



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」 (P.1-1)
- 「FCoE の考慮事項」 (P.1-1)
- 「FCoE でサポートされるトポロジ」 (P.1-16)
- 「FCoE の動作」 (P.1-23)
- 「その他の情報」 (P.1-29)

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」 (P.1-2)
- 「FCoE およびスパンニングツリー プロトコルの考慮事項」 (P.1-3)
- 「FCoE および仮想ポート チャネル (vPC) の考慮事項」 (P.1-5)
- 「長距離 FCoE に合わせたバッファ割り当ての変更」 (P.1-9)
- 「FCoE の統合リンクおよび専用リンク」 (P.1-10)
- 「Cisco Nexus 5000 シリーズ スイッチ FCoE の考慮事項」 (P.1-12)
- 「プライオリティ フロー制御と Enhanced Transmission Selection に関する考慮事項」 (P.1-13)
- 「Cisco Nexus の相互運用性」 (P.1-16)

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 レベルのいずれかで HA を使用して実現するのかわかりません。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」(P.1-2)
- 「VLAN から VSAN への番号付け」(P.1-3)

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 0E.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、何といた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、フラッドリングは発生せず、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ッ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」 (P.1-6)
- 「第 2 世代 CNA の要件」 (P.1-6)
- 「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)
- 「vPC での FCoE VLAN 設定」 (P.1-8)

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 チャンネル 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 チャンネル 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 チャンネルを設定し、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 チャンネルで 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

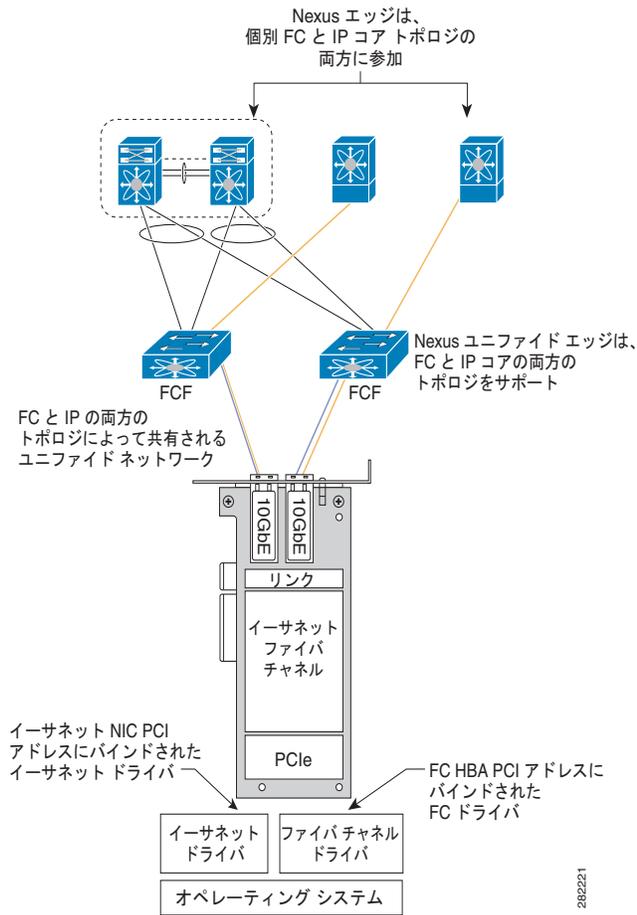
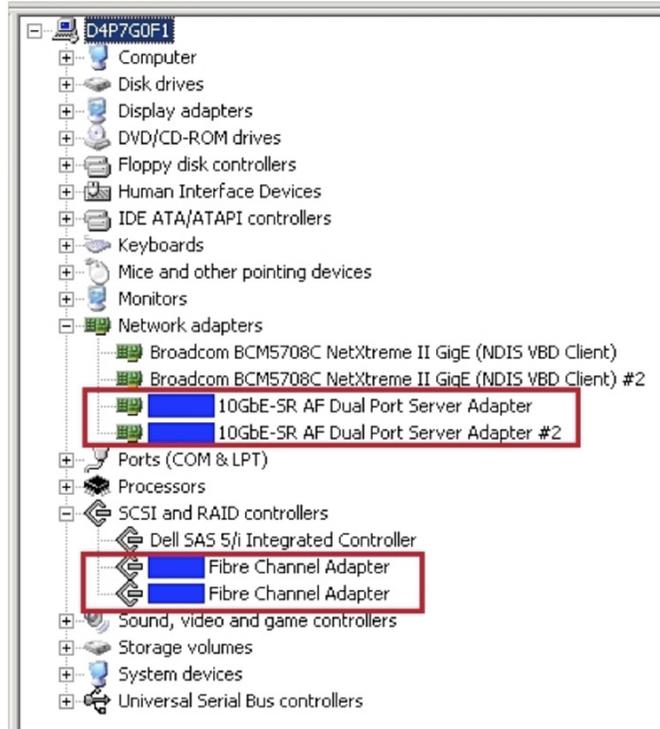


図 1-2 アダプタのコントロール パネル表示



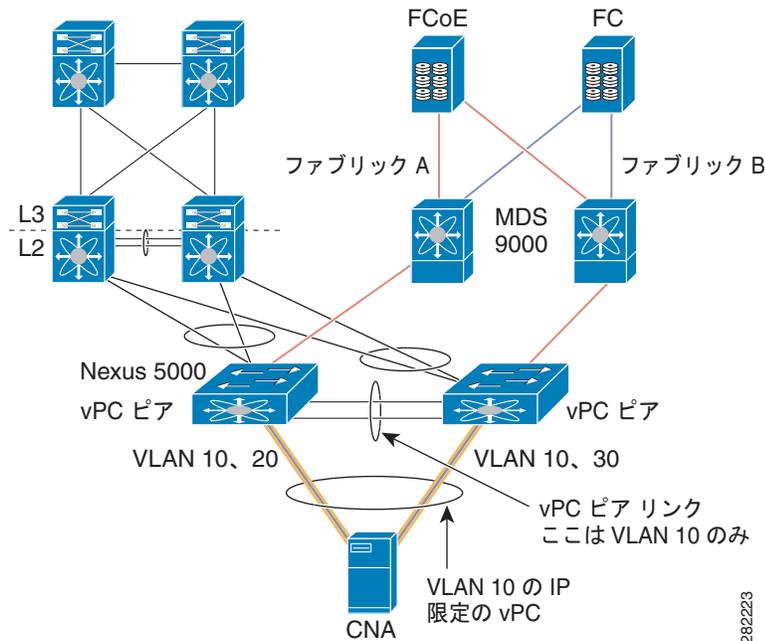
(注)

- 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



262223

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）を送信するように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。

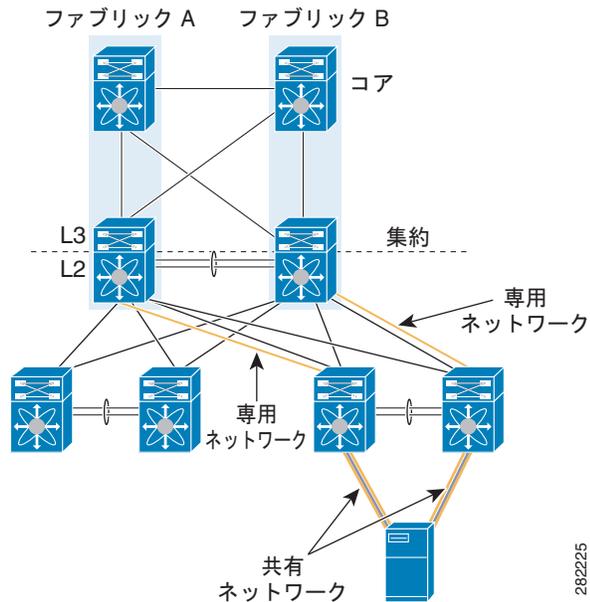
リンク統合は、イーサネット LAN トラフィックおよび SAN ストレージ トラフィックで、ホストとスイッチ間または 2 台のスイッチ間で同じ物理ネットワークを共有している場合を指します。

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 トラフィックの範囲を説明する 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、オーバーサブスクリプト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せん。

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-qos fcoe-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依じて、スイッチまたは拡張モジュールのリポートが必要です。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」 (P.1-14)
- 「PFC および ETS の設定の変更」 (P.1-14)
- 「PFC および ETS の設定を変更するときのホスト側の問題」 (P.1-15)

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せん。

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、中央のスウィ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 スウィッチング 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](#)」 (P.1-16)
- 「[マルチ ホップ FCoE ソリューション](#)」 (P.1-23)

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](#)」 (P.1-16)
- 「[vPC およびアクティブ/スタンバイ](#)」 (P.1-17)
- 「[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](#)」 (P.1-18)
- 「[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](#)」 (P.1-18)
- 「[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](#)」 (P.1-19)
- 「[FIP スヌーピングブリッジ](#)」 (P.1-20)
- 「[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](#)」 (P.1-21)
- 「[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](#)」 (P.1-22)

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 チャンネル 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ポートが必要であり、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、リポ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 チューニング、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

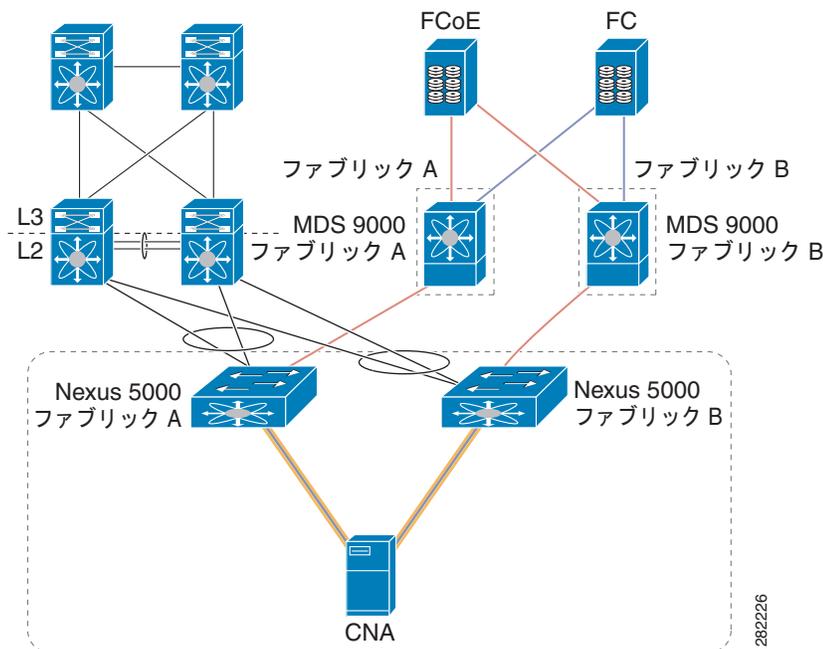
きる、Cisco Nexus 製品で導入されたテクノロジーです。vPC の利点は、アクティブ/スタンバイ設定の倍の帯域幅を持つアクセスをサーバに提供することおよび障害が発生した場合にスパンニングツリーよりも高速なコンバージェンス能力もあることです。

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。

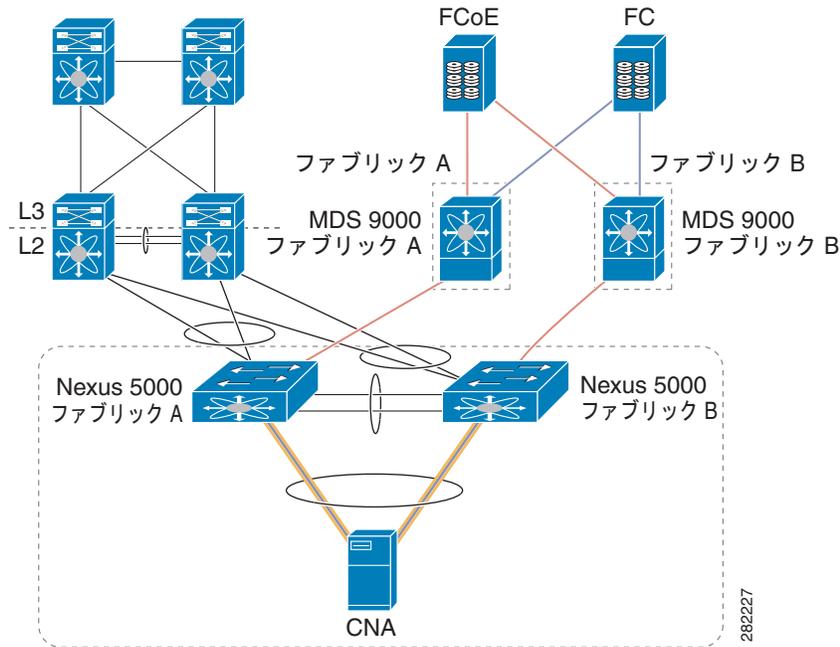
図 1-5 アクティブ/スタンバイ トポロジの 2 台の Cisco Nexus 5000 シリーズのスイッチに接続するデュアルポート CNA



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。

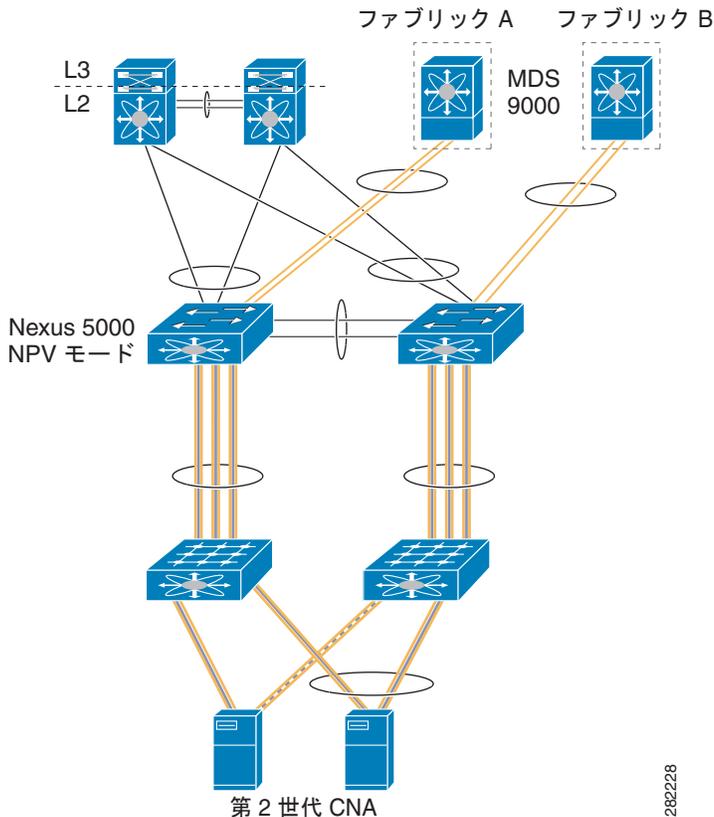
Cisco Nexus 5000 シリーズスイッチと Cisco Nexus 2000 ファブリックエクステンダのトポロジ

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 チャンネル 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。

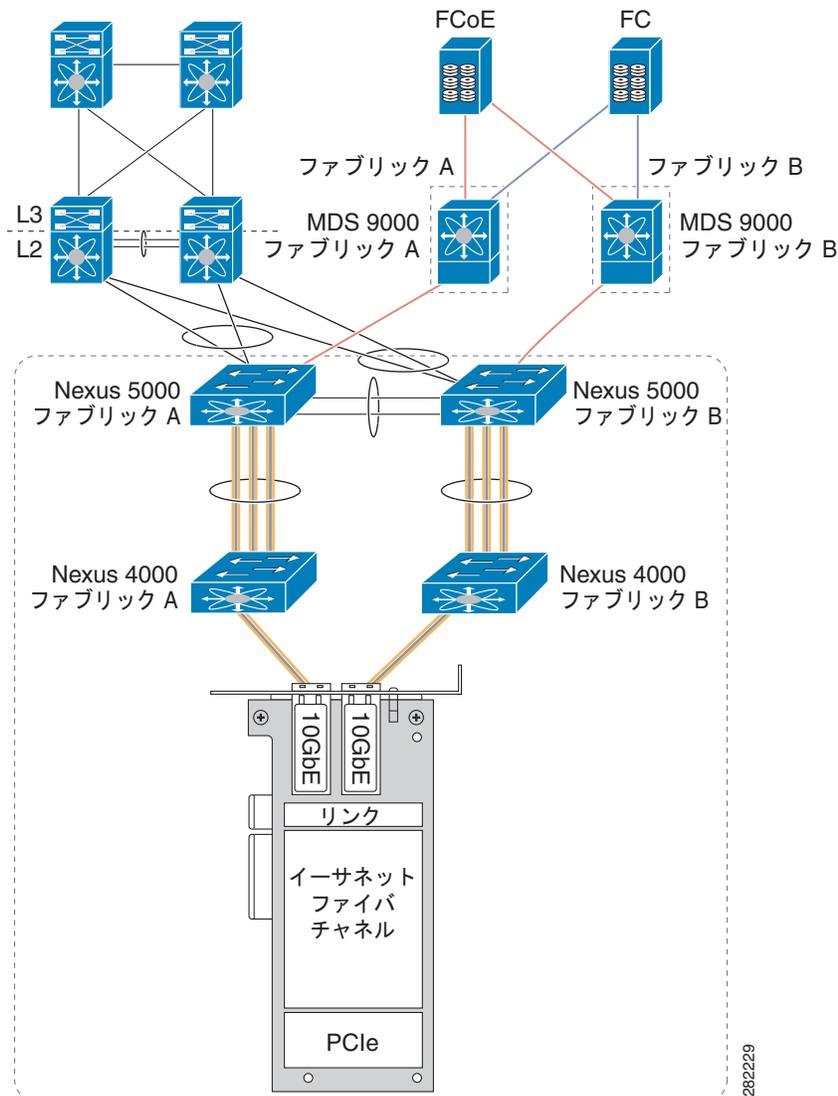
Cisco Nexus 4000 シリーズスイッチは、IBM ブレードシャーシの FIP スヌーピングデバイスであり、通過する FCoE フレームをサポートするには、Cisco Nexus 5000 シリーズ FCF スイッチに接続する必要があります。Cisco Nexus 4000 シリーズスイッチには、14 台のブレードサーバのそれぞれに接続さ

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 FCoE 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

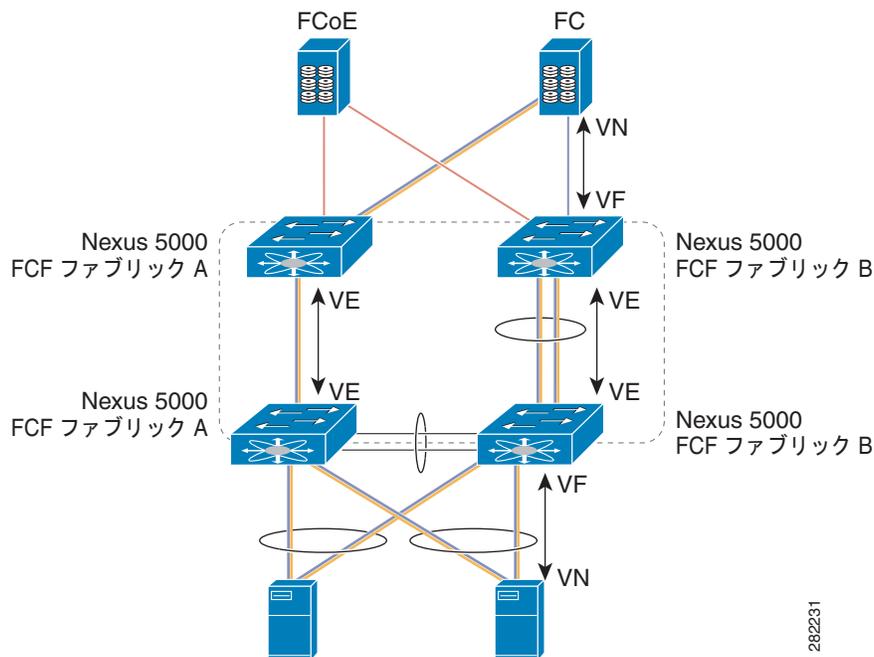


マルチ ホップ FCoE ソリューション

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。

282231

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」 (P.1-24)
- 「FC および FCoE トラフィックの SPAN」 (P.1-25)
- 「ロール ベース アクセス コントロール」 (P.1-26)

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 p:
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 ファミリー 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 ファミリー 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」 (P.1-27)
- 「LAN 管理者ロール」 (P.1-27)
- 「SAN 管理者ロール」 (P.1-27)

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 管理の範囲に入りますが、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が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が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」 (P.1-28)
- 「ホストへの LACP および FCoE」 (P.1-28)
- 「NPIV コアとしての Cisco Nexus 5000 シリーズ スイッチの導入」 (P.1-28)
- 「Cisco Nexus 5010 スイッチまたは Cisco Nexus 5020 スイッチの VE ポート」 (P.1-29)

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

