



Department of Information Technology

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 Word

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 1/2-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.

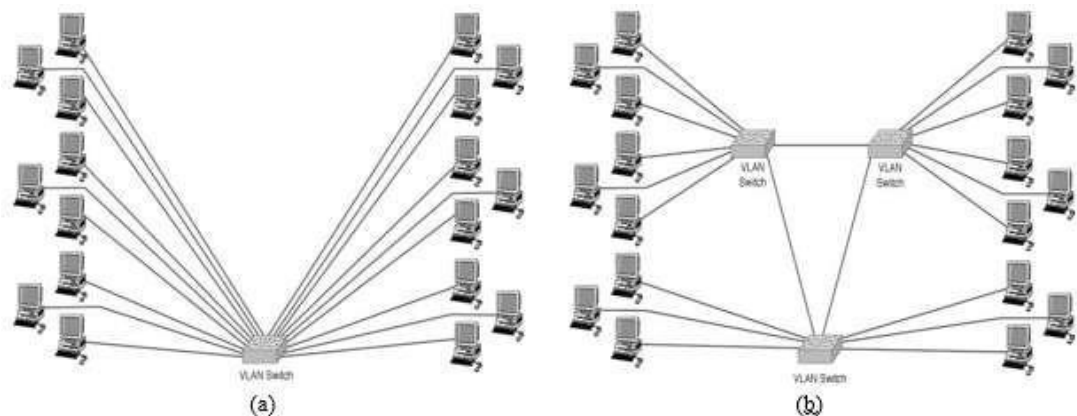


Figure 1: Types of VLAN design (a) single switch VLAN (b) multiswitch VLAN

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]:

$$\begin{aligned}\text{Number of subnets} &= 2^x & (1) \\ \text{Number of hosts per subnet} &= 2^y - 2 & (2) \\ \text{Block size} = \text{Increment} &= 256 - \text{subnet mask} & (3)\end{aligned}$$

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:

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

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 $2^x = \text{number of subnets}$

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	First valid 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

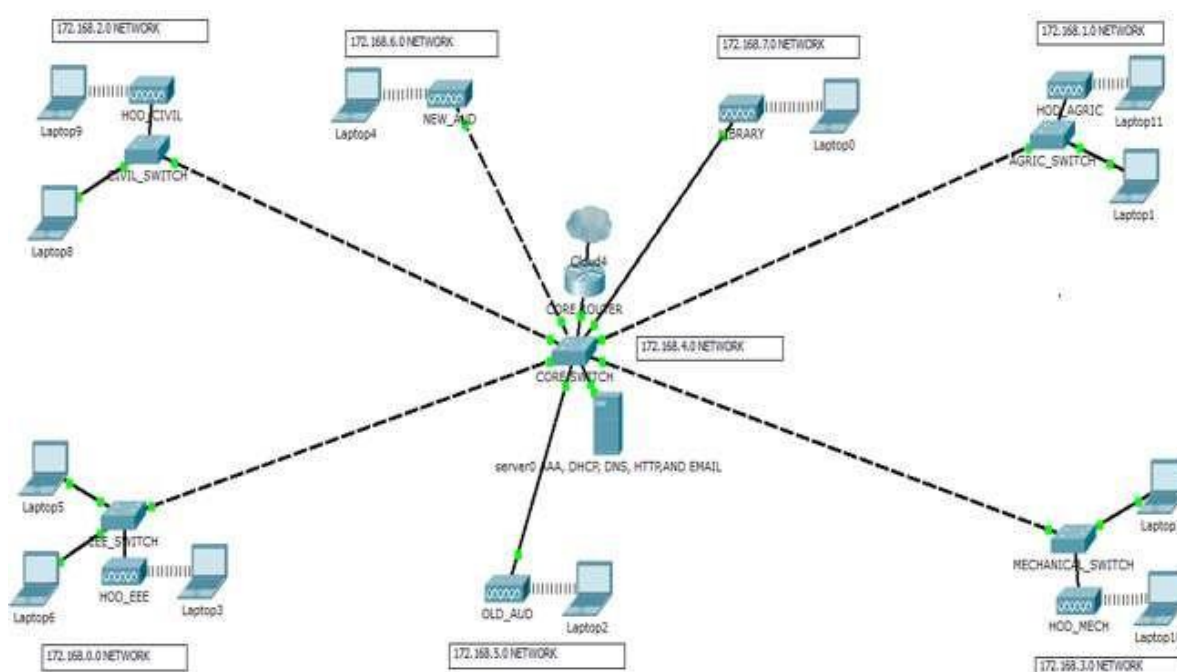


Figure 2: Complete diagram of the college of engineering local area network as created in packet tracer environment

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 nth 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 Engineering
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 Engineering
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:

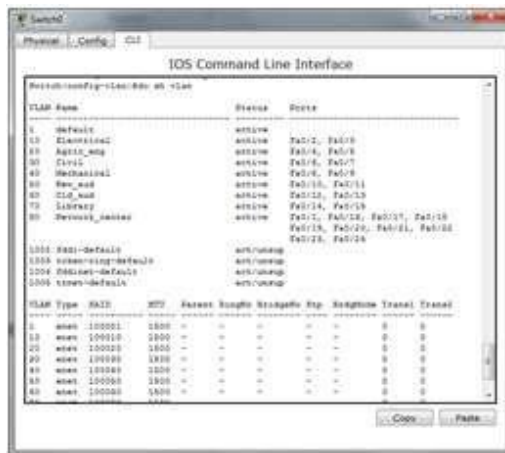
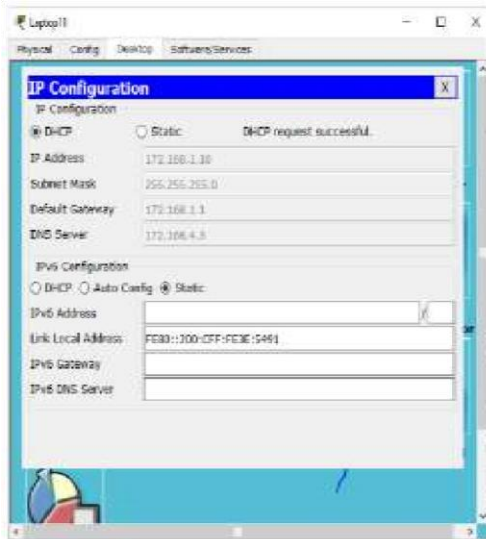
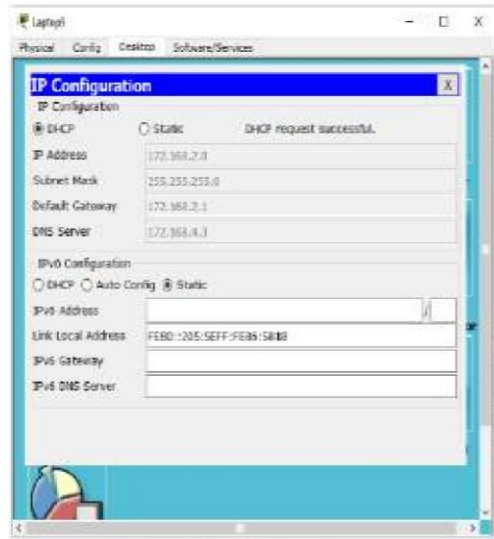


Figure 3 shows the IOS Command Line Interface for a switch. It displays a table of VLANs and their associated ports.

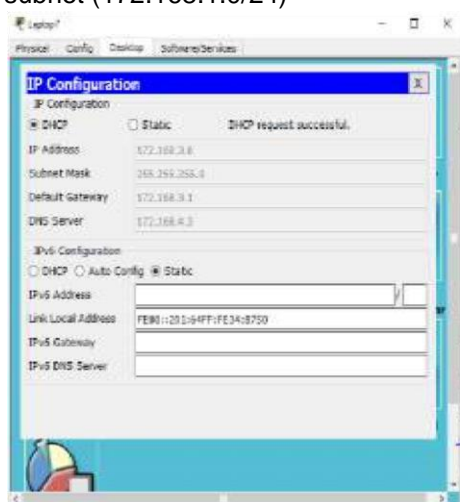
VLAN Name	Ports
10	FastEthernet0/24
20	FastEthernet0/25
30	FastEthernet0/26
40	FastEthernet0/27
50	FastEthernet0/28
60	FastEthernet0/29
70	FastEthernet0/30
80	FastEthernet0/31
90	FastEthernet0/32
100	FastEthernet0/33
110	FastEthernet0/34
120	FastEthernet0/35
130	FastEthernet0/36
140	FastEthernet0/37
150	FastEthernet0/38
160	FastEthernet0/39
170	FastEthernet0/40
180	FastEthernet0/41
190	FastEthernet0/42
200	FastEthernet0/43
210	FastEthernet0/44
220	FastEthernet0/45
230	FastEthernet0/46
240	FastEthernet0/47
250	FastEthernet0/48
260	FastEthernet0/49
270	FastEthernet0/50
280	FastEthernet0/51
290	FastEthernet0/52
300	FastEthernet0/53
310	FastEthernet0/54
320	FastEthernet0/55
330	FastEthernet0/56
340	FastEthernet0/57
350	FastEthernet0/58
360	FastEthernet0/59
370	FastEthernet0/60
380	FastEthernet0/61
390	FastEthernet0/62
400	FastEthernet0/63
410	FastEthernet0/64
420	FastEthernet0/65
430	FastEthernet0/66
440	FastEthernet0/67
450	FastEthernet0/68
460	FastEthernet0/69
470	FastEthernet0/70
480	FastEthernet0/71
490	FastEthernet0/72
500	FastEthernet0/73
510	FastEthernet0/74
520	FastEthernet0/75
530	FastEthernet0/76
540	FastEthernet0/77
550	FastEthernet0/78
560	FastEthernet0/79
570	FastEthernet0/80
580	FastEthernet0/81
590	FastEthernet0/82
600	FastEthernet0/83
610	FastEthernet0/84
620	FastEthernet0/85
630	FastEthernet0/86
640	FastEthernet0/87
650	FastEthernet0/88
660	FastEthernet0/89
670	FastEthernet0/90
680	FastEthernet0/91
690	FastEthernet0/92
700	FastEthernet0/93
710	FastEthernet0/94
720	FastEthernet0/95
730	FastEthernet0/96
740	FastEthernet0/97
750	FastEthernet0/98
760	FastEthernet0/99
770	FastEthernet0/100
780	FastEthernet0/101
790	FastEthernet0/102
800	FastEthernet0/103
810	FastEthernet0/104
820	FastEthernet0/105
830	FastEthernet0/106
840	FastEthernet0/107
850	FastEthernet0/108
860	FastEthernet0/109
870	FastEthernet0/110
880	FastEthernet0/111
890	FastEthernet0/112
900	FastEthernet0/113
910	FastEthernet0/114
920	FastEthernet0/115
930	FastEthernet0/116
940	FastEthernet0/117
950	FastEthernet0/118
960	FastEthernet0/119
970	FastEthernet0/120
980	FastEthernet0/121
990	FastEthernet0/122
1000	FastEthernet0/123
1010	FastEthernet0/124
1020	FastEthernet0/125
1030	FastEthernet0/126
1040	FastEthernet0/127
1050	FastEthernet0/128
1060	FastEthernet0/129
1070	FastEthernet0/130
1080	FastEthernet0/131
1090	FastEthernet0/132
1100	FastEthernet0/133
1110	FastEthernet0/134
1120	FastEthernet0/135
1130	FastEthernet0/136
1140	FastEthernet0/137
1150	FastEthernet0/138
1160	FastEthernet0/139
1170	FastEthernet0/140
1180	FastEthernet0/141
1190	FastEthernet0/142
1200	FastEthernet0/143
1210	FastEthernet0/144
1220	FastEthernet0/145
1230	FastEthernet0/146
1240	FastEthernet0/147
1250	FastEthernet0/148
1260	FastEthernet0/149
1270	FastEthernet0/150
1280	FastEthernet0/151
1290	FastEthernet0/152
1300	FastEthernet0/153
1310	FastEthernet0/154
1320	FastEthernet0/155
1330	FastEthernet0/156
1340	FastEthernet0/157
1350	FastEthernet0/158
1360	FastEthernet0/159
1370	FastEthernet0/160
1380	FastEthernet0/161
1390	FastEthernet0/162
1400	FastEthernet0/163
1410	FastEthernet0/164
1420	FastEthernet0/165
1430	FastEthernet0/166
1440	FastEthernet0/167
1450	FastEthernet0/168
1460	FastEthernet0/169
1470	FastEthernet0/170
1480	FastEthernet0/171
1490	FastEthernet0/172
1500	FastEthernet0/173
1510	FastEthernet0/174
1520	FastEthernet0/175
1530	FastEthernet0/176
1540	FastEthernet0/177
1550	FastEthernet0/178
1560	FastEthernet0/179
1570	FastEthernet0/180
1580	FastEthernet0/181
1590	FastEthernet0/182
1600	FastEthernet0/183
1610	FastEthernet0/184
1620	FastEthernet0/185
1630	FastEthernet0/186
1640	FastEthernet0/187
1650	FastEthernet0/188
1660	FastEthernet0/189
1670	FastEthernet0/190
1680	FastEthernet0/191
1690	FastEthernet0/192
1700	FastEthernet0/193
1710	FastEthernet0/194
1720	FastEthernet0/195
1730	FastEthernet0/196
1740	FastEthernet0/197
1750	FastEthernet0/198
1760	FastEthernet0/199
1770	FastEthernet0/200
1780	FastEthernet0/201
1790	FastEthernet0/202
1800	FastEthernet0/203
1810	FastEthernet0/204
1820	FastEthernet0/205
1830	FastEthernet0/206
1840	FastEthernet0/207
1850	FastEthernet0/208
1860	FastEthernet0/209
1870	FastEthernet0/210
1880	FastEthernet0/211
1890	FastEthernet0/212
1900	FastEthernet0/213
1910	FastEthernet0/214
1920	FastEthernet0/215
1930	FastEthernet0/216
1940	FastEthernet0/217
1950	FastEthernet0/218
1960	FastEthernet0/219
1970	FastEthernet0/220
1980	FastEthernet0/221
1990	FastEthernet0/222
2000	FastEthernet0/223
2010	FastEthernet0/224
2020	FastEthernet0/225
2030	FastEthernet0/226
2040	FastEthernet0/227
2050	FastEthernet0/228
2060	FastEthernet0/229
2070	FastEthernet0/230
2080	FastEthernet0/231
2090	FastEthernet0/232
2100	FastEthernet0/233
2110	FastEthernet0/234
2120	FastEthernet0/235
2130	FastEthernet0/236
2140	FastEthernet0/237
2150	FastEthernet0/238
2160	FastEthernet0/239
2170	FastEthernet0/240
2180	FastEthernet0/241
2190	FastEthernet0/242
2200	FastEthernet0/243
2210	FastEthernet0/244
2220	FastEthernet0/245
2230	FastEthernet0/246
2240	FastEthernet0/247
2250	FastEthernet0/248
2260	FastEthernet0/249
2270	FastEthernet0/250
2280	FastEthernet0/251
2290	FastEthernet0/252
2300	FastEthernet0/253
2310	FastEthernet0/254
2320	FastEthernet0/255
2330	FastEthernet0/256
2340	FastEthernet0/257
2350	FastEthernet0/258
2360	FastEthernet0/259
2370	FastEthernet0/260
2380	FastEthernet0/261
2390	FastEthernet0/262
2400	FastEthernet0/263
2410	FastEthernet0/264
2420	FastEthernet0/265
2430	FastEthernet0/266
2440	FastEthernet0/267
2450	FastEthernet0/268
2460	FastEthernet0/269
2470	FastEthernet0/270
2480	FastEthernet0/271
2490	FastEthernet0/272
2500	FastEthernet0/273
2510	FastEthernet0/274
2520	FastEthernet0/275
2530	FastEthernet0/276
2540	FastEthernet0/277
2550	FastEthernet0/278
2560	FastEthernet0/279
2570	FastEthernet0/280
2580	FastEthernet0/281
2590	FastEthernet0/282
2600	FastEthernet0/283
2610	FastEthernet0/284
2620	FastEthernet0/285
2630	FastEthernet0/286
2640	FastEthernet0/287
2650	FastEthernet0/288
2660	FastEthernet0/289
2670	FastEthernet0/290
2680	FastEthernet0/291
2690	FastEthernet0/292
2700	FastEthernet0/293
2710	FastEthernet0/294
2720	FastEthernet0/295
2730	FastEthernet0/296
2740	FastEthernet0/297
2750	FastEthernet0/298
2760	FastEthernet0/299
2770	FastEthernet0/300
2780	FastEthernet0/301
2790	FastEthernet0/302
2800	FastEthernet0/303
2810	FastEthernet0/304
2820	FastEthernet0/305
2830	FastEthernet0/306
2840	FastEthernet0/307
2850	FastEthernet0/308
2860	FastEthernet0/309
2870	FastEthernet0/310
2880	FastEthernet0/311
2890	FastEthernet0/312
2900	FastEthernet0/313
2910	FastEthernet0/314
2920	FastEthernet0/315
2930	FastEthernet0/316
2940	FastEthernet0/317
2950	FastEthernet0/318
2960	FastEthernet0/319
2970	FastEthernet0/320
2980	FastEthernet0/321
2990	FastEthernet0/322
3000	FastEthernet0/323
3010	FastEthernet0/324
3020	FastEthernet0/325
3030	FastEthernet0/326
3040	FastEthernet0/327
3050	FastEthernet0/328
3060	FastEthernet0/329
3070	FastEthernet0/330
3080	FastEthernet0/331
3090	FastEthernet0/332
3100	FastEthernet0/333
3110	FastEthernet0/334
3120	FastEthernet0/335
3130	FastEthernet0/336
3140	FastEthernet0/337
3150	FastEthernet0/338
3160	FastEthernet0/339
3170	FastEthernet0/340
3180	FastEthernet0/341
3190	FastEthernet0/342
3200	FastEthernet0/343
3210	FastEthernet0/344
3220	FastEthernet0/345
3230	FastEthernet0/346
3240	FastEthernet0/347
3250	FastEthernet0/348
3260	FastEthernet0/349
3270	FastEthernet0/350
3280	FastEthernet0/351
3290	FastEthernet0/352
3300	FastEthernet0/353
3310	FastEthernet0/354
3320	FastEthernet0/355
3330	FastEthernet0/356
3340	FastEthernet0/357
3350	FastEthernet0/358
3360	FastEthernet0/359
3370	FastEthernet0/360
3380	FastEthernet0/361
3390	FastEthernet0/362
3400	FastEthernet0/363
3410	FastEthernet0/364
3420	FastEthernet0/365
3430	FastEthernet0/366
3440	FastEthernet0/367
3450	FastEthernet0/368
3460	FastEthernet0/369
3470	FastEthernet0/370
3480	FastEthernet0/371
3490	FastEthernet0/372
3500	FastEthernet0/373
3510	FastEthernet0/374
3520	FastEthernet0/375
3530	FastEthernet0/376
3540	FastEthernet0/377
3550	FastEthernet0/378
3560	FastEthernet0/379
3570	FastEthernet0/380
3580	FastEthernet0/381
3590	FastEthernet0/382
3600	FastEthernet0/383
3610	FastEthernet0/384
3620	FastEthernet0/385
3630	FastEthernet0/386
3640	FastEthernet0/387
3650	FastEthernet0/388
3660	FastEthernet0/389
3670	FastEthernet0/390
3680	FastEthernet0/391
3690	FastEthernet0/392
3700	FastEthernet0/393
3710	FastEthernet0/394
3720	FastEthernet0/395
3730	FastEthernet0/396
3740	FastEthernet0/397
3750	FastEthernet0/398
3760	FastEthernet0/399
3770	FastEthernet0/400
3780	FastEthernet0/401
3790	FastEthernet0/402
3800	FastEthernet0/403
3810	FastEthernet0/404
3820	FastEthernet0/405
3830	FastEthernet0/406
3840	FastEthernet0/407
3850	FastEthernet0/408
3860	FastEthernet0/409
3870	FastEthernet0/410
3880	FastEthernet0/411
3890	FastEthernet0/412
3900	FastEthernet0/413
3910	FastEthernet0/414
3920	FastEthernet0/415
3930	FastEthernet0/416
3940	FastEthernet0/417
3950	FastEthernet0/418
3960	FastEthernet0/419
3970	FastEthernet0/420
3980	FastEthernet0/421
3990	FastEthernet0/422
4000	FastEthernet0/423
4010	FastEthernet0/424
4020	FastEthernet0/425
4030	FastEthernet0/426
4040	FastEthernet0/427
4050	FastEthernet0/428
4060	FastEthernet0/429
4070	FastEthernet0/430
4080	FastEthernet0/431
4090	FastEthernet0/432
4100	FastEthernet0/433
4110	FastEthernet0/434
4120	FastEthernet0/435
4130	FastEthernet0/436
4140	FastEthernet0/437
4150	FastEthernet0/438
4160	FastEthernet0/439
4170	FastEthernet0/440
4180	FastEthernet0/441
4190	FastEthernet0/442
4200	FastEthernet0/443
4210	FastEthernet0/444
4220	FastEthernet0/445
4230	FastEthernet0/446
4240	FastEthernet0/447
4250	FastEthernet0/448
4260	FastEthernet0/449
4270	FastEthernet0/450
4280	FastEthernet0/451
4290	FastEthernet0/452
4300	FastEthernet0/453
4310	FastEthernet0/454
4320	FastEthernet0/455
4330	FastEthernet0/456
4340	FastEthernet0/457
4350	FastEthernet0/458
4360	FastEthernet0/459
4370	FastEthernet0/460
4380	FastEthernet0/461
4390	FastEthernet0/462
4400	FastEthernet0/463
4410	FastEthernet0/464
4420	FastEthernet0/465
4430	FastEthernet0/466
4440	FastEthernet0/467
4450	FastEthernet0/468
4460	FastEthernet0/469
4470	FastEthernet0/470
4480	FastEthernet0/471
4490	FastEthernet0/472
4500	FastEthernet0/473
4510	FastEthernet0/474
4520	FastEthernet0/475
4530	FastEthernet0/476
4540	FastEthernet0/477
4550	FastEthernet0/478
4560	FastEthernet0/479
4570	FastEthernet0/480
4580	FastEthernet0/481
4590	FastEthernet0/482
4600	FastEthernet0/483
4610	FastEthernet0/484
4620	FastEthernet0/485
4630	FastEthernet0/486
4640	FastEthernet0/487
4650	FastEthernet0/488
4660	FastEthernet0/489
4670	FastEthernet0/490
4680	FastEthernet0/491
4690	FastEthernet0/492
4700	FastEthernet0/493
4710	FastEthernet0/494
4720	FastEthernet0/495
4730	FastEthernet0/496
4740	FastEthernet0/497
4750	FastEthernet0/498
4760	FastEthernet0/499
4770	FastEthernet0/500
4780	FastEthernet0/501
4790	FastEthernet0/502
4800	FastEthernet0/503
4810	FastEthernet0/504
4820	FastEthernet0/505
4830	FastEthernet0/506
4840	FastEthernet0/507
4850	FastEthernet0/508
4860	FastEthernet



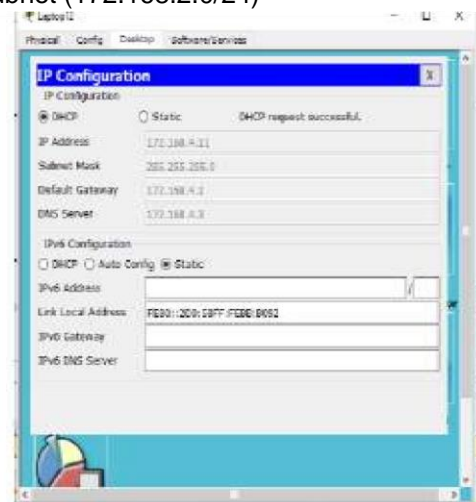
Agric subnet (172.168.1.0/24)



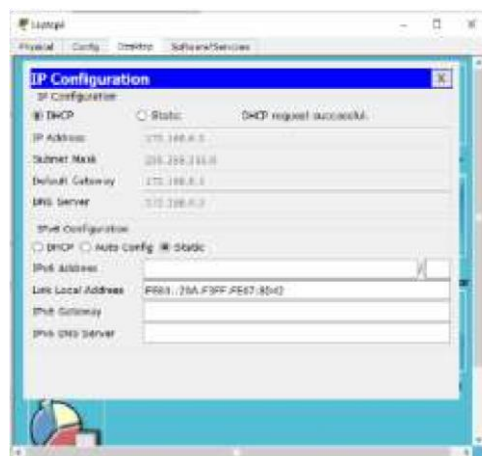
civil subnet (172.168.2.0/24)



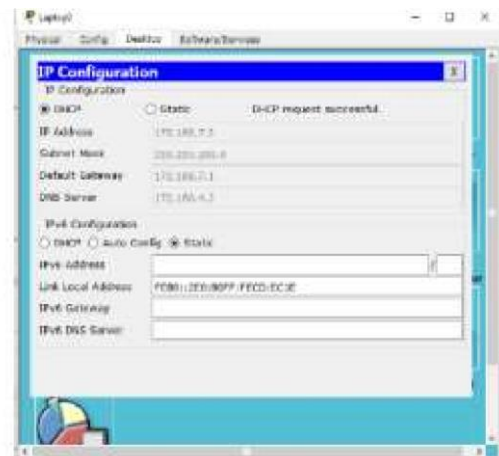
Mech subnet (172.168.3.0/24)



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.

```

Command Prompt

PC>ping 172.168.0.5

Pinging 172.168.0.5 with 32 bytes of data:

Reply from 172.168.0.6: bytes=32 time=14ms TTL=127
Reply from 172.168.0.6: bytes=32 time=13ms TTL=127
Reply from 172.168.0.6: bytes=32 time=9ms TTL=127
Reply from 172.168.0.6: bytes=32 time=13ms TTL=127

Ping statistics for 172.168.0.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 9ms, Maximum = 14ms, Average = 9ms

PC>

```

Network Center□elect

```

Command Prompt

PC>ping 172.168.2.8

Pinging 172.168.2.8 with 32 bytes of data:

Reply from 172.168.2.8: bytes=32 time=11ms TTL=127
Reply from 172.168.2.8: bytes=32 time=6ms TTL=127
Reply from 172.168.2.8: bytes=32 time=5ms TTL=127
Reply from 172.168.2.8: bytes=32 time=4ms TTL=127

Ping statistics for 172.168.2.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 6ms, Average = 4ms

PC>

```

Network center□civil

```

Command Prompt

PC>ping 172.168.6.1

Pinging 172.168.6.1 with 32 bytes of data:

Reply from 172.168.6.1: bytes=32 time=1ms TTL=255
Reply from 172.168.6.1: bytes=32 time=3ms TTL=255
Reply from 172.168.6.1: bytes=32 time=3ms TTL=255
Reply from 172.168.6.1: bytes=32 time=13ms TTL=255

Ping statistics for 172.168.6.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 13ms, Average = 4ms

PC>

```

Network center□new aud

```

Command Prompt

PC>ping 172.168.7.5

Pinging 172.168.7.5 with 32 bytes of data:

Request timed out.
Reply from 172.168.7.5: bytes=32 time=46ms TTL=127
Reply from 172.168.7.5: bytes=32 time=13ms TTL=127
Reply from 172.168.7.5: bytes=32 time=11ms TTL=127

Ping statistics for 172.168.7.5:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 11ms, Maximum = 46ms, Average = 10ms

PC>

```

Network center□library

```

Command Prompt

PC>ping 172.168.1.6

Pinging 172.168.1.6 with 32 bytes of data:

Request timed out.
Reply from 172.168.1.6: bytes=32 time=9ms TTL=127
Reply from 172.168.1.6: bytes=32 time=9ms TTL=127
Reply from 172.168.1.6: bytes=32 time=9ms TTL=127

Ping statistics for 172.168.1.6:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 9ms, Average = 0ms

PC>

```

Network center□agric

```

Command Prompt

PC>ping 172.168.3.8

Pinging 172.168.3.8 with 32 bytes of data:

Reply from 172.168.3.8: bytes=32 time=14ms TTL=127
Reply from 172.168.3.8: bytes=32 time=5ms TTL=127
Reply from 172.168.3.8: bytes=32 time=13ms TTL=127
Reply from 172.168.3.8: bytes=32 time=63ms TTL=127

Ping statistics for 172.168.3.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 13ms, Maximum = 63ms, Average = 34ms

PC>

```

Network center□Mech

```

Command Prompt

PC>ping 172.168.5.6

Pinging 172.168.5.6 with 32 bytes of data:

Reply from 172.168.5.6: bytes=32 time=13ms TTL=127
Reply from 172.168.5.6: bytes=32 time=12ms TTL=127
Reply from 172.168.5.6: bytes=32 time=13ms TTL=127
Reply from 172.168.5.6: bytes=32 time=13ms TTL=127

Ping statistics for 172.168.5.6:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 12ms, Maximum = 13ms, Average = 12ms

PC>

```

Network center□old aud

```

Command Prompt

Packet Tracer PC Command Line 1.0
PC>ping 172.168.4.11

Pinging 172.168.4.11 with 32 bytes of data:

Reply from 172.168.4.11: bytes=32 time=27ms TTL=127
Reply from 172.168.4.11: bytes=32 time=50ms TTL=127
Reply from 172.168.4.11: bytes=32 time=56ms TTL=127
Reply from 172.168.4.11: bytes=32 time=56ms TTL=127

Ping statistics for 172.168.4.11:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 27ms, Maximum = 56ms, Average = 47ms

PC>

```

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.

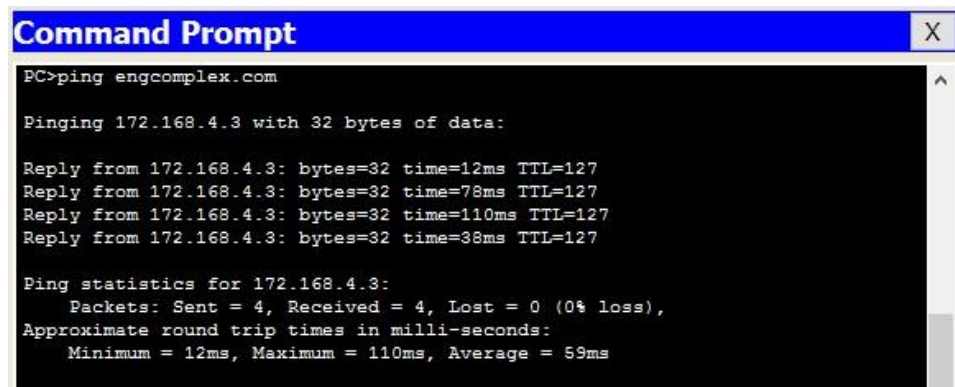

```
C:\Users\jones>ping 10.3.1.249

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.

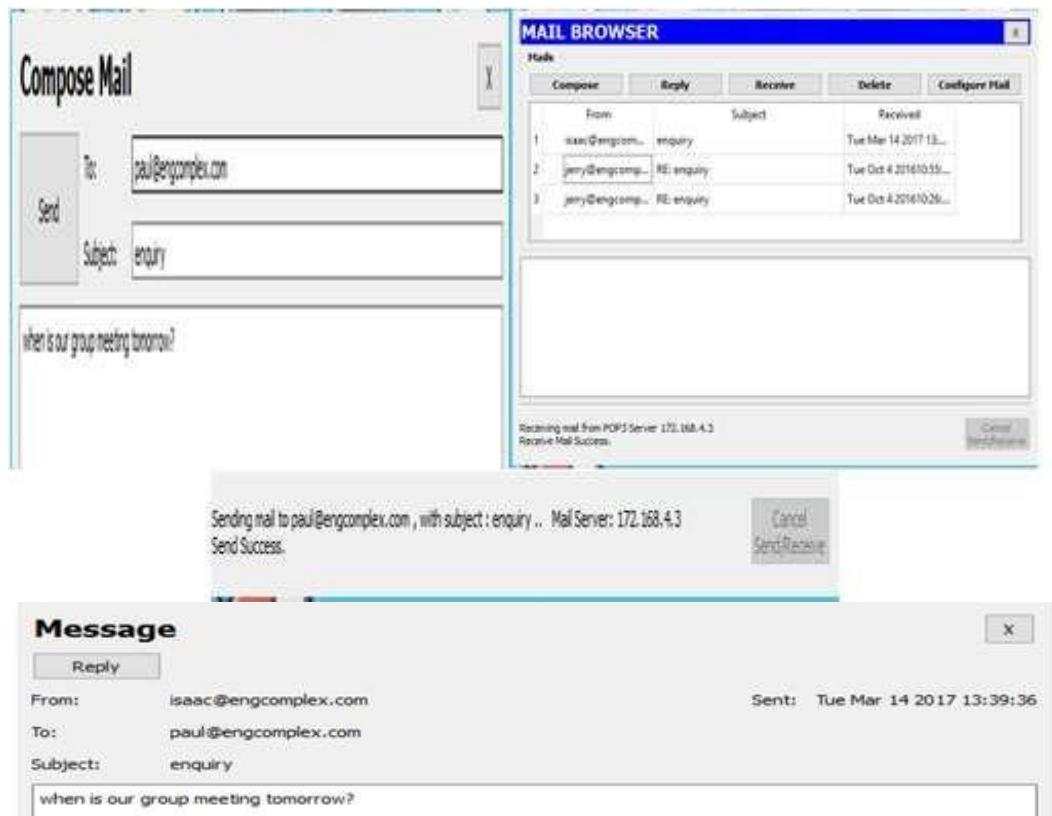


Figure 9: E-mail service result

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)		$\sum (\text{Weight} * \text{Scale Factor})/5 = \underline{\hspace{2cm}}$				

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/Socket_Java.pdf