Virtual Device Context Configuration Guide, Cisco DCNM for LAN, Release 6.x

June 2012

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-27532-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Virtual Device Context Configuration Guide, Cisco DCNM for LAN, Release 6.x

CONTENTS

Send document comments to dcnm-docfeedback@cisco.com.

New and Changed Information

As of Cisco DCNM Release 5.2, Cisco Fabric Manager and Cisco Data Center Network Manager for LAN are merged into one unified product called Cisco Data Center Network Manager (DCNM) that can manage both LAN and SAN environments. As a part of this product merger, the name Cisco DCNM for SAN replaces the name Cisco Fabric Manager.

The following documentation changes support the merged Cisco DCNM product:

- Cisco DCNM product documentation for Cisco DCNM Release 5.2 is retitled with the name Cisco DCNM for LAN.
- Cisco Fabric Manager product documentation for Cisco DCNM Release 5.2 is retitled with the name Cisco DCNM for SAN.
- Cisco DCNM for SAN product documentation is now published to the Data Center Network Manager listing page on Cisco.com: http://www.cisco.com/en/US/products/ps9369/tsd_products_support_configure.html

  This URL is also the listing page for Cisco DCNM for LAN product documentation.
- Cisco Fabric Manager documentation for software releases earlier than Cisco DCNM Release 5.2, retains the name Cisco Fabric Manager and remains available at its current Cisco.com listing page: http://www.cisco.com/en/US/products/ps10495/tsd_products_support_configure.html

  You should continue to use the Cisco Fabric Manager documentation if you are using a release of Cisco Fabric Manager software that is earlier than Cisco DCNM Release 5.2.
- The name DCNM-SAN is used in place of Cisco DCNM for SAN in the user interface of Cisco Data Center Network Manager; likewise, the name DCNM-LAN is used in place of Cisco DCNM for LAN in the user interface. To match the user interface, the product documentation also uses the names DCNM-SAN and DCNM-LAN.
- The following new publications support both Cisco DCNM for LAN and DCNM for SAN, and address the new licensing model, the new installation process, and the new features of Cisco DCNM:
  - *Cisco DCNM Installation and Licensing Guide*
  - *Cisco DCNM Release Notes*

For a complete list of Cisco DCNM documentation, see the “Related Documentation” section in the Preface.

This chapter provides release-specific information for each new and changed feature in the *Virtual Device Context Configuration Guide, Cisco DCNM for LAN, Release 6.x*. The latest version of this document is available at the following Cisco website: http://www.cisco.com/en/US/products/ps9369/products_installation_and_configuration_guides_list.html

To check for additional information about Cisco DCNM Release 5.x, see the *Cisco DCNM Release Notes, Release 5.x,* available at the following Cisco website: http://www.cisco.com/en/US/products/ps9369/prod_release_notes_list.html

summarizes the new and changed features for the *Virtual Device Context Configuration Guide, Cisco DCNM for LAN, Release 6.x*, and tells you where they are documented.

New and Changed Features for Release 5.x

Feature	Description	Changed in Release	Where Documented
Admin VDC Support	Administrator VDC is the VDC which enables you to perform switch wide administrative functions. There are no ports, port operations, or protocols associated with the administrator VDC.	6.1(1)	Chapter 4, "Managing VDCs."
Support for F2 module-type	Added F2 module-type support for creating a VDC wizard.	5.2(2a)	Chapter 3, "Creating VDCs with the VDC Setup Wizard" and Chapter 4, "Managing VDCs"
FCoE VDC enhancements	Added FCoE support for creating a VDC wizard.	5.2(1)	Chapter 4, "Managing VDCs"
Suspending and Resuming VDCs	Added support for suspending and resuming an active nondefault VDC.	5.2(1)	Chapter 3, "Creating VDCs with the VDC Setup Wizard"
Support for N7K-F132XP-15 module	Added support for the N7K-F132XP-15 module.	5.1(1)	Chapter 1, "Overview", Chapter 3, "Creating VDCs with the VDC Setup Wizard", and Chapter 4, "Managing VDCs"
Managing VDCs	Added the ability to save the VDC configuration of the physical device to the startup configuration or to a bootflash file.	5.1(1)	Chapter 4, "Managing VDCs"

For a complete list of Cisco DCNM documentation, see the "Related Documentation" in the Preface.

Preface

This preface describes the audience, organization, and conventions of the *Virtual Device Context Configuration Guide, Cisco DCNM for LAN, Release 6.x*. It also provides information on how to obtain related documentation.

This chapter includes the following sections:

Audience

This publication is for experienced network administrators who configure and maintain Cisco NX-OS devices.

Document Organization

This publication is organized into the following chapters:

Title	Description
Chapter 1, "Overview"	Presents an overview of virtual device contexts (VDCs).
Chapter 2, "Configuring VDC Resource Templates"	Provides information about creating and configuring VDC resource templates.
Chapter 3, "Creating VDCs with the VDC Setup Wizard"	Provides information about creating VDCs.
Chapter 4, "Managing VDCs"	Provides information about managing VDCs.

Document Conventions

This document uses the following conventions:

Note Means reader *take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Related Documentation

This section contains information about the documentation available for Cisco DCNM and for the platforms that Cisco DCNM manages.

This section includes the following topics:

- Cisco DCNM Documentation, page viii
- Cisco Nexus 1000V Series Switch Documentation, page ix
- Cisco Nexus 2000 Series Fabric Extender Documentation, page ix
- Cisco Nexus 3000 Series Switch Documentation, page ix
- Cisco Nexus 4000 Series Switch Documentation, page x
- Cisco Nexus 5000 Series Switch Documentation, page x
- Cisco Nexus 7000 Series Switch Documentation, page x

Cisco DCNM Documentation

The Cisco DCNM documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps9369/tsd_products_support_series_home.html

The documentation set for Cisco DCNM includes the following documents:

Release Notes

Cisco DCNM Release Notes, Release 6.x

Cisco DCNM

The following publications support both Cisco DCNM for LAN and DCNM for SAN, and address the new licensing model, the new installation process, and the new features of Cisco DCNM:

- *Cisco DCNM Fundamentals Guide, Release 6.x*
- *Cisco DCNM Installation Guide, Release 6.x*

Cisco DCNM for LAN Configuration Guides

FabricPath Configuration Guide, Cisco DCNM for LAN, Release 6.x

Interfaces Configuration Guide, Cisco DCNM for LAN, Release 6.x

Layer 2 Switching Configuration Guide, Cisco DCNM for LAN, Release 6.x

Security Configuration Guide, Cisco DCNM for LAN, Release 6.x

System Management Configuration Guide, Cisco DCNM for LAN, Release 6.x

Unicast Configuration Guide, Cisco DCNM for LAN, Release 6.x

Virtual Device Context Configuration Guide, Cisco DCNM for LAN, Release 6.x

Virtual Device Context Quick Start, Cisco DCNM for LAN

Web Services API Guide, Cisco DCNM for LAN, Release 5.x

Cisco DCNM for SAN Configuration Guides

Fabric Configuration Guide, Cisco DCNM for SAN, Release 6.x

High Availability and Redundancy Configuration Guide, Cisco DCNM for SAN, Release 6.x

Intelligent Storage Services Configuration Guide, Cisco DCNM for SAN, Release 6.x

Inter-VSAN Routing Configuration Guide, Cisco DCNM for SAN, Release 6.x

Interfaces Configuration Guide, Cisco DCNM for SAN, Release 6.x

IP Services Configuration Guide, Cisco DCNM for SAN, Release 6.x

Quality of Service Configuration Guide, Cisco DCNM for SAN, Release 6.x

Security Configuration Guide, Cisco DCNM for SAN, Release 6.x

SMI-S and Web Services Programming Guide, Cisco DCNM for SAN, Release 6.x

System Management Configuration Guide, Cisco DCNM for SAN, Release 6.x

Cisco Nexus 1000V Series Switch Documentation

The Cisco Nexus 1000V Series switch documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

Cisco Nexus 2000 Series Fabric Extender Documentation

The Cisco Nexus 2000 Series Fabric Extender documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps10110/tsd_products_support_series_home.html

Cisco Nexus 3000 Series Switch Documentation

The Cisco Nexus 3000 Series switch documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps11541/tsd_products_support_series_home.html

Cisco Nexus 4000 Series Switch Documentation

The Cisco Nexus 4000 Series switch documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps10596/tsd_products_support_series_home.html

Cisco Nexus 5000 Series Switch Documentation

The Cisco Nexus 5000 Series switch documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps9670/tsd_products_support_series_home.html

Cisco Nexus 7000 Series Switch Documentation

The Cisco Nexus 7000 Series switch documentation is available at the following URL:

http://www.cisco.com/en/US/products/ps9902/tsd_products_support_series_home.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

Overview

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

This chapter includes the following sections:

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. 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.

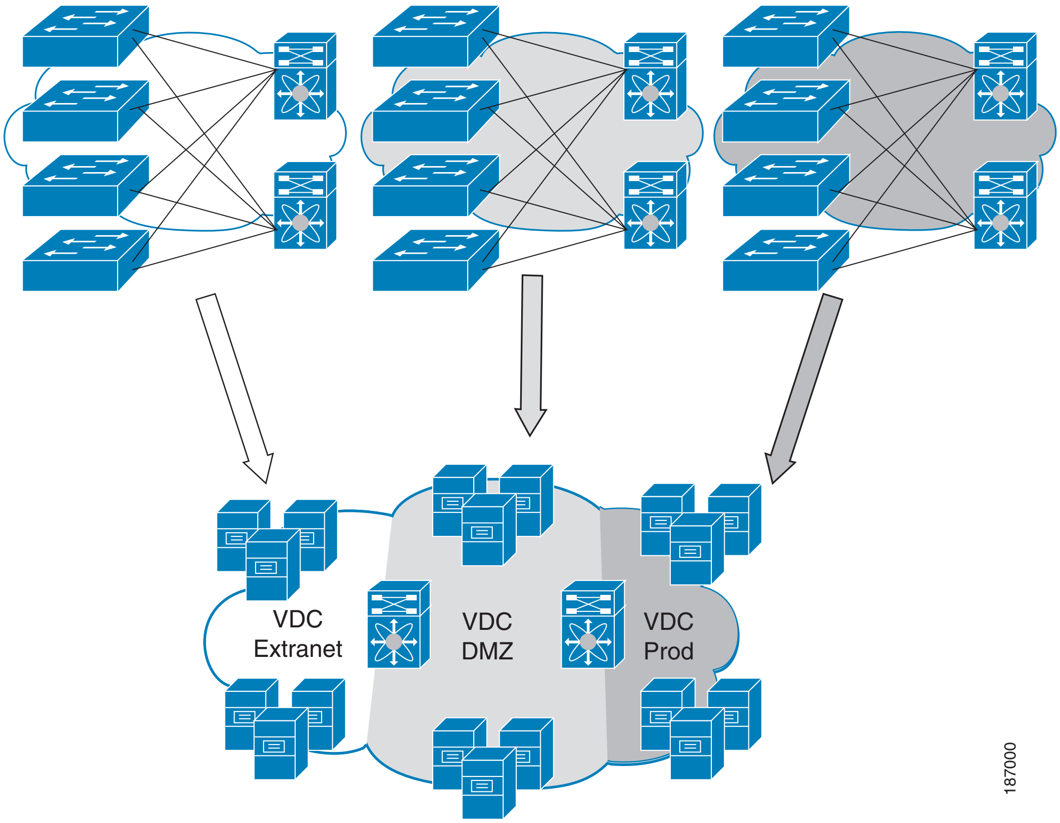
Beginning with Cisco NX-OS release 5.2(1) for the Nexus 7000 Series devices, you can configure Fibre Channel over Ethernet (FCoE). You must configure a dedicated storage VDC to run FCoE on the Cisco Nexus 7000 Series devices. See the *Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500* for information on FCoE.

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 to use virtual routing and forwarding (VRF) instance names and VLAN IDs independent of those used in other VDCs. Each VDC administrator interacts with a separate set of processes, VRFs, and VLANs.

Note The numbers between FCoE and Ethernet VLANs must be unique. That is, the numbers 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 number space for FCoE and Ethernet is shared only for those VDCs configured for port sharing. See *Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500* for information on configuring FCoE.

Figure 1-1 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 1-1 Segmentation of Physical Device



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 1-3
- MAC Addresses, page 1-4
- Default VDC, page 1-4
- Communication Between VDCs, page 1-4
- Storage VDCs, page 1-5

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 Figure 1-2).

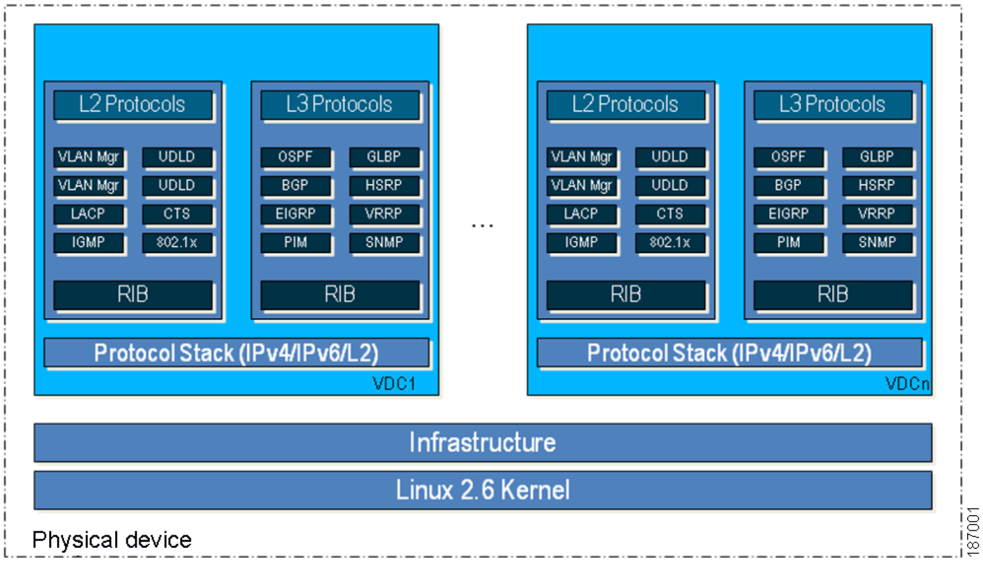
The infrastructure also enforces isolation across VDCs. A fault that is generated within a VDC does not impact the services in other VDCs. This feature limits the impact of software faults and greatly improves reliability of the device.

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 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



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 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 to create, change attributes for, or delete a nondefault VDC. The Cisco 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 1-8).

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 that is allocated to one VDC to a port that is 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 1-7).

Storage VDCs

Beginning with Cisco NX-OS Release 5.2(1) for the Nexus 7000 Series devices, you can run FCoE on the F Series modules. You 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.

After you create the storage VDC, you assign specified FCoE VLANs. Finally, you configure interfaces on the 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.

Note You can create storage VDCs only on the F Series module. On the F Series module, you must assign the interfaces on the port group to the same VDC. See the "Physical Resources" section on page 1-5 for information on the port groups for the F Series module.

For more information about creating VDCs with FCoE, see Chapter 3, "Creating VDCs with the VDC Setup Wizard" and the *Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500* book.

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 (see the "VDC Default User Roles" section on page 1-8).

This section includes the following topics:

- Physical Resources, page 1-5
- Logical Resources, page 1-7
- VDC Resource Templates, page 1-7
- Configuration Files, page 1-8

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.

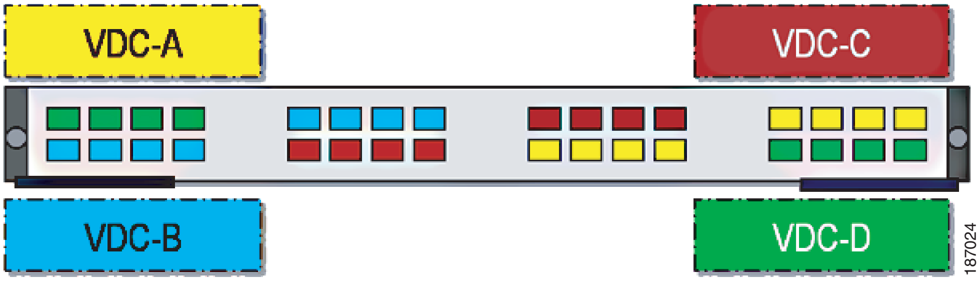
Initially, all physical interfaces belong to the default VDC (VDC 1). When you create a new VDC, the Cisco NX-OS software creates the virtualized services for the VDC without allocating any physical interfaces to it. After you create a new VDC, you can allocate a set of physical interfaces from the default 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 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 four port groups that consist of 2, 4, 8, or 12 interfaces each, depending on the module: N7K-M148GS-11L, N7K-M148GT-11, N7K-M148GS-11, N7K-M132XP-12, or N7K-M108X2-12L. You must assign all interfaces in the corresponding port group to the same VDC. See the example for module N7K-M132XP-12 in Figure 1-3.

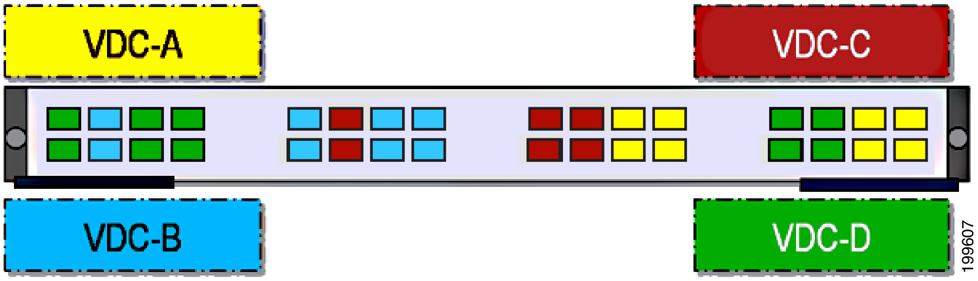
Figure 1-3 Example Interface Allocation for Port Groups on a Cisco 7000 Series 10-Gbps Ethernet Module (N7K-M132XP-12)



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. You must assign the specified port pairs in the same VDC (see Figure 1-4).

For more information on ports that can be paired, see Chapter 3, “Creating VDCs with the VDC Setup Wizard.”

Figure 1-4 Example Interface Allocation for Port Groups on a Cisco 7000 Series 10-Gbps Ethernet Module (N7K-F132XP-15)



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*.

Logical Resources

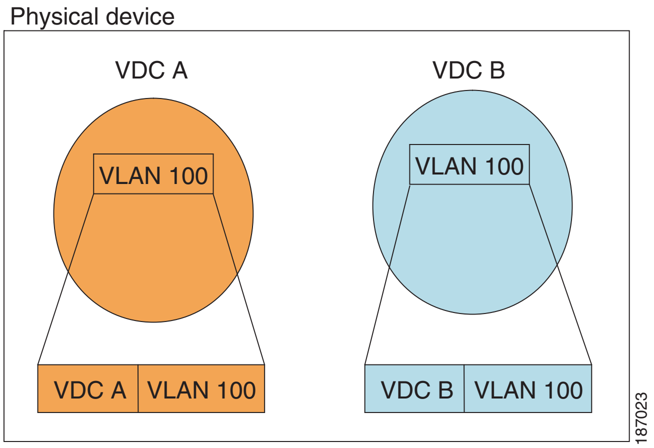
Each VDC acts as a separate logical device within a single physical device, which means that all the namespaces are unique within a VDC. However, you cannot use an identical namespace within a storage VDC and an Ethernet VDC.

When you create a VDC, it has its own default VLAN and VRF that 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 an another logical entity in another VDC. For example, each VDC can support a maximum of 4096 VLANs. The Cisco 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 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 Figure 1-5).

Figure 1-5 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.

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 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 the VDC with no impact to other VDCs.

This section includes the following topics:

- VDC Default User Roles, page 1-8
- Configuration Modes, page 1-9
- VDC Management Connections, page 1-10

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 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 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. This role allows access to all the network-operator-only **show** commands such as the **show running-config vdc** and **show install all status** commands. 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. 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. 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. For more information on user accounts and roles, see the *Security Configuration Guide, Cisco DCNM for LAN, Release 5.x*.

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. The following example shows how to enter VDC configuration mode:

```
switch# configure terminal
switch(config)# vdc Enterprise
switch(config-vdc)#
```

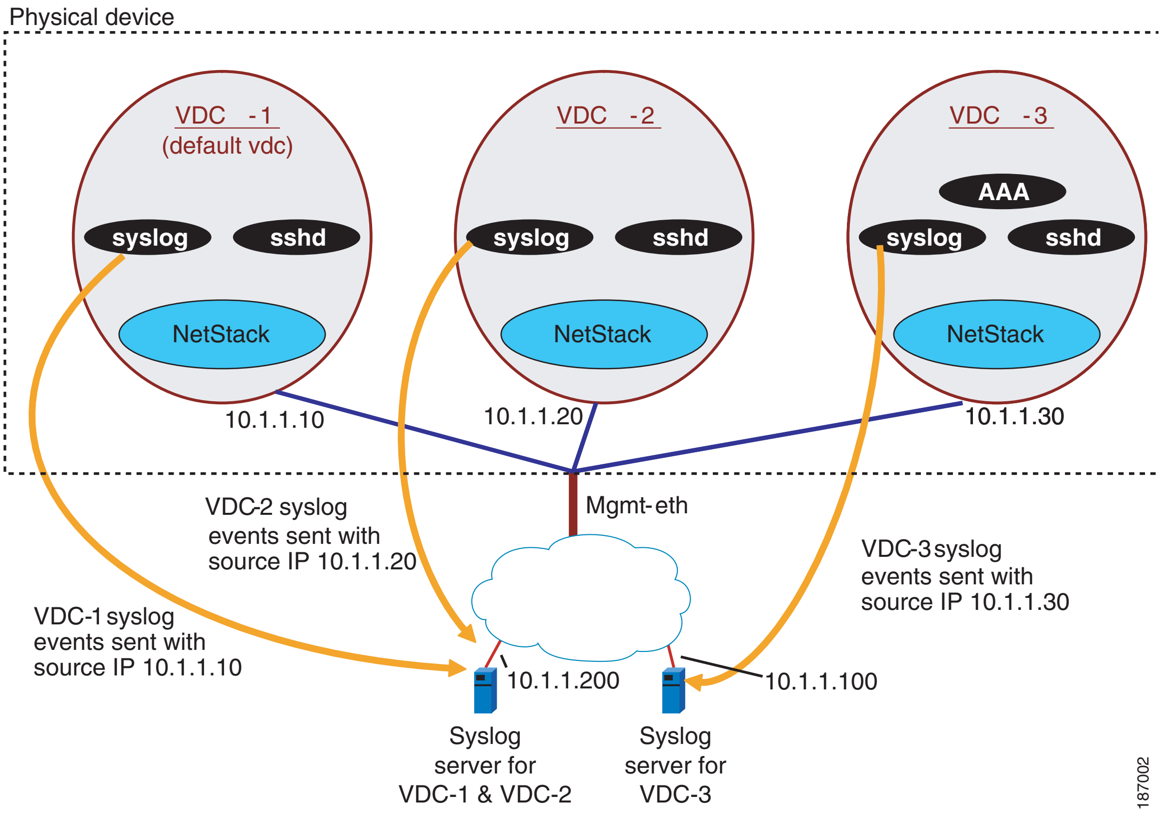
In the global configuration mode in a VDC, you can configure Cisco NX-OS features for nondefault VDCs. You can access this configuration mode by logging in to the VDC and entering global configuration mode.You must have a user role that allows read and write access to the VDC to use this configuration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

```
switch-Enterprise# configure terminal
switch-Enterprise(config)#
```

VDC Management Connections

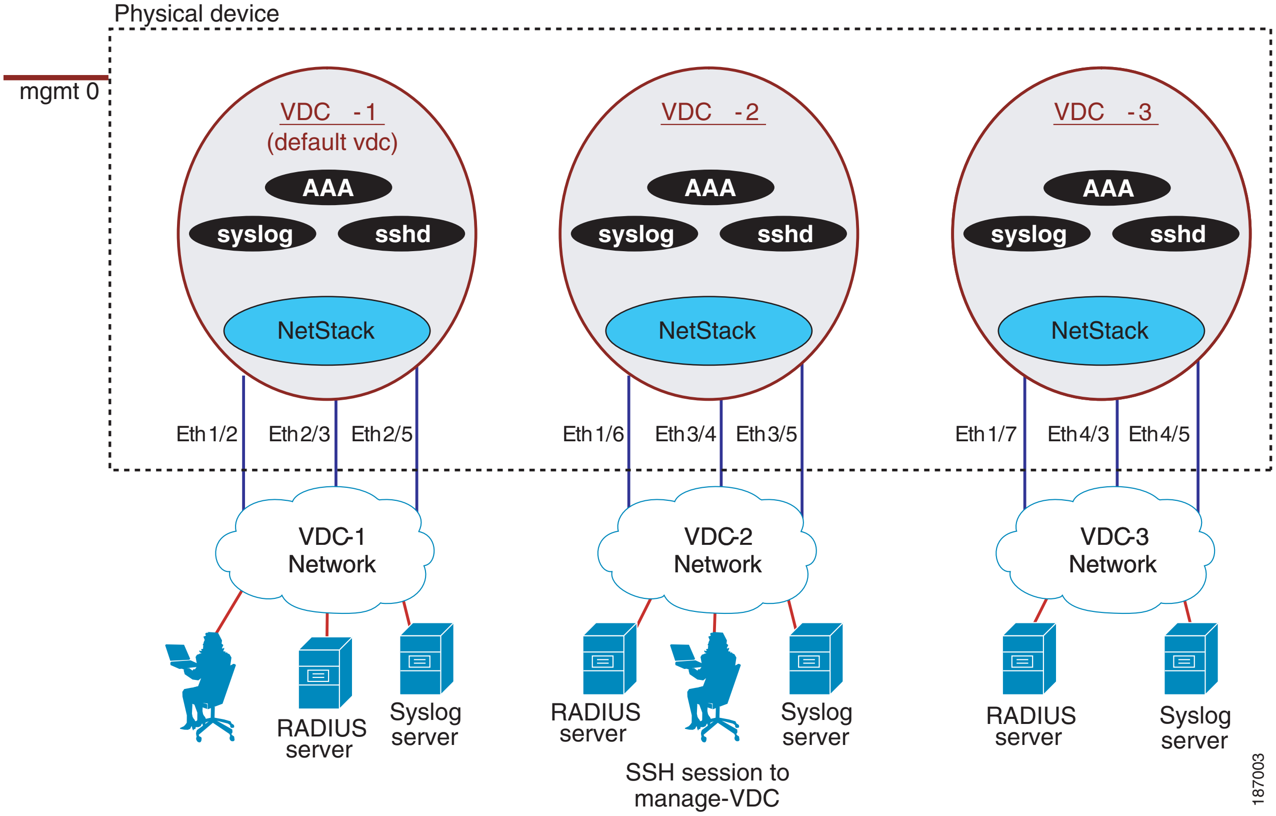
The Cisco NX-OS software provides a virtual management (mgmt 0) interface for out-of-band management for each VDC. You can configure this interface with a separate IP address that is accessed through the physical mgmt 0 interface (see Figure 1-6). Using the virtual management interface allows you to use only one management network, which can share the AAA servers and syslog servers among the VDCs.

Figure 1-6 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 1-7). Using the in-band management allows you to use only separate management networks, which ensures the separation of the AAA servers and syslog servers among the VDCs.

Figure 1-7 In-Band VDC Management Example

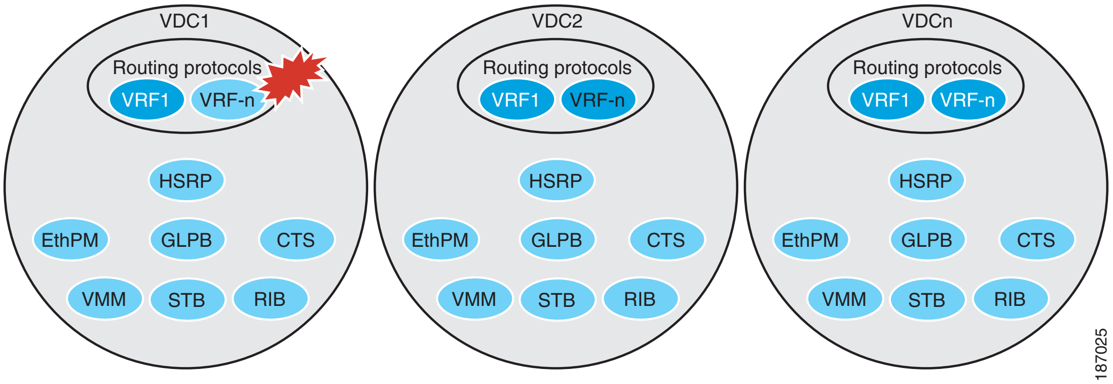


VDC Fault Isolation

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.

Figure 1-8 shows that a fault in a process running in VDC 1 does not impact any of the running processes in the other VDCs.

Figure 1-8 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 on 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 on HA in the Cisco NX-OS software, see the *Cisco Nexus 7000 Series NX-OS High Availability and Redundancy Guide, Release 5.x*.

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, the exceptions are as follows:

- 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.
- FCoE—Beginning with the Cisco NX-OS Release 5.2(1) for the Nexus 700 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 more information about creating VDCs with FCoE, see Chapter 3, “Creating VDCs with the VDC Setup Wizard” and the *Cisco NX-OS FCoE Configuration Guide.*

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

CHAPTER 2

Configuring VDC Resource Templates

This chapter describes how to configure virtual device context (VDC) resource templates on Cisco NX-OS devices.

This chapter includes the following sections:

Information About VDC Resource Templates

VDC resource templates set the minimum and maximum limits for shared physical device resources when you create the VDC. The Cisco NX-OS software reserves the minimum limit for the resource to the VDC. Any resources allocated to the VDC beyond the minimum are based on the maximum limit and availability on the device.

You can explicitly specify a VDC resource template or you can use the default VDC template provided by the Cisco NX-OS software. VDC templates set limits on the following resources:

- IPv4 multicast route memory
- IPv6 multicast route memory
- IPv4 unicast route memory
- IPv6 unicast route memory
- Port channels
- Switch Port Analyzer (SPAN) sessions
- VLANs
- Virtual routing and forwarding instances (VRFs)

Note The default IPv4 and IPv6 route memory available for all VDCs on the supervisor is 250 MB. Beginning with Cisco NX-OS Release 5.2(1), the default memory is 300 MB. This amount remains the same with both the 4-GB and the 8-GB supervisor (see *Adding Memory to a Cisco Nexus 7000 Series Supervisor* for information on 8-GB supervisor modules). You can have approximately 11,000 routes, each with 16 next hops, in 16 MB of route memory. The **show routing memory estimate routes** *number-of-routes* **next-hops** *number-of-next-hops* command shows the amount of unicast RIB (IPv4 RIB and IPv6 RIB) shared memory needed to support the specified number of routes and next hops.

If you do not set a limit for a resource in a VDC resource template, the default limits for that resource are the same as those in the default VDC resource template. Table 2-1 lists the default VDC resource template limits.

Table 2-1 VDC Default Template Resource Limits

Resource	Minimum	Maximum
IPv4 multicast route memory[1]	8	8
IPv6 multicast route memory[1]	2	2
IPv4 unicast route memory[1]	8	8
IPv6 unicast route memory[1]	4	4
Port channels	0	768
SPAN sessions	0	2
VLANs	16	4096
VRFs	16	8192

[1] Route memory is in megabytes.

Note You cannot change the limits in the default VDC resource template.

Note Only the network administrator can change a VDC template in the default VDC.

Licensing Requirements for VDC Templates

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	VDC templates require no license. Any feature not included in a license package is bundled with the Cisco DCNM and is provided at no charge to you. For an explanation of the Cisco DCNM licensing scheme, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.
Cisco NX-OS	VDC templates require no license. Any feature not included in a license package is bundled with the Cisco NX-OS system images and is provided at no extra charge to you. For an explanation of the Cisco NX-OS licensing scheme for your platform, see the licensing guide for your platform.

Platform Support

The following platform supports this feature. For platform-specific information, including guidelines and limitations, system defaults, and configuration limits, see the corresponding documentation.

Platform	Documentation
Cisco Nexus 7000 Series Switches	Cisco Nexus 7000 Series Switches Documentation

Configuring VDC Resource Templates

The maximum amount of system resources assigned to a VDC is limited by the VDC resource template used when the VDC is created. You can create VDC resource templates to use when creating VDCs to use resource limits other than those provided in the default VDC resource template.

Note If you do not set limits for a resource in a VDC resource template, the default limits are the limits for that resource in the default VDC resource template (see Table 2-1 on page 2-2).

Adding a VDC Resource Template

You can add a VDC resource template.

BEFORE YOU BEGIN

Ensure that you have discovered the physical device using a username that has the network-admin role.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Virtual Devices**.

Step 2 From the Summary pane, double-click the device to display the list of VDCs.

Step 3 Click the default VDC with the icon.

Step 4 From the Details pane, click the **Resource Templates** tab.

Step 5 Right-click in the Details pane and choose **Add Template** from the drop-down list.

Step 6 At the cursor, enter the new VDC resource template name and press the **Enter** key.

Step 7 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Adding a Resource Limit to a VDC Resource Template

You can add a resource limit to a VDC resource template.

Note You cannot change the configuration of the default templates.

BEFORE YOU BEGIN

Ensure that you have discovered the physical device using a username that has the network-admin role.

Create a VDC resource template (see the "Adding a VDC Resource Template" section on page 2-3).

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Virtual Devices**.

Step 2 From the Summary pane, double-click the device to display the list of VDCs.

Step 3 Click the default VDC with the ▣ icon.

Step 4 From the Details pane, click the **Resource Templates** tab.

Step 5 Double-click the **VDC resource template**.

Step 6 Right-click on the **VDC resource template** and choose **Add Resource Limit** from the drop-down list.

Step 7 Choose a VDC resource from the drop-down menu.

Step 8 In the limit cell under Minimum, enter the minimum limit.

Step 9 In the limit cell under Maximum, enter the maximum limit.

Step 10 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Changing a Resource Limit in a VDC Resource Template

You can change the values of a resource limit in a VDC resource template.

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

Note You cannot change the configuration of the default resource templates.

BEFORE YOU BEGIN

Ensure that you have discovered the physical device using a username that has the network-admin role.

Ensure that a VDC resource template has been created in the default VDC (see the "Adding a VDC Resource Template" section on page 2-3).

Ensure that resource limits have been added to the VDC resource template (see the "Adding a Resource Limit to a VDC Resource Template" section on page 2-3).

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Virtual Devices**.

Step 2 From the Summary pane, double-click the device to display the list of VDCs.

Step 3 Click the default VDC with the ▣ icon.

Step 4 From the Details pane, click the **Resource Templates** tab.

Step 5 Double-click the **VDC resource template**.

Step 6 Click the limits to change and enter the new values.

Step 7 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Deleting a Resource Limit from a VDC Resource Template

You can delete a resource limit from a VDC resource template.

Note You cannot change the configuration of the default resource templates.

BEFORE YOU BEGIN

Ensure that you have discovered the physical device using a username that has the network-admin role.

Ensure that a VDC resource template has been created in the default VDC (see the "Adding a VDC Resource Template" section on page 2-3).

Ensure that resource limits have been added to the VDC resource template (see the "Adding a Resource Limit to a VDC Resource Template" section on page 2-3).

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Virtual Devices**.

Step 2 From the Summary pane, double-click the device to display the list of VDCs.

Step 3 Click the default VDC with the icon.

Step 4 From the Details pane, click the **Resource Templates** tab.

Step 5 Double-click the **VDC resource template** to display the resource limits.

Step 6 Click the resource limit to delete.

Step 7 In the Details pane, right-click and choose **Delete Resource Limit** from the drop-down list.

Step 8 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Deleting a VDC Resource Template

You can delete a VDC resource template.

Note You cannot delete the default resource templates.

BEFORE YOU BEGIN

Ensure that you have discovered the physical device using a username that has the network-admin role.

Ensure that a VDC resource template has been created in the default VDC (see the "Adding a VDC Resource Template" section on page 2-3).

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Virtual Devices**.

Step 2 From the Summary pane, double-click the device to display the list of VDCs.

Step 3 Click the default VDC with the icon.

Step 4 From the Details pane, click the **Resource Templates** tab.

Step 5 Click the **VDC resource template**.

Step 6 In the Details Pane, right-click and choose **Delete Template** from the drop-down list.

Step 7 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Field Descriptions for VDC Resource Templates

This section includes the following topic:

- Field Description: Virtual Devices: Default VDC: Resource Template Tab, page 2-6

Field Description: Virtual Devices: Default VDC: Resource Template Tab

This tab allows you to configure VDC resource templates for the physical device.

Table 2-2 Field Description: Virtual Devices: Default VDC: Resource Template Tab

Element	Description
Name	Resource name.
Minimum	Minimum limit. The minimum limit is reserved for the VDC.
Maximum	Maximum limit. The maximum limit is allocated on a first-come, first-serve basis.

Additional References for VDC Resource Templates

For additional information related to implementing VDCs, see the following sections:

- Related Documents for VDC Resource Templates, page 2-7

Related Documents for VDC Resource Templates

Related Topic	Document Title
Cisco DCNM Licensing	*Cisco DCNM Installation and Licensing Guide, Release 5.x*
Cisco NX-OS Licensing	*Cisco NX-OS Licensing Guide*
VDC commands	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference, Release 5.x*

Feature History for VDC Resource Templates

Table 2-3 lists the release history for this feature.

Table 2-3 Feature History for VDC Resource Templates

Feature Name	Releases	Feature Information
VDC resource templates	5.2(1)	No change from Release 5.1.
VDC resource templates	5.1(1)	No change from Release 5.0.
VDC resource templates	5.0(2)	No change from Release 4.2.
VDC resource templates	4.2(1)	No change from Release 4.1.

CHAPTER 3

Creating VDCs with the VDC Setup Wizard

This chapter describes how to create virtual device contexts (VDCs) on Cisco Data Center Network Manager (DCNM).

This chapter includes the following sections:

Information About Creating VDCs

In Cisco NX-OS, only a user with the network-admin role can create VDCs. You can create up to three VDCs.

Beginning with the Cisco NX-OS Release 5.2(1), you can run FCoE on the Cisco Nexus 7000 Series devices. You must create a storage VDC to run FCoE. The storage VDC cannot be the default VDC and you can have one storage VDC on the device. See the *Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500* for information on configuring FCoE.

This section includes the following topics:

VDC Resource Templates

VDC resource templates describe the minimum and maximum resources that the VDC can use. If you do not specify a VDC resource template when you create a VDC, the Cisco NX-OS software uses the default template. Table 3-1 lists the resource limits for the default VDC template for nondefault VDCs.

Table 3-1 Default VDC Template Resource Limits for Nondefault VDCs

Resource	Minimum	Maximum
Port channels	0	768
SPAN sessions	0	2
IPv4 multicast route memory[1]	8	8
IPv6 multicast route memory[1]	2	2
IPv4 unicast route memory[1]	8	8
IPv6 unicast route memory[1]	4	4
VLANs	16	4096
VRFs[2]	16	8192

[1] Route memory is in megabytes.

[2] VRFs = virtual routing and forwarding instances

Table 3-2 lists the resource limits for the global VDC template used for the default VDC.

Note All resources not listed for the global VDC resource template default to the limits in the default VDC template listed in Table 3-1.

Table 3-2 Global VDC Template Resource Limits for the Default VDC

Resource	Minimum	Maximum
IPv4 multicast route memory[1]	48	48
IPv6 multicast route memory[1]	8	8
IPv4 unicast route memory[1]	16	16
IPv6 unicast route memory[1]	32	32

[1] Route memory is in megabytes.

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

For information about configuring VDC resource templates, see Chapter 2, “Configuring VDC Resource Templates.”

You can change the individual resource limits after you create the VDC as follows:

- Change an individual resource limit for a single VDC.
- Change the resource limits in a nondefault VDC resource template and apply the template to the VDC.

For information on managing VDC resource limits after you create a VDC, see Chapter 4, “Managing VDCs.”

Storage VDCs

Beginning with Cisco NX-OS Release 5.2(1), you can run FCoE on the Cisco Nexus 7000 Series devices. You must create a separate storage VDC when you run FCoE on the device. Only one of the VDCs can be a storage VDC, and the default VDC cannot be configured as a storage VDC.

See the *Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500* for information on configuring FCoE. You allocate specified FCoE VLANs to the storage VDC as well as specified interfaces.

You can configure shared interfaces that carry both Ethernet and Fibre Channel traffic. In this specific case, the same interface belongs to more than one VDC. The shared interface is allocated to both an Ethernet and a storage VDC.

High-Availability Policies

The high-availability (HA) policies for a VDC defines the action that the Cisco NX-OS software takes when an unrecoverable VDC fault occurs.

You can specify the HA policies for single supervisor module and dual supervisor module configurations when you create the VDC. The HA policy options are as follows:

- Single supervisor module configuration:
  - Bringdown—Puts the VDC in the failed state. To recover from the failed state, you must reload the physical device.
  - Reload— Reloads the supervisor module.
  - Restart—Takes down the VDC processes and interfaces and restarts it using the startup configuration.
- Dual supervisor module configuration:
  - Bringdown—Puts the VDC in the failed state. To recover from the failed state, you must reload the physical device.
  - Restart—Takes down the VDC processes and interfaces and restarts it using the startup configuration.
  - Switchover— Initiates a supervisor module switchover.

The default HA policies for a nondefault VDC that you create is restart for a single supervisor module configuration and switchover for a dual supervisor module configuration. The default HA policy for the default VDC is reload for a single supervisor module configuration and switchover for a dual supervisor module configuration.

For information on changing the HA policies after you create a VDC, see Chapter 4, “Managing VDCs.”

Allocating Interfaces

The only physical resources that you can allocate to a VDC are the physical interfaces. You can assign an interface to only one VDC, except in the specific case of shared interfaces that carry both Fibre Channel and Ethernet traffic. You allocate a shared interface to both an Ethernet VDC and to the storage VDC. When you move an interface from one VDC to another VDC, the interface loses its configuration.

When you first create a VDC, you can specifically allocate interfaces to it. All interfaces initially reside in the default VDC (VDC 1). After you allocate the interfaces to a VDC, you can only view and configure them from that specific VDC. You can also remove interfaces from a VDC by moving them back to the default VDC.

Caution When you move an interface, all configuration on the interface is lost and the interfaces are in the down state.

Note Beginning with Cisco 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.

You must be aware of the hardware architecture of your platform when allocating interfaces to a VDC. For example, the Cisco Nexus 7000 Series 32-port, 10-Gbps Ethernet module (N7K-M132XP-12) requires that you assign all four interfaces in a port group to the same VDC.

The Cisco Nexus 7000 Series 32-port, 10-Gbps Ethernet module (N7K-F132XP-15) requires that you assign the specified two interfaces in a port group to the same VDC.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 assign all four interfaces in a port group to the same VDC. Table 3-3 shows the port numbering for the port groups.

Table 3-3 Port Numbers for Port Groups on the Cisco Nexus 7000 Series 32-Port, 10-Gbps Ethernet Module (N7K-M132XP-12)

Port Group	Port Numbers
Group 1	1, 3, 5, 7
Group 2	2, 4, 6, 8
Group 3	9, 11, 13, 15
Group 4	10, 12, 14, 16
Group 5	17, 19, 21, 23
Group 6	18, 20, 22, 24
Group 7	25, 27, 29, 31
Group 8	26, 28, 30, 32

You must allocate the interfaces on your physical device in the specified combination on the Cisco Nexus 7000 Series 32-port 10-Gbps Ethernet module (N7K-F132XP-15). This module has 16 port groups that consist of 2 ports each. You must assign the specified port pairs in the same VDC. Table 3-4 shows the port numbering for the port groups.

Table 3-4 Port Numbers for Port Groups on the Cisco Nexus 7000 Series 32-Port, 10-Gbps Ethernet Module (N7K-F132XP-15)

Port Group	Port Number
Group 1	1 and 2
Group 2	3 and 4
Group 3	5 and 6
Group 4	7 and 8
Group 5	9 and 10
Group 6	11 and 12
Group 7	13 and 14
Group 8	15 and 16
Group 9	17 and 18
Group 10	19 and 20
Group 11	21 and 22
Group 12	23 and 24
Group 13	25 and 26
Group 14	27 and 28
Group 15	29 and 30
Group 16	31 and 32

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

For information about changing the interface allocation after you create a VDC, see Chapter 4, "Managing VDCs."

VDC Management Connections

The Cisco NX-OS software provides a virtual management (mgmt 0) interface for out-of-band management of each VDC. You can configure this interface with a separate IP address that is accessed through the physical mgmt 0 interface. You also use one of the Ethernet interfaces on the physical device for in-band management. For more information on management connections, see the "VDC Management Connections" section on page 1-10.

Initializing a New VDC

A new VDC is similar to a new physical device. You must set the VDC admin user account password and perform the basic configuration to establish connectivity to the VDC.

Licensing Requirements for VDCs

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	Creating nondefault VDCs requires an Advanced Services license. For an explanation of the Cisco DCNM licensing scheme, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x.*
Cisco NX-OS	Creating nondefault VDCs requires an Advanced Services license. For an explanation of the Cisco NX-OS licensing scheme for your platform, see the licensing guide for your platform.

Note The Cisco DCNM and Cisco NX-OS software allow a grace period to create and use nondefault VDCs without an Advanced Services license. If the grace period expires before you obtain a license, all VDC configuration is removed from the physical device.

Platform Support

The following platform supports this feature. For platform-specific information, including guidelines and limitations, system defaults, and configuration limits, see the corresponding documentation.

Platform	Documentation
Cisco Nexus 7000 Series Switches	Cisco Nexus 7000 Series Switches Documentation

Creating a VDC with the VDC Setup Wizard

Users with the network administrator (network-admin) role can create virtual device contexts (VDCs). VDC resource templates limit the amount of physical device resources available to the VDC. The Cisco NX-OS software provides a default resource template, or you can create resource templates.

BEFORE YOU BEGIN

Ensure that you have discovered the physical device using a username that has the network-admin role.

Obtain an IPv4 or IPv6 address for the management interface (mgmt 0) if you want to use out-of-band management for the VDC.

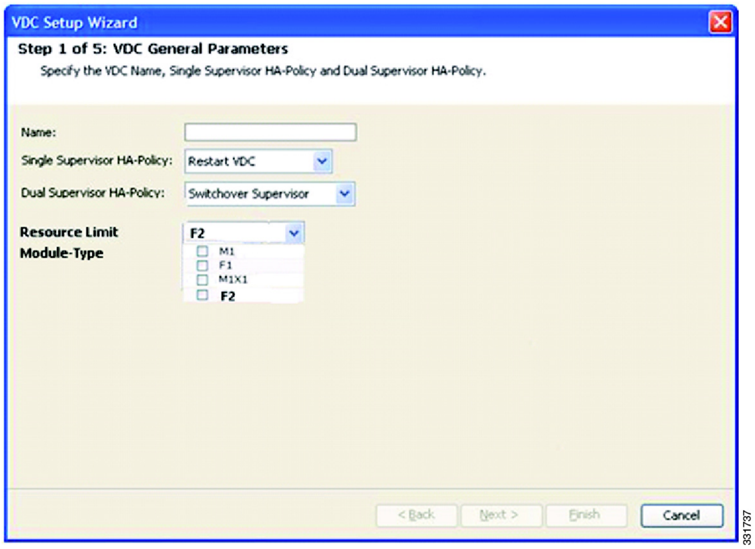
DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Virtual Devices**.

Step 2 From the Summary pane, click a physical device.

Step 3 From the menu bar, choose **File > New > Create VDC...** to bring up the VDC Setup Wizard and display the VDC General Parameters dialog box (see Figure 3-1).

Figure 3-1 VDC General Parameters Dialog Box



Step 1 of 5: VDC General Parameters

Specify the VDC Name, Single Supervisor HA-Policy and Dual Supervisor HA-Policy.

Name:

Single Supervisor HA-Policy: Restart VDC

Dual Supervisor HA-Policy: Switchover Supervisor

Resource Limit Module-Type: F2

□ M1
□ F1
□ M1X1
□ F2

Step 4 In the Name field, enter the VDC name.

Step 5 (Optional) In the Single Supervisor HA-Policy field, click the down arrow and choose the HA policy for the VDC when the physical device has a single supervisor module.

Step 6 (Optional) In the Dual Supervisor HA-Policy field, click the down arrow and choose the HA policy for the VDC when the physical device has dual supervisor modules.

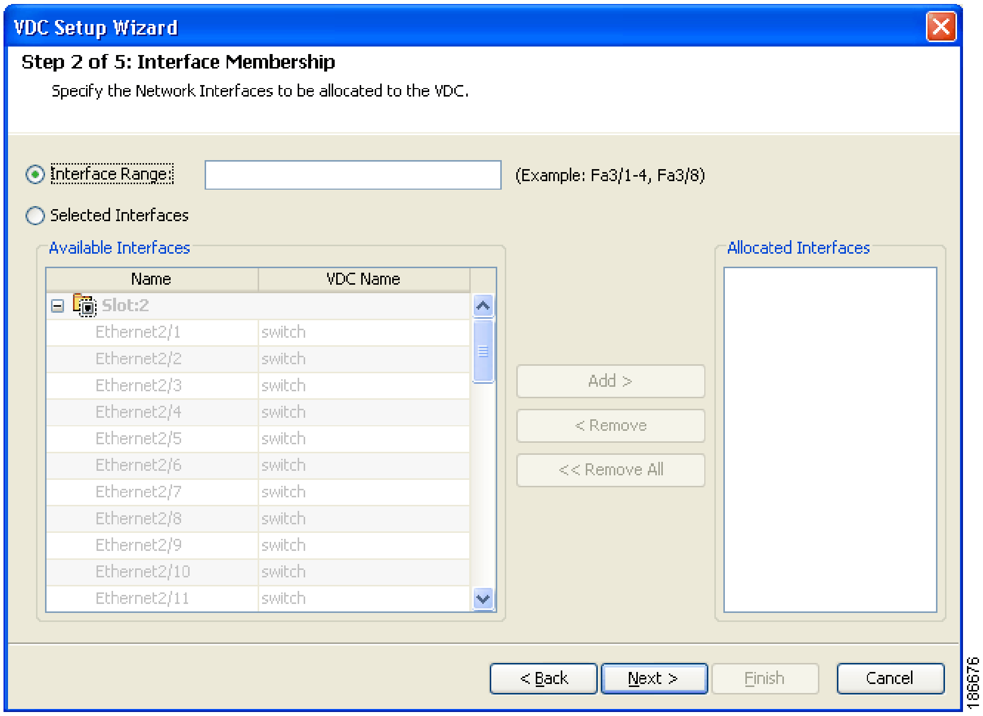
Step 7 (Optional) In the Resource Limit Module-Type field, click the down arrow and choose the module-type for the VDC. You can choose M1, F1, M1XL, or F2 as the module-type.

Note F2 module-type cannot be combined or selected with any other module-types.

Step 8 Click **Next**.

The Interface Membership dialog box appears (see Figure 3-2).

Figure 3-2 Interface Membership Dialog Box



VDC Setup Wizard

Step 2 of 5: Interface Membership

Specify the Network Interfaces to be allocated to the VDC.

● Interface Range: (Example: Fa3/1-4, Fa3/8)

○ Selected Interfaces

Available Interfaces

Name	VDC Name
Slot:2	
Ethernet2/1	switch
Ethernet2/2	switch
Ethernet2/3	switch
Ethernet2/4	switch
Ethernet2/5	switch
Ethernet2/6	switch
Ethernet2/7	switch
Ethernet2/8	switch
Ethernet2/9	switch
Ethernet2/10	switch
Ethernet2/11	switch

Allocated Interfaces

Step 9 Choose the interfaces that you want to allocate to the VDC.

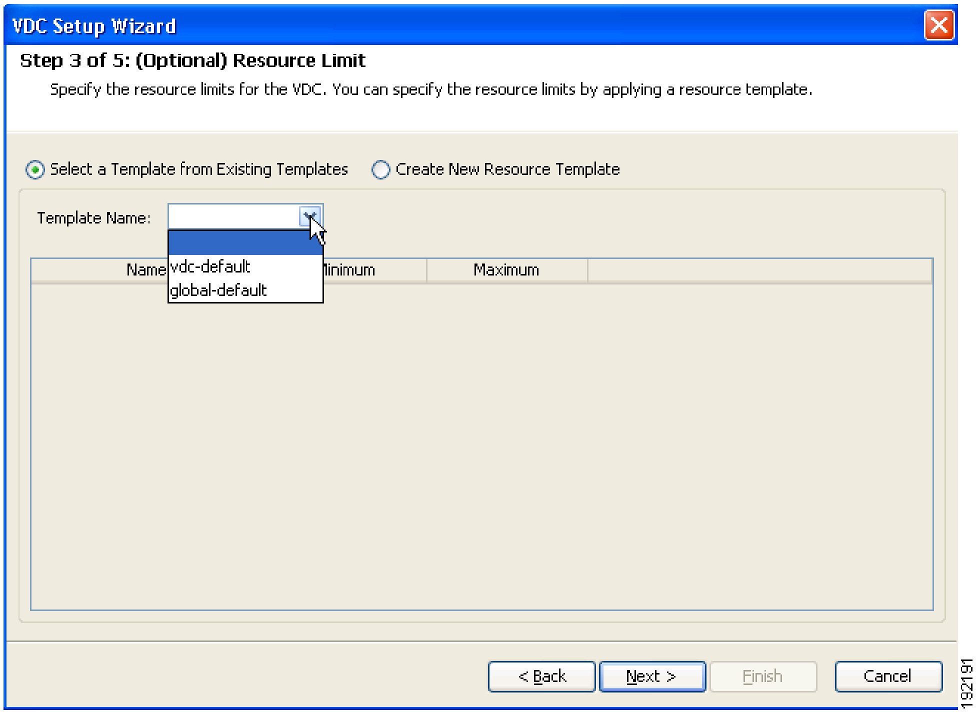
Note When you allocate an interface to a VDC, the interface configuration is lost. You cannot assign a port to a VDC if the port type is not supported for the module-type of a VDC. For example, if module-type for the VDC is F2, then only F2 card ports can be allocated.

Step 10 Click **Next**.

The Resource Limit dialog box appears.

Step 11 (Optional) To use an existing resource templates, from the Template Name field, click on the down arrow and choose a resource template from the drop-down list (see Figure 3-3).

Figure 3-3 Resource Limit Dialog Box Using an Existing Resource Template


VDC Setup Wizard

Step 3 of 5: (Optional) Resource Limit

Specify the resource limits for the VDC. You can specify the resource limits by applying a resource template.

● Select a Template from Existing Templates ○ Create New Resource Template

Template Name:

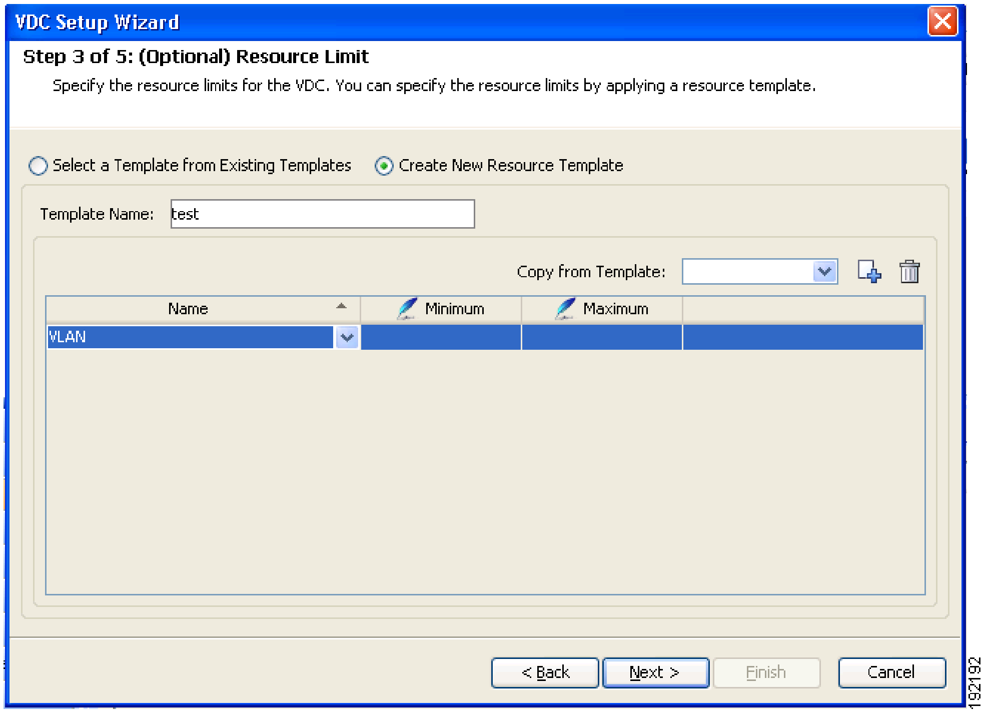
vdc-default
global-default

Note If you do not select a resource template, Cisco DCNM uses the vdc-default template.

Step 12 (Optional) To create a new resource template, follow these steps:

a. Click the **Create New Resource Template** radio button (see Figure 3-4).

Figure 3-4 Resource Limit Dialog Box Creating a New Resource Template



VDC Setup Wizard

Step 3 of 5: (Optional) Resource Limit

Specify the resource limits for the VDC. You can specify the resource limits by applying a resource template.

○ Select a Template from Existing Templates ● Create New Resource Template

Template Name: test

Copy from Template:

Name	Minimum	Maximum
VLAN		

b. From the Template Name field, enter the resource template name.

c. Click the icon to add a new resource row.

A new resource limit row appears.

d. From the cell under Name, click the down arrow and choose a resource from the drop-down list.

e. Click the cell under Minimum and enter the minimum limit.

f. Click the cell under Maximum and enter the maximum limit.

g. To set additional resource limits, repeat Step c through Step f.

h. (Optional) To delete a row, click the row to delete and click the icon.

The resource limit row disappears.

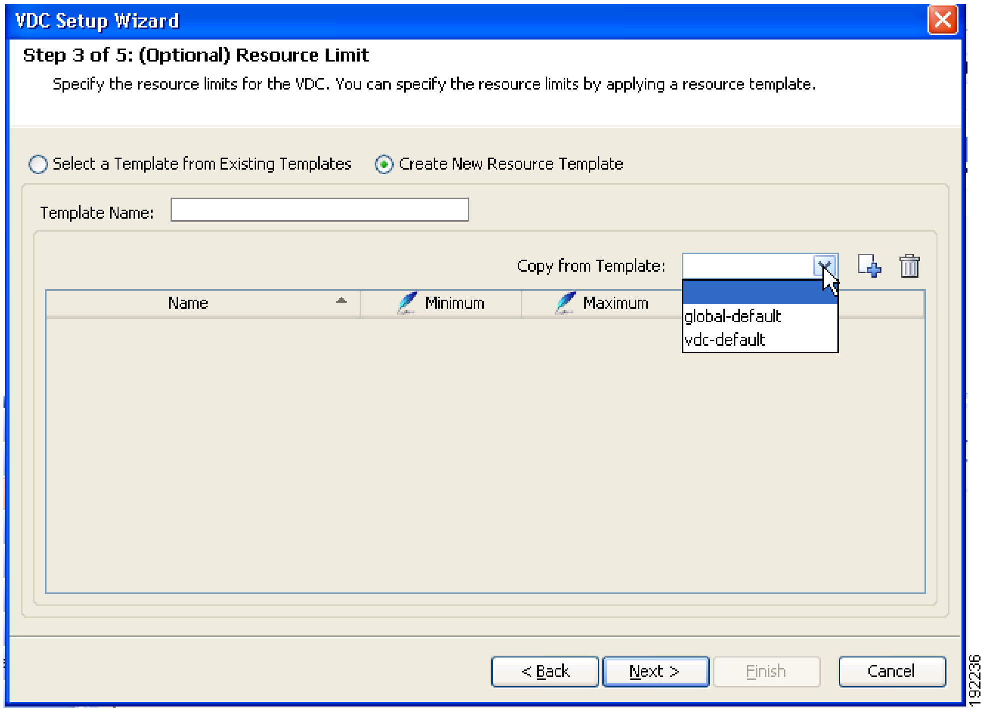
Note If you do not select a resource template, Cisco DCNM uses the vdc-default template.

Step 13 (Optional) To create a new resource template from an existing resource template, follow these steps:

a. Click the **Create New Resource Template** radio button.

b. From the Copy from Template field, click the down arrow and click a resource template (see Figure 3-5).

Figure 3-5 Resource Limit Dialog Box Copying a Resource Template



VDC Setup Wizard

Step 3 of 5: (Optional) Resource Limit

Specify the resource limits for the VDC. You can specify the resource limits by applying a resource template.

○ Select a Template from Existing Templates ● Create New Resource Template

Template Name:

Copy from Template:

c. (Optional) Modify the resource fields as needed.

d. (Optional) To add a row, follow the procedure described in Step 12.

e. (Optional) To delete a row, click the row to delete and click the 🗑 icon.

The resource limit row disappears.

Note If you do not set up resource limits, Cisco DCNM uses the vdc-default template resource limits.

Step 14 (Optional) To change the resource limits, follow these steps:

a. Click the ⊞ icon to add a new resource row.

A new resource limit row appears.

b. From the cell under Name, click the down arrow and choose a resource from the drop-down list.

c. Click the cell under Minimum and enter the minimum limit.

d. Click the cell under Maximum and enter the maximum limit.

e. To change additional resource limits, repeat Step a through Step f.

f. (Optional) To delete a row, click the row to delete and click the 🗑 icon.

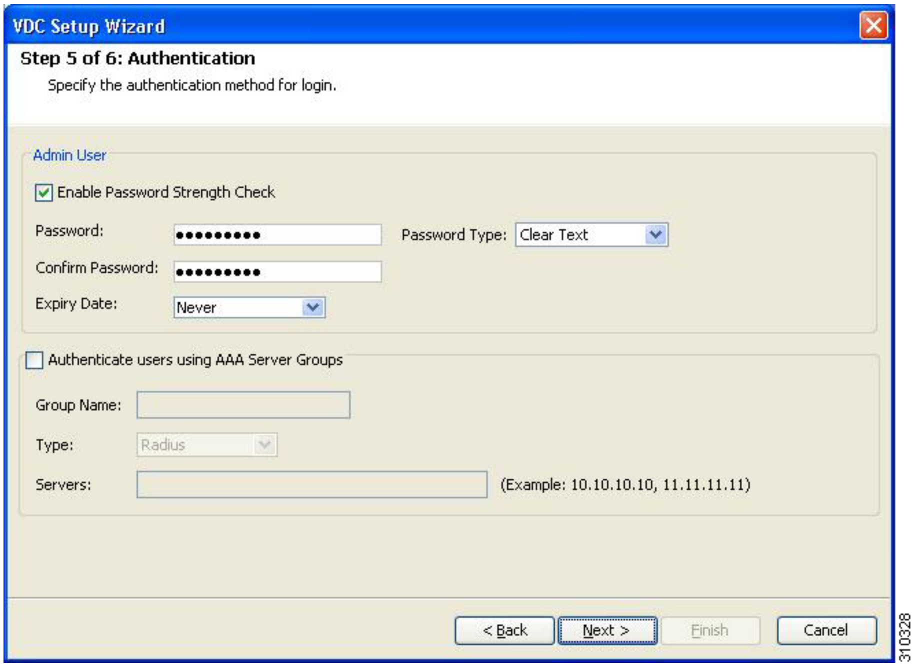
The resource limit row disappears.

Note If you do not set up resource limits, Cisco DCNM uses the vdc-default template resource limits.

Step 15 Click **Next**.

The Authentication dialog box appears (see Figure 3-6).

Figure 3-6 Authentication Dialog Box



VDC Setup Wizard

Step 5 of 6: Authentication

Specify the authentication method for login.

Admin User

☑ Enable Password Strength Check

Password: ●●●●●●●●●   Password Type: Clear Text

Confirm Password: ●●●●●●●●●

Expiry Date: Never

□ Authenticate users using AAA Server Groups

Group Name:

Type: Radius

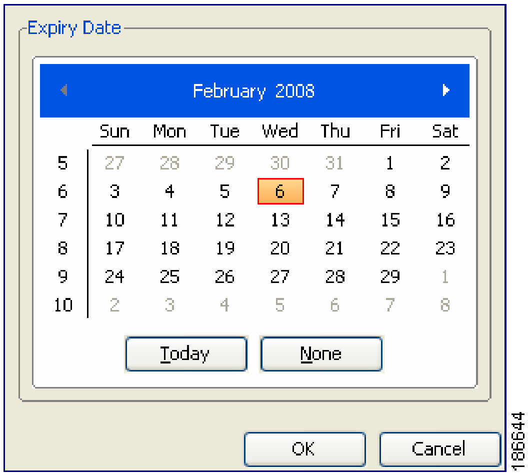
Servers: (Example: 10.10.10.10, 11.11.11.11)

Step 16 In the Password field, enter the admin user password.

Step 17 In the Confirm Password field, reenter the admin user password.

Step 18 (Optional) In the Expiry Date field, click the down arrow and choose an expiry date for the admin user from the Expiry Date dialog box (see Figure 3-7).

Figure 3-7 Expiry Date Dialog Box



Expiry Date

February 2008

	Sun	Mon	Tue	Wed	Thu	Fri	Sat
5	27	28	29	30	31	1	2
6	3	4	5	6	7	8	9
7	10	11	12	13	14	15	16
8	17	18	19	20	21	22	23
9	24	25	26	27	28	29	1
10	2	3	4	5	6	7	8

Step 19 (Optional) In the Password Type field, click the down arrow and choose from the drop-down list.

Step 20 (Optional) Check the **Authenticate users using AAA Servers** check box and enter the AAA server information as follows:

a. In the Group Name field, enter an AAA server group name.

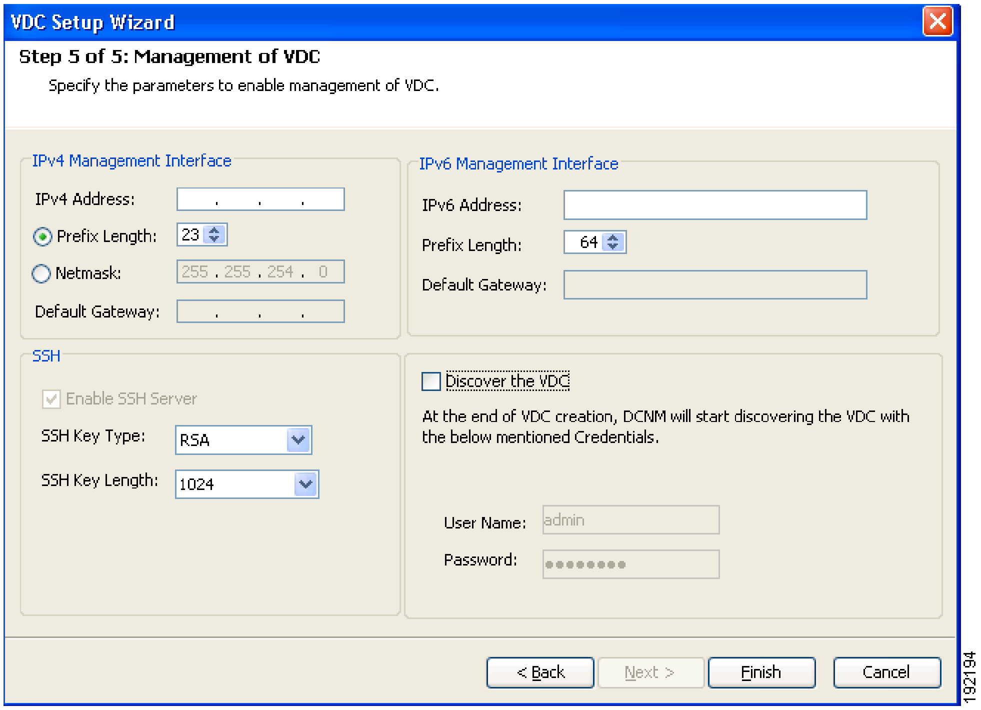
b. In the Type field, click the down arrow and choose the type of server group.

c. In the Servers field, enter one or more host server IPv4 or IPv6 addresses or names, separated by commas.

Step 21 Click **Next**.

The Management of VDC dialog box appears (see Figure 3-8).

Figure 3-8 Management of VDC Dialog Box



VDC Setup Wizard

Step 5 of 5: Management of VDC

Specify the parameters to enable management of VDC.

IPv4 Management Interface

IPv4 Address: . . .

● Prefix Length: 23

○ Netmask: 255 . 255 . 254 . 0

Default Gateway: . . .

IPv6 Management Interface

IPv6 Address:

Prefix Length: 64

Default Gateway:

SSH

☑ Enable SSH Server

SSH Key Type: RSA

SSH Key Length: 1024

□ Discover the VDC

At the end of VDC creation, DCNM will start discovering the VDC with the below mentioned Credentials.

User Name: admin

Password: ●●●●●●●●

Step 22 In the Management Interface area, enter the IPv4 or IPv6 address information.

Step 23 In the SSH area, click the down arrows and choose the SSH key type and SSS key length.

Step 24 In the Default Gateway area, enter the default IPv4 or IPv6 gateway address.

Step 25 In the Discover the VDC area, uncheck the **Discover the VDC** check box to prevent automatic discovery.

Step 26 Click **Finish**.

Note Creating a VDC can take a few minutes depending on the amount of resources that the device must reserve for the VDC.

Step 27 Manually discover the VDC as described in the "Discovering VDCs" section on page 4-23.

Step 28 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Suspending a VDC

You can suspend an active nondefault VDC.

You must save the VDC running configuration to the startup configuration before suspending the VDC. Otherwise, you will lose the changes to the running configuration. For instructions, see the *System Management Configuration Guide, Cisco DCNM for LAN, Release 5.x*.

Note You cannot suspend the default VDC.

Caution Suspending a VDC disrupts all traffic on the VDC.

BEFORE YOU BEGIN

Log in to the default VDC with a username that has the network-admin user role.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Virtual Devices**.

Step 2 From the Summary pane, double-click the device to display the list of VDCs.

Step 3 Right-click the VDC to suspend.

Step 4 Choose **Suspend VDC**.

Step 5 Click **Yes** when asked to confirm your decision. The VDC's status changes from Active to Suspended.

Resuming a VDC

You can resume a nondefault VDC from the suspended state. The VDC resumes with the configuration saved in the startup configuration.

BEFORE YOU BEGIN

Log in to the default VDC with a username that has the network-admin user role.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Virtual Devices**.

Step 2 From the Summary pane, double-click the device to display the list of VDCs.

Step 3 Right-click the VDC to resume.

Step 4 Choose **Resume VDC**. The VDC's status changes from Suspended to Active.

RELATED TOPICS

- Configuring VDC Resource Templates, page 2-1
- Managing VDCs, page 4-1

Additional References for Creating VDCs

For additional information related to creating VDC, see the following sections:

- Related Documents for Creating VDCs, page 3-15

Related Documents for Creating VDCs

Related Topic	Document Title
Cisco DCNM Licensing	*Cisco DCNM Installation and Licensing Guide, Release 5.x*
Cisco NX-OS Licensing	*Cisco NX-OS Licensing Guide*
Cisco Nexus 7000 Series 32-port, 10-Gbps Ethernet module	*Cisco Nexus 7000 Series Hardware Installation and Reference Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference, Release 5.x*
FCoE	*Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*
FCoE command reference	*Cisco NX-OS FCoE Command Reference for Cisco Nexus 7000 and Cisco MDS 9500*

Feature History for Creating VDCs

Table 3-5 lists the release history for this feature.

Table 3-5 Feature History for Creating VDCs

Feature Name	Releases	Feature Information
Support for F2 module-type	5.2(2a)	Added F2 module-type support for creating a VDC wizard.
Suspending and Resuming VDCs	5.2(1)	Added support for suspending and resuming an active nondefault VDC.
Support for N7K-F132XP-15 module	5.1(1)	VDC supports the N7K-F132XP-15 module. This module has 16 port groups that consist of 2 ports each.
Creating VDCs	5.0(2)	No change from Release 4.2.
Creating VDCs	4.2(1)	No change from Release 4.1.

CHAPTER 4

Managing VDCs

This chapter describes how to manage virtual device contexts (VDCs) on Cisco Data Center Network Manager (DCNM).

After you create a VDC, you can change the interface allocation, VDC resource limits, and the high availability (HA) policies. You can also save the VDC configuration on the physical device to the startup configuration or to a bootflash file.

This chapter includes the following sections:

Information About Managing VDCs

After you create a VDC, you can change the interface allocation, VDC resource limits, and the single-supervisor and dual-supervisor high availability (HA) policies. You can also save the VDC configuration of the physical device to the startup configuration or to a bootflash file.

This section includes the following topics:

Interface Allocation

When you create a VDC, you can allocate I/O interfaces to the VDC. Later, the deployment of your physical device might change and you can reallocate the interfaces as necessary.

Note Beginning with Cisco 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 four port groups that consist of 2, 4, 8, or 12 interfaces each, depending on the module: N7K-M148GS-11L, N7K-M148GT-11, N7K-M148GS-11, N7K-M132XP-12, or N7K-M108X2-12L. You must assign all interfaces in the corresponding port group to the same VDC. See the example for module N7K-M132XP-12 in Figure 4-1.

Figure 4-1 Example Interface Allocation for Port Groups on a Cisco Nexus 7000 Series 10-Gbps Ethernet Module (N7K-M132XP-12)

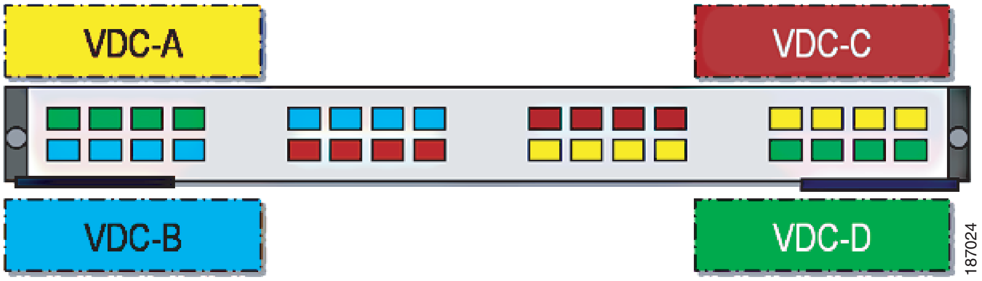


Table 4-1 shows the port numbering for the port groups.

Table 4-1 Port Numbers for Port Groups on the Cisco Nexus 7000 Series 32-Port, 10-Gbps Ethernet Module (N7K-M132XP-12)

Port Group	Port Numbers
Group 1	1, 3, 5, 7
Group 2	2, 4, 6, 8
Group 3	9, 11, 13, 15
Group 4	10, 12, 14, 16
Group 5	17, 19, 21, 23
Group 6	18, 20, 22, 24
Group 7	25, 27, 29, 31
Group 8	26, 28, 30, 32

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. You must assign the specified port pairs in the same VDC (see Figure 4-2).

Note You can configure the limit-resource line-card type command only from the VDC configuration mode and not from a VDC resource template.

Figure 4-2 Example Interface Allocation for Port Groups on a Cisco 7000 Series 10-Gbps Ethernet Module (N7K-F132XP-15)

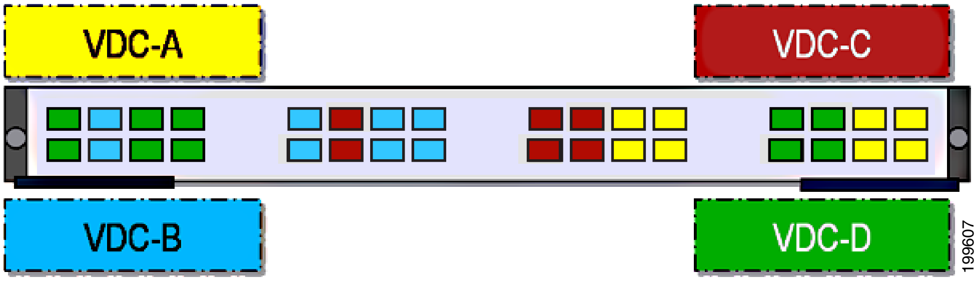


Table 4-2 shows the port numbering for the port groups.

Table 4-2 Port Numbers for Port Groups on the Cisco Nexus 7000 Series 32-Port, 10-Gbps Ethernet Module (N7K-F132XP-15)

Port Group	Port Numbers
Group 1	1 and 2
Group 2	3 and 4
Group 3	5 and 6
Group 4	7 and 8
Group 5	9 and 10
Group 6	11 and 12
Group 7	13 and 14
Group 8	15 and 16
Group 9	17 and 18
Group 10	19 and 20
Group 11	21 and 22
Group 12	23 and 24
Group 13	25 and 26
Group 14	27 and 28
Group 15	29 and 30
Group 16	31 and 32

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*.

Note When you add or delete interfaces, the Cisco NX-OS software removes the configuration and disables the interfaces.

VDC Resource Limits

You can change the resource limits for your VDC individually as your needs change. You can change the following limits for the following resources:

- IPv4 multicast route memory
- IPv6 multicast route memory
- IPv4 unicast route memory
- IPv6 unicast route memory
- Port channels
- Switched Port Analyzer (SPAN) monitor sessions
- VLANs
- Virtual routing and forwarding instances (VRFs)

HA Policies

The HA policy determines the action that the physical device takes when the VDC encounters an unrecoverable field. You can change the HA policy for the VDC that was specified when you created the VDC.

Note You cannot change the HA policies for the default VDC.

Saving VDC Configurations

A user with the vdc-admin or network-admin role can save the running configuration of all VDCs on the physical device to the startup configuration or can save the running configuration of a single VDC to a file in the bootflash directory.

MAC Addresses

The default VDC has a management MAC address. Beginning with Cisco Release 5.2(1) for the Nexus 7000 Series devices, subsequent nondefault VDCs that you create are assigned MAC addresses automatically as part of the bootup process.

You will see a syslog message if there are not sufficient MAC addresses to supply all the VDCs on the device.

Shared Interfaces

In the current Cisco NX-OS VDC model, you can move interfaces to a given VDC. The interface that is moved is dedicated to that VDC and carries all control and data traffic. VDCs are not aware of the interfaces present in the other VDCs, which gives complete administrative fault-isolation to the user.

With FCoE technology, both Ethernet and FCoE traffic are carried on the same physical Ethernet interface. In the FCoE VDC, the physical layer protocols (except for CDP, LACP and UDLD, which are LAN protocols) are not enabled. If an FCoE-capable interface is moved to the FCoE VDC, carrying pure Ethernet traffic on that interface is not possible because the LAN protocols are not enabled. In order to carry both LAN and SAN traffic, a shared interface between the LAN and SAN VDCs is required.

M1/F1 Separation

The module-type (line card) based VDCs are supported in Cisco Nexus 7000 Series devices. Beginning with Cisco NX-OS Release 5.2(1), all modules are categorized into three types — M1, F1, and M1XL. By default, all three line card types are allowed in a VDC.

You can restrict the allocated ports based on the module-type configuration. When changing the module type for a VDC, the unsupported ports are moved to the unallocated pool. You cannot move a port to a VDC if the port type is not supported for that VDC.

Cisco DCNM supports the configuration of M1/F1 line cards on the VDC. When changing the allowed types on a VDC, Cisco DCNM removes the ports that are no longer supported and moves them to an unallocated pool.

Cisco DCNM enables users to manage unallocated ports and bind the unallocated ports to any other VDCs that support this port type. When a user tries to move a port to a new VDC, Cisco DCNM checks whether ports of that type are allowed inside the VDC.

FCoE VDC Enhancements

You can assign an interface to be a shared interface only on the F Series module and not on the M Series module. For more information about FCoE VDCs, see the *Cisco Nexus 7000 Series NX-OS Virtual Device Context Configuration Guide, Release 5.x*.

Beginning with Cisco NX-OS Release 5.2 (1), the following components have been added to the Virtual Device screen to support shared interfaces:

- Summary Table
- VDC Setup Wizard
- Details Pane
- Interface Association Pane

Licensing Requirements for Managing VDCs

The following table shows the licensing requirements for this feature:

Product	License Requirement
Cisco DCNM	Managing nondefault VDCs requires an Advanced Services license. Managing the default VDC requires no license. For an explanation of the Cisco DCNM licensing scheme, see the *Cisco DCNM Installation and Licensing Guide, Release 5.x*.
Cisco NX-OS	Managing nondefault VDCs requires an Advanced Services license. Managing the default VDC requires no license. For an explanation of the Cisco NX-OS licensing scheme for your platform, see the licensing guide for your platform.

Note The Cisco DCNM and Cisco NX-OS software allow a grace period of 120 days to use VDCs without an Advanced Services license. If the grace period expires before you obtain a license, all nondefault VDC configuration is removed from the physical device.

Platform Support

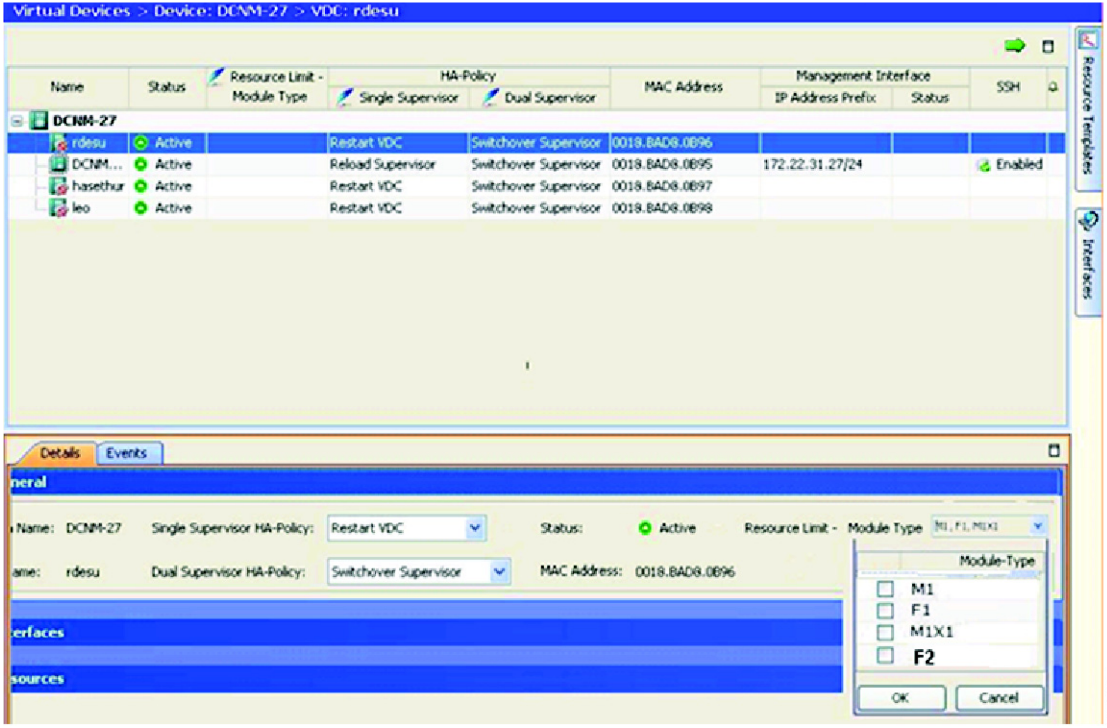
The following platform supports this feature. For platform-specific information, including guidelines and limitations, system defaults, and configuration limits, see the corresponding documentation.

Platform	Documentation
Cisco Nexus 7000 Series Switches	Cisco Nexus 7000 Series Switches Documentation

Managing VDCs

Figure 4-3 displays the VDC Summary dialog box.

Figure 4-3 VDC Summary Dialog Box



Virtual Devices > Device: DCNM-27 > VDC: rdesu

Name	Status	Resource Limit - Module Type	HA-Policy		MAC Address	Management Interface		SSH
			Single Supervisor	Dual Supervisor		IP Address Prefix	Status	
DCNM-27								
rdesu	Active		Restart VDC	Switchover Supervisor	0018.BAD8.0B96			
DCNM...	Active		Reload Supervisor	Switchover Supervisor	0018.BAD8.0B95	172.22.31.27/24		Enabled
hasethur	Active		Restart VDC	Switchover Supervisor	0018.BAD8.0B97			
leo	Active		Restart VDC	Switchover Supervisor	0018.BAD8.0B98			

neral

Name: DCNM-27 Single Supervisor HA-Policy: Restart VDC Status: Active Resource Limit - Module Type M1, F1, M1X1

ame: rdesu Dual Supervisor HA-Policy: Switchover Supervisor MAC Address: 0018.BAD8.0B96

Module-Type
- □ M1
- □ F1
- □ M1X1
- □ F2

This section includes the following topics:

- Allocating Interfaces to a VDC, page 4-8
- Selecting a VDC Type, page 4-9
- Administrator VDC Support, page 4-9
- Creating an Ethernet VDC, page 4-10
- Creating an Storage VDC, page 4-14
- Allocating a Storage VLAN on the Ethernet VDC, page 4-18
- Choosing Storage-Capable Interfaces, page 4-19
- Associating an Interface to an Storage VDC, page 4-19
- Changing VDC Resource Limits, page 4-20
- Changing the HA Policies, page 4-20
- Saving All VDC Configurations to the Startup Configuration, page 4-22
- Saving the VDC Configuration to a Bootflash File, page 4-22
- Discovering VDCs, page 4-23
- Deleting a VDC, page 4-23

Send document comments to dcnm-docfeedback@cisco.com.

Allocating Interfaces to a VDC

You can allocate one or more interfaces to a VDC. When you allocate an interface, you move it from one VDC to another VDC. The interfaces are in the down state after you move them.

Note When you allocate an interface, all configuration on the interface is lost.

BEFORE YOU BEGIN

Ensure that you have discovered the physical device using a username that has the network-admin role.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Virtual Devices**.

Step 2 From the Summary pane, double-click the device to display the list of VDCs.

Step 3 Click the VDC to change.

The Details tab appears in the Details pane.

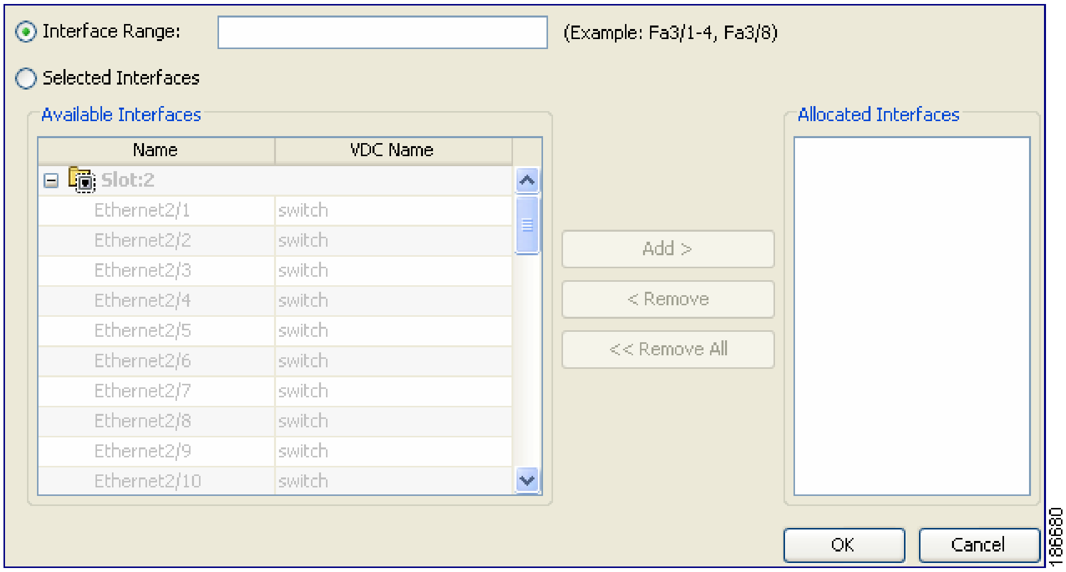
Step 4 From the Details pane, click **Interfaces**.

Step 5 Right-click in the Interfaces area and choose **Add Interface** from the drop-down list.

A new row appears.

Step 6 From the cell under Interface Name in the new row, click the down arrow to display the interfaces dialog box (see Figure 4-4).

Figure 4-4 Interfaces Dialog Box



● Interface Range: (Example: Fa3/1-4, Fa3/8)

○ Selected Interfaces

Available Interfaces

Name	VDC Name
⊟ Slot:2	
Ethernet2/1	switch
Ethernet2/2	switch
Ethernet2/3	switch
Ethernet2/4	switch
Ethernet2/5	switch
Ethernet2/6	switch
Ethernet2/7	switch
Ethernet2/8	switch
Ethernet2/9	switch
Ethernet2/10	switch

Allocated Interfaces

Step 7 From the dialog box, you can enter the range of interfaces or select specific interfaces to allocate.

Step 8 Click **OK**.

Step 9 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Step 10 (Optional) To change the configuration of an interface in the VDC, click the interface, then right-click, and choose **Manage** in the drop-down list.

Selecting a VDC Type

You can select a VDC type.

BEFORE YOU BEGIN

Log in to the default VDC with a username that has the network-admin user role.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Virtual Devices**.

Step 2 From the Summary pane, double-click the device to display the list of VDCs.

In the Virtual Devices screen, the Summary Table component is enhanced to support shared interfaces.

The Summary Table contains a new column Type to display the VDC type. This column is not editable.

Step 3 The following VDC types are displayed:

- Ethernet
- Storage

The default VDC type is Ethernet.

Administrator VDC Support

Administrator VDC is the VDC which enables you to perform switch wide administrative functions. There are no ports, port operations, or protocols associated with the administrator VDC. Unlike the default VDC, the only function of administrator VDC is to enable administrative operations on the switch and the customized VDCs. Therefore in the DCNM all the screen operations, port, and port related oprations will be disabled for Administrator VDC.

Note The administrator VDC feature is applicable only to the Cisco Nexus 7000 series switches with supervisor-2 line cards.

You can migrate from default VDC to administrator VDC using CLI commands.

Use the `system admin-vdc` command to migrate the default VDC to administrator VDC and to move all the ports to unallocated pool and to remove any other additional configuration.

You can use the `system admin-vdc migrate migrated vdc` command to migrate the default VDC to administrator VDC and move all the ports and port related configurations to the newly created migrated VDC.

DCNM will trigger a rediscovery immediateky after a default VDC is migrated to an administrator VDC, and all the administrator VDCs will be displayed in the topology with the ‘A’ icon to identify them.

If no migration is performed then the default VDC is automatically turned into administraotr VDC and any additional confifuration is removed.

Note Administrtor VDC and Default VDC cannot exist together in a switch.

You can click on the **Copy Run to Start** and **Copy Run to Start for All VDCs** buttons to perform the respective actions.

Creating an Ethernet VDC

The VDC wizard can be used to create a Ethernet VDC.

BEFORE YOU BEGIN

Log in to the default VDC with a username that has the network-admin user role.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Virtual Devices**.

Step 2 From the Summary pane, double-click **Virtual Devices**.

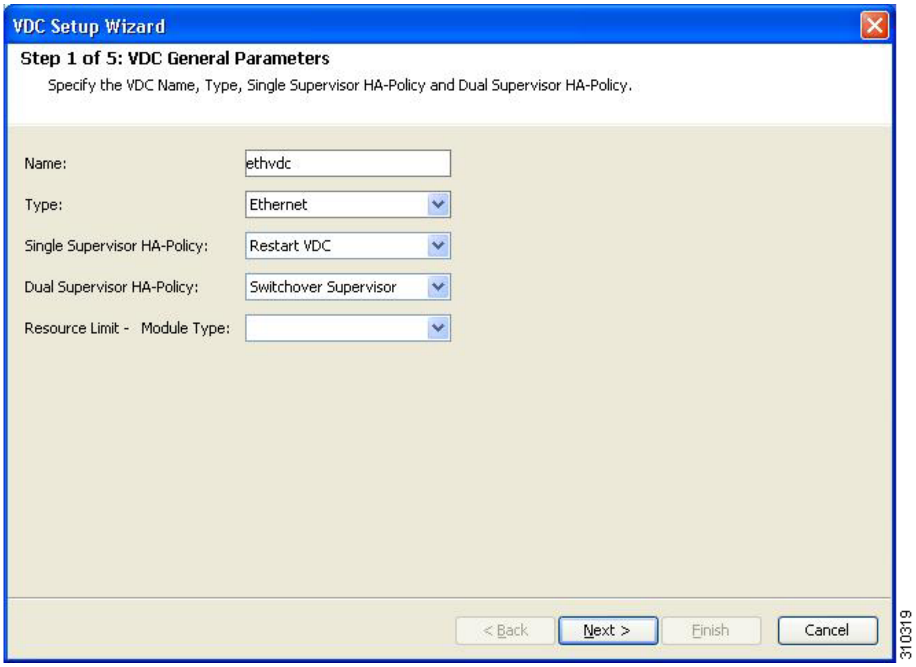
The VDC Summary Table screen is displayed.

Step 3 Right-click on the **Summary Table**. The context menu appears.

Step 4 In the context menu, choose **Create VDC**. The VDC wizard appears.

Step 5 Specify the VDC name, VDC type, single supervisor HA policy, dual supervisor HA policy and the module type (see Figure 4-5).

Figure 4-5 VDC General Parameters Screen


VDC Setup Wizard

Step 1 of 5: VDC General Parameters

Specify the VDC Name, Type, Single Supervisor HA-Policy and Dual Supervisor HA-Policy.

Name: ethvdc

Type: Ethernet

Single Supervisor HA-Policy: Restart VDC

Dual Supervisor HA-Policy: Switchover Supervisor

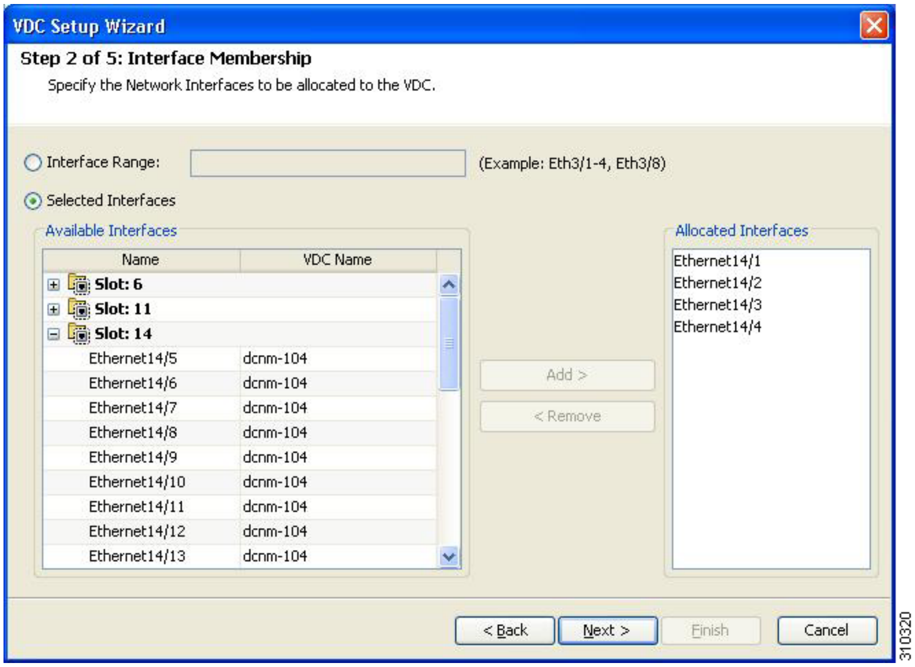
Resource Limit - Module Type:

Step 6 Click **Next**.

The Membership Interfaces screen appears.

Step 7 Specify the network interfaces (dedicated interfaces membership) to be allocated to the VDC (see Figure 4-6).

Figure 4-6 Interface Membership Screen


VDC Setup Wizard

Step 2 of 5: Interface Membership

Specify the Network Interfaces to be allocated to the VDC.

○ Interface Range: (Example: Eth3/1-4, Eth3/8)

● Selected Interfaces

Available Interfaces

Name	VDC Name
Slot: 6	
Slot: 11	
Slot: 14	
Ethernet14/5	dcnm-104
Ethernet14/6	dcnm-104
Ethernet14/7	dcnm-104
Ethernet14/8	dcnm-104
Ethernet14/9	dcnm-104
Ethernet14/10	dcnm-104
Ethernet14/11	dcnm-104
Ethernet14/12	dcnm-104
Ethernet14/13	dcnm-104

Allocated Interfaces

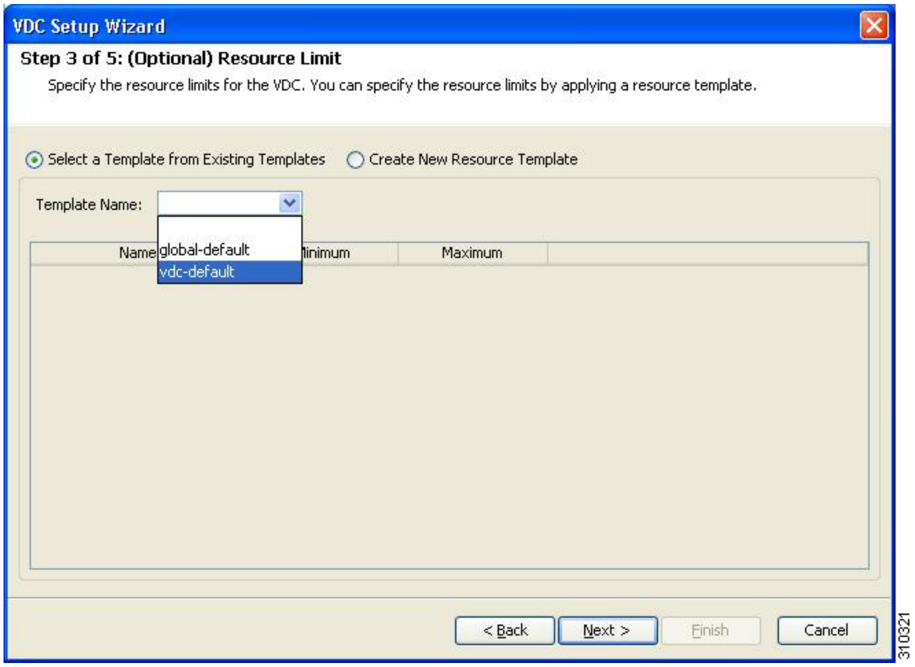
Ethernet14/1
Ethernet14/2
Ethernet14/3
Ethernet14/4

Step 8 Click **Next**.

The Resource Limits screen appears.

Step 9 (Optional) Specify the resource limits for the VDC (see Figure 4-7).

Figure 4-7 Resource Limit Screen



VDC Setup Wizard

Step 3 of 5: (Optional) Resource Limit

Specify the resource limits for the VDC. You can specify the resource limits by applying a resource template.

● Select a Template from Existing Templates ○ Create New Resource Template

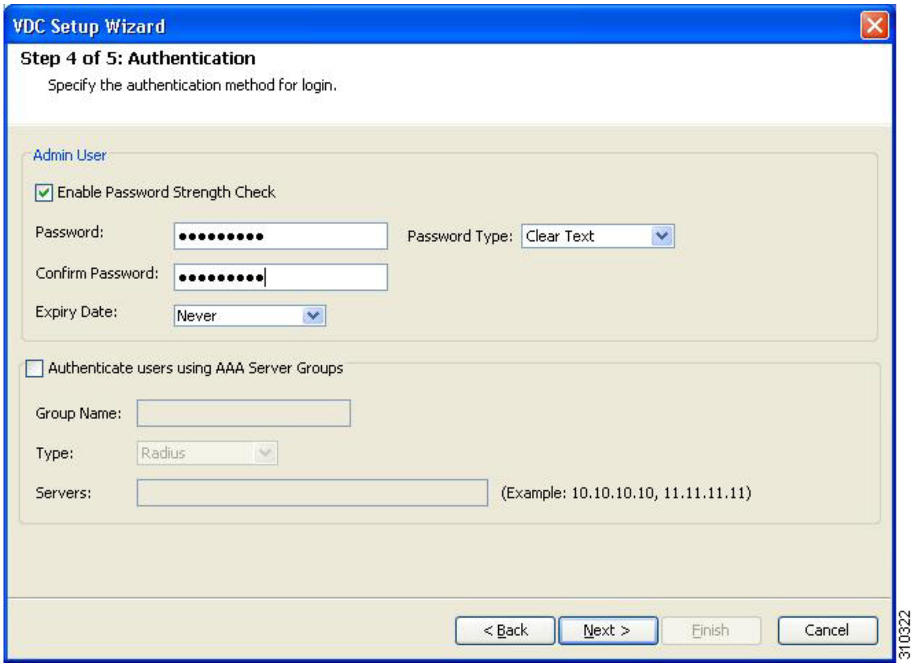
Template Name:

Step 10 Click **Next**.

The Authentication screen appears.

Step 11 Specify the authentication method for login (see Figure 4-8).

Figure 4-8 Authentication Screen



VDC Setup Wizard

Step 4 of 5: Authentication

Specify the authentication method for login.

Admin User

☑ Enable Password Strength Check

Password: ●●●●●●●●● Password Type: Clear Text

Confirm Password: ●●●●●●●●●

Expiry Date: Never

□ Authenticate users using AAA Server Groups

Group Name:

Type: Radius

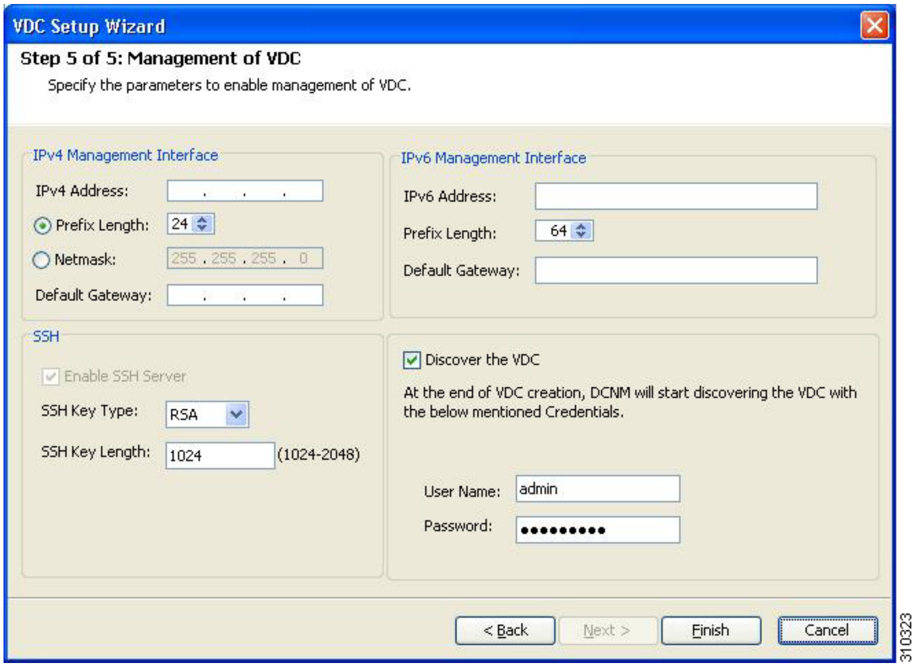
Servers: (Example: 10.10.10.10, 11.11.11.11)

Step 12 Click **Next**.

The VDC Management screen appears.

Step 13 Specify the parameters to enable management of the VDC (see Figure 4-9).

Figure 4-9 Management of VDC Screen



VDC Setup Wizard

Step 5 of 5: Management of VDC

Specify the parameters to enable management of VDC.

IPv4 Management Interface

IPv4 Address: . . .

● Prefix Length: 24

○ Netmask: 255 . 255 . 255 . 0

Default Gateway: . . .

IPv6 Management Interface

IPv6 Address:

Prefix Length: 64

Default Gateway:

SSH

☑ Enable SSH Server

SSH Key Type: RSA

SSH Key Length: 1024 (1024-2048)

☑ Discover the VDC

At the end of VDC creation, DCNM will start discovering the VDC with the below mentioned Credentials.

User Name: admin

Password: ●●●●●●●●●●

Step 14 Click **Finish** to complete the Ethernet VDC setup wizard.

Creating an Storage VDC

You can create an storage VDC. In storage VDC, you can allocate storage VLANs on Ethernet VDCs. The allocated storage VDC creates VLANs in the dedicated VLAN range. Shared interfaces uses storage VLANs to carry both Ethernet and storage traffic. It is required that the VLANs should be mutually exclusive between Ethernet and storage VDCs.

Note

- Starting with the Cisco DCNM Release 6.1(1), if you donot have the license for storage VDC you can only add and delete storage VDCs. If you need to access the complete functionalities then it is mandatory that you procure a license.
- Starting with the Cisco DCNM Release 6.1(1), the storage VDCs can be discovered and managed.

BEFORE YOU BEGIN

Log in to the default VDC with a username that has the network-admin user role.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Virtual Devices**.

Step 2 From the Summary pane, double-click **Virtual Devices**.

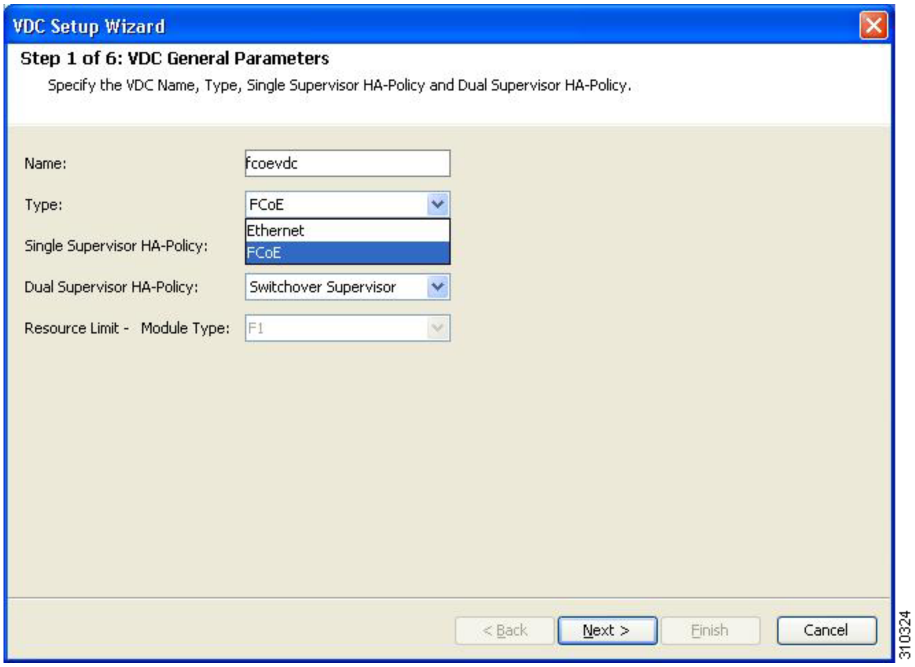
The VDC Summary Table screen appears.

Step 3 Right-click the **Summary Table**. The context menu appears.

Step 4 In the context menu, choose **Create VDC**. The VDC wizard appears.

Step 5 Specify the VDC name, VDC type, single supervisor HA policy, dual supervisor HA policy, and the module type (see Figure 4-10).

Figure 4-10 VDC General Parameters Screen



VDC Setup Wizard

Step 1 of 6: VDC General Parameters

Specify the VDC Name, Type, Single Supervisor HA-Policy and Dual Supervisor HA-Policy.

Name: fcoevdc

Type: FCoE

Single Supervisor HA-Policy:

Dual Supervisor HA-Policy: Switchover Supervisor

Resource Limit - Module Type: F1

Step 6 Click **Next**.

The Storage VLAN Allocation screen appears.

Step 7 Specify the Storage VLANs to be allocated on the Ethernet VDC (see Figure 4-11).

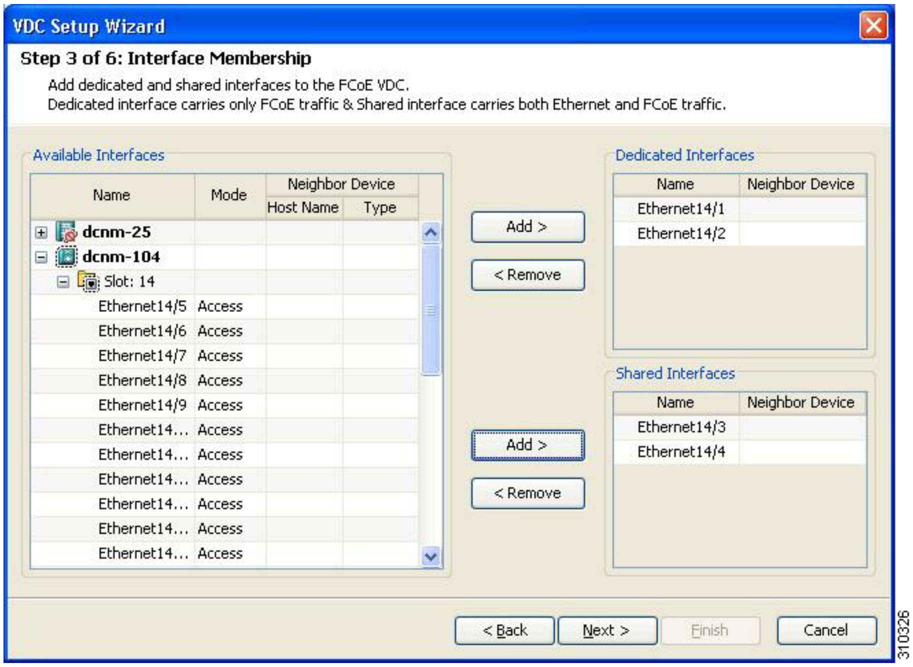
Step 8 Click **Next**.

The Interface Membership screen appears.

Step 9 Add the dedicated and shared interfaces to the Storage VDC (see Figure 4-11).

Note The dedicated interface carries only Storage traffic and the shared interface carries both the Ethernet and the Storage traffic.

Figure 4-11 Interface Membership Screen



VDC Setup Wizard

Step 3 of 6: Interface Membership

Add dedicated and shared interfaces to the FCoE VDC.
Dedicated interface carries only FCoE traffic & Shared interface carries both Ethernet and FCoE traffic.

Available Interfaces

Name	Mode	Neighbor Device	
		Host Name	Type
⊞ dcnm-25			
⊟ dcnm-104			
⊟ Slot: 14			
Ethernet14/5	Access		
Ethernet14/6	Access		
Ethernet14/7	Access		
Ethernet14/8	Access		
Ethernet14/9	Access		
Ethernet14...	Access		
Ethernet14...	Access		
Ethernet14...	Access		
Ethernet14...	Access		
Ethernet14...	Access		
Ethernet14...	Access		

Dedicated Interfaces

Name	Neighbor Device
Ethernet14/1	
Ethernet14/2	

Shared Interfaces

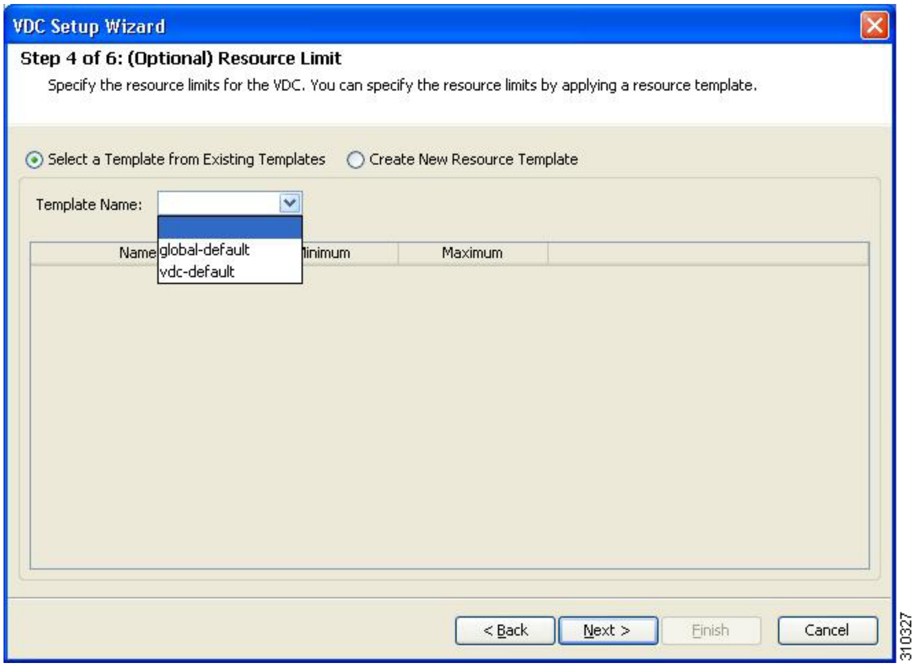
Name	Neighbor Device
Ethernet14/3	
Ethernet14/4	

Step 10 Click **Next**.

The Resource Limit screen appears.

Step 11 (Optional) Specify the resource limits for the VDC (see Figure 4-12).

Figure 4-12 Resource Limit Screen



VDC Setup Wizard

Step 4 of 6: (Optional) Resource Limit

Specify the resource limits for the VDC. You can specify the resource limits by applying a resource template.

● Select a Template from Existing Templates ○ Create New Resource Template

Template Name:

global-default
vdc-default

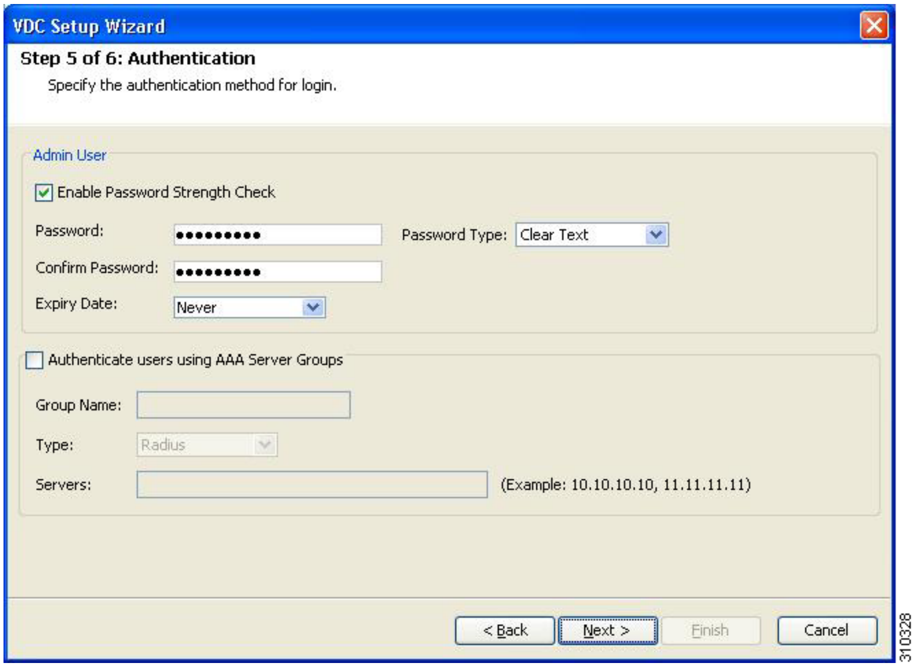
Name	Minimum	Maximum

Step 12 Click **Next**.

The Authentication screen appears.

Step 13 Specify the authentication method for login (see Figure 4-13).

Figure 4-13 Authentication Screen



VDC Setup Wizard

Step 5 of 6: Authentication

Specify the authentication method for login.

Admin User

☑ Enable Password Strength Check

Password: ●●●●●●●●● Password Type: Clear Text

Confirm Password: ●●●●●●●●●

Expiry Date: Never

☐ Authenticate users using AAA Server Groups

Group Name:

Type: Radius

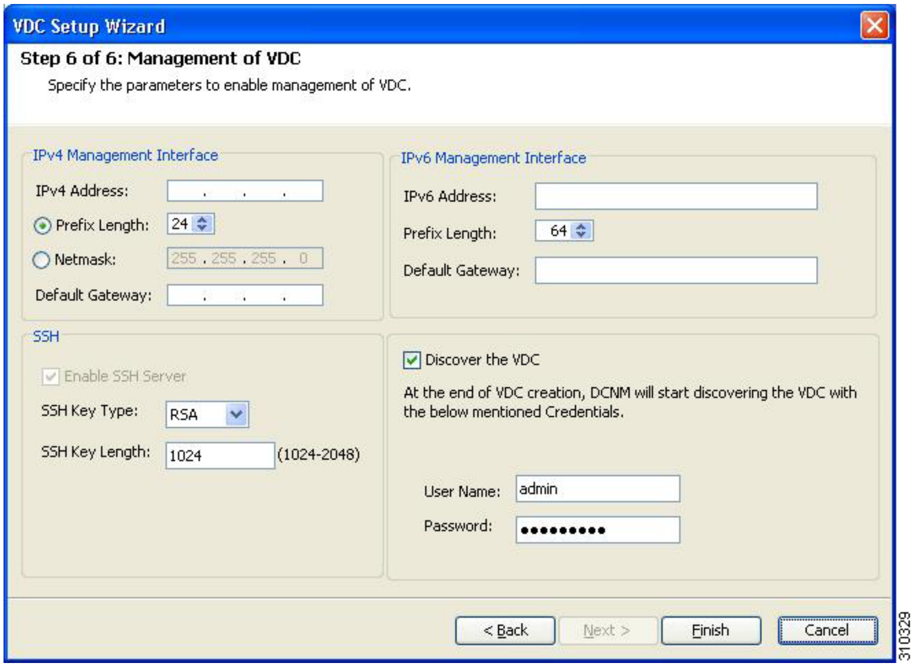
Servers: (Example: 10.10.10.10, 11.11.11.11)

Step 14 Click **Next**.

The VDC Management screen appears.

Step 15 Specify the parameters to enable the management of the VDC (see Figure 4-14).

Figure 4-14 Management of VDC Screen



VDC Setup Wizard

Step 6 of 6: Management of VDC

Specify the parameters to enable management of VDC.

IPv4 Management Interface

IPv4 Address: . . .

● Prefix Length: 24

○ Netmask: 255 . 255 . 255 . 0

Default Gateway: . . .

IPv6 Management Interface

IPv6 Address:

Prefix Length: 64

Default Gateway:

SSH

☑ Enable SSH Server

SSH Key Type: RSA

SSH Key Length: 1024 (1024-2048)

☑ Discover the VDC

At the end of VDC creation, DCNM will start discovering the VDC with the below mentioned Credentials.

User Name: admin

Password: ●●●●●●●●●

Step 16 Click **Finish** to complete the Storage VDC setup wizard.

Allocating a Storage VLAN on the Ethernet VDC

You can allocate an storage VLAN on an Ethernet VDC using the VDC details pane. For information on storage, see the *Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*.

BEFORE YOU BEGIN

Log in to the default VDC with a username that has the network-admin user role.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Virtual Devices**.

Step 2 From the Summary pane, double-click on **Virtual Devices**.

The Summary Table screen is displayed.

Step 3 In the Summary Table, choose the **Storage VDC**.

Step 4 In the Details pane, expand the **Storage VLAN Allocation**.

Step 5 Right-click on the table. The context menu is displayed.

Step 6 In the context menu, choose **Add Row**. A dialog box is displayed.

Step 7 From the dialog box, choose the **Ethernet VDC** and click **OK**.

Note You can associate only one Ethernet VDC with an Storage VDC for interface sharing.

Step 8 Specify the Storage VLANs in the newly added rows for the selected VDC.

Step 9 From the menu bar, choose **File > Deploy** to apply your changes to the device.

The specified VLANs will be allocated on an Ethernet VDC that is created only in an Storage VDC.

Choosing Storage-Capable Interfaces

Beginning with Cisco NX-OS Release 5.2 (1), the interface table in details pane will have a new column "Shared". This column will show whether the interface is dedicated (or) shared. For information on Storage, see the *Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*.

BEFORE YOU BEGIN

Log in to the default VDC with a username that has the network-admin user role.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Virtual Devices**.

Step 2 From the Summary pane, double-click the device to display the list of VDCs.

The Summary Table screen is displayed.

Step 3 In the Summary Table, select the **Storage VDC**.

Step 4 In the Details pane, expand **Interfaces**.

Step 5 Right-click on the interfaces table. The context menu is displayed.

Step 6 In the context menu, select **Add Interface**. A dialog box is displayed.

Step 7 From the dialog box, select the interfaces that you want to dedicate or share.

The dedicated interfaces will carry only the Storage traffic and the shared interfaces will carry both the Storage and the Ethernet traffic.

The Available Interfaces table shows the Storage capable interfaces in the Ethernet VDC.

Associating an Interface to an Storage VDC

You can add dedicated or shared Storage-capable interfaces with Storage VDC using the Interface association screen. For information on Storage, see the *Cisco NX-OS FCoE Configuration Guide for Cisco Nexus 7000 and Cisco MDS 9500*.

BEFORE YOU BEGIN

Log in to the default VDC with a username that has the network-admin user role.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Virtual Devices**.

Step 2 From the Summary pane, double-click the device to display the list of VDCs.

The Summary Table screen appears.

Step 3 In the Summary Table, choose the **Storage VDC**.

Step 4 In the Details pane, expand **Interfaces**.

Step 5 Choose a desired interface in the association pane and right-click on the context menu.

Step 6 In the context menu, choose **Add as Dedicated/Share Interface** to add the selected interfaces as dedicated or shared interfaces to the Storage VDC.

Changing VDC Resource Limits

You can change the limits on the VDC resources. Changes to the limits take effect immediately except for the IPv4 and IPv6 routing table memory limits, which take effect after the next VDC reset, physical device reload, or physical device stateful switchover.

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

BEFORE YOU BEGIN

Ensure that you have discovered the physical device using a username that has the network-admin role.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Virtual Devices**.

Step 2 From the Summary pane, double-click the device to display the list of VDCs.

Step 3 Click the VDC to change.

The Details tab appears in the Details pane.

Step 4 From the Details pane, click **Resources**.

Step 5 Double-click the limit to change and enter the new value.

Step 6 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Changing the HA Policies

You can change the HA policies for a VDC. The VDC HA policies are as follows:

- Dual supervisor modules:
  - Bringdown—Puts the VDC in the failed state. To recover from the failed state, you must reload the physical device.

  - Restart—Restarts the VDC. This process includes shutting down all the interfaces within that VDC and stopping all the virtualized services processes. The Cisco NX-OS software restarts all the virtualized services saved in the startup configuration and brings the interfaces back up with the configuration saved in the startup configuration. Any configuration that you did not save in the startup configuration prior to the restart is lost.
  - Switchover—Initiates a supervisor module switchover.
- Single supervisor modules:
  - Bringdown—Puts the VDC in the failed state. To recover from the failed state, you must reload the physical device.
  - Reload—Reloads the supervisor module.

Caution With the reload action, any configuration that you did not save in the startup configuration prior to the reload is lost.

Note The reload action affects all interfaces and all VDCs on the physical device.

  - Restart—Restarts the VDC. This process includes shutting down all the interfaces within that VDC and stopping all the virtualized services processes. The Cisco NX-OS software restarts all the virtualized services saved in the startup configuration and brings the interfaces back up with the configuration saved in the startup configuration. Any configuration that you did not save in the startup configuration prior to the restart is lost.

Caution With the reload action, any configuration that you did not save in the startup configuration prior to the reload is lost.

Note You cannot change the HA policies for the default VDC.

BEFORE YOU BEGIN

Ensure that you have discovered the physical device using a username that has the network-admin role.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Virtual Devices**.

Step 2 From the Summary pane, double-click the device to display the list of VDCs.

Step 3 Click the VDC to change.

The Details tab appears in the Details pane.

Step 4 From the Single Supervisor HA-Policy field, click the down arrow and choose an HA policy from the drop-down list.

Step 5 From the Dual Supervisor HA-Policy field, click the down arrow and choose an HA policy from the drop-down list.

Step 6 From the menu bar, choose **File > Deploy** to apply your changes to the device.

Saving All VDC Configurations to the Startup Configuration

You can save the running configuration of all the VDCs on the physical device to the startup configuration.

BEFORE YOU BEGIN

Ensure that you have discovered the physical device using a username that has the vdc-admin or network-admin role.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Virtual Devices**.

Step 2 From the Summary pane, double-click the device to display the list of VDCs.

Step 3 Right-click the device with the VDC configurations that you want to save.

Step 4 Choose **Copy Run to Start for All Vdc(s)**.

Step 5 Click the icon in the bottom left corner of the screen.

The Status pane appears and shows whether the VDC configurations were copied successfully to the startup configuration.

Saving the VDC Configuration to a Bootflash File

You can save the running configuration for an individual VDC to a file in the bootflash directory.

BEFORE YOU BEGIN

Ensure that you have discovered the physical device using a username that has the vdc-admin or network-admin role.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Virtual Devices**.

Step 2 From the Summary pane, double-click the device to display the list of VDCs.

Step 3 Right-click the VDC with the configuration that you want to save.

Step 4 Choose **Copy Run to Bootflash file**.

The Enter Bootflash File Name window appears.

Step 5 In the Bootflash File Name field, enter the name of the file to which the running configuration will be copied and click **OK**.

Step 6 Click the icon in the bottom left corner of the screen.

The Status pane appears and shows whether the VDC configuration was copied successfully to the bootflash file.

Discovering VDCs

You can discover a nondefault VDC with user credentials that are different from the default VDC.

BEFORE YOU BEGIN

Ensure that you have set the correct logging severity levels in the VDC using the Cisco NX-OS device command-line interface (CLI) (see the *Cisco DCNM Fundamentals Configuration Guide, Release 5.x*).

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **DCNM Server Administration > Devices and Credentials**.

Step 2 From the menu bar, choose **Devices and Credentials > New Device**.

A new line appears in the Devices list.

Step 3 Click the cell under IP Address in the new line and enter the IP address of the VDC to discover.

Step 4 Double click the cell under User Credentials in the new line and click the down arrow to display the user credentials dialog. Enter the user credentials information and click **OK**.

Step 5 From the menu bar, choose **Devices and Credentials > Discover**.

Deleting a VDC

When you delete a VDC, the Cisco NX-OS software removes the configuration for all interfaces allocated to the VDC and returns the interfaces to the default VDC. Deleting a VDC stops all virtualized services and removes any configuration within that VDC.

Note You cannot delete the default VDC (VDC 1).

Caution Deleting a VDC disrupts all traffic on the VDC.

BEFORE YOU BEGIN

Ensure that you have discovered the physical device using a username that has the network-admin role.

DETAILED STEPS

Step 1 From the Feature Selector pane, choose **Virtual Devices**.

Step 2 From the Summary pane, double-click the device to display the list of VDCs.

Step 3 Click the VDC to delete.

Step 4 From the menu bar, choose **Virtual Devices > Delete VDC**.

The VDC disappears from the list in the Summary pane.

Field Descriptions for VDC Management

This section includes the following topics:

Field Description: Virtual Devices: Summary Pane

Table 4-3 Field Description: Virtual Devices: Summary Pane

Element	Description
Name	Name of the physical or VDC device.
Status	Status of the VDC.
Single Supervisor HA Policy	Single supervisor HA policy for the virtual device.
Dual Supervisor HA Policy	Dual supervisor HA policy for the virtual device.
MAC Address	MAC address for the virtual device.
Management Interface IP Address Prefix	IP address and prefix for the VDC management interface.
Management Interface Status	Status of the VDC management interface.
SSH	SSH status.

Field Description: Virtual Devices: virtual device: Details Tab: General Section

Table 4-4 Field Description: Virtual Devices: virtual device: Details Tab: General Section

Element	Description
Switch Name	Name of the physical device.
VDC Name	Name of the virtual device.
Single Supervisor HA Policy	Single supervisor HA policy for the virtual device.

Table 4-4 Field Description: Virtual Devices: virtual device: Details Tab: General Section (continued)

Element	Description
Dual Supervisor HA Policy	Dual supervisor HA policy for the virtual device.
Status	Status of the virtual device.
MAC Address	MAC address for the virtual device.

Field Description: Virtual Devices: virtual device: Details Tab: Interfaces Section

Table 4-5 Field Description: Virtual Devices: virtual device: Details Tab: Interfaces Section

Element	Description
Interface Name	Name of the Ethernet interfaces allocated to the virtual device.
Mode	Mode for the interface.
Admin Status	Administrative status for the interface.
Operational Status	Operational status for the interface.
Description	Description for the interface.

Field Description: Virtual Devices: virtual device: Details Tab: Resources Section

Table 4-6 Field Description: Virtual Devices: virtual device: Details Tab: Resource Section

Element	Description
Name	Name of the resource.
Allocation	
Minimum	Minimum guarantee limit for a resource.
Maximum	Maximum limit for a resource on an as-available basis.
Current Usage	
Used	Amount of a resource currently in use.
Available	Amount of the resource currently not used.
Used Percent	Percent of the total resource for the virtual device.

Field Description: Virtual Devices: Create VDC: VDC General Parameters

Table 4-7 Field Description: Virtual Devices: Create VDC: VDC General Parameters

Element	Description
VDC Name	Name of the VDC.
HA Policy	HA policy of the selected VDC.

Field Description: Virtual Devices: Create VDC: Authentication

Table 4-8 Field Description: Virtual Devices: Create VDC: Authentication

Element	Description
Local User Database	User Name—Name of the user.
	Password—Password Field.
	Expiry Date.
AAA Server Groups	Group Name—Name of the group.
	Type—Server type.
	Servers—Disables the authentication.
No Authentication	Disable Authentication.

Field Description: Virtual Devices: Create VDC: Management of VDC

Table 4-9 Field Description: Virtual Devices: Create VDC: Authentication

Element	Description
Management Interface	IPv4 address.
	Prefix Length—IPv4 Prefix Length.
	Netmask—IPv4 Netmask.
	IPv6 address.
SSH	Enable SSH server—Enable or disable SSH server.
	SSH key length.
	SSH key type.
XML Agent	Enable XML agent.

Additional References for Managing VDCs

For additional information related to managing VDCs, see the following sections:

- Related Documents for Managing VDCs, page 4-27

Related Documents for Managing VDCs

Related Topic	Document Title
Cisco DCNM Licensing	*Cisco DCNM Installation and Licensing Guide, Release 5.x*
Cisco NX-OS Licensing	*Cisco NX-OS Licensing Guide*
Cisco Nexus 7000 Series 32-port 10-Gbps Ethernet module	*Cisco Nexus 7000 Series Hardware Installation and Reference Guide*
Command reference	*Cisco Nexus 7000 Series NX-OS Virtual Device Context Command Reference, Release 5.x*

Feature History for Managing VDCs

Table 4-10 lists the release history for this feature.

Table 4-10 Feature History for Managing VDC

Feature Name	Releases	Feature Information
Administrator VDC Support	6.1.(1)	Added administrator VDC support managing VDC.
Storage VDC Support	6.1.(1)	Added Storage VDC information for VDC wizard.
Support for F2 module-type	5.2(2a)	Added F2 module-type support for creating a VDC wizard.
FCoE VDC enhancements	5.2(1)	Added FCoE support for creating a VDC wizard.
Support for N7K-F132XP-15 module	5.1(1)	VDC supports the N7K-F132XP-15 module. This module has 16 port groups that consist of 2 ports each.
Saving VDC configurations	5.1(1)	You can save the VDC configuration of the physical device to the startup configuration or to a bootflash file.
Managing VDCs	5.0(2)	No change from Release 4.2.
Restarting VDCs	4.2(1)	You can restart active nondefault VDCs and nondefault VDCs in the failed state.
VDC prompt format	4.2(1)	You can change the format of the command-line interface (CLI) prompt for nondefault VDCs.

INDEX