Best Practices for Building and Securing a VDI Implementation

Russel Wilkinson

Sr. Systems Engineer

VMware

VMWORLD 2006

Agenda

- Virtual Desktop Infrastructure (VDI) Overview
- VDI Benefits
- VDI Architecture Review
- VDI Performance Tweaks

Agenda

- Virtual Desktop Infrastructure (VDI) Overview
- VDI Benefits
- VDI Architecture Review
- VDI Performance Tweaks

VMware Desktop Product Line

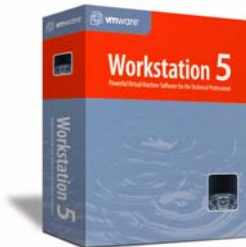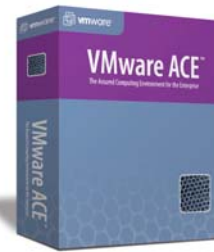| Individually Administered Desktops	Managed Desktops

Free Virtual Machine Run-Time

Desktop Virtualization for IT Professionals

Secure, Managed Desktop Virtualization

Server-based Desktop Virtualization

Player

Workstation

ACE

VDI

VDI – Overview

Thin Client or PC
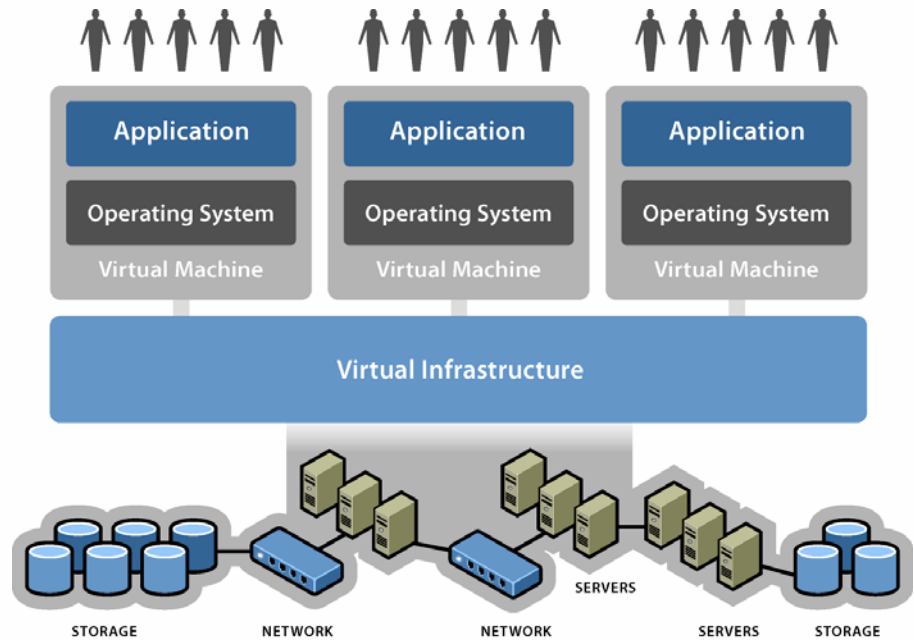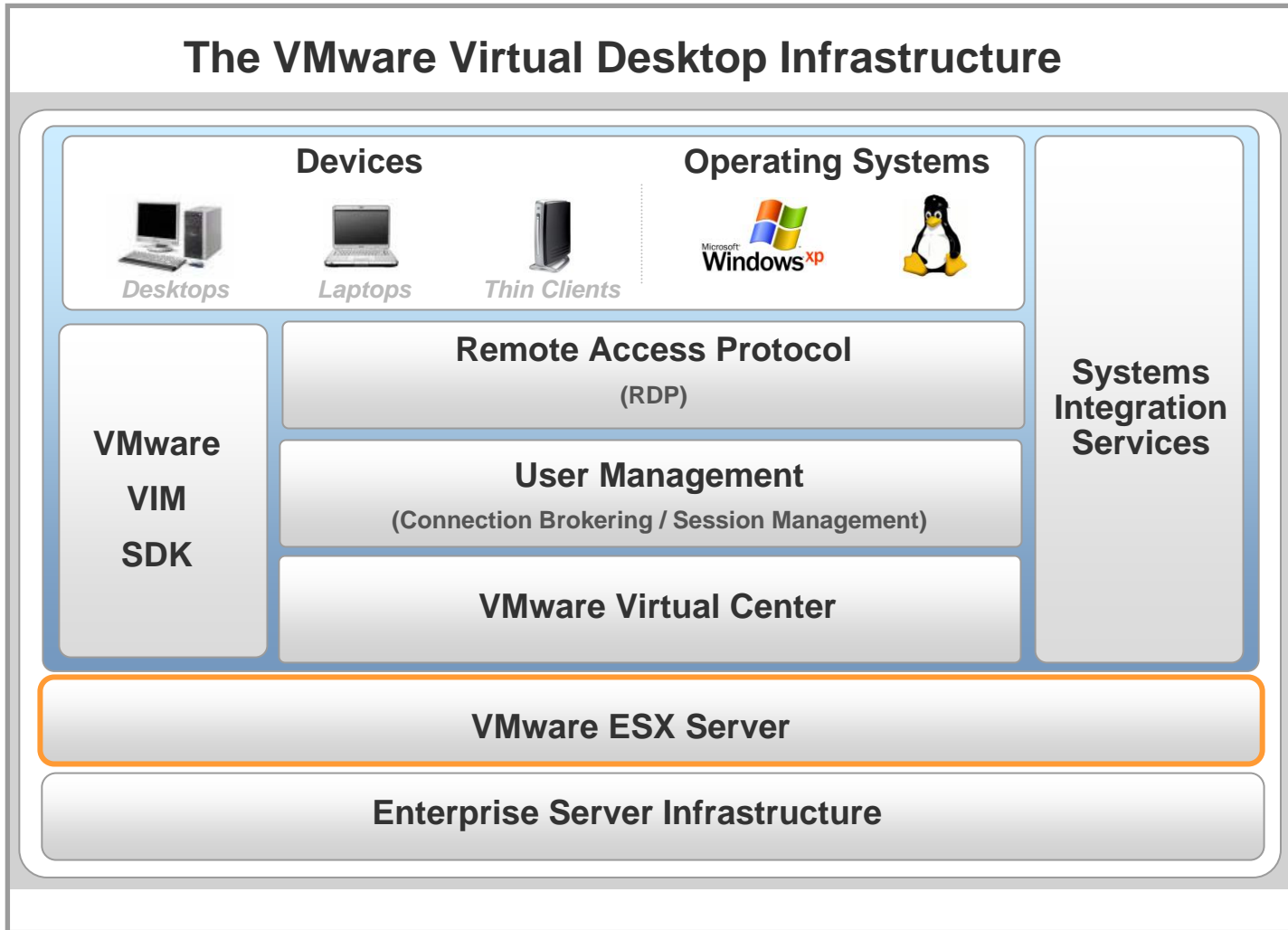
Virtual Infrastructure 3 Server
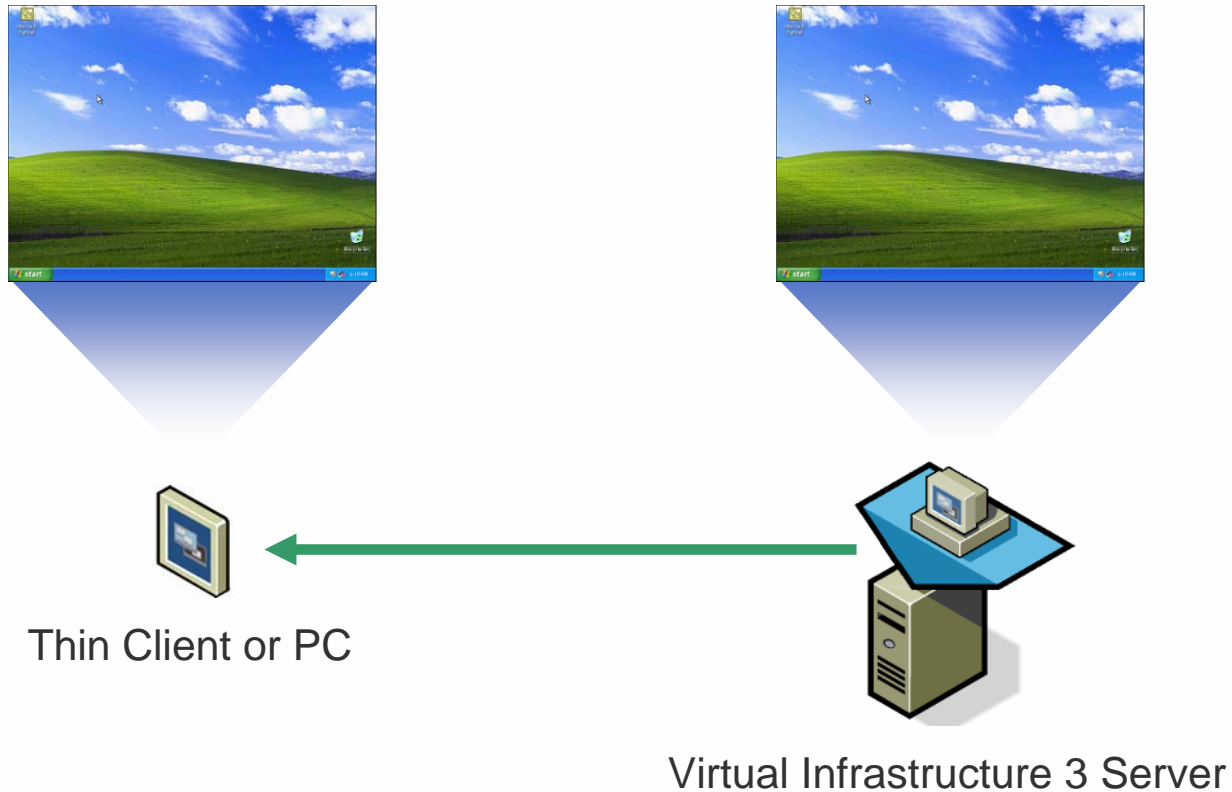
- VDI leverages Virtual Infrastructure 3 and a remote control protocol such as RDP to provide users access to a standardized remote desktop.

VDI – Key Concepts

- VDI is a usage scenario for Virtual Infrastructure 3. VI3 is the core product which hosts the virtualized desktops.

- VDI describes various ways of using VI3 in conjunction with other hardware and software to provide remote desktop access.

- A VI3 implementation can simultaneously support both server and desktop uses.

- VDI solutions can be tailored to specific needs and use cases by selecting the proper tools, architecture, and 3rd-party components.

VDI - The Building Blocks

The VMware Virtual Desktop Infrastructure

Devices

Desktops　　Laptops　　Thin Clients

Operating Systems

Windows xp

VMware VIM SDK

Remote Access Protocol

(RDP)

User Management

(Connection Brokering / Session Management)

VMware Virtual Center

Systems Integration Services

VMware ESX Server

Enterprise Server Infrastructure

Agenda

- Virtual Desktop Infrastructure (VDI) Overview
- VDI Benefits
- VDI Architecture Review
- VDI Performance Tweaks

VDI Benefits – Centralization

- Close to IT Operations
  - Virtual Machines are located in the Data Center, close to the support staff that tends to them.
  - Management tools can access desktop VMs over high-speed local networks for patching and system maintenance.
- Application Performance
  - Close proximity to servers maintains application performance regardless of where the client is located.
- Security
  - All data resides on a secure network inside the corporate firewall.
  - Remote users only 'view' data so it never gets transferred to insecure devices which might be lost, stolen, or hijacked.

VDI Benefits – Compatibility

- Real Desktop Operating Systems
  - Virtual Machines run Windows XP just like physical hardware so applications work normally without modification.
  - Applications can make system level changes such as registry writes and DLL replacements where necessary.
  - Existing corporate desktop configurations can be easily imported.
- Isolation
  - Each Virtual Machine runs separately, so a crashed VM or a poorly behaving application does not affect other users on the same server.
  - VDI is suitable for developers because any type of change can be made to a VM without affecting other users.
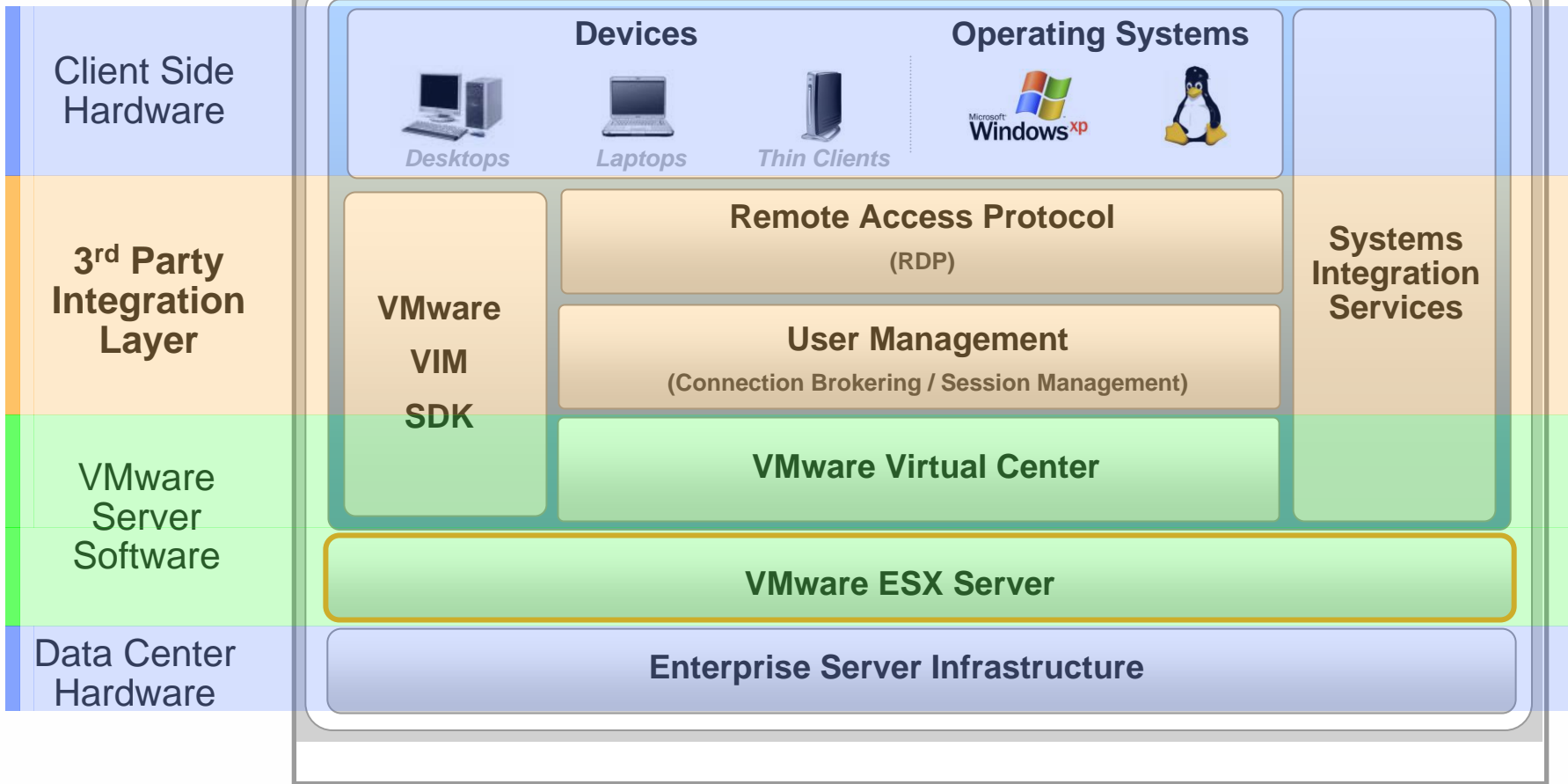
VDI Benefits – Virtualization

- **Homogenous Virtual Hardware**
  - All Virtual Machines use the same virtual hardware.
  - One base image can be used for many different VMs – driver management is greatly simplified.
  - Templates can be created in Virtual Center to aid rapid deployment of new Virtual Machines
- **VDI is Virtual Infrastructure**
  - VI3 Servers and Virtual Center are the core components.
  - Virtualized Server and Desktop spaces can leverage the same hardware, architecture, and infrastructure.
  - Automatic Load-Balancing and High Availability through VMware HA, DRS, and VMotion features.

Agenda

- Virtual Desktop Infrastructure (VDI) Overview
- VDI Benefits
- VDI Architecture Review
- VDI Performance Tweaks

VDI – Architecture Review

The VMware Virtual Desktop Infrastructure

| Client Side Hardware	**Devices**			**Operating Systems**	
	Desktops	*Laptops*	*Thin Clients*		
3rd Party Integration Layer	**VMware VIM SDK**	**Remote Access Protocol** (RDP)			**Systems Integration Services**
		User Management (Connection Brokering / Session Management)			
VMware Server Software		**VMware Virtual Center**			
	VMware ESX Server				
Data Center Hardware	**Enterprise Server Infrastructure**				

VDI Architectures – Basic Implementation

- A "One-to-One" relationship between endpoints and Virtual Machines is established.

- End-users are assigned a hostname or an IP address of a VM which belongs to them.

- Connections take place over an existing secured corporate network.

- Remote viewing of VMs is done through desktop RDP software, or through the built-in features of a Thin Client.
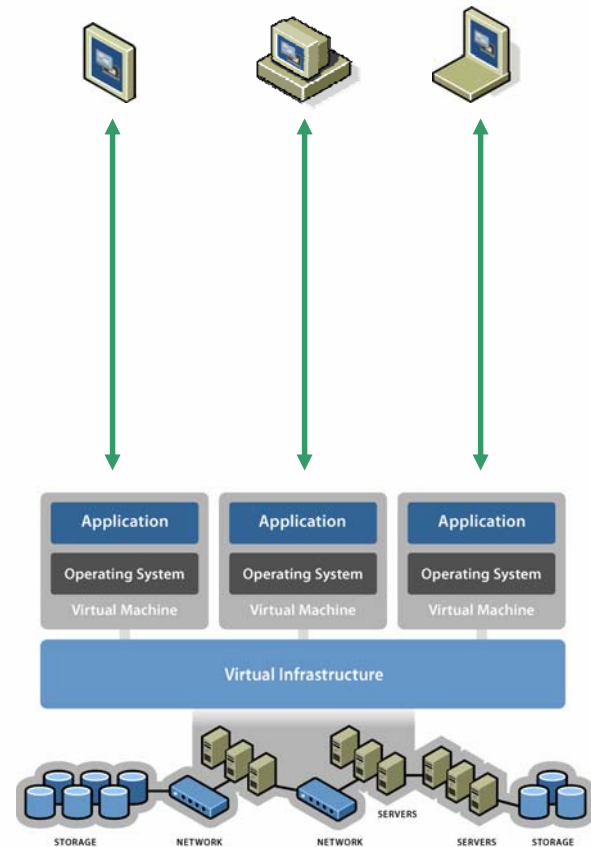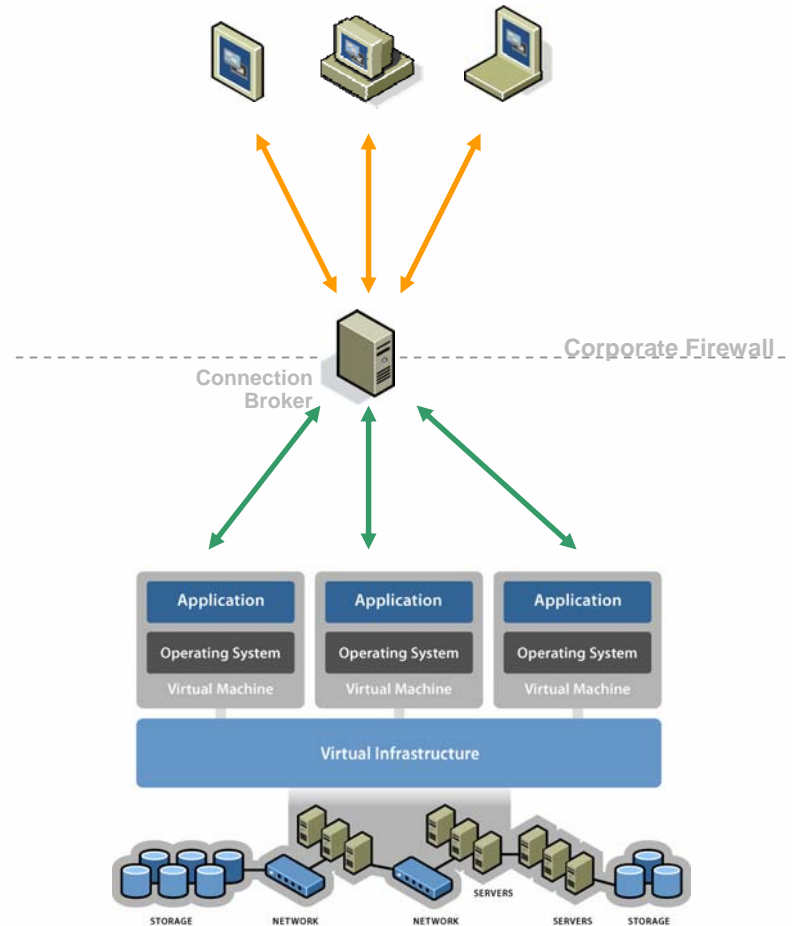
VDI Architectures – Simple Brokering

- End-users are given a web address on the corporate network for the connection broker.

- After authenticating, the connection broker provides a list of available resources to the end user.

- The end-user establishes a connection directly to the VM using desktop or web-based RDP software, or through built-in features of the Thin Client.
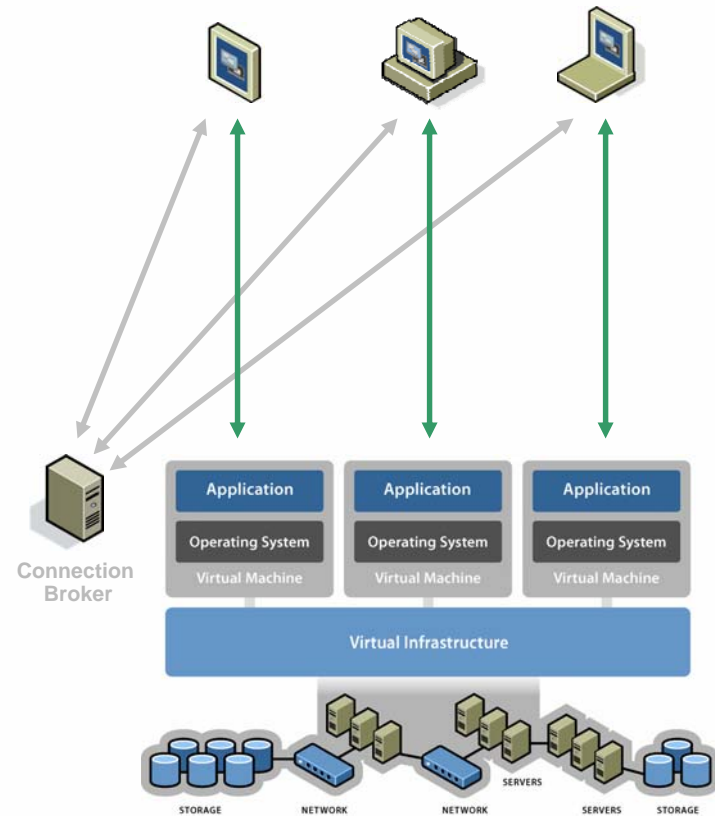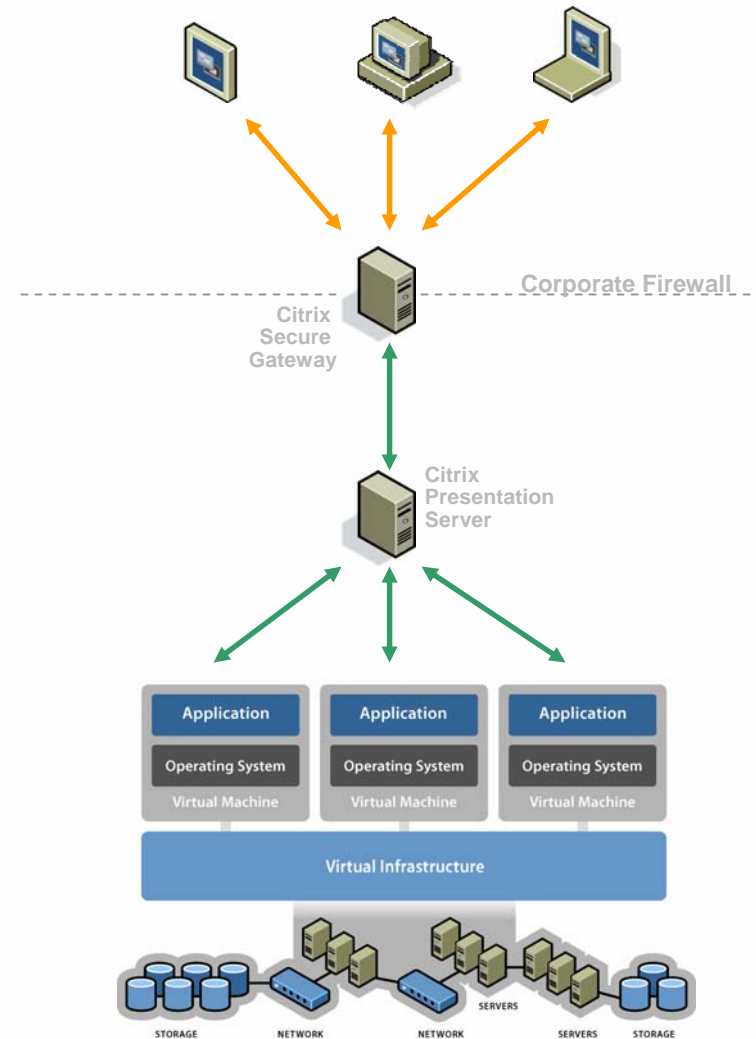
VDI Architectures – Tunneled Brokering

- End-users are given a public web address for the connection broker.

- After authenticating, the connection broker provides a list of available resources to the end user.

- The connection broker links the end-user via an encrypted tunnel to the VM or resource provided.

- The encrypted tunnel is typically a mini-VPN component designed to route specific traffic such as RDP.

Corporate Firewall

Connection Broker

Application | Application | Application
Operating System | Operating System | Operating System
Virtual Machine | Virtual Machine | Virtual Machine

Virtual Infrastructure

STORAGE   NETWORK   NETWORK   SERVERS   STORAGE
SERVERS

VDI Architectures – Proxied Brokering

- End-users are given a public web address for the Citrix Secure Gateway.

- After authenticating, the Citrix Gateway connects end-users to the Presentation Server which provides a list of desktop and applications which are published.

- The Citrix Presentation Server links the end-user via an encrypted tunnel to the VM or resource provided.

- The encrypted tunnel carries ICA traffic from the endpoint to the Presentation Server and RDP from the Presentation Server to the Virtual Machine.


Corporate Firewall

Citrix Secure Gateway

Citrix Presentation Server

Application	Application	Application
Operating System	Operating System	Operating System
Virtual Machine	Virtual Machine	Virtual Machine

Virtual Infrastructure

STORAGE   NETWORK   NETWORK   SERVERS   SERVERS   STORAGE

VDI – Protocol Overview

- Remote Desktop Protocol
  - Good performance, supports audio output.
  - Viewers available for many platforms and as a browser plug-in.
- Virtual Network Computing
  - Server exists for almost any platform.
  - Various commercial and free versions available.
  - Performance varies by implementation, no audio support.
- Independent Computing Architecture
  - Excellent performance and bi-directional audio support.
  - Requires Citrix Presentation Server.
- Remote Graphics Software (RGS)
  - Best graphics performance.
 - Per-node Licensing required from Hewlett-Packard.

VDI Printing – Network Printing

- A network printer is located near the endpoint.

- Printer drivers for the network printer are installed in the Virtual Machines.

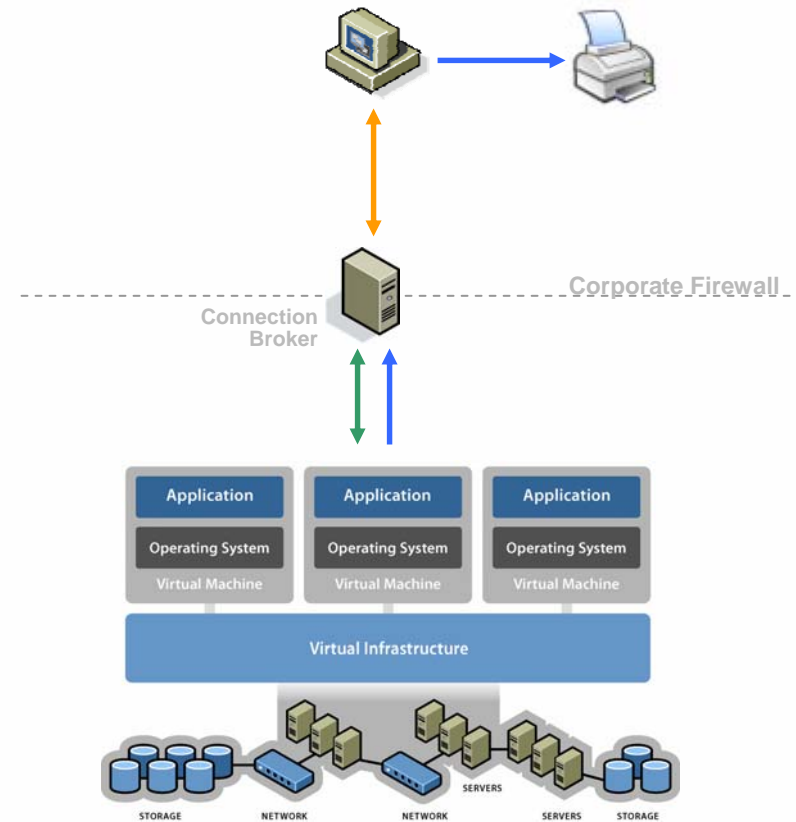- Connections take place over an existing secured corporate network.
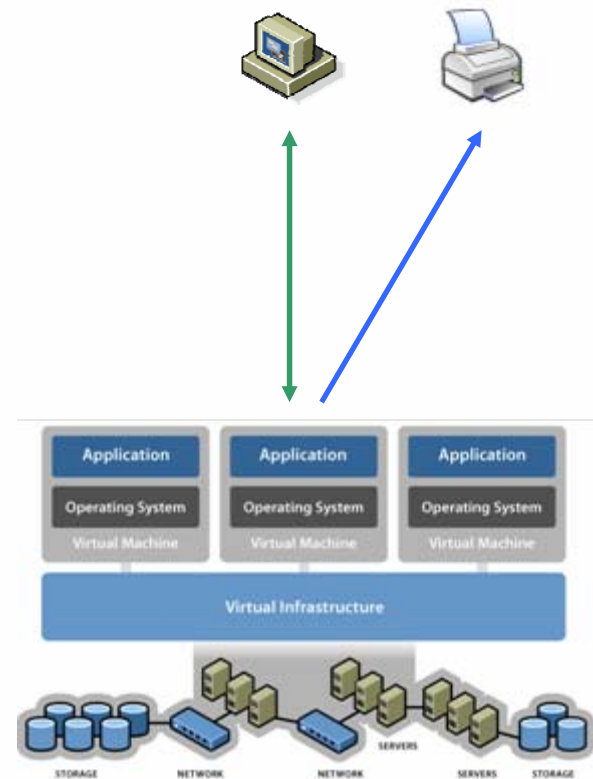
VDI Printing – 3rd-Party Universal Print Drivers

- A network printer is located near the endpoint.

- A "universal printer driver" is installed on the VM which grabs print jobs.

- A client component is installed on the endpoint which receives jobs from the universal printer driver software.

- The client component prints the job directly to the printer connected to the endpoint.

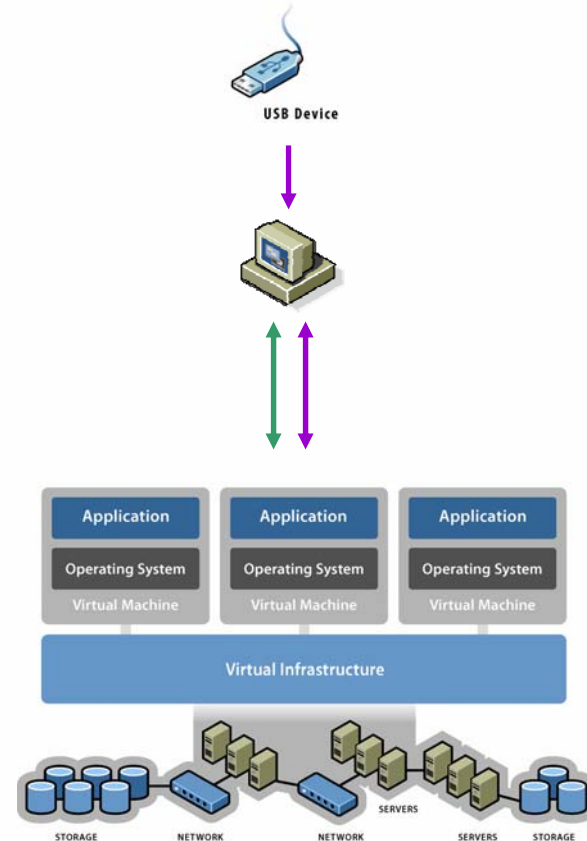- Universal printer drivers do not generally work with thin clients.
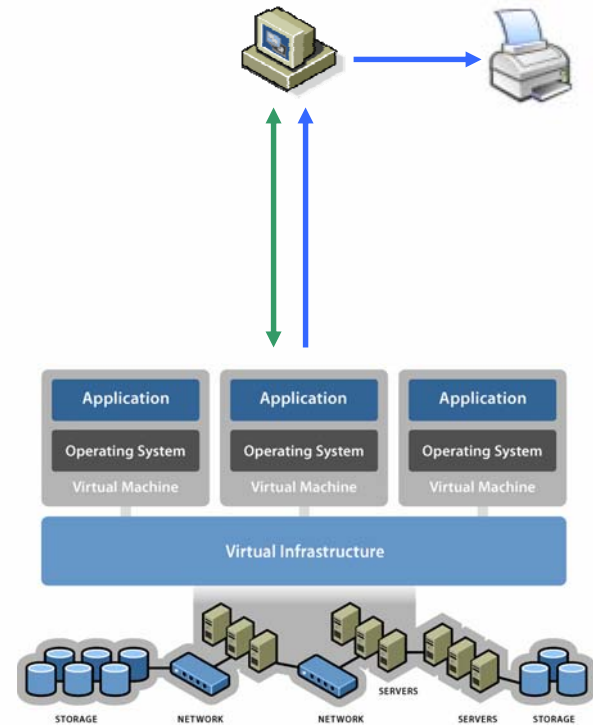
VDI Printing – 3rd-Party Brokered Printing

- A print driver which generates a standard format such as PDF is installed on the VM.

- Jobs are printed in PDF format to a user-specific location.

- The connection broker lists available jobs for 'pickup' by the end-user.

- The end-user downloads the PDF from the connection broker and prints the document.


Corporate Firewall

Connection Broker

Application | Application | Application
Operating System | Operating System | Operating System
Virtual Machine | Virtual Machine | Virtual Machine

Virtual Infrastructure

STORAGE   NETWORK   NETWORK   SERVERS   STORAGE
SERVERS

VDI and USB – Software USB-over-Ethernet

- A software server component is installed on the end-point.

- Users attach USB devices directly to the PC for redirection.

- A client component is installed inside the VM.

- The client component connects the devices on the client to the VM which makes them appear to be directly connected.

- Software solutions do not work with thin clients.

- Support for high-throughput devices is very limited.

USB Device

Application	Application	Application
Operating System	Operating System	Operating System
Virtual Machine	Virtual Machine	Virtual Machine

Virtual Infrastructure

STORAGE   NETWORK   NETWORK   SERVERS   STORAGE
SERVERS

VDI and USB – Hardware USB-over-Ethernet

- A hardware USB-over-Ethernet device is located near the endpoint.

- Users attach USB devices to the hardware device for redirection.

- A client component is installed inside the VM.

- The client component connects a port on the hardware device to the VM which makes it appear to be directly connected.

- Devices can have multiple ports, and ports can be divided across different VM's.
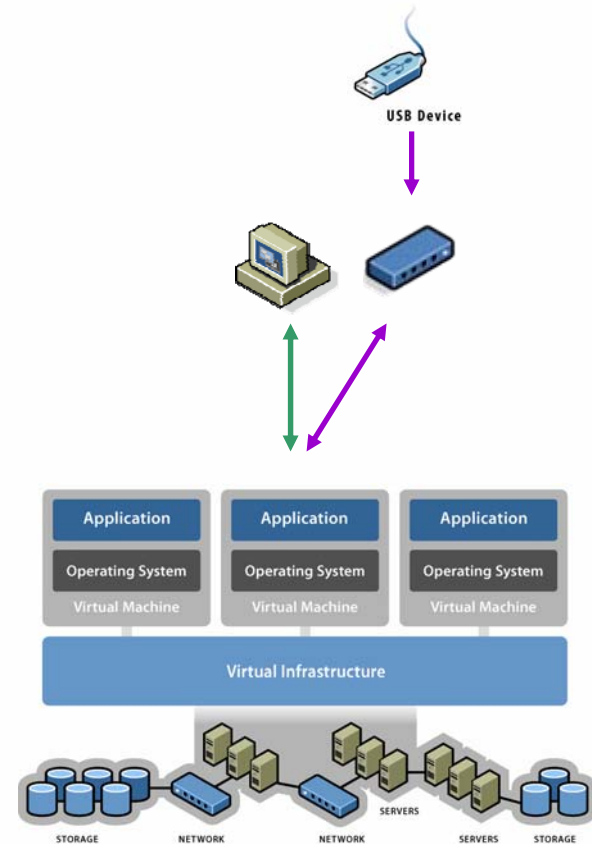
Agenda

- Virtual Desktop Infrastructure (VDI) Overview
- VDI Benefits
- VDI Architecture Review
- VDI Performance Tweaks

VDI – Performance Tweaks

- ESX System Changes
  - Follow guidelines in our white papers
    - http://www.vmware.com/pdf/esx_performance_tips_tricks.pdf
    - http://www.vmware.com/vmtn/resources/esx_resources.html
    - http://www.vmware.com/pdf/vdi_sizing_vi3.pdf

- RDP Client Change
  - Disable remote computer sound
  - Disable local device map-through
    - Disk Drives, Printers, & Serial Ports
  - Optimize the performance options for dial-up connections

VDI – Performance Tweaks

- Virtual Machine System Changes
  - Ensure that floppy drive (if present) is not connected at startup
  - Ensure that cd-rom drive (if present) is not connected at startup
  - Disable COM1 & COM2 in the BIOS

- Windows XP Level Changes
  - Turn off all theme enhancements except for font smoothing
    - Right-click "My Computer" -> Select "Properties"
    - Choose the "Advanced Tab"
    - Under Performance Section Choose "Settings"
    - Choose "Adjust for Best Performance"
      - Optionally choose settings deemed necessary

VDI – Performance Tweaks

- Windows XP Level Changes (cont'd)
  - Disable all screensavers
  - Ensure full hardware acceleration
    - Control Panel -> Display -> Settings Tab -> Advanced Button
    - Troubleshooting Tab -> Set acceleration to full
  - Install VMware Tools and switch NIC to vmxnet
  - Ensure SP2 is installed or apply MS Q811080
  - Disable the logon screen saver
    - HKU\.DEFAULT\Control Panel\Desktop
      - "ScreenSaveActive"=dword:00000000

VDI – Performance Tweaks

- Windows XP Level Changes (cont'd)
  - Disable Control+Alt+Delete to bring up logon screen
    - HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
      - "DisableCAD"=dword:00000001
  - Improve Windows Kernel Memory Management
    - HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management
      - "DisablePagingExecutive"=dword:00000001
  - Launch Windows Desktop as a Separate Process
    - HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer
      - "DesktopProcess"=dword:00000001

VDI – Performance Tweaks

- Active Directory
  - Create and publish a GPO for folder redirection to the users' storage space on the SAN for the following
    - Application Data
    - Desktop
    - Start Menu
    - My Documents (and all sub-class special folders)

How Do I Learn More About VDI?

- ■ Attend Other VMworld Sessions and Labs on VDI:
  - > MED0062: How Collier County Public Schools Deployed the Largest Virtualized Desktop Environment in the World, Tuesday 11/07/2006 @ 11:45 am
  - > MED9518: Best Practices for Building and Securing a VDI Implementation, Tuesday 11/07/2006 @ 2:00 pm
  - > MED3499: Building a Scalable, Dynamic Call Center using VMware Virtual Desktop Infrastructure, Wednesday 11/08/2006 @ 11:45 am
  - > MED9913: Healthcare Organizations and Virtual Desktop Solutions: Kindred Healthcare – A Case Study, Wednesday 11/08/2006 @ 2:00 pm
  - > MED3757: VDI Customer Panel, Thursday 11/09/2006 @ 9:30 am
  - > Plus many more partner sessions on VDI…
- ■ Visit www.vmware.com/VDI

Thanks!!!

Russel Wilkinson
rwilkinson@vmware.com
248-375-0225 (Office/Cell)

Presentation Download

Please remember to complete your
session evaluation form
and return it to the room monitors
as you exit the session

The presentation for this session can be downloaded at
http://www.vmware.com/vmtn/vmworld/sessions/

Enter the following to download (case-sensitive):

Username: cbv_rep
Password: cbvfor9v9r

VMWORLD 2006