Virtual Device Context (VDC)の技術概要

Cisco® Nexus 7000 シリーズ スイッチには、データセンター用に設計された新しいオペレーティング システムである Cisco NX-OS ソフトウェア プラットフォームが搭載されています。Cisco MDS 9000 SAN-OS プラットフォームでの実績に基づいた Cisco NX-OS は、スイッチをデバイス レベルで仮想化できる Virtual Device Context（VDC; 仮想デバイス コンテキスト）をサポートします。接続ユーザは、それぞれの VDC が物理スイッチのフレームワーク内にある 1 つのデバイスであるかのように扱うことができます。VDC はスイッチ内の独立した論理エンティティとして実行され、独自のソフトウェア プロセス セットを維持し、独自の構成を持ち、個別の管理者によって管理されます。

このドキュメントでは、Cisco NX-OS の VDC サポートについて説明します。

1. Cisco NX-OS と仮想デバイス コンテキスト

Cisco NX-OS は、Cisco MDS 9000 SAN-OS をベースにして、データセンターへの導入を目的として開発されました。このオペレーティング システムは、主要な レイヤ 2 および 3 プロトコルと、Cisco IOS® ソフトウェアが提供する主な機能をすべて備えています。そのなかには、構成に使用する Cisco IOS ソフトウェアの従来からのルック アンド フィールに加えて、Cisco ISSU（In Service Software Upgrades）、優れた障害検出、Cisco GOLD（Generic Online Diagnostics）や EEM（Embedded Event Manager）などの分離メカニズムといった機能があります。Cisco NX-OS は、プロセスの独立した開始と停止をサポートするモジュラ アーキテクチャに基づいており、固有の保護メモリ領域で実行されるマルチスレッド プロセスをサポートします。

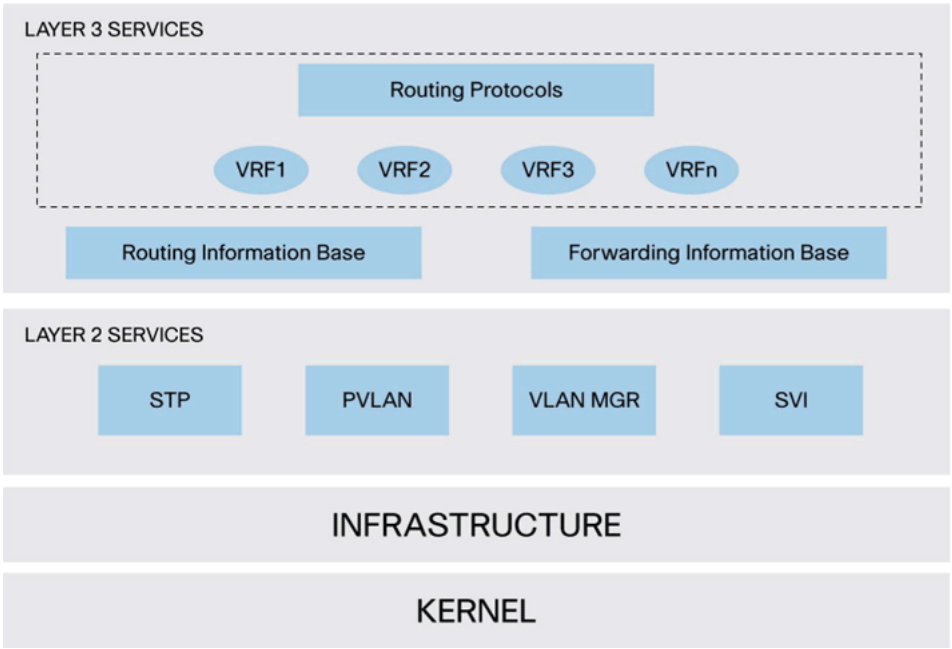
Cisco Nexus 7000 シリーズは、Cisco IOS ソフトウェアに含まれる数々の仮想化テクノロジーを継承しています。レイヤ 2 では、Virtual LAN（VLAN; 仮想 LAN）により、Cisco Nexus 7000 シャーシ内のブリッジ ドメインが仮想化されます。レイヤ 3 の仮想化については、VRF（Virtual Route Forwarding）インスタンスの概念を通じてサポートされます。VRF を使用すると、レイヤ 3 のフォワーディング テーブルおよびルーティング テーブルを仮想化できます。Cisco NX-OS ソフトウェア プラットフォームの仮想化機能は、VDC の概念をサポートするように拡張されています。VDC を使用すると、デバイス自体を仮想化することによって、物理的には 1 台のスイッチを複数の論理デバイスとして提供できます。VDC 内には、VLAN と VRF の一意かつ独立したセットを含めることができます。各 VDC には物理ポートを割り当てることができるため、ハードウェア データ プレーンも仮想化できます。各 VDC 内では、独立した管理ドメインを使って VDC を管理できるため、管理プレーン自体も仮想化できます。

スイッチ コントロール プレーンの定義には、スイッチ CPU（セントラル スーパーバイザに存在）によって処理されるすべてのソフトウェア機能が含まれます。コントロール プレーンは、ルーティング情報ベースや、レイヤ 2 およびレイヤ 3 の各種プロトコルの実行など、多数の重要なソフトウェア プロセスをサポートします。これらすべてのプロセスは、スイッチ

と他のネットワーク ノードの間のインタラクションにとって重要です。コントロール プレーンは、多数のハードウェア アクセラレーション機能を実現するデータ プレーンをプログラミングする役割も担っています。

スイッチ コントロール プレーンは、既定の状態では VDC 1 と呼ばれる単一のデバイス コンテキストを実行し、このデバイス コンテキスト内で約 80 のプロセスを実行します。これらのプロセスのいくつかは他のスレッドに分岐することがあり、その結果として、構成されているサービスによっては同時に 250 ものプロセスがシステム上でアクティブに実行されることがあります。次の図に示すように、この単一のデバイス コンテキスが OS のインフラストラクチャおよびカーネル コンポーネントの上で多数のレイヤ 2 および 3 サービスを実行させます。

図 1　単一の既定 VDC によるデフォルト動作モード



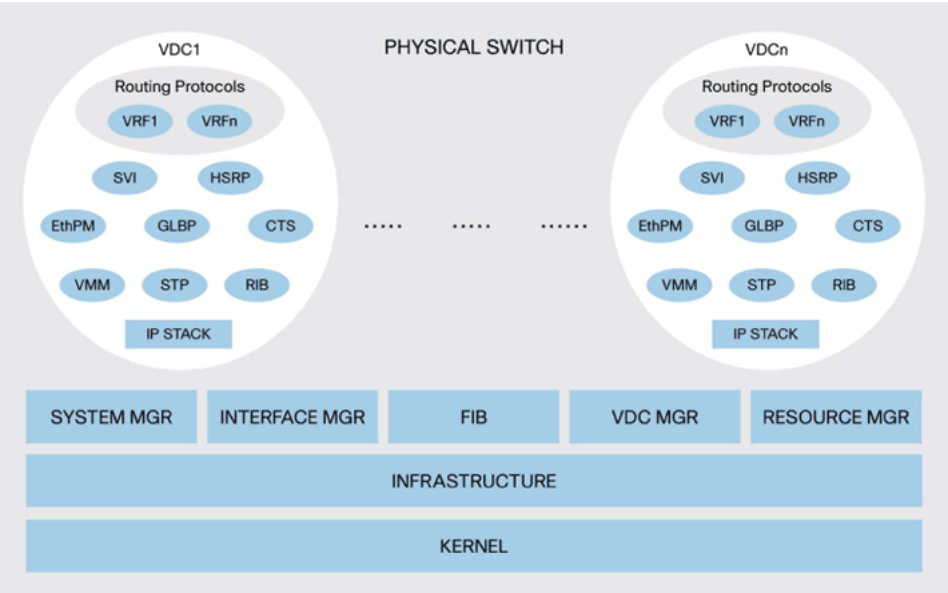
このプロセスの集合体は、いわば単一の物理デバイスのコントロール プレーンを構成します（他の VDC が有効になっていないと仮定します）。VDC 1 は常にアクティブで有効になっており、削除することはできません。重要なのは、このデフォルト モードであっても、VRF と VLAN を通じた仮想化サポートは、デフォルト VDC（または任意の VDC）内で使用できるということです。これを仮想化のネストと考えることもできます。上位レベルに VDC を構成することができ、その VDC 内に複数の VRF および VDC が存在することができます。将来のソフトウェア リリースでは、たとえば VRF 内の MTR というように、機能のネスト レベルを増やすことができるようになるかもしれません。

後から（追加の）VDC を有効にするとは、スイッチ内に存在するデバイス コンテキストごとにこれらのプロセスを複製することを意味します。こうすると、重複する VRF 名および VLAN ID を使用することが可能になります。たとえば、あるデバイス コンテキスト内に manufacturing という名前の VRF を設定し、別の VDC 内の VRF に同じ「manufacturing」という名前を適用することができます。したがって、VDC の管理者は実質的に、独自のプロ

セス セットと、独自の VRF および VLAN セットを操作することになります。つまり、それぞれ独自の論理（または仮想）スイッチ コンテキストとなります。これにより、管理コンテキストが明確になり、VDC 間の構成の分離および独立のための基盤が実現します。

図 2 に、VDC を実現する主要なソフトウェア要素を示します。VDC モードでは、VDC 単位の障害分離、VDC 単位の管理、データ トラフィックの分離、強化されたセキュリティなどのさまざまな利点を実現できます。物理インターフェイスなどのハードウェア リソースも VDC 間で分割することができます。ハードウェア パーティショニングのサポートについては、後で説明します。

図 2　VDC モード



VDC を使用すると、スイッチの管理者に付加的な利益をもたらす、さまざまな可能性が開けます。VDC の活用例として、以下のようなものがあります。

- 異なるユーザ部門のトラフィック間に、安全性の高いネットワーク パーティションを設ける
- 各部門が独自の構成を管理および維持できるようにする
- 新しい構成オプションや接続オプションをテストするためのデバイス　コンテキストを、運用システムに影響を与えることなく提供する（VDC の主要な用途の 1 つ）
- 複数の部門のスイッチ　プラットフォームを単一の物理プラットフォームに統合しつつ、OS、管理、およびトラフィックについては独立性を維持する
- デバイス　コンテキストをネットワーク管理者および運用者のトレーニングのために使用する

2. VDC のアーキテクチャ

Cisco NX-OS ソフトウェア プラットフォームは、VDC サポートの基盤を提供します。以下のセクションでは、このソフトウェア プラットフォーム内での VDC のサポートについて、さらに詳しく説明します。

2.1 VDC アーキテクチャのレイヤ

VDC モードで実行されているシステムのアーキテクチャ ダイアグラム（図 2）を分析すると、プラットフォームのすべてのアーキテクチャ要素が仮想化されているわけではないことがわかります。すべてのレイヤが仮想化されるわけではありませんが、主要なコンポーネントはすべて、VDC の概念をサポートすることを目的として構築されています。

この OS の心臓部は、カーネルとインフラストラクチャ レイヤです。カーネルは、スイッチで実行されるすべてのプロセスおよび VDC をサポートできます。ただし、カーネルのインスタンスは常に 1 つしか存在しません。インフラストラクチャ レイヤは、上位レイヤのプロセスと、物理スイッチのハードウェア リソース（TCAM など）の間のインターフェイスとして機能します。このレイヤのインスタンスが 1 つであることにより、ハードウェア リソースを管理する際の複雑さが軽減されます。また、インフラストラクチャ レイヤが 1 つであるため、このシステムの管理プロセスを重複させる必要がなく、パフォーマンスのスケーリングが可能になります。

インフラストラクチャ レイヤの制御下では、他にもいくつか重要なシステム プロセスが動作します。これらのシステム プロセスも、一意のエントリとして存在します。もちろん、VDC のサポートで重要な役割を果たすプロセスは、VDC マネージャです。VDC マネージャは、VDC の作成と削除を行います。さらに、システム マネージャやリソース マネージャなどの他のインフラストラクチャ コンポーネントに VDC 関連の API を提供し、それらのコンポーネントが独自の関連機能を実行できるようにします。

VDC が作成されると、VDC のスタートアップに必要な、VDC 単位で実行されるすべてのサービスの起動をシステム マネージャが行います。新しいサービスが構成されると、システム マネージャは適切なプロセスを起動します。たとえば、Marketing という名前の VDC で OSPF が有効にされた場合、システム マネージャはその VDC のための OSPF プロセスを起動します。VDC が削除されると、システム マネージャはその VDC に関連するすべてのプロセスを破棄します。

リソース マネージャは、VDC 間でのリソースの割り当てと配布を管理する役割を持っています。リソース　マネージャによって管理されるリソースの例として、VLAN、VRF、PortChannel、物理ポートがあります。このことについては、後で詳しく説明します。

インフラストラクチャ レイヤおよび関連するマネージャの上位に位置するのは、VDC 単位で実行されるプロセスです。これらの各プロセスは、独自の保護メモリ領域セット内で実行されます。障害分離は、VDC を使用することで得られる大きな利点の 1 つです。ある VDC でプロセスに障害が発生しても、別の VDC で実行されているプロセスには影響が及びません。

2.2 VDC のリソース割り当て

VDC の作成時に、選択したスイッチ リソースをその VDC に割り当て、それらのリソースの排他的な使用を保証することができます。リソース テンプレートは、リソースの割り当てを制御し、それらのリソースを VDC にどの程度割り当てられるかを定義します。VDC 管理者および VDC 内のユーザは、このテンプレートを変更できません。このテンプレートを変更できるのは、スーパーユーザだけです。スーパーユーザは、スイッチの構成に変更を加えるための最高レベルの権限を有するユーザです。スーパーユーザは、VDC 1（デフォルト VDC）のドメイン内に存在します。スーパーユーザは、デバイス コンテキスト間で物理スイッチ リソースを指定することに加えて、任意の VDC 構成を変更したり、VDC を作成および削除したり、各 VDC の管理者とユーザを作成および削除することができます。テンプレートはス

イッチ構成とは別に管理されます。そのため、スーパーユーザはテンプレートが以前に適用されていた VDC のリソース割り当てに影響を与えることなく、そのテンプレートを編集することができます。更新されたテンプレートを VDC に適用するときは、そのテンプレートを再適用する必要があります。これによって、テンプレートがアクティブ化されてコピーされ、実行中の構成とマージされます。透過的なバックアップという点では、テンプレートと構成のマージにより、プライマリ構成をバックアップするだけで、VDC に固有のすべての構成をバックアップできます。ほとんどのスイッチ リソースは VDC に割り当てることが可能です。表 1 に、VDC に割り当てることができるリソースと、割り当てることができないリソースを示します。

表 1. スイッチ リソース

VDC に割り当てることができるスイッチ リソース	VDC に割り当てることができないスイッチ リソース
物理インターフェイス、PortChannel、ブリッジ ドメインおよび VLAN、HSRP および GLBP グループ ID、SPAN	CPU*、メモリ*、FIB などの TCAM リソース、QoS、セキュリティ ACL * 将来のリリースでは、CPU やメモリを VDC に割り当てられるようになる予定です。

VDC 単位で割り当てることができる多数のリソースについては、それらのリソースが通常はグローバルでの管理になるということが重要な点です。たとえば、アクティブな VDC 間で配分できる Cisco EtherChannel® リンク バンドルの数は、シャーシあたり 256 です。これら 256 の Cisco EtherChannel リンク バンドルを 2 つの VDC で使用した場合、シャーシ内の他の VDC ではリンク バンドルが使えなくなります。Cisco EtherChannel のロード バランシング オプションはグローバル構成であり、VDC 単位で設定することはできません。もう 1 つの例は SPAN です。スイッチでは 2 つの SPAN セッションを使用できます。VDC A と VDC B の両方で SPAN セッションを「監視セッション 1」として構成することは可能ですが、ハードウェアの内部では、これらのセッションは異なる SPAN セッションとして認識されます。これもまた、SPAN がグローバル リソースとして管理されることの直接的な結果です。先ほどのリンク バンドルの例と同じく、これら 2 つのセッションが占有されると、他の VDC で使用できる SPAN セッションはなくなります。

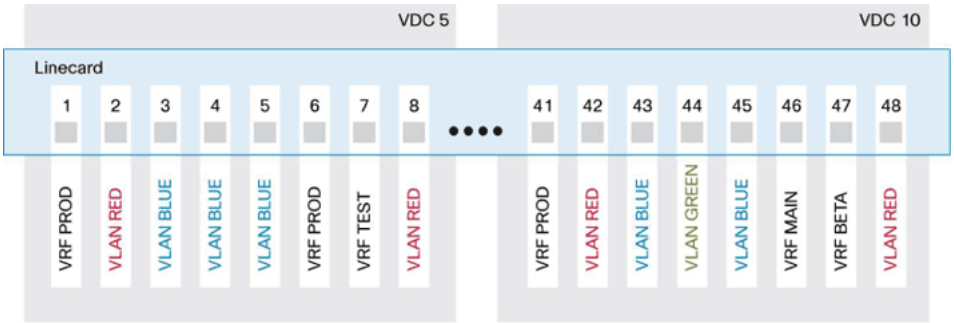
VDC バンドルを作成すると、Cisco Nexus 7000 シリーズ スイッチの論理的な表現が作成されます。ただし、初期状態では物理インターフェイスは割り当てられません。物理スイッチ ポートは、VDC 間で共有できないリソースです。既定では、スイッチのすべてのポートはデフォルト VDC（VDC 1）に割り当てられます。新しい VDC を作成するときに、スーパーユーザは物理ポートのセットをデフォルト VDC から新しく作成した VDC に割り当て、ネットワーク上の他のデバイスと通信する手段を新しい VDC に与える必要があります。VDC に割り当てられた物理ポートは、当該の VDC に排他的に結び付けられ、他の VDC はそのポートにアクセスできません。VDC 間通信は、スイッチ内では行われません。異なる VDC 間で通信できるようにするには、それらの VDC のポート間で独立した外部接続を行う必要があります。

VDC には、さまざまなポート タイプを割り当てることができます。これには、レイヤ 2 ポート、レイヤ 3 ポート、レイヤ 2 トランク ポート、PortChannel（Cisco EtherChannel）ポートが含まれます。同じ物理インターフェイスに関連付けられた SVI などの論理インターフェイスは、現在の実装内の別の VDC に割り当てることはできません。したがって、物理インターフェイスを仮想化し、作成された論理インターフェイスを別の VDC に関連付けることはできません。ただし、物理インターフェイスを仮想化し、作成された論理インターフェイ

スに異なる VRF または VLAN を関連付けることは可能です。つまり、VDC に物理インターフェイスを割り当て、VLAN と VRF に論理インターフェイスと物理インターフェイスを割り当てることはできます。

この例を図 3 に示します。ポート 1 ～ 8 は VDC 5 に属し、ポート 41 ～ 48 は VDC 10 に属します。各 VDC 内では、ポートがさらに仮想化され、VLAN または VRF に属します。

図 3　VDC の仮想化



デフォルト VDC レベルのルート管理者がポートを VDC に割り当てた後、そのポートを管理（構成および使用）するのは VDC 管理者の役割です。たとえば、show interface コマンドなど、他の関連コマンドを実行することによって確認できるのは、対象の VDC に割り当てられたインターフェイスだけです。

各 VDC は独自の構成ファイルを持ち、その VDC の制御下にあるポートの実際の構成に影響を与えます。さらに、このローカル構成には、VDC ユーザ ロールとそのユーザに割り当てられるコマンド スコープなどの、VDC に固有の構成要素が含まれます。VDC ごとに構成ファイルが独立しているため、VDC に加えられた運用構成の変更が別の VDC に影響を与えることはありません。

VLAN は、Cisco NX-OS で拡張されたもう 1 つの重要なリソースです。Cisco Nexus 7000 シリーズ スイッチでは、最大 16,384 の VLAN を複数の VDC にまたがって定義できます。各 VDC は、IEEE 802.1q 標準に準拠し、最大で 4096 の VLAN をサポートします。新たに拡張された VLAN サポートでは、外部からの VLAN を VDC 単位の VLAN にマップできます。混乱を避けるため、この VDC 単位の VLAN をブリッジ ドメインと呼びます。この方法では、VDC 管理者は 802.1q の VLAN ID 範囲内の任意の番号の VLAN を作成できます。新たに作成した VLAN は、VDC によってスイッチで使用できるデフォルトの 16,384 のブリッジ ドメインのいずれかにマップされます。これにより、同じ物理スイッチの VDC で VLAN ID を再利用しながら、OS レベルでは VLAN を物理スイッチのコンテキスト内の一意のブリッジ ドメインにすることが可能になります。たとえば、VDC A と VDC B の両方で VLAN 100 を作成し、それらをブリッジ ドメイン 250 および 251 にそれぞれマップすることができます。それぞれの管理者は、VLAN 100 を参照する show コマンドを使用して、その VLAN の監視と管理を行います。

3. VDC を使用した Cisco Nexus 7000 スイッチ リソースのスケーリング

ライン カードは、ローカル ハードウェア フォワーディング エンジンを使用して、レイヤ 2 およびレイヤ 3 のフォワーディングをハードウェア内で実行します。VDC を使用すると、このローカル フォワーディング エンジンがレイヤ 2 およびレイヤ 3 の処理を行うために使用するリソースを最適化できます。これについては、次のセクションで詳しく説明します。

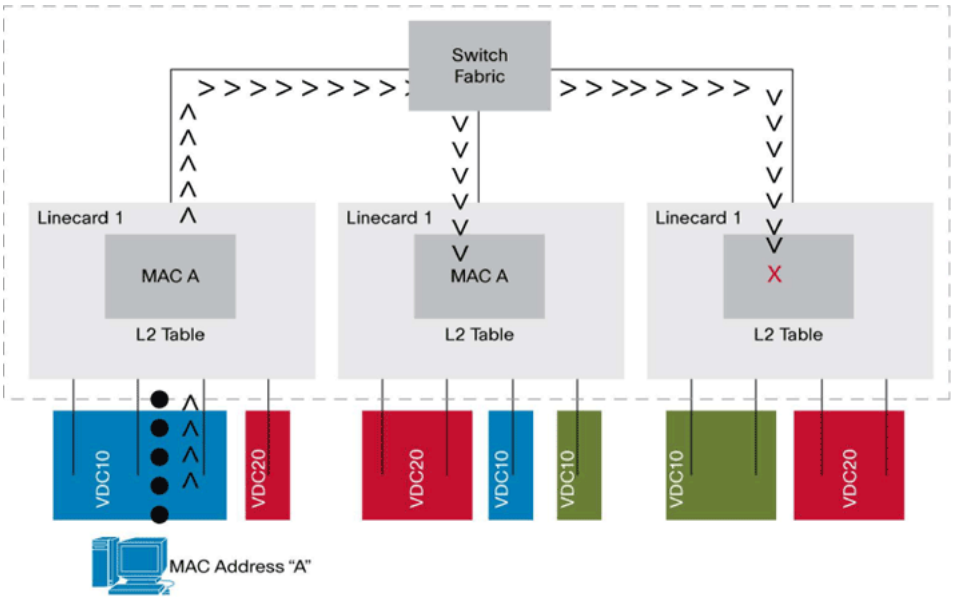
3.1 VDC によるレイヤ 2 アドレス ラーニング

各ライン カードのフォワーディング エンジンは、レイヤ 2 アドレス ラーニングを行い、レイヤ 2 フォワーディング テーブルのローカル コピーを維持します。各ライン カードの MAC アドレス テーブルは、128,000 の MAC アドレスをサポートします。新しい MAC アドレスを学習すると、ライン カードはその MAC アドレスのコピーを他のライン カードに転送します。これにより、レイヤ 2 アドレス ラーニング プロセスがライン カード間で同期されます。

レイヤ 2 ラーニングは VDC のローカル プロセスであるため、各ライン カードに配置されるアドレスに直接的な影響を与えます。

図 4 に、VDC の存在が分散型のレイヤ 2 ラーニング プロセスに与える影響を示します。ライン カード 1 では、MAC アドレス A がポート 1/2 から学習されます。このアドレスは、ライン カード 1 のローカル レイヤ 2 フォワーディング テーブルに配置されます。その後、この MAC アドレスはライン カード 2 および 3 に転送されます。ライン カード 3 は VDC 10 に属するポートを持たないため、VDC 10 から学習した MAC アドレスを配置しません。一方、ライン カード 2 は VDC 10 内のローカル ポートを持つため、MAC アドレス A をローカル フォワーディング テーブルに配置します。

図 4　MAC アドレス ラーニング



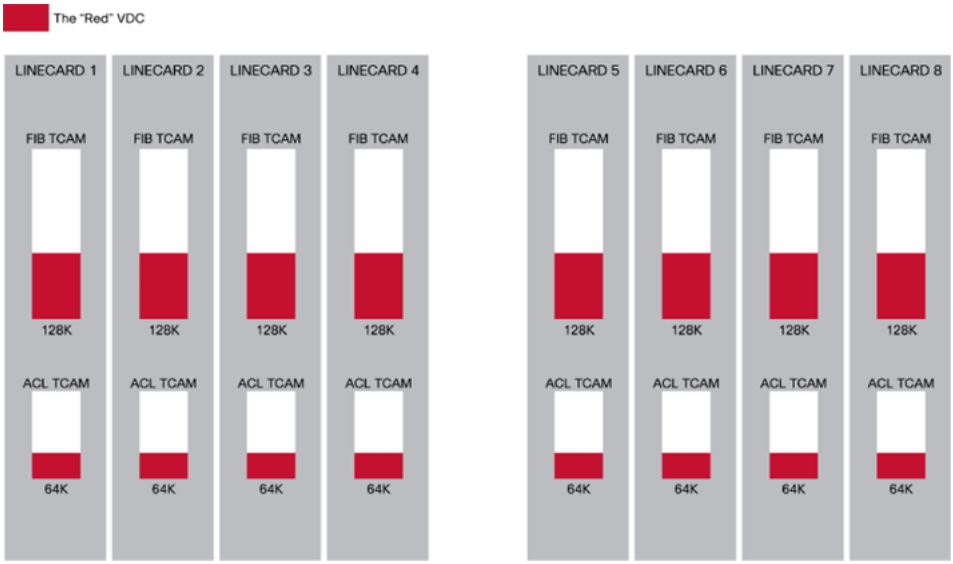
このレイヤ 2 ラーニングの実装により、Cisco Nexus 7000 シリーズ スイッチは、VDC がライン カードに対して一意である場合に、レイヤ 2 MAC アドレス テーブルの使用をより効率的にスケーリングする方法を提供します。

3.2 レイヤ 3 リソースと VDC

各ライン カードのフォワーディング エンジンは、フォワーディング インフォメーション ベース（フォワーディング プレフィックスを格納するために使用されます）内の 128,000 のエントリ、64,000 のアクセス制御リスト、512,000 の入力 NetFlow エントリ、および 512,000 の出力 NetFlow エントリをサポートします。

デフォルト VDC が唯一のアクティブな VDC である場合、学習したルートと ACL は各ライン カードの TCAM テーブルに読み込まれます。これにより、各ライン カードには適切なフォワーディング決定を行うために必要な情報がローカルで保持されます。このしくみを図 5 に示します。ここでは、デフォルトの「red」VDC に対するルートが FIB TCAM と ACL TCAM に存在します。

図 5　既定のリソース割り当て



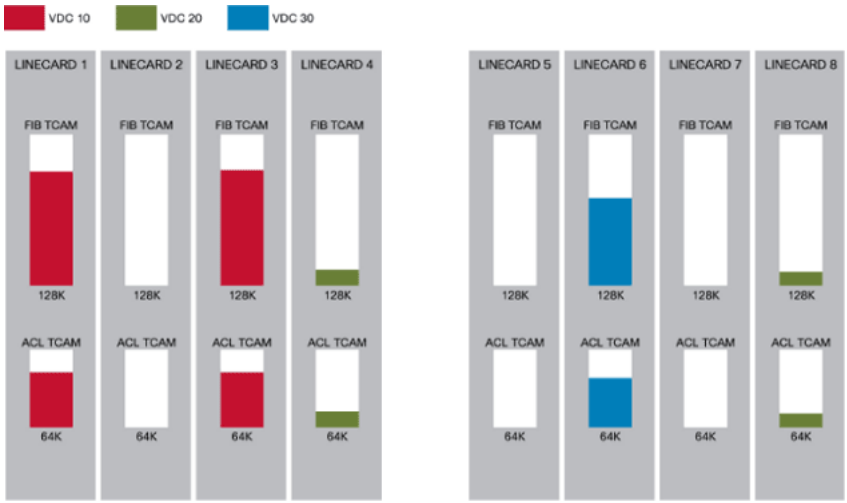
物理ポート リソースが複数の VDC 間に分かれている場合、フォワーディング情報と関連する ACL を格納するために必要なものは、その VDC に関連するライン カードだけです。これにより、前の例で示した既定のシステム制限を越えて、リソースをスケーリングすることが可能になります。表 2 に例を示します。

表 2.　リソース分離の例

VDC	ルート数	ACE（Access Control Entries）の数	割り当てられたライン カード
10	100,000	50,000	LC 1、LC 3
20	10,000	10,000	LC 4、LC 8
30	70,000	40,000	LC 6

この例では、リソースは図 6 に示すように割り当てられます。

図 6　リソースの分割



ポートのサブセットを特定の VDC に割り当てると、それぞれのライン カードの FIB および ACL TCAM に、その VDC のフォワーディング情報と ACL が提供されます。これにより、それらの TCAM リソースは、前述の単純なシステム制限を越えて使用できるようになります。前の例では、フォワーディング エントリの物理制限が 128,000 であるスイッチに、合計 180,000 のフォワーディング エントリが登録されています。同様に、Cisco ACE デバイスのシステム制限が 64,000 であるにもかかわらず、合計 100,000 の ACL が登録されています。さらに重要なのは、ライン カード 2、5、および 7 の FIB および ACL TCAM 領域が空いており、追加の VDC で使用できるということです。これにより、リソースの使用が前述の定義済みシステム制限を大幅に超えて拡張されます。

FIB および ACL の TCAM と同じく、NetFlow TCAM の使用も、複数の VDC がアクティブな場合はより細分化されます。先ほどと同じように、一連のライン カードがあり、それぞれのライン カードが異なる VDC に属するようにセットアップすることを考えてみます。

フローが識別されると、そのライン カード上のローカル NetFlow TCAM でフロー レコードが作成されます。入力 NetFlow と出力 NetFlow の両方が入力ライン カードで実行されるため、フローが格納されるのは、この入力ライン カードの NetFlow TCAM になります。フローの収集とエクスポートは常に VDC 単位で行われます。VDC X のフローが、VDC Y の一部であるコレクタにエクスポートされることはありません。ライン カード X の NetFlow TCAM で作成されたフローは、同じ VDC の一部である他のライン カードの NetFlow TCAM に複製されることはありません。これにより、TCAM の使用が最適化されます。

4. コントロール プレーン プロセスに対する VDC の影響

これまでのセクションでは、一部のシステム リソースがグローバルな意味を持ち、グローバル レベルで管理されるのに対し、その他のシステム リソースはグローバルな意味を持たず、VDC レベルで管理されるということを説明しました。これらのリソースと同じく、コントロール プレーン プロセスにも、有効時にグローバルな意味を持つものと、VDC 単位の意味を持つものがあります。次のセクションでは、VDC に関連する主要なコントロール プレーン プロセスについて説明します。

4.1 CoPP（Control Plane Policing）

スイッチ コントロール プレーンは、スイッチの動作を制御します。このエンティティに不具合が生じると、スイッチの動作に影響が出る可能性があります。CoPP は、コントロール プレーンが処理するように送信されるパケット数に対してレート制限を行うことにより、コントロール プレーンを保護するメカニズムです。

CoPP は、デフォルト VDC から有効にされ、デフォルト VDC でのみ実行されます。ただし、その適用範囲はシステム全体に及び、すべての VDC からコントロール プレーンに送信されたすべてのパケットが CoPP の対象となります。つまり、発信元の VDC に応じた異なる方法でトラフィックを監視するためにポリシーで使用できる VDC 認識は存在しません。

4.2 QoS（Quality of Service）

CoPP と異なり、QoS はグローバルまたは VDC 単位で構成が意味を持ちます。

VDC に固有の QoS リソースの例として、ターゲット トラフィックに対する速度制限動作を提供するために使用できるポリサーがあります。ポリサーはシステム全体に関わるリソースですが、構成後は対象の VDC 内のポートに対してのみ意味を持ちます。物理ポートに固有の QoS 構成も、そのポートが属する VDC のみに対して意味を持ちます。このタイプの QoS ポリシーの例として、ポート バッファの輻輳管理を提供するために使用される WRED（Weighted RED）があります。

QoS ポリシーが適用されるトラフィックを識別するために使用される分類 ACL は、VDC 単位のリソースのもう 1 つの例です。これらの ACL は、VDC 内で構成され、その VDC のポートに適用されます。さらに重要なことは、これらの QoS ACL は、対象となる VDC でポートを持つライン カードの ACL TCAM のみに配置されるということです。そのため、複数の VDC を作成することは、1 つの VDC で使用できる制限を越えて TCAM リソースをスケーリングする上で有効です。

CoS/キュー マッピングや DCSP/キュー マッピングなどのサービスを提供するために使用される QoS マップや、超過トラフィックや違反トラフィック用のマークダウン マップの多くは、グローバルな意味を持つ QoS 構成要素の一例です。入力 DSCP 値を変更する方法を提供する DSCP ミューテーション マップも、グローバルな意味を持ちます。これらのミューテーション/キュー マップや CoS/キュー- マップを変更すると、すべての VDC に入るパケットに影響が及びます。

4.3 EEM（Embedded Event Manager）

EEM（Embedded Event Manager）は、発生したイベントに基づいて動作を自動化できる、イベント型のサブシステムです。OIR イベントや、何らかの syslog メッセージの生成などのイベントが発生したとき、このシステムは、あらかじめ設定された一連の動作を定義したユーザ記述スクリプト（アプレット）を呼び出すことができます。

EEM ポリシー（アプレット）は、VDC のコンテキスト内で構成されます。ほとんどのイベントは各 VDC から認識されますが、デフォルト VDC のみが認識できるイベントもあります。このタイプのイベントの例として、Cisco GOLD 診断実行結果など、ライン カード自体によって生成されるイベントがあります。

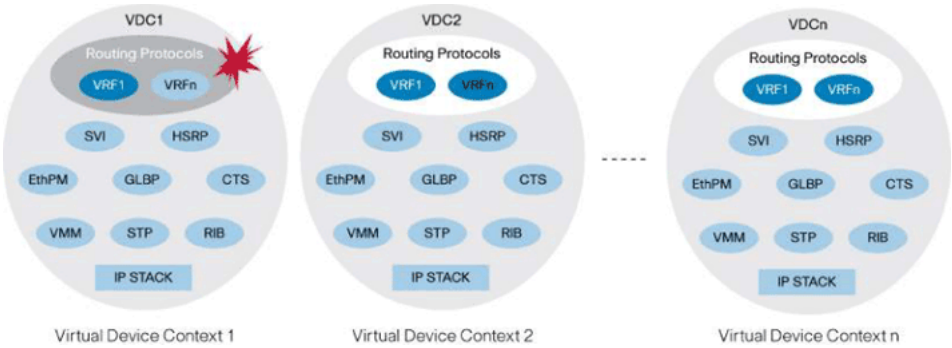
EEM は、EEM イベントおよび統計情報のログを VDC 単位で保持します。ポリシーの構成と管理を行えるのは、VDC 管理者だけです。VDC ユーザは EEM ポリシーを管理できません。

5. VDC の障害分離

1 つの物理スイッチで複数の VDC を作成した場合、VDC のアーキテクチャでは、その VDC 内の障害が他の VDC に影響を与えることはありません。したがって、たとえば、ある VDC で開始されたスパニング ツリーの再計算は、同じ物理シャーシ内の他の VDC のスパニング ツリー ドメインに影響を与えません。OSPF プロセスのクラッシュの場合も、障害はその VDC のローカルだけに隔離されます。このように、VDC 内でのプロセス分離は障害分離において重要な役割を果たし、VDC という概念を採用する組織にとっての主要な利点です。

図 7 に示すように、VDC 1 で実行されるプロセスの障害は、他の VDC で実行中のプロセスに影響を与えません。他の同様のプロセスは、障害が発生しているプロセスによる問題に妨げられることなく、継続して実行されます。

図 7　VDC 単位の障害分離



障害分離は、VDC 単位のデバッグ コマンドを提供する機能によって強化されます。syslog による VDC 単位のメッセージ ロギングは、VDC の障害分離機能のもう 1 つの重要な特徴です。これら 2 つの機能を組み合わせることで、管理者が問題を見つけるための強力なツールが実現します。

複数の VDC を作成すると、構成も分離されます。各 VDC には、それぞれ一意な構成ファイルが存在し、NVRAM に個別に格納されます。各 VDC には多数のリソースがあります。それらのリソースに対応する番号や ID は、複数の VDC 間で同じであっても、他の VDC の構成に影響を与えることはありません。たとえば、同じ VRF ID、PortChannel 番号、VLAN ID、管理 IP アドレスが複数の VDC に存在していてもかまいません。さらに重要な点は、このような構成分離により、VDC 間で構成が保護されるだけでなく、VDC が別の VDC の誤った構成変更から隔離されることです。

6. ハイアベイラビリティと VDC

Cisco NX-OS ソフトウェア プラットフォームは、コントロール プレーンに障害が発生した場合にデータ プレーンへの影響を最小限に抑えるハイアベイラビリティ機能セットを備えています。サービスの再起動から、ステートフル スーパーバイザ スイッチオーバー、データ トラフィックに影響を与えない ISSU に至るまで、さまざまなハイアベイラビリティ サービス レベルが用意されています。

コントロール プレーンに障害が発生した場合、管理者には、VDC に関して実行される動作を VDC ごとに構成して定義できる複数のオプションが用意されています。具体的には、再起動（Restart）、停止（Bringdown）、リセット（Reset）の 3 つです。再起動オプションは、VDC を削除し、実行中の構成でその VDC を再作成します。この動作は、シャーシ内に存在するスーパーバイザが 2 つであるか 1 つであるかに関係なく発生します。停止オプション

は、単に VDC を削除します。リセット オプションは、シャーシにスーパーバイザが 1 つだけ存在する場合は、アクティブなスーパーバイザのリセットを実行します。スーパーバイザが 2 つ存在する場合は、スーパーバイザ スイッチオーバーを実行します。

デフォルト VDC には、常にリセットのハイアベイラビリティ オプションが割り当てられます。以降に作成される VDC には、停止に対応するデフォルト値が割り当てられます。この値は、構成によって変更できます。

ステートフル スイッチオーバーは、シャーシ内の 2 つのスーパーバイザがある場合にサポートされます。通常の稼働時には、プライマリ スーパーバイザが冗長スーパーバイザとの間で、常に状態の交換と同期を行います。アクティブ（プライマリ）スーパーバイザの応答性を監視するために、ソフトウェア プロセス（ウォッチドッグ）が使用されます。プライマリ スーパーバイザに障害が発生すると、システムによって高速スイッチオーバーが実行されます。コントロール プレーン レイヤとデータ プレーン レイヤの両方でフェールオーバーが発生します。スーパーバイザ スイッチオーバーでは、データ プレーンはハードウェアに書き込まれた状態を維持することにより、レイヤ 2 およびレイヤ 3 派生のフォワーディング エントリを引き続き使用します。コントロール プレーンでは、NSF（Nonstop Forwarding）の一部であるグレースフル リスタート プロセスが使用され、レイヤ 3 のフェールオーバーが提供されます。レイヤ 2 では、ローカルでのステートフルな PSS メカニズムにより、コントロール プレーンが維持されます。このプロセスにより、以下が実現します。

- フェールオーバー時にも中断のないフォワーディング
- 障害から安定した稼働状態への迅速な復旧
- 復旧プロセス中にネットワークが不安定な状態になることのない、無停止の復旧メカニズム

ISSU は、VDC に直接関係する、ハイアベイラビリティのもう 1 つの重要な側面です。ISSU により、2 つのスーパーバイザを実行するシャーシに新しいバージョンのソフトウェアをインストールしてアクティブ化することができます。ソフトウェア アップグレードをバックアップ スーパーバイザに適用し、その後、アップグレードしたスーパーバイザにスイッチオーバーします。次に、もう一方のスーパーバイザを同じ新しいソフトウェア セットでアップグレードします。この間、システムはデータ フローを中断なく維持します。このとき、ISSU を VDC 単位で適用することはできません。シャーシにインストールされたソフトウェアは、すべてのアクティブな VDC に適用されます。

Cisco NX-OS ソフトウェア プラットフォームでは、HSRP や GLBP などの FHRP（First Hop Routing Protocol）が提供されます。これらのサービスは、接続ホストに対して、デフォルト ゲートウェイの冗長性を提供します。ISSU と異なり、各 FHRP サービスは VDC 単位で使用できます。管理者は、VDC を作成する作業の一環として、各 VDC で使用できるいくつかの FHRP グループを定義できます。

7. VDC の構成

このセクションでは、VDC を作成し、リソースを割り当てるための手順について説明します。

7.1 最初の VDC 設定

VDC の構成作業は、VCD を作成することから始まります。1 つのシステムに同時に存在できる VDC は、最大で 4 つです。デフォルト VDC（VDC 1）が常にアクティブであるため、最大で 3 つの追加 VDC を CLI から作成できることになります。VDC を作成するには、以下に示すように、構成モードで vdc <vdc の名前> コマンドを使用します。

```
switch# conf t
switch(config)# vdc production
switch(config-vdc)# show vdc
vdc_id vdc_name        state            mac
------ --------        -----            ----
1 switch               active           00:18:ba:d8:4c:3d
2 production           active           00:18:ba:d8:4c:3e

switch(config-vdc)# show vdc detail
vdc id: 1
vdc name:switch
vdc state:active
vdc mac address:00:18:ba:d8:4c:3d
vdc ha policy:RESET
vdc id: 2
vdc name:production
vdc state:active
vdc mac address:00:18:ba:d8:4c:3e
vdc ha policy:BRINGDOWN
```

VDC を作成すると、システムは VDC 構成モードになります。このモードでは、追加の構成オプションを VDC に割り当てることができます。以下の出力からわかるように、VDC の作成時には構成ステートメントの既定のセットが割り当てられます。

```
switch# show run | begin vcd
<snip>
vdc production id 2
    template default
    hap bringdown
    limit-resource vlan minimum 16 maximum 4094
    limit-resource span-ssn minimum 0 maximum 2
    limit-resource vrf minimum 16 maximum 8192
```



```
    limit-resource port-channel minimum 0 maximum 256
    limit-resource glbp_group minimum 0 maximum 4096
<snip>
```

これらの構成ステートメントは、VDC に許可されるリソース消費の定義を提供します。これらのリソースには、VLAN、VRF、SPAN、PortChannel、および GLBP グループ ID が含まれます。ただし、リソース制限の割り当ては、コマンド ラインを使用して変更できます。以下に、リソース制限を変更する方法の例を示します。

```
switch(config)# vdc production
switch(config-vdc)# limit-resource vlan minimum 32 maximum 4094
switch(config-vdc)# show run | begin vdc
<snip>
vdc production id 2
    template default
    hap bringdown
    limit-resource vlan minimum 32 maximum 4094
    limit-resource span-ssn minimum 0 maximum 2
    limit-resource vrf minimum 16 maximum 8192
    limit-resource port-channel minimum 0 maximum 256
    limit-resource glbp_group minimum 0 maximum 4096
<snip>
```

この例は、production VDC の VLAN の最低数を 16 から 32 に変更する方法を示しています。

また、リソース テンプレートを使用して VDC にリソースを割り当てることもできます。リソース テンプレートの構成作業は、以下の例に示すように、構成モードで行います。

```
switch(config)# vdc resource template n7000switch
switch(config-vdc-template)# limit-resource vlan minimum 32 maximum 256
switch(config-vdc-template)# limit-resource vrf minimum 32 maximum 64
switch(config-vdc-template)# exit
```

作成したリソース テンプレートは、以下の例に示すように VDC に割り当てることができます。

```
switch(config)# vdc 2 template n7000switch
switch(config-vdc)# show vdc resource template
    template::n7000switch
    --------
       Resource           Min             Max
       ----------         -----           -----
       vrf                32              64
       vlan               32              256
```



```
    template ::default
    --------
       Resource           Min            Max
       ----------         -----          -----
       glbp_group         0              4096
       port-channel       0              256
       span-ssn           0              2
       vlan               16             4094
       vrf                16             8192
  switch(config-vdc)#
```

VDC を作成すると、VDC 構成モードに切り替わります。次の作業は、この VDC に物理ポートを割り当てることです。物理ライン カードのポートを複数の VDC 間で共有することはできません。既定では、すべての物理ポートはデフォルト VDC に属します。VDC の作成時に、以下の CLI オプションを使用して、ポートをその VDC の制御下に置くことができます。

```
  switch(config)# show vdc membership vdc_id:1 vdc_name:
  switch interfaces:
         Ethernet3/1         Ethernet3/2         Ethernet3/3
         Ethernet3/4         Ethernet3/5         Ethernet3/6
         Ethernet3/7         Ethernet3/8         Ethernet3/9
         Ethernet3/10        Ethernet3/11        Ethernet3/12
         Ethernet3/13        Ethernet3/14        Ethernet3/15
         Ethernet3/16        Ethernet3/17        Ethernet3/1
         Ethernet3/19        Ethernet3/20        Ethernet3/21
         Ethernet3/22        Ethernet3/23        Ethernet3/24
         Ethernet3/25        Ethernet3/26        Ethernet3/27
         Ethernet3/28        Ethernet3/29        Ethernet3/30
         Ethernet3/31        Ethernet3/32        Ethernet3/33
         Ethernet3/34        Ethernet3/35        Ethernet3/36
         Ethernet3/37        Ethernet3/38        Ethernet3/39
         Ethernet3/40        Ethernet3/41        Ethernet3/42
         Ethernet3/43        Ethernet3/44        Ethernet3/45
         Ethernet3/46        Ethernet3/47        Ethernet3/48
  vdc_id:2 vdc_name:production interfaces:


  switch(config)# vdc production
```



```
switch(config-vdc)# allocate interface ethernet 3/48
switch(config-vdc)# show vdc membership

vdc_id:1 vdc_name:switch interfaces:
       Ethernet3/1         Ethernet3/2         Ethernet3/3
       Ethernet3/4         Ethernet3/5         Ethernet3/6
       Ethernet3/7         Ethernet3/8         Ethernet3/9
       Ethernet3/10        Ethernet3/11        Ethernet3/12
       Ethernet3/13        Ethernet3/14        Ethernet3/15
       Ethernet3/16        Ethernet3/17        Ethernet3/18
       Ethernet3/19        Ethernet3/20        Ethernet3/21
       Ethernet3/22        Ethernet3/23        Ethernet3/24
       Ethernet3/25        Ethernet3/26        Ethernet3/27
       Ethernet3/28        Ethernet3/29        Ethernet3/30
       Ethernet3/31        Ethernet3/32        Ethernet3/33
       Ethernet3/34        Ethernet3/35        Ethernet3/36
       Ethernet3/37        Ethernet3/38        Ethernet3/39
       Ethernet3/40        Ethernet3/41        Ethernet3/42
       Ethernet3/43        Ethernet3/44        Ethernet3/45
       Ethernet3/46        Ethernet3/47

vdc_id:2 vdc_name:production interfaces:
       Ethernet3/48
```

この例は、物理ポート Ethernet 3/48 を production VDC の制御下に移動する方法を示しています。このポートと、puroduction VDC に割り当てられた他のポートの追加構成は、production VDC 内から完了する必要があります。

7.2 VDC の切り替え

VDC を作成し、リソース制限を指定し、物理ポートを割り当てたら、管理者はその VDC に切り替えて、追加の構成作業を行う必要があります。デフォルト VDC CLI から、以下のコマンドを使用してアクティブな VDC を確認できます。

```
switch# show vdc

vdc_id   vdc_name          state          mac
------   --------          -----          ----------
1        switch            active         00:18:ba:d8:4c:3d
2        production        active         00:18:ba:d8:4c:3e
3        beta              active         00:18:ba:d8:4c:3f
```


管理者が VDC を切り替えるには、switchto コマンドを使用します。デフォルト VDC 内からは、前述の VDC リストに表示されている任意の VDC に移動できます。たとえば、production VDC に切り替えるには、次のようにします。

```
switch# switchto vdc ?
  production     VDC number 2
  beta           VDC number 3
  switch         VDC number 1
switch# switchto vdc production
Cisco Nexus Operating System (NX-OS) Software
TAC support:http://www.cisco.com/tac
Copyright (c) 2002-2007, Cisco Systems, Inc. All rights reserved.The
copyrights to certain works contained herein are owned by other
third parties and are used and distributed under license.Some parts
of this software may be covered under the GNU Public License or the
GNU Lesser General Public License.A copy of each such license is
available at
http://www.gnu.org/licenses/gpl.html and
http://www.gnu.org/licenses/lgpl.html
switch(vdc)# show vdc current-vdc
Current vdc is 2
switch(vdc)#
```

管理者がデフォルト VDC から別の VDC に切り替えると、CLI プロンプトは新しい VDC に移動したことを反映するように変更されます。いったんデフォルト VDC 以外の VDC に移動すると、VDC 間を移動する機能が制限されます。先ほどの例では、production VDC 内で switchto コマンドを使用しても、デフォルト VDC のときと同じ表示は得られません。これを以下に示します。

```
switch(vdc)# show vdc current-vdc
Current vdc is 2
switch(vdc)# switchto vdc ?
    production VDC number 2
switch(vdc)#
```

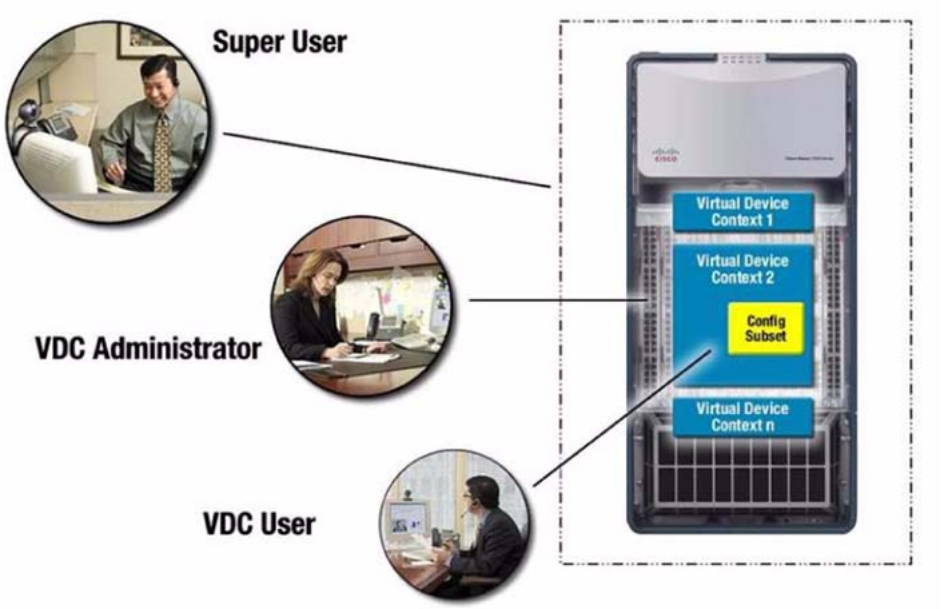
この出力を見ると、production VDC 内のユーザは、システム内に他のアクティブ VDC が存在するにも関わらず、別の VDC への switchto 権限を持たないことがわかります。いったん production VDC に切り替えたら、要件を満たすように構成作業を続けます。

8. VDC の管理

VDC アーキテクチャは、物理スイッチおよび VDC を管理するために使用できるいくつかの管理者レベルを定義します。各レベルは、スイッチに対してグローバル レベルと VDC 内からの両方で呼び出すことができる構成コマンドへのアクセス権を定義します。特定のユーザ ロールのスコープに含まれないコマンドは、そのユーザに対しては表示されないか、または実行されるとエラーを返します。

以下の図に示すように、ユーザ レベルには、スーパーユーザ、VDC 管理者、VDC ユーザの 3 つがあります。これらの各ユーザ ロールについて、以下のセクションで詳しく説明します。

図 8　VDC のユーザ ロール



スーパーユーザ

管理者ツリーの最上位に位置するのは、スーパーユーザ ロールです。Cisco Nexus 7000 シリーズ スイッチを初めて起動すると、デフォルト VDC（VDC 番号 1）が有効になります。このモードでスイッチを構成するために使用される管理者レベルは、基本的に、スーパーユーザのロールに与えられるレベルと同じです。追加の VDC を作成および削除する権限を持っているのは、スーパーユーザです。このレベルの管理者は、すべてのグローバル コマンドを呼び出すことに加えて、指定した VDC に物理スイッチ ポートを割り当てることができます。スーパーユーザには、グローバル スコープを持つ他のコマンドを呼び出す権限があります。これらのコマンドは、スイッチ上のすべての VDC の動作に影響を与え、システム全体をリロードしたり、グローバル IP アドレス（管理 IP アドレスなど）を変更したり、ブート イメージの場所を構成する機能を含みます。

VDC 管理者

VCD の作成時に、スーパーユーザはその VDC の VDC 管理者も作成します。VDC 管理者は、スイッチに存在する 2 つ目のユーザ タイプです。このユーザは、VDC の範囲内で、その VDC の構成に変更を加えたり、他の VDC とは関係なく VDC 構成を保存できます。VDC 管理者は、複数の VDC にまたがる管理スコープを持つこともできます。ただし、このユーザ タイプでは、スーパーユーザ ロールがアクセスできるグローバル構成オプションや物理リソース割り当てオプションを実行することはできません。さらに、管理対象の VDC を含めて、VDC の作成や削除を行うこともできません。

VDC ユーザ

特定の VDC の範囲内で、VDC 管理者は 3 番目のレベルのユーザである VDC ユーザを作成できます。VDC ユーザは、スイッチにログインし、VDC 管理者によって定義される構成コマンドのサブセットを呼び出すことができます。VDC 管理者は、ロールの一部として、許可

されるコマンドのサブセットを定義します。VDC ユーザは、VDC 管理者によって割り当てられるロールの権限を継承します。合計で最大 256 のロールをスイッチ上で一度に定義し、アクティブにすることができます。

物理スイッチに複数の VDC が存在する場合、スーパーユーザは VDC 管理者および VDC ユーザに複数の VDC へのアクセスを許可することができます。VDC の切り替えは、Cisco NX-OS によってサポートされる機能です。これによって有効なユーザは、スイッチに対してデバイス コンテキスト間の移動を指示することができます。この機能では、セキュリティが重要な要素です。そのため、切り替えを行うユーザは新しい VDC に最初に移動する際、再認証を行う必要があります。状態が維持されるため、その後の移動では再認証は不要です。スーパーユーザが VDC 間を移動するときは、認証は不要です。VDC へのアクセス権は、より幅広い RBAC（Role-Based Access Control）とは別のものです。RBAC は、セキュリティ アクセス許可を定義し、ロールと関連付ける方法を提供します。ユーザには 1 つ以上のロールが与えられます。また、ネットワークをトラバースするユーザ データには、ネットワーク デバイスがそのユーザのアクセス権を判断するためのタグが割り当てられます。

9. まとめ

Cisco NX-OS ソフトウェア プラットフォームの VDC は、仮想化サポートを拡張し、真のデバイス仮想化を実現します。物理スイッチの仮想化には、優れた障害分離などのさまざまな運用上の利点があり、アベイラビリティの向上につながります。さらに、VDC の範囲内でのトラフィック分離は、ユーザ データのセキュリティの強化を実現します。1 台の物理スイッチ内に多数のスイッチ コンテキストが存在することで、組織内の複数の論理グループにまたがって物理スイッチ リソースをスケーリングすることが可能になります。これにより、管理効率が向上すると共に、運用コストが軽減されます。

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

お問い合せ先

09.06