



**THE ANALYSIS OF THE WIRELESS SERVICE
IN UNIVERSITY OF BENIN TO OPTIMISE ITS FUNCTION BY
IBHAWAEGBELE OSEMUDIAMEN VICTORY
ENG1609413
OF
THE DEPARTMENT OF COMPUTER ENGINEERING, FACULTY OF
ENGINEERING,
A PROJECT REPORT SUBMITTED IN PARTIAL FULFILMENT OF
THE REQUIREMENT FOR THE DEGREE OF BACHELOR OF
ENGINEERING (B.ENG) IN COMPUTER ENGINEERING,
UNIVERSITY OF BENIN, EDO STATE, NIGERIA.
DECEMBER 2022.**

CERTIFICATION

This is to certify that this project report titled “Analysis on the wireless service in Uniben to optimise its function” by the undergraduate students in the Department of Computer Engineering, Faculty of Engineering, University of Benin, Edo state, satisfactorily completed this work on his own as partial fulfilment of the requirement for the award of Bachelor Degree in Engineering in the department of Computer Engineering.

Engr. Dr. Iruansi
(Supervisor)

Date

Engr. Dr. Okosun
(Head of Department)

Date

ACKNOWLEDGEMENT

We are sincerely grateful to God almighty for the guidance, grace, and strength to start and finish this work. For the financial and moral support from my parents.

We wish to appreciate the University of Benin for allowing us to exercise and explore our technical and academic know-how. We also wish to appreciate our project supervisor in the person of Engr Dr. Iruansi whose contribution, guidance, and support led to the success of this project.

DEDICATION

This project is dedicated to God almighty for the inspiration and direction throughout this project and to our parents for their unending support. This project is also dedicated to my late mom Mrs Faith Obiageri Ibhawaegbele.

ABSTRACT

In today's technologically advanced culture, wireless networks are a need and an essential part of daily life. Wireless networks, which are very important and regularly utilised, must provide the necessary performance and be accessible in the necessary locations. Although the performance and reliability of wireless network connection technology has increased since its debut, there is still reliance on wired network services. A wireless network is a computer network that joins network nodes together using radio frequency as the communication channel. Wireless networking is a technique for connecting many wireless devices.

The wireless service at the University of Benin (UNIBEN) is utilised as a case study in this research project. The examination and optimization of the institution's network served as the foundation for this study. This examines the structure and operation of wireless networks, as well as assessing the wireless network's network capacity, security vulnerabilities, performance, and other factors. Based on facts and statistics that are subsequently collected in reaching a conclusion on the state of wireless services in the institution, conclusions were reached. The research employs survey and experimental research methodologies. Further testing equipment used to evaluate wireless connection were explored. This research describes approaches for wireless network optimization and troubleshooting.

TABLE OF CONTENT

List of figures	i
List of Tables	ii
CHAPTER ONE	Error! Bookmark not defined.
INTRODUCTION	9
1.1 Background Of Study	9
1.2 Problem Statement	10
1.3 Aim And Objectives	11
1.3.1 Aim	Error! Bookmark not defined.
1.3.1 Objectives	11
1.4 Scope Of Study	12
1.4 Relevance Of Research	12
CHAPTER TWO	13
LITERATURE REVIEW	13
2.1 Introduction to Network Concepts	13
2.1.1 Network Architecture	14
2.1.2 Network Topography	15
2.1.3 Packets Transmission in Mesh Network Topology	18
2.2 Network Medium	19
2.3 Key Network Terminologies	19
2.4 The OSI Model	25
2.4.1 The Seven Layers Of the OSI Model	26
2.6 Review Of Related Works	29

CHAPTER THREE	36
METHODOLOGY	36
3.1 Overview Of The University of Benin Network	36
3.2 Process flow for the methodology to be adopted in this research	38
3.2 Network Troubleshooting Methods	39
3.3 Network Troubleshooting Command-Line Tools	41
3.3 Method For Network Analysis	43
3.3 Method For Network Optimisation	47
CHAPTER FOUR	49
RESULTS, ANALYSIS AND DISCUSSIONS	49
4.1 Testing and Results	49
4.1.1 Wireless Network Speed Test	50
4.2 Bill Of Engineering Measurement And Evaluation (BEME) Error!	
Bookmark not defined.	
CHAPTER FIVE	52
CONCLUSION AND RECOMMENDATION	52
5.1 Conclusion	52
5.2 Recommendation	53
REFERENCES	54

LIST OF FIGURES

Figure 2.1 Simple Network Diagram

Figure 2.2 Bus Topology

Figure 2.3 Star Topology

Figure 2.4 Ring Topology

Figure 2.5 Mesh Topology

Figure 2.6 Network Router

Figure 2.7 Network Hub

Fig 2.8 Network Repeater

Figure 2.9 LAN Tester

Figure 2.10 OSI Model

Figure 3.1 An overview of UNIBEN's Wireless network structure.

Figure 3.2 Process flow for the methodology to be adopted in this research

Figure 3.3 SolarWinds Network Performance Monitor Interface

Figure 3.4 SolarWinds NetFlow Traffic Analyzer (NTA) Interface

Figure 3.5 Paessler PRTG Network Monitor Interface

Figure 4.1 Insider Network Testing Interface

LIST OF TABLE

Table 4.1 Table for the bill of engineering measurement and evaluation

CHAPTER ONE

INTRODUCTION

1.1 Background Of Study

Wireless networks are computer networks that are not linked by any form of connection. The deployment of a wireless network allows businesses to avoid the costly procedure of installing wires in buildings or connecting multiple equipment locations. Wireless systems are built on radio waves, which are implemented at the physical level of network structure. Wireless technology, which includes radio, cellular, infrared, and satellite, is a method of delivering data from one point to another that does not require physical connections. A historical viewpoint gives a wide overview of the key changes in this sector. Many phases of progress in wireless communications, telegraph, and radio applications lead to today's mainstream wireless networks. Many companies and sectors are venturing into the wireless industry. (*What Is Wireless Network?*, n.d.)

Educational institutions, airports, and hotels are the industries most committed to implementing wireless technology for business travellers' communications requirements. The three networks, WLAN, WBAN, and WPAN, have become an important part of our everyday lives due to the many services and data they supply. In the health industry, Wireless Body Area

Network (WBAN) is used to track and exchange data about a person's health problems. WBAN uses physiological signal devices to supply its services. WPAN links all household equipment (such as PDAs, scanners, and printers) to the internet across a 10-metre radius. (Verma, 2016)

ALOHAnet, the first professional wireless network, was built at the University of Hawaii in 1969 and became online in June 1971. NCR's WaveLAN product line, launched in 1986, was the first commercial wireless network. Wireless LANs can enable network access without the use of several wires. Wireless connections can be used to expand or replace wired infrastructure in situations where layering cables would be too expensive or impossible. In temporary deployments, a wireless network may be beneficial or even required. Wireless networking is a potential alternative in some places, such as historic heritage buildings, where extra wiring is forbidden. The wireless "no new wires" phenomena, along with PLC networking, has been a key stimulus for home networking and alternative broadband internet. ("ALOHAnet," 2022)

1.2 Statement of The Problem

It is important to note that almost all aspects of our daily lives and activities rely on network connections, the need for a wireless network system cannot be overstated. Network connections are directly or indirectly required by households, offices, schools, and a number of other institutions. This is accurate,

but there are either a limited number of wireless networks or connectivity challenges. This study seeks to pinpoint the weaknesses in the network architecture of the University of Benin's wireless network services and provide comprehensive answers to important questions like:

- How dependable is the University of Benin's wireless network?
- Is it necessary to make improvements?
- What type of network architecture does the ICT department use?
- Is the network infrastructure and hardware sufficient to provide the school's students and staff with the required wireless service?

1.3 Aim Of The Study

The aim of the research is to conduct a thorough investigation into the wireless service at the University of Benin (UNIBEN) and to determine how to enhance its functionality and usability.

1.4 Objective of The Study

The specific objective of the research are;

- To analyse the wireless network structure of UNIBEN.
- A review of the network providers of the institution's network.
- Deploy testing tools and software to test the institution's network and its reliability

- A review of networking testing techniques used in testing wireless networks
- Reviewing network optimization techniques and deploying them to optimise the institution's wireless network services.

1.5 Scope Of The Study

The research assesses the data received from UNIBEN's wireless network analysis, as well as reviews networking methodologies and devices used to test, develop, and optimise wireless networks. This study will also assess performance aspects such as throughput, coverage, reliability, and signal strength.

1.6 Significance Of The Study

In an organisation, business, or institution, every minute matters, and a wireless network is a valuable tool for increasing productivity and promoting information sharing. People can go where they need to while still having access to papers, emails, apps, and other resources with untethered access to documents, emails, applications, and other resources. A learning institution is no exception. This research is an important one as it helps organisations and institutions such as the University of Benin recognise a need to review and improve on existing network infrastructure.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction to Network Concepts

A network is a group of two or more computers that can share resources such as data and applications, office equipment, an Internet connection, or some combination of these. Devices communicate with one another via node connections.

Examples of Networks include;

- Local Area Networks (LAN) - As the name implies, a local area network (LAN) is usually limited to spanning a certain geographic place such as an office building, a single department inside a corporate office, or even a home office.
- Virtual LANs (VLANs) - A VLAN is similar to a LAN except that it is not physically built to look like the individual LANs. Instead, it is constructed logically. They both operate in the same manner, with identical hosts, servers, and printers.
- Wide Area Networks (WANs) are used to connect LANs. WANs are typically utilised when the LANs that must be connected are separated by a significant distance. We employ WAN networks to span enormous geographic areas and genuinely go the distance.

(Computer Network | Definition & Types | Britannica, n.d.)

It is good to note the word Internet from the term internetwork. An internetwork is a type of WAN that connects a bunch of networks, or intranets.

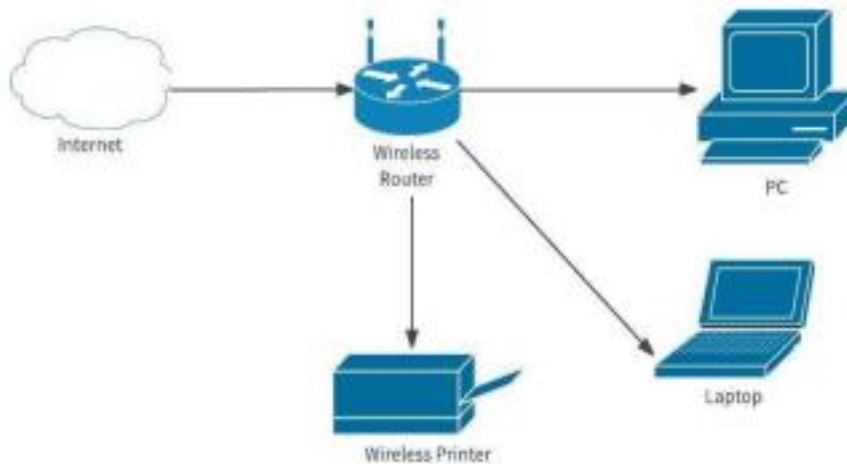


Figure 2.1 Simple Network Diagram

2.1.1 Network Architecture

Network architecture is classified into two types:

1. **Peer to Peer** - Computers connected in peer-to-peer networks have no central or particular authority—they are all peers, which means they are all equals in terms of authority. Its computer network is set up to allow certain files and folders to be shared with everyone or with specific individuals. (*Computer Network Architecture - Javatpoint, n.d.*)
2. **Client/Server** - A client-server network is a network in which a central computer, often known as a server, hosts data and other types of resources. Clients, such as laptops and desktop computers,

contact the server and request data or other resources from it. It is made up of a set of computers (referred to as clients) that send requests for network services to a server. (*What Is Network Architecture?*, n.d.)

2.1.2 Network Topography

The physical or logical arrangement of a network is referred to as its topology. It specifies how distinct nodes are arranged and linked to one another. Network topology, on the other hand, may define how data is transported between these nodes. It should be emphasised that a node in a network or diagram is a point where lines or paths connect or branch. (“Network Topology,” 2022)

There are two kinds of network topologies:

- **Physical topology:** This topology focuses on the physical layout of the connected devices and nodes.
- **Logical topology:** This focuses on the data transit pattern between network nodes.

Physical topology comprises of:

- **Bus Topology:** On a local area network, every computer and network device is connected to a single cable (LAN). Although this is a basic, low-cost topology, the single point of failure poses a concern.

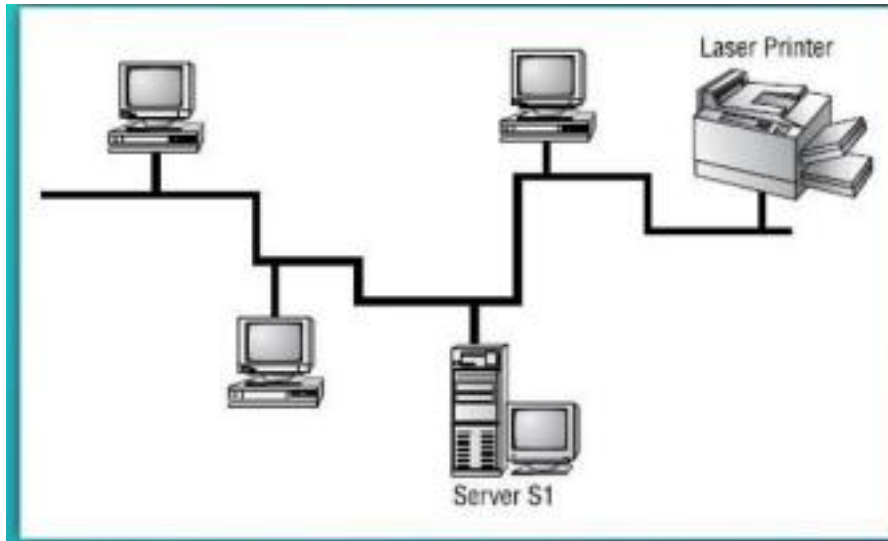


Figure 2.2 Bus Topology

- **Star Topology:** In a star topology, network devices are connected through cables to a central computer known as a hub or switch. Data is passed through the switch or hub as nodes communicate across the network. Individual node or cable failure does not always result in network outage, but the failure of a central device can. This is the most desired and widely used topology.

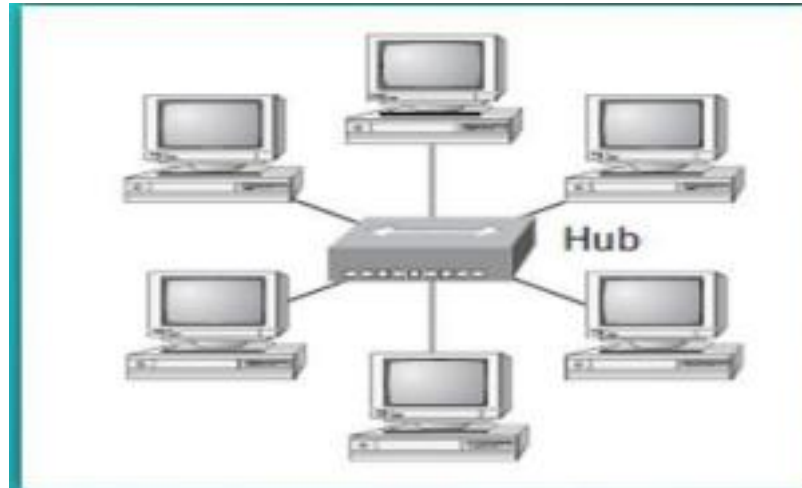


Figure 2.3 Star Topology

- **Ring Topology:** A local-area network (LAN) with a ring topology. In other words, all of the nodes are linked in a closed loop. Data packets or packets of data pass around the ring, with each node accessing packets directed to it.

A ring network has the advantage of being able to travel greater distances than other types of networks since each node regenerates packets as they pass through it. (“Network Topology,” 2022)

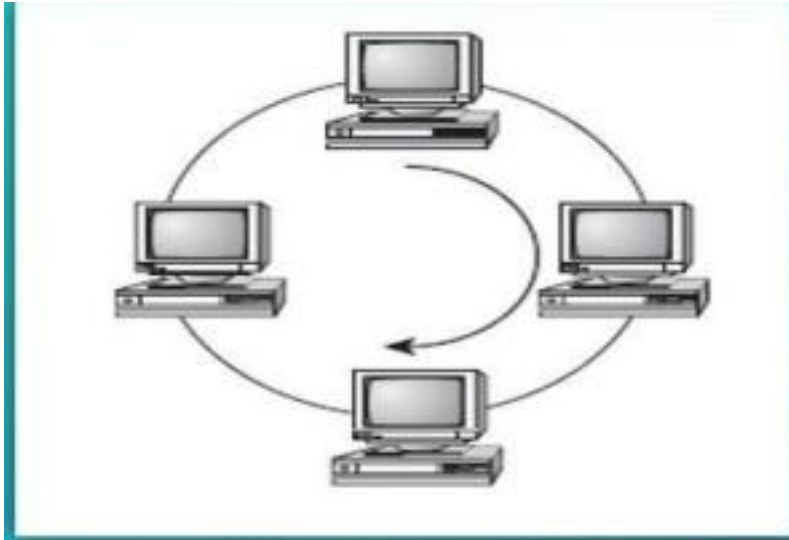
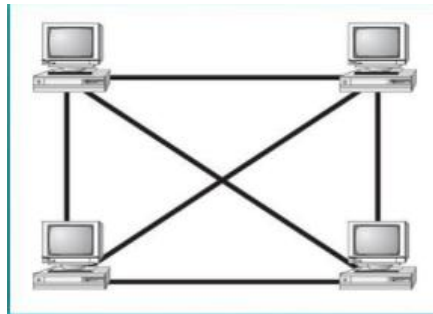


Figure 2.4 Ring Topology

- **Mesh Topology** - A point-to-point link to other nodes or devices. The



network nodes are all linked together.

Figure 2.5 Mesh Topology

2.1.3 Packets Transmission in Mesh Network Topology

Routing and Flooding are two methods for transmitting packets or data through a mesh topology. Routing logic is implemented by nodes in accordance with network needs. As an example, routing directs packets to the destination using the shortest path possible. Alternatively, routing logic that is aware of faulty links and avoids certain nodes, etc. We can even implement routing logic to

reconfigure failed nodes. Because flooding sends the identical data to all network nodes, no routing logic is necessary. If the network is resilient (strong enough to endure obstacles), data loss is extremely improbable. However, it causes unnecessary network load. (*Mesh Topology - an Overview | ScienceDirect Topics*, n.d.)

2.2 Network Medium

This refers to the paths or means utilised to connect network nodes. They are classified into two groups:

- **Bounded/Guided Media** - The physical links between the devices are referred to as Bounded/Guided Media. Coaxial Cable, Fiber Optic Cable, Twisted Pair Cable, and other physical media are examples of physical media.
- **Unbounded/Unguided media** - Examples of unbounded/unguided media, also known as wireless media, are microwave, radio, and wireless fidelity (Wi-Fi)

(*Network Medium - Definition and More*, n.d.)

2.3 Key Network Terminologies

- **Connection:** A connection is a term used in networking to describe pieces of connected data that are sent via a network. This implies that a connection is established prior to data transfer (by following protocol protocols) and then deconstructed at the conclusion of the data transfer.

- **Packet:** A packet is the most fundamental unit of data that is transferred through a network. Packets are the envelopes that convey your data (in pieces) from one end point to the other when communicating over a network.
- **Network Interface:** A network interface can refer to any type of software that connects to networking hardware. For example, if your computer has two network cards, you can control and configure each network interface connected with them separately.
- **LAN:** The term "local area network" (LAN) refers to a network that is limited to a single location. It refers to a network or a segment of a network that is not publicly available on the internet. A LAN is an example of a home or workplace network.
- **WAN:** The term "wide area network" (WAN) refers to a network that spans a large area. It refers to a network that is substantially larger than a LAN. While WAN is a useful phrase for describing vast, scattered networks in general, it is most commonly used to refer to the internet as a whole.
- **MAN:** A metropolitan area network (MAN) is a computer network that connects computers in a metropolitan region, which can be a single large metropolis, a collection of cities and towns, or any significant area with several buildings. A metropolitan area network (MAN) is larger than a

local area network (LAN) but smaller than a wide area network (WAN) (WAN).

- **WLAN:** A wireless LAN (WLAN) is a wireless computer network that connects two or more devices using wireless communication to form a local area network (LAN) inside a certain region, such as a home, school, computer lab, campus, or office building. This allows users to travel throughout the region while remaining connected to the network. A WLAN can also enable access to the rest of the Internet via a gateway. The most extensively used computer networks in the world are wireless LANs based on IEEE 802.11 standards. These are frequently referred to as Wi-Fi, which is a Wi-Fi Alliance trademark.
- **Servers:** Servers are high-configuration computers that oversee the network's resources. Users have access to network resources through the network operating system, which is normally installed on the server. File servers, database servers, print servers, and more types of servers exist.
- **Clients:** Clients are computers that access and use network resources by requesting and receiving services from servers.
- **Peers:** Peers are computers in a workgroup network that give and receive services from other peers.
- **Transmission Media:** The routes through which data is transported from one device to another in a network are known as transmission media.

the name given to this feature. The terms "bridging" and "routing" are used interchangeably.

(*"Network Devices"* 2015)

- ❖ **Network Hub:** A Hub is a networking device that allows you to connect multiple PCs to a single network. It is used to connect segments of a LAN. A hub stores various ports, so when a packet arrives at one port, it is copied to various other ports. Hub works as



a common connection point for devices in a network.

Figure 2.7 Network Hub

- ❖ **Repeaters:** A repeater is an electronic device in a communication channel that increases the power of a signal and retransmits it, allowing it to travel further.



Fig 2.8 Network Repeater

- ❖ **CAT5e Ethernet Cable:** The term Cat5e refers to the Category 5 Enhanced cabling standard for networks. Cat5e cables are often utilised within Ethernet infrastructures to support 10BASE-T (**Ethernet**), full-duplex 100BASE-TX (Fast Ethernet), and 1000BASE-T (Gigabit Ethernet) networks. Cat5e technology provides a performance of up to 100 MHz.
- **Testing Devices** such as network testers. A network cable tester is an electronic device that measures the conductivity and connectivity between two ends of a cable. It also checks and measures signals for correct wiring. Example of a network testing device is the LAN tester.



Figure 2.9 LAN Tester

2.4 The OSI Model

The Open Systems Interconnection (OSI) model defines seven layers through which computer systems communicate over a network. It was the first standard model for network communications, and it was adopted in the early 1980s by all major computer and telecommunications corporations. The present Internet is built on the simpler TCP/IP paradigm rather than the more complex OSI model. The OSI 7-layer model, on the other hand, is still extensively used because it helps visualise and understand how networks work, as well as isolate and diagnose networking problems. (“Network Architecture,” 2022)

The OSI model not only provides a framework for creating and implementing networking standards, devices, and internetworking schemes but also explains the networking from a modular perspective, making it easier to understand and troubleshoot.

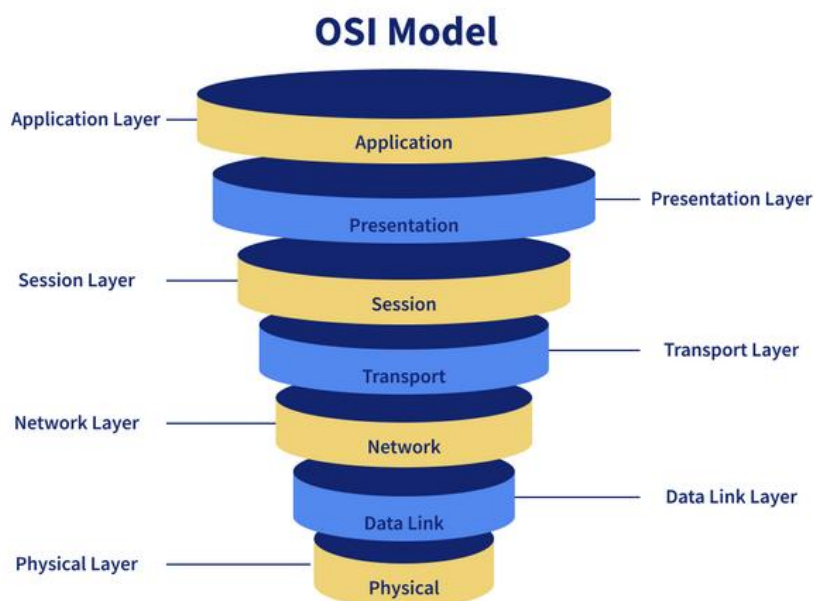


Figure 2.10 OSI Model

2.4.1 The Seven Layers Of the OSI Model

- The Application Layer (Seventh Layer) - This is the last layer and the topmost layer of the OSI model. This layer provides an interface between application programs running in the system and network. If any application needs to access any resource that is available in a remote system, it interacts with this layer. Examples; SSH (Secure Shell), FTP (File Transfer Protocol) and TFTP (Trivial File Transfer Protocol), etc.
- The Presentation Layer (Sixth Layer) – The presentation layer works as the translator in the OSI model. When receiving data from the application layer, it converts that data in such a format that can be sent over the network. When receiving data from the session layer, it reconverts that data in such a format that the application which will use the incoming data can understand. ASCII, BMP, GIF, JPEG, WAV, AVI, and MPEG are the few examples of standards and protocols which work in this layer.
- The Session (Fifth Layer) – It is responsible for setting up, managing, and dismantling sessions between presentation layer entities and providing dialogs between computers. When an application makes a network request, this layer checks whether the requested resource is available in the local system or in the remote

system. If a requested resource is available in a remote system, it tests whether a network connection to access that resource is available or not. If network connection is not available, it sends an error message back to the application informing that connection is not available. If a network connection is available, it establishes a session with a remote system.

- The Transport Layer (Fourth Layer) – The transport layer is the fourth layer of the OSI model. It provides following functionality;
- Segmentation: On sending a computer, it breaks the data stream into smaller pieces before transmission. Each piece is known as segment and the process of breaking data into smaller pieces is known as segmentation. On the receiving computer, it joins all segments back in the data stream. So the upper layers receive data in the format in which it was sent.
- Data Transportation: This layer establishes a logical connection between sending system and receiving system and uses that connection to provide end-to-end data transportation. For data transportation, it mainly uses two protocols; TCP and UDP. TCP protocol is used for reliable data transportation. UDP protocol is used for unreliable data transportation.
- Multiplexing: Connection multiplexing allows multiple applications to send and receive data simultaneously.

- Network Layer (Third Layer) – This layer decides whether the packet is intended for a local system or remote system. It also specifies the standards and protocols which are used to move the data packets across the networks.
- Data Link (Second Layer) – This layer defines how networking components access the media and what transmission methods they use. This layer has two sub-layers; MAC and LLC.
- MAC (Media Access Control): This sub layer defines how the data packets are placed in media.
- LLC (Logical Link Control): This sub layer identifies the network layer protocol.
- Physical Layer (First Layer): This layer specifies the standards for devices, media and technologies which are used in moving the data across the network. On the sending computer, it converts digital signals received from the Data Link layer into analog signals and loads them in physical media. On the receiving computer, it picks analog signals from media and converts them into digital signals and transfers them to the Data Link layer for further processing. (“OSI Model,” 2022)

2.6 Review Of Related Works

Wireless technology is not a new notion; in fact, it has played a significant part in networking and communication, which are employed in practically all daily activities at home, school, and organisations. Several works have been assembled solely for the aim of evaluating this developing technology; such works will be assessed as they relate to wireless network technologies. This section will review related literature that have been done in light of networks and wireless networks.

In a paper by **Oscar et al (2005)** , the authors reviewed the performance analysis of hybrid broadband access technologies using PLC and Wi-Fi. The study used performance measurement to show that whenever communication takes place on the same floor or between two floors, the throughput performance of hybrid and non-hybrid access is quite similar. When connection is performed between more than two floors, this demonstrates that hybrid technology can increase signal quality in areas where Wi-Fi is not available. The research work was limited to just the throughput of the hybrid network, it did not cover other element parameters such as coverage and cost.

In another research titled “ Electric-Fi Your Data: Measuring and Combining Power-Line Communications with Wi-Fi”, **Christina et al (2010)** showed that combining PLC with Wi-Fi networks can result in significant performance benefits. They developed an experimental framework and looked into PLC performance. They looked at its geographical and temporal variation,

as well as the various time scales of PLC channel variability. They've provided recommendations for effective metric estimation in hybrid setups. They discovered that link quality and variability are highly correlated, which has a direct impact on probing overhead and accurate calculations. The research focuses on comparing wireless and PLC performance and looks into older PLC and Wi-Fi specifications. The authors give testbed measurements for criteria including coverage, throughput, and connectivity from 20 households, but not for cost

Similar Research done on the comparative performance study of wireless and power line networks by **Yu-Ju Lin et al (2003)**, the authors aimed at comparing the IEEE 802.11x and HomePlug 1.0 protocols in terms of their ability to provide networking functionality in a practical and theoretical manner. It can be seen from the theoretical calculations that HomePlug 1.0 and 802.11x have similar maximum efficiency. Although the higher maximum PHY data rate of 802.11a would suggest that it should perform better than the other two protocols, its coverage in field tests was not as good. Results showed that PLC and wireless technology, as examined in this study, offer significant room for improvement above present standards, however the authors did not specify. However they failed in trying to integrate the advantages and disadvantages of the two technologies in order to create a better network.

Ki Wong et al (2017) gave an analysis of wi-fi performance data for a wi-fi throughput prediction approach. Two contributions are presented in this

thesis. First, a Wi-Fi data visualisation tool that was created to demonstrate changes in physical layer metrics over time. Second, this thesis examined the relationship between Wi-Fi performance parameters and the saturation throughput, a Wi-Fi performance indicator. Using Support Vector Machine (SVM) learning techniques, this thesis shows how to exploit a constrained Wi-Fi parameter set to reliably estimate Wi-Fi throughput in a controlled radio communication environment.

It is a trade-off between estimation accuracy and complexity. As a result, more precise environment parameters such as packet size, 802.11n frame aggregation size, or signal reflection (multi-path fading) that could increase forecast accuracy are not captured by such measurements.

Sébastien Henri et al (2011) proposed a research that described Hybrid Networks. In the research titled “Empower Hybrid Networks: Exploiting Multiple Paths Over Wireless And Electrical Mediums.”, the authors used an approach where they created a distributed congestion controller that converges to utility-optimal allocations. It also allows them to create a new multipath routing method that calculates the most efficient combinations of paths for simultaneous use. To our knowledge, this is the first time congestion-control and multipath-routing algorithms have been implemented in hybrid PLC/Wi-Fi networks. EMPoWER is a distributed and practical algorithm that achieves performance comparable to that of optimal but impractical methods. The research work was able to provide a model for the multipath of a hybrid

network, but not for a non-hybrid network such as a wireless network. Because of the impractical algorithms, no actual implementation was carried out during the study.

M. K. Lee et al. (2020) reviewed homeplug 1.0 powerline communication lans -protocol description and performance results. The HomePlug 1.0 protocol, which is based on Orthogonal Frequency Division Multiplexing (OFDM) and Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), is described in this document, along with improvements to allow priority channel access. It then uses a simulation model, ideal laboratory measurements with actual HomePlug 1.0 devices, and field experiments in a residential building to offer performance results for the HomePlug 1.0 protocol. At the application level, simulation and laboratory data rates were about 6 Mbps, and field tests yielded rates ranging from 1.6 to 5.3 Mbps. The use of Homeplug devices for performance testing presents a fairly high cost. The research does provide an alternate way for multiple priority channel access.

In a comparative study of hybrid network (powerline communication and wifi) and wireless network using university of benin's computer engineering laboratory as a case study by **Aideyan I. Winifred and K.B Erameh (2020)**, the author's study evaluated the two networks for building a small/home office network without the need for additional cable installation. The hybrid network has a higher transmission throughput than the wireless network, which is only

average. Because of its slightly higher maximum data rate, the hybrid network took the lead at data rates of 5 Mbps and above. The results showed that the hybrid network outmatches the wireless network. But the wireless network performs better under congested conditions such as overloading from electrical appliances; this really affected the loss rate of the hybrid network. So the best option to get greater throughput is a combination of both. This however, is more expensive.

In evaluating the network performance of an ad hoc wireless network, **C. K. Toh et al (2002)**, the impact of different packet sizes, beaconing intervals, and route hop counts on route discovery time, communication throughput, end-to-end delay, and packet loss was investigated. The authors also conducted mobility tests and assessed the time spent reconstructing routes. The file transfer times associated with safely delivering information over multihop wireless connections (through TCP) are also shown.

The results of the experiments showed that it is possible to add ad hoc networking functionality to current wireless PCs. Beaconing intervals have less of an impact on end-to-end performance in ad hoc routes than packet size or route length. With the exception of very high beaconing frequencies, transmission throughput is more dependent on packet size and route length. Packet loss, on the other hand, is unaffected by the size of the packet, the length of the route, or the frequency of beaconing. Traditional networks are slower than ad-hoc networks. They are typically less secure due to the widespread use

of wireless connections (which are less secure than cable connections) and the lack of a central device to manage network security.

D. Helen and D. Arivazhagan (2014) examined the applications, advantages and challenges of ad hoc networks. The review aimed at uncovering the design, application, and features of ad hoc networks, as well as discuss many tough challenges and propose a possible solution based on new technology. Because of recent advancements in the field of ad hoc networking, nodes can now create a self-creating, self-organising, and self-administering wireless network. It is a crucial aspect of future pervasive computing environments due to its inherent flexibility, lack of infrastructure, ease of deployment, auto setup, low cost, and possible uses.

In a research into reliability modelling, analysis and prediction of wireless mobile communications, **Raja et al (2014)** introduced a methodology for modelling, forecasting, and analysing theoretical wireless connection reliability based on characteristics such as fading, mobility, and interference, among others. The analysis and prediction are based on the part stress technique, which assumes time-dependent elements/components and their Transmission Times To Failure. Other reliability analysis approaches, such as Fault Tree Analysis and Accelerated Testing of Wireless Systems, are also supported by the proposed framework, which can be used to improve the components. The testing and analysis technique employed here involved lots of technicalities and

are not also realisable in the real world application. Furthermore, the cost of extensive analysis presents its own challenges.

CHAPTER THREE

METHODOLOGY

In the previous section the concept of networks and networking technologies was discussed, this section will focus on methods used in the analysis of the wireless network structure at the university of Benin. Highlighting troubleshooting methods for networks and methods to optimise wireless network connectivity across the Institutions network.

3.1 Overview Of The University of Benin Network

The University of Benin's wireless network architecture includes a Central Network Node located at the institution's ICT centre. This node acts as a redistribution point for internet access throughout the institution. This network transmission is facilitated by network devices. Cat5 cables are used to connect network access from the central Node to specific places within the institution that have network access. Routers are typically located in each faculty and some departments. Network connections run from the central node to routers located at crucial sites throughout the individual faculties.

Routers are used to divide a large network into smaller networks. Network routers transmit and receive data from one network to another. Routers divide vast networks into logical pieces known as subnets, making it easier to redistribute the network from the central node. The routers are linked to network

repeaters. The network repeaters' purpose is to extend transmissions so that the signal can go further or be received on the other side of an impediment. They are also known as network extenders.

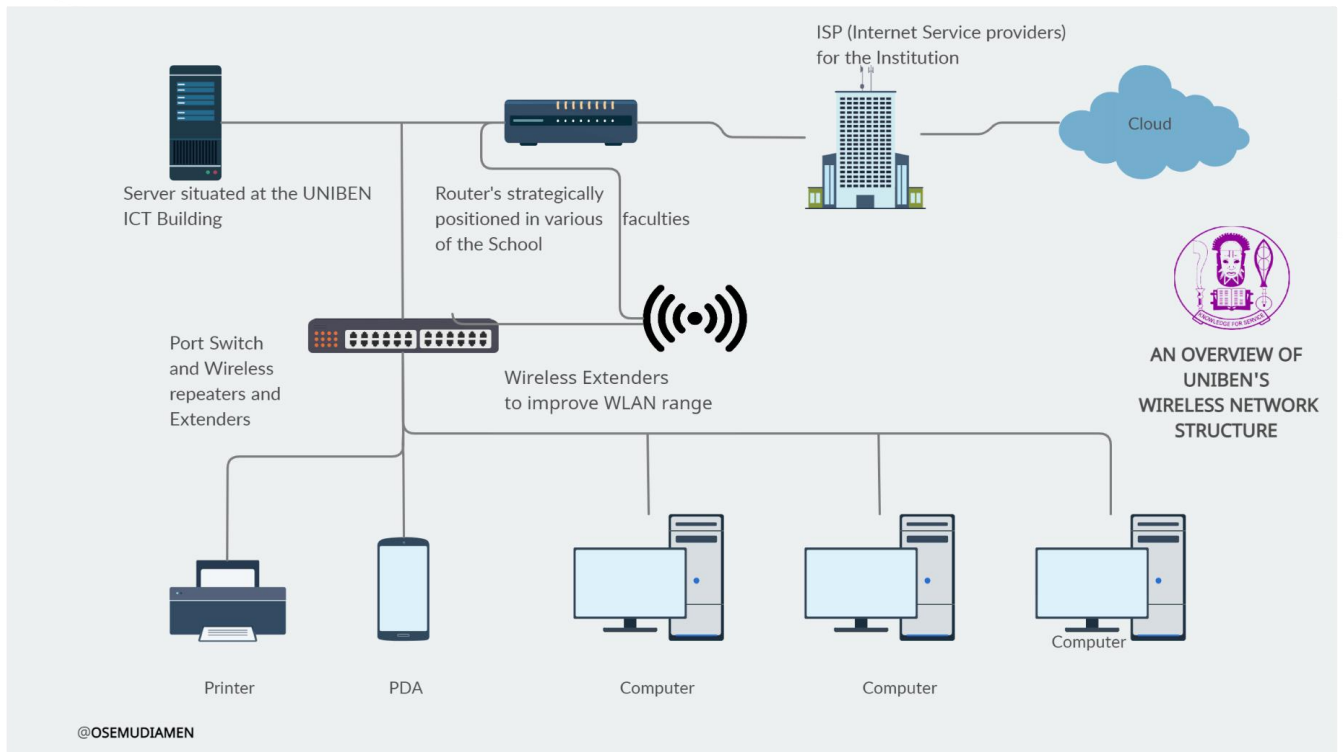
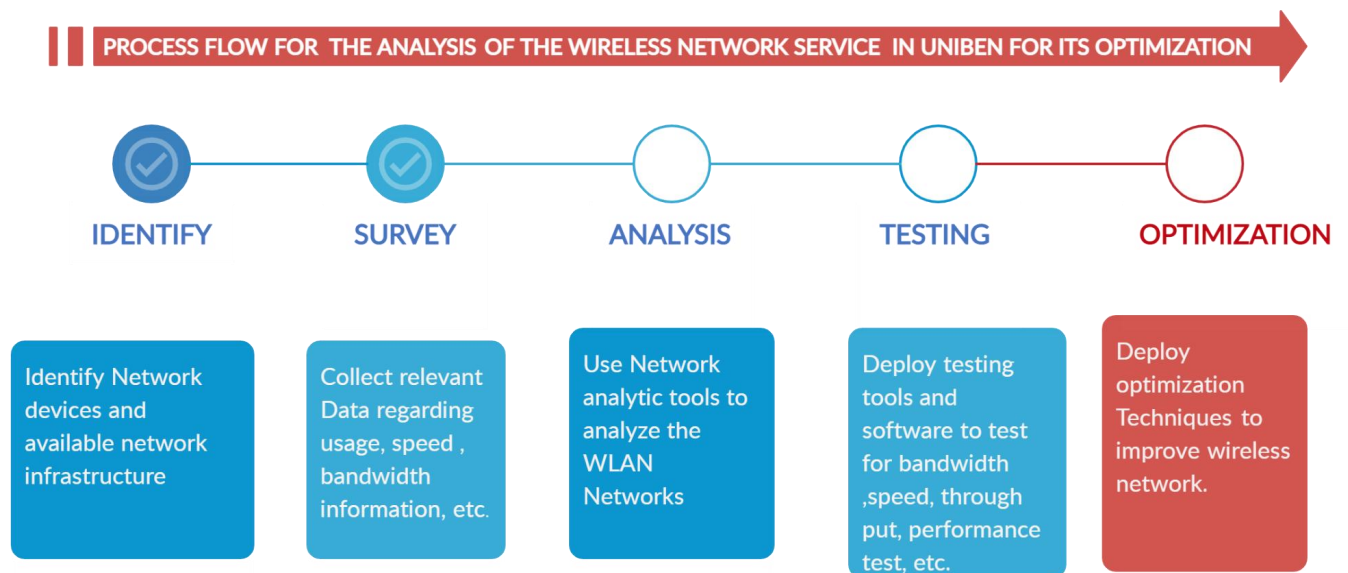


Figure 3.1 An overview of UNIBEN's Wireless network structure.

Survey and Experimental Research methodologies are used in this project research, which includes data collection, analysis, network testing, troubleshooting, and optimization depending on the specified objectives. The research methodology block diagram depicts a subsequent design process in Figure 3.2 below.



@OSEMUDIAMEN

Figure 3.2 Process flow for the methodology to be adopted in this research

The research into the examination of the wireless service in UNIBEN to enhance its function will begin by identifying essential network infrastructure and the type of devices connected to them, as shown in the block diagram above. The evaluation uses Ekahua, a premier Wi-Fi tool for creating, validating, optimising, and debugging wireless networks. Wireshark and InSSIDer are also used for survey and analytic purposes in this research.

inSSIDer is a free Wi-Fi scanner that displays the RSSI values of all local wireless networks as well as the channels they use. Wireshark is a packet analyzer and sniffer. It records network traffic on the local network and stores it for further analysis. Wireshark records network traffic from Ethernet, Bluetooth, Wireless (IEEE.802.11), Token Ring, Frame Relay, and other protocols.

3.2 Network Troubleshooting Methods

The practice of discovering problems with a network using a rigorous and repeatable methodology and then solving those problems using testing methodologies is referred to as troubleshooting. Troubleshooting is more effective than randomly trying things until the network works since it allows you to target particular network components and evaluate each for functionality.

The following are ways to troubleshoot networks.

- 1. Examine the hardware.** Check all of your hardware to ensure it's properly connected, turned on, and operating before you start troubleshooting. If a cord has come loose or someone has turned off an important router, this could be the source of your networking problems. It's pointless to go through the debugging process if all you need to do is plug a cord in. Check that all switches are in the correct positions and have not been mistakenly bumped. After that, switch the hardware off and on again. This is the basis of IT troubleshooting, and while it may appear simplistic, it frequently solves the problem. Simple problems can be resolved by power cycling your modem, router, and computer.
- 2. Use the command `ipconfig`.** Open the command prompt and enter "ipconfig" (without the quotation marks) into the terminal. The IP address of your router is displayed as the Default Gateway (last). The number next to "IP Address" is your computer's IP address. If your computer's IP

address begins with 169, it is not getting a genuine IP address. If it does not begin with 169, your computer is being assigned a genuine IP address by your router. To get rid of your current IP address and request a new one, type "ipconfig /release" followed by "ipconfig /renew." In certain circumstances, this will solve the problem. If you still can't receive a valid IP address from your router, try connecting your computer directly to the modem through an ethernet connection.

3. Ping and tracert are useful tools. If your router is operational and your IP address does not begin with 169, the issue is most likely between your router and the internet. Now is the time to employ the ping tool. Ping a well-known, large server, such as Google, to see if it can communicate with your router. To ping Google DNS servers, open a command line and type "ping 8.8.8.8"; you may optionally add "-t" to the end (ping 8.8.8.8 -t) to continue pinging the servers while you troubleshoot. If the pings fail to send, the command prompt will return basic error information.

4. Perform a DNS lookup. To see if the server you're attempting to connect to is down, use the command "nslookup." If you do a DNS check on google.com and get results like "Timed Out," "Server Failure," "Refused," "No Response from Server," or "Network Is Unreachable," it could mean the problem is with the DNS server for your destination. (Alternatively, you can use nslookup to check your own DNS server.)

- 5. Contact the Internet service provider.** If none of the above resolves the issue, contact your internet service provider to discover if they are experiencing problems. You can also use a smartphone to seek outage maps and similar information to see whether others in your region are experiencing the same issue.
- 6. Examine virus and malware protection.** Next, ensure that your antivirus and malware products are up and running and that they haven't detected anything that could be damaging your network and preventing it from functioning.
- 7. Examine the database logs.** Examine all of your database logs to ensure that the databases are working properly. If your network is operational but your database is full or dysfunctional, it may be causing issues that impair network performance.

(A Guide to Network Troubleshooting, n.d.)

3.3 Network Troubleshooting Command-Line Tools

To obtain detailed information about the network status, enter the following commands into the command line one at a time:

- **Ping:** Ping is a TCP/IP utility that sends a datagram to the host supplied in the command. The receiving host returns the datagram if the network is operational.

- **tracert/traceroute** —A TCP/IP utility for determining the path data takes to reach a specific destination. This tool can help you identify problems by determining where you are losing packets in the network.
- **nslookup** — A DNS utility that returns the IP address associated with a hostname or vice versa. This tool is useful for identifying DNS name resolving issues.
- **ipconfig** – A TCP/IP application for Windows that checks network settings and connections. It may provide you with a host's IP address, subnet mask, and default gateway, as well as other critical network information.
- **Ifconfig** is a TCP/IP application for Linux or UNIX that displays the current network interface settings and allows you to assign an IP address to a network interface. This command, like ipconfig on Windows, will provide essential information about the network and its state.
- **netstat** — A command-line utility that displays the status of all active network connections. This tool is useful for determining which services are active on a given system.
- **tcpdump** — A utility for retrieving packet data from a query string given to a network interface. It is free on Linux and may be downloaded as a command for Windows.

- **pathping** — A TCP/IP command that provides information about network latency and packet loss. It can assist you in troubleshooting network packet loss issues.

(Understanding the Networking Commands, n.d.)

3.3 Method For Network Analysis

As part of the project objectives to analyse the wireless network of the University Of Benin, analysis tools and method of use is shown in this section. Below are popular network analysis tools that can be employed in analysing a wireless network.

1. **SolarWinds Network Performance Monitor:** SolarWinds Network Performance Monitor is designed as all-in-one network monitoring software with an integrated network analysis tool. NPM can provide network monitoring reports, a QoE dashboard for traffic analysis, and intelligent alerting to inform IT personnel when crucial performance indicators exceed predefined limits. It may also present current and historical performance information in user-friendly dashboards and charts to assist IT teams in determining the root of a problem.

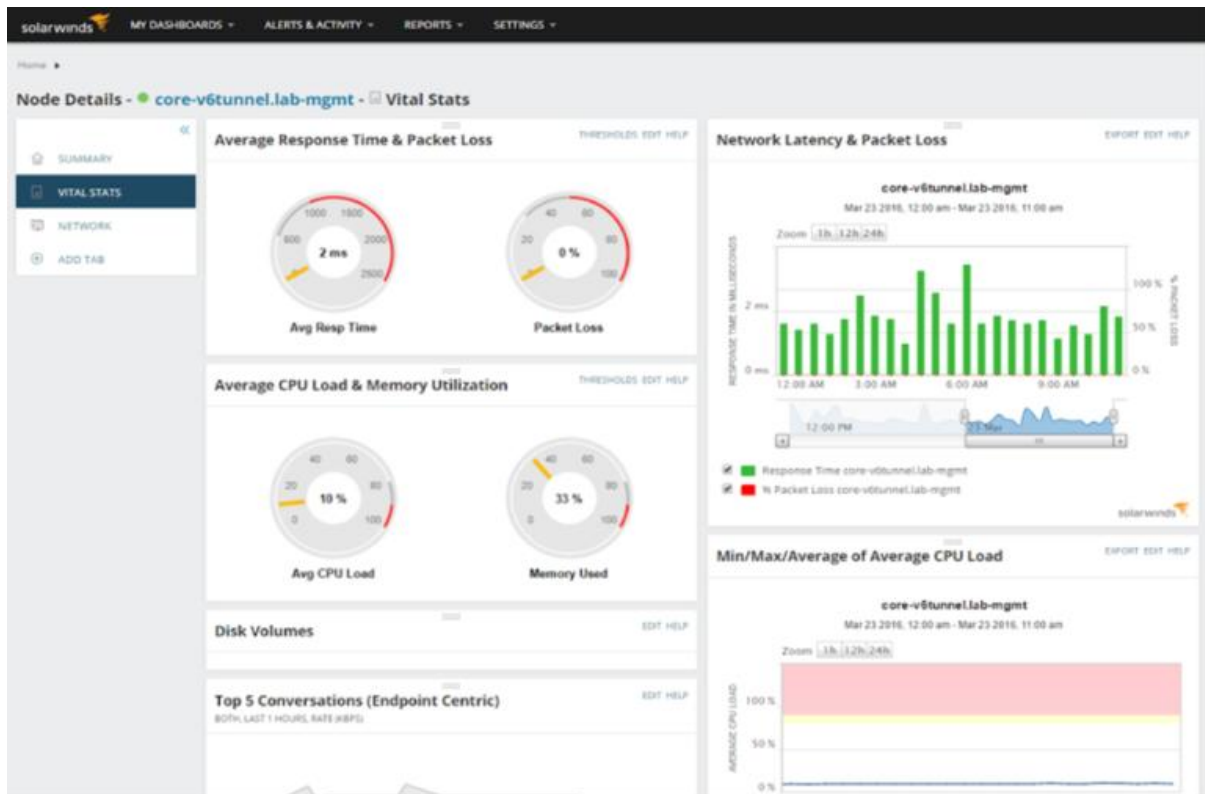


Figure 3.3 SolarWinds Network Performance Monitor Interface

2. SolarWinds NetFlow Traffic Analyzer (NTA): The SolarWinds NetFlow Traffic Analyzer (NTA) software is designed to be a powerful network traffic and bandwidth analysis tool. IT teams may use NTA to simply view total bandwidth use and follow flow for popular vendors like Cisco NetFlow v5 and v9, sFlow, Juniper, and IPFIX. The technology can assist administrators in identifying endpoints and apps that generate high traffic, allowing them to swiftly detect bandwidth hogs. Admins can expand network capacity or limit top talkers to prevent performance degradation depending on whether the bandwidth is being used for business purposes. NTA also provides charts, tables, and customisable network bandwidth reports to assist customers in better monitoring

current and historical traffic data, analysing bandwidth usage trends, and generating useful insights.

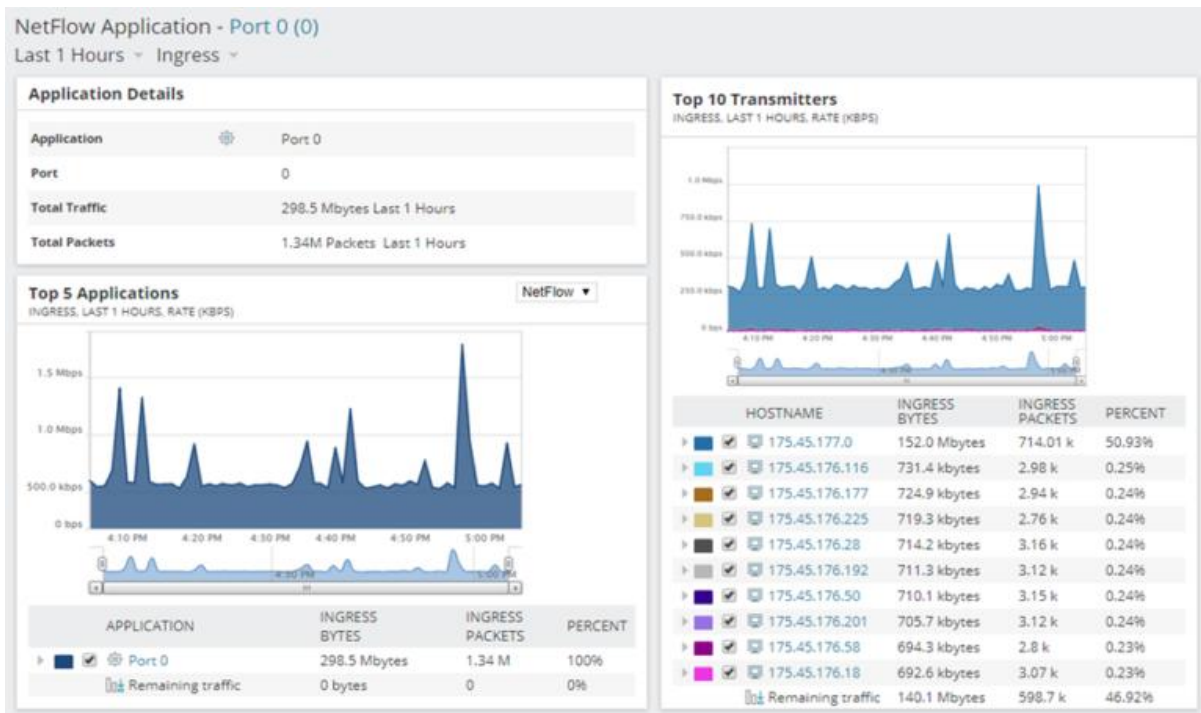


Figure 3.4 SolarWinds NetFlow Traffic Analyzer (NTA) Interface

3. Paessler PRTG Network Monitor: Paessler PRTG Network Monitor is intended to be an easy-to-use network monitoring tool that teams can use to acquire a comprehensive perspective of complicated IT networks. It can also assist network administrators in monitoring the bandwidth and resource usage of various devices and apps in order to provide lag-free performance and avoid delays. It can help with network investigation and diagnostics by using SNMP, NetFlow, and packet sniffing. PRTG Network Monitor is also designed to provide a comprehensive set of sensors for applications, operating systems, and hardware. Additionally,

network administrators can configure bespoke alarms to investigate unusual developments in network data flow.



Figure 3. 5 Paessler PRTG Network Monitor Interface

The methods presented in this section covers the network troubleshooting techniques available for use in troubleshooting a network. This can be employed in the UNIBEN wireless network structure. These methods are effective in network troubleshooting . Analytic tools and command-line tools can also be employed in the analysis process of the network conditions of the institution’s wireless network.

(Top Five Network Analysis Tools Top Five Network Analysis Tools, 2022)

3.3 Method For Network Optimisation

1. Standards For Wireless Networks

For the finest performance and dependability, invest in enterprise-class Wi-Fi Certified equipment that supports 802.11n (which was ratified in October 2009). 802.11n works at 2.4 and 5.0 gigahertz and has substantially higher throughput than the earlier 802.11a/b/g specifications.

2. Setting Up Your Access Point

To ensure wireless coverage across broad spaces, complex wireless network deployments necessitate a site study and a design that includes repeaters. To illustrate, consider a small office/home office scenario with one Wi-Fi access point (or router) running 802.11n at 2.4GHz. Place your access point as centrally as possible, off the ground and away from walls and heavy metal objects like filing cabinets.

3. Configuring Your Access Point's Wireless Standards

Access points are more stable and perform better when they only have to deal with one wireless standard at a time, therefore configure your access point to just support 802.11n. Naturally, all of your wifi devices must support 802.11n. Try to enable as few standards as feasible, such as 802.11n, or 802.11g and 802.11n if that isn't practicable.

4. Width Of The Channel

After you've configured the wireless standards on the access point, you can select between 20 and 40 megahertz channel widths. By selecting 40MHz, you

can achieve 300Mbps throughput by combining two 20MHz channels (referred to as channel bonding). However, not all 802.11n-certified devices provide a channel width of 40MHz at 2.4GHz.

(consultant et al., n.d.)

CHAPTER FOUR

RESULTS, ANALYSIS AND DISCUSSIONS

In the previous chapters, the concept of networking was reviewed. These concepts depicted the use of networks, network devices, key troubleshooting concepts, and analysis tools that played a vital role in describing a useful methodology for the operation of wireless network systems. A general overview of the wireless system used in the university of benin was also examined.

4.1 Testing and Results

This section focuses on the test and analysis of the wireless sections and proffers testing parameters commonly deployed in wireless networks. In this project research iPerf is utilised for testing. It provides information on bandwidth, loss, and other characteristics. It determines the quality of a network's device connections. It can be used to determine whether or not a link is appropriate for VoIP. It may plot the data it collects over time in order to see how network conditions evolve. A throughput Test tool will be utilised for performance testing. TamoSoft's Throughput Test is a free Performance Analysis software. TamoSoft's software will assist you in determining whether Quality of Service has been properly implemented throughout the network. After testing and analysing the wireless network connection, optimizers such as WLAN optimizers can be used to improve it.

General practises for improving and optimising wireless networks include, automating a reboot schedule, upgrading your router with a new antenna, disabling older wireless protocols, changing the channel width, keeping your router updated, experimenting with router location, optimising your router's channel settings, and switching the router to a different band.



Figure 4.1 inSSIDer Network Testing Interface

4.1.1 Wireless Network Speed Test

This test is carried out to test the speed of wifi connectivity used in a network. The most common speed tests used are provided by “fast.com” and “speedtest.net”. A WLAN testing is commonly used to provide an overview of the wireless system as well as an understanding of its health and operation. This

type of evaluation delves far further into your WLAN system than a single passive, active, or spectrum site study. A wireless LAN evaluation is a comprehensive approach that, in conjunction with other wireless site inspections, is used to analyse the setup of your wireless system in order to acquire a full knowledge of why you're encountering wifi performance issues.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATION

5.1 Conclusion

It's a good thing technology is evolving so quickly: demand for wireless networks is increasing even quicker. The ordinary individual no longer connects to a network simply through a computer. They can be linked on numerous computers, a smartphone, and a tablet at the same time. As the expanse of people using wireless networks grow especially, in specified area use like businesses, organisations, schools, there is a need for a fully optimised wireless network with a capacity to serve the number of persons in a designated area.

In conclusion, the project's goal was to undertake an extensive research into the wireless service at the University of Benin (UNIBEN) and decide ways to improve its functioning and usability. To accomplish this goal, the deployment of specific objectives that entered on how to, analyse the wireless network structure of UNIBEN, and assessment of the network providers of the institution's network was instigated. Review of networking testing techniques used in testing wireless networks, Review of network optimization strategies and deployment to optimise the institution's wireless network services.

5.2 Recommendation

No matter how sturdy an organisation's network may seem, best networking practices suggest periodic evaluation of the network setup and configuration is a necessity and this should be employed in the wireless network infrastructure available at the University of Benin.

REFERENCES

- A Guide to Network Troubleshooting*. (n.d.). Default. Retrieved December 4, 2022, from <https://www.comptia.org/content/guides/a-guide-to-network-troubleshooting>
- AB&R®. (2013, October 24). The Growing Importance of Wireless Networks. *AB&R*. <https://www.abr.com/growing-importance-wireless-networks/>
- ALOHAnet. (2022). In *Wikipedia*.
<https://en.wikipedia.org/w/index.php?title=ALOHAnet&oldid=112187978>
- Aideyan I. Winifred, K.B Erameh, “A Comparative Study of Hybrid Network (Powerline Communication and WiFi) and Wireless Network Using University of Benin’s Computer Engineering Laboratory as a Case Study”, *NIPES Journal of Science and Technology Research*, 2020.
- Bangan, X., Hischke, S. and Walke, B. “The role of ad hoc networking in future wireless communications”. *Int. Conf. on Commun. Technol. (ICCT 2003)*. 2: 1353-1358, 2003.
- Christian TchapanA, Hassnaa Moustafa, “Hybrid Wireless Networks: Applications, Architectures and New Perspectives”, Researchgate Conference Paper · October 2006.

C. Vlachou, S. Henri, and P. Thiran. “Electri-Fi Your Data: Measuring and Combining Power-Line Communications with Wi-Fi (Technical Report 210617)”. *Infoscience EPFL*, 2015.

Computer network | Definition & Types | Britannica. (n.d.). Retrieved December 4, 2022, from <https://www.britannica.com/technology/computer-network>

Computer Network Architecture—Javatpoint. (n.d.). Retrieved December 8, 2022, from <https://www.javatpoint.com/computer-network-architecture>

Computer Networking Terminology. (n.d.). Retrieved December 4, 2022, from https://www.tutorialspoint.com/basics_of_computer_science/basics_of_computer_science_networking_terminology.htm

consultant, R. S. T. R. S. is a technology, Management, T. S. in, server, security of M., & experience, client technologies H. is a M. C. S. E. with more than 15 years of. (n.d.). *6 Steps to Optimise Your Wireless Network*. Technology Solutions That Drive Government. Retrieved December 4, 2022, from <https://fedtechmagazine.com/article/2010/10/6-steps-optimize-your-wireless-network>

D. Helen, D. Arivazhagan, “Applications, Advantages and Challenges of Ad Hoc Network”, *Journal of Academia and Industrial Research (JAIR)* *Volume 2, Issue 8* January 2014

ECSA, S. S. (2020, March 19). How To Perform A Successful WiFi Penetration Test. *PurpleSec*. <https://purplesec.us/perform-wireless-penetration-test/>

Mesh Topology—An overview | ScienceDirect Topics. (n.d.). Retrieved December 8, 2022, from <https://www.sciencedirect.com/topics/computer-science/mesh-topology>

Hung-Yun Hsieh, Raghupathy Sivakumar, "Performance Comparison of Cellular and Multi-hop Wireless Networks: A Quantitative Study ", *ACM SIGMETRICS*, 2001

Network architecture. (2022). In *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Network_architecture&oldid=1112433926

Network Devices Explained. (n.d.). <https://Blog.Netwrix.Com/>. Retrieved December 4, 2022, from <https://blog.netwrix.com/2019/01/08/network-devices-explained/>

Network Devices (Hub, Repeater, Bridge, Switch, Router, Gateways and Brouter). (2015, July 8). *GeeksforGeeks*. <https://www.geeksforgeeks.org/network-devices-hub-repeater-bridge-switch-router-gateways/>

Network medium—Definition and more. (n.d.). The-Definition.Com. Retrieved December 8, 2022, from <https://the-definition.com/term/network-medium>

Network topology. (2022). In *Wikipedia*.

https://en.wikipedia.org/w/index.php?title=Network_topology&oldid=1125906977

OSI model. (2022). In *Wikipedia*.

https://en.wikipedia.org/w/index.php?title=OSI_model&oldid=1124194854

P. Tinnakorn Srisuphan, P. Purkayastha, and B. Mohanty. "Coverage and capacity analysis of hybrid home networks". In *IEEE International Conference on Computing, Networking and Communications (ICNC)*, 2014

Professor Anders Vastberg KTH , Professor Ki Wong Sung Telenor ”

Analysis of Wi-Fi performance data for a Wi-Fi throughput prediction approach” June 2017.

Raja Sattiraju, Hans D. Schotten, "Reliability Modeling, Analysis and Prediction of Wireless Mobile Communications", *IEEE 79th Vehicular Technology Conference (VTC Spring)*, 2014.

Roxana Zoican, Dan Galatchi, "Mobility in Hybrid Networks

Architectures", *proceedings of IEEE TELSIS*, 2005.

Top Five Network Analysis Tools Top Five Network Analysis Tools. (2022,

September 16). Software Reviews, Opinions, and Tips - DNSstuff.

<https://www.dnsstuff.com/network-analysis-tools-2>

Understanding the Networking Commands: A Walkthrough to Top 8

Commands | Simplilearn. (n.d.). Simplilearn.Com. Retrieved December

8, 2022, from <https://www.simplilearn.com/tutorials/cyber-security-tutorial/understanding-the-networking-commands>

Verma, E. P. (2016, February 23). *Types of Wireless networking technology and Comparison* | *Engineer's Portal*. <https://er.yuvayana.org/types-of-wireless-networking-technology-and-comparison/>

What Is Network Architecture? (n.d.). Cisco. Retrieved December 8, 2022, from <https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-network-architecture.html>

What is OSI Model | 7 Layers Explained | Imperva. (n.d.). *Learning Center*. Retrieved December 4, 2022, from <https://www.imperva.com/learn/application-security/osi-model/>

What is a Wireless Network? - Definition from Techopedia. (n.d.). Techopedia.Com. Retrieved December 4, 2022, from <http://www.techopedia.com/definition/26186/wireless-network>

Y.-J. Lin, H. A. Latchman, R. E. Newman, and S. Katar. A comparative performance study of wireless and power line networks. *Communications Magazine, IEEE*, 41(4):54–63, 2003.