブリックの分離を維持するために、各ファブリックの Cisco Nexus 5000 FCF スイッチは、同じ FC-MAP 値を持つように設定する必要があります。FC-MAP 値は、ファブリック A とファブリック B の間で異なる必要があります。FC-MAP の設定の詳細については、第 3 章「FCoE ポートの設定例」を参照してください。異なる FC-MAP を持つ 2 台の Cisco Nexus 5000 シリーズ スイッチ間での VE ポートの動作はサポートされていません。これにより、ファブリック A の FCF をファブリック B の FCF に接続することによってファブリックがマージされないことが保証されます。図 1-10 に、VE ポートを使用した FCF 接続を示します。

図 1-10　VE ポートと FCF のマッピング



（注）　vPC を介する VE ポートはサポートされていません。

FCoE の動作

この項では、次のトピックについて取り上げます。

FCoE 統計情報のトラッキング

Cisco Nexus 5000 シリーズ スイッチのインターフェイスを通過する FCoE トラフィックの FCoE 統計情報は、物理イーサネット インターフェイスまたはポート チャネル インターフェイスにバインドされている vFC インターフェイスの統計情報をモニタリングすることによって表示できます。

この項では、次のトピックについて取り上げます。

- 「VE ポート統計情報のトラッキング」（P.1-24）
- 「VF ポート統計情報のトラッキング」（P.1-24）

VE ポート統計情報のトラッキング

次に、VE ポート統計情報をモニタする例を示します。

```
switch(config-if)# show inter vfc 300
vfc300 is trunking
    Bound interface is port-channel300
    Hardware is Virtual Fibre Channel
    Port WWN is 21:2b:00:05:9b:77:f5:7f
    Admin port mode is E, trunk mode is on
    snmp link state traps are enabled
    Port mode is TE
    Port vsan is 1
    Trunk vsans (admin allowed and active) (3,5)
    Trunk vsans (up) (3,5)
    Trunk vsans (isolated) ()
    Trunk vsans (initializing) ()
    1 minute input rate 15600 bits/sec, 1950 bytes/sec, 21 frames/sec
    1 minute output rate 43664 bits/sec, 5458 bytes/sec, 21 frames/sec
    51295547 frames input, 10484381916 bytes
    0 discards, 0 errors
    39089018 frames output, 10620127132 bytes
    0 discards, 0 errors
    last clearing of "show interface" counters never
    Interface last changed at Mon Jan 17 19:05:27 2011
```

VF ポート統計情報のトラッキング

次に、VF ポート統計情報をモニタする例を示します。

```
switch(config-if)# show inter vfc 31
vfc31 is trunking (Not all VSANs UP on the trunk)
    Bound interface is Ethernet1/1
    Hardware is Virtual Fibre Channel
    Port WWN is 20:1e:00:05:9b:77:f5:7f
    Admin port mode is F, trunk mode is on
    snmp link state traps are enabled
    Port mode is TF
    Port vsan is 3
    Trunk vsans (admin allowed and active) (3)
    Trunk vsans (up) (3)
    Trunk vsans (isolated) ()
    Trunk vsans (initializing) ()
    1 minute input rate 6912756368 bits/sec, 864094546 bytes/sec, 8640880 frames/sec
    1 minute output rate 6963590568 bits/sec, 870448821 bytes/sec, 396313 frames/sec
    789408333283 frames input, 78940833327276 bytes
    0 discards, 0 errors
    36207053863 frames output, 79510690165704 bytes
    0 discards, 0 errors
```

```
    last clearing of "show interface" counters never
    Interface last changed at Mon Jan 17 19:05:21 2011
```

FC および FCoE トラフィックの SPAN

この項では、次のトピックについて取り上げます。

- 「可能な SPAN 送信元」（P.1-25）
- 「可能な SPAN 宛先」（P.1-25）
- 「SPAN の設定例」（P.1-25）

可能な SPAN 送信元

次に、可能な SPAN 送信元を示します。

- FC インターフェイス（5500 プラットフォームの rx ソースのみ）
- VFC インターフェイス
- VSAN（5500 プラットフォームではサポートされません）
- VLAN
- イーサネット インターフェイス
- ポート チャネル インターフェイス
- SAN ポート チャネル インターフェイス

可能な SPAN 宛先

次に、可能な SPAN 宛先を示します。

- FC インターフェイス
- イーサネット インターフェイス

SPAN の設定例

次に、イーサネット 1/1 の設定情報を表示する例を示します。

```
switch(config)# show running-config interface eth 1/1
interface Ethernet1/1
    switchport monitor
```

次に、フェールオーバーのためにすべてのインターフェイスのヘルス モニタリングを表示する例を示します。

```
switch(config)# show running-config monitor all
monitor session 1 type local
    no description
    source interface vfc33 both
    destination interface Ethernet1/1
    no shut
```

次に、セッション 1 のヘルス モニタリングの例を示します。

```
switch(config)# show monitor session 1
    session 1
```

```
---------------
type : local
state : up
source intf :
    rx : vfc33
    tx : vfc33
    both : vfc33
source VLANs :
    rx :
source VSANs :
    rx :
destination ports : Eth1/1
Legend: f = forwarding enabled, l = learning enabled
```

次に、ヘルス モニタリング設定の例を示します。

```
switch(config)# show running-config monitor
monitor session 1
    source interface fc3/1 tx
    destination interface Ethernet1/1
    no shut
```

次に、すべてのセッションのヘルス モニタリングの例を示します。

```
switch(config)# show monitor session all
session 1
---------------
type : local
state : up
source intf :
    rx : fc3/1
    tx : fc3/1
    both : fc3/1
source VLANs :
    rx :
source VSANs :
    rx þ:
destination ports : Eth1/1
Legend: f = forwarding enabled, l = learning enabled
```

ロール ベース アクセス コントロール

統合 I/O 機能を展開する Cisco Nexus ファミリ スイッチをしている場合は、LAN および SAN 管理者のロールが統合されます。Cisco Nexus シリーズ ファミリ スイッチでこの 2 つの異なるロールを管理しやすくするために、Role Based Access Control（RBAC）機能がさまざまな管理操作を容易にします。

データセンター内に統合 I/O を展開する場合は、次の 3 種類のロールを定義することを推奨します。

- 統合管理者：このロールには、LAN および SAN の両方の動作に影響するすべてのアクションが含まれます。このロールは、グローバル管理者と呼ばれることがあります。
- LAN 管理者：このロールは、LAN の動作に影響する一連のアクションを含む一方で、SAN の動作に影響を与える可能性があるアクションは拒否します。
- SAN 管理者：このロールは、SAN の動作に影響する一連のアクションを含む一方で、LAN の動作に影響を与える可能性があるアクションは拒否します。

これらは、LAN および SAN の別々の管理チームが、干渉を受けずに目的のネットワークの管理制御を保持する運用モデルを適用するために使用する一般的なロールです。動作をより厳密に定義する必要がある場合は、より限定されたロールを追加できます。

この項では、次のトピックについて取り上げます。

統合管理者ロール

統合管理者ロールは、すべての操作を実行できます。また、統合管理者は統合ネットワークの初期設定で大きな役割を果たします。

統合ネットワーク設計を実装する前に、統合トラフィックに使用される物理インターフェイスと VLAN が識別および定義する必要があります。FCoE の標準実装には、物理イーサネット インターフェイスまたは MAC アドレスに、仮想ファイバ チャネル インターフェイス（vFC）をバインドする必要があります。 また、FC トラフィックを伝送するために使用する VSAN を、対応するイーサネット VLAN にマッピングする必要があります。イーサネット インターフェイスおよび VLAN は、通常は LAN 管理のスコープに入りますが、統合インターフェイスおよび FCoE VLAN は、LAN 管理ドメインから分離できるように識別する必要があります。

シスコでは、統合 I/O に使用するインターフェイスを特定することおよび実装が始まる前に、FCoE で使用する VLAN の範囲を指定することを推奨します。 統合管理者ロールは、これらの統合インターフェイスおよび FCoE VLAN を設定します。

LAN 管理者ロール

このロールには、LAN トラフィックに影響するすべての権限が割り当てられます。また、このロールは、SAN トラフィックに影響を与えるおそれのあるすべてのアクションを拒否します（FCoE および FC）。LAN 管理者ロールと、統合 I/O を使用しないレガシー データセンターの LAN 管理者の主要な相違点の 1 つは、FCoE トラフィックを伝達する物理イーサネット ポートをシャット ダウンできない点です。場合によっては、FC とイーサネット トラフィックの両方が同時にリンクを移動するため、ポートのシャットダウンは SAN の動作に影響を与えるおそれがあります。

SAN の動作に影響を与えることがあり、その結果、LAN 管理者のロールから制限する必要のあるコマンドのリストについては、第 2 章「FCoE および RBAC の設定」を参照してください。個々のネットワーク設計によって、コマンドの追加の制限が必要となる場合があります。

SAN 管理者ロール

このロールには、SAN トラフィックに影響するすべての権限が割り当てられます。また、このロールは、LAN トラフィックに影響を与えるおそれのあるアクションを拒否します。

統合環境の SAN 管理と、レガシー SAN 環境は、似ています。現在、統合 I/O はサーバとトップオブラック Cisco Nexus 5000 スイッチの間だけで動作します。ここで、FC リンクは、既存の SAN インフラストラクチャのコアに戻ります。Cisco Nexus 5000 スイッチ内の FC モジュールは、NPV またはスイッチ モードで動作できます。スイッチは、通常は NPV モードで動作し、管理の観点からすると、NPV モードで動作する FC ブレードまたはファブリック スイッチと同じです。

LAN の動作に影響を与えることがあり、その結果、SAN 管理者のロールから制限する必要のあるコマンドのリストについては、第 2 章「FCoE および RBAC の設定」を参照してください。個々のネットワーク設計によって、コマンドの追加の制限が必要となる場合があります。

FCoE の制限

この項では、次のトピックについて取り上げます。

第 1 世代および第 2 世代 CNA の制限

FCoE が Cisco Nexus 5000 シリーズ スイッチに導入された時期に、シスコでは、QLogic および Emulex と協力して第 1 世代の CNA アダプタを作成しました。これらの CNA では、CIN-DCBX と愛称が付けられた DCBX プロトコルの先行標準の実装を使用しました。これらのアダプタは、FCoE 標準で定義されている標準 FIP 実装（FC-BB-5）もサポートしておらず、通常、Pre-FIP アダプタと呼ばれます。

FCoE 規格が承認された 2009 年からは、標準 FIP および FCoE をサポートした第 2 世代 CNA が Emulex と QLogic によって製造されました。また、これらの CNA は IEEE DCBX が承認されるまで、複数のベンダーによって事実上の標準と取り決められた、CEE-DCBX と愛称が付けられた DCBX プロトコルの先行標準バージョンを採用しました。

第 2 世代 CNA を必要とするプラットフォームおよびトポロジ

Cisco Nexus 5010 スイッチおよび Nexus 5020 スイッチは、第 1 世代と第 2 世代の両方の CNA と後方互換性がありますが、Nexus 2000 ファブリック エクステンダおよび Nexus 5500 プラットフォームのスイッチは、第 2 世代 CNA 接続だけをサポートします。また、ホストが FCoE とネイティブ イーサネットだけのいずれを実行しているのかを問わず、vPC を使用するホストをファブリックに接続するときは、第 2 世代 CNA が必要です。

ホストへの LACP および FCoE

現在、ホスト側の vPC を介した FCoE を展開する場合、vFC インターフェイスは vPC に関連付けられたポート チャネル インターフェイスにバインドされます。したがって、FCoE トラフィックをスイッチングする前に、ポート チャネル インターフェイスがアップ状態で、転送を実施している必要があります。イーサネット環境で vPC を実行するときは、両側の設定が必ず一貫するように、ポート チャネルの両側でパラメータをネゴシエートするために LACP を使用することを推奨します。

ただし、ポート チャネル インターフェイスを起動するために LACP で使用するイーサネット設定パラメータに不整合がある場合、仮想ポート チャネルの両側は停止したままになります。これは、ホストからの FCoE トラフィックが、LAN/イーサネット側の正しい設定に現在依存することを意味します。この依存関係が発生する場合は、vPC および FCoE を同じホストに展開するときにスタティック ポート チャネルの設定（channel-group # mode on）を使用することを推奨します。

NPIV コアとしての Cisco Nexus 5000 シリーズ スイッチの導入

Nexus 5000 シリーズ スイッチは、NPV と NPIV 機能の両方をサポートしています。ダウンストリーム NPV スイッチが接続された NPIV コア スイッチとして機能している場合は、相互に通信しているホストおよびターゲットは、同じダウンストリーム NPV デバイスに接続できないことに注意してください。

Cisco Nexus 5010 スイッチまたは Cisco Nexus 5020 スイッチの VE ポート

Cisco Nexus 5000 シリーズおよび Cisco Nexus 5500 プラットフォーム スイッチは VE ポート接続をサポートしています。Cisco Nexus 5010 および Nexus 5020 スイッチでは、シングル ポート チャネルまたは複数の個別のリンクを使用して、2 台のスイッチ間に VE ポートを設定できます。複数のポート チャネルを使用して、2 台のスイッチ間で設定された VE ポートはサポートされません。これは、Cisco Nexus 5010 スイッチと Cisco Nexus 5020 スイッチの VE ポートで使用可能な MAC アドレスの数と関係があります。この制限は、Cisco Nexus 5500 プラットフォームには適用されません。

その他の情報

『*Cisco Nexus 5000 Series NX-OS SAN Switching Configuration Guide*』の「Configuring FCoE NPV」を参照してください。

http://www.cisco.com/en/US/products/ps9670/products_installation_and_configuration_guides_list.html

Cisco Nexus 5000 シリーズ スイッチの概要 : http://www.cisco.com/en/US/products/ps9670/index.html

Cisco Nexus 5000 シリーズ構成ガイド : http://www.cisco.com/en/US/products/ps9670/products_installation_and_configuration_guides_list.html

Fibre Channel over Ethernet の情報 : www.fcoe.com

CHAPTER 2

FCoE および RBAC の設定

この章では、FCoE 動作に関連する RBAC の設定について説明します。次の項で構成されています。

グローバル管理者のアクション

グローバル管理者ロールは制限されず、すべてのコマンドを使用できます。

LAN 管理者のアクション

この項では、LAN 管理者が実行できないコマンドを示します。リストされていないコマンドは、暗黙で許可されます。

グローバル レベルの拒否アクション

```
switch(config)# feature lacp
switch(config)# feature tacacs+
switch(config)# feature udld
switch(config)# feature fcoe
switch(config)# aaa *
switch(config)# boot *
switch(config)# cfs *
switch(config)# class-map *
switch(config)# device-alias *
switch(config)# diagnostic *
switch(config)# fex *
switch(config)# hw-module logging onboard *
switch(config)# license *
switch(config)# line *
switch(config)# lldp *
switch(config)# monitor session *
switch(config)# ntp *
switch(config)# policy-map *
switch(config)# privilege *
switch(config)# radius-server *
switch(config)# role *
switch(config)# snmp-server *
```

```
switch(config)# spanning-tree
    bridge assurance *
    loopguard *
    mode *
    mst *
    pathcost *
    port type *
    vlan <fcoe-vlan>
switch(config)# ssh *
switch(config)# system
    core *
    default switchport *
    jumbomtu *
    qos *
switch(config)# tacacs+ *
switch(config)# telnet server enable
switch(config)# trunk protocol enable
switch(config)# username *
switch(config)# vrf  *
switch(config)# xml server *
```

この項では、次のトピックについて取り上げます。

VLAN レベルの拒否アクション

すべての VLAN に対する拒否アクション

```
switch(config)# vlan vlan
switch(config-vlan)# fcoe
```

事前に決定された FCoE VLAN に対する拒否アクション

```
switch(config)# no vlan fcoe-vlan
switch(config)# vlan fcoe-vlan *
switch(config)# spanning-tree vlan fcoe-vlan *
switch(config-mst)# instance n vlan fcoe-vlan
switch(config)# mac-address-table aging-time t vlan fcoe-vlan
switch(config)# mac-address-table static aaaa.bbbb.cccc vlan fcoe-vlan
switch(config-monitor)# source vlan fcoe-vlan
switch(config)# vlan fcoe-vlan
switch(config-vlan)# ip igmp snooping *
```

インターフェイス レベルの拒否アクション

インターフェイス レベルの拒否アクション

（注）　管理インターフェイスへのアクセスは統合管理者だけに制限されます。

```
switch(config)# interface mgmt *
```

FCoE トラフィックの伝送用として指定されている事前に決定されたイーサネット インターフェイスに対する拒否アクション

```
switch(config-if)# bandwidth *
switch(config-if)# fcoe *
switch(config-if)# flowcontrol *
switch(config-if)# link debounce *
switch(config-if)# lldp *
switch(config-if)# priority-flow-control *
switch(config-if)# service-policy *
switch(config-if)# shutdown
switch(config-if)# shutdown force
switch(config-if)# spanning-tree bpdufilter
switch(config-if)# spanning-tree bpduguard
switch(config-if)# spanning-tree cost *
switch(config-if)# spanning-tree guard *
switch(config-if)# spanning-tree link-type *
switch(config-if)# spanning-tree mst *
switch(config-if)# spanning-tree port type *
switch(config-if)# spanning-tree port-priority *
switch(config-if)# speed *
switch(config-if)# switchport host
switch(config-if)# switchport mode *
switch(config-if)# switchport monitor
switch(config-if)# switchport trunk native vlan <fcoe-vlan>
switch(config-if)# switchport trunk allowed vlan <range>
switch(config-if)# switchport trunk allowed vlan add <fcoe-vlan>
switch(config-if)# switchport trunk allowed vlan all
switch(config-if)# switchport trunk allowed vlan except *
switch(config-if)# switchport trunk allowed vlan none
switch(config-if)# switchport trunk allowed vlan remove <fcoe-vlan>
```

FC 拒否アクション

FC 拒否アクション

（注）　LAN 管理者は SAN 関連のコマンドを実行できません。

```
switch(config)# fabric-binding *
switch(config)# fcalias *
switch(config)# fcdomain *
switch(config)# fcdroplatency *
switch(config)# fcflow *
switch(config)# fcid-allocation *
switch(config)# fcinterop *
switch(config)# fcns *
switch(config)# fcroute *
switch(config)# fcs *
switch(config)# fcsp *
switch(config)# fctimer *
switch(config)# fdmi *
switch(config)# fspf *
switch(config)# in-order-guarantee
switch(config)# interface fc *
switch(config)# interface san-port-channel *
switch(config)# interface vfc *
switch(config)# npiv *
switch(config)# npv *
switch(config)# port-security enable
switch(config)# port-track enable
```

```
switch(config)# rib *
switch(config)# rlir *
switch(config)# rscn *
switch(config)# scsi-target *
switch(config)# system default zone *
switch(config)# vsan database  *
switch(config)# wwn *
switch(config)# zone *
switch(config)# zoneset *
```

SAN 管理者のアクション

この項では、SAN 管理者が実行できないコマンドを示します。リストされていないコマンドは、暗黙で許可されます。

グローバル レベルの拒否アクション

```
switch(config)# feature * (except feature fcoe)
switch(config)# aaa *
switch(config)# boot *
switch(config)# cfs *
switch(config)# class-map *
switch(config)# device-alias *
switch(config)# diagnostic *
switch(config)# fex *
switch(config)# hw-module logging onboard *
switch(config)# ip *
switch(config)# ipv6 *
switch(config)# license *
switch(config)# line *
switch(config)# lldp *
switch(config)# mac-address-table *
switch(config)# monitor session *
switch(config)# ntp *
switch(config)# policy-map *
switch(config)# privilege *
switch(config)# radius-server *
switch(config)# role *
switch(config)# snmp-server *
switch(config)# spanning-tree
    bridge assurance *
    loopguard *
    mode *
    mst *
    pathcost *
    port type *
    vlan <non-fcoe-vlan>
switch(config)# ssh *
switch(config)# system
    core *
    default switchport *
    jumbomtu *
    qos *
switch(config)# tacacs+ *
switch(config)# telnet server enable
switch(config)# trunk protocol enable
switch(config)# username *
switch(config)# vrf  *
switch(config)# xml server *
```

この項では、次のトピックについて取り上げます。

VLAN レベルの拒否アクション

事前に決定された Non-FCoE VLAN に対する拒否アクション

```
switch(config)# no vlan <non-fcoe-vlan>
switch(config)# vlan <non-fcoe-vlan>*
switch(config)# spanning-tree vlan <non-fcoe-vlan>*
switch(config-mst)# instance n vlan <non-fcoe-vlan>
switch(config)# mac-address-table aging-time t vlan <non-fcoe-vlan>
switch(config)# mac-address-table static aaaa.bbbb.cccc vlan <non-fcoe-vlan>
switch(config-monitor)# source vlan <non-fcoe-vlan>
switch(config)# vlan <non-fcoe-vlan>
switch(config-vlan)# ip igmp snooping *
switch(config-if)# spanning-tree vlan <non-fcoe-vlan>
```

インターフェイス レベルの拒否アクション

インターフェイス レベルの拒否アクション

（注）　管理インターフェイスへのアクセスは統合管理者だけに制限されます。

```
switch (config)# interface mgmt *
```

FCoE トラフィックの伝送用でないとして指定されている事前に決定されたイーサネット インターフェイスに対する拒否アクション

SAN 管理者はこれらのインターフェイスの **no** コマンドを実行できます。

FCoE トラフィックの伝送用として指定されている事前に決定されたイーサネット インターフェイスに対する拒否アクション

この拒否リストはイーサネット、ポート チャネル、および FCoE トラフィックの伝送用として指定されている vEthernet インターフェイスに適用されます。

```
switch(config-if)# bandwidth *
switch(config-if)# fcoe *
switch(config-if)# flowcontrol *
switch(config-if)# link debounce *
switch(config-if)# lldp *
switch(config-if)# priority-flow-control *
switch(config-if)# service-policy *
switch(config-if)# shutdown
switch(config-if)# shutdown force
switch(config-if)# shutdown lan // TBD. This is a new command to shut stop LAN VLANs
switch(config-if)# spanning-tree bpdufilter
switch(config-if)# spanning-tree bpduguard
switch(config-if)# spanning-tree cost *
switch(config-if)# spanning-tree guard *
switch(config-if)# spanning-tree link-type *
switch(config-if)# spanning-tree mst *
switch(config-if)# spanning-tree port type *
switch(config-if)# spanning-tree port-priority *
```

```
switch(config-if)# speed *
switch(config-if)# switchport host
switch(config-if)# switchport mode *
switch(config-if)# switchport monitor
switch(config-if)# switchport trunk native *
switch(config-if)# switchport trunk allowed vlan <range>
switch(config-if)# switchport trunk allowed vlan add <non-fcoe-vlan>
switch(config-if)# switchport trunk allowed vlan all
switch(config-if)# switchport trunk allowed vlan except *
switch(config-if)# switchport trunk allowed vlan none
switch(config-if)# switchport trunk allowed vlan remove <non-fcoe-vlan>
```

LAN 拒否アクション

LAN 拒否アクション

SAN 管理者は LAN 関連のコマンドを実行できません。

```
switch(config)# cdp *
switch(config)# ip igmp snooping *
switch(config)# port-channel load-balance ethernet
switch(config)# rmon
switch(config)# track
```

設定例

次の設定は、LAN と SAN の両方の管理ロールを作成するために使用されます。これらの設定は、各ロールに割り当てるコマンドか、割り当てを控えるコマンドに関する、上記のアウトラインに従っています。すべてのコンフィギュレーション コマンドが自動で許可されるグローバル管理者には、設定は不要です。

（注） この設定は、vFC 1 がイーサネット 1/1 にマッピングされ、VLAN 100 が FCoE VLAN に指定されていると想定しています。この設定は、特定の環境および FCoE トラフィックの伝送用として事前に決定されているイーサネット ポートと VLAN に基づいています。

LAN-Admin 設定

role name LAN-admin

記述は vlan 100 で fcoe がイネーブルになっており、eth1/1 が vfc にバインドされた（fcoe）インターフェイスであることを前提としています

rule 97 deny command config t ; feature lacp

rule 96 deny command config t ; feature tacacs+

rule 95 deny command config t ; feature udld

rule 94 deny command config t ; feature fcoe

rule 93 deny command config t ; aaa *

rule 92 deny command config t ; boot *

rule 91 deny command config t ; cfs *

rule 90 deny command config t ; class-map *

rule 89 deny command config t ; device-alias *

rule 88 deny command config t ; diagnostic *
rule 87 deny command config t ; fex *
rule 86 deny command config t ; hw-module logging onboard *
rule 85 deny command config t ; license *
rule 84 deny command config t ; line *
rule 83 deny command config t ; lldp *
rule 82 deny command config t ; monitor session *
rule 81 deny command config t ; ntp *
rule 80 deny command config t ; policy-map *
rule 79 deny command config t ; privilege *
rule 78 deny command config t ; radius-server *
rule 77 deny command config t ; role *
rule 76 deny command config t ; snmp-server *
rule 75 deny command config t ; ssh *
rule 74 deny command config t ; system *
rule 73 deny command config t ; no system *
rule 72 deny command config t ; tacacs+ *
rule 71 deny command config t ; telnet server enable
rule 70 deny command config t ; trunk protocol enable
rule 69 deny command config t ; username *
rule 68 deny command config t ; vrf *
rule 67 deny command config t ; xml server *
rule 66 deny command config t ; fabric-binding *
rule 65 deny command config t ; fcalias *
rule 64 deny command config t ; fcdomain *
rule 63 deny command config t ; fcdroplatency *
rule 62 deny command config t ; fcflow *
rule 61 deny command config t ; fcid-allocation *
rule 60 deny command config t ; fcinterop *
rule 59 deny command config t ; fcns *
rule 58 deny command config t ; fcroute *
rule 57 deny command config t ; fcs *
rule 56 deny command config t ; fcsp *
rule 55 deny command config t ; fctimer *
rule 54 deny command config t ; fdmi *
rule 53 deny command config t ; fspf *
rule 52 deny command config t ; in-order-guarantee
rule 51 deny command config t ; npiv *

rule 50 deny command config t ; npv *
rule 49 deny command config t ; port-security enable
rule 48 deny command config t ; port-track enable
rule 47 deny command config t ; rib *
rule 46 deny command config t ; rlir *
rule 45 deny command config t ; rscn *
rule 44 deny command config t ; scsi-target *
rule 43 deny command config t ; vsan database *
rule 42 deny command config t ; wwn *
rule 41 deny command config t ; zone *
rule 40 deny command config t ; zoneset *
rule 39 deny command config t ; vlan * ; fcoe *
rule 38 deny command config t ; vlan * ; no fcoe *
rule 37 deny command config t ; spanning-tree vlan 100
rule 36 permit command config t ; spanning-tree vlan *
rule 35 deny command config t ; spanning-tree *
rule 34 deny command config t ; mac-address-table aging-time * vlan 100
rule 33 deny command config t ; mac-address-table static * vlan 100 *
rule 32 deny command config t ; monitor session * ; source vlan 100
rule 31 deny command config t ; vlan 100 *
rule 30 deny command config t ; no vlan 100 *
rule 29 deny command config t ; interface Ethernet1/1 ; bandwidth *
rule 28 deny command config t ; interface Ethernet1/1 ; fcoe *
rule 27 deny command config t ; interface Ethernet1/1 ; flowcontrol *
rule 26 deny command config t ; interface Ethernet1/1 ; link debounce *
rule 25 deny command config t ; interface Ethernet1/1 ; lldp *
rule 24 deny command config t ; interface Ethernet1/1 ; priority-flow-control *
rule 23 deny command config t ; interface Ethernet1/1 ; service-policy *
rule 22 deny command config t ; interface Ethernet1/1 ; shutdown
rule 21 deny command config t ; interface Ethernet1/1 ; shutdown force
rule 20 deny command config t ; interface Ethernet1/1 ; spanning-tree bpdufilter *
rule 19 deny command config t ; interface Ethernet1/1 ; spanning-tree bpduguard *
rule 18 deny command config t ; interface Ethernet1/1 ; spanning-tree cost *
rule 17 deny command config t ; interface Ethernet1/1 ; spanning-tree guard *
rule 16 deny command config t ; interface Ethernet1/1 ; spanning-tree link-type *
rule 15 deny command config t ; interface Ethernet1/1 ; spanning-tree mst *
rule 14 deny command config t ; interface Ethernet1/1 ; spanning-tree port type *
rule 13 deny command config t ; interface Ethernet1/1 ; spanning-tree port-priority *

rule 12 deny command config t ; interface Ethernet1/1 ; speed *
rule 11 deny command config t ; interface Ethernet1/1 ; switchport host
rule 10 deny command config t ; interface Ethernet1/1 ; switchport mode *
rule 9 deny command config t ; interface Ethernet1/1 ; switchport monitor
rule 8 deny command config t ; interface Ethernet1/1 ; switchport trunk native vlan 100
rule 7 deny command config t ; interface Ethernet1/1 ; switchport trunk allowed vlan *
rule 6 deny command config t ; interface Ethernet1/1 ; switchport trunk allowed vlan add 100
rule 5 deny command config t ; interface Ethernet1/1 ; switchport trunk allowed vlan all
rule 4 deny command config t ; interface Ethernet1/1 ; switchport trunk allowed vlan except *
rule 3 deny command config t ; interface Ethernet1/1 ; switchport trunk allowed vlan none
rule 2 deny command config t ; interface Ethernet1/1 ; switchport trunk allowed vlan remove 100
rule 1 permit read-write
interface policy deny
  permit interface eth1/1-40
vlan policy deny
  permit vlan 100-200
vsan policy deny

SAN-Admin 設定

role name SAN-admin

記述は vlan 100 で fcoe がイネーブルであり、vfc1 が eth1/1 にバインドされていると想定しています
rule 83 permit command config t ; vlan * ; fcoe *
rule 82 deny command config t ; vlan * ; *
rule 81 deny command config t ; ip igmp snooping *
rule 80 deny command config t ; cdp *
rule 79 deny command config t ; port-channel load-balance ethernet *
rule 78 deny command config t ; rmon *
rule 77 deny command config t ; track *
rule 76 deny command config t ; no ip igmp *
rule 75 deny command config t ; no cdp *
rule 74 deny command config t ; no port-channel load-balance *
rule 73 deny command config t ; no rmon *
rule 72 deny command config t ; no track *
rule 71 deny command config t ; interface * ; switchport trunk native *
rule 70 deny command config t ; interface * ; switchport trunk allowed vlan *
rule 69 deny command config t ; interface * ; switchport trunk allowed vlan add 100
rule 68 deny command config t ; interface * ; switchport trunk allowed vlan all
rule 67 deny command config t ; interface * ; switchport trunk allowed vlan except *

rule 66 deny command config t ; interface * ; switchport trunk allowed vlan none
rule 65 deny command config t ; interface * ; switchport trunk allowed vlan remove 100
rule 64 deny command config t ; interface * ; bandwidth *
rule 63 deny command config t ; interface * ; fcoe *
rule 62 deny command config t ; interface * ; flowcontrol *
rule 61 deny command config t ; interface * ; link debounce *
rule 60 deny command config t ; interface * ; lldp *
rule 59 deny command config t ; interface * ; priority-flow-control *
rule 58 deny command config t ; interface * ; service-policy *
rule 57 deny command config t ; interface * ; shutdown
rule 56 deny command config t ; interface * ; shutdown force
rule 55 deny command config t ; interface * ; shutdown lan
rule 54 deny command config t ; interface * ; spanning-tree bpdufilter
rule 53 deny command config t ; interface * ; spanning-tree bpduguard
rule 52 deny command config t ; interface * ; spanning-tree cost *
rule 51 deny command config t ; interface * ; spanning-tree guard *
rule 50 deny command config t ; interface * ; spanning-tree link-type *
rule 49 deny command config t ; interface * ; spanning-tree mst *
rule 48 deny command config t ; interface * ; spanning-tree port type *
rule 47 deny command config t ; interface * ; spanning-tree port-priority *
rule 46 deny command config t ; interface * ; speed *
rule 45 deny command config t ; interface * ; switchport host
rule 44 deny command config t ; interface * ; switchport mode *
rule 43 deny command config t ; interface * ; switchport monitor
rule 42 deny command config t ; no vlan 100 *
rule 41 permit command config t ; feature fcoe
rule 40 deny command config t ; feature *
rule 39 deny command config t ; aaa *
rule 38 deny command config t ; boot *
rule 37 deny command config t ; cfs *
rule 36 deny command config t ; class-map *
rule 35 deny command config t ; device-alias *
rule 34 deny command config t ; diagnostic *
rule 33 deny command config t ; fex *
rule 32 deny command config t ; hw-module logging onboard *
rule 31 deny command config t ; ip *
rule 30 deny command config t ; ipv6 *
rule 29 deny command config t ; license *

```
rule 28 deny command config t ; line *
rule 27 deny command config t ; lldp *
rule 26 deny command config t ; mac-address-table *
rule 25 deny command config t ; monitor session *
rule 24 deny command config t ; ntp *
rule 23 deny command config t ; policy-map *
rule 22 deny command config t ; privilege *
rule 21 deny command config t ; radius-server *
rule 20 deny command config t ; role *
rule 19 deny command config t ; snmp-server *
rule 18 deny command config t ; spanning-tree bridge assurance *
rule 17 deny command config t ; spanning-tree loopguard *
rule 16 deny command config t ; spanning-tree mode *
rule 15 deny command config t ; spanning-tree mst *
rule 14 deny command config t ; spanning-tree pathcost *
rule 13 deny command config t ; spanning-tree port type *
rule 12 deny command config t ; ssh *
rule 11 deny command config t ; system core *
rule 10 deny command config t ; system default switchport *
rule 9 deny command config t ; system jumbomtu *
rule 8 deny command config t ; system qos *
rule 7 deny command config t ; tacacs+ *
rule 6 deny command config t ; telnet server enable
rule 5 deny command config t ; trunk protocol enable
rule 4 deny command config t ; username *
rule 3 deny command config t ; vrf *
rule 2 deny command config t ; xml server *
rule 1 permit read-write
vlan policy deny
  permit vlan 100-100
interface policy deny
  permit interface fc3/1-4
  permit interface Ethernet1/1
  permit interface vfc1
```

CHAPTER 3

FCoE ポートの設定例

この付録では、FCoE トポロジに関するポートの設定例について説明します。内容は次のとおりです。

VE ポートの設定例

ここでは、Cisco Nexus 5000 シリーズ スイッチの FCoE VE ポート実装の設定例を示します。この設定は、スイッチ モードのスイッチを対象としています。FCoE の発信側はこのラボで使用されます。Nexus 5000 シリーズ スイッチの FC GEM に FC F ポート ストレージを直接接続することまたは FCoE ターゲットを使用することのいずれかが可能です。

（注） この例は、両方のファブリックで 2 台の Cisco Nexus 5000 シリーズ スイッチ間の VE ポートの設定に使用できます。サーバ設定は含まれません。

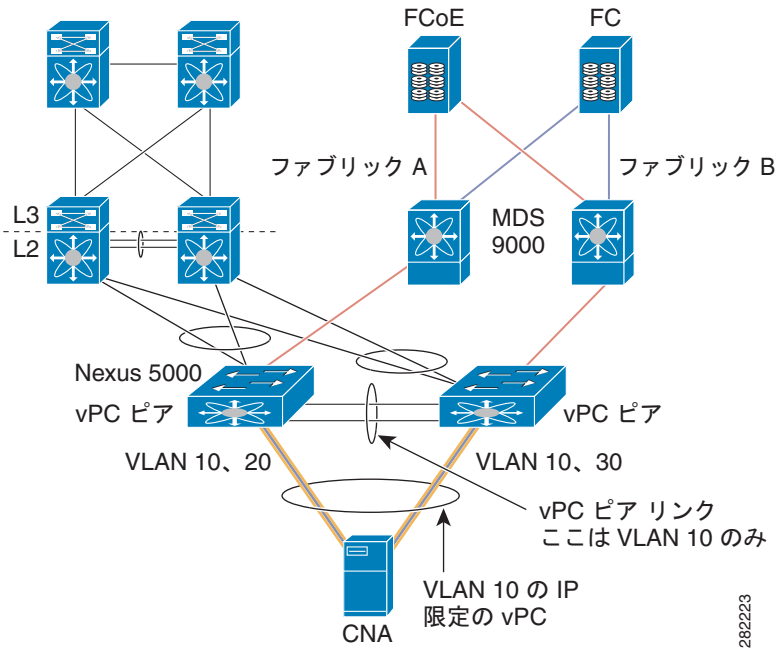
FCoE VE ポート トポロジの例

図 3-1 に、設定例に使用するトポロジを示します。このトポロジでは、次の設定パラメータを使用しています。

- ファブリック A の FCoE VLAN：10
- ファブリック A の FCoE VSAN：10
- ファブリック B の FCoE VLAN：20
- ファブリック B の FCoE VSAN：20
- 両方のファブリックをまたがるイーサネット専用 VLAN：200

設定時にこれらの値を選択する必要があります。

図 3-1　FCoE VE ポート トポロジ



（注）　FCoE VLAN/VSAN の番号がファブリック内で同一である必要はありません。ベスト プラクティスとして、混乱を避けるために、2 台のファブリック間の別の FCoE VLAN 番号および VSAN 番号を使用します。1 台のファブリックに ODD VLAN/VSAN、別のファブリックに EVEN VLAN/VSAN を割り当てる設定が一般的です。これは 2 台のファブリック間で番号を分離するための一例にすぎません。

FCoE のイネーブル化および QoS 設定の検証

ステップ 1　FCoE をイネーブルにします。

```
switch# configure terminal
switch(config)# feature fcoe
FC license checked out successfully
fc_plugin extracted successfully
FC plugin loaded successfully
FCoE manager enabled successfully
FC enabled on all modules successfully
```

ステップ 2　（任意）デフォルトの Quality of Service（QoS）設定を使用しない場合は、独自のポリシーを指定します。

（注）　注：カスタム ポリシーを使用するときは、QoS ポリシーに **class-fcoe** を含める必要があります。

```
switch(config) system qos
switch(config-sys-qos)# service-policy type qos input fcoe-customized-in-policy-name
switch(config-sys-qos)# service-policy type queuing input
fcoe-customized-in-policy-name
switch(config-sys-qos)# service-policy type queuing output
fcoe-customized-out-policy-name
```

```
switch(config-sys-qos)# service-policy type network-qos fcoe-customized-nq-policy-name
```

ステップ 3　FCoE のポリシーマップが実行コンフィギュレーションに含まれることを確認します。

（注）　注：ステップ 2 で、カスタマイズされた QoS ポリシーマップ名を指定した場合は、カスタマイズされたマップ名でデフォルト マップ名を必ず置き換えてください。

```
switch(config-sys-qos)# show policy-map system

  Type network-qos policy-maps
  ============================

  policy-map type network-qos system
    class type network-qos class-fcoe
      match qos-group 1

      pause no-drop
      mtu 2158
    class type network-qos class-default
      match qos-group 0

      mtu 1500

  Service-policy (qos) input:   system
    policy statistics status:   disabled

    Class-map (qos):   class-fcoe (match-any)
      Match: cos 3
      set qos-group 1

    Class-map (qos):   class-default (match-any)
      Match: any
      set qos-group 0

  Service-policy (queuing) input:   default-in-policy
    policy statistics status:   disabled

    Class-map (queuing):   class-fcoe (match-any)
      Match: qos-group 1
      bandwidth percent 50

    Class-map (queuing):   class-default (match-any)
      Match: qos-group 0
      bandwidth percent 50

  Service-policy (queuing) output:   default-out-policy
    policy statistics status:   disabled

    Class-map (queuing):   class-fcoe (match-any)
      Match: qos-group 1
      bandwidth percent 50

    Class-map (queuing):   class-default (match-any)
      Match: qos-group 0
      bandwidth percent 50
```

Nexus 5000 シリーズの Quality of Service の設定は次の 3 種類の主要要素で構成されています。

- クラス マップおよびポリシーマップ タイプ qos：分類用
- クラス マップおよびポリシーマップ タイプ network：drop、no drop、キュー サイズなどのネットワーク プロパティ用

- クラス マップおよびポリシーマップ タイプ queueing：帯域割り当て用

この演習は、FCoE の帯域割り当てと、COS の設定の変更で構成されています。

QoS に class-fcoe の正しい設定がないと、次の問題が発生する可能性があります。

- vFC インターフェイスが起動しない（CNA では FCoE のために DCB パラメータのアドバタイズメントが必要）
- I/O のドロップの検出

（注）　QoS には、次のガイドラインがあります。

- 分類ポリシーマップは入力だけで適用されます
- ネットワーク ポリシーマップはグローバル（システム）に適用されます
- キューイング ポリシーマップは通常は出力で意味を持ちますが、この演習では CNA から Cisco Nexus 5000 シリーズ スイッチへの帯域割り当ての制御に使用するため、この場合は入力に適用します

Cisco NX-OS Release 5.0(2)N1(1) からは、no-drop クラスのバッファ割り当てを変更できます。

```
switch(config-pmap-nq)# policy-map type network-qos nqos_policy
switch(config-pmap-nq)# class type network-qos nqos_class
switch(config-pmap-nq-c)# pause no-drop buffer-size <size> pause-threshold <threshold>
resume-threshold <threshold>
```

ステップ 4　FCoE システム クラスがアクティブであることを確認します。

```
switch(config-sys-qos)# show queuing interface ethernet 1/1
Ethernet1/1 queuing information:
TX Queuing
        qos-group sched-type oper-bandwidth
        0 WRR 50
        1 WRR 50
RX Queuing
        qos-group 0
        q-size: 370240, HW MTU: 1500 (1500 configured)
        drop-type: drop, xon: 0, xoff: 2314
        Statistics:
        Pkts received over the port : 0
        Ucastpkts sent to the cross-bar : 0
        Mcastpkts sent to the cross-bar : 0
        Ucastpkts received from the cross-bar : 0
        Pkts sent to the port : 0
        Pkts discarded on ingress : 0
        Per-priority-pause status : Rx (Inactive), Tx (Inactive)
        qos-group 1
        q-size: 79360, HW MTU: 2158 (2158 configured)
        drop-type: no-drop, xon: 128, xoff: 252
        Statistics:
        Pkts received over the port : 0
        Ucastpkts sent to the cross-bar : 0
        Mcastpkts sent to the cross-bar : 0
        Ucastpkts received from the cross-bar : 0
        Pkts sent to the port : 0
        Pkts discarded on ingress : 0
        Per-priority-pause status : Rx (Inactive), Tx (Inactive)
Total Multicast crossbar statistics:
        Mcastpkts received from the cross-bar : 0
```

ステップ 5　両方のアップストリーム Cisco Nexus 5000 シリーズ スイッチ（この例では、CORE_N5k-1 および CORE_N5k-2）で、ステップ 1 およびステップ 4 を繰り返します。

VE ポートの設定

この例の FCoE VLAN および VSAN の番号は次のとおりです。

- ファブリック A は FCoE VLAN 10 および VSAN 10 を使用します
- ファブリック B は FCoE VLAN 20 および VSAN 20 を使用します

（注）　ファブリック A に 2 台のスイッチとファブリック B に 2 台のスイッチがあります。同じファブリックのスイッチ間で VE ポートを起動するには、スイッチ間で FCoE VLAN/VSAN が一致する必要があります。

ステップ 1　ファブリック A の Nexus 5000 シリーズ スイッチで VSAN を設定します。

```
switch(config)#
switch(config)# vsan database
switch(config-vsan-db)# vsan 10
```

ステップ 2　ファブリック A のために FCoE VLAN から VSAN へのマッピングを設定し、起動していて、動作していることを確認します。

```
switch(config)# vlan 10
switch(config-vlan)# fcoe vsan 10
switch(config-vlan)#
switch(config-vlan)# show vlan fcoe
Original VLAN ID        Translated VSAN ID      Association State
----------------      ------------------      -----------------
10                        10 Operational
switch(config-vlan)#
```

ステップ 3　ファブリック A のアップストリーム Nexus 5000 シリーズ スイッチで、ステップ 1 およびステップ 2 を繰り返します。

ステップ 4　ファブリック B の Nexus 5000 で VSAN を設定します。

```
switch(config)#
switch(config)# vsan database
switch(config-vsan-db)# vsan 20
```

ステップ 5　ファブリック B のために FCoE VLAN から VSAN へのマッピングを設定し、起動していて、動作していることを確認します

```
switch(config)# vlan 20
switch(config-vlan)# fcoe vsan 20
switch(config-vlan)#
switch(config-vlan)# show vlan fcoe
Original VLAN ID        Translated VSAN ID      Association State
----------------      ------------------ -----------------
20                        20 Operational
switch(config-vlan)#
```

ステップ 6　ファブリック B のアップストリーム Nexus 5000 シリーズ スイッチで、ステップ 1 およびステップ 2 を繰り返します。

ステップ 7　vFC インターフェイスをバインドする基礎となる 10 ギガビット イーサネット ポートを設定します。VE ポートは、2 台のスイッチ間の FCoE トラフィックを物理的に転送するために、このインターフェイスを使用します。このインターフェイスは、適切な FCoE VLAN およびイーサネット VLAN をトランキングするように設定する必要があります（この例では、イーサネット トラフィックを伝送するために VLAN 200 を使用しています）。

このラボで、スイッチを接続する 10 ギガビット イーサネット インターフェイスを上記のトポロジに示します。

- ファブリック A は FCoE VLAN 10 および VSAN 10 を使用します
- ファブリック B は FCoE VLAN 20 および VSAN 20 を使用します
- PODX-N5K-1（ファブリック A）はイーサネット 1/15 を使用して CORE N5K1 に接続します
- PODX-N5K-2（ファブリック B）はイーサネット 1/16 を使用して CORE N5K2 に接続します

ファブリック A における両方のスイッチの設定：

```
switch(config)# vlan 200
switch(config)# interface ethernet 1/15
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 10, 200
switch(config-if)#
```

ファブリック B における両方のスイッチの設定：

```
switch(config)# vlan 200
switch(config)# interface ethernet 1/16
switch(config-if)# switchport mode trunk
switch(config-if)# switchport trunk allowed vlan 20, 200
switch(config-if)#
```

ステップ 8　VE ポートにバインドされるスイッチ上の vFC インターフェイスを設定し、VSAN データベースの VSAN 44 にこの vFC インターフェイスを追加します。

VE ポートの vFC 番号を次に示します。

- ファブリック A は FCoE VLAN 10 および VSAN 10 を使用します
- ファブリック B は FCoE VLAN 20 および VSAN 20 を使用します
- POD1-N5K-1（ファブリック A）はイーサネット 1/15 を使用して CORE N5K1 に接続します
- POD1-N5K-2（ファブリック B）はイーサネット 1/16 を使用して CORE N5K2 に接続します
- POD1-N5K-1（ファブリック A）は vfc 15 を使用し、これをイーサネット 1/15 にバインドします
- POD1-N5K-2（ファブリック B）は vfc 16 を使用し、これをイーサネット 1/16 にバインドします

ファブリック A における両方のスイッチの設定：

```
switch(config)# int vfc 15
switch(config-if)# switchport mode e
switch(config-if)# switchport trunk allowed vsan 10
switch(config-if)# bind interface eth 1/15
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# vsan database
switch(config-vsan-db)# vsan 10 interface vfc 15
switch(config-vsan-db)# show vsan membership
vsan 1 interfaces:
fc2/1             fc2/2             fc2/3             fc2/4
fc2/5             fc2/6             fc2/7             fc2/8
vsan 10 interfaces:
vfc15
vsan 4079(evfp_isolated_vsan) interfaces:
vsan 4094(isolated_vsan) interfaces:
```

```
switch(config-vsan-db)# exit
```

ファブリック B における両方のスイッチの設定：

```
switch(config)# int vfc 16
switch(config-if)# switchport mode e
switch(config-if)# switchport trunk allowed vsan 20
switch(config-if)# bind interface eth 1/16
switch(config-if)# no shutdown
switch(config-if)# exit
switch(config)# vsan database
switch(config-vsan-db)# vsan 20 interface vfc 16
switch(config-vsan-db)# show vsan membership
vsan 1 interfaces:
fc2/1             fc2/2             fc2/3             fc2/4
fc2/5             fc2/6             fc2/7             fc2/8
vsan 20 interfaces:
vfc16
vsan 4079(evfp_isolated_vsan) interfaces:
vsan 4094(isolated_vsan) interfaces:
switch(config-vsan-db)# exit
```

（注） これらのインターフェイス設定は、同じファブリックで 2 台のスイッチを接続する ISL の両側に設定する必要があることに注意してください。

ステップ 9 vFC が起動し、動作していることを確認します。デフォルトでは、vFC はトランキングとして示されます。適切な物理インターフェイスにバインドされていることおよび VSAN 44 が使用可能で、vFC インターフェイスで起動されていることを確認します。

ファブリック A の両方のスイッチを確認します。

```
switch(config)# show int vfc 15
        vfc15 is trunking
        Bound interface is Ethernet1/15
            Hardware is Virtual Fibre Channel
            Port WWN is 20:0e:00:0d:ec:b4:43:7f
            Peer port WWN is 00:00:00:00:00:00:00:00
            Admin port mode is E, trunk mode is on
        snmp link state traps are enabled
            Port mode is TE
            Port vsan is 10
        Trunk vsans (admin allowed and active) (10)
            Trunk vsans (up)                        (10)
            Trunk vsans (isolated)                  ()
            Trunk vsans (initializing)              ()
            1 minute input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
            1 minute output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
              13 frames input, 1028 bytes
                0 discards, 0 errors
              13 frames output, 1180 bytes
                0 discards, 0 errors
        last clearing of "show interface" counters never
            Interface last changed at Sat Nov  6 17:58:39 2010
```

ファブリック B の両方のスイッチを確認します。

```
switch(config)# show int vfc 16
        vfc16 is trunking
        Bound interface is Ethernet1/16
            Hardware is Virtual Fibre Channel
            Port WWN is 20:0e:00:0d:ec:b4:43:7d
            Peer port WWN is 00:00:00:00:00:00:00:00
            Admin port mode is E, trunk mode is on
```

```
snmp link state traps are enabled
    Port mode is TE
    Port vsan is 20
Trunk vsans (admin allowed and active) (20)
    Trunk vsans (up)                        (20)
    Trunk vsans (isolated)                  ()
    Trunk vsans (initializing)              ()
    1 minute input rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
    1 minute output rate 0 bits/sec, 0 bytes/sec, 0 frames/sec
      13 frames input, 1028 bytes
        0 discards, 0 errors
      13 frames output, 1180 bytes
        0 discards, 0 errors
last clearing of "show interface" counters never
    Interface last changed at Sat Nov  6 17:58:39 2010
```

CHAPTER 4

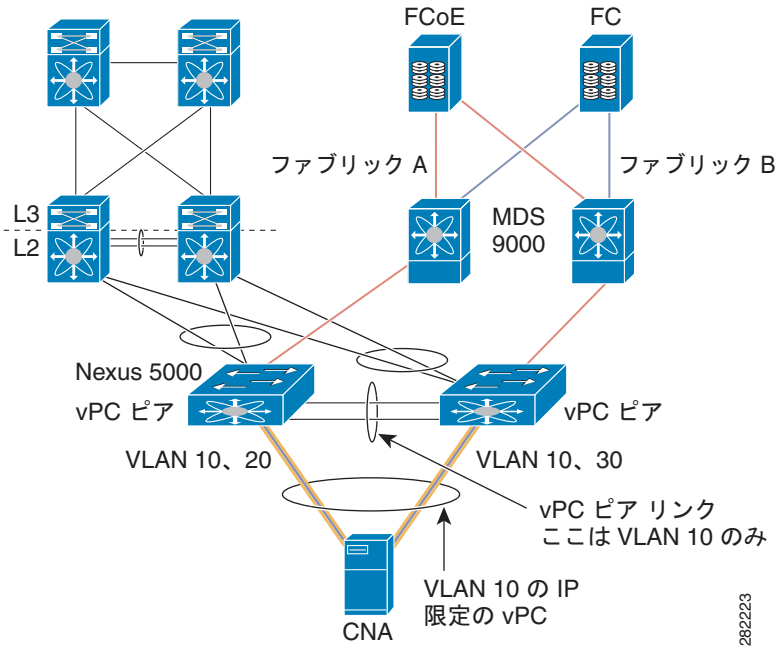
vPC を使用した FCoE の設定例

Cisco NX-OS Release 4.1(3)N1(1) 以降では、Cisco Nexus 5000 シリーズ スイッチは、設定することによって帯域幅を増やせる vPC と、イーサネット ファブリックに対する増強されたロードバランシングをサポートします。この付録では、vPC を使用する場合に、Cisco Nexus 5000 シリーズ スイッチで FCoE を設定する方法に関する設定例を示します。具体的な内容は次のとおりです。

- 「Cisco Nexus 5000 シリーズ スイッチの vPC の設定例」（P.4-2）
- 「Cisco Nexus 5000 シリーズ スイッチの FCoE の設定例」（P.4-5）

図 4-1 に、この付録で説明する例で使用するトポロジを示します。

図 4-1　　Nexus 5000 FCoE および vPC ラボ トポロジ



設定例では、次のパラメータが含まれています。

switchname: n5k-tme-1

switchname: n5k-tme-2

mgmt ip: 172.25.182.66

mgmt ip: 172.25.182.67

設定例には、次のハードウェアが含まれています。

- Dell サーバ PE2950
- QLogic QLE8142（Schultz）第 2 世代 CNA
- Cisco NX-OS Release 4.1(3)N1(1) を実行している 2 台の Cisco Nexus 5010 スイッチ

設定例は次の考慮事項と要件を含んでいます。

1. DCBX をサポートする第 2 世代 CNA が必要です。
2. 別のスイッチへの単一のホスト CNA ポート チャネル接続。単一スイッチのポート チャネルで、ポート チャネルまたは vPC に複数のメンバー ポートが含まれている場合、FCoE インターフェイスは機能しません。
3. Cisco NX-OS Release 4.1(3)N1(1) またはそれ以降のリリース。
4. FC 機能パッケージ（FC_FEATURES_PKG）は FCoE を実行するために必要です。これがインストールされていない場合、90 日持続する一時ライセンスがあります。

この付録は、次の項で構成されています。

Cisco Nexus 5000 シリーズ スイッチの vPC の設定例

この例では、基本設定（IP アドレス（mgmt0）、スイッチ名、管理者のパスワードなど）がスイッチで完了していると仮定します。

次に、基本的な vPC を設定する例を示します。vPC の設定の詳細については、『*Cisco Nexus 5000 Series vPC Quick Configuration Guide*』を参照してください。

（注）　設定は、vPC トポロジの両方のピア スイッチで実行する必要があります。

ステップ 1　両方のピア スイッチで vPC 機能をイネーブルにします。

```
tme-n5k-1# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
tme-n5k-1(config)# feature vpc
tme-n5k-1(config)#

tme-n5k-2# conf t
Enter configuration commands, one per line.  End with CNTL/Z.
tme-n5k-2(config)# feature vpc
tme-n5k-2(config)#
```

ステップ 2　vPC ドメインおよびピアのキープアライブの宛先を設定します。

```
tme-n5k-1(config)# vpc domain 2
tme-n5k-1(config-vpc-domain)# peer-keepalive destination 192.165.200.229

tme-n5k-2(config)# vpc domain 2
tme-n5k-2(config-vpc-domain)# peer-keepalive destination 192.165.200.230
```

（注）　この設定では、スイッチ tme-n5k-1 の管理 IP アドレスは 192.165.200.229、スイッチ tme-n5k-2 の管理 IP アドレスは 192.165.200.230 です。

ステップ 3　vPC ピアリンクとして使用するポート チャネル インターフェイスを設定します。

```
tme-n5k-1(config)# int port-channel 1
tme-n5k-1(config-if)# vpc peer-link
```

（注）　vPC ピアリンクでは、スパニングツリー ポート タイプは、ネットワーク ポート タイプに変更されます。これにより、STP ブリッジ保証（デフォルトでイネーブル）がディセーブルでなければ、vPC ピアリンクの STP ブリッジ保証がイネーブルになります。

```
tme-n5k-2(config)# int port-channel 1
tme-n5k-2(config-if)# vpc peer-link
```

ステップ 4　ピア キープアライブに到達できることを確認します。

```
tme-n5k-1(config)# show vpc peer-keepalive
vPC keep-alive status           : peer is alive
--Destination                   : 172.25.182.167
--Send status                   : Success
--Receive status                : Success
--Last update from peer         : (0   ) seconds, (975 ) msec
tme-n5k-1(config)#

tme-n5k-2(config)# show vpc peer-keepalive
--PC keep-alive status           : peer is alive
--Destination                   : 172.25.182.166
--Send status                   : Success
--Receive status                : Success
--Last update from peer         : (0   ) seconds, (10336 ) msec
tme-n5k-2(config)#
```

ステップ 5　vPC ピア リンク ポート チャネルにメンバー ポートを追加し、このポート チャネル インターフェイスを起動します。

```
tme-n5k-1(config-if-range)# int po 1
tme-n5k-1(config-if)# switchport mode trunk
tme-n5k-1(config-if)# no shut
tme-n5k-1(config-if)# exit
tme-n5k-1(config)# int eth 1/39-40
tme-n5k-1(config-if-range)# switchport mode trunk
tme-n5k-1(config-if-range)# channel-group 1
tme-n5k-1(config-if-range)# no shut
tme-n5k-1(config-if-range)#

tme-n5k-2(config-if-range)# int po 1
tme-n5k-2(config-if)# switchport mode trunk
tme-n5k-2(config-if)# no shut
tme-n5k-2(config-if)# exit
tme-n5k-2(config)# int eth 1/39-40
tme-n5k-2(config-if-range)# switchport mode trunk
tme-n5k-2(config-if-range)# channel-group 1
tme-n5k-2(config-if-range)# no shut
tme-n5k-2(config-if-range)#

tme-n5k-1(config-if-range)# show int po1
port-channel 1 is up
Hardware: Port-Channel, address: 000d.ecde.a92f (bia 000d.ecde.a92f)
MTU 1500 bytes, BW 20000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA
Port mode is trunk
full-duplex, 10 Gb/s
Beacon is turned off
Input flow-control is off, output flow-control is off
Switchport monitor is off
```

```
Members in this channel: Eth1/39, Eth1/40
Last clearing of "show interface" counters never
1 minute input rate 1848 bits/sec, 0 packets/sec
1 minute output rate 3488 bits/sec, 3 packets/sec
tme-n5k-1(config-if-range)#

tme-n5k-2(config-if-range)# show int po1
port-channel1 is up
Hardware: Port-Channel, address: 000d.ecdf.5fae (bia 000d.ecdf.5fae)  MTU 1500 bytes,
BW 20000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA
Port mode is trunk
full-duplex, 10 Gb/s
Beacon is turned off
Input flow-control is off, output flow-control is off
Switchport monitor is off
Members in this channel: Eth1/39, Eth1/40
Last clearing of "show interface" counters never
minute input rate 1848 bits/sec, 0 packets/sec
minute output rate 3488 bits/sec, 3 packets/sec
tme-n5k-2(config-if-range)#
```

ステップ 6　vPC を作成し、メンバー インターフェイスを追加します。

```
tme-n5k-1(config)# int po 11
tme-n5k-1(config-if)# vpc 11
tme-n5k-1(config-if)# switchport mode trunk
tme-n5k-1(config-if)# no shut
tme-n5k-1(config-if)# int eth 1/1
tme-n5k-1(config-if)# switchport mode trunk
tme-n5k-1(config-if)# channel-group 11
tme-n5k-1(config-if)# spanning-tree port type edge trunk
tme-n5k-1(config-if)#
```

警告　**エッジ ポート タイプ（PortFast）は、単一のホストに接続されているポートだけでイネーブルにする必要があります。エッジ ポート タイプ（PortFast）がイネーブルの場合、このインターフェイスにハブ、コンセントレータ、スイッチ、ブリッジなどの一部のデバイスを接続すると、一時的なブリッジング ループが発生することがあります。このタイプの設定は、慎重に行う必要があります**

```
tme-n5k-2(config)# int po 11
tme-n5k-2(config-if)# vpc 11
tme-n5k-2(config-if)# switchport mode trunk
tme-n5k-2(config-if)# no shut
tme-n5k-2(config-if)# int eth 1/1
tme-n5k-2(config-if)# switchport mode trunk
tme-n5k-2(config-if)# channel-group 11
tme-n5k-2(config-if)# spanning-tree port type edge trunk
```

警告　**エッジ ポート タイプ（PortFast）は、単一のホストに接続されているポートだけでイネーブルにする必要があります。エッジ ポート タイプ（PortFast）がイネーブルの場合、このインターフェイスにハブ、コンセントレータ、スイッチ、ブリッジなどの一部のデバイスを接続すると、一時的なブリッジング ループが発生することがあります。このタイプの設定は、慎重に行う必要があります。**

（注）　vPC トポロジを介した FCoE を実行するには、ポート チャネルは単一のメンバー インターフェイスのみ持てます。

（注）　ポート チャネル インターフェイスの下に設定された vPC 番号は、両方の Nexus 5000 スイッチで一致する必要があります。ポート チャネル インターフェイス番号が両方のスイッチで一致している必要はありません。

ステップ 7　vPC インターフェイスが起動していて、動作していることを確認します。

```
tme-n5k-1(config-if)# show vpc statistics vpc 11
port-channel11 is up
vPC Status: Up, vPC number: 11
Hardware: Port-Channel, address: 000d.ecde.a908 (bia 000d.ecde.a908)
MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA
Port mode is trunk
full-duplex, 10 Gb/s
Beacon is turned off
Input flow-control is off, output flow-control is off
Switchport monitor is off
Members in this channel: Eth1/1
Last clearing of "show interface" counters never
minute input rate 4968 bits/sec, 8 packets/sec
minute output rate 792 bits/sec, 1 packets/sec
tme-n5k-1(config-if)#

tme-n5k-2(config-if)# show vpc statistics vpc 11
port-channel11 is up
vPC Status: Up, vPC number: 11
Hardware: Port-Channel, address: 000d.ecdf.5fae (bia 000d.ecdf.5fae)
MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
reliability 255/255, txload 1/255, rxload 1/255
Encapsulation ARPA
Port mode is trunk
full-duplex, 10 Gb/s
Beacon is turned off
Input flow-control is off, output flow-control is off
Switchport monitor is off
Members in this channel: Eth1/1
Last clearing of "show interface" counters never
minute input rate 4968 bits/sec, 8 packets/sec
minute output rate 792 bits/sec, 1 packets/sec
tme-n5k-1(config-if)#
```

Cisco Nexus 5000 シリーズ スイッチの FCoE の設定例

vPC が 2 台の Nexus 5000 間に設定されれば、FCoE トポロジの設定に進むことができます。この虎の巻では、IP アドレス（mgmt0）、スイッチ名、パスワード、管理者などを指定する基本設定が Nexus 5000 スイッチ上で実施済みであり、前の項に従って vPC 設定が完了していると想定しています。次の手順では、vPC トポロジとともに FCoE トポロジを設定するために必要な FCoE の基本設定を行います。

ステップ 1　Nexus 5000 上で FCoE をイネーブルにします。

```
tme-n5k-1(config)# feature fcoe
FC license checked out successfully
fc_plugin extracted successfully
FC plugin loaded successfully
FCoE manager enabled successfully
```

```
FC enabled on all modules successfully
tme-n5k-1(config)#

tme-n5k-2(config)# feature fcoe
FC license checked out successfully
fc_plugin extracted successfully
FC plugin loaded successfully
FCoE manager enabled successfully
FC enabled on all modules successfully
fme-n5k-2(config)#
```

（注）　これが完了するまでに数分かかることがあります。

ステップ 2　VSAN を作成して、FCoE トラフィックの伝送用として指定されている VLAN にマッピングします。

```
tme-n5k-1(config)# vsan database
tme-n5k-1(config-vsan-db)# vsan 100
tme-n5k-1(config-vsan-db)# exit
tme-n5k-1(config)# vlan 100
me-n5k-1(config-vlan)# fcoe vsan 100
tme-n5k-1(config-vlan)# show vlan fcoe
VLAN      VSAN      Status
--------  --------  --------
100       100       Operational
tme-n5k-1(config-vlan)#

tme-n5k-2(config)# vsan database
tme-n5k-2(config-vsan-db)# vsan 101
tme-n5k-2(config-vsan-db)# exit
tme-n5k-2(config)# vlan 101
tme-n5k-2(config-vlan)# fcoe vsan 101
tme-n5k-2(config-vlan)# show vlan fcoe
VLAN      VSAN      Status
--------  --------  --------
101       101       Operational
tme-n5k-2(config)#
```

（注）　VLAN 番号および VSAN 番号が同じである必要はありません。

ステップ 3　vPC リンクの通過を許可される VLAN を設定します。

```
tme-n5k-1(config)# int po 11
tme-n5k-1(config-if)# switchport trunk allowed vlan 1, 100
tme-n5k-1(config-if)# show int trunk
--------------------------------------------------------------------------------
Port          Native    Status        Port
--------------------------------------------------------------------------------
Eth1/1         1       trnk-bndl     Po11
Eth1/39        1       trnk-bndl     Po1
Eth1/40        1       trnk-bndl     Po1
Po1            1       trunking      --
Po11           1       trunking      --

--------------------------------------------------------------------------------
Port          Vlans Allowed on Trunk
--------------------------------------------------------------------------------
Eth1/1        1,100
Eth1/39       1-3967,4048-4093
Eth1/40       1-3967,4048-4093
Po1           1-3967,4048-4093
Po11          1,100
```

```
--------------------------------------------------------------------------------
Port          Vlans Err-disabled on Trunk
--------------------------------------------------------------------------------
Eth1/1        none
Eth1/39       100
Eth1/40       100
Po1           100
Po11          none

--------------------------------------------------------------------------------
Port          STP Forwarding
--------------------------------------------------------------------------------
Eth1/1        none
Eth1/39       none
Eth1/40       none
Po1           1
Po11          1,100
tme-n5k-1(config-if)#

tme-n5k-2(config)# int po 11
tme-n5k-2(config-if)# switchport trunk allowed vlan 1, 101
tme-n5k-2(config-if)# show int trunk
--------------------------------------------------------------------------------
Port          Native    Status        Port
--------------------------------------------------------------------------------
Eth1/1         1       trnk-bndl     Po11
Eth1/39        1       trnk-bndl     Po1
Eth1/40        1       trnk-bndl     Po1
Po1            1       trunking      --
Po11           1       trunking      --

--------------------------------------------------------------------------------
Port          Vlans Allowed on Trunk
--------------------------------------------------------------------------------
Eth1/1        1,101
Eth1/39       1-3967,4048-4093
Eth1/40       1-3967,4048-4093
Po1           1-3967,4048-4093
Po11          1,101

--------------------------------------------------------------------------------
Port          Vlans Err-disabled on Trunk
--------------------------------------------------------------------------------
Eth1/1        none
Eth1/39       101
Eth1/40       101
Po1           101
Po11          none

--------------------------------------------------------------------------------
Port          STP Forwarding
--------------------------------------------------------------------------------
Eth1/1        none
Eth1/39       none
Eth1/40       none
Po1           1
Po11          1,101
tme-n5k-2(config-if)#
```

ステップ 4　仮想ファイバ チャネル インターフェイス（vfc）を作成し、前のステップで作成した VSAN に追加します。

```
tme-n5k-1(config)# int vfc 1
```

```
tme-n5k-1(config-if)# bind interface po11
Warning: VFC will not come up for pre-FIP CNA
tme-n5k-1(config-if)# no shut
tme-n5k-1(config-if)#

tme-n5k-2(config)# int vfc 1
tme-n5k-2(config-if)# bind interface po11
Warning: VFC will not come up for pre-FIP CNA
tme-n5k-2(config-if)# no shut
tme-n5k-2(config-if)#

tme-n5k-1(config)# vsan database
tme-n5k-1(config-vsan-db)# vsan 100 interface vfc 1
tme-n5k-1(config)# show vsan membership
vsan 1 interfaces:
fc2/1             fc2/2             fc2/3             fc2/4
fc2/5             fc2/6             fc2/7             fc2/8

vsan 100 interfaces:
vfc1

vsan 4079(evfp_isolated_vsan) interfaces:

vsan 4094(isolated_vsan) interfaces:
tme-n5k-1(config)#

tme-n5k-2(config)# vsan database
tme-n5k-2(config-vsan-db)# vsan 101 interface vfc 1
tme-n5k-2(config)# show vsan membership
vsan 1 interfaces:
fc2/1             fc2/2             fc2/3             fc2/4
fc2/5             fc2/6             fc2/7             fc2/8

vsan 101 interfaces:
vfc1

vsan 4079(evfp_isolated_vsan) interfaces:

vsan 4094(isolated_vsan) interfaces:
tme-n5k-2(config)#
```

ステップ 5　vfc が起動し、動作していることを確認します。

```
tme-n5k-1(config-if)# show int brief
--------------------------------------------------------------------------------
Ethernet      VLAN   Type    Mode   Status   Reason          Speed
--------------------------------------------------------------------------------
Eth1/1        1      eth    trunk   up       none            10G(D)
Eth1/2        1      eth    access  up       none            10G(D)
Eth1/38       1      eth   access  down   SFP not inserted    10G(D)
Eth1/39       1      eth   trunk   up       none            10G(D)
Eth1/40       1      eth   trunk   up       none            10G(D)

--------------------------------------------------------------------------------
Port-channel VLAN  Type Mode   Status  Reason                 Speed
--------------------------------------------------------------------------------
Po1           1      eth   trunk  up      none            a-10G(D)  none
Po11          1      eth   trunk  up      none            a-10G(D)  none

--------------------------------------------------------------------------------
Port   VRF          Status IP Address                       Speed    MTU
--------------------------------------------------------------------------------
mgmt0  --           up     172.25.182.166                   1000     1500
```

```
--------------------------------------------------------------------------------
Interface   Vsan       Admin   Admin   Status       SFP   Oper  Oper  Port
--------------------------------------------------------------------------------
vfc1        100    F      on      up    --     F    auto   --
tme-n5k-1(config-if)#

tme-n5k-2(config-if)# show int brief
--------------------------------------------------------------------------------
Ethernet      VLAN   Type    Mode   Status   Reason          Speed    Port
--------------------------------------------------------------------------------
Eth1/1        1      eth    trunk   up       none            10G(D)   11
Eth1/2        1      eth    access  up       none            10G(D)   --
Eth1/38       1      eth   access  down   SFP not inserted    10G(D)   --
Eth1/39       1      eth   trunk   up       none            10G(D)   1
Eth1/40       1      eth   trunk   up       none            10G(D)   1

--------------------------------------------------------------------------------
Port-channel VLAN  Type Mode   Status  Reason                Speed  Protocol
--------------------------------------------------------------------------------
Po1           1      eth   trunk  up      none            a-10G(D)  none
Po11          1      eth   trunk  up      none            a-10G(D)  none

--------------------------------------------------------------------------------
Port   VRF          Status IP Address                      Speed    MTU
--------------------------------------------------------------------------------
mgmt0  --           up     172.25.182.167                  1000     1500

--------------------------------------------------------------------------------
Interface   Vsan       Admin   Admin   Status       SFP   Oper  Oper
--------------------------------------------------------------------------------
vfc1        101     F      on      up    --     F    auto   --
tme-n5k-2(config-if)#
```

ステップ 6　仮想ファイバ チャネル インターフェイスがファブリックにログインしたことを確認します。

```
tme-n5k-1# show flogi database
--------------------------------------------------------------------------------
INTERFACE      VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
vfc1     100    0x540000 21:00:00:c0:dd:11:2a:01 20:00:00:c0:dd:11:2a:01

Total number of flogi = 1.
tme-n5k-2# show flogi database
--------------------------------------------------------------------------------
INTERFACE      VSAN    FCID           PORT NAME               NODE NAME
--------------------------------------------------------------------------------
vfc1           101  0x540000  21:00:00:c0:dd:11:2a:01 20:00:00:c0:dd:11:2a:01

Total number of flogi = 1.
```

ステップ 7　vPC が起動し、動作していることを確認します。

```
tme-n5k-1(config-if)# show vpc statistics vpc 11
port-channel11 is up
vPC Status: Up, vPC number: 11
Hardware: Port-Channel, address: 000d.ecde.a908 (bia 000d.ecde.a908)
    MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA
    Port mode is trunk
    full-duplex, 10 Gb/s
    Beacon is turned off
```

```
    Input flow-control is off, output flow-control is off
    Switchport monitor is off
    Members in this channel: Eth1/1
    Last clearing of "show interface" counters never
    1 minute input rate 4968 bits/sec, 8 packets/sec
    1 minute output rate 792 bits/sec, 1 packets/sec

tme-n5k-2(config-if)# show vpc statistics vpc 11
port-channel11 is up
vPC Status: Up, vPC number: 11
Hardware: Port-Channel, address: 000d.ecdf.5fae (bia 000d.ecdf.5fae)
    MTU 1500 bytes, BW 10000000 Kbit, DLY 10 usec,
    reliability 255/255, txload 1/255, rxload 1/255
    Encapsulation ARPA
    Port mode is trunk
    full-duplex, 10 Gb/s
    Beacon is turned off
    Input flow-control is off, output flow-control is off
    Switchport monitor is off
    Members in this channel: Eth1/1
    Last clearing of "show interface" counters never
    1 minute input rate 4968 bits/sec, 8 packets/sec
    1 minute output rate 792 bits/sec, 1 packets/sec
```

CHAPTER 5

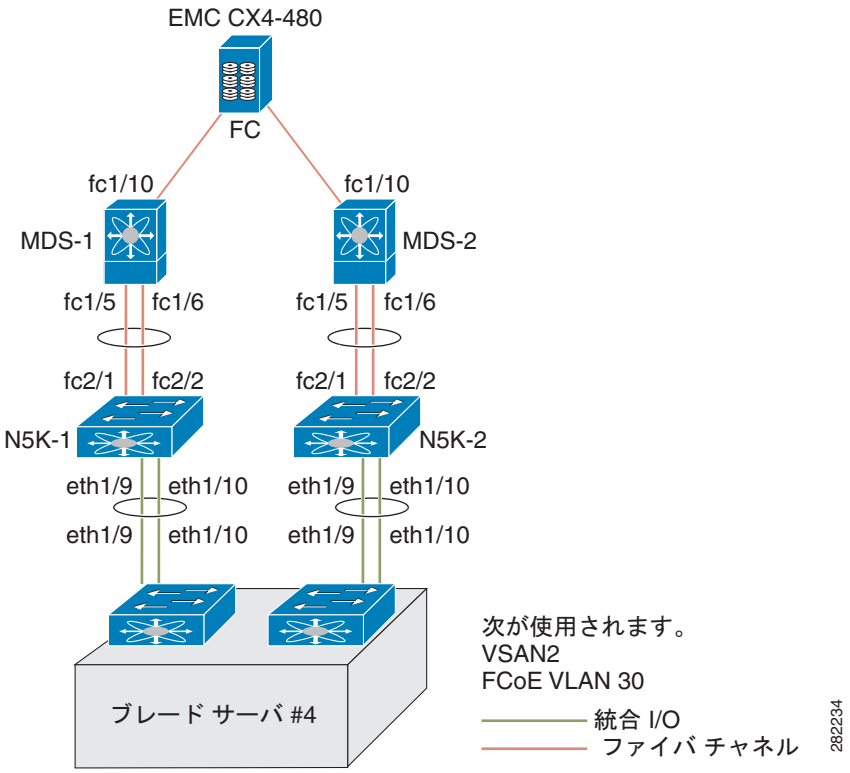
Cisco Nexus 4000 シリーズ スイッチによる FCoE の設定例

ここでは、FCoE を使用して Cisco MDS 9000 シリーズ ファミリ スイッチの FC ストレージにアクセスする Cisco Nexus 5000 シリーズ スイッチに接続された、Cisco Nexus 4000 シリーズ スイッチに接続する IBM ブレード サーバの設定方法に関する設定例を示します。Cisco Nexus 4000 シリーズ スイッチは FIP スヌーピング ブリッジであるため、CNA で行われる FLOGI は Cisco Nexus 4000 シリーズ スイッチにログインしないで、FCF である Cisco Nexus 5000 シリーズ スイッチにログオンします。Cisco Nexus 4000 シリーズ スイッチ ブレード サーバの vFC インターフェイスを作成しても、Cisco Nexus 5000 シリーズ スイッチがスイッチングと NPV いずれのモードなのかは変更されません。ここで、実際に実行されるファブリック ログインは、Cisco Nexus 5000 シリーズ スイッチのモードによって決まります。

- スイッチング モードの Cisco Nexus 5000 シリーズ スイッチ：Cisco Nexus 5000 シリーズ スイッチにログインします。
- NPV モードの Cisco Nexus 5000 シリーズ スイッチ：ログインは Cisco MDS 9000 シリーズ ファミリ スイッチまたは NPIV が設定された FC スイッチのアップストリームで行われます。

この例では、スイッチング モードの Cisco Nexus 5000 シリーズ スイッチです。図 5-1 に、例で使用されているトポロジを示します。

図 5-1　Nexus 4000 FCoE ラボ トポロジ



次のハードウェアが使用されました。

- IBM Blade シャーシ モデル BCH
- Qlogic QMI8142 を使用して Windows 2003 を実行している IBM HS22 ブレード サーバ
- Cisco NX-OS Release 4.1(2)E1(1) を実行している Cisco Nexus 4000 シリーズ スイッチ
- Cisco NX-OS Release 4.1(3)N1(1) を実行している Cisco Nexus 5010 スイッチ
- Cisco SAN-OS Release 4.1(3a) を実行する Cisco MDS 9124 ディレクタ スイッチ
- EMC CX4-480

この付録は、次の項で構成されています。

スイッチング モードの Cisco Nexus 5000 シリーズ スイッチ

この例の手順に従う前に、Cisco Nexus 5000 シリーズ スイッチの基本設定（IP アドレス（mgmt0）、スイッチ名、管理者のパスワードなど）が完了しており、FCoE がディセーブルになっていることを確認してください。

実働環境でこの設定例を使用するには、FC 機能パッケージのライセンスがインストールされている必要があります。そうでない場合は、90 日後に期限切れになる一時ライセンスがあります。ライセンスが期限切れになると、機能はディセーブルになります。

Cisco Nexus 5000 シリーズ スイッチでは、デフォルトで FCoE はディセーブルです。

次に、FCoE をイネーブルにする例を示します。

```
n5k-2# show interface brief
--------------------------------------------------------------------------------
----------------------
Ethernet VLAN Type Mode Status Reason Speed Port
Interface                 Ch #
Eth1/1 1 eth access up none 10G(D) --
Eth1/2 1 eth access up none 10G(D) --
[snip]
Eth2/4 1 eth access down SFP not inserted 10G(D) --
--------------------------------------------------------------------------------
Port VRF Status IP Address Speed MTU
--------------------------------------------------------------------------------
mgmt0 -- up 172.25.182.164 1000 1500
```

（注）　Cisco Nexus 5010 スイッチに搭載された 4x4 GEM カードであるにもかかわらず、FC インターフェイスはありません。

```
n5k-2# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
n5k-2(config)# feature fcoe
FC license checked out successfully fc_plugin extracted successfully FC plugin loaded
successfully FCoE manager enabled successfully FC enabled on all modules successfully
```

（注）　Cisco NX-OS Release 4.1(3)N1(1) 以降では、FCoE をイネーブルにするときにスイッチをリブートする必要はありません。FCoE がイネーブルの場合、Cisco Nexus 5000 シリーズ スイッチは、デフォルトでスイッチング モードです。

```
n5k-2(config)# show feature
Feature Name Instance State
fcsp 1 disabled
fcoe 1 enabled
fex 1 enabled

n5k-2(config)# show interface brief
--------------------------------------------------------------------------------
----------------------
Interface Vsan Admin Admin Status SFP Oper Oper Port
Mode Trunk Mode Speed Channel
Mode (Gbps)
--------------------------------------------------------------------------------
----------------------
fc2/1 1 auto on down swl -- --
fc2/2 1 auto on down swl -- --
```

```
fc2/3 1 auto on down swl -- --
fc2/4 1 auto on sfpAbsent -- -- --
--------------------------------------------------------------------------------
----------------------
Ethernet VLAN Type Mode Status Reason Speed Port
Interface Ch #
--------------------------------------------------------------------------------
----------------------
Eth1/1 1 eth access up none 10G(D) --
Eth1/2 1 eth access up none 10G(D) --
```

（注）　FC インターフェイスを表示するには、**show interface brief** コマンドを使用します。

Cisco MDS ディレクトリ シリーズに接続された Cisco Nexus 5000 シリーズ スイッチの SAN ポート チャネルの設定

次に、Cisco MDS 9000 ディレクタに接続された Cisco Nexus 5000 シリーズ スイッチの SAN ポート チャネルを設定する例を示します。冗長性を確保するために、FC インターフェイスからの SAN ポート チャネルを作成することを推奨します。

ステップ 1　Cisco Nexus 5000 シリーズ スイッチの SAN ポート チャネルを設定します。

```
Fn5k-2# configure terminal
n5k-2(config)# interface san-port-channel 1
n5k-2(config-if)# interface fc2/1-2
n5k-2(config-if)# channel-group 1
```

（注）　san-port-channel 1 に fc2/1 fc2/2 を追加したら、ポート チャネルをディセーブルにする必要があります。これは、ポート チャネルのもう一方の端にあるスイッチでも実行する必要があります。次に、インターフェイスを起動するために両端でインターフェイスを停止します。

```
n5k-2(config-if)# no shut
n5k-2(config-if)# interface san-port-channel 1
n5k-2(config-if)# no shut
n5k-2(config-if)# show san-port-channel database
san-port-channel 1
Administrative channel mode is on Operational channel mode is on Last membership
update is successful 2 ports in total, 0 ports up Age of the port-channel is
0d:00h:17m:14s
Ports: fc2/1 [down] fc2/2 [down]
n5k-2(config-if)#
```

（注）　Cisco MDS 9000 シリーズ ディレクタが設定されていないため、SAN ポート チャネルは、この時点では停止しています。

ステップ 2　Cisco Nexus 5000 シリーズ スイッチと Cisco MDS 9124 スイッチ間のポート チャネルを作成するために Cisco MDS 9124 スイッチを設定します。

（注）　Cisco Nexus 5000 の SAN ポート チャネルを MDS に対して設定してある場合は、Cisco MDS 9000 シリーズ スイッチで同じ設定を行う必要があります。Cisco MDS 9000 シリーズ スイッチの SAN ポート チャネル設定をポート チャネルと呼びます。

```
mds9124-2# configure terminal
mds9124-2(config)# interface port-channel 1
mds9124-2(config-if)# interface fc1/5, fc1/6
mds9124-2(config-if)# channel-group 1 force
```

（注）　ポート チャネル 1 に fc1/5 fc1/6 を追加した後にポート チャネルをディセーブルにする必要があります。これは、ポート チャネルのもう一方の端にあるスイッチでも実行する必要があります。次に、インターフェイスを起動するために両端でインターフェイスを停止します。

（注）

```
mds9124-2(config-if)# no shut
mds9124-2(config-if)# interface port-channel 1
mds9124-2(config-if)# no shut
```

ステップ 3　Cisco Nexus 5000 シリーズ スイッチの SAN ポート チャネルが稼働中であることを確認します。**show san-port-channel database** コマンドを使用して、SAN ポート チャネルの設定を表示します。

```
n5k-2(config-if)# show san-port-channel database
san-port-channel 1
Administrative channel mode is on
Operational channel mode is on
Last membership update is successful
2 ports in total, 2 ports up
First operational port is fc2/2
Age of the port-channel is 0d:00h:25m:10s
Ports: fc2/1 [up]
fc2/2 [up] *
```

Cisco Nexus 4000 シリーズ スイッチに接続された Cisco Nexus 5000 シリーズ スイッチのポート チャネルの設定

次に、Cisco Nexus 4000 シリーズ スイッチに接続された Cisco Nexus 5000 シリーズ スイッチのポート チャネルを設定する例を示します。

ステップ 1　Cisco Nexus 5000 シリーズ スイッチのポート チャネルを設定します。

このポート チャネルは、Cisco Nexus 4000 シリーズ スイッチから Cisco Nexus 5000 シリーズ スイッチに着信するトラフィックに冗長性を提供するように設定されます。この例では、すべての VLAN がポート チャネルを通過できます。FCoE VLAN およびネイティブ VLAN がポート チャネルを通過できる必要があります。実稼働環境では、ネットワーク管理者は、このネットワークを通過するように他の VLAN を指定できます。

```
n5k-2# configure terminal
n5k-2(config)# feature lacp
n5k-2(config)# interface port-channel 2 mode active
n5k-2(config-if)# interface eth1/9-10
n5k-2(config-if)# channel-group 2
```

```
n5k-2(config)# interface port-channel 2
n5k-2(config-if)# switchport mode trunk
n5k-2(config-if)# no shut
n5k-2#
```

ステップ 2　Cisco Nexus 4000 シリーズ スイッチのポート チャネルを設定します。

```
bch1-n4k-b9# configure terminal
bch1-n4k-b9(config)# feature lacp
bch1-n4k-b9(config)# interface port-channel 20
bch1-n4k-b9(config-if)# interface eth1/15-16
bch1-n4k-b9(config-if)# channel-group 2 mode active
bch1-n4k-b9(config)# interface port-channel 2
bch1-n4k-b9(config-if)# switchport mode trunk
bch1-n4k-b9(config-if)# no shut
bch1-n4k-b9(config-if)#
```

Cisco Nexus 4000 シリーズ スイッチの仮想ファイバ チャネル インターフェイスの設定

次に、Cisco Nexus 4000 シリーズ スイッチの vFC インターフェイスを設定する例を示します。

ステップ 1　Cisco Nexus 5000 シリーズ スイッチで、Cisco MDS 9000 シリーズ スイッチの実稼働 VSAN と一致するように VSAN を設定します。これはワンタイム設定です。

ステップ 2　Cisco Nexus 5000 シリーズ スイッチで、VSAN にマッピングするために FCoE VLAN を設定します（VLAN-to-VSAN マッピング）。これはワンタイム設定です。

ステップ 3　Cisco Nexus 4000 シリーズ スイッチで、Nexus 5000 シリーズ スイッチの FCoE VLAN と一致する FIP スヌーピング VLAN を設定します。これはワンタイム設定です。

ステップ 4　Cisco Nexus 4000 シリーズ スイッチで、FCoE トラフィック（FIP スヌーピング）を許可する、アップリンクを設定します。

ステップ 5　Cisco Nexus 4000 シリーズ スイッチのブレード サーバで、FCoE トラフィックのイーサネット インターフェイスを設定します。

ステップ 6　Cisco Nexus 5000 シリーズ スイッチで、vFC を設定します。

ステップ 7　Cisco Nexus 4000 シリーズ スイッチのブレード サーバで、ブレード サーバの MAC アドレスに vFC をバインドします。

ステップ 8　vFC が正しい VSAN にあることを確認します。

（注）　上記の作業を完了すると Nexus 4000 からブレード サーバにある FCoE CNA に確実に接続できるようになります。

Cisco Nexus 5000 シリーズ スイッチの VSAN の設定

Fabric Manager、Device Manager、または CLI を使用して Cisco Nexus 5000 シリーズ スイッチの VSAN を設定できます。次に、CLI 設定作業および Fabric Manager または Device Manager GUI の作業の例を示します。

この例は、Cisco MDS 9000 シリーズのストレージが VSAN 2 にあることを示します。Cisco Nexus 5000 シリーズ スイッチに設定されている vFC がストレージ デバイスと通信できるように、VSAN を設定します。

```
n5k-2# configure terminal
n5k-2(config)# vsan database
n5k-2(config-vsan-db)# vsan 2
n5k-2(config-vsan-db)# show vsan vsan 1 information
name:VSAN0001 state:active
interoperability mode:default
loadbalancing:src-id/dst-id/oxid
operational state:up
vsan 2 information
name:VSAN0002 state:active
interoperability mode:default
loadbalancing:src-id/dst-id/oxid
 operational state:down
        vsan 4079:evfp_isolated_vsan
        vsan 4094:isolated_vsan
```

Cisco Nexus 5000 シリーズ スイッチの FCoE VLAN の設定

VLAN を設定してから、CLI を使用して特定の VSAN に VLAN をマッピングできます。Fabric Manager および Device Manager はこの設定には使用できません。シスコでは、FCoE トラフィックに個別の VLAN および標準イーサネット トラフィックに個別の VLAN を設定することを推奨します。

次に、FCoE VLAN を作成する例を示します。

```
n5k-2# configure terminal
        n5k-2(config)# vlan 30
        n5k-2(config-vlan)# fcoe vsan 2
        n5k-2(config-vlan)# show vlan fcoe
VLAN
VSAN
Status
--------
--------
--------
30
2
Operational
```

Cisco Nexus 4000 シリーズ スイッチの FIP スヌーピング VLAN の設定

Cisco Nexus 4000 シリーズ スイッチでは、デフォルトで FIP スヌーピング機能はディセーブルです。シスコでは、基本設定中にプロンプトが表示されたら、FCoE および FIP スヌーピングをイネーブルにし、たとえば、適切なサービス クラス（CoS）である no drop、MTU、および QoS を設定して、初期設定後にこれらの機能を手動で設定する必要をなくすことを推奨します。

次に、FIP スヌーピングがイネーブルになっていることを確認する例を示します。

```
bch1-n4k-b9# show feature
```

```
Feature Name Instance State
tacacs 1 disabled lacp 1 enabled [snip] fipsm 1 enabled
```

VLAN 30 として Cisco Nexus 5000 シリーズ スイッチに設定されている FCoE VLAN を使用する場合は、Cisco Nexus 4000 シリーズ スイッチの VLAN を作成するために同じ VLAN 番号を使用する必要があり、この VLAN を FIP スヌーピング VLAN として設定する必要があります。

次に、Cisco Nexus 4000 シリーズ スイッチの VLAN を設定する例を示します。

```
bch1-n4k-b9# configure terminal
bch1-n4k-b9(config)# vlan 30
bch1-n4k-b9(config-vlan)# fip-snooping enable
```

FCoE トラフィックを許可する Cisco Nexus 4000 シリーズ スイッチ アップリンクの設定

この例では、すべての VLAN が Cisco Nexus 4000 シリーズ スイッチと Cisco Nexus 5000 シリーズ スイッチの間のアップリンクを通過できるようにするポート チャネルを前の項ですでに作成しました。ポート タイプ モード fcf で FIP スヌーピングを行うために、アップリンク（この場合はポート チャネル）をイネーブルにする必要があります。

次に、アップリンクを設定する例を示します。

```
bch1-n4k-b9# configure terminal
bch1-n4k-b9(config)# interface port-channel 20
bch1-n4k-b9(config-if)# fip-snooping port-mode fcf
```

Cisco Nexus 4000 シリーズ スイッチでの FCoE トラフィック用ブレード サーバ イーサネット インターフェイスの設定

CLI を使用して、ブレード サーバを設定できます。Fabric Manager および Device Manager はこの設定には使用できません。

FCoE VLAN（VLAN 30）がブレード サーバのイーサネット インターフェイス（イーサネット 1/4）を通過できるようにします。ほとんどの場合、CNA のポートでは、通常のイーサネット トラフィックと、異なる VLAN に存在する FCoE トラフィックの両方を許可します。デフォルトでは、Cisco Nexus 4000 シリーズ スイッチ上のすべてのイーサネット インターフェイスは、アクセス モードであり、VLAN 1 にあります。

次に、複数の VLAN（トランク）を許可するようにイーサネット インターフェイスを設定する例を示します。

```
bch1-n4k-b9#configure terminal
bch1-n4k-b9(config)#interface ethernet 1/4
bch1-n4k-b9(config-if)# switchport mode trunk
bch1-n4k-b9(config-if)# switchport trunk allowed vlan 1,30
```

（注） 上記のコマンドは必須ではありませんが、許可される VLAN を指定する場合は、FCoE VLAN が例に示すように、許可リストにあることを確認してください。

```
bch1-n4k-b9(config-if)# spanning-tree port type edge trunk
Warning: Edge port type (portfast) should only be enabled on ports connected to a single
host. Connecting hubs, concentrators, switches, bridges, etc... to this  interface when
edge port type (portfast) is enabled, can cause temporary bridging loops.
Use with CAUTION

Creating vFC Interfaces on the Nexus 5000 - CLI
```

トランク設定が完了したら、Cisco Nexus 5000 シリーズ スイッチの vFC インターフェイスを作成します。Device Manager または CLI を使用して vFC インターフェイスを設定できます。

CNA は Cisco Nexus 4000 シリーズ スイッチのイーサネット インターフェイス eth1/4 で接続されており、Cisco Nexus 5000 シリーズ スイッチに物理的に接続されていないため、FCoE を実施している CNA の MAC アドレスに vFC をバインドする必要があります。現時点では、Cisco Nexus 4000 シリーズ スイッチと相互運用可能なブレード サーバ上の FCoE を実施するベンダーは Qlogic のみです。Qlogic では、標準イーサネット トラフィック用に 1 個と FCoE 専用にもう 1 個の 2 個の個別 MAC アドレスを提供します。

次に、IBM Blade シャーシの特定のブレード サーバから MAC アドレスを指定する例を示します。

```
bch1-n4k-b9# show fip-snooping vlan-discovery
 Legend:
Interface VLAN FIP MAC
Eth1/4 1 00:c0:dd:04:0c:df
 Eth1/5 1 00:c0:dd:04:0d:13
```

Cisco Nexus 5000 シリーズ スイッチでこのブレード サーバの vFC を作成するには、このブレード サーバで識別されている MAC アドレスを使用します。

次に、vFC が VSAN 2 に移動される例を示します。Cisco Nexus 4000 シリーズ スイッチでデバイスに対する vFC 番号を作成するときのベスト プラクティスとして、いずれのブレード シャーシのいずれのブレード サーバに vFC がマッピングされているのかを簡単に識別できる番号設定方式を作成する必要があります。この例では、1 台目の IBM ブレード シャーシのスロット 4 に搭載されたブレード サーバ BCH1 を使用しています。この例では、このブレード サーバの vFC はインターフェイス vfc104 です。

```
n5k-2# configure terminal
n5k-2(config)# interface vfc 104
n5k-2(config-if)# bind mac-address 00:c0:dd:04:0c:df
n5k-2(config-if)# no shutdown
n5k-2(config-if)# show vsan membership
vsan 1 interfaces:
fc2/1 fc2/2 fc2/3 fc2/4 san-port-channel 1 vfc104
vsan 2 interfaces:
vsan 4079(evfp_isolated_vsan) interfaces:
vsan 4094(isolated_vsan) interfaces:
n5k-2(config-if)# vsan database ð
this will get to the VSAN database
 n5k-2(config-vsan-db)# vsan 2 interface vfc104
n5k-2(config-vsan-db)# show vsan membership
vsan 1 interfaces: fc2/1 fc2/2 fc2/3 fc2/4 san-port-channel 1
 vsan 2 interfaces:
vfc104
vsan 4079(evfp_isolated_vsan) interfaces:
n5k-2# show interface vfc104
vfc104 is up
```

バインドされた MAC は 00:c0:dd:04:0c:df、FCF プライオリティは 128、ハードウェアは仮想ファイバチャネル、ポート WWN は 20:67:00:0d:ec:b2:b9:bf、管理ポート モードは F、トランク モードはオン、SNMP リンク状態トラップはイネーブル、ポート モードは F、FCID は 0xcd0000、ポート VSAN は 2
[snip]

Device Manager を使用した vFC インターフェイスの設定

次に、Device Manager を使用して vFC インターフェイスを作成する例を示します。

ステップ 1　Device Manager を開き、Cisco Nexus 5000 シリーズ スイッチにログインします。

図 5-2　Device Manager の [Login] ウィンドウ

ステップ 2　1 台の vFC を設定するには、Device Manager のメニューから [Interface] > [Virtual Interfaces] > [Fibre Channel] を選択します。Quick Configuration ツールを使用して複数の vFC を設定し、物理インターフェイスに一度にバインドすることもできます。

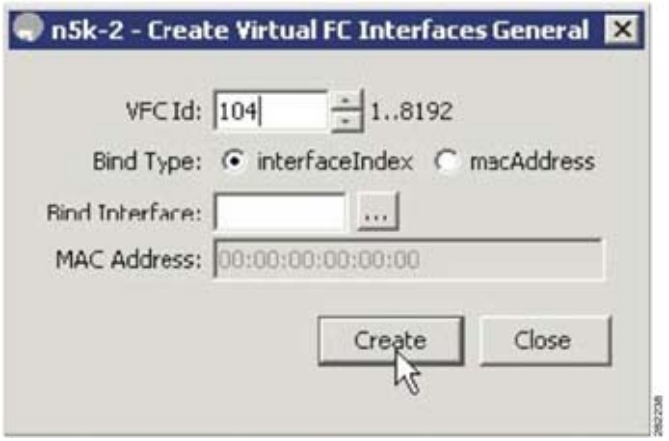
図 5-3　Device Manager のメニュー

ステップ 3　[Virtual FC Interfaces] ウィンドウで [Create] をクリックして vFC を作成します。

図 5-4　[Virtual FC Interfaces] ウィンドウ

ステップ 4　[Create Virtual FC Interfaces General] ウィンドウで、VFC ID、バインド タイプおよびインターフェイス（バインド タイプに応じて物理または MAC アドレス）を入力し、[Create] をクリックします。新しい vFC ID を持つ vFC を表示するウィンドウが再表示されます。

図 5-5　[Create Virtual FC Interfaces General] ウィンドウ



（注）　ベスト プラクティスとして、ブレード サーバに戻る vFC を認識可能な vFC を作成します。たとえば、104 は、ブレード サーバ 4 の BCH1 と相互に関連します。

ステップ 5　[Virtual FC Interfaces] ウィンドウから、[Bind Type] > [macAddress] を選択します。

図 5-6　インターフェイスから MAC アドレスへのバインド タイプの変更

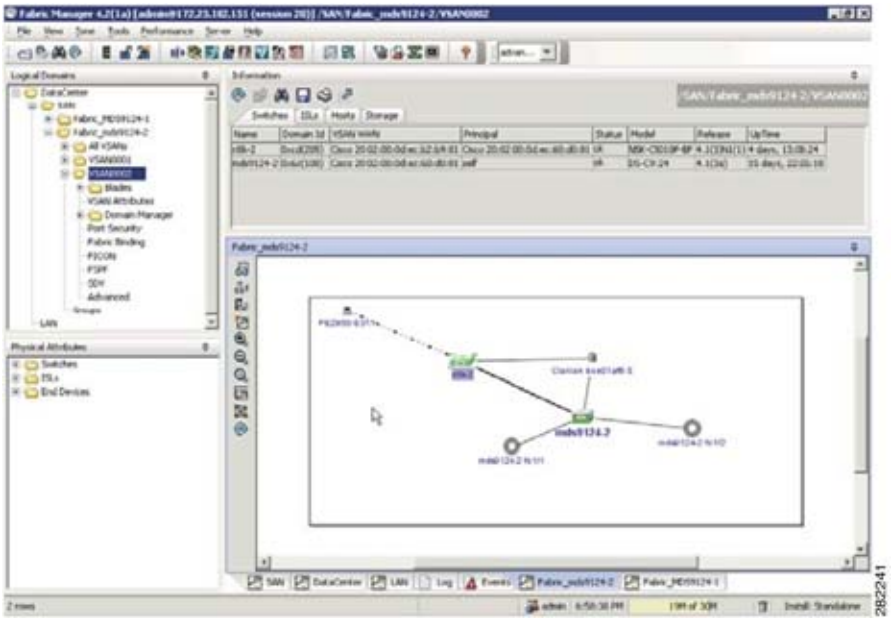
バインド タイプが macAddress に設定されている場合、[Bind MAC Address] カラムでブレード サーバの MAC アドレスを入力できます。この例では、00:c0:dd:04:0c:df が MAC アドレスです。デフォルトでは、VSAN メンバーシップが down および VSAN 1 に設定されています。これらのセクションを編集して、たとえば、VSAN 2 および up にすることができます。

ステップ 6　[Apply] をクリックして変更をコミットしてから、[Refresh] をクリックして vFC が稼働していることを検証します。

図 5-7　Device Manager で設定済みの vFC の MAC アドレス

これにより、Cisco Nexus 5000 シリーズ スイッチにアップリンクした Cisco Nexus 4000 シリーズ スイッチの FCoE 設定が完了します。ゾーン分割、LUN マスキングなどのファブリック管理は、既存の SAN 管理者ツールを使用して管理されます。vFC は標準 FC デバイスとして Fabric Manager に表示されますが、ホストへの実線ではなく、Cisco Nexus 5000 シリーズ スイッチからホストへの破線が表示されます。

図 5-8　FCoE デバイスを含む Fabric Manager ビュー



CHAPTER 6

FCoE NPV の使用

この章では、Cisco Nexus 5000 シリーズ デバイスで Fiber Channel over Ethernet（FCoE）の N ポート バーチャライゼーション（NPV）を設定する方法について説明します。

この章の内容は、次のとおりです。

FCoE NPV について

Cisco NX-OS Release 5.0(3)N2(1) 以降では、Cisco Nexus 5000 シリーズ デバイスで FCoE NPV がサポートされます。FCoE NPV 機能は、FCoE Initialization Protocol（FIP）スヌーピングの拡張版であり、FCoE 対応ホストから FCoE 対応 FCoE フォワーダ（FCF）デバイスに安全に接続する方法を提供します。FCoE NPV 機能には次の利点があります。

- FCoE NPV には、FCF でのホストのリモート管理に付随する管理上およびトラブルシューティング上の問題がありません。
- FCoE NPV は、トラフィックエンジニアリング、VSAN 管理、管理、およびトラブルシューティングといった NPV の機能を維持しながら、NVP 機能の拡張として FIP スヌーピングを実装します。
- FCoE NPV と NPV を共に使用することで、FC と FCoE ポートを介した通信を同時に行えるようになるため、FC から FCoE トポロジに移動する際に、スムーズに移行できます。

FCoE NPV ライセンス

FCoE NPV をイネーブルにするには、次のいずれかの方法を選択します。

- FCoE をイネーブルにしてから NPV をイネーブルにする：この方法では、**feature fcoe** コマンドを使用して FCoE をイネーブルにしてから、**feature npv** コマンドを使用して NPV をイネーブルにする必要があります。FCoE がイネーブルになったときのデフォルトの動作モードは、FC スイッ

チングです。NPV をイネーブルにすると、モードは NPV モードに変わります。NPV モードへの切り替えにより、自動的に書き込み消去が行われ、システムがリロードされます。リロードされると、システムは NPV モードで稼働します。NPV モードを終了し、FC スイッチング モードに戻るには、**no feature npv** コマンドを入力します。NPV モードを終了すると、書き込み消去とデバイス リロードもトリガーされます。この方法には、ストレージ プロトコル サービス パッケージ（FC_FEATURES_PKG）ライセンスが必要です。

- FCoE NPV をイネーブルにする：**feature fcoe-npv** コマンドを使用して FCoE NPV をイネーブルにすると、モードが NPV に変わります。この方法を使用すると、書き込み消去とリロードは行われません。この方法では、ライセンス パッケージ（FCOE_NPV_PKG）が別途必要です。このライセンスも、ストレージ プロトコル サービス ライセンスに含まれています。

VNP ポート

FCoE NPV ブリッジから FCF への接続は、ポイントツーポイント リンク上でのみサポートされます。これらのリンクは、個々のイーサネット インターフェイスまたはポート チャネル インターフェイスになります。イーサネット インターフェイスに接続された FCF ごとに、vFC インターフェイスを作成し、バインドする必要があります。これらの vFC インターフェイスは、VNP ポートとして設定する必要があります。

VNP ポートでは、FCoE NPV ブリッジが、それぞれ固有の eNode MAC アドレスが付いた複数の eNode を持つ FCoE 対応ホストをエミュレートします。デフォルトでは、VNP ポートはトランク モードでイネーブルになります。

VNP ポートには、複数の VSAN を設定できます。VNP ポート VSAN に対応する FCoE VLAN を、バインドしたイーサネット インターフェイスに設定する必要があります。

（注） Cisco Nexus 5000 シリーズ デバイスの VNP ポートは、それぞれ固有の Fabric Provided MAC-Addresses（FPMA）が付いた複数のイーサネット ノードを持つ FCoE 対応ホストをエミュレートします。

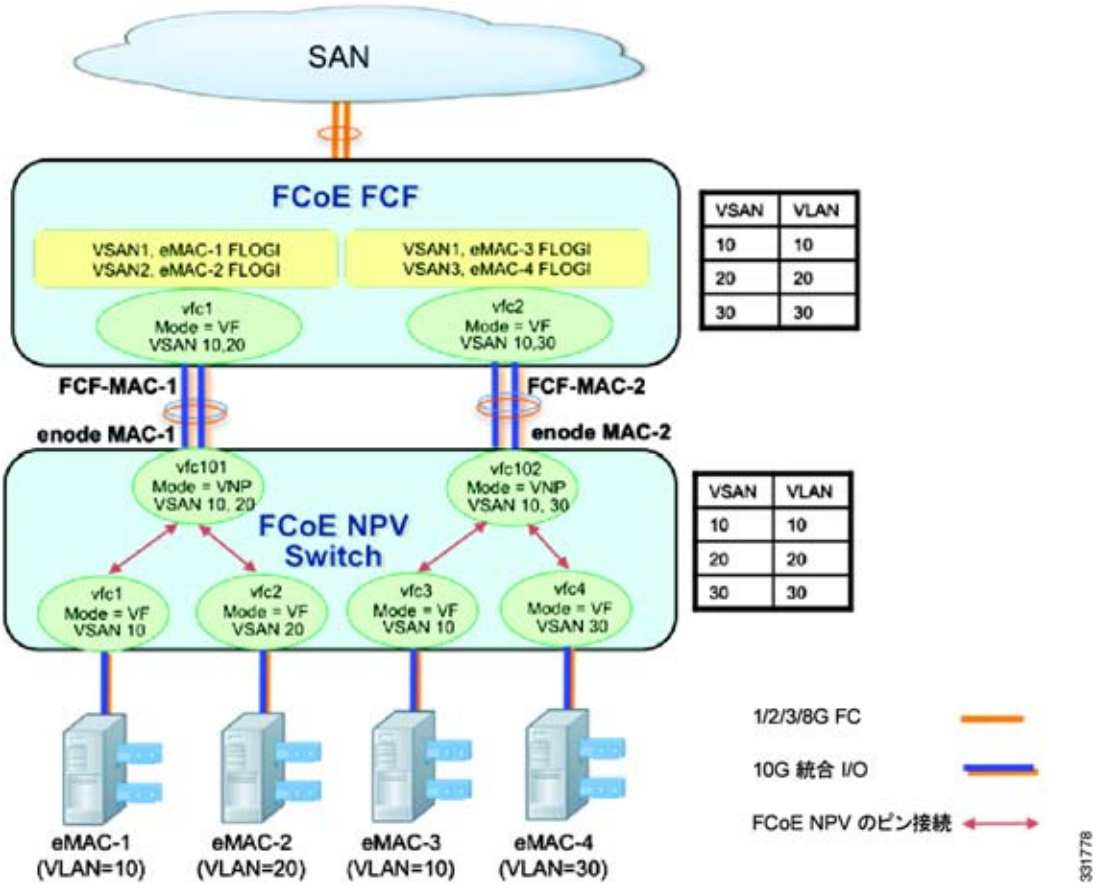
FCoE NPV の設定

図 6-1 にあるように、FCoE-NPV デバイスは、統合型ネットワーク アダプタ（CNA）と FCoE FCF デバイス間の FIP 制御メッセージおよびファブリック ログイン（FLOGI）をプロキシしています。FIP スヌーピング ブリッジとは異なり、FCoE NPV は VSAN を認識し、CNA から FCF アップリンクへのログインをマッピング（またはピン接続）するときに VSAN を考慮します。イニシエータ（eNode）からの FLOGI については、FCoE NPV および FCF デバイスに接続する各ポート チャネル インターフェイス（VNP）からなる 2 つのリンク間でロードバランスが行われます。

（注） Cisco Nexus 5000 シリーズ デバイスでは、FCoE NPV 機能によって FLOGI は FDISC に変換されません。

（注） VNP、VF、および VE の各インターフェイスにバインドされているイーサネット インターフェイス上の FCoE VLAN に対しては、スパニングツリー プロトコル（STP）がディセーブルになります。

図 6-1　FCoE NPV のピン接続、VSAN に基づいた FLOGI



FCoE NPV デバイスでは、サーバ側のポートにバインドされた VFC インターフェイスは VF モードで設定され、FCoE FCF 側の VFC インターフェイスは VNP ポートとして設定されます。次の設定例では、FCoE NPV デバイスが FCOE_NPV_PKG ライセンスを使用して FCoE NPV 機能をイネーブルにしています。VNP ポートですべての VSAN を許可する代わりに、特定の VSAN リストを選択して許可することをお勧めします。

```
switch(config)# feature fcoe-npv
switch(config)# vsan database
switch(config-vsan-db)# vsan 1-2
switch(config)# vlan 10
switch(config-vlan)# fcoe vsan 1
switch(config)# vlan 20
switch(config-vlan)# fcoe vsan 2
switch(config)# interface eth1/1
switch(config-if)# switchport mode trunk
switch(config)# interface Eth1/2
switch(config-if)# switchport mode trunk
switch(config)# interface vfc1
switch(config-if)# bind interface eth1/1
switch(config-if)# switchport trunk allowed vsan 1
switch(config-if)# no shut
switch(config)# interface vfc2
switch(config-if)# bind interface eth1/2
switch(config-if)# switchport trunk allowed vsan 2
switch(config-if)# no shut
switch(config)# interface vfc101
```

```
switch(config-if)# switchport trunk allowed vsan 10
switch(config-if)# switchport trunk allowed vsan add 20
switch(config-if)# no shut
switch(config)# vsan database
switch(config-vsan-db)# vsan 1 interface vfc1, vfc101
switch(config-vsan-db)# vsan 2 interface vfc2
```

QoS 要件

Cisco Nexus 5500 プラットフォーム デバイスの場合、すべてのタイプの QoS ポリシーマップで class-fcoe を設定する必要があります。

次に、すべての QoS ポリシーマップで class-fcoe を設定する例を示します。

```
switch# config t
switch(config)# system qos
switch(config-sys-qos)# service-policy type qos input fcoe-default-in-policy
switch(config-sys-qos)# service-policy type queuing input fcoe-default-in-policy
switch(config-sys-qos)# service-policy type queuing output fcoe-default-out-policy
switch(config-sys-qos)# service-policy type network-qos fcoe-default-nq-policy
```

（注） 前述の QoS の設定は、Cisco NX-OS Release 5.0(3)N2(1) またはそれ以前のリリースを実行する Cisco Nexus 5548 および Cisco Nexus 5596 プラットフォームでは必須です。NX-OS Release 5.1(3)N1(1) より、この設定は、FCoE トラフィックに対するユーザ定義のカスタム ポリシーがすでに存在している場合を除いて自動的に適用されます。ユーザ定義のポリシーがすでに設定されている場合、デフォルトの QOS ポリシーは適用されません。

FCoE NPV の機能

FiberChannel NPV 機能は次のとおりです。

- 自動トラフィック マッピング
- スタティック トラフィック マッピング
- ディスラプティブ ロード バランシング
- FCoE NPV ブリッジでの FCoE 転送
- VNP ポートを介して受信された CoE フレームは、L2_DA が、VF ポートでホストに割り当てられている FCoE MAC アドレスのいずれかに一致する場合にのみ転送されます。それ以外の場合、これらのフレームは破棄されます。

（注） ポート チャネルの VNP ポートを介した FCoE NPV では、FIP ネゴシエーションにのみ自動トラフィック マッピングが使用されます。ポート チャネルの VNP ポートを介した FCoE トラフィック分散は、計算されたハッシュ値に基づきます。

FCoE 対応デバイスとの相互運用性

Cisco NX-OS Release 5.0(3)N2(1) 以降、Cisco Nexus 5000 シリーズ デバイスは次の FCoE 対応デバイスと相互運用します。

- FCF 機能（FCoE NPV および VE）の実行がイネーブルな Cisco MDS 9000 シリーズ マルチレイヤ デバイス。
- FCF 機能（FCoE NPV および VE）の実行がイネーブルな Cisco Nexus 7000 シリーズ デバイス。

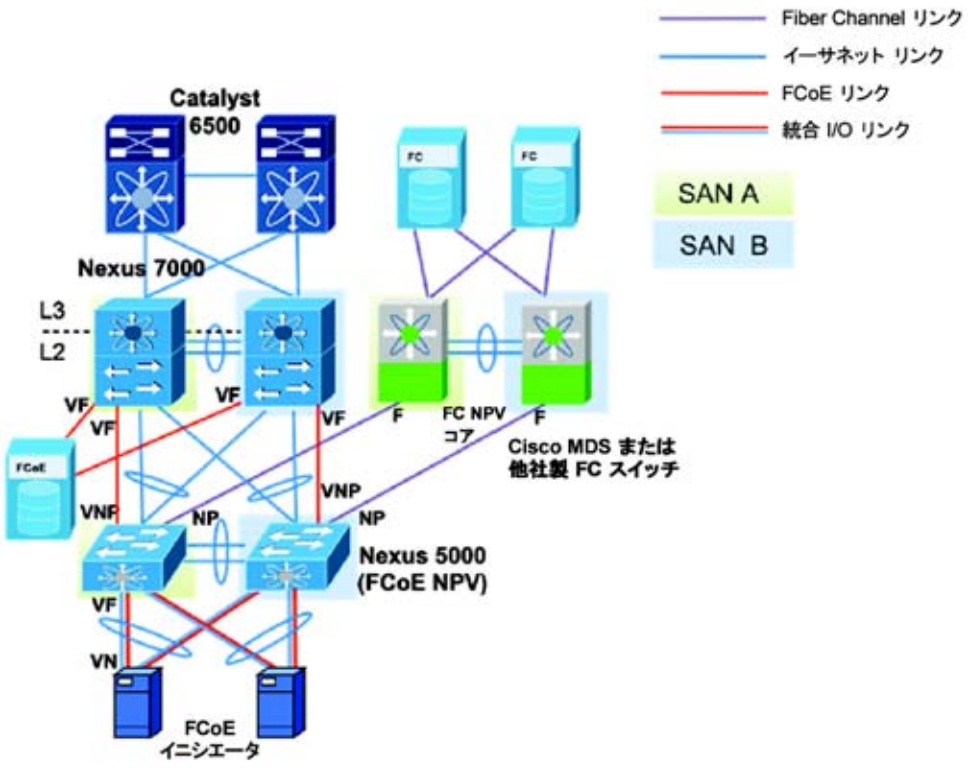
- FIP スヌーピングがイネーブルな Cisco Nexus 4000 シリーズ デバイス。

Cisco Nexus 5000、Cisco Nexus 7000、および Cisco MDS 9500 デバイスを使用したネットワーク設計

Cisco NX-OS Release 5.2 以降、Cisco Nexus 7000 シリーズ サーバでは、32 ポート 10G SFP+ F1 ラインカードで FCoE 機能がサポートされます。Cisco NX-OS Release 5.2 以降、Cisco MDS 9500 マルチレイヤ ディレクタでは、10 Gbps 8 ポートの FCoE モジュールで FCoE がサポートされます。SAN の設計要件に基づいて、Cisco Nexus 7000 シリーズ、Cisco Nexus 5000 シリーズ、および Cisco MDS 9000 シリーズ デバイスの組み合わせを使用して、単一ホップ、マルチホップ、またはマルチプル ティアの FCoE ネットワークを設計できます。

図 6-2 は、Cisco Nexus 7000 シリーズ、Cisco Nexus 5000 シリーズ、および Cisco MDS 9000 シリーズ デバイスを使用した、推奨されるマルチプル ティアの FCoE 設計トポロジを示しています。Cisco Nexus 5000 シリーズ デバイスは、FCoE NPV および FC NPV を同時に実行でき、既存の SAN ネットワークとの接続性を維持しながら、サーバと CNA の接続性を FCF デバイスに提供します。

図 6-2　FCoE NPV を使用したマルチホップの統合化 FCoE ネットワーク設計



ETS に対するカスタム QoS の設定

デフォルトで、Cisco Nexus 5000 シリーズ、Cisco Nexus 7000 シリーズ、および Cisco MDS 9000 シリーズ デバイスは FCoE トラフィックに CoS 値 3 を使用します。FCoE が Cisco Nexus 5000 シリーズ デバイスでイネーブルである場合、CoS 3 は no-drop サービス（PFC 設定）に対して自動的に設定され、輻輳が生じると（ETS 設定）、保証帯域幅の 50 パーセントが FCoE トラフィックに割り当てられます。

FCoE の no-drop トラフィック クラスに対する Cisco Nexus 7000 シリーズ デバイスおよび Cisco MDS 9000 シリーズ デバイスのデフォルト ETS 設定は、70 パーセントです。

Cisco Nexus 7000 シリーズ デバイスで FCoE トラフィックに QoS を設定するには、次のコマンドが必要です。

```
N7K-1# configure terminal
N7K-1(config)# system qos
N7K-1(config-sys-qos)# service-policy type network-qos default-nq-7e-policy
```

（注）　Cisco Nexus 7000 シリーズ、Cisco Nexus 5000 シリーズ、および Cisco MDS 9000 シリーズ デバイスの場合、FCoE トラフィックに対するデフォルトの CoS 値 3 を維持しながら、同じエンドツーエンドの保証帯域幅がこの FCoE no-drop クラスに割り当てられていることを確認します。

統合リンクと専用リンクの使用

FCoE の統合リンクと専用リンクのコストと利点の兼ね合いについては、「FCoE の統合リンクおよび専用リンク」の項に説明があります。この項では、Cisco Nexus 7000 シリーズおよび Cisco MDS 9000 シリーズ デバイスを使用して FCoE ネットワークを設計するときに考慮すべき設計上の考慮事項とリンク タイプの選択について取り上げています。

FCoE リンクはストレージ仮想デバイス コンテンツ（VDC）の一部であり、イーサネット VDC の一部ではないため、専用リンクを使用して、Cisco Nexus 7000 シリーズと Cisco Nexus 5000 シリーズ デバイスの間の FCoE トラフィックを伝送することをお勧めします。Cisco Nexus 7000 シリーズ デバイスのストレージ VDC にアクセスする統合リンクは、このリンク上を伝送されるイーサネット トラフィックをドロップします。同様に、Cisco Nexus 7000 シリーズ デバイスでイーサネット VDC の一部として設定されている統合リンクは、そのリンク上で伝送されるすべての FCoE トラフィックをドロップします。イーサネットおよび FCoE トラフィックに専用リンクを使用するネットワーク設計では、LAN と SAN の両ネットワークのハイ アベイラビリティ機能を使用します。

Cisco MDS 9000 シリーズ デバイスはイーサネット トラフィックのスイッチングをサポートしていないため、Cisco Nexus 5000 シリーズおよび Cisco MDS 9000 シリーズ デバイスを接続するインターフェイスにイーサネット VLAN がマップされないようにすることをお勧めします。イーサネット LAN トラフィックを Cisco MDS 9000 シリーズ デバイスに誘導すると、トラフィックのブラック ホールが生じ、トラフィックが失われる可能性があります。

Cisco Nexus 7000 シリーズ デバイス用のストレージ VDC

VDC は Cisco Nexus 7000 シリーズ デバイスで使用できるため、デバイス レベルで仮想化を行うことができ、そこで論理エンティティを作成してプロセスの分離と耐障害性を実現できます。FCoE については、入力トラフィックがストレージ VDC である別個の VDC で処理されるように、専用リンクを設定できます。

Cisco Nexus 7000 シリーズ デバイスでは、次のようにして FCoE トラフィックのストレージ VDC を作成する必要があります。

```
N7K-1# configure terminal
N7K-1(config)# vdc fcoe_vdc type storage
Note:  Creating VDC, one moment please...
N7K-1(config)# limit-resource module-type f1
N7K-1(config)# allow feature-set fcoe
N7K-1(config-vdc)# allocate interface ethernet 3/1-32
```

ポートを移動すると、ソース VDC でこのポートに関連付けられているすべての設定が削除されます。

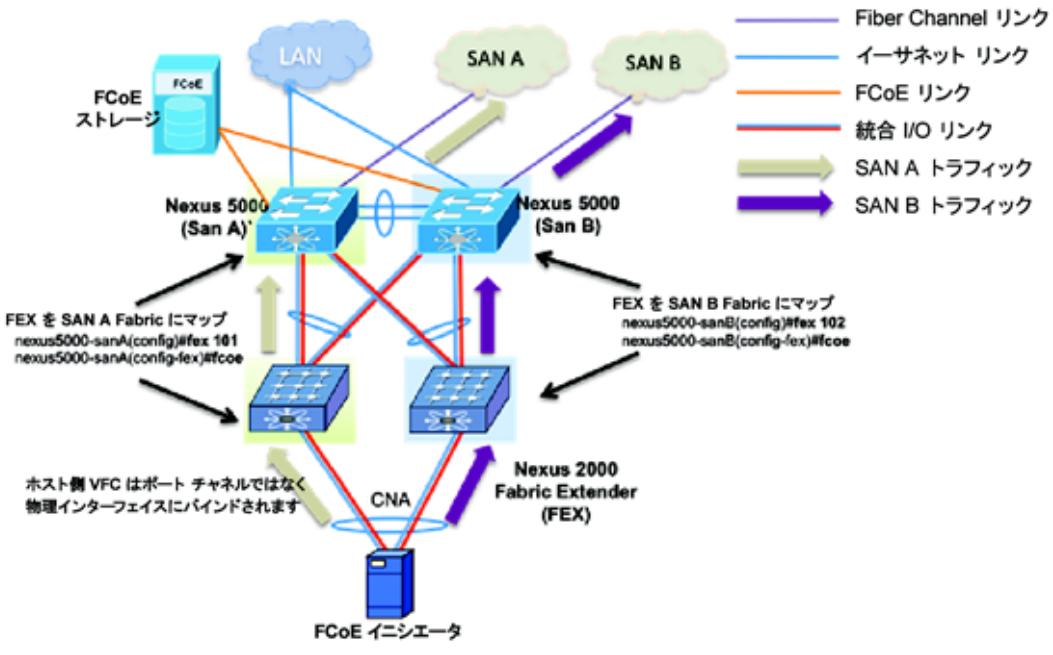
FCoE および拡張 vPC に関する考慮事項

Cisco NX-OS Release 5.1(3)N1(1) 以降、Cisco Nexus 5000 シリーズ デバイスでは拡張 vPC（EVPC）で FCoE がサポートされます。EVPC トポロジでは、SAN ファブリック分離ルールに違反するため、FCoE トラフィックが FEX から複数の Cisco Nexus 5000 シリーズ デバイスに転送されないようにすることが重要です。

この動作は、各 FEX に 1 台の Cisco Nexus 5000 シリーズ デバイスだけを関連付けることによって実装されます。Cisco Nexus 2000 と Cisco Nexus 5000 のペアは、1 つの FCoE SAN ファブリックのみに属します。

図 6-3 に、eVPC レイヤの vPC を使用した FCoE ネットワーク設計を示します。FEX で受信されたサーバ FCoE トラフィックは、関連付けられた Cisco Nexus 5000 シリーズ デバイスにのみ送信されます。FEX の設定に **fcoe** コマンドを使用すると、FEX デバイスが 1 台の Cisco Nexus 5000 シリーズ デバイスに関連付けられます。FCoE トラフィックには 1 つの vPC リンクが使用されるので、SAN A と SAN B の分離を実装しやすくなります。

図 6-3　　eVPC レイヤの vPC を使用した FCoE ネットワーク設計



次に、FEX および Cisco Nexus 5000 シリーズ デバイスを FCoE SAN ファブリックと関連付ける例を示します。

```
nexus5000-sanA(config)# fex 101
nexus5000-sanA(config-fex)# fcoe
nexus5000-sanB(config)# fex 102
nexus5000-sanB(config-fex)# fcoe
```

（注）　FEX に関連付けられたホスト側の VFC リンクを切断し、FCoE トラフィック障害が生じる可能性があるため、同じ FEX を複数の Cisco Nexus 5000 シリーズ デバイスに関連付けないでください。

LACP ベースのホスト vPC を介したイニシエータの SAN ブート

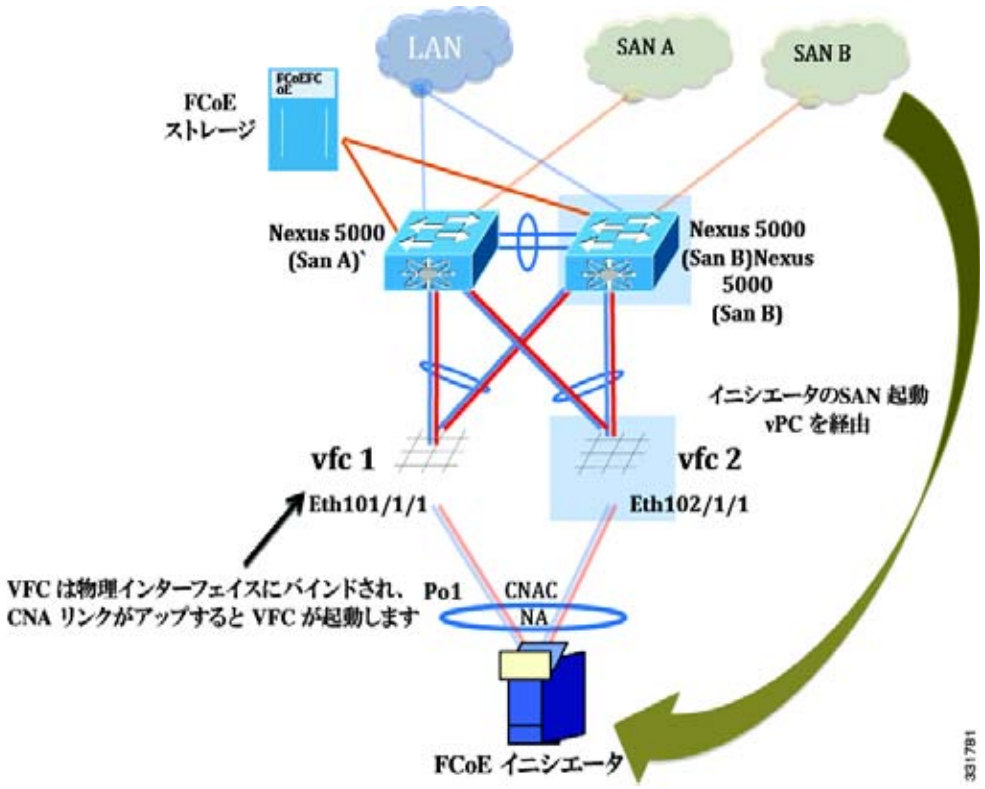
Cisco NX-OS Release 5.1(3)N1(1) 以降、Cisco Nexus 5000 シリーズ デバイスは Link Aggregation Control Protocol（LACP）ベースの vPC でのイニシエータの SAN ブートをサポートします。この制限事項は、LACP ベースのポート チャネルに固有です。ホスト側の VFC インターフェイスは、ポート チャネル自体ではなく、ポート チャネル メンバにバインドされます。このバインディングにより、最初の構成で LACP ベースのポート チャネルに依存することなく、CNA/ホスト バス アダプタ（HBA）のリンクがアップした時点で、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 6-4 は、イニシエータが vPC を介して SAN から起動するように設定されたネットワーク設計を示しています。VFC1 は、ポート チャネル 1 の一部である物理インターフェイス Eth101/1/1 にバインドされています。VFC インターフェイスは、ホスト側の vPC のチャネルメンバ状態がアップになると同時にアップになり、イニシエータが vPC を介して SAN から起動できるようにします。

次に、ホスト側 FEX を設定する例を示します。

```
nexus5000-sanA(config)#fex 101
nexus5000-sanA(config-fex)#fcoe
nexus5000-sanA(config)#interface vfc 1
nexus5000-sanA(config-if)#bind interface eth101/1/1
nexus5000-sanA(config)#interface eth101/1/1
nexus5000-sanA(config-if)#channel-group 1
nexus5000-sanB(config)#fex 102
nexus5000-sanB(config-fex)#fcoe
nexus5000-sanB(config)#interface vfc 1
nexus5000-sanB(config-if)#bind interface eth102/1/1
nexus5000-sanB(config)#interface eth102/1/1
nexus5000-sanB(config-if)#channel-group 1
```

図 6-4　vPC を介して SAN から起動するように発信側が設定されたネットワーク設計



（注）　ホスト vPC 設定への VFC バインディングは、FEX が FEX Straight Through トポロジ（非 EVPC モード）に設定されている場合にのみ許可されます。この機能により、Cisco NX-OS Release 5.1(3)N1(1) よりも前の設定およびサポートされいるすべてのトポロジとの下位互換性が保たれます。

（注）　複数の VFC インターフェイスと複数の vPC メンバをバインドすることはできません。

（注）　ローカル Cisco Nexus 5000 シリーズ デバイスに関連付けられていない FEX にメンバ ポートが存在する場合は、2 レイヤ vPC トポロジのポート チャネルのメンバに VFC をバインドできません。

Adapter-FEX を使用した FCoE 機能

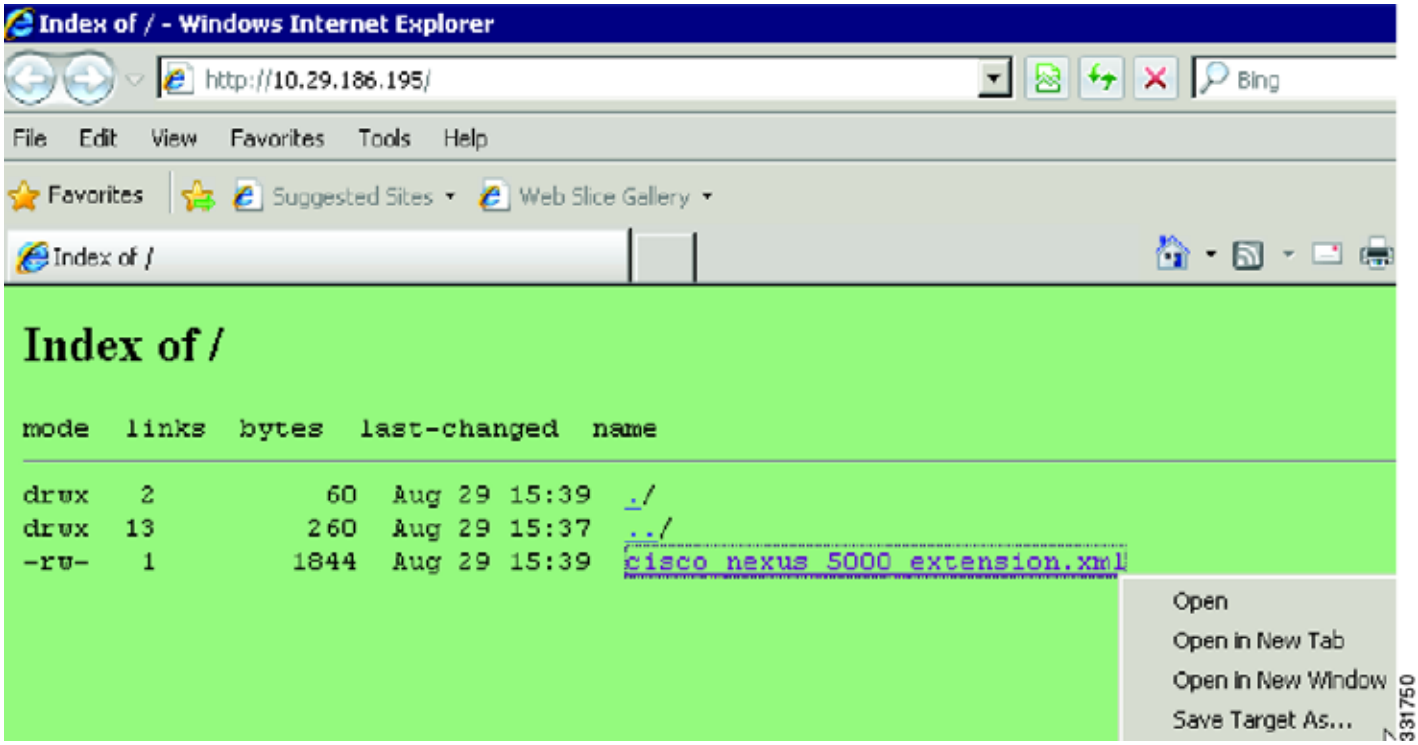
概要

Cisco NXOS 5.1(3)N1(1) 以降、Cisco Nexus 5000 シリーズ デバイスは、P81E アダプタを使用して Cisco UCS サーバに接続している場合、vEthernet インターフェイス上で FCoE をサポートできます。Cisco UCS P81E 仮想インターフェイス カードは、Cisco UCS C シリーズのラックマウント サーバで使用するように設計され、仮想化が最適化された Fibre Channel over Ethernet（FCoE）PCI Express

（PCIe）2.0 x8 10 Gbps アダプタです。Adapter-FEX モードで設定すると、2 つの統合ポートを 2 つの FCoE チャネルに分割できるので、オペレーティング システムに使用できる 4 つの vHBA インターフェイスが作成されます。

図 6-5 は、Adapter-FEX を介した FCoE のトポロジの実装を示しています。Adapter-FEX を介した FCoE ネットワーク設計の場合、Cisco Nexus シリーズ 5000 シリーズと FEX の間に vPC を使用する設定が現在サポートされています。同時に、P81E アダプタのホスト側を Active/Stanby モードに設定する必要があります。FCoE および EVPC トポロジの場合、FEX は FCoE トラフィックの転送に対して 1 つの Cisco Nexus 5000 シリーズ ファブリックに関連付けられます。ホスト HBA は Active/Standby モードに設定されているため、Adapter FEX を介した FcoE のトポロジを実装するには、別個のイーサネットまたは vEthernet から VFC へのマッピングを他の FEX と Cisco Nexus 5000 シリーズ ペアで実行する必要があります。

図 6-5　Adapter-FEX を介した FCoE のトポロジの実装



VFC を vEthernet インターフェイスにバインドするには、Cisco Nexus 5000 シリーズ デバイスで次の設定が必要です。FCoE については、ホスト側で Active/Standby モードを使用して Adapter-FEX を展開できます。

```
nexus5000-sanA(config)# install feature-set virtualization
nexus5000-sanA(config)# feature-set virtualization
nexus5000-sanA(config)# feature vmfex
nexus5000-sanA(config)# interface vfc 1
nexus5000-sanA(config-if)# bind interface veth 1
nexus5000-sanA(config-if)# interface veth 1
nexus5000-sanA(config-if)# bind interface eth101/1/1 channel 3
nexus5000-sanA(config-if)# interface eth101/1/1
nexus5000-sanA(config-if)# switchport mode vntag
nexus5000-sanA(config-if)# fex 101
nexus5000-sanA(config-fex)# fcoe

nexus5000-sanB(config)# interface vfc 2
nexus5000-sanB(config-if)# bind interface veth 2
nexus5000-sanB(config-if)# interface veth 2
```

```
nexus5000-sanB(config-if)# bind interface eth102/1/1 channel 4
nexus5000-sanB(config-if)# interface eth102/1/1
nexus5000-sanB(config-if)# switchport mode vntag
nexus5000-sanB(config-if)# fex 102
nexus5000-sanB(config-fex)# fcoe
```

（注）　仮想マシンの vNIC は、Cisco Nexus 5000 シリーズ デバイスの vEthernet インターフェイスにマッピングされるため、冗長性を保つために設定された 2 台の Cisco Nexus 5000 シリーズ デバイス間では vEthernet インターフェイス番号が固有である必要があります。

（注）　FCoE トラフィックに専用リンクを使用することにより、FCoE および FCoE NPV 機能を FabricPath と共存させることができます。

（注）　VNP ポートを使用して Cisco Nexus 5000 シリーズ デバイスに接続しているときは、Cisco UCS P81E アダプタで NPIV モードはサポートされません。

（注）　Cisco UCS P81E 仮想インターフェイス カードを使用したイニシエータの SAN ブートは、ネットワーク インターフェイスの仮想化機能がイネーブルである場合のみサポートされます。

Cisco Nexus 5000 シリーズ デバイスでの FCoE ポート プロファイルの作成

Cisco Nexus 5000 シリーズ デバイスで vEthernet ポート プロファイルを作成するためおよび vCenter への接続を形成するためには、次の設定が必要です。

ポート プロファイルの設定：

```
nexus5000-sanA(config)# config t
nexus5000-sanA(config)# port-profile type vethernet vnic-fcoe-1
nexus5000-sanA(config)# switchport mode trunk
nexus5000-sanA(config)# switchport trunk allowed vlan 1,100
nexus5000-sanA(config)# state enabled
```

vCenter への SVS 接続：

```
nexus5000-sanA(config)# svs connection vCenter-Nexus5000
nexus5000-sanA(config)# protocol vmware-vim
nexus5000-sanA(config)# remote ip address 172.28.3.19 port 80 vrf management
nexus5000-sanA(config)# dvs-name SJC-LAB
nexus5000-sanA(config)# vmware dvs datacenter-name TME-LAB
nexus5000-sanA(config)# connect
```

（注）　vCenter を使用して SVS 接続を設定すると、Cisco Nexus 5000 シリーズ デバイスで作成されたポート プロファイルが自動的に vCenter にプッシュされます。

Cisco UCS サーバでの vHBA の作成およびポート プロファイルへのバインディング

UCS サーバの Cisco UCS P81E アダプタの Adapter-FEX 機能は、Cisco UCS Manager CLI を使用して設定します。次に、Cisco UCS Manager CLI に接続して、vHBA インターフェイスを作成する例を示します。

```
sjc-xdm-054$ ssh -l admin ucs-afex-02.cisco.com
admin@ucs-afex-02.cisco.com's password:
ucs-afex-02# scope chassis
ucs-afex-02 /chassis # show adapter

PCI Slot Product Name   Serial Number  Product ID     Vendor
-------- -------------- -------------- -------------- --------------------
1        UCS VIC P81E   QCI1532A34U    N2XX-ACPCI01   Cisco Systems Inc
ucs-afex-02 /chassis # scope adapter 1
ucs-afex-02 /chassis/adapter # set niv-mode enabled
ucs-afex-02 /chassis/adapter # create host-fc-if vHBA-P81E-01
ucs-afex-02 /chassis/adapter # set port-profile vnic-fcoe-1
ucs-afex-02 /chassis/adapter/host-fc-if *# set channel-number 7
ucs-afex-02 /chassis/adapter/host-fc-if *# commit
ucs-afex-02 /chassis/adapter/host-fc-if # show detail
Name vHBA-P81E-01:
World Wide Node Name: 10:00:E8:B7:48:4E:0A:A0
    World Wide Port Name: 20:00:E8:B7:48:4E:0A:A0
    FC SAN Boot: disabled
    Persistent LUN Binding: disabled
    Uplink Port: 0
    MAC Address: E8:B7:48:4E:0A:A0
    CoS: N/A
    VLAN: NONE
    Rate Limiting: N/A
    PCIe Device Order: ANY
    EDTOV: 2000
    RATOV: 10000
    Maximum Data Field Size: 2048
    Channel Number: 5
    Port Profile: vnic-fcoe-1
```

（注）　Cisco NX-OS Release OS 5.1(3)N1(1) の Cisco UCS C シリーズ Cisco Integrated Management Controller（CIMC）グラフィカル ユーザ インターフェイス（GUI）を使用した 3 つ以上の vHBA インターフェイスの作成はサポートされていません。

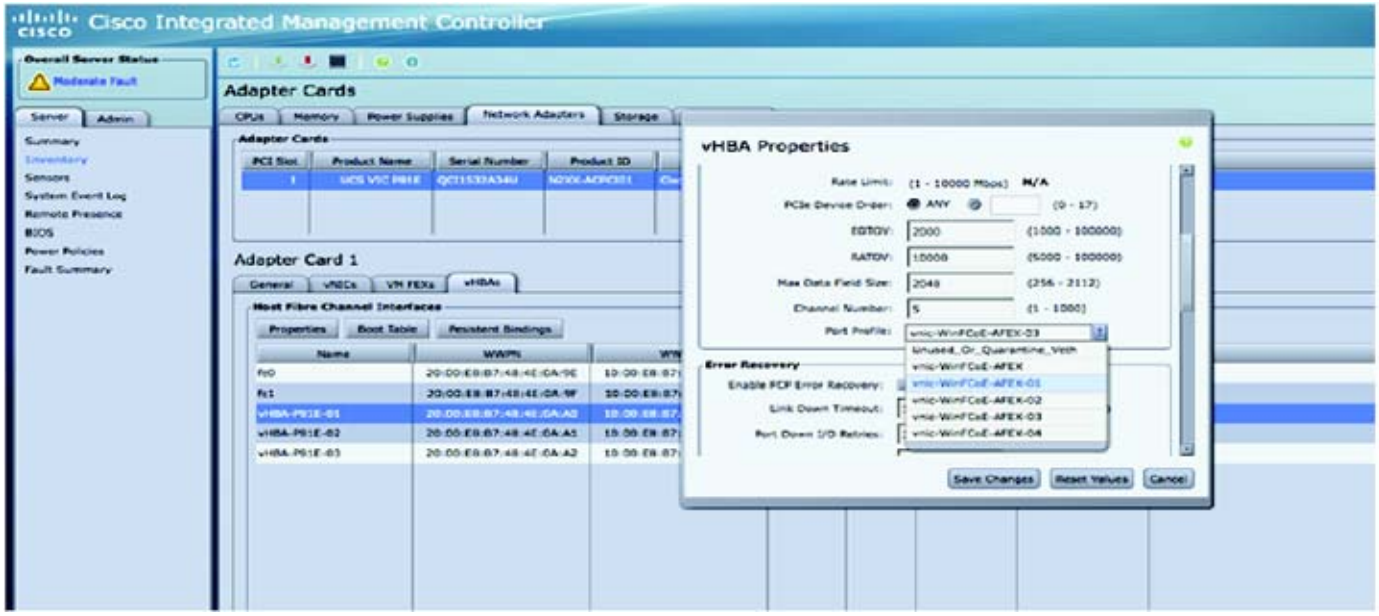
CIMC を使用したポート プロファイルへの vHBA のバインディング

UCS C シリーズ サーバの CLI を使用して作成された仮想 HBA インターフェイスは、CIMC GUI を使用してポート プロファイルにマッピングできます。CIMC は、UCS C シリーズ サーバ用の管理サービスであり、サーバ内で実行されます。CIMC コンポーネントには、Web ブラウザを使用してアクセスできます。

Cisco Nexus 5000 シリーズ デバイスに作成されたポート プロファイルは、VNTag リンクを使用して Cisco UCS P81E アダプタにプッシュされます。VNTag は、アダプタによって送信元と宛先の vNIC を識別するために割り当てられる固有のタグです。ポート プロファイルは、CIMC のドロップダウン メニューに表示されます。

図 6-6 は、CIMC ツールを使用してポート プロファイルを vHBA インターフェイスにマッピングする方法を示しています。

図 6-6　CIMC ツールを使用した vHBA インターフェイスへのポート プロファイルのマッピング



INDEX

C

D

E

F

I

M

N

P

Q

V

あ

い

か

さ

し

す

せ

そ

て

と

ね

は

ふ

ゆ

り

ろ

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/