White Paper

Cisco Nexus 7000 Series Virtual Device Context Deployment Scenarios and Recommended Practices

What You Will Learn

This document discusses the applicability, use cases, and recommended practices related to the logical virtualization of a single physical platform using the virtual device context (VDC) feature of Cisco® NX-OS Software.

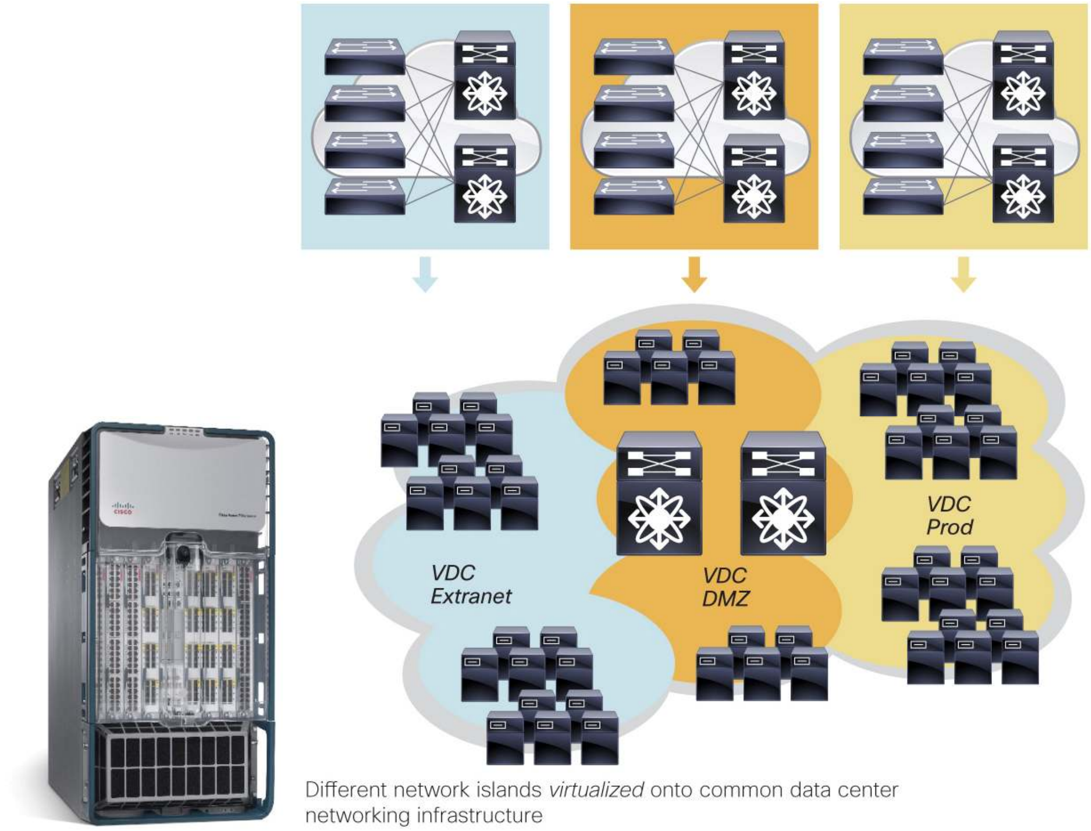
This document is written for network architects, engineers, and operations personnel with an interest in the design, deployment, and possible use cases related to the Cisco NX-OS VDC feature set.

Virtual Device Context Overview

Cisco's VDC feature helps enable the virtualization of a single physical device in one or more logical devices (Figure 1). Each of the provisioned logical devices is configured and managed as if it were a separate physical device. Operating system processes and hardware resources can be partitioned and grouped to form a VDC. This logical partitioning of the device throughout the control, data, and management planes provides similar fault domain isolation and enables the approximation of air-gapped multidevice network environments. In fact, the same VLAN number can be configured in different VDCs without problems. Note, though, that the VDC is a local construct and does not extend between two devices.

To enable the VDC functions, an Advanced license is required and must be associated with the serial number of a Cisco Nexus® 7000 Series Switch chassis. For a Fibre Channel over Ethernet (FCoE) deployment, the storage VDC must be enabled through a Storage license associated with a specific line card (F1 or, soon, F2), and the Advanced license on the chassis is not required (unless more than one Ethernet VDC is needed).

Figure 1. Different Network Islands Virtualized onto Common Data Center Networking Infrastructure



Different network islands *virtualized* onto common data center networking infrastructure

The business benefits of VDCs are clear. Consolidation of multiple networks onto a single infrastructure in a reliable and secure way leads to significant cost savings (up to 50 percent) in both capital expenditures (CapEx) and operating expenses (OpEx), as numerous customers have attested. Savings include reduced footprint, reduced power consumption, streamlined cabling, and simplified management.

- Some typical use cases for the Cisco Nexus 7000 Series VDC feature are as follows:
- Separate production, development, and test environments
- Separate intranet from DMZ and extranet
- Separate environments for mission-critical applications
- Separate departments within the same organization

Currently, four VDCs are supported. Future enhancements tied to the introduction of new hardware are also under evaluation to provide even greater scalability in the maximum number of VDCs.

In general, physical interfaces cannot be shared by multiple VDCs. This one-to-one assignment of physical interfaces to VDCs is at the basis of complete isolation among the configured contexts. However, there are two exceptions:

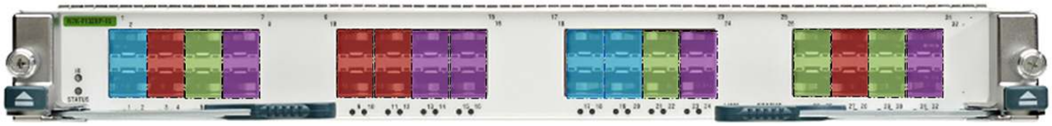
- The out-of-band management interface (mgmt0) can be used to manage all VDCs. Each VDC has its own representation for mgmt0 with a unique IP address that can be used to send syslog, SNMP and other management information.

- When a storage VDC is configured, a physical interface can belong to one VDC for Ethernet traffic and to the storage VDC for FCoE traffic. Traffic entering the shared port is sent to the appropriate VDC according to the frame's EtherType. Specifically, the storage VDC will get the traffic with EtherType 0x8914 for FCoE Initialization Protocol (FIP) and 0x8906 for FCoE.

Physical interfaces can be assigned to a VDC with a high degree of freedom. However, there are differences among different I/O modules because of the way the VDC feature is enforced at the hardware level. The easy way to learn the specific capabilities of the installed hardware is by entering the **show interface x/y capabilities** command to see the port group associated with a particular interface. Here is a summary of available options:

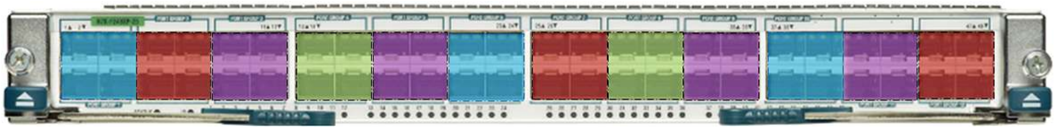
- On the F1 32-port 1 and 10 Gigabit Ethernet module (N7K-F132XP-15), interfaces belonging to the same port group (for example, 1 and 2) must be assigned to the same VDC, as shown in Figure 2.

Figure 2. Port Groups for N7K-F132XP-15



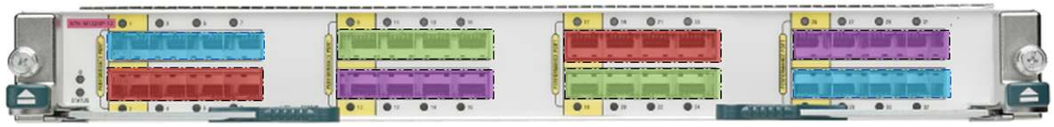
- On the F2 48-port 1 and 10 Gigabit Ethernet module (N7K-F248XP-25), interfaces belonging to the same port group (for example, 1, 2, 3, and 4) must be assigned to the same VDC, as shown in Figure 3.

Figure 3. Port Groups for N7K-F248XP-25



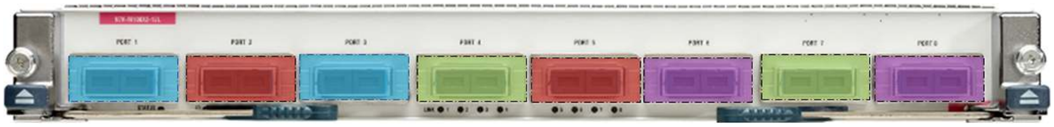
- On the M1 32-port 10 Gigabit Ethernet modules (N7K-M132XP-12 and N7K-M132XP-12L), interfaces belonging to the same port group (for example, 1, 3, 5, and 7) must be assigned to the same VDC, as shown in Figure 4.

Figure 4. Port Groups for N7K-M132XP-12 and 12L



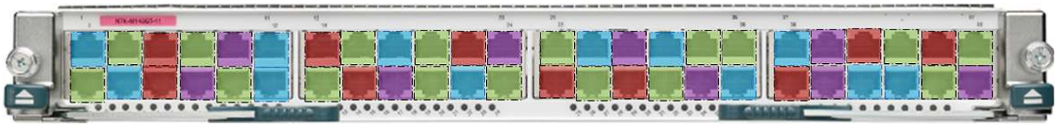
- On the M1 8-port 10 Gigabit Ethernet module (N7K-M108X2-12L), there are no restrictions for assigning interfaces to VDCs, as shown in Figure 5.

Figure 5. Port Groups for N7K-M108X2-12L



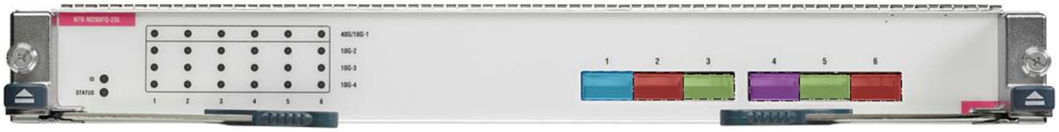
- On the M1 48-port 10/100/1000 and 1 Gigabit Ethernet modules (N7K-M148G**x**-12 and N7K-M148G**x**-12L), there are no restrictions for assigning interfaces to VDCs, as shown in Figure 6. However, for optimization purposes, you should keep any group of consecutive 12 ports in the same VDC.

Figure 6. Port Groups for N7K-M148Gx-12 and 12L



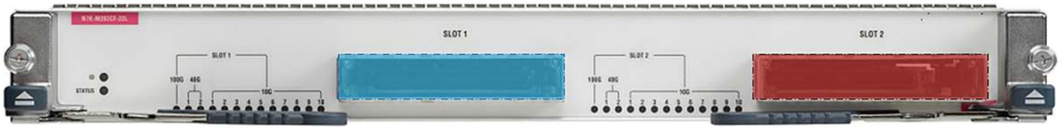
- The M2 6-port 40 Gigabit Ethernet module (N7K-M206QF-23L) has no restrictions for assigning interfaces to VDCs, as illustrated in Figure 7.

Figure 7. Port Groups for N7K-M206QF-23L



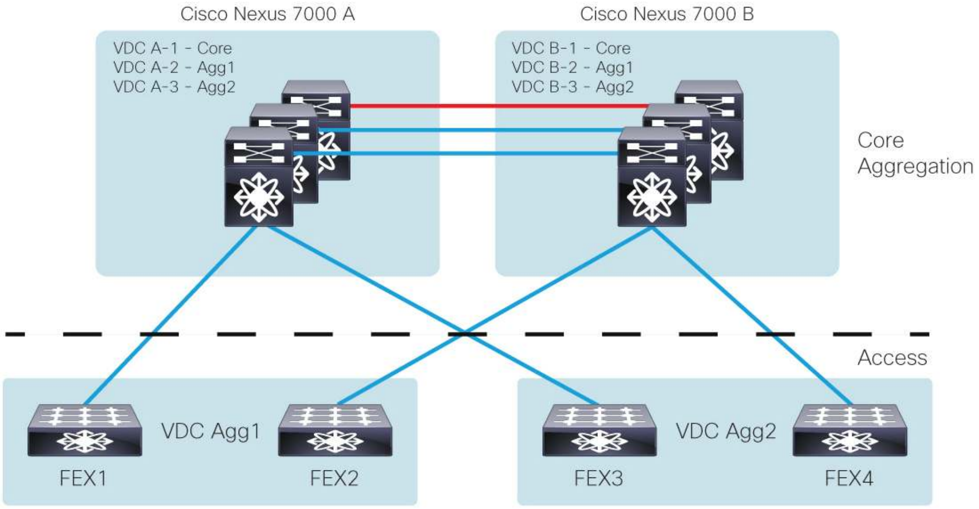
- The M2 2-port 100 Gigabit Ethernet module (N7K-M202CF-23L) has no restrictions for assigning interfaces to VDCs, as illustrated in Figure 8.

Figure 8. Port Groups for N7K-M202CF-23L



- On the Cisco Nexus 2000 Series Fabric Extenders (FEX modules) connected to the Cisco Nexus 7000 Series Switches, all interfaces must be assigned to the same VDC, as shown in Figure 9.

Figure 9. Cisco Nexus 7000 Series with Fabric Extenders in VDCs



Users can get access to the full feature set, or to part of it, depending on their role and associated privileges. Because of this advanced role-based access control (RBAC), different users can manage different VDCs. In addition to the four predefined user roles, many others can be configured as needed.

The technology that supports VDCs has been available since the launch of the Cisco Nexus 7000 Series in April 2008 and is extremely well validated in the field. Thousands of customers have adopted and benefited from VDCs so far.

Common Deployment Scenarios

The following section examines some common deployment scenarios in which VDCs can be applied to meet operation requirements while reducing physical infrastructure requirements. The scenarios presented are generalized to apply to most environments, but they can easily be customized to more tightly integrate with specific use cases similar to these.

VDCs for Service Insertion and Firewalled Security Environments

VDCs can be used in almost any situation that requires traffic direction or engineering through a service device. The additional benefits of logical separation of data plane, control plane, and management planes can make service insertion or policy enforcement more deterministic and secure for sensitive environments. This requirement is very typical of high-security environments such as the immediate network infrastructure surrounding firewall deployments. While not specifically a security feature on their own, the VDC feature does provide the level of logical separation within a single physical device that is needed to approximate an air-gapped physically separate infrastructure.

By creating separate VDCs for the logical areas adjacent to a firewall, the network administrator can create logically diverse network areas that are effectively separated and cannot be easily bypassed or joined. This firm logical separation is resistant to firewall device bypass through accidental or intentional device reconfiguration. Essentially, the only way to bypass the firewall device in a scenario that properly deploys VDCs is to connect a physical cable from one VDC to another.

Figure 10 shows the configuration of traditional firewall separation with VLANs. Figure 11 shows the deployment configuration for VDCs with a firewall. In the VDC example, two VDCs have been created, and in total three VDCs are in use. The default VDC, which exists on the system from initial bootup, is used to create two additional VDCs. After the two additional VDCs are created, the default VDC acts as the administrative VDC for all other VDCs. Because of the overall administrative powers associated with the administrative VDC, the administrative VDC should be reserved strictly for VDC administration in high-security environments. The two additional VDCs created are used for the “clean” and “dirty” (that is, inside and outside) security areas of the firewall infrastructure.

Figure 10. Traditional Firewall Separation with VDCs

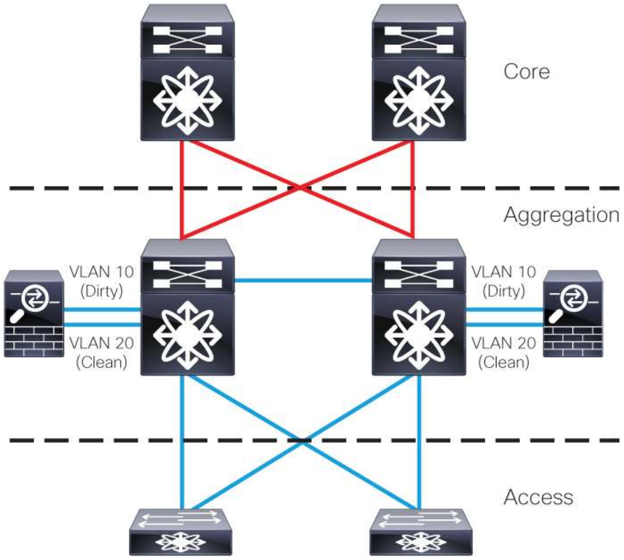
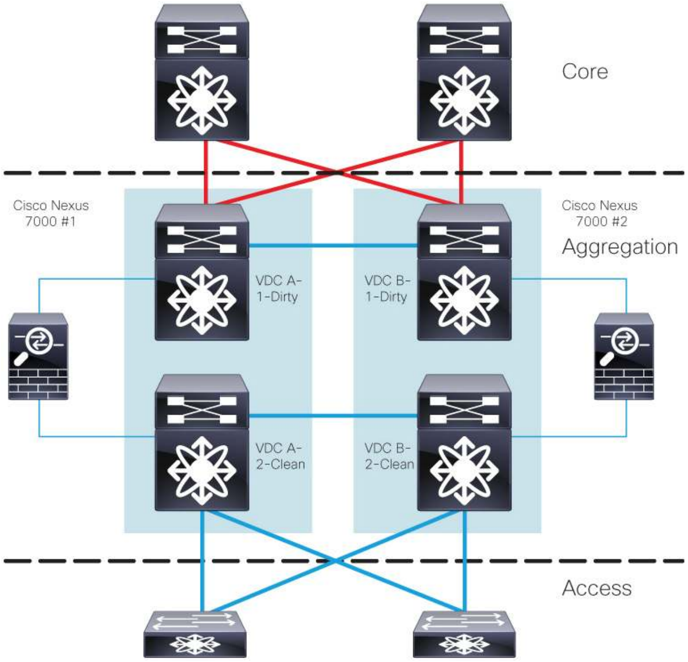


Figure 11. Enhanced Firewall Separation with VDCs



The deployment of a service insertion strategy using VDCs in a similar manner can also offer greater integration and scalability in certain cases. For example, the insertion of service devices that transparently pass spanning tree Bridge Protocol data units (BPDUs) in a Multiple Spanning Tree (MST) environment would impose limitations as to which and how many of the total VLANs could be used for ingress and egress areas of the service device. This limitation occurs because two VLANs sharing the same MST instance would consider traffic passing through a transparent device to be part of a bridge loop and would place the path in a blocking mode. In nonvirtualized environments, this behavior effectively limits the number of deployable VLANs to half of the available VLANs. The only design option to alleviate this limitation is to use a Per-VLAN Spanning Tree (PVST) protocol. However the use of a per-VLAN option typically limits overall scalability. The use of VDCs in this case can enable slightly greater scalability in an MST environment by allowing the use of different ingress and egress VDCs, each using separate and distinct MST domains. Since each MST instance between VDCs is identified as different and unique, spanning tree will converge in a nonblocking topology between VDCs. This approach effectively multiplies the number of usable MST instances by the number of VDCs deployed.

VDCs for Horizontal Device Consolidation

VDCs can be used to consolidate parallel physical devices that share the same functional role characteristics across one or more administrative domains or service areas (horizontal consolidation). For example, aggregation switches can be consolidated in a data center that delivers service to three different service groups such as business units in an enterprise or, in the case of a service provider environment, multiple customers. In a traditional configuration, each service group’s data center access domain would be isolated from the other service groups through physically independent aggregation devices. This separation may be implemented to satisfy availability requirements or service-level agreements (SLAs) on a per-group or per-customer basis. An alternative design for this deployment is to use Cisco Nexus 7000 Series VDCs to create virtualized logical aggregation devices within a single physical platform. This configuration can provide some facility resource utilization advantages by optimizing the use of space, power, and cooling while delivering isolation comparable to separate devices between service groups.

A physically separate solution (Figure 12) would typically be able to scale to a larger maximum size because of the nature of linear platform resource scaling associated with additional devices; however, until that level of scale is required, any investment in the linear growth of those resources represents a cost:benefit challenge because some resources may be idle. With the VDC approach (Figure 13), growth can be more closely managed to accommodate the actual environment and use requirements. Additionally, if future growth requires evolution to dedicated independent physical devices, the actual migration from VDCs to physical devices is simplified because of the structure of VDC configurations. VDC configurations mimic independent physical configurations so closely that they can be ported to new devices easily.

Figure 12. Typical Physical Topology

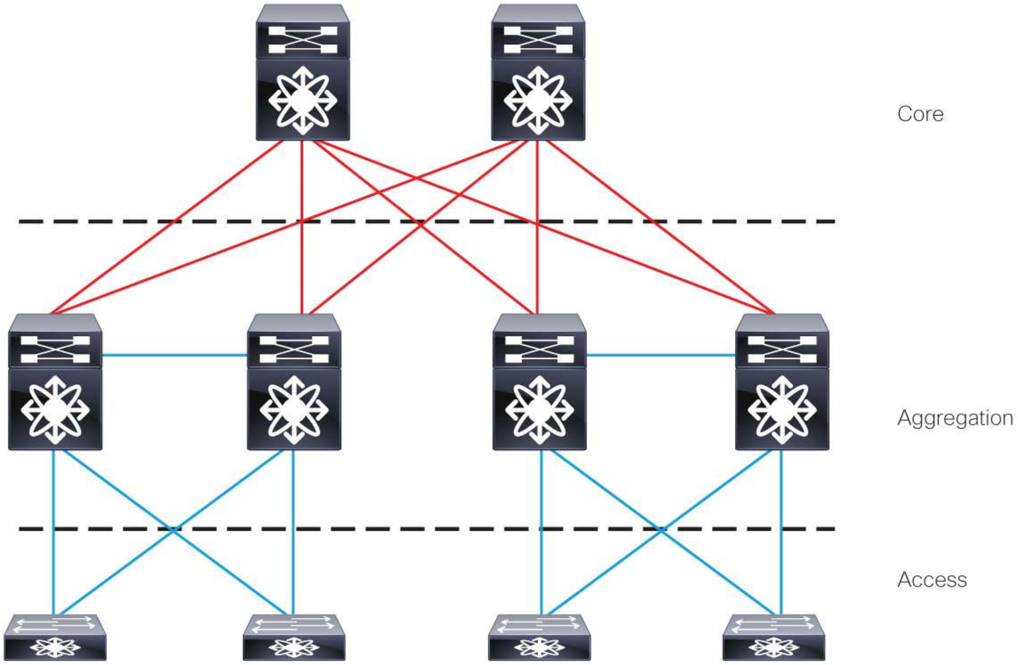
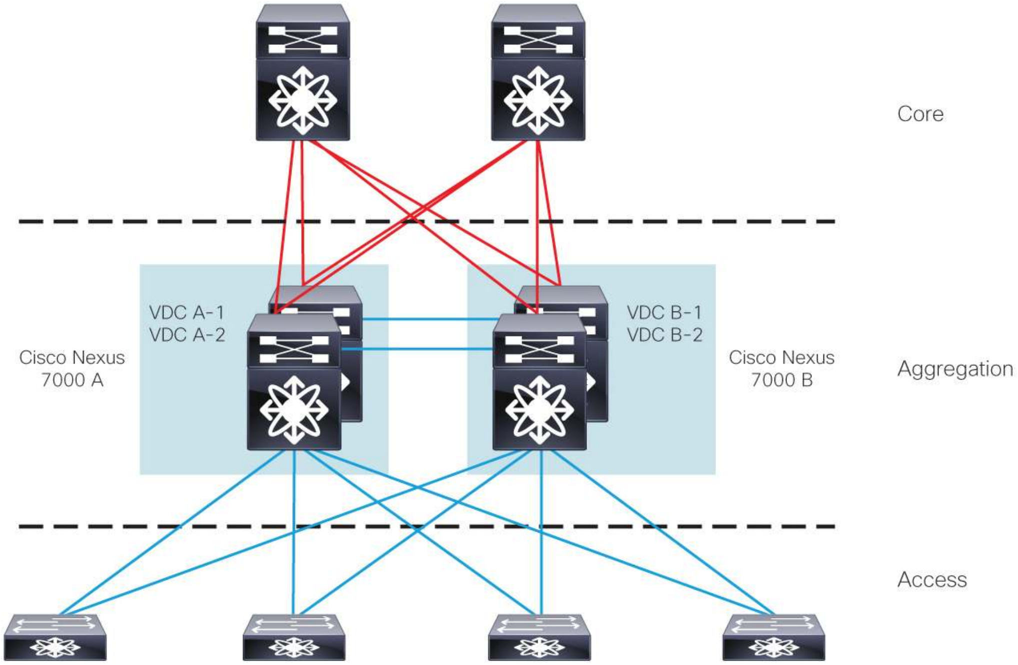


Figure 13. Horizontal Consolidation with VDCs



In the example of horizontal consolidation using VDCs, the consolidation of multiple aggregation devices connected to a common core-edge device produces virtual aggregation switches. Because VDCs deliver virtualization across data, control, and management planes, configuration and management options are more flexible than what is offered by other virtualization solutions such as Virtual Route Forwarding (VRF) instances and VLANs. With VDCs, the virtual aggregation devices may all be under the control of one administrative or service domain, as is the case in most enterprise environments, or they may be separately controlled or maintained within various administrative or service domains: for example, on a per-business unit or per-application basis. In service provider environments, the use of VDCs can enable consolidation while still allowing the allocation of individual device management at the customer or subscriber level. In either case, the extended virtualization offered by VDCs provides more options for organizational and operations structure than has previously been available.

Typical use cases include multi-tenant data center environments, mergers and acquisitions, and service provider hosted and co-location environments.

VDCs for Vertical Device Consolidation

VDCs can also be used to consolidate physical devices that provide different functional characteristics or roles in a network topology (vertical consolidation). For example, a network architect may vertically consolidate a data center core-edge device and a data center aggregation-level device. This type of collapsed core and aggregation layer provides benefits similar to those in the horizontal consolidation scenario: better use of the platform interface density and facility resources such as space, power, and cooling. Vertical consolidation also maintains the existing administrative or operations organizational structure. Regardless of whether the device tiers (core and aggregation) are controlled by a single operations management group or different groups (the core layer managed by one group, and the aggregation layer managed by another group), the organizational structure in control of the virtual devices does not change and remains consistent with the characteristics offered in a physically separate device solution. This consistency occurs because of the complete virtualization of the management and operations planes of the VDCs as well as the data and control planes. By allowing the independent configuration of management and operations services functions such as authentication, authorization, and accounting (AAA) and monitoring (Simple Network Management Protocol [SNMP] and XML) can be configured to cater to separate independent groups on a per-VDC basis.

Figure 14 shows a typical physical topology, and Figure 15 shows a topology using VDCs.

Typical use cases include a collapsed core and aggregation layer for small to medium-size environments, development environments, and branch offices or remote locations.

Figure 14. Typical Physical Topology

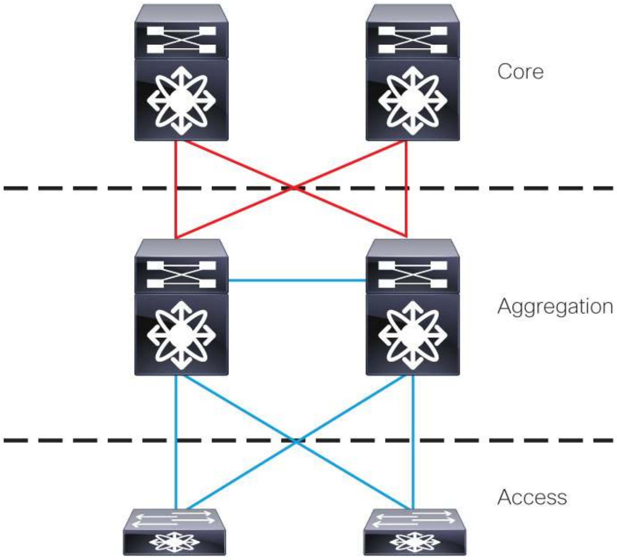
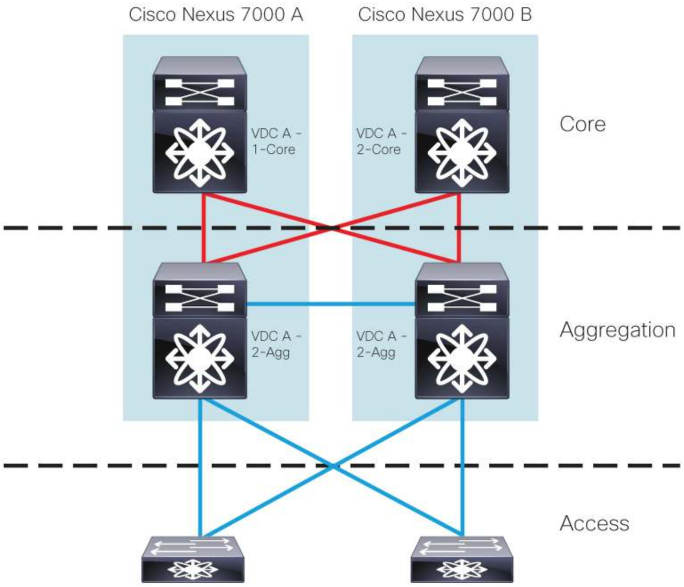


Figure 15. Vertical Consolidation with VDCs



VDCs for Combined Horizontal and Vertical Consolidation

In cases in which achieving the highest possible density is critical, you can deploy a combined horizontal and vertical consolidation strategy using VDCs. By using VDCs to reduce the footprint necessary to deliver the roles of several network component devices, this type of strategy provides the benefit of optimizing the use of the allocated facilities resources, such as space, power, and cooling. A combined horizontal and vertical consolidation strategy also can provide overall cost benefits compared to similar implementations using individual physical devices.

As the name implies, a combined horizontal and vertical consolidation strategy uses both horizontal and vertical consolidation, as depicted in prior examples, to combine similar and dissimilar network device roles and functions into one physical device spread across multiple logical devices. Again, the VDCs provide the same characteristic benefits seen earlier: control, data, and management plane separation that is capable of providing access and management to the individual virtual devices through one or more administrative or service domains. The service density of this solution again provides immediate benefits in terms of the facilities resource footprint by making optimal use of the allocated space, power, and cooling resources.

Typical use cases include collapsed core and aggregation topologies for small to medium-size deployments, mergers and acquisitions, and service provider hosted and co-location environments.

Figure 16 shows a typical physical topology, and Figure 17 shows a topology using VDCs.

Figure 16. Typical Physical Topology

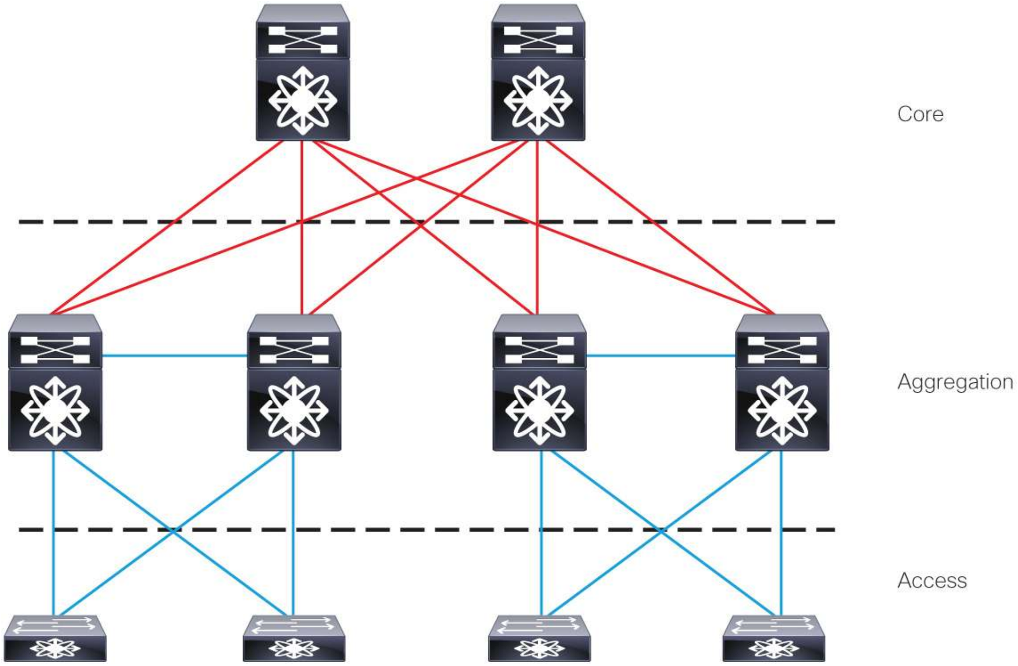
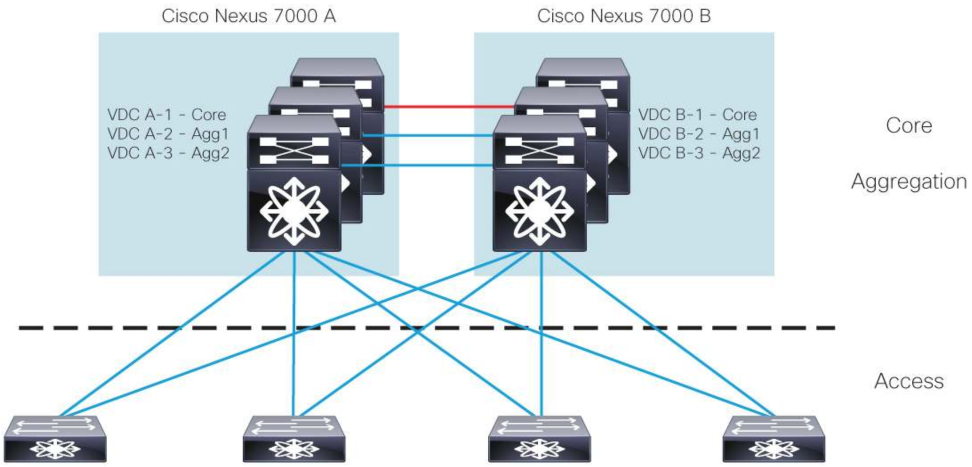


Figure 17. Combined Horizontal and Vertical Consolidation with VDCs



Virtual Device Contexts for Advanced Capabilities

In some cases, the advanced capabilities available on the Cisco Nexus 7000 Series can benefit from the use of VDCs. For example, Layer 2 extension across data centers with Cisco Overlay Transport Virtualization (OTV) can benefit from the creation of a dedicated VDC when a given VLAN requires both OTV encapsulation and switch virtual interface (SVI) routing. A dedicated VDC is also required to separate FCoE traffic from generic Ethernet traffic and maintain the classical dual-fabric design that is familiar to most Fibre Channel operators. Also, when the Cisco FabricPath capability is enabled to build very large Layer 2 domains without the burden of a spanning-tree algorithm, the combined adoption of VDCs can address several deployment challenges in a clean and effective way and allow a more flexible design.

VDC Recommended Practices

- For high-security sensitive environments, you should reserve the default VDC as the administrative VDC and use it strictly for the administration of the other VDCs. With this approach, you should not run data path traffic through the administrative VDC unless absolutely necessary.
- In all VDC environments, access to the default VDC should be restricted to the use of accounts with the least privileges necessary to accomplish operation tasks. For example, unless a particular user must configure global VDC parameters or provision other VDCs, you should assign that account the **vdc-admin** role and not the **network-admin** role.
- If the administrative VDC must be used for traffic, allocate the VDCs so that the domain with the highest availability requirements, or highest priority, is in the administrative VDC. This approach reduces the likelihood that operations on a lower-priority or less critical VDC (for example, resource reallocation or system reload operations) will affect the highest-priority or more critical domain.

- If VDCs have separate administrative domains (different VDCs administrators), you should apply AAA for authentication and authorization with care. Authenticating to the same AAA server across VDCs will implicitly apply authentication as if all VDCs were managed by a single administrative domain. To correctly segregate administrative domains among VDCs and prevent an administrative account for one VDC from gaining access and privileges on another VDC, the following options are available:
    - Create different admin user groups on the AAA server and use a feature such as network access restriction (on Cisco Secure Access Control System [ACS]) to limit the access of those user groups to specific AAA client IP addresses or groups. Since each VDC receives its AAA traffic from its local management interface IP address, this approach will enable the distinction between VDCs and essentially limit the access of a given VDC admin group to a specific subset of VDCs. The AAA server will identify the requesting VDC client IP address and take that factor into account during the authorization decision process.
    - Use a different AAA server for each VDC. VDCs allow the definition of discrete AAA servers for each VDC. The administrative accounts should be configured so that the admin account for any given VDC does not exist in the user database of the other AAA servers.
- Explicitly configure the high-availability policy of newly created VDCs as **restart** or **bring down** in a dual-supervisor configuration to reduce the effects of a failure within a single VDC. The default high-availability policy for VDCs in a dual-supervisor system is **switchover**. This policy will initiate a supervisor switchover of all VDCs if a failure occurs in a single VDC.
- The Cisco Nexus 7000 Series has a fully distributed architecture in which every module is capable of independent forwarding decisions and is equipped with a local forwarding engine and hardware forwarding tables. When assigning interface resources, dedicating an entire module to a VDC helps ensure that other VDCs will not compete for the same Layer 2 and 3 table resources, which could affect local hardware forwarding. Assigning a module to a VDC also helps ensure that a module failure will be isolated to the particular context.
- The Control Plane Policing (CoPP) hardware mechanism, regulating the amount of traffic destined to the control plane, is distributed on a per-module basis. Assigning a module entirely to a VDC helps ensure that individual VDCs have dedicated CoPP thresholds and clear provision of bandwidth to enable detailed control of traffic destined for the control plane.
- Review the CoPP policy and rate limits to help ensure that they are appropriate for the deployment environment. The system will apply CoPP collectively for all VDCs because there is only one logical in-band control-plane interface. Help ensure that the configured limits will meet the requirements of all necessary control-plane traffic for all active VDCs.

VDC Security Certifications

- VDC separation is industry certified. In 2010, NSS Labs certified the Cisco Nexus 7000 Series VDC feature for Payment Card Industry (PCI)-compliant environments. See https://www.nsslabs.com/reports/network-switch-virtualization-cisco-nexus-7000-q2-2010.
- Federal Information Processing Standards (FIPS 140-2) certification was completed in 2011. See http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1533.pdf.
- In 2011, the Cisco Nexus 7000 Series was awarded Common Criteria Evaluation and Validation Scheme (CCEVS) 10349 certification with EAL4 conformance. See http://www.niap-ccevs.org/cc-scheme/st/vid10349/.

Configuring and Managing VDCs

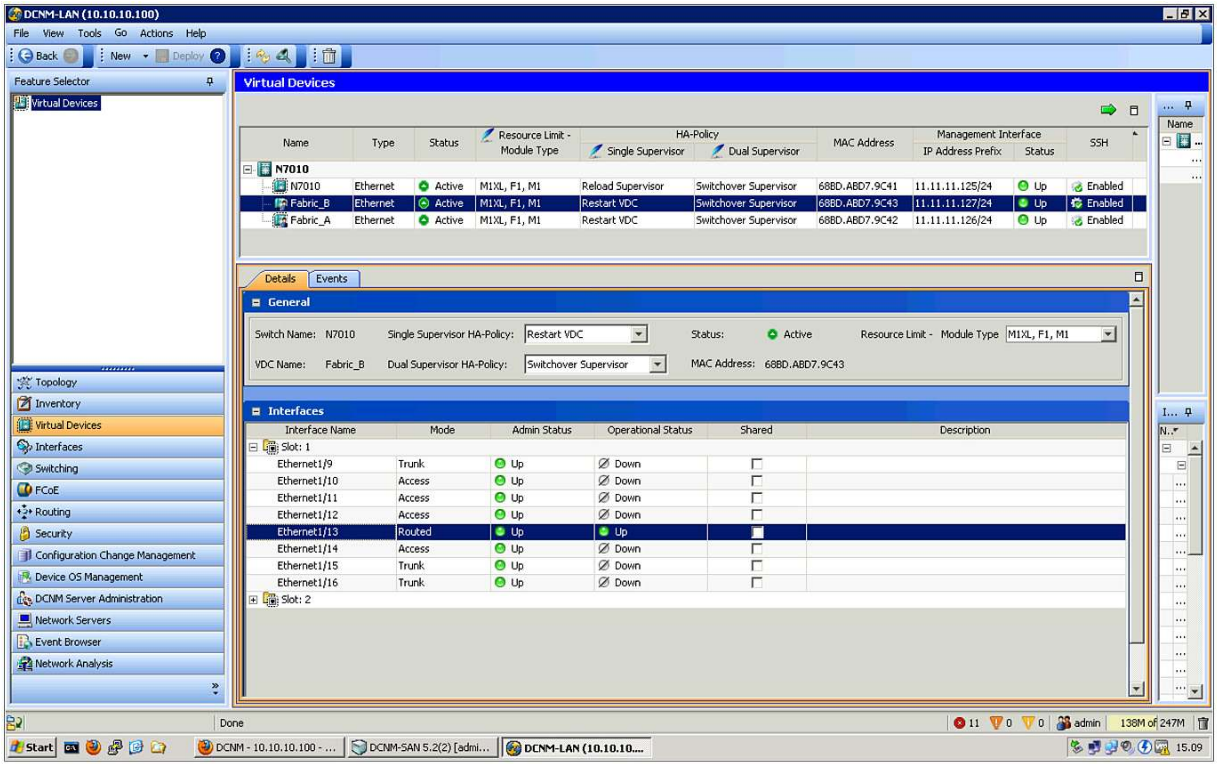
Despite being an advanced function enabled by sophisticated Cisco ASICs, the basic steps to enable and configure VDCs on a Cisco Nexus 7000 Series Switch are straightforward:

```
N7K1-VDC1# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
N7K1-VDC1(config)# vdc N7K1-VDC2
Note: Creating VDC, one moment please ...
N7K1-VDC1(config-vdc)# show vdc
vdc_id vdc_namestate mactype lc
--------------------------------------------
1 N7K1-VDC1 active 00:26:51:c7:34:41Ethernet m1f1m1xl
2 N7K1-VDC2 active 00:26:51:c7:34:42Ethernet m1f1m1xl
3 N7K1-VDC3 active 00:26:51:c7:34:43Ethernet m1f1m1xl
4 N7K1-VDC4 active 00:26:51:c7:34:44Ethernet m1f1m1xl

N7K1-VDC1(config-vdc)# allocate interface e8/1-12
Moving ports will cause all config associated to them in source vdc to be
removed. Are you sure you want to move the ports (y/n)? [yes] yes
N7K1-VDC1(config-vdc)# show vdc membership
vdc_id: 4 vdc_name: N7K1-VDC2 interfaces:
Ethernet8/1 Ethernet8/2 Ethernet8/3
Ethernet8/4 Ethernet8/5 Ethernet8/6
Ethernet8/7 Ethernet8/8 Ethernet8/9
Ethernet8/10 Ethernet8/11 Ethernet8/12
```

Many customers used to Cisco switches and routers rely on the familiar Cisco NX-OS command-line interface (CLI), but another tool for configuring and managing a Cisco Nexus 7000 Series Switch is also available. Cisco Data Center Network Manager (DCNM) is a user friendly GUI that offers a single pane for all configuration, monitoring, and troubleshooting tasks on Cisco Nexus 7000 Series Switches and other data center products based on Cisco NX-OS. The Cisco DCNM management tool offers a subset of capabilities for free, but a license is required for the full set of features. For VDCs, Cisco DCNM can provide a quick overview of configured VDCs and ports assigned to them, as shown in Figure 18.

Figure 18. Cisco DCNM VDC Management



Virtual Devices

Name	Type	Status	Resource Limit - Module Type	HA-Policy		MAC Address	Management Interface		SSH
				Single Supervisor	Dual Supervisor		IP Address Prefix	Status	
N7010									
N7010	Ethernet	Active	M1XL, F1, M1	Reload Supervisor	Switchover Supervisor	68BD.ABD7.9C41	11.11.11.125/24	Up	Enabled
Fabric_B	Ethernet	Active	M1XL, F1, M1	Restart VDC	Switchover Supervisor	68BD.ABD7.9C43	11.11.11.127/24	Up	Enabled
Fabric_A	Ethernet	Active	M1XL, F1, M1	Restart VDC	Switchover Supervisor	68BD.ABD7.9C42	11.11.11.126/24	Up	Enabled

General

Switch Name: N7010 Single Supervisor HA-Policy: Restart VDC Status: Active Resource Limit - Module Type M1XL, F1, M1

VDC Name: Fabric_B Dual Supervisor HA-Policy: Switchover Supervisor MAC Address: 68BD.ABD7.9C43

Interfaces

Interface Name	Mode	Admin Status	Operational Status	Shared	Description
Slot: 1					
Ethernet1/9	Trunk	Up	Down	□	
Ethernet1/10	Access	Up	Down	□	
Ethernet1/11	Access	Up	Down	□	
Ethernet1/12	Access	Up	Down	□	
Ethernet1/13	Routed	Up	Up	□	
Ethernet1/14	Access	Up	Down	□	
Ethernet1/15	Trunk	Up	Down	□	
Ethernet1/16	Trunk	Up	Down	□	
Slot: 2					

Conclusion

From the various scenarios explored in this document, it is obvious that VDCs offer a great amount of flexibility, with design options to optimize the use of existing or new data center space. With facility resources quickly becoming limiting factors in overall design scalability, the availability of additional tools to increase utilization, combined with the capability to preserve operations and service delivery organizational structure, is critical. The VDC feature of the Cisco Nexus 7000 Series platform offers these benefits to the network architect and engineer while remaining transparent to operations.

For More Information

- Cisco Nexus 7000 Series VDC feature: http://www.cisco.com/en/US/prod/collateral/switches/ps9441/ps9402/ps9512/White_Paper_Tech_Overview_Virtual_Device_Contexts.html
- Case studies: http://www.cisco.com/en/US/products/ps9402/prod_case_studies_list.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-701112-00 11/12