Cisco ネットワーク管理者のための HP バーチャルコネクトの解説

「HP バーチャルコネクト 1.2x の機能と Cisco ネットワーク インフラストラクチャとの相互運用についての技術説明」

目次

概要

このホワイトペーパーでは、Cisco ネットワークインフラストラクチャとの相互運用性に関連する、バーチャルコネクトイーサネットの背景にあるネットワーキングテクノロジについて説明します。バーチャルコネクト(VC)は HP BladeSystem c-Class サーバブレードを外部ネットワークと相互接続する新しい方法であるため、実装を担当する多くの方から、バーチャルコネクトが既存の Cisco ネットワークインフラストラクチャにどのように統合されるのかについて質問が寄せられています。このホワイトペーパーでは特に、バーチャルコネクトイーサネットで使用されている中核となるイーサネットのネットワーキングテクノロジと、Cisco ネットワークインフラストラクチャと相互運用する方法について説明しています。

免責事項、前提条件、バージョン

このホワイトペーパーの目的は、Cisco のスイッチおよびルータとの相互運用性に特に重点を置いて、バーチャルコネクトのコンポーネントおよび操作について技術的な説明をすることです。本書はバーチャルコネクトの操作および構成のすべての面を包括的に説明するものではなく、またバーチャルコネクトと他社のイーサネットソリューションとを比較分析するものでもありません。

本書では、読者がCiscoの用語および機器の操作に十分習熟しており、HP BladeSystem c-Classエンクロージャ、HP BladeSystem c-Classサーバブレード、およびHP BladeSystemバーチャルコネクトの基礎についての十分な知識があることを前提としています。HP BladeSystem c-Classコンポーネントの詳しい情報については、http://www.hp.com/jp/bladesystemおよびhttp://h50146.www5.hp.com/products/servers/bladesystem/c/component/ic.htmlを参照してください。

事前に以下の文書を読んでおくことをお勧めします。

- 『Non-technical Summary of Virtual Connect Technology』(英語)
- ホワイトペーパー『HP BladeSystem c-Classに実装されている HP Virtual Connect テクノロジ』
- 『Virtual Connect User Guide (version 1.2x)』(英語)

このホワイトペーパーは、バーチャルコネクトのファームウェアバージョン 1.2xまでで提供されている機能に基づいて書かれたものです。新しいファームウェアのリリースでは、新しい機能が導入されていたり、既存の機能の動作方法に対する変更が加えられている場合があります。本書の情報と実際の動作が一致しない場合、管理者はご使用のファームウェアバージョンに合ったバーチャルコネクトのマニュアルおよびリリースノートを参照することをお勧めします。どちらの資料も、http://www.hp.com/go/bladesystem/documentationの「Install Your Solution」タブ(英語)からオンラインで見つけることができます。

はじめに

バーチャルコネクトは HP BladeSystem c-Class のお客様に向けた画期的なネットワーキング製品として、2007 年 2 月から発売されています。バーチャルコネクトはサーバブレードネットワーク接続のより優れた管理方法を求めるお客様の声に直接応えるものとして設計および開発されました。既存の問題を解決する優れた方法をもたらすすべての新製品に共通することですが、管理者にとっては、新製品導入による影響を十分理解し、使用する環境に安心して導入できることが非常に重要です。お客様の環境にバーチャルコネクトを導入することで確実に影響を受けるのは、サーバ管理者だけではなく、LAN 管理者および SAN 管理者も同じです。もっと具体的に言うと、バーチャルコネクトの導入は LAN 管理者にも影響を及ぼすため、バーチャルコネクトとその操作および既存の Cisco ネットワークインフラストラクチャとの相互運用性について十分に検討することがきわめて重要です。

このホワイトペーパーでは、読者は HP BladeSystem c-Class アーキテクチャの基本について十分な知識があることを想定していますが、バーチャルコネクトテクノロジを理解する上で鍵となる重要ないくつかの点について確認します。まず、本書の全体を通して使用される用語を定義した一覧を掲載します。次に、HP BladeSystem c-Class アーキテクチャの中核となるネットワーキングコンポーネントの概要を簡単に説明した後、バーチャルコネクトイーサネットのコンポーネントおよびテクノロジについて掘り下げて説明します。その後の項では、バーチャルコネクトと外部の Cisco インフラストラクチャを接続する際に使用される多くのネットワーク機能について詳しく説明します。

定義

ACL (VACL)	Access Control List (アクセス制御リスト) または VLAN Access Control List (VLAN アクセス制御リスト)の略。ネットワークデバイス間でのネットワークトラフィックの通過を許可または拒否するルールのセット
BPDU	Bridge Protocol Data Unit (ブリッジ プロトコル データ ユニット)の略。同じスパニングツリードメインのスイッチ間で交換されるスパニングツリー構成フレーム
CDP	Cisco Discovery Protocol の略。直接接続された 2 つの Cisco デバイス間でネイバー情報を交換するために使用する Cisco 独自仕様のプロトコル
CX-4	バーチャルコネクトで使用される、10Gbit 銅線イーサネットを使用したネットワーク接続のための業界標準のケーブル接続仕様
外部ネットワーク	VC ドメインの外側のネットワークおよび関連するネットワークデバイス
内部クロスコネクト	水平方向に隣接する 2 つの VC-Enet モジュールを相互接続する見えないポート(エンクロージャのシグナルミッドプレーン内で配線済み)
LACP	Link Aggregation Control Protocol (リンクアグリゲーション制御プロトコル)の略。ポートトランク/チャネルを形成する 2 つのデバイス間で交換する 802.3ad リンクアグリゲーション構成フレーム
LAG	Link Aggregation Group (リンクアグリゲーショングループ)の略。ポートトランク/チャネルグループに対する 802.3ad の用語
LLDP	Link Layer Discovery Protocol の略。CDP に似た機能を提供する IEEE プロトコル
論理パス	単一の物理ポートまたは単一のポートチャネル。どちらも単一の通信パスのことを表す。
LOM	LAN On Motherboard の略。サーバのシステムボートに組み込まれた NIC
ポートトランク(チャネルグループ)	負荷分散の目的で、単一の論理ポートおよび単一の論理パスとして動作する 2 つ以上のポートからなるグループ。802.3ad と EtherChannel はどちらもポートトランク テクノロジ
サービス品質(QoS)	ネットワークトラフィックの分類、優先順位付け、キューイング、マーキングなどに関連して使用される幅広い用語
サーバプロファイル	サーバベイに割り当てられているバーチャルコネクトドメイン内のオブジェクトで、サーバの LAN 接続および SAN 接続の設定を含む(vNet の割り当て、管理対象の MAC アドレスおよび WWN、サーバのブートパラメータ、PXE 構成、およびファイバチャネルのブートパラメータ)
SFP	ホットプラグ対応のモジュール式 1Gbit ポート。着脱可能なモジュールにより、1Gbit の速度での電気的接続および光接続が可能
共有アップリンクセット(SUS)	バーチャルコネクトで使用する用語で、IEEE 802.1Q VLAN トランキングを使用して、1 つまたは複数の VC アップリンクを VLAN トランクとして構成してスイッチに接続すること
スタッキングリンク	同じ VC ドメインにある 2 つの VC ポートを直接接続するリンク
VC	Virtual Connect (バーチャルコネクト)の略。すべてのバーチャルコネクト コンポーネント(イーサネットおよびファイバチャネル モジュール、Virtual Connect Manager)の総称として使用される広義語
VC-Enet	Virtual Connect Ethernet (バーチャルコネクト イーサネット)モジュールの略
VC-FC	Virtual Connect Fibre Channel (バーチャルコネクト ファイバチャネル)モジュールの略
VCM	Virtual Connect Manager (バーチャルコネクトマネージャ)の略。バーチャルコネクトドメインの管理に使用するユーザーインタフェース(Web または CLI)
バーチャルコネクトドメイン	同じエンクロージャ内にあって同じ Virtual Connect Manager によって制御される、すべての VC-FC モジュールと、スタックされたすべての VC-Enet モジュール
バーチャルコネクトネットワーク(vNet)	単一のレイヤ 2 ネットワークまたはブロードキャストドメインで構成される、VC ポートの論理グループ(ダウンリンクどうし、またはダウンリンクとアップリンク)。

VC ダウンリンク	エンクロージャのミッドプレーンを経由してサーバの NIC ポートに直接接続される、外からは見えないポート。
VCEM	Virtual Connect Enterprise Manager の略。単一コンソールからの管理機能を 100 個の VC ドメインに拡張した、単独のソフトウェア製品。
VC アップリンク	エンクロージャに外部接続を提供する、VC-Enet モジュールの表面上に見えるポート
VLAN トランク	VLAN タギングが有効に設定された、単一の物理ポートまたは単一のポートチャネル。同じ論理パス上で 1 つまたは複数の VLAN に接続性を提供するために使用する。
XFP	ホットプラグ対応のモジュール式 10Gbit ポート。着脱可能なモジュールにより、10Gbit の速度での電気的接続および光接続が可能

HP BladeSystem アーキテクチャの概要

HP BladeSystem c-Class システムは、エンクロージャ、サーバブレード、ストレージブレード、PCI 拡張ブレード、インターコネクトモジュール(スイッチ、バーチャルコネクト、およびパススルーモジュール)、ブレードをインターコネクトモジュールに接続する NonStop シグナルミッドプレーン、共有電源バックプレーン、パワーサプライ、ファン、前面の LCD 画面(Insight Display)、およびエンクロージャ管理コントローラ(Onboard Administrator モジュール)で構成されています。BladeSystem c-Class では、エンクロージャの稼働時間を最大化するために、リダンダントでホットプラグ対応のコンポーネントを多数使用しています。図 1 は、c7000 エンクロージャでのアーキテクチャの実装を示しています。

HP BladeSystem のアーキテクチャでは、c7000 および c3000 の 2 つのエンクロージャフォームファクタが利用できます。HP BladeSystem c7000 エンクロージャには、ハーフハイトサーバまたは他のデバイスブレードが最大 16 台、フルハイトサーバブレードが最大 8 台、または 2 つのブレードフォームファクタの組み合わせを収容できます。また c7000 には背面にインターコネクトモジュール用のベイが 8 つあります。HP BladeSystem c3000 エンクロージャには、ハーフハイトサーバまたは他のデバイスブレードが最大 8 台、フルハイトサーバブレードが最大 4 台、または 2 つのブレードフォームファクタの組み合わせを収容できます。また c3000 には背面にインターコネクトモジュール用のベイが 4 つあります。

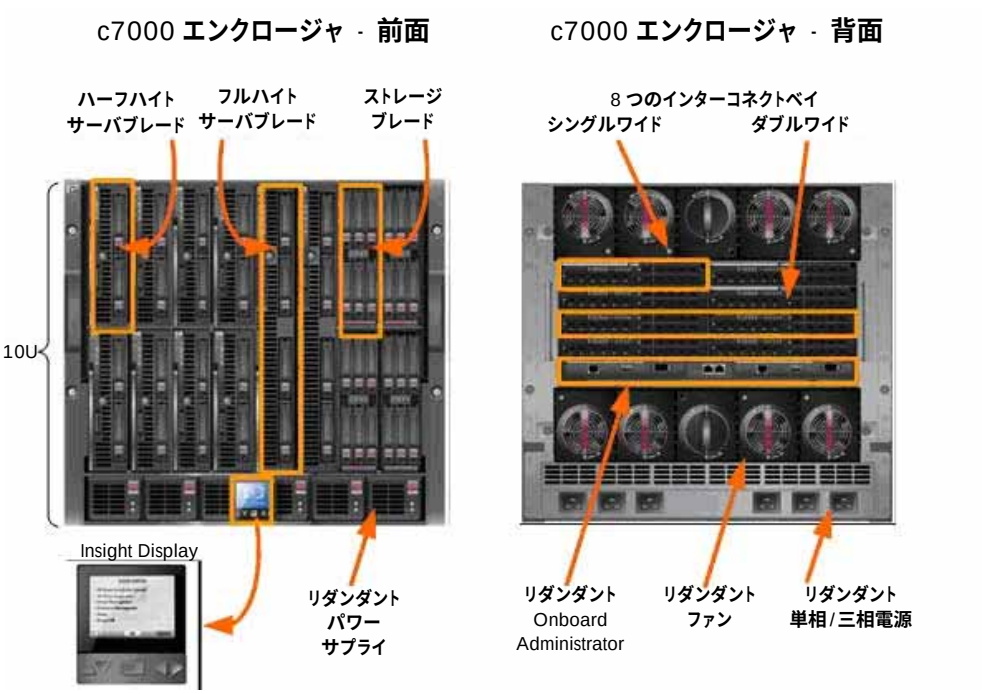
サーバブレード内のオプションのメザニンカードによって、インターコネクトモジュールのネットワーク接続が可能になります。サーバブレードとネットワークファブリックとの間の接続は、完全にリダンダントにすることができます。お客様は必要なメザニンカードを選んでブレード内部のメザニンスロットに装着し、エンクロージャ背面のインターコネクトベイにインターコネクトモジュールを設置して、ネットワークファブリック接続を構築することができます。メザニンカードのオプションには、イーサネット、ファイバチャネル、および Infiniband が含まれます。ただし、ファイバチャネルと Infiniband は本書では扱いません。

エンクロージャは 1 つまたは 2 つの Onboard Administrator モジュールを格納します。Onboard Administrator の提供するエンクロージャベースの管理機能とインテリジェンスにより、消費電力と温度状態の監視、正しいハードウェア構成、ネットワーク構成の簡素化が、インフラストラクチャ全体を通じて可能になります。エンクロージャ前面にある Insight Display パネルにより、構成と管理が容易に行えます。2 つ目の Onboard Administrator モジュールを取り付けて、このモジュールをアクティブスタンバイモードで完全なリダンダントコントローラとして機能させることもできます。

c7000 エンクロージャは単相または三相のいずれかの電源入力を使用でき、最大 6 台(1 台あたり 2250W)のパワーサプライを搭載できます。パワーサプライはパッシブな電源バックプレーンに接続して、そこから電力を共有方式ですべてのコンポーネントに分配します。

エンクロージャを冷却するために、HP はアクティブ冷却ファンというファンを設計しました。c7000 エンクロージャは、最大 10 個までのホットプラグ対応アクティブ冷却ファンを搭載できます。アクティブ冷却ファンは、エンクロージャ全体にリダンダントな冷却を提供するために効率よく高い性能を発揮するように設計されており、将来の冷却ニーズにも十分に対応可能です。

図 1. c7000 エンクロージャコンポーネントの概観



c-Classケーブル接続レイアウト

c-Class サーバブレードは各種メザニンカードを使用して、エンクロージャ背面のインターコネクトベイ経由で各種ネットワークファブリックに接続します。これらのファブリックには、イーサネット、ファイバチャネル、Infiniband などがあります。メザニンカードはサーバブレードのメザニンスロットに挿入します。これらのメザニンスロット(図 2 の M1、M2、および M3)は基本的に、タワー型サーバおよびラックマウント型サーバなどの非ブレード型のハードウェアに見られるものと同じ PCI-e 拡張スロットです。サーバブレードにある複数の種類のメザニンカードは、NonStop シグナルミッドプレーンを経由して、エンクロージャ背面の特定のインターコネクトベイに配線されています(図 2 を参照)。

すべての c-Class サーバブレードには、少なくとも 2 つのオンボード(LOM)の NIC ポートがあります。これらの LOM ポートは、ハーフハイトサーバでは 2 つ (NIC 1 および NIC 2)、フルハイトサーバでは 4 つ(NIC 1 から NIC4)あり、インターコネクト 1 および 2 に接続されています(図 2 を参照)。現在のところ、インターコネクト 1 および 2 に接続されているネットワークファブリックの種類はイーサネット LOM ポートだけであるため、ベイ 1 および 2 に使用できるインターコネクトモジュールの種類はイーサネットモジュール(スイッチ、パススルー、またはバーチャルコネクト)だけです。

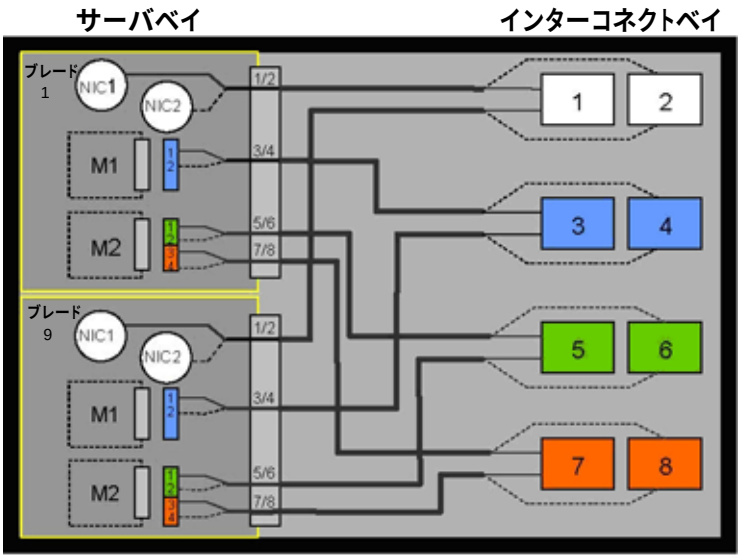
ハーフハイトサーバの場合、メザニンスロット 1 (M1)にはインターコネクトベイ 3 および 4 に接続する最大 2 つのイーサネットポートがあります。メザニンスロット 2 (M2)にはインターコネクトベイ 5 から 8 に接続する最大 4 つのイーサネットポートがあります。ハーフハイトサーバの最大の構成は、すべてイーサネットを使用する場合、NIC は合計 8 つで、それぞれの NIC ポートが 8 つのインターコネクトベイに対して1つずつ接続されます。

フルハイトサーバの場合、メザニンスロット 1 (M1)にはインターコネクトベイ 3 および 4 に接続する最大 4 つのイーサネットポートがあります。メザニンスロット 2 (M2)にはインターコネクトベイ 5 から 8 に接続する最大 4 つのイーサネットポートがあります。またメザニンスロット 3 (M3) にも、インターコネクトベイ 5 から 8 に接続する最大 4 つのイーサネットポートがあります。フルハイトサーバの最大の構成は、すべてイーサネットを使用する場合、NIC は合計 16 で、8 つのインターコネクトベイにそれぞれ 2 つの NIC ポートが接続されます。

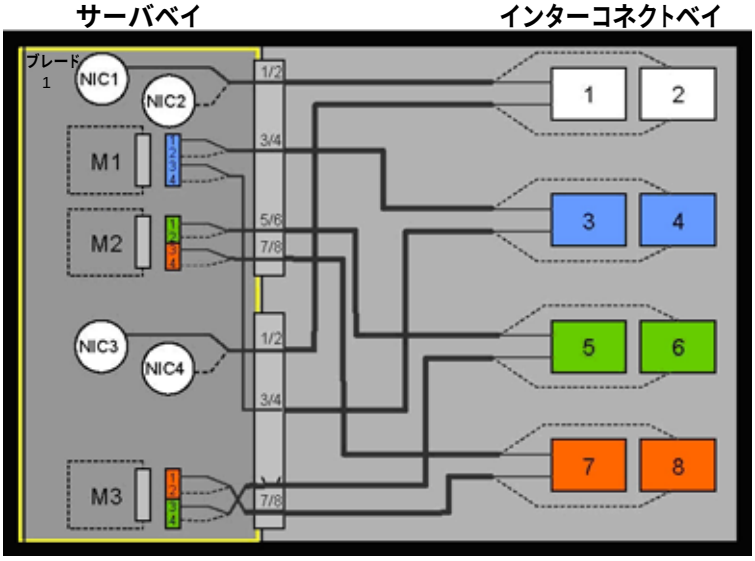
メザニンスロットはイーサネット以外の I/O テクノロジ(ファイバチャネルまたは InfiniBand など)も実装できますが、本書ではイーサネットを中心に扱います。

図 2. ハーフハイトおよびフルハイトのサーバブレードでのインターコネクトベイへの I/O マップ(c7000 エンクロージャの場合)

c7000 エンクロージャのハーフハイトサーバ



c7000 エンクロージャのフルハイトサーバ



(c3000 エンクロージャのポートマッピングについては付録 B を参照)

c-Classイーサネットインターコネクトのオプション

BladeSystem c7000 エンクロージャには、パススルーモジュール、イーサネットおよびファイバチャネルスイッチ、バーチャルコネクトモジュール、およびInfiniBand等の高帯域幅ファブリックなどの各種インターコネクトオプションがあります。HPのWebサイト(http://www.hp.com/go/bladesystem/interconnects (英語))には、使用できるc-Classインターコネクトモジュールについての最新情報があります。

Cisco 社および Blade Network Technologies 社 (BNT)のイーサネットスイッチでは、従来の方法でネットワーク管理ができます。ブレードスイッチの主な利点としては、高速アップリンクを使用してケーブルを統合できること、ブレードの電源および冷却インフラストラクチャが共有できることが挙げられます。

利用可能なブレードスイッチオプションには以下のものがあります。

- Cisco Catalyst Blade Switch 3020
- Cisco Catalyst Blade Switch 3120 (3120G および 3120X)
- HP GbE2c Ethernet ブレードスイッチ
- HP GbE2c Layer 2/3 Ethernet ブレードスイッチ
- HP 1:10Gb Ethernet BL-c スイッチ
- HP 10Gb Ethernet BL-c スイッチ

サーバと LAN を 1 対 1 で直接接続する必要がある場合、イーサネットパススルーモジュールも使用できます。HP イーサネットパススルーモジュールは、サーバと外部イーサネットスイッチの間での 16 ポートの透過的な 1 対 1 のポート接続を提供します。

最後に、バーチャルコネクトも、c-Class イーサネットスイッチまたはイーサネットパススルーモジュールに代わるオプションとして使用できます。

HP バーチャルコネクトテクノロジ

概要

バーチャルコネクトとは、HP BladeSystem c-Class エンクロージャ用のインターコネクトモジュールと組み込みソフトウェアのセットで、これによってサーバ接続のセットアップおよび管理が簡素化されます。HP バーチャルコネクトのポートフォリオには、HP BladeSystem c-Class 用 1/10Gb バーチャルコネクト イーサネットモジュール、HP BladeSystem c-Class 用 1/10Gb-F バーチャルコネクト イーサネットモジュール、および HP BladeSystem c-Class 用 4Gb バーチャルコネクト ファイバチャネル モジュールなどがあります。すべてのモジュールは、組み込みの HP Virtual Connect Manager またはオプションの Virtual Connect Enterprise Manager (VCEM)で管理されます。バーチャルコネクトはサーバエッジの仮想化を実装するため、サーバ管理者は外部の LAN 環境および SAN 環境から変更を認識させずに、サーバブレードをエンクロージャ内でアップグレード、交換、または移動することができます。

Virtual Connect Manager は、HP BladeSystem c-Class 用 1/10Gb バーチャルコネクト イーサネットモジュールおよび 1/10Gb-F バーチャルコネクト イーサネットモジュールに組み込まれています。管理者がこれにアクセスするには、Onboard Administrator (OA)で提供されている Web リンク、OA から内部シリアル経由で CLI 接続、組み込みの Virtual Connect Manager Web サーバへの直接接続、Virtual Connect Manager に SSH で CLI 接続、の 4 つの方法があります。

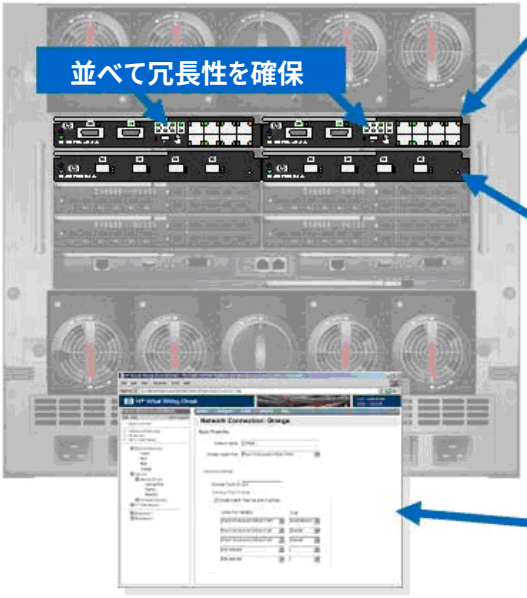
Virtual Connect Manager を使用して構成されるバーチャルコネクトドメインは、バーチャルコネクトモジュールと合計 16 のサーバベイが設置された単一の HP BladeSystem c-Class エンクロージャで、サーバベイにはサーバブレードとストレージブレードを取り混ぜて実装できます。VC ドメインでは、どのサーバブレードも VC モジュールに接続された任意の LAN または SAN にアクセスするよう構成でき、またサーバブレードは同じ VC ドメイン内のサーバブレードの予備として使用できます。

VC ドメイン内のイーサネットモジュールをスタックする (ケーブル接続する) ことによって、ドメイン内のすべてのサーバブレードを、任意の外部ネットワーク接続にアクセスするように設定することができます。別の I/O ベイにあるファイバチャネルモジュール(VC-FC)は、個別の FC SAN ファブリックにそれぞれ直接接続されます。この構成を使用すると、Virtual Connect Manager は外部の LAN または SAN の構成を変更することなく、サーバプロファイルを VC ドメイン内のどのサーバベイにでも展開および移動することができます。

Virtual Connect Enterprise Manager (VCEM)は単独のソフトウェア製品で、単一コンソールからの管理機能を100 個のVCドメインに拡張し、管理対象のMACアドレスおよびWWN (World Wide Name)の単一のプールを提供し、バーチャルコネクトサーバプロファイルのVCドメイン間での移動およびサーバベイ間での自動フェイルオーバーを可能にします。本書の説明および例では、組み込みのVirtual Connect Managerについて言及し、VCEMについては扱いません。VCEMについての詳細は、http://www.hp.com/jp/vcemを参照してください。

バーチャルコネクトのコンポーネント

バーチャルコネクトのインフラストラクチャを構成する主要なコンポーネントは 3 つあります。コンポーネントのうち 2 つがハードウェアで、1 つがソフトウェアです。3 つの主要なコンポーネントは、バーチャルコネクト イーサネットモジュール、バーチャルコネクト ファイバチャネルモジュール、Virtual Connect Manager (VCM)、およびオプションの Virtual Connect Enterprise Manager (VCEM)です。



バーチャルコネクト イーサネットモジュール
- 選択したデータセンタネットワークに VC イーサネットポートを接続
- データセンタへのアップリンクの集約/タギングをサポート
- あらゆるデータセンターのスイッチ環境 (Cisco、Nortel、HP ProCurve など) への接続に対する「LAN セーフ」

＋

バーチャルコネクト ファイバチャネルモジュール
- 複数サーバの FC HBA ポート(Qlogic/Emulex)を NPIV を使用して FC アップリンクを集約
- データセンタの FC スイッチ(Brocade、Cisco、McData など)にエンクロージャを接続
- FC ファブリックではスイッチとして認識されない
- VC-FC のインストールには VC イーサネットが必要

＋

Virtual Connect Manager (*組み込み*)
- 1 つのVCエンクロージャでのサーバ接続、MACアドレス、およびWWNを管理

Virtual Connect Enterprise Manager
- 単一コンソールから 100 台のエンクロージャを管理
- エンクロージャ単位でのライフタイムライセンス

バーチャルコネクト イーサネットモジュールは、以下の 2 つが使用できます。

- HP 1/10Gb バーチャルコネクト イーサネットモジュール
  - 16 x 1Gb ダウンリンク(ミッドプレーン)
  - 1 x 10Gb クロスコネクト(CX-4)
  - 2 x 10Gb 銅線アップリンク(CX-4)
  - 8 x 1Gb (1000/100/10)銅線アップリンク(RJ-45)

- HP 1/10Gb-F バーチャルコネクトイーサネットモジュール
  - 16 x 1Gb ダウンリンク(ミッドプレーン)
  - 1 x 10Gb クロスコネクト(CX-4)
  - 1 x 10Gb 銅線アップリンク(CX-4)
  - 2 x 10Gb SR または LR ファイバアップリンク(XFP)
  - 2 x 1Gb ファイバアップリンク(SFP)
  - 4 x 1Gb (1000/100/10)銅線アップリンク(RJ-45)

Virtual Connect Manager (VCM)の目的は、バーチャルコネクトドメインを 1 ヶ所で管理する機能を提供することです。つまり、バーチャルコネクトドメインとすべての VC イーサネットおよび VC ファイバチャネルのモジュールの構成、管理、監視といったあらゆる側面が、VCM によって提供されます。

VCM は、インターコネクトベイ 1 または 2 にインストールした HP 1/10Gb または HP 1/10Gb-F イーサネットモジュールのいずれかに組み込まれて実行されます。VCM は VC イーサネットモジュールに搭載された独自の CPU、メモリ、およびフラッシュリソースを使用します。

バーチャルコネクト イーサネットモジュールがインターコネクトベイ 1 および 2 の両方にインストールされると、VCM は高可用性モードで実行されます。デフォルトでは、インターコネクトベイ 1 のバーチャルコネクト イーサネットモジュールがアクティブな VCM で、インターコネクトベイ 2 のバーチャルコネクト イーサネットモジュールがスタンバイ VCM になります。バーチャルコネクトドメインの構成は、構成が変更されるたびに、アクティブな VCM からスタンバイ VCM に対してチェックポイントされます。この方法によって、アクティブな VCM として機能しているバーチャルコネクト イーサネットモジュールに障害が発生した場合、バーチャルコネクトドメインの構成設定を失うことなく、スタンバイのイーサネットモジュールがアクティブな VCM の役割を引き継ぐことができます。

注記:
VCM は一度に 1 つのバーチャルコネクト イーサネットモジュールでしかアクティブになりませんが、これはバーチャルコネクト イーサネットモジュールで提供されるイーサネット接続機能とは関係ありません。ドメイン内のすべてのバーチャルコネクトモジュールが常にアクティブとして機能し、すべてのバーチャルコネクトモジュールにあるすべてのポートが、ネットワークトラフィックをアクティブな状態で同時に伝達するよう構成することができます。

バーチャルコネクトの技術仕様

- 128Gbps のブリッジング ファブリック
- HOL (Head of Line)ブロッキングの防止機能を持つ 2 MB のダイナミックメモリ(ブリッジング バッファ)
- すべてのパケットサイズおよびあらゆる条件についてのラインレート転送
- 16384 個の MAC アドレスに対応
- 1024 個の IGMP グループおよびブリッジングエントリに対応
- 最大転送ユニットは 9216 バイト(ジャンボフレーム)
- 64 バイトフレームでのシングルモジュールの平均レイテンシは 3.8 マイクロ秒
- 1518 バイトフレームでのシングルモジュールの平均レイテンシは 3.8 マイクロ秒

Virtual Connect Managerのユーザーインタフェース

Virtual Connect Manager (VCM)には、バーチャルコネクト(VC)ドメインを管理および監視するために、Web、SSH CLI、および SNMP の 3 つのユーザーインタフェースがあります。

Webインタフェースおよび SSH CLIインタフェースは、VCドメインの管理に使用される、ほぼ同じ一連の機能を提供します。これらのインタフェースについての詳細は、『Virtual Connect Users Guide』(http://www.hp.com/go/bladesystem/documentation)(英語) を参照してください。

VC の SNMP 実装を行うと、管理者は VC ドメインおよび関連するモジュールを監視することができます。SNMP 構成は Virtual Connect Manager によって制御され、VC ドメイン内のすべてのモジュールに適用されます。プライマリモジュールに存在する SNMP エージェント ソフトウェア モジュールによって、SNMP プロトコルを使用して管理されている情報にアクセスできます。管理されている情報は MIB と呼ばれる階層型データベースとして提供されます。管理されている情報の各要素は、オブジェクト ID と呼ばれる一意の識別子によって識別されます。VC-Enet モジュールには SNMP の基本サポートが提供されています。

VC-Enet モジュールは、以下の SNMP MIB の適用可能なグループをサポートします。

- Compaq Host MIB
- Compaq System Info MIB
- RFC 3418 SNMPv2-MIB
- RFC 2863 IF-MIB
- RFC 4188 BRIDGE-MIB

VC-Enet モジュールは以下の SNMP トラップをサポートします。

- CPQ-HOST MIB からの cpqHoSWRunningStatusChangeTrap
- SNMPv2-MIB からの coldStart トラップ

バーチャルコネクトのポートの説明

ポートには、VC ダウンリンク、VC アップリンク、および内部クロスコネクトの 3 種類があります。

- **VC ダウンリンク**
  - エンクロージャのミッドプレーンを経由してサーバの NIC ポートに直接接続する、外からは見えないポート
  - 直接接続したサーバブレードの NIC に接続機能を提供することが唯一の役割
- **VC アップリンク**
  - VC ドメインに外部接続を提供する、VC-Enet モジュールの表面上に見えるポート
  - スタッキングリンク、ネットワーク分析用ポート(「ポート監視」の項を参照)、通常モード (1 つまたは複数の vNet または共有アップリンクセットに外部接続を提供)などの役割がある
- **内部クロスコネクト**
  - 水平方向に隣接する 2 つの VC-Enet モジュールを相互接続する見えないポート
  - 唯一の役割はスタッキングリンクとしての機能

バーチャルコネクト イーサネット接続の概要

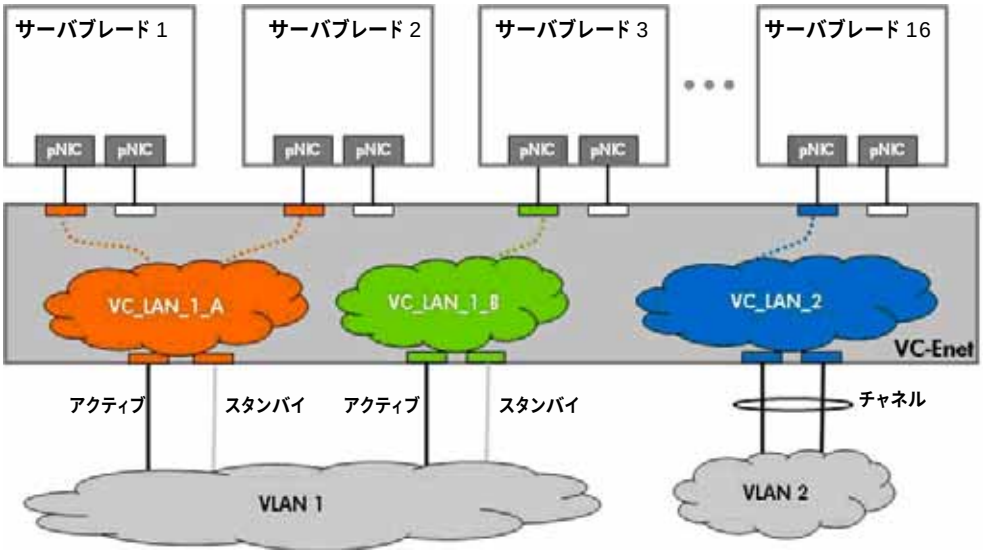
バーチャルコネクトは多くの機能がありますが、その主な目的は、c-Class エンクロージャ内のサーバブレードに内部および外部のネットワーク接続を提供することです。イーサネットの場合、バーチャルコネクトはこの目的を実行するために、VC ダウンリンクポート(サーバ NIC)と他の VC ダウンリンクポート、および外部のスイッチドネットワークに接続された VC アップリンクポートをレイヤ 2 で一緒にブリッジします。バーチャルコネクトによって、管理者はどのアップリンクとダウンリンクが同じレイヤ 2 ネットワークに割り当てられているかを、バーチャルコネクトネットワーク(vNet または共有アップリンクセット)を使用して制御することができます。

VC 管理者は vNet を定義し、必要に応じて、外部ネットワーク接続を提供するために VC アップリンクを vNet に割り当てます。vNet を定義すると、サーバ管理者はこれをサーバの NIC ポートに割り当てることができます。サーバ管理者がサーバプロファイルを 1 つのサーバベイから別のサーバベイに移動すると、vNet の割り当てと、管理されている MAC アドレス(「VC が管理する MAC アドレス」の項を参照)が使用されている場合、その MAC アドレスがプロファイルと一緒に移動します。これによってサーバ管理者はネットワーク管理者の支援を仰ぐことなく、サーバの「イーサネット接続プロファイル」を 1 つのベイから別のベイに簡単に移動できます。

vNet はエンクロージャ内に限定されたネットワークの複数の VC ダウンリンクをまとめてブリッジするのに使用できますが、1 つ以上の VC ダウンリンクと 1 つ以上の VC アップリンクを相互にブリッジして、エンクロージャ内のサーバブレードに外部ネットワーク接続を提供するのにも使用できます。vNet は、複数の VC アップリンクを一緒にブリッジして 2 つの外部デバイス間の接続、または 2 つの外部ネットワーク間の接続を提供するために使用することはできません。バーチャルコネクトは転送デバイスではなく、そのように構成することはできません。つまり、VC はサーバブレード間の内部接続を提供したり、サーバブレードに外部接続を提供することはできますが、2 つの外部デバイス間の接続を提供することはできません。バーチャルコネクトネットワーク(vNet)の基本的な定義は、単一のレイヤ 2 ネットワークまたはブロードキャストドメインで構成される、VC ポート(ダウンリンクどうし、またはダウンリンクとアップリンク)の論理グループです。vNet は VMware テクノロジで使用されている vSwitch に似ています(詳細な比較については、「VC と VMware ネットワーキングテクノロジの比較」を参照)。vNet は、後述の「高度なバーチャルコネクトイーサネット設計」の項で見られるように、VLAN と常に 1 対 1 の相関関係を持つわけではありません。

同じ vNET に割り当てられたサーバの NIC ポートは、エンクロージャを出ることなく直接(レイヤ 2 で)通信できます。次の図で、サーバブレード 1 とサーバブレード 2 は、VC ドメイン内で互いに通信することができます。また、別の vNet にあるサーバの NIC ポートは、バーチャルコネクトによって他のサーバの NIC ポートから(レイヤ 2 で)隔離されます。サーバブレード 16 はサーバブレード 1 から 3 までとは隔離されています。

図 3. vNet のさまざまな使用方法



(上の図の要素については、付録 A の説明を参照)

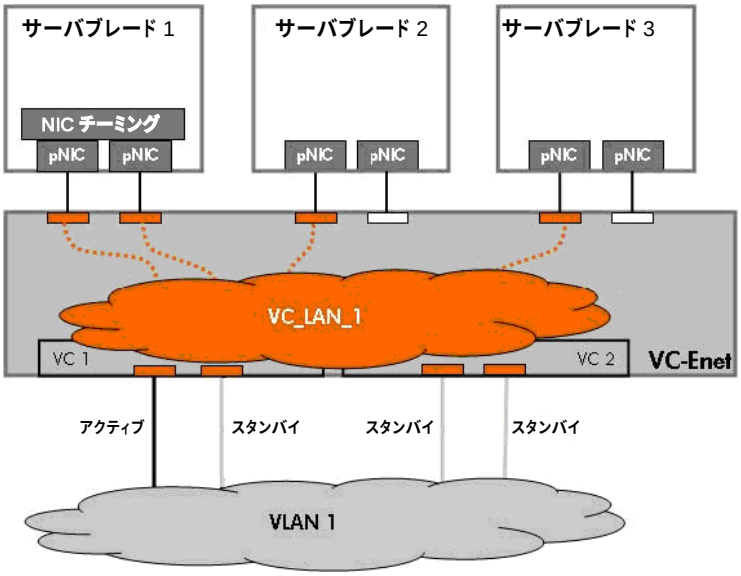
注記:
レイヤ 2 接続とは、ルータまたはレイヤ 3 スイッチを経由せずに、任意のプロトコルを転送するイーサネットフレームを直接交換することで互いに通信できる 2 つのデバイスとして定義されています。レイヤ 2 ネットワークは「ブロードキャストドメイン」として定義されることもあります。たとえば、ある vNet 内でフレームをブロードキャストすると、その vNet に割り当てられているポートのみがブロードキャストフレームを受信します(外部デバイスが複数の vNet を一緒にブリッジしている場合はこの限りではありません)。

VC アップリンクのフォールトトレランス

バーチャルコネクトは、バーチャルコネクトネットワークおよび関連するサーバの NIC ポートに対して、フォールトトレランスとロードバランシングの両方を提供するように構成できます。管理者は vNet の接続モードを「Failover」に設定して vNet がフォールトトレランス モードのみで動作するように選択するか、または接続モードを「Auto」に設定することで、フォールトトレランスにロードバランシングを追加するよう選択することができます。

管理者が複数の VC アップリンクを同じ vNet に割り当てた場合、VC は vNet (または共有アップリンクセット)に対するデフォルト動作(接続モードが「Auto」)として、802.3ad LACP (Link Aggregation Control Protocol)を使用したポートチャネル(EtherChannel)のネゴシエーションを試行します。LACP ネゴシエーションに失敗すると、vNet はフォールトトレランス モードのみで動作します。バーチャルコネクトは NIC チーミングと同じように、1 つの VC アップリンクポートをアクティブポートとして使用し、他のすべての VC アップリンクポートはスタンバイ(ブロッキング)モードとなります。この動作は VC のループ防止機構の一部です(「バーチャルコネクトのループ防止テクノロジ」の項を参照)。例として次の図を参照してください。

図 4. フォールトトレランスのみの vNet 構成



(上の図の要素については、付録 A の説明を参照)

管理者は vNet の接続モードを「failover」に設定することで、vNet (または共有アップリンクセット)をフォールトトレランスのみに手動で構成することを選択できます。vNet の接続モードを「failover」に設定すると、LACP プロトコルが vNet に対して無効になり、管理者は VC アップリンクの「Port Role」を「Primary」または「Secondary」に変更することができます。このポートの役割の設定によって、管理者はどの VC アップリンクをアクティブなアップリンクに優先的に設定するかを手動で選択することができます。

注記:
Cisco スイッチに接続された VC アップリンクを示す構成の例については、後述の「バーチャルコネクトイーサネットと Cisco の構成例」の項を参照してください。

vNet (または共有アップリンクセット)は、アクティブなアップリンクがリンクを失うと、1 つのアップリンクから別のアップリンクにフェイルオーバーします。アクティブなアップリンクのリンクが失われたことを VC が検出すると、VC は同じ vNet に割り当てられている使用可能なスタンバイアップリンクのグループから、新しいアクティブなアップリンクをすぐに選択します。新しいアクティブアップリンクを選択するこのプロセスは、通常は 5 秒以内に行われます。上位の Cisco スイッチが、vNet に関連付けられたすべてのアップリンク上で正しく構成されていれば、サーバ接続は 5 秒以内で復旧するはずです。以前アクティブだったアップリンクのリンクが復旧すると、VC は自動的にフェールバックします。外部の Cisco スイッチポートが、PortFast を有効にすることで正しく構成されていれば、サーバへの接続は 5 秒以内で復旧するはずです。

バーチャルコネクトは「Fast MAC Cache Failover」というメカニズムを使用して、上位の Cisco スイッチポートの CAM テーブルをプロアクティブに更新します。vNet が 1 つのアップリンクから別のアップリンクにフェイルオーバーまたはフェールバックすると、このメカニズムは新しいアクティブアップリンク上で単一のフレームを、VC ドメイン内でアクティブなすべてのサーバの MAC アドレスに送信します。Fast MAC Cache Failover により、バーチャルコネクトは外部の Cisco インフラストラクチャを特定の vNet のアクティブな VC アップリンクの新しい場所ですばやく更新することができます。Fast MAC Cache Failover は Cisco スイッチでリンクステートトラッキングに使用される CAM テーブル更新プロセスとたいへん良く似ています。

VC アップリンクのロードバランシング

バーチャルコネクトは、LACP (Link Aggregation Control Protocol)を使用した IEEE 802.3ad ポートトランキングまたはポートチャネリング(EtherChannel)の方法によって、同じ物理 VC-Enet モジュール上の複数の VC アップリンクにまたがるロードバランシング(およびフォールトトレランス)を提供しています。vNet (または共有アップリンクセット)は、「connection mode」を「failover」でなく「Auto」(デフォルト)にしておく必要があります。

外部スイッチが Cisco スイッチである場合、EtherChannel のポートは「mode active」または「mode passive」のいずれかに設定する必要があります。Cisco スイッチでは、これらの両方のモードで 802.3ad LACP (VC がサポートする唯一のポートチャネリングプロトコル)が使用できます。「mode on」、「mode desirable」、または「mode auto」に設定されているときは、VC は Cisco スイッチポートのポートチャネリングをサポートしません。

注記:
VC と Cisco スイッチの間で EtherChannel を構成できるのは、VC の vNet の接続モードが「Auto」で、Cisco スイッチのチャネルグループが「mode active」または「mode passive」に設定されている場合だけです。

バーチャルコネクト アップリンクポートを使用したポートトランキング / ポートチャネリングには、以下の 4 種類のシナリオがあります。

- **同じ VC モジュール、同じ外部スイッチ、同じポートチャネルグループ**

  同じ物理 VC-Enet モジュールからの VC アップリンクが、同じ vNet (または共有アップリンクセット)に割り当てられて、またその VC アップリンクが、同じポートチャネルグループに割り当てられ、LACP プロトコルが有効に設定された同じ外部 Cisco スイッチのポートに接続される場合、VC は単一のポートチャネルを自動的に構成します。

- **同じ VC モジュール、同じ外部スイッチ、別のポートチャネルグループ**

  同じ物理 VC-Enet モジュールからの VC アップリンクが、同じ vNet (または共有アップリンクセット)に割り当てられて、またその VC アップリンクが、別のポートチャネルグループに割り当てられ、LACP プロトコルが有効に設定された同じ外部 Cisco スイッチのポートに接続される場合、VC は複数のポートチャネルを自動的に構成する場合があります。

- **同じ VC モジュール、別の外部スイッチ**

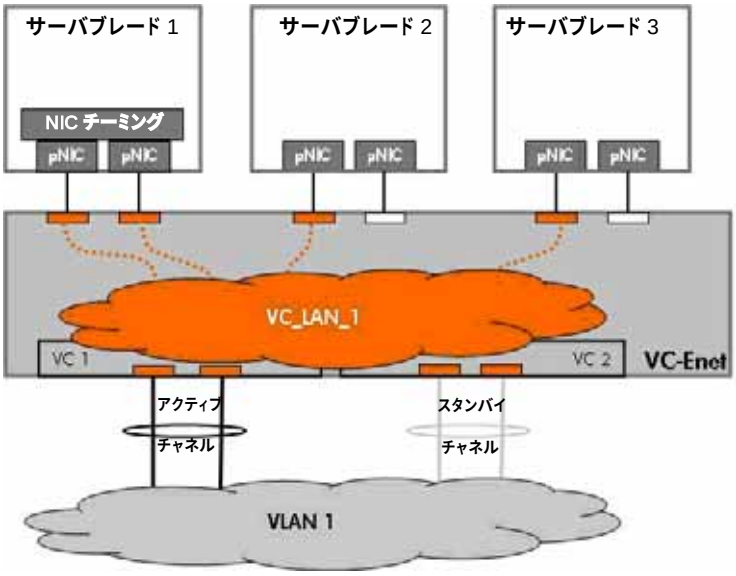
  同じ物理 VC-Enet モジュールからの VC アップリンクが、同じ vNet (または共有アップリンクセット)に割り当てられて、またその VC アップリンクが、ポートチャネルグループに割り当てられ、LACP プロトコルが有効に設定された別の外部 Cisco スイッチのポートに接続される場合、VC は複数のポートチャネルを自動的に構成する場合があります。

- **別の VC モジュール、同じあるいは別の外部スイッチ**

  別の物理 VC-Enet モジュールからの VC アップリンクが、同じ vNet (または共有アップリンクセット)に割り当てられて、またその VC アップリンクが、ポートチャネルグループに割り当てられ、LACP プロトコルが有効に設定された同じ(または別の)外部 Cisco スイッチのポートに接続される場合、VC は複数のポートチャネルを自動的に構成する場合があります。

上で説明したように、vNet に対する VC のデフォルト動作(接続モードが「Auto」の場合)では、802.3ad LACP を使用して、ポートチャネル(EtherChannel)のネゴシエーションが試行されます。1 つ以上の VC アップリンクポートで LACP ネゴシエーションに成功した場合、VC イーサネットモジュールと外部スイッチの間にポートチャネルが構成されます。vNet は 1 つまたは複数の外部スイッチと複数のポートチャネルを構成することがあります。それぞれのポートチャネルは、単一の論理パスとして動作します。前述のシンプルなフォールトトレランスの項で説明したように、vNet はいつでもアクティブな論理パスを 1 つだけ持つことができます。したがって、複数のポートチャネルを持つ vNet は 1 つのポートチャネルだけをアクティブな論理パスとして使用し、同じ vNet 内の別のポートチャネルはすべてスタンバイモードになります。例として次の図を参照してください。

図 5. ロードバランシングおよびフォールトトレランスにポートチャネリングを使用する vNet



(上の図の要素については、付録 A の説明を参照)

注記:
ポートチャネルが構成できるのは、同じ物理 VC イーサネットモジュール上の VC アップリンクポートが同じ外部スイッチに接続されている場合だけです。VC は異なる VC イーサネットモジュールにまたがるポートチャネルをサポートしません。

ポートチャネリング(802.3ad)ロードバランシング アルゴリズム

VC-Enet のポートチャネリングの実装(EtherChannel)では、ポートチャネルを構成する物理ポート全体にフレームを分散するために、ロードバランシング アルゴリズムを使用しています。複数の物理ポート全体にフレームを分散するにあたって最も注意すべき点は、「フレームの順序」です。2 つのネットワークデバイス間での特定の対話(FTP 転送や telnet セッションなど)の場合、送信者が送信した順序でネットワークインフラストラクチャがフレームを配信するのが最も適しています。これによって、受信側でのフレームの並べ替えが最小限に抑えられます。また、TCP にはフレームを正しい順序に戻すヘッダ情報がありますが、UDP など他のプロトコルにはこの情報がありません。そのため、フレームの順序が非常に重要になります。つまり、どのロードバランシング アルゴリズムをポートチャネリングで使用するとしても、フレームの負荷を均一化しつつ、フレームの順序を維持する必要があるということです。これは、同じ対話からのフレームに対しては同じロードバランシングの決定を下すアルゴリズムを使用することで実現できます。

EtherChannel **の一般的なロードバランシング アルゴリズム(下に行くほど良い方法)**

- **送信元の MAC アドレス**
  同じ MAC アドレスから送信されるすべての対話を識別して、ポートチャネル内の単一リンクで負荷を均一化する
- **宛先 MAC アドレス**
  同じ MAC アドレスを宛先とするすべての対話を識別して、ポートチャネル内の単一リンクで負荷を均一化する
- **送信元 IP アドレス**
  同じ IP アドレスから送信されるすべての対話を識別して、ポートチャネル内の単一リンクで負荷を均一化する

- **宛先 IP アドレス**

  同じ IP アドレスを宛先とするすべての対話を識別して、ポートチャネル内の単一リンクで負荷を均一化する

VC
- **送信元および宛先 MAC アドレス**

  2 つの MAC アドレスの間で交わされるすべての対話を識別して、ポートチャネル内の単一リンクで負荷を均一化する
- **送信元および宛先 IP アドレス**

  2 つの IP アドレスの間で交わされるすべての対話を識別して、ポートチャネル内の単一リンクで負荷を均一化する
- **送信元および宛先 IP アドレスと TCP または UDP ポート(ソケット)**

  2 つの IP アドレスの間で交わされる特定の対話を識別して、ポートチャネル内の別々のリンクで負荷を均一化できる

バーチャルコネクトでは、ロードバランス対象のフレームの種類に応じて、最後の 3 つのアルゴリズムから 1 つを選んで使用します。

ユニキャストフレームの場合、VC は、TCP または UDP ヘッダがある場合はソケット(上記の最良の方法)を使用し、TCP または UDP ヘッダがない IP フレームであれば送信元および宛先 IP アドレスを使用し、IP フレームでなければ送信元および宛先 MAC アドレスを使用してロードバランスを行います。

ブロードキャスト、マルチキャスト、および不明なユニキャスト(宛先の検索に失敗した)フレームは、ユニキャストフレームとは少し違った方法で処理されます。これらは、VC がこれらのフレームをチャネルの最初のポートに必ずしも毎回送信しないようにロードバランスされます。チャネルのポートを決定するのに使用されるアルゴリズムは、送信元および宛先 MAC アドレス、送信元のポートチャネル番号(送信元がポートチャネルの場合)、またはモジュール ID とポート番号(送信元が通常のポートであってポートチャネルでない場合)に基づいています。

VC は使用可能な対話固有の情報(TCP/UDP、IP、MAC の順)を使用して、ポートチャネル内のポート全体にトラフィックをロードバランスするため、VC はこの機能についてユーザーが構成できる設定を提供していません。また、ロードバランシング アルゴリズムは同じポートチャネルの両側で一致させる必要はありません。つまり、あるアルゴリズムを VC 側で使用して、直接接続する Cisco スイッチでは別のアルゴリズムを使用することができるということです。接続に影響を及ぼさずに、それぞれの側で独自のアルゴリズムを実装できます。結果として、HP は直接接続した Cisco スイッチでは送信元および宛先 IP と TCP/UDP ポートに基づくロードバランシング アルゴリズムを使用するよう推奨していますが、これは必須の要件ではないということです。外部の Cisco スイッチが送信元および宛先 MAC アドレスまたは送信元および宛先 IP アドレスに基づくアルゴリズムを使用しても、バーチャルコネクトとも連動します。

注記:
EtherChannel 用に構成された Cisco スイッチに接続された VC アップリンクを示す構成の例については、後述の「**バーチャルコネクトイーサネットと Cisco の構成例**」の項を参照してください。

VC アップリンクおよび VLAN トランキング

バーチャルコネクトでは IEEE 802.1Q **を使用した** VC **アップリンク上の** VLAN **タギング(トランキング)をサポートしており、サーバブレードの** NIC **ポート上で** VLAN **タギングをサポートするよう構成できます。**

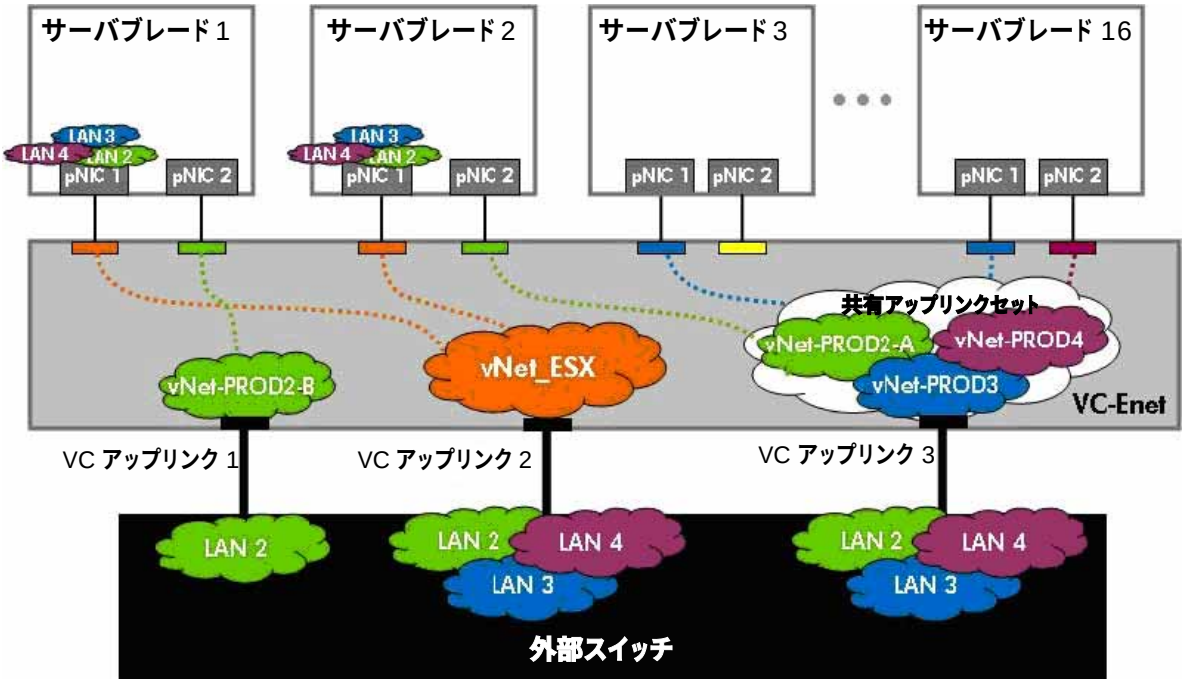
VC **アップリンクは以下に示す** 3 **つのモードのうち** 1 **つで動作できます。**

- **VLAN トランキングモード**
  - **外部スイッチポートでの共有アップリンクセット**(SUS)**とタギング**
  - VC **アップリンクが** SUS **のメンバーで、外部スイッチの** VLAN **トランクポートに接続されている場合、**VLAN **トランクポートとして動作します。**
  - **複数の** vNet**、複数の** VLAN
  - **サーバの** NIC **ポート上でのタギングはなし**
  - **例: 図** 6 **の「**VC **アップリンク** 3**」**
- **VLAN トンネリングモード**
  - **外部スイッチポートでの単一の** vNet **とタギング**
  - VC **アップリンクが単一の** vNet **のメンバーで、外部スイッチ上の** VLAN **トランクポートに接続されている場合、**Cisco **スイッチの「**dot1qtunnel**」モードに相当するモードで動作します。**
  - **単一の** vNet**、複数の** VLAN
  - **サーバの** NIC **ポートでのタギングあり**
  - **例: 図** 6 **の「**VC **アップリンク** 2**」**
- **アクセスモード**
  - **外部スイッチポートでの単一の** vNet**、タギングなし**
  - VC **アップリングが単一の** vNet **のメンバーで、アクセスモードで外部スイッチに接続されている場合、**Cisco **スイッチの「**access**」モードに相当するモードで動作します。**
  - **単一の** vNet**、単一の** VLAN
  - **サーバの** NIC **ポートでのタギングなし**
  - **例: 図** 6 **の「**VC**アップリンク** 1**」**

VC **が** VC **アップリンク上で** VLAN **タギングをサポートするよう構成されている場合**(VLAN **トランキングモード**)**、**VC **がタグを解釈し(つまり、タグを除去および挿入し、タグ情報に基づいてフレームの** vNet **メンバーシップを分類する)、**VC **がそのタグの終端点である(つまりサーバでは** VLAN **タグが見えない)ことを意味します。これは** VC **で「共有アップリンクセット」**(SUS)**を使用することで実行できます。**SUS **は** VLAN **トランク(タギング)として構成される** 1 **つまたは複数の** VC **アップリンクで、外部の** VLAN **を** VC **ドメイン内の特定の** vNet **と関連付けます。管理者は** SUS **を作成し、**1 **つまたは複数の** VC **アップリンクを追加し、その** VC **アップリンクでどの** VLAN **タグを伝送するかを定義して、定義した各** VLAN **の** vNet **名**(ASCII)**をつけます。つまりこれは、**SUS **内のアップリンクポートが複数の** vNet **に外部接続を提供することを意味します。言い換えると、**1 **つまたは複数の** vNet **が外部ネットワーク接続用のアップリンクのセットを共有するということです。こういう理由で「共有アップリンクセット」という用語が使用されています。図** 6 **の「**VC **アップリンク** 3**」を参照してください。**

VC **アップリンクポートが単一の** vNet **に割り当てられて、**VLAN **トランキングモードで外部スイッチポートに接続される場合、**VC **アップリンクと** vNet **はデフォルトでは** VLAN / CoS **トンネリングモードまたは** dot1qtunnel **モードで動作します。言い換えると、**vNet **はすべてのフレームを同じレイヤ** 2 **ドメイン**(vNet)**内に保持するということですが、**VC **では異なる** VLAN **タグを外部ネットワークからサーバの** NIC **ポートへ伝送したり、またその逆方向へ伝送することが可能です。図** 6 **の「**VC **アップリンク** 2**」を参照してください。**VC **アップリンクポートが単一の** vNet **に割り当てられて、外部のスイッチポートにアクセスモードで接続される場合、**VC **アップリンクと** vNet **はアクセスモードで動作し、単一の** VLAN **(スイッチ側のアクセス** VLAN**)のタグなしフレームのみを伝送します。図** 6 **の「**VC **アップリンク** 1**」を参照してください。つまり、外部スイッチポートの構成に応じて、単一の** vNet **が単一の** VLAN **を表したり複数の** VLAN **を表したりすることができるということです。**

図 6. VLAN タギングの例



(上の図の要素については、付録 A の説明を参照)

上の図の説明:

- VC アップリング 3 は共有アップリンクセット(SUS)に割り当てられていて、VLAN 2 から VLAN 4 までのタグが付けられています。
    - 外部スイッチポートは VLAN 2 から VLAN 4 を伝送するトランクポートです。
    - VLAN 2 は vNet-PROD2-A、VLAN 3 は vNet-PROD3、VLAN 4 は vNet-PROD4 で表されます。
- VC アップリンク 2 は vNet_ESX に割り当てられていて、802.1Q トンネリングモードで動作します。
    - 外部スイッチポートは VLAN2 から VLAN 4 を伝送するトランクポートです。
    - vNet_ESX は VLAN 2 から VLAN 4 を表す単一の vNet です。
- VC アップリンク 1 は vNet-PROD2-B に割り当てられていて、アクセスモードで動作します。
    - 外部スイッチポートは VLAN 2 に割り当てられているアクセスポートです。
    - vNet-PROD2-B は「アクセスモード」で動作する、外部の VLAN 2 用の vNet を表しています。

- サーバ 1 とサーバ 2 の両方の NIC 1 は、サーバ上で VLAN タギングが構成されています。両方のサーバで、NIC 1 は VLAN 2 から VLAN 4 までを表しています。
- 他のすべての NIC は VLAN タギングを使用していません。これらすべての NIC は単一の VLAN に接続されています(VLAN の関連付けは色を参照)。
- サーバ 1 の NIC 1 はサーバ 2 の NIC 1 と VC ドメイン内で直接対話できます。
- サーバ 1 の NIC 2 がサーバ 2 の NIC 2 と対話するには、フレームはまず VC アップリンク 1 を通って VC ドメインを出て、VLAN2 上の外部スイッチを通過してから、VC アップリンク 3 から VC ドメインに再び入る必要があります。

共有アップリンクセットは個別の vNet が行うのと同じ方法でアップリンクの冗長性を管理します。言い換えると、複数のアップリンクが 1 つの共有アップリンクセットに割り当てられると、アップリンクはフェイルオーバーのみのモードで動作するか、ポートチャネリング(EtherChannel)モードで動作することができます。また、すべての VLAN と、これに関連付けられた単一の共有アップリンクセット内の vNet は、同じアクティブアップリンクまたは同じアクティブポートチャネルを使用します。

注記:
VLAN トランキング用に構成された Cisco スイッチに接続された VC アップリンクを示す構成の例については、後述の「バーチャルコネクトイーサネットおよび Cisco の構成例」の項を参照してください。Cisco スイッチのコマンドは、VC が VLAN トランキングモードでも VLAN トンネリングモードでも同じです。

サポートされない Cisco VLAN プロトコル

バーチャルコネクトでは、Cisco の 2 つの独自仕様 VLAN プロトコル(VTP および DTP)はサポートしていません。

VTP (VLAN Trunking Protocol)は、単一の VLAN データベースを同じドメイン内の複数のスイッチにわたって管理するために使用する Cisco の独自仕様プロトコルです。VC は Cisco のデバイスではないため、VTP をサポートしていません。したがって、仮に VC ドメインの構成が間違っていても、VTP ドメインに悪影響を及ぼすことは一切ありません。VC は VTP をサポートしていないため、管理者はトランキングが必要なすべての VLAN を VC アップリンクポートに追加する必要があります。

DTP (Dynamic Trunking Protocol)は、直接接続された一対の Cisco ポートの間で VLAN トランキング構成を自動化するために使用される Cisco の独自仕様プロトコルです。DTP を有効にすると、1 つの Cisco スイッチポートで VLAN トランキングが構成できて、これと相対するスイッチポートでもそれに一致した VLAN トランキング構成を自動的に構成することができます。VC は Cisco のデバイスではないため、DTP をサポートしていません。管理者は、直接接続した Cisco スイッチポート上で「switchport nonegotiate」コマンドを使用して DTP を無効にすることをお勧めします。

バーチャルコネクトとNICチーミング

バーチャルコネクト(VC)は、サーバの NIC ポートでの NIC チーミング(または NIC ボンディング)に対応しています。x86 上の Windows については、VC はネットワークフォールトトレランス(NFT)とトランスミット ロードバランシング(TLB)をサポートしていますが、スイッチアシスト ロードバランシング(SLB)はサポートしていません。Integrity 上の Windows については、VC は NFT、TLB、およびチーム内に 2 つの NIC ポートしかないスタティックなデュアルチャネルをサポートしていますが、SLB はサポートしていません。Linux の場合、VC はサーバの NIC ポートで 802.3ad (スタティックまたは LACP を使用したダイナミック)を必要としないすべての種類の NIC ボンディングをサポートしています。

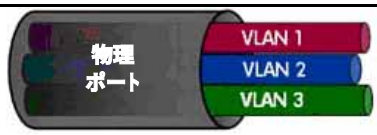
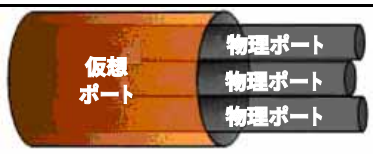
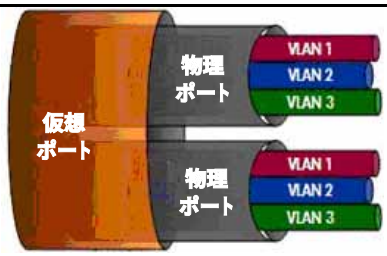
また VC は、NIC チーミング(ボンディング)が有効になっているサーバで使われている vNet で設定できる「SmartLink」と呼ばれる機能もサポートしています。SmartLink 機能は、関連付けられた vNet のすべての VC アップリンクが切断されたときに、VC ダウンリンク(サーバの NIC ポート)を無効にします。基本的に SmartLink の機能は、vNet のアップリンクのリンクダウン イベントを、チーム内のサーバの NIC に伝播することです。これによって NIC チーミングソフトウェアが、(すべてのアップリンクがダウンした)vNet から、機能しているアップリンクを持つ別の vNet にフェイルオーバーできるようにしています。SmartLink は、チーム内の NIC ポートが別々の vNet に接続されている場合に、NIC チーミング構成でのみ使用されます(「図 12. VC ドメインでの vNet および EtherChannel の高度な使用例」を参照)。HP では、vNet に割り当てられているすべてのサーバの NIC ポートが NIC チーミングを使用していて、少なくとも 1 つの別の vNet にも接続されている場合にのみ、SmartLink を vNet で有効にすることを推奨しています。

Windows での NIC チーミングについての詳細な情報は、本書の末尾にある「追加リソース」の項にあるリンクを参照してください。

バーチャルコネクトとCiscoの用語比較

バーチャルコネクト(VC)では従来の多くのネットワーキング用語に加えて、新しいネットワーキング用語が使用されています。VC はサーバブレードをコアネットワークに相互接続する新しい方法であるため、VC の機能を適切に言い表す新しい用語が必要になったからです。VC のネットワーキング用語のすばやい理解に役立てるため、以下の表に VC と Cisco のネットワーキング用語の比較をまとめました。

表 1. バーチャルコネクトと Cisco のポートトランキングおよび VLAN トランキングの用語比較

業界標準	Cisco Catalyst	HP バーチャルコネクト	図
VLAN トランキング (802.1Q)	トランキング (ISL*または 802.1Q)	共有アップリンクセット (802.1Q)	
ポートトランキング (スタティック、802.3ad LACP)	EtherChannel (スタティック、PAgP*、または 802.3ad LACP)	自動 (802.3ad LACP)	
VLAN トランキング + ポートトランキング	トランキング + EtherChannel (* Cisco の独自仕様)	共有アップリンクセット + 自動	

VCアップリンクポートのためのCisco構成ガイドライン

VLANタグ付きのVCアップリンク(共有アップリンクセット)構成ガイドライン

アクション	コマンド
• VLAN カプセル化を 802.1Q に設定	*“switchport trunk encapsulation dot1q”*
• スイッチポートモードを trunk に設定	*“switchport mode trunk”*
• PortFast の有効化	*“spanning-tree portfast trunk”*
• DTP の無効化	*“switchport nonegotiate”*
• 自動ネゴシエーションの有効化	*“speed auto”* ***および*** *“duplex auto”* (該当する場合)
• LLDP の有効化	*“lldp transmit”* ***および*** *“lldp receive”* (サポートされる場合)
• (オプション) BPDUGuard の有効化	*“spanning-tree bpduguard enable”*

タグなしのVCアップリンク(通常のVCネットワーク/vNet)構成ガイドライン

アクション	コマンド
• Cisco スイッチポートモードを access に設定	*“switchport mode access”*
• PortFast の有効化	*“spanning-tree portfast”*
• DTP の無効化	*“switchport nonegotiate”*
• 自動ネゴシエーションの有効化	*“speed auto”* ***および*** *“duplex auto”* (該当する場合)
• LLDP の有効化	*“lldp transmit”* ***および*** *“lldp receive”* (サポートされる場合)
• (オプション) BPDUGuard の有効化	*“spanning-tree bpduguard enable”*

ポートチャネリングの構成ガイドライン

アクション	コマンド
• インタフェースチャネルプロトコルを LACP に設定	*“channel-protocol LACP”*
• インタフェースをポートチャネルに割り当て(X は同じグループのすべての Cisco ポートについて同じ)、LACP を有効化	*“channel-group X mode active”* ***または*** *“channel-group X mode passive”*
ポートチャネルがタグなし(アクセスモード)の場合、上記のタグなしのVCアップリンクについての構成ガイドラインを参照してください。コマンドはポートインタフェースだけではなく、ポートチャネルインタフェースにも必ず適用してください。	
ポートチャネルがタグ付き(VLANトランクモード)の場合、上記のタグ付きのVCアップリンクについての構成ガイドラインを参照してください。コマンドはポートインタフェースだけではなく、ポートチャネルインタフェースにも必ず適用してください。	

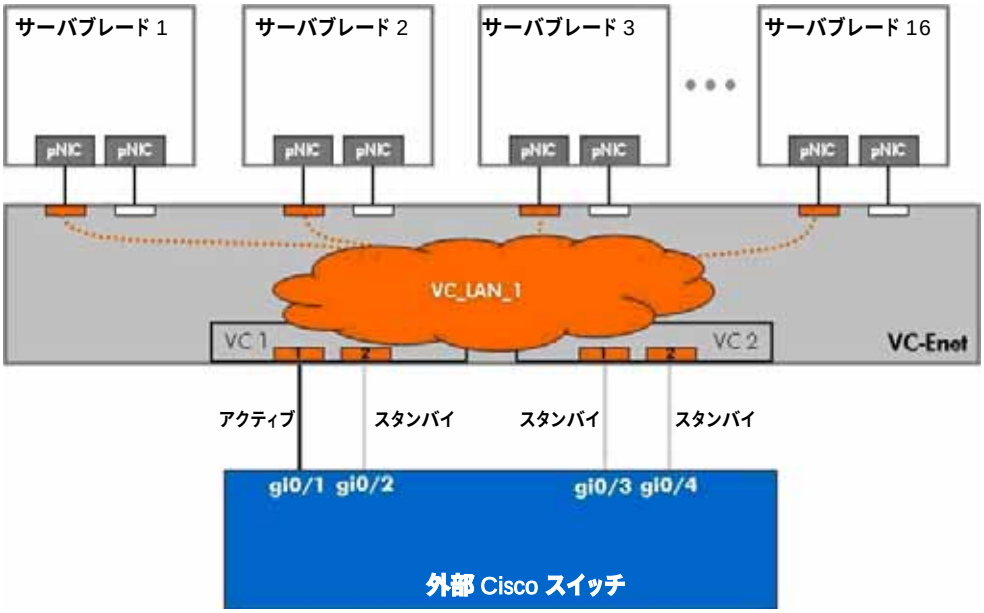
バーチャルコネクトイーサネットとCiscoの構成例

以下の 4 つの構成例は、バーチャルコネクトに接続したときの Cisco インフラストラクチャの構成方法について管理者が概略を把握できるようにするために示すものです。構成例は簡単なものから複雑なものの順になっており、基本的なフォールトトレランス、VLAN トランキング、ポートチャネリング、ポートチャネリングと VLAN トランキングの併用の順になっています。

構成例 1: VC アップリンクを Cisco アクセスポートに接続する

図 7 は、VC と Cisco の単純なフォールトトレランスのシナリオと、Cisco スイッチに必要な最小の構成を示しています。VC アップリンクは「VC_LAN_1」という名前の vNet に割り当てられていて、外部の VLAN 1 に相当します。vNet の接続モードは「failover」に設定されています。サーバの NIC はすべてタグなしです。

図 7. Cisco のアクセスポートに接続された VC アップリンク



外部 Cisco スイッチの構成

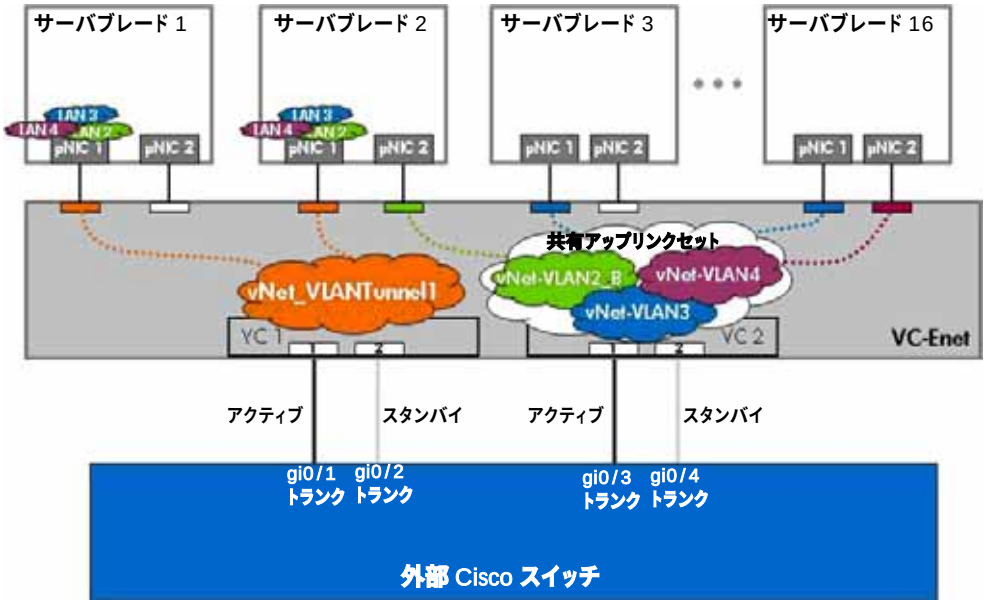
```
interface GigabitEthernet0/1
  description "VC1 Uplink 1"
  switchport mode access
  switchport access vlan 1
  spanning-tree portfast
!
interface GigabitEthernet0/2
  description "VC1 Uplink 2"
  switchport mode access
  switchport access vlan 1
  spanning-tree portfast
!
interface GigabitEthernet0/3
  description "VC2 Uplink 1"
  switchport mode access
  switchport access vlan 1
  spanning-tree portfast
!
interface GigabitEthernet0/4
  description "VC2 Uplink 2"
```

```
 switchport mode access
 switchport access vlan 1
 spanning-tree portfast
```

構成例 2: VC アップリンクを Cisco VLAN トランクポートに接続する

図 8 は、VC と Cisco の VLAN トランキングのシナリオと、Cisco スイッチに必要な最小の構成を示しています。VC-Enet モジュールの VC1 のアップリンクは、「vNet_VLANTunnel1」という名前の vNet に割り当てられていて、この vNet は、ID 2 から ID 4 までの外部 VLAN からサーバ 1 およびサーバ 2(どちらも NIC 1 で VLAN タギングを使用する VMware ESX Server)への 802.1Q トンネルとして機能します。VC-Enet モジュールの VC2 のアップリンクは VLAN トランクポートで、共有アップリンクセットに割り当てられています。共有アップリンクセットは ID 2 から ID 4 までの VLAN が構成されていて、これらはそれぞれ「vNet_VLAN2_B」、「vNet_VLAN3」、および「vNet_VLAN4」に対応しています。サーバ 2 の NIC 2 と、サーバ 3 およびサーバ 16 のすべての NIC はタグなしで、共有アップリンクセットの単一の VLAN に割り当てられています。さらに、共有アップリンクセットおよび vNet_VLANTunnel1 は両方とも接続モードが「failover」に設定されています。

図 8. Cisco の VLAN トランクポートに接続された VC アップリンク



外部 Cisco スイッチの構成

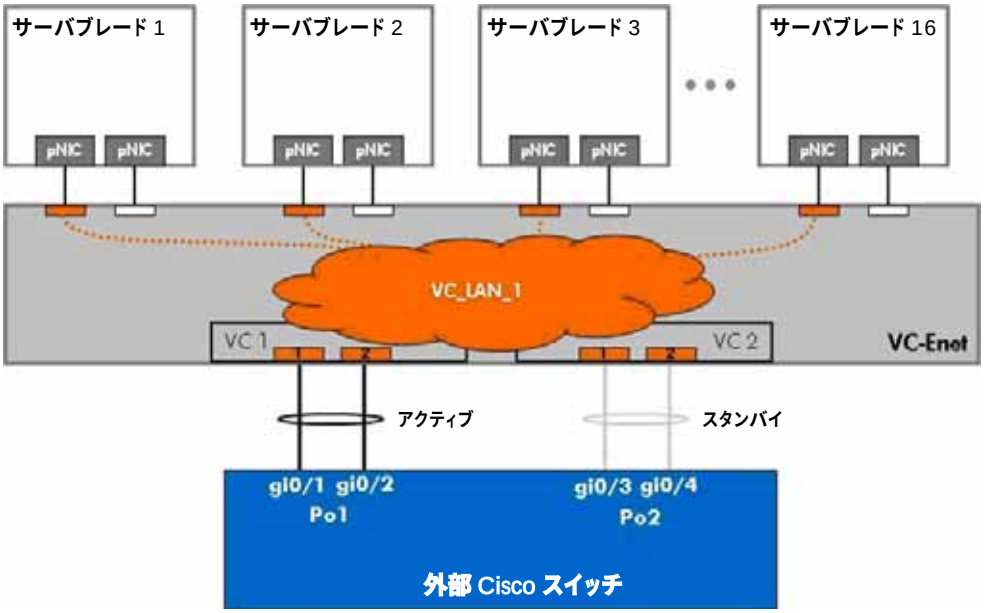
```
interface GigabitEthernet0/1
  description "VC1 Uplink 1, Po1"
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 2,3,4
  witchport mode trunk
  spanning-tree portfast trunk
!
interface GigabitEthernet0/2
  description "VC1 Uplink 2, Po1"
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 2,3,4
  switchport mode trunk
  spanning-tree portfast trunk
!
interface GigabitEthernet0/3
  description "VC2 Uplink 1, Po2"
  switchport trunk encapsulation dot1q
```

```
  switchport trunk allowed vlan 2,3,4
  switchport mode trunk
  spanning-tree portfast trunk
!
interface GigabitEthernet0/4
  description "VC2 Uplink 2, Po2"
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 2,3,4
  switchport mode trunk
  spanning-tree portfast trunk
```

構成例 3: VC アップリンクを Cisco EtherChannel に接続する

図 9 は、VC と Cisco のポートチャネリングのシナリオと、Cisco スイッチに必要な最小の構成を示しています。VC アップリンクは「VC_LAN_1」という名前の vNet に割り当てられていて、外部の VLAN 1 に相当します。vNet の接続モードは「auto」に設定されています。サーバの NIC はすべてタグなしです。

図 9. 2 つの Cisco EtherChannel に接続された VC アップリンク



外部 Cisco スイッチの構成

```
interface Port-channel1
  description "Port Channel to VC1"
  spanning-tree portfast
!
interface Port-channel2
  description "Port Channel to VC2"
  spanning-tree portfast
!
interface GigabitEthernet0/1
  description "VC1 Uplink 1, Po1"
  channel-protocol lacp
  channel-group 1 mode active
  spanning-tree portfast
!
interface GigabitEthernet0/2
  description "VC1 Uplink 2, Po1"
```

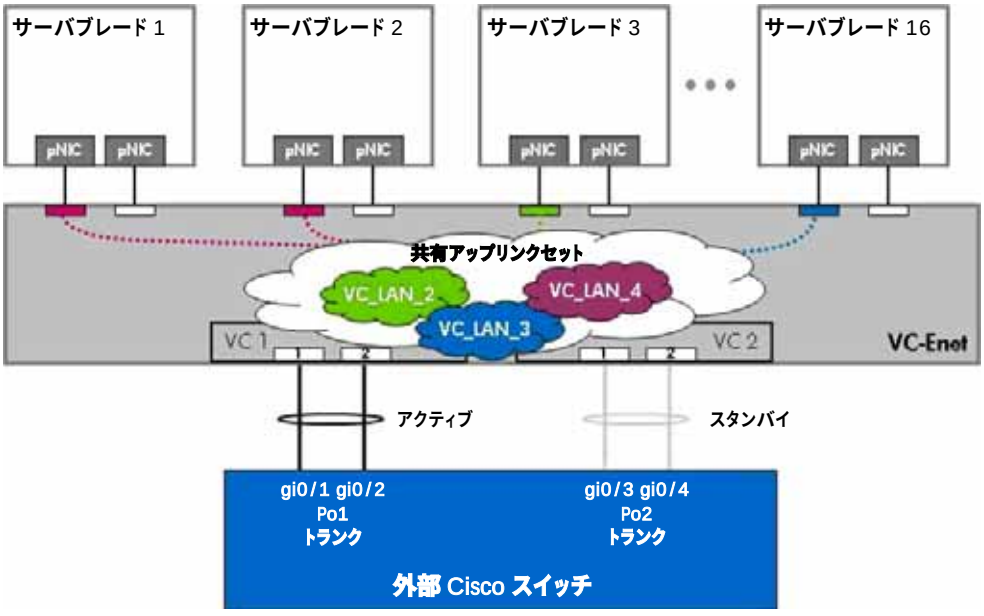
```
  channel-protocol lacp
  channel-group 1 mode active
  spanning-tree portfast
!
interface GigabitEthernet0/3
  description "VC2 Uplink 1, Po2"
  channel-protocol lacp
  channel-group 2 mode active
  spanning-tree portfast
!
interface GigabitEthernet0/4
  description "VC2 Uplink 2, Po2"
  channel-protocol lacp
  channel-group 2 mode active
  spanning-tree portfast
```

注記:
このシナリオでは、PortFast **コマンドはポートチャネルインタフェースでのみ必要で、物理インタフェースには不要です。ただし、ポートチャネルが無効になって、アップリンクが単純なフェイルオーバーモードを使用する場合に備えて、物理インタフェースも含めて** PortFast **コマンドを適用しておくのがベストプラクティスです。**

構成例 4: VC アップリンクを Cisco EtherChannel VLAN トランクに接続する

図 10 **は、**VC **と** Cisco **の** EtherChannel **および** VLAN **トランキングのシナリオと、**Cisco **スイッチに必要な最小の構成を示しています。**4 **つの** VC **アップリンクは** VLAN **トランクポートで、すべて共有アップリンクセットに割り当てられています。共有アップリンクセットは** ID 2 **から** ID 4 **までの** VLAN **が構成されていて、それぞれ「**vNet_LAN2**」、「**vNet_LAN3**」、および「**vNet_LAN4**」に対応しています。サーバの** NIC **はすべてタグなしで、共有アップリンクセットの単一の** VLAN **に割り当てられています。なお、共有アップリンクセットの接続モードは「**auto**」に設定されています。**

図 10. 2 **つの** Cisco EtherChannel **に接続され、**VLAN **トランクでもある** VC **アップリンク**



外部 Cisco スイッチの構成

```
interface Port-channel1
  description "Port Channel to VC1"
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 2,3,4
  switchport mode trunk
  spanning-tree portfast trunk
!
interface Port-channel2
  description "Port Channel to VC2"
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 2,3,4
  switchport mode trunk
  spanning-tree portfast trunk
!
interface GigabitEthernet0/1
  description "VC1 Uplink 1, Po1"
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 2,3,4
  switchport mode trunk
  channel-protocol lacp
  channel-group 1 mode active
  spanning-tree portfast trunk
!
interface GigabitEthernet0/2
  description "VC1 Uplink 2, Po1"
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 2,3,4
  switchport mode trunk
  channel-protocol lacp
  channel-group 1 mode active
  spanning-tree portfast trunk
!
interface GigabitEthernet0/3
  description "VC2 Uplink 1, Po2"
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 2,3,4
  switchport mode trunk
  channel-protocol lacp
  channel-group 2 mode active
  spanning-tree portfast trunk
!
interface GigabitEthernet0/4
  description "VC2 Uplink 2, Po2"
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 2,3,4
  switchport mode trunk
  channel-protocol lacp
  channel-group 2 mode active
  spanning-tree portfast trunk
```

注記:
このシナリオでは、「PortFast Trunk」コマンドおよびトランキングコマンドはポートチャネルインタフェースでのみ必要で、物理インタフェースには不要です。ただし、ポートチャネルが無効になって、アップリンクが単純なフェイルオーバーモードを使用する場合に備えて、物理インタフェースもポートチャネルインタフェースと同じように構成しておくのがベストプラクティスです。

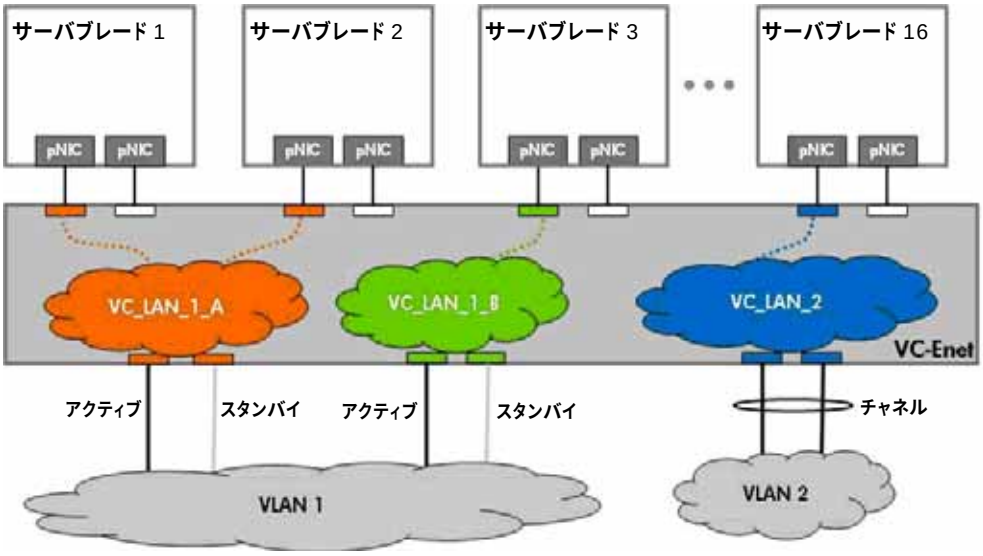
高度なバーチャルコネクトイーサネット設計

バーチャルコネクトに vNet を実装することで、管理者は多岐に渡る複雑なネットワーキングの設計に対処するための創造的なソリューションを実装することができます。通常、vNet は単一の VLAN を表しますが、バーチャルコネクトドメイン内では複数の vNet で単一の VLAN を表すことができます。同じ VLAN に別々の vNet を使用することによって、管理者はサーバの NIC 単位でトラフィックフローを制御することができます。以下にいくつか例を示します。

高度な VC-Enet の設計: 設計例その 1

図 11 に示すように、管理者は 1 つの vNet (VC_LAN_1_A)を使用して、サーバ 1 の NIC とサーバ 2 の NIC を、VLAN 1 に割り当てられている外部スイッチポートに接続する VC アップリンクに結合することができます。この場合、VC ドメイン内で VC_LAN_1_A は VLAN 1 に相当します。サーバ 1 およびサーバ 2 は VC_LAN_1_A 内では直接対話ができ、VC ドメインから出る必要はありません。またどちらのサーバも、アクティブな VC アップリンクポートを経由して、VLAN 1 上にあるデバイスと対話できます。さらに、管理者は別の vNet (VC_LAN_1_B)を作成して、サーバ 3 をこれに割り当てることができます。VC_LAN_1_B に割り当てられた NIC ポートがないため、バーチャルコネクトは、サーバ 3 の NIC ポートが VC ドメイン内の他の NIC ポートと直接対話することを許可しません。VC_LAN_1_B も VC ドメイン内では VLAN 1 を表しています。サーバ 3 は実質的に、VLAN 1 に接続するための専用 VC アップリンクを持つことになります。外部のスイッチドネットワークが許可する場合、サーバ 3 は VC_LAN_1_B のアクティブなアップリンクを通って VC ドメインを出て、外部 Cisco スイッチを通過し、VC_LAN_1_A のアクティブなアップリンクから VC ドメインに再び入ることで、サーバ 1 およびサーバ 2 と通信できます。

図 11. vNet のさまざまな使用を示す VC ドメイン



(上の図の要素については、付録 A の説明を参照)

高度な VC-Enet の設計: 設計例その 2

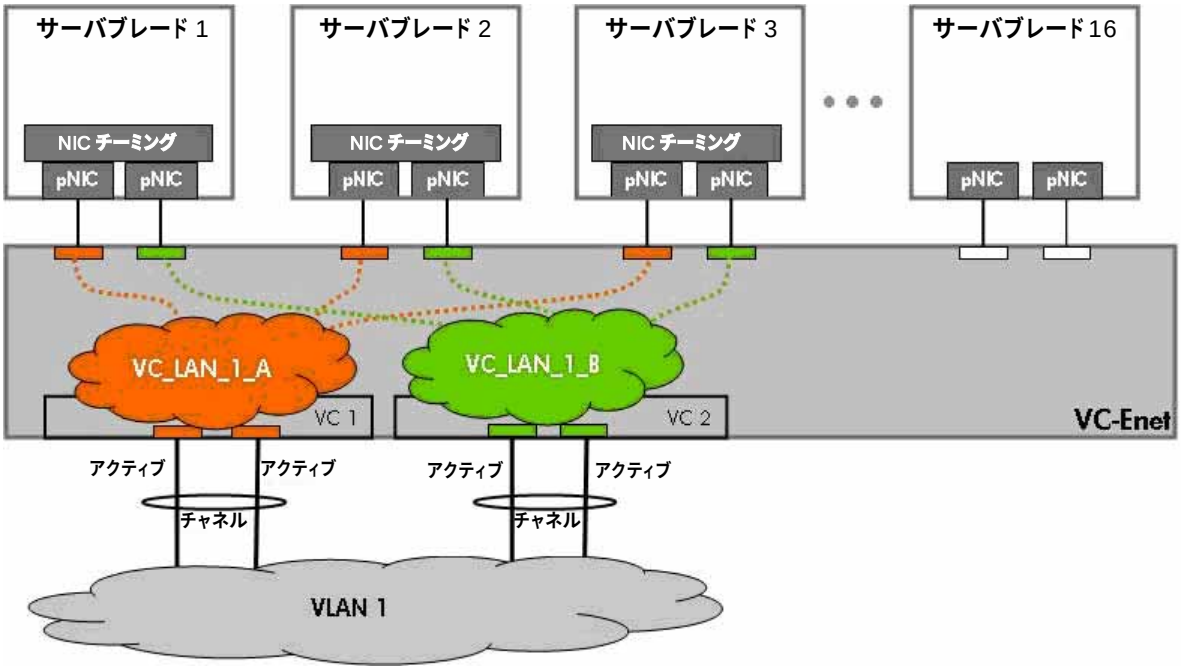
vNet を使用した高度な構成の別の例を、図 12 で示します。図 12 で、サーバブレード 1 から 3 は外部ネットワークと 4Gb の通信経路で接続する必要があります。しかし、別々の VC モジュールのポートを使用して、単一点障害を排除する必要があります(リダンダント VC モジュール)。モジュール 1 の 2 つのアップリンクポートとモジュール 2 の 2 つのアップリンクポートが同じ vNet に割り当てられている場合、VC は 2 つのポートチャネル(2 つの論理パス)を構成します。「VC アップリンクのロードバランシング」の項で説明したように、VC はネットワークのループを防ぐ必要があるため、同時にアクティブになるのは 1 つの論理パスだけです。したがって、1 つのチャネル全体がスタンバイモードになるため、サーバの帯域幅は 4 Gb から 2 Gb に低下します。

この問題を解決するには、1 つでなく 2 つの vNet を使用します。それぞれの vNet には、単一のポートチャネルを構成する複数のアップリンクポートが割り当てられます。それぞれの vNet は単一のポートチャネルだけを持つため、vNet の論理パスは 1 つだけとなって、そのポートチャネルはアクティブになります。その結果、両方のポート

チャネルがアクティブになります。VC は vNet 間をフレームが飛び越えることを許可しないため、ループは生じません。両方のポートチャネルがアクティブとなるため、VC ドメインと VLAN 1 の接続は 4Gb となります(2Gb のポートチャネルが 2 つ)。

両方のポートチャネルを使用するためには、複数のサーバを 2 つの vNet に分けるか、または(図 12 で示すように) NIC チーミングを使用して、各サーバを両方の vNet に接続することもできます。NIC チーミングを使用して各サーバを両方の vNet に接続する場合、NIC チーミングドライバのロードバランシング アルゴリズムによって、データフレームの負荷を各 vNet にどのように均一化するかが制御されます。

図 12. VC ドメインでの vNet および EtherChannel の高度な使用例



(上の図の要素については、付録 A の説明を参照)

高度な VC-Enet の設計: 設計例その 3

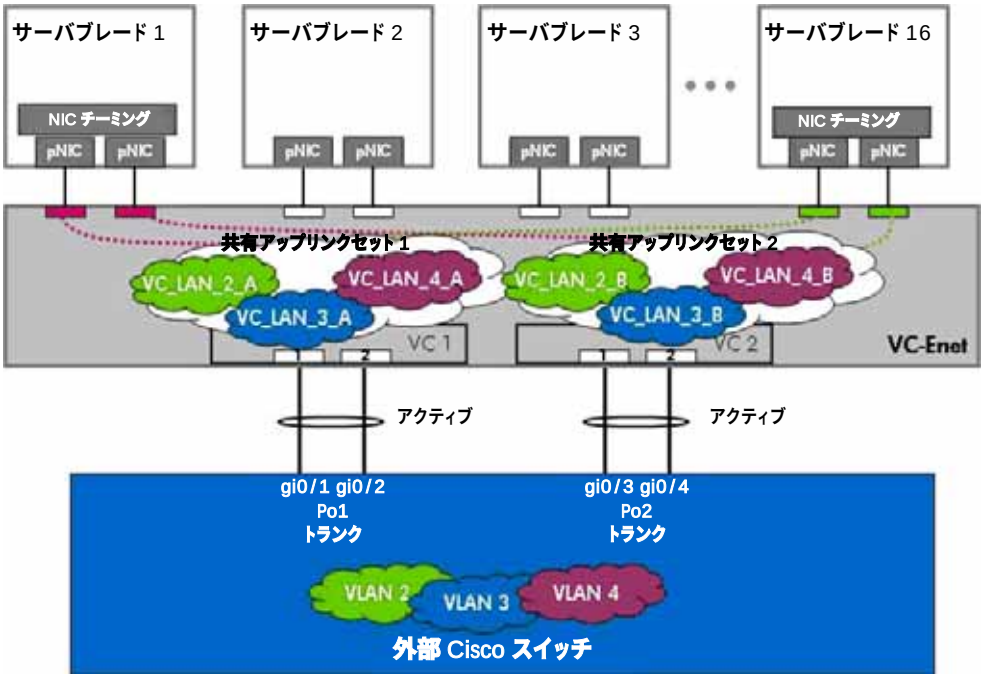
この例では、サーバブレード 1 および 16 は外部ネットワークの異なる VLAN と 4Gb の通信経路で接続する必要があります。しかし、別々の VC モジュールのポートを使用して、単一点障害を排除する必要があります(リダンダント VC モジュール)。モジュール 1 の 2 つのアップリンクポートとモジュール 2 の 2 つのアップリンクポートが同じ vNet に割り当てられている場合、VC は 2 つのポートチャネル(2 つの論理パス)を構成します。「VC アップリンクのロードバランシング」の項で説明したように、VC はネットワークのループを防ぐ必要があるため、同時にアクティブになるのは 1 つの論理パスだけです。したがって、1 つのポートチャネル全体がスタンバイモードになるため、サーバの帯域幅は 4 Gb から 2 Gb に低下します。

この問題を解決するには、1 つでなく 2 つの共有アップリンクセットを使用します。それぞれの共有アップリンクセットには、単一のポートチャネルを構成する複数のアップリンクポートが割り当てられます。それぞれの共有アップリンクセットは単一のポートチャネルだけを持つため、共有アップリンクセットの論理パスは 1 つだけとなって、そのポートチャネルはアクティブになります。その結果、両方のポートチャネルがアクティブになります。VC は同じ共有アップリンクセット内の vNet 間をフレームが飛び越えることを許可せず、また異なる共有アップリンクセットにある vNet 間をフレームが飛び越えることも許可しないため、ループは生じません。両方のポートチャネルがアクティブとなるため、VC ドメインでは、VLAN 2 から VLAN4 へのサーバブレードの接続は、4Gb の共有接続となります (2Gb のポートチャネルが 2 つ)。

両方のポートチャネルを使用するためには、複数のサーバを分けて、それぞれの共有アップリンクセットに関連付けられた vNet に接続するか、または(図 13 で示すように) NIC チーミングを使用して、両方の共有アップリンクセット内で同じ外部 VLAN に相当する vNet にそれぞれのサーバを接続することもできます。たとえば、サーバブレード 1 にある 1 つの NIC は VC_LAN_4_A に、もう 1 つの NIC は VC_LAN_4_B に割り当てられています。チーミン

グされた両方の NIC は VLAN 4 に有効に割り当てられて、両方の論理パス全体でロードバランシングまたはフォールトトレランス、あるいはその両方を同時に提供することが可能になります。NIC チーミングを使用して各サーバを複数の vNet に接続する場合、NIC チーミングドライバのロードバランシング アルゴリズムによって、データフレームの負荷を各 vNet にどのように均一化するかが制御されます。

図 13. VC ドメインでの共有アップリンクセット、EtherChannel、およびタグなしのサーバ NIC の高度な使用例



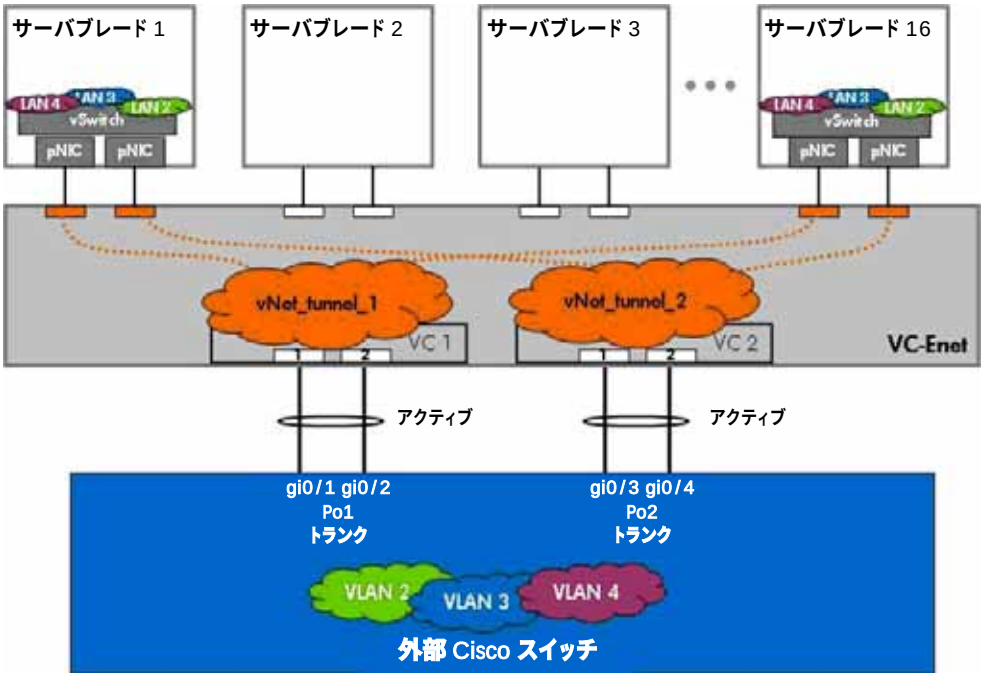
(上の図の要素については、付録 A の説明を参照)

高度な VC-Enet の設計: 設計例その 4

高度な設計の最後の例を図 14 に示します。この図では、2 つの VMware ESX Server(サーバ 1 およびサーバ 16)が、それぞれ 2 つの vNet (vNet_tunnel_1 と vNet_tunnel_2)に接続されています。どちらの vNet もそれぞれ独自の 2Gb ポートチャネル経由で VLAN 2 から VLAN 4 をトンネリングしています。それぞれの VMware ESX Server には VLAN 2 から VLAN 4 までのタグが付けられていて、3 つの VLAN のどれにでも仮想マシン(VM)を割り当てることができます。どちらのポートチャネルもアクティブであるため、NIC ポートをいずれかの vNet に割り当てたサーバブレードに VLAN をトンネリングすることによって、VC ドメインは、サーバブレードを VLAN 2 から VLAN 4 までに接続する 4Gb の共有接続(2Gb のポートチャネルが 2 つ)を提供することになります。

両方のポートチャネルを使用するためには、複数のサーバを分けて、それぞれの共有アップリンクセットに関連付けられた vNet に接続するか、または(図 14 で示すように) NIC チーミング / ボンディングを使用して、各サーバを vNet に接続することもできます。たとえば、サーバブレード 1 の 1 つの NIC ポートは vNet_tunnel_1 に、もう 1 つの NIC ポートは vNet_tunnel_2 に割り当てることができます。どちらの vNet も VLAN 2 から VLAN 4 の 802.1Q トンネルに相当します。また、どちらの NIC ポートも VMware ESX Server の同じ vSwitch に割り当てられています。これによって vSwitch はどちらかの NIC ポートを使用して、アクティブな 2Gb の論理パス経由で任意の VLAN に到達することができます。VLAN 2 から VLAN 4 までは、この VC ドメイン内では 2 つのアクティブな 2Gb ポートチャネル(合計 4Gb)によって表されます。

図 14. VC ドメインでの共有アップリンクセット、EtherChannel、およびタグ付きのサーバ NIC の高度な使用例



(上の図の要素については、付録 A の説明を参照)

同じ外部 VLAN を表す複数の vNet を作成することが管理者にとって必要になる理由を、以下に示します。

- 特定の vNet のアップリンクに接続した Cisco スイッチポートで、特定のポートセキュリティ、QoS、ACL、プライベート VLAN などの設定を適用するため。
  - 設定は VLAN 上の複数のサーバブレード(全部ではない)に適用する必要があるため、同じ設定を必要とするサーバをグループ化するために複数の vNet が使用されます。
- 同じ外部 VLAN または VLAN トランクに対してアクティブ/アクティブの VC アップリンク構成を行うため。
  - VC は 1 つの vNet に対して常に 1 つのアクティブ論理パスのみを許可することによって、ネットワークのループを防いでいます。同じ VLAN に複数の vNet を使用することで、同じ VLAN に複数のアクティブな VC アップリンクを提供しつつ、ネットワークのループを防ぐことができます。
  - 複数のサーバを複数の vNet に分けたり、または NIC チーミングを使用して、サーバを複数の vNet へのデュアルホーム サーバとしたりすることができます。

VCとVMwareネットワーキングテクノロジの比較

バーチャルコネクトが LAN 上でどのように動作するかを理解する 1 つの方法として、バーチャルコネクトのネットワーキングコンポーネントとその機能を VMware ESX Server のネットワーキングコンポーネントと比較することがあります。VMware ESX Server で使用されているネットワーキングテクノロジは一般に理解されていて、多くのお客様に受け入れられているため、VC と VMware ESX Server との間の多くの類似点を理解することは、バーチャルコネクトが外部ネットワークからどのように見え、またどのように動作するかについてより深く理解するのに役に立ちます。混乱を避けるために付け加えておきますが、バーチャルコネクトと VMware ESX Server は根本的に異なる製品であり、データセンター内での全く異なるニーズに対処するものです。この比較は、あくまでもバーチャルコネクトをより深く理解する目的で、ネットワーキングテクノロジに関する 2 つの製品の類似点を理解するためのものです。

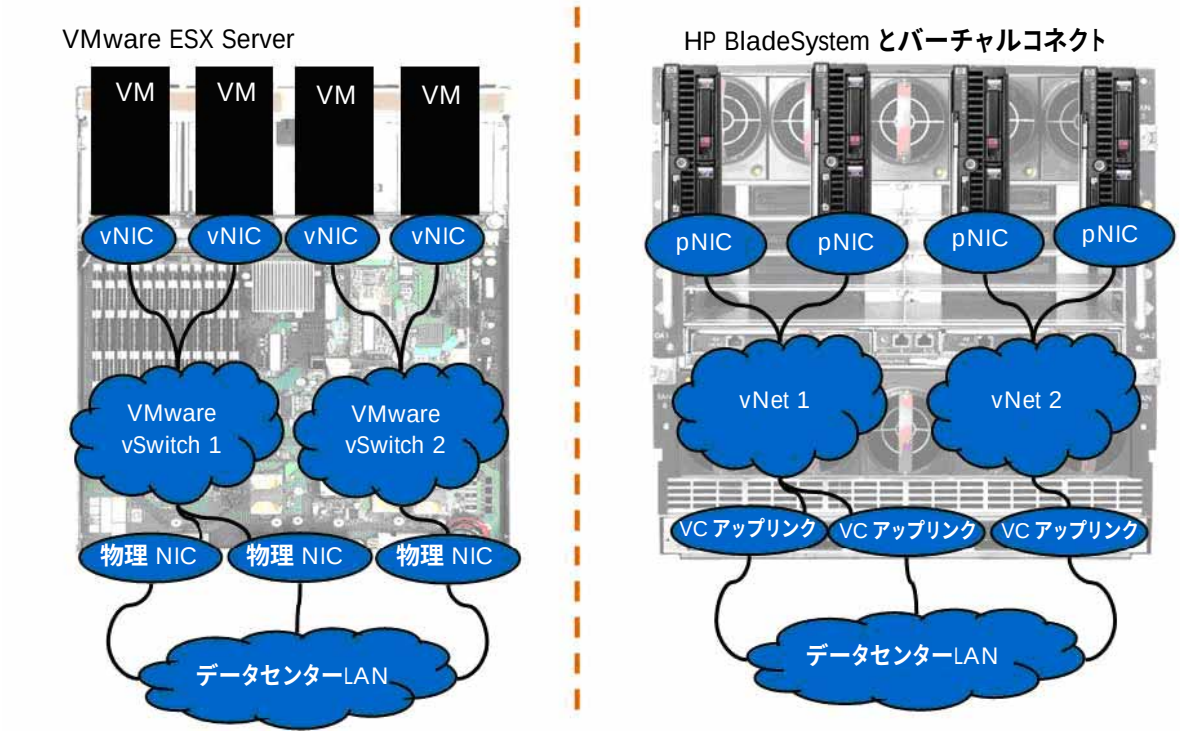
VMwareコンポーネントの説明

図 15 の左側に示すように、VMware ESX Server とは、仮想マシン(VM)と呼ばれる仮想サーバの 1 つまたは複数のインスタンスを物理サーバ上でホスト可能にするための、サーバ仮想化ソフトウェア(VMware)を実行する単一の物理サーバです。また VMware ESX Server は、vSwitch と呼ばれるレイヤ 2 ブリッジを仮想的に(ソフトウェアで)実装したものを使用して、複数の内部サーバ(VM)に対して外部ネットワーク接続を提供しています。VM の仮想 NIC (vNic)は vSwitch の 1 つに割り当てられ、vSwitch が VMware ESX Server 上の I/O スロットにある実際の物理 NIC に割り当てられます。vSwitch は外部ネットワーク接続を提供するために、自身に割り当てられた 1 つまたは複数の物理 NIC (アップリンク)を持つことができます。複数の物理 NIC が同じ vSwitch に割り当てられている場合、その vSwitch に割り当てられた内部サーバ(VM)に、ネットワークの冗長性またはロードバランシング、あるいはその両方が提供されます。これにより物理 NIC は、それぞれの物理 NIC を経由して外部ネットワークと通信している VM の数によって、1 つまたは複数の MAC アドレスを外部ネットワークに提示します。

VCコンポーネントの比較説明

図 15 の右側に示すように、c-Class エンクロージャとは、サーバブレードと呼ばれる 1 つまたは複数の実際の物理サーバをホストする、単一の物理エンクロージャです。また c-Class エンクロージャは、バーチャルコネクト イーサネット ネットワーク(vNet)と呼ばれるレイヤ 2 ブリッジをハードウェアで実装したものを使用して、複数の内部サーバ(サーバブレード)に対して外部ネットワーク接続を提供しています。サーバブレードの物理 NIC (pNic)がいずれか 1 つの vNet に割り当てられ、vNet が c-Class エンクロージャ上の I/O ベイにある VC-Enet モジュールの実際の物理アップリンクポートに関連付けられます。vNet は外部ネットワーク接続を提供するために、自身に割り当てられた 1 つまたは複数の VC アップリンクを持つことができます。複数の VC アップリンクが同じ vNet に割り当てられている場合、その vNet に割り当てられた内部サーバ(サーバブレード)に、ネットワークの冗長性またはロードバランシング、あるいはその両方が提供されます。これにより VC アップリンクは、それぞれの VC アップリンクを経由して外部ネットワークと通信しているサーバブレードの数によって、1 つまたは複数の MAC アドレスを外部ネットワークに提示します。

図 15. VMware ESX Server とバーチャルコネクト エンクロージャの比較



コンポーネントとその機能を比較すれば、なぜ多くのお客様が、バーチャルコネクトを設置した c-Class エンクロージャを 1 つの VMware ESX Server と同じように扱うかがはっきり分かります。言い換えると、VC を使うことで、ネットワークに対してエンクロージャ全体をあたかも大きな VMware ESX Server のように見せることができるということです。ネットワークの冗長性およびロードバランシング、セキュリティ、ポート監視などの側面から見て、VC はエンクロージャ全体についてのネットワーク接続を簡素化し、エンクロージャ全体を 1 つの VMware ESX Server のように動作させます。

ネットワーキングテクノロジの観点から 2 つの製品が似ていることを再確認するために、類似点を並べた表を以下に示します。

表 2. ネットワーキングテクノロジにおける VC と VMware との類似点

	VMware	バーチャルコネクト
複数のサーバにネットワーク接続を提供する	✓ (仮想)	✓ (物理および仮想)
リダンダントな外部接続を内部サーバに提供する	✓	✓
負荷を均一化した外部接続を内部サーバに提供する	✓	✓
外部ネットワークから複数の MAC アドレスが pNIC (VMware)または VC アップリンク上に見える	✓ (VM から)	✓ (サーバブレードから)

内部サーバを別々のレイヤ 2 ドメイン(ブロードキャストドメイン)に隔離するように構成できる	✓	✓
内部サーバを直接通信するように構成できる	✓	✓
pNIC/ VC アップリンクをポートトランク(EtherChannel)として構成できる	✓	✓
pNIC/ VC アップリンクを VLAN トランクとして構成できる	✓	✓
BPDU を外部ネットワークに転送しない	✓	✓
データセンターのスパニングツリーに参加しない	✓ (内部ループ防止機能を使用)	✓ (内部ループ防止機能を使用)
仮想(ソフトウェア)コンポーネントを使用して、内部サーバと外部ネットワークの間でフレームを受け渡す	✓	×
ハードウェアコンポーネントを使用して、内部サーバと外部ネットワークの間でフレームを受け渡す	×	✓
オペレーティングシステムに依存しない	×	✓
Itanium プラットフォームと x86 プラットフォームの両方をサポートする	×	✓

バーチャルコネクトのループ防止テクノロジ

バーチャルコネクトのループ防止テクノロジは、前述の「VC と VMware ネットワーキングテクノロジの比較」の項で説明した内容に基づいて説明すると、最も分かりやすくなります。VC のループ防止テクノロジは、ProLiant サーバで使用されている NIC チーミング/ボンディング テクノロジとたいへん良く似ています。

VMware と VC を比較した図 15 に戻ってみると、VMware ESX Server は NIC ボンディングテクノロジを使用して、ロードバランシングまたはフォールトトレランス、あるいはその両方を vSwitch 1 およびこれに関連する VM に提供しています。vSwitch 1 はデータセンターの LAN にリダンダント接続されていますが、ループは構成されていません。さらに、VMware ESX Server とデータセンターの LAN との間のループを防ぐためのスパニングツリーも必要ありません。その代わり、VMware ESX Server の NIC ボンディングテクノロジによって、1 つの論理パス(1 つの NIC ポート、または 1 つのチャネルグループ/ポートトランク)だけが同時にアクティブになるように許可することで、ネットワークのループを防いでいます。これと比較すると、VC アップリンクも同じ方法でループを防ぎます。つまり、バーチャルコネクトネットワーク(vNet)の単位に基づいて、各 vNet は同時に 1 つのアクティブな論理パスだけを許可することで、データセンターの LAN でのループを防ぎます。

vNet に関連付けられた VC アップリンクポートの動作は、vSwitch に関連付けられた NIC ポートと比較できます。どちらの場合でも、データセンターの LAN でのループを防ぐためのスパニングツリーは必要ありません。その代わりに、いずれの場合でも、常に 1 つのアクティブ論理パスのみを許可する「ポートボンディング」テクノロジを使用します。

バーチャルコネクト イーサネットモジュールのスタッキング

バーチャルコネクトでは、任意の VC イーサネットモジュール上の任意の VC アップリンクが、任意のサーバダウンリンクのための外部接続を提供するように管理者が構成できます。また VC は、任意の VC イーサネットモジュール上のどのサーバダウンリンクの組み合わせの間ででも接続できるように構成できます。バーチャルコネクトでは、VC イーサネットモジュール間で「スタッキングリンク」を使用することで、この柔軟な接続機能を提供しています。

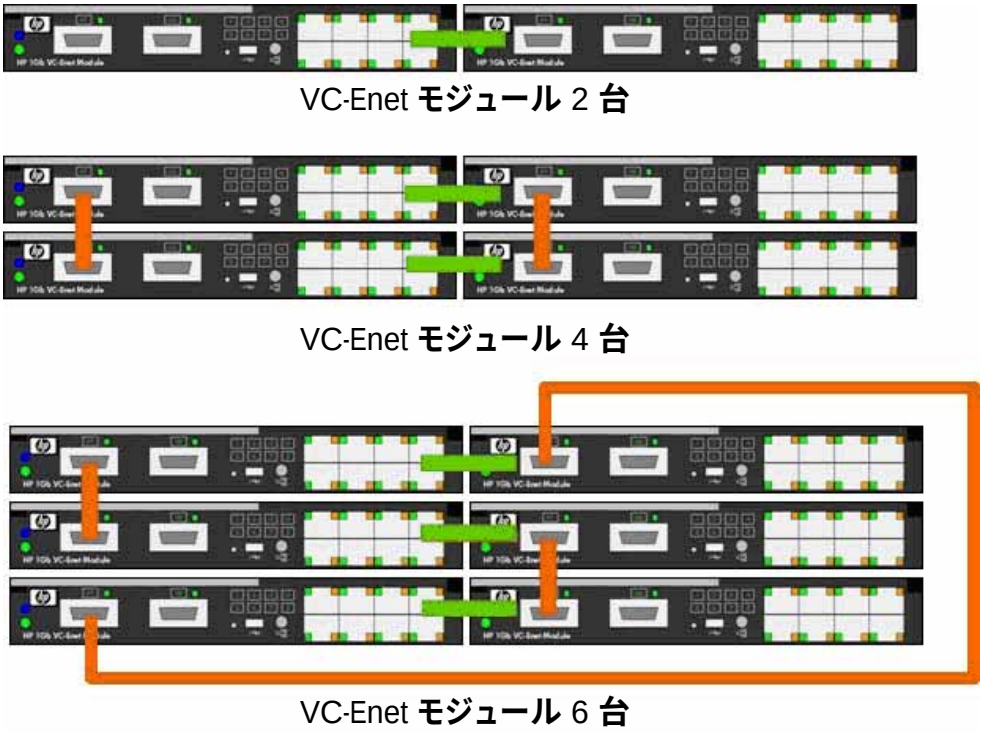
スタッキングリンクによって、VC ドメイン内のすべての VC イーサネットモジュールが 1 つのデバイスとして構成され、そのように動作させることができます(ポートチャネリングは除く)。スタッキングリンクは、サーバ NIC のチームに対する PCI バスの関係と同じく、VC イーサネットモジュールのグループに対して、すべてのデバイスを一体として一緒に動作させることができる共通の通信パスとなります。

同じ VC ドメインにある、いずれか 2 つのバーチャルコネクト イーサネットモジュールが、1Gb または 10Gb ポートを使用して相互に直接接続されると、2 つのモジュールは LLDP を使用して、そのリンクをスタッキングリンクとして自動ネゴシエーションを行います。アップリンクをスタッキングリンクにするための手動での構成は不要です。2 つの VC アップリンクを接続するだけです。

次の図で、緑色の水平の線は、水平方向に隣接する VC モジュールの間にデフォルトで存在する内部スタッキングリンクを表しています。オレンジ色の垂直の線は外部スタッキングリンクを表しており、HP では 10Gb または 1Gb のポートを使用して配線することを推奨しています。次の図で示す推奨最小構成は、それぞれの VC イーサネットモジュールにスタッキングリンクの冗長性を提供するものです。

注記:
スタッキングリンクは、同じバーチャルコネクトドメイン内のすべてのバーチャルコネクト イーサネットモジュールで必須となります。

図 16. VC スタッキングリンクの推奨最小構成



バーチャルコネクトのスタッキングリンクの最適化

バーチャルコネクトのスタッキングリンクは、ダウンリンク(サーバの NIC ポート)と VC アップリンクの間の物理パスを提供します。つまり、フレームが経由しなければならない VC アップリンクが少ないほど、フレームが外部ネットワークに到達する上で生じるレイテンシが少なくなります。フレームが経由しなければならない VC モジュールが 1 つ増えるごとに、フレームのレイテンシが約 3.8 マイクロ秒加算されます。ホップごとにレイテンシが加算されるため、管理者は図 16 で示す推奨最小構成にスタッキングリンクの追加が必要だと思うかもしれません。

vNet または共有アップリンクセット単位で見ると、アクティブなアップリンク(またはポートチャネル)を持つ VC-Enet モジュールは、すべてのサーバフレームが外部ネットワークに向かって VC ドメインを出るために使用するモジュールです。たとえば、サーバの NIC ポート(vNet1 に割り当てられている)が VC-Enet モジュール 2 に接続していて、vNet1 のアクティブなアップリンクが VC-Enet モジュール 6 に接続されている場合、モジュール 2 は最短のスタッキングリンクパスを経由してフレームをモジュール 6 に送信します。図 16 で示すようなスタッキングリンクを使用してモジュールがスタッキングされている場合、モジュール 2 はモジュール 5 へのスタッキングリンクを経由したモジュール 6 へのパスを使用します。次にモジュール 5 は直接接続された内部スタッキングリンクを使用してモジュール 6 にフレームを伝送し、アップリンクを経由して外部ネットワークにフレームを送出します。モジュール 2 は、モジュール 5 を経由する短いパスが失われた場合、モジュール 1、モジュール 3、モジュール 4、モジュール 6 の順に通る長いパスを使用できます。

管理者は意図的にスタッキングリンクを追加して、モジュール間のスタッキングリンクのパスを短くすることもできます。上のシナリオを使用した例では、管理者はモジュール 2 とモジュール 6 の間にスタッキングリンクを追加できます。追加すると、モジュール 2 はモジュール 6 に直接接続されたスタッキングリンクを使用して、モジュール 6 のアクティブなアップリンクにフレームを送信することができます。各モジュールのレイテンシは 3.8 マイクロ秒ときわめて低いため、スタッキングリンクを意図的に追加することはあまり一般的ではありません。

VCが管理するMACアドレス

バーチャルコネクトで提供されている多くの機能の 1 つに、サーバブレードの MAC アドレスを「管理」する機能があります。厳密に言えば、バーチャルコネクトはサーバブレードの MAC アドレスを「管理」するのであって、「仮想化」するわけではありません。MAC アドレスを「仮想化」することと MAC アドレスを「管理」することとの違いについては、多くの VC 実装担当者にはあまりよく知られていません。

「仮想化された」MAC アドレスとは、実際には物理 NIC に所有も使用もされていない MAC アドレスです。多くの場合、仮想化された MAC アドレスとは、物理 NIC の実際の MAC アドレスをサーバから認識させずに置換する MAC アドレスです。つまり、サーバは X という MAC アドレスでネットワークと通信していると認識していますが、実際の MAC アドレス X は何らかのデバイスによって仮想 MAC アドレス Y に置換されます。この種の実装方法では、MAC アドレス管理の多くの利点が失われます。

「管理された」MAC アドレスとは、実際に物理 NIC に所有され、使用されている MAC アドレスです。サーバはただ単に管理者によって、特定の物理 NIC ポートの特定の MAC アドレスを使用するように割り当てられています。この管理された MAC アドレスは事実上、工場出荷時に物理 NIC に書き込まれた MAC アドレスとしてサーバに認識されます。

VC が管理する MAC アドレスには、以下の利点があります。

- **「見た目どおり」(サーバ上に)あるものが実際に(ネットワーク上で)得られる**

  サーバが MAC アドレスだと認識するものと、外部ネットワークがサーバの MAC アドレスだと認識するものとの間に差異がありません。これによってネットワークに関連する問題のトラブルシューティングが大幅に簡素化されます。

- **サーバアプリケーションのライセンス設定がハードウェアの変更後も維持される**

  多くのサーバアプリケーションのライセンス付与メカニズムでは、サーバの MAC アドレスをキーオフできます。サーバの MAC アドレスが(故障した NIC の交換、別の物理サーバでのサーバイメージのブートなどにより)変更されると、アプリケーションのライセンスを新しい MAC アドレスを使用して再度ライセンス付与しなければならない場合があります。仮想化された MAC アドレスではこの問題を防ぐことができません。しかし VC では管理された MAC アドレスを使用することによって、サーバイメージはそれがどの物理サーバで実行されているかに関係なく、VC が管理する MAC アドレスを常に参照するため、この問題を防止できます。

- **ネットワークデバイスのパフォーマンスに影響しない**

  仮想化されたMACアドレスでは、ネットワークデバイス(スイッチなど)が、サーバが送信するすべてのフレームを操作して、サーバの MAC アドレスを仮想化された MAC アドレスに置換することが必要になる場合があります。さらに、送信元の MAC アドレスがネットワークデバイスによって編集されると、ネットワークデバイスによってフレームのチェックサム(CRC)を再計算する必要があります。サーバが送信するフレームが多いほどネットワークデバイスの処理が増えるため、ネットワークデバイスのパフォーマンスに影響が出る可能性があります。一方、VC では管理された MAC アドレスを使用するため、サーバは管理された MAC アドレスを使用して送信します。ネットワーク上のどのデバイス(VC またはスイッチ)についても、サーバのフレームを操作する必要はありません。その結果、ネットワークのパフォーマンスに一切影響しません。

VC が管理する MAC アドレスを持つサーバブレードがエンクロージャから取り外されると(またはエンクロージャにある状態のサーバブレードから VC のサーバプロファイルが割り当て解除されると)、サーバブレードは工場出荷時に物理 NIC に書き込まれた実際の MAC アドレスに自動的に戻ります。これによって、サーバブレードをデータセンター内であちこち移動した場合に生じる、ネットワーク上での MAC アドレスの重複に関連する問題を防ぎます。

Virtual Connect Manager (VCM)では、サーバブレードの MAC アドレスを管理するための、ドメイン全体を対象とした以下の 3 つの選択肢があります。

- **静的、工場出荷時のデフォルトの MAC アドレス**

  名前が示すように、この設定ではサーバの MAC アドレスを管理しないようバーチャルコネクトに指示します。サーバは、工場出荷時に書き込まれた元の MAC アドレスだけを使用します。

- **ユーザー定義の MAC アドレス**

  この設定では、バーチャルコネクトがサーバブレードに割り当てるのに使用するローカルに管理された MAC アドレスの範囲を管理者が定義できます。

- **HP の定義済み MAC アドレス(推奨)**

  この設定では、HP が予約した MAC アドレスプールからサーバの MAC アドレスを割り当てるようにバーチャルコネクトに指示します。このオプションでは、1024 個の MAC アドレスが入った 64 の範囲から 1 つを管理者が選択できます。

さらに、ユーザー定義または HP の定義済みのいずれかの設定をドメイン全体のデフォルト設定として使用しているとき、工場出荷時の MAC アドレスを代わりに使用するよう選択することによって、個々の VC サーバプロファイルがドメイン全体の設定を上書きできるオプションもあります。

VC が管理する MAC アドレスについては、以下の点が重要です。

- VC はサーバブレード上にある物理 NIC ポートの MAC アドレスのみを管理します。VC は物理サーバ上で実行できる仮想サーバで使用される MAC アドレスは管理しません。
- サーバがエンクロージャから取り外されたり、VC サーバプロファイルがサーバに適用されない場合、サーバの MAC アドレスは工場出荷時のアドレスに戻ります。
- VC は、ポートあたり複数の MAC アドレスを必要とする多機能アダプタに対応するために、NIC ポート 1 つあたり 2 つの MAC アドレスを生成します。
- VCが管理するMACアドレスプールを管理するための集中データベースが必要なお客様は、Virtual Connect Enterprise Managerの使用をご検討ください。詳細はhttp://www.hp.com/jp/vcemを参照してください。

スパニングツリー

バーチャルコネクトは外部の Cisco ネットワークからは別の「イーサネットスイッチ」として見えないため、これら 2 つの製品について語るとき、「スパニングツリーの相互運用性」のテーマは論点にはなりません。言い換えると、1 つのサーバ(複数の NIC を持つもの)がスパニングツリーを構成する必要がないのと同じように、バーチャルコネクト(複数のアップリンクを持ち、それらが外部の Cisco ネットワークには複数の NIC のように見える)もスパニングツリーを構成する必要はありません。つまり、VC のアップリンクポートは STP BPDU (スパニングツリー構成フレーム)を送信または受信せず、マルチホームサーバが外部スイッチドインフラストラクチャによる STP の実装環境を妨害できないのと同様にこれを妨害できないため、ネットワーク管理者は VC と Cisco の間での STP 相互運用性の問題を心配する必要はありません。またこれは、PVST+サポート、Rapid Spanning Tree、MST などに関するすべての問題が、バーチャルコネクトの展開の論点とはならないことを意味します。

VC のアップリンクポートをネットワークから見ると、複数の MAC アドレスを持つ「従来どおりの普通のサーバポート」のようにしか見えないため、VC のアップリンクポートに接続する Cisco のダウンリンクポートは、サーバの NIC ポートに直接接続するのと同じように構成することを HP ではお勧めしています。つまり、Cisco ダウンリンクポートは「アクセス」または「トランク」ポートとして PortFast を有効に設定して構成してください。サーバポートに直接接続する他の Cisco スイッチポートについて BPDUGuard をふだん有効にしているお客様については、BPDUGuard を有効にすることも選択できます。以上をまとめると、バーチャルコネクトでは、VMware ESX Server が外部ネットワークと接続するのとほとんど同じように c-Class エンクロージャが外部ネットワークに接続できることを考えると、バーチャルコネクトも VMware ESX Server と同じように、外部ネットワークのスパニングツリードメインに参加しない理由が容易に理解できるということです。

PortFast

スパニングツリーPortFast 機能は、サーバの NIC ポートなどのエッジデバイスに接続する Cisco スイッチポート用に設計されました。この機能によって、Cisco スイッチポートはスパニングツリーの「リスニング」および「ラーニング」ステージを回避して、すぐさま「フォワーディング」ステージに移ることができます。この機能を有効にすることで、スパニングツリーがループを防ぐためにポートをブロックする必要があるか判断するのを待たずに、エッジデバイスはネットワーク通信をすぐに開始することができます(この判断プロセスは、デフォルトのスパニングツリーのタイマーでは 30 秒以上かかることがあります)。エッジデバイスはネットワークにループをもたらすものではないため、ループを防ぐためのスパニングツリーは必要ではなく、PortFast 機能を使用してスパニングツリーを有効に回避できます。この機能の利点は、サーバの NIC ポートが、差し込んでから 30 秒またはそれ以上タイムアウトせずにネットワーク上ですぐに通信できることです。これは PXE および DHCP などの時間の影響を受けやすいプロトコルについては特に便利です。

VC アップリンクはネットワークでは(チーミングされたサーバの NIC のように)エッジデバイスとして動作するため、スパニングツリーは直接接続した Cisco スイッチポートでは必要ありません。つまり、PortFast は VC アップリンクに直接接続した Cisco スイッチポートで有効に設定できるということです。

注記:
PortFast を Cisco のアクセスポートで有効にするインタフェースコマンドは「spanning-tree portfast」です。PortFast を Cisco のトランクポートで有効にするインタフェースコマンドは「spanning-tree portfast trunk」です。

BPDUガード

BPDU ガードは PortFast を有効に設定した Cisco スイッチポートのための安全機能です。BPDU ガードを有効に設定すると、スイッチは PortFast を構成したポートで BPDU フレーム(スパニングツリー構成フレーム)の受信を監視することができます。PortFast および BPDU ガードを有効に設定したスイッチポートで BPDU を受信すると、BPDU ガードはスイッチポートを err-disable (シャットダウン)の状態にします。PortFast を有効に設定したポートは別のスイッチ(BPDU を転送するもの)に接続してはならないため、BPDU ガードは PortFast が有効に設定されたポートが別のスイッチに接続されることを防ぎます。これによって、そのポートでスパニングツリーを回避したことが原因で発生するループを防止し、そのポートに接続したどのデバイスもルートブリッジになりません。

VC はネットワークのエッジデバイスとして動作し、VC はデータセンターのスパニングツリーに参加しない(つまり VC アップリンク上で BPDU を転送しない)ため、BPDU ガードは VC アップリンクに接続された Cisco スイッチポートで必要に応じて使用することができます。

注記:
BPDU ガードを Cisco のポートで有効にするインタフェースコマンドは「spanning-tree bpduguard enable」です。

Unidirectional Link Detection (UDLD)

UDLD は、直接接続された 2 つの Cisco デバイスの間でのみ動作する Cisco の独自機能です。UDLD (UniDirectional Link Detection)の目的は、ループの検出および防止のためにスパニングツリーが使用されている状況で、単一方向のリンクを検出することです。単一方向リンクが検出されない場合、スパニングツリーでループが正しく検出されず、ネットワーク上のループを防ぐためのポートのブロックが行われません。スパニングツリーは VC アップリンクと外部の Cisco スイッチの間では使用しないため、単一方向リンクによってスパニングツリーのループが生じることはありえません。したがって、UDLD は VC アップリンクには不要で、サポートもされていません。

サービス品質(QoS)

バーチャルコネクトの現在のファームウェアバージョンでは、トラフィックの分類、マーキング、または優先順位付けについて、ユーザーが構成できる設定には対応していません。さらに VC では、フレームの優先順位付けにレイヤ 2 のサービス品質マーキング(802.1p Class of Service)もレイヤ 3 のサービス品質マーキング(TOS、DSCP)も使用していません。ただし、サーバと Cisco スイッチの間でのあらゆる展開と同じように、VC アップリンクに接続された Cisco スイッチポートに QoS 設定を適用できます。

サーバブレードの NIC ポートにレイヤ 2 の QoS マーキング(Class of Service)を受信させる必要がある場合、管理者はサーバの NIC ポートを 802.1Q / p トンネリングモードで動作する vNet に割り当てる必要があります。詳細は、前述の「VC アップリンクおよび VLAN トランキング」の項を参照してください。

セキュリティ

ACLとVLAN ACL

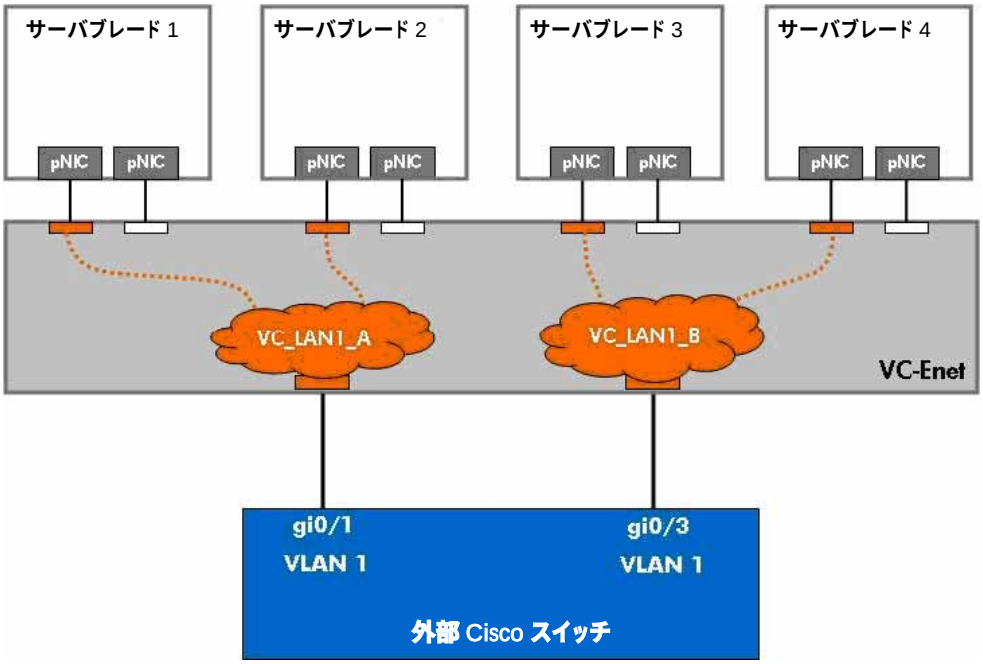
現在のファームウェアバージョンでは、バーチャルコネクトはユーザーが構成できるポートまたは VLAN ACL **をサポートしていません。ただし管理者は、上位の** Cisco **スイッチで構成された** ACL **または** VACL **を利用するように配備した** vNet **を特別に設計することができます。**

たとえば図 17 **の例では、**4 **つのサーバブレードは** 2 **つの異なる** vNet **に分かれていますが、すべて** VLAN 1 **上にあります。どちらの** vNet **のアップリンクポートも、**VLAN 1 **に割り当てられた** Cisco **スイッチポートに接続されているため、どちらの** vNet **も** VC **ドメイン内では** VLAN 1 **に相当します。サーバ** 1 **は** VC **ドメインを出ずにサーバ** 2 **と直接通信できますが、外部** Cisco **スイッチを通過せずにサーバ** 3 **またはサーバ** 4 **と対話することはできません。サーバ** 1 **のトラフィックは、インタフェース** gi0/1 **に接続された** vNet VC_LAN1_A **を経由して** VC **ドメインを出て、**Cisco **スイッチによってインタフェース** gi0/3 **に切り替えられ、**vNet VC_LAN1_B **を経由してサーバ** 3 **に到達します。**

サーバ 1 **のトラフィックは外部** Cisco **スイッチを通過してサーバ** 3 **またはサーバ** 4 **のいずれかに到達する必要があるため、サーバ** 1 **のトラフィックは外部** Cisco **スイッチで構成されているポート** ACL **または** VLAN ACL **の影響を受けます。この場合、管理者は外部** Cisco **スイッチの** VLAN 1 **に** VACL **を適用して、サーバ** 1 **がサーバ** 3 **と通信するのを防ぐ一方で、サーバ** 1 **とサーバ** 4 **との通信を許可できます。**

上記のシナリオは、複雑なネットワーク構成に対応するために管理者が vNet **を創造的に使用できる多くの方法のほんの一例にすぎません。**

図 17. **複数の** vNet **を使用してサーバ間のトラフィックを強制的に外部** Cisco **スイッチを通過させる**



ポートセキュリティ

多くのネットワーク管理者は「ポートセキュリティ」と呼ばれる Cisco スイッチの機能を使用して、ネットワークにセキュリティを追加しています。管理者はこの機能を使って、特定のスイッチポートで学習できる MAC アドレスの数を制御したり、特定の MAC アドレスへの接続を制限したりすることができます。この機能は一般的に、別のハブまたはスイッチがネットワーク接続されることを防ぐため、デスクトップおよびノートパソコンが接続された Cisco スイッチポートで有効にされています。この機能を有効にすることで、管理者はスイッチポートで学習させる MAC アドレスの数が指定した数を超えた場合に、ポートを自動で遮断(err-disable)するように構成できます。許可されていないスイッチまたはハブがポートに接続されると、管理者が許可した数を超える MAC アドレスが学習される可能性があるため、スイッチポートが遮断されます。これによって、許可されていないスイッチまたはハブは、管理者がポートを再び有効化するまで隔離されます。

またポートセキュリティはデータセンターにおいて、サーバの NIC に接続された Cisco スイッチポートにも使用できます。サーバの NIC ポートは通常、1 つの MAC アドレスしか使用しないため、この機能がポートの遮断の原因となることはありません。ただし、VC アップリンクに接続された Cisco スイッチポートでポートセキュリティが有効に設定されていて、管理者が BladeSystem エンクロージャ内のサーバが使用する MAC アドレス数よりも少ない MAC アドレス数を設定すると、ポートセキュリティ機能により Cisco スイッチポートが遮断されることがあります。これによって、BladeSystem エンクロージャは外部ネットワークから隔離されます。

バーチャルコネクトに接続した Cisco スイッチポートでポートセキュリティを使用する必要がある場合、許可する MAC アドレスの数を、エンクロージャ内で使用する MAC アドレスの数以上にする必要があります。将来エンクロージャに追加するサーバや、仮想サーバ(ESX VM など)が使用する仮想 MAC アドレスについても考慮に入れてください。

VC アップリンクに接続した Cisco スイッチポートで特定の MAC アドレスだけが通信できるようにポートセキュリティを構成した場合、管理者はユーザー定義の範囲で HP が管理する MAC アドレスを使用したほうが作業が簡単になることにお気づきになるでしょう。ユーザー定義の範囲に手動で構成したのと同じ範囲の MAC アドレスを許可するようポートセキュリティを構成するだけで済みます。

特定の数の MAC アドレスを許可する場合でも、または特定の MAC アドレスを許可する場合でも、ポートセキュリティを構成するときは、VC アップリンクがフェイルオーバーした後に通信上の問題が起こらないようにするために、同じ vNet (または共有アップリンクセット)に割り当てられたすべての Cisco ポートを、同じポートセキュリティ設定で構成する必要があります。

プライベートVLAN

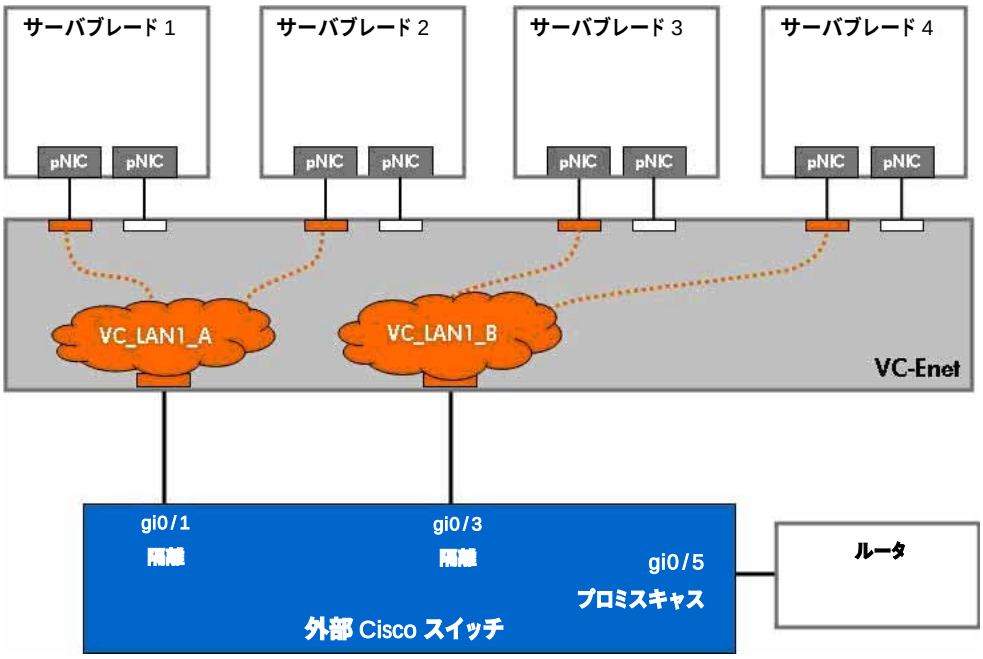
プライベート VLAN (PVLAN)とは、同じ VLAN に割り当てられたスイッチポートを、同じ VLAN 内の別のスイッチポートからレイヤ 2 で隔離することができる Cisco の機能です。この種類の機能の利点は、セキュリティの強化です。たとえば、管理者は同じ IP サブネットを使用して同じ VLAN に複数のサーバを割り当てて、サーバはデフォルトゲートウェイと直接通信することのみを許可し、サーバ相互の通信は許可しないようにすることができます。

VC ファームウェアの現在のリリースでは、バーチャルコネクトは単一の vNet 内でのプライベート VLAN のサポートを実装していません。ただし、管理者がサーバのポートを別々の vNet に割り当てることによって、サーバのポートをレイヤ 2 で完全に分離できます。各 vNet は独立したレイヤ 2 ネットワーク/ブロードキャストドメインです。バーチャルコネクト内部では、vNet 間でのフレームの受け渡しが許可されていません。つまり、お客様は複数の vNet を使用して VC 内でサーバを互いに隔離できるということです。

管理者は複数の vNet を使用して、上位の Cisco スイッチで構成されている PVLAN の機能を拡張することができます。以下の例では、VC の 2 つの vNet と Cisco のプライベート VLAN を使用して 2 つの「コミュニティ」グループと 1 つのプロミスキャスポートが作成されています。4 つのサーバはすべて同じ VLAN (VLAN 1)上にありますが、2 つの異なる vNet (VC_LAN1_A と VC_LAN1_B)に割り当てられているため、VC 内のレイヤ 2 で隔離されています。これら 2 つの vNet は Cisco スイッチにアップリンクされていて、Cisco スイッチでは VLAN 1 がプライベート VLAN として構成されています。VC_LAN1_A に接続されているインタフェース gi0/1 は「隔離」ポートであるため、VC_LAN1_A がルータポート(プロミスキャス)と通信することだけを許可します。また、VC_LAN1_B も VLAN 1 の「隔離」ポートとして構成されたインタフェース gi0/3 に接続されているため、やはりルータとの対話のみが可能です。サーバ 1 とサーバ 2 は VC ドメイン内で相互に直接通信できますが、サーバ 3 やサーバ 4 と通信するためには、どちらも外部 Cisco スイッチを通過する必要があります。その結果、サーバ 1 または 2 からサーバ 3 または 4 へのすべての通信は、外部スイッチでの PVLAN 構成の影響を受けることになります。gi0/1 および gi0/3 が隔離ポートで、gi0/5 がプロミスキャスポートの場合、サーバ 1 およびサーバ 2 は相互の通信とルータとの通信が可能ですが、サーバ 3 またはサーバ 4 との通信はできません。サーバ 3 およびサーバ 4 についても同じことが当てはまり、サーバ相互の通信とルータとの通信は可能ですが、サーバ 1 およびサーバ 2 とは通信できません。VC_LAN1_A および VC_LAN1_B は、どちらも PVLAN による「コミュニティ VLAN」として機能します。

注記: すべてのサーバは同じ VLAN (VLAN 1)上にあり、同じサブネットの IP アドレスを割り当てることができます。

図 18. 複数の vNet を使用して外部 Cisco スイッチの PVLAN 構成を拡張する



(隔離ポート、プロミスキャスポート、およびコミュニティ VLAN についての説明は、Cisco の資料を参照してください)

マルチキャストと IGMP スヌーピング

IGMP スヌーピング機能によって、VC-Enet モジュールがサーバブレードの IGMP メンバーシップアクティビティを監視(スヌープ)して、vNet でのマルチキャストトラフィックの処理を最適化し、ネットワークリソースの使用率を最大化することができます。現在では、IGMP v1 および v2 (RFC2236)のみがサポートされています。

IGMP スヌーピングのアイドルタイムアウト間隔は、デフォルトでは 260 秒に設定されています。この値は、IGMP v2 仕様(RFC2236)で指定されている「グループメンバーシップ間隔(Group Membership Interval)」の値に基づくものです。ネットワークリソースの使用率を最適化するためには、この間隔をネットワークのマルチキャストルータの構成と一致するように設定してください。

デフォルトでは、VC はすべてのマルチキャストグループをプルーニングではなくフラッディングします。特定のマルチキャストグループがサーバの NIC ポートから明示的な join メッセージを受信した場合、そのマルチキャストグループ(およびそのグループのみ)が、join メッセージを転送しないすべてのサーバの NIC ポートに対して排除されます。他のすべてのマルチキャストグループはフラッディングを継続します。

IGMP スヌーピングの構成については、『Virtual Connect User Guide』の説明を参照してください。

SPAN (ポート監視)

バーチャルコネクトは、バーチャルコネクト経由で外部ネットワークに接続されているサーバのネットワーク上の問題に対するトラブルシューティングに役立つポート監視機能をサポートしています。管理者は VC によって、VC ドメインごとにアクティブなポート監視セッションを 1 つ定義できます。

監視セッションには、少なくとも 1 つの「監視ポート」と 1 つの「アナライザポート」を構成する必要があります。「監視ポート」リストはサーバのダウンリンクのリストで、このトラフィックがミラー対象となります。「アナライザポート」は、ネットワークアナライザの接続先となる VC アップリンクポートです。VC は監視ポートのトラフィックをアナライザポートにミラーします。

ポート監視セッションは、最大 16 のサーバダウンリンクのトラフィックをアナライザポートにミラーできます。任意の VC アップリンクをアナライザポートとして定義でき、また任意のサーバダウンリンクを監視ポートとして選択できます。VC イーサネットモジュールには依存しません。

さらに、管理者はミラー対象のトラフィックの方向(サーバが受信、サーバから発信、または両方)を選択することができます。

ロギング

バーチャルコネクトには、VC ドメインイベントおよびタイムスタンプを記録するローカルシステムログが用意されています。ローカルシステムログは編集不能で、手動での消去が許可されていません(セキュリティ目的のため)。ログは循環ログで、バッファが一杯になると古いエントリが除去されます。

一元化されたユーザーアクセス制御(LDAP)

最新バージョンの VC ファームウェアでは、一元化されたユーザーアクセス制御として TACACS+および RADIUS はサポートされていません。VC は現在、LDAP (Lightweight Directory Access Protocol)のみをサポートしています。

LDAP の実装についての詳細は、『Virtual Connect User Guide』を参照してください。

Cisco Discovery Protocol (CDP)

Cisco Discovery Protocol (CDP)は、直接接続された 2 つの Cisco デバイス間でのデバイス ID および機能情報の交換に使用する Cisco 独自仕様のプロトコルです。各 Cisco デバイスは CDP によって、直接接続された他の Cisco デバイスの ID および機能を示す表を管理者に示すことができます。この情報の主な用途の 1 つは、トラブルシューティングです。

バーチャルコネクトは CDP をサポートしていません。VC はデフォルトで LLDP (Link Layer Discovery Protocol)と呼ばれる業界標準プロトコルをサポートしています。LLDP は機能的には CDP と同じですが、これらの 2 つのプロトコルに互換性はありません。多くの Cisco スイッチは LLDP をサポートしています。グローバル構成コマンド「lldp run」およびインタフェースコマンド「lldp transmit」と「lldp receive」は、LLDP をサポートする Cisco スイッチで LLDP を有効に設定するために使用します。実行コマンド「show lldp neighbors」は、LLDP ネイバー情報を Cisco スイッチコンソールに表示します。

バーチャルコネクトは各ポートの統計ページの下部に、各 VC アップリンクについての LLDP ネイバー情報を表示します。

追加リソース

HP サービス:

http://www.hp.com/go/bladesystem/services(英語)

BladeSystem ソリューション:

http://www.hp.com/go/bladesystem/solutions(英語)

Virtual Connect Cookbook:

http://www.hp.com/go/bladeconnect (「Virtual Connect Interest Group」を参照)(英語)

バーチャルコネクトのドキュメント:

http://www.hp.com/go/bladesystem/documentation(英語)

バーチャルコネクトのファームウェア:

http://www.hp.com/go/bladesystemupdates(英語)

HP NIC チーミング(Windows 用)のホワイトペーパー:

http://h50146.www5.hp.com/products/servers/proliant/whitepaper/compaq/whitepaper184.pdf (日本語)

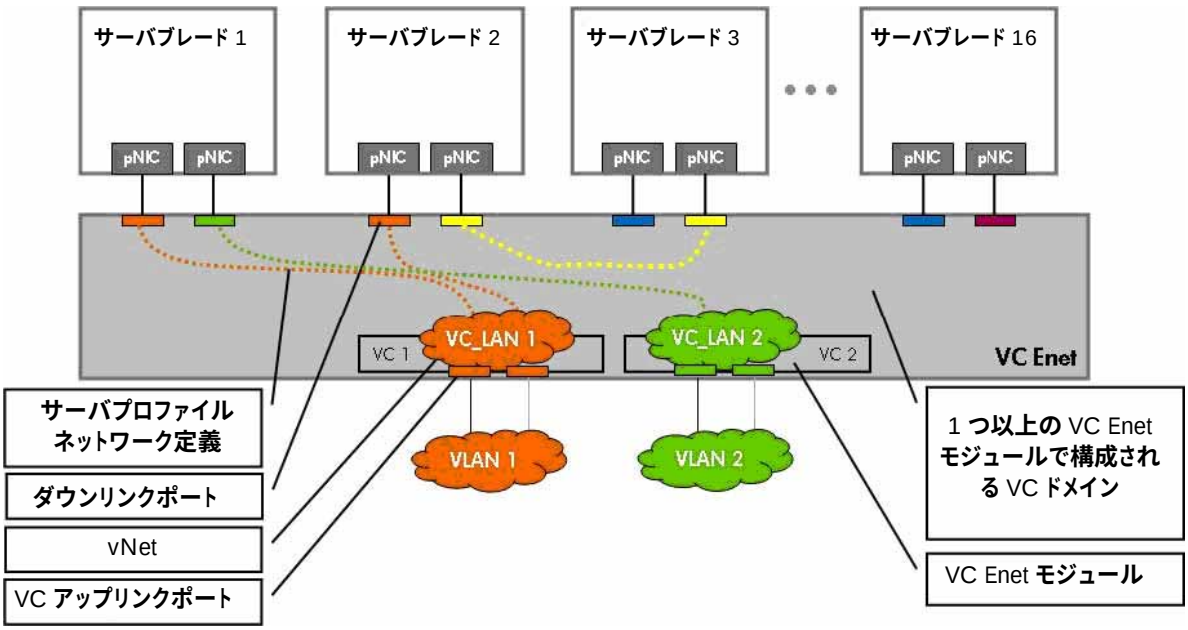
ftp://ftp.compaq.com/pub/products/servers/networking/TeamingWP.pdf(英語)

著者について

M. Sean McGee (CCIE #18040)は、HP BladeSystem Engineering 部門のシニアネットワークアーキテクトです。Sean の HP での職歴は、10 年前に、レベル 3 のサポートグループでスイッチング製品およびルーティング製品をサポートする、Networking Products Division に配属されたときにさかのぼります。彼は長年にわたってデータセンターのネットワーキングテクノロジに自らの専門能力を発揮し、HP のエンジニアリンググループでの最近数年間は、HP ProLiant NIC、HP NIC チーミング、HP BladeSystem イーサネットスイッチアーキテクチャ、および HP BladeSystem バーチャルコネクトの開発を担当しました。HP BladeSystem Engineering 部門の一員である Sean は、新製品の社内ネットワーキングテクノロジ コンサルタントとして、お客様、パートナー、および HP フィールドエンジニアのテクニカルトレーナーとして、および HP BladeSystem 製品を導入するお客様のネットワーク設計コンサルタントとして、多くのエンジニアリンググループとの共同作業に従事しています。

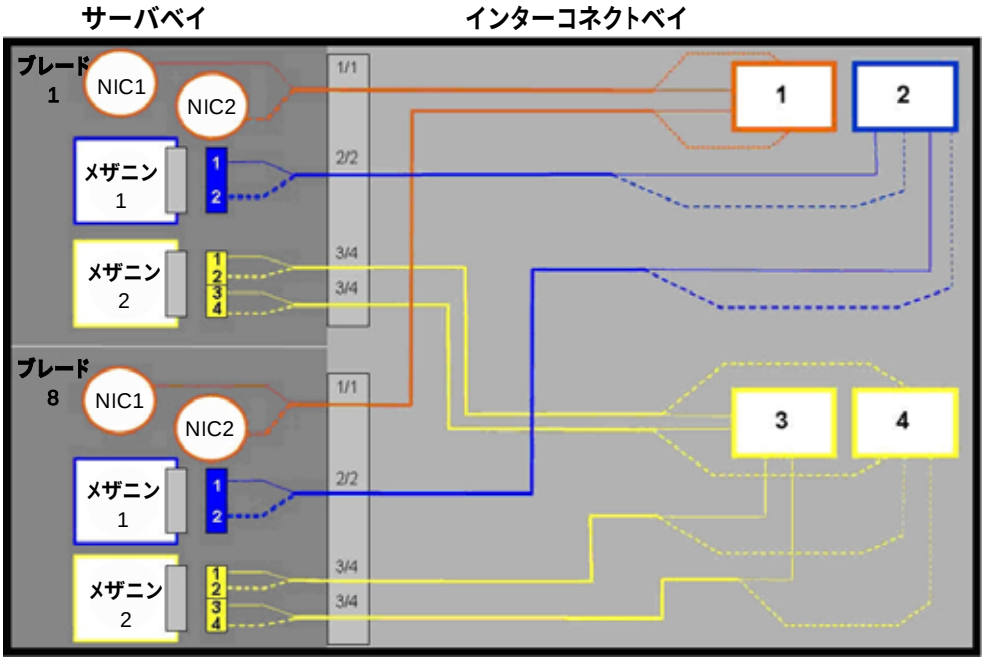
付録

付録A: VCネットワーク図の説明

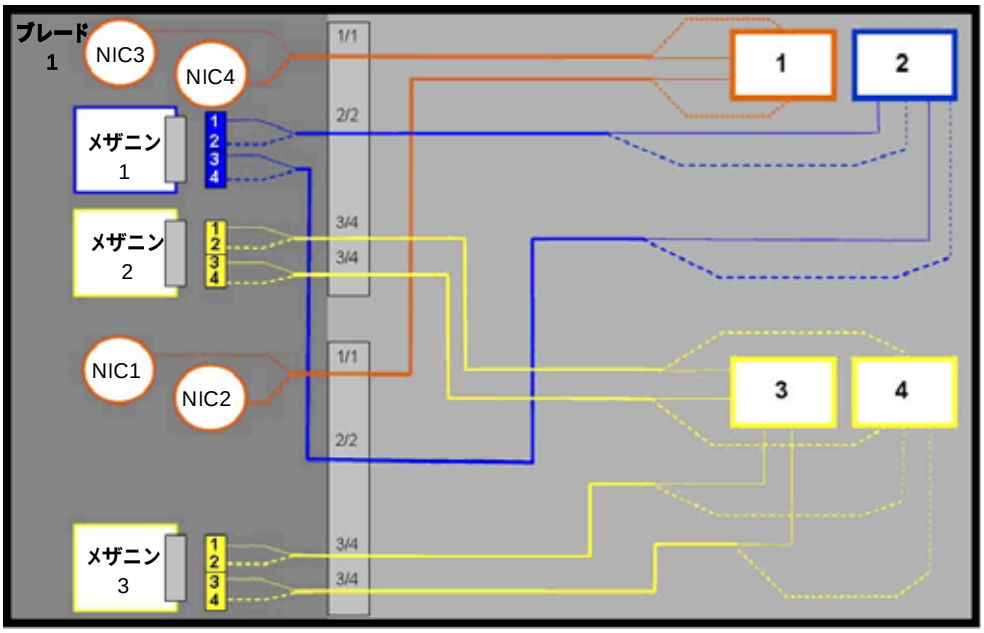


付録B: c3000ポートマッピング図

ハーフハイトサーバ



フルハイトサーバ



付録C: よくある質問

Q1: スタンバイの VC アップリンクポートに多くの破棄フレーム(廃棄フレーム)があるのはなぜですか？

A1: 外部スイッチには、どの VC リンクがアクティブなアップリンクでどれがスタンバイのアップリンクかという概念がありません。外部スイッチから見れば、アップリンクの 1 つが他のものより活発に動作しているということです。つまり、外部スイッチはある種類のフレームをスタンバイリンクに送信し続け、スタンバイリンクはこれを廃棄しているということです。これにはすべてのブロードキャスト、マルチキャスト、および不明なユニキャスト(外部スイッチの CAM テーブルで宛先の参照に失敗したもの)が含まれます。スタンバイリンクで受信されるこれらのフレームはすべて破棄されて、カウンタに反映されます。

Q2: vNet の優先チャネルにするポートチャネルを手動で選択できますか？

A2: いいえ。VC は現在、LACP を有効にした状態(接続モード「auto」)で、vNet (または共有アップリンクセット)の「port role」を設定することをサポートしていません。VC は次の条件に基づいて、どのポートチャネルがアクティブでどれがスタンバイかを決定します。1 – ポートチャネルあたりの動作中のアップリンク数、2 – 各ポートチャネルで提供されている合計帯域幅、3 – 前の 2 つが同じ場合、最も小さい MAC アドレス(TOE タグを参照)を持つ VC モジュールが、アクティブポートチャネルを提供します。この情報を使用して、管理者はメインのポートチャネルにアップリンクを 1 つ追加して構築し、これを優先ポートチャネルとして設定することができます。

Q3: 同じポートチャネルの両側では同じロードバランシング アルゴリズムを使用する必要がありますか？

A3: いいえ、ポートチャネルのそれぞれの側で別のロードバランシング アルゴリズムを使用することができます。

Q4: ネットワークトレースアナライザを VC アップリンクポートに接続したときに、LLDP (Link Layer Discovery Protocol)フレームが確認できます。VC は LLDP をどのように処理しているのでしょうか。またこれを無効にできますか？

A4: LLDP は CDP (Cisco Discovery Protocol)に相当する IEEE プロトコルです。これはレイヤ 2 プロトコルで、隣接するデバイスに自分自身(およびその機能セットの一部)を通知することと、接続された他のデバイスをネットワークから見つけることの両方が可能です。LLDP は帯域幅が極めて低く、じゃまになりません。VC はアップリンクまたはクロスコネクトの 1 つが同じ VC ドメイン内の別の VC モジュールに直接接続されているため、スタッキングリンクが構成できるかを判断するために LLDP を使用します。現在ではこれを無効にする方法はありません。

Q5: スタッキングリンクを構成するための CX4 10Gb ケーブルを持っていません。代わりに複数の 1Gb RJ-45 リンクを組み合わせることはできますか？

A5: はい、モジュール間に複数の 1Gb リンクを追加すると、VC は自動でそれらを集約して、単一の 802.3ad ポートトランクを構成します。

Q6: 802.3ad ポートトランキングを構成したいのですが、トラフィックを通過させることができません。何がおかしいのでしょうか？

A6: VC では現在、802.3ad ポートトランクの LACP だけをサポートしています。Cisco の PAgP は VC でサポートされていません。VC の将来バージョンではこの機能を拡張する機能を追加する予定です。LACP を Cisco スイッチで正しく動作させるためには、チャネルモードをアクティブまたはパッシブのいずれかに設定する必要があります。VC では VCM の左側のツリービューにある[Hardware Overview]で必要なイーサネットモジュールをクリックすることで、イーサネットとポートトランクの詳細な統計情報を表示できます。

Q7: バーチャルコネクト内にクラスタハートビートネットワークを設定するにはどうすればいいですか？

A7: VC 内に vNet を作成して、VC アップリンクポートをこれに割り当てないようにします。次にクラスタ内の各ブレードから「ハートビート」NIC をこの vNet に割り当てます。すべてのハートビートトラフィックは vNet 内に閉じ込められ、エンクロージャ外部には送信されません。

Q8: 17 個以上の VC アップリンクを必要としています。アップリンクを追加するために VC イーサネットモジュールを追加した場合、サーバで使用する NIC を追加する必要がありますか？

A8: いいえ、VC イーサネットモジュールを追加して他の VC イーサネットモジュールとスタッキングすれば、アップリンクポートを使用できます。任意の VC イーサネットモジュールの任意の VC アップリンクを、任意の VC イーサネットモジュールの任意のダウンリンクに対して外部接続を提供するために使用できます。

Q9: サーバブレードの NIC を増やす必要があります。ダウンリンクポートを追加するために VC イーサネットモジュールを追加した場合、これらの新しいダウンリンクポートを接続するのに使用する VC アップリンクポートを追加する必要がありますか？

A9: いいえ、VC イーサネットモジュールを追加して、他の VC イーサネットモジュールとスタッキングすれば、新しいダウンリンクポートは既存の VC-Enet モジュールのアップリンクを使用するように構成できます。任意の VC イーサネットモジュールの任意の VC アップリンクを、任意の VC イーサネットモジュールの任意のダウンリンクに対して外部接続を提供するために使用できます。

Q10: インターコネクトベイ 1 の VC イーサネットモジュールがアクティブな Virtual Connect Manager で、ベイ 2 の VC モジュールがスタンバイだということはわかりましたが、これはつまり、ベイ 1 の VC モジュールだけがサーバブレードにイーサネット接続を提供しているということでしょうか？

A10: いいえ。どちらの VC モジュールがアクティブな Virtual Connect Manager を実行しているかにかかわらず、すべての VC モジュールを同時に使用してネットワーク接続を提供することができます。

Q11: VC は iSCSI をサポートしていますか？

A11: はい、VC は iSCSI と互換性があります。VC はレイヤ 2 デバイスで、iSCSI は TCP/IP の上の上位層プロトコルであるため、VC は iSCSI に固有の機能を何も実装していません。しかし、他のプロトコルの場合と同じように、iSCSI を実行するサーバにも VC はネットワーク接続を提供できます。

Q12: サーバブレードの接続を復元するためのフェイルオーバーが、予想以上に時間がかかる(20 秒以上)のはなぜですか？

A12: VC アップリンクポートに接続された上位の Cisco スイッチポートで、PortFast が有効になっているかを確認してください(「spanning-tree portfast」または「spanning-tree portfast trunk」)。

Q13: VC は STP とネットワーク上で対話しますか？

A13: いいえ。VC アップリンクポートはサーバの NIC ポートとまったく同じように見えるため(VMware ESX Server 上の物理 NIC ポートと同じ)、VC は VC アップリンクポートで STP をサポートしていません。

Q14: BPDU は VC アップリンクポートから外部 Cisco スイッチポートに送信されると考えてもよいですか？

A14: いいえ。VC アップリンクポートは BPDU を送信しません。

Q15: 使用中の L3 ルーティングプロトコルのいずれかを、VC ドメインを通じて延長できますか？

A15: VC はレイヤ 2 デバイスであるため、どのルーティングプロトコルもサポートしていません。ただし、OSPF、RIP、RIP2 などのレイヤ 3 のルーティングプロトコルをサーバで使用して、VC を通じて透過的に操作することができます。

Q16: 送信および受信のロードバランシングを行う、VC ドメイン全体で完全な冗長性を持った NIC チーミングを構成できますか？

A16: はい。ただし HP の Integrity ブレードで、INP (Windows/Linux の場合)、APA (HP-UX の場合)、または Smart Load Balancing (x86 上の Linux の場合)を使用している場合に限ります。x86 上の Windows 用のソリューションは現在ありません。

Q17: VC 1/10 Gb-F と VC 1/10Gb を同じエンクロージャで混在させることができますか？

A17: はい。これは帯域幅を増やしつつ、ケーブルとポートの使用を最小限に抑えるための優れた方法です。

Q18: VC は、ホストベース VLAN タギングをサポートする VMware および他の OS をサポートしていますか？

A18: はい。本書の該当する項を参照してください。

Q19: 他社ブランドの SFP および XFP を VC 1/10 Gb-F モジュールで使用できますか？

A19: いいえ。サポートされているのは HP ブランドの SFP および XFP モジュールだけです。

Q20: VC ファームウェアをアップグレードするとき、VC を停止する必要がありますか？

A20: 一般的には、定期的なメンテナンスの時間帯に VC ファームウェアをアップグレードすることを推奨しています。ただし、ソリューション全体が冗長構成となっていれば、VC はすべてのモジュールに対し、強制的でないローリングアップグレードを実行することができます。

Q21: **障害が発生した** VC **アップリンクポートからスタンバイの** VC **アップリンクポートへのフェイルオーバーは、どのくらいの時間がかかりますか？**

A21: **最適化された構成であれば、**5 **秒以内です。**

Q22: **ポートチャネル**(LAG)**のフェイルオーバーは、どのくらいの時間がかかりますか？**

A22: **最適化された構成であれば、**5 **秒以内です。**

Q23: vNet **がアップリンク間でフェイルオーバーするとき、チーミング** NIC **のフェイルオーバーはどのくらいの時間がかかりますか？**

A23: **最適化された構成であれば、**5 **秒以内です。**

Q24: VC-Enet **の** XFP **ポートを、**Cisco **スイッチの** XENPACK **または** X2 **ポートに接続できますか？**

A24: Cisco**からは、**XENPACK、X2、**および**XFP**モジュールは、同じポートタイプを使用していれば互換性があると説明されています。**VC**がサポートしているのは** 10GB-LR**と** 10GB-SR**のみのため、**Cisco**の**XENPACK、X2、**および**XFP**モジュールで** 10GBASE-LR**または** 10GBASE-SR**モジュールを使用していれば、バーチャルコネクトはこれらのモジュールと互換性があるはずです。**Cisco**のスイッチは、数種類のポートおよびトランシーバと、多種多様のインタフェースモジュールをサポートしているため、**HP**はすべての組み合わせをテストしていません。**
http://www.cisco.com/en/US/prod/collateral/modules/ps5455/prod_brochure0900aecd8034bba6.pdf
(**英語**)

Q25: **バーチャルコネクトは** IP **以外のレイヤ** 3 **プロトコル**(IPv6、IPX、AppleTalk **など**)**と互換性がありますか？**

A25: **バーチャルコネクトは管理インタフェース**(Web、SSH CLI、**または** SNMP)**上では** IP (IPv4)**のみをサポートしています。バーチャルコネクトのブリッジング機能に関して言えば、**VC **はブレードシステムで使用されているレイヤ** 3 **以上のすべてのプロトコルをサポートしています。バーチャルコネクトはレイヤ** 2 **デバイスであるため、レイヤ** 3 **プロトコルを理解しません。つまりサーバブレードは、イーサネットフレーム内に収容して伝送される、あらゆる上位層プロトコル**(IPv4、IPv6、IPX、AppleTalk **など**)**を使用して** VC **経由で通信することができます。**

Q26: **バーチャルコネクトはジャンボフレームをサポートしていますか？**

A26: **はい。**VC-Enet **は最大** 9216 **バイトまでのサイズのイーサネットフレームをサポートしています。**

Q27: **バーチャルコネクトはサーバの** NIC **へのダウンリンクで、**EtherChannel/802.3ad/SLB **をサポートしていますか？バーチャルコネクトに接続されているサーバの** NIC **で** LACP **ポートトランキングを使用できますか？**

A27: **いいえ。バーチャルコネクトはサーバの** NIC **へのダウンリンクで、**EtherChannel/802.3ad **をサポートしていません。**

486216-001、2008 **年** 2 **月**