Sushil Chand Chaudhary

Design and Implementation of a Virtualized Home Network Education Environment

Helsinki Metropolia University of Applied Sciences

Bachelor of Engineering

Information Technology

Thesis

8 June 2015

Helsinki Metropolia University of Applied Sciences

Author(s) Title Number of Pages Date	Sushil Chand Chaudhary Design and Implementation of a Virtualized Home Network Education Environment 38 pages 8 June 2015
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Networking
Instructor(s)	Juho Vesanen, Lecturer

This project aimed to present and implement the virtual technology that would allow a media engineering student to access the individual PCs in the virtual environment to perform their lab exercises. The project was planned to be done in two parts.

The working of the project in the first part was to create and test the virtual network in a small scale environment. A simple virtual network was created and tested with the help of a single virtual router, virtual switches and two virtual computers as hosts in VMware Workstation 10. The second part was focused on implementing and scaling the virtual network in large number using VMware vSphere Hypervisor (ESXi). In this part, virtual network was created on a large scale with multiple switches and a router and installed in the server environment. The project was scaled and implemented to support a maximum number of students at the same time. The router and switches erased previous configuration automatically. This part was also focused for students to gain access to individual PCs in the virtual environment in a convenient way.

Successful design and implementation of the project eased the media engineering students to perform their lab exercises. This project was designed for basic networking lab exercises; therefore the student cannot work for advanced networking exercises in this virtual network environment.

Keywords	VMware ESXi, VMware Workstation ,router ,switch, IP

Contents

1 Introduction

The virtualization technology simply means moving a physical system in a virtual environment. It has become the most important factor today in the IT sector. The number of organizations and institutions adopting virtual technology are increasing rapidly. Today virtualization is being used by numerous growing organizations from educational organizations to scientific organization [1]. The idea of virtualization technology was brought to the field due to the limited resources and growing industry in the IT sector. The use of virtualization technology benefits an organization by reducing use of network resources, increasing security measures, manpower and hence providing economic benefits to organizations.

Virtualization technology allows to run multiple operating systems at a instance within a single computer. Virtualization separates a layer between hardware and software. The operating system uses the resources from the hypervisor not from the host hardware. Basically virtualization technology provides an ability to stimulate a hardware platform in the software which is installed in the hypervisor. Virtualization technology separates the connection of the software application from the host hardware component. Of course, there is a host hardware resource supporting the virtual instance (hypervisor). With virtualization technology, multiple servers can be consolidated into more powerful servers. Also, the multiple virtual machines can be grouped together to form a network within a single physical machine.

Virtualization has mainly three areas in the field of IT which is growing enormously: network virtualization, storage virtualization and server virtualization. In this project, network and server virtualization were the focus. The virtualization technology that was used in the project was VMware because the software and tools required for this technology were easily available at the school's webstore. VMware Workstation 10 was used to virtualize the network while the VMware ESXi server was used to virtualize the server.

2 Goals

The goals of the project were to build a virtual network where a student could use the network for educational purposes. The project was focused on virtualizing a typical home network, and it was based on the concept of the virtual network. The project provides readers with information about the virtual technology and differences between a physical home network and a virtual network. Below is the figure 1 illustrates the home network that every student or reader use when accessing the public Internet. The project was aimed to virtualize this type of a home network and allow the user or student to use it for educational purposes within the Metropolia Network in Leppävaara.

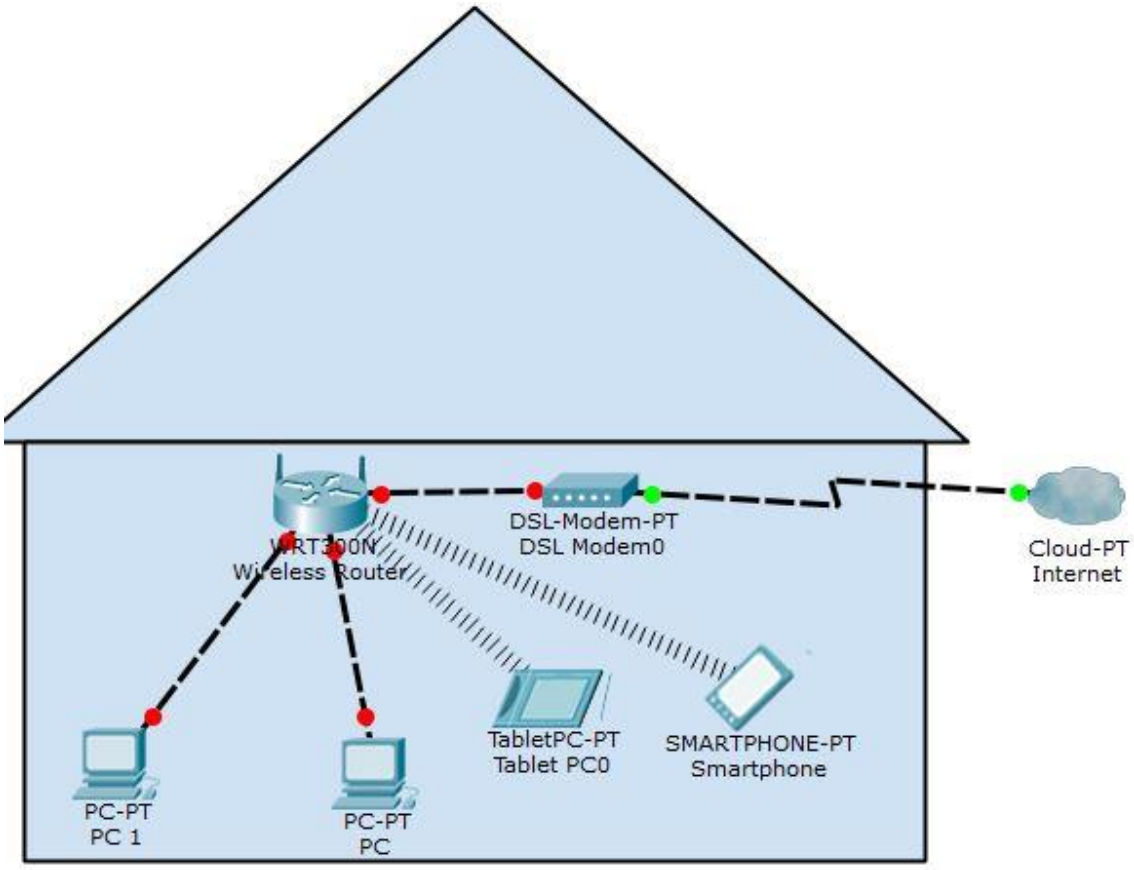

Figure 1.Basic Home Network

Referring to the above figure 1, the home network consists of a several network devices connected to the ISP (Internet Service Provider). The end user is the one who uses the enddevice to connect to the Internet. Every home that has an Internet connection contains modem depending upon the type of Internet connection. The modem can be a cable modem, DSL modem depending upon the type of subscription the user have. Today basically every ISP provides DSL subscription and every home has a point

which divides the network into a WAN (Wide Area Network) network and a Home network. In figure 1, a cable/DSL modem separates the home network from WAN network.

The above home network contains a home router and multiple end-devices connected to it. There are a number of home routers available in the market (D-link, Linksys). The Home router allows multiple end-device connections. There are many ports in the router, so that many network devices (printer, laptops, computer) can be connected at an instance. Without a Home Router only one device can be connected to the Internet at a time. The goal of the project was to virtualize the above home network type and apply it to the education environment. The project was focused on the Metropolia education environment but can be applied outside the Metropolia premises.

In the Metropolia education environment there are several courses regarding networking. The courses contain tasks related to IP networking. All the laboratory classrooms are fully equipped with modern routers and switches. The students starting the course are scared to use those switches and routers as they do not have enough knowledge and information. The Students also encounter cable problems when working with a real-device in a lab environment. Student within a low level of CCNA 1 knowledge cannot figure out problems and hence they are enforced to spend most of the time reconfiguring cable problems. Also, they have no idea if there is a power failure within the network devices. From the teacher perspective, there might be problems with a limited number of IP laboratory classrooms. CCNA1 course does not require routers and switches, but when the classrooms are reserved for CCNA level 1, it might create a problem in the lectures as the other high-level CCNA course requires modern routers and switches.

As a solution the CCNA classes could be carried out in normal class-rooms with computers. However, this does not meet the requirements, as computers in normal classrooms are connected to the Internet and students are not granted authorities to make any change in computers. So this project was carried in order to find a solution to the above problem. So it was necessary to design and implement a virtual network which could be a solution to the problem. Figure 2 Virtualized Home Network illustrates a solution to the above discussed problem.

.

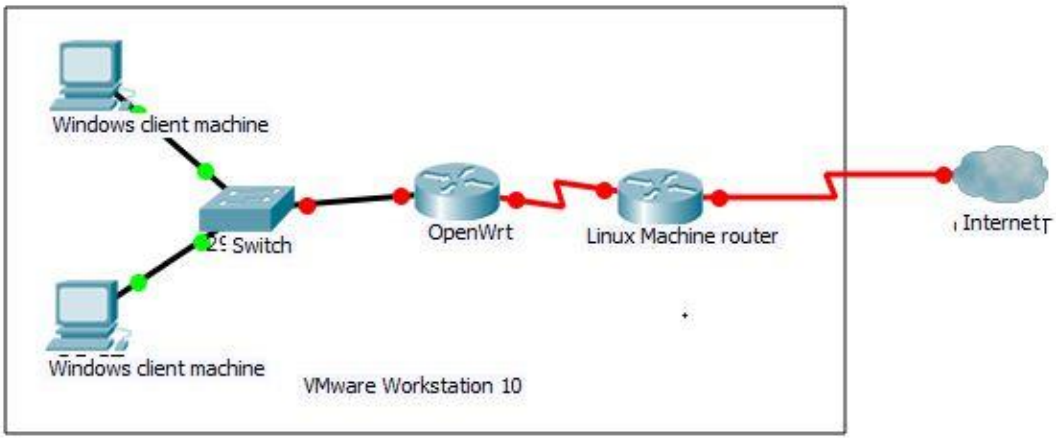

Figure 2.Virtualized Home Network

After virtualization of the home network discussed above, the virtual network resides in the single physical computer as shown above in figure 2. The virtualized network contains four virtual machines. The home router was replaced by Openwrt which was installed in the Virtual machine. The Virtual switch was created to connect the enduser device to Openwrt which is a router for end devices. The OpenWrt was connected to the Linux machine router.

In the project, a virtual lab environment was created for students to perform their basic laboratories. The virtual network was created in the VMware workstation 10 and copied on the VMware ESXi server. The idea of deploying virtual machines was to access the virtual machines remotely using the VNC (virtual networking computing) concept. The user can connect the virtual machines with the help of a VNC viewer which is described in section 4.2.4. The student now can get rid of the cable and layer 1 problems because the virtual machines are already configured and connected to each other. The student does not have to cable the network device which saves time and more effort can be put into learning than solving the cable problems. The students can also make network changes and settings on the computers. The computers were configured in the way that erases all the configuration and settings made by students and revert into the initial state after every reboot. Upon successful design and implementing of the project, lecturers can take their classes anywhere at Metropolia and allow students and lecturers to use the laboratories.

3 Theoretical Background

3.1 Network Virtualization

It is a technique to utilize the available network resources and combining hardware network resources and the software network resources to function as a single administrative unit [4]. The virtual network is the simple physical network except that the network is installed on the software. The virtual network only uses the resources of the existing physical network. The benefit of network virtualization is to get rid of physical layer problems and provide the user with efficient, controlled, and secure sharing of the networking resources [4].

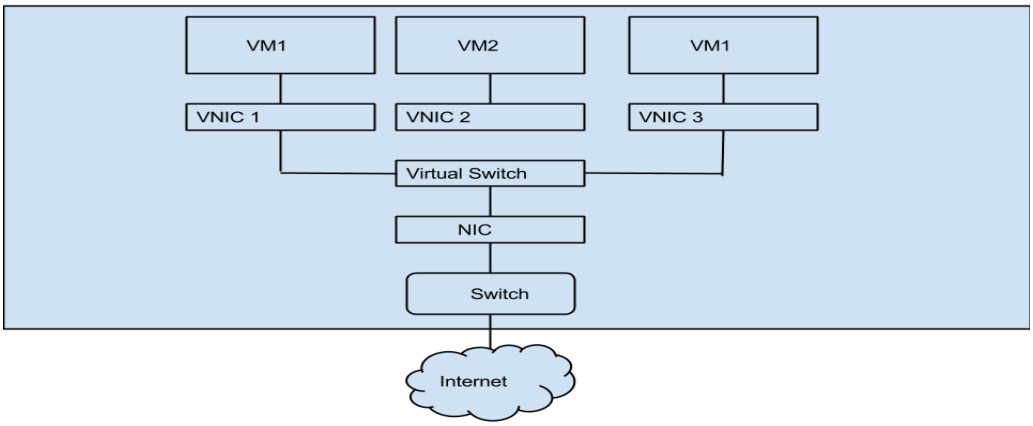

Figure 3.Basic Virtual Network

The above figure 3 is the basic virtual network created in a single host. The host is connected to the switch which is connected to the public Internet. The hypervisor VMware Workstation is running in the host. The virtual machines (zone1, zone2, zone3) are connected to virtual switch which is running within the physical host. There are two types of the virtualized network.

The External Virtual Network consists of several networks that are administrated by software as a single entity. The building blocks of classic external virtual networks are the switch hardware and the VLAN software technology. The External Virtual Network is created along with the physical network to allow the virtual machines to communicate

with the public Internet [4]. Virtual machines installed on Workstation and able to communicate with Internet are examples of the External Virtual Network

The Internal Virtual Network consists of several virtual machines running on the host computer. It can communicate with other virtual machines within the same network providing a virtual network on the single host. Virtual Network Interface card (VNICs) and virtual switches are the devices required in this type of network. These types of networks are built for the education testing purpose [5].

This project focused on how to create a virtual network during the initial phase of the project. The virtual network resides behind the physical network. The virtual network connects the physical network in several ways. The virtual network is connected to the external network via the physical network and the benefit of the virtual network is that it is unknown to the external network and any damages in the virtual network will not affect the physical network. The VMware workstation provides several ways to create virtual PCs and connect to the virtual network.

- Bridge Networking – These types of networking configures the virtual PC as separate computer on the network. This type of PCs are unware of the other virtual PCs in the virtual network. The PCs with the bridge networking enabled are connected to the virtual network adapter that lies in the physical network and can access the internet via physical network [6].

- Network Address Translation (NAT) - In these types of network connection, the NAT allows the virtual machines to access the network resources using the host´s IP address. When using the NAT, the virtual machine does not have its own IP address on the external network. Instead a separate private network is set up on the host computer. The virtual machine gets and address on the network from the VMware virtual DHCP server. The VMware NAT device passes data between one or more virtual machines and the external network [6].

- Host-Only Networking – These types of networking provides a network connection between virtual machines and the host computer. The virtual machine and the host virtual adapter that is created automatically when installing VMware are connected to a private Ethernet network. Addresses on this type of network to the virtual machines are provided by VMware DHCP server [6].

3.2 Benefits

Virtualization has mainly three areas in the field of IT which are growing enormously; network virtualization, storage virtualization and server virtualization. There are many reasons why virtualization is growing rapidly. The virtualization technology allows the business or offices to run with fewer resources while providing the infrastructure to meet the today's requirements. With this technology, the time spent in the administrative task can be reduced in day-to-day IT routine tasks such as adding and removing servers, or developing new applications. It also reduces the risk and data loss in the IT sector. It takes several hours to install an operating system on a desktop computer. However the virtualization technology takes a few minutes to copy same the virtual machine and create new virtual machines and function as a desktop computer, which saves time and effort. Many businesses, organisations and educational institutions losses the data during disaster, or emergencies. So virtualization can dramatically shorten the downtime of the IT services and improve the services significantly [2].

Space and cost factor are the next factors that push the organisation and institution to virtualize technology. The organisation running multiple servers and computers requires larger area and increase the operation cost of the organisation. With virtualization, the spaces used by several computer and servers could be reduced by running several computers on a server and reduces the operating cost of the organisation. It also helps in growing the awareness of the whole world towards power reduction and consumption. In this project, network and server virtualization will be focused.

3.3 Hypervisor

Hypervisor, also called a virtual machine monitor (vmm) is computer application software, firmware or hardware that offers a platform to create and run virtual machines. The physical machine (computer) on which a hypervisor runs one or more virtual machines is called a host machine. Each virtual machine is called a guest machine. There are two types of hypervisors (Type-1, Type-2) as described below.

Type -1 hypervisor runs directly on the computer's hardware. For this reason they are called bare metal hypervisors. A guest operating system runs as a process on the host. VMware ESX/ESXi, Citrix Xenserver are the examples of type-1 hypervisor.

Type – 2 hypervisor runs on the top of computers operating system. It abstract guest operating system from the host operating system. VMware workstation and VirtualBox are example of type-2 hypervisors.

3.3.1 VMware ESXi Server

VMware ESXi is a type-1 hypervisor which runs directly on the top of physical server. VMware developed ESX and ESXi server as a bare metal which mean it does not require operating system for installation. It runs only on the server with 64 bit with x86 CPU and at least 2 cores with minimum of 2GB of internal memory. It is an advanced, smaller-footprint version of VMware ESX server. This virtualization software creates and runs its own Kernel, which runs after the Linux kernel bootstraps the hardware. It is the most important part of vSphere. ESXi is the component used for the virtualization server. It is used to deploy the multiple virtual machines on it. Each virtual machine shares the same physical resources and can run instantly at the same time. The management functionality of the virtual machines can be done remotely [7].

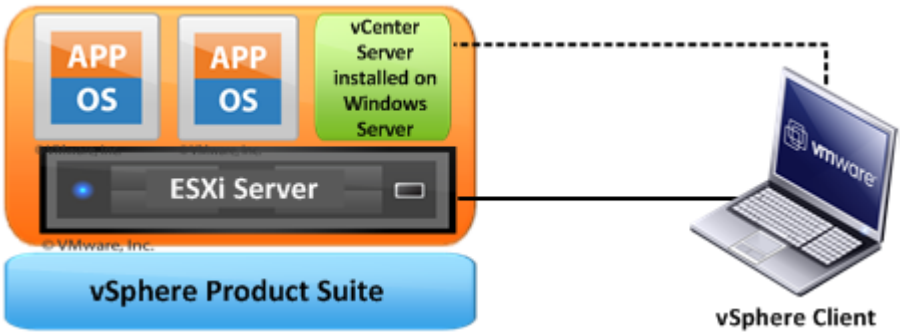

Figure 4.VMware ESXi Working , (Reprinted from VMware ESX and VMware ESXi) [8]

Figure 4 above shows the vSphere suite in more detail. ESXi is a hypervisor which is installed in a physical computer. vSphere Client is installed on the laptop or desktop computer which is used to access and manage the virtual machines running in the ESXi server. vSphere client is used to access the ESXi server directly in a small environment. To manage the ESXi server in larger environment which runs dozens of virtual machines, vCenter server is preferred [9].

To manage and access the virtual machines and server which run on top of the ESXi server, the other part of the vSphere suit called vSphere client or vCenter is required. It can also be managed through the console terminal. vSphere client is installed on the client machine (e.g administrator's laptop). The vSphere client is used from client machine to connect to the ESXi server and to perform management task [9].

VMware ESXi server has many features. Because of its features and high performance in the field of server virtualization, it has become the most used software for the server virtualization. Below listed are the key features of the ESXi server.

- The ESXi architecture uses service console for the management taks including the script execution and third-party agent installation.
- When compared to the ESX server, it has simple security profile configuration.
- It uses a small direct console user interface rather than a full server console.
- VMware Virtual Symmetric Multiprocessing (SMP) enhances virtual machine performance by allowing the single virtual machine to use up to eight physical processors, simultaneously [8].

ESXi needs fewer patches when compared to ESX, because of its more compact size and reduced number of components. This helps to shorten service windows and reduce security vulnerabilities.

The idea of implementing the VMware ESXI 5.5 in the project was to deploy virtual machines on the server. The virtual machines were copied from the workstation 10 to ESXi server. So users can access them from anywhere within the network. With the hypervisor type-2, they cannot be accessed remotely. The virtual machines created in the VMware workstation could not be accessed remotely because VMware Workstation 10 is a type 2 hypervisor. The virtual machines running on the ESXI host can be remotely managed, just by connecting to the server within the network. Additional security logging measures can be done when virtual machines are running on the ESXI host.

3.3.2 VMware Workstation 10

VMware workstation is a type-1 hypervisor that runs on x64 computers used for the desktop virtualization technology. It enables one or more virtual machines to run at the same time on a single physical computer. All the virtual machines share the resources form the host computer. VMware Workstation supports various operating systems like Windows, Linux, Mac OS as a guest operating system. It is one of the most popular products used for desktop virtualization. It is easily available for download on official webpage of VMware [10].

VMware Workstation 10 has new features that the previous version of VMware lacked. VMware Workstation has a feature to support Microsoft Windows 8.1. It has an extended hardware, which supports up to 16 virtual CPUs and 64 GB of RAM for a virtual machine. It has an additional HDD controller (serial ATA controller).Workstation 10 allow setting up the expiry time for the virtual machine, after which the particular machine cannot be accessed or started. The feature can be useful for testing purposes of the machines [11]. VMware workstation supports bridging existing host network adapters and shares physical disk drives and USB devices with virtual machines. VMware workstation includes the ability to designate multiple virtual machines as a team which can then be powered on, powered off, suspended or resumed as a single object, making it particularly useful for testing client-server environments.

The VMware workstation cannot be installed on a host computer when a VMware product exists. The only VMware products that can share the host system workstation are VMware vSphere client and VMware vCenter Converter Standalone. To install a VMware workstation, the user has to uninstall other VMware software installed on the host computer. The project computer had previously been installed VMware Player, so the VMware player was uninstalled and replaced with the VMware workstation. VMware Workstation 10 was used from Metropolia webstore for students.

3.4 Virtual Network Computing (VNC)

VNC is a Remote Frame Buffer Protocol (RFB) based technology for remote desktop sharing. It enables the desktop display of one computer to be remotely viewed and controlled over network connections. This technology is useful on a home computer, allowing users to access their desktops from another part of the house or while travelling. It is also useful for the home network. It works using a client and server model. A VNC client (VNC viewer) must be installed on the local computer and the server components must be installed on a remote computer [12]. VNC works similarly to the Remote Desktop application built into a newer version of Microsoft Windows. Unlike Windows Remote Desktop, VNC runs on older Windows computers, Linux/Unix and other non-Windows operation systems. The remote computer here refers to the virtual machines in the ESXi server which is explained below in section 4.2.4

VNC was created as an open source research project in the late 1990s. It was developed at American telephone and telegraph company (AT&T) laboratories. Since that time, several mainstream remote desktop solutions have been created based on the VNC. The original development team produces the real VNC package. Other popular derivatives include Ultra VNC and Tight VNC [12].The reasons for using a VNC system are given below

- VNC can be useful for the worker to access the resources of an organization remotely travelling abroad. The workers can access their files and documents residing in the home or office computer from anywhere. With this system, students or users forgetting their laptops can access their file and document from the universities computer when VNC is enabled. This system helps to save time and minimize losses.

- VNC technology allows the IT administrator, IT support and helpdesk to maintain the computer of the organization or company. This helps in reduction of the downtime of the IT services of a company and organization and thus helps in smooth functioning of the IT services.

- In educational institutions, a VNC system can be used to monitor student's computers by the teacher during an online exam. The teacher can monitor the exam by just using a computer. [13.]

The idea of implementing the VNC in the project was to access virtual machines running in the ESXi server remotely. With this application, the user can access virtual machines remotely anywhere within the Metropolia network. The user desktop or laptop should have a tool for supporting VNC. This task could be done via vSphere client. The vSphere client gives view of the virtual machines running in the ESXi server. Users are not permitted to manage every virtual machine running on the ESXi server. The students are only permitted to access the client computer. So it is better to use the VNC technology than a vSphere client to access the computer remotely.

3.5 VNC Viewer

The VNC Viewer is a component of VNC. It is supplied for the Windows platform. The VNC viewer for Windows is designed to run stand-alone without requiring any other packages to be installed first. To run the VNC Viewer, the user has to connect to the VNC server. Because of its wide range of features, VNC viewer was selected to be used for the VNC tools to access the virtual machines remotely.

VNC has cross-platform remote features which can establish a connection between two computers running different operation systems. The client running the Microsoft Windows operating system can connect to the remote computer running a Linux Operating system. This feature provides the user with the option to work with different operating systems. VNC is available in a wide range of languages providing user with option to work with the language they like. It is available in major language (English, French, German, and Spanish). VNC Viewer has authentic features with 128-bit AES encryption, so that only an authorized user can access the virtual machines and the server. The passwords are always encrypted. User can make a transfer of file in either direction or print document or files connected to the printers. The data transmitted in either direction between the computers are encrypted with 256-bit encryption and the data or information cannot be sniffed nor tampered. With these features, the VNC provides, it was best recommended to use VNC viewer as the VNC component to access the virtual machine remotely [14]. Figure 5 illustrates the VNC viewer tool taken from the project computer trying to establish connection to remote virtual machine.

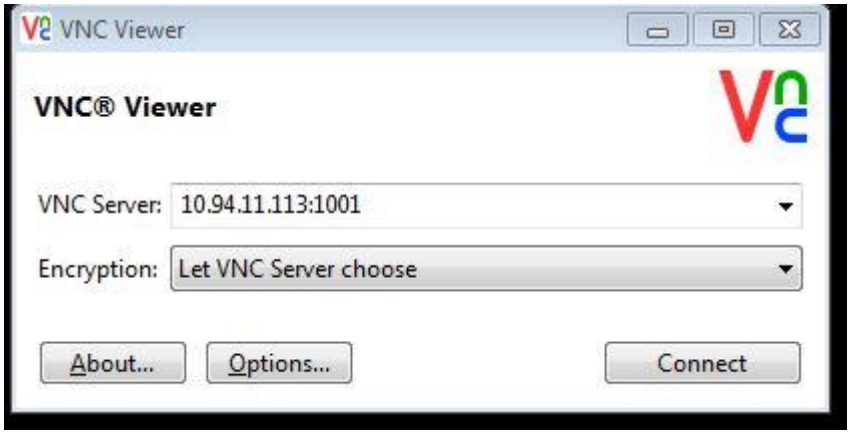

Figure 5.VNC Viewer connecting server

Figure 5 is a screenshot taken when connecting the VNC server in the laboratory. The IP address (10.94.11.113) in the figure is the IP address of the server which was VMware ESXi server as explained in section 3.3.1. The screenshot was taken from the client computer running the VNC viewer to connect the server. The number 1001 after the IP address is the port number of the virtual machine. Every virtual machine has a unique port number.

3.6 OpenWrt

The OpenWrt is an embedded operating system which is basically used for routing the network traffic in an embedded device. It is based on a Linux kernel and is an open router firmware. It provides a fully writable file system with optional package management which makes it easier to upgrade the router's operating system than to stick with the application and software provided by the vendor. OpenWrt provides a framework to build an application without having to create a firmware image and distribution around it. OpenWrt has been renowned as the best firmware solution for the embedded network devices in terms of performance, stability, extensibility, robustness and design. The open architecture of the OpenWrt enables the user to use packet inspection and intrusion detection which helps the user to save the resources which worth thousands of dollars. Currently there are more than 2000 software packages in the official repository. [15.].

Like home routers available in the market, OpenWrt has features apart from just functioning as a router. Below listed are the key features, that makes OpenWrt as the most popular firmware for the network embedded devices.

- The OpenWrt has a SSH server which can be used to for SSH tunnelling. This feature allows access to websites securely over public Internet. It also allows access to the website which is restricted to a certain geographical area while travelling abroad anywhere in the world.

- The Openwrt allows the user to perform traffic-shaping and the quality of services on the packets travelling through the OpenWrt. Similar to Home Router, it provides user with option to prioritize traffic to the specific computer connected to it.

- The User can capture and analyse the network traffic originating and passing through the OpenWrt. This feature helps to monitor and analyse the network traffic.

- The Openwrt has asoftware repositories that contain packages allowing it to function as a web server, IRC server and BitTorrent tracker. It can be wise to use OpenWrt as a web server than a computer avoiding excess use of power, because router consumes less power than a computer.

- OpenWrt helps to set up VPN (Virtual Private Network) similar to SSH tunnelling described above. [16.]

In the lab, one of the virtual machines runs OpenWrt as a guest operating system. The idea of using OpenWrt was to act as a DHCP server for two client virtual machines. OpenWrt can be managed from the command-line, by logging it via SSH, or by using it by web-based interfaces from the browser. OpenWrt also includes BusyBox which includes a number of common command-line utilities, like Vi editor. It can be managed by the IP address 192.168.1.1 from the web-based interface.

3.7 Virtual Switch

A virtual switch is a software application that allows one virtual machine to communicate with other virtual machine of the same type. In the virtualization terminology, a virtual switch is also referred to vSwitch. The virtual switche are usually embedded into installed software. But they may also be included in a server's hardware as a part of its

firmware. A virtual switch is completely virtual and can connect to a network interface card (NIC). The virtual switch merges physical switches into a single logical switch. This helps to increase the bandwidth and create mesh between the server and switches. A virtual switch helps in easy deployment and migration of virtual server. It allows the network administrator to manage virtual switch deployed through a hypervisor. In VMware Workstation 10, a total of nine switches can be created for VMware networking purpose. By default, VMware Workstation has specific named switches and networks associated with it. The bridge network uses VMnet0. The host-only network uses VMnet1, and the NAT network connection uses VMnet8. Virtual switches are nothing but combination of logical ports [17].

Compared to a physical switch, it is easy to roll out new functionality which can be hardware or firmware-related. Depending upon the operating system running on the host, multiple virtual machines (PCs) can be connected to the virtual Ethernet switch. On a Windows host an unlimited number of virtual network devices can be connected to a virtual switch, whereas 32 virtual networks can be connected to virtual switch running a Linux operating system.

3.8 vSphere Standard Switches

vSphere networking relies on abstract network device called vSphere Standard Switches. It provides network connectivity to hosts and virtual machines. It can bridge traffic between virtual machines within the same network and connects to the external network. It is similar to the physical Ethernet switch. The vSwitch uses the physical NIC (pNIC) associated with the host server to connect the virtual network to the physical network. In VMware these switches are also called uplink adapters [18].

vSphere Standard Switches has a 120 default switch port which is more in number than the physical switch [18]. The physical switch has the port of 24, 48 ports. Virtual machines and physical NICs on the host use the logical ports on the switch. Each network adapter in the virtual machines uses one separate port on the vSphere Standard Switch. VMware can create a virtual network from a vSwitch which can be mapped to one or more uplink adapters. When the vSwitch has a bridged connection to the physical network, then the virtual machine residing in the ESXi server can communicate to the external network, meaning virtual machines are not limited to communicating solely across the virtual network.

vSphere Standard Switches has the key properties that makes easier to use in VMware networking and configuration. The switch has 120 default ports, but it can be changed into the required port according to the network. It allows users to change the speed and the duplex of the uplink adapter. More uplink adapters can be added in the Switches. The change in the speed of the adapter enhances the virtual network performance [18].

vSphere standard switches are attached to the VMkernel inside a host server. The vSphere Standard Switch is responsible for routing network traffic to the VMkernel, VM network, and the services console. VMkernel is used to manage features like vMotion, fault tolerance, the network file system (NFS) , internet small computers system interfaces (Iscsi). VM network enables virtual machines running on an ESX or ESXi host to connect the virtual and physical network

3.9 Virtual Network Interface Card

Virtual Network adapter is the logical or software instance of physical network adapter that allows a virtual machine to connect other virtual machine or to Internet .It does not have any physical part like a physical network interface card. Virtual network interface card have their own network address as the physical network card has. With virtual network interface can be connected to the physical devices or it can be connected to the virtual device on a network.

A virtual network interface card in a network provides a secure network environment. It helps to share and access the resources on a network, test the strength and reliability of network connections. It also helps in troubleshooting the network problems and test the network software and maintaining physical components. Figure 6 shows virtual network interface card from the project computer.

Figure 6.Virtual network adapter

Figure 6 was taken from the virtual machine which was configured OpenWrt. In the figure, the virtual machine has two interface cards and was assigned to VMnet2 and VMnet3. The grouping of virtual network interface card creates the virtual switch. In the figure VMnet2 and VMnet3 are virtual switches.

3.10 Virtual Machine

Virtual machine is a software based computer which functions similarly to a physical computer. The virtual machine runs on top of the desktop application. It is installed on the software called Hypervisor which has been explained above in section 3.3. It has all the virtual components that a physical computer does. It has its own virtual hardware, virtual CPU, memory, hard drive, network interface and other devices. The virtual machines share the resources with the physical computer. Every component in the virtual machine resides within the files and is backed by the physical resources. Virtual machine provides additional benefits of portability, management and security.

The virtual machine is a composition of several types of files. The major files that make virtual machines function as physical computers are a configuration file, virtual disk file, NVRAM setting file and the log file. Figure 7 shows types of virtual machines file [20].

File	Usage	Description
.vmx	*vmname*.vmx	Virtual machine configuration file
.vmxf	*vmname*.vmxf	Additional virtual machine configuration files
.vmdk	*vmname*.vmdk	Virtual disk characteristics
-flat.vmdk	*vmname*-flat.vmdk	Virtual machine data disk
.nvram	*vmname*.nvram or nvram	Virtual machine BIOS or EFI configuration
.vmsd	*vmname*.vmsd	Virtual machine snapshots
.vmsn	*vmname*.vmsn	Virtual machine snapshot data file
.vswp	*vmname*.vswp	Virtual machine swap file
.vmss	*vmname*.vmss	Virtual machine suspend file
.log	vmware.log	Current virtual machine log file

Figure 7.Virtual Machine files system

Figure 5 illustrates type of a file system of virtual machines. It provides information about the file and their file type. The configuration file is the file where every configurations and settings of the virtual machines are stored, and it is stored as vmname.vmx. Here vmname is the name of the virtual machine. If the name of the virtual machine is **test**, the file associated with it is named as test.vmx. test.vmfx etc. All these files are stored in the file on the hard drive of the physical computer. There are many software tools where virtual machines can be created and maintained. VMware Workstation and VMware VirtaulBox are the example of the software where virtual machines are created.

The concept of virtual machines allows the user to use, two or more operating system at the same time. The physical computer can have two or more operating system installed on it, but cannot operate two or more operating system at the same time. The concept of virtual machine solves the problem. The user can run Linux and Mac operating system installed in two different virtual machines at the same time. With the virtual machines, the user can test the new operating system, since installing and uninstalling the operating system do not harm the physical computer. The user can test the software in the multiple platforms (Linux, Windows, Mac). The business or organization can take advantage of running all the servers in virtual machines in a single computer [21]. This technology is termed as server Virtualization.

4 Implementation

The project was completed in two parts. The first one was working within the VMware workstation, and the other one was with the VMware ESXi server. Virtual machine creation, configuration and testing were done in both parts. Working with VMware Workstation eased the project as the virtual machines were created and its network was copied to the VMware ESXi.

4.1 VMware Workstation Virtual Network

The project work was started by installing the VMware workstation 10 on a computer. VMware workstation was installed because the virtual machine could be created inside it, which was part of the project. After the VMware workstation 10 was installed, the next task was to create a virtual network with a combination of virtual machines, a virtual router and virtual switches. Figure 8 shows the network which was created in VMware workstation 10.

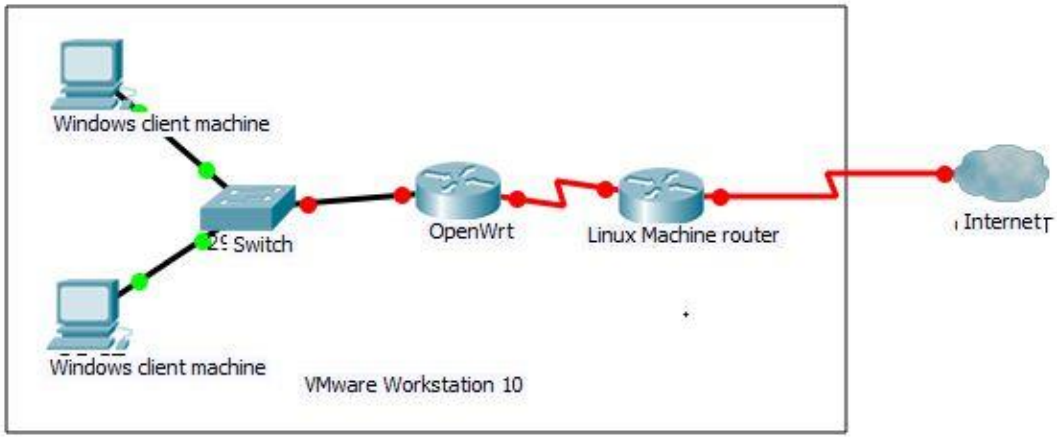

Figure 8.Virtual Network of the Project [Reprinted]

Figure 8 describes the virtual network of the project. The network contains two client computer, Openwrt and the router. The network devices are virtual, meaning the client computers are virtual machines which are connected to Openwrt. The Openwrt acts as DHCP server, and provides IP addresses to the client computers. The Openwrt is connected to the Router. The Linux operating system was installed on a virtual machine and the configuration was made to act as a router. The router is connected to the physical network. The goal of the project was to create a virtual network shown above

in figure 5 and to make a successful connection from the client computer to the Internet. Microsoft Windows 8 operating system was installed on the client computers. The Openwrt was installed in virtual machines to act as a virtual router.

4.1.1 Installing the VMware Workstation

The beginning of the final year project started with installing the VMware Product which was best suitable and convenient for the project work. There are many VMware product available in the market for commercial and non-commercial users. Since this project require only a few virtual computers, VMware workstation 10 software application was the best suitable. So it was decided to use this product during the project work. This product is compatible with both Windows and Linux operating systems.

There are limitations of software and hardware to install the VMware workstation 10. The physical computer on which the workstation is installed is called as Host and the operating system which on the virtual machines is called a guest operating system. To install the Workstation 10 on a host, the host must have a 64-bit x86 CPU that meets the following requirements [7,19].

- LAHF/SAHF support in long mode
- 1.3 GHz or faster core speed.

During the installing of Workstation 10, the installer checks the host with supported processor or not. If the installer does not find the supported processor then the installation process is aborted by installer.

4.1.2 Creating Virtual Machines

A virtual Machine is a software computer that acts like a physical machine and runs an operating system and applications. It uses the resources from the physical machines on which it runs. The benefit of using a virtual machine is that it provides same functionality as a physical computer.

Once the VMware workstation installation was done, the next further step was to install the Virtual PC inside the VMware workstation. Four virtual machines with the capacity

of 20 GB storage capacity each and 512 MB internal memory each was installed. The virtual machine installation procedure is same as the installation procedure of an operating system in a physical machine. The following procedure guides to create new virtual machines in VMware workstation 10

- VMware workstation was started
- New Virtual Machine Wizard was started
- On the screen of New Virtual Machine Wizard, **Next** was clicked
- **Custome** Method for configuring Virtual Machine between **Typical** and **Custom**
- Guest operation system from the option was selected
- Name and folder for the Virtual machine was specified
  The given name was appeared on the list of virtual machine in the VMware Workstation. The given name was used as folder where the files associated with this virtual machine was stored. The folder contains the configuration and disk file.

- Number of processor for the virtual machine was specified.
- Memory setting was adjusted.
  Generally 512 MB of memory space is enough for the testing purpose, In the project, 512 MB of memory space was assigned. The user can specify the memory space depending upon the host system and the number of virtual machines.
- Networking capablities of the virtual machine was configured
  Bridge netwoking must be if the virtual machine has separate IP address
  Network address translation (NAT) must be selected if the virtual machine does not have IP address but want to be connected to Internet. [22.]

4.1.3 OpenWrt Setup

The most important configuration part within the virtual network configuration was configuring OpenWrt. It can be considered the backbone component of the virtual netw ork that was created in the project. This virtual machine on which OpenWrt was installed also must have two network interfaces. One interfaces was connected to router while, other card was connected to switch, where the client machines are connected. The IP

address of the interfaces which was connected to router was assigned statically. While the IP address of the interfaces connected to the switch was given automatically. The default IP address of the interface was 192.168.1.1. Openwrt can be configured from command line terminal and from the web interfaces as well. The configuration includes DHCP server configuration, iproute configuration, Interface address configuration. Openwrt was accessed by typing 192.168.1.1 in the address bar of the browser from the client computers. Figure 9 shows the web-based configuration of the Openwrt.

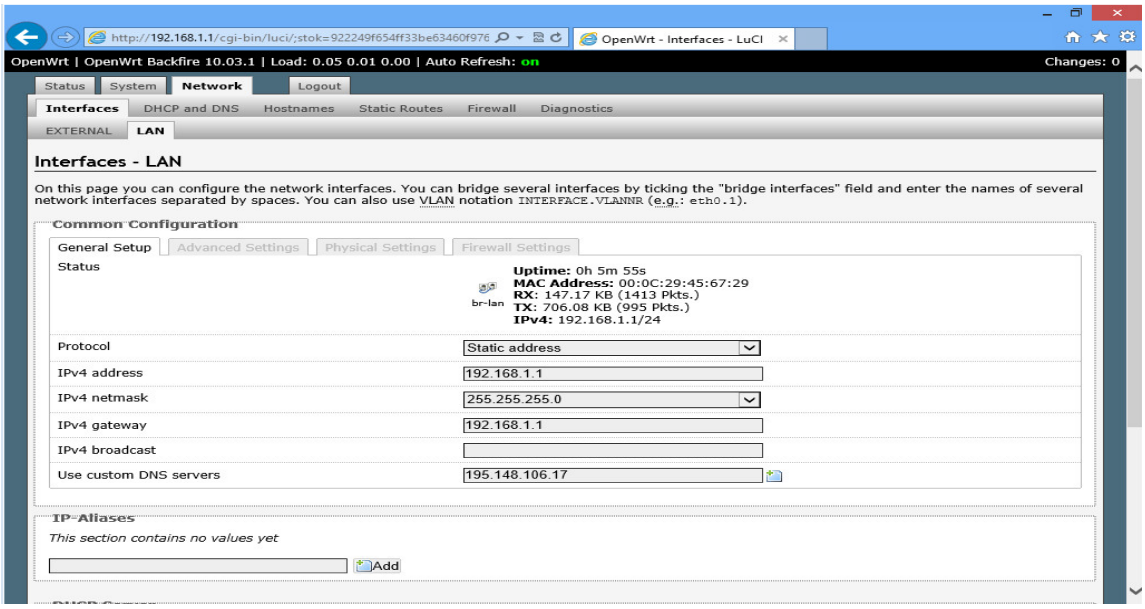

Figure 9.Web based interface of the OpenWrt from the client Machine

Figure 9 shows, the OpenWrt running in the Virtual machine which acts as a DHCP server for the client machines. The figure also shows that OpenWrt can be browsed by the address 192.168.1.1 from the any of client machines because the OpenWrt and two client machines belong to the same network. A static route was also assigned so that traffic from the client computer was carried to the Internet.

4.1.4 Configuring of Virtual Machine as Router

A total of four virtual machines were installed. The first machine acted as the router which forwarded the traffic from the client to the public Internet. The basic function of the router is to forward packets from one interface to other interface. Originally the machine has been installed with only one network adapter which is insufficient for the machine to act as a router as shown in figure 10.

```
sushilc@ubuntu:~$ sudo ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:a1:b6:14
          inet addr:192.168.146.10  Bcast:192.168.146.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fea1:b614/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:78 errors:0 dropped:0 overruns:0 frame:0
          TX packets:156 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:8882 (8.8 KB)  TX bytes:18396 (18.3 KB)
```

Figure 10.Virtual interface of the virtual machine

Figure 10, illustrates that the virtual machine in the network has only one virtual Ethernet adapter named as eth0. The eth0 adapter is the first network adapter for the machine in the Linux operating system. The above Ethernet adapter was created during the creation of virtual machines which was mentioned in section 4.1.2.

The Linux machine must have two network cards installed to act as router. The next task was to install the network card in the Linux machine. One network card connects to the Internet and other network card connects to the machine running OpenWrt. VMware Workstation 10 allows adding total of 10 network adapter in virtual machines. The instruction for adding of network adapter is listed below.

- Virtual machines must be powered off prior to make any changes and setting
- Open virtual machine setting editor by clicking **right** and selecting **setting**
- Click the **hardware** tab and click **Add**
- From the list of option, select the **Network adapter** and proceed to next step by clicking **Next**.
- Select the required network type, (bridge, NAT, and Host-only). Host-only option was selected for the project.
- Click next to **Finish** adding of the network adapter.

The above instruction clearly helps to create new a network adapter in the virtual machine. The addition of the new virtual Ethernet adapter can be confirmed by issuing ifconfig in Linux machines and ipconfig in the command terminal.

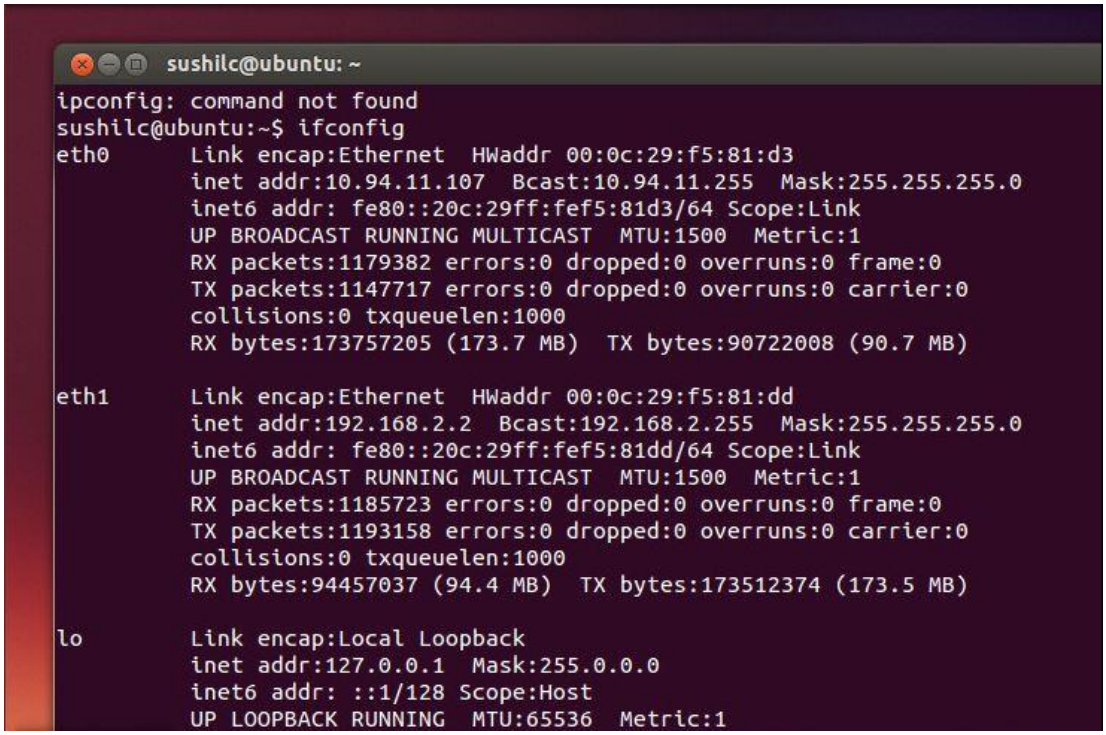

Figure 11.Virtual machine with two network adapters.

Figure 11 is the output of the command after issuing ifconfing in the Linux terminal. From the output it can be seen that the next network adapter was added to the machine. The adapter number is given automatically when the virtual network adapter is created. In the Linux system, the number starts from 0. Therefore the first network adapter is numbered as 0, and the next one as 1.

The network interface eth0 was configured as a bridged network which was connected to the physical network while the next interface card eth1 was configured as a custom network which was connected to the Openwrt. The idea of adding network interface card was to connect the virtual machines to the two different networks. From figure 10, it can be concluded that the eth0 has to 10.94.11.107 address which connects to the physical network where eth1 has network address 192.168.2.2 which was connected to the Openwrt. The interfaces with a bridged network receive the IP address automatically. For the next interface the IP configuration was done statically by editing the file /etc/network/interfaces via text editor.

```
iface eth1 inet static
address 192.168.2.2
netmask 255.255.255.0
```

With the above modification in the file /etc/network/interfaces, the IP address for the network interfaces eth1 was assigned.

Figure 11 shows that the machine had two network interface card added. Interface eth0 and eth1 belong to different networks. Since the packet has to travel through the machine, the machine has to act as a router and the properties of the routers are to connect two different network. So the idea was that the machine had to be configured in a way that routes packets from one network to another network. Figure 12 shows basic configuration or file edition tasks that help to accomplish the Linux machine to act as a router.

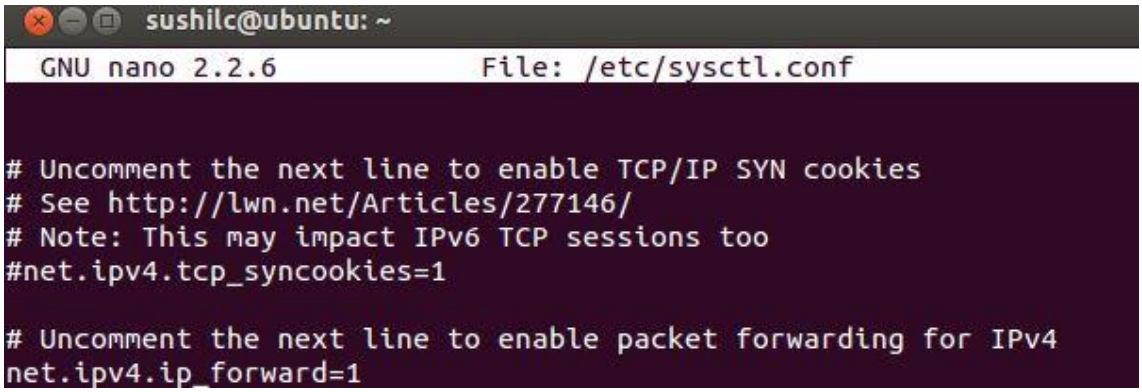

Figure 12.Basic task for IP forwarding

The basic idea of the above configuration is that once the IP forwarding was enabled , then the packet arriving to one interface was forwarded to the next interface of the device regardless any firewall or security. This basic configuration was done by uncommenting the line shown above in the figure by text editor. In the project, nano text editor was used. User can use Vi as the text editor also.

The next step for configuring the Linux machine as a router was to edit the iptables. Iptables is a command-line firewall utility that uses policy chain to allow or block traffic for Linux operating system. Normally the the iptables are pre-installed in unix operating system or any distribution of Linux operating system. The iptables runs without any rules by default. The primary function of iptables is to control the incoming and outgoing packet through the interfaces. Iptables can be called as the basic firewall system in the Linux operating system. The iptables rules were created by issuing the following commands given below.

- sudo iptables -t nat -A POSTROUTING -o eth1 -j MASQUERADE
- sudo iptables -A FORWARD -i eth1 -o eth0 -m state -–state RELATED,ESTABLISHED -j ACCEPT
- sudo iptables -A FORWARD -i eth0 -o eth1 -j ACCEPT

The above created iptables were saved to function as the rules effectively after every reboot of the router machines. The iptalbes resides in the volatile memory before saving, so rebooting the computer without saving removes all the iptables. The iptables can be saved to make permanent change by issuing the command **iptables-save > /etc/iptables.rules** [23]**.**

4.1.5 Configuring Virtual Machine as Client Machine

Among the four virtual machines that were created in the VMware Workstation 10, the remaining two machines acted as a client machines in the virtual network. The client machines had Windows 8 installed as a guest operating system. The client computer had only one network adapter installed on it. The interfaces of the both client computer was connected to the vnet 5 where one of the interfaces of Openwrt was also connected. So with these connections, the client computer and Openwrt belong to the same network. So OpenWrt can be browsed from the client computer. The aim of including the client machine in the network is to help users to perform testing tasks within the machines. Among the four virtual machines, the users will be concerned with only these two client machines as they will be provided with full administrative rights to access these machines.

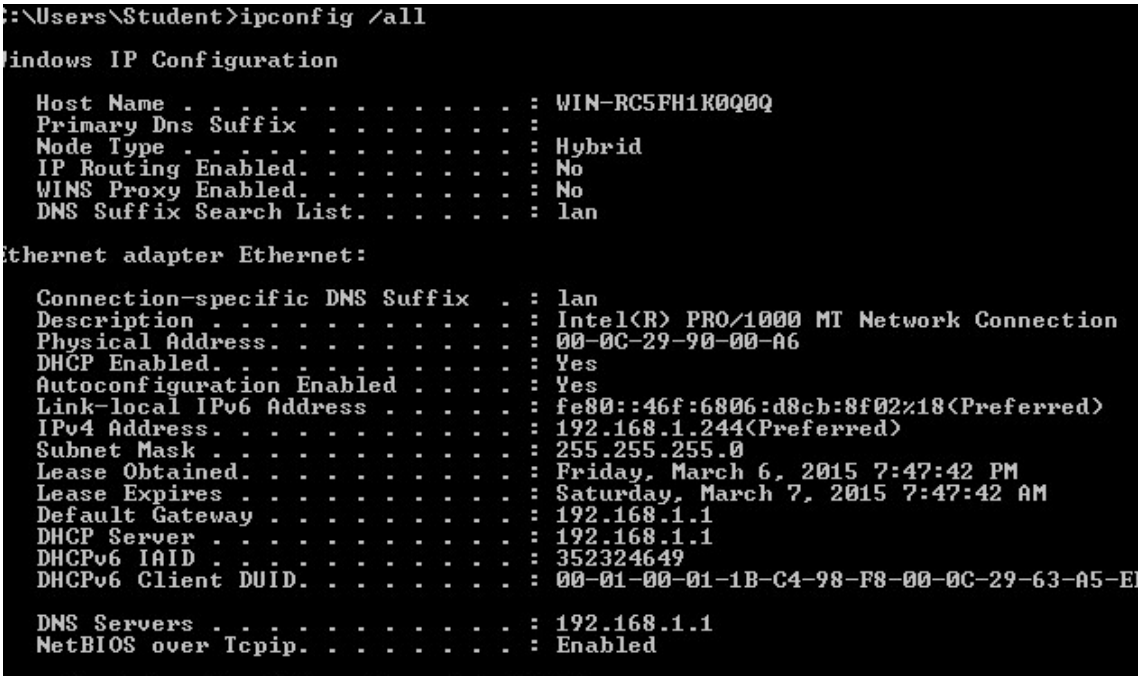

Figure 13.Configuration of the client machine

Figure 13 illustrates the IP configuration of the client machines which act as DHCP client. The machines have an IP address of 192.168.1.224 which belong to the same network of the DHCP server. The configuration also concluded 192.168.1.1 as a DHCP server which was the IP address of the machine running OpenWrt. Figure 13, also shows extra information that the machine with OpenWrt acts as Default gateway for the client machines, meaning that the traffic originating from the client machines passes through the OpenWrt machine.

4.1.6 Testing of Virtual Network

After the configuration of all the virtual machines, idea of the virtual network was that the client machine should be able to connect to the Internet. The client computers get an IP address from the OpenWrt machine which acts as a DHCP server for the client computer. One interface of OpenWrt machine was connected to Linux router and other interfaces of Linux router was connected to the internet. The testing result was considered successful if the client computer connected to the public internet. Figure 14 shows connectivity to the Internet from one of the client computer.

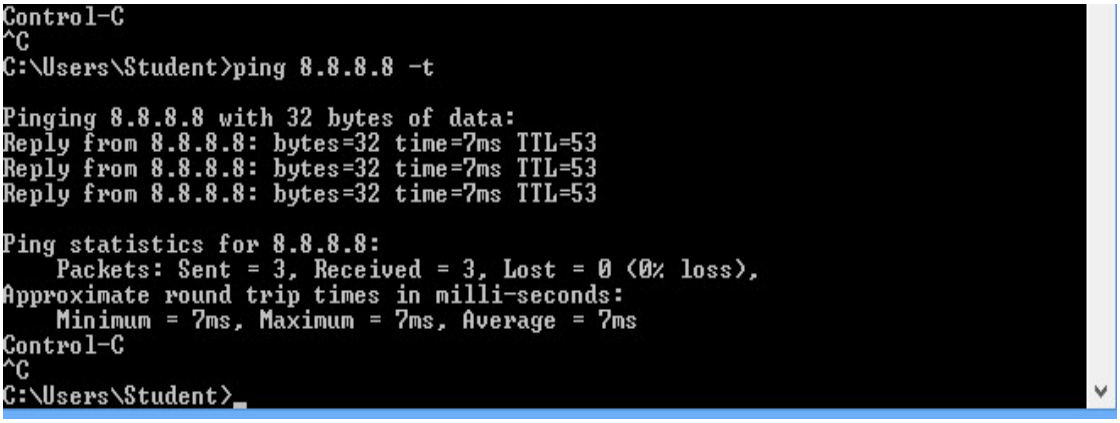

Figure 14.Testing connectivity to the internet.

The 8.8.8.8 address in the figure 14 is Google DNS server, which is generally pinged to check the connectivity to the internet. From the above figure it can be concluded that there had been reply from the destination, (8.8.8.8) which confirms the successful operating of virtual network. It was tested from the other client machine as well and the results were the same, meaning the other client computer was able to make connection to the internet. Also the client computers were able to make connections to every machine (router, OpenWrt) in the network.

So the first task of the project was to create a virtual network and test the end to end connectivity. The project began by installing the VMware workstation 10 in the physical computer and ended with successful testing and operation of the network. The methodology and process is explained above and gives clear vison, how and what was done in the project. There were challenges and problems during working with the project. The first problem faced was the memory problem in the physical computer. The project computer had only 4 GB of memory installed on it,which was insufficient to create the virtual machines. The operating system itself occupies 2 GB of memory, and only 2 GB was remaining for the virtual machines. Each virtual machine was created with memory of 512 MB which make a total of 2 GB of memory. So there was no memory left for the system and as a result the performance of the physical computer was slowed down.

The problem was solved by installing extra 4GB of memory on physical computer. The problem was explained to the supervisor and the lab assistant of the school. They installed extra 4 GB of memory which helped in the smooth working of the project.

4.2 VMware ESXi Virtual Network

In this part, the virtual network was created and tested on the VMware ESXi server. VMware ESXi server can run multiple virtual machines on a single host. It allows the virtual machines to be accessed remotely with the VNC technology which was explained in section 3.5. In the previous task, a virtual network was created and tested in VMware Workstation 10. The next task was to create and test the virtual network in VMware ESXi server. The task was to optimize the network and virtual machines. Along with the creation and testing the network, an additional task was to configure the client machines in such a way that it would reboot itself when the user or student would accidently shut down the client virtual machine.

4.2.1 Copying Virtual Machine to ESXi server

After the successful creation and testing of the virtual network in the VMware workstation 10, the task was to create the virtual network in the ESXi server so that the user can access the virtual machines in ESXi server from anywhere within the network. The task could be done in two different ways. Either the network could be created by creating new virtual machines in the ESXi server manually or by copying the existing virtual machines from VMware Workstation 10 to ESXi server. During the project, the virtual machines were copied from Workstation 10 to ESXi server which was easy and convenient way to do it. The benefits of copying virtual machines were saving time and the machines were error free. Figure 15 illustrates computer when the Virtual machines were copied to ESXi server.

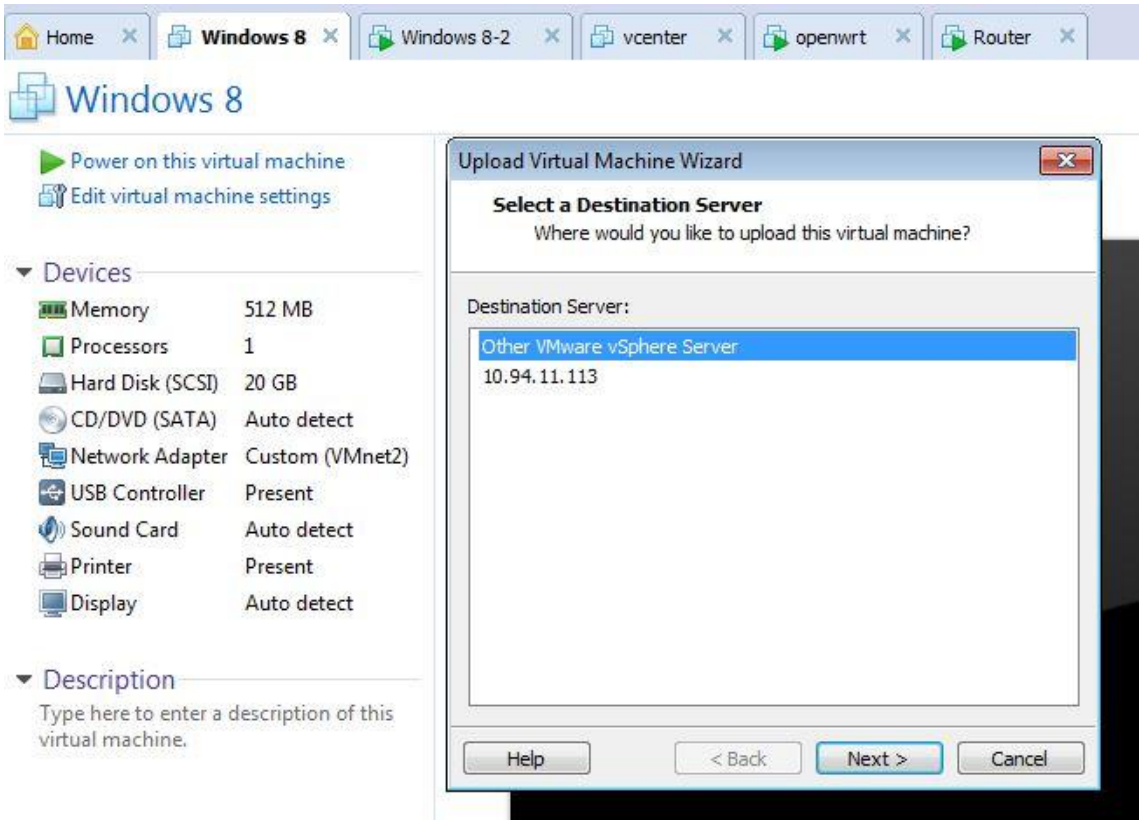

Figure 15.Copying the virtual machine

In figure 15, one of the client machines named as Windows 8 was copied from workstation to ESXi server. When copying, the workstation automatically searches for the server. In the project work, the only connected server was ESXi server which IP address was 10.94.11.113 as show in figure. Below given is the list of how the machines were copied.

- In the beginning, the desired virtual machine was powered off.
- By right clicking on the machines, the option **manage** was selected, and from the option **upload** was selected.
- The upload virtual machine wizard then appeared as shown in figure 15.
- By clicking **next,** the next wizard appeared where the hostname, username and password was provided for the ESXi server.
- The next wizard was for selecting the destination location for the virtual machine. In the lab, the host contained two data store named as datastore 1 and datastore 2. The datastore 2 was selected in the project work. All the configuration file and folder resided in datastore 2 after selecting it.

All the other virtual machines were copied from VMware Workstation 10 to ESXi server in the same way explained above. When all the machines were copied, the virtual network did not exist in VMware ESXi server. The virtual machines were connected to the physical network and thus able to access the Internet. So the next task was to configure the virtual network with the virtual machines copied from VMware Workstation 10

4.2.2 Creating Standard Switches

In vSphere networking, vSwitches can be mapped to one or more network adapter. A standard switch that has not any network adapter associated is called internal vSwitch. The virtual machines connected to internal vSwitch cannot communicate with other machines outside the host. To create the standard switch in the project.VMware ESXi was accessed remotely from vSphere client by issuing username and password..ESXi host was clicked and networking was selected from the option. In networking section, the configuration section, add networking was clicked. Then virtual machine was selected from the connection type and network adapter was selected

The virtual switch was created with the above instruction. Since the router had to be connected to the Internet, one of the interface connected to the physical network was bridged to the physical network. In the project, Eth1 of the Linux Router was configured as a bridge connection. The next interface Eth 0 was connected to the internal virtual switch.

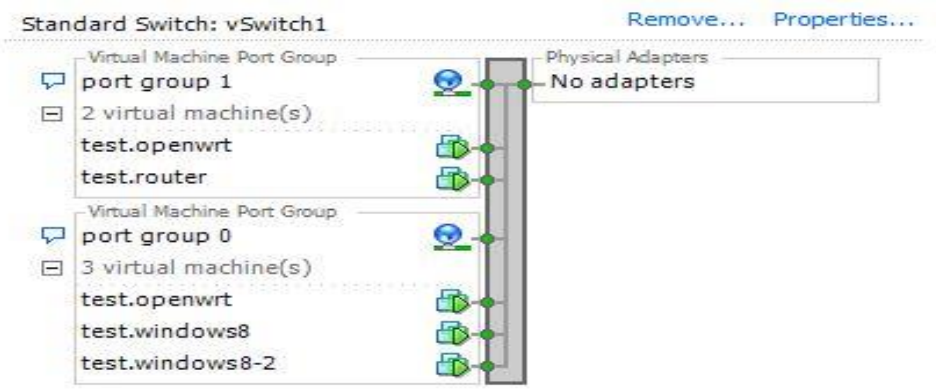

Figure 16.Configuration of test.router in ESXi server

Figure 16 shows the vStandard switch created in the project. The assigning of Network adapters to the different port group creates the vSphere standard Switch. From the

above figure, it can be concluded that the vSphere standard was created and , the virtual machines was assigned to different port group. test.Openwrt and has test.router has two interfaces and belongs to different port group (group 1 and group 0).

4.2.3 ESXi Server Management

The virtual machines in the ESXi server have to be running all the time. There might occur a problem in the server if there is a power failure. So the challenge was to meet the problem and the problem was solved successfully. The virtual machine was configured in a way that the machines can restart automatically when the ESXi server starts. The client machine in the ESXi server was configured so that students have full administrative right to use it. The users or students were not provided the administrative rights to access the router and Openwrt. The ESXi server was enabled to SSH login for management tasks [24].

4.2.4 VNC configuration

vSphere client gives a complete view of all the virtual machines that were created in the VMware ESXi server. When accessing the virtual machines via vSphere Client, the student could access all the virtual machine which was not a part of the project. The project was to access only the client computer regardless any other virtual machines. This problem was overcome by introducing the concept VNC virtual network computing which is explain above in section 3.4.

VNC allows the client Virtual machines to be accessed remotely. In the project, VNC Viewer was used to access the client virtual machine remotely. VNC viewer was not able to connect to client virtual machines. Additional setting and configuration was applied in the configuration file (.vmx) of the virtual machines. Below given is the setting and additional configured parameters in the .vmx file of the virtual machines.

- RemoteDisplay.vnc.enables = [true | false]
- RemoteDisplay.vnc.port = [port]
- RemoteDisplay.vnc.password = [optional]

Figure 17 shows a is the screen shoot of the configuration file of one of the client computers from the project. The additional parameters were configured to allow the virtual machine to be accessed remotely.

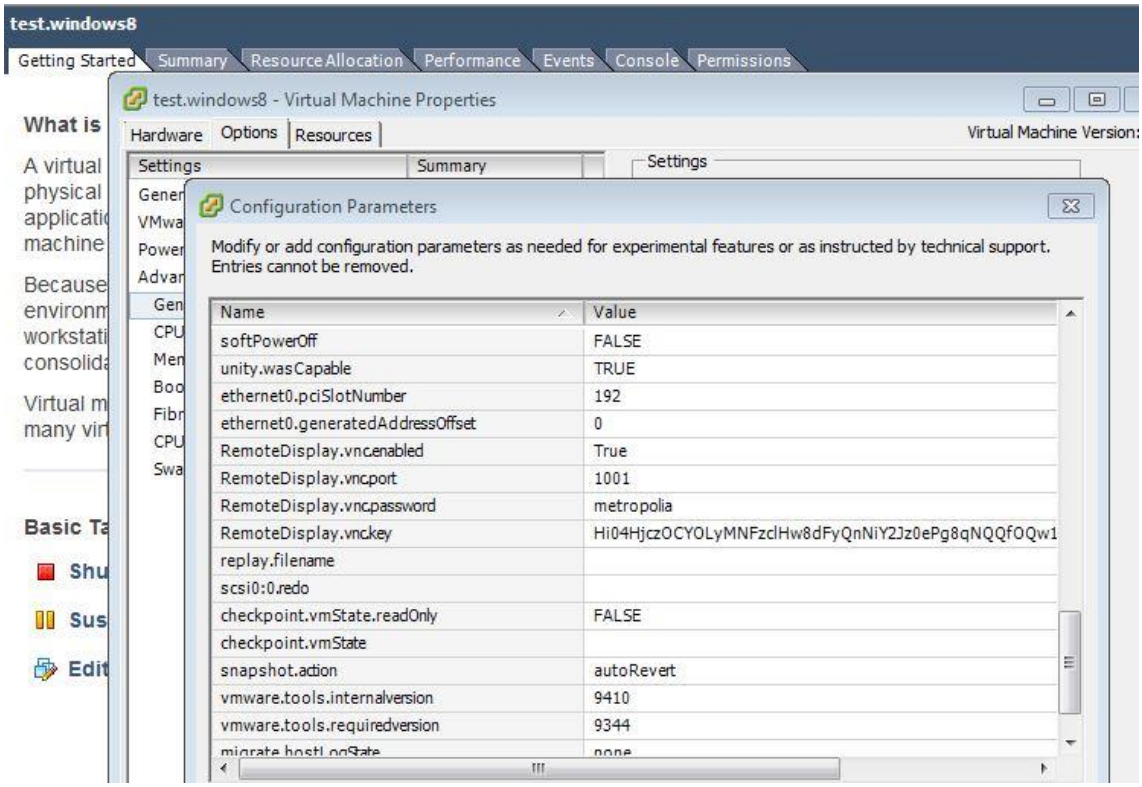

Figure 17.VNC configuration of Client machine

The parameter (RemoteDisplay.vnc.enabled) allow the virtual machine to be remotely accessed. The parameter (RemoteDisplay.vnc.port) is the important parameter because without the port number the VNC viewer does not know to which computer connect. Unassigned port number creates problem, when the VNC viewer connects to the server where multiple virtual machines are running at instant. From the figure, it can be informed that the port 1001 was to be assigned to the client machine. The port number had to be unique, meaning two Virtual machines cannot be assigned with the same port number. The password parameters are optional, but for the security purpose, it was best recommended to assign password so that only authorized students or users are able to connect to the virtual machines.

4.2.5 Testing Network

After a virtual network was created in the ESXi server connectivity and communication between the virtual machines were tested. The client computer was able to access the Internet. The task was similar to the creation and testing of the virtual network in VMware workstation 10. The difference was that a standard switch was introduced for creation of a virtual network in the ESXi server.

VNC testing was also performed. The client machine in the ESXi server was accessed remotely within the network as configured and explained above in section 4.2.4. The virtual machines were powered OFF, and they were powered ON automatically as configured and explained in section 4.2.4. The file was created in the virtual machine and powered OFF, and after two minutes the machines were powered ON automatically. The previous created file was removed, which was exactly how the virtual machine was configured with the concept of a snapshot. Figure 18 is the screnshoot of a computer when testing connection.

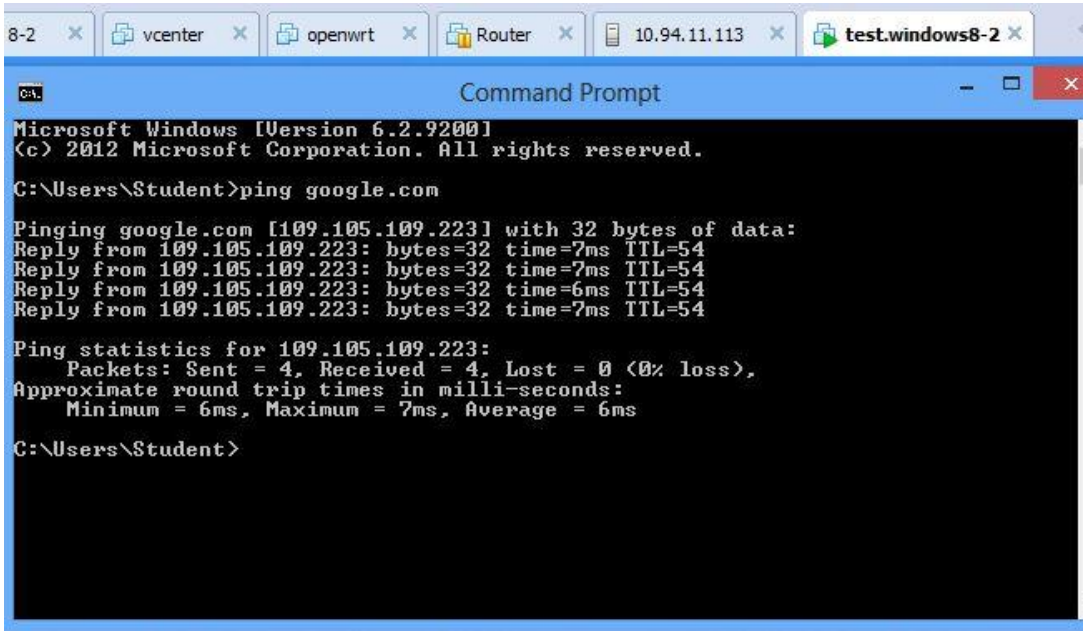

Figure 18.Testing of Internet connectivity

The above screenshot was taken from the client computer in the ESXi server during the testing time. The connection was tested by pinging to Google.com. It can be seen that the reply has been sent from the google as a response to request. The client computer was able to connect to Internet or server outside the network.

5 Conclusion

The final year project was started to virtualize a Home Network and implement it in an educational institution for the learning purpose. The project was done in two parts, working with the client and server side. As a result, the goal was achieved and a Home Network was virtualized. The final year project was carried out to solve the problem at Metropolia UAS regarding the network-related classes.

Network virtualization has become very popular from small scale (Home Network) to large scale (production environment) virtualization. More and more organizations and institution are adopting this technology. The use of this technology helps organizations and institutions in better performance of IT services to reduce the expenses. There are new virtualization software tools and products produced every day. The virtualization technology offers higher availability and uptime of the IT services. This technology has become cheaper implementation than a physical technology, thus allowing a company or business to make more profit and run the business smoothly.

With the virtualization technology, schools and universities can take full advantage of it. Virtual learning can be implemented in those institutions. For example, now the student at Metropolia can perform an exercise on a virtual computer leaving the classrooms space for the other students and teachers. Students get rid of physical layer problems like cable or power, which allows them to put more time into learning. The student and readers now understand the difference between the physical and virtual network after studying the project. The project benefits users by providing the information about the virtual technology and its implementation in the IT sector. After reading this thesis, student will be motivated towards the virtualization technology. As an outcome of the project, teachers monitor the students' computers from their own computers with a VNC system.

References

1 Burger, Thomas . The Advantages of Using Virtualization Technology in the Enterprise [online] 2012
URL:https://software.intel.com/en-us/articles/the-advantages-of-using-virtualization-technology-in-the-enterprise
Accessed 15 January 2015

2 The Benefits of Virtualization for Small and Medium Business [online]
URL:http://www.vmware.com/files/pdf/VMware-SMB-Survey.pdf
Accessed 23 April 2015

3 Microsoft Research. Diagnosing Home Network Misconfiguration using Shared Knowledge [online] 2015
URL: http://research.microsoft.com/en-us/projects/netprints/
Accessed 25 April 2015

4 Overview of Network Virtualization [online] 2012
URL: https://docs.oracle.com/cd/E26502_01/html/E28992/gfkbw.html
Accessed 15 Janaury 2015

5 Configuring Virtual Networks
URL: https://technet.microsoft.com/en-us/library/cc816585(v=ws.10).aspx
Accessed 23 April 2015

6 Selecting the Network Connection Type for a Virtual Machine
URL: https://pubs.vmware.com/workstation-9/index.jsp?topic=%2Fcom.vmware.ws.using.doc%2FGUID-3B504F2F-7A0B-415F-AE01-62363A95D052.html
Accessed 17 March 2015

7 vSphere ESXi Hypervisor [online] 2015
URL: https://www.vmware.com/products/vsphere/features/esxi-hypervisor
Accessed 23 April 2015

8 VMware ESX and VMware ESXi [online]
URL: http://www.vmware.com/files/pdf/VMware-ESX-and-VMware-ESXi-DS-EN.pdf
Accessed 23 April 2015

9 Giri, Bipin. Difference between vSphere, ESXi and vCenter [online] 2012
URL:http://www.mustbegeek.com/difference-between-vsphere-esxi-and-vcenter/
Accessed 12 Feburary 2015

10 Download VMware Workstation [online] 2015
URL:https://my.vmware.com/web/vmware/info/slug/desktop_end_user_computing/vmware_workstation/11_0
Accessed 21 May 2015

11 Dinesh. Major New Features of VMware Workstation 10 [online] 2014
URL: http://www.sysprobs.com/whats-new-features-of-vmware-workstation-10
Accessed 10 Feburary 2015

12 Rouse, Margaret . Virtual Network Computing (VNC) [online]
URL: http://searchnetworking.techtarget.com/definition/virtual-network-computing
Accessed 13 March 2015

13 What is VNC (Virtual Networking Computing) [online]
URL: http://www.remoteaccess.org/what-is-a-vnc/
Accessed 15 March 2015

14 Features. [online]
URL: https://www.realvnc.com/products/vnc/
Accessed 17 March 2015

15 Sharma, Mayank . Supercharge Your Router with OpenWRT [online] 2013
URL: http://www.maketecheasier.com/supercharge-router-with-openwrt/
Accessed 25 March 2015

16 Hoffman, Chris. What Is OpenWrt And Why Should I Use It For My Router [online] 2013
URL: http://www.makeuseof.com/tag/what-is-openwrt-and-why-should-i-use-it-for-my-router/
Accessed 25 March 2015

17 Virtual Switch [online] 2015
URL:https://www.vmware.com/support/ws5/doc/ws_net_component_vswitch.html
Accessed 25 March 2015

18 vSphere Standard Switches [online] 2015
URL: http://pubs.vmware.com/vsphere-51/index.jsp#com.vmware.vsphere.networking.doc/GUID-350344DE-483A-42ED-B0E2-C811EE927D59.html
Accessed 27 March 2015

19 Supported Processors. Getting Started with VMware Workstation [online]
URL: https://www.vmware.com/pdf/desktop/ws10-getting-started.pdf
Accessed 15 April 2015

20 What Is a Virtual Machine [online]
URL: https://pubs.vmware.com/vsphere-51/index.jsp#com.vmware.vsphere.vm_admin.doc/GUID-CEFF6D89-8C19-4143-8C26-4B6D6734D2CB.html
Accessed 15 April 20015

21 Hoffman, Chris. What is Virtual Machine [online] 2012
URL: http://www.makeuseof.com/tag/virtual-machine-makeuseof-explains/
Accessed 15 April 2015

22 VMware Workstation 5.0 setting New Virtual Machine [online]
URL:https://www.vmware.com/support/ws5/doc/ws_newguest_setup_simple_steps.html
Accessed 25 April 2015

23 Shinnde, Mandar. How to: Configure Ubuntu as a Router [online] 2013
URL: http://www.yourownlinux.com/2013/07/how-to-configure-ubuntu-as-router.html
Accessed 15 Feburary 2015

24 Damodaran, Sreejesh. ESXi bash script to automate Power ON VM if its Powered OFF [online] 2014
URL: http://pingforinfo.com/cronjob-poweron-vm/
Accessed 15 Marc