End-to-End Virtualization and Management

Sid Nag
Global Enterprise Architect
Agenda

- Virtualization—Introduction
- OS Virtualization
- Server Virtualization
- Storage Virtualization
- Network Virtualization
- End-to-End (E2E) Virtualization
- Virtualization and Environment
- Conclusion
Virtualization—Introduction
Virtualization—Introduction

- Virtualization allows entities to share physical resources in an effective way
  - Virtual Machines (VM) sharing computer hardware (HW) resources
  - VLANs/VSANs sharing a physical port
  - VPNs sharing a physical network
Virtualization—Introduction

- Virtualization isolates entities from each other
  - A VM isolated from others from crash/security threat
  - VLAN/VSAN/VPN traffic isolated from each other
- Virtualization isolates layer N (upper layer) from layer N-1 (lower layer)
  - Layer N unaffected when Layer N-1 replaced or modified
  - ISO/OSI Layering
  - Virtualization and abstraction can be synonymous
    → Virtualization requires abstraction
- Virtualization hides details of virtualized resources
Virtualization Motivation—Today’s Data Center

- Server Sprawl
- Single application per server
- Longer deployment time
- Management complexity
- Power, cooling, weight significant factor
- Longer maintenance window

- High OPEX: Complexity and Overhead caused by redundant DC Components
- High CapEX: Resources are only 20% utilized

Source: Gartner

<table>
<thead>
<tr>
<th>Industry</th>
<th>Cost of Downtime/hr</th>
</tr>
</thead>
<tbody>
<tr>
<td>Travel Industry</td>
<td>330,654</td>
</tr>
<tr>
<td>Media Industry</td>
<td>340,432</td>
</tr>
<tr>
<td>Professional Services</td>
<td>532,510</td>
</tr>
<tr>
<td>Health Care Industries</td>
<td>636,030</td>
</tr>
<tr>
<td>Transportation</td>
<td>668,856</td>
</tr>
<tr>
<td>Consumer Products</td>
<td>785,719</td>
</tr>
<tr>
<td>Banking</td>
<td>996,802</td>
</tr>
<tr>
<td>Pharmaceuticals</td>
<td>1,082,252</td>
</tr>
<tr>
<td>Retail</td>
<td>1,107,274</td>
</tr>
<tr>
<td>Insurance</td>
<td>1,202,444</td>
</tr>
<tr>
<td>Financial Institutions</td>
<td>1,495,134</td>
</tr>
<tr>
<td>Manufacturing</td>
<td>1,610,654</td>
</tr>
<tr>
<td>Telecom</td>
<td>2,066,245</td>
</tr>
<tr>
<td>Energy</td>
<td>2,817,846</td>
</tr>
</tbody>
</table>

Source: Meta group: IT Performance Engineering and measurement strategies: quantifying performance loss, 10/2000
Virtualization—Benefits

- Physical resource sharing
- HW resource consolidation
- IT optimization
- Management simplified
- Lower CAPEX and OPEX cost
- Downtime on the order of few milliseconds to few minutes (not hours or days)

- 10 2P Xeon servers to 2 4P Xeon servers
  
  Hardware savings = $38k
  Operational Savings = $76k

Source: VMWare
Virtualization—The “Virtual” Part! 😊

- How about virtualizing regular and decaf? 😊
OS Virtualization
Agenda

- OS Virtualization
- Benefits of OS Virtualization
- OS Virtualization Types
  - Native/Full Virtualization
  - Para Virtualization
  - Container/OS-based Virtualization
  - Host-based Virtualization
- OS Virtualization Performance Issues
- OS Virtualization in x86 Hardware (HW)
OS Virtualization—Introduction

- Virtualization applied to computer and OS domains
- A typical OS virtualizes computer hardware components to certain extent
  - Virtual CPU: Processes time-sharing a CPU
  - Virtual Memory: Processes having its own memory span independent from physical memory
- OS Virtualization goes further allowing multiple OSs and their applications run on a single physical hardware
  - OS is now a Guest OS
  - OS+Applications: Virtual Machine (VM)
- A Hypervisor or Virtual Machine Monitor (VMM) controls the hardware resources
  - Guest OS no longer has full control over HW
OS Virtualization—Benefits

- HW resource consolidation
- Physical resource sharing
- Given that average server utilization is ~20%, OS Virtualization can be a viable solution for consolidation and IT/DC optimization
OS Virtualization—Benefits

- Migration to new software
  - Keep old version and access to it
  - Certain applications with new OS may not be available yet
OS Virtualization—Benefits

- Live migration from machine to machine while VM is running
  - Downtime on the order of few milliseconds to few minutes, not hours or days
- Load-balancing
- Maintenance without application shutdown
- High-availability
Virtual Machine Monitor (VMM) or Hypervisor

- The main component of OS virtualization is a VMM or Hypervisor
- A thin layer of software controlling and managing bare hardware resources
- Facilitates virtualization of HW resources
- Arbitrates guest OS access to HW
- Manages VMs (create, Destroy, etc.)
OS Virtualization Types—Native/Full

- VMM runs on bare machine
- VMM virtualizes (emulates) hardware
  Virtualizes x86 ISA (Instruction Set Architecture)
- Guest OS unmodified
- VMs: Guest OS+Applications run under the control of VMM
- Systems
  - VMware ESX Server
  - IBM z/VM
  - Linux KVM (Kernel VM)
OS Virtualization Types—Container-Based

- VMM inside a Host OS (Kernel)
- VMs (also known as Virtual Private Server) fully isolated
- Host OS modified to isolate different VMs
  
  Example: Kernel data structure changed to add context ID to differentiate between identical uids between different VMs
  
  Thus VMs isolated from each other in kernel

- No Guest OS
- Fault isolation not possible (OS crash)
- Applications/users see container VM as a virtual host/server
- VMs can be booted/shut down like regular OS
- Systems
  
  Linux VServer
OS Virtualization Types—Host-Based

- Like Native, but based on a Host OS
- VMM inside a Host OS
  - Kernel-mode driver
- Multiple Guest OS support
- VMM emulates hardware for guest OSs
- Systems
  - Microsoft Virtual Server
    - Host OS: XP, 2003
    - Guest OS: NT, 2000, 2003, Linux
OS Virtualization Types—Para-Virtualization

- VMM runs on bare machines
- Guest OS modified to make calls (hypercall) to or receive events from VMM
  - Example, OS hypercalls into VMM when it updates hardware data structures like page table or initiates a DMA operation
- Support of arbitrary guest OS not possible because of OS modification
  - Unmodified guest OS can be supported with Virtualization support in hardware architecture (Intel VT-x, AMD Pacifica)
- Few thousand lines of code change (relative to 6 million lines in Linux)
- Application Binary Interface (ABI) remains intact, hence application binaries run unmodified within VM
- Open-source OS modification easy
- Systems
  - Xen
    - Guest OS: XenoLinux, NetBSD, FreeBSD, Solaris 10, Windows (in progress)
VM Migration Example

- Shows live migration of a Web Server VM with only 201ms of downtime
  While the server was being migrated to another machine, it was still processing requests

  SPECweb99 is the SPEC benchmark for evaluating the performance of WWW Servers

  The Standard Performance Evaluation Corporation (SPEC) is a non-profit corporation formed to establish, maintain and endorse a standardized set of relevant benchmarks that can be applied to the newest generation of high-performance computers

- Source and destination machines have to be compatible
Performance issues

Network Intensive Applications: Send/Receive over TCP connections

- HW: IBM x3550 server with two VT-enabled dual-core 2GHz Intel Xeon 5130 CPUs for a total of four CPU cores
- Storage: 2 73GB SAS disk drives; NIC: 1 Gbps; Two clients (Dell 1950) running Windows 2003 R2
- Clients connect to server with LinkSys SR2016 GE switch
- XenEnterprise with Xen HVM support (HVM supports Intel VT and AMD-v)

Source: XenSource
OS Virtualization—Conclusion

- May have to pay performance penalties depending on Application types
  - CPU bound
  - Memory bound
  - IO bound
- HW support may reduce penalties, but penalties will remain
  - Multiple levels of indirections, traps, context switches
- HW support will not eliminate VMM
  - VMM needed for controlling multiple VMs
- New VM management support needed
  - VM resource allocation, sizing
  - VM migration management
  - VM and VMM performance monitoring
  - VM management integrated with Server and Network Management in DC
Server Virtualization
Server Virtualization—Introduction

- Application Servers not tied to a hardware
- Servers for applications allocated from available server pool
- Facilitated by OS Virtualization
- Facilitated by Grid Technology
- Server virtualization may depend on OS virtualization, but not necessarily
- OS Virtualization scope is a single server HW or a few of them in case of VM migration
- Server virtualization scope can be whole IT/DC distributed over LAN/MAN/WAN
Virtualizing Server Resources

- Detach Application Servers from server Hardware

  - Mail Server
    - Windows
    - Hardware
    - Av. load 20%
  - Web Server
    - Linux 2.4
    - Hardware
    - Av. load 40%
  - DB Server
    - Linux 2.6
    - Hardware
    - Av. load 10%

  3 Hardware: Same class & Spec

- Virtual Server from multiple pooled servers (VM or no VM support)

  Application deployment requirement 2Ghz, 3GB, 500 Mbps

  Virtual Server
  - 2Ghz, 3GB, 700 Mbps

  Web Server
  - Linux 2.4
  - Hardware
    - 1Ghz, 2GB
    - 100 Mbps
    - Hardware
  - 2Ghz, 2GB
    - 100 Mbps
  - Hardware
    - 2Ghz, 4GB
    - 1 Gbps

  Web Server
  - Linux 2.4
  - Hardware
    - 2Gb, 600 Mbps

  DB Server
  - Linux 2.4
  - Hardware
    - 1Ghz, 2GB
    - 100 Mbps
Virtual Servers Across Wider Network

- Virtual servers by pooling resources (in a Grid) across LAN, MAN and WAN

Pooled Servers

DC (Data Center) 1

Servers/Clusters

IB

SAN

FC

DC LAN

MAN/WAN

LAN

Customer/RemoteSite1

FE/GbE: Fast/Gig Ethernet

IB: InfiniBand

FC: Fiber Channel

Customer/Remote Site 2
Grid Technology for Virtual Servers

- Grid Middleware and systems (Globus GT4, LSF, etc.) can be used to pool servers
- Pooled servers can be offered as virtual servers
- A Virtual server mapped to multiple servers via schedulers
Storage Virtualization
Storage Virtualization—Introduction

- What is virtualized
  - Block
  - Disk
  - Tape
  - File System

- Where virtualized
  - Host/Server
  - Network
  - Storage Device/subsystem
No Virtualization

- LUNs (Logical Unit Number) assigned directly to hosts
- No dynamic allocation of physical disk space
- Changes in physical configuration impact hosts/applications
- Unused space cannot be re-assigned to another host
Storage Virtualization

- LUNs mapped to virtual volumes (VV)
- Hosts/applications see VV
Storage Virtualization—Network-Based: Benefits

- Non-disruptive volume movements, replication across heterogeneous storage
Network Virtualization
Network Virtualization—Introduction

- Physical or Logical network entities are virtualized
- VLAN
- VSAN
- VPN
  - L2 VPN
  - L3 VPN
- Virtual Network Services
  - Virtual Firewall (FW)
  - VPN
- Virtual Router
SAN Virtualization— VSAN

- Separate physical fabrics
- Over-provisioning ports on each island
- High number of switches to manage

Collapsed Fabric with VSANs

- Common redundant physical infrastructure
- Less over-provisioning required—lower $$
- Fewer switches to manage
- Move unused ports non-disruptively
- Analogous to Ethernet VLANs
SAN Virtualization—VSAN

VSAN header is added at ingress point indicating membership.

No special support required by end nodes.

VSAN header is removed at egress point.

Enhanced ISL (EISL) Trunk carries tagged traffic from multiple VSANs.

Trunking E_Port (TE_Port)

Fibre Channel Services for Blue VSAN

Fibre Channel Services for Red VSAN

Fibre Channel Services for Blue VSAN

Fibre Channel Services for Red VSAN
# Layer 2 and 3 VPN

<table>
<thead>
<tr>
<th>Layer 2</th>
<th>Layer 3</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Point to Point</strong></td>
<td><strong>Multipoint</strong></td>
</tr>
<tr>
<td>Ethernet over MPLS</td>
<td>GRE</td>
</tr>
<tr>
<td>ATM/Frame Relay over MPLS</td>
<td>IPSec</td>
</tr>
<tr>
<td>HDLC and PPP over MPLS</td>
<td>VPLS</td>
</tr>
<tr>
<td>L2TPv3</td>
<td>(Virtual Private LAN Service)</td>
</tr>
<tr>
<td><strong>Layer 3</strong></td>
<td><strong>MPLS L3 VPN</strong></td>
</tr>
</tbody>
</table>
MPLS VPN

- Routing in each individual VPN sites (such as Green VPN) is isolated from others via Virtual Routing Forwarding (VRF) tables
- Routing not allowed between different VPNs (unless explicitly configured)
- VRF is a virtual routing instance in a physical router
- Separate Global RT is used for global or Internet routing
- VRF can be extended to CE and called the VRF-Lite or Multi-VRF

Multi-tenant building
MPLS VPN extended to Enterprise or DC core
VPLS: Virtual Private LAN Service

- Network virtualized as an L2 switch
VPLS: Virtual Private LAN Service

- MAC table instances per customer and per Customer VLAN on PE
  - Virtual Forwarding Instance (VFI)
  - Like a MAC bridge

Diagram:
- CE
- PE
- VFI
- Emulated VC
- Emulated Tunnel (Pseudowire-based)
- Attachment VC
Virtual Firewall

- Catalyst FWSM Virtual Firewall (VFW)
  FW per Context
  context example: particular customer or VPN

- MPLS VPN VRF associated with VFW for VPN-based firewalls
Virtual L4-L7 Network Services

- Catalyst 6500 ACE (Application Control Engine)

**Virtual partitions definable by**
- Customer
- Business organization
- Application
- Application tier

**All L4-L7 services available to each virtual partition**

**Guaranteed resources for each partition**
- By performance
- By network
- By management

**Role-based Access Control for each partition**
ACE Virtualization Benefits – Multi-tier DC Consolidation

Enterprise Network

Firewalls

LB

Front-end servers

LB

Application servers

LB

DataBase servers

Enterprise Network

Front-end Firewalls

Front-end servers

Application servers

DataBase servers

FE virtual context

APP virtual context

DB virtual context
ACE Virtualization Benefits – Service Velocity

- Adding a New Application in the Data-Center with ACE…

New Partition

Security Role
Network Role
Application Role

SecOps Add Firewall Rules

CASE # 1202

NetOps Creates Virtual Partition

CASE # 1201

ACE benefits delivered to Cisco IT:
- Up to 70% reduction in number of devices
- Up to 66% increase in service velocity (66% decrease in time-to-deployment)

Applications Team Gives Specs to SysAdmin, NetOp and SecOp… SysAdmin Installs Servers

The Application Team Can Now Proceed to Verify the Configurations, Fine-tune the L5 Rules, Verify ACL Counters, and Much More!
Virtual Router

- Virtual Router (VR) similar to OS VM
- Multiple VRs sharing physical HW
- Cisco CRS-1
E2E Virtualization
All Encompassing Virtualization 😊

Virtualize all the Virtuals and keep the Virtual University open😊

And when it came to the virtual VC, the virtual deans, the virtual heads of department and the virtual committees, we thought, "Oh, blow it!"

- Virtualize all the Virtuals and keep the Virtual University open😊
E2E Virtualization—Introduction

- Combine all or any combination of virtualization
- OS VM + Virtual Storage + Virtual Network
- Deploy an App VM with associated virtualized storage, VSAN and the Virtual Network that the App belongs to (App traffic crosses to) → E2EVM
- E2EVM detached from physical entities (HW, storage, Network)
- E2EVM requires support from Network/Service Management Systems (N/SMS)
  - E2EVM elements (virtualized storage and network entities) distributed over the network
  - Requires E2E configuration, provisioning, and other management support
  - Cisco N/SMS: VFrame, ANA (Active Network Abstraction)
E2E Virtualization—Example

- Web and associated backend DB server served as Virtualized App/DB Server (App VM)
- Server HW served from Virtual Server (from server pool)
E2E Virtualization—Example

- Virtual Storage served from virtualized SAN storage
- Virtual SAN associated with Server HW or App VM
- App VM connects to Virtual Storage via VSAN
E2E Virtualization—Example

- Departments/remote sites/branches connect to App VMs in DC via Virtual Network
- Virtual Network served as VLAN + Virtual FW + MPLS VPN
Virtualization and Environment
Virtualization Is Green?

- Pacific Gas and Electric this week announced a plan to pay as much as 50% of the setup costs—a maximum $4 million per customer—for its customers who opt to use virtualization software to reduce server counts and power and cooling costs in their data centers.

Network World, 11/09/06
Cisco SAN Virtualization—Impact
Conclusion
Conclusion

- In a networked world virtualization has to be looked into from all levels and E2E
  Not just from OS and server virtualization perspective

- E2E Virtualization has the potential to facilitate
  Effective IT optimization
    - Server and network element consolidation
    - Optimization in the DC and across LAN, MAN and WAN
  Effective deployment of networked applications and services (A&S)
    - By detaching A&S from underlying devices (HW) and network

- Because of its E2E reach in the network, Cisco and partners are in a unique position to support effectively E2E networked virtualization
  Cisco tools: VFrame, Cisco Active Network Abstraction (ANA)
Conclusion

- Challenges in virtualization that should be addressed in an effective way
  - What and how to virtualize
  - How E2E aspect can be effectively virtualized
  - How performance can be improved
  - Security issues
  - Software licensing issues
Q and A