Service Oriented Virtual DC Design

Višnja Milovanović
Consulting Systems Engineer
Data Center & Virtualization
Setting the Stage: What’s the Meaning of Virtual?

If you can see it and it is there
It’s **real**

If you can’t see it but it is there
It’s **transparent**

If you can see it and it is not there
It’s **virtual**

If you can not see it and it is not there
It’s **gone**
Setting the Stage: Delivering a Service
(With End-to-End Automation)

Before
- Machine-oriented
- Manual provisioning
- Hard to control utilization
- High provisioning & ops cost
- Extended provisioning time
- Configuration risk

After
- Service-oriented
- Self-service; automated provisioning
- Elasticity (capacity-on-demand)
- Optimized provisioning & ops cost
- Rapid provisioning
- Increased Resiliency and Availability
Use Case: Acquisition of New Sales Force, Consolidation and Rapid Provisioning via Templates

Create 500 Virtual Desktops to Enable New Team to Access Corporate Information and Applications

Increase Database Capacity to Support Sales Consolidation Effort

Create 500 New Mailboxes
**Agenda**

**Data Center Virtualization Overview**
- Front-End Data Center Virtualization
  - Core Layer
  - Aggregation Layer
  - Networking Services
  - Access Layer
- Server Virtualization
  - Unified Computing System
  - Virtual Access Layer
  - Virtualized Services
  - Server IO Virtualization
- Back-End Virtualization
  - Unified Fabric & FCoE
  - SAN & Storage

**Q&A**
Virtualized Network Infrastructure: Evolution and Considerations

**Typical DC Challenges**
- L2 Fate-sharing
- VLAN Location
- L2 Adjacency
- Higher Scale
- L3 Access
- App Environments

**What are the implications...**
- Dynamic “routing protocol” for L2 (e.g.: IS-IS)
- Any VLAN anywhere resonates well
- Lower oversubscription
- Larger subnet sizes
- Global VLANs
- Specific app environments Designs

---

**Density & quantity of aggregation switches**

**Density and Capabilities of access switch**

**Access Ports in management domain**

**Modern Pod**
Virtualized Data Center Infrastructure
(2 Layers)

OTV: Layer 2 Extension

Leaf Layer

Spine Layer

Unified Fabric: Multi-Hop FCoE + Unified Ports
Virtualized Servers + VM Mobility
Virtualized Services

1/10GE
FC
Converged FCoE link
Dedicated FCoE link
Virtualized Data Center Infrastructure
Maintaining Dual SAN Fabrics with Layer2 Multipath (Fabric Path)

FabricPath enabled for LAN traffic

Dual Switch core for SAN A & SAN B

All Access and Aggregation switches are FCoE FCF switches

Dedicated FCoE links between switches are VE_Ports

Storage VDC (Nexus 7000 only) for additional operation separation at high function agg/core (aka spine)

- SAN can utilize higher performance, higher density, lower cost Ethernet switches (F2 module on Nexus 7000 and unified ports on Nexus 5500)
- (*) FC connectivity to storage only available on Nexus 5000/5500. FCoE target and NAS / iSCSI target connectivity to any Nexus switch.
Virtualized Data Center Infrastructure
Virtualized Data Center Switch — 1 Layer?

Nexus 5500 with L3 module and vPC+

Nexus 2200

ASA 5500

ACE 4710

Nexus 5500 with L3 module and vPC+

Nexus 5500 with L3 module and vPC+

Nexus 5500 with L3 module and vPC+

ASA 5500

ACE 4710

Nexus 2200

DC @ SMB Customer

Co-Lo @ Stock Exchange
Agenda

Data Center Virtualization Overview

Front-End Data Center Virtualization
- Core Layer
- Aggregation Layer
- Networking Services
- Access Layer

Server Virtualization
- Unified Computing System
- Virtual Access Layer
- Virtualized Services
- Server IO Virtualization

Back-End Virtualization
- Unified Fabric & FCoE
- SAN & Storage

Q&A
Virtual Device Contexts (VDC)
Separate Resource Allocation Domains (Layer 3)

Linecard 1 (M1)
- FIB TCAM Size: 128K - 1M
- ACL TCAM Size: 64K - 128K

VDC-2
- IP routes: 100K
- ACL entries: 50K

VDC-1
- IP routes: 20K
- ACL entries: 10K

Linecard 2 (M1)
- FIB TCAM Size: 128K – 1M
- ACL TCAM Size: 64K - 128K

Linecard 4 (F2)
- FIB TCAM Size: 32K
- ACL TCAM Size: 16K - 192K

VDC-3
- Storage VDC
  E.g.: FCoE on F1 linecard(s)

Linecard 3 (F1)
- FIB TCAM Size: 1K - 16K
- ACL TCAM Size: 1K - 16K

VDC-4
- F2 linecard(s)
  (from M1-F1 combination)
Front-End: Aggregation Layer

1 GbE Server Access & 4/8Gb FC via dual HBA (SAN A // SAN B)

10Gb DCB / FCoE Server Access or 10 GbE Server Access & 4/8Gb FC via dual HBA (SAN A // SAN B)
vPC is a Port-channeling concept extending link aggregation to two separate physical switches
Allows the creation of resilient L2 topologies based on Link Aggregation.
Eliminates the need for STP in the access-distribution Layer

Enable seamless VM Mobility, Server HA Clusters
Scale Available Layer 2 Bandwidth
Dual-homed server operate in active-active mode
Simplify Network Design
Available on Nexus 7000 and Nexus 5000 / 5500
Logical View with FabricPath:
Distributed Topology without L2 loops

Virtual Access Switch POD
(Nexus 7000 / 5x00 + Nexus 2200)

FabricPath

S10 S20 S30 S40

vPC+ allows dual-homed connections from edge ports into FabricPath domain with active/active forwarding. E.g.: Classical Ethernet switch, Layer 3 router, dual-homed server, etc.

Unified Computing System (UCS)

Virtual Blade Switching (VBS)

Server
Front-End: Networking Services

1 GbE Server Access & 4/8Gb FC via dual HBA (SAN A // SAN B)

10Gb DCB / FCoE Server Access or 10 GbE Server Access & 4/8Gb FC via dual HBA (SAN A // SAN B)
Data Center Virtualized Services
Physical Appliances/Modules Context Combination Example

“Front-End” VRFs (MSFC)

Firewall Module Contexts

ACE Module Contexts

“Back-End” VRFs (MSFC)

Server Side VLANs

* vX = VLAN X
** BU = Business Unit
### VMDC Sample Containers

**Flexible framework allows variations as need be**

<table>
<thead>
<tr>
<th>Bronze</th>
<th>Silver</th>
<th>Gold</th>
<th>Palladium</th>
<th>Expanded</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="bronze.png" alt="Diagram" /></td>
<td><img src="silver.png" alt="Diagram" /></td>
<td><img src="gold.png" alt="Diagram" /></td>
<td><img src="palladium.png" alt="Diagram" /></td>
<td><img src="expanded.png" alt="Diagram" /></td>
</tr>
</tbody>
</table>

- Predefined containers provide examples for different types of deployments
- Automated provisioning and management logic for each container type is predefined in the Management and Orchestration software
- Customers can choose from existing models or define their own customized models

© 2013 Cisco and/or its affiliates. All rights reserved.
Business Continuance and Disaster Recovery?

Benefits

- Workload balancing across data centers and clouds
- Proactive response to disruptions – mitigates risks of Approaching disasters, viz. hurricanes, floods, etc., Power grid maintenance, Data center maintenance and migrations
- Planned events scheduled over a period of time
- Backup and Disaster Recovery aaS

The Solution:

- VMotion enabled over Cisco DCI solution

- Cisco Data Center Interconnect (DCI) Solution based on OTV, VPLS, EoMPLS, LISP
- NetApp’s FlexCache-enabled Intelligent Storage Arrays
- EMC’s VPLEX + Avamar
- VMware vSphere & VMotion Technologies

© 2013 Cisco and/or its affiliates. All rights reserved.
Cisco FEXlink: Virtualized Access Switch
Nexus 2200 Fabric Extender (FEX)

Cisco Nexus® 5500 + Cisco Nexus® 2000 FEX

Distributed High Density Edge Switching System (up to 4096 virtual Ethernet interfaces)

Cisco Nexus® 7000 + Cisco Nexus® 2000 FEX

Cisco Nexus® 2000 FEX
To2R: Nexus 2200 Deployment Example

- **Access Layer**
  - Nexus 2200
  - Nexus 5500

- **Aggregation Layer**
  - Nexus 7000
  - Nexus 7000
  - vPC
IEEE 802.1BR: Bridge Port Extension

Fully specifies a Port Extender (FEX Equivalent)
- Extends ports of a switch to lower entities in a network

Port Extenders are not individually managed
- Their ports become ports of the controlling switch

Cascading Port Extenders
- Allows one to choose the appropriate controlling switch
- Frame replication supported for efficient multicast / flooding

Traffic from each “Extended Port” is reliably segregated to an E-channel and identified by a tag containing an E-channel identifier (ECID)
- Does not require prior knowledge of MAC addresses; switch performs standard learning functions
- Works with all devices including VEBs, VEPAs, individual VMs, physical services, and devices providing transparent services

Controlling Bridge + PE = Extended Bridge
- Single Point of Management
IEEE Bridge Port Extender = Cisco FEX (Fabric Extender)
UCS 1280 Virtual Interface Card (VIC)

Customer benefits
- Dual 4x 10 GE (80 Gb per host)
- VM-FEX scale, up to 112 VM interfaces /w ESX 5.0

Feature details
- Dual 4x 10 GE port-channels to a single server slot
- Host connectivity PCIe Gen2 x16
- PCIe Gen 2 x16 bandwidth limit is 32 Gbps
- HW Capable of 256 PCIe devices
  - OS restriction apply
- PCIe virtualization OS independent (same as M81KR)
- Single OS driver image for both M81KR and 1280 VIC
- FabricFailover supported
- Eth hash inputs: Source MAC Address, Destination MAC Address, Source Port, Destination Port, Source IP address, Destination IP address, and VLAN
- FC Hash inputs: Source MAC Address, Destination MAC Address, FC SID and FC DID
Agenda

Data Center Virtualization Overview
Front-End Data Center Virtualization
  Core Layer
  Aggregation Layer
  Networking Services
  Access Layer
Server Virtualization
  Unified Computing System
  Virtual Access Layer
  Virtualized Services
  Server IO Virtualization
Back-End Virtualization
  Unified Fabric & FCoE
  SAN & Storage
Q&A
Front-End: Servers Layer

Servers Layer

1 GbE Server Access & 4/8Gb FC via dual HBA (SAN A // SAN B)
10Gb DCB / FCoE Server Access, or 10 GbE Server Access & 4/8Gb FC via dual HBA (SAN A // SAN B)
Cisco Unified Computing System (UCS)

Form Factor Independence

LAN
Any IEEE Compliant LAN

SAN A
Any ANSI T11 Compliant SAN

SAN B
ANSI T11 Compliant SAN

One Logical Chassis to Manage*

LAN Connectivity
SAN Networking
Blade Chassis’
Server Blades
Rack Servers
Server Identity Management
Monitoring, Troubleshooting
etc.

*architectural limit of 320 servers with 160 servers supported as of UCS release 2.0
Network Has Complete Visibility to Servers

UCS Service Profiles Capture more than MAC & WWN
MAC, WWN, Boot Order, Firmware, network & storage policy

Stateless compute where network & storage see all movement
Better diagnostics and QoS from network to blade, policy follows

Service Profiles deliver Service Agility regardless of Physical or Virtual Machine

Server Name: SP-A
UUID: 56 4d cd 3f 5b 61
MAC: 08:00:69:02:01:FC
WWN: 5080020000075740
Boot Order: SAN, LAN
Stateless Computing @ UCS

Old Deployment:
- Web Servers
  - Blade
- Oracle RAC
  - Blade
  - Blade
  - Blade
  - Blade
  - Blade
  - Blade
- VMware
  - Blade
  - Blade
  - Blade
  - Blade
  - Blade
  - Blade

Total Server Deployment
14 Servers
Reduction of 4 Servers
22% CapEx Savings

Cisco UCS Deployment: (still 18 Service Profiles)
- Web Servers
  - Blade
  - Blade
  - Blade
  - Blade
  - Blade
  - Blade
  - Blade
- Oracle RAC
  - Blade
  - Blade
  - Blade
  - Blade
  - Blade
  - Blade
- VMware
  - Blade
  - Blade
  - Blade
  - Blade
- Burst Capacity
  - Blade
  - Blade
- HA Spare
  - Blade

Cisco’s Deployment:
- Resources provisioned based on business need
- Still HA with fewer spares
Cisco VN-Link

What is that and which problems does it solve?

“Layer 9” issue 😞 !

- VN-Link (or Virtual Network Link) is a term that refers to a VM specific link that is created between the VM and Cisco switch.
  - Logical equivalent & combination of a NIC, a Cisco switch interface and the RJ-45 patch cable that hooks them together.
Virtual Access Layer @ Virtualized Servers

Nexus 1000v

Virtual Access Layer

Layer 3
Layer 2 - 1GE
Layer 2 - 10GE
10 GE DCB
10 GE FCoE/DCB
4/8 Gb FC

Nexus 7000
10 GE Core

Nexus 7000
10 GE Aggr

Network Services

L3
L2

MDS 9500
SAN Director

MDS 9200
SAN Director
Port Profiles “How to”

Nexus 1000V automatically enables port groups in vCenter via API
Server Admin uses vCenter to assign vnic policy from available port groups
Nexus 1000V automatically enables VM connectivity at VM power-on

“WEB Apps” Port Profile:
- PVLAN 108, Isolated
- Security Policy = Port 80 and 443
- Rate Limit = 100 Mbps
- QoS Priority = Medium
- Remote Port Mirror = Yes
Cisco Nexus 1000v multi-hypervisor support

Consistent architecture, feature-set & network services ensures operational transparency across multiple hypervisors.
Cisco Virtual Networking and Cloud Network Services

Cloud Network Services

Virtualized/Cloud Data Center

WAN Router

Switches

Servers

Physical Infrastructure

VSG

• VM-level controls
• Zone-based FW

Nexus 1000V

• Distributed switch
• NX-OS consistency

ASV 1000V

• Edge firewall, VPN
• Protocol Inspection

vWAAS

• WAN optimization
• Application traffic

CSR 1000V (Cloud Router)

• WAN L3 gateway
• Routing and VPN

Ecosystem Services

• Citrix NetScaler VPX virtual ADC
• Imperva Web App. Firewall

6000+ Customers

Shipping

Shipping

Shipping

6000+ Customers

Shipping

Shipping

6000+ Customers

Shipping

Shipping

6000+ Customers

Shipping

Shipping

6000+ Customers

Shipping

Shipping

6000+ Customers

Shipping

Shipping

6000+ Customers

Shipping

Shipping
Securing Tenant Edge with ASA 1000V

- Proven Cisco Security…Virtualized Physical – virtual consistency
- Collaborative Security Model VSG for intra-tenant secure zones Virtual ASA for tenant edge controls
- Seamless Integration With Nexus 1000V & vPath
- Scales with Cloud Demand Multi-instance deployment for horizontal scale-out deployment
Cisco Nexus 1000v InterCloud

Enterprise DC
- Physical Services
- Virtual Services
- Nexus HW Switches
- Cloud Manager
- ASR 1K/9K

Public Cloud
- Virtual Services
- vPath
- L2-VPC
- Cloud Service Router
- Secure L2 Extension (Cloud GW)

Enterprise Campus
- Remote Access

Enterprise Branch
- ISR

Kumo Benefits:
Security * Consistency * Control

Cisco Nexus 1000v InterCloud Solutions
Agenda

Data Center Virtualization Overview

Front-End Data Center Virtualization
- Core Layer
- Aggregation Layer
- Networking Services
- Access Layer

Server Virtualization
- Unified Computing System
- Virtual Access Layer
- Virtualized Services
- Server IO Virtualization

Back-End Virtualization
- Unified Fabric & FCoE
- SAN & Storage

Q&A
Unified Fabric Flexibility and Serialized Re-Use

- Ability to re-provision any compute unit to leverage any access method to the data stored on the ‘spindle’
- Serialized Re-Use – Boot from SAN and Run from NAS
- Virtualization requires that the Storage Fabric needs to exist everywhere the IP fabric does
Unified I/O Architecture Consolidation

Initial Goal

No Consolidated IO

I/O Consolidation with FCoE

- Ethernet
- FC
- FCoE

LAN
SAN A
SAN B
Nexus 5000
Example: Embedded FCoE at Cisco UCS

From ad hoc and inconsistent...

...to structured, but siloed, complicated and costly...

...to simple, optimized and automated
Thank you.