



CHAPTER 1

Overview

This chapter describes virtual device contexts (VDCs) supported on the Cisco NX-OS devices.

This chapter includes the following sections:

- [Overview of VDCs, page 1-1](#)
- [VDC Architecture, page 1-2](#)
- [VDC Resources, page 1-4](#)
- [VDC Management, page 1-6](#)
- [VDC Fault Isolation, page 1-9](#)
- [Cisco NX-OS Feature Support in VDCs, page 1-10](#)

Overview of VDCs

The Cisco NX-OS software supports VDCs, which partition a single physical device into multiple logical devices that provide fault isolation, management isolation, address allocation isolation, service differentiation domains, and adaptive resource management. You can manage a VDC instance within a physical device independently. Each VDC appears as a unique device to the connected users. A VDC runs as a separate logical entity within the physical device, maintains its own unique set of running software processes, has its own configuration, and can be managed by a separate administrator.

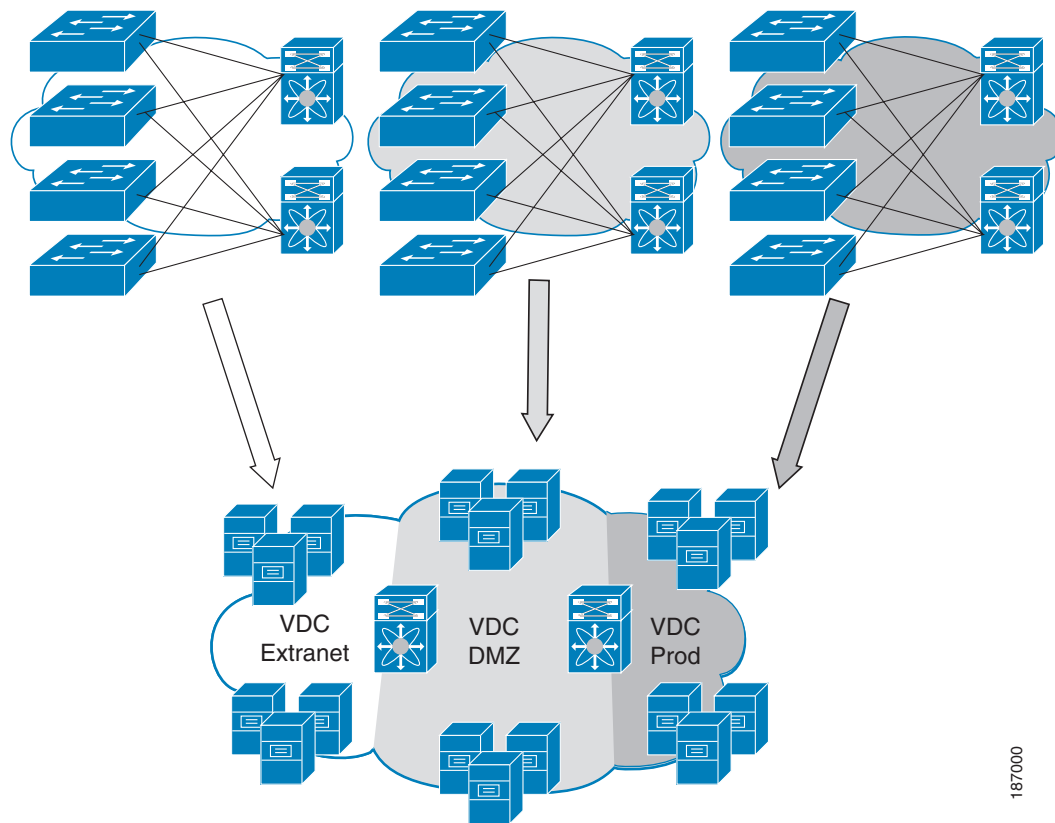
VDCs also virtualize the control plane, which includes all those software functions that are processed by the CPU on the active supervisor module. The control plane supports the software processes for the services on the physical device, such as the routing information base (RIB) and the routing protocols.

When you create a VDC, the NX-OS software takes several of the control plane processes and replicates them for the VDC. This replication of processes allows VDC administrators to use virtual routing and forwarding instance (VRF) names and VLAN IDs independent of those used in other VDCs. Each VDC administrator essentially interacts with a separate set of processes, VRFs, and VLANs.

[Figure 1-1](#) shows how the NX-OS software segments the physical device into VDCs. The benefits include VDC-level fault isolation, VDC-level administration, separation of data traffic, and enhanced security.

Send document comments to nexus7k-docfeedback@cisco.com

Figure 1-1 Segmentation of Physical Device



187000

VDC Architecture

The Cisco NX-OS software provides the base upon which VDCs are supported.

This section includes the following topics:

- [Kernel and Infrastructure Layer, page 1-2](#)
- [Default VDC, page 1-3](#)
- [Communication Between VDCs, page 1-4](#)

Kernel and Infrastructure Layer

The basis of the NX-OS software is the kernel and infrastructure layer. A single instance of the kernel supports all of the processes and VDCs that run on the physical device. The infrastructure layer provides an interface between the higher layer processes and the hardware resources of the physical device, such as the ternary content addressable memory (TCAM). Having a single instance of this layer reduces the complexity for the management of the hardware resources and helps scale the NX-OS software performance by avoiding duplication of the system management process (see [Figure 1-2](#)).

Send document comments to nexus7k-docfeedback@cisco.com

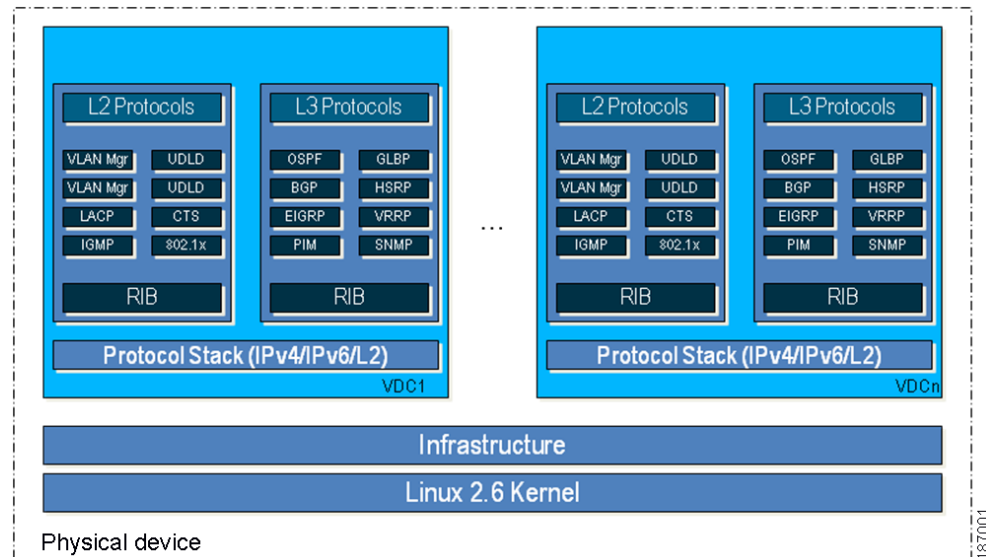
The infrastructure also enforces isolation across VDCs. A fault that is generated within a VDC does not impact the services in other VDCs. This feature limits the impact of software faults and greatly improves reliability of the device.

Along with the infrastructure layer, some nonvirtualized services have only a single instance for all VDCs. These infrastructure services participate in creating VDCs, moving resources across VDCs, and monitoring individual protocol services within a VDC.

The NX-OS software creates a virtualized control plane for each VDC. The virtualized control plane within the VDCs processes all the protocol-related events.

All the Layer 2 and Layer 3 protocol services run within a VDC. Each protocol service started within a VDC runs independently of the protocol services in other VDCs. The infrastructure layer protects the protocol services within VDC so that a fault or other problem in a service in one VDC does not impact other VDCs. The NX-OS software creates these virtualized services only when a VDC is created. Each VDC has its own instance of each service. These virtualized services are unaware of other VDCs and only work on resources assigned to that VDC. Only a user with the network-admin role can control the resources available to these virtualized services.

Figure 1-2 VDC Architecture



Default VDC

The physical device always has one VDC, the default VDC (VDC 1). When you first log in to a new NX-OS device, you begin in the default VDC.

You must be in the default VDC to create, change attributes for, or delete a nondefault VDC. The NX-OS software can support up to four VDCs, including the default VDC, which means that you can create up to three VDCs.

If you have the network-admin role privileges, you can manage the physical device and all VDCs from the default VDC (see the “[VDC Default User Roles](#)” section on page 1-6).

Send document comments to nexus7k-docfeedback@cisco.com

Communication Between VDCs

The NX-OS software does not support direct communication between VDCs on a single physical device. You must make a physical connection from a port allocated to one VDC to a port allocated to the other VDC to allow the VDCs to communicate. Each VDCs has its own VRFs for communicating with other VDCs (see the “[Logical Resources](#)” section on page 1-5).

VDC Resources

If you have the network-admin user role, you can allocate physical device resources exclusively for the use of a VDC. Once a resource is assigned to a specific VDC, you can manage it only from that VDC. The NX-OS software allows you to control how the logical and physical resources are assigned to each VDC. User logging directly into the VDC can only see this limited view of the device and can manage only those resources that the network administrator explicitly assigns to that VDC. Users within a VDC cannot view or modify resources in other VDCs.

**Note**

You must have the network-admin role to allocate resources to a VDC (see the “[VDC Default User Roles](#)” section on page 1-6).

This section includes the following topics:

- [Physical Resources](#), page 1-4
- [Logical Resources](#), page 1-5
- [VDC Resource Templates](#), page 1-6
- [Configuration Files](#), page 1-6

Physical Resources

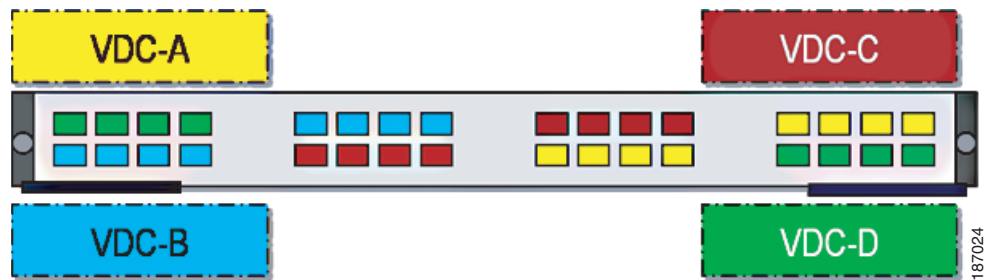
The only physical resources that you can allocate to a VDC are the Ethernet interfaces. Each physical Ethernet interface can belong to only one VDC at any given time. Initially, all physical interfaces belong to the default VDC (VDC 1). When you create a new VDC, the NX-OS software creates the virtualized services for the VDC without allocating any physical interfaces to it. After you create a new VDC, you can allocate a set of physical interfaces from the default VDC to the new VDC. Once you allocate a physical interface to a VDC, you can configure it only in that VDC and no other VDC has access to that interface, including the default VDC.

When you allocate an interface to a VDC, all configuration for that interface is erased. You, or the VDC administrator, must configure the interface from within the VDC. Only the interfaces allocated to the VDC are visible for configuration.

You can allocate the interfaces on your physical device in any combination, except for the interfaces on the Cisco Nexus 7000 Series 32-port 10-Gbps Ethernet module (N7K-M132XP-12). This module has eight port groups that consist of four interfaces each. You must you assign all four interfaces in a port group to the same VDC (see [Figure 1-3](#)).

Send document comments to nexus7k-docfeedback@cisco.com

Figure 1-3 Example Interface Allocation for Port Groups on a Cisco 7000 Series 10-Gbps Ethernet Module



For more information on port groups in the Cisco Nexus 7000 Series 32-port 10-Gbps Ethernet module, see the *Cisco Nexus 7000 Series Hardware Installation and Reference Guide*.

Logical Resources

Each VDC acts as a separate logical device within a single physical device, which means that all the namespaces are unique within a VDC.

When you create a VDC, it has its own default VLAN and VRF that is not shared with other VDCs. You can also create other logical entities within a VDC for the exclusive use of that VDC. These logical entities include SPAN monitoring sessions, port channels, VLANs, and VRFs.

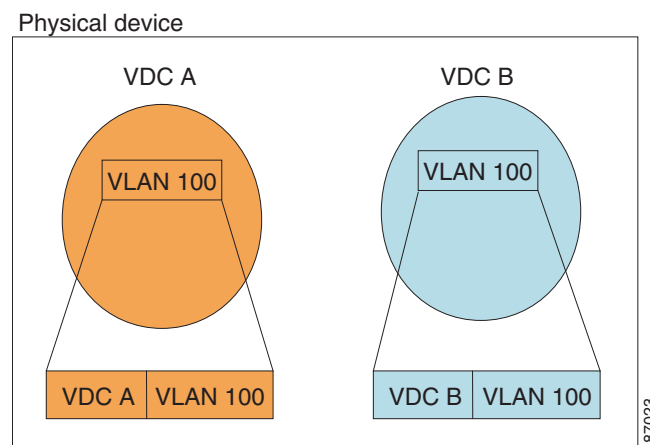


Note

You can have a maximum of two SPAN monitoring sessions on your physical device.

When you create a logical entity in a VDC, only users in that VDC can use it even when it has the same identifier as another logical entity in another VDC. For example, each VDC can support a maximum of 4096 VLANs. The NX-OS software supports up to four VDCs and, therefore, 16,384 unique VLANs. A VDC administrator can configure VLAN IDs independently of the VLAN IDs used in other VDCs on the same physical device. For example, if VDC administrators for VDC A and VDC B both create VLAN 100, these VLANs are internally mapped to separate unique identifiers (see [Figure 1-4](#)).

Figure 1-4 Example VLAN Configuration for VDCs



Send document comments to nexus7k-docfeedback@cisco.com

VDC Resource Templates

A network administrator can allocate resources to VDCs using resource templates. Each resource template describes how a set of resources are allocated to a VDC. When you create a VDC, you use a VDC resource template to set limits on the number of certain logical entities that you can create in the VDC. These logical entities include port channels, SPAN monitor sessions, VLANs, IPv4 and IPv6 route memory, and VRFs. You can create a VDC resource template or use the default VDC resource template provided by the NX-OS software.

For more information on VDC resource templates, see [Chapter 2, “Configuring VDC Resource Templates.”](#)

Configuration Files

Each VDC maintains a separate configuration file in NVRAM, reflecting the configuration of interfaces allocated to the VDC and any VDC-specific configuration elements such as VDC user accounts and VDC user roles. The separation of the VDC configuration files provides security and fault isolation that protects a VDC from configuration changes on another VDC.

Separate VDC configuration files also provide configuration isolation. The resources in each VDC might have IDs that overlap without affecting the configuration of the other VDCs. For example, the same VRF IDs, port-channel numbers, VLAN IDs and management IP address can exist on multiple VDCs.

VDC Management

Each VDC can be managed by a different VDC administrator. An action taken by a VDC administrator in one VDC does not impact users in other VDCs. A VDC administrator within a VDC can create, modify, and delete the configuration for resources allocated to VDC with no impact to other VDCs.

This section includes the following topics:

- [VDC Default User Roles, page 1-6](#)
- [Configuration Modes, page 1-7](#)
- [VDC Management Connections, page 1-8](#)

VDC Default User Roles

The Cisco NX-OS software has default user roles that the network administrator can assign to the user accounts that administer VDCs. These user roles make available a set of commands which the user can execute after logging into the device. All commands that the user is not allowed to execute are hidden from the user or return an error.

**Note**

You must have the network-admin or vdc-admin role to create user accounts in a VDC.

Send document comments to nexus7k-docfeedback@cisco.com

The Cisco NX-OS software provides default user roles with different levels of authority for VDC administration as follows:

- **network-admin**—The network-admin role exists only in the default VDC and allows access to all the global configuration commands. Network administrators have access to all features on the physical device. Network administrators can create and delete VDCs, allocate resources for these VDCs, manage device resources reserved for the VDCs, and configure features within any VDC. Network administrators can access nondefault VDCs using the **switchto vdc** command from the default VDC. Only the network administrator can access all the commands related to the physical state of the device.
- **network-operator**—The network-operator role exists only in the default VDC and allows users to display information for all VDCs on the physical device. Users with network-operator roles can access nondefault VDCs using the **switchto vdc** command from the default VDC.
- **vdc-admin**—Users who have the vdc-admin role can configure all features within a VDC. Users with either the network-admin or vdc-admin role can assign the vdc-admin role to user accounts within the VDC. All configurations for the interfaces allocated to a VDC must be performed within the VDC. Users with the vdc-admin role are not allowed to execute any configuration commands related to the physical device.
- **vdc-operator**—Users assigned with the vdc-operator role can display information only for the VDC. Users with either the network-admin or vdc-admin role can assign the vdc-operator role to user accounts within the VDC. The vdc-operator role does not allow the user to change the configuration of the VDC.

If you do not need more than three VDCs, we recommend that you leave the default VDC as an admin VDC and use the other VDCs as active data-plane virtual switches. Make sure to restrict default VDC access to a select few administrators who are allowed to modify the global configuration (network-admin role). Remember that you can configure some features (such as CoPP, rate limits, and IP tunnels) only in the default VDC.

If the default VDC must be used for data-plane traffic, administrators who require default VDC configuration access but not global configuration access should be assigned the vdc-admin role. This role restricts administrative functions to the default VDC exclusively and prevents access to global VDC configuration commands.

For more information on user accounts and roles, see the [Cisco Nexus 7000 Series NX-OS Security Configuration Guide, Release 4.1](#).

Configuration Modes

The NX-OS software has two main configuration modes for VDCs, VDC configuration mode in the default VDC and global configuration mode within the VDC itself.

In the VDC configuration mode in the default VDC, you can allocate interfaces to the VDCs and change VDC attributes. You can enter VDC configuration mode from global configuration mode on the default VDC. Only users with the network-admin role can access VDC configuration mode. The following example shows how to enter VDC configuration mode:

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

Send document comments to nexus7k-docfeedback@cisco.com

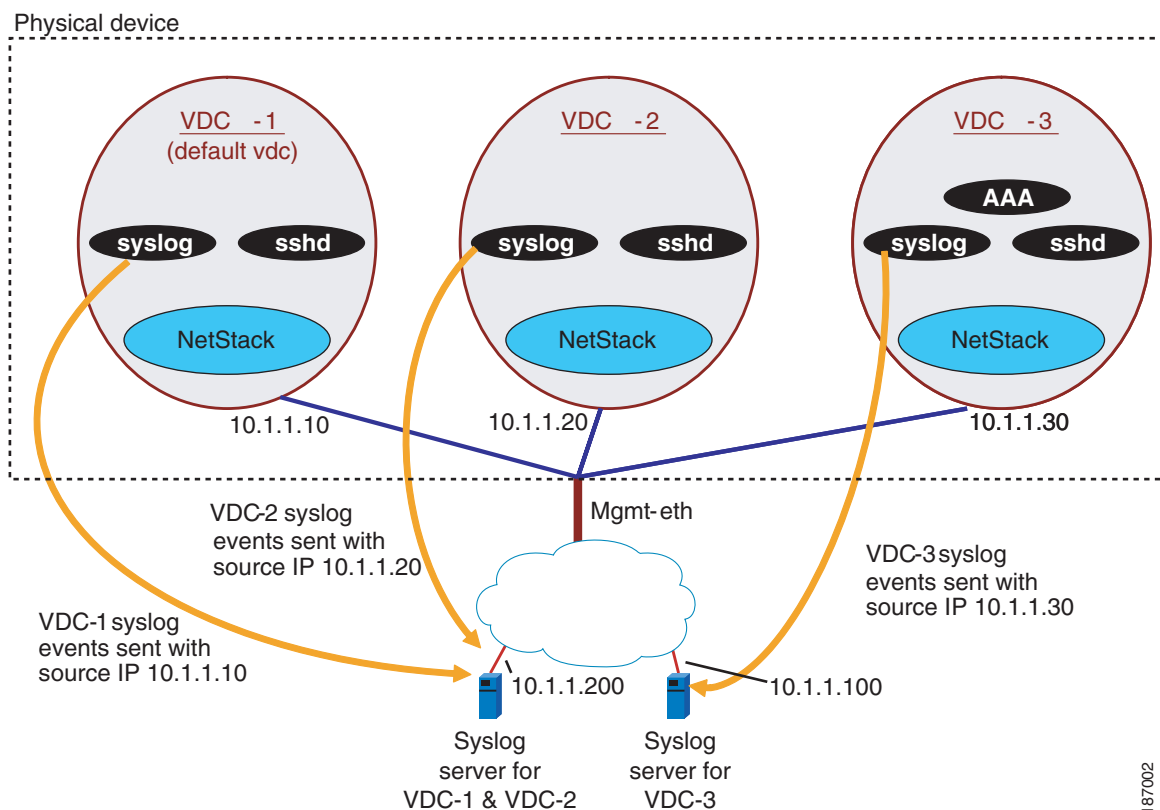
In the global configuration mode in a VDC, you can configure NX-OS features for nondefault VDCs. You can access this configuration mode by logging in to the VDC and entering global configuration mode. You must have a user role that allows read and write access to the VDC to use this configuration mode. The following example shows how to enter global configuration mode for a VDC:

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

VDC Management Connections

The NX-OS software provides a virtual management (mgmt 0) interface for out-of-band management for each VDC. You can configure this interface with a separate IP address that is accessed through the physical mgmt 0 interface (see Figure 1-5). Using the virtual management interface allows you to use only one management network, which can share the AAA servers and syslog servers among the VDCs.

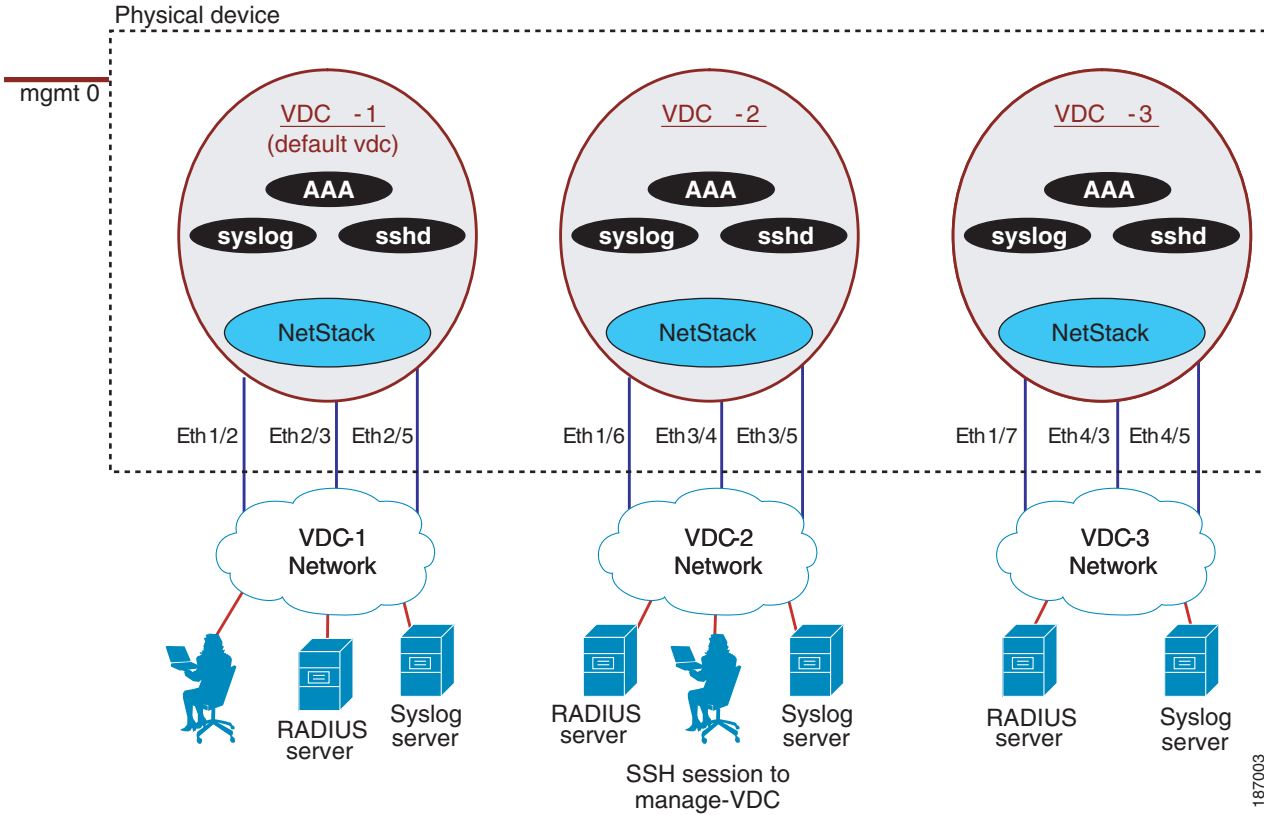
Figure 1-5 Out-of-Band VDC Management Example



VDCs also support in-band management. You can access the VDC using one of the Ethernet interface allocated to the VDC (see Figure 1-6). Using the in-band management allows you to use only separate management networks, which ensure the separation of the AAA servers and syslog servers among the VDCs.

[Send document comments to nexus7k-docfeedback@cisco.com](mailto:nexus7k-docfeedback@cisco.com)

Figure 1-6 In-Band VDC Management Example



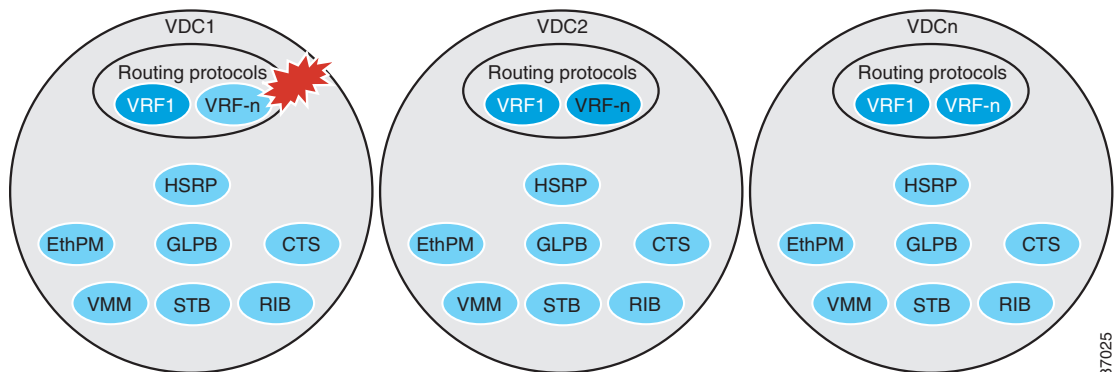
187003

VDC Fault Isolation

The VDC architecture can prevent failures within one VDC from impacting other VDCs on the same physical device. For instance, an OSPF process that fails in one VDC does not affect the OSPF processes in other VDCs in the same physical device.

Figure 1-7 shows that a fault in a process running in VDC 1 does not impact any of the running processes in the other VDCs.

Figure 1-7 Fault Isolation within VDCs



187025

Send document comments to nexus7k-docfeedback@cisco.com

The NX-OS software also provides debugging and syslog message logging at the VDC level. VDC administrators can use these tools to troubleshoot problems with the VDC.

For more information on VDC troubleshooting, see the *Cisco Nexus 7000 Series NX-OS Troubleshooting Guide, Release 4.1*.

The Cisco NX-OS software incorporates high availability (HA) features that minimize the impact on the data plane should the control plane fail or a switchover occurs. The different HA service levels provide data plane protection, including service restarts, stateful supervisor module switchovers, and in-service software upgrades (ISSUs). All of these high availability features support VDCs.

For more information on HA in the NX-OS software, see the *Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 4.1*.

Cisco NX-OS Feature Support in VDCs

VDC support for the Cisco NX-OS software features varies, depending on the feature. For most of the NX-OS software features, configuration and operation is local to the current VDC. However, there are the following exceptions:

- Control plane policing (CoPP)—Because of the hardware support, you can configure CoPP policies only in the default VDC. The CoPP policies apply across all VDCs on the physical device.
- Rate limits—Because of the hardware support, you can configure rate limits only in the default VDC. The rate limits apply across all VDCs on the physical device.
- IP tunnels—You can create VDC tunnels only in the default VDC.

For information on VDC support for a specific feature, see the configuration information for that feature.