Virtual Device Context (VDC) Design and Implementation Considerations with Nexus 7000
Ron Fuller– CCIE #5851 (R&S/Storage)
Technical Marketing Engineer, Nexus 7000 rfuller@cisco.com

Follow us on Twitter for real time updates of the event:
@ciscoliveeurope, #CLEUR
Housekeeping

- We value your feedback- don't forget to complete your online session evaluations after each session & the Overall Conference Evaluation which will be available online from Thursday
- Visit the World of Solutions and Meet the Engineer
- Visit the Cisco Store to purchase your recommended readings
- Please switch off your mobile phones
- After the event don’t forget to visit Cisco Live Virtual: www.ciscolivevirtual.com
- Follow us on Twitter for real time updates of the event: @ciscoliveeurope, #CLEUR
Course Objective

- What you will learn…..
- VDC Configuration Guidelines
- Common VDC Use Cases
- How to use VDCs with Advanced Applications
Agenda

- Virtual Device Context (VDC) Overview
  - What are VDCs?
  - VDC Types
  - Resource Allocation
  - Interface Allocation
  - VDC Operation and Management
  - Leading practices

- Consolidation with VDCs
- Segmentation with VDCs
- Advanced Applications and VDCs
- Q&A
Virtual Device Context (VDC) Overview
What are Virtual Device Contexts (VDCs)?

- What is a switch?
  - Control plane
  - Data plane
  - Management plane

- VDCs enable the virtualization of these planes and hardware resources

- Enables collapsing of multiple logical networks into single physical infrastructure

- Helps scale physical resources of device

- Appropriate for typical silo designs such as:
  - Production, Dev, Test
  - Intranet, DMZ, Extranet
  - Organization A, B C
  - Application A, B, C
  - Customer A, B, C

Different network islands virtualized onto common data center networking infrastructure
Virtual Device Contexts (VDCs)

- **VDC—Virtual Device Context**
  - Flexible separation/distribution of **Software Components**
  - Flexible separation/distribution of **Hardware Resources**
  - Securely delineated **Administrative Contexts**

- **VDCs are not…**
  - The ability to run different OS levels on the same box at the same time
  - based on a **hypervisor** model; there is a single ‘infrastructure’ layer that handles h/w programming…

---

### Protocol Stack (IPv4 / IPv6 / L2)

- **VDC A**
  - Layer-2 Protocols: VLAN mgr, UDLD, CDP, 802.1X, LACP
  - Layer-3 Protocols: OSPF, BGP, EIGRP, PIM, GLBP, HSRP, VRRP, SNMP

- **VDC B**
  - Layer-2 Protocols: VLAN mgr, UDLD, CDP, 802.1X, LACP
  - Layer-3 Protocols: OSPF, BGP, EIGRP, PIM, GLBP, HSRP, VRRP, SNMP

- **VDC n**
  - Layer-2 Protocols
  - Layer-3 Protocols
Virtualization Hierarchy
Where are VDCs reside in the "Big Picture"

<table>
<thead>
<tr>
<th>Nexus 7000</th>
<th>VDC1</th>
<th>VDC2</th>
<th>VDC3</th>
<th>VDC4</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>VLAN VLAN VLAN</td>
<td>VLAN VLAN VLAN</td>
<td>VLAN VLAN VLAN</td>
<td>VLAN VLAN VLAN</td>
</tr>
<tr>
<td></td>
<td>VRF VRF VRF</td>
<td>VRF VRF VRF</td>
<td>VRF VRF VRF</td>
<td>VRF VRF VRF</td>
</tr>
</tbody>
</table>
Virtual Device Contexts

VDC Resources

When creating VDCs, certain resources are shared across VDCs while others must be dedicated to a VDC.

- **Global Resources**: Resources that can only be allocated, set, or configured globally for all VDCs from the master VDC are referred to as Global Resources – i.e.: boot image configuration, Ethanalyzer session, CoPP.

- **Dedicated Resources**: Resources that are allocated to a particular VDC are referred to as dedicated resources - examples include Layer 2 and Layer 3 ports, VLANs, IP address space, etc…

- **Shared Resources**: Some resources are shared between VDCs – for example the OOB Ethernet management port.
NX-OS Software Packaging
Licenses Overview

- **Simplified Software Management**
  8 NX-OS enforceable licenses enable full suite of functionalities for any switching deployment

- **Grace Period License**
  120 days of full feature use with ample warning as grace period comes to the end

- **Non-Disruptive Licensing**
  No disruption in service when moving from grace license to purchased licenses

- **Licenses are associated with chassis S/N#**
VDC Certification

- VDC separation is industry certified
- NSS Labs for PCI Compliant Environments
- FIPS 140-2
- Common Criteria Evaluation and Validation Scheme – Certification #10349
Agenda

- Virtual Device Context (VDC) Overview
  - What are VDCs?
  - VDC Details
    - Resource Allocation
    - Interface Allocation
    - VDC Operation and Management
    - Leading practices
- Consolidation with VDCs
- Segmentation with VDCs
- Advanced Applications and VDCs
- Q&A
VDC Details
The Default VDC

- Fully functional VDC with all capabilities
- Some tasks can only be performed in the default VDC
  - VDC creation/deletion/suspend
  - Resource allocation – interfaces, memory
  - NX-OS Upgrade across all VDCs
  - EPLD Upgrade – As directed by TAC or to enable new features
  - Ethanalyzer captures – control plane traffic
  - Feature-set installation for Nexus 2000, FabricPath and FCoE
  - Control Plane Policing (CoPP)
  - Port Channel load balancing
  - Hardware IDS checks control
  - ACL Capture feature enable
- Default VDC can be used for production traffic with no issues
  - Some customers may choose to reserve it for administrative functions
VDC Details
Non-Default VDC

- Fully functional VDC with all capabilities
- Changes in non-default VDC only affect that particular VDC
- Independent processes started for each protocol in each VDC
- Discrete configuration file per VDC
- Discrete checkpoints per VDC
- Discrete RBAC, TACACS, SNMP, etc.
VDC Types
“Module-Type” Modes

In release 5.1, “module-type” parameter defines the behavior for each VDC.

Different I/O module types can be specified:

- m1 – specifies VDC can contain M1 modules
- m1-xl – specifies VDC can contain M1-XL modules
- m2-xl - specifies VDC can contain M2-XL modules
- f1 – specifies VDC can contain F1 modules
- f2 – specifies VDC can contain F2 modules

limit-resource module-type f1 m1 m1-xl m2-xl (default) – Allows mix of M1, M1-XL, M2 and F1 modules in the VDC
VDC Types

F2 VDCs

F2 Modules cannot coexist in the same VDC as other non-F2 modules.

Require the creation of a F2 only VDC using limit-resource module-type f2.

In a new configuration where only F2 modules are present, the system will automatically set the default VDC to F2 mode.*

When F2 is added to an existing configuration, ports are placed in VDC0 to be allocated to F2 VDCs by the admin.

*This check is only done once when no configuration exists.
VDC Types
Examples of Limiting Module Type

Want F1-only VDC
  limit-resource module-type f1
Want F2-only VDC
  limit-resource module-type f2
Want M1/M1-XL-only VDC
  limit-resource module-type m1 m1-xl
Want M1-XL with F1 VDC
  limit-resource module-type m1-xl f1
Want M2-XL-only VDC
  limit-resource module-type m2-xl

• In a VDC in one of these modes, conflicting modules are placed in “suspended” state on OIR

• Power is applied, module is in “ok” status, but interfaces are not available for configuration

• Only VDC allocation is allowed for such interfaces (e.g., to move F1 interfaces from an M1-only VDC to an F1 or mixed-mode VDC)
VDC Types
Storage VDC

- Enables separation of job functions for LAN and SAN Admin
- Creates a “virtual” MDS within the Nexus 7000
  - Participates as a full Fibre Channel Forwarder (FCF) in the network
  - Zoning, FC alias, fcdomains, IVR, Fabric Binding, etc
- FCoE Target Support
- FCoE ISLs to other switches – Nexus 7000, 5000, MDS
- Only one storage VDC per chassis
  - Does not require Advanced License (VDCs)
  - Does count towards total VDC count – 4 per Nexus 7000
Agenda

- Virtual Device Context (VDC) Overview
  - What are VDCs?
  - VDC types
  - Resource Allocation
    - Interface Allocation
    - VDC Operation and Management
    - Leading practices
- Consolidation with VDCs
- Segmentation with VDCs
- Advanced Applications and VDCs
- Q&A
Resource Allocation

- Ability to allocate resources “as needed”
- Different VDCs may have different requirements
- Production vs. Test/Dev
- Multi-tenancy into shared infrastructure
## Resource Allocation
### Dedicated Resources that can be Allocated

Certain resources can be allocated and limited to a given VDC:

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>m4route-mem</td>
<td>Set ipv4 route memory limits</td>
</tr>
<tr>
<td>m6route-mem</td>
<td>Set ipv6 route memory limits</td>
</tr>
<tr>
<td>module-type</td>
<td>Controls which type of modules are allowed in this vdc</td>
</tr>
<tr>
<td>monitor-session</td>
<td>Monitor local/erspan-source session</td>
</tr>
<tr>
<td>monitor-session-erspan-dst</td>
<td>Monitor erspan destination session</td>
</tr>
<tr>
<td>port-channel</td>
<td>Set port-channel limits</td>
</tr>
<tr>
<td>u4route-mem</td>
<td>Set ipv4 route memory limits</td>
</tr>
<tr>
<td>u6route-mem</td>
<td>Set ipv6 route memory limits</td>
</tr>
<tr>
<td>vlan</td>
<td>Set VLAN limits</td>
</tr>
<tr>
<td>vrf</td>
<td>Set vrf resource limits</td>
</tr>
</tbody>
</table>

### How much RAM do I allocate for my routing tables?

- Routing table memory limits are in MB. For an idea of MB to routes you can use the command “show routing ipv4|ipv6 memory estimate routes <1000-1000000> next-hops <1-16>”

- u4route-mem and u6route-mem limits are **only applied after a switchover or reload** – they are not hot updates.
Resource Allocation
Default Resource Allocation

- Default allocations allow for majority of deployment scenarios
- 8MB of memory allows for approx 6000 routes with 16 next hops
- Can be modified by using VDC templates as needed

N7K1-VDC1# show vdc N7K1-VDC2 resource

<table>
<thead>
<tr>
<th>Resource</th>
<th>Min</th>
<th>Max</th>
<th>Used</th>
<th>Unused</th>
<th>Avail</th>
</tr>
</thead>
<tbody>
<tr>
<td>------</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>------</td>
<td>------</td>
</tr>
<tr>
<td>vlan</td>
<td>16</td>
<td>4094</td>
<td>35</td>
<td>0</td>
<td>4059</td>
</tr>
<tr>
<td>monitor-session</td>
<td>0</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>monitor-session-erspan-dst</td>
<td>0</td>
<td>23</td>
<td>0</td>
<td>0</td>
<td>23</td>
</tr>
<tr>
<td>vrf</td>
<td>2</td>
<td>4096</td>
<td>2</td>
<td>0</td>
<td>4086</td>
</tr>
<tr>
<td>port-channel</td>
<td>0</td>
<td>768</td>
<td>0</td>
<td>0</td>
<td>752</td>
</tr>
<tr>
<td>u4route-mem</td>
<td>8</td>
<td>8</td>
<td>1</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>u6route-mem</td>
<td>4</td>
<td>4</td>
<td>1</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>m4route-mem</td>
<td>8</td>
<td>8</td>
<td>1</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>m6route-mem</td>
<td>5</td>
<td>5</td>
<td>1</td>
<td>4</td>
<td>4</td>
</tr>
</tbody>
</table>
Agenda

- Virtual Device Context (VDC) Overview
  - What are VDCs?
  - VDC Types
  - Resource Allocation
  - Interface Allocation
    - VDC Operation and Management
    - Leading practices
- Consolidation with VDCs
- Segmentation with VDCs
- Advanced Applications and VDCs
- Q&A
Ports are assigned on a per VDC basis and cannot be shared across VDCs.

Once a port has been assigned to a VDC, all subsequent configuration is done from within that VDC.

Each port on a N7K-M206QF-23L has its own ASIC.
Interface Allocation
Interface Allocation N7K-M202CF-22L

Ports are assigned on a per VDC basis and cannot be shared across VDCs.

Once a port has been assigned to a VDC, all subsequent configuration is done from within that VDC.

Each port on a N7K-M202CF-22L has its own ASIC.
Interface Allocation
Interface Allocation N7K-M132XP-12 and L

Ports are assigned on a per VDC basis and cannot be shared across VDCs.

Once a port has been assigned to a VDC, all subsequent configuration is done from within that VDC.

N7K-M132XP-12 & L require allocation in port groups of four to align ASIC resources.
Interface Allocation
Interface Allocation N7K-F132XP-15

Ports are assigned on a per VDC basis and cannot be shared across VDCs unless using FCoE.

Once a port has been assigned to a VDC, all subsequent configuration is done from within that VDC.

N7K-F132XP-15 Requires allocation in port groups of two to align ASIC resources.
Interface Allocation
Interface Allocation N7K-F248XP-25

Ports are assigned on a per VDC basis and cannot be shared across VDCs.

Once a port has been assigned to a VDC, all subsequent configuration is done from within that VDC.

N7K-F248XP-25 Requires allocation in port groups of four to align ASIC resources.
Interface Allocation
Interface Allocation N7K-M108X2-12L

Ports are assigned on a per VDC basis and cannot be shared across VDCs.

Once a port has been assigned to a VDC, all subsequent configuration is done from within that VDC.

Each port on a N7K-M108X2-12L has its own ASIC.
Interface Allocation
Interface Allocation 10/100/1000 Modules

Ports are assigned on a per VDC basis and cannot be shared across VDCs. Once a port has been assigned to a VDC, all subsequent configuration is done from within that VDC.

*Note – The M1 48 port line cards have 4 port groups of 12 ports. Recommendation is to have all members of a port group in the same VDC.
Interface Allocation
VDC and Interface Allocation

Ports are allocated in VDC config mode

N7K1-VDC1# configure
Enter configuration commands, one per line. End with CNTL/Z.
N7K1-VDC1(config)# vdc N7K1-VDC2
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

N7K1-VDC1(config-vdc)# allocate interface ethernet 4/1
Entire port-group is not present in the command. Missing ports will be included automatically
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]

Note that FEX ports only exist in the VDC where their parent interfaces reside

Ports being allocated
Disruptive warning!
Easier allocation in NX-OS 5.2
Interface Allocation
Shared Interfaces

- Exception to the rule allowing an interface to exist in only one VDC
- Splits traffic based on Ethertype
- Ethernet VDC “owns” interface
- Storage VDC sees the interface as well

FCoE Initialization Protocol (FIP) Ethertype 0x8914 and FCoE 0x8906 only are directed to the storage VDC. All other Ethertypes are directed toward the Ethernet VDC
Interface Allocation
Requirements for Shared Interfaces

- Interfaces must be on N7K-F132XP-15 modules
- Shared between Default VDC and Storage VDC
- Shared between non-default VDC and Storage VDC
- Ethernet VDC is where interface is allocated
  - Must be configured as a 802.1q trunk in the Ethernet VDC
  - Both ports on the ASIC must be configured for sharing
- Storage VDC is allocated shared interfaces
Interface Allocation
Configuring Shared Interfaces

Interfaces already allocated to N7K1-VDC1

N7K1-VDC1# config
N7K1-VDC1(config)# vdc fcoe

N7K1-VDC1(config-vdc)# allocate fcoe-vlan-range 2000-2100 from vdc N7K1-VDC1
N7K1-VDC1(config-vdc)# allocate shared interface e3/25-26

Ports that share the port group of the interfaces you have specified will be affected as well. Continue (y/n)? [yes] yes

N7K1-VDC1(config-vdc)# end

N7K1-VDC1# switchto vdc fcoe

FCoE# show int brief

<table>
<thead>
<tr>
<th>Interface</th>
<th>Status</th>
<th>Type</th>
<th>Trunk</th>
<th>Speed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eth3/25</td>
<td>up</td>
<td>eth</td>
<td>down</td>
<td>auto</td>
</tr>
<tr>
<td>Eth3/26</td>
<td>up</td>
<td>eth</td>
<td>down</td>
<td>auto</td>
</tr>
</tbody>
</table>

Interfaces can be controlled per VDC
Communicating Between VDCs

- Must use front panel port to communicate between VDCs
  - No soft cross-connect or backplane inter-VDC communications

- Storage shared ports can communicate with each other *within* their respective VDC

- Front panel ports align security models, ensure QoS, ACL, Netflow, etc. resources

- No restrictions on L2/L3 or linecard models

- When using vPC or vPC+ between VDCs, ensure domain IDs are unique
Virtual Device Contexts

VDC Resource Utilization (Layer 2)

Layer 2 learning with multiple active VDCs also has a positive impact on resource utilization - MAC addresses learnt in a VDC are only propagated to other linecards when that linecard has a port in that VDC...

MAC Address A

MAC “A” is propagated to linecard 2 and 3 but only linecard 2 installs MAC due to local port being in VDC 10
Virtual Device Contexts
VDC Resource Utilization (Layer 3)

When only the default VDC is active, the FIB and ACL TCAM on each linecard is primed with forwarding prefixes and policies associated with that default VDC as shown below…
Virtual Device Contexts
VDC Resource Utilization (Layer 3)

FIB and ACL TCAM resources are more effectively utilized…

<table>
<thead>
<tr>
<th>Linecard 1</th>
<th>Linecard 2</th>
<th>Linecard 3</th>
<th>Linecard 4</th>
<th>Linecard 5</th>
<th>Linecard 6</th>
<th>Linecard 7</th>
<th>Linecard 8</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="128K" alt="FIB" /></td>
<td><img src="128K" alt="FIB" /></td>
<td><img src="128K" alt="FIB" /></td>
<td><img src="128K" alt="FIB" /></td>
<td><img src="128K" alt="FIB" /></td>
<td><img src="128K" alt="FIB" /></td>
<td><img src="128K" alt="FIB" /></td>
<td><img src="128K" alt="FIB" /></td>
</tr>
<tr>
<td><img src="64K" alt="TCAM" /></td>
<td><img src="64K" alt="TCAM" /></td>
<td><img src="64K" alt="TCAM" /></td>
<td><img src="64K" alt="TCAM" /></td>
<td><img src="64K" alt="TCAM" /></td>
<td><img src="64K" alt="TCAM" /></td>
<td><img src="64K" alt="TCAM" /></td>
<td><img src="64K" alt="TCAM" /></td>
</tr>
</tbody>
</table>
Control Plane Policing and VDCs

- CoPP works per forwarding engine, as such it is VDC "agnostic"

- If ports for the same forwarding engine are shared between VDCs and CoPP thresholds are violated, CoPP will start dropping matching traffic for all ports of this forwarding engine,

- This behavior might break the separation of VDCs

- If ports of one forwarding engine belong to different VDCs you can limit this effect:

  - The ACL e.g. for ARP and ICMP are use "match protocol" but didn't specify networks.

  - If VDCs using different IP ranges, it is possible to define different CoPP policies based on IP ACLs per protocol
Agenda

- Virtual Device Context (VDC) Overview
  - What are VDCs?
  - VDC Types
  - Resource Allocation
  - Interface Allocation
- VDC Operation and Management
  - Leading practices
- Consolidation with VDCs
- Segmentation with VDCs
- Advanced Applications and VDCs
- Q&A
VDC Types
VDC Creation - Ethernet

N7K1-VDC1# conf t
N7K1-VDC1(config)# vdc N7K1-VDC4
Note: Creating VDC, one moment please ...

N7K1-VDC1(config-vdc)# show vdc

<table>
<thead>
<tr>
<th>vdc_id</th>
<th>vdc_name</th>
<th>state</th>
<th>mac</th>
<th>type</th>
<th>lc</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>N7K1-VDC1</td>
<td>active</td>
<td>00:26:51:c7:34:41</td>
<td>Ethernet</td>
<td>m1 f1 m1xl</td>
</tr>
<tr>
<td>2</td>
<td>N7K1-VDC2</td>
<td>active</td>
<td>00:26:51:c7:34:42</td>
<td>Ethernet</td>
<td>m1 f1 m1xl</td>
</tr>
<tr>
<td>3</td>
<td>N7K1-VDC3</td>
<td>active</td>
<td>00:26:51:c7:34:43</td>
<td>Ethernet</td>
<td>m1 f1 m1xl</td>
</tr>
<tr>
<td>4</td>
<td>N7K1-VDC4</td>
<td>active</td>
<td>00:26:51:c7:34:44</td>
<td>Ethernet</td>
<td>m1 f1 m1xl</td>
</tr>
</tbody>
</table>

N7K1-VDC1(config-vdc)# show vdc N7K1-VDC4 detail

vdc id: 4
vdc name: N7K1-VDC4
vdc state: active
vdc mac address: 00:26:51:c7:34:44
vdc ha policy: RESTART
vdc dual-sup ha policy: SWITCHOVER
vdc boot Order: 1
vdc create time: Mon May 16 00:12:38 2011
vdc reload count: 0
vdc restart count: 0
vdc type: Ethernet
vdc supported linecards: m1 f1 m1xl
VDC Types
VDC Creation – Ethernet – F2 Module

N7K1-VDC1# conf t
N7K1-VDC1(config)# vdc N7K1-VDC4 limit-resource module-type f2
Note: Creating VDC, one moment please ...

N7K1-VDC1(config-vdc)# show vdc

<table>
<thead>
<tr>
<th>vdc_id</th>
<th>vdc_name</th>
<th>state</th>
<th>mac</th>
<th>type</th>
<th>lc</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>N7K1-VDC1</td>
<td>active</td>
<td>00:26:51:c7:34:41</td>
<td>Ethernet</td>
<td>m1 f1 m1xl</td>
</tr>
<tr>
<td>2</td>
<td>N7K1-VDC2</td>
<td>active</td>
<td>00:26:51:c7:34:42</td>
<td>Ethernet</td>
<td>m1 f1 m1xl</td>
</tr>
<tr>
<td>3</td>
<td>N7K1-VDC3</td>
<td>active</td>
<td>00:26:51:c7:34:43</td>
<td>Ethernet</td>
<td>m1 f1 m1xl</td>
</tr>
<tr>
<td>4</td>
<td>N7K1-VDC4</td>
<td>active</td>
<td>00:26:51:c7:34:44</td>
<td>Ethernet</td>
<td>f2</td>
</tr>
</tbody>
</table>

N7K1-VDC1(config-vdc)# show vdc N7K1-VDC4 detail

vdc id: 4
vdc name: N7K1-VDC4
vdc state: active
vdc mac address: 00:26:51:c7:34:44
vdc ha policy: RESTART
vdc dual-sup ha policy: SWITCHOVER
vdc boot Order: 1
vdc create time: Mon May 16 00:12:38 2011
vdc reload count: 0
vdc restart count: 0
vdc type: Ethernet

vdc supported linecards: f2
VDC Types
VDC Creation - Storage

N7K1-VDC1(config)# vdc FCoE type storage
Note: Creating VDC, one moment please ...

N7K1-VDC1(config-vdc)# show vdc

<table>
<thead>
<tr>
<th>vdc_id</th>
<th>vdc_name</th>
<th>state</th>
<th>mac</th>
<th>type</th>
<th>lc</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>N7K1-VDC1</td>
<td>active</td>
<td>00:26:51:c7:34:41</td>
<td>Ethernet</td>
<td>m1 f1 m1xl</td>
</tr>
<tr>
<td>2</td>
<td>N7K1-VDC2</td>
<td>active</td>
<td>00:26:51:c7:34:42</td>
<td>Ethernet</td>
<td>m1 f1 m1xl</td>
</tr>
<tr>
<td>3</td>
<td>N7K1-VDC3</td>
<td>active</td>
<td>00:26:51:c7:34:43</td>
<td>Ethernet</td>
<td>m1 f1 m1xl</td>
</tr>
<tr>
<td>4</td>
<td>FCoE</td>
<td>active</td>
<td>00:26:51:c7:34:44</td>
<td>Storage</td>
<td>f1</td>
</tr>
</tbody>
</table>

N7K1-VDC1(config-vdc)# show vdc FCoE detail

vdc id: 4
vdc name: FCoE
vdc state: active
vdc mac address: 00:26:51:c7:34:44
vdc ha policy: RESTART
vdc dual-sup ha policy: SWITCHOVER
vdc boot Order: 1
vdc create time: Mon May 16 00:28:33 2011
vdc reload count: 0
vdc restart count: 0

vdc type: Storage
vdc supported linecards: f1
Navigating Between VDCs

- From the default VDC, use the switchto vdc <name> command

  N7K1-VDC1# switchto vdc N7K1-VDC2

  N7K1-VDC2#

  N7K1-VDC2# switchback

  N7K1-VDC1#

- To return to the default VDC use the switchback

- Tip – Use the cli alias command

  cli alias name agg1 switchto vdc N7K1-VDC2

  cli alias name agg2 switchto vdc N7K1-VDC3

  cli alias name fcoe switchto vdc FCOE
Reload and Suspend VDCs

- Only non-default VDCs can be suspended, resumed, reloaded or restarted

- Reload is just like reloading a box – clean boot for that VDC
  
  N7K1-VDC1# reload vdc N7K1-VDC4

- Suspend performs config save and graceful cleanup before suspending
  
  N7K1-VDC1# (config-vdc)# vdc N7K1-VDC4 suspend
Nexus 7000 Operational Management

Providing Powerful and Flexible User Control

Role Based Access Control

Framework to create ad hoc roles for any type of user

✓ Very flexible and powerful control over users

✓ Upon login, every user gets assigned a “role” that defines the privileges of the user that gained access to system

✓ The roles are groups of rules that permit or deny a set of operations on NX-OS components
Virtual Device Contexts
VDC Administration

- 4 Named Default Roles
  - network-admin
  - network-operator
  - vdc-admin
  - vdc-operator
- Admin has all rights (read-write)
- Operator has read only rights
- Roles defined for Priv-15 through 0
  - Ease integration into TACACS structure
VDC Leading Practices

- Reserve VDC 1 (default) as the administrative VDC
- On VDC 1, assign accounts with minimum privileges necessary to accomplish operational tasks

- Utilize a linecard per VDC for improved HA and VDC isolation
- Customize VDC HA policy and resource configurations as necessary
  
  Dual-sup default is switchover and single-sup default is restart

- 8GB of RAM may be required depending on number of VDCs and features enabled – Reference URL at the end

Nexus7K(config-vdc)# ha-policy dual-sup <policy> single-sup <policy>
Nexus7K(config-vdc)# limit-resource vlan minimum <#> maximum <#>
Out-of-Band Management Network

Use the management VRF on the Nexus 7000 for all management system connectivity.

Use mgmt0 or Connectivity Management Processor (CMP) ports…or both!

- Mgmt0 IP address for default and non-default VDCs must be from same subnet
- Assign different IP address for redundant CMP (same IP address for redundant mgmt0 interface)
- Doesn’t preclude the use of in-band management (Loopback, VLAN, etc)

Separate physical infrastructure is ideal

Common segment in the box
Managing Virtualization: VDCs and DCNM

- Wizard-based Configuration
  - Interfaces Allocation Across VDC
  - Resource Limit Enforcement with Templates
  - Resource consumption monitoring
  - IPv4 and IPv6 Capable

- VDC aware Fault & Performance Monitoring
- VDC aware RBAC
- Topology Representation
  - VDC per Chassis
  - VDC to VDC Connectivity
Consolidation with VDCs
Hierarchical Network Design

- Offers hierarchy—each layer has specific role
- Modular topology—building blocks
- Easy to grow, understand, and troubleshoot
- Creates small fault domains—clear demarcations and isolation
- Promotes load balancing and redundancy
- Promotes deterministic traffic patterns
- Incorporates balance of both Layer 2 and Layer 3 technology, leveraging the strength of both
- Utilizes Layer 3 routing for load balancing, fast convergence, scalability, and control
Consolidation with VDCs

- Enables consolidation while maintaining hierarchy
- Reduction of physical footprint
  - 4:1 is possible
- Maintains majority of change and failure domain separation
- Provides consistent functionality and features across the network
  - ISSU, QoS, Netflow, etc
Consolidation with VDCs (cont)

- Considerations
  - VDC to forwarding engine mapping
  - Single chassis is still a single point of failure
    - Highly available – yes, but still a single chassis
  - EPLD Upgrade impact on VDCs – multiple modules recommended
  - MAC table sizing bound to “lowest common denominator”
  - Limited number of SPAN sessions
    - ACL Capture can help in many instances
Vertical Consolidation 1

- Consolidation of Core and Aggregation while maintaining network hierarchy
- No reduction in port count or links but fewer physical switches
Vertical Consolidation 2

- Consolidation of Core, Aggregation and Access while maintaining network hierarchy
- Plan accordingly for port/ASIC allocation – might need more cards than you think!
Segmentation with VDCs
Internet Edge/DMZ/Core

- Option to meet multiple needs – XL VDC, DMZ and Core
- Maintains security model with logical separation
MPLS and VDCs

Key considerations

- Secure and flexible way of software process partitioning
- All MPLS features are VDC aware
- Each VDC operates as separate MPLS router (LSR):
  - No internal communication between VDCs
  - Multiple logical P / PE routers can be configured
  - Each VDC has independent label space for prefix labels: LDP, VPN, TE
  - Note: per-VRF VPN labels - globally significant for whole chassis, all others are locally significant to VDC
MPLS and VDCs

Use cases

- Vertical consolidation – collapse layers of P/PE routers

- Horizontal consolidation – collapse PE’s from several PODs
Advanced Applications with VDCs
VDC Functionality with Features

- Using VDCs resolves some hardware restrictions required for features like OTV
- VDCs can provide a migration strategy to new hardware and line cards
- VDCs provide consolidation and separation that makes storage administrators comfortable – virtual MDS
- VDC allows us to do things that allow us to solve layer 8-10 issues 😊
Overlay Transport Virtualization (OTV)
Overlay Transport Virtualization

OTV is a “MAC in IP” technique to extend Layer 2 domains OVER ANY TRANSPORT

Nexus 7000
First platform to support OTV!
OTV at the Aggregation Layer

OTV Design Options

- No universal response where to place the OTV Edge Device
- Main Options:
  - OTV at the Core Layer
  - OTV at the Aggregation Layer (most common – discussed in this presentation)
OTV and SVI Separation

- **Guideline:** The current OTV implementation on the Nexus 7000 requires the separation between SVI routing and OTV encapsulation for a given VLAN.

- This separation can be achieved with having two separate devices to perform these two functions.

- An alternative, **cleaner and less intrusive** solution is the use of **Virtual Device Contexts (VDCs)** available with Nexus 7000 platform:
  - A dedicated OTV VDC to perform the OTV functionalities
  - The Aggregation-VDC used to provide SVI routing support.
OTV and SVI Separation
VDC Models

- Two different deployment models:
  - **OTV Appliance on a Stick**
  - **Inline OTV Appliance**

- Common Uplinks for Layer3 and DCI

- OTV Appliance on a Stick
  - OTV VDC
  - SVIs
  - L3
  - L2

- Join Interface
- Internal Interface

- No difference in OTV functionality between the two models
- The Inline OTV Appliance requires availability of Core downstream links

- Dedicated Uplink for DCI
- Uplinks to the Layer3 Transport

- Inline OTV Appliance
  - OTV VDC
  - SVIs
  - L3
  - L2
OTV at the Aggregation Layer

- DC Core performs only Layer 3 role
- STP and unknown unicast domains isolated between PODs
- Intra-DC and inter-DC LAN extension provided by OTV
- Ideal for single aggregation block topology

Recommended for Greenfield
OTV at the Aggregation Layer
OTV at the Aggregation Layer
OTV at the Aggregation Layer

- The Firewalls host the Default Gateway
- No SVIs at the Aggregation Layer
- No Need for the OTV VDC
Fibre Channel over Ethernet (FCoE)
### Fibre Channel over Ethernet (FCoE)

**FCoE**
- Mapping of FC frames over Ethernet
- Enables FC to run on a lossless Ethernet

**Benefits**
- Wire Server Once
- Fewer cables and adapters
- Software Provisioning of I/O
- Interoperates with existing SANs
- No gateway—stateless
- Standard – June 3, 2009
Traditional Data Center Design

Ethernet LAN and Fibre Channel SAN

- Physical and Logical separation of LAN and SAN traffic
- Additional Physical and Logical separation of SAN fabrics
- Purposely Built Networks
  - LAN: Loss and Out of Order Tolerant
  - SAN: Loss and Out of Order Intolerant
- Limited in Scale
Converged Access

- Shared Physical, Separate Logical LAN and SAN traffic at Access Layer
- Physical and Logical separation of LAN and SAN traffic at Aggregation Layer
- Additional Physical and Logical separation of SAN fabrics
- Storage VDC *(Nexus7000 only)* for additional management / operation separation
- Higher I/O, HA, fast re-convergence for host LAN traffic
- **Edge-Core** Topology
- Use where Core switch is required to provide Storage services to many Edge devices
Converged Network Fabrics w/ Dedicated Links

- LAN and SAN traffic share physical switches and traffic uses dedicated links between switches.
- All Access and Aggregation switches are FCoE FCF switches.
- Storage VDC (Nexus7000 only) for additional operation separation at high function Aggregation/Core.
- Improved HA, load sharing and scale for LAN vs. traditional STP topologies.
- SAN can utilize higher performance, higher density, lower cost Ethernet switches for the aggregation/core.
- **Edge-Core-Edge** Topology connectivity to existing SAN.
- Use where future growth has number of Storage devices **exceeding** ports in the Core.
Converged Network Fabrics with Dedicated Links

- LAN and SAN traffic share physical switches and traffic use dedicated links between switches
- All Access and Aggregation switches are FCoE FCF switches
- Storage VDC (*Nexus7000 only*) for additional operational separation at high function Aggregation/Core
- Improved HA, load sharing and scale for LAN vs. traditional STP topologies
- SAN can utilize higher performance, higher density, lower cost Ethernet switches for the Edge, Aggregation/Core
- Standardize on platform, OS and I/O
- **Edge-Core-Edge** Topology with scalable and dense Ethernet switches at the Edge
- FC connectivity only available on Nexus 5000
Data Center Design with E-SAN

- Same topologies as existing networks, but using Nexus Unified Fabric Ethernet switches for SANs
- Physical and Logical separation of LAN and SAN traffic
- Additional Physical and Logical separation of SAN fabrics
- Ethernet SAN Fabric carries FC/FCoE & IP based storage (iSCSI, NAS, …)
- Common components: Ethernet Capacity and Cost
- Standardize on OS, I/O and Platform
- Storage administrators in Large Data Centers almost always prefer this model (distinct storage management plane)
Converged Network with Dedicated Links

- FabricPath enabled for LAN traffic
- Dual Switch core for SAN A & SAN B
- All Access and Aggregation switches are FCoE FCF switches
- Dedicated links between switches are VE Ports
- Storage VDC (Nexus 7000 only) for additional operation separation at high function agg/core
- Improved HA and scale over vPC (ISIS, RPF, … and N+1 redundancy)
- SAN can utilize higher performance, higher density, lower cost Ethernet switches
- FC connectivity only available on Nexus 5000
Introducing Cisco FabricPath
An NX-OS Innovation for Layer 2 Networks

Layer 2 strengths
- Simple configuration
- Flexible provisioning
- Low cost

Layer 3 strengths
- Leverage bandwidth
- Fast convergence
- Highly scalable

Fabric Path

Simplicity
Flexibility
Bandwidth
Availability
Cost
Architecture Flexibility Through NX-OS

- **Spanning-Tree**
  - Single
  - Up to 10 Tbps

- **vPC**
  - Dual
  - Up to 20 Tbps

- **FabricPath**
  - 16 Way
  - Up to 160 Tbps

Layer 2 Scalability

Infrastructure Virtualization and Capacity
Cisco FabricPath

- Eliminates Spanning Tree related limitations
- Multi-pathing across all links, high cross-sectional bandwidth
- High resiliency, faster network reconvergence
- Any VLAN anywhere in the fabric eliminates VLAN scoping

Traditional Spanning Tree Based Network
- Blocked Links

Cisco FabricPath Network
- All Links Active

160+ Tbps switching capacity
Parallel FabricPath Core

- **Motivations:** Consolidation and whole-network scale
- **Removes access connections and aggregation mesh limitations**

- **Meshed agg model overly complex after a certain point**
- **Add FabricPath core parallel to L3 core to interconnect FabricPath Pods**

![Diagram showing L3, FabricPath, VPC+, and VPC connections](image-url)
Parallel FabricPath Core with VDCs

- Exact same model as prior slide but with VDCs instead of separate physical switches
- Note – VDCs not required for FabricPath
Summary

- VDCs Unlock the full potential of Nexus 7000
- VDCs can be used for many uses
  - Consolidation – vertical and horizontal
  - Security and segmentations
  - Advanced applications
    - Overlay Transport Virtualization (OTV)
    - Fibre Channel over Ethernet (FCoE)
    - FabricPath
Course Objective

- What we learned…
- VDC Configuration Guidelines
- Common VDC Use Cases
- How to use VDCs with Advanced Applications
Additional References

- **VDC White Paper on CCO**
  

- **8GB RAM Flowchart**
  

- **Common Criteria Certification #10349**
  
  - http://www.niap-ccevs.org/st/vid10349/

- **FIPS 140-2**
  

- **NSS Labs**
  
  http://www.nsslabs.com/

- **Follow us on Twitter**
  
  @CiscoNexus7000
Recommended Reading

NX-OS and Cisco Nexus Switching
Next-Generation Data Center Architectures

The complete guide to planning, configuring, managing, and troubleshooting NX-OS in enterprise environments

Kevin Corbin, CCIE® No. 11577
Ron Fuller, CCIE No. 5851
David Jansen, CCIE No. 5952
Please complete your Session Survey

We value your feedback

- Don't forget to complete your online session evaluations after each session. Complete 4 session evaluations & the Overall Conference Evaluation (available from Thursday) to receive your Cisco Live T-shirt.

- Surveys can be found on the Attendee Website at www.ciscolivelondon.com/onsite which can also be accessed through the screens at the Communication Stations.

- Or use the Cisco Live Mobile App to complete the surveys from your phone, download the app at www.ciscolivelondon.com/connect/mobile/app.html

1. Scan the QR code
   (Go to http://tinyurl.com/qrmelist for QR code reader software, alternatively type in the access URL above)

2. Download the app or access the mobile site

3. Log in to complete and submit the evaluations

http://m.cisco.com/mat/cleu12/
Thank you.