Subject:	**Networking Lab (ITL401)**		
Class:	**SE IT / Semester – IV (CBCGS) / Academic year: 2017-18**		
Name of Student:	**Kazi Jawwad A Rahim**		
Roll No:	**28**	**Date of performance (DOP) :**	
Experiment No:	**13**	**Date of checking (DOC) :**	
Title: Case study on designing network topology			
Marks:		**Teacher's Signature:**	

1. Aim: Case study on designing network topology

2. Prerequisites:

Knowledge of

1. Topology
2. Networking Devices
3. IP Addressing, Subnetting

3. Hardware Requirements:

1. PC with minimum 2GB RAM

4. Software Requirements:

1. Linux (Ubuntu 10.04)/ Windows
2. Microsoft World

5. Learning Objectives:

1. To understand and analyze requirements of network.
2. To be able to identify infrastructure components and the roles they serve, and design infrastructure including devices, topologies, protocols, systems software.

6. Course Objectives Applicable: LO 6

7. Program Outcomes Applicable: PO2, PO4

8. Program Education Objectives Applicable: 1, 3

Design and Simulation of Local Area Network Using Cisco Packet Tracer

----

Computer networks have become extremely important in our present-day society. A majority of companies depend on the proper functioning of their networks for communications, administration, automation, e-business solutions, etc. The Local Area Network (LAN) is the most basic and important computer network owned by individual companies and could be used for interconnection with wide area networks. A LAN permits effective cost sharing of high-value data processing equipment such as mass storage media, mainframe computers or minicomputers, and high-speed printers. Resource sharing is probably equally as important where a LAN serves as the access vehicle for an intranet or the Internet. In view of this, system managers need professional tools to help them with the design and maintenance of LANs. A simulation tool offers a way to predict the impact on the network of a hardware upgrade, a change in topology, an increase in traffic load or the use of a new application. So in this paper, a LAN network is designed using Cisco Packet Tracer. The paper describes how the tool can be used to develop a simulation model of the LAN for the College of Engineering of the University of Agriculture, Makurdi, Nigeria. The study provides an insight into various concepts such as topology design, IP address configuration and how to send information in form of packets in a single network and the use of Virtual Local Area Networks (VLANs) to separate the traffic generated by different departments.

I. INTRODUCTION

The need for computer networking was borne out of the need to use personal computers for sharing information within an organization in form of messages, sharing files and data bases and so forth. Whether the organization is located in one building or spread over a large campus, the need for networking the computers cannot be over emphasized. As the name implies, a Local Area Network (LAN) interconnects computers in a limited geographic area. It provides high-bandwidth communication over inexpensive transmission media [1]. The corporate LAN has evolved from a passive background business component to a highly active, visible core asset that enterprises rely on to support day-to-day operations critical to their market success. Today's network is a strategic instrument that must be accessible anytime from anywhere-simultaneously offering fast, secure, reliable services at scale regardless of location [2]. The main purpose of a network is to reduce isolated users and workgroups. All systems should be capable of communicating with others and should provide desired information. Additionally, physical systems and devices should be able to maintain and provide satisfactory performance, reliability and security. Resource sharing is probably equally of immense importance where a LAN serves as the access vehicle for an intranet or the Internet [2]. In view of this, system managers need professional tools to help them with the design and maintenance of LANs [3]. A simulation tool offers a way to predict the impact on the network of a hardware upgrade, a change in topology, an increase in traffic load or the use of a new application. So in this paper, a LAN network is designed using Cisco Packet Tracer.

Cisco Packet Tracer (CPT) is a multi-tasking network simulation software that can be used to perform and analyse various network activities such as implementation of different topologies, selection of optimum path based on various routing algorithms, creation of appropriate servers, subnetting, and analysis of various network configuration and troubleshooting commands [4]. In order to start communication between end user devices and to design a network, we need to select appropriate networking devices like routers, switches, and hubs and make physical connection by connecting cables to serial and fast Ethernet ports from the component list of packet tracer [4]. Networking devices are costly so it is better to perform first on packet tracer to understand the concept and behaviour of the network [4].

The paper describes how the CPT tool can be used to develop a simulation model of the LAN for the College of Engineering of the University of Agriculture, Makurdi, Nigeria. The study provides an insight into various concepts such as topology design, IP address configuration and how to send information in form of packet in a single network and the use of Virtual Local Area Networks (VLANs) to separate the traffic generated by the different departments. VLANs are a new type of LAN architecture using intelligent, high-speed switches [5]. The simulation results and performance analyses showed that the design was successful.

The rest of the paper is organized as follows: Section 2 discusses the different LAN topologies. This is followed by a discussion in section 3 on the different types of transmission media. VLANs are discussed in section 4. The concept of IPv4 addressing and subnetting is presented in section 5. In section 6, the development of the LAN simulation model is presented; while section 7 presents the model's simulation and results analyses. Lastly in section 8 is the conclusion.

II. NETWORK TOPOLOGY

According to [4], for interconnectivity of components, network topology describe the physical and logical appearance and interconnection between arrangement of computers, cables and other components in a data communication network and how it can be used for taking a packet from one device and sending it through the network to another device on a different network. A network topology is the physical layout of computers, cables, and other components on a network. There are a number of different network topologies, and a network may be built using multiple topologies. The different types of network topologies are: Bus topology, Star topology, Mesh topology, Ring topology, Hybrid topology and Wireless topology.

The bus topology typically uses a cable running through the area requiring connectivity. Devices that need to connect to the network then tap into this nearby cable. To prevent signal bounce, a terminator is designed to absorb the signal when the signal reaches the end.

The Star Topology is a network topology in which all the clients or machines on the network are connected through a central device known as a hub or switch. Each workstation has a cable that goes from the network card to the hub or switch device. One of the major benefits of the star topology is that a break in the cable causes only the workstation that is connected to the cable to go down, not the entire network as it is with the bus topology.

In a mesh topology, every workstation has a connection to every other machine or workstation on the network. The mesh topology is not so common in today's networks probably because of the cost of implementation.

In a ring topology, all computers are connected via a cable that loops in a ring or circle. A ring topology is a circle that has no start and no end. Signals travel in one direction on a ring while they are passed from one computer to the next, with each computer regenerating the signal so that it may travel the distance required. Some networks of today are implemented by having a combination of more than one topology: star and bus, star and ring, ring and bus or ring, bus and star. Networks implemented in this way are said to be hybrids.

A wireless topology is one in which few cables are used to connect systems. The network is made up of transmitters that broadcast the packets using radio frequencies. The network contains special transmitters called wireless access points which extend a radio sphere in the shape of a bubble around the transmitter. Wireless topology can either be an ad-hoc or an infrastructure based implementation [6].

III. COMMUNICATION MEDIA

Network devices are connected together using a medium, the medium can be cables which can either be coaxial cable or twisted pair cable or it can be by optic fibre cables or the medium can be free space (air) by the use of radio waves. A discussion of the media is as outlined below [7]:

3.1 Coaxial Cable

This cable is composed of two conductors. One of the conductors is an inner insulated conductor and this inner insulated conductor is surrounded by another conductor. This second conductor is sometimes made of a metallic foil or woven wire. Because the inner conductor is shielded by the metallic outer conductor, coaxial cable is resistant to electromagnetic interference (EMI). Coaxial cables have an associated characteristic impedance, which needs to be balanced with the device (or terminator) with which the cable connects. There are two types of coaxial cables: Thicknet (10Base5), and Thinnet (10Base2). The two differ in thickness (1/4-inch for thicknet and ½-inch for thinnet) and in maximum cable distance that the signal can travel (500 meters for thicknet and 185 meters for thinnet). A transceiver is often connected directly to the ThickNet cable using a connector known as vampire tap.

3.2 Twisted Pair Cable

This is the most popular LAN media type in use today. Individual insulated copper strands are intertwined into a twisted pair cable. Two categories/types of twisted pair cable include Shielded Twisted Pair (STP) and Unshielded Twisted Pair (UTP). To define industry-standard pinouts and color coding for twistedpair cabling, the TIA/EIA-568 (Telecommunication Industry Association/Electronic Industries Alliance) standard was developed. The first iteration of the TIA/EIA-568 standard has come to be known as the TIA/EIA568-A standard, which was released in 1991. In 2001, an updated standard was released, which became known as TIA/EIA-568-B. The pinout of these two standards is the same however, the color coding of the wiring is different. Table 1 shows the TIA/EIA-568 standard.

Table I: TIA/EIA-568 Wiring Standard

Pin No.	TIA/EIA-568-A	TIA/EIA-568-B
1	Green-white	Orange-white
2	Green	Orange
3	Orange-white	Green-white
4	Blue	Blue
5	Blue-white	Blue-white
6	Orange	Green
7	Brown-white	Brown-white
8	Brown	Brown

Three types of cabling exist for UTP cable and they are: Straight through cable**,** Cross over cable and Roll over cable. The straight through cable is used to connect either a host to a switch or hub or to connect a router to a switch or hub. The Cross over cable can be used to connect a switch to switch, hub to a hub, host to host, hub to switch and a router direct to host. Roll over cables are not used to connect any Ethernet devices together, rather, they are used to connect a host to a router console serial communication (com) port.

3.3 Optic Fiber Cable

An alternative to copper cabling is fiber–optic cabling, which sends light through an optic fiber. Using light instead of electricity makes fiber optics immune to EMI. Also depending on the layer 1 technology being used, fiber-optic cables typically have greater maximum distance between networked devices and greater data carrying capacity.

3.4 Wireless

Not all media is physical, as is the case with wireless technologies. Wireless clients gain access to a wired network by communicating via radio waves with a wireless access point (AP). The access point is then hardwired to a LAN. All wireless devices connecting to the same AP are considered to be on the same shared network segment, which means that only one device can send data to and receive data from an AP at any one time (half duplex communication).

IV. VIRTUAL LOCAL AREA NETWORKS (VLANs)

VLANs are a new type of LAN architecture using intelligent, high-speed switches. Unlike other LAN types, which physically connect computers to LAN segments, VLANs assign computers to LAN segments by software. VLANs have been standardized as IEEE802.1q and IEEE802.1p. There are two basic designs of VLANS. They are: Single-switch VLANs and Multiswitch VLANs (Fig. 1) [5].

4.1 Single Switch VLANs

With single switch VLANs, computers are assigned to VLANs using special software, but physically connected together using a large physical switch. Computers can be assigned to VLANs in four ways:

- Port-based VLANs assign computers according to the VLAN switch port to which they are attached
- MAC-based VLANs assign computers according to each computer's data link layer address
- IP-based VLANs assign computers using their IP-address
- Application-based VLANs assign computers depending on the application that the computer typically uses. This has the advantage of allowing precise allocation of network capacity.

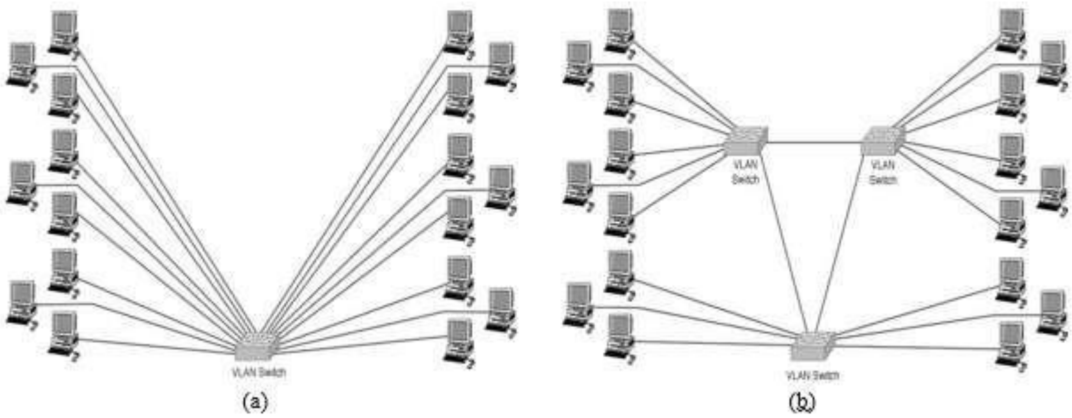


Figure 1: Types of VLAN design (a) single switch VLAN (b) multiswitch VLAN

4.2 Multiswitch VLANs

Multiswitch VLANs send packets between multiple switches, making VLANs with segments in separate locations possible. When a frame is sent between switches it is modified and includes a tag field carrying VLAN information field. When the frame reaches the final switch, the tag field is removed prior to the frame being sent to its destination computer. Multiswitch VLANs can also prioritize traffic using the IEEE802.1p standard in the hardware layers and the RSVP standard in the internetwork layers. IEEE802.1p works with the IEEE802.11ac frame definition which includes a special priority field.

V. IPv4 ADDRESSING AND SUBNETTING

An IP address is a numeric identifier assigned to each machine on an IP network. It designates the specific location of a device on the network. IP addressing was designed to allow hosts on one network to communicate with hosts on different networks regardless of the type of LAN the hosts are participating in [8].

5.1 IPv4 Address Structure

An IPv4 address is a 32-bit address. However rather than writing out each individual bit value, the address is typically written in dotted-decimal notation, for example 192.168.23.100. Each number represents an 8-bit portion of the 32 bits in the address and each of these four divisions of an IP address is called an octet. An IP address is composed of two types of addresses: network address and host address and the IP address component that determines which bits refer to the network and which bits refer to the host is called subnet mask. An example of a subnet mask is 255.255.255.0.

5.2 Classes of Addresses

There are five classes of IP addresses and they are shown in the Table 2 [8].

Table II: Classes of IP addresses

Address Class	Value in First Octet
A	1 – 126
B	128 – 191
C	192 – 223
D	224 – 239
E	240 – 255

IP addresses can be dynamically configured using DHCP or they can be statically configured by inputting it manually on the device.

5.3 Subnetting

Subnetting is the process of stealing bits from the host part of an IP address in order to divide the larger network into smaller sub-networks called subnets [8]. After subnetting, network subnet host fields are created. An IP address is always reserved to identify the subnet and another one to identify the broadcast address within the subnet. Subnetting can be done in three basic ways, one of which is subnetting based on the number of subnetworks you wish to obtain from a single block of IP address; another way is to subnet based on the number of host computers or devices you want to be connected to that sub-network and finally subnetting by reverse engineering which is a scenario in which a subnet mask and an IP address block is given and the number of subnetworks and number of hosts per each subnet are found [8]. For example, if a public IP address block of 192.168.23.1 with a subnet mask of 255.255.255.252 is purchased from our ISP and because this block has only two valid hosts, this IP address is used to assign to our Router interface so that traffic can be directed from our network to the ISP and from there to the internet. A private IP address block is then chosen to carry out IP addressing within our network. Because of the expected clients on this network, a Class B address is chosen for the internal network and it is 172.168.0.0 with a mask of 255.255.0.0. Based on the power of 2s, there are some equations that allow us to determine the required details, and these are [8]:

$$\text{Number of subnets} = 2^x \qquad (1)$$

$$\text{Number of hosts per subnet} = 2^y - 2 \qquad (2)$$

$$\text{Block size} = \text{Increment} = 256 - \text{subnet mask} \qquad (3)$$

5.4 Subnet Mask

For the subnet scheme to work, every host (machine) on the network must know which part of the host address will be used as the subnet address. This is accomplished by assigning subnet mask to each machine. A subnet mask is a 32-bit value that allows the recipient of an IP packet to distinguish the network ID portion of the IP address from the host ID portion of the IP address. Table 3 shows the default subnet masks for all classes of network [8].

Table III: Subnet Mask for Different Classes of Networks

Class Of IP	Format	Default Subnet Mask
A	Network.node.node.node	255.0.0.0
B	Network.network.node.node	255.255.0.0
C	Network.network.network.node	255.255.255.0

VI. DEVELOPMENT OF LAN SIMULATION MODEL

We require at least 252 hosts per subnet and using (2) gives:

$$\text{Number of hosts } = 2^y - 2$$
$$252 = 2^y - 2$$
$$254 = 2^y$$
$$y = 7.988 = 8$$

Therefore the number of unmasked bits in the subnet mask is 8 which also implies that the number of masked bits is 8 i.e. x = 8; hence the new subnet mask is represented in binary as 11111111.11111111.11111111.00000000 which is 255.255.255.0 in decimal and the number of subnets that can be obtained using this scheme is 2^x = number of subnets

Number of subnets = 2^8 = 256 subnets, block size= 256 – 255 = 1. Therefore the subnets obtained are given in tabular form in Table 4.

Table IV: Subnets obtained from the Subnetting Scheme

S/No.	Network Address	Firstvalid Host	Last Valid Host	Broadcast
1	172.168.0.0	172.168.0.1	172.168.0.254	172.168.0.255
2	172.168.1.0	172.168.1.1	172.168.1.254	172.168.1.255
3	172.168.2.0	172.168.2.1	172.168.2.254	172.168.2.255
4	172.168.3.0	172.168.3.1	172.168.3.254	172.168.3.255
5	172.168.4.0	172.168.4.1	172.168.4.254	172.168.4.255
6	172.168.5.0	172.168.5.1	172.168.5.254	172.168.5.255
7	172.168.6.0	172.168.6.1	172.168.6.254	172.168.6.255
8	172.168.7.0	172.168.7.1	172.168.7.254	172.168.7.255

Each serial number entry in the table represents a subnet and this goes on till the number reaches 256 which is the total number of subnets that were obtained. Each of those entries is assigned to a department in the College of Engineering and some of the remaining blocks are assigned to the Library, New Auditorium and the Old Auditorium respectively. If any block is unassigned it will be kept for future expansion of the network. The assignment of the subnets to the units is as follows:

Electrical Engineering 172.168.0.0/24
Agricultural Engineering 172.168.1.0/24
Civil Engineering 172.168.2.0/24
Mechanical Engineering 172.168.3.0/24
Network Centre 172.168.4.0/24
Old Auditorium 172.168.5.0/24
New Auditorium 172.168.6.0/24
Library 172.168.7.0/24

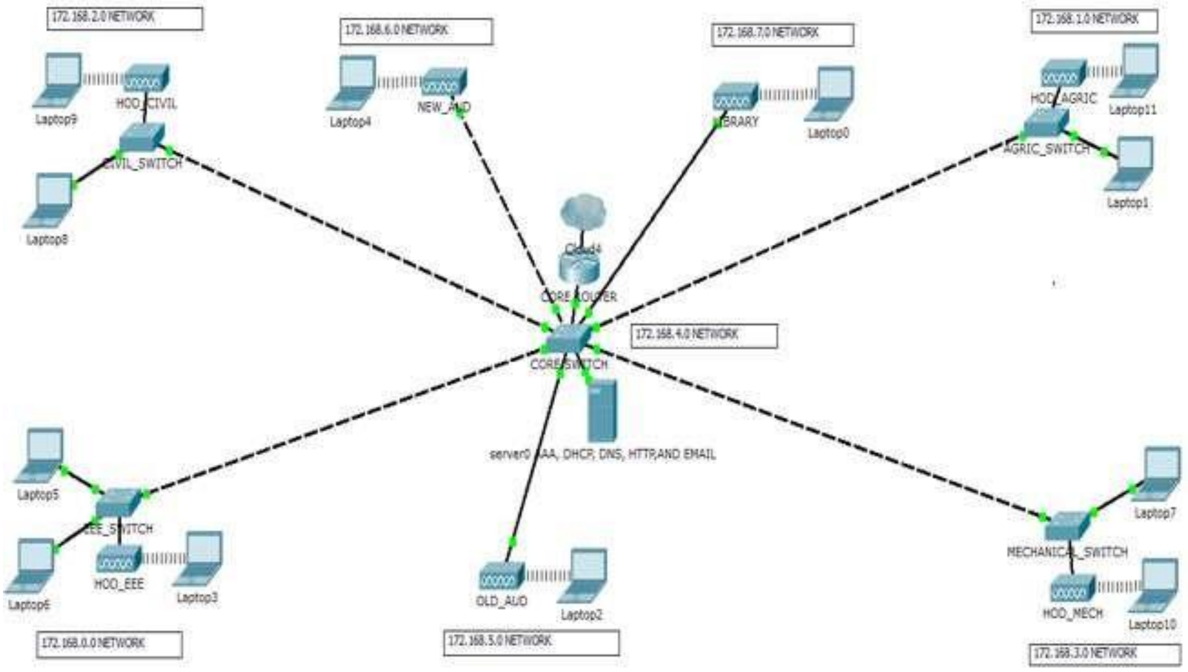


Figure 2: Complete diagram of the college of engineering local area network as created in packet tracer environment

The diagram of Fig. 2 is the complete diagram of the Local Area Network and at the core it consists of the router, switch and servers forming the Network Operating Centre (NOC) and all the departments in the College are just a mere extension of this network at the core. The IP address chosen for the internal network is 172.168.0.0 and it has been subnetted to obtain IP address blocks that are assigned to the different departments and sections of this LAN.

6.1 Switch Configurations

The configurations to be made on the switch are, making some ports access ports and a port as the trunk port to the Router, configuring a default-gateway, creating VLANs and assigning switch ports to the VLANs.

6.2 Trunk-to-Router

To create a trunk port on the switch that will connect to the router, and all other access ports, we login to the switch and using the command Line interface (CLI), use the following commands.

Switch(config)# int fastethernet 0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#spanning-tree portfast trunk
Switch(config-if)#interface range fa0/2 – 24
Switch(config-if-range)#switchport mode access
Switch(config-if-range)#end

6.3 Creating VLANs

There are four departments in the College of Engineering, each of which will be on a separate VLAN and also New Auditorium, Library and the Old Auditorium will be linked to the network, each on its own VLAN. In all we need to create eight (8) VLANs. To create a VLAN on a switch, the following command is used:

Switch(config)#vlan [id].

To create the VLAN for Electrical Engineering Department and also give it an appropriate name for easy identification, we give the following commands:

Switch(config)#vlan 10
Switch(config-vlan)#name Electrical

We use the two commands above repeatedly to create VLANs for the other departments, each VLAN with its own ID and name.

6.4 Assigning Switch Ports to VLANs

The VLANs have been created and even though active, they don't have switch ports associated with them. This makes the switch still just a single broadcast domain. To assign switch ports to the VLANs, the following commands are used:

Switch(config)#interface [interface type] [interface identifier]
Switch(config-if)#switchport access vlan [vlan id]

The first command is used to select the switch port to assign to the VLAN. The "interface type" in the command can be a gigabitethernet or fastethernet port, and the "interface identifier" can be 0/1, 0/2,…0/n for the first, second or up to the n^{th} port on the switch. In the second command, "vlan id" is the ID of the VLAN the port is to be a part of. To assign port 2 and 3 to the electrical VLAN, we apply the commands:

Switch(config)#interface fastethernet0/2
Switch(config-if)#switchport access vlan 10
Switch(config-if)#interface fastethernet0/3
Switch(config-if)#switchport access vlan 10

The reason for assigning two ports to one VLAN is for redundancy.

6.5 Configuring Default-Gateway

The switches in the departments need to have a gateway for packets that are destined outside the network (VLAN), and this can be configured using the command below:

Switch(config)#ip default-gateway [ip address].

Where “ip address” in the command, is the IP address for the interface connecting the VLAN to the Router. Hence, for VLAN 10 (Electrical Engineering), the command is entered as:

EEESW(config)#ip default-gateway 172.168.0.1

FOR VLAN 20: Agricultural Engineerimg
AGRICSW(config)#ip default-gateway 172.168.1.1

For VLAN 30: Civil Engineering
CIVSW(config)#ip default-gateway 172.168.2.1

For VLAN 40: Mechanical Engineerimg
MECHSW(config)#ip default-gateway 172.168.3.1

6.6 Router Configurations

The router is the most powerful networking device and for it to perform its functions on the network, the configurations to be made are, DHCP, DHCP relay, inter VLAN routing, Network Address Translation (NAT), creating sub-interfaces for each VLAN on the Core Switch.

6.7 Create Sub-Interfaces for Each VLAN

For packets of different VLANs to reach the router, there must be appropriate interfaces linking the router and the VLAN and because router with large number of interfaces are more costly to purchase, as a result of which sub-interfaces are created on the router interface connecting to the trunk port on the switch. This can be done by giving the command below:

Admin_router(config)#interface [interface type] [interface identifier break]

Where: “interface type” is either a gigabitethernet port or a fastethernet port and “interface identifier break” starts the creation of the sub-interfaces e.g. 0/1.1 to create the first sub-interface. The set of commands below configures the router sub-interfaces, enables DHCP relay, also it implements NAT and finally inter-VLAN routing.

Admin_router#configure terminal
Admin_router(config)# interface gig0/1
Admin_router(config-if)#no ip address
Admin_router(config-if)#duplex auto
Admin_router(config-if)#speed auto
Admin_router(config-if)#interface gig0/1.1
Admin_router(config-subif)#description VLAN10_interface
Admin_router(config-subif)#encapsulation dot1q 10
Admin_router(config-subif)#ip address 172.168.0.1 255.255.255.0
Admin_router(config-subif)#ip nat inside
Admin_router(config-subif)#ip helper-address 172.168.4.3
Admin_router(config-subif)#end

These commands are applied repeatedly, having in the mind the ID for the different VLANs and the IP address to the VLAN.

6.8 Wireless Access Point Configurations

The setup of the wireless access point is done by opening up the graphical user interface of the access point in Packet Tracer and then clicking on the config tab to access type of configurations available for the access point.

Click on port 0 under the interface section to set the bandwidth of the Ethernet connection to the access point, and then set the duplex (half duplex or full duplex). Click on port 1 under the interface section to configure the SSID of the access point, authentication type (none, WEP, WPA-PSK, WPA2-PSK) and if any authentication type is chosen provide the passphrase for network connectivity.

6.9 Server Configuration

The LAN design will require the services of a DHCP server, DNS server, HTTP server, and the AAA server for authentication. Taking each server, the setup is as follows:

6.10 DHCP Server Setup

The DHCP server is configured by opening up the graphical user interface of server0 and after selecting DHCP service from the services tab, turns on the DHCP service after which we configure the address pools that will be used on our network. The address pools can be configured as follows:

For VLAN 10:
Poolname: VLAN10
Default gateway: 172.168.0.1
DNS server: 172.168.4.3
Start IP address: 172.168.0.5
Subnet mask: 255.255.255.0
Maximum number of users: 251

For VLAN 20:
Poolname: VLAN20
Default gateway: 172.168.1.1
DNS server: 172.168.4.3
Start IP address: 172.168.1.5
Subnet mask: 255.255.255.0
Maximum number of users: 251

For VLAN 30:
Poolname: VLAN30
Default gateway: 172.168.2.1
DNS server: 172.168.4.3
Start IP address: 172.168.2.5
Subnet mask: 255.255.255.0
Maximum number of users: 251

For VLAN 40:
Poolname: VLAN40
Default gateway: 172.168.3.1
DNS server: 172.168.4.3
Start IP address: 172.168.3.5
Subnet mask: 255.255.255.0
Maximum number of users: 251

For VLAN 50:
Poolname: VLAN50
Default gateway: 172.168.6.1
DNS server: 172.168.4.3
Start IP address: 172.168.6.5
Subnet mask: 255.255.255.0
Maximum number of users: 251

For VLAN 60:
Poolname: VLAN60
Default gateway: 172.168.5.1
DNS server: 172.168.4.3
Start IP address:172.168.5.5
Subnet mask: 255.255.255.0
Maximum number of users: 251

For VLAN 70:
Poolname: VLAN70
Default gateway:172.168.7.1
DNS server: 172.168.4.3
Start IP address: 172.168.7.5
Subnet mask: 255.255.255.0
Maximum number of users: 251

For VLAN 80:
Poolname: serverpool
Default gateway: 172.168.4.1
DNS server: 172.168.4.3
Start IP address: 172.168.4.12
Subnet mask: 255.255.255.0
Maximum number of users: 244

After entering all these information on the prompt, click on the add button for each VLAN entry to add the pool to the DHCP server. Some IP addresses are excluded to give room for expansion or the connection of network equipment that will require manual IP assignment. VLAN 80 is the VLAN for the network operating centre. That is why the maximum number of users on it is less. This is due to the exclusion of more IP addresses to be assigned to the equipment in the centre.

6.11 DNS Server Setup

The setup of the DNS server is done by opening the server0 graphical user interface (GUI), and after selecting the services tab, then select the DNS service. Turn on the DNS service and enter the fully qualified domain Name (FQDN) e.g engcomplex.com in the name section and its IP address in the address section, then click on add to add the A record on the DNS server.

6.12 HTTP Server Setup

The setup of the HTTP server is done by opening up the graphical user interface of server0 in Packet Tracer and after selecting the services tab, selects the HTTP service. A window shows with the configuration options for the web server. Click on import on the web server window to upload web pages that have been programmed to the server.

6.13 Email Server Setup

To set up the email server, we open up server0 and after clicking on services tab, select the email service and a window opens up with the type of configurations available for the email server. And the configurations are; Turn on secure message transfer protocol (SMTP) service.

- Turn on POP3 service
- Enter the domain name for your mail server i.e. engcomplex.com in our case. And then click on set to set the domain.
- In the user setup section, setup the username and password for each user on the email server and then click on "+" to add the user to the mail server.
- To change a user's password, click on the user on the mail server and then click on the change password. A prompt will come up with the option to enter the new password after which click on ok to change the password.

6.14 AAA Server Settings

In Cisco Packet Tracer, after placing the server-PT in the workspace, we click on the icon and when it opens up, click on the services tap and then select AAA, after which, turn on the AAA service, enter the client name (router's hostname), client IP (IP address of the router's interface that is connected to the AAA server), key (server key), and then the AAA server type which can be either Radius server or TACACS server. And then down to the user setup, enter the username and password for all the users that should have access to the networked devices.

6.15 Securing the Network

Security configurations on the network include:

6.15.1 Setting up Passwords on All Switches and the Router

This can be done by connecting to the switch or router using the console port and then opening up terminal window to bring up the command line interface, then the following commands is entered:

Router>enable
Router#configure terminal
Router(config)#enable secret group8
Router(config)#service password-encryption
Router(config)#end
Router#write memory

From the above configurations, the password for the router is set to group 8 and password encryption is enabled using the "service password-encryption" command and the commands are saved to memory. The same procedure is followed to apply the same commands to the switch.

6.15.2 Setting up Console Port and Telnet Connection Passwords

This can be done by opening up the CLI of the switch or router entering the following commands:

Router(config)#line vty 0 4
Router(config-line)#password group8
Router(config-line)#login
Router(config-line)#end
Router(config)#line console 0
Router(config-line)#password group8
Router(config-line)#login
Where group8 is the password set up for both the telnet (vty) and console port connections.

6.15.3 Setting up Secure Shell (SSH)

Secure shell is a more secure version telnet as the passwords are encrypted before they are sent over the network. Setting up secure shell involves the following commands:

Router(config)#hostname Admin_router
Admin_router(config)#ip domain-name engcomplex.com
Admin_router(config)#crypto key generate rsa general-key modulus 1024
Admin_router(config)#ip ssh authentication-retries 3
Admin_router(config)#line vty 0 1180
Admin_router(config)#transport input ssh telnet

The modulus of 1024 indicates the strength of the rsa key to be generated.

6.15.4 Setting up an AAA Model on the Router

AAA assists in authenticating, authorizing and accounting on the network but only authentication is implemented in this report and the AAA model is implemented on the router by making the following configurations.

Admin_router(config)#aaa new-model
Admin_router(config)#tacacs-server host 172.168.4.1 key secret
Admin_router(config)#aaa authentication login ACCESS group tacacs+
Admin_router(config)#line console 0
Admin_router(config-line)#login authentication ACCESS
Admin_router(config-line)#end
Admin_router#write memory

VII. PRESENTATION OF RESULTS

The results obtained from the design and analyses of the network is presented as follows:

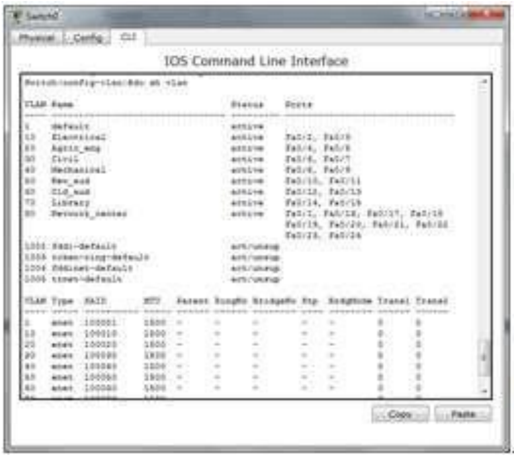


Figure 3: VLANs created on the switch

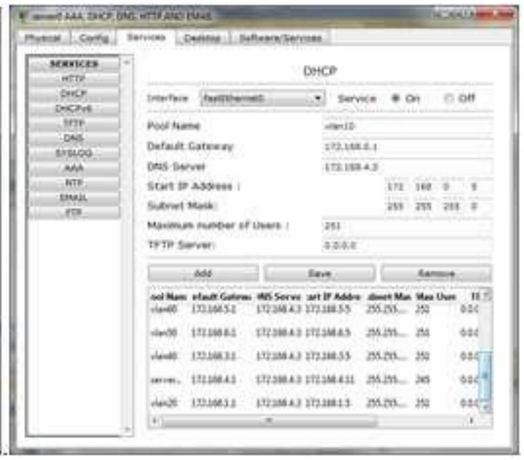
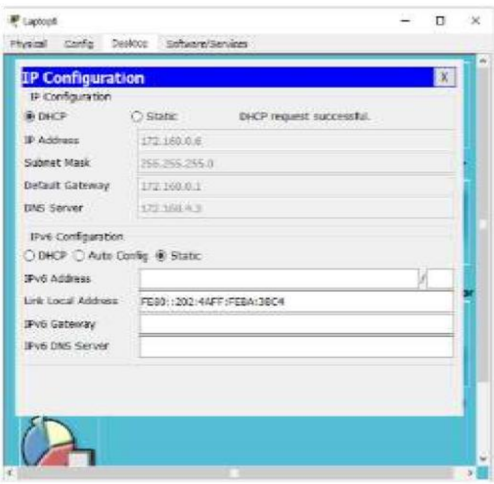


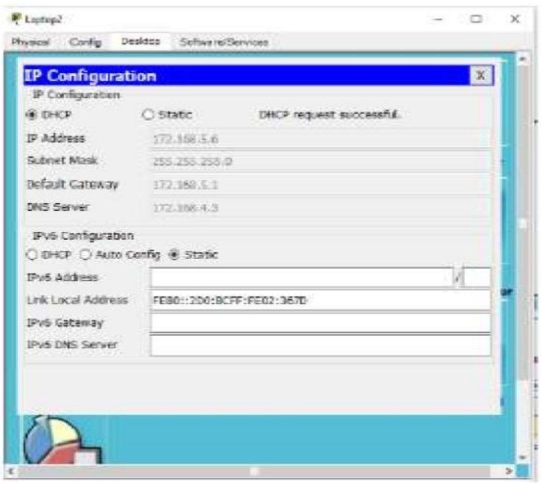
Figure 4: DHCP server pools

Fig. 3 shows the created VLANs running on the switch, their ID and switch ports associated to each VLAN. Fig. 4 shows the results after the configuration of the DHCP server, showing the address pools for each VLAN created on the Network

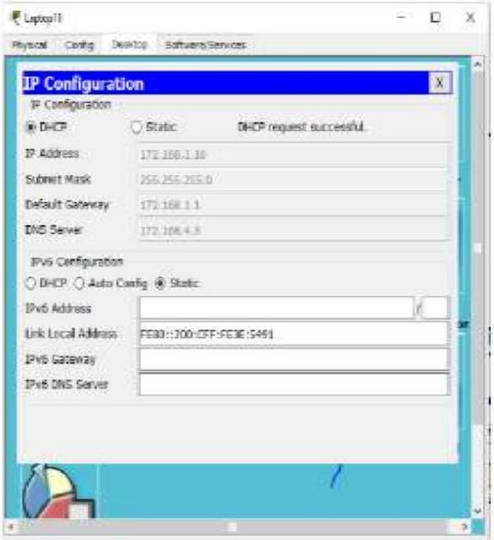
A dynamic address configuration was done on the network, i.e. when a client device connects to the network; it is offered an IP address that is available in that network address pool, that the client is connected to. Fig. 5 shows client devices successfully obtaining an IP address that is appropriate to the VLAN the devices are connected to.



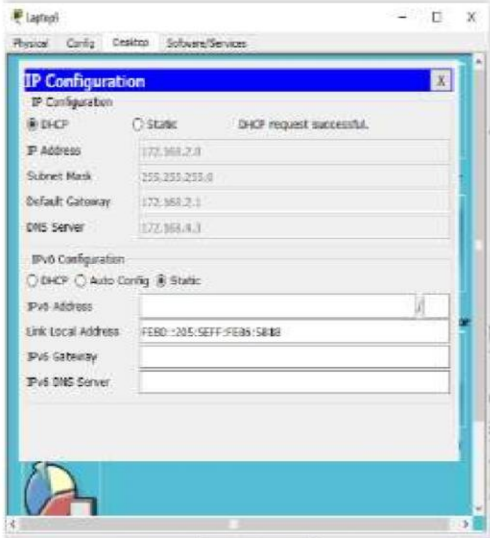
Electrical subnet (172.168.0.0/24)



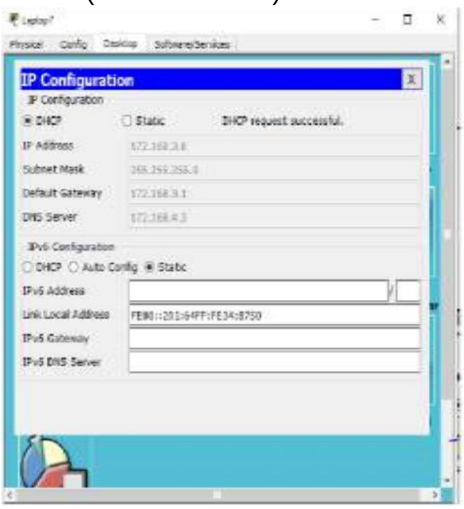
old_aud subnet (172.168.5.0/24)



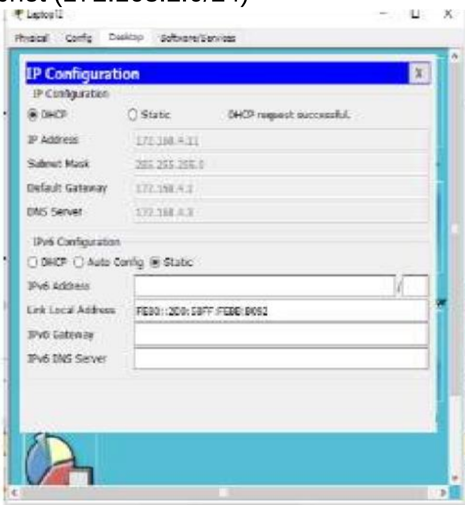
Agric subnet (172.168.1.0/24)



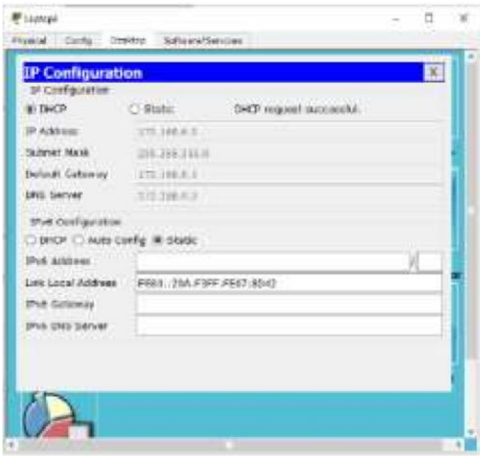
civil subnet (172.168.2.0/24)



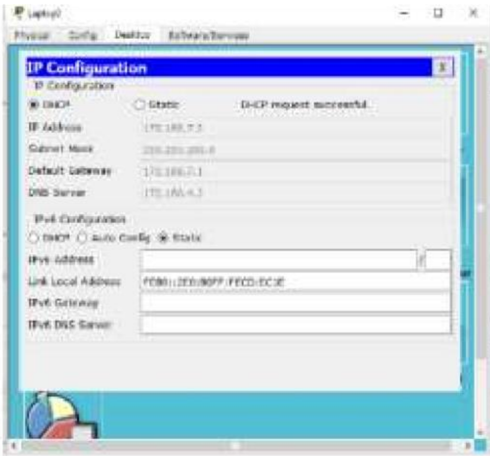
Mech subnet (172.168.3.0/24)



Network center subnet (172.168.4.0/24)



New_aud subnet (172.168.6.0/24)



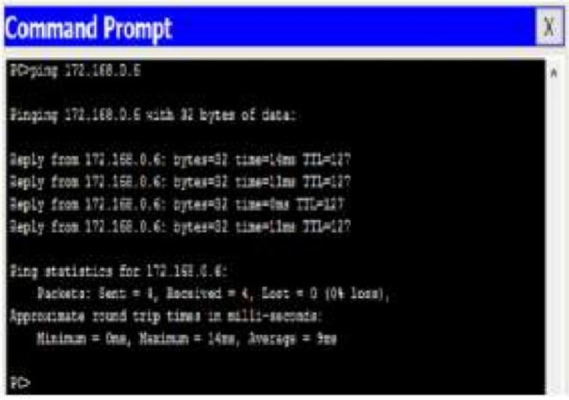
library subnet (172.168.7.0/24)

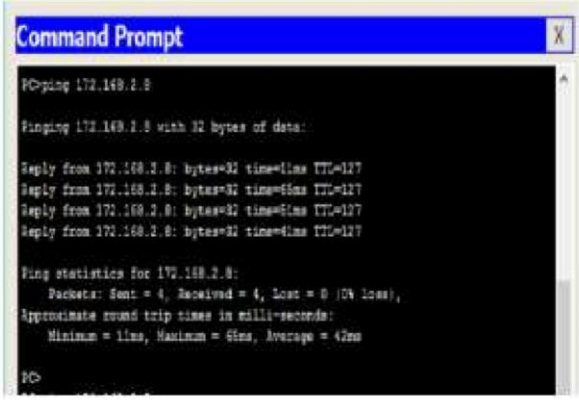
Figure 5: Client obtaining IP address information

From Fig. 5, it is shown that each client connected to the network is obtaining IP address information dynamically, according to the subnet the client is connected to.

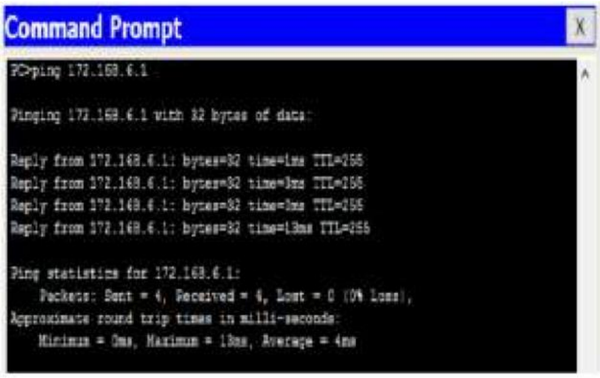
7.1 Ping Test

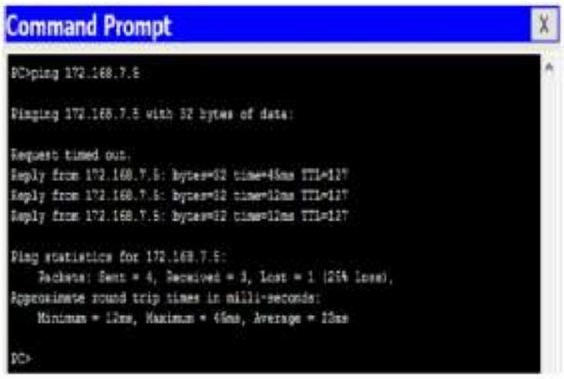
Network connectivity and communication can be tested using a ping command, followed by the domain name or the IP address of the device (equipment) one wishes to test connectivity to. Two VLANs have been added to the existing network and the ping test was performed to test if the devices connected to those VLANs are communicating with the rest of the devices on the network. The results obtained are as shown in Fig. 6.



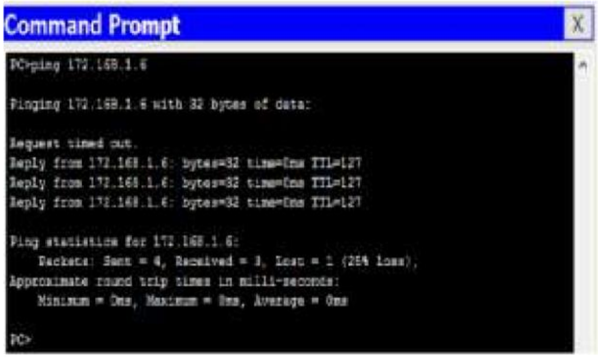


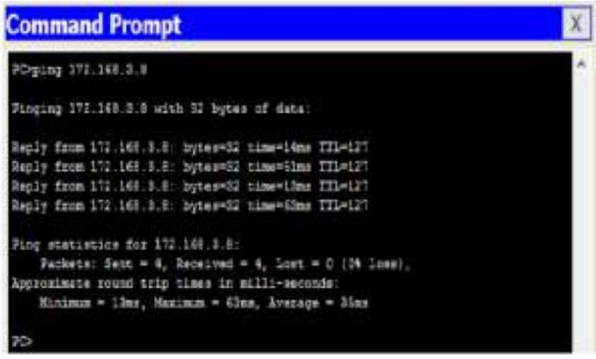
Network Center□elect Network center□civil



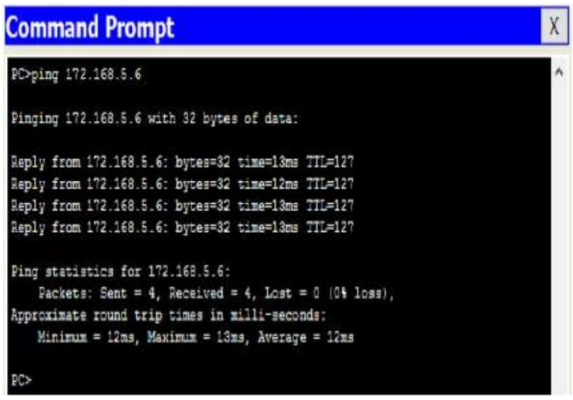


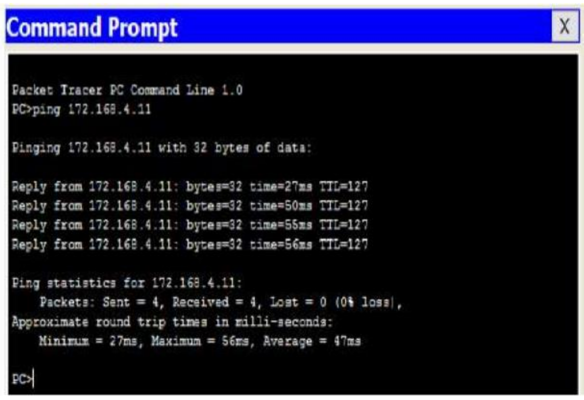
Network center□new aud Network center□library





Network center□agric Network center□Mech

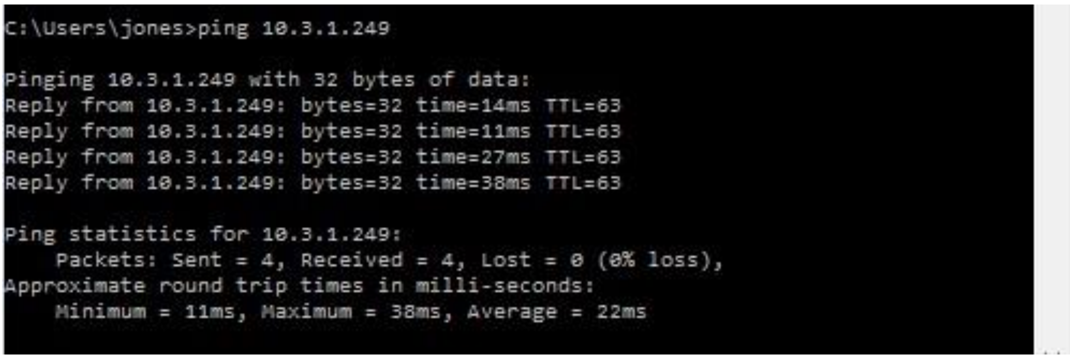




Network center□old aud Mech□network center

Figure 6: Ping tests

From Fig. 6, it is observed that the network is performing well, this is because when we compared the ping test of the network designed to the ping test on the existing network of College of Engineering, University of Agriculture, Makurdi, the values were similar. Fig. 7 shows the ping test on the live network in existence.



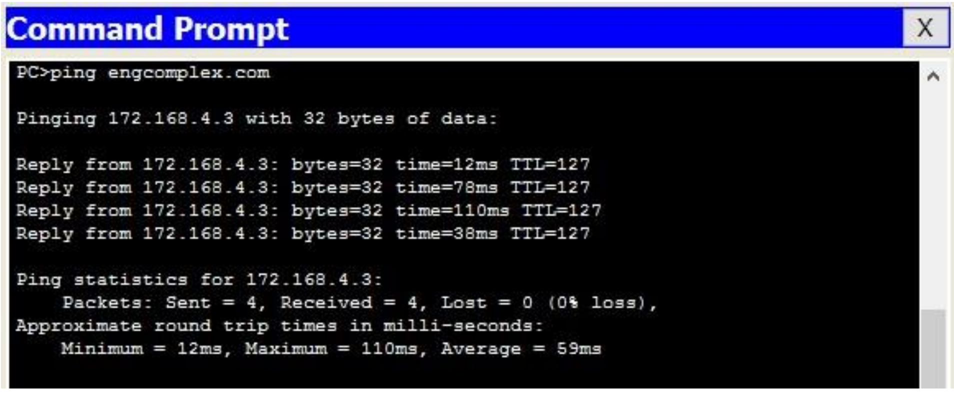
```
C:\Users\jones>ping 10.3.1.249

Pinging 10.3.1.249 with 32 bytes of data:
Reply from 10.3.1.249: bytes=32 time=14ms TTL=63
Reply from 10.3.1.249: bytes=32 time=11ms TTL=63
Reply from 10.3.1.249: bytes=32 time=27ms TTL=63
Reply from 10.3.1.249: bytes=32 time=38ms TTL=63

Ping statistics for 10.3.1.249:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 11ms, Maximum = 38ms, Average = 22ms
```

Figure 7: Ping test to a server on the UAM network

Using ping to test to confirm that our DNS configuration is working properly, the domain name engcomplex.com was pinged in one of the PC and observed if it translated the domain name to a valid IP address. Fig. 8 shows the result of the test.



```
Command Prompt
PC>ping engcomplex.com

Pinging 172.168.4.3 with 32 bytes of data:

Reply from 172.168.4.3: bytes=32 time=12ms TTL=127
Reply from 172.168.4.3: bytes=32 time=78ms TTL=127
Reply from 172.168.4.3: bytes=32 time=110ms TTL=127
Reply from 172.168.4.3: bytes=32 time=38ms TTL=127

Ping statistics for 172.168.4.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 110ms, Average = 59ms
```

Figure 8: Pinging a domain name

From Fig. 8, it is observed that the domain name engcomplex.com gets translated to 172,168.4.3 which is the address of the web server hosting the website.

7.2 Email Service

The email service results show a message from a registered email user on the network, sending a mail to another registered mail user. Fig. 9 displays the results of the email service.

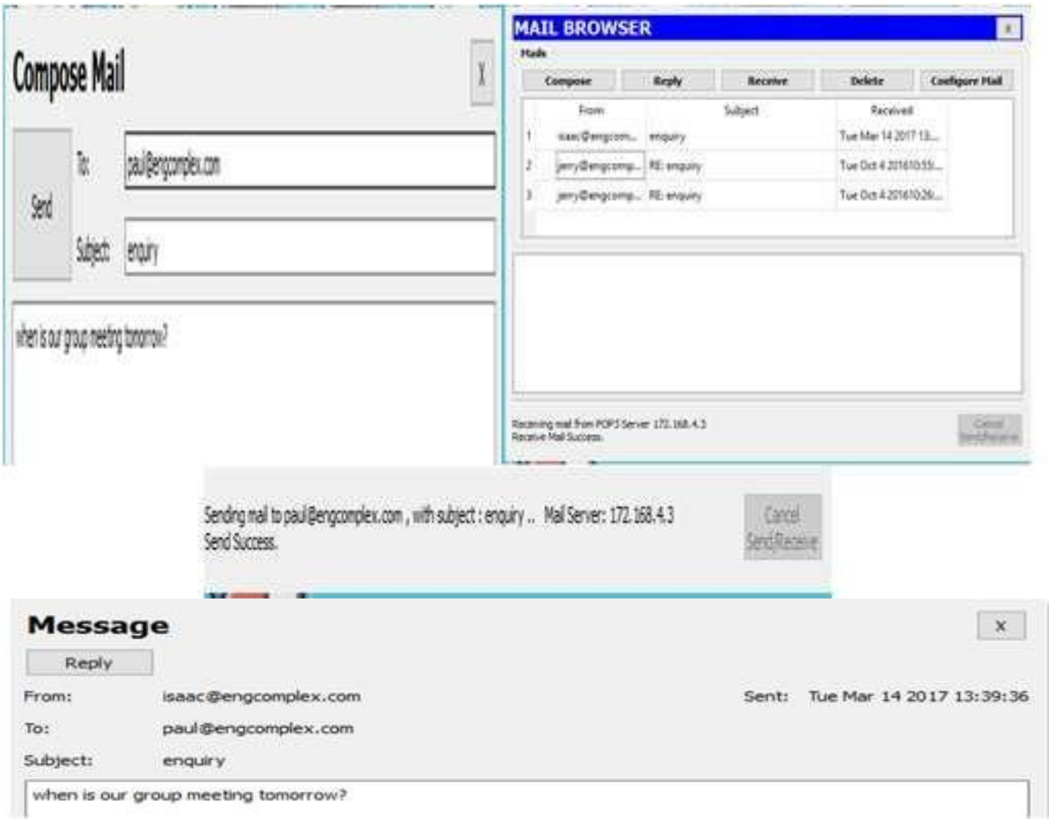


Figure 9: E-mail service result

From the results, it is seen that the mail server set up on the network is working properly.

VIII. CONCLUSION

In this paper, a Local Area Network (LAN) that uses both wired and wireless topology have been implemented with some important concepts like DHCP, DNS, Email, VLANs in a single network using Cisco Packet Tracer. VLANs have been used to logically group clients on the network, and with the aid of a router and switch configurations, data packets routed from one device to another. It is also noteworthy that, the configuration and specifications are for the initial prototype and can further be developed and additional functionality can be added to increase support and coverage. The procedures provide a veritable approach for the design of LANs for end-to-end IP network connectivity for next generation network (NGN) architecture implementations.

9. EXPERIMENT/ASSIGNMENT EVALUTION

SR	Parameters	Weight	Excellent	Good	Average	Poor	Not as per requirement
		Scale Factor ->	5	4	3	2	0
1	Technical Understanding	25					
2	Performance / Execution	25					
3	Question Answers	20					
4	Punctuality	20					
5	Presentation	10					
	Total out of 100 --> #(to be converted as per term-work evaluation applicable to the subject)	**∑ (Weight * Scale Factor)/5 = ________**					

10. REFERENCES

[1] http://www.buyya.com/java/Chapter13.pdf
[2] http://www.scit.wlv.ac.uk/~in8297/CP4044/lectures/L07.pdf
[3] http://www.kiv.zcu.cz/~ledvina/Knihovnicka/Sockets_Java.pdf