122nd ASEE Annual Conference & Exposition
June 14 - 17, 2015
Seattle, WA
Paper ID #13534

Hands-on Networking & Security Labs on Demand

Dr. Emil H Salib, James Madison University

Professor in the Integrated Science & Technology Department at James Madison University. Current Teaching - Wire-line & Wireless Networking & Security and Cross Platform Mobile Application Development. Current Research - Mobile IPv6 and Design for Motivation Curriculum

Ryan Lutz, James Madison University

Hands-On Networking & Security Labs On-Demand

Dr. Emil H Salib, Ryan Lutz, Ryan Carter
Integrated Science & Technology Department, James Madison University, Harrisonburg, VA
salibeh@jmu.edu, lutzra@dukes.jmu.edu, carterra@dukes.jmu.edu

Abstract

Virtualization is one of the most effective ways to increase efficiency, boost productivity and reduce expenses in an enterprise environment through the deployment of a platform such as VMware vSphere Suite. In academic classrooms, virtualization has also been adopted but in the form of a standalone desktop application such as VWware Workstation, Microsoft Hyper-V, Virtualbox, and QEMU to name a few. However, these standalone arrangements require a large amount of resources to be available on each of the workstations in our networking and security lab. Also, these arrangement demand the software updates and upgrades to a large number of workstations. This environment is not efficient and even sometimes wasteful. A student often needs the full computing power available at their workstation, but productive time is also lost when the workstations are idle, unable to be shared amongst other students in or outside the lab.

To address the efficiency and wastefulness issues of the networking and security lab at James Madison University, we have decided to use the VMware vSphere software suite that is typically deployed in enterprise operational environments. However, the issue with vSphere is that it lacks some of the basic functionality that is readily available on the standalone VMware Workstation software. Also, it limits the ability for each student or group to have their own hardware network interfaces when they need to integrate external physical networks with the virtual machines under vSphere. The vSphere suite was not designed to have dynamic networking where each user would be able to control and manipulate multiple VM's and appliances internal and external to the vSphere Operating System (ESXi). As a result we embarked on an aggressive re-purposing of the vSphere suite to take advantage of its efficiency, while also increasing its robustness to match that of what is available on a VMware Workstation, in a project known within the department as Hands-on Networking on Demand.

In this paper, we describe how two senior students and their advisor successfully virtualized the networking and security lab without losing any of the functionality that the lab currently has with the use of VMware Workstation. After many unsuccessful attempts to adapting the vSphere enterprise model suggested by VMware and others, the students gave up on the traditional architecture and creatively developed their own simple architecture. This architecture uses readily available appliances such as Untangle and takes full advantage of the pass-through of client hardware interfaces. After conducting trials with the new centralized architecture, the students found the lab experience much more pleasant and gained new network functionality that increased their creativity. We anticipate that the effort and time required by instructors and system administrators to set up and manage labs will markedly decrease, particularly, with the ability to centrally monitor the classroom progress and the students' utilization of servers' resources.

1. Introduction

Cloud computing is an up and coming technology that is gaining popularity as the speeds of our networks increase. Cloud computing [1-3] is the distribution of computing resources across the network. It normally has a central system, or server stack, that completes all of the computing processes while a remote client has the ability to control the operating environment through a "portal" or "window." This technology has thrown the hardware industry into a paradigm shift,

whereby enterprises would probably not purchase hardware, but instead simply lease, or buy the rights to, a certain amount of computing power that is maintained and owned by the cloud computing service provider. There are many advantages to this arrangement, making computing power much cheaper for small to medium-size businesses, allowing them to use devices such as tablets and still be able to perform powerful computing processes.

One of the biggest markets could be college campuses [4]. The current paradigm we reside in has students making the decision between large laptops with more computing power and the small laptops that are portable and easy to carry. Due to the large amount of traveling that many college students endure, many students find the less powerful, more portable option more inviting. Yet, what if they did not have to make the choice? Instead, the campus could host servers to allow student to lease computing power to create a more flexible computing environment while not making the students carry heavy computers around campus.

This has been the primary motivation behind the adoption of this project by two senior students as their senior capstone project. In this paper, we provide highlights of the challenges, successes and results. The purpose of the project was to virtualize the Telecom, Networking and Security (TNS) Lab in our college. Currently the lab is outfitted with 24 stations for students to use. Each station consists of a desktop running Linux Ubuntu and an iMac. Students use VMware Workstation: a local resources virtualization environment. VMware Workstation is an excellent program that allows students to deploy multiple operating systems with multiple types of network interface adapters that allow for an agile and flexible way to teach students networking, security and telecommunications concepts in a hands-on lab.

The issue with using VMware Workstation is that it requires a large amount of resources to be available on each of the workstations in the lab. Each desktop must be constantly upgraded to handle the demand. This is not efficient. It limits students to working on a single desktop where their work is saved, which is subject to tampering by other students looking to finish their own work. It is also wasteful. Students only need the full extent of the computing power available at their machine for short time. Most of the time the computing power sits idle, unable to be shared across the lab. To address these issues, two senior students took on, as their capstone senior project, the task of migrating from VMware Workstation local and distributed environment to VMware vSphere suite [5] central environment.

vSphere is a cloud computing and virtualization product by VMware that allows users to create virtual machines and access them on any physical machine, or client, on the network. This system is more efficient than over VMware Workstation. First, it allows for the consolidation of resources, meaning that upgrades to CPU and memory are made to one machine, not all of the workstations in the lab. Second, it allows the dynamic allocation of resources among the groups, allowing for the full use of processing power and not allowing it to sit idle on a single machine. It also allows students to have a secure environment by allowing each student access to a personal work environment, free from tampering by other students. Third, it allows them to access their VMs and work from anywhere in the college building. Furthermore, the use of vSphere allows instructors to rapidly set up environments, monitor classroom progress, and maintain the current state of the classroom work.

However, the issue with vSphere is that it has been applied primarily and used in academic classrooms for system administration [6] and not for teaching hands-on networking classes. As is, it lacks networking the robustness that is found in the VMware Workstation software. It is well

known that vSphere has not been designed for dynamic networking, in which each user would be able to control and manipulate multiple VMs, vSwitches and appliances. Also, it has not been offered for a hybrid physical and virtual networking arrangement for a user or a group of two or three students. To successfully realize the objectives of the project, we supplemented the vSphere networking capabilities to meet the needs of the hands-on Telecom, Networking and Security classes and labs. In other words, we ***repurposed*** the vSphere software suite to take advantage of its efficiency, while also enhance its networking robustness to match VMware Workstation networking capabilities.

This paper is organized as follows. In section 2, we provide an overview of the project goal and objectives. The project solution system architecture is detailed in section 3 while section 4 focuses on the project solution implementation. Examples of networking labs implementation are illustrated in section 5. In section 6, we offer our conclusion and potential future work.

2. Project Goal & Objectives

Original goal and objectives:
The initial goal of the project was to create a robust and supportive environment to support the teaching and learning environment of the Telecom, Networking and Security (TNS) classes offered by the College of Science and Engineering (CISE) at James Madison University.

The objectives of the project were to:

- Create a central virtualization learning environment using VMware vSphere suite for teaching hands-on networking courses to replace the current desktop VMware Workstations,
- Increase access to and the running speed of the TNS Lab learning environment,
- Enable instructors to rapidly and easily configure the central virtual teaching environment in support of TNS hands-on networking classes, and
- Provide for each student team a secure learning environment to prevent the potential of accidental corruption of their work by other individuals or groups.

A vSphere software suite license was made available to us by the VMware organization under the VMware Academic Program [7]. To start, we evaluated a number of server configurations to meet the expected traffic, processing demands and storage needs. Two Dell Precision T7600 tower servers, each fitted with dual Xeon E5-2630 CPU's, 256 gigabytes of RAM, 2x10G NIC and 3 TB's of storage were selected and purchased by the department.

Additional Objectives
After the servers had the VMware vSphere ESXi and vCenter software installed, we configured the software for implementing the first hands-on networking labs. We discovered a series of challenges in the vSphere virtualization environment, however. The vSphere suite did not have networking capabilities equivalent to the VMware Workstation environment. First, vSphere Standard vSwitches, unlike the vmnet switches available on VMware Workstation, neither support Dynamic Host Configuration Protocol (DHCP) nor Network Address Translation (NAT). Although, vSphere has a Distributed Switch object with DHCP capability, it was not available to us under the VMware Academic License Program. Second, there was not a way to enable each virtual machine on the ESXi to have access to one or more of client hardware devices such as 802.11 Wireless Network Interface for each individual client or group. In other words, we did not

have a way to integrate external hardware network devices with the VMs running on the vSphere/ESXi host for each team of students.

As a result of these issues, we decided to update our objectives to include the following:

- Supplement the Standard vSwitch networking functionality of the vSphere suite with DHCP and NAT capabilities for each student group, and
- Fully integrate the client external networking hardware devices of the VMs on the vSphere/ESXi for each student group.

3. Solution System Architecture

VSphere 5.5 Suite Virtualization Environment

The various components of the virtualization environment platform known as vSphere suite are as follows [5]. The black boxes at the bottom of Figure 1 represent the Dell Machines running the ESXi hypervisor platform. The virtual machine run on top of the ESXi VMware infrastructure. The vCenter provides administrative and resource management to the resources running on the ESXi platform and could be hosted either on a separate machine, from the ESXi or as an appliance within the ESXi environment. At the very top, Figure 1 shows the desktops running vSphere Web Client (also known as client) that connect and make use of the VMs. They also can pass through some of their hardware devices to the VMs.

ESXi is a bare bones hypervisor software of the VMware vSphere software suite. It is the foundation of the system and is directly installed onto the Dell server that is used to host the software. It is possible to interface with the ESXi in one of two ways. For the initial setup of ESXi, we connected a monitor directly to the server. In this case, we were presented with a minimalistic Graphical User Interface (GUI) that allowed us to set up the basic operational features such as the networking interfaces and basic administrative configurations. We could also access the server via the vSphere client. It is Windows-based application that allows access to the datastore (see Figure 3) and VMs running on the ESXi host.

VMware vSphere Suite also includes another software component known as vCenter; it is a separate software from ESXi hypervisor. It is used in conjunction with ESXi to enhance the administrative and resource management of the vSphere Suite. It acts as a middleman: a facilitator between the clients and the ESXi server. One of the key functions made available by vCenter is the vSphere Web Client. This could be viewed as a replacement of the vSphere Client. The vSphere Web Client, unlike vSphere Client, is a cross-platform tool that allows users and administrators to access the ESXi server via a web browser; that is, without the need to install the outdated standalone “thick” vSphere Windows-based client.

An integral part of the vSphere Web Client is the components known as the Integration Plug-in. It is a portal that allows vCenter/ESXi to interface with the hardware running on the client machine (e.g., desktop). For example, via the Integration Plug-in, a client can integrate into its assigned virtual machines the physical hard drive, serial or USB ports residing on the machine running the vSphere Web Client (or client for short). This feature is also known as client Devices Passthrough.

A key networking component of vSphere Suite is known as the vSphere Standard Switch (vSwitch for short) [8]. It is a virtual switch that can be configured on ESXi and is managed by the vSphere Client or the vSphere Web Client through the vCenter server. It works much like a physical Ethernet switch. It detects which virtual machines are logically connected to each of its virtual

ports and uses that information to forward traffic to the correct virtual ports and machines (See Figure 2). A vSphere Standard Switch (vSwitch) can be connected to a physical switch via the host physical Ethernet adapter, also referred to as uplink adapter, to join virtual networks with physical networks.

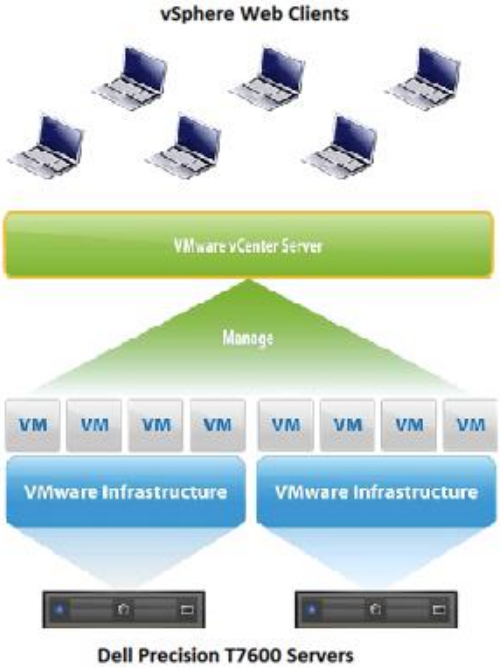

Figure 1. VMware vSphere Suite Virtualization Platform

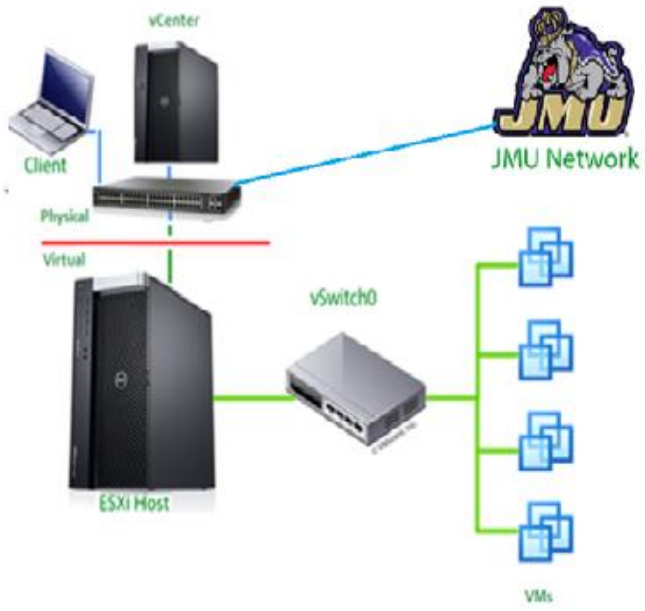

Figure 2. Typical vSphere Suites Environment

4. Solution Implementation

Installation and configuration of vSphere Software Suite

Initially we installed ESXi 5.0 on the Dell Precision Servers, assigned the Network Interface Cards (NICs) static public IP addresses and connected the server directly to the University public network. However, we faced numerous challenges during the installation of the vCenter 5.0 on a separate machine and integrating it with the ESXi host. For example, we had an issue with the web client not finding the proper port on the ESXi to route traffic to the SSO (Single Sign On) service on the vCenter server to allow users to log into the system. This was a critical issue for us since we wanted to take advantage of vCenter integration (see later) with the University Active Directory (students' credentials).

In our search for solutions to these challenges, we realized that we had access to the latest vSphere 5.5 suite under the VMware Academic License Program. We decided to install and run vCenter 5.5 as a virtual appliance on the ESXi hosts to reduce the hardware costs (eliminating the need for a separate desktop) and speed up the response time of the vSphere Web Clients. However, we found out that ESXi 5.0 was not compatible with vCenter 5.5. When reinstalling ESXi 5.5, we chose to put the server on a private network in the Telecom, Networking and Security (TNS) lab. We avoided issues with port blocking on the University network, which had been a source of delays and frustration. The private network allowed us to set IP addresses as we needed them and avoid the need for constant negotiation for opening ports on the University access control application. The ESXi and vCenter servers were given static private IP addresses by a Wireless Access Point

that we configured and dedicated for the use with this project.

To complete the installation of the vCenter appliance to manage the ESXi host, we needed to create and name a new data center under the localhost location, which is directly associated with our vCenter instance (see Figure 3). Under the Datacenter, we added our ESXi host using the ESXi assigned static private IP address. In addition, we made a change to the layout of the hard disk on the Dell Server. We made sure to partition it so that the boot image resided on one partition and the VMs stored in the datastore on a different partition. This results in a noticeable improvement in the I/O performance of the overall vSphere environment.

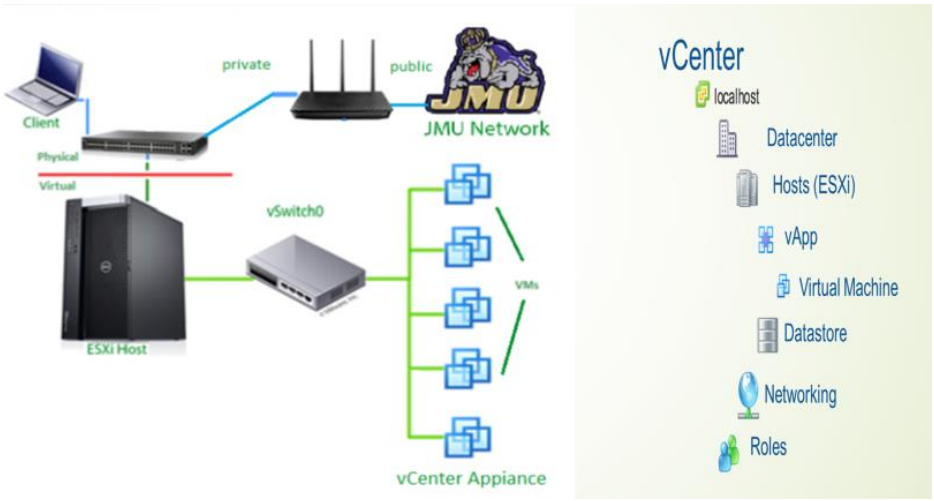

Figure 3. Model for rapid Deployment

Model for Rapid Deployment

A key objective of the project is to rapidly deploy new and existing networking and security labs. Towards realizing this objective, we identified and implemented the following capabilities:

Integration with University Active Directory

To create a model for rapid deployment, we needed to find a way to add and set the roles of students with minimum effort. The vCenter server keeps all of the information such as the users, their privileges, and which VMs belong to them. It also provides the GUI that the users make use of to utilize the hardware of their client machine (via the Passthrough functionality). At first, we added users manually to the local vCenter server. We found this to be tedious and time consuming. So we looked into ways of integrating our vCenter server to the University Active Directory (Univ/AD).

Active directories at James Madison University are used to authenticate users over a larger variety of applications including student ability to log into the campus computers and applications. Although our vCenter server was behind a NAT, we were still able to connect the vCenter server to the Univ/AD. As a result, we were able to make use of the University Active Directory and the information that it stores to add the students (users) to the vCenter. This integration allowed an instructor to just add new users to the system and not have to create them on the local server and maintain a separate list of the users of each class. By binding the vCenter server to the University active directory, students could log into the vCenter server using their Student eID and password.

Roles, User Permissions and Privileges

We also defined roles on the vCenter server, one for the students and another for the instructor and administrator. The students had the permission to change any settings on the virtual machines contained in their vApp. A vApp is a collection of resources that can be assigned to a user and can contain VMs, appliances and vSwitches. As a result a student group would not be able to see or access objects on the server outside of their own vApp. The instructor or the administrator has access to vApps, vApp templates, VMs, VM templates, vSwitches and computing resources on the ESXi host. Designating these roles to the users on the vCenter server significantly enhanced the operational effectiveness and robustness of our deployment model. Another enhancement we applied, in addition to adding the users in the vCenter server via the integration with the University Active Directory, is the ability for the instructors to define groups to which users can be added. Each group can be granted specific privileges which are passed down to the users in the group. Groups are allowed to create networks on their vSwitches but are not allowed to have access to the vSwitches of other groups.

vApps and Resources Pools

vApps and Resources Pools [5] software applications are made available as part of the vSphere, vCenter and ESXi software suite. These are software applications (or objects) perform roughly the same task, but yet are different. The Resources Pools are simply that: they can be allocated to a user of the software and limit the total resources available to that user. vApp provides that same functionality, yet it also provides the functionality to deploy a template and re-deploy an entire vApp package. A vApps is a container of resources that can be assigned to a user or a group and offers resource controls and management for the virtual machines and other appliances (such as Untangle DHCP/NAT Server/appliance [9]) that are part of the vApp definition. An entire vApp could be cloned, powered on, powered off, suspended, or shutdown. After exploring both the Resource Pools and vApp applications, we chose the vApp for the following reasons: (1) the rapid creation and deployment of vApp OVA files (OVA is a file that can be exported and used to replicate an entire vApp) and (2) the ability to maintain an environment where each group is only allowed to configure their assigned resources within their assigned vApp.

We were able to build a model that could save the instructors a significant amount of time when deploying new networking and security labs. The following is a brief description of the model. An instructor starts with the creation of one or more virtual machines that would meet the needs of the students throughout the semester. Using these VMs, the instructor would create VM templates which are files stored in the datastore on the server. These templates could be used by the instructor and/or the students (if permitted) to create new VMs without the hassle of going through the entire ISO installation process. Once the instructor decides on the additional resources (such as Untangle appliance and/or vSwitches) that are dictated by the networking design, the next step is to create a vApp package and export that vApp to an Open Virtual Appliance (OVA) [10] template. OVA is merely a single file distribution of the same file Open Virtualization Format (OVF) package, stored in the TAR format. The OVA file can be used by an administrator to recreate and clone an entire vApp environment for each of the student groups in a class with relatively few steps. It is definitely so much easier and less time consuming than using VMware Workstation to deploy so many virtual machines for each group on the desktops.

Repurposing vSphere 5.5 for Networking Labs
vSphere 5.5 Networking Limitations

At first we thought that the vSphere Suite 5.5 system is equivalent to VMware's Workstation for Desktop Computers, where we would have the same ability to change network connection types (Bridged, NAT and Host-Only) and turn on or off a built-in DHCP capability [11]. Unfortunately, that was not the case. Although we found a vSphere application called Distributed Virtual Switch (dvSwitch) which is advertised for networking across multiple ESXi hosts, it turns out to be an incomplete solution, overkill for meeting our needs and requires license fee beyond the available funding to the project.

Another major issue that we faced in planning the migration from the VMware Workstation to the vSphere environment was that we were no longer able to take advantage of the physical Ethernet port built into the client machine. Initially, we thought the problem could be resolved through the use of vSphere Web Client Integration Plug-in. The Web Client Integration Plug-in allows some of the physical devices (such CD/DVD Drive and USDB ports) on the client machine (used to access VMs) to be passed through to the user's VMs. Unfortunately, after consulting with VMware, we found that it was not possible to pass through certain hardware devices such as Networking Interface Cards (NICs) which is a critical device in the integration of the virtual environment (inside the vSphere platform) with many of the physical devices outside the vSphere virtualization environment.

Up until this point we held onto the VMware Workstation as our reference of how we want to configure and deploy vSphere Suite. Confronted with the above issues, we had to recast our mental model of vSphere suite and how we should go about configuring its components to achieve our goal of migrating the hands-on networking labs from the decentralized standalone VMware Workstation environment to the shared centralized vSphere Suite environment. To make the project a viable replacement for the current configuration, we needed a way to

- Provide DHCP and NAT functionality for student groups on the vSphere Suite platform
- Pass through the Client Network Interface Card (NIC) to the VMs assigned to the student groups

Addressing the Networking limitations of vSphere Suite

Dynamic Router with NAT and DHCP Functionality

To resolve the first problem, we need to add the NAT and DHCP capabilities to the vSphere Standard vSwitch. The main virtual switch on the server (typically labeled as vSwitch 0) is used for bridged connection with the host. Since we wanted to keep all of the groups separated, we created a Standard Virtual Switch and Port Group for each of the student groups. After looking into a few software packages and appliances (Pfsense, Cisco iOS, Untangled) we chose Untangled to provide the NAT and DHCP functionality for a number of reasons. First, it is a free software. Second, it gives almost the same overall looks and feel as the firmware of a traditional Wireless Home Access Point such as DD-WRT or Tomatoes. Third, it has a GUI that the students could access through the NAT gateway interface from one of the VMs connected to the "inside" bridge of the NAT. The GUI allows the students to readily manage the NAT and DHCP settings without having to directly access the Untangled VM appliance. Note that the Untangle DHCP assigns private IP addresses on the NAT-inside interfaces just as a physical wireless router (Access Point) does on the LAN side. Figure 4 shows the network topology that we created to demonstrate how the Untangle DHCP and NAT functionality can be added to each group's vApp environment and package. The red line in Figure 4 signifies the demarcation between the physical and virtual networking environments.

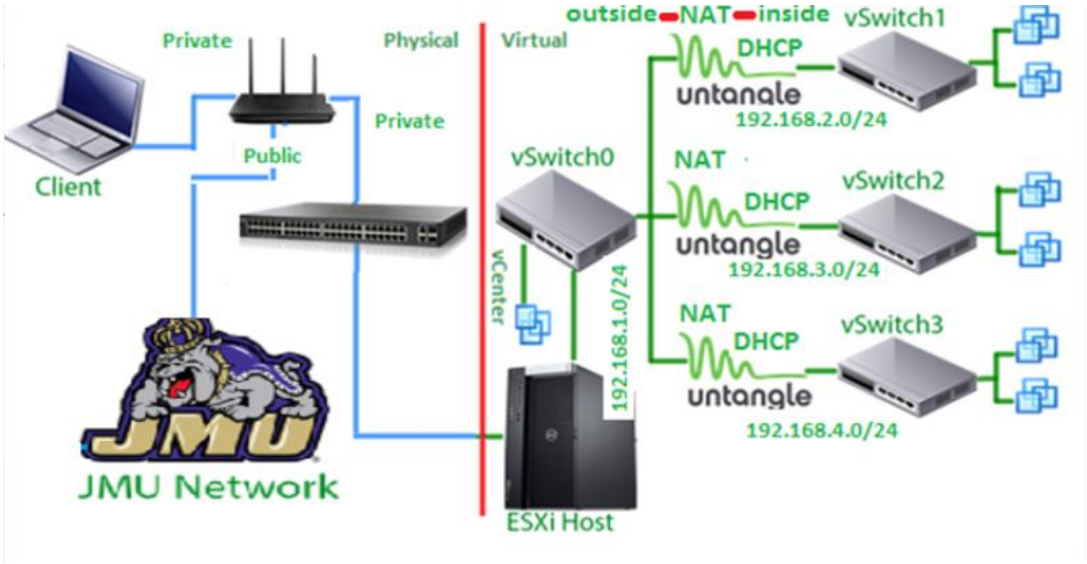

Figure 4. Network diagram including Untangle Virtual Appliance with NAT and DHCP

Integrating Client Hardware Devices to VMs

To provide a solution to the second problem, that is, to enable the client to pass through the client machine Ethernet port to the VMs, we explored the Web Client Integration Plug-in in slightly different way. Since USB ports are supported by the Web Integration Plug-in for pass-through to the VMs, we decided to use a USB to Ethernet adapter on the client (as shown in Figure 5). With the software driver for the USB to Ethernet adaptor installed on the client (for testing purposes)

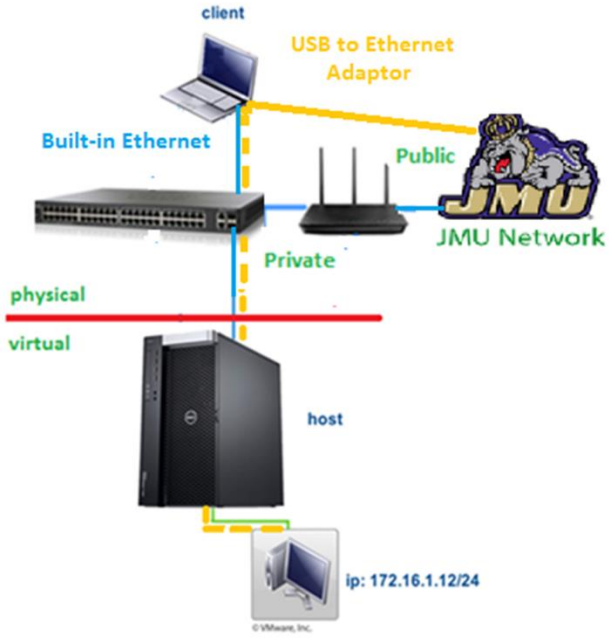

Figure 5. Connecting two VMs via Client Hardware Pass-through Capability

and the VM (for integration purposes), we were able to pass through an Ethernet port to the VM through a simple and inexpensive USB to Ethernet adaptor. This solution has allowed us to directly connect a VM to many physical devices on the client machine. For example, we

successfully passed through to the VMs on the ESXi USB wireless adapters plugged into the client machine.

5. Examples of Networking Labs Implementation

After resolving the networking limitations of the vSphere suite software, we were able to complete most of the hands-on networking labs that are in use today as part of the Telecom, Networking and Security (TNS) sector and concentration classes using the USB to Ethernet adaptor pass-through and the Untangled DHCP and NAT appliances. The following networking and security lab examples are provided here to demonstrate how these new capabilities have been applied in performing the TNS labs on the vSphere repurposed environment.

Lab 1: Connecting two VMs via an Ethernet Cable

This is a basic lab that new TNS (Telecom, Networking and Security) students are required to perform in their first introductory networking class. Here, they connect two VMs via an Ethernet cable. The goal of the lab is to show the students that one does not need a switch or a router for two computers to communicate with each other. In addition, they are introduced to how to configure static IP addresses and subnet masks on the network adaptors. We wanted to recreate the experience of connecting two machines (in this case two VMs using a physical Ethernet cable. So we took two USB to Ethernet adapters, plugged them into the client computer, and passed each them to a VM on the ESXi server. Figure 6 shows the network topology of the setup. The second part of this lab is for the students to connect the VMs to a physical Ethernet hub. In this case the

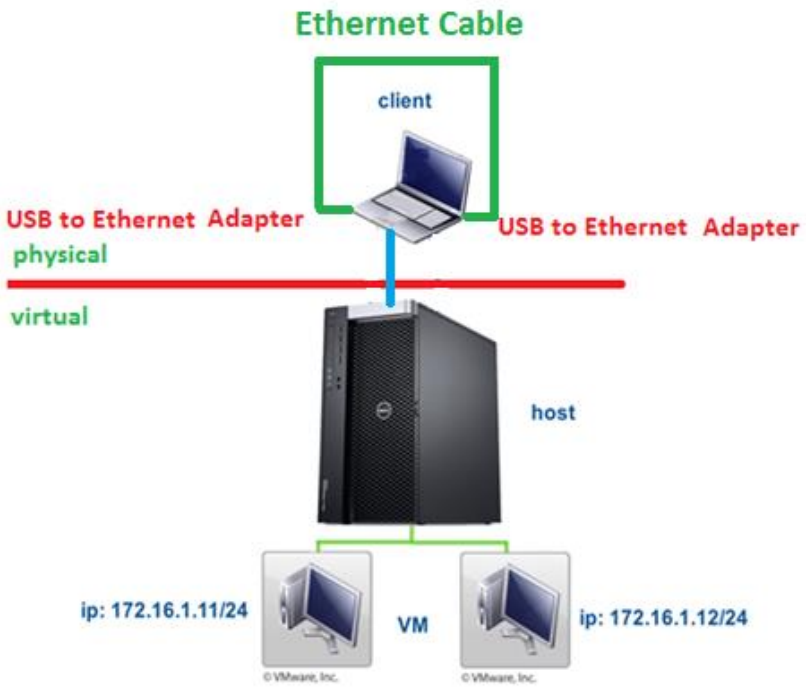

Figure 6. Connecting two VMs via Client Hardware Pass-through Capability

students would have the ability to add a third VM or a physical computer to monitor the traffic exchanged between the first two VMs. This demonstration should help the students to a better understanding of the virtualization and networking environment.

Lab 2: Web Services and Web Hosting

Not only is vSphere an effective way to create a more flexible and agile learning environment, it also allows the instructors and students to configure and create on-the-go web servers for their projects. In one specific networking class, the students are tasked with building an end to end hardware/software working application. The class is divided into front end (User experience/mobile app), middle component (database and web servers), and back end (Arduino/Sensors and/or Raspberry Pi/Sensors) and application integration sub-teams. The members of the sub-teams apply most of the skills they learnt in the TNS & Information Knowledge Management (IKM) sectors and concentrations. During the development of these projects, the students typically would select a computer in the TNS lab to run their database and web servers. A problem comes up when a student from another group or class, even if unknowingly, make changes to the machine that may impact the project web server operations and functions. With vSphere that cannot happen. Now the instructor and administrator of the course can allocate isolated and secured resources to the project that are configured so that they can be accessed only by the web server creator and maintainer. We have also configured the network in such a way that all IP addresses from 192.168.1.40 to 192.168.1.49 are set aside in the Access Point to allow students to statically set the IP addresses of the web and database servers. Figure 7 shows a basic network topology that has been created to demo the above described scenario. The web server VM is assigned a static IP address (reserved and managed by the AP) and is bridged onto the host machine via vSwitch0. The AP facilitates the connection from the client to the vSphere suite via LAN (802.3) or WLAN (802.11).

Figure 7. Web Server & Services Network Topology using the re-purposed vSphere platform

Lab 3: Connection to Wireless AP and Penetration Testing

In this example, we used a virtual machine to perform 802.11 (WPA/WPA2 personal) wireless penetration testing as shown in Figure 8. We were able to pass through a USB wireless adapter on the client machine to the Backtrack VM on the server via vSphere Web Client Integration Plug-in. The attacking Backtrack VM has also been placed in monitoring/sniffing mode and thus allowing the machine to scan for wireless traffic. To start the de-authentication attack, we used a program called airmon-ng to listen for 802.11 packets. Once we identified our victim; a wireless client (MacBook) connected to the access point and configured for Personal WPA/WPA2 security mode, we launched the de-authentication attack. This attack forced the MacBook to disconnect from the Access Point. We stopped the de-authentication attack to allow the MacBook machine to reconnect to the AP. Upon reconnecting to the access point, the attacking VM (Backtrack) was able to capture the WPA/WPA2 authentication handshake. Then, we ran offline aircrack-ng to crack the pre-shared key with the help of a wordlist dictionary available on Backtrack. The successful completion of this lab confirmed that the repurposed vSphere environment is capable of supporting sophisticated security and networking labs.

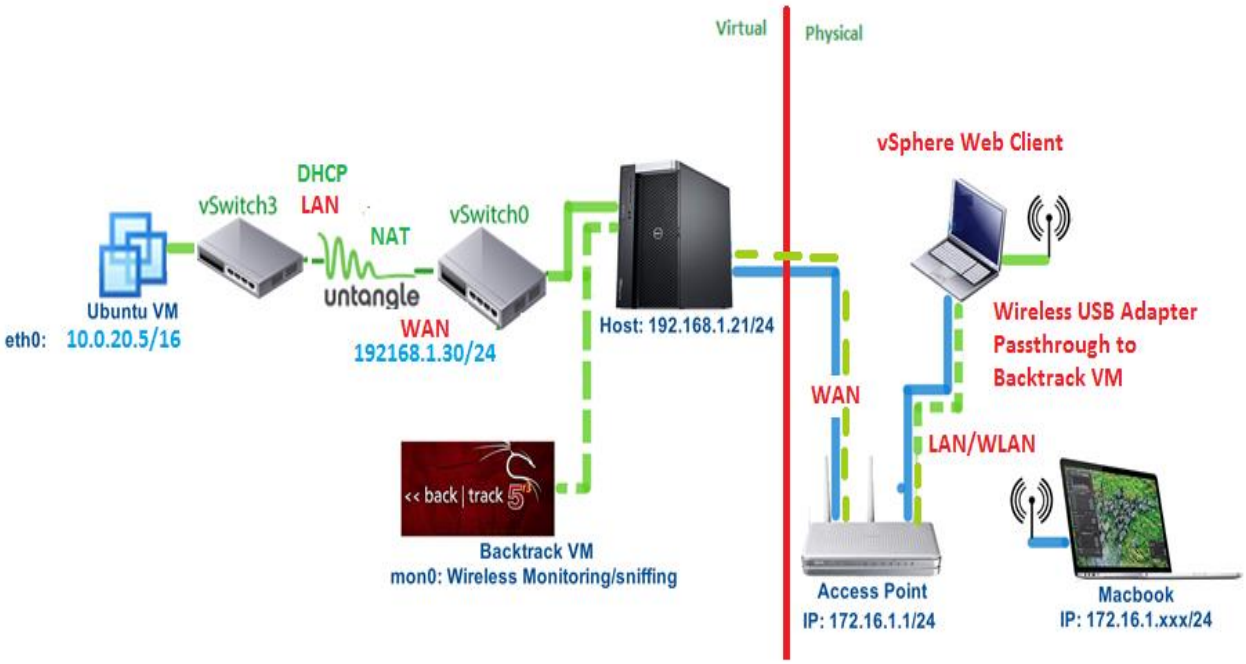

Figure 8. Hybrid Physical and Virtual Network Topology for 802.11 penetration testing

.

6. Conclusion and Future Work

The year-long project to virtualize the TNS lab presented us with many challenges. However, at the end, we gained a diverse, strong understanding of cloud computing represented by the VMware vSphere Suite and how it could be applied in teaching hands-on networking and security classes. We acquired strong working knowledge of how to integrate the vCenter to the University Active Directory (AD). This was a great contribution to our professional knowledge as ADs are used widely in the business and enterprise environments. Having the chance to work with the University networking team gave us a greater understanding of the real world operational issues and challenges. While some of the methods did not work right from the first time and we had to go back to the drawing board many times over, we were able to work through most of the

challenges using effective research techniques, taking chances and making mistakes until we eventually delivered a successful project.

After completing this project, we found that we were able to successfully virtualize the TNS lab without losing any functionality with the VMware Workstation environment. In fact, we actually gained many new functionality most noticeably rapid deployment of labs and efficient management of computing resources. By creating our own deployment model, networking architecture and using elements such as the Untangle appliance and USB to Ethernet adapters, we found that we were able to get the environment to perform tasks with the vSphere suite that we have not seen done before.

With the architecture now deployed and able to be used by the students, we have found that the Lab experience appear much more pleasant and the ability to perform new networking arrangement that were previously not possible has the creativity of the students on a higher level. By completing this project the learning experience in the Lab has been elevated for the students and the effort and time required by instructors and administrators to set up and manage the Labs have greatly reduced. We will continue to collect quantitative assessment data for future publication. In conclusion, we have successfully accomplished the objectives of the project as stated in section 2 of this paper.

Here is a list of potential future work that we, as a department and college, will continue to pursue:

- Experiment with advanced storage and I/O hardware and software to continue to improve the speed and reliability of the TNS lab
- Incorporate the use of thin clients via Horizon View. This would help in the consolidation of resources by ridding the lab of expensive desktops and replacing them with inexpensive thin clients
- Introduce Dynamic DNS to the virtual environment as a way of enhancing the flexibility of the system for rapid deployment
- Introduce additional appliances, such as Cisco (Cloud Services Routers), Vyatta route appliances, VoIP Private Branch Exchange (such as Asterisk), Nagios Net Monitoring, Firewalls (such as Smooth wall), and more
- Establish a VPN support that would allow students to gain access to their workspace from off-site locations
- Explore VMware vCloud. It should allow for more advanced routing and more robust networking
- Explore the application of VxLANs (Virtual Extensible LAN) across hosts

Acknowledgment
The authors would like to thank the Integrated Science & Technology (ISAT) Department and James Madison University for the fund granted for purchasing the two servers so that this project could be completed, without them this project would not have been possible. We would like also to thank Chrissy Rothgeb and Livia Griffith for helping us implement the active directory integration and spending the time and effort that made this project a success. Many thanks go to the VMware support team and online communities that have been proven invaluable to us in the successful delivery of this project.

Bibliography
[1] Sultan, N., Cloud computing for education: A new dawn. *International Journal of Information Management, 30,* 109-116.
[2] Vouk, M., Cloud Computing - Issues, Research and Implementations. *Journal of Computing*

and Information Technology, *16*, 235 - 246.
[3] Khmelevsky, Y. & Voytenko, V., Cloud Computing Infrastructure Prototype for University Education and Research. *Proceeding WCCCE '10 Proceedings of the 15th Western Canadian Conference on Computing Education*, *1*.
[4] Cisco, "College Lowers Desktop Costs in Computer Labs by 30 Percent with Virtual Desktops." *Cisco*.
http://www.cisco.com/c/en/us/products/collateral/unified-communications/7800-series-media-convergence-servers/case_study_c36-717074.html, Retrieved Wed. 4 April 2014.
[5] VMware vSphere 5.5 Documentation, https://www.vmware.com/support/pubs/vsphere-esxi-vcenter-server-pubs.html
[6] Wang, X., Hembroff, G., & Yedica, R., Using VMware VCenter Lab Manager in Undergraduate Education for System Administration and Network Security. *SIGITE '10 Proceedings of the 2010 ACM conference on Information technology education*, 43 - 52.
[7] VMware Academic Program, https://labs.vmware.com/academic/licensing-overview, Retrieved January 2015.
[8] vSphere Networking - vSphere 5.5 - VMware Documentation, http://pubs.vmware.com/vsphere-55/topic/com.vmware.ICbase/PDF/vsphere-esxi-vcenter-server-55-networking-guide.pdf, Retrieved December 2015
[9] Untangled Users Guide. (2013, August 15). *Untangled Users Guide*. http://wiki.untangle.com/index.php/User_Guide, Retrieved April 1, 2014,
[10] Damian Karlson, OVA's and OVF's: What are they and what's the difference? https://damiankarlson.com/2010/11/01/ovas-and-ovfs-what-are-they-and-whats-the-difference/, Retrieved January, 2015
[11] VMware Workstation 11.0, Using VMware Workstation, http://www.vmware.com/support/pubs/ws_pubs.html, Retrieved January 2015