BASIC DESIGN OF A LOCAL AREA NETWORK FOR SMALL BUSINESSES

DOUTIMFI, TARIEMI GODPOWER
ND/COMP.SC/19/019

A PROJECT SUBMITTED TO THE DEPARTMENT OF COMPUTER SCIENCE, FACULTY OF SCIENCES, BAYELSA STATE POLYTECHNIC ALEIBIRI, P.M.B. 168, EKEREMOR FOR THE AWARD OF NATIONAL DIPLOMA IN COMPUTER SCIENCE.

MAY 18, 2022

ABSTRACT

This Project envisages the design of a local area network (LAN) by adopting a design model that will be suitable for small businesses with less than 20 users using the Windows 7/10 operating system. The concept of hierarchical design was adopted in building the network as compared to other network design models, hierarchical models was easier to managed, expandable, and problems were easily identified and solved, as network devices were selected based on purpose and functions. The design involves dividing the network into discrete layers; each layer performs specific functions in the network. Cost and congestion in terms of network traffic flow within and out of network were considered in choosing the right bandwidth for network operation. The basic system requirement for the network devices within the LAN was established and appropriate configuration and installation were carried out to support the effective operation of the network. Each device on the network was assigned a unique hostname and IP address, taking into account standard address planning. It was ensured that no two devices had same IP address to avoid conflict. Private IP address was used as the network address. Data integrity within the network was strongly emphasized and it was achieved by implementing firewall security within the network interface considering the security policy of the organization. The network address translation concept also provides security within the network by using a public address when the users interact across the network.

DECLARARTION

I, Doutimifi Tariemi Godpower Matriculation number ND/comp.sci/19/019 hereby declares that, the study on Design of Basic Network for Small Businesses (A case study of global consult property) is carried out by me in the department of computer science in faculty of Sciences, Bayelsa State Polytechnic Aleibiri.

Doutimifi Tariemi Godpower

(Researcher)

CERTIFICATION

This is to clarify that this project was undertaken by DOUTIMIFI, TARIEMI GODPOWER and supervised and approved as having met the requirement for the award of National Diploma in the Department of computer science, School of Applied Science, Bayelsa State Polytechnic Aleibiri.

Mr. Assor Emmanuel D.

(Supervisor)

Date 18/05/2022

Mr. Paul Yerikema

Head of Department

Date 18th May 2022.

DEDICATION

I dedicate this project to God Almighty for His provision and guidance for this project work and to my lovely parents Mr. & Mrs. Doutimifi G.F for all their support.

ACKNOWLEDGEMENT

I Acknowledge with great appreciation to God Almighty, the one who gave me wisdom and understanding for the successful completion of the project work. And those who have been very instrumental in one way or the other in the course of my educational pursuit.

I am very grateful to my project supervisor Mr. Assor Emmanuel D. for his preciously spearing much of his time throughout the period of the research work. His brilliant discussions, kindness and accessibility will not be forgotten, I sincerely thank him for his selfless sacrifice, fatherly assistance and teachings, I acquired valuable knowledge from him during the course of this research work.

My special thanks go to my Head of Department Mr. Paul Yerikema, Mr. Sese Ogbere for all the knowledge they impacted in me.

I am very grateful for my beloved parents Mr. & Mrs. Doutimifi G.F whom I am greatly indebted to Daddy and Mummy May God reward you with long life for the harvest of your labor. And to my one and only lovely siblings Doutimifi Ebiumini and Doutimifi Emomotimi and my wonderful friend Oglafa your lavishly encouragement and fatherly assistance May God Almighty bless you all.

TABLE OF CONTENTS

CHAPTER ONE

INTRODUCTION

1.1 BACKGROUND OF THE STUDY

Networking is a basic concept for an interconnection of system through a channel with the sole purpose of exchanging information by implementing certain set of rules which are defined within the system. Different systems can connect in various ways to achieve certain objectives. However, one major way by which an organization connects to achieve their desire goal is through the adoption of local area network (LAN), which is the interconnection of computers and network devices within a geographical area and providing shared access to printers, file servers and other network devices. I had observed the rate of adoption of modern technology among SMEs (small-medium enterprises) especially looking into an Africa business region and I have come to realized that the steps have not been improving unlike the fast implementation of modern technology concept for efficient business operation in other developed countries. Having known this, I was challenged with resolving reasons why SMEs has failed in prompt acceptance of modern technology in transforming their business operation. However, some that do adopt these technologies has not shown progressive report in their business activities over time unlike their counterparts in western countries while others lack the technological know-how, however implementing the wrong technological model and still results in little success over time. My effort towards answering the above question results in my findings that most the African business organizations adopted and implemented the wrong Information technology model by choosing inappropriate design models in building their business network hence having issues like over budgeting, network security threats, scalability, traffic collision, mal-operation and many more. The question of designing and selecting appropriate network design models for small businesses will form the basis of my Project work.

I will carefully highlight the effective model for small business design and briefly explain the major system requirements and configuration of devices that make up the network, emphasizing its management, security, scalability and its general documentation. It is important for small businesses to adopt technological processes that allow them provide services that will bring about competitive advantages. One such process is by building an enabling network for smooth business operations with no difficulty of information addition and consolidation. Effective communication and resource sharing are key issues among network users in any organization network and this can be achieved when there is a right network structure in place. There should also be a progressive flow of data and resource sharing among hosts within and across the organization network without fear of compromise. The network should be designed so that the hosts have parallel access to devices on the network and can communicate with each other at all time on the network. With the addition of IT in small businesses, their operational frequencies have been greatly improved. The production and execution of networking concepts like LAN (local area network) has also created a framework for which transactions between computers within and across a network that were not in the past possible a reality. Objective of the Project is to design a network model for small businesses that will support efficient and secure means of data communication and resource exchange among different hosts on same the LAN and across other networks through the use of viable industrial technological standards, considering the cost-effectiveness, security and business growth (scalability). A LAN is a fundamental requirement for doing business; hence, one must understand the concept of a well-designed LAN and be able to select appropriate devices to support the network specifications for a small sized business. This Project includes the basic design of a LAN, its complete documentation, configuring and installation of appropriate network devices, firewall installation and functional testing, installation, labeling

and certification of structured cabling. Required software properly installed on the hosts and with the aid of my instructor.

1.2 STATEMENT OF PROBLEM

Having known this, I was challenged with resolving reasons why SMEs has failed in prompt acceptance of modern technology in transforming their business operation. However, some that do adopt these technologies has not shown progressive report in their business activities over time unlike their counterparts in western countries while others lack the technological know-how, however implementing the wrong technological model and still results in little success over time while others lack funding for the installation of the appropriate network devices.

1.3 OBJECTIVE OF THE STUDY

The objectives of this study is to implement the modern technology concepts for effective business operations.

One of the major objectives is to be able to decide the right LAN architecture that satisfies the size of one's business, which is easy to manage and expand and also where problems are easily identified and managed more quickly

1.4 JUSTIFICATION OF THE STUDY

Effective communication and resource sharing are key issues among network users in any organization network and this can be achieved when there is a right network structure in place. There should also be a progressive flow of data and resource sharing among hosts within and across the organization network without fear of compromise. The network should be designed so that the hosts have parallel access to devices on the network and can communicate with each other at all time on the network.

1.5 THE SCOPE OF THE STUDY AND LIMITATION

This study focused on building local area network for small business owners by using peer to peer network for easy communication in business operations. Given the duration for the completion of the study, one of the major constraint I faced was funding to get the necessary equipment. However, seeking financial support from family members and friends and adding more time to my academic work was helpful to the achieving of the work.

CHAPTER TWO

LIERATURE REVIEW

2.0 CONCEPT OF NETWORKING

A network is basically two or more computers connected by a cable or by a wireless radio connection so that they can exchange information. Networks are all about sharing. Specifically, networks are about sharing three things: files, resources, and programs.

Sharing files

Networks enable you to share information with other computers on the network. Depending on how you set up your network, you can share files with your network friends in several different ways. You can send a file from your computer directly to a friend's computer by attaching the file to an email message and then mailing it. Or you can let your friend access your computer over the network so that your friend can retrieve the file directly from your hard drive.

Sharing resources

You can set up certain computer resources — such as hard drives or printers — so that all computers on the network can access them. For example, the laser printer attached to Ward's computer in a *shared resource,* which means that anyone on the network can use it. Without the network, Faith, Wally, and would have to buy their own printers.

Sharing programs

Instead of keeping separate copies of programs on each person's computer, put programs on a drive that everyone shares. For example, if ten computer users all

use a particular program, you can purchase and install ten copies of the program, one for each computer. Or you can purchase a ten-user license for the program and then install just one copy of the program on a shared drive. Each of the ten users can then access the program from the shared hard drive. In most cases, however, running a shared copy of a program over the network is unacceptably slow. A more common way of using a network to share programs is to copy the program's installation disks or CDs to a shared network drive. Then you can use that copy to install a separate copy of the program on each user's local hard drive. For example, Microsoft Office enables you to do this if you purchase a license from Microsoft for each computer on which you install Office.

2.1 OSI Model

In every communication processes there must be rules to enhance mutual understanding on a common communicating platform. If we assume a class of students that engage in communication and everyone has to talk at the same time, then there will be a problem of understanding, but if there are rules that must be considered to know who and when to talk, then there will be much more understanding in their communication. The same principle is applicable to computers on a network that transmit and exchange resources simultaneously, thereby hindering network traffic which might also result in loss of data. There must be rules to enhance effective and smooth communication among devices on a network and these rules can be refers to as PROTOCOL. Protocols enabled an entity in one host to interact with a corresponding entity at the same layer in another host. Protocols define the rules that govern the communications between computers connected to a network. A protocol specification consists of the *syntax*, which defines the kinds and formats of the messages exchanged, and the *semantic*, which specifies the action taken by each entity when specific events occur. **OSI** is an

stands for **Open Systems Interconnection model** and it is a standard for designing of computer networking and functioning. OSI consists of seven layers, each playing a specific role when applications are communicating over the network. During the sending process, each layer (from top to down) will add a specific header to the raw data. At the reception, headers are eliminated equally until the data arrive to the receiving application.

OSI Protocols layers:

- Layer 1- Physical Layer
- Layer 2- Data Link Layer
- Layer 3- Network Layer
- Layer 4- Transport Layer
- Layer 5- Session Layer
- Layer 6- Presentation Layer
- Layer 7-Application Layer

2.1.1 Introduction to TCP/IP

The Transmission control protocol TCP/IP is the communication protocol for the internet and it defines the rule computers must follow to communicate with one another over the internet. Browsers and servers use TCP/IP to connect to the Internet. A browser uses TCP/IP to access a server while the server uses TCP/IP to send HTML (Hyper text makeup language) back to a browser. A TCP/IP is an industry standard suite of protocols that is designed for large networks consisting of network segments that are connected by routers. TCP/IP is the protocol that is used on the Internet which is the collection of thousands of networks worldwide that connect research facilities, universities, libraries, government agencies, private companies, and individuals. (Davies 2006, 27.) TCP/IP has become so successful

because it delivers a few basic services that everyone needs (file transfer, electronic mail, remote logon) across a very large number of client and server systems. Several computers can use TCP/IP along with other protocols on a single LAN. "TCP/IP a two layer program, the higher layer is Transmission Control Protocol which manages the assembling of a message or file into smaller packets that are transmitted over the internet and received by TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. TCP/IP uses the client/server model of communication in which a computer user requests and is provided a service by another computer. TCP/IP is primarily point-to point, meaning each communication is from point or host on the network to another host." (TechTarget 2012.) Higher layer protocols also use the TCP/IP to connect to the internet. These protocols include the World Wide Web's Hypertext Transfer Protocol (HTTP), the File Transfer Protocol (FTP), Telnet (TELNET) which make it easy for one to logon to remote computers, and the Simple Mail Transfer Protocol (SMTP). These and other protocols are packaged together with TCP/IP as a suite. Inside the TCP/IP standard there are several protocols for handling data communication: TCP (Transmission Control Protocol) communication between applications

UDP (User Datagram Protocol) simple communication between applications

IP (Internet Protocol) communication between computers

ICMP (Internet Control Message Protocol) for errors and statistics

DHCP (Dynamic Host Configuration Protocol) for dynamic addressing. (TechTarget 2012.)

2.2 LAN Network structure for SMEs

A LAN (Local area network) is a computer network that provides connectivity and data sharing features to a limited number of users in a small geographical area. LAN equipment is usually owned by an organization, and the medium may be own or leased from a telephone company or a common carrier. However, a personal computers or workstation interconnected to the medium (twisted pair; fiber optics) through connectors to servers. A LAN is interconnected with other networks via switches and router. (Cisco 2012.) Different business organizations implement different LAN structure based on the company size of employees and mode of operation. A small enterprise consists of employees that are within the range of (0-49) employees, micro firms (0-9) employees and medium firms (50249) employees. These three sizes of employees make up the term small-medium enterprises (SMEs), though the interpretation varies from country to country as regards the number that constitutes a particular business size. (Jones-Evans 2006, 10-12.) This Project scope considered an organization within the size of a small –medium enterprises and this help in choosing the best network topology from the numerous topologies available in the networking concept. A Network topology describes the shape or structure of a network which does not indicate the shape or structure of the devices on the network. A LAN is an example of network which has both physical and logical topologies.

2.2.1 Network Topology Types

Basically there are two categories of Network Topologies:

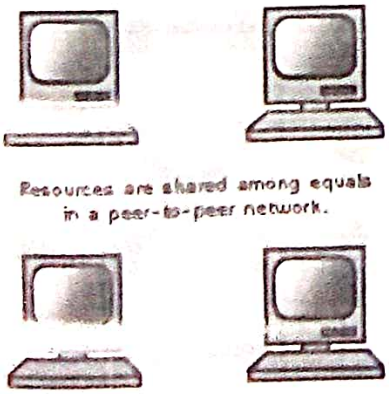
Physical Topology The physical topology is concerned with the physical cabling, nodes location, layout of the cabling and in general the physical aspect of the network. However, this is determined by cost, speed of data transfer and size (Wikipedia 2012.)

Logical Topology

The logical topology deals with the way signals or data interact/travel within the network media from one device to another without disturbing the physical connection. The logical topologies are determined by network protocols while physical topologies are determine by physical layout of cables and network devices (Wikipedia 2012.) Every physical topology has its own set of rules and standards which determine issues such as cable length between nodes, segment number including computer per segment and speed of data transfer (Cisco 2012.) **The most common network topologies are:**

- Peer- peer topology
- Star topology
- Mesh topology
- Bus topology
- Ring topology
- Tree topology
- Hybrid topology

Peer-Peer Network:



GRAPH 2. PEER-PEER Network (adapted from network topology, Winkelman)

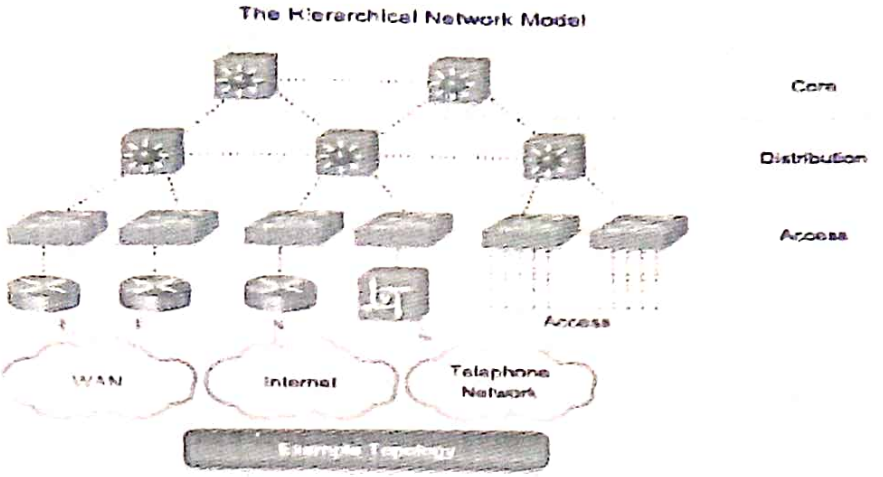
This connection is very easy to establish and it connects two endpoints within a network. In Peer-to-peer network operating systems enable users to share resources and files located on their computers and to access shared resources found on other computers. (Winkelman 1997-2011.) it is also one of the easiest types of architectures to create. Individual users have responsibility over who can access data and resources in their computers. Accounts, passwords and permissions are saved in a local data base and are used to determine what someone can do when connecting to your computer. In this topology each computer in this type of network may allow or deny access to other computers, as access to data and resources is controlled on each a machine. for example, a user could share a folder containing a payroll information on his or her computer allowing other users to access the files in that folder. As such, peer to peer networks are generally used in small development and in situations where security isn't a major concern, as in the case of home networks or small businesses.

2.3 Hierarchical Network Model in SMEs

In designing a LAN that will be suitable for Small Enterprises, the basic issue is to understand the design model that will be easy to manage and expand in terms of business growth. The design of LAN requires adequate understanding of the network operation and traffic which will assist in selecting the appropriate network design among other various types of network designs. This will also help in choosing devices that will be effective for the network. (Cisco 2012.) The suitable model in the design of network for Small-Medium Enterprise is to implement the hierarchical network model in which all the devices on the network are separated into different layers for ease of management and one can determine the function

perform by each device on the network easily (Cisco 2012). The Hierarchical design model (see Graph 8) is divided into three different functional layers and each layer does it parts to efficiently deliver frames to the intended LAN destination. The layers are ***Core Layer, Access Layer***and***Distribution Layer***as shown in (Graph 8).

GRAPH



8. Hierarchical network model (Adopted from Cisco 2012)

Access Layer

The main function of the Access layer (Graph 8) is to enable user access the network and controlling which devices are allowed to communicate over the network. The access layer extends from an individual work area to the individual distribution facility. The access layer includes the switches where all access cabling ultimately terminates. Devices like the PCs, switches, printers, hubs, wireless point and IP can also be found in the access layer. (Cisco 2012.)

2.3.2 Distribution Layer

The distribution layer (see Graph 8) serves as a consolidation point for access layer switches. When a multiple individual distribution facility like switches is distributed around a building, the signals or blinks from each of these switches will terminate at the distribution layer switch. The distribution layer is responsible for pulsing enforcement and inter-van routing. The switches at the distribution layer are of high

performance devices that have high availability and redundancy to ensure reliability (Cisco 2012).

2.3.3 Core Layer

The Core layer (see Graph 8) access the consolidation point of the distribution layer network devices, and it is a high speed redundant network backbone. An example of a network core is the equipment that ties together the multiple distribution layer switches in COU = A UNIVERSITY network layout. The core layer must be highly available and redundant hence being capable of transmitting large amount of data quickly. (Cisco 2012.)

2.4 Benefit of Hierarchical Network

There are many benefits associated with Hierarchical network model among them are as follows:

Scalability: Hierarchical networks can be expanded easily and more devices can be added on each layer to accommodate traffic.

Redundancy: Redundancy at the core and distribution level ensures path availability.

Performance: Link aggregation between levels and high performance core and distribution level switches allow for near wire-speed throughout the network.

Security: Port security at the access level and policies at the distribution level make the network more secure.

Manageability: Consistency between switches at each level makes management more simple and easy.

Maintainability: The modularity of hierarchical design allows the network to scale without becoming complicated. (Cisco 2012.)

2.5 Principle of Hierarchical Network Design in SMEs

2.5.1 Network Diameter

In designing an efficient LAN network for SMEs, it is highly important to consider the network diameter, which is the longest path of the shortest paths a packet takes to get to its destination from source. Similarly, it could be regarded as the numbers of devices a frame encounter before it gets to its final destination. (Anand 2010, 4-27.) Each switch on the network introduces some degree of latency, which is the time spent by devices to process a frame and the lower the latency the better the network (Cisco 2012). In the hierarchical network, the diameter should remain consistence for better performance of the core layer hence the distance from one end device to another should remain the same. (Pasricha &Jagu 2004, 81.)

2.5.2 Bandwidth

The amount of data that can be transmitted in a fixed amount of time is called bandwidth and it is express in bits per second (bps) or bytes per second (Pasricha &Jagu 2004, 70-71). An ideal network structure should be able to provide optimal bandwidth utilization. The network bandwidth can be aggregated by combining two or more connections to achieve a logically singular higher bandwidth connection. However, once the bandwidth requirements of the network are established, links between specific switches can be aggregated, which is called link aggregation. Link aggregation allows multiple switch port links to be combined in other to achieve higher throughput between switches. (Cisco 2012.)

2.5.3 Redundancy

The concept of redundancy is an important factor is LAN design because its account for network availability. It is the ability of the network to survive a single cable failure in switch-to-switch links. Redundancy is of high important in a LAN network for SMEs because of high exchange of resources and failure in the

communication links can result in negative consequences that can lead to loss of data and bad quality of service. Redundancy provides alternate links to the core and distribution layer in case of any fault in links. (Cisco 2012.)

2.5.4 Converged Network

Small and Medium Enterprise are integrating the concept of voice and video communication over data network for smooth and reliable operation. The devices needed to actualize the video over internet protocol (VoIP) are quite expensive and depend on size of the organization to be able to afford the cost. It requires some special switches and other network infrastructure that require complex management to make it effective. The advantage of a converged network is that it is an advance technology and it is just one network to manage because they all converge onto single hierarchical network. (Cisco 2012.)

2.6 BASIC LAN SECURITY FOR SMALL BUSINESSES

This chapter emphasizes the need to protect activities on LAN network by providing basic security against any threats and ensuing that the network is secure. For every resource exchange within and outside the network there is always need for data integrity and this can be achieved by ensuring that no external intrusion has access or tampered with the data hence affecting its original state. LAN network is a network where devices are connected and resources are exchange, however maintaining network security is the act of preventing and ensuring transmission on the network access is always secured. Most organization spent huge sum of money and time protecting their data and ensuring their network were never comprised hence affecting data integrity. Most company does have their assets in form of data stored on their server and they do protect it from unauthorized access by creating a data usage policy which constitutes correct data usage and protection (Cole 2011, chapter 27.) For the purpose of my Project, the security focuses on the minimizing

the vulnerability of the network to threats and unauthorized access. Since it's a LAN network which basically deals with education resources stored on the server which require basic security unlike Banks data stored in their network servers require adequate and optimal protection. Most of the service on the LAN will be internal and little will be external hence there will be need to protect the network from internal threats also.

threats

With an increasing in the number of users having connection to networks results in security threats and causes harm on the increase. For the fact that information are being transmitted across the network, there is need to maintain information integrity because information over the network are vulnerable to threats. Network threats vary depending on the network operation which is a determines the type of data stored on the network. A government organization requires an extensive protection against over so many factors unlike LAN network for small education purpose. My Project does not focus on finance since the major internet threat is basically on the issue with financially motivated firm. Possible observable threats for the scope of my Project include but not limited to:

1. **Human error**

Human error could results from direct attacks to computer system or any network device as a result of deliberate action by users. Human error are regarded as internal error and they could also be as result of hardware malfunction, theft of equipment, unauthorized access to server, vandalism and access to the server by a non-administrator. Data can also be theft by giving privileges to users thereby allowing them to download, modify and copy personal file belonging to other users on the network. (Cobb 2011, chapter 3.)

2. Natural cause

Aside human error threats can also result from environmental disasters such as hurricane, tornadoes, fire, floods, earthquakes, lighting and thunder storms. Lack of fire extinguisher in offices, building located near to flood or earthquake prone area, exposing the network intense or non-pleasant temperature and many more were many causes of natural threats to network (Petri 2011.)

3. Viruses and Worms

Viruses could be regarded as a piece of code that is loaded onto a host computer without the knowledge of the user, however this program run against user wishes and causing a huge amount of damage to user computer. Virus can be notice when user computer freezes as result of downloading malicious program or when user open malicious email (Webopedia 2012.) These threats can be curb installing antivirus software like Microsoft expression, Norton and many more.

4. Spam

Spam is flooding the internet with many copies of the same message, in an attempt to force the message on user who would not otherwise choose to use it. Spam [illegible] any physical effect on the network hence cannot destroy the network elements. Spam filters can be used to curb the effect of spamming and spam filters comes with email provider online (Barman 2012.) One can guide against this mail [illegible] by just deleting any noticed spam mail.

5. Password

Password should be a private issue hence user should protect their individual password from unauthorized access. Open password can cause data theft and serious

harm. Network access should also be password protected to prevent external authorized access which might causes major threats unto the network.

6. Shared Computers

By sharing computer with other users on the network may also result in threats. There is need to unchecked remember my ID on the shared computer and never leave a computer unattended to when signed in and always remember to sign out completely any session open. Password should never be shaved and must be changed always to avoid comprehension by unauthorized users. Threats on network are set to capture important personal information and there is need to guide against this every time. The network administrator must be regularly update software and checking for any threats vulnerability but threats such as password attacks still have

2.6.2 LAN Security policy for Small Enterprise

In a Local Area Network there is need for network devices to exchange resources within the network and across the network, hence ensuring that their transactions across the network are threat free. In other for organization to protect their network, there is need for security policy guidance that will serve as overall protector for the organization networks (Barman 2001, 77.) Network management policy varies from company to company and also from country to country depending on size and operations. The policy implementation in a school is different from that implemented in banks, telecommunication and many more organizations. For the scope of my Project the security **policy statement** shall be as follow: It shall be the sole responsibility of the network/system administrator to provide optimal protection and integrity to all educational data and proprietary software system, whether held on the server or local storage media, or remotely and ensure the continued availability of data and programs to all authorized users and members of

staff, and to ensure the confidentiality of all data, software and configuration controls.

...y of Main Security Policy

- The access to the internet and other external service shall be restricted to authorized personnel only.
- Only authorized and licensed software shall be installed on the workstation and shall be done by the administrator.
- Passwords shall be given by the administrator at the initial long-in and users are require to change their password after first logged in and also after every 2-3months or if there has been any notice of comprehension by an external person.
- In case there is need for any hardware or software replacement, it should be reported to the system administrator, which should be fixed in shortest possible time.
- All diskette drives and removable media from external sources must be virus checked and scanned before they are used within the learning center.
- Users are allowed to fill the network log which could be used to monitor the network performance and manage in case there is defect in performance.
- The server and workstations will be protected from virus threats with virus scanning software and the task is the sole right of the system administrator.
- Network devices like switches, router, and hubs shall be protected from unauthorized access and cables shall also be protected from water or any hazard.
- To prevent data lost, back-up shall be carried out regularly and with data can be protected.
- Users shall be informed about the security policy and procedures.

- In case there is virus infection, users shall report as fast as possible to administrator to prevented effect multiplication.

2.6.3 Firewall

Firewall could be regarded as a device that allows multiple networks to communicate with one another, especially when there is communication between a co-operate network and a public network where there is different levels of trust according to a defined security policy (Dameon 2004, 1.) As every investor in the stock market main focus is to protect and manage their investment, so also every organization deem it necessary to protect their network. Network devices need to be protected from external threats during interaction with external devices on different network and ensuring the network is properly secured. Though, Local Area Network offers resource sharing and offers degree of interaction with external network thereby allowing different traffic into the network but to secure this operation there must be a certain security solution within the network. A centralize security solution can be used on an internal network device which can be achieved by using a firewall solution, hence making it much easier to manage security policies and their implementation (Richard 2004, 44.) Many workstation operating systems do come with installed software based firewalls that do protect against external threats from public internet. Windows firewall is included in Windows 7 operating system which assists in preventing unauthorized traffic to pass through the firewall. The administrator can set up basic firewall (in-bound and out-bound) rules, which determine what traffic goes in and out of the network (Panek 2011, 26.) Firewalls are of two types which are the **software based** and the **hardware based**, the software base are internal to computer system and they work with the most operating system because they are built-in software. They are designed to guide only the computer in which they are installed and not the general network. The latter are configured in-between the network and the connecting cable/modem. They are

external hardware devices which are refer to as Network firewalls. Some network devices like Switches do include firewall security built in them. However, hardware firewalls provides high external security against external threats since they are separate devices and possess their own operating environment. The hardware firewall is much more effective and quite expensive unlike the software firewall (Tech-Faq 2012.) For the scope of my Project, the Windows firewall setting was achieved by choosing **Star->ControlPanel->Large Icons View->Windows Firewall** and then clicking Turn On or off for both private and public network. The choice of on or off, the setting on will block external traffic except the one specified and setting it to off will give room to external traffic to connect (Panek 2011, 26-27.)

2.6.4 Network Address Translation

Network Address Translation is an Internet Protocol Mechanism that is described in RFC (Request for comments 3022) as the process where a network device like Firewall, assigns a public address to a computer inside a private network and the main aim of using NAT is to reduce the number of public IP address in a private network. Network Address Translation becomes important when a host with private IP address need to access the public network like the internet (Oppenheimer 2004, 197.) Private network addresses ranges from (10.0.0.0 – 10. 255.255.255, 172.16.0.0 – 172.31.255.255, and 192.168.0.0 - 192.168.255.255) and NAT implementation is common for network using this private addresses. The Network Address Translation work effective for workstation that is having their resources inside the network and they only need to access the file server and printer. The network administrator schedules a pool of addresses that the host can use for translation when the host within the network is sending a packet across the network. The host needs to have a public address in order to get responses from their request hence the NAT is responsible for assigning this public address (Oppenheimer 2004,

197.) Network Address Translation is an important concept in Firewall security because it masquerades the private IP address behind the public address of firewall to communicate with the internet hence allowing for stricter measures of access to resources on both side of the firewall. One public address is required for hundreds of users because when NAT is implemented all users inside a private network have same public IP address. Network Address Translation does offer port address translation for mapping of several addresses to the same address whereby all traffic from a Local Area Network has same address. The port numbers are used to differentiate separate conversations and it reduces the number of needed outside addresses (Oppenheimer 2004, 197.)

CHAPTER THREE

SYSTEM REQUIREMENT AND DEVICE CONFIGURATION

Before deploying a LAN structure for any business operation there is a need for one to ascertain the type of services to be provided on the Local Area Network. My project envisages a small computer training center; whose focus is introducing/training students on basic IT appreciation courses. These services and operations determine the type of hardware and software to be deployed on the topology. It is also better to prepare a base map of the topology to be deployed in case of business growth which requires adding of more network devices. The map will make it easier in integrating additional devices considering the existing topology on ground and help in terms of trouble-shooting. However, it is important to consider the number of hops that data must travel before getting to destination from source. It is important to keep this hops count as minimal as possible hence enhancing performance gains. Network equipment deserves investing in, considering the average life span of network devices like switches, firewall, PCs which is around 4-5years depending on usage but every organization tries to maximize their usage by running equipment for longer time. There could be a port failure and power malfunction if cheaper and less expensive devices were purchased for commercial purpose. Since all data and communications of the business will run through the equipment, it is worthwhile investing in quality devices.

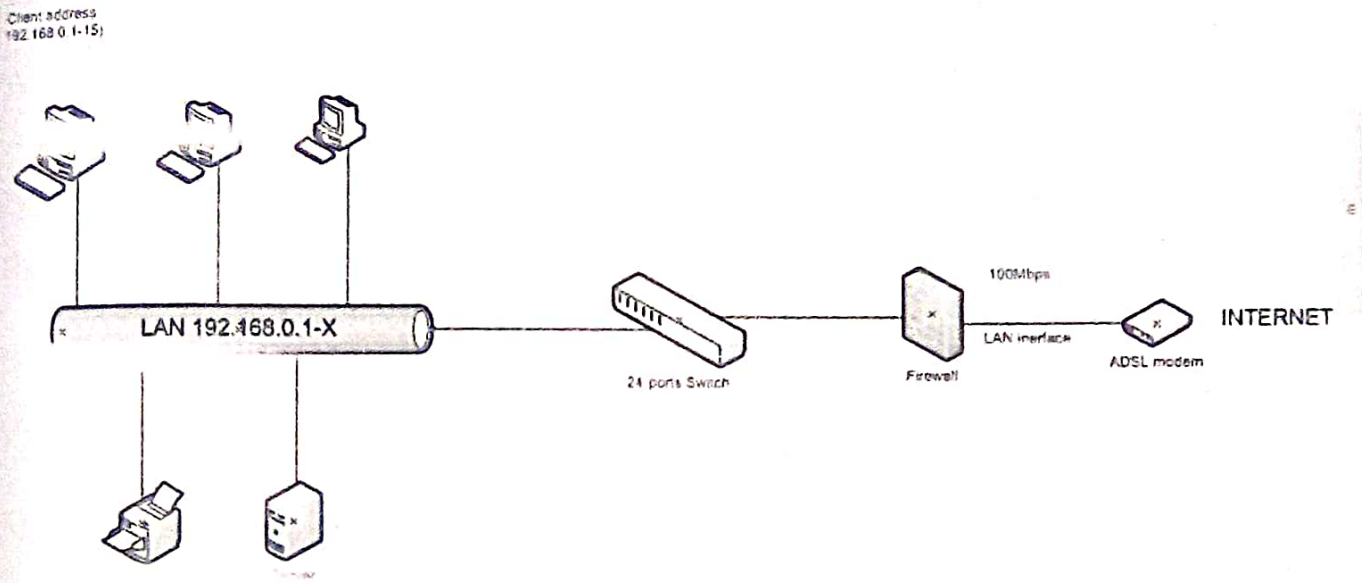
3.1 Physical Topology

An efficient network requires adequate planning to ensure that the network will support the business needs hence emphasizes was made on the following key question while designing the LAN for SMEs:

- What are the needs for the business?

- What important issues should be considered to support the current and future needs of business?
- What is the financial implication/ cost consideration?

SCENARIO



GRAPH 9. Network Topology

The Laboratory work entails the design of the above topology (see Graph 9) and configuration of the network devices for effective operation. The Ethernet LAN consists of 15PCs, a 24-port switch, an ADSL Modem, Network Printer, Firewall and connecting cables as presented in the topology diagram.

3.2 Hardware Requirements and Configuration

General requirements

A minimum of 1.0 Mbps to any host computer in the LAN and 100Mbps to the server host in the LAN was envisaged. There should be an access to the internet from any host computer in the LAN. I implemented a file server for study material

and student account management. TCP/IP routed protocol. Bus Topology was implemented.

The required hardware devices for the design of the LAN are as follows:

15 workstations for student and staff with individual account

A Network Printer

ADSL Modem (since it's a small network, it is always cheaper to purchase device that can perform multiple functions like the ADSL Modem that can also act as the LAN in built in a single device)

File server

NIC (Network Interface Card)

Connecting cables

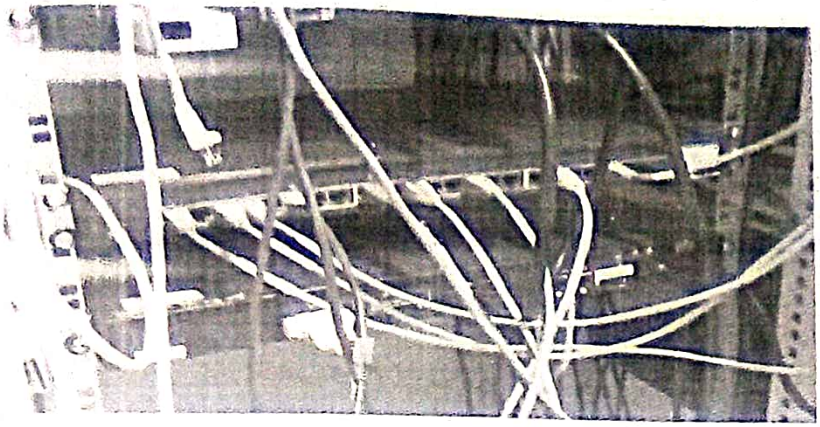
Cooling Fan

Cabinet

UPS

Backup(RAID SYTSTEM)

A Standard room

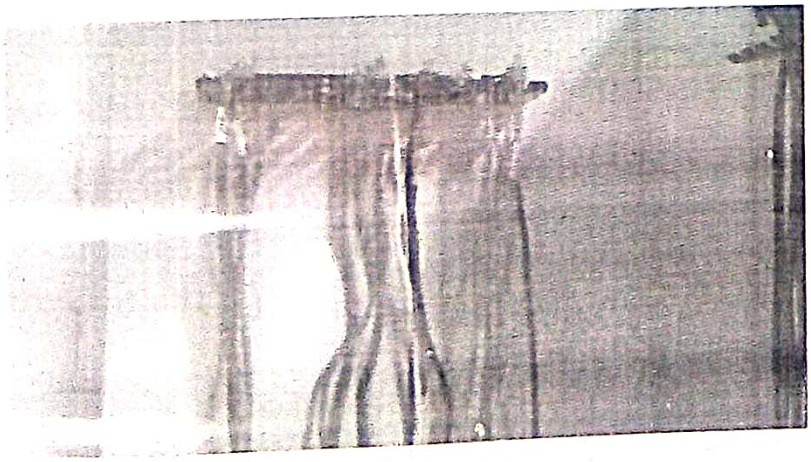


GRAPH 10. 24 Ports Catalyst 2950 series

The term switch (see Graph 10) is a short form for "switching hub", it enables the cables to connect up and branch out. Switches are different from hub because they only send packets to the intended recipient while hub broadcast all packets to every host on the network. (Ross 2009, 28.) Data switches are available in several sizes and shapes with port sizes ranging from 4,6,8,12,24 ports and selection is based on [illegible] scope (Ross 2009, 30.) Each node on the network connects to the switch via a cable plugged into a socket called *port*.

Switch configuration

There was no special configuration done on the switch. However, the switch was designed to provide different channels to and fro the network via the ADSL modem that acted as an interface to the internet.



GRAPH 11. Connecting Cables

The cabling was carried out as shown in the topology. The cables were run from the switch to the network out on the wall where each host can connect easily via an Ethernet cable and a connector. All the Ethernet cables consist of 4 color-coded pairs of wires twisted together: brown with brown and white, green with green and white. Ethernet cables and connectors include Category 5 (CAT5), enhanced Category 5 (CAT5e) or Category 6 (CAT6) depending on the amount of data transmission and sensitivity to interference (Ross 2009, 27-30.) For the purpose of my Project CAT5e was used because of its reliability, cost and performance in a small network.

Workstation PCs

The selection of PCs to be used as workstations was based on the activities/Task on the Network. The PCs that will be used for workstation must meet the requirement and be compatible with software to be installed on it. The PCs were only used for training purposes.

The specification includes:

Processor: Intel core i3-2120 processor (3MB Cache, 3.30GHz)

Memory: 2GB*2 dual channel DDR3 SDRAM at 1333MHz

Hard drive: 250GB* 2 SATA hard drive (7200RPM)

Video Card: Intel HD Graphics (VGA, HDMI)

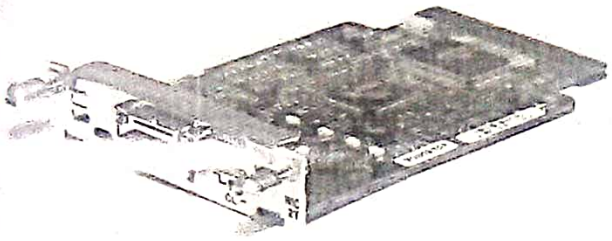
Optical Drive: 16x DVD+ /RW Drive

Configuration:

To configure the PCs for the workstation, the basic configuration was to make them efficient to be compatible with the activities on the network. The basic configuration is to ensure that the PCs contain slots for NIC (Network Interface Card) card which

allow access of the PCs to the network (Nelson 2003, 57.) The MAC (Media Access Control) address uniquely identifies system on the network based on the MAC address written on the NIC card.

NIC (Network Interface Card)



GRAPH 12. Cisco Network Card (adopted from Cisco 2012)

The NIC is an important component in networking and it is a separate expansion card that is fitted into an expansion slot on the system board inside the PC case. It provides the physical connection between a computer and a network cable including other transmission medium and a computer cannot communicate on a network without a network interface card (Nelson 2003, 59.) The NIC receives electrical signal pulses and translates them to binary data while during sending data, the NIC converts computer data into energy pulses and transmits them on network media. It functions at the Data Link and Physical Link of the OSI model. (Cisco 2012.)

Configuration of NIC

The configuration is done in three stages as follows:

IRQ (interrupts request) setting: This enables direct communication between the device and CPU. (Nelson 2003, 59.)

I/O (input/output) ports: This identifies memory area used to transfer information between CPU and NIC. (Nelson 2003, 59.)

Base Memory Address: This assigns a memory buffer area to store incoming and outing data frames. (Nelson 2003, 59.)

Basically these devices come with installation CDs and make installation much easier nowadays and everyone can install common network devices easily. (Nelson 2003, 59.)

File Server

A file server is nothing but PC with higher functionality than PCs used as workstation. A server computer is more suited to do the work it is designated to do and it is built with more expensive parts depending on it purpose. It is the central computer responsible for managing the network and host using the NOS (Network operating system) and all application software (Anand 2010, 16.) It contains programs and data and makes them available to hosts on the network. A server PC is different from workstation PCs in the sense that it needs to be more reliable.

Configuration

...figuration of a server depends on the number of users, volume of data being stored and processed, speed required and majorly on task it is been schedule to execute. The PC to be used as a server must be configured to include a Dual ... Redundant Hard drives or power supplies, scalable to meet current and future needs and able to process data faster and more efficiently.

Network Printer

A network printer (see Graph 12) is the same as printer but differs because it can be accessed by all hosts on the network. However, it is assigned a unique IP address on the network for identification.

Configuration

The configuration is done by connecting the printer via an Ethernet cable with a connector to the network and installing the driver that came with the printer on the server. This gives access to all the hosts on the network.

ADSL (Asymmetric Digital Subscriber Line) Modem

GRAPH 13. Cisco Adsl Modem (adopted from Cisco 2012)

The ADSL modem is a network device that has an interface to the ISP (Internet Service Provider) and to the LAN; it can function as the router and provide connection from the ISP to LAN. This is similar to same topology in COU (UNIVERSITY Network), where the ADSL connects to splitter and from there to the switch where the hosts have access. The ADSL modem offers basic network functionality such as NAT (Network Address Translation) and DHCP (Dynamic Host Configuration Protocol), which one can use to have access to multiple private addresses for a server and hosts but for the scope of my Project a static IP address was being used. Much of the addressing will be discuss in the later chapter.

Configuration

For the scope of this Project, the modem was just configured to allow access to the internet hence providing access to the internet to the hosts and other network devices via the switch.

Backup

f transferring data from business hosts to separate storage devices such as a tape drive. There is need to backup important data files and this backups can be carried out periodically in case of accident or other permanent interference the network. For the scope of my Project since it is a learning Centre, backup will be carried out weekly on system files and daily on critical files and data files. Backup will be carried out using a tape of size 500TB for my d can change due to circumstances.

Configuration

No special configuration was required because the device was plugged into the USB port of the server and the driver will be installed for its compatibility.

UPS

The Uninterruptible Power Supply is an alternative power source for the mains power supply. The capacity depends on networking power consumption. It is much needed due to my business environment.

Cooling fans

Cooling fans provides cooling effect to subdue the heat produce by network devices t their performance and may results to delay in data transmission.

The cabinet is a location for the switch, modem and other core layer equipment and at this point all the wiring that connects to the network converges. The cabinet can sometimes be referred to as wiring closet (Ross 2009, 50.)

3.3 Software Requirement and installation

Software requirement and installation is an important aspect of my Project work because it entails the installation of different software, which is regarded as set of instructions in form of programs, data or code for the effective operation of the hardware on the network and in processing of data. Some of the hardware was designed with an inbuilt operating system which allows the hardware to work efficiently on the network. The type of operation in an organization determines the kind of software to be installed on workstation and they vary for different organizations. Software can be divided into two categories which are:

System software

The system software includes operating system, servers, device drivers, compilers and all other utilities that enable the computer to carry out its function. They provide a basis for running application software.

Application Software

Application software is regarded as programs that do real work for users. They Microsoft Office, database management systems, Pdf readers, 7-zip, internet browser, Skype and many more. The application software is simply regarded as application for end users. The application software cannot run without the operation software. For the scope of my Project, the major system and application software's that will be require by the host computers and the devices on the Local Area Network will be discussed. The required software includes:

Windows 7 Operating System

Device drivers

Windows Server 2008 R2

Programming compiler (Eclipse, NetBeans)

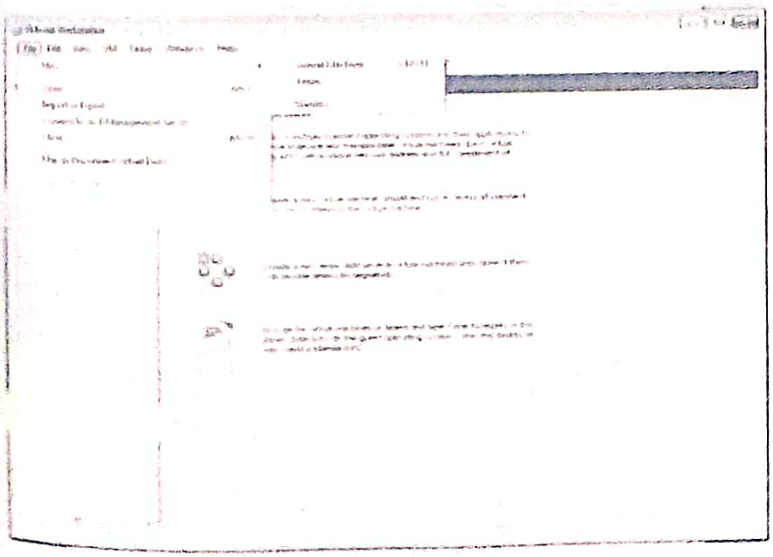
Freeware software which include: Microsoft Office, Pdf-reader, 7-Zip, Internet explorer

Imaging Software which includes: Fog, Clonezilla, Symantec Ghost, Altiris

Installation of Windows 7 Operating system on Host computers

The host's computers were prepared to meet the requirement for the installation of a Windows7 Operating System. The laboratory work was done with a virtual machine already installed on a CNA Lab computer for the purpose of practice. The network was bridged to use the local environment different from school network which made it easier to work with the virtual machine having access to the internet. The Procedure for the Installation of window 7 OS on our VMware was as follows:

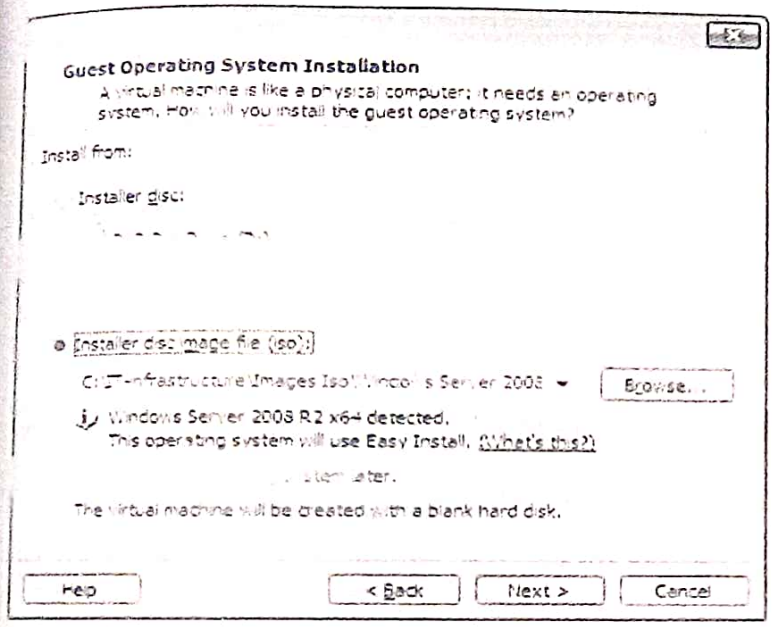
select file->new->Virtual machine as show in (Graph 15)



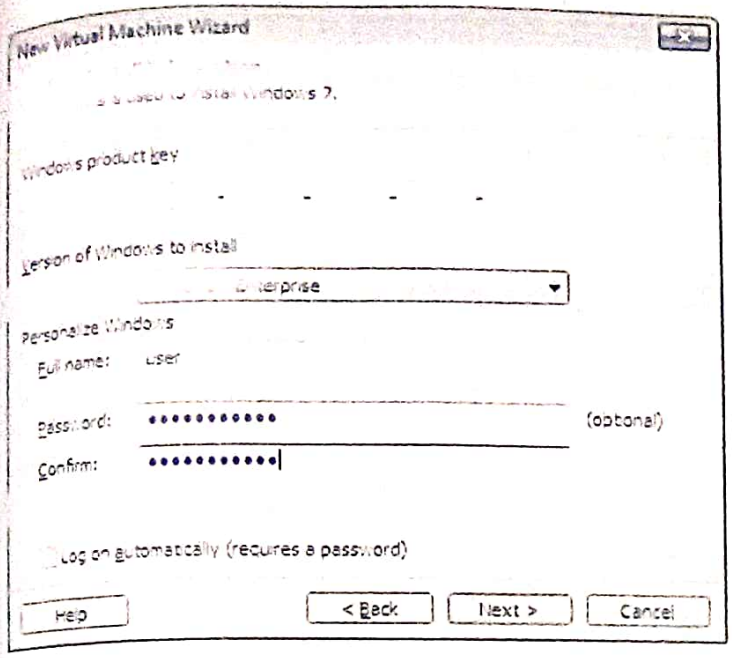
GRAPH 15. Starting new Virtual Machine

Select typical (Recommended)installation mode for fast and easy installation.

Select Installed disc image file (ISO) (see Graph 16) and browse the location of the DVD image file on the host computer hard disc. This is the location where we will load the installation data. The Image file is a single file used to store DVD or CD information and it is a kind of a virtual DVD. Click next.

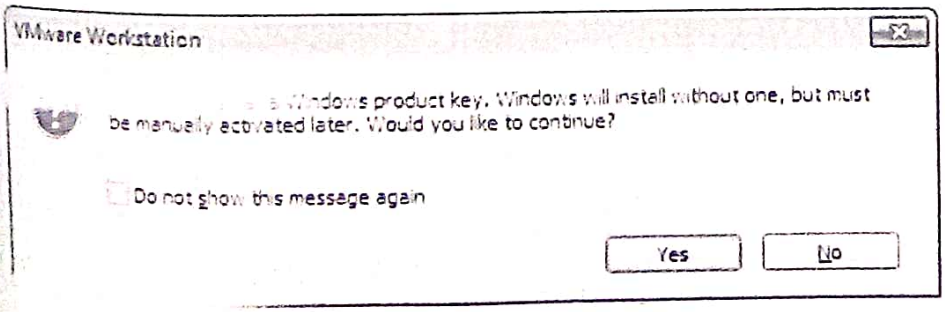


GRAPH 16. Window showing access to Image File



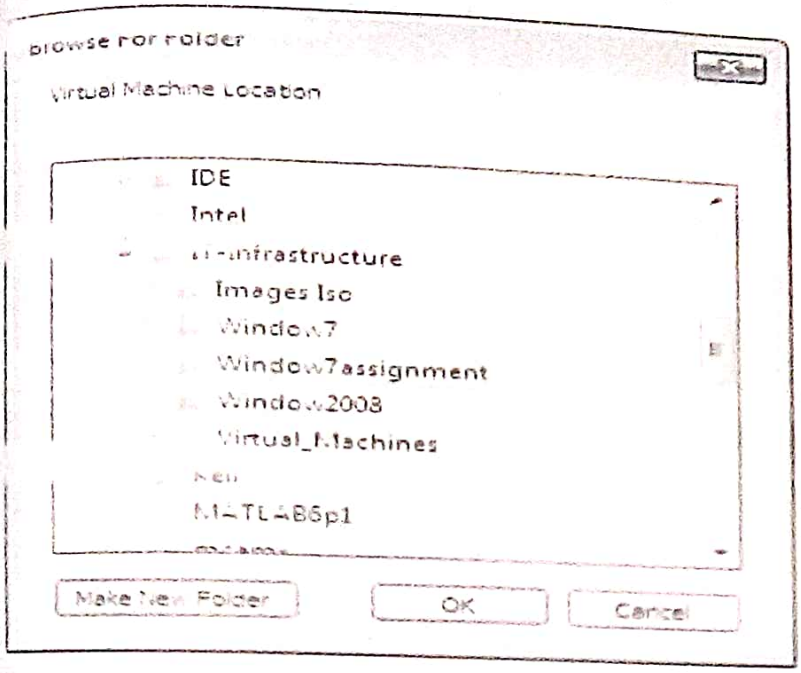
GRAPH 17. Password and Product Key request

We do not need to enter Windows product key (see Graph 17), as the Windows7 2008 can be operated for 30 days without the product key. Select Windows 7 Enterprise version to be installed. There can be multiple versions of Windows in the installed image file. Enter user as the full name and a password. enter a password twice to eliminate the possibility of an error in the writing. Click next. You might get an information window telling you about product key (Graph 18) as shown below just Click next as we are aware that the product key is missing and click yes to continue.



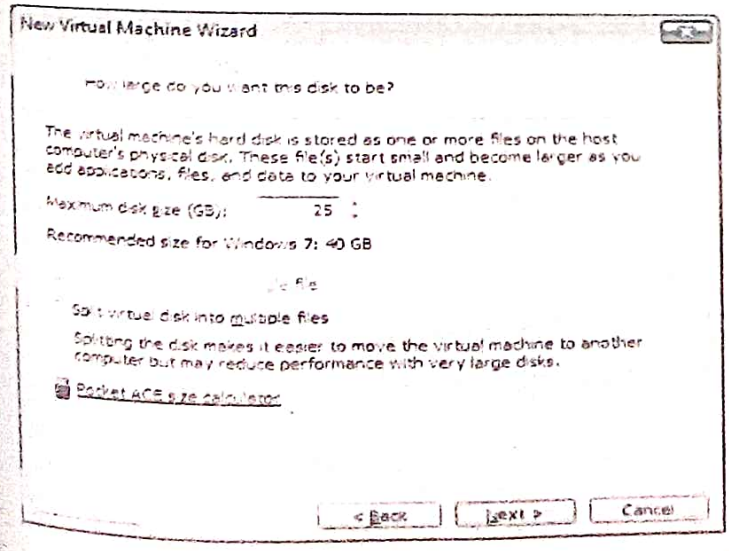
GRAPH 18. Information on Product Key

The virtual machine was named Windows 7. A location was selected to store the virtual disc file of the virtual machine. It must be somewhere where you can find it easily later on, so I made a new folder (see Graph 19) as shown **C:\IT-infrastructure\Windows7assignment.**



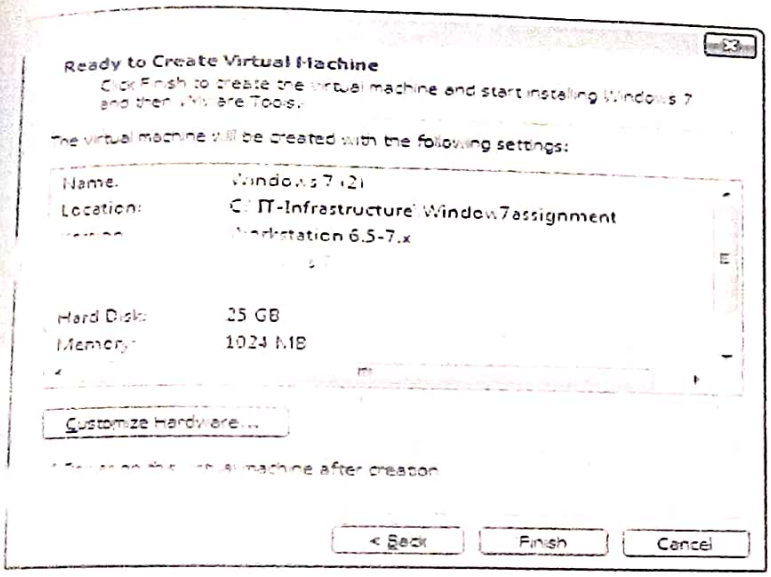
GRAPH 19. Folder for new Window 7

OK was selected and the below window was displayed (Graph 20). I selected clicked next and specified the disk size as 25GB as shown (see Graph 20) which will be enough for the required task.



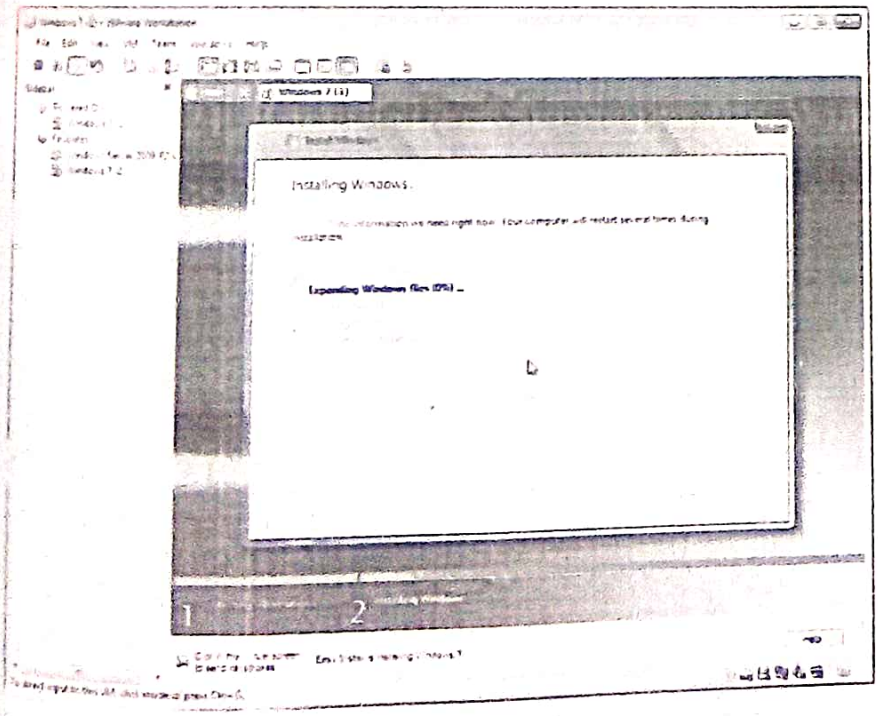
GRAPH 20. Disc size specification

(see Graph 20) and there was a summary screen (see Graph 21) where you can review the settings. After the summary window, the finished button was selected (see Graph 21) to complete and next to boot up the new virtual installation of Windows 7 can start.

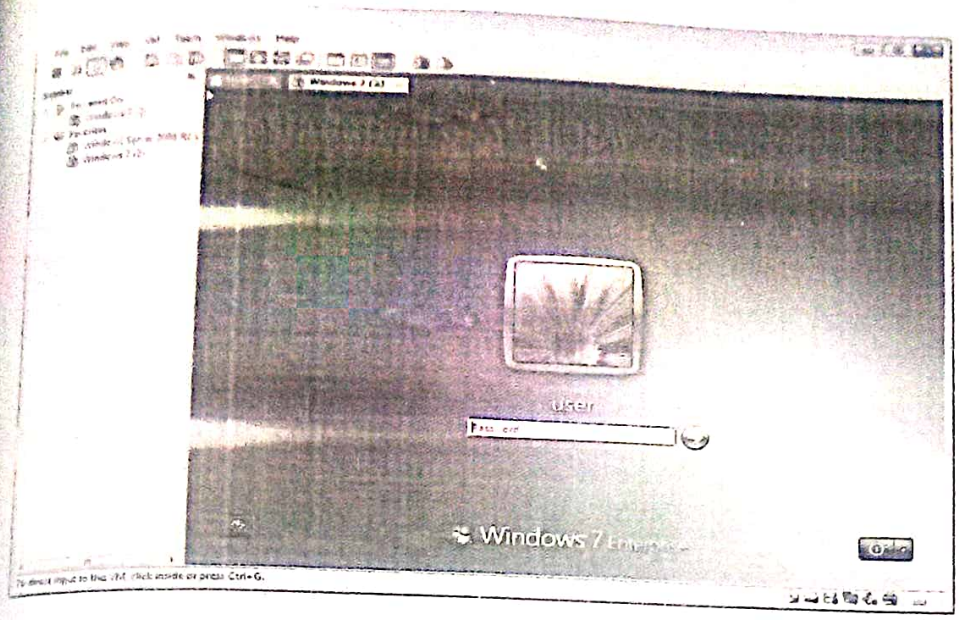


GRAPH 21. Installation Summary for Window 7

OsThe (Graph 22) shows the installation process.



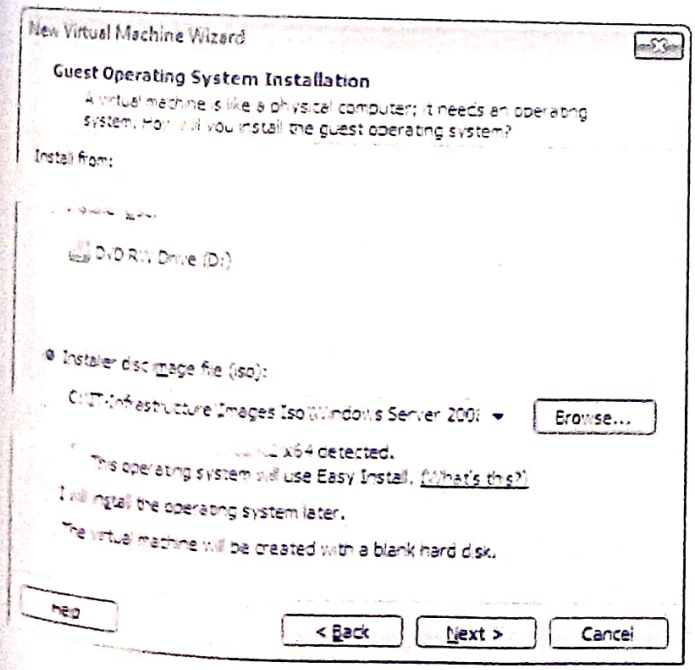
GRAPH 22. Installation of Window 7



GRAPH 24. Screen showing complete Installation of Window 7

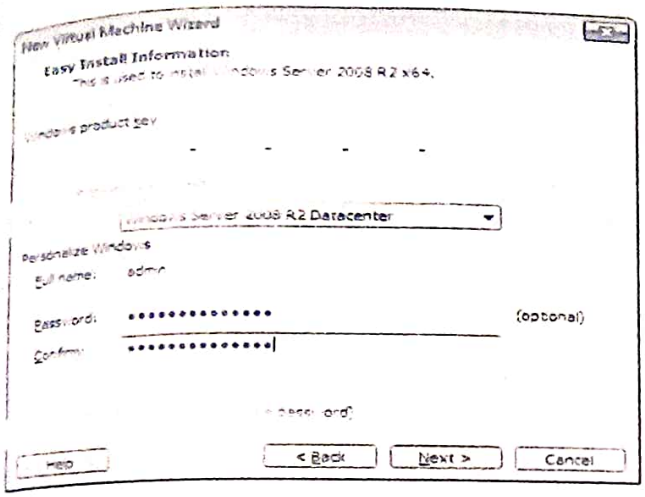
INSTALLATION OF WINDOW SERVER 2008 R2

The same installation process similar to that of Window 7 is also applicable for the window server 2008R2, the ISO file (image of an entire CD, DVD represented in a single ISO file) was selected (see Graph 25) and the standard R2 was selected and click next to proceed.



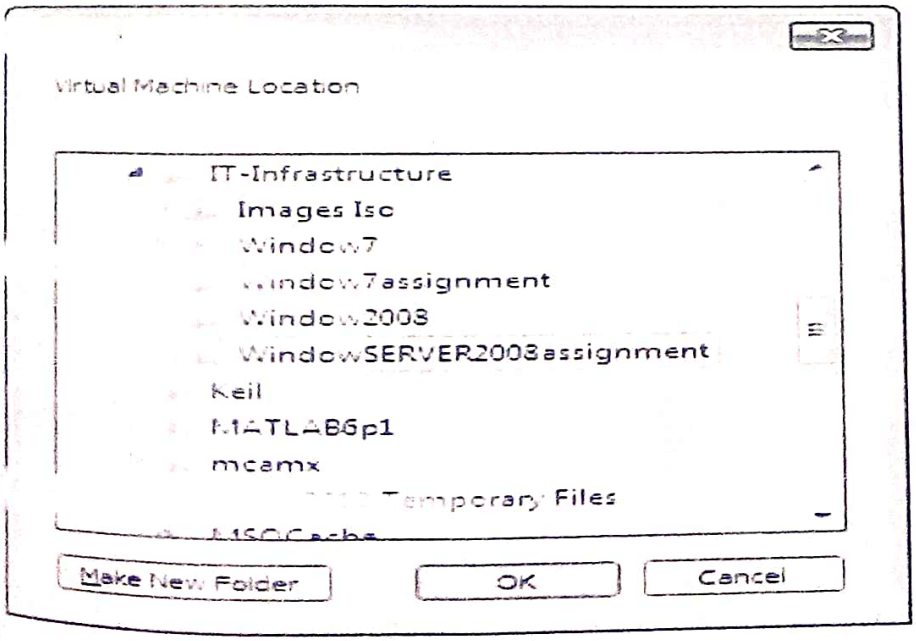
GRAPH 25. Image File for Window Server R2

The requested name and password was entered according to specification and next was selected to proceed (Graph 26)



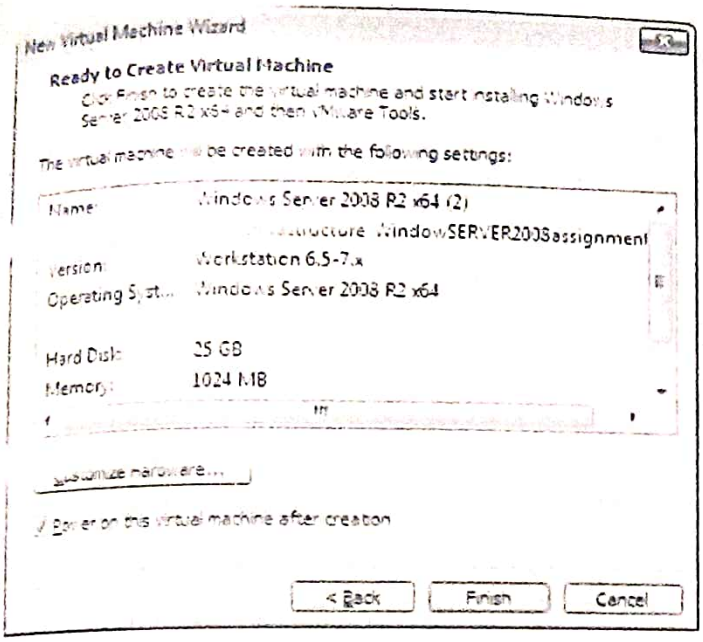
GRAPH 26. Screen showing personal Windows Information

A subfolder was also created similar to that of Window7 and named WindowServer2008assignment (see Graph 27) and saved.

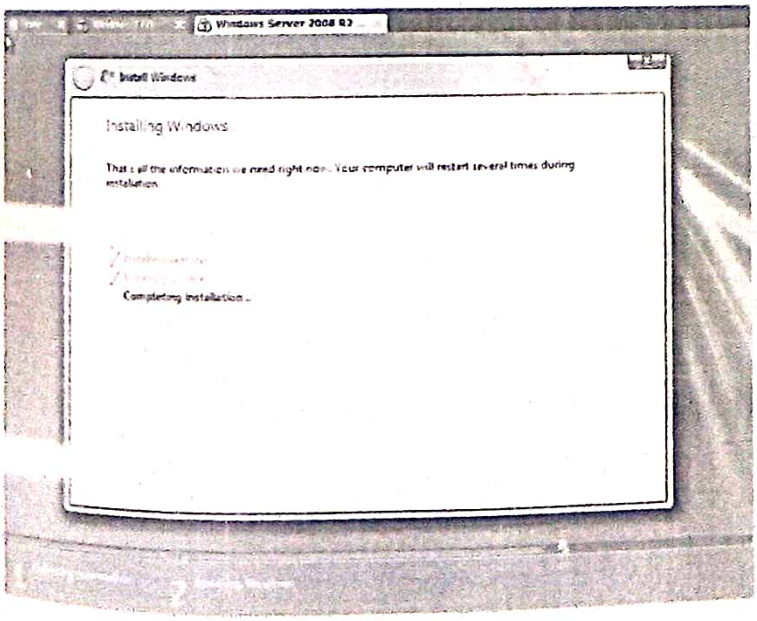


GRAPH 27. Folder for new WindowsServer2008

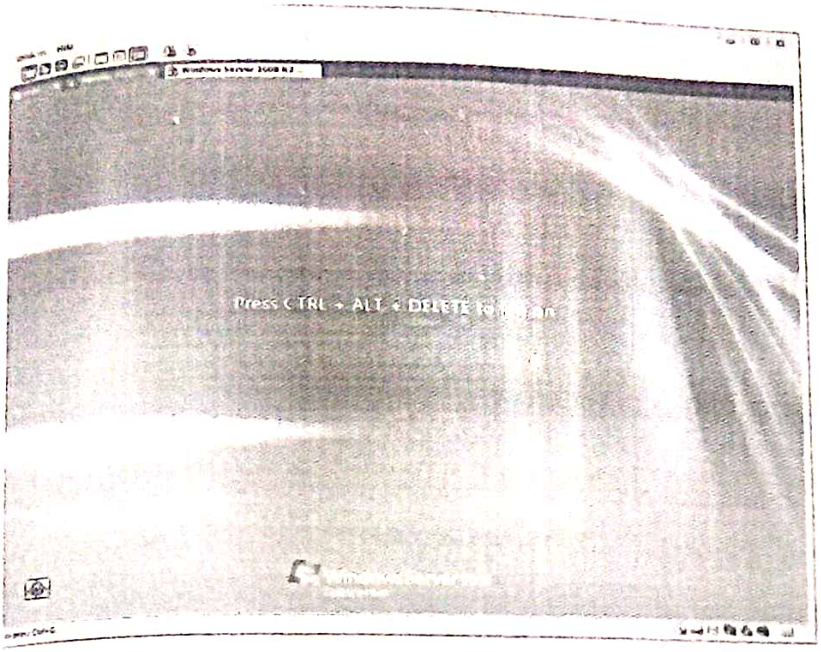
The disk size was also given to be 25GB and next button was selected to continue the installation. After specifying the disk capacity, the summary window (see Graph 28) appeared and Finish was selected and the installation process for the window server starts and continues as show in Graph 29. The complete installation was shown in Graph 30.



GRAPH 30. Summary screen for Windows Server



GRAPH 31. Installation process for Windows Server 2008



GRAPH 32. Completely installed Windows Server 2008

Imaging software

The imaging software is used to automate system software and program software installations on the workstations. These are achieved by making a master image with one computer and clone that image to the rest of the computers. Imaging software includes Norton, Symantec, Altiris the freeware Fog and many more.

Device drivers

The device drivers are program that controls a device (network printer) and many device comes with the operating system but for other devices, one may need to load the driver when the devices is connected to your computer.

Application software

The application software are freeware and do come with an installation CD/DVD that entails the installation procedure. The installation of application software such as Office, 7-zip and many more were always easy to download and install.

Network Bandwidth

Bandwidth is the amount of data that passes through a network connection over a period of time and it is measured in bits per second (bps). A LAN refers to interconnected computers within a small geographical area where the hosts can effectively share resources. However, for a LAN to be effective there is a need to consider the bandwidth usage of the network and LAN usually has a very high and super data transfer rate. The next step in designing of a local area network for small business is to estimate the broadband by considering the traffic flow within and across the network. Bandwidth is defined as the communication capacity of a channel. The host's quality of service (QoS) on a LAN is very important and it depends so much on the network bandwidth, and the traffic generated from device and hosts on the network. All application uses varying bandwidth and the network bandwidth can be monitor by various network bandwidths monitoring software. The installation and procedure for LAN monitoring is outside the scope of my Project but it is important to estimate the LAN network bandwidth by estimating the traffic from different sources on the network. Considering the fact that my Project provides a simple networked solution for a small office and it is a traditional LAN setup with a single 24-ports switch, including 15 hosts and an ADSL modem acting as a router to route IP to the network. It was established that the bandwidth will be shared by all the devices and hosts on the network, unlike VLAN (Virtual Local Area Network) which consists of different LAN segments and can offer more bandwidth (Clark & Hamilton 1999, 122-123.) The LAN was designed so that all the hardware

on the network are faultless and also the connecting cables, Ethernet adapters are error free because any problem with the LAN hardware can result in slow or non-functional network.

Estimation of bandwidth

I considered a case of a computer institute that consists of 15computers, operating for 8hrs daily. The most bandwidth requires application on the workstations is [illegible] designing software for creating 3D CAD engineering drawing.

ESTIMATION OF BANDWIDTH CHOICE

15 Students with 300MB of data downloaded everyday per student. Working hours is 8hrs per day.

Bandwidth calculation

[illegible] of data downloads for 8hrs

data per hour 4500/8 = 562,5MB per hour

562,5/3600 = 0.156MBps

Since 1Byte = 8bits:

Which is the same as 0.156*8 = 1.248Mbps.

The download rate of the institute was greater than IMbps (Megabits per sec) and for cost effective, a download rate not greater than 10Mbps will be advisable. The institute uploads 4GB of data every day to clients during the night hours. At this point there is less traffic on the line because it is not working hours. The upload rate [illegible] longer time at the speed of IMbps and which is enough for the data to be uploaded. It will take 8-9 hours to upload 4GB of data at that speed.

To calculate the times required for uploading this amount of data:

Since the non-Operating hours were from 10pm until 6am which is 8 hours, we can decide to have the upload rate as:

3200Mbp 8hrs which is equiv. to 3200/(8*60*60)= 0.1Mbps , so at this rate its going take 8hrs to upload before working hour to minimize cost hence the best option in term of cost and efficiency is: **10Mbits/s download rate and 1Mbits/s upload rate at 55Euros per month.**

CHAPTER FOUR

4 LAND ADDRESS PLANNING FOR SMALL BUSINESSES

The importance and essence of any network is the ability of the network devices and hosts to communicate and be able to share resources within and across the network. For communication to be effective there must be a message sent to a destination from a source and vice-versa. All networks recognize two kinds of addresses which are the logical (network layer) and physical (or Mac or hardware) address. The MAC address are assigned to device's NIC (Network Interface Card) by the device manufacturer while the logical address are manually or automatically assigned following some certain sets of protocols. In the TCP/IP protocols the IP is the core protocol which is responsible for logical addressing hence the networking addressing are basically call IP address. (Dean 2009, 147.) More devices are making connection to the internet as technology advances and it has been suggested that at a point the IPv4 addresses will be exhausted and in solving this problem gives room to new version of IP address called IPv6 that will complement for IPv4. However, IPv4 addresses were still so much in use and they co-exist with IPv6 for a significant amount of time through certain transition mechanism. The IPv4 addresses can be represented in a dotted 32 bits format while the IPv6 have a size of 128bits and it has so much large address space over IPv4. (Mun & Lee2005, 115-[illegible]) In a LAN network design for small business, every host needs to communicate with a resource on another host or on another network outside or within the organization (Cisco 2012.) The communication could be inform of sending and receiving emails, accessing new products on web-site, instant messaging, file sharing and many more. The subject of address planning is synonymous to post office procedure of letter delivery, in which the sender address must be established. Likewise, for a message to be sent on a network there is need for proper address

planning and with this plans one can establish an effective internet and intranet communication. Addressing is a key feature in network layer protocols that enables efficient communication between hosts on same or different networks. Information on the network are in form of packets or frames which needs to be identify with the source and destination addresses at ends of the frames. The device on the network must understand the concept of TCP/IP to exchange information on the network. All small business was designed with the objective of meeting the future challenges of new applications as the business grow and a key factor is achieving this by creating a flexible and scalable IP addressing structure that can support the growth (Reid & Lorenz2008, 13

IP addressing in LAN for Small Enterprise

IP addressing is an important factor in transmitting packets/frames between host on same LAN and over the internet. It is a method of identifying hosts and devices on the network , however to send and receive messages on an IP network, every host must be assigned a unique 32-bits size address which are typically represented in a format known as dotted decimal. The 32-bits length address can be broken down into four octets (1 octet = 8bits) and each octet is converted to decimal number and separated by dots (Reid & Lorenz2008, 138.) Considering for instance an IP which is represented in dotted form decimal known as octet in the form of **10.10.16.1** that is only associated to IP-v4. The value in each octet ranges from 0-255 Decimal which is the same as **00000000-11111111** in binary; hence the above IP address is the same as **00001010.00001010.00010000.00000001** in binary. By convention, the first few bits of the address indicate the class that the address belongs to:

TABLE 1. Summary of IP address classes (Odom 2004, 103)

Classes of address	Size of network part of address in	Size of host part of address in bits	Default mask for each class of

	bits		network
A	8	24	255.0.0.0
B	16	16	255.255.0.0
C	24	8	255.255.255.0

The ranges of addresses that fall within each class are

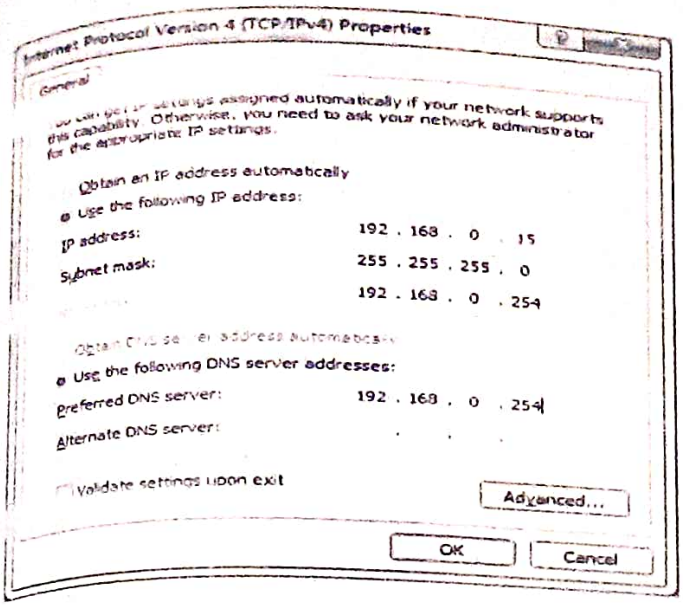
Class A 10.0.0.0 – 10.255.255.255

Class B 172.16.0.0 – 172.31.255.255

Class C 192.168.0.0 – 192. 168.255.255

Scenario

The addressing of the network devices was carried out after cable connection had been completed. This was to ensure that the host can communicate with each other and also with the ADSL modem, which was the network interface. The ping command was used to test connectivity within the LAN and also outside the LAN by pinging a random website. The ipconfig /all command were used to display the summary of network information.

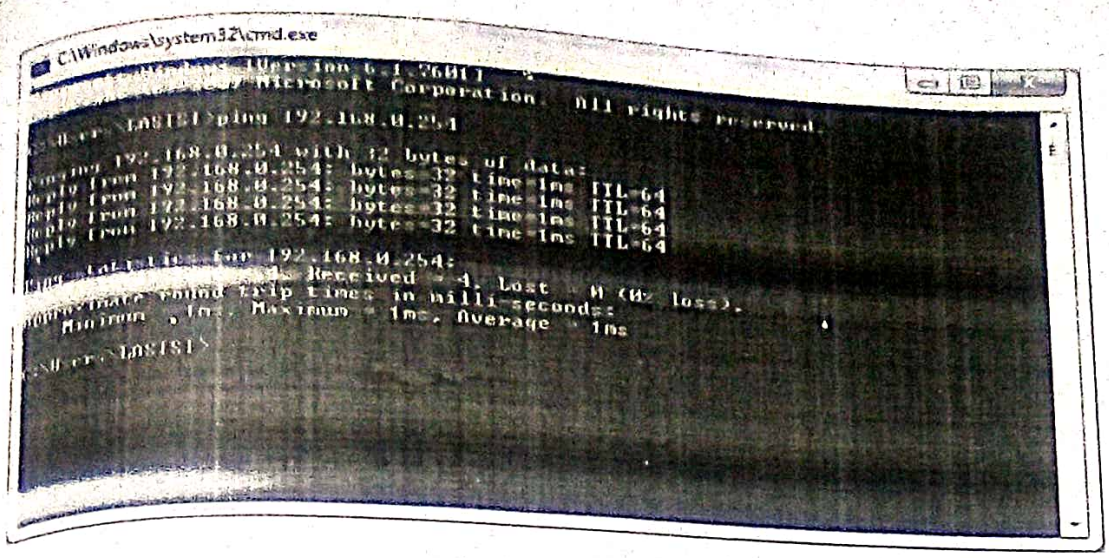


GRAPH 33. Host addressing

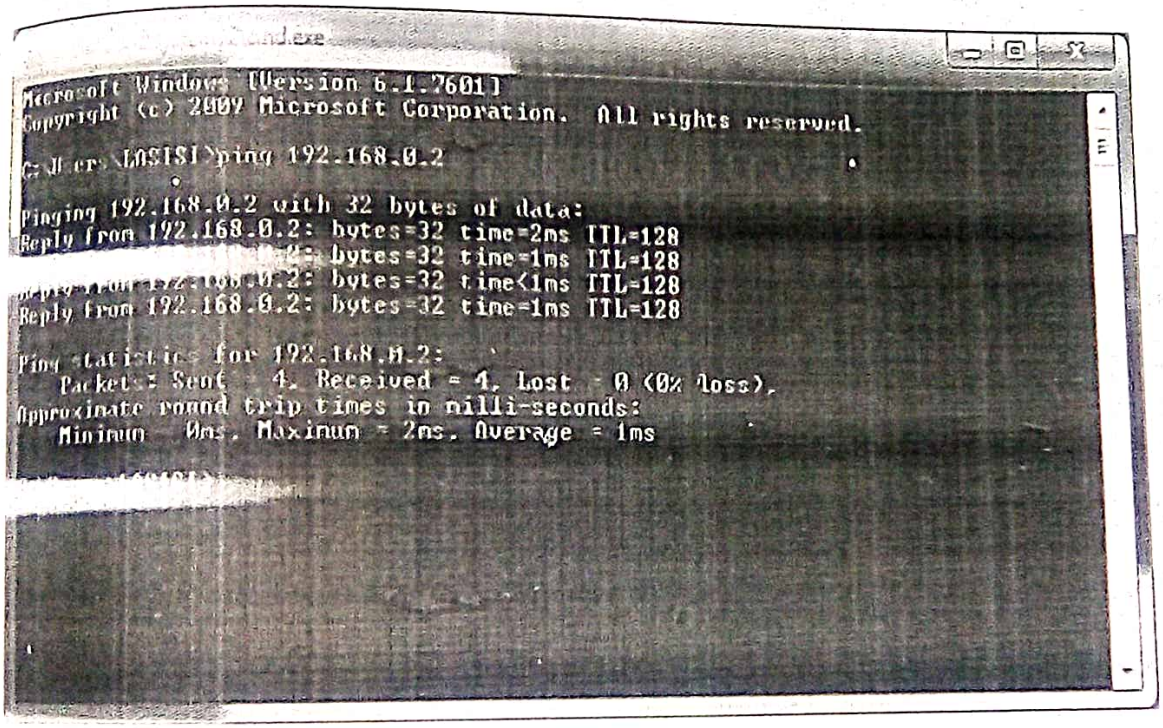
Graph 33 illustrate the IPv4 addressing set-up for the hosts IP address 192.168.0.15 , subnet mask 255.255.255.0 and default gateway of 192.168.0.254 which was the address of the ADSL modem in the network..

Connection testing:

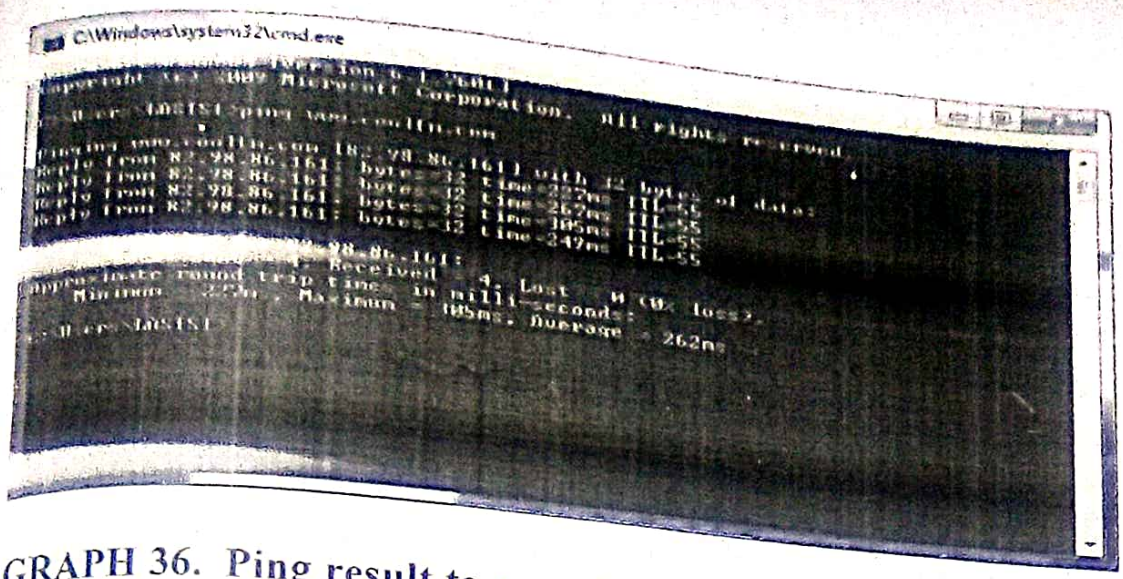
After the addressing of each host with individual unique IP address the connection to the ADSL was tested by using the command **ping 192.168.0.254** and the result was displayed in Graph 34, which indicates that the connection to internet and back to the host was successful. The connection to individual host was also tested by pinging their unique IP address with the command **ping host Ip address.** Pinging at host **192.168.0.2** show the result display in Graph 35.the result shows that the pinging was successful hence host communication n the network was successive. Also I pinged at a random website by issuing the command **ping website name** and the result was show in Graph 36, which show that the host can also communicate with another host on different network. Graph 37 displayed the network summary from a host on the network, the result show that network was implementing IPv4 address, gateway address, Mac address of host and subnet masks.



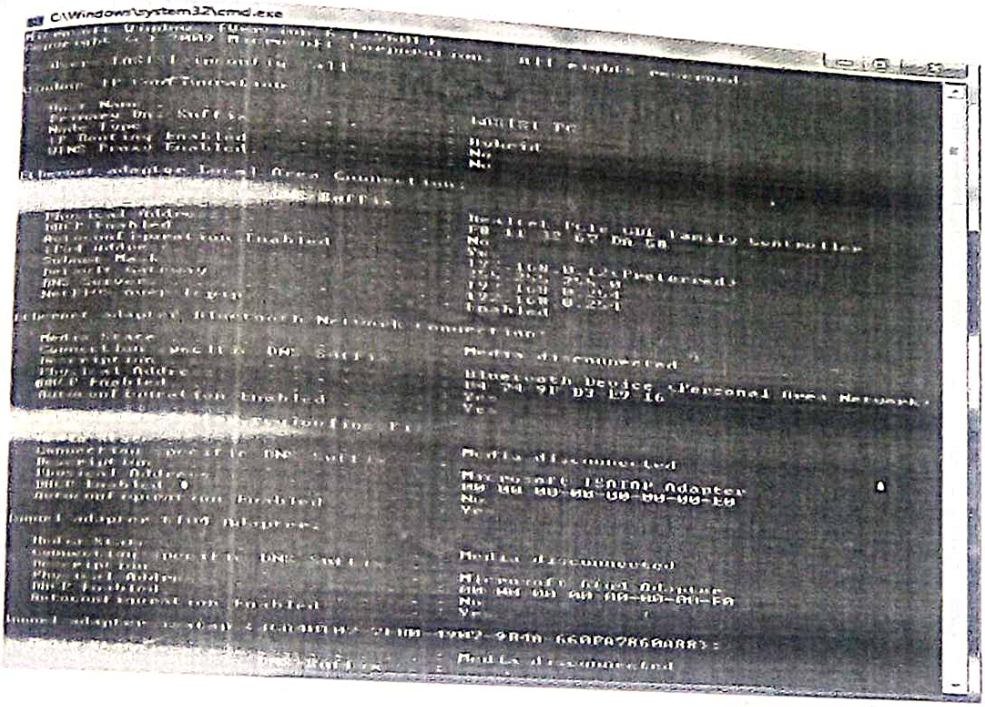
GRAPH 34. Ping to ADSL Modem (GATEWAY)



GRAPH 35. Ping result to host 192.168.0.2



GRAPH 36. Ping result to a random website



GRAPH 37. Summary of host network information

4.2 LAN Standards

LAN technologies are standardized by the Institute of Electrical and Electronics Engineers (IEEE) Project 802 and the IEEE exists for most types of commercial network. The IEEE numbers are used to designate network standard and help one to identify compatible networking topologies when intending to connect to equipment to certain network. Several LAN standards like ARCnet, Token Ring and FDDI

known in the past but they are barely used now. The Ethernet LAN technology is the most pronounced technology today and well compatible with wireless standard (Parsons & Oja2009, 247.)

Architecture of IEEE 802 Standards:

- IEEE 802.1B and 802.1K: LAN management defines an OSI management-compatible architecture and services and protocols elements for use in a LAN environment for performing remote management.
- IEEE 802.1F: defines common definitions and procedure for IEEE 802 Management information.
- IEEE STD 802.7: IEEE recommended practice for broadband local area networks.
- Network type IEEE 802.2: Defines the LLC sub-layer protocol
- Network type IEEE 802.3: Network with a bus-topology and access method CSMA/CD, 10 Mbps. Defines the MAC and physical layer for CSMA/CD.
- Network type 802.4: Network with a bus topology and the access method token passing, 2.5Mbps.
- IEEE 802.14 standard protocol for cable TV based broadband communication network.
- Network type IEEE 802.5: Network with a ring-topology and access method token passing, 4Mpbs, defines the MAC and physical layer for a token ring protocol. (Peters 2012).
- IEEE 802.10 standard for LAN security:
- 802.10 -1998 IEEE Standard for Local and Metropolitan Area Networks: Interoperable LAN security.
- 802.10a- 1999 supplement to 802.10 -1998, standard for interoperable LAN/MAN security architecture framework.

- 802.10c – 1998 supplement to 802.1998, key management. IEEE 802.11 Standard for wireless network (Nelson 2003, 44-48.)

CHAPTER FIVE

CONCLUSION

The Project work looks into challenges faced by small businesses owner in getting the right technology into their business. However, as businesses continue to grow, the demand for hardware's devices, software and other peripherals devices are on the increase and also sharing become problematic. The knowledge of Networking dealt with in this Project has suggested that rather than purchasing separate hardware for each computers, a network provides the solution for hosts to effectively shared a single network printer. However, networks become the foundation for a productive and secure small business operation and thus provide important information about the hosts on the network. An effective technology is [illegible] small businesses aiming to increase its productivity and adopting the right networking concept can help business to stay competitive by increasing its productivity and by reducing hardware costs. The Hierarchical design model considered in the design of business LAN network provides better networks that make information and resources sharing easier, provide better security implementation and enable easy backup facilities. The knowledge of hierarchical design model used in this work was an important benchmark to test the traffic of the network. The basic topology considered allows for the grouping of hosts by function and implementing security within the layer 3 designs. The Network address plan was properly carried out by considering the number of hosts and network devices. However, appropriate network devices were used at each layer of the hierarchical model to carry out a designated role during network operation. Among other benefits of using the hierarchical design model include scalability, manageability, redundancy, security, reliability and cost, which actually commend the model as effective over other models. Investing also in durable and quality network devices was also a point to note while designing an objective network. The

main interest as regards this work was that it's going to be my dictionary when implementing this project back home and can also serve as a reference point to other intending colleague in the field of Networking. A LAN security measure was highly emphasized by implementing organization policies that suite the operation of services on the network. The administrator can monitor and prevent unauthorized access into the network by configuring firewall at the network interface. This prevents the host from security threats and provides a secured network of higher transmissions integrity. Considering cost and business size, it can be recommended that, the concept of VLAN (Virtual Local Area Network) technology can be adopted in segmenting network, hence protecting hosts from security vulnerabilities. VLAN can be configured on Cisco switches that run on cisco IOS system software with function of reducing the size of broadcast domains and allowing groups or users to be logically grouped without the need to be physically located in the same place.

ABBREVIATIONS

SMEs	Small and medium Enterprise
IOS	Internetwork Operating System.
IP	Internet Protocol.
Gbps	Gigabit bytes per second.
CPU	Central Processing Unit.
bps	bytes per second.
MAC	Media Access Control.
NAT	Network Address Translation.
NIC	Network Information Center.
PAT	Port Address Translation.
TCP	Transmission Control Protocol
UDP	User Datagram Protocol.
URL	Universal Resource Locator.
VLAN	virtual LAN.
WAN	wide-area network.
LAN	Local area network
CISCO	Computer Information System Company
ARP	Address Resolution Protocol

VoIP	Voice over internet protocol
OS	Operating System
PC	Personal Computer

REFERENCES

Anand, k. 2010. Networking concepts and Netware. New Delhi India: Himalaya Publishing House.

Barman, S. 2001. Writing Information Security Policies. Sams publishing.

Cisco, 2012. Cisco campus network design guide. Available: http://www.cisco.com/en/US/netsol/ns815/networking_solutions_program_home.html. Accessed 27 April, 2012.

Clark, K & Hamilton, K. 2006. Cisco LAN Switching. First edition August 2006. IN, USA: Cisco press.

Cobb, C. 2011. Network Security for dummies. Boulevard, IN: John Wiley & sons.

Cole, E. 2011. Network Security Bible. (2nd Edition). Boulevard, IN: John Wiley &sons.

Dameon, D. 2004. Essential check Point Firewall-1 NG: An installation, configuration, and troubleshooting. Boston, MA: Addison- Wesley professional

Davies, J. 2008. TCP/IP Fundamentals for Microsoft Windows. Edited by Anne Taussig. Redmond, WA: Microsoft Corporation.

Dean, T. 2009. Network+ guide to networks. Fifth edition. Boston, MA: Cenage learning.

Jones-Evans, S. 2006. Enterprise and small business. Principles, practice and policy. (Second edition). Harlow, UK: Pearson Education Gate.

Mueller, S. 2012. What is spam? Available:http://spam.abuse.net/overview/whatisspam.html. Accessed: 20th April 2012

Mun, Y &Lee,H. 2005. Understanding IPv6. 233 spring street, New York, USA: Springer Business Media, Inc.

Nelson, A 2003. Introduction to Networking and Server Administration. Coronado Phoenix, AZ: GeniPress, LLC.

Network bandwidth 2012. University of California. Available: http://www.ucsc.edu/security/bandwidth.html. UC Santa Cruz, 1156 High Street, Santa Cruz, CA 95064. Accessed on 17th April, 2012.

Network topology, 2012. Available: http://simple.wikipedia.org/wiki/Network_topology#Daisy_chain. Accessed 4th April 2012

Networking, 2012. Available: http://en.wikipedia.org/wiki/network_topology. Accessed 3rd April 2012.

Oppenheimer, P. 2004. Top-Down Network Design. Second edition. IN, USA: Cisco press.

Panek, W. 2011.McTs Microsoft Windows 7 Configuration Study Guide: Exam 70-680. Boulevard, IN: John Wiley & sons.

Parsons, J &Oja, D. 2010. New Perspectives Computer concepts. Boston, MA: Cengage Learning.

Pasricha, H &Jagu, D. 2004. Designing Networks with Cisco. Hingham, MA: Charles River media.

Petri, 2011. Network Threats. Available: http://www.petri.co.il/cisco.htm. Accessed 17th April, 2012.

Reid, A & Lorenz, J. 2008. Working at a Small to Medium Business Or ISP. Indianapolis, IN: Cisco Press.

Richard Deal. A. 2004. Cisco Router Firewall Security.IN, USA: Cisco press.

Ross, J. 2009. Network Know-How: An essential guide for the accidental Admin. SanFrancisco, CA: No Starch Press.

TCP/IP Network 2012. TCP/IP Networks-IEEE LAN's. Available: http:// www.citap.com/documents/tcp-ip/tcpip007.htm. Accessed: 24th April 2012.

Tech –faq 2012. Firewall. Available: http://www.tech-faq.com/firewall.html. Accessed 23rd April, 2012.

Techtarget 2012. TCP/IP definition. Available: http://www.searchnetworking.techtarget.com/definition/TCP-IP/. Accessed 2nd April 2012.

Webopedia2012.Virus.Available: http://www.webopedia.com/TREM/V/Virus.html. Accessed 20th April 2012.

Wendell Odom, 2004. CCNA ICND Exam certification Guide.IN, USA: Cisco press. Winkelman, R. 2012. Hardware. Florida Center for Instructional Technology, College of Education, University of Florida. Available: http://www.fcit.usf.edu/network/chap3/chap3.htm. Accessed 20 April, 2012.

Wong J. 2012 NetworkTopology.Available:http://www.Wongwong.com/archives/166. Accessed 25th April, 2012.