Overview

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

- Licensing Requirements, on page 1
- Information About VDCs, on page 1
- VDC Architecture, on page 3
- VDC Resources, on page 5
- VDC Management, on page 10
- VDC Fault Isolation, on page 14
- VDC Module Type Compatibility, on page 14
- Cisco NX-OS Feature Support in VDCs, on page 15

Licensing Requirements

For a complete explanation of Cisco NX-OS licensing recommendations and how to obtain and apply licenses, see the *Cisco NX-OS Licensing Guide*.

Information About 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.

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 managed by a separate administrator.

The following guidelines and limitations apply to VDC user roles:

- All VDC users have bootlfash read access, for all VDCs using Python shell access.
- The default VDC admin user has read/write access across VDCs which use Python shell access.
- EEM events are always executed using network-admin privileges.

VDC Operator role users only have access to CLI command ***source*** to execute Python scripts.

VDCs also virtualize the control plane, which includes all those software functions that are processed by 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.

Beginning with Cisco NX-OS Release 5.2(1) for the Cisco Nexus 7000 Series devices, you can configure Fibre Channel over Ethernet (FCoE). See the Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500 for information about FCoE. Beginning with Cisco NX-OS Release 6.1(1), you can enable FCoE on the F248XP-25[E] Series with Supervisor 2 and Supervisor 2E modules. You must configure a dedicated storage VDC to run FCoE on the Cisco Nexus 7000 Series devices. See Chapter 5, “Managing VDCs,” for information about configuring storage VDCs.

Beginning with Cisco NX-OS Release 6.2(2), the Supervisor 1 module supports an admin VDC with the same functionalities of Supervisor 2/2e modules. You can only allocate mgmt0 interface to the admin VDC. The Supervisor 2E module supports the new Cisco Nexus 7718 switch and the Cisco Nexus 7710 switches. These switches support F2e line cards only. For more information, see the Cisco Nexus 7000 Series Hardware Installation and Reference Guide.

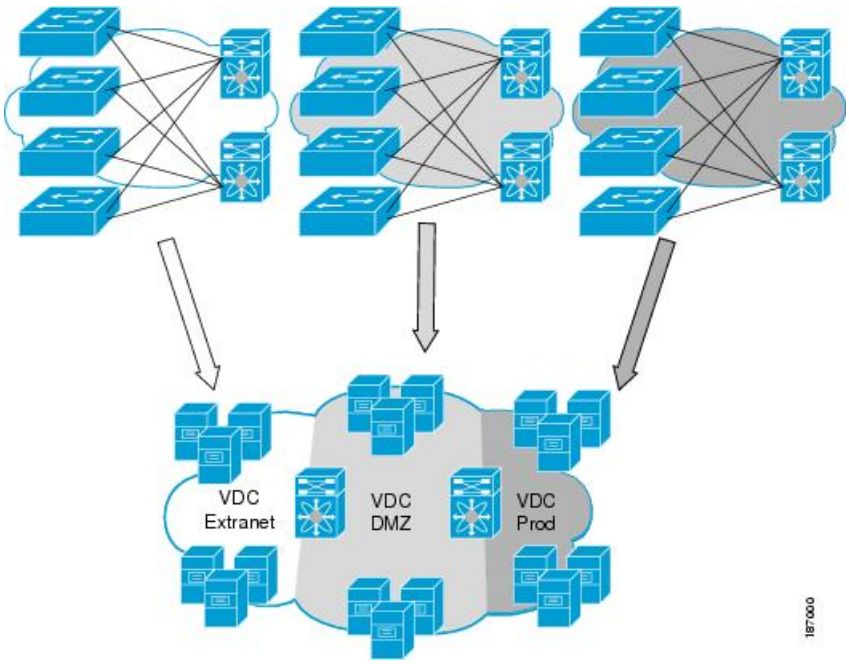
When upgrading from any releases before Release 6.2(2) by changing the boot variables and rebooting with the new code using a manual upgrade, all the interfaces that are assigned to default VDC (VDC 1) after the upgrade might become unallocated. You cannot perform configuration conversion or data structure conversion during a manual upgrade. You might be required to manually allocate the interfaces to the correct nonadmin VDC and copy all configurations to startup and reload the switch. Verify using the **show vdc membership** command.

When you create a VDC, the Cisco NX-OS software takes several of the control plane processes and replicates them for the VDC. This replication of processes allows VDC administrators working in Ethernet VDCs to use virtual routing and forwarding (VRF) instance 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.

Note However, the numbers must be unique between FCoE and Ethernet VLANs. That is, the numbers that are used on the FCoE VLANs in the storage VDCs must be different than any of the VLAN numbers used in the Ethernet VDCs. You can repeat VLAN numbers within separate Ethernet VDCs. The VLAN numbering space for FCoE and Ethernet is shared only for those VDCs configured for port sharing. See the Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500 for information about configuring FCoE.

The figure below shows how the Cisco 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.

Figure 1: Segmentation of a Physical Device



VDC Architecture

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

Kernel and Infrastructure Layer

The basis of the Cisco 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 Cisco NX-OS software performance by avoiding duplication of the system management process (see the figure below).

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 the reliability of the device.

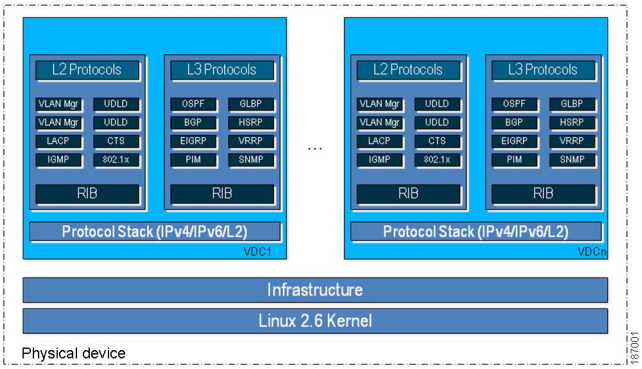
Along with the infrastructure layer, some nonvirtualized services have only a single instance for all VDCs. These infrastructure services participate in creating VDCs, moving resources across VDCs, and monitoring individual protocol services within a VDC.

The Cisco 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 that is started within a VDC runs independently of the protocol services in other VDCs. The infrastructure layer protects the protocol services within a VDC so that a fault or other problem in a service in one VDC does not impact other VDCs. The Cisco 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 that are assigned to that VDC. Only a user with the network-admin role can control the resources available to these virtualized services.

Figure 2: VDC Architecture



MAC Addresses

The default VDC has a MAC address. Subsequent nondefault VDCs that you create are assigned MAC addresses automatically as part of the bootup process.

Default VDC

The physical device always has at least one VDC, the default VDC (VDC 1). When you first log in to a new Cisco NX-OS device, you begin in the default VDC. You must be in the default VDC or admin VDC to create, change attributes for, or delete a nondefault VDC. Cisco NX-OS releases prior to 6.1 can support up to four VDCs, including the default VDC, which means that you can create up to three nondefault VDCs.

If you have the network-admin role privileges, you can manage the physical device and all VDCs from the default VDC.

Communication Between VDCs

The Cisco 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.

Storage VDCs

The storage VDC is one of the nondefault VDCs and it does need a license. However, a storage VDC does not need a VDC license because it relies on the FCoE license installed to enable the FCoE function on the modules. Beginning with Cisco NX-OS Release 5.2(1) for the Nexus 7000 Series devices, you can run FCoE on the F1, F2 and F2e Series modules, depending upon your specific release version. You can create separate storage VDCs to run FCoE. You can have only one storage VDC on the device, and you cannot configure the default VDC as a storage VDC.

Note You cannot perform multiple VLAN-VSAN mapping configuration in a single instance in Cisco NX-OS Release 8.4(1). You have to come out of the configuration mode after configuring a single VLAN-VSAN mapping and then re-enter the configuration mode to configure the next mapping.

Note Starting with Cisco NX-OS Release 6.2(2), we do not support the interoperability of F1 and F2 Series modules in any VDC, either in a dedicated mode or in a shared mode. If you have configured F1 and F2 Series modules as supported line cards in a storage VDC during an In-Service Software Upgrade (ISSU) to Cisco NX-OS Release 6.2(2) or later releases, before ISSU, reconfigure your storage VDC by using the limit-resource module-type command (for information, see the see the "Changing VDC Resource Limits" section) to avoid any unnecessary disruption to the system.

After you create the storage VDC, you assign specified FCoE VLANs. Finally, you configure interfaces on the Cisco Nexus 7000 Series device as either dedicated FCoE interfaces or as shared interfaces, which can carry both Ethernet and FCoE traffic. See the *Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500* for information on configuring FCoE.

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 Cisco NX-OS software allows you to control how the logical and physical resources are assigned to each VDC. Users 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

Physical Resources

The only physical resources that you can allocate to a VDC are the Ethernet interfaces. For the Ethernet VDCs, each physical Ethernet interface can belong to only one VDC, including the default VDC, at any given time. When you are working with shared interfaces in the storage VDC, the physical interface can belong to both one Ethernet VDC and one storage VDC simultaneously, but to no more than one of each.

Initially, all physical interfaces belong to the default VDC (VDC 1). When you create a new VDC, the Cisco 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.

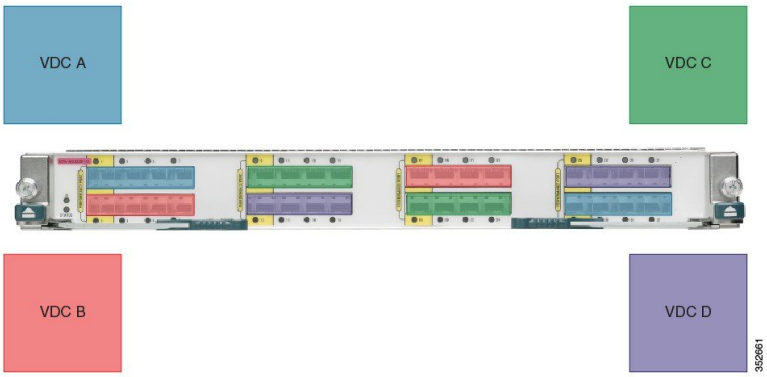
When you allocate an interface to a VDC, all configuration for that interface is erased. You, or the VDC administrator, must configure the interface from within the VDC. Only the interfaces allocated to the VDC are visible for configuration.

Note Beginning with Cisco NX-OS Release 5.2(1) for Nexus 7000 Series devices, all members of a port group are automatically allocated to the VDC when you allocate an interface.

The following Cisco Nexus 7000 Series Ethernet modules have the following number of port groups and interfaces:

- N7K-M202CF-22L (1 interface x 2 port groups = 2 interfaces 100G modules)—There are no restrictions on the interface allocation between VDCs.
- N7K-M206FQ-23L (1 interface x 6 port groups = 6 interfaces 40G modules)—There are no restrictions on the interface allocation between VDCs.
- N7K-M224XP-23L (1 interface x 24 port groups = 24 interfaces 10G modules)—There are no restrictions on the interface allocation between VDCs.
- N7K-M108X2-12L (1 interface x 8 port groups = 8 interfaces)—There are no restrictions on the interface allocation between VDCs.
- N7K-M148GS-11L, N7K-M148GT-11, N7K-M148GS-11 (12 interfaces x 4 port groups = 48 interfaces) and N7K-M148GT-11L (same as non-L M148) (1 interface x 48 port groups = 48 interfaces)—There are no restrictions on the interface allocation between VDCs, but we recommend that interfaces that belong to the same port group be in a single VDC.
- N7K-M132XP-12 (4 interfaces x 8 port groups = 32 interfaces) and N7K-M132XP-12L (same as non-L M132) (1 interface x 8 port groups = 8 interfaces)—All M132 cards require allocation in groups of 4 ports and you can configure 8 port groups. Interfaces belonging to the same port group must belong to the same VDC. See the example for this module in Figure 1-3.
- N7K-M132XP-12L (same as non-L M132) (1 interface x 8 port groups = 8 interfaces)—All M132 cards require allocation in groups of 4 ports and you can configure 8 port groups.

Figure 3: Example Interface Allocation for Port Groups on a Cisco 7000 Series 10-Gbps Ethernet Module (N7K-M132XP-12)

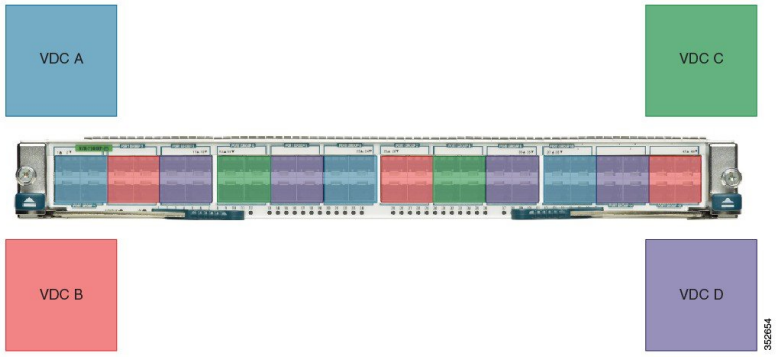


On the Cisco Nexus 7000 Series 32-port, 10-Gbps Ethernet module N7K-F132XP-15, you must allocate the interfaces on your physical device in the specified combination. This module has 16 port groups that consist of 2 ports each (2 interfaces x 16 port groups = 32 interfaces). Interfaces that belong to the same port group must belong to the same VDC (see the figure below). For more information about ports that can be paired. For more information about implementing FCoE on this module, see the *Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*.

Figure 4: Example Interface Allocation for Port Groups on a Cisco 7000 Series 10-Gbps Ethernet Module (N7K-F132XP-15)

On the Cisco Nexus 7000 Series 48-port, 10-Gbps Ethernet modules N7K-F248XP-25[E] and N7K-F248XT-25[E], you must allocate the interfaces on your physical device in the specified combination. These modules have 12 port groups that consist of 4 ports each (4 interfaces x 12 port groups = 48 interfaces). Interfaces that belong to the same port group must belong to the same VDC (see the figure below).

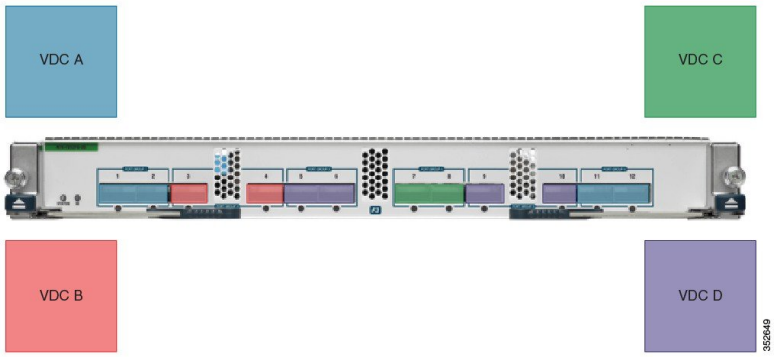
Figure 5: Example Interface Allocation for Port Groups on the Cisco Nexus 7000 Series 10-Gbps Ethernet Module N7K-F248XP-25[E] and N7K-F248XT-25[E]



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

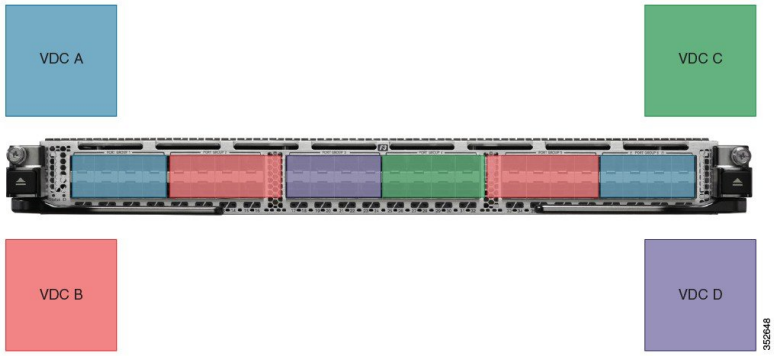
On the Cisco Nexus 7000 Series 12-port, 40-Gbps Ethernet modules N7K-F312FQ-25, you must allocate the interfaces on your physical device in the specified combination. These modules have 6 port groups that consist of 2 ports each (2 interfaces x 6 port groups = 12 interfaces). Interfaces that belong to the same port group must belong to the same VDC.

Figure 6: Cisco Nexus 7000 Series 12-port, 40-Gbps Ethernet modules N7K-F312FQ-25



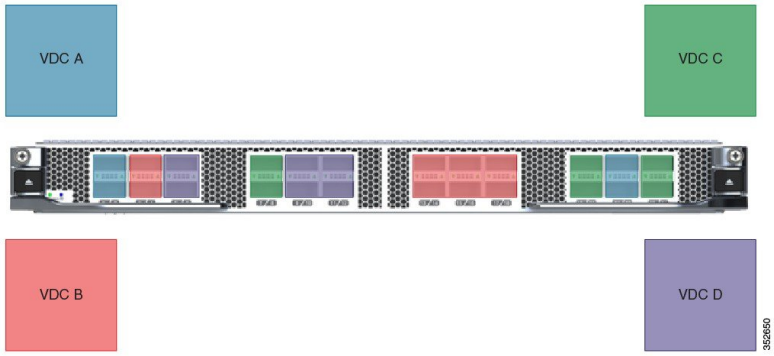
On the Cisco Nexus 7700 Series 48-port, 10-Gbps Ethernet modules N7K-F348XP-25, you must allocate the interfaces on your physical device in the specified combination. These modules have 6 port groups that consist of 8 ports each (8 interfaces x 6 port groups = 48 interfaces). Interfaces that belong to the same port group must belong to the same VDC.

Figure 7: Cisco Nexus 7700 Series 48-port, 10-Gbps Ethernet modules N77-F348XP-25



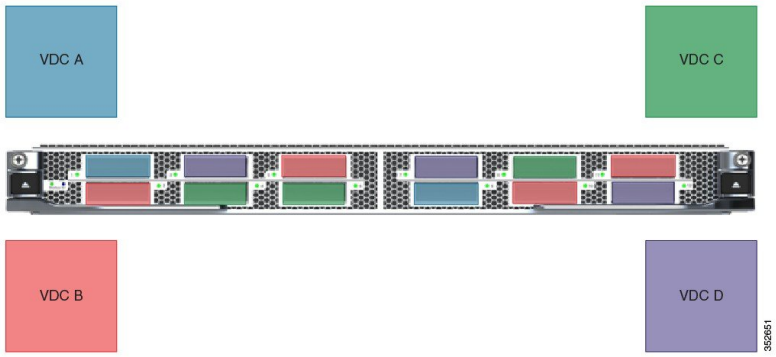
On the Cisco Nexus 7700 Series 24-port, 40-Gbps Ethernet modules N7K-F324QF-25, you must allocate the interfaces on your physical device in the specified combination. These modules have 12 port groups that consist of 2 ports each (2 interfaces x 12 port groups = 48 interfaces). Interfaces that belong to the same port group must belong to the same VDC.

Figure 8: Cisco Nexus 7700 Series 24-port, 40-Gbps Ethernet modules N77-F324QF-25



On the Cisco Nexus 7700 Series 12-port, 100-Gbps Ethernet modules N7K-F312CK-26, you must allocate the interfaces on your physical device in the specified combination. These modules have 12 port groups that consist of 1 port each (1 interface x 12 port groups = 12 interfaces).

Figure 9: Cisco Nexus 7700 Series 12-port, 100-Gbps Ethernet modules N77-F312CK-26



Note When the breakout feature is used on the N7K-40 and N77-40G modules, all interfaces that are broken out stay in the same VDC as their original parent port group.

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. However, you cannot use an identical namespace within a storage VDC and an Ethernet VDC.

When you create a VDC, it has its own default VLAN and VRF that are 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, which include SPAN monitoring sessions, port channels, VLANs, and VRFs, are for Ethernet VDCs.

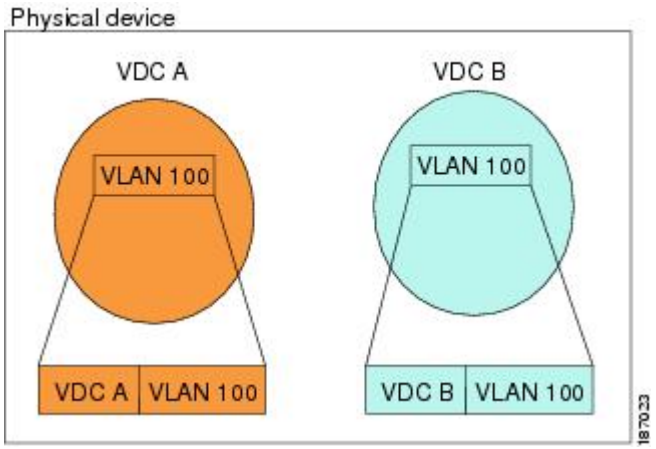
Note You can have a maximum of two SPAN monitoring sessions on your physical device.

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.

A VDC administrator can configure VLAN IDs independently of the VLAN IDs used in other Ethernet VDCs on the same physical device. For example, if VDC administrators for Ethernet VDC A and Ethernet VDC B both create VLAN 100, these VLANs are internally mapped to separate unique identifiers (see the figure below).

For more information on VDC support and the maximum number of VLANs, see the *Cisco Nexus 7000 Series NX-OS Verified Scalability Guide*.

Figure 10: Example VLAN Configuration for Ethernet VDCs



Note When you are working with both storage VDCs and Ethernet VDCs, the VLAN ID and logical entity must be entirely separate for the storage VDCs.

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 Cisco NX-OS software.

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 Ethernet 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.

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 that 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.

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 (such as **reload** and **install**) and all the features on the physical device. A custom user role is not granted access to these network-admin-only commands or to other commands that are scoped admin-only. Only the network administrator can access all the commands that are related to the physical state of the device. This role can perform system-impacting functions such as upgrading software and running an Ethernet analyzer on the traffic. 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 also access nondefault VDCs using the **switchto vdc** command from the default VDC. When network administrators switch to a nondefault VDC, they acquire vdc-admin permissions, which are the highest permissions available in a nondefault VDC.
- 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 create, modify, or remove 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 on the Supervisor 1 module. 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 Control Plane Policing [CoPP] and rate limits only in the default VDC. You cannot configure the default VDC as a storage 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 with the vdc-admin role. This role restricts administrative functions to the default VDC exclusively and prevents access to global VDC configuration commands.

Configuration Modes

The Cisco 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.

This example shows how to enter VDC configuration mode:

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

This example shows how to switch to VDC Enterprise from the default VDC:

```
switch# switchto vdc Enterprise
Cisco Nexus Operating System (NX-OS) Software
TAC support: http://www.cisco.com/tac
Copyright (c) 2002-2012, Cisco Systems, Inc. All rights reserved.
The copyrights to certain works contained in this software are
owned by other third parties and used and distributed under
license. Certain components of this software are licensed under
the GNU General Public License (GPL) version 2.0 or the GNU
Lesser General Public License (LGPL) Version 2.1. A copy of each
such license is available at
http://www.opensource.org/licenses/gpl-2.0.php and
http://www.opensource.org/licenses/lgpl-2.1.php
```

In the global configuration mode in a VDC, you can configure Cisco 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.

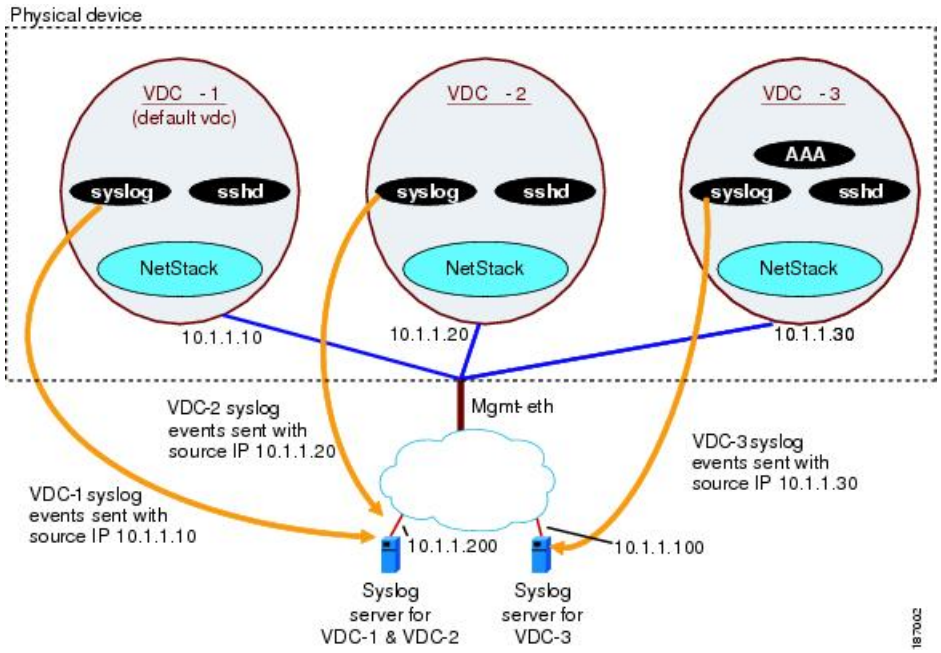
This example shows how to enter global configuration mode for a VDC:

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

VDC Management Connections

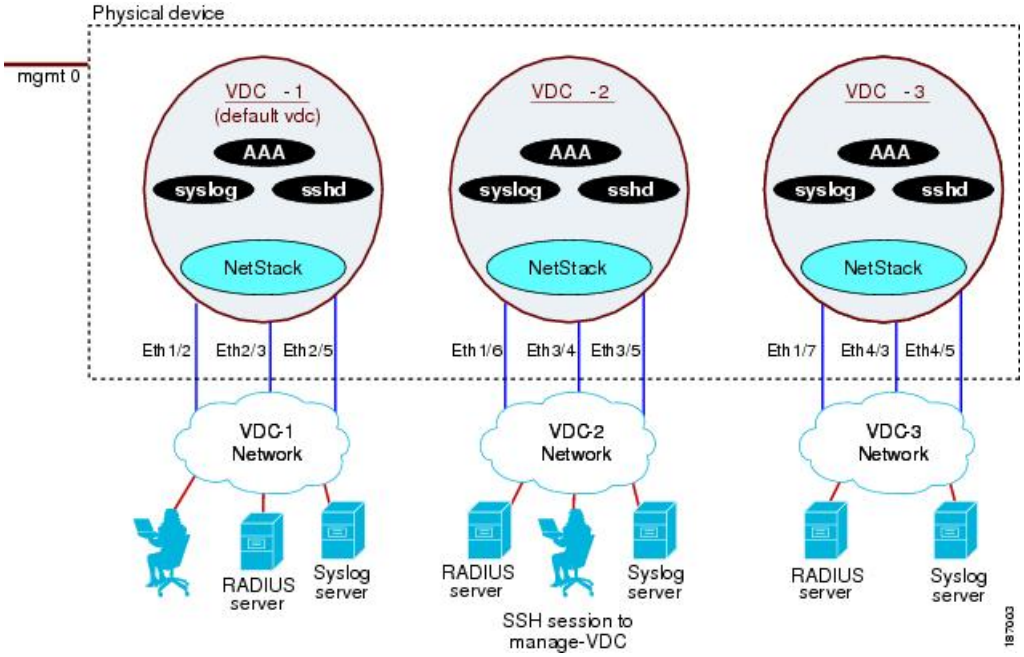
The Cisco NX-OS software provides a virtual management (mgmt 0) interface for out-of-band management for each VDC. You can configure this interface with a separate IP address that is accessed through the physical mgmt 0 interface (see Figure 1-7). Because the virtual management interface allows you to use only one management network, you can share the AAA servers and syslog servers among the VDCs.

Figure 11: Out-of-Band VDC Management Example



VDCs also support in-band management. You can access the VDC using one of the Ethernet interfaces that are allocated to the VDC (see the figure below). Because the in-band management allows you to use only separate management networks, you can ensure the separation of the AAA servers and syslog servers among the VDCs.

Figure 12: In-Band VDC Management Example

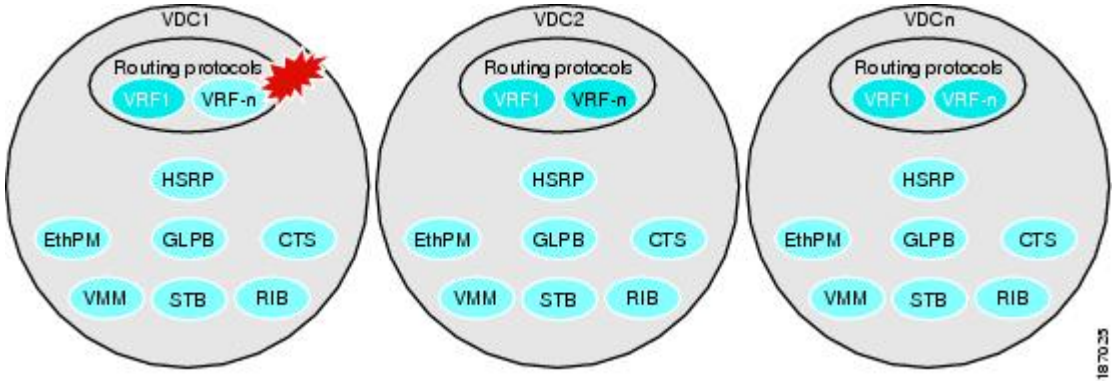


VDC Fault Isolation

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

The figure below shows that a fault in a process running in VDC 1 does not impact any of the running processes in the other VDCs.

Figure 13: Fault Isolation within VDCs



The Cisco 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 about VDC troubleshooting, see the *Cisco Nexus 7000 Series NX-OS Troubleshooting Guide*.

The Cisco NX-OS software incorporates high availability (HA) features that minimize the impact on the data plane if the control plane fails 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 about HA in the Cisco NX-OS software, see the *Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide*.

VDC Module Type Compatibility

Table 1: VDC Module Type Compatibility for Release 8.0(1)

	F1	F2	M2XL	F2e(F2CR)	F3	M3
F1	True	False	True	False	False	False
F2	False	True	False	True	True	False
M2XL	True	False	True	True	True	True
F2e(F2CR)	False	True	True	True	True	False

	F1	F2	M2XL	F2e(F2CR)	F3	M3
F3	False	True	True	True	True	True
M3	False	False	True	False	True	True

Note Xbow platform supports F2e, F3 and M3 modules only

M3-M2-F3 combination is blocked for Cisco Nexus 7000 Series Switches.

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 Cisco NX-OS software features, configuration and operation are local to the current VDC. However, exceptions are as follows:

- Control Plane Policing (CoPP)—Because of the hardware support, you can configure CoPP policies only in the default or admin VDCs. The CoPP policies apply across all VDCs on the physical device.
- Fabric Extender—You must install the Cisco Nexus 2000 Series Fabric Extender feature set in the default or admin VDCs before you can enable the Fabric Extender in any VDC (including the default VDC). For more information about the Fabric Extender, see the *Configuring the Cisco Nexus 2000 Series Fabric Extender*.
- FabricPath—You must install the FabricPath feature set in the default or admin VDCs before you can enable FabricPath in any VDC (including the default VDC). For more information about FabricPath, see the *Cisco NX-OS FabricPath Configuration Guide for Nexus 7000*.
- FCoE—You must install the FCoE feature set in the default or admin VDCs before you can enable FCoE in any VDC (including the default VDC). For more information about FCoE, see "Creating VDCs," and the *Cisco NX-OS FCoE Configuration Guide for Nexus 7000 and MDS 9500*.
- Multiprotocol Label Switching (MPLS)—You must install the MPLS feature set in the default or admin VDCs before you can enable MPLS in any VDC (including the default VDC). For more information about MPLS, see the *Cisco Nexus 7000 Series NX-OS MPLS Configuration Guide*.
- 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—In Cisco NX-OS releases prior to 4.2, you can create VDC tunnels only in the default VDC. However, beginning with Cisco NX-OS Release 4.2(1), you can put tunnel interfaces into nondefault VDCs and VRFs.
- FCoE—Beginning with the Cisco NX-OS Release 5.2(1) for the Nexus 7000 Series devices, VDCs have FCoE support to provide users with local area network (LAN)/storage area network (SAN) management separation on one physical Ethernet interface. The Cisco NX-OS supports both Ethernet and FCoE only in nondefault VDCs that control the Ethernet and storage portions of the network. You can have only one storage VDC configured on the device.

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