Teaching Local Area Networking in a Secure Virtual Environment

Gary D. Steffen

Electrical and Computer Engineering Technology
Indiana University – Purdue University Fort Wayne

Abstract

Space, cost and security are all concerns when instructing local area networks. Teaching even the most basic networking techniques requires a minimum of two computers per student with additional systems for more involved experiments. The overhead and space requirements become quite staggering for large class sizes. The students, just learning and unaware, can furthermore be susceptible to outside intrusion or cause accidental adverse affects upon the network to which they attach. Teaching local area networking in a virtual environment can reduce space, cost, and security concerns.

The initial discussion looks at how the virtual environment works by enabling multiple operating systems and their applications to run concurrently on a single physical machine. These operating systems and applications are isolated in secure virtual machines that co-exist on a single piece of hardware. Consideration is given on how traditional basic networking techniques can be adapted to the virtual environment. Important topics include the setup of a virtual environment, managing multiple student environments, properly securing virtual machines, and laboratory experiments in virtual environments.

Introduction

Space and money have always been a concern when teaching any computer class at Indiana University-Purdue University Fort Wayne (IPFW). Like many establishments of higher education the battle to stay current with hardware and software needs can seem staggering. This can multiply itself when talking about the instruction of the local area networking (LAN) course.

Students in modern local area networking courses can expect to be introduced to several different network operation systems (NOS) and client side operating systems. Creating the smallest of these networks would require, at a minimum, two computers per group, one of these systems being the server and other the client. Teaching more realistic and involved local area networking techniques requires several additional computers per group.

In the past, limited hardware and space required student group sizes for experiments to be quite large (3 to 4 people). A constant complaint of the student was the lack of time working with the NOS because of the group size. To help limit group size, reduce needed space, and overt cost, the Electrical and Computer Engineering Technology (ECET) Department at IPFW has

implemented the use of virtual computing in the instruction of local area networking. The use of server virtualization offers an opportunity to stretch dollars through more complete utilization of available processor cycles and to substantially reduce hardware costs through consolidation. [1]

Virtual Computing

Virtual computers are time and money savers for testing software and web sites, for education or sales, or for running software designed for old computers on today's hardware. A virtual-machine utility creates seemingly separate PCs inside your host system. Each acts like a full-fledged standalone computer system running its own OS (such as Windows, Linux and other x86-complient operating systems), and these guest virtual machines act as if they are connected by a wired Ethernet network to the host system. [2]

The use of virtual computing allows for the creation of a centralized, homogenous, virtual network. Independent virtual machines consisting of NOS and client computers can coexist on a single host system. Each virtual machine has its own self-regulated environment and hardware created by the underlying virtual software. The need for an external network is not necessary since a virtual network can be created between virtual machines. Virtual machine software is usually based on several common properties[3]:

- *Isolation*- A virtual machine software that allows multiple applications to run in different virtual machines.

- *Extensibility*- Any "one size fits all" approach provided to an operating system can greatly limit a platform's flexibility. The virtual machine should adjust to the specific applications needs.

- *Efficiency*- The virtual machine must provide essentially the same properties as separate physical machines using more modest resources.

- *Compatibility*- Virtual machines that can run today's operating systems, such as Linux and Windows, and applications without need for modifications.

- *Security*- A virtual machine is a relatively simple program with a narrow, stable, well-defined interface to the software running above it.

Connectix's Virtual PC for Windows and VMware Workstation are the most popular virtual machine utilities, and each company has released powerful new versions. Virtual PC emphasizes ease of use and doesn't approach the industrial-strength, virtual hardware and networking options of VMware[2]. VMware is able to build complex, enterprise-level virtual networks simply and is capable of running virtual SCSI disks and real USB-based hardware. Based on ease of use and industrial support VMware was chosen for implementation at IPFW.

VMware Workstation 4.0

VMware is a software company founded in 1998. The desktop version, VMware Workstation, installs on top of an existing host operating system such as Windows NT/2000/XP or Linux. This Virtual machine technology supports complex guest operating systems, and lets them share SCSI and USB peripherals with host systems. Besides MS-DOS, Windows 3.1, 95, 98, ME, Windows NT, 2000, and XP, the software supports many popular versions of Linux, several beta versions of Microsoft .NET Server, FreeBSD and Novell NetWare 6.0. VMware Workstation supports ISO image file, which resembles a physical CD-ROM to the guest operating system and contains the contents of the CD-ROM [4].

Furthermore, VMware workstation 4.0 provides additional tools to help simplify management.

- *VMware tools*- This adds a 32-bit display and high display resolution, grab and release of the mouse cursor, copying and pasting between virtual machines and host, and improved mouse performance.

- *Snapshots*- VMware Workstation 4 lets you make a point-in-time copy of the running system state, saved to disk, and allows the user to revert back to a previously saved state at any time. This is excellent for student use in the laboratory environment.

- *Tab Between Virtual Machines*- In the Quick Switch mode, you can tab between virtual machines with a mouse click.

- *Drag and Drop and Shared Folders*- You can easily share files between guest and host virtual machines by a shared folder or drag and drop file icons between systems. This works well when students are generating laboratory reports consisting of multiple virtual machines.

- *Virtual Network Support*- VMware has virtual Ethernet switches supporting: NetBEUI, Microsoft Networking, TCP/IP, Samba, Novell, Netware and Network File System(NFS)

Creating a Secure Virtual Environment

The creation of a secure virtual environment is important to the success of the local area networking experiments. This secure environment <protects against> not only includes external but also internal risks. These internal risks include limiting the student access to the host computer, limiting student access to potentially harmful external systems, and limiting students from each other. The typical external risks to the virtual environment include computer hackers and malicious code.

VMware supports several networking configurations that can be used between the host and virtual machines. Selection of the proper configuration is important to the security of the virtual machines:

- *Bridged Networking*- Bridged networking connects a virtual machine to a network using the host computer's Ethernet adapter. If you use bridged networking, your virtual

machine needs to have its own identity on the physical network. For example, on a TCP/IP network, the virtual machine needs its own IP address. The virtual operating system may acquire an IP address and other network details automatically from a DHCP server or may be set manually.

If bridged networking is used, the virtual machine is a full participant on the physical network. It has access to other machines on the network and can be contacted by other machines on the network as if it were a physical computer on the network. This makes the virtual machine fully susceptible to outside intrusion (hacking) and malicious software (viruses/worms).

- *Host-Only Network*- Host-only networking creates a network that is completely contained within the host computer. This approach can be useful if you need to set up an isolated virtual network that isn't connected to a physical network. Your virtual machines and the host virtual adapter are connected to a private TCP/IP network. Addresses on this network are provided by the VMware DHCP server.

- *Network Address Translation (NAT)* - NAT gives a virtual machine access to network resources using the host computer's IP address.

  NAT works by translating addresses of virtual machines in a virtual network to that of the host machine. When a virtual machine sends a request to access a network resource, it appears to the network resource as if the request came from the host machine (*figure 1*)[5].

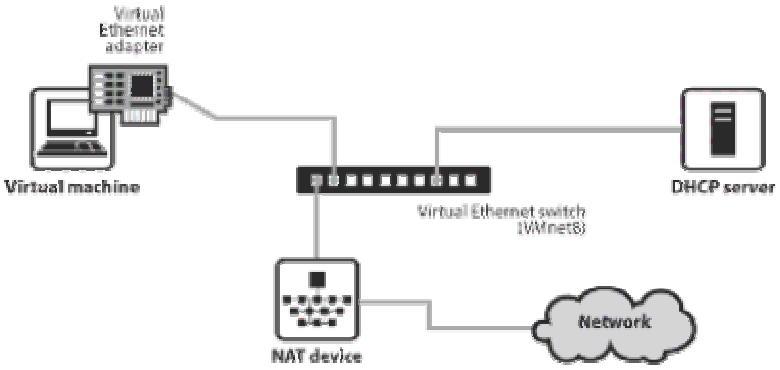

Figure 1.

Using NAT the virtual machine does not have its own IP address on the external network. Instead, a separate virtual network is set up on the host computer. Your virtual machine gets an address on the virtual network from the VMware virtual DHCP server. Then the VMware NAT passes network traffic between the virtual machines and the external network. It identifies incoming data packets from the external network intended for each virtual machine and relays them to the correct destination.

Limiting security concerns was a primary objective in the development of the local area networking class using virtual machines. Past local area network setups made conflicts between student groups common. These conflicts included selecting the same domain names, workgroup

names, and computer names, as well as, conflicts between multiple DNS, WINS and DCHP Servers. Possible attacks from malicious code and hacking were also of concern.

ECET implemented VMware Workstation 4.0 on a host computer running Redhat Linux 9.0. Linux was chosen as the host OS because of its stability and firewall capabilities. The underlying host Linux system can be setup once with the proper network configuration and then locked from students' changes. Students receive accounts on the host to access their own VMware environment. The student is unable to make any changes to the host system.

The network configuration chosen for our implementation was NAT. NAT allowed the capability to access the Internet without making the virtual machines participants on the external network. Using NAT with the host firewall, allows only outgoing traffic and incoming response traffic for the virtual machines. All generic incoming traffic is stopped (*figure 2*). This limits the possibility of external malicious attacks.

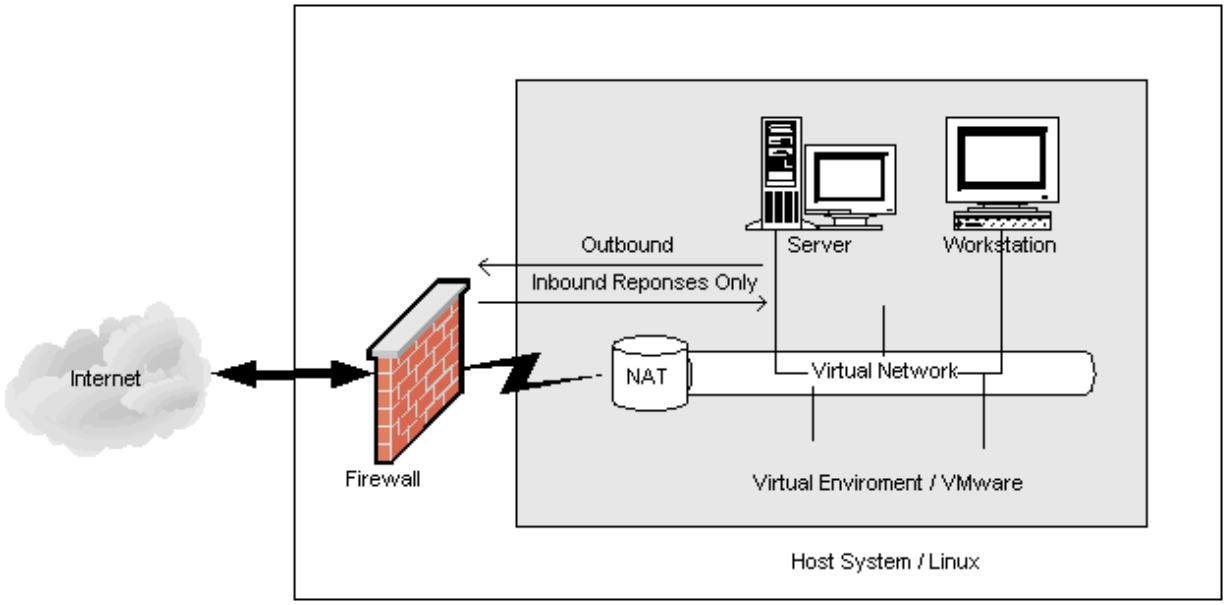

Figure 2.

Teaching in a Virtual Environment

The challenge of converting existing local area networking laboratories to VMware is not actually in the changing of experiments. Very little, if any, changes needed to be made to the existing laboratory experiments. The challenge of converting to VMware is typically of a technical nature:

- *Learning VMware*- The need to spend time learning VMware so it can be presented to the students. The interface to VMware is fairly straight forward and takes minimal time to learn. Tabs allow you to choose which virtual machine you want to access. (*Figure 3*)

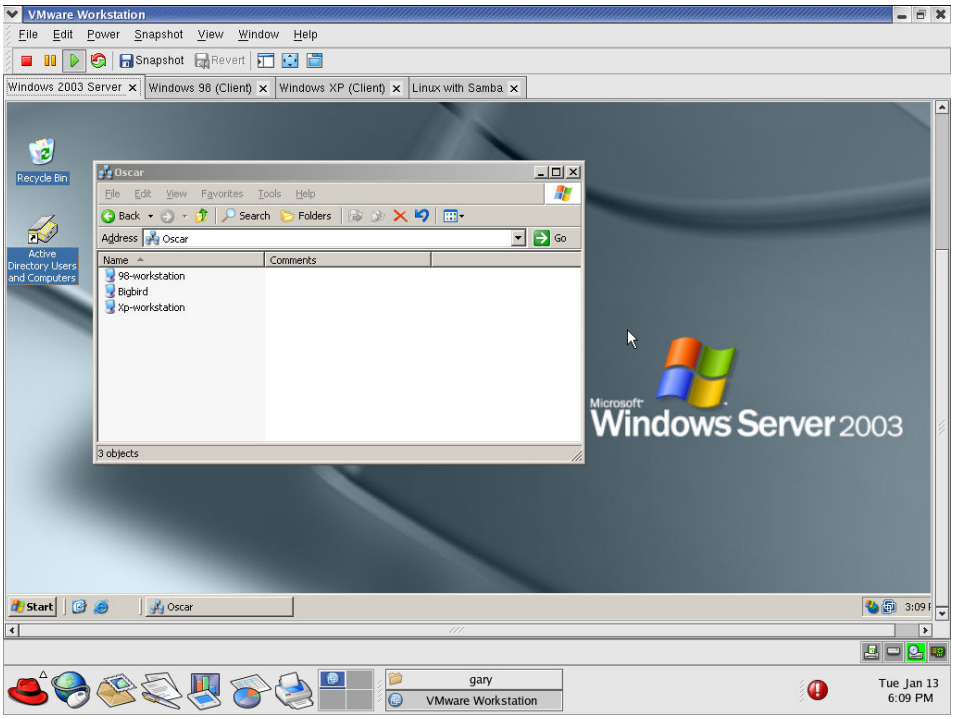

Figure 3.

- *Hardware Requirements*- Since multiple operating systems will be running concurrently, the system requirements are high. A mid-level Pentium IV with 1G RAM and large hard drive is minimally advisable.

- *Installing/Setup of VMware*- This can be the greatest challenge. Getting the host system setup, accounts created, and VMware properly installed can take the majority of the time. Once setup and working properly on a single system, it can be quickly transferred to other laboratory computers.

- *Student Orientation to VMware*- Some additional time will need to be set aside for the student instruction of VMware. Creation of a simple two page handout can help facilitate this.

- *New Experiments*- Since the number of virtual machines running is only limited by the host resource, more machines can be created than with a traditional laboratory. Not being limited allows for the creation of new labs on such topics such as:
    - Domain and Backup Domain Controllers
    - Active Directories, Trees, and Forests
    - Interfacing between Linux Samba, and Windows Servers[6]

- *Explanation of NAT*- With the introduction of the NAT, time must be taken to explain IP addressing on the virtual machine to the student. The VMware virtual DHCP server can automatically assign IPs or it can be turned off. Without the VMware virtual DHCP, the student must manually assign the IP information or setup their individual virtual DHCP server.

There are, of course, downsides to server virtualization. An outage of a single host system risks bringing down multiple processes in one fell swoop[7]. A single failure to the host eliminates all virtual machines.

Furthermore, creating a virtual environment allows less hands-on time for the student with the data communications equipment. In our case, the student is assigned an additional laboratory experiment that requires the setup of a physical communication switch and network attached to the host computer for Internet access. The student can view virtual network traffic flow between the virtual machines with any popular traffic monitoring software package. VMware supports the use of virtual machines as firewalls or routers, but the hands-on topic is saved for another course in wide area networking.

Overall, VMware has made a very large positive impact on our local area networking course. A few of the goals set forth when implementing virtual machines were to use limited space, stabilize cost, increase security, simplify management and enhance the students education. Today we are teaching more students in smaller groups (each student can have their own virtual machine) with the same amount of computers. Furthermore system management has been simplified for technical support and security issues have been addressed.

The greatest measure of impact is the enhancement of the student's education. "This is very cool" is a typical response of a student introduced to virtual computing. Students now have the capability to manage their own network, without sharing, which allows a deeper learning experience. This deeper experience has led to faster laboratory completion. The time gained is used to add additional topics to further enhance their education.

[1] James R. Borck, "Virtual Virtuosity", InfoWorld, Volume 24 Issue 6, 2002
[2] Edward Mendelson, "Run a PC Inside Your PC", PC Magazine, Volume 22 Issue 12, July 2003
[3] Tal Garfinkel, Ben Pfaff, Fim Chow, Mendel Rosenblum, and Dan Boneh, "Terra: A Virtual Machine-Based Platform for Trusted Computing", Proceedings of the nineteenth ACM Symposium on Operating Systems, 2003
[4] Kim Lei and Phillip T. Rawles, "Strategic Decisions on Technology Selections for Facilitating a Network/Systems Laboratory Using Real Options& Total Cost of Ownership Theories", ACM, Proceedings of the 4th Conference on Information Technology Curriculum on Information Technology Education, 2003
[5] http://www.vmware.com
[6] Gary Steffen, "Teaching Local Area Networking Using Samba Instead of Windows", ASEE 2003 Annual Conference Program and Proceedings, 2003
[7] Jeffrey Burt, "Virtual Machines Get Tune Up", eWeek, Volume 20 Issue 45, November 2003

GARY D. STEFFEN
Gary currently services as an Assistant Professor in the Electrical and Computer Engineering Technology Department at Indiana-Purdue University Fort Wayne. Previously, he served 10 years as the Manager of Electronic and Computer Support specializing in computer networking. Gary received a Masters degree from Ball State University in 2000 and recently completed the "Information and Security Assurance Certificate" from Purdue University sponsored by the NSA. His current areas of interest include local area networking, network security and wireless networking.