

**FOURAH BAY COLLEGE
UNIVERSITY OF SIERRA LEONE**

**NETWORK SECURITY USING VIRTUAL PRIVATE
NETWORK AND SURVEILLANCE IP CAMERAS**

BY

IBRAHIM SALIEU KAMARA

ID: 34022

A Project Submitted to the Department of Electrical and Electronic Engineering, Fourah Bay College, University of Sierra Leone, in part fulfillment of the requirement for the Award of the degree of Bachelor of Engineering with Honours in Electrical and Electronic Engineering.

March, 2021

CERTIFICATION

This is to certify that Ibrahim Salieu Kamara, with registration number 34022, has successfully completed this dissertation under my supervision, and I hereby approve of its submission to the Department of Electrical and Electronic Engineering, Fourah Bay College, University of Sierra Leone.

Ing. JONAS PROFESSOR REDWOOD-SAWYERR

IBRAHIM SALIEU KAMARA

SUPERVISOR'S SIGNATURE & DATE

STUDENT'S SIGNATURE & DATE

DEDICATION

This work is dedicated to my late father and brother; Pa Salieu and Mashud Chernor Salieu Kamara, whose memory could not be forgotten. They would have been happy to live and see entrepreneurs, doctor and engineers in our family but they are no more. Their departure on earth lived a void in the Kamara Family. May their souls rest in perfect peace.

ACKNOWLEDGEMENT

I would like to take this opportunity to first and foremost thank the Almighty Allah for giving me the wisdom and strength in writing of this project. I will always glorify you and worship you alone.

I extend my sincere gratitude and thanks to my noble supervisor; Ing Professor Redwood-Sawyer for the guide and support he had given me in writing out this project. The department of electrical and electronic engineering, Fourah Bay College, University of Sierra Leone for providing me the platform to study and practice electrical engineering; the Tiwai Memory Masters (TMM) Freetown-Sierra Leone for guiding and providing me a career path in networking and telecommunications. These institutions helped me greatly in knowing the principles of electrical and computer engineering. I must express my sincere thanks to these institutions.

My family has helped me tremendously in my course of study and I have to give thanks to every family member who help me greatly in my years of studying electrical engineering. I give special thanks and appreciations to my mother Ya Kadiatu Sesay and my elder sister Yainkain Kamara and the rest of the family members. Special thanks to my friends and love ones especially Stella Haja Kargbo who was by my side at the time of writing this project. I love you all.

ABSTRACT

Internet theft or fraud is growing rapidly across the globe due to the growing number of computer scientists whom some of them may have the intention to use their technological skills in the odd ways. Governments and financial institutions are looking for concrete ways to minimise this online theft activities. Some of the best solutions to limit this is to implement network security systems by using Virtual Private Network (VPN); the term given to a logical connection of private networks in which the activities of the network systems are encrypted and decrypted so that if someone sits along the Internet will not be able to translate the intelligent of communication. This security system is applicable when corporate network head offices want to link to their branches offices remotely. It is under this concept that the project ***“Network Security Using Virtual Private Network and Surveillance IP Cameras”*** was designed to actually mitigate network fraud. The National Social Security and Insurance Trust (NASSIT) is a case study as they are currently putting security measures in place to their Wide Area Network (WAN).

Surveillance IP Cameras system were provided using Internet of Things (IoTs) to provide registration login system that will display images in control room monitors. Enable secret passwords are in place before someone logs into the network device. The principle behind this project is to ensure that the network in operation security is a priority.

A software like Packet Tracer will provide all the simulation steps for this project design. A number of stages to achieve that is to first have Virtual Local Area Networks (VLANs) configured to separate the broadcast domain, Dynamic Host Configuration Protocol (DHCP) to dynamically give IP addresses to end host devices, routing to forward IP packets across networks. With all these in place, we configure the VPN and the surveillance IP Cameras.

TABLE OF CONTENTS

CERTIFICATION.....	i
DEDICATION	ii
ACKNOWLEDGEMENT	iii
ABSTRACT	iv
LIST OF FIGURES.....	ix
LIST OF TABLES	xi
CHAPTER ONE.....	1
1 Introduction.....	1
1.2 Brief Review and Background of the Research.....	2
1.3 Need for the Research.....	3
1.4 The Aims of the Project.....	3
1.5 The Objectives of the Project	4
1.6 Project Plan Scope	5
CHAPTER TWO.....	7
2.1 Internet Functionalities	7
2.2 Virtual Private Network.....	8
2.2.1 IPSec VPN	9
2.2.2 Internet Security Association Key Management Protocol (ISAKMP)	9
2.3 The OSI (Open System Interconnections) Model	11
2.3.1 Layer 7 - Application.....	12
2.3.2 Layer 6 - Presentation.....	13
2.3.3 Layer 5 – Session.....	13
2.3.4 Layer 4 – Transport	14
2.3.5 Layer 3 – Network.....	15
2.3.6 Layer 2 – Data Link Layer.....	15
2.3.7 Layer 1 – Physical.....	17
2.4 Network Devices.....	17
2.4.1 Network Switch	17

2.4.2 Routers	18
2.4.3 Wireless Access Point (WAP)	19
2.5 Network Topologies	19
2.5.1 Bus Topology.....	19
2.5.2 Star Topology	20
2.5.3 Ring Topology	21
2.5.4 Mesh Topology	22
2.6 Network Types.....	23
2.6.1 LAN (Local Area Network).....	24
2.6.2 MAN (Metropolitan Area Network).....	24
2.6.3 WAN (Wide Area Network).....	25
2.6.4 PAN (Personal Area Network)	26
2.7 Optical Fiber Communication	27
2.7.1 Physical Structure of an Optical Fiber.....	28
2.7.2 Types of Optical Fibers	29
2.7.3 Fiber Splicing.....	29
□ Advantages of using Optical Fiber.....	30
□ Disadvantages of using Optical Fiber	30
Applications of Fiber Optics.....	30
2.8 Internet Protocol	31
2.8.1 Versions of IP Addresses.....	31
2.8.2 Classes of IPV4 Addresses	31
2.8.3 Some examples of classes A to C IP Addresses in Decimal Notation	33
2.8.4 Types of IP Addresses	33
2.8.5 Types of Address	35
2.8.6 Loopback IP Addresses	35
CHAPTER THREE.....	36
3.1 Methodology	36
3.2 Physical Network Setup and Hardware Device Installations	36
3.2.1 Network Faceplate and Jack Pinout.....	37

3.2.2 Running Network Cablings	37
3.2.3 Category 6 Cable (Cat 6)	38
3.2.4 The Role of the Data Center	38
3.3 Network Hardware Devices Installations	40
3.4 Logical Network Setup	40
3.4.1 IP Address Subnetting	41
3.5 Feasibility Studies.....	44
3. 4 Assigning VLANs	45
3.5 Logical Network Hierarchical Model.....	46
CHAPTER FOUR	48
4.1 NASSIT Network Design	48
4.1.1 Physical Network Architecture.....	49
4.1.2 Packet Tracer 7.2.1 Exploration	49
4.2 Renaming Network Devices	50
4.3 VLANs Configuration	51
4.3.1 Router on a Stick.....	52
4.4 DHCP Configurations.....	53
4.5 Routes and Routing Protocols	54
4.5.1 Types of Routes	54
4.5.2 Routing Information Protocol Version 2 (RIP V2)	55
4.6 Testing for Reachability	57
4.7 Call Manager Express (CME) for Voice over IP (VoIP)	57
4.7.1 VoIP Configuration	58
4.8 Server Administration Managements	59
4.8.1 Some Server Resources Administration	60
4.8.1 DNS Servers	60
4.8.1.2 Web Servers.....	60
4.8.3 File Servers	61
4.8.1.4 Network Time Protocol Server (NTP).....	62
4.9 VPN Configuration.....	62

4.9.1 ISAKMP IKE Phase I Configurations.....	65
4.9.2 ISAKMP IKE Phase II Configurations	66
4.9.3 Testing for Encapsulated VPN Payloads.....	66
4.10 Internet of Things (IoTs) with Motion Detector and IP Camera.....	68
4.10.1 Webcam-IP Camera.....	68
4.10.2 Motion Detector.....	69
CHAPTER FIVE.....	74
5.1 Summary and Conclusion.....	74
5.2 Results and Discussions.....	75
5.3 Challenges.....	75
5.4 Recommendations.....	76
5.5 References.....	77
Appendices.....	78
Appendix A1 VLANs Configurations	78
Appendix A2 802.1Q Configurations.....	79
Appendix B	80
<i>DHCP Configurations</i>	80
Appendix C	81
ISP_ROUTER, Point to Point & VPN ROUTERS Configurations	81
Appendix D.....	82
VPN ROUTERS Configurations	82
Appendix E	83
ROUTING	83
ISP ROUTER.....	83
Appendix F	84
TELEPHONY-SERVICE.....	84
Appendix G.....	87
<i>HTML Syntax for the HTTP Server</i>	87
Appendix H.....	87
IPSec VPN Configurations	87

LIST OF FIGURES

Figure 2.1: IPSec VPN Encryption Tunnel.....	8
Figure 2.2: Plain Text Payload Header	10
Figure 2.3: IPSec Tunnel Mode Payload Header.....	11
Figure 2.4: MAC Address	16
Figure 2.5: CISCO Switch	18
Figure 2.6: CISCO Network Router and MODEM Router	18
Figure 2.7: Wireless Access Point.....	19
Figure 2.8: Bus Topology.....	20
Figure 2.9: Star Topology	21
Figure 2.10: Ring Topology	22
Figure 2.11: Mesh Topology	23
Figure 2.12: LAN Setup Network	24
Figure 2.13: MAN Network	25
Figure 2.14: WAN Network Type.....	26
Figure 2.15: PAN Network	27
Figure 2.16: Optical Glass Fiber	27
Figure 2.17: Physical Structure of Optical Fiber	28
Figure 2.18: A Photo of Splicing Optical Fiber	30
Figure 2.19: Host and Network Bit IDs IPV4 Classes.....	32
Figure 3.1: Network Faceplate and Jack Pinout.....	37
Figure 3.2: Punching STP Cat6 Cables to the Patch Panel.....	38
Figure 3.3: Data Center containing Network Racks	39
Figure 3.4: Network Installation Devices	40
Figure 3.5: A Display of Point to Point NASSIT Offices Routing across the Country	45
Fig 3.6: The Logical network Hierarchical model Architecture.....	47
Figure 4.1: NASSIT Network Design Topology	48
Figure 4.2: NASSIT Network Physical Design	49
Figure 4.3: Packet Tracer 7.2.1 Working Environment.....	50
Figure 4.4: Routing Information Advertising Neighbouring Networks	54
Figure 4.5: RIP V2 Routing Table	56
Figure 4.6: OSI Model Practical Detail.....	57
Figure 4.8: IP Phone Call between two Networks	59

Figure 4.9: A Display of the Corporate NASSIT Network Website	61
Figure 4.10: Enabling Security License	63
Figure 4.11: IPSec VPN Decision for VPN Routers	64
Figure 4.12: Encrypted IP Header of the Payload Networks	67
Figure 4.13: SADB IPSec VPN Security Verified.....	68
Figure 4.14: Webcam and Motion Detector in Packet Tracer	70
Figure 4.15: Webcams and Motion Detector True Physical Appearances	70
Figure 4.16: IoT Devices.....	71
Figure 4.17: IoT Registration Server Login	72
Figure 4.18: The Motion Detector and IP Camera are ON displaying image on the IoT monitor	72
Figure 4.19: IP Camera Image Control Conditions	73

LIST OF TABLES

Table 2.1: OSI Model Layers showing corresponding PDUs.....	12
Table 2.2: Class-full IP Addresses	32
Table 3.1: Usable IPV4 Classful Range.....	41
Table 3.2: VLANs Subnetting.....	42
Table 3.3 a: Borrowing Six Host Bits from the Subnet Mask	43
Table 3.3 b: New Subnet Mask Form	43
Table 3.4: Subnet Blocks of VLAN 20 DATA Networks	44
Table 3.5: Assigning VLANs to Network Devices.....	46
Table 3.6: Assigning Subnet IP Addresses to VLANs	46
Table 4.1: Devices Renaming in CLI.....	51

CHAPTER ONE

1 Introduction

The expansion of an office network infrastructure with its head office containing the centralised servers and other network devices with the other offices that it spans across is crucial to increase the production and the efficiency of an organisation. For this reason any government, financial institution or organisation that wants to enjoy secured establish links of its offices and remote access of the system resources using the Internet as a medium need a secured network. A secured network prevent vulnerability of data capturing in the presence of a third party. A Virtual Private Network (VPN) offers a solution to limit individuals trying to break into the network in remote locations. The network security could be much more robust and reliable if the organisation consider the thereat which could be in the form of remote access and physical attacks in which a third party trying to intrude into the network system and capture packet (data) that does not meant to be viewed by the general public.

The design and implementation of Virtual Private Network (VPN) offers a perfect solution to limit individuals from breaking into the designed network system. VPN is a network design system that transmit data across networks in an encrypt format and the data can only be decrypted in the destination network by using the agreed key exchange pairs within the network parties.

VPN has its limitation in terms of security system. VPN security level is limited on logical viewpoints for remote attacks. It does not prevent an organisation's network from physical attacks. Physical attacks in the sense an individual break in into the data center and do some changes to the network configurations.

For this reason surveillance IP cameras will be used to monitor network systems against physical attacks. These network devices use intelligent motion detector and webcam technology to constantly capture any physical object that passes across install network devices in control rooms. Enable secret passwords are also crucial to prevent unauthorise individual from login into network devices.

The design and implementation of simulation tool like Cisco Packet Tracer offers a way to predict expected real network physical design.

1.2 Brief Review and Background of the Research

This project research is based on a related real life network design with the aim of establishing a secured network where the researcher took NASSIT as a case study. In the internship period, the researcher is an intern student at a network design institution “Tiwai Memory Masters Solution (TMM)” was at the aim of designing the said network in which the above mentioned securities are to be implemented.

The NASSIT is a case study as they are currently expanding their network offices in Freetown, North, East and the Southern parts of the country. It is very difficult for the researcher to bring along his supervisor and senior lecturers to the network site locations where he is currently working as an intern student. For this reason, a simulation tool software like packet tracer can actually predict the output of the network design with respect to the physical setup and the logical configurations. A review of visiting NASSIT offices and get information from administration helps to determine how the actual network design will be.

Image photos of building sites, logical flow charts and real geographical locations with Google Map to fully actualise and track major locations of the network offices across the country to physically see how the routing information travel across networks are also carried out. The network devices are setup and configure with packet tracer and troubleshoot to capture out all possible faults that may cause the network to fail in its real lifetime operation.

1.3 Need for the Research

As network implementations have just taken it form in the country from the olden system where few network devices like routers, analog telephone system (the Panasonics), switches and few Personal Computers (PCs) are installed in offices with Internet access, they do not fully equipped with strong network security systems. Network designers have proven it that most of these big government offices and financial institutions do data sharing across their offices in a decrypted (plain texts) formats. For this reason office networks need to be design and kept secured. It is the aim of this project trying to provide all the network security design systems in global standard. It is very hard to get the project done with all the above named facilities being implemented but persistent research and meet along with network expertise will greatly help the project achieve its goals. And when the goals are achieve any government or financial institutions that will follow these security protocols will no longer fear the dangers of network attacks physically and remotely.

1.4 The Aims of the Project

The aim of this project design is to provide a secure network design by implementing VPN and surveillance IP Camera security to ensure secure and robust network system.

- **Site-to-site:** Tunnel mode IPSec VPN connection between VPN gateways to establish data encryption and private IP address translation before the IP packets enter into the Internet as insecure medium. The process of encrypting and transferring data between networks is transparent to end-users.
- **Surveillance IP Camera:** IP Cameras use Internet of Things to capture images in network control rooms as means to prevent and control physical attacks.
- Also enable secret password will be in place to every network device to prevent unauthorise login to the network devices.

1.5 The Objectives of the Project

- **Reduce Broadcast Domain**

The project is design in order to simulate the NASSIT organisation network with Virtual Area Network (VLANs) to separate the traffic generated by different subnetworks. VLANs are new type of LANs architecture using intelligent high speed switches concept to break large broadcast domain into smaller broadcast domains. Consider VLAN as a subnet that means two different subnets cannot communicate with each other without router, different VLANs also require router to communicate.

- **Provides Dynamic Host Configuration Protocol (DHCP) Server**

To reduce the work of the network administrator to manually configure each client's host device, the DHCP Sever employs client – server architecture in which a DHCP server is configured with a pool of available IP addresses and assigns one of them to a DHCP host request.

- **Routing Information Protocols**

This will enable the routing or forwarding of IP packets from one network to the other by agreeing with the Open System Interconnection (OSI) layer 3.

- **VPN Configurations**

Access lists to permit VPNs encapsulated, encrypted, decapsulated and decrypted IP packets between VPN networks across the Internet. With access lists VPN permission in place, we now configure the VPNs.

- **IoT Server Registration Login**

The IoT server registration login enable us to provide an IoT account to completely have control of the surveillance IP Cameras with the use of the motion detector respectively.

1.6 Project Plan Scope

The project has been divided into five chapters. Chapter one of course gives brief introduction of the project.

Chapter two focus on the literature review. The literature review gives theoretical frameworks that supports related areas to the project design. Here we shall discuss Internet functionalities, the Open System Interconnections (OSI) Model, network devices, network topologies, network types, Optical Fiber Communication, Internet Protocol (IP) addressing etc.

Chapter three will focus specifically with the methodology, which split or modularises the project design scope.

The methodology breaks down the project into small building blocks thereby explaining the physical network topology and the subnetting that will break down a single IP address and allocate the new subnets to various networks form the project's WAN network.

In chapter four, we now bring the building blocks of the methodology done in chapter three and join them to achieve the project goal.

The design requirement will be done showing all the configurations and supporting image figures.

The VLANs are first configure to the network switches, a configured DHCP should be able to release an IP addresses and assign them to the network devices within the network, a routing protocol version 2 (RIP V2) configuration to route IP packets within and outside the networks, server managements and IP telephony for voice over IP (VoIP) etc. Finally the IPSec VPNs are configure to the routers that connect to the Internet and surveillance IP cameras will be configure.

Chapter five will be a short chapter that will summarise, conclude and give challenges, recommendations and references on related areas of the project design. This chapter will verify that the project aims and objectives are obtain. The summary and the conclusion will give supporting facts to show that what was planned in the project design stages are achieved. The limitations clearly shows what could have done to make the project more robust but not included in the project. These limitations could be the hardware and software requirements that have impact on the entire project's designs, the time frame to submit the project etc.

Finally, the project will provide appendix that clearly outline the complex configurations of the network designs.

CHAPTER TWO

2.1 Internet Functionalities

A computer network is a group of computers linked to each other that enables them to communicate with another computers and share resources such as data, and application programmes etc. [8].

The Internet is the global system of interconnected computer networks that uses the Internet protocol suite to communicate between network devices [1]. It is a network of networks that consists of private, public, academic, business, and government networks of local to global scope linked by a broad array of electronic, wireless, and optical networking technologies etc. The Internet carries a vast range of information resources and services, such as the inter-linked hypertext documents and applications of the World Wide (WWW), electronic mail, telephony services and file sharing etc.

The origin of the Internet was dated back to the development of packets switching and research commissioned by the United States Department of Defense in the 1960s to enable time-sharing of computers. The primary precursor network, the ARPANET (Advanced Research Projects Agency Network), initially served as a backbone for interconnection of regional academic and military networks in the 1970s. The funding of the National Science Foundation Network (NSFNET) as a new backbone in the 1980s, as well as private funding for other commercial extensions, led to worldwide participation in the development of new networking technologies, and the merger of many networks.

The linking of commercial networks and enterprises by the early 1990s marked the beginning of the transition to the modern Internet and generated a sustained exponential growth as generations of institutional, personal computers and mobile devices were connected to the network.

2.2 Virtual Private Network

A VPN is a logical connection of private networks that encrypt the traffic and hide the end host IP address between networks as the traffic passes through the Internet as an unsecure medium. A site-to-site VPN refers to private network connections in which the network of one location is connected to the network of another location via a VPN. Frame Relay, ATM, and MPLS VPNs are examples of site-to-site VPNs [16]. A VPN is a combination of tunnel interface and encrypted text as shown in the figure below.

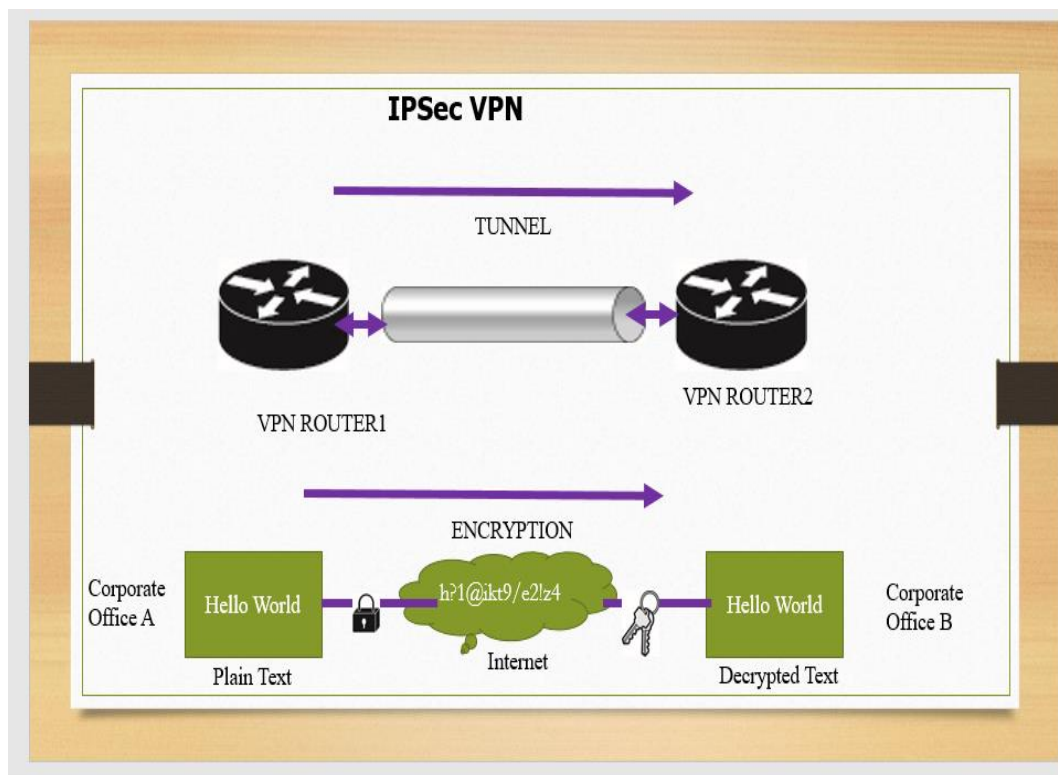


Figure 2.1: IPSec VPN Encryption Tunnel

2.2.1 IPSec VPN

IPSec is designed to provide security that encrypt the traffic and hide a host IP address as the traffic passes through the Internet [17].

The set of security services offered by the IPSec VPN includes access control, connectionless integrity, data origin authentication, protection against replays, confidentiality, and limited traffic flow etc.

VPN do not only extend to routers and other network devices it can also be use by mobile users to enable them do a secure surfing of the Internet. A mobile VPN provides the same level of security as does by any other network device.

- Public WIFI (Wireless Fidelity) are not secure as anybody can do packet sniffing to view your online activities.
- A better way to limit this is to have a client VPN install on your mobile device.
- A number of mobile VPN applications are now freely available on Play Store. They are light weight and easy to install. Some of the most secure VPN applications: Aza VPN Lite, 3X VPN, Lion VPN, KUTO VPN, Thunder VPN etc.

2.2.2 Internet Security Association Key Management Protocol (ISAKMP)

ISAKMP is a protocol used to establish security association and cryptographic keys among secured connected networks. The communication between the remote networks is an Internet Key Exchange (IKE) happen in two phase. IKE Phase 1 and IKE Phase II.

The setup in the IKE Phase I cryptography is given by the mnemonic “**HAGLE**”

- **H** – Hash (MD5, SHA-1) the method used to scramble the plain texts.

- **A** – Authentication to identify VPN pair routers.
- **G** – Group is a Diffie Hellman Group (DH Group) the password key length agreement.
- **L** – Lifetime, how often the IKE phase should be review.
- **E** – Encryption to establish a secured tunnel.

The purpose of IKE Phase II is to negotiate the setup IPSec tunnel interface and feed the encrypted data into it. IPSec VPN operates in two modes:

- **Transport Mode**

In transport mode, only the IP packet is encrypted, the IP header of the host device do not as it passes across the Internet.

- **Tunnel Mode**

In tunnel mode, both the IP packet and the IP header are encrypted. With tunnel mode we add a new IP header on top of the original IP packet. This could be useful when you are using private IP addresses and you need to tunnel your traffic over the Internet.

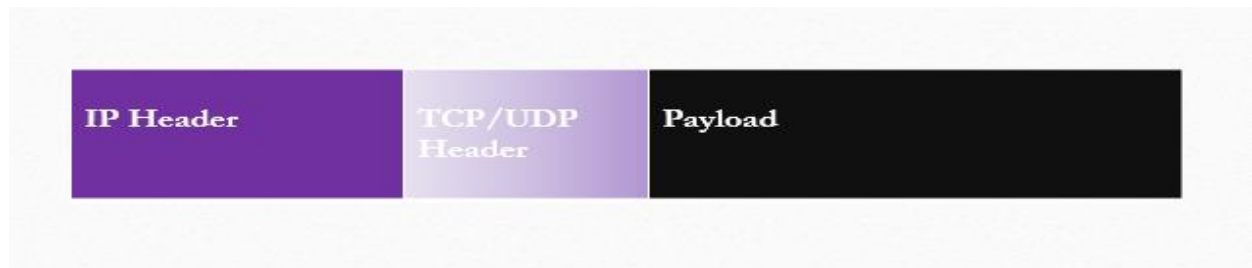


Figure 2.2: Plain Text Payload Header

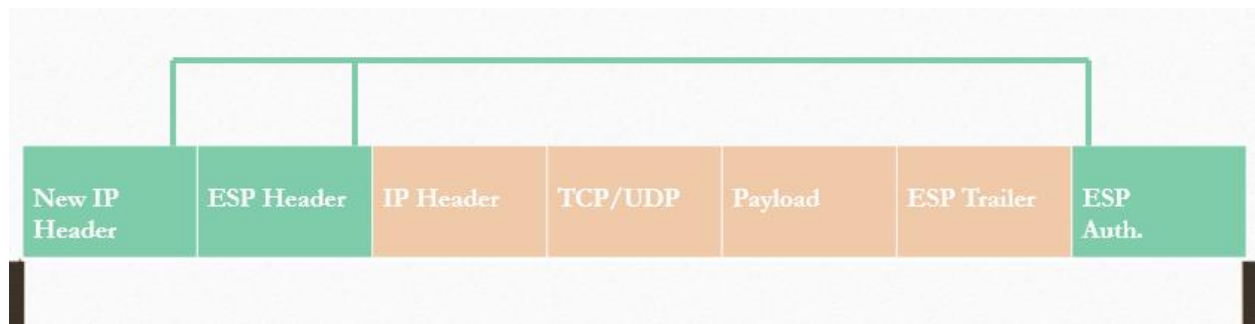


Figure 2.3: IPSec Tunnel Mode Payload Header

2.3 The OSI (Open System Interconnections) Model

The International Organisation for standardisation (ISO) has defined a standard called Open Systems Interconnection (OSI) Reference Model. It is a conceptual model that characterises and standardises the internal functions of a communication system by giving seven outline layers [2]. The Physical Layer, Data Link Layer, Network Layer, Transport Layer, Session Layer, Presentation Layer and the Application Layer. The concept of each of these layers shall be discuss in the course of the project development and how they can help the network administrators in troubleshooting and setting up a standard network layout [3].

Due to the rapid growth of computer networks caused by compatibility problems the ISO released the OSI Model in **1984** to make different hardware devices able to communicate to one another effectively.

Data exist in each layer has a unit call Protocol Data Unit (PDU). Each layer performs the functions of the layer above and below it. The seven layers of the OSI are given in the table below.

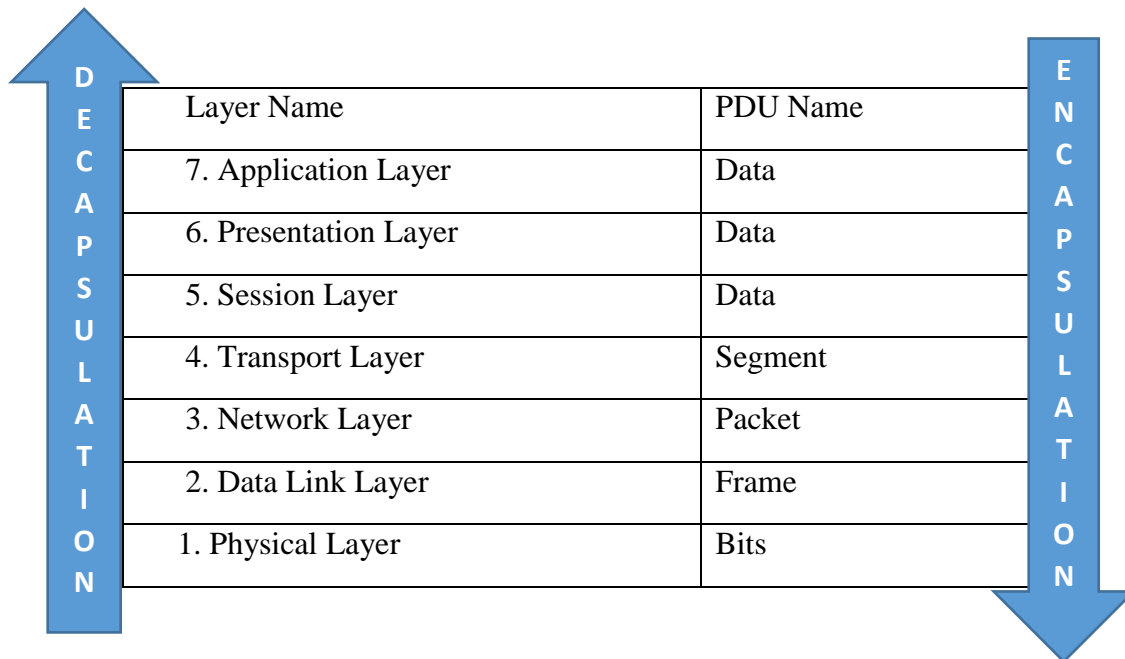


Table 2.1: OSI Model Layers showing corresponding PDUs

2.3.1 Layer 7 - Application

The application layer is used by network application programmes for providing services and interfaces to the end users. This layer enables users to load application programmes such as web browser, e-mail etc.

Some functions of the application layer are:

- i. Web Surfing ii. File transfer iii. Email
- iv. Virtual Terminal v. Mail services vi. Directory services

Devices found in the application layer are; Computers, Firewalls etc.

The protocols of the application layer are;

HTTP – Hypertext Transfer Protocol

FTP – File Transfer Protocol

SMTP – Simple Mail Transfer Protocol

TELNET – Terminal Network

POP3 – Post Office Protocol

2.3.2 Layer 6 - Presentation

The presentation layer receives data from the session or application layer. It deals with syntax and semantic of the information exchange between sending and receiving devices [4]. The presentation layer compresses, encrypts and translate this data into readable format and then send it over the session or application layer. Functions of the presentation layer are:

- (i). **Data compression:** For speedily and easy transfer, big file of data are compressed from their original sizes.
- (ii). **Data Encryption:** The data is converted into cipher text and appear scramble so that when capture by unauthorise receiver cannot understand its content information.
- (iii). **Data Decryption:** data is decrypted or converted into plain text to readable format for the authorise receiver.

Devices used in the presentation layer are: PCs, Firewalls, routers etc.

The protocols of the presentation layer are:

SSL – Secure Sockets Layer.

ASCII – American Standard Code for Information Interchange.

EBCDIC – Extended Binary Coded Decimal Interchange Code.

2.3.3 Layer 5 – Session

The session layer is responsible for dialog control and synchronisation [5]. The session layer establish, maintains and terminates sessions between application programmes. The functions of the session layer are:

i. Dialog Control: The session layer allows two systems to enter into a dialog. It allows the communication between two processes to take place in either simplex – only one device is the sender, half duplex – one way at a time and full duplex – both devices can send and receive at the same time.

ii. Synchronisation: For a system sending a file of 100 pages, if at the event of sending the pages and it turn out to be only 80 pages are sent are the remaining 20 pages get corrupted, an inserted checkpoint will account for the remaining 20 pages and resend them back.

The devices used in the session layer are:

NETBIOS – Network Basic Input Output System.

NSF – Network File System.

2.3.4 Layer 4 – Transport

The transport layer controls the reliability of communication through segmentation, flow control and error control. The data receive from the transport layer is divided into smaller data unit called segments. Each segment contain a source, destination port number and sequence number. The port number help to direct each segment to the correct application. Sequence number helps to reassemble segments in correct order to form correct message at the receiving device. Flow control the amount of data to be transmitted. Below are some of the functions of the transport layer.

i. Flow control: Like the data link layer, the transport layer is responsible for flow control of data from end-to-end rather than across a single link [5].

ii. Error Control: Error correction is through acknowledgements and retransmission.

It ensures reliable point to point delivery of data. Gateway routers, PCs and Firewalls are some of the network devices found in the transport layer. And the main transport layer protocols are the TCP – Transmission Control Protocol and UDP - User Datagram Protocol.

2.3.5 Layer 3 – Network

The network layer is responsible for the delivery of individual packets from one network to another. The network layer has routers as network devices that route IP packets across networks.

The network layer is responsible:

i. Logical Addressing: These are IP addresses assigned to network devices that allow the delivery of packet within and outside another network.

ii. Routing: shortest path determination for the delivery of packets take place here.

Devices user in the network layer are: Routers, Firewalls. Protocols used in the network layer are: IPV4, IPV6, Arp resolution Protocol (ARP), Internet Control Message Protocol (ICMP) etc.

2.3.6 Layer 2 – Data Link Layer

The data link layer is responsible for moving frames of data from one hop or node to the next.

The functions of data link layer are:

i. Flow control: It adds a header and trailer indicating the devices sending and receiving the data.

ii. Physical Addressing: Media Access Control (MAC). The physical address of the sending and receiving devices. These are unique addresses given to network devices.

The devices use in the data link layer are: Switches, bridges, Network Interface Cards (NICs) etc.

The protocols used in the data link layer are; Ethernet (IEEE 802.3), Token Ring etc.

MAC addresses is a six octet written in hexadecimal physical address assigned to network adapters by manufactures that are unique to every device in the network.

MAC address is a hardware address embedded in the NIC card.

It is these MAC addresses that layer two switches use to find hosts on a network and send the data direct to other devices. The quality of the switch to remember MAC addresses make it robust over the hub.

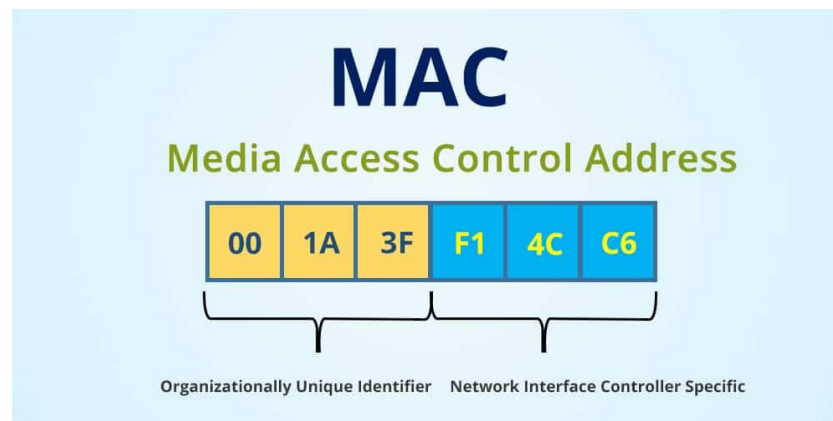


Figure 2.4: MAC Address

A MAC address may look like 00-1A-3F-F1-4C-C6. The uniqueness of MAC addresses is ensured by the Institute of Electrical and Electronics Engineers (IEEE), which assigns networking device vendors specific blocks of MAC addresses for the devices they produce.

The first 3 bytes (24 bits) represent the manufacturer of the card, and the last 3 bytes (24 bits) identify the particular card from that manufacturer.

To know the MAC address of your PC, open your *command prompt* and type “*ipconfig/all*” then press enter [10]. The row indicated by “*Physical Address*” is your MAC address number.

2.3.7 Layer 1 – Physical

The physical layer is responsible for moving individual bits from one host to another. The physical layer converts binary bits and transmit them over the media.

The media can be an electrical signal; the medium in which the converted bits passed is a copper wire, optical signal for optical fiber and radio signal in the case of air as a medium respectively [6].

Devices in the physical layer are: hubs, Cables, Straight Through, Cross Over, Computers etc. The protocols of the Physical Layer are: Bluetooth, DSL, IEEE 802.3 etc.

2.4 Network Devices

These are physical hardware that have software embedded in that facilitate the network connectivity and resources sharing. These devices form the network architecture and topology.

2.4.1 Network Switch

A switch is an intelligent layer two network device that has many collision and one broadcast domains.

Many collision domain means that every port on the switch can communicate to any other port without collision and broadcast domain means that any broadcast from one interface or port will be send to all the other interfaces. A switch is a central connecting device for nodes in the network. A switch remembers MAC addresses and send the data from the sending node to the intended destination of the receiving node.



Figure 2.5: CISCO Switch

2.4.2 Routers

A router connects networks together. In other words if one network wants to establish a connection to a remote network the router is responsible to link them together as it uses routing system to point to point links to route IP packets. Routers operate at the network level of the OSI Model.

For home networks the router is responsible to connect the home network to the Internet and provide several network services such as DHCP, DNS. Routers also provide both Wi-Fi and Ethernet connections.



Figure 2.6: CISCO Network Router and MODEM Router

2.4.3 Wireless Access Point (WAP)

A WAP connect wireless devices to an Ethernet network to access the Internet.



Figure 2.7: Wireless Access Point

2.5 Network Topologies

Network topology is the way a network is arranged, including the physical and logical description of how links and nodes are set up and relate to each other. Choosing the right topology for your company's operational model can increase performance while making it easier to locate faults and troubleshoot errors. There are several different types of network topologies and all are suitable for different purposes, depending on the overall network size and organisation's aims and objectives.

2.5. 1 Bus Topology

A bus topology orients all the devices on a network along a single cable running in a single direction from one end of the network to the other—which is why it is sometimes called a “line topology” or “backbone topology.” Data flow on the network also follows the route of the cable, moving in one direction. The figure below shows a bus topology.

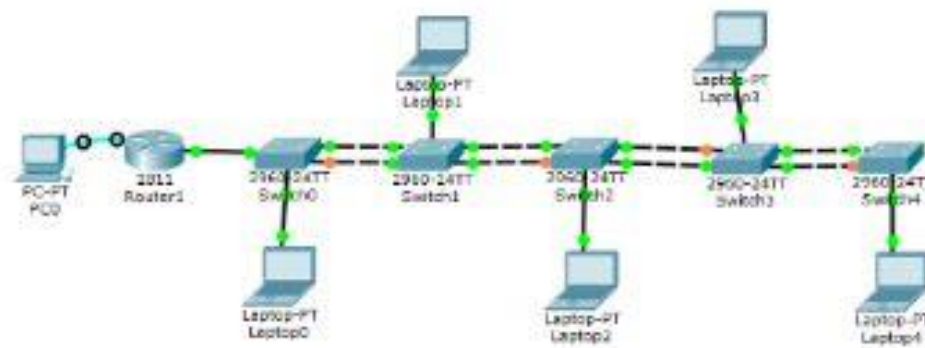


Figure 2.8: Bus Topology

A greater advantage of the bus topologies are, cost-effective choice for smaller networks because the layout is simple, allowing all devices to be connected via a single coaxial or RJ45 cable.

The disadvantage of the bus topology is that if the cable experiences a failure, the whole network goes down, which can be time-consuming and expensive to restore.

2.5.2 Star Topology

A star topology, the most common network topology set out so that every node in the network is directly connected to one central switch via coaxial, twisted-pair, or fiber-optic cable.

This central node manages data transmission as information sent from any node on the network has to pass through it to reach its destination.

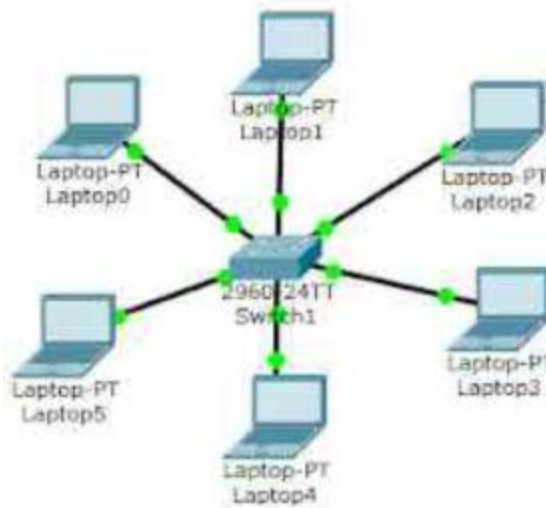


Figure 2.9: Star Topology

Because each of the nodes is independently connected to the central switch, if one cabling connection goes down, the rest of the network will continue functioning unaffected, making the star topology a stable and secure network topology.

On the other hand, if the central switch goes down, the rest of the network cannot function. But if the central switch is properly managed and kept in good working condition the mean time to repair will take longer and availability of the device will always present.

2.5.3 Ring Topology

Ring topology is where nodes are arranged in a circular or ring layout. The data can travel through the ring network in either one direction or both directions, with each central device having at least two neighbours.

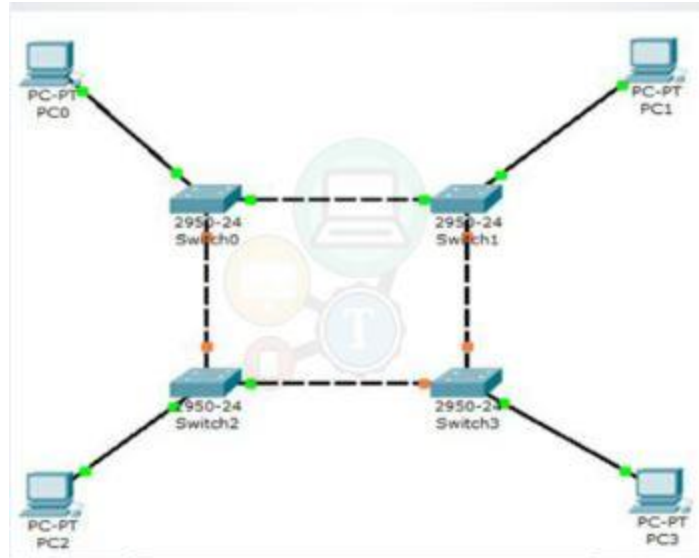


Figure 2.10: Ring Topology

Since each device is only connected to one node on either side when data is transmitted, the packets also travel along the circle, moving through each of the intermediate nodes until they arrive at their destinations.

Even though it is popular, a ring topology is still vulnerable to failure without proper network management. Since the flow of data transmission moves unidirectional between nodes along each ring, if one node goes down, it can break the path that receive data from that link and the data will cease to flow.

2.5.4 Mesh Topology

A mesh topology is an intricate and elaborate structure of point-to-point connections where all the central nodes are interconnected to one another.

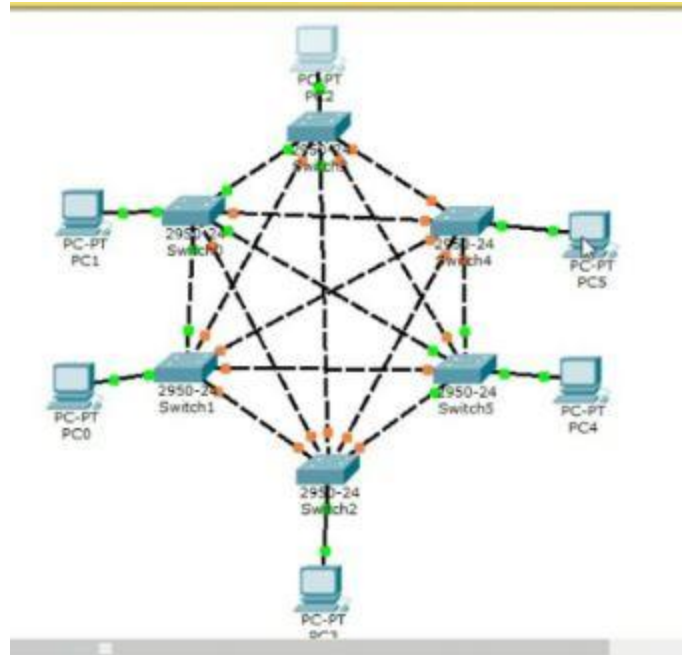


Figure 2.11: Mesh Topology

Mesh topologies are reliable and stable, and the complex degree of interconnectivity between nodes makes the network resistant to failure. For instance, no single device going down can bring the network offline.

Mesh topologies are incredibly labour-intensive. Each interconnection between nodes requires a cable and configuration once deployed, so it can also be time consuming to set up.

2.6 Network Types

Depending on the requirements and coverage of the geographical areas one could choose the network type design that will suit the organization setup. There are many types of networks existing in today's computer connectivity.

2.6.1 LAN (Local Area Network)

- Local Area Network is a group of network devices connected to each other in a small area such as building, office or a campus.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable etc.
- It is less costly as it is built with inexpensive hardware such as PCs, hubs, switches, network adapters, and Ethernet cables etc.
- The data is transferred at an extremely faster rate in Local Area Networks.

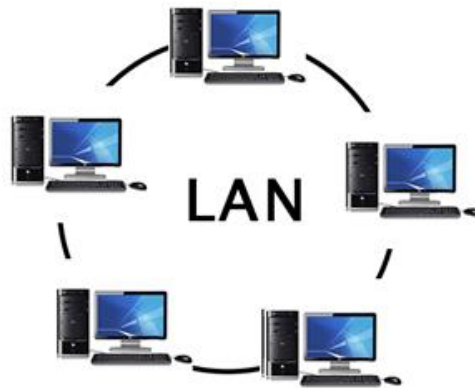


Figure 2.12: LAN Setup Network

2.6.2 MAN (Metropolitan Area Network)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting different LANs to form MAN.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line or other links.

- It covers a higher range than LAN.

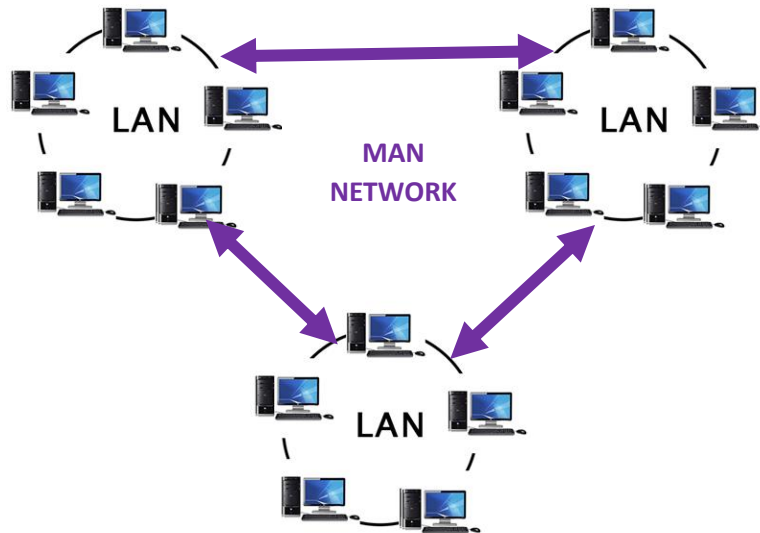


Figure 2.13: MAN Network

2.6.3 WAN (Wide Area Network)

- A Wide Area Network is a network that extends over a large geographical area such as states, countries or the globe. A Wide Area Network is quite bigger network than the MAN network.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fiber optic cable or satellite links.
- The Internet the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government education etc.

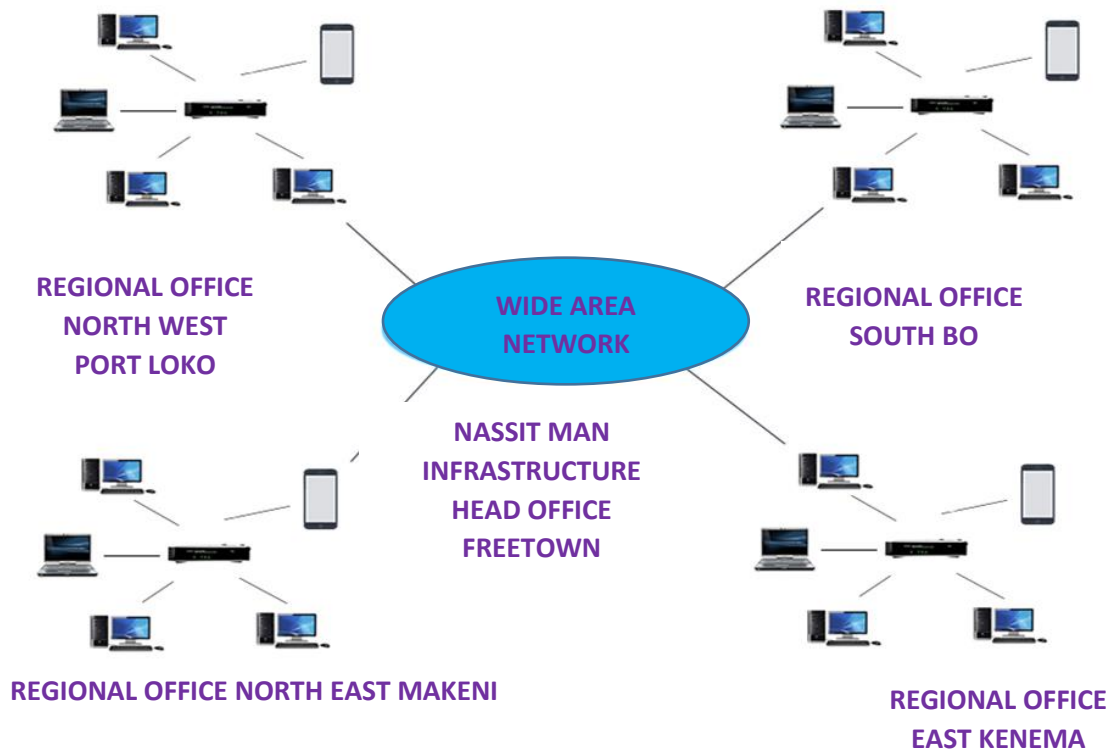


Figure 2.14: WAN Network Type

2.6.4 PAN (Personal Area Network)

- Personal Area Network is a network arranged by an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting computers and other peripheral devices such as devices connected to computer.
- Devices in PAN are PCs, laptop, mobile phones, smart phones, media player and play stations.



Figure 2.15: PAN Network

2.7 Optical Fiber Communication

An optical fiber can be understood as a dielectric waveguide glass tube, which operates at optical frequencies. The device or a tube, if bent or if terminated to radiate energy, is called a waveguide. This glass tube has a diameter 0.25 to 0.5 mm and carry light pulse signals up to a distance over several kilometers without signal loss as compared to copper cable.



Figure 2.16: Optical Glass Fiber

2.7.1 Physical Structure of an Optical Fiber

The most commonly used optical fiber is single solid di-electric cylinder of radius and index of refraction n_1 . The following figure explains the parts of an optical fiber [9].

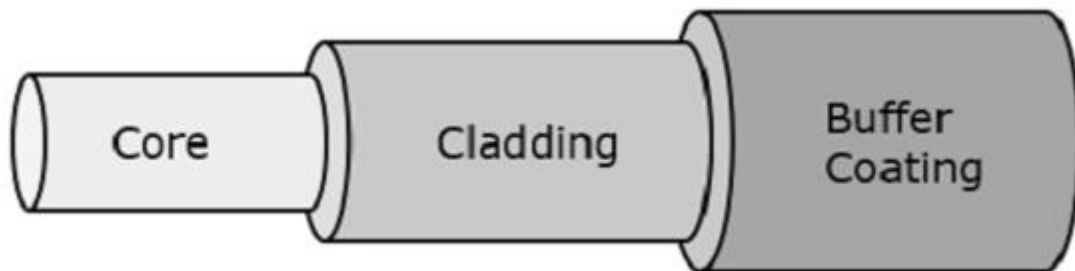


Figure 2.17: Physical Structure of Optical Fiber

This cylinder is known as the Core of the fiber. A solid di-electric material surrounds the core, which is called as Cladding. Cladding has a refractive index n_2 which is less than n_1 . The core is usually made of glass plastic. The core is the light-carrying portion of the fiber.

The cladding surrounds the core. The cladding is made of a material with a slightly lower index of refraction than the core.

Buffer; the outer layer which serves as a shock absorber to protect the core and cladding from damage. The coating usually comprises one or more coats of a plastic material to protect the fiber from the physical environment.

2.7.2 Types of Optical Fibers

Depending upon the material composition of the core, there are two types of fibers used commonly. They are :

- **Step-Index Fiber:** The refractive index of the core is uniform throughout and undergoes an abrupt change or step at the cladding boundary.
- **Graded-Index Fiber:** The core refractive index is made to vary as a function of the radial distance from the center of the fiber. Both of these are further divided into:
- **Multi-Mode Fiber:** These are excited with LEDs (Light Emitting Diodes) and travel several kilometers without signal distortion.
- **Single-Mode Fiber:** These are excited with laser lights and travel several kilometers more than multi-mode fiber with greater speed.

2.7.3 Fiber Splicing

An interesting aspect of fiber communication is the *splicing or joining methodology*. Fiber splicing is the act of joining two optical fibers end-to-end.

The goal is to fuse the two fibers together in such a way that light passing through the fibers is not scattered or reflected back by the splice, so that the splice and the region surrounding it are almost as strong as the intact fiber. A splicing machine is used in fiber splicing and when joining two pieces of fiber glasses together, the misalignment losses should not be greater than 0.02 decibel (i.e. 0.02db). Below is a photo of the researcher splicing multimode optical fiber, using a splicing machine.



Figure 2.18: A Photo of Splicing Optical Fiber

✓ **Advantages of using Optical Fiber**

- The transmission bandwidth of the fiber optic cables is higher than the copper cables.
- The amount of data transmission is higher in fiber optic cables.
- The power loss is very low and hence helpful in long-distance transmissions.
- Fiber optic cables are immune to electromagnetic interference.
- These are not affected by electrical noise.
- The space occupied by these cables is much less.

✓ **Disadvantages of using Optical Fiber**

Although fiber optics offer many advantages, they have the following drawbacks.

- Though fiber optic cables last longer, the installation cost is high.
- They are fragile if not enclosed in a plastic sheath. Hence, more protection is needed than copper ones.

Applications of Fiber Optics

- Used in telephone systems.

- Used in sub-marine cable networks.
- Used in data link for computer networks.
- Used in CCTV surveillance IP cameras that require longer length cabling where copper cable will not be suitable.

2.8 Internet Protocol

An IP address is a 32 bits numeric number assigned to a host on an IP network [11]. It is a software address that designates the specific location of a device on the network. IP address has a mask called subnet mask. This subnet mask is sub divided into network and host IDs. Example of IP address in dotted decimal is 192.168.1.10 255.255.255.0.

An IP address consist of two parts, one is Network ID and other is Host ID. Network ID should be the same for all the PCs in a network segment and Host ID should be unique for each PC. If two PCs are having different network IDs then they will not be able to communicate with each other directly. So network ID should be the same for all the PC's in the same segment.

2.8.1 Versions of IP Addresses

There are two versions of IP addresses that currently coexist in the global Internet: IP version 4 (IPv4) and IP version 6 (IPv6).

IPv4 addresses are 32 bits long, and IPv6 addresses 128 bits long. However, because of the growth of the Internet and the depletion of available IPv4 address, a new version of IP (IPv6), using 128 bits for the IP address, was standardised in 1988 [12].

2.8.2 Classes of IPV4 Addresses

TCP/IP defines five classes of IPV4 addresses: classes A, B, C, D, and E. Each class has a range of valid IP addresses. The value of the first octet determines the class.

IP addresses from the first three classes (A, B and C) can be used for host addresses. The other two classes are used for other purposes.

The system of IP address classes was developed for the purpose of Internet IP addresses assignment. The classes created were based on the network size. For example, for small number of networks with a very large number of hosts, the Class A was created. The Class C was created for numerous networks with small number of hosts. The figure below shows classes A to C IP addresses with Network bits ID (NID) and Host bits ID (HID).

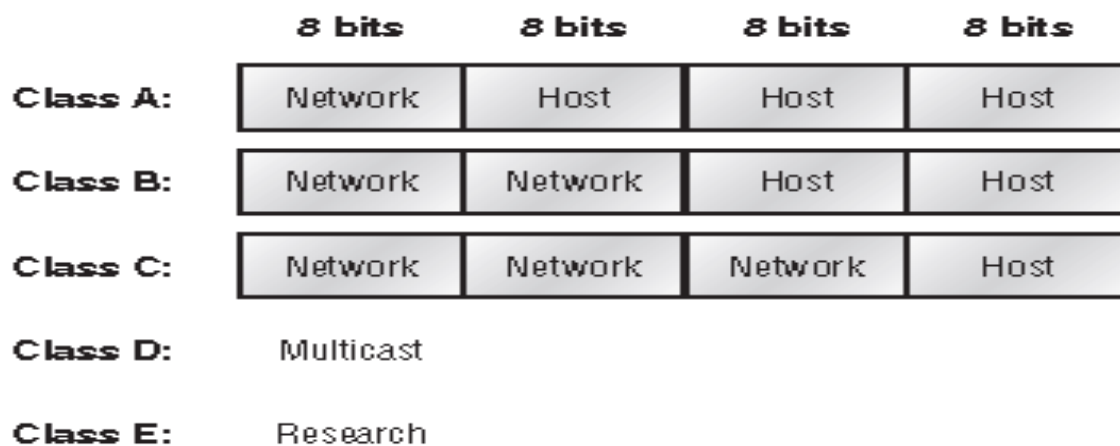


Figure 2.19: Host and Network Bit IDs IPV4 Classes

IP Class	Network ID	Class Range	Number of Network on each Host	Host ID	Number of Hosts on each Network	Subnet Mask
Class A	N	1-126	$2^7 - 2 = 126$ Networks	H.H.H	$2^{24} - 2 \approx 16.8$ Million Hosts	255.0.0.0/8
Class B	N.N	128 - 191	$2^{14} - 2 = 16,000$ Networks	H.H	$2^{16} - 2$ 65,000 Hosts	255.255.0.0
Class C	N.N.N	192 - 223	$2^{21} - 2 \approx 2.1$ Million Hosts	H	$2^8 - 2 = 254$ Hosts	255.255.255.0

Table 2.2: Class-full IP Addresses

Class D is used for Multicast (224-239)

Class E is used for Research (240-255)

2.8.3 Some examples of classes A to C IP Addresses in Decimal Notation

Class A – 10.10.2.1

Class B – 172.16.60.10

Class C – 192.168.100.2.1

In dotted binary notation we could easily recognise these classes if a classes starts with either;

Class A **0**0000000 = 0 to 01111111 = 127

Class B **1**0000000 = 128 to **1**0111111 = 191

Class C **11**000000 = 192 to **11**011111 = 223

A close look at the above IP addresses binary formats showed that a Class A IP address start with the first bit being **0**, Class B IP address is identified by looking at the first binary bit to be a **1** and a Class C IP address has the first two binary bits to **11** respectively.

2.8.4 Types of IP Addresses

If every host on every network has to have real routable IP address, we would have run out of IP addresses. By using private IP addresses network institutions, ISPs and home users will always have IP addresses for their network devices. This is economical because they can use private IP addresses on their inside networks and get along it. There are two types of IP addresses.

- **Private IP Addresses**

These are IP addresses that can be used on private networks, but they are not routable through the Internet. They are only available for home or office networks.

The allowable private IP range that reside in any private network; 10.0.0.0/8 to 10.255.255.255 for Class A, 172.16.0.0/16 to 172.31.255.255 for Class B and 192.168.0.0/24 to 192.168.255.255 respectively. These are just fine to route within private networks. If these ranges are to move across the Internet to reach other networks they have to use public IP addresses given by Internet Service Providers ISPs.

Public IP Addresses

These are IP addresses that are routable on the Internet. A public IP address is sometimes called an Internet IP. The ISP could readily give any available public IP addresses for sale to private network clients. Those that are not mentioned in the classes A, B and C range IP addresses are public IP addresses allow to be routable throughout the Internet.

1.0.0.0/8 to 8.8.8.0, 172.32.0.0/16 and 192.0.3/24 are some examples of public IP addresses ranges that the ISPs can offer for sale.

Public IP addresses are unique to every network and cannot be duplicated.

However public IP addresses are addresses that we can give to DNS server or host name that host the websites, point to point devices etc. DNS servers sometimes have private IP addresses but have to be translated into public before route to the Internet by a network address translation (NAT) or IPsec VPN routers. Examples of public IP addresses are: 172.217.22.14, 8.8.8.0, 1.1.1.0, 160.19.155.11, 47.144.221.167 etc.

2.8.5 Types of Address

- **Unicast** - When a packet is sent to a single host e.g. host 10.0.0.1 is sending a packet to 10.0.0.2
- **Multicast** - When a packet is sent to group of host using a multicast IP address. E.g. Host 10.0.0.1 is sending a packet to 224.0.0.5
- **Broadcast** - When a Packet is sent to all hosts in the network.

2.8.6 Loopback IP Addresses

A special IP address that a machine uses to communicate to itself. This can have implications for security and bandwidth usage as you typically want to avoid using the Internet to communicate to local software and devices. The IP addresses 127.0.0.1 to 127.255.255.255 are reserved for loopback. It is a common convention to use 127.0.0.1 and a host known as "localhost." Services that are local to a host typically bind to this IP on different ports [13].

CHAPTER THREE

3.1 Methodology

The design of any reliable network has to be viewed at both physical and logical levels. The physical level involves the network cabling, fiber glass cables, network hardware devices such as network racks, cabinets, patch panels, jack pinout etc. The physical level is the first stage in the network design after the research and network planning. When this stage is completed troubleshooting is carried out with the use of troubleshoot testers – network wire testers to test for continuity. The second stage involves IP address planning in which some classful IP addresses are subnetted to classless IP addresses which produce various subnetworks and hosts to economically manage the IP addresses.

A number of feasibility studies are carried out to know exactly how to setup the network design efficiently. The feasibility studies involved was:

- A visit to the NASSIT offices to know how the VLANs are setup. This was the information that helps the researcher to properly give appropriate VLAN names to network devices based on their functionalities.
- The researcher also did some point-to-point site draft by using Google Map to link all the possible routing locations which the actual design will use to route network resources.

3. 2 Physical Network Setup and Hardware Device Installations

Network devices and cables are used to run a physical network setup. The choice of these devices depends on the client's budget for the design.

But also it should not be minimised to the point that he did not choose substandard materials because this could reduce the network performance and hence the credibility of the designer. And hence the tradeoff should be chosen such that ample optimisation is done to get the design done in the most professional manner.

3.2.1 Network Faceplate and Jack Pinout

The purpose of the network faceplate is to receive a well wired jack pinout being mounted on the wall. It is from this faceplate and jack pinout that end host devices like PCs connect their RJ45 patch cables to get access to the company's network resources as shown below.



Figure 3.1: Network Faceplate and Jack Pinout

3.2.2 Running Network Cablings

A complete network setup has cablings running from end host devices to the network cabinet which houses the patch panels and switches connected together by ports numbering sequence in one building – floor section. Uplink or trunk cables are run from one floor to the other to ensure continuity from one cabinet to the next.

Cables are also run from the switches inside the cabinet to the data center where big network racks are situated. The purpose of the network racks is to house all the network devices such as servers, VLAN switches, gateways (routers), Firewalls etc.

3.2.3 Category 6 Cable (Cat 6)

An STP – Shielded Twisted Pair is a robust network cable for running physical cabling connections. This cable connect end host devices from a wall plate (faceplate) to the patch panel mounted in the cabinet. No matter the distance from the end host to the cabinet, this cable has to be run at length distance not greater than 100 meters to avoid signal losses due to distortion.

One end of this cable is punched to the jack pinout, screw to the faceplate, fix firmly into the wall and the other end is punched to the patch panel with the right category colour conventions.



Figure 3.2: Punching STP Cat6 Cables to the Patch Panel

3.2.4 The Role of the Data Center

Data centers are confined racks of network devices that house institutions network resources. With data center, network devices such as server racks , fiber patches, VLAN switches, core routers etc. that have all major configurations are installed.

The place or office has all the security measures in place because if breakdown or failure occur to these devices the entire network will shut down from the head office to its connected branch offices.

No unauthorised person is allowed in server control rooms. For this reason it is always equipped with full air conditioning to maintain the devices' normal working temperature. The figure below gives photos of the NASSIT data center control room in its initial installation.

Data centers are an integral part of the enterprise, designed to support business applications and provide services such as:

- Big data, machine learning and artificial intelligence.
- Data storage, management, backup and recovery.
- Host an organisation's databases and websites, email, files etc.



Figure 3.3: Data Center containing Network Racks

3.3 Network Hardware Devices Installations

So far the discussion of physical network setup, it can be concluded that the cabling and network device connections have physical architecture ranging from host end user clients, wall plates, cabinets to the data center as shown in Figure 3.4.

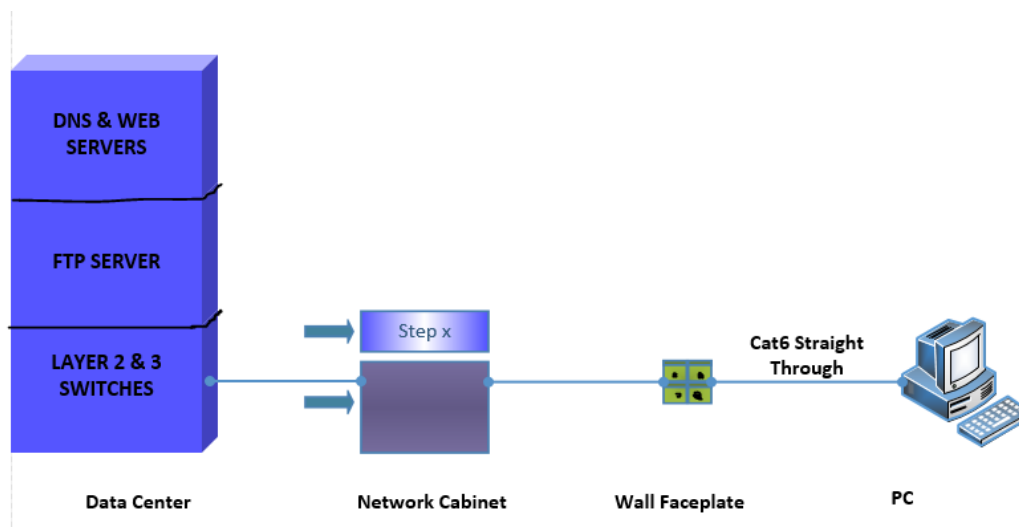


Figure 3.4: Network Installation Devices

3.4 Logical Network Setup

A logical network diagram usually show network devices like routers (gateways), firewalls etc. with logically assigned IP addresses to the devices. At the logical stage, network devices can now communicate effectively based on the configured protocols. A network setup like this is seen to have all the logical protocols and information in it based on the layer in which the network device resides. A logical network shows subnets, VLAN policies, IP addresses, routing information protocols (RIPs) in it.

3.4.1 IP Address Subnetting

The literature review had shown the usefulness of the IPV4 address as a classful address. As networking devices continue to grow rapidly over the years due to increase in Internet Technology, the assigning of IPs from IPV4 to network devices is now becoming obsolete.

IPV4 has octet networks (**N**) and host bits (**H**) designs structure of **N.H.H.H**, **N.N.H.H** and **N.N.N.H** for classes A, B and C respectively. If by default 2 is raised to the power of any of these octets one will obtain the number of networks and host bits formed for each of these classes. The table below demonstrates this process:

IP Class	Network & Host Portions	Total Number of Networks ($2^{x-\text{octets}}$)	Total Number of Hosts ($2^{y-\text{octets}}$)	Dotted Decimal Notation
Class A	N.H.H.H	$2^7-2 = 126$	$2^{24}-2$ 16.7 million	255.0.0.0
Class B	N.N.H.H	2^{14} 16,000	$2^{16}-2$ 65,000	255.255.0.0
Class C	N.N.N.H	221 2.1 million	$2^8-2 = 252$	255.255.255.0

1 Table 3.1: Usable IPV4 Classful Range

From Table 3.1, we can see the classful IP addresses of A, B and C with network and host portions in dotted decimal notations.

- **Classless Inter Domain Routing (CIDR)**

“CIDR allows a block of IP address to be further collapsed into multiple adjacent IP addresses onto one network prefix and share one network IP address among multiple physical networks.

By manipulating the zero host bits a single IP address can be obtained from either classes A, B or C by splitting it into several subnetworks and hosts. This phenomenon is called “IP Address Subnetting.”

The IP address sub-netted could produce much larger subnetworks and hosts if a class of more host is chosen. The choice of an IP address class to be sub-netted is greatly depend on how small or large the network setup will be. In this case, choosing a class A will be of preference to either B or C for a larger network IP address planning.

From theory, we can now choose two sizable subnet IP addresses and use them throughout the life time of project. Suitable choices are classes B and A.

Default IP	Default Subnet Mask	First Subnet	Second Subnet	Third Subnet	Fourth Subnet	New Subnet Mask
172.17.0.0/16	255.255.0.0	172.17.4.0	172.17.8.0	172.17.12.0	172.17.16.0	255.255.252.0
172.17.0.0/16	255.255.0.0	172.17.2.0	172.17.6.0	172.17.10.0	172.17.14.0	255.255.255.0
10.0.0.0/8	255.0.0.0	10.1.1.0	10.1.4.0	10.1.8.0	10.1.12.0	255.255.255.252
10.0.0.0/8	255.0.0.0	10.1.16.0	10.1.20.0	10.1.24.0	10.1.28.0	255.255.255.252

Table 3.2: VLANs Subnetting

The concept of how table 3.2 subnetworks is obtain will be explain here. The project targeted four subnetworks: NASSIT Head Office Freetown, Regional Offices North (Makeni), East (Kenema) and South (Bo) respectively. Four Class B subnetworks are sufficient, but for future growth of these office networks we specifically design and reserve more than the required subnetworks.

The binary notation of the above table class B IP address for **VLAN 20 DATA** subnet indicated by the blue borrowed six host bits in the subnet mask column below.

Network	Subnet Mask in Decimal	Subnet Mask In Binary
172.17.0.0	255.255.0.0	11111111.11111111.00000000.00000000

Table 3.3 a: Borrowing Six Host Bits from the Subnet Mask

From Table 3.3a, six host bits (zero bits) are borrowed, changed them to ones and used them for the subnet resulting in $2^6 = 64$ -subnetworks. The new subnet mask for the IP in both binary and decimal notation will now look like:

Network	Subnet Mask in Decimal	Subnet Mask in Binary
172.17.0.0	255.255.252.0	11111111.11111111.11111100.00000000

Table 3.3 b: New Subnet Mask Form

The blocks of each subnet is obtained by taking the difference between 256 and the octet subnet mask that receives the binary borrowed bits i.e. **252** and then $256 - 252 = 4$ -ranges. In general, if the subnet IP address block is x, the next block is $(x + 4)$. Therefore each subnet block will differ by a range of 4. The table below gives each of the IP Subnet blocks.

Subnet Block No.(n)	IP Address (x + 4)	Subnet Mask
1	172.17. 0.0/22	255.255.252.0
2	172.17. 4.0/22	255.255.252.0
3	172.17. 8.0/22	255.255.252.0
4	172.17. 12.0/22	255.255.252.0
n +
64	172.17. 252.0/22	255.255.252.0

Table 3.4: Subnet Blocks of VLAN 20 DATA Networks

The steps and methods above are the subnet procedures for VLAN 20 DATA IP address blocks. In a similar manner the other remaining subnet block VLANs; VOICE, SERVER and Point 2 Point IP block (P2) are obtain by following the same procedures.

3.5 Feasibility Studies

In order to actually visualise and pinpoint the locations of the selected NASSIT offices project design, its appropriate map points had been tracked using Google Map. Below is a Google Map survey showing the point-to-point locations of the routing views which the logical output network design will take. The wireless access point icons are the sites that clearly specify the actual locations where the reference offices design are situated.

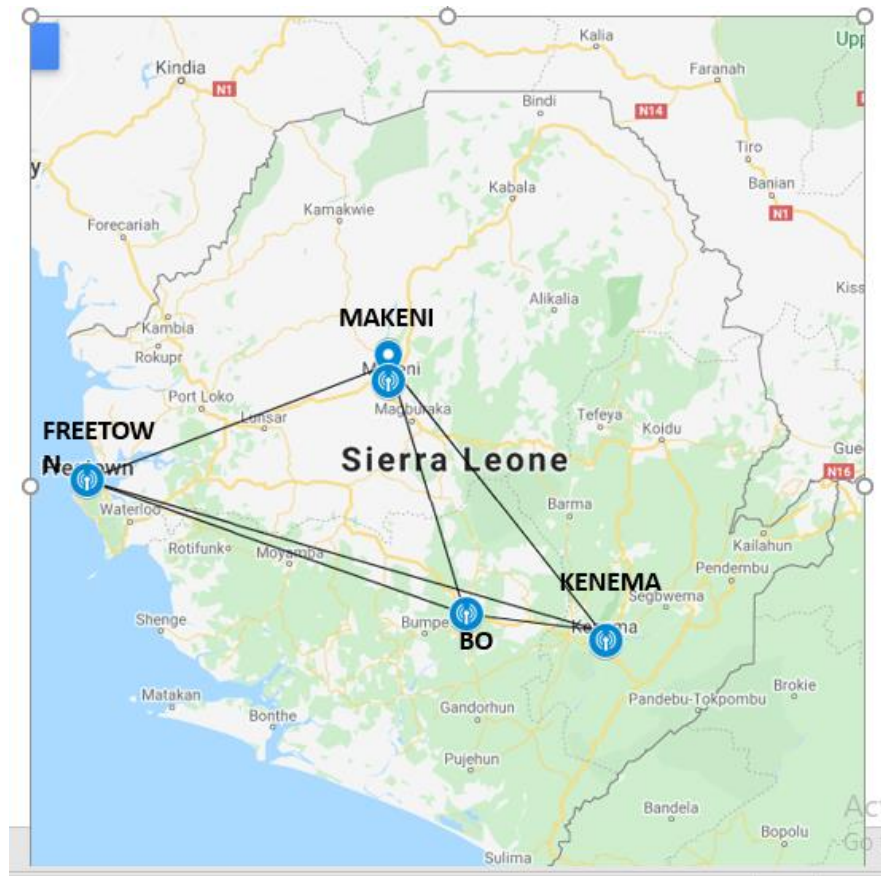


Figure 3.5: A Display of Point to Point NASSIT Offices Routing across the Country

3. 4 Assigning VLANs

VLAN concept was discussed in the chapter on of the introductory but it does not give a clear concept of practical applications. A network switch by default has one broadcast and multiple collision domains. If this happens it will reduce the intelligence and efficiency of telecommunication. A collection of network devices connected to a switch produces multiple collision domain in which each of the devices can receive a broadcast when a device is sending frames to another device.

VLAN is the grouping and breaking of a single broadcast domain of network devices logically. Switches with VLANs configuration will provide a reliable communication in which if a device ‘x’ is to send a frame to device ‘y’ the remaining devices connected to that switch will not recognise that a communication has taken place.

VLAN No	Name	Comments
10	VOICE	For telephony-services
20	DATA	To support data and file sharing
30	SERVER	For server management

Table 3.5: Assigning VLANs to Network Devices

Let us now allocate subnet block IP addresses to the VLANs that we shall use in the project design. The VLANs VOICE, DATA and SERVER that will receive the subnet IP blocks are given in the table below.

VLAN No.	Name	Subnet Block IP			
		Freetown	Makeni	Kenema	Bo
10	VOICE	172.17.2.0/24	172.17.6.0/24	172.17.10.0/24	172.17.14.0/24
20	DATA	172.17.4.0/22	172.17.8.0/22	172.17.12.0/22	172.17.16.0/22
30	SERVER	172.17.18.0/24	172.17.18.0/24	172.17.18.0/24	172.17.18.0/24

Table 3.6: Assigning Subnet IP Addresses to VLANs

3.5 Logical Network Hierarchical Model

The logical network hierarchical model is a network topology carrying configurations that help network designers provide a reliable, scalable and efficient running network.

A network design with these layers approach rules provides ease to troubleshoot when downtime or faults occur. The layers are describe below.

- **Access List Layer**

The Access layer consist of configured VLAN switches and other protocols that connect all end hosts devices. The architecture shown in Figure 3.7 shows how end host devices are connected to the switches to share resources.

- **Distribution Layer**

This layer is tied-down between the access layer and the core layer and the devices in it are mainly Firewalls or VPN routers that provide authorise access to end host devices. In the project design, the VPN routers take care of the unwanted packet filtering policy.

- **Core Layer**

The core layer constitutes of devices mainly gateway router devices that transfer traffic or route packets from one LAN to another. Fig 3.7 shows all the three hierarchical layers model.

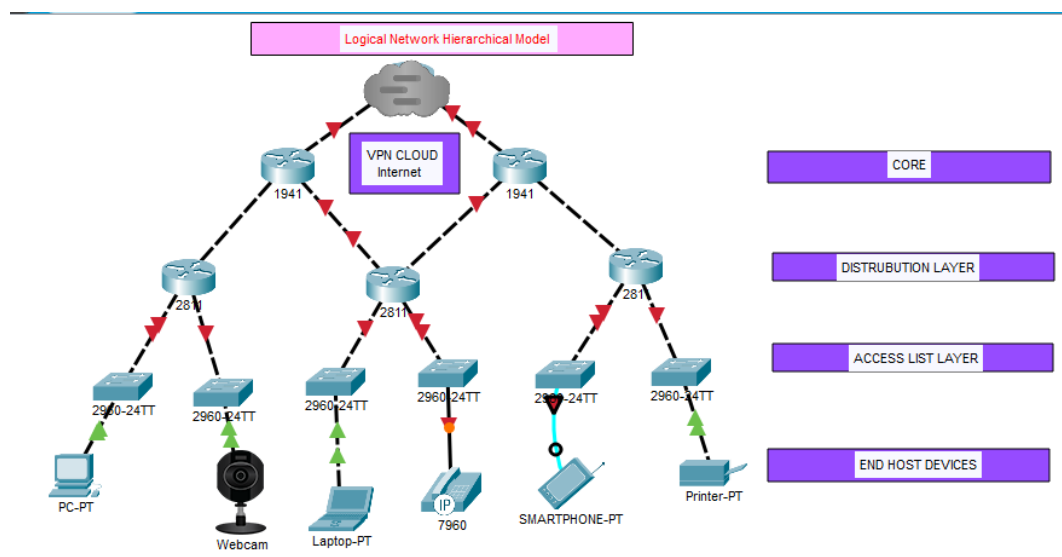


Fig 3.6: The Logical network Hierarchical model Architecture.

CHAPTER FOUR

4.1 NASSIT Network Design

So far the network design has gone through, the main services offered by the network design are data for files and other documents sharing, IP telephony service for voice, IoT to control IP Cameras and server management system. Below is a display of the coupling project design of the NASSIT network in a well simulated environment with Packet Tracer 7.2.1

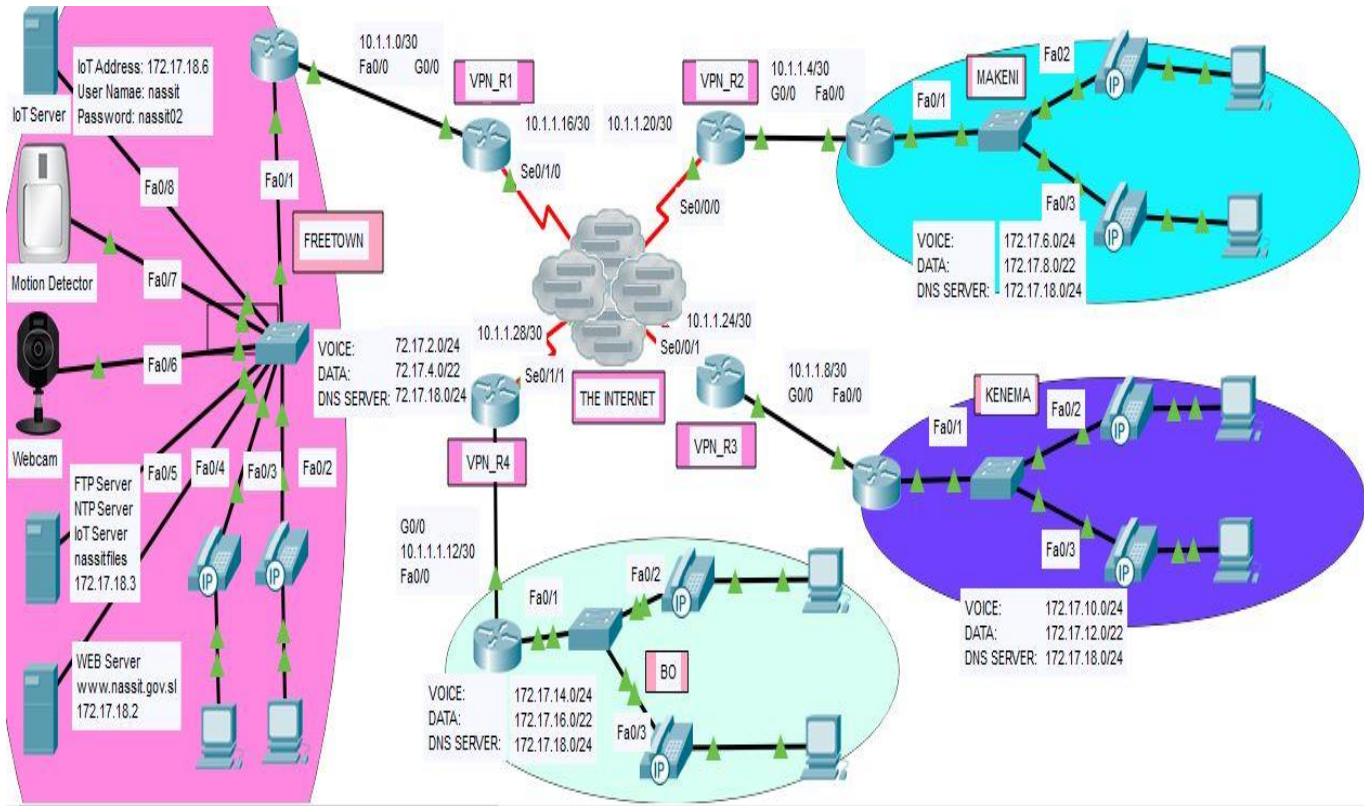


Figure 4.1: NASSIT Network Design Topology

4.1.1 Physical Network Architecture

The network office locations are connected through the Internet. The VPN tunnels are setup in the Internet through VPN routers to create path ways for encrypted data so that hackers could not spy the intelligence of communication across these networks. The figure below clearly shows how the physical network management setup would look like.

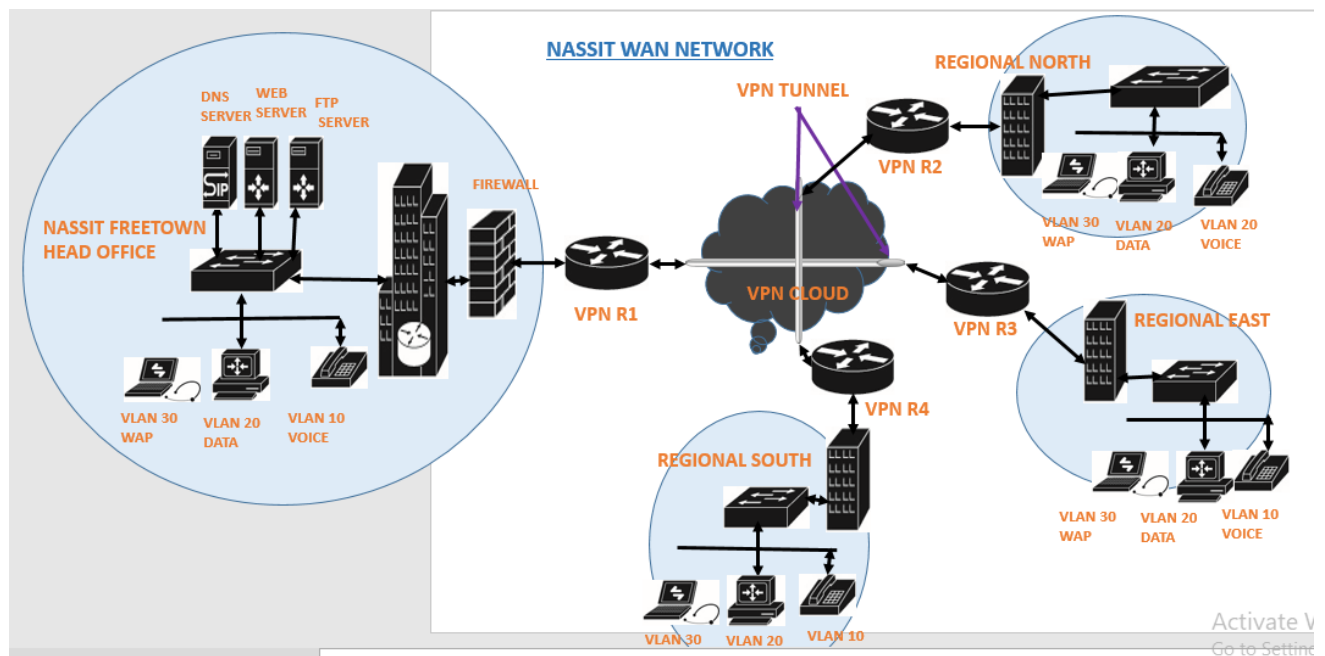


Figure 4.2: NASSIT Network Physical Design

4.1.2 Packet Tracer 7.2.1 Exploration

The CISCO Packet Tracer Network Simulator has its window display showing the tabs, ribbons, taskbar and the window working environment where you place the network devices. The figure below shows the main active used areas for the network designs and testing.

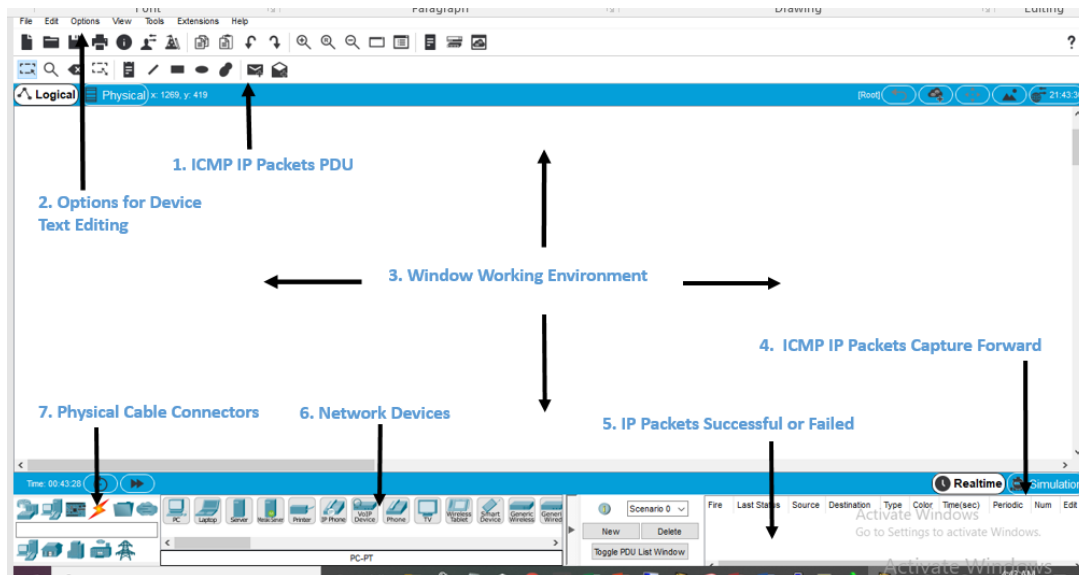


Figure 4.3: Packet Tracer 7.2.1 Working Environment

4.2 Renaming Network Devices

The naming of network devices is done with respect to the function of the individual device as well as the location of the office in which the devices are situated. Now that the devices have been placed in the packet trace working environment with all the connections with it, it is now time to rename them in the command line interface (CLI). A switch and router situated in the Freetown network will be renamed from “Switch” to “FREETOWN_NET”, the “Router” as “FREETOWN_GATEWAY” etc. This is done so that the major role and location of a device can be easily identify. The table below gives each of the device names. You cannot see these names physically, but you do see them when you open the device in the CLI interface. Select any device, open it in CLI and enter the necessary command to rename it. In the “*config mode*” type:

!

```
hostname FREETOWN_NET
```

!

You can now see the switch changes from its default name “Switch” to “FREETOWN_NET”. In a similar manner all the other devices are rename in the same way. Table 4.1 gives a summary of the renaming network devices.

Office	Device Name	Default	Rename in CLI	Comment
Freetown	Switch		FREETOWN_NET	Carrying Freetown Office VLANs
	Router		GATEWAY_FREETOWN	Contains Data and Voice configurations
	Router		VPN_R1	For VPN Configuration
North	Switch		NORTH_NET	Carrying North Office VLANs
	Router		GATEWAY_NORTH	Contains Data and Voice configurations
	Router		VPN_R2	For VPN Configuration
EAST	Switch		EAST_NET	Carrying East Office VLANs
	Router		GATEWAY_EAST	Contains Data and Voice configurations
	Router		VPN_R3	For VPN Configuration
South	Switch		SOUTH_NET	Carrying South Office VLANs
	Router		GATEWAY_SOUTH	Contains Data and Voice configurations
	Router		VPN_R4	For VPN Configuration
Internet	Router		ISP	For VPN Cloud Tunnels

Table 4.1: Devices Renaming in CLI

4.3 VLANs Configuration

We configure the VLANs in the switch to point to the Interfaces connected to end host devices and to show which group of devices belong to a particular VLAN.

Before we start the network device configurations let us enable each device with a secret password so that unauthorise person would not login into the hardware device to see the system configurations. We will use *nassit02* as an example enable secret password to every device.

These configuration steps are done for every VLAN switch in each of the network offices. The number of commands to achieve that in the *config mode* are explained below and *Appendix A1* has all the configuration commands for the VLANs.

- Name the VLAN Number: vlan 10 for VLAN 10
- Name the VLAN Name: VOICE for VoIP
- Give the interfaces in the switch to access that VLAN
- Now configure the switch VLAN interface that connected to the router as a trunk so as to terminate all the VLAN traffic as a default VLAN 1

4.3.1 Router on a Stick

The IEEE introduced the 802.1Q referred to as Dot1q standard that supports a router on a stick configuration to forward data, voice and other VLAN tags given to a switch trunk.

The router connected to this switch port carrying VLAN traffic should also know the existence of the VLANs in that switch by its trunk port. The router on a stick uses the inter VLAN routing to forward all the VLAN traffic within and outside the network. Its configuration is simple.

By having subnet IP addresses in mind for the VLAN networks, the router need to know only its VLAN interface, encapsulation and the IP address of its interface.

4.4 DHCP Configurations

A DHCP protocol allows a DHCP server to automatically assign IP addresses to end host devices. A very neat, efficient, robust and professional system that gives IP addresses to every device connected to the network when a DHCP, is configured and redirected to a particular network instead of manually configuring the individual devices.

The DHCP configuration is given in *Appendix B* and its configuration steps are explained below.

- The router already has an IP address with its interface connected to the switch. For this reason we exclude this IP address in the configuration. Also if the network management wants to reserve some DHCP IP addresses for later use it is important to exclude them now.
- Give the VLAN that will receive the DHCP Pool. That is the configuration takes the dhcp pool followed by the VLAN number and name.
- Give the network and the default router to reach that network. Option and the IP address of the router is also added if the dhcp pool is for voice to allow the IP phones to receive IP addresses from the DHCP router.
- Include the DNS server that will enable the end host devices to communicate directly to the HTTP server.

When all the above mentioned steps are achieved accurately each end host device receives a DHCP IP address when the DHCP button is enabled in the device desktop physical setup. Communication can now flow within a network. If you ping an ICMP message to any end host within the network reachability is achieved with a payload or a packet being sent and received within a network.

4.5 Routes and Routing Protocols

It is now time to send payloads to reach each of the networks around the WAN network design. The intelligence of the router with configured routing information protocols (RIPs) makes it possible to route IP packets within and outside the networks by learning the available networks and storing them in its routing table. It is a layer three protocol that forward IP packets from one network to another. It does this by advertising the networks connected to its interfaces. The figure below has three networks. The 172.17.4.0/22, the point 2 point link between R1 and R2 is 10.1.1.0/30 and 192.168.1.0/24. Router R1 only knows about its two connected networks to its interfaces. If either PC 1 or PC 2 wants to communicate with PC 3 the two routers R1 and R2 have to advertise the networks connected to their interfaces. This is achieved by using the Routing Information Protocols.

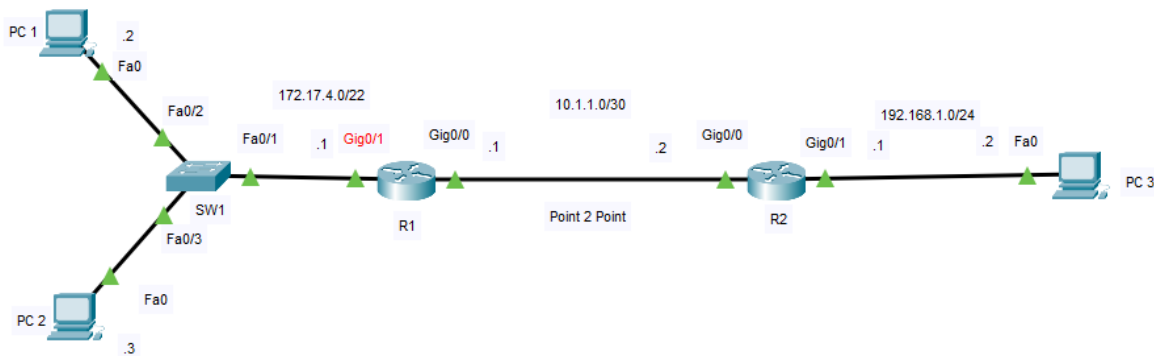


Figure 4.4: Routing Information Advertising Neighbouring Networks

4.5.1 Types of Routes

- **Static Route**

This type of route allows optimal path between all possible pairs of sources and destinations in the given networks to advertise.

The router uses a manually configured routing entry rather than information from dynamic routing traffic. The static route is directly configured on active interfaces of the router and being added to the routing table by a network administrator. An example of static route is RIP Version 1 (RIP V1).

Dynamic Route

In dynamic route the routing is not directly configured on the active interfaces of the router instead the router uses its intelligence and learns dynamic routes by running a routing protocol. RIP V2, open shortest path first (OSPF) and enhanced interior gateway routing protocol (EIGRP) are examples of dynamic routes.

4.5.2 Routing Information Protocol Version 2 (RIP V2)

The RIP V2 uses hop count to count the number of routes between the source and the destination networks. The RIP V2 supports both classful and classless routing and it sends subnet masks in the routing table. To configure RIP V2, you just need to go the CLI interface of the router and in the *config mode*, enter the RIP command followed by the version and the network you want to advertise. When this is done in each of the routers it is now possible to reach each of the hosts in the entire network. **Appendix E** gives all the commands used to configure RIP V2. RIP V2 uses routing table to show its connected networks and the metric distance of the hops count. RIP V2 belongs to the vector distance routing protocol which does the routing system by a rumor obtained by the neighbouring routers in which each router shares information about the routing they know and the metric cost to reach the targeted networks.

RIP is easy to configure, greatly support all router series as compared to EIGRP which supports only CISCO routers. RIP does not require update every time the topology of the network changes. However, RIP is only based on hop count to reach a designated host.

That means it does not choose a route of better bandwidth or speed but chooses the shortest path to reach the destination. But it is still much more preferable since it supports all router series.

All routers in this network design are configured with RIP Version 2 and therefore ICMP *ping* messages can now move across end host devices. The RIP routing table is shown below giving information about its connected networks when one router is taken as reference.

```
GATEWAY_FREETOWN#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/30 is subnetted, 8 subnets
C    10.1.1.0 is directly connected, FastEthernet0/0
R    10.1.1.4 [120/3] via 10.1.1.2, 00:00:02, FastEthernet0/0
R    10.1.1.8 [120/3] via 10.1.1.2, 00:00:02, FastEthernet0/0
R    10.1.1.12 [120/3] via 10.1.1.2, 00:00:02, FastEthernet0/0
R    10.1.1.16 [120/1] via 10.1.1.2, 00:00:02, FastEthernet0/0
R    10.1.1.20 [120/2] via 10.1.1.2, 00:00:02, FastEthernet0/0
R    10.1.1.24 [120/2] via 10.1.1.2, 00:00:02, FastEthernet0/0
R    10.1.1.28 [120/2] via 10.1.1.2, 00:00:02, FastEthernet0/0

172.17.0.0/16 is variably subnetted, 9 subnets, 2 masks
C    172.17.2.0/24 is directly connected, FastEthernet0/1.10
C    172.17.4.0/22 is directly connected, FastEthernet0/1.20
```

Figure 4.5: RIP V2 Routing Table

4.6 Testing for Reachability

ICMP Ping messages can now reach any host in the network when a payload is sent from one host device to the other irrespective of the individual host location across the networks. Let us now send packets by verifying the OSI Model and the Outbound PDU Details.

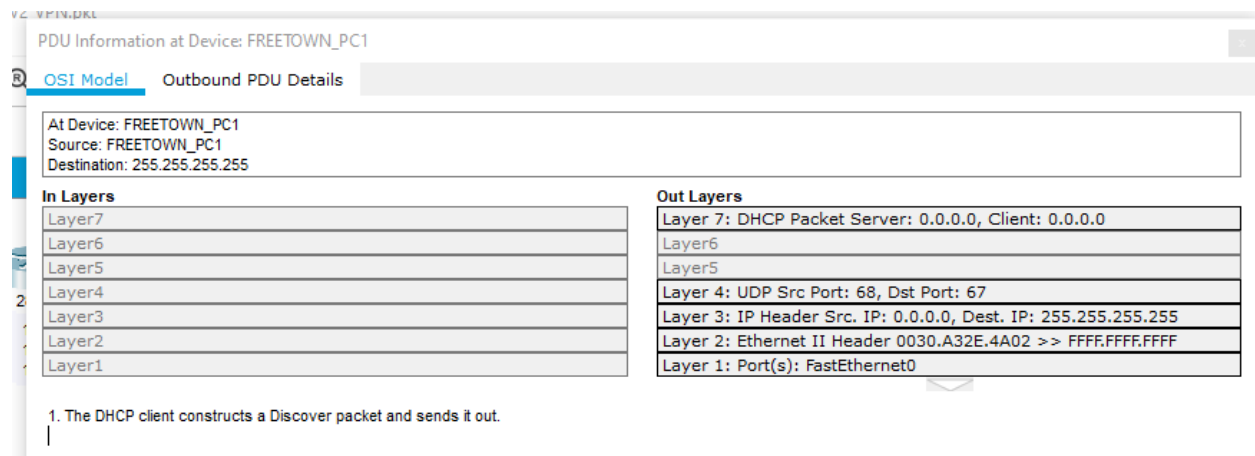


Figure 4.6: OSI Model Practical Detail

From the OSI Model shown in the figure above, layer 6 and layer 5 have no information about the payload while layer 7 has. The reason being that the OSI TCP/IP Model in details takes layer 5, 6 and 7 to be a one layer as the application layer. Layer 7 shows that the payload IP address is obtained from a DHCP. Layer 4 displays the UDP source destination ports of **68** and of **67**. Layer 3 gives the IP header of source and destination IP address of the sending and the receiving devices. Layer 2 is an Ethernet Header of the source and destination MAC addresses. Layer 1 displays the Ethernet port of the device interface of the PC respectively.

4.7 Call Manager Express (CME) for Voice over IP (VoIP)

VoIP is the transmission of voice from one IP phone located in one network to another IP phone within the same network or another network over the Internet.

Developed around 1995, originally it served as a work-around for long-distance and international telephone charges. VoIP telephony utilises Internet Protocol to make distance IP phone calls instead of using the mobile subscriber telephone lines.

This helps government and financial institutions to spend less on voice communication. Less than two decades old, VoIP has revolutionised communication all around the world.

4.7.1 VoIP Configuration

The first step of the VoIP configuration is to enter the telephony service in the global configuration mode of the CME or gateway router and clearly define the maximum number of IP phones that should be configured in the network. The IP phones will automatically obtain IP addresses from the DHCP server configured in the router previously.

The second step is to configure the MAC addresses of each phone followed by the series type of the phones (7960 Series IP Phones) and the dial number patterns such as 1001, 1002 etc. for the FREETOWN_NET network example system. A dial pattern of four digits minimum for the IP phone numbers. *Appendix F* has all the configurations for the IP telephony system.

When once the above configuration steps are establish, IP phone calls can now work within the network. But to enable an IP phone call from one network to another, a dial peer pattern must be set up to clearly define a session target IP address network and the destination pattern of the IP phone numbering to reach the phones in that network. We now try to make IP phone calls within and outside the networks.

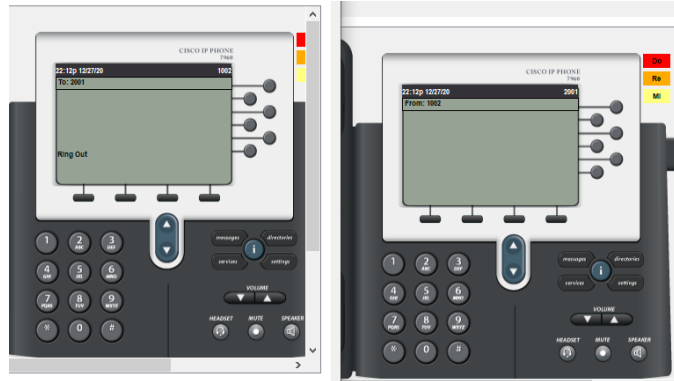


Figure 4.8: IP Phone Call between two Networks

The figure above shows two IP phones from NASSIT Freetown Headquarter Network to Northern Province Network. The IP phone with dial number **1002** made a call to IP phone with dial number **2001**. The call was successful. In a similar manner any phone can make a call within and outside the network respectively.

4.8 Server Administration Managements

The functions of the data centers as server systems was discussed in chapter three of the methodology. Server is the most important software applications that house any network resources that users can share. This project deals with a centralise system in which the head office has all the server resources that can be distributed to various sub offices. Here, the server resources that will be readily available are: web servers responding to HTTPS requests, FTP file server to share files between network device and NTP server to synchronise system clock for IP telephony service. For a network device to function as a server, the device must be configured to listen to requests from clients on a network connection. This functionality can exist as part of the operating system as an installed application.

4.8.1 Some Server Resources Administration

The project scope is to design a secure network where some server resources are provided as discussed below.

4.8.1 DNS Servers

Domain Name System (DNS) server is an application server that provides name resolution to client computers by converting names easily understood by end users into machine-readable IP addresses. When a client needs the address of a system. It sends a DNS request with the name of the desired resource to a DNS server. The DNS server responds with the necessary IP address from its table of DNS names.

In general, to access an HTTPS DNS server you either enter the IP address of the server or its domain name. For example Google domain name is www.google.com is the same as the IP address 8.8.8.8 to access the google website.

Therefore, having DNS names for your server management administration means all servers IP addresses will accept text as domain names which are easy to enter into the browser windows by end users. The DNS server that will enable you access NASSIT website for this project is www.nassit.gov.sl with IP address 192.168.1.1.

4.8.1.2 Web Servers

“One of the most abundant types of servers in today’s market is a web server. A web server is a special kind of application server that hosts programs and data requested by users across the Internet or an Intranet. Web servers respond to requests from browsers running on client computers for web pages, or other web-based services. Common web servers include Apache web servers, Microsoft Internet Information Services.”

In this project the web server is configured and each of the PCs has a DNS server IP address point to the corporate website. By opening any PC's browser and entering either the domain name or the DNS IP address you can access the NASSIT website. The result shown below gives detail information of the NASSIT website when the DNS domain name or IP address (www.nassit.gov.sl or 172.17.18.2) is entered into any of the PCs' browser.



Figure 4.9: A Display of the Corporate NASSIT Network Website

4.8.3 File Servers

File servers store and distribute files for multiple clients or users connected to it with a user account and authorisation levels. In this project, we provided an FTP user account with user name "*nassit*" and password "*nassit02*". These are the information you need to enter when you get access to the FTP domain name. File server hardware can be designed to maximise the read and write speeds performance of server devices. For a client to access a file from the file server remotely a client account must be provided in the file server.

The client account takes the username, password and authorisation levels giving restriction levels as right to access the files. The restriction is given by the acronym **RWDLN**.

- **R** is Read, an authorisation given to an FTP client to only read a file document from the FTP server.
- **W** is for Write, an authorisation level given to an FTP client to write and make changes to a file document from the FTP server.
- **D** for Delete, the right for an FTP client to delete a file document.
- **N** is to Re-Name and make update to given file document from the file server.
- **L** is for List, gives you the ability to list the file documents in any random order.

4.8.1.4 Network Time Protocol Server (NTP)

A network time protocol (NTP) server is used by network devices to synchronise their clocks over the Internet. If you ever have wrong date and time settings and notice that the date and time reset to a correct clock setting when your phone or PC is connected to the Internet, it is the NTP server that makes use of its system configuration to correct IP phones' date and time. We shall use the NTP server to correct the system clock for the IP phones' date and time. Enable the NTP clock to set the phones date and time.

4.9 VPN Configuration

We are at the event of making a live IPSec VPN configuration taking two VPN sites as example. We need to enable and install the security license in each of the two routers that will enable us to configure the VPN policies. Let us enable the security license in each of the VPN routers by entering the commands shown in **Appendix I**. The enable security license is shown below.

```

-----
Device#      PID                      SN
-----
*0           CISCO1941/K9                  FTX152489XU-

Technology Package License Information for Module:'cl900'

-----
Technology    Technology-package      Technology-package
              Current        Type                Next reboot
-----
ipbase        ipbasek9                Permanent          ipbasek9
security      securityk9              Evaluation         securityk9
data          disable                 None               None

Configuration register is 0x2102

```

Figure 4.10: Enabling Security License

A decision is made to the VPN routers for the incoming traffic. If the incoming traffic is an access list to an IPSec VPN then the payload IP headers and the data are encrypted and forward to the next IPSec VPN router or else entered in plain text to the destination network. The flow chart below will make this point clearly understood.

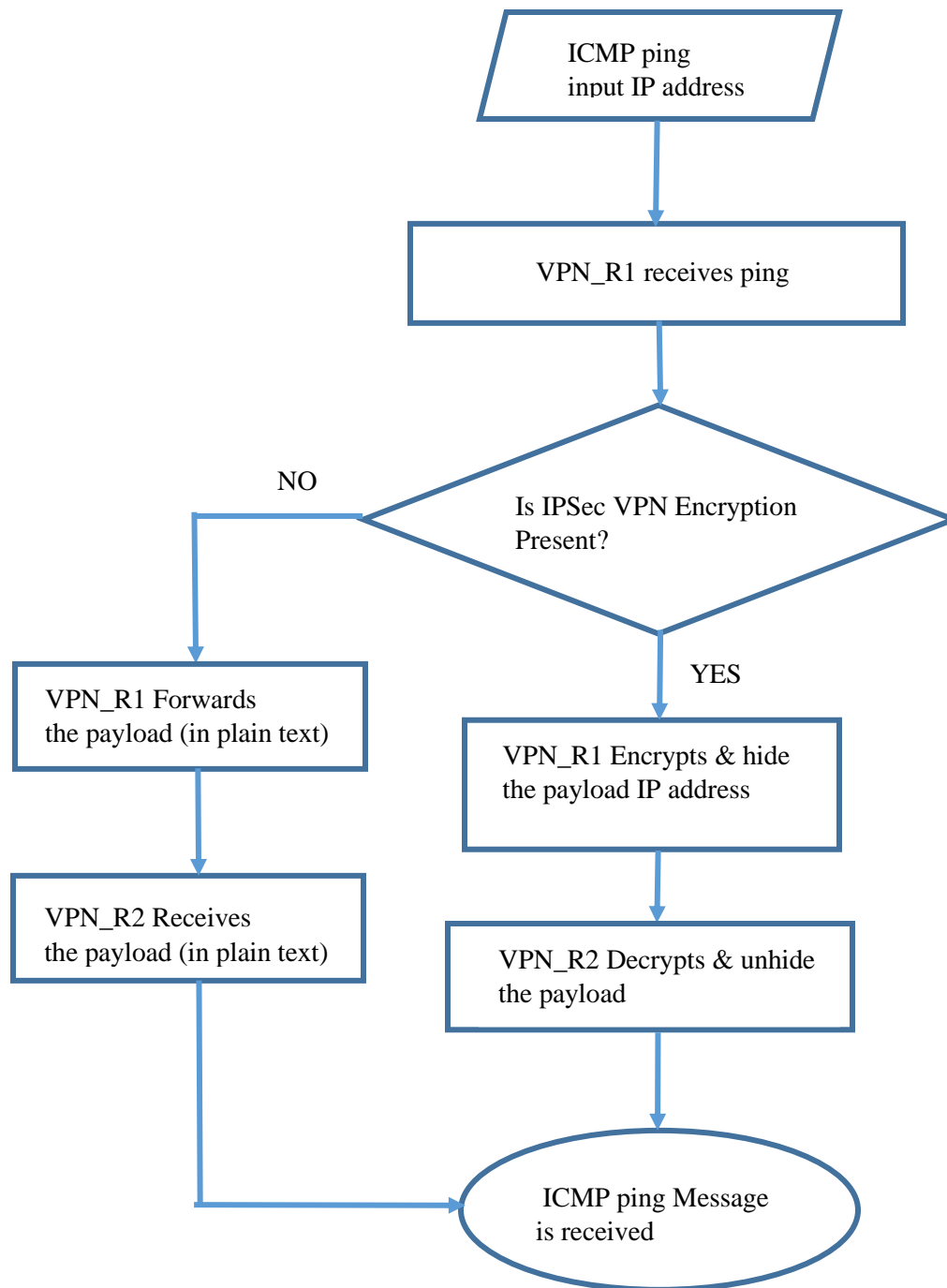


Figure 4.11: IPSec VPN Decision for VPN Routers

We now give access lists to each of the VPN routers such that if one of the routers **VPN_R1** or **VPN_R2** sees a network traffic carrying IPSec VPN packets from its neighbouring router to decrypt the encrypted traffic and grant permission in entering into its network in plain text based on the agreed shared IKE policies. *Appendix I* shows the access lists permit network configurations.

4.9.1 ISAKMP IKE Phase I Configurations

We now enter into IKE Phase I ISAKMP Policy configurations making use of the IKE Phase I acronym “**HAGLE**” mentioned previously in the review chapter. The **H**ashing algorithm has to cypher or scramble the data between the two VPN routers will accept a pre-shared key, a strong password to **A**uthenticate and decrypt the data known only by the VPN routers. The password is a set of random numbers defined by Diffie Hellman **G**roups. The IKE policy is a **L**ifetime **E**ncryption that shows how often the IKE setup should be changed and replaced. The Advance Encryption Standard (AES) uses AES 256 bits key encryption method in the configurations. Which means if a hacker tries to sniff a packet he has 2^{256} combination trials which is practically impossible to break into a network tied with IPSec VPN. In summary, ISAKMP IKE Phase I is used to establish a secure password and tunnel interface between the pairs of the VPN point-to-point routers.

- Authenticate and protect the identities of the IPsec peers.
- Negotiate a matching IKE policy between IPsec peers to protect the IKE exchange.
- Perform an authenticated Diffie-Hellman exchange to have matching shared secret keys.
- Setup a secure tunnel for IKE phase 2.

4.9.2 ISAKMP IKE Phase II Configurations

In IKE Phase II encryption is setup to the VPN routers making reference to the outgoing routers' interfaces that connect to the Internet. With these configurations applied to each of the VPN routers, the ISAKMP IPsec policy is now completed. What is now left is to verify that the IP addresses of individual network is being hidden upon reaching the VPN router before it goes through the tunnel and passes across the Internet. We shall also verify that the plain text has been encrypted and decrypted between the negotiated IPsec VPN routers.

4.9.3 Testing for Encapsulated VPN Payloads

It is so interesting that any network that is tied down with IPsec VPN has its IP addresses hidden by the VPN router before it passes to the Internet as an insecure medium. Let us now verify that and see what exactly we are saying here. We shall send an ICMP message from one network connected to one of the VPN routers and view its outbound PDU (outgoing traffic) and see if the payload IP address changes. A source and destination IP addresses *ping* of 172.17.4.20 to reach 172.17.8.20 IP addresses are hidden instead the *ping* takes source and destination IP addresses of the configured IPsec VPN routers of 10.1.1.18 and 10.17.1.1.22 respectively.

- The IP packets are decapsulated (host IP address is unhide) and decrypted (scrambled texts are converted to plain text) in the interface of the VPN router that receives the payload so that it can enter in plain text to the destination network.

```
interface: Serial0/0/0
  Crypto map tag: VPN-MAP, local addr 10.1.1.18

  protected vrf: (none)
  local  ident (addr/mask/prot/port): (172.17.4.0/255.255.255.0/0/0)
  remote  ident (addr/mask/prot/port): (172.17.8.0/255.255.255.0/0/0)
  current_peer 10.1.1.22 port 500
    PERMIT, flags={origin_is_acl,}
    #pkts encaps: 23, #pkts encrypt: 23, #pkts digest: 0
    #pkts decaps: 33, #pkts decrypt: 33, #pkts verify: 0
    #pkts compressed: 0, #pkts decompressed: 0
    #pkts not compressed: 0, #pkts compr. failed: 0
    #pkts not decompressed: 0, #pkts decompress failed: 0
    #send errors 1, #recv errors 0

    local crypto endpt.: 10.1.1.18, remote crypto endpt.:10.1.1.22
    path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
    current outbound spi: 0x7FC7036E(2143748974)

    inbound esp sas:
      spi: 0x5C6850D7(1550340311)
  --More--
```

Figure 4.13: SADB IPsec VPN Security Verified

4.10 Internet of Things (IoTs) with Motion Detector and IP Camera

CISCO had added the Internet of Things (IoTs) to packet tracer to enable network designers to automate electronic homes and offices devices to clearly predict how the actual implementation would look like. Electronics devices like these do not require complex programming but they do automate when certain procedures are followed. This project will actually look at a few of the IoT devices. IP Webcams, IoT Server and Motion Detector.

4.10.1 Webcam-IP Camera

IP Webcam is a network surveillance security camera that receives IP address from the network and tracks the movement of objects around its area of focus.

Webcams are not just like the old types anymore that accept plug and play to display images in monitor control rooms. They are now equipped with advanced systems where the network engineer provides admin account with password and dynamically or statically configured IP addresses. When this is achieved the users could even view webcam recording activities with their phones. The output obtain from a webcam are audios and videos that are displayed on monitor screens. A network video recorder (NVR) is a specialised hardware network switch like and software solution that is used in IP video surveillance streaming. For mass storage system of audios, images and videos, NVR has slots to allow USB flash drives and SD cards to embed in.

4.10.2 Motion Detector

- The function of the motion detector is to detect the presence of an object and triggers an alert to notify the camera that there is a target around its place of protection.
- The target could be the presence of a given mass moving object that alerts the IP Camera to take photos, audio, videos etc. and store them on a storage device as security evidences.
- The motion detector could also be programmed to detect the presence of smoke or fire and then activate the fire alarm or extinguisher for security attention.
- The figure below shows the software physical appearances of the Webcam and the Motion Detector.



Figure 4.14: Webcam and Motion Detector in Packet Tracer



**IP Camera
HIKVISION**



**Dome IP Camera
HIKVISION**



Honeywell 5898 Motion Detector



Bosch ISC PDL-W18G Motion Detector

Figure 4.15: Webcams and Motion Detector True Physical Appearances

- To have IP cameras display in IoT Server Monitor you must sign in and register with an IoT account.
- Select any server from packet tracer network devices.
- Add IP Camera, Motion Detector and connect them to the IoT server.
- Assign IP addresses for each of the devices

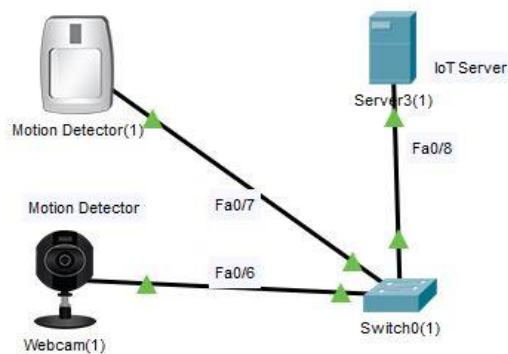


Figure 4.16: IoT Devices

- Sign in to the IoT browser with the IP address of the IoT server to open an IoT user account, select [sign up now](#).
- Enter the user name and password you want to name your account with, click *Sign In* to login to the IoT device.



Figure 4.17: IoT Registration Server Login

Go to the config mode of the webcam and the motion detector, select the Remote Server and then add the account you have registered with the registration server in each of the devices. When once the necessary registrations have been establish we can now login safely to the IoT server monitor to see a display of the motion detector and the IP camera's image. The motion detector is ON by holding down the **Alt** key on the keyboard and bringing the cursor to its sensor.

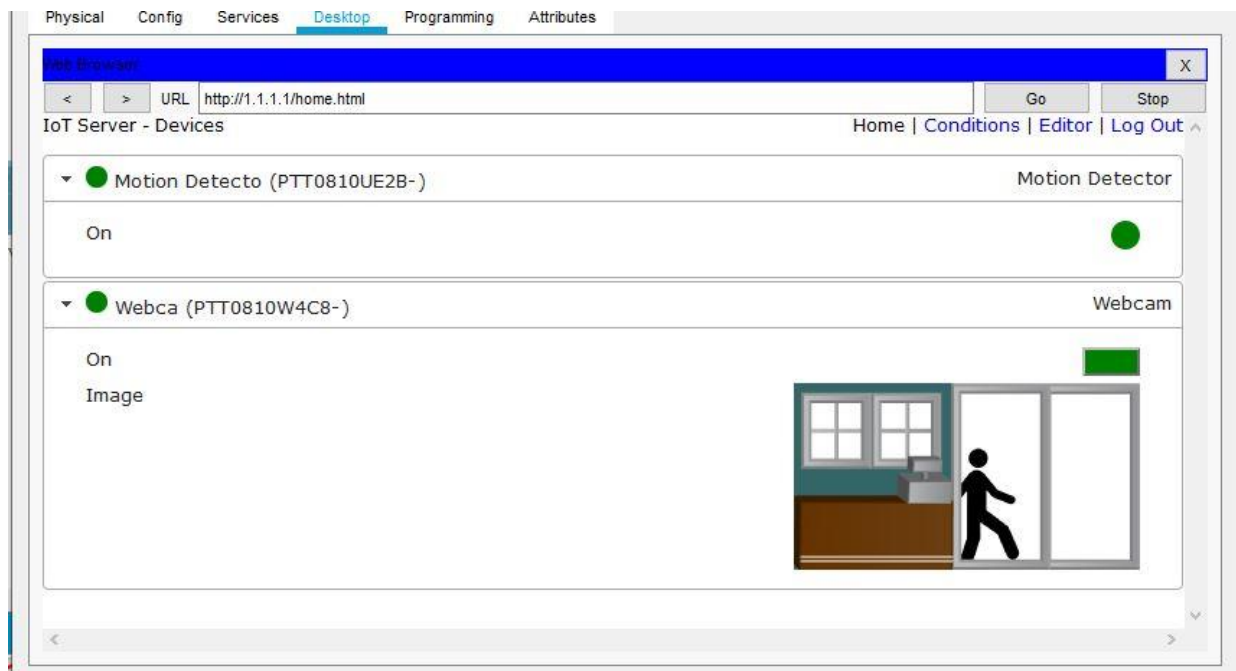
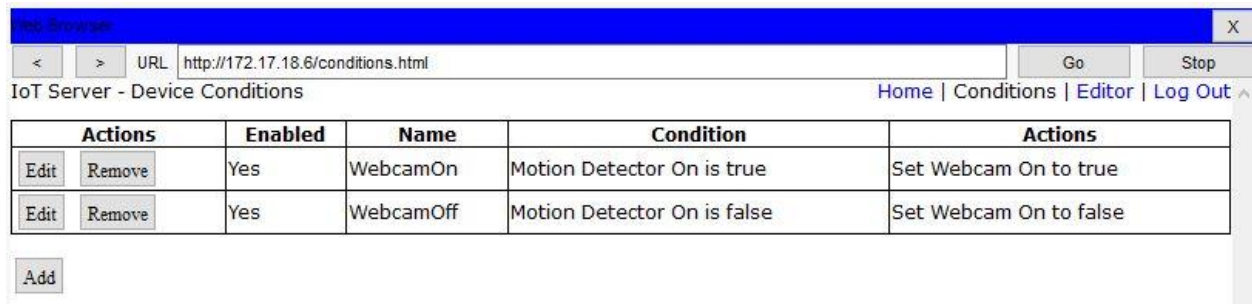


Figure 4.18: The Motion Detector and IP Camera are ON displaying image on the IoT monitor

We now establish two condition to allow the motion detector to completely control the content of the image to display on the IoT Monitor screen as shown in the figure below.



The screenshot shows a web browser window titled "IoT Server" with a URL of "http://172.17.18.6/conditions.html". The page header includes "IoT Server - Device Conditions" and navigation links: "Home | Conditions | Editor | Log Out". Below the header is a table with two rows of conditions. Each row has columns for "Actions", "Enabled", "Name", "Condition", and "Actions". The first row is for "WebcamOn" with the condition "Motion Detector On is true" and the action "Set Webcam On to true". The second row is for "WebcamOff" with the condition "Motion Detector On is false" and the action "Set Webcam On to false". Below the table is an "Add" button.

Actions		Enabled	Name	Condition	Actions
Edit	Remove	Yes	WebcamOn	Motion Detector On is true	Set Webcam On to true
Edit	Remove	Yes	WebcamOff	Motion Detector On is false	Set Webcam On to false

[Add](#)

Figure 4.19: IP Camera Image Control Conditions

- The first condition has a name WebcamOn that will display the image moving action to true only if the motion detector On state is set to true.
- The second condition has a name WebcamOff that will set off the image to false only if the motion detector On state is set to false.

With these conditions in place the IP Camera will only be ON if the motion detector is ON and detect a moving object of valuable mass and then activate the camera to capture the object.

CHAPTER FIVE

5.1 Summary and Conclusion

The network security aims for the project scope are obtained because when either of the VPN routers is tied down with IPSec VPNs with respect to a neighbouring network the text or data that travels across the IPSec VPN routers has IP address payloads hidden and the plain texts are encrypted before passing through the Internet as an insecure medium. The IP address payloads are unhidden and the encrypted texts are decrypted so that the data is seen in plain text to the designated host network. Some proofs of these are shown in Figure 4.8 which tells us that:

- The IP packets are encapsulated and the data is encrypted at the IPSec VPN source router.
- The IP packets are decapsulated and the data is decrypted at the IPSec VPN destination router.

The objectives are useful because they enable us to obtain accurate expected results and their presence make the IP packet traffics flow across the networks.

The project also aimed at developing IoT IP camera surveillance security in which the IP camera captures and records images by the control of the motion detector. The IP camera together with the motion detector linked to the IoT server which serve as the central registration login system is useful in achieving the surveillance system.

In all, a network design simulation like this with strong security system is reliable and safer to implement into governmental agencies and financial institutions to connect cooperate offices to their branch offices remotely across the country.

5.2 Results and Discussions

The IP addresses of hosts' devices are hidden together with the data being sent and received is encrypted and decrypted by the pairs of access lists IPsec VPN routers. Also, the surveillance IP camera has the ability to capture images when the motion detector detects images. These are clear results that the project aims and objectives hold on all conditions. The OSI Model also supports its layers' approach when IP packets are sent the content of the PDU clearly showed the layers functionalities. A project like this is useful because the continual increase in online identity theft and the hijacking of sensitive customer data by anonymous hackers is increasing due to the increase in the number of computer scientists who may have intention to do packet eavesdropping, that is stealing corporate network information for individual profit. VPNs can be an effective means of securing your business's data and thereby safeguarding your reputation.

Government offices and financial institutions are looking for Bachelor degree graduates in Electrical Engineering and Computer Science to securely manage their network systems.

5.3 Challenges

So many challenges were faced in this project design stages but the aim was achieved. The environmental factor as a result of time frame, software and hardware requirements are some of the challenges faced during the projected design stages.

The environmental factor as a result of time frame is due to the time the researcher had to manage in his short semester courses to attend lectures and be prepared for the exam.

Furthermore, the researcher was still an intern student in which his staying at the place of internship will be terminated if he developed the habits of being absent from work.

The software was also another challenge faced throughout the project design stages. The Packet Tracer with the 7.2.0 and 7.3.0 series versions have some problems.

Towards the end of the project design the 7.3.0 Packet Tracer did not display images in the IoT server monitor. But with a couple of trials and research it was observed that the 7.2.0 version does support and display image of the IP camera in the IoT server monitor. So it is a back and forth swing between versions to choose what is actually good to achieve the project aims.

The hardware requirement posed another problem in the project design stages because the configurations in the real network designs are distributed to various real hardware devices such as switches, routers, IP cameras, motion detectors to handle VLANs, DHCPs, telephony services, routings etc. but all of these are handle by a single PC with Packet Tracer being installed in it. This will cause the software to fail and terminate unless it has to be reopen again.

5.4 Recommendations

A project like this would not have been successful if the researcher is not currently working in an internship network design and installation firm. For this reason I do recommend that the department should prioritise and make request to engineering firms to enable students being place in industrial attachments. With this, it will greatly help the students come up with interesting project design topics for their partial fulfillment degree programmes to obtain career paths that will enable students or graduates' successful in the world of engineering applications.

The supervisors have great roles to play in students' final year projects. It is not like entirely helping the student in doing his project but the guide and support by saying "it could be done" is sufficient to help the student reach his project aims and objectives.

I therefore do recommend “*Ing Professor Redwood-Sawyerr*” my supervisor to be a good supervisor because he has the time and patience to go through a student’s project word by word!!

The project was successful but in order to get a total control of the server management system a Demilitarise zone (DMZ) should be designed separately to separate the NASSIT Head Quarter Servers and link them to all the offices for access. Even though is not a requirement but it is necessary to have a DMZ zone to access the HTTP web server. The researcher used RIP V2 routing Information Protocol to route the networks but also RIPv like OSPF or EIGRP can also be applied.

5.5 References

- [1] <https://en.wikipedia.org/wiki/Internet>
- [2] <https://searchnetworking.techtarget.com/definition/OSI>
- [3] OSI_Model_and_Network_Devices You Tube Video
- [4] OSI Model – Open System Interconnection – Functions of 7 OSI Layers in Hindi You Tube Video
- [5] DATA COMMUNICATIONS AND NETWORKING Fourth Edition by Behrouz A. Forouzan
- [6] OSI Model Explained_OSI Amination_Open System Interconnection_OSI 7 You Tube Video
- [7] <https://www.dnsstuff.com/what-is-network-topology#what-is-network-topology>
- [8] <https://www.javatpoint.com/types-of-computer-network>
- [9]https://www.tutorialspoint.com/principles_of_communication/principles_of_optical_fiber_communications.htm
- [10] <https://networkencyclopedia.com/mac-address/>
- [11] EENG-531-Lecture 5-Internet-Data Link na Physical Layers
- [12] https://en.wikipedia.org/wiki/IP_address
- [13] <https://simplicable.com/new/private-ip>
- [14] <https://study-ccna.com/types-of-ip-addresses/>
- [15] <https://www.insiorealeone.net/business/internet-service-providers/>
- [16] Network Design and Computer Management, 120 credits
- [17] Guide to Virtual Private Networks via the Internet between WMO Information System Centres
Virtual Private Networks (VPNs) Overview by: GREG SOUTH

APPENDICES

Appendix A1 VLANs Configurations

FREETOWN_NET

```
!  
en  
conf t  
vlan 10  
name VOICE  
vlan 20  
name DATA  
vlan 30  
name SERVER  
exit  
int range fa0/2-3  
switchport mode access  
switchport access vlan 20  
switchport voice vlan 10  
exit  
  
int range fa0/4-5  
switchport mode access  
switchport access vlan 30  
exit  
int fa0/1  
switchport mode trunk  
!
```

NORTH_NET

```
!  
vlan 10  
name VOICE  
vlan 20  
exit  
int range fa0/2-3  
switchport mode access  
switchport access vlan 20  
switchport voice vlan 10  
exit  
int fa0/1  
switchport mode trunk  
!  
  
EAST_NET  
!  
vlan 10  
name VOICE  
vlan 20  
exit  
int range fa0/2-3  
switchport mode access  
switchport access vlan 20  
switchport voice vlan 10  
exit  
int fa0/1
```

switchport mode trunk

!

SOUTH_NET

!

vlan 10

name VOICE

vlan 20

exit

int range fa0/2-3

switchport mode access

switchport access vlan 20

switchport voice vlan 10

exit

int fa0/1

switchport mode trunk

!

GATEWAY_FREETOWN

!

int fa0/1.10

encapsulation dot1Q 10

ip address 172.17.2.1 255.255.255.0

exit

int fa0/1.20

encapsulation dot1Q 20

ip address 172.17.4.1 255.255.252.0

exit

int fa0/1.30

encapsulation dot1Q 30

ip address 172.17.18.1 255.255.255.0

exit

int fa0/1

no shut

!

GATEWAY_NORTH

!

int fa0/1.10

encapsulation dot1Q 10

ip address 172.17.6.1 255.255.255.0

exit

int fa0/1.20

encapsulation dot1Q 20

Appendix A2 802.1Q Configurations

ip address 172.17.8.1 255.255.252.0

exit

int fa0/1

no shut

!

GATEWAY_EAST

!

int fa0/1.10

encapsulation dot1Q 10

ip address 172.17.10.1 255.255.255.0

exit

int fa0/1.20

encapsulation dot1Q 20

ip address 172.17.12.1 255.255.252.0

exit

int fa0/1

```

no shut
!
GATEWAY_SOUTH
!
int fa0/1.10
encapsulation dot1Q 10
ip address 172.17.14.1 255.255.255.0
exit
int fa0/1.20
encapsulation dot1Q 20
ip address 172.17.16.1 255.255.252.0
exit
int fa0/1
no shut
!

```

Appendix B

DHCP Configurations

GATEWAY_FREETOWN

```

!
ip dhcp excluded-address 172.17.2.1
ip dhcp pool VOICE
network 172.17.2.0 255.255.255.0
default-router 172.17.2.1
option 150 ip 172.17.2.1
exit
ip dhcp excluded-address 172.17.4.1
172.17.4.19
ip dhcp pool DATA20
network 172.17.4.0 255.255.252.0

```

```

default-router 172.17.4.1
dns-server 172.17.18.2
exit
ip dhcp excluded-address 172.17.18.1
ip dhcp pool SERVER30
network 172.17.18.0 255.255.255.0
default-router 172.17.18.1
dns-server 172.17.18.2
!

```

GATEWAY_NORTH

```

!
ip dhcp excluded-address 172.17.6.1
ip dhcp pool VOICE
network 172.17.6.0 255.255.255.0
default-router 172.17.6.1
option 150 ip 172.17.6.1
exit
ip dhcp excluded-address 172.17.8.1
172.17.8.19
ip dhcp pool DATA20
network 172.17.8.0 255.255.252.0
default-router 172.17.8.1
dns-server 172.17.18.2
!

```

GATEWAY_EAST

```

!
ip dhcp excluded-address 172.17.10.1
ip dhcp pool VOICE
network 172.17.10.0 255.255.255.0
default-router 172.17.10.1
option 150 ip 172.17.10.1

```

exit

*ip dhcp excluded-address 172.17.12.1
172.17.12.19*

ip dhcp pool DATA20

network 172.17.12.0 255.255.252.0

default-router 172.17.12.1

dns-server 172.17.18.2

!

GATEWAY_SOUTH

!

ip dhcp excluded-address 172.17.14.1

ip dhcp pool VOICE

network 172.17.14.0 255.255.255.0

default-router 172.17.14.1

option 150 ip 172.17.14.1

exit

ip dhcp excluded-address

172.17.16.1 172.17.16.19

ip dhcp pool DATA20

network 172.17.16.0 255.255.252.0

default-router 172.17.16.1

dns-server 172.17.18.2

exit

!

Appendix C

ISP_ROUTER, Point to Point & VPN ROUTERS Configurations

Appendix C1

ISP_ROUTER

!

interface Serial0/0/0

ip address 10.1.1.21 255.255.255.252

clock rate 64000

interface Serial0/0/1

ip address 10.1.1.25 255.255.255.252

clock rate 64000

interface Serial0/1/0

ip address 10.1.1.17 255.255.255.252

clock rate 64000

interface Serial0/1/1

ip address 10.1.1.29 255.255.255.252

clock rate 64000

!

Appendix C

Point-to-Point (P2P) Configuration

GATEWAY_FREETOWN

!

en

conf t

int fa0/0

ip add 10.1.1.1 255.255.255.252

no shut

exit

!

GATEWAY_NORTH

!

en

```

conf t
int fa0/0
ip add 10.1.1.5 255.255.255.252
no shut
exit
!
```

GATEWAY_EAST

```

!
```

```

en
conf t
int fa0/0
ip add 10.1.1.9 255.255.255.252
no shut
exit
!
```

GATEWAY_SOUTH

```

!
```

```

en
conf t
int fa0/0
ip add 10.1.1.13 255.255.255.252
no shut
exit
!
```

Appendix D

VPN ROUTERS Configurations

VPN_R1

```

!
```

```

en
conf t
hostname VPN_R1
int se0/1/0
ip add 10.1.1.18 255.255.255.252
no shut
```

```

int g0/0
ip add 10.1.1.2 255.255.255.252
no shut
!
```

VPN_R2

```

!
```

```

en
conf t
hostname VPN_R2
int se0/0/0
ip add 10.1.1.22 255.255.255.252
no shut
```

```

int g0/0
ip add 10.1.1.6 255.255.255.252
no shut
!
```

VPN_R3

```

!
```

```

conf t
hostname VPN_R3
int se0/0/1
ip add 10.1.1.26 255.255.255.252
no shut
exit
```

```

int g0/0
ip add 10.1.1.10 255.255.255.252
no shut
!

```

VPN_R4

```

!
host VPN_R4
int se0/1/1
ip add 10.1.1.30 255.255.255.252
no shut
exit
int g0/0
ip add 10.1.1.14 255.255.255.252
no shut
!

```

Appendix E

ROUTING

ISP ROUTER

```

!
en
conf t
router rip
version 2
no auto-summary
network 10.0.0.0
!

```

GATEWAY_FREETOWN

```

!

```

```

en
conf t
router rip
version 2
no auto-summary
network 10.0.0.0
network 172.17.0.0
!

```

GATEWAY_NORTH

```

!
router rip
version 2
no auto-summary
network 10.0.0.0
network 172.17.0.0
!

```

GATEWAY_EAST

```

!
router rip
version 2
no auto-summary
network 10.0.0.0
network 172.17.0.0
!

```

GATEWAY_SOUTH

```

!
router rip
version 2
no auto-summary
network 10.0.0.0

```

network 172.17.0.0

!

VPN_R1

!

router rip

version 2

no auto-summary

network 10.0.0.0

!

VPN_R2

!

router rip

version 2

no auto-summary

network 10.0.0.0

!

VPN_R3

!

router rip

version 2

no auto-summary

network 10.0.0.0

!

VPN_R4

!

router rip

version 2

no auto-summary

network 10.0.0.0

!

Appendix F

TELEPHONY-SERVICE

FREETOWN- NETWORK-TELEPHONY-SYSTEM

!

telephony-service

max-ephone 2

max-dn 3

ip source-address 172.17.2.1 port 2000

create cnf-files

exit

ephone 1

mac-address 0003.E42E.AB57

type 7960

exit

ephone 2

mac-address 0090.0CC2.D9D8

type 7960

exit

ephone-dn 1

number 1001

exit

ephone-dn 2

number 1002

exit

ephone 1

button 1:1

exit

ephone 2


```

button 1:2
exit
!
NORTH-NETWORK-TELEPHONY-SYSTEM
!
telephony-service
max-ephone 2
max-dn 3
ip source-address 172.17.6.1 port 2000
create cnf-files
exit
ephone 1
mac-address 00D0.BAD6.B40D
type 7960
exit
ephone 2
mac-address 0001.C7BC.A055
type 7960
exit
ephone-dn 1
number 2001
exit
ephone-dn 2
number 2002
exit
ephone 1
button 1:1
exit
ephone 2

```

```

button 1:2
!
EAST-NETWORK-TELEPHONY-SYSTEM
!
telephony-service
max-ephone 2
max-dn 3
ip source-address 172.17.10.1 port 2000
create cnf-files
exit
ephone 1
mac-address 0001.C9CE.0155
type 7960
exit
ephone 2
mac-address 0030.F2DE.1306
type 7960
exit
ephone-dn 1
number 3001
exit
ephone-dn 2
number 3002
exit
ephone 1
button 1:1
exit
ephone 2
button 1:2
!

```

SOUTH-TELEPHONY-SYSTEM

```
!  
telephony-service  
max-ephone 2  
max-dn 3  
ip source-address 172.17.14.1 port 2000  
create cnf-files  
exit  
ephone 1  
mac-address 000A.F3A1.2A01  
type 7960  
exit  
ephone 2  
mac-address 00D0.BCC8.633C  
type 7960  
exit  
ephone-dn 1  
number 4001  
exit  
ephone-dn 2  
number 4002  
exit  
ephone 1  
button 1:1  
exit  
ephone 2  
button 1:2  
!
```

Appendix F.II

DIAL-PLAN

GATEWAY_FREETOWN_DIAL_PLAN

```
!  
dial-peer voice 2000 voip  
destination-pattern 2...  
session target ipv4:172.17.6.1  
exit  
dial-peer voice 3000 voip  
destination-pattern 3...  
session target ipv4:172.17.10.1  
exit  
dial-peer voice 4000 voip  
destination-pattern 4...  
session target ipv4:172.17.14.1
```

GATEWAY_NORTH_DIAL_PLAN

```
!  
dial-peer voice 1000 voip  
destination-pattern 1...  
session target ipv4:172.17.2.1  
exit  
dial-peer voice 3000 voip  
destination-pattern 3...  
session target ipv4:172.17.10.1  
exit  
dial-peer voice 4000 voip  
destination-pattern 4...  
session target ipv4:172.17.14.1
```

```
!
```

GATEWAY_EAST_DIAL_PLAN

```
!  
dial-peer voice 1000 voip  
destination-pattern 1...  
session target ipv4:172.17.2.1  
exit  
dial-peer voice 2000 voip  
destination-pattern 2...  
session target ipv4:172.17.6.1  
exit  
dial-peer voice 4000 voip  
destination-pattern 4...  
session target ipv4:172.17.14.1  
!
```

GATEWAY_SOUTH_DIAL_PLAN

```
!  
dial-peer voice 1000 voip  
destination-pattern 1...  
session target ipv4:172.17.2.1  
exit  
dial-peer voice 2000 voip  
destination-pattern 2...  
session target ipv4:172.17.6.1  
exit  
dial-peer voice 3000 voip  
destination-pattern 3...  
session target ipv4:172.17.10.1  
exit  
!
```

Appendix G

HTML Syntax for the HTTP Server

```
!  
<html>  
  <center><font size='+2'  
    color='amber'>National Social Security  
    Insurance Trust (NASSIT) SL  
    Ltd</font></center>  
  
  <hr><marquee behavior =  
    "alternate"><h2>Welcome to the National  
    Social Security Insurance Trust (NASSIT) SL  
    Ltd</h2></marquee>  
  
  <center><br><a  
    href='helloworld.html'>NASSIT-  
    Home</a></center>  
  
  <center><br><a  
    href='copyrights.html'>NASSIT-Contact  
    Addresses:</a></center>  
  
  <center><br><a href='image.html'>NASSIT-  
    Vacancy Announcement-Sierra  
    Leone</a></center>  
  
  <center><br><a href='cscoptlogo177x111.jpg'  
    >Follow Us On Facebook</a></center>  
</html>  
!
```

Appendix H

IPSec VPN Configurations

Enable Security Licenses

```
!  
license boot module c1900 technology-package  
securityk9  
!  
VPN_R1  
!
```

*access-list 100 permit ip 172.17.4.0 0.0.0.255
172.17.8.0 0.0.0.255*

*access-list 100 permit ip 172.17.18.0 0.0.0.255
172.17.8.0 0.0.0.255*

VPN_R1 ISAKMP Policy Phase I

crypto isakmp policy 10

encryption aes 256

authentication pre-share

group 5

crypto isakmp key vpn address 10.1.1.22

!

VPN_R1 ISAKMP Policy Phase II

!

*crypto ipsec transform-set VPN-P2 esp-aes esp-
sha-hmac*

crypto map VPN-MAP 10 ipsec-isakmp

description VPN connection to VPN_R2

set peer 10.1.1.22

set transform-set VPN-P2

match address 100

int se0/1/0

crypto map VPN-MAP

!

VPN_R2

!

*access-list 100 permit ip 172.17.8.0 0.0.0.255
172.17.4.0 0.0.0.255*

*access-list 100 permit ip 172.17.8.0 0.0.0.255
172.17.18.0 0.0.0.255*

*access-list 100 permit ip 172.17.6.0 0.0.0.255
172.17.2.0 0.0.0.255*

!

*access-list 100 permit ip 172.17.2.0 0.0.0.255
172.17.6.0 0.0.0.255*

VPN_R2 ISAKMP Policy Phase I

!

crypto isakmp policy 10

encryption aes 256

authentication pre-share

group 5

crypto isakmp key vpn address 10.1.1.18

!

VPN_R2 ISAKMP Policy Phase II

!

*crypto ipsec transform-set VPN-P2 esp-aes esp-
sha-hmac*

crypto map VPN-MAP 10 ipsec-isakmp

description VPN connection to VPN_R1

set peer 10.1.1.18

set transform-set VPN-P2

match address 100

int se0/0/0

crypto map VPN-MAP

!