CHAPTER 1

概要

この章では、Cisco NX-OS デバイスでサポートされる Virtual Device Context（VDC; 仮想デバイス コンテキスト）について説明します。

この章では、次の内容について説明します。

VDC の概要

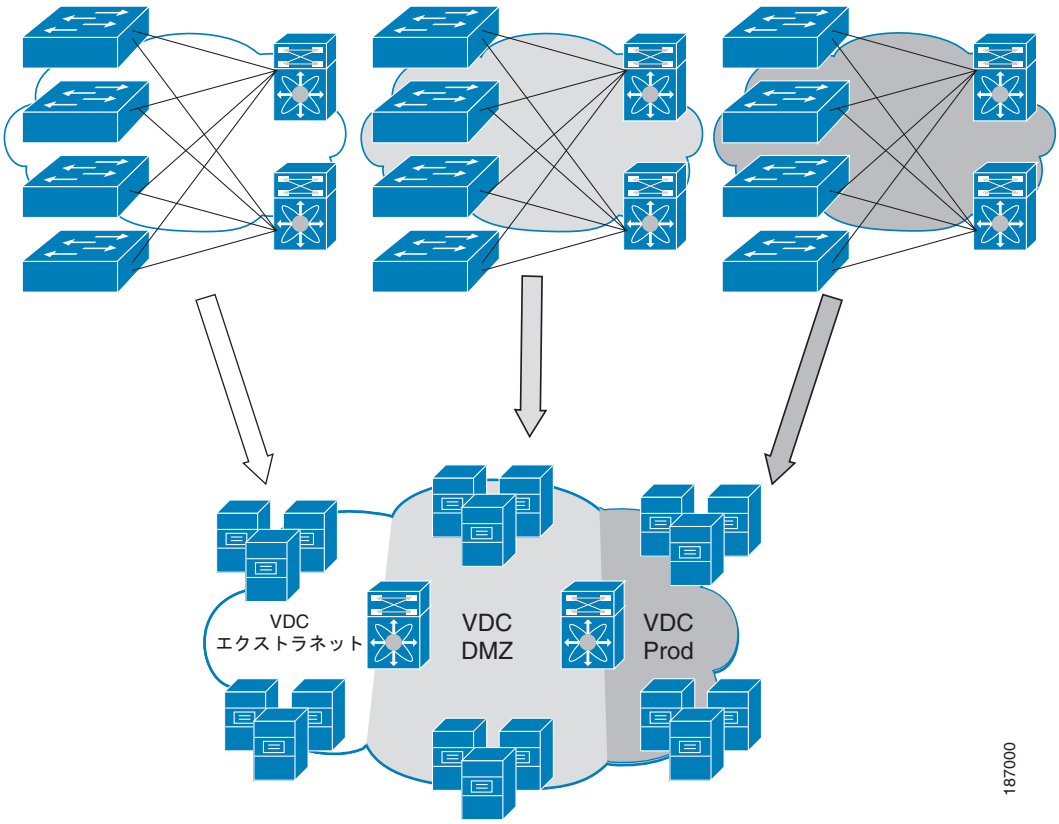
Cisco NX-OS ソフトウェアは VDC をサポートします。これは、1 つの物理デバイスを複数の論理デバイスとして分割する機能であり、障害の切り分け、管理の分離、アドレス割り当ての分離、サービス差別化ドメイン、および適応型リソース管理を可能にします。個々の VDC インスタンスは、1 つの物理デバイス内で独立して管理できます。接続ユーザには、個々の VDC は一意のデバイスとして表示されます。VDC は物理デバイス内で、個別の論理エンティティとして実行されます。VDC は、実行中の一連のソフトウェア プロセスを独自に管理し、独自の構成を持つことができます。また、個別の管理者による管理が可能です。

VDC はコントロール プレーンの仮想化もサポートしています。これには、アクティブ スーパーバイザ モジュール上の CPU 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、Routing Information Base（RIB; ルーティング情報ベース）やルーティング プロトコルなど、物理デバイス上のサービスに対するソフトウェア処理をサポートします。

VDC を作成すると、Cisco NX-OS ソフトウェアはコントロール プレーンのプロセスをいくつか抽出し、VDC 用に複製します。このようにプロセスが複製されることで、VDC の管理者は Virtual Routing and Forwarding（VRF; 仮想ルーティング / 転送）インスタンス名および VLAN ID を、他の VDC で使用されているものと独立して使用できます。基本的に、各 VDC 管理者は個別のプロセス、VRF、および VLAN のセットを操作します。

図 1-1 は、Cisco NX-OS ソフトウェアが物理デバイスを複数の VDC に分割する仕組みを示します。これには、VDC レベルの障害分離、VDC レベルの管理、データ トラフィックの分離、およびセキュリティの強化といった利点があります。

図 1-1　物理デバイスの分割



VDC のアーキテクチャ

Cisco NX-OS ソフトウェアは、VDC をサポートするための基盤を提供します。

ここでは、次の内容について説明します。

カーネルおよびインフラストラクチャ層

Cisco NX-OS ソフトウェアは、基本的にカーネルおよびインフラストラクチャ層で構成されています。1 つのカーネル インスタンスが、物理デバイス上で実行されるすべてのプロセスおよび VDC をサポートします。インフラストラクチャ層は、上位層のプロセスと、Ternary Content Addressable Memory（TCAM）など、物理デバイス上のハードウェア リソースとのインターフェイスを提供します。この層のインスタンスは 1 つしかないので、ハードウェア リソースの管理が複雑化せず、システム管理プロセスの重複も防止できるため、Cisco NX-OS ソフトウェアのパフォーマンスを向上できます（図 1-2 を参照）。

また、このインフラストラクチャにより、VDC 間の分離が保証されます。ある VDC 内で発生した障害は、他の VDC 内のサービスに影響を与えません。この機能により、ソフトウェア障害の影響を制限でき、デバイスの信頼性が大きく向上します。

インフラストラクチャ層だけでなく、いくつかの非仮想化サービスについても、すべての VDC に対して 1 つのインスタンスだけが存在します。これらのインフラストラクチャ サービスは、VDC の作成、VDC 間でのリソースの移動、および VDC 内の個々の各プロトコル サービスのモニタリングに参加します。

Cisco NX-OS ソフトウェアにより、VDC ごとに 1 つの仮想化コントロール プレーンが作成されます。VDC 内の仮想化コントロール プレーンは、すべてのプロトコル関連イベントを処理します。

レイヤ 2 およびレイヤ 3 プロトコル サービスはすべて、VDC 内で実行されます。ある VDC 内で開始された各プロトコル サービスは、他の VDC 内のプロトコル サービスとは独立して実行されます。インフラストラクチャ層は VDC 内のプロトコル サービスを保護し、あるサービスで生じた障害や問題が、他の VDC に影響を与えないようにします。Cisco NX-OS ソフトウェアがこのような仮想化サービスを作成するのは、VDC の作成時だけです。各 VDC は、各サービスに対する独自のインスタンスを保持します。仮想化されたこれらのサービスは他の VDC を意識せず、自身の VDC に割り当てられたリソースだけを処理します。これらの仮想化サービスに対して有効なリソースを制御できるのは、network-admin ロールを持つユーザだけです。

図 1-2　　VDC のアーキテクチャ

デフォルトの VDC

物理デバイスはデフォルトの VDC（VDC 1）として、常に 1 つの VDC を持ちます。Cisco NX-OS デバイスに最初にログインすると、デフォルトの VDC が開始されます。

デフォルト以外の VDC を作成、属性変更、または削除するには、デフォルトの VDC で作業する必要があります。Cisco NX-OS ソフトウェアでは、デフォルトの VDC を含めて最大 4 つの VDC がサポートされます。つまり、最大 3 つの VDC を作成できます。

ネットワーク管理者（network-admin）のロール権限を持っている場合は、デフォルト VDC から物理デバイス、およびすべての VDC を管理できます（「VDC デフォルト ユーザ ロール」（P.1-7）を参照）。

VDC 間の通信

Cisco NX-OS ソフトウェアは、1 つの物理デバイス上の VDC 間での直接的な通信をサポートしていません。VDC 間の通信を可能にするには、1 つの VDC に割り当てられたポートと、他の VDC に割り当てられたポートとの間で物理接続を確立する必要があります。各 VDC は、他の VDC と通信するための独自の VRF を保持します（「論理リソース」（P.1-5）を参照）。

VDC のリソース

network-admin ロールを持つユーザは、物理デバイス リソースを、VDC だけに使用されるように特別に割り当てることができます。特定の VDC にリソースを割り当てた場合、このリソースはこの VDC だけから管理できます。Cisco NX-OS ソフトウェアでは、各 VDC に論理および物理リソースを割り当てる方法を制御できます。VDC に直接ログインしたユーザは、このように限定されたデバイス ビューだけを表示でき、ネットワーク管理者がこの VDC に明示的に割り当てたリソースだけを管理できます。VDC 内のユーザは、他の VDC 内のリソースを表示または変更できません。

（注）　VDC にリソースを割り当てるには、network-admin ロールが必要です（「VDC デフォルト ユーザ ロール」（P.1-7）を参照）。

ここでは、次の内容について説明します。

- 「物理リソース」（P.1-4）
- 「論理リソース」（P.1-5）
- 「VDC リソース テンプレート」（P.1-6）
- 「設定ファイル」（P.1-6）

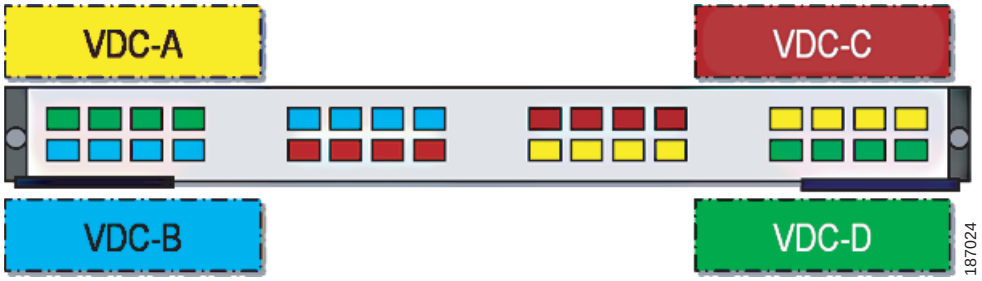
物理リソース

VDC に割り当てることができる物理リソースは、イーサネット インターフェイスだけです。個々の物理イーサネット インターフェイスは、一度に 1 つの VDC だけに所属できます。初期状態では、すべての物理インターフェイスはデフォルト VDC（VDC 1）に属します。VDC を新規作成すると、Cisco NX-OS ソフトウェアによってこの VDC に対する仮想化サービスが作成されますが、このサービスに物理インターフェイスは割り当てられません。VDC を新規作成したあとは、デフォルト VDC から新規 VDC に、一連の物理インターフェイスを割り当てることができます。いったん VDC に物理インターフェイスを割り当てると、この設定はこの VDC でしか行えず、デフォルト VDC も含め、他の VDC からはこのインターフェイスにアクセスできません。

VDC にインターフェイスを割り当てると、このインターフェイスのすべての設定は消去されます。ユーザまたは VDC 管理者は、この VDC 内でインターフェイスを設定する必要があります。設定時には、この VDC に割り当てられたインターフェイスだけが表示されます。

Cisco Nexus 7000 シリーズ 32 ポート 10 Gbps イーサネット モジュール（N7K-M132XP-12）のインターフェイスを除き、物理デバイスに任意の組み合わせでインターフェイスを割り当てることができます。このモジュールには 8 つのポート グループがあり、各ポートは 4 つのインターフェイスから構成されます。1 つのポート グループに含まれる 4 つのインターフェイスすべてを同一の VDC に割り当てる必要があります（図 1-3 を参照）。

図 1-3　Cisco 7000 シリーズ 10 Gbps イーサネット モジュールのポート グループでのインターフェイスの割り当て例



Cisco Nexus 7000 シリーズ 32 ポート 10 Gbps イーサネット モジュールのポート グループに関する詳細については、『*Cisco Nexus 7000 Series Hardware Installation and Reference Guide*』を参照してください。

論理リソース

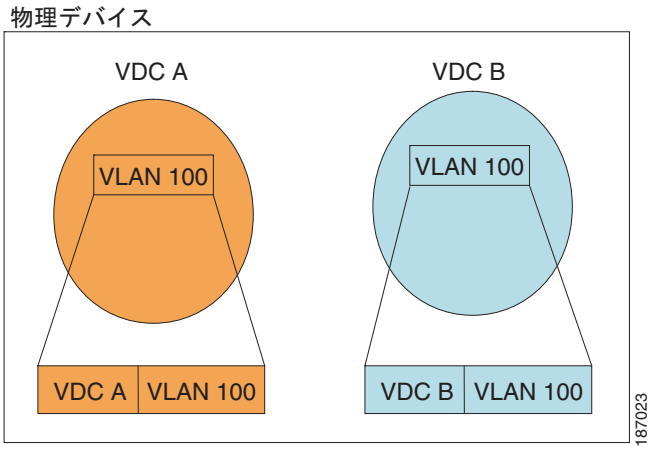
各 VDC は、1 つの物理デバイス内で個別の論理デバイスとして動作するため、すべての名前空間は VDC 内で一意となります。

VDC を作成すると、各 VDC は他の VDC と共有しない独自のデフォルト VLAN および VRF を保持します。VDC 内に他の論理エンティティを作成して、この VDC だけに使用されるように設定することもできます。たとえば、SPAN モニタリング セッション、ポート チャネル、VLAN、VRF などの論理エンティティです。

（注）　物理デバイス上で、最大 2 つの SPAN モニタリング セッションを保有できます。

VDC 内に作成した論理エンティティは、この VDC 内のユーザだけが使用できます。これは、他の VDC 内の別の論理エンティティとして同一の識別子が存在する場合でも同様です。たとえば、個々の VDC は最大 4096 の VLAN をサポートできます。Cisco NX-OS ソフトウェアは最大 4 つの VDC をサポートするため、一意の VLAN の数は 16,384 となります。VDC 管理者は VLAN ID を、同じ物理デバイス上の他の VDC で使用されている VLAN ID とは独立して設定できます。たとえば、VDC A の管理者と VDC B の管理者がそれぞれ VLAN 100 を作成した場合、これらの VLAN は、内部的には個別の一意の識別子にマッピングされます（図 1-4 を参照）。

図 1-4　VDC の VLAN 設定例



VDC リソース テンプレート

ネットワーク管理者は、リソース テンプレートを使用してリソースを VDC に割り当てることができます。各リソース テンプレートを使用すると、一連のリソースを 1 つの VDC に割り当てる方法を指定できます。VDC の作成時に VDC リソース テンプレートを使用すると、VDC 内に作成可能な特定の論理エンティティ数を制限できます。たとえば、ポート チャネル、SPAN モニタリング セッション、VLAN、IPv4 および IPv6 ルート メモリ、VRF などの論理エンティティです。VDC リソース テンプレートは独自に作成することも、Cisco NX-OS ソフトウェアに付属のデフォルトの VDC リソース テンプレートを使用することもできます。

VDC リソース テンプレートの詳細については、第 2 章「VDC リソース テンプレートの設定」を参照してください。

設定ファイル

各 VDC は、NVRAM 内に個別の設定ファイルを維持します。これには、VDC に割り当てられたインターフェイス設定のほか、VDC ユーザ アカウント、VDC ユーザ ロールといった、すべての VDC 固有の設定要素が反映されます。VDC 設定ファイルが個別に維持されることで、セキュリティと障害分離が保証され、他の VDC に対して行われる設定変更から VDC を保護できます。

個別の VDC 設定ファイルによって、設定の分離も可能になります。各 VDC のリソースに、互いに重複する ID を割り当てた場合でも、他の VDC の設定に影響が及ぶことはありません。たとえば、複数の VDC に対し、同一の VRF ID、ポート チャネル番号、VLAN ID、および管理 IP アドレスを設定することもできます。

VDC の管理

各 VDC は、異なる VDC 管理者によって管理できます。ある VDC に対して VDC 管理者が行う処理は、他の VDC ユーザに影響を与えません。VDC 管理者は VDC 内で、この VDC に割り当てられたリソースの設定を作成、変更、および削除できますが、これによって他の VDC が影響を受けることはありません。

ここでは、次の内容について説明します。

VDC デフォルト ユーザ ロール

Cisco NX-OS ソフトウェアには、VDC を管理するユーザ アカウントに対し、ネットワーク管理者が割り当てることのできるデフォルトのユーザ ロールがあります。これらの各ユーザ ロールを使用すると、デバイスにログインしたユーザが実行可能なコマンドのセットを有効にできます。ユーザが実行を許可されていないすべてのコマンドは、ユーザから非表示にされているか、またはエラーを返します。

（注）　VDC 内でユーザ アカウントを作成するには、network-admin または vdc-admin ロールが必要です。

Cisco NX-OS ソフトウェアには、VDC の管理におけるさまざまな権限レベルのデフォルト ユーザ ロールが用意されています。各ロールの種類は次のとおりです。

- network-admin - network-admin ロールはデフォルト VDC 内だけに存在し、すべてのグローバル コンフィギュレーション コマンド（**reload** や **install** など）および物理デバイスのすべての機能へのアクセスが可能です。カスタム ユーザ ロールには、これらのネットワーク管理者専用のコマンドや管理者だけを対象としたその他のコマンドへのアクセス権が付与されません。デバイスの物理状態に関するすべてのコマンドにアクセスできるのは、ネットワーク管理者だけです。このロールでは、ソフトウェアのアップグレードやトラフィックのイーサネット アナライザの実行などのシステムに影響する機能を実行できます。ネットワーク管理者は VDC の作成と削除、これらの VDC へのリソースの割り当て、VDC に予約されたデバイス リソースの管理、すべての VDC 内での機能設定を行えます。また、ネットワーク管理者はデフォルト VDC から **switchto vdc** コマンドを使用することで、デフォルト以外の VDC にもアクセスできます。ネットワーク管理者が デフォルト以外の VDC に切り替えると、vdc-admin 権限を取得します。この権限はデフォルト以外の VDC で使用できる最上位の権限です。
- network-operator：network-operator ロールはデフォルト VDC 内だけに存在し、物理デバイス上のすべての VDC についての情報の表示を許可します。このロールを使用すると、**show running-config vdc** や **show install all status** などのネットワーク オペレータ専用の **show** コマンドにアクセスできます。network-operator ロールを持つユーザは、デフォルト VDC から **switchto vdc** コマンドを使用することで、デフォルト以外の VDC にもアクセスできます。
- vdc-admin：vdc-admin ロールを持つユーザは、1 つの VDC 内の全機能を設定できます。network-admin または vdc-admin ロールのいずれかを持つユーザは、VDC 内で、ユーザ アカウントを作成、変更、または削除できます。VDC に割り当てたインターフェイスに対するすべての設定は、この VDC 内で実行する必要があります。vdc-admin ロールを持つユーザには、物理デバイス関連のコンフィギュレーション コマンドの実行は許可されません。
- vdc-operator：vdc-operator ロールを割り当てられたユーザは、この VDC に対する情報だけを表示できます。network-admin または vdc-admin ロールのいずれかを持つユーザは、VDC 内で、ユーザ アカウントに vdc-operator ロールを割り当てることができます。vdc-operator ロールを持つユーザは、VDC の設定変更は許可されません。

必要な VDC が 3 つ以下の場合、admin VDC をデフォルト VDC のままにして、その他の VDC をアクティブ データ プレーンの仮想スイッチとして使用することをお勧めします。グローバル コンフィギュレーション（network-admin ロール）を変更できる管理者を選択するための デフォルトの VDC アクセスが制限されていることを確認してください。デフォルト VDC では一部の機能（CoPP、レート リミット、および IP トンネル）だけを設定できることに注意してください。

デフォルト VDC はデータ プレーン トラフィックに使用する必要がある場合、デフォルト VDC 設定アクセスを必要としているものの、グローバル設定は必要ない管理者を vdc-admin ロールに割り当てる必要があります。このロールでは、管理機能がデフォルト VDC だけに制限され、グローバル VDC コンフィギュレーション コマンドにはアクセスできません。ユーザ アカウントおよびロールの詳細については、『*Cisco DCNM Security Configuration Guide, Release 5.x*』を参照してください。

コンフィギュレーション モード

Cisco NX-OS ソフトウェアには、VDC に対して主に 2 つのコンフィギュレーション モードが用意されています。デフォルト VDC 内で使用する VDC 設定モードと、VDC 自身の中で使用するグローバル コンフィギュレーション モードです。

デフォルト VDC で VDC コンフィギュレーション モードを使用すると、VDC にインターフェイスを割り当てたり、VDC の属性を変更したりできます。デフォルト VDC では、グローバル コンフィギュレーション モードから VDC コンフィギュレーション モードに切り替えることができます。VDC コンフィギュレーション モードには、network-admin ロールを持つユーザだけがアクセスできます。次に、VDC コンフィギュレーション モードを開始する方法を示します。

```
switch# config t
switch(config)# vdc Enterprise
switch(config-vdc)#
```

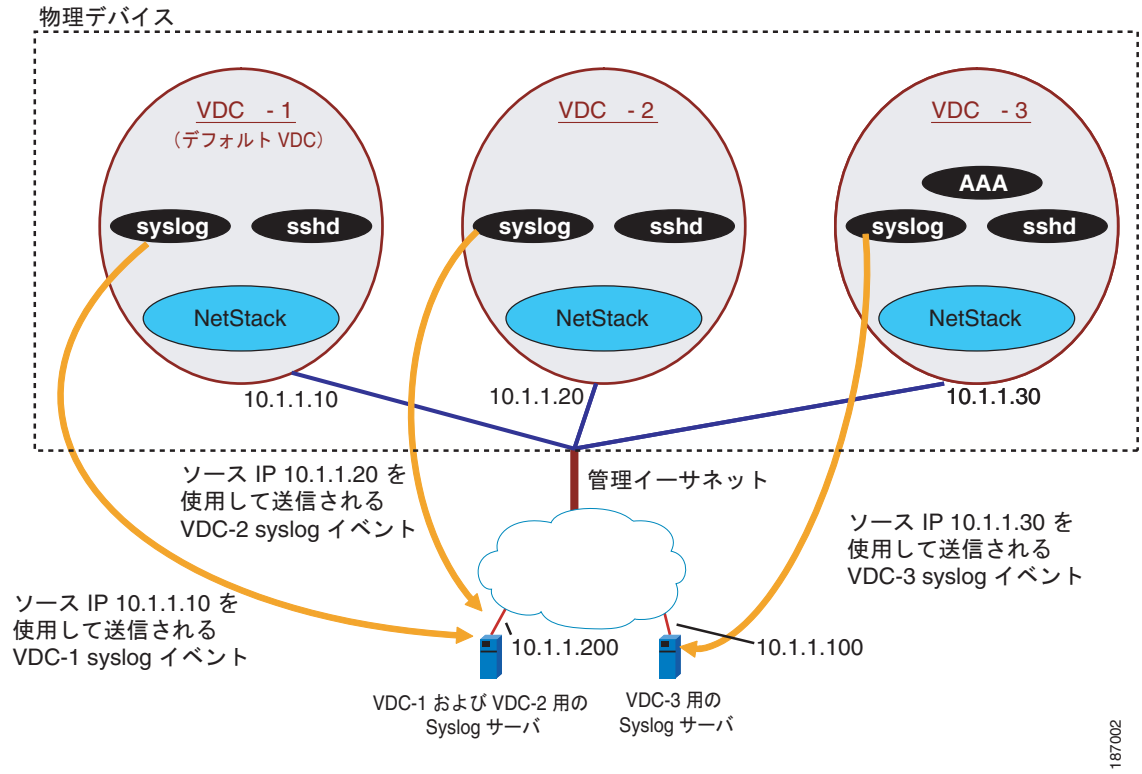
VDC でのグローバル コンフィギュレーション モードでは、デフォルト以外の VDC に対して Cisco NX-OS の各機能を設定できます。このコンフィギュレーション モードにアクセスするには、VDC にログインし、グローバル コンフィギュレーション モードを開始します。この設定モードを使用するには、該当 VDC への読み取りおよび書き込みアクセスを許可するユーザ ロールが必要です。次に、VDC に対してグローバル コンフィギュレーション モードを開始する方法を示します。

```
switch-Enterprise# config t
switch-Enterprise(config)#
```

VDC の管理接続

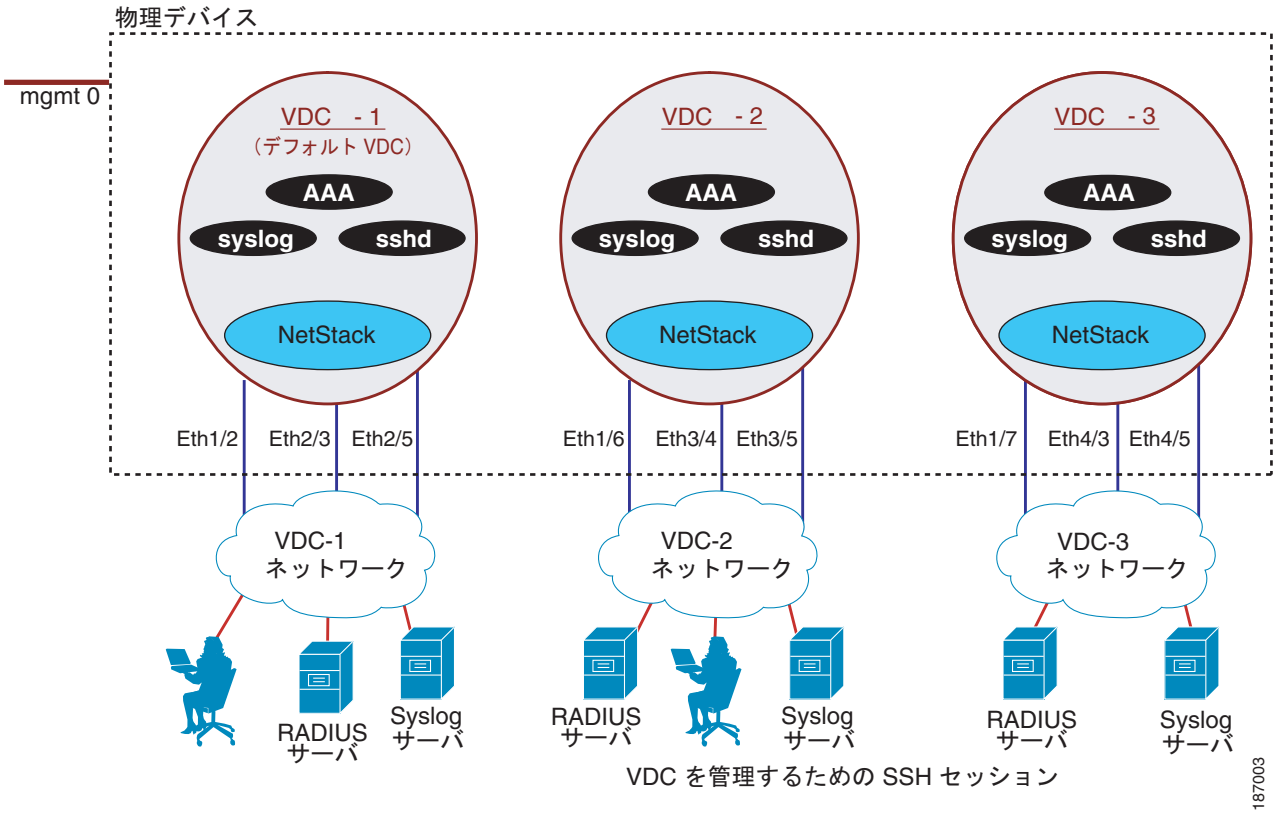
Cisco NX-OS ソフトウェアは、各 VDC の帯域外管理用に、仮想管理（mgmt 0）インターフェイスを備えています。このインターフェイスは、物理 mgmt 0 インターフェイスからアクセスする個別の IP アドレスを使用して設定できます（図 1-5 を参照）。この仮想管理インターフェイスを使用する場合は、1 つの管理ネットワークだけを使用するため、VDC 間で AAA サーバおよび Syslog サーバを共有できます。

図 1-5　帯域外 VDC 管理の例



VDC は帯域内管理もサポートします。VDC に割り当てられたいずれかのイーサネット インターフェイスを使用して、VDC にアクセスできます（図 1-6 を参照）。帯域内管理を使用する場合は、個別の管理ネットワークだけを使用するため、VDC 間で AAA サーバおよび Syslog サーバを分離できます。

図 1-6　帯域内 VDC 管理の例

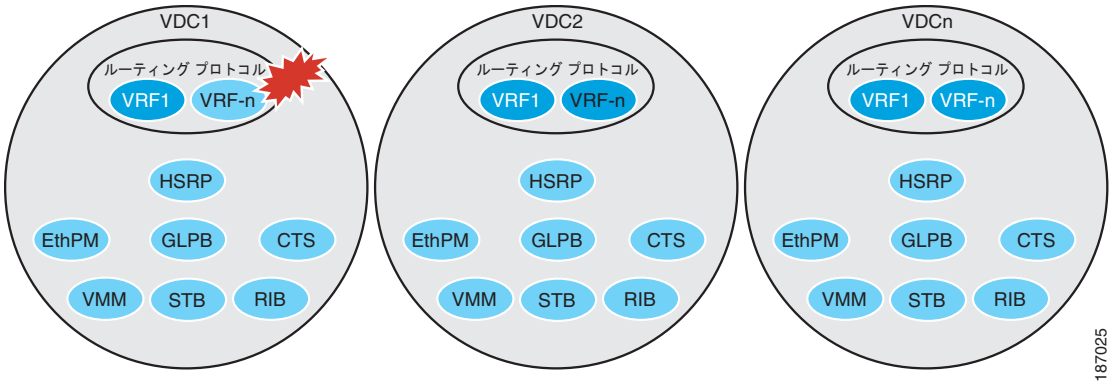


VDC の障害分離

VDC アーキテクチャでは、1 つの VDC で起きた障害が、同じ物理デバイス上の他の VDC に影響を与えることを防止できます。たとえば、ある VDC 内で OSPF プロセスが失敗しても、同じ物理デバイス上の他の VDC で実行される OSPF プロセスは影響を受けません。

図 1-7 に示すように、VDC 1 で実行されるプロセスに障害が発生した場合、他の VDC で実行されるプロセスにはまったく影響がありません。

図 1-7　VDC 内の障害分離



Cisco NX-OS ソフトウェアでは、VDC レベルでのデバッグおよび Syslog メッセージ ロギングも行えます。VDC 管理者はこれらのツールを使用して、VDC 内の問題のトラブルシューティングを行えます。VDC トラブルシューティングの詳細については、『*Cisco Nexus 7000 Series NX-OS Troubleshooting Guide, Release 5.x*』を参照してください。

Cisco NX-OS ソフトウェアには High Availability（HA; ハイ アベイラビリティ）機能が組み込まれているため、コントロール プレーンに障害が生じた場合、またはスイッチオーバーが発生した場合でも、他のデータ プレーンが受ける影響を最小限に抑えられます。サービス再起動、スーパーバイザ モジュールのステートフルなスイッチオーバー、インサービス ソフトウェア アップグレード（ISSU）など、さまざまな HA サービス レベルによってデータ プレーンの保護が実現されます。これらのすべてのハイ アベイラビリティ（HA）機能は、VDC をサポートします。Cisco NX-OS ソフトウェアの HA の詳細については、『*Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x*』を参照してください。

VDC での Cisco NX-OS 機能のサポート

Cisco NX-OS ソフトウェアの各機能に対する VDC のサポートは、機能によって異なります。現在の VDC では、ほとんどの Cisco NX-OS ソフトウェア機能の設定および操作をローカルに行えます。ただし、次の例外があります。

- Control Plane Policing（CoPP; コントロール プレーン ポリシング）：ハードウェア サポートにより、CoPP ポリシーはデフォルト VDC 内だけで設定できます。CoPP ポリシーは、物理デバイス上の全 VDC に適用されます。
- レート リミット：ハードウェア サポートにより、レート リミットはデフォルト VDC 内だけで設定できます。レート リミットは、物理デバイス上の全 VDC に適用されます。
- IP トンネル：VDC トンネルは、デフォルト VDC 内だけに作成できます。

特定の機能に対する VDC サポートについては、各機能の設定情報を参照してください。