UNIVERSITY OF GHANA

COLLEGE OF BASIC AND APPLIED SCIENCES

SCHOOL OF PHYSICAL AND MATHEMATICAL SCIENCES

DEPARTMENT OF COMPUTER SCIENCE

DEPLOYMENT AND STUDY OF VOIP-OVER-WLAN BASED INTRACOM ON UG CAMPUS

LINDA OTOO

JULY 2020

UNIVERSITY OF GHANA

COLLEGE OF BASIC AND APPLIED SCIENCES

SCHOOL OF PHYSICAL AND MATHEMATICAL SCIENCES

DEPARTMENT OF COMPUTER SCIENCE

DEPLOYMENT AND STUDY OF VOIP-OVER-WLAN BASED INTRACOM ON UG CAMPUS

BY

LINDA OTOO

(10187140)

THIS THESIS IS SUBMITTED TO THE UNIVERSITY OF GHANA, LEGON IN PARTIAL FULFILLMENT OF THE REQUIREMENT FOR THE AWARD OF MPHIL IN COMPUTER SCIENCE DEGREE

JULY 2020

DECLARATION

I LINDA OTOO declare that this thesis DEPLOYMENT AND A STUDY OF VOIP-OVER WLAN BASED INTRACOM ON UG CAMPUS is my own work carried out from research under the supervision of Prof. Ferdinand Kastriku of the Department of Computer Science University of Ghana, Legon as part of a requisite for the award of Master of Philosophy degree. I assert that the statements made and conclusions drawn are outcome of my research work except where due reference is made and affirm that this thesis has not been submitted for the award of any other degree of this university or elsewhere.

....

Linda Otoo

Date: **7th October, 2020**

This thesis has been submitted for our approval as supervisors:

Prof. Ferdinand A. Kastriku ....

(Principal supervisor)

Date: **7th October, 2020**

Jamal-DeenAbdulai (PhD)..

(Co-supervisor)

Date: **7th October, 2020**

ABSTRACT

Communication between people over a distance has evolved over the centuries from smoke signals, drum beating era to telephony and the current era of mobile wireless communication. The evolution of Internet Protocol has encouraged the introduction of VOIP systems on a converged data network and has indicated many benefits of the VOIP systems on a converged data network even though there are challenges as well. A test bed of VOIP-Over-WLAN was built at the Department of Computer Science of University of Ghana, Legon. The wireless environment of the location was surveyed to read values of Radio Frequency parameters that measure the performance of a resilient wireless network and quality of voice transmitted. The study has shown that the inherent challenges of the wireless LAN could be monitored and managed with wireless survey tools. Good results were obtained for the quality of voice transmitted at the various of the location. This is an indication that the VOIP system was properly designed and the wireless environment is ready for such a system.

DEDICATION

I dedicate this thesis to the few Kind Hearted people in the world today ready to share their Love to anyone anywhere at any time.

ACKNOWLEDGEMENT

I am grateful to my faithful God for all He is to me. And for the successful completion of this work.

I am thankful to my supervisors for their immense support and advice especially, Prof. Ferdinand A. Kastriku for the birth of the research idea, the guidelines, his stringent advice and encouragement. I am very grateful Sir.

My many thanks to my two Angels: Michael and Gabriel, colleagues and friends especially Clifford, Laurene, Wasilatu and Apphia Aidoo for their motivations and needed support.

To my family, I thank you so much. By you I am birthed anew each day. I am really honoured to have encountered all of you.

A big thank you to all my five mothers: Regina Annoh, Gertrude Aboagye, Dorcas Horatio-Larbie, Vera Dowuona and Rose Doris Boateng. God bless you richly.

TABLE OF CONTENT

LIST OF FIGURES

LISIT OF TABLES

LIST OF ACRONYMS AND ABBREVIATIONS

ACK	Acknowledgement
AVG RTT	Average Round Trip Time
DIFFSERV	Differentiated Services
BSS	Basic Service Set
CCQ	Client Connection Quality
CODEC	Code and Decode
CPU	Central Processing Unit
CSMA /CA	Carrier Sense Multiple Access with Collision Avoidance
CTS	Clear To Send
CU	Currently Unused
DS	Differentiated Service
DSCP	Differentiation Service Code Point
DSSS	Direct Sequencing Spread Spectrum
FHSS	Frequency Hopping Spread Spectrum
GSM	Global System for Mobile Communication
IAX	Inter-Asterisk Exchange Protocol
IBSS	Independent Basic Service Set
ICMP	Internet Control Message
ICWL	Intra-Campus Wireless LAN
IETF	Internet Engineering Task Force
IP	Internet Protocol
IPSEC	Internet Protocol Security
INTSERV	Integrated Services
ISM	Industrial Scientific and Medical
ITU-T	International Telecommunication Union
LAN	Local Area Network
LOS	Line Of Sight
MMS	Multimedia Messaging Service
MOS	Mean Opinion Scores
MPLS	Multiprotocol Label Switching
NCA	National Communication Authority

OSI	Open Systems Interconnection
PBX	Private Branch Exchange
PHB	Per-Hob Behavior
PING	Packet Internet Groper
PoE	Power over Ethernet
POTS	Plain Old Telephone Service
PSTN	Public Switch Telephone Networks
QoS	Quality of Service
RF	Radio Frequency
RSVP	Resource Reservation Protocol
RTP	Real-Time Transport Protocol
RTS	Request To Send
SDP	Signal Description Protocol
SIP	Session Initiation Protocol
SMS	Short Message Service
SNR	Signal to Noise Ratio
SS	Signal to Noise Ratio
TCP	Transmission Control Protocol
TOS	Type of Service
TTL	The Time To Live
UA	User Agent
UDP	User Datagram Protocol
UG	University of Ghana, Legon
VLAN	Virtual Local Area Network
VOIP	Voice over Internet Protocol
VPN	Virtual Private Network
WAP	Wireless Access Point
WEP	Wi-Fi Equivalent Privacy
WLAN	Wireless Local Area Network
WNIC	Wireless Network Interface Card
WPA	Wi-Fi Protected Access
3G	Third Generations
4G	Fourth Generations

CHAPTER 1: INTRODUCTION

This chapter explains the background, motivation and objectives of the research study. The Chapter also outlines and discusses the research questions, limitations and contributions of the study. Finally, the overall organization of the study is described.

1.1 Background of the Study

The University of Ghana (UG), is the premier and the largest university in Ghana. It was established for the purpose of providing and promoting university education, learning and research. UG is run on a collegiate system and comprises of four main colleges and a school of graduate studies(University of Ghana 2016). In addition to the colleges, the University has other faculties and several research institutions and centres for learning and research. The University has fourteen (14) residence halls and three (3) hostels for students' accommodations and several residences for staff. These buildings mentioned earlier are all decorated with tall ornamental trees and flowers to beautify and produce oxygen for the living organisms on the Campus. Social amenities such as fire service station, police station and hospital are all on UG campus. Currently, the University has a student population of about 40,000 and staff population of approximately 2,000 (University of Ghana 2016).

These facilities mentioned earlier are of several metres spatially distant from each other and there is a need for people within this localized community to communicate across several distances with ease.

Communication on UG campus over the years till now has been enabled by the Telecommunications networks, particularly the Public Switch Telephone Networks (PSTN), the Global System for Mobile Communication (GSM) enabled cell phones, and more recently the 3^{rd} and 4^{th}Generation (3G/4G) smart phones. The high tariffs and other extensive charges of these services, especially when the parties involved are on different networks have made it very expensive for students to afford. Given that the students live in a community may be reasonably assumed that a considerable number of the students mostly communicate locally within the confinement of UG Community. In recent times, there have been some initiatives and campaigns by some telecom firms advertising for cheaper and free communication services. These campaigns only pull subscribers from other communications network companies which end up growing a large pool of clientele and later escalating their charges to enormous heights. To this end, having a free-access to intra-mobile communication on UG campus will be a great relief to students, and to a large extent the whole UG community.

The access to a free intra - mobile communication service on the UG campus is possible using Voice over Internet Protocol (VOIP) over Wireless Local Area Network (wireless LAN), that is, VOIP-over-wireless-LAN. This VOIP technology emerged as a result of the global evolution of the Internet and the widespread growth of networks, making the Internet an integral part of our daily life and causing a rise in demand of the Internet applications (El-metwally 2012).

VOIP is the transmission of voice traffic through the Internet or private data network based on packet switch instead of the traditional public switch network which is based on circuit-switching (Mupparapu 2008). When using VOIP the voice is encoded appropriately at the sender's end of the communication channel and sent as packets through the data network. After the data arrives at the receiver's end, it is decoded and transformed back into voice signal (Scores 2013)(Voice et al. 1974).
The data network of the VOIP transmissions could be a wired or wireless network. Wireless LANs are being used widely to deploy VOIP technology currently since the number of mobile users has widely increased (Banerji and Chowdhury 2013). WLANs are a key element

in any location where access to network resources is vital at anytime and anywhere (Beuran 2006). Using VOIP on wireless LANs enables support of mobile devices within the campus. Although this seems attractive and promising, it only brings out the specific issues related to WLAN. This may discourage many people to think of deploying VOIP over WLAN even though it is very cost effective.

1.2 Problem Statement

VOIP refers to the real-time transmissions of voice signals as packetized data across networks by using the Internet Protocol (Kumar 2006). This technology is a current potential alternative to the various traditional means of communications on the UG campus providing a versatile, flexible and cost-effective solution to voice communications (Benefits of Using VoIP Technology - 2015). The technology is mostly deployed on a converged data network which could be wired or wireless to discourage waste of resources.

The Internet Protocol (IP) which is the fundamental protocol for the VOIP technology was originally designed for non-real-time data transmissions (Toral-Cruz et al. 2011). IP just offers a "best-effort" service with no Quality of Service guarantee (Behrouz A.Forouzan 2013). When the data network is converged to reduce or prevent wastage of resources it becomes the very reason why voice quality degrades since different applications on the network have different resources requirement. Real-time applications like VOIP are sensitive to delay whereas transmissions are very resilient (Voice et al. 1974). The contention of network resources in the converged network

coupled with the challenges of the "best-effort" service provided by the IP boosts the voice quality challenges in voice communications of the VOIP technology. This implies that contention must be managed by means of QoS mechanisms in order to ensure efficient management of resources to enable good voice quality in VOIP system (Beuran 2006)(Behrouz A.Forouzan 2013).

The traditional VOIP system on a converged data wired network have had many of their challenges resolved by researchers with QoS techniques. However, the underlying data network to enable mobility and flexibility of the voice transmission within the coverage area of the VOIP system is the wireless LAN. This is a significant network that contributes to the success of the VOIP technology with flexibility and mobility in all locations but the general inherent challenges and the spontaneous behaviour of the wireless technology are strong forces that affect the quality of voice transmitted in a VOIP system. VOIP systems, when deployed on a converged data network, ensure competition of resources between data and voice packets. This together with the challenges of best-effort services and the inherent challenges of the wireless network as the main network medium for the voice transmission in VOIP system is enough a challenge to prevent one from installing the VOIP system to provide cheap or free communications services.

To fully enjoy the benefits of the VOIP over a wireless network, there is the need to alleviate competitions of resources between the data packets and the voice packets on a converged network. Over the years, researchers have discovered some techniques that are used on the converged network so resources could be managed properly to avoid competitions. Among such techniques are the use of VLAN, MPLS, INTSERV and the DIFFSERV (Behrouz A.Forouzan 2013)These techniques are good only to some extent since they are with various forms of challenges at the various layers of the OSI model of the networking framework. Again, some researchers have suggested the use of separate data network for data and voice packets (“Consider Separating Your Data and VoIP Networks,” 2012; “Help How to separate

VOIP and data networks while only using one router? - Spiceworks," 2016; "Pros & Cons: Keeping voice & data on separate networks," 2013.; "The Importance of VLAN Segmentation for Voice and Data," 2014). It has been argued by other researchers that the suggestion to use separate networks for data and voice within the same localized area is not cost effective and aids wastage of resources ("Internet Telephony," 2018; "Voice over IP," 2018; "VoIP project, one network or two? - Luminet," 2017).

Researchers of the VOIP technology are yet to see an excellent technique to counter the known challenges of the VOIP system deployed over a converged wireless data network with the least difficulty and challenge (Kazemitabar, H .Ahmed, S .Nisar, K .Said, A.Hasbullah 2010; Mehdi 2009). However, cost expensive nature of a VOIP system deployed over a separate data network needs to be reviewed again since cost expensiveness is subjective.

Examining the high tariffs of the existing GSM communication services of local calls within the Campus, on the average, the current rate per charge on a minute call from one network to another is twelve (12) pesewas (Airtel Ghana | Legacy Tariff 2017). There are five (5) communication networks in the country, two of them charge thirteen (13) pesewas per minute on-call air time("Tariffs," 2014; "Vodafone Ghana | Vodafone Call rate / Tariff,"2014.), and the other two charges eleven (11) pesewas and the last network charges ten (10) pesewas (4/9 New Tariffs (GHC) Per Minute | Tigo Ghana 2014). Statistically, if on an average each student on Legon Campus makes five (5) calls locally (not considering MMS and SMS text messages) within the campus each day, the total charges for the 12 months of the year would accrue to:

- Calculations for calls within different networks

  0.12 pesewas * 5 = 0.60 pesewas

0.60 pesewas * 20, 000 (half the student's population) = GHS 12, 000.00 daily

GHS 12,000.00 * 30 (days of a month) = GHS 360,000.00

GHS 360,000.00 * 12 (months of a year) = GHS 4,320,000.00 a year.

The above mathematical illustration considers only portion of the student population and it excludes staff and other auxiliary members of the University of Ghana.

In order to address the cost associated with communication services on the Campus, a platform for VOIP system is to be built over a private wireless LAN to examine how well the system will behave on the wireless network on the UG campus.

The students and the general populace including the University as an institution would benefit substantially from the adoption of this technology. Students will have time to concentrate on their studies and academic work, as communication is fully facilitated at a no-cost rate locally; they will not be burdened with charges from phone calls. This could go a long way to boost research work and efficient collaboration to complete planned projects. Revenues that would have been used to pay communication bills could be redirected to other need-based projects within the university. In addition, by being the first university in the country to adopt this solution, University of Ghana, Legon stands to achieve significant recognition as an institutional pace-setter in the areas of technology, developmental value, and tech-driven solutions.

1.3 Significance of the Study

The findings of this study will aid in identifying which of the known inherent challenges of the WLAN for the VOIP system has the least effect whiles taking a critical look at the landscape of the campus, its population at different times and the devices used within the campus at the various time. The reason why those parameters could be affected on the UG campus and the countermeasures to be used to ensure good quality of voice in the VOIP communication services within the campus.

Again, the study will be used in providing very cheap if not free means of communication for faculty and staff on the University of Ghana campus (Wei, Bouslimani, and Sellal 2012). This proactive measure would make the University of Ghana one of the elitist places to do most complex research-based projects, even in Africa, once this technology is harnessed efficiently. This technology would allow the various adjunct offices and extended administrative bodies within the University also cut down on the cost of communication. This lamplight could cause a greater demand from other universities and organizations to seek to use this means of communication in their localized office buildings from the University of Ghana.

The results of the study will go a long way to create awareness of an opportunity to save on cost within other institutions in the country and this study would be the standard. Universities and other organizations that apply the recommended approach derived from the results of this study would be able to access free means of communication on their localized networked buildings. There would be terms and conditions attached, with respect to considerations to the department and the researcher on the findings from this study.

1.4 Scope of the Study

In the deployment of VOIP-over-wireless-LAN on the campus, there was the need to first build an Intra-Campus Wireless LAN (ICWL). ICWL is the sole network upon which the VOIP would be deployed on the University of Ghana campus; the computer science department has been designated as a Centre for the study and experimental works, thus, the need to setup a wireless LAN at this Centre. Asterisk Private Branch Exchange (PBX) was built on a Personal computer on the wireless LAN. Then this established network will be extended through wireless access points to the other parts of the University. This would be done by the use of devices with the following characteristics:

- flexible to deploy and maintain
- very cost-effective on operational expenditure and devices
- low power consumption (POE)

Several RF surveys were conducted to read parameters that measure the quality of voice transmitted for the analysis and assessed the general wireless environment of the Centre. The VOIP test bed was also assessed at various locations of the Centre and values for jitter, packet loss, etc. were mapped with SNR, Noise floor, distance, etc.

1.5 Objectives of the Study

i. The main objective of this study is to design and implement an intra-mobile communication network based on VOIP-over-wireless-LAN test bed on UG campus and to examine if the proposed VOIP-over-wireless-LAN system is feasible to adopt on UG-Legon, campus.

ii. To determine how the inherent challenges of wireless technology can be managed to support the VOIP-over-wireless-LAN system.

iii. To compare the performance of VOIP-over-wireless-LAN to GSM.

1.6 Research Questions

To achieve the objectives mentioned in Section 1.5, the study seeks to answer the following research questions:

i. What are the main components and determinants that ensure quality performance of VOIP-over-wireless–LAN?

ii. To what extent is the wireless LAN technology suitable for the VOIP application?

iii. What are the inherent challenges of the wireless LAN technology that affects the parameters that measure the quality of VOIP?

1.7 Limitations of the Study

This primarily should have provided cheap communication services at the various locations of the entire UG campus was not achieved as a result of insufficient funds for the studies as well as the needed time and logistics to build a whole new campus wireless network for the VOIP system. Hence a portion of the campus was examined with the VOIP test bed to provide the free means of communication services at the centre.

1.8 Contribution of the Study

The study successfully achieved the aim of deploying test bed at the Centre and analyzed its general performance. In Section 1.5, we discussed that the basic protocol upon which the VOIP operate is the IP and IP offers Best Effort service and does not guarantee quality of service, the study has shown how well the VOIP technology will behave on a wireless LAN deprived of Internet connectivity to provide mobility of the voice communication service to the centre managing the inherent challenges of the wireless network.

1.9 Organization of the Study

This Chapter presented the introduction of the study, which includes the background, problem statement, significance, and objectives of the study. In addition, the research questions that were addressed, and the scope and limitations of the study were presented. The remainder of this thesis is organized as follows. Chapter 2 reviews wireless LAN communication technology, VOIP, VOIP-over-wireless-LAN and PBX. Chapter 3 describes the proposed system, that is, VOIP-over-wireless-LAN, and its implementation. Chapter 4 presents and discuss the experimental results, and Chapter 5 presents the conclusion and future work of the study.

CHAPTER 2: LITERATURE REVIEW

The chapter reviews wireless communication technology, Electromagnetic waves, VOIP systems and the underlying protocols, techniques and architectures used in designing a wireless network for VOIP systems. The chapter again presents a proposed VOIP test bed architecture for the Computer Science department at UG-Legon Campus.

2.1 Wireless Communication Technology

Communication between people over long distances has evolved over the centuries from the initial wireless systems of smoke signals, drum beating era to the wired systems of telegraph and telephone, and to the current era of mobile wireless communication (Kennedy, 2011; Woller&Gebhardt, 2012). As such, currently, we are seeing a full cycle of wireless technology (i.e. from a smoke signal and drums to mobile wireless) through wired (telegraphy and telephony) and back to wireless (use of radio frequency signals) in human history. This ancient technology where signals are transmitted over a distance without the assistance of wires or cables through communicating devices is presently the technology which refers to the transmission of electromagnetic signals from a device to another without wires, cables or electrical conductors (Sanguino& Roberts, 2011). In this form of communication, signals are normally broadcasted through the air from a source point. And these signals are made available to devices capable of receiving them (Sinclair, 1997). This form of communication is of various types depending on the distance covered by the wireless network and the range of frequency used (Gast, 2005; Sinclair, 1997; Woller&Gebhardt, 2012).

To better understand the wireless communication technology, we would discuss the electromagnetic wave, architecture and techniques of the technology.

2.1.1 Electromagnetic Wave

Energy is transferred from one point to another in waves and are mostly measured by parameters such as amplitude, frequency and wavelength (“BBC - Standard Grade Bitesize Physics - Communication using waves : Revision, Page 5,” 2014; Pain, 2005). The two main forms of waves are the mechanical and electromagnetic waves (“Types of Waves, Mechanical Waves & Electromagnetic Waves • SSP,” 2014). Electromagnetic wave propagation is mostly done through space or material medium whereas, in a mechanical wave, propagation is done only through a material medium (NASA, 2010). An electromagnetic wave is a special type of wave and the more reason why audio signals are converted to this form of a wave as it can travel through outer space (vacuum) as well as a material medium. These electromagnetic waves are formed by the vibration of an electric charge. This vibration creates a wave which has both electric and a magnetic component. Examples of electromagnetic waves are radio wave, infrared microwave, X-rays and gamma-rays.

These waves have several uses including communication, cooking, imaging, sensing. For communications, radio waves transmissions are used. In radio wave transmission, audio signals are broadcast from a source point to the receiver. Audio signals are of low frequencies (20HZ-20kHz) and cannot be directly propagated in the air over an appreciable distance even when converted to electrical energy (Nagar & Delhi-, 2016). This is because the energy of a wave is directly proportional to the frequency of the wave (Nagar & Delhi-, 2016). Therefore, at audio frequencies (20HZ-20kHz) the signal power is quite small and radiation is not practicable (Communications & Authority, 2006; Nagar & Delhi-, 2016). Radiation of electrical energy of an audio signal is only practicable at frequencies above 20 kHz hence the need to modulate the signal. At low frequencies, bigger antennas are required for signal reception as such also calls for modulation of the low frequency signals. Modulation is the process of changing some characteristic (amplitude, frequency or phase) of a carrier wave in accordance with the intensity of the signal (Nagar & Delhi-, 2016). In view of this, it is important to modulate an audio signal and convert the signal to an electromagnetic wave to enable communication over an appreciable distance and through a vacuum in wireless communication.

2.1.2 Architecture and Techniques

There is a need for a wireless network to be built before wireless communication can be established when building a mass communication system. However, for any simple wireless communication system, a source point and a receiver are just needed. The components that build the wireless network are known as stations (Nagar & Delhi-, 2016). A station could be a Wireless Access Point (WAP) or a Client (computer, phone, etc.). These stations are equipped with a Wireless Network Interface Card (WNIC) (Lammle, 2008). A wireless network could be made of one or more access point(s) and this is said to be a Basic Service Set (BSS) and a wireless network without an access point is known as the Independent Basic Service Set (IBSS) or ad-hoc wireless network (Lammle, 2008).

Wireless Access Point (WAP)

This serves as the base station of the wireless network which enables transmission and reception of radio waves for the wireless-enabled device to communicate (Sinclair, 1997).

WAP enables the connection of all the wireless devices together. It normally has an antenna for reception and transmission (Sanguino& Roberts, 2011).

Wireless Network Interface Card (WNIC)

This is a controller installed in the host device to enable network connections. This also has an antenna for both transmission and reception (McCabe, 2007).

Wireless Antenna

This is sometimes referred to as aerial. An antenna is an electronic device used for transmission and reception of data in the form of an electromagnetic wave (Michigan, 2002). There are two (2) major classifications of an antenna associated with radio wave based wireless network. These are the Omni directional and Directional Antenna. This classification is based on the antenna's ability to transmit signals in all directions or focused direction. Antennae can be further broken down by their individual style of construction such as Omni, dipole, flat panel, Yagi and parabolic dish (Stallings, 1997). Building a resilient wireless network for wireless communication is very essential to ensure reliable communication services.

Wireless Transmission

In wireless communication, the atmosphere serves as the media for transmission (Ji& Technology, 2017). This media is limitless, which means that there is no single pathway for the signal in the atmosphere. However, every wireless signal needs a dedicated channel so the transmission would be enabled (Jalendry&Verma, 2015; Ji& Technology, 2017; Kazemitabar). The channel is set in the WAP and the WNIC automatically tunes its transceiver to the frequency of the WAP. This form of transmission uses the Industrial, Scientific and Medical (ISM) frequency bands. There are two main forms of the ISM band. They are the 2.4GHZ and the 5GHZ frequency bands. These bands are under both international and local regulatory authorities, the ITU-T and NCA respectively. The IEEE 802.11b/g standards define a total number of 14 channels in the 2.4GHZ band. It has been identified that two or more transmitters cannot be used simultaneously to avoid Radio Frequency interferences. Ideally, only three channels can be used simultaneously within the 2.4GHZ band. In knowing the individual channels in the 2.4GHZ band, it enables one to make the right choice of channel to be used in a particular time at a particular wireless environment.

Wireless Transmission Modes

In wireless communication technology, there are three (3) main techniques that describe how the signals are transmitted in the network. The classifications of these techniques are dependent on the rate at which signals are transmitted and retransmitted (in the case of RF interferences) and the type of frequency band used. Single-frequency, Spread Spectrum and orthogonal frequency-division multiplexing are the techniques used in wireless communication for transmission of signals. This research will limit the studies to only Spread Spectrum as the technique for transmissions in the 2.4GHZ frequency band. The spread spectrum technique divides the frequency band into channels. Multiples channels are used simultaneously or sequentially in this technique. When multiple channels are simultaneously used, the technique is said to be Frequency Hopping and it's referred to as Direct Sequential Spread Spectrum for sequentially multiple channels usage.

Frequency Hopping Spread Spectrum (FHSS)

This technique is known by its own name since data packets hop from one channel to another in a set pattern determined by an algorithm. The main reason for the usage of this technique is to avoid interferences even though it's limited to a maximum of a 2Mbps.

Direct Sequencing Spread Spectrum (DSSS)

This technique divides the unlicensed frequency band (2.4GHZ) into several overlapping channels with only three channels not overlapping so could be used simultaneously. The data rate for this technique is mostly 11Mbps. Wireless network mostly uses Direct sequencing since it has a better rate at which data is transmitted compared to FHSS even though mostly affected by RF interference.

Wireless Media Access Control (CSMA/CA)

It has been established earlier that the media for transmission of signals from a source point is the airwave and much unlimited therefore the need to manage access to media (Lammle, 2008). The main protocol used in the management of access to a channel in a wireless environment is the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) (Sanguino& Roberts, 2011; Stallings, 1997). In such a medium, a client usually sends a request to send (RTS), waits for either a clear to send (CTS) or busy signal from the WAP. This is repeated until the client is cleared to send data. The WAP in return sends an acknowledgment (ACK) after the data has been received by the client. This media access control protocol is very useful to wireless communication technology since it solves the broadcast storms, hidden terminal and exposed terminal problem known in a wired network that uses the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) protocol (Beuran, 2006; Cisco Systems, 2015).

Wireless Security

Wireless security consists of techniques and methods used in the prevention of unauthorized access or damage to wireless network devices and data. Wireless security is important since WLAN radio waves are broadcasted and any wireless device within the environment could have access. Hence, the need to authenticate privatized and authorized access to the wireless LAN so that the right users will have access and signals would be protected from unauthorized users. The common types of wireless security are Wired Equivalent Privacy

(WEP) and WIFI Protected Access (WPA) (Ji& Technology, 2017) but WPA is mostly preferred since WEP has been identified to be weak (HKSAR, 2008).

2.2 VOIP Technology

VOIP is the transmission of voice traffic through the Internet or private data network based on packet switch instead of the traditional public switch network which is based on circuit-switch. In VoIP, communication can be established in three main ways: computer-to-computer, computer-to-phone and phone-to-phone. The main aim of VoIP system is to provide an alternative service to other services that are either very hard or very expensive to implement using the traditional PSTN; and to enable the integration of voice, video and data applications on the same network. There are several protocols and technique enable the usage of VOIP. The traditional VOIP architecture is shown in figure 2.1 and its details are discussed below.

2.2.1 Switching

Voice transmission for some time now has always been through the PSTN. The PSTN uses the Circuit Switch network in Voice transmission. A switch is a network device that provides a connection between two or more devices, thereby avoiding the need for permanent and dedicated lines between individual end devices. Switching is said to provide the means through which a signal can be transmitted from one source device to a destination device without the need for a dedicated and permanent connection. Two forms of switching are usually employed, a packet switch and circuit switch. In a circuit switch network, there is the provision of a dedicated communication channel for the transmission of the voice signal.

There are three main phases in circuit switch networks:

1. Connection setup: data transmission can take place only after a connection has been established between the source and destination devices. The source device makes a reservation of resources to be used.
2. Data transfer: the audio signals are transmitted from the source device to the destination device using the dedicated resources.
3. Connection teardown: after transmission between the source and destination station is over, the connection is dismantled.

In packet switching, messages are fragmented into suitable block size and are encapsulated with headers to enable transmission. There is no resource allocation for a packet. This means that there is no reserved bandwidth on the links, and there is no scheduled processing time for each packet. Resources are allocated on demand. The allocation is done on a first-come-first-served basis. When a switch receives a packet, no matter what the source or destination is, the packet must wait if there are other packets being processed.

Over the years, voice transmission has only been possible on the traditional PSTN and not on cellular networks. PSTN also known as Plain Old Telephone Service POTS uses circuit-switched networks for voice transmission. Circuit switch has been very efficient in voice transmission since it was specifically developed for voice communication. PSTN is well engineered for voice transmission and it is very reliable with 99.999% availability of service. It is very secure, excellent in voice transmission but requires much bandwidth (about 64kbs) for transmission.

2.2.2 Reasons for VoIP Adoption

Even though circuit networks for voice communication has been very efficient, it is unable to deal with new and emerging applications services enabled by advances in technology such as are offline, busy, online and instant messages, etc. Additionally, PSTN is expensive and not cost effective. There are also major infrastructural costs associated with implementing PSTN. The main aim of a VoIP system is to provide services that are either very hard or very expensive to implement using the traditional PSTN (Lazzez, 2013). Again, PSTN is expensive and people nowadays would want to talk much more on phone and communicate in myriad ways like the email, etc (Lazzez, 2013). PSTN is just not suitable. VoIP also allows for the integration of voice, video and data applications on the same network. This integration allows quicker integration of multiple services improving the way users collaborate which enhance productivity.

Figure 2.1: The Traditional VoIP Architecture

VoIP as defined earlier is the transmission of voice signals over Internet Protocol. The main components of the traditional VOIP architecture are the following:

- Client devices: These are electronic devices with which clients or users place and receive calls.
- VOIP gateway: This is a device that serves as a bridge between the IP network and the PSTN network. It converts telephony traffic from the PSTN network into IP packets for transmission over an IP network. When the traffic is from the IP network, it converts IP packets into telephony traffic for transmission across the PSTN network.
- Router: This is a network device that joins the networks together, it forwards packets from one network to another network.

- IP network: This is the communication network that uses Internet Protocol to send and receive data between the end devices.
- Signaling protocol: This enables the communicating end users to signal themselves for the connection set-up, maintenance and termination.

VoIP is deployed either on centralized (client/server) architecture or decentralized (peer-to-peer) architecture or both. Client/Server architecture was the most common form of architecture used until researchers identified certain challenges such as the server could be down and nothing works again. Deployment of Peer to Peer architecture in VoIP manages to provide some solutions for the challenges in client/server architecture (Butcher, Li, &Guo, 2007). However, Peer to Peer architecture also has its own challenges as well. VoIP requires a means for prospective communication devices to locate each other and to signal the other party their desire to communicate. Signaling protocols are therefore needed for the establishment of VoIP communication among the end system devices named above. Some of the popular signaling protocols are H323 and SIP (Butcher et al., 2007)

2.2.3 Signaling Protocol

The main purpose of the signal protocol in VOIP is to provide the under listed functions:

1. Session establishment: the receiver device decides to accept, reject or redirect the call.
2. User location: the caller first has to find the location of the destination device
3. Call participant management: it allows endpoints to join or leave an existing session.

4. Session negotiation: the endpoints involved in the call should concur upon a set of properties for the session. (Latif, 2007)

Session Initiation Protocol (SIP)

Session Initiation Protocol is an application layer protocol designed for signaling and controlling multimedia sessions. It is designed by the Internet Engineering Task Force (IETF) to provide services of establishing, maintaining and terminating a call. This protocol relies on peer-to-peer architecture whereas the services provided are on request and response basis. The peers in the session are called User Agents (UA) (BehrouzA.Forouzan, 2013) (Aigbe&Akpojaro, 2014). A UA can function either as a client that initiates the SIP request or as a server that listens to request from clients and responds accordingly. SIP is a protocol that is made of a message header and a body. It is designed to run on UDP, TCP or SCTP using the port 5060. SIP just as any other signaling protocol provides the services of signaling protocol discussed earlier. The protocol's messages are of two main types; Request and Response messages. Some of the Request messages designed by the Internet Engineering Task Force (IETF) are discussed below (Aigbe&Akpojaro, 2014; Wang, Member, Liew, Member, & Li, 2005). In addition to SIP, the Signal Description Protocol (SDP) is used for the negotiation of parameters such as CODEC and media type.

Table 2.1: The types of messages used in the signal protocol

Request Message	Response Message
Invite	Information Responses
Ack	Successful Responses

Options	Redirection
Cancel	Client Failure
Register	Server Failure
Bye	Global Failure

Source: https://www.3cx.com/pbx/sip-methods

H323 Protocols

H323 is a collection of protocols standardized by the International Telecommunication Union (ITU-T) in 1996 for voice and video transmission over the internet protocol. Table 2.2 defines the individual protocols that form the H323 protocol suite (Arora, 2000; Latif, 2007).

Table 2.2: The types of the protocol implemented in the H323 protocol set and their use

Protocol	Use
G.71 or G.723.1	For compression of voice signals
Q.931	Is used for establishing and terminating connections

H223 (also known as RAS)	Registration/Admission/Status defines call setup messages and procedures used to establish a call as well as messages used for users' registration and call admission
H235	Defines security profiles for the H323 protocol suite such as authentication, message integrity, signature security and voice encryption
H450	Defines additional services like call hold, call waiting, call forwarding, etc

Source: ITU-T Recommendation H.225.0 was revised by ITU-T Study Group 16 (2001-2004)

CODEC

This is a combination of two words Code and Decode (CODEC). It is a computer program that uses compression and decompression algorithms to either shrink data stream to reduce transmission bandwidth and storage space at the ingress of the network or to decompress a compacted data to be received at the endpoint of the network (Toral-Cruz, Argaez-Xool, Estrada-Vargas, & Torres-Rom, 2011). There are many ITU-T codecs but the popular ones for VOIP are G.711, G.729, and G.723.1 (K.Mishra, K. Singh, & Patel, 2012).

Codecs are very important in VoIP since they define the voice quality, the required network bandwidth utilization, the storage space required for transmission of the stored audio signal and computation requirements, etc (K.Mishra et al., 2012). When talking about the VoIP codecs there is the need to talk about Mean Opinion Score (MOS) used to measure the quality of the audio signal after its compression (Hersent, Petit, &Gurle, 2005). These score standardized by the ITU-T ranges from 1-5 where 1 is the worst and 5 is the best (Cisco, 2007).

2.2.4 Transmission Protocols

In addition to the signaling protocol in VoIP, there are the transmission protocols that enable packet delivery in VoIP. These protocols are the RTP, RTCP, TCP and UDP (Latif, 2007).

Transmission Control Protocol (TCP)

The TCP is known to be the most widely used transport protocol on the Internet. However, there are some challenges to this protocol when dealing with real-time traffic. The challenges may include the inbuilt-retransmission mechanisms of the TCP which may not be useful for real-time traffic. Again, TCP does not support the transmission of timely information which is most needful to real-time traffic. UDP which is the other most used transport protocol does not also include timing information and therefore the need for a new protocol RTP to enable delivery of real-time data (Arora, 2000; BehrouzA.Forouzan, 2013).

Real-Time Transport Protocol (RTP)

The RTP is a protocol that specifies the means for the transmission of multimedia data over network services. RTP was originally designed by the IETF as a transport protocol and not a transport layer protocol. RTP is mostly used upon the transport layer protocol User Datagram Protocol (UDP) for the transmission of data that are with real-time characteristics i.e. generally delay sensitive data. It is important to note that RTP does not guarantee real-time delivery of voice data since it is dependent on network characteristics. RTP defines a standardized packet format for delivering audio and video over IP networks. RTP is used in addition to a control protocol, the Real-Time Transport Protocol (RTCP) which enables the monitoring of data delivery over a large network.

UDP

User Datagram Protocol is a connectionless and unreliable protocol of the transport layer designed for network applications that have a very low tolerance to latency and packet loss. This protocol provides services to the application layer and services from the network layer with the use of port numbers. UDP enables the process to process communication. To send a message from the client program to the server program, the UDP provides the services of encapsulation and de-capsulation of the request and response messages respectively. Encapsulation occurs at the source device when a client has a request message to be transmitted; it passes the message to the transport layer along with a pair of socket address and some other information. Packets upon reaching its destination are de-capsulated. When the request message arrives and the UDP delivers the message to the process running at the application layer, the sender socket address is passed in case it needs to respond to the message received (Arora, 2000; BehrouzA.Forouzan, 2013; Latif, 2007). UDP is not known to provide guaranteed services. This protocol is connectionless hence jitter (variations indelay) is a known common challenge. UDP does not provide error control, flow control and congestion control provided by other transport layer protocols (BehrouzA.Forouzan, 2013).

Internet Protocol (IP)

IP is the main protocol of the network layer. It defines the means by which packets are transmitted from host to host. This protocol provides best-effort services from the data-link layer to the transport layer. Best effort means that IP does not guarantee delivery i.e. IP packets can be corrupted, be lost or arrive in an out of order fashion or even delay in arriving at the destination. IP provides the following services: packetization, fragmentation, and packets delivery at the network layer. Figure 2.2 shows the format of a packet and its headers.

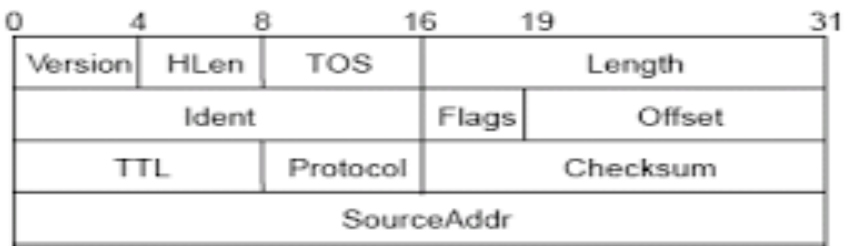


Figure 2.2: Datagram format

2.2.5 Challenges in VoIP

1. The Quality of Voice transmitted is mostly affected by delay, jitter and packet loss since the various protocols (IP and UDP) that enables VoIP are all connectionless which means that voice signal transmitted can reach their destination in an out of order fashion, could be delayed or even cause loss of packet due to congestions in the network.
2. VOIP is deployed in an already existing data network (converged networks) hence the need to compete for the available resource with other network traffic is a necessity. This may cause the network to exceed its capacity which may lead to packet loss, delay and jitter.
3. Furthermore, an IP network was designed for data networks and not for VoIP. Therefore, when voice is transmitted over IP it results in a square peg in a round hole problem.
4. Voice compression (codec) to reduce bandwidth consumption also degrades the voice quality
5. VoIP system like any other system is challenged with security issues.

2.3 Quality of Service (QoS)

It is clear that due to the true nature of IP networks, voice packets sent across the IP network is affected with transmission problems such as latency, jitter and packet loss. Latency (delay): this is the time it takes for voice signal to be transmitted from the source to the destination. Delay can be categorized into process delay, queuing delay, propagation delay and transmission delay. ITU-T has defined a standardized value for the total delay in VoIP which is <=150 for a circuit-switched (Backs &Pohlmann, 2008; Stallings, 1997).

Jitter

This is said to be the variations in delay. It is a common problem of the connectionless network so a jitter buffer at the receivers end is used to curtail this problem, however, the use of the jitter buffer adds up to the delay. ITU-T standardized value for jitter is 20ms for one way trip (BehrouzA.Forouzan, 2013).

Packet Loss

This is the failure of the transmitted packets sent to reach their destination. This occurs when packets are broken and dropped due to congestion in the network. Packet loss may also occur when the network exceeds its capacity in terms of resources. ITU-T standardized value for packet loss is actually 0-1% for VoIP (BehrouzA.Forouzan, 2013).

QoS is the collection of mechanisms to provide guaranteed service. The performance guarantee of a VoIP system can be attained if the VoIP system is deployed on a separate network that does not share resources with other data traffic. Unfortunately, this encourages waste of resources (BehrouzA.Forouzan, 2013).

The Internet Engineering Task Force group (IETF) has designed two different techniques that enable resource reservation for particular traffic and prioritization of packets to enable guarantee service. The protocols are Integrated Services (IntServ) and Differentiated Services (DiffServ) (BehrouzA.Forouzan, 2013; Kumar, 2006).

INTSERV

This QoS technique uses the RSVP (Resource Reservation Protocol) for the reservation of resources such as CPU, bandwidth, etc. for specific traffic flow. IntServ normally classifies the packets, schedules them for forwarding and devices (routers) use the call admission protocol to determine the availability of resources. RSVP which is a connection-oriented protocol uses two types of messages. They are the Path and the Resv messages. The path message is sent by the source device which stores information of the receiver in the multicast path. After the path message has been received, the receiver then sends the Resv message. This message makes resource reservation on the devices that support the RSVP (BehrouzA.Forouzan, 2013; Stallings, 1997).

In this technique, the source device defines the flow specifications which are of two main types, the Rspec (Resource Specification) which defines the resource that flow needs to reserve. Tspec (Traffic Specification) defines the traffic flow characteristics. After a router receives a flow specification from an application, it decides to admit or reject the service based on the availability of resources. There are two main types of service classification in the IntServ technique. They are the guarantee service which is designed for real-time traffic that needs a guarantee end-to-end delay and the controlled service designed for applications that can tolerate delay but sensitive to overload network and packet loss. Scalability and service limitations are the main challenges in the IntServ (BehrouzA.Forouzan, 2013; Stallings, 1997)

DIFFSERV

Differentiation Service (DiffServ) is a model designed by the IETF to counter the challenges in the IntServ (Woller&Gebhardt, 2012). In this technique, packets are marked into classes for different forms of priorities (Mehdi, 2009) as shown in Table 2.3. Each packet in DiffServ contains the Differentiated Service (DS) field (BehrouzA.Forouzan, 2013). The value of this field is set at the Ingress. DS replaces the existing ToS field of the IP datagram. DS contains two other fields which are the DSCP (Differentiation Service Code Point) and CU (Currently Unused). DSCP is a code that defines the Per-Hob Behavior (PHB) for each node that receives a packet. Three main types of PHB are defined and the code defines the kind of service the application would receive (Chen, 2013; Cisco, 2001; Davidson, 2006)

1. DE PHB: default PHB is the same as the best effort service delivery by the IP.
2. EA PHB: Expedited Forwarding provides the low packets loss, low latency and ensured bandwidth services.
3. AF PHB: Assured Forwarding

One main challenge with the DiffServ of the QoS Technique is that low prioritized packets could be congested to cause packet loss over time. This would be a waste of resources once packets are dropped.

Table2.3: The commonly used DSCP values

DSCP value	Hex value	Decimal value	Meaning	Drop probability	Equivalent IP precedence value

101110	0x2e	46	Expedited forwarding (EF)	N/A	101 - Critical
000000	0x00	0	Best effort	N/A	000 - Routine
001010	0x0a	10	AF11	Low	001 - Priority
001100	0x0c	12	AF12	Medium	001 - Priority
001110	0x0e	14	AF13	High	001 - Priority
010010	0x12	18	AF21	Low	010 - Immediate
010100	0x14	20	AF22	Medium	010 - Immediate
010110	0x16	22	AF23	High	010 - Immediate
011010	0x1a	26	AF31	Low	011 - Flash
011100	0x1c	28	AF32	Medium	011 - Flash
011110	0x1e	30	AF33	High	011 - Flash
100010	0x22	34	AF41	Low	100- Flash override
100100	0x24	36	AF42	Medium	100 - Flash override
100110	0x26	38	AF43	High	100 - Flash override

Source: (Banerji and Chowdhury 2013; K.Mishra, K. Singh, and Patel 2012)

2.4 Security

VOIP suffers from all known attacks associated with any Internet application since the technology is a voice over internet protocol. Security is a major issue to Internet applications and since VOIP is to work through the Internet then VOIP is not immune from the security challenges of the Internet. VoIP usage is advancing and the need to secure voice signals from unauthorized access (confidentiality), unauthorized change in the voice signal (Integrity) and availability of VoIP service to unauthorized users when in need (availability) (Behrouz A. Forouzan, 2013; Dantu, Fahmy, Schulzrinne, &Cangussu, 2009; Sanguino& Roberts, 2011; Voice et al., 1974). There are various measures and techniques designed to counter security attacks in data networks which works so well. However, these mechanisms have not proven to be absolutely excellent for VoIP systems since voice transmission is real-time traffic unlike the e-mail, etc (Nwebonyi, 2014; Obidinnu&Ibor, 2016; Phithakkitnukoon, Dantu, &Baatarjav, 2008).

Some classifications of VoIP security attacks have been defined over the years. These are;

1. Attacks against availability: this normally aims at interrupting the VoIP service in the form of Denial of Service (DoS). Examples are call flooding, malformed messages, spoofed messages, etc.
2. Attacks against confidentiality: this also aims at providing illegal means of gaining access to the media, user identities, password, etc for other forms of deceptive operations. Eavesdropping, network analysis, etc.
3. Attacks against integrity: this aims at causing a change in the VoIP message. It could be a deletion, injecting or replacing certain information in the VoIP message. Examples are call rerouting and black holing etc.
4. Attacks against social context: this attack aims at using a stolen legitimate user's identity in transmission of false information which the target user may the target may not know to be false. An example is the man-in-the-middle attack.

2.5 Security Measures

The main identified solutions of the VoIP attacks are in two main categories. These are the VoIP protocols and Virtual Private Network (VPN) (Ayokunle, 2012; Ilyas&Tomader, 2016). VoIP protocols that ensure the provision of security in the VoIP system are the signaling and transmission protocols (Ilyas&Tomader, 2016). In VoIP, security is usually provided at the call set up stage or to the transmission media. Signaling protocols used in VoIP provide a suite of security services that prevent some of the attacks against availability, confidentiality and integrity identified (Batchvarov, 2004; Ilyas&Tomader, 2016). Examples of the signaling protocols are the SIPS with SDP and H.235 of the H.323 collection of protocols. SRTP with the SRTCP protocols also define a security profile of the RTP which prevents some attacks against availability, confidentiality and integrity. VPN uses the applications on IPSEC to provide security measures that prevent all the attacks defined earlier (HKSAR, 2008).

VoIP protocols alone have not been able to solve the man in the middle challenge except with the use of the VPN that uses the IPSEC applications to provide general VoIP security against all the attacks. However, IPSEC causes an increase in bandwidth consumption since there is an additional use of bandwidth for cryptographic functions for the VoIP messages. In (Backs &Pohlmann, 2008), the author concluded that bandwidth usage for a secured VoIP system is doubled of the unsecured. There is also an assertion that the encryption and decryption toprovide secure transmission in VoIP increases the challenges of QoS. The author in (Backs &Pohlmann, 2008), again identified the values of the delay, jitter and packet loss to be very negligible.

2.6 PBX

Private Branch Exchange is a traditional circuit switch telephone system that enables an organization to manage its own communication system internally (Wadhwa, 2007). PBX is exclusively owned by the organization and that saves the cost of communication since a single telephone line from the provider is fragmented to several lines known as extensions for local communication within the premises of the organization (Kumar, 2006). It is made of both software and hardware. PBX normally has its own proprietary phones to be used (Scores, 2013). Over the years, the massive growth of data networks and increased open knowledge of packet switching led to the development of VOIP and new PBX systems such as IP-PBX (Mehdi, 2009). The IP-PBX uses the Internet Protocol (IP) to carry voice communication on the data network. The advent of VOIP technology enabled great development towards IP-PBX and this new technology has become a great supporter of VOIP systems in providing cheap and myriad forms of communication over a data network (Bansal, 1998; Beyh&Kagioglou, 2004). The advancement of the PBX has introduced soft PBX and Softphones to enable VOIP communication (Rana, 2013).

2.7 Soft PBX

This is a software form of PBX that is much simpler and cheap to deploy than a proprietary hardware PBX (Mupparapu, 2008). The software is normally installed on a Linux or Windows operating system as the server for the phone system. There are several examples of open source soft PBX for phone systems (“Open Source VOIP Software - VoIP-Info,” 2003). Asterisk is the mother of all the exiting soft PBX (Bryant, Madsen, &Meggelen, 2013). Asterisk PBX software comes in various distributions which are normally installed on the various distributions of Linux operating depending on the various requirements of the VOIP system to be built (Bryant et al., 2013). Presently there are some of the soft PBX that are windows compatible. In as much as there are various software of PBX for VOIP system, the researcher prefers Asterisk PBX or any of its distributions since it's been in the system for a long while now and there are documentations available to aid one in the face of challenges. There exist some online forums that discuss issues related to the usage of Asterisk PBX.

2.8 Softphones

The traditional PBX has its own defined hardware phones to be used as clients of the PBX server (Qadeer, Shah, &Goel, 2012). The soft PBX also have softphones software which is installed on client devices to enable communication ("PBX Software - VoIP-Info," 2003). Softphones are application software that enables telephone calls over the Internet. These applications referred to as clients are available for smart devices (Android and iPhones), Windows, Linux and Mac computers (Bryant et al., 2013). Softphones are designed to act as a traditional telephone. It appears as an image of a handset with a display panel and buttons with which the user can interact (Qadeer et al., 2012). For communication to be established between the softphone and the PBX server, both end systems must support the same voice over internet protocol and at least one common audio codec (Rana, 2013). Most softphones support SIP or the Inter-Asterisk Exchange protocol (IAX) (Bryant et al., 2013). There are many open source softphones but the researcher prefers the Zoiper softphone since one can view statistics of the performance of the wireless network and the voice quality during a telephone call session.

2.9 VoIP-over-WLAN

Several issues are identified as challenges of both wireless technology and VOIP from the existing literature review discussed in this chapter. Some countermeasures are introduced to solve those challenges. However, these countermeasures are also with some challenges that need to be solved. This session is dedicated to the discussion of the complete Research Idea to build a test bed of a VOIP system at the Department of Computer Science of the University of Ghana, Legon campus for free local communication, taking measures to dodge the identified challenges with both VOIP and the wireless technology.

In building the test bed, the VOIP server is built on a separate wireless LAN devoid of Internet connection. This choice of wireless network is a necessity to enable mobility of the free communication service within the defined range of coverage area whiles preventing the VOIP application from competing with other data applications for resources. This is to contest the challenges of the QoS techniques.

Intserv which is the first technique developed to fight QoS challenges has also been identified with scalability and service limitation challenges whiles the advent of Diffserv was to solve the challenges identified with Intserv technique has the possibility of causing low prioritized packets to be congested which can cause packet loss over a long time (BehrouzA.Forouzan, 2013; Hersent et al., 2005; K.Mishra et al., 2012). This would be a waste of resources once packets are dropped (Lazzez, 2013). Again one would ask the question of when to prioritize which has its own challenges as well.

Amor Lazzez has argued that since the challenges of VOIP deployment over a converged network are enormous it would be better if institutions wanting to deploy VOIP would have to do that over a separate network or use virtual LAN (VLAN) to separate the data traffic from the voice traffic (Lazzez, 2013). Egbenyon Donal and Cisco group argued that the use of a separate network to deploy VOIP in an institution is a waste of resource since there is an already existing network that can be used hence; there is no need to build a new network for the deployment of VOIP (Cisco, 2001; Egbenyon, 2011). Then some authors proposed the use of MPLS, VLANs and IP precedence with DiffServ Code points. However, Quality of service runs through all the network layers whiles the mostly considered layers are 1,2 and 3 but layer 2 and 3 are preferred most.

In as much as these techniques sound good, there are some challenges with the use of VLAN; this means that data traffic would be on a different VLAN and that of Voice traffic would also be on a different VLAN. The challenge here is how the network would be separated when softphones are used instead of the traditional hardware VOIP phones. With the use of IP precedence with DiffServ code point, there would be an increase to the known delay in VOIP. This technique can only be used in a layer 3 type of network since it uses the Type of Service (TOS) bits length of the IP format to set the precedence.

The researcher does not agree to the fact that deploying VOIP over a separate network is a waste of resource but rather thinks VOIP could be deployed over a separate network built with off the shelf devices and easy to deploy and maintain devices eliminating the internet so data applications would not compete with voice traffic. The usage of off the shelf devices for the development of the WLAN can be seen to be cheap and this will not create wastage to add to the challenges of VOIP system as compared to the screechy voices one could hear when VOIP is deployed on a converged data network.

With the known challenges of INTSERV in terms of service limitations and scalability of the system, This QoS is not an option for consideration in the deployment of the VOIP system on the Legon campus. DIFFSERV is also not an option since the classifications of the applications is enough a challenge before advancing to the servicing of the highly prioritized packets which when done for a long time will cause low prioritized packets to be congested and this may lead to network breakdown. Hence the building of the proposed VOIP system on a separate private data network to provide free local calls services on the university campus as shown in figure 2.3. These and many more are the reasons for the proposed architecture of the VOIP test bed system at the Centre.

Figure 2.3: The proposed VOIP architecture

Figure 2.4 exhibits the portion of the computer science department for the wireless coverage for the building of the test bed of the VOIP system.

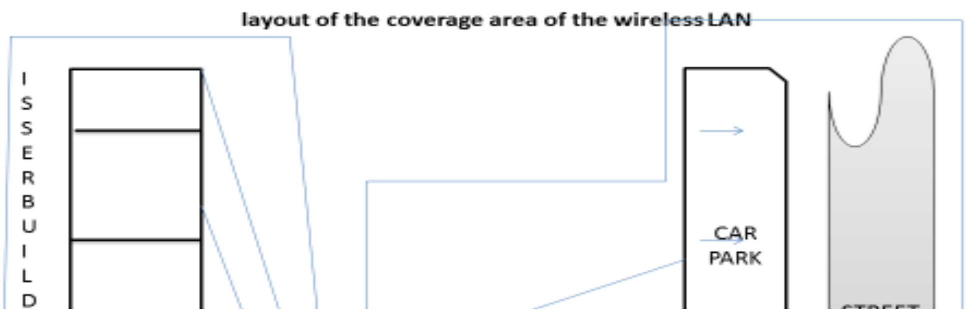


Figure 2.4: The layout of the coverage area of the VOIP-over-WLAN

2.10 Chapter Summary

The underlying technologies and techniques that enable wireless communications and for that matter VOIP are fully discussed in this chapter. The Chapter also presented the challenges with the technology, the countermeasures of those challenges and the comprehensive research idea construed from the existing literature review. It continued to explain how the proposed design architecture of the test bed of the VOIP system will contest the known challenges of the QoS techniques to build the resilient system proposed. The next Chapter presents the details of the design and implementation of the VOIP system.

CHAPTER 3: DESIGN AND IMPLEMENTATION OF VOIP-OVER-WLAN

The Chapter brings together the methodology used to design and implement the VOIP-over--WLAN test bed at the Computer Science Department, UG, and the evaluation of the general performance of the test bed. The discussion in this Chapter is focused on the resources used for the design and implementation of the VOIP-over-WLAN test bed; the steps carried out to design and implement the test bed; the Radio Frequency (RF) parameters measured to examine a reliable and efficient wireless network; and finally the parameters measured to evaluate the overall performance of the VOIP test bed.

3.1 Introduction

The VOIP application is built on a private wireless network deprived of an internet connection whose main objective is to transmit voice packets and not data packets between nodes. In designing a wireless network for VOIP application, a 2.5GHz band was used since it is an unlicensed band and there was no need for authorization from the government regulatory body. The band also provides a good coverage area to the defined location enabling mobility whiles making it easier for client devices such as smart phones to be connected to the network.

To be sure of how well the wireless network will behave under the necessary conditions for which it was built, a site survey was done to read the various parameters that define the wireless network connectivity, and to identify RF interferences in the wireless environment (and if any, countermeasures could be administered). VOIP applications were installed on both the server and client devices to enable free communication over the defined location of the wireless coverage area. The VOIP installed on the server (i.e. Asterisk PBX) is responsible for mapping extensions numbers to Session Initiation Protocol (SIP) addresses, establishing and maintaining calls, and tearing down the session. And the soft phones installed on the client devices enable calls to flow among the communicating devices. Various scenarios were defined so VOIP communication could be established at the various locations within the defined coverage area of the wireless network. The statistical tools on the softphones were used to monitor the numerous parameters that measure the quality of voice transmissions these results were tabulated and presented in the graph for evaluations. See

Figure 3.1 which depicts the overall process used to design and implement the VOIP-over-WLAN test bed.

3.2 System Requirements

The general system requirements for the design and implementation of the VOIP-over-WLAN test bed are both hardware and software. The details of the hardware specification and software that were used for the design and implementation of the test bed are presented in this Section.

Hardware specification

1. Wireless Access Point with bridge mode: Ubiquiti Nanostation Loco M2 with air OSv5.6 and above. The most current version of the air operating system (OS) was released in November 2017 (i.e. air OSv8.4.3). Ubiquiti Networks (UBNT) provides a variety of high–end wireless networking products that utilize innovative and groundbreaking wireless technology.
2. A Personal Computer or Laptop with Wireless Network Interface Card *WNIC*: To connect the Personal Computer or Laptop to the wireless network. HP Pavilion x360[3]Convertible with Windows 10 Pro 64bit as the OS, and Intel Core (TM)i3-6100U CPU @ 2.30GHz(4CPUs) as the processor, and a memory of 4GB.
3. Standard category 5 (cat 5) LAN cable.
4. Power-over-Ethernet adapter (this normally comes with the Ubiquiti Nanostation).

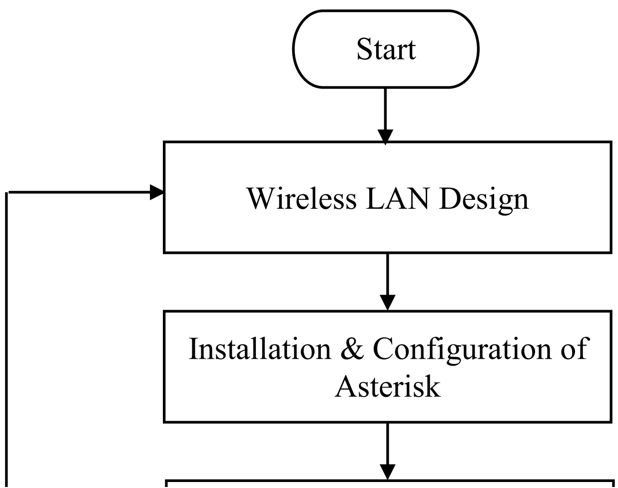


Figure 3.1: The flowchart of the overall process used to design and implement the VOIP-over-WLAN test bed

Software

The software packages that were used to build the test bed are as follows:

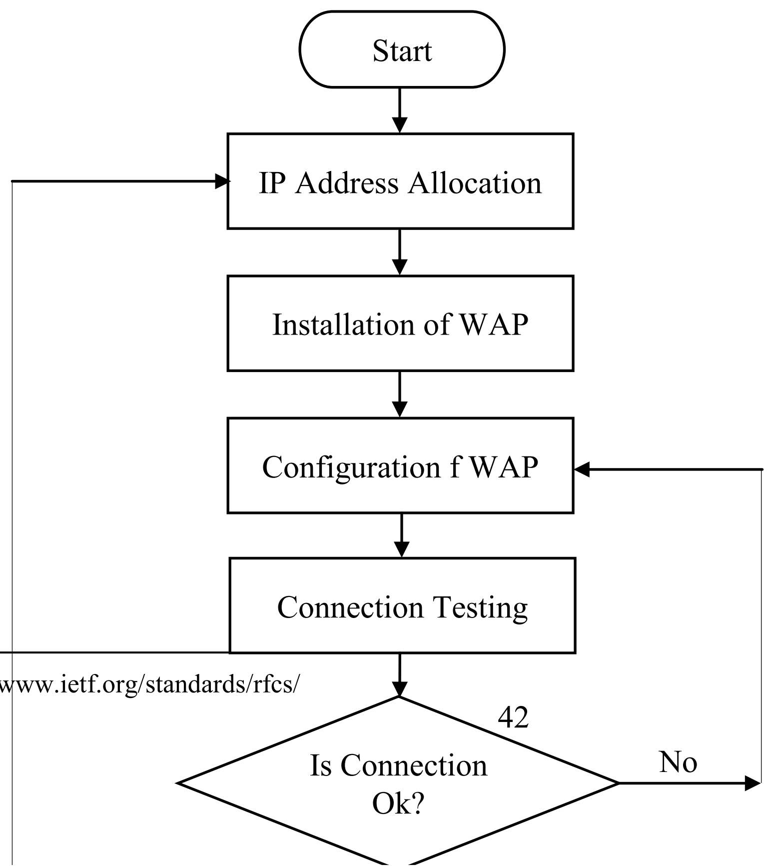
1. Asterisk 13.15.0
2. Ubuntu 64bit
3. VMware Workstation 12.0 player
4. RF survey

3.3 The Wireless LAN

This Section explains in detail the various steps used in the design and implementation of the reliable wireless LAN for the VOIP application, and Figure 3.2 shows the flowchart of the details.

3.3.1 IP address allocation

Before the start of the wireless network design, the unique identification number of the IP network was a natural concern. This unique identifier of a network known as an IP address is a numeric address assigned to each device on an IP network. It designates the location of a device on the network. This enables effective communication among devices on the network. To allocate IP addresses for the wireless network, an available subnet was identified from which all the IP numbers were obtained. These unique numbers were statically assigned to the various devices (i.e. clients, server, WAP) on the wireless network. Request for Comments[1] (RFC) have defined standards in the allocation of IP addresses, these standards were adhered to in the assignment of the IP addresses to the devices.



[1] https://www.ietf.org/standards/rfcs/

Figure 3.2: The flowchart of the detailed steps in the design and implementation of the wireless LAN.

3.3.2 Installation of the WAP

To provide a good coverage area to the defined location of the wireless network, a place at Computer Science Department Research Laboratory, UG, was identified for the installation of the Wireless Access Point (WAP). The WAP was installed on the wall connecting with LAN cables and Power Over Ethernet POE to the respective ports of the WAP, and the Laptop together with the power cord plucked in the power socket. The diagram in Figure 2.3 also shows the network topology. The Ethernet adapter was configured with a static IP address for the WAP configurations to be done automatically. The laptop was used to lunch a browser to provide the default static IP address for the Ubiquiti device to be properly configured.

3.3.3 Configuration of the WAP

The Ubiquiti Nano station locom2 device manual provides detailed documentation on the configuration of the WAP. However, a brief description of the configurations that were made are presented here as follows:

1. The network mode was set to bridge since this mode extends the wired LAN at the Computer Science Department Research Laboratory wirelessly to the defined coverage area.
2. The wireless mode was also set to Access Point (AP) to enable wireless clients such as laptops, smart phones, and tablets to be connected to the wireless network.
3. The channel/frequency was initially set to channel 13 to avoid various forms of channel interferences. However, the same channel was maintained after the survey of the wireless environment since it was a very good choice for the wireless environment.
4. The channel width was set to 20MHz is to avoid interferences with other 2.5 GHz networks.

After the configuration of the WAP, the various monitoring tools on the Ubiquiti device displayed various information regarding the wireless connection. These monitoring tools are the throughput, station, station information with various statistics such as device name, signal to noise ratio (SNR), noise floor, transmitted signal, received signal and client connection quality CCQ in percentage (%). These and many more statistics were recorded on the wireless environment at the Computer Science Department Research Laboratory for performance evaluations during the RF site survey.

3.4 RF Site Survey

This was an important and a necessary activity since it exposed the real wireless environment so that the identified interferences can be counter-measured, enabling the wireless network to be resilient and reliable. Building the wireless network could be said to have been easy. However, for the wireless network to thrive under the necessary conditions it was built was a great challenge. And the only way to ensure that the wireless network performs well at the Laboratory was by the RF site survey to measure and analyze some wireless network performance parameters.

3.4.1 RF survey and monitoring tools

There are many open source tools for RF site survey. This study only made use of the survey and monitoring tools of the Ubiquiti Nano station Loco M2 identified under tools on the (configuration/installation) menu. The main tools used were the site survey, ping and discovery with statistics such as signal level, noise level, scanned frequencies, Mac address, device name, SNR, frequency/channel, IP address, packet count, packet size, TTL, a packet received, packet loss, etc.

3.4.2 Parameters measurements

The site survey tool was used to scan the frequencies, SNR, and channel of the various AP in the wireless environment. These values were analyzed to see if the channel chosen required changed to prevent co-channel and adjacent channel interferences. It only happened that a change of channel was not important since the value was good for the test bed. The default channel values could be seen in figure 3.15.

The statistical values of the wireless network parameters such as noise floor, transmit CCQ, SNR and CCQ% were obtained for the individual connected mobile/client devices. Client devices placed at the various locations were pinged from the laptop to read values for round trip time RTT, packet loss, the time to live TTL, a packet received, signal strength, and SNR. Figure 3.4 depicts the wireless environment frequencies, and Figures 3.5 – 3.14 show that screenshots of the wireless network parameters that were measured at various positions indicated on the study coverage area map shown in Figure 2.4.

Site Survey

Scanned Frequencies:
2.412GHz 2.417GHz 2.422GHz 2.427GHz 2.432GHz 2.437GHz 2.442GHz 2.447GHz 2.452GHz 2.457GHz 2.462GHz 2.467GHz 2.472GHz

MAC Address	SSID	Device Name	Encryption	Signal / Noise, dBm	Frequency, GHz	Channel
26:18:D6:E2:4F:0B	STAFF		NONE	-95 / -98	2.437	6
DC:9F:DB:B2:29:8E	eduroam		WPA	-30 / -97	2.412	1
DE:9F:DB:B2:29:8E	STAFF		WPA	-31 / -97	2.412	1
90:94:E4:33:FB:62	RIPS PHD		WPA2	-72 / -97	2.412	1
EE:9F:DB:B2:29:8E	Management		WPA	-28 / -97	2.412	1
FE:9F:DB:B2:29:8E	STUDENT		WPA	-30 / -97	2.412	1
9C:D6:43:C9:7A:DC	CSCD-Library		WPA2	-88 / -98	2.432	5
24:1F:A0:59:59:FF	hairvanity		WPA	-89 / -98	2.437	6
E4:7D:EB:04:74:E6	Kxng WiFI		WPA	-60 / -98	2.437	6
04:18:D6:E2:49:DD	CONF		WPA	-91 / -98	2.462	11
00:08:54:99:DA:42	WLAN-11g-GW		WPA	-60 / -98	2.462	11

Figure 3.4: Screenshot of the wireless environment frequencies

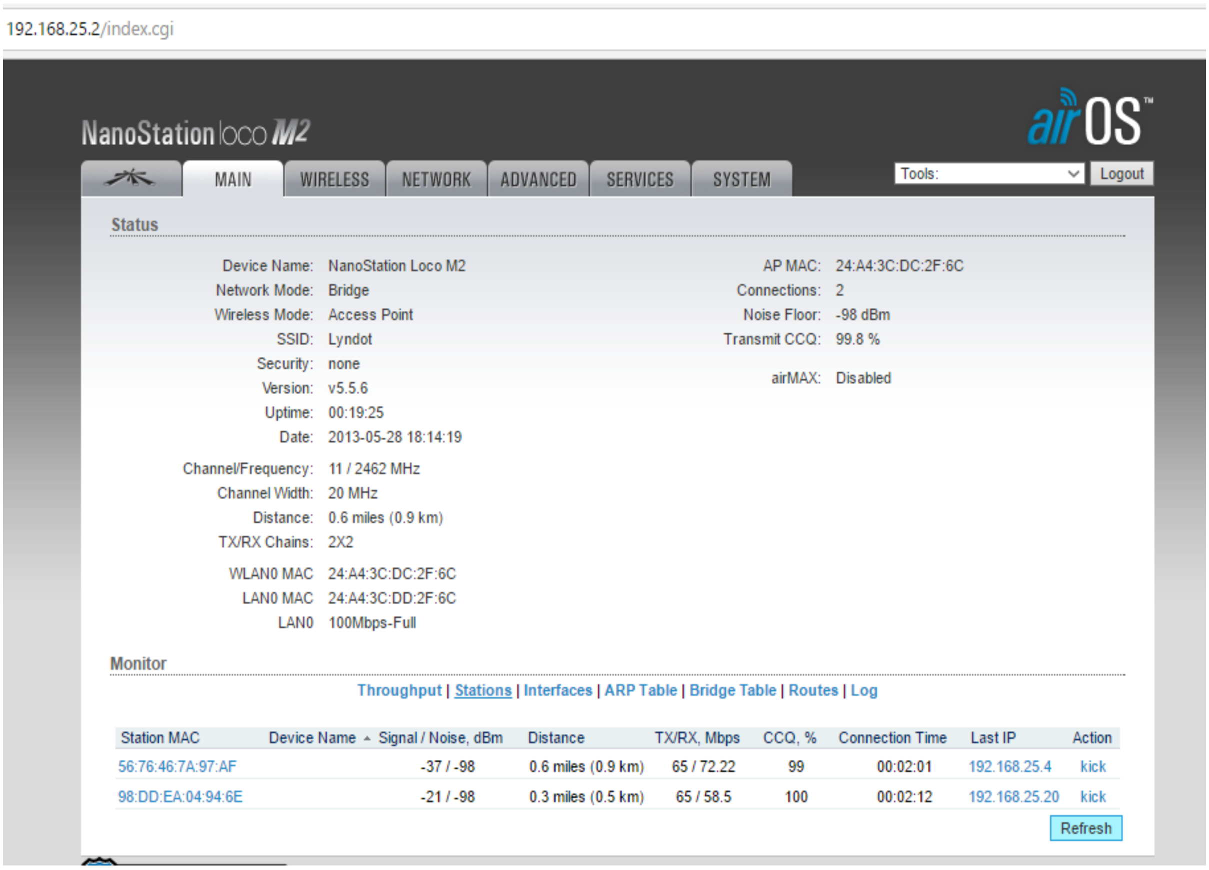


Figure 3.5: Screenshot of parameter values of the mobile phone inside the Research Lab

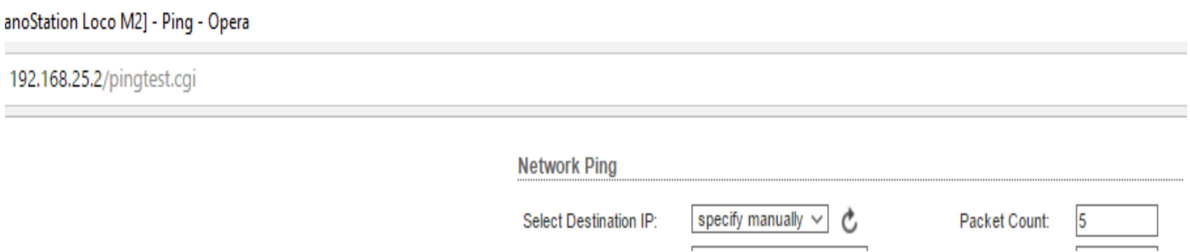


Figure 3.6: Screenshot of mobile phone pinged inside the Research Lab

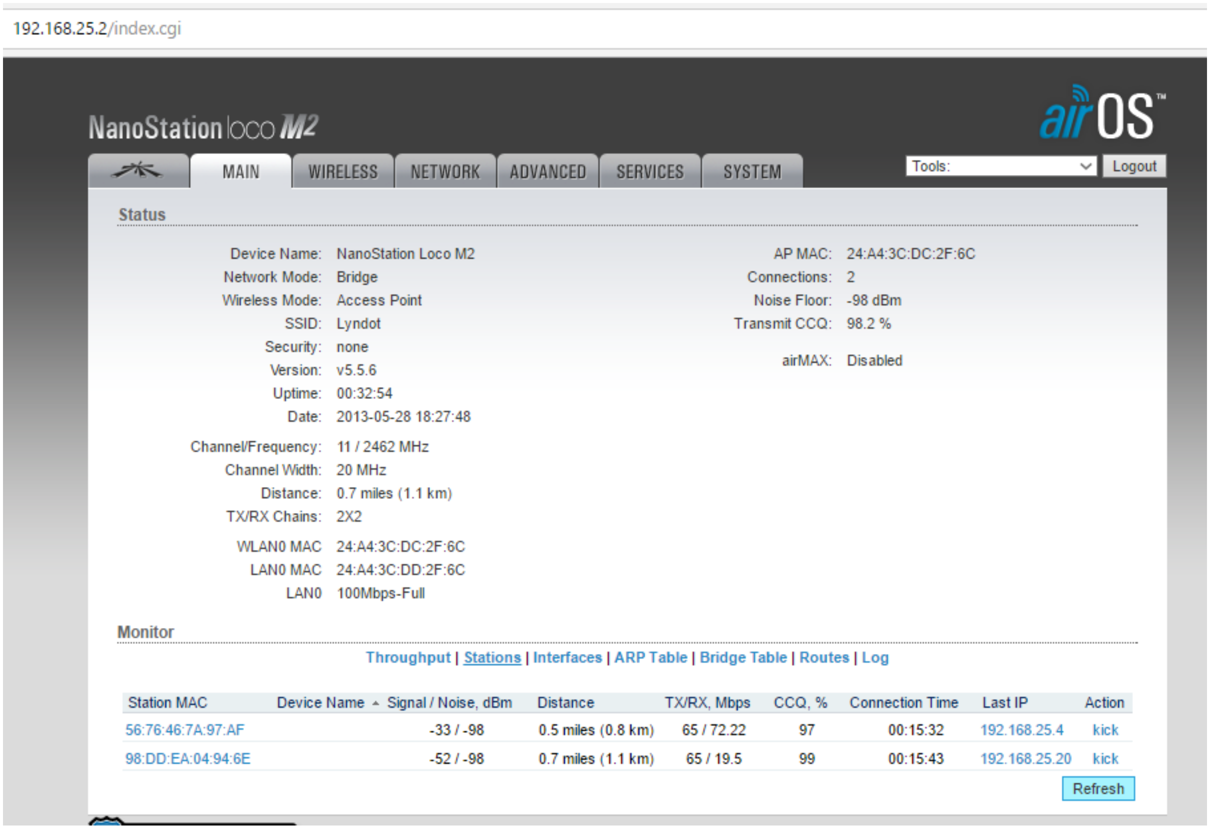


Figure 3.7: Screenshot of parameter values of the mobile phone at the entrance of the Research Lab

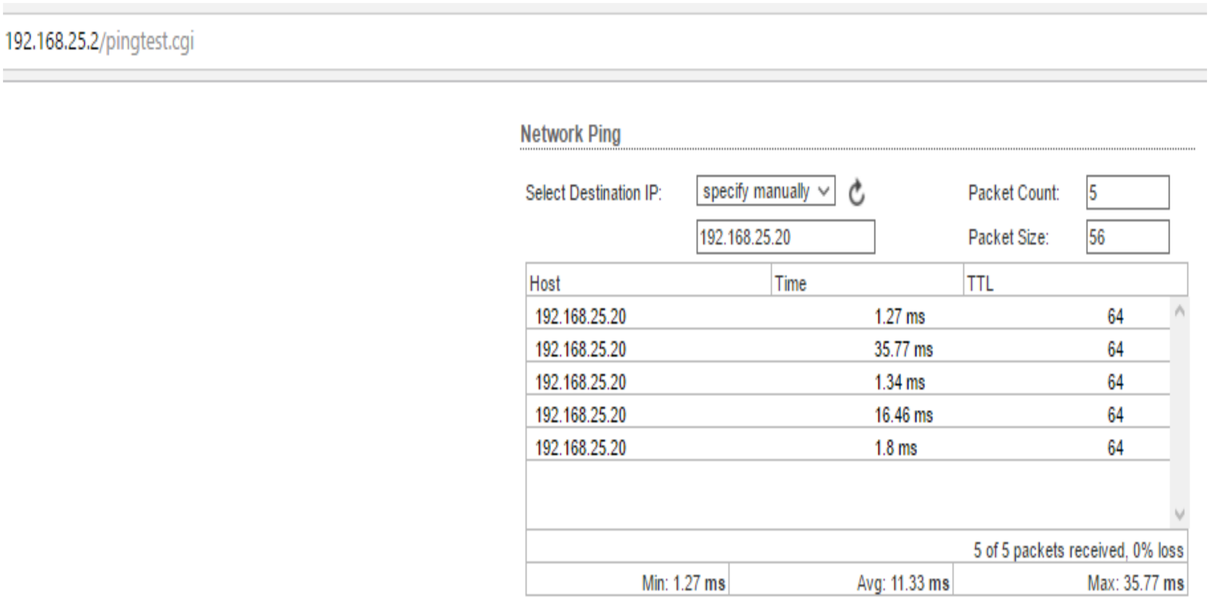


Figure 3.8: Screenshot of mobile phone pinged at the entrance to the Research Lab

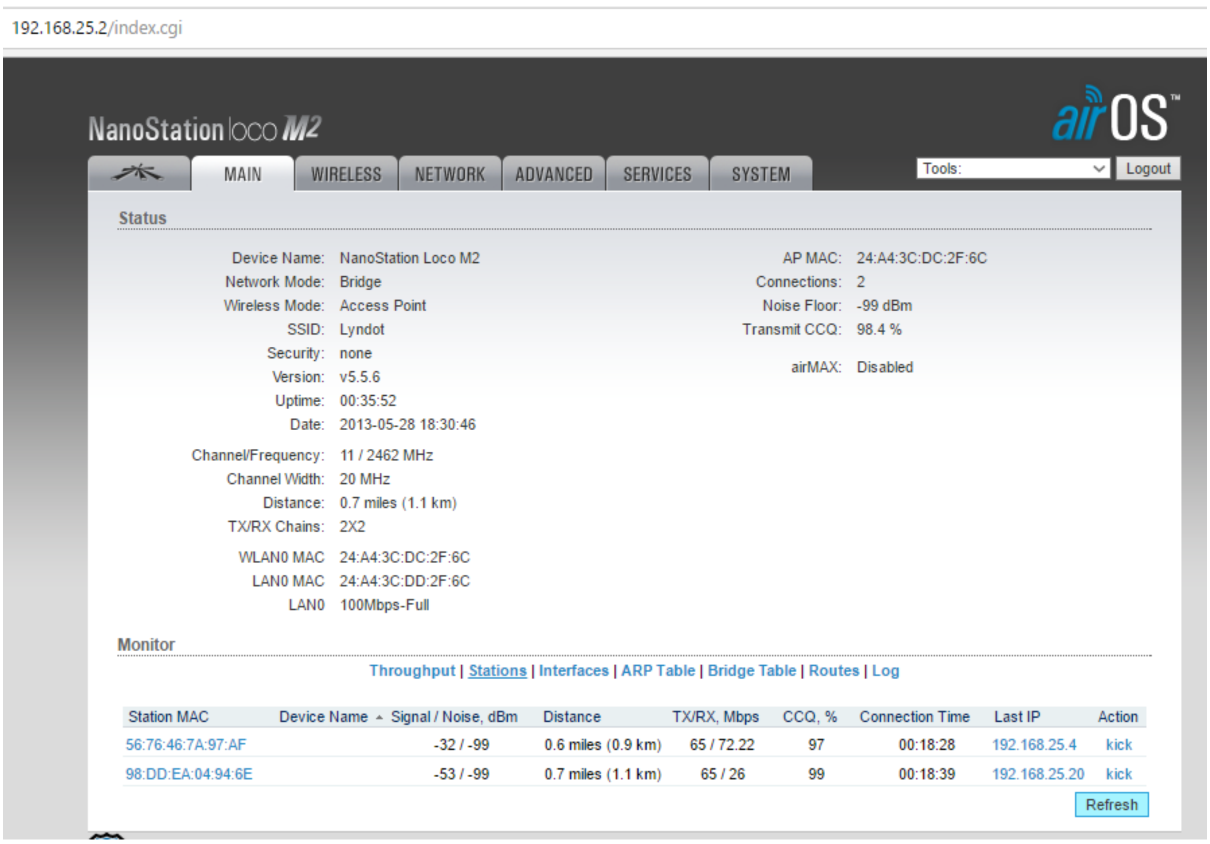


Figure 3.9: Screenshot of parameter values of the mobile phone at the Software Lab

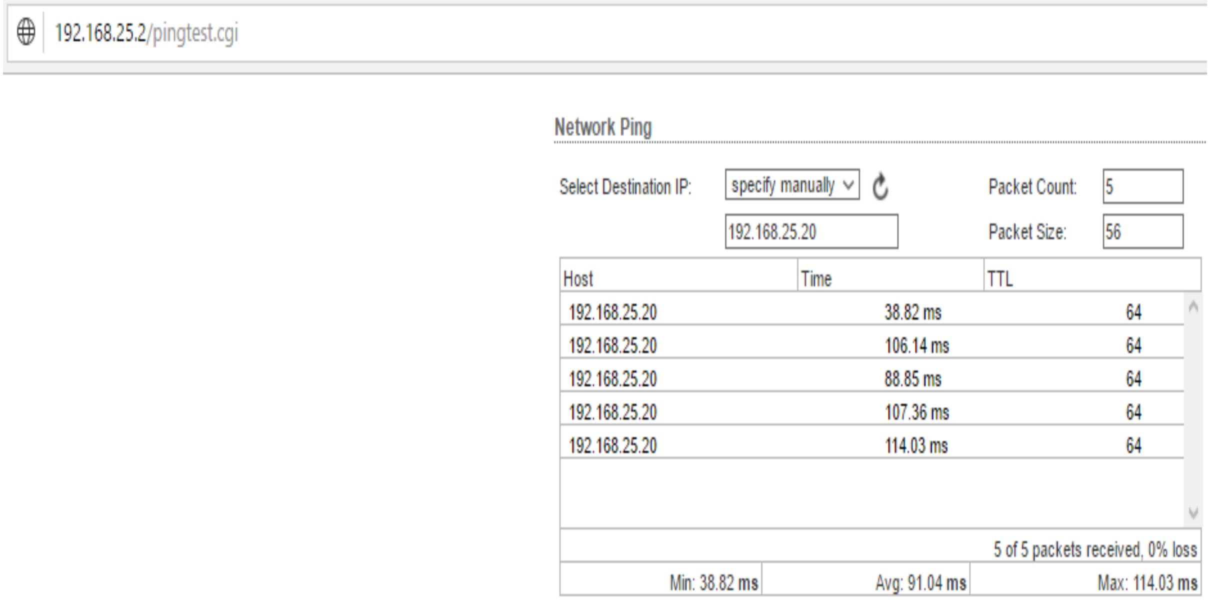


Figure 3.10: Screenshot of mobile phone pinged at the Software Lab

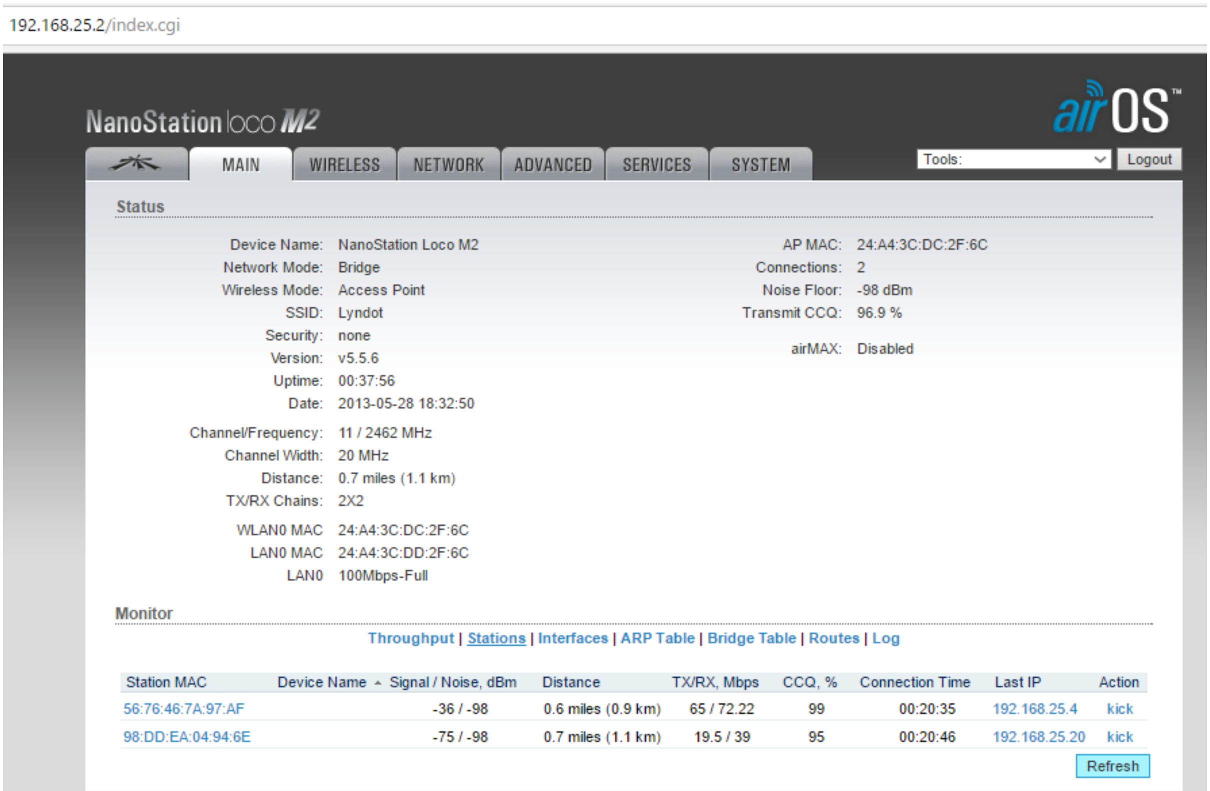


Figure 3.11: Screenshot of parameter values of the mobile phone at the Car Park

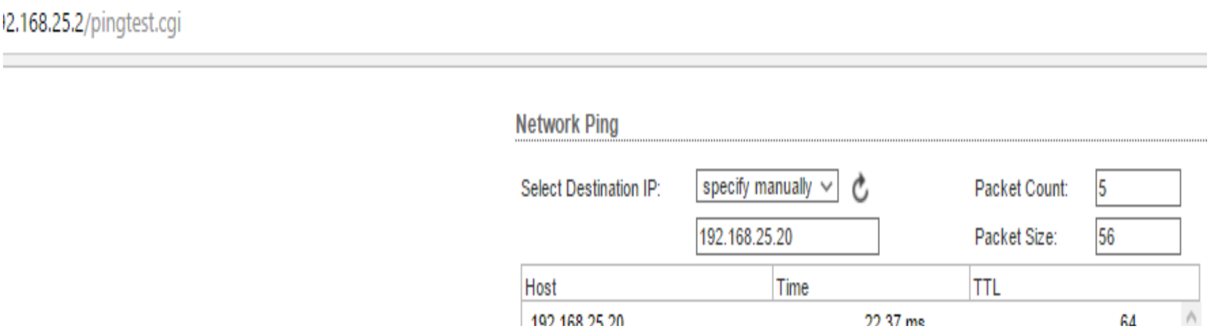


Figure 3.12: Screenshot of mobile phone pinged at the Car Park

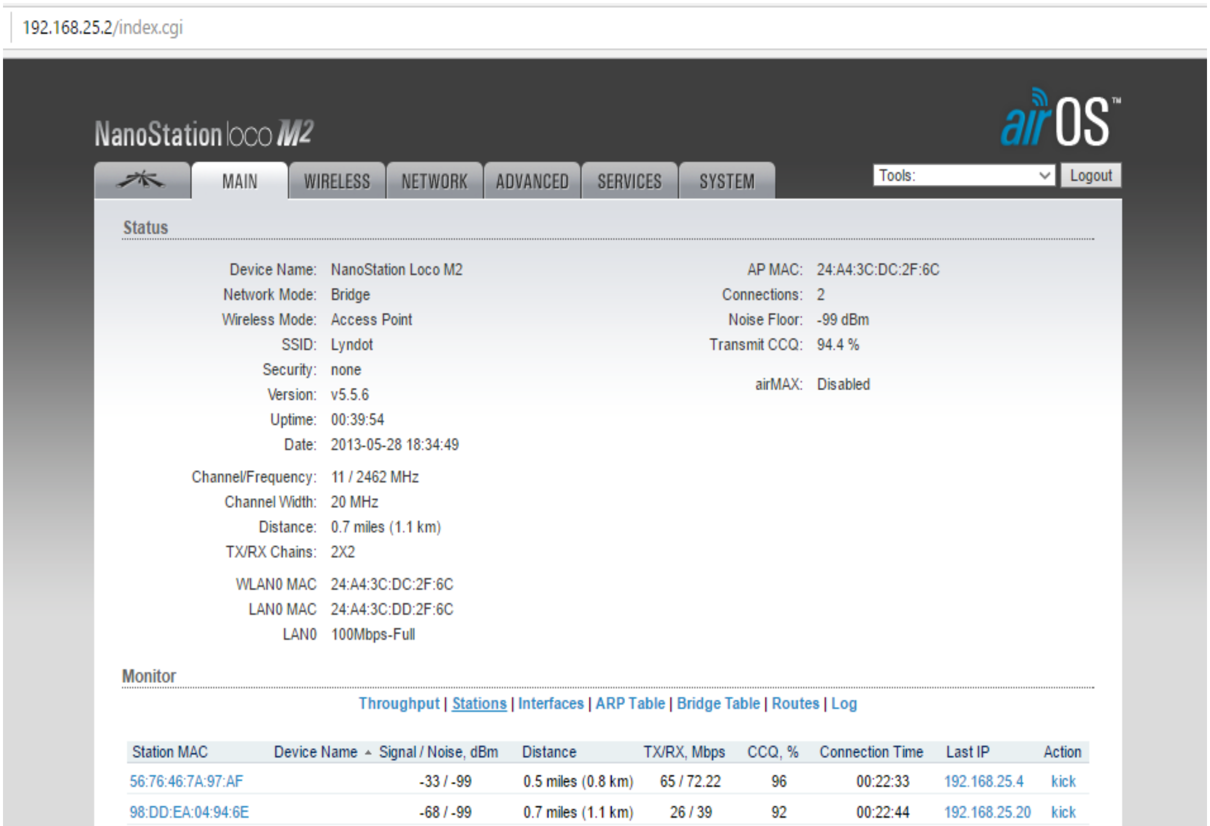


Figure 3.13: Screenshot of parameter values of the mobile phone at the end of the ISSER Road

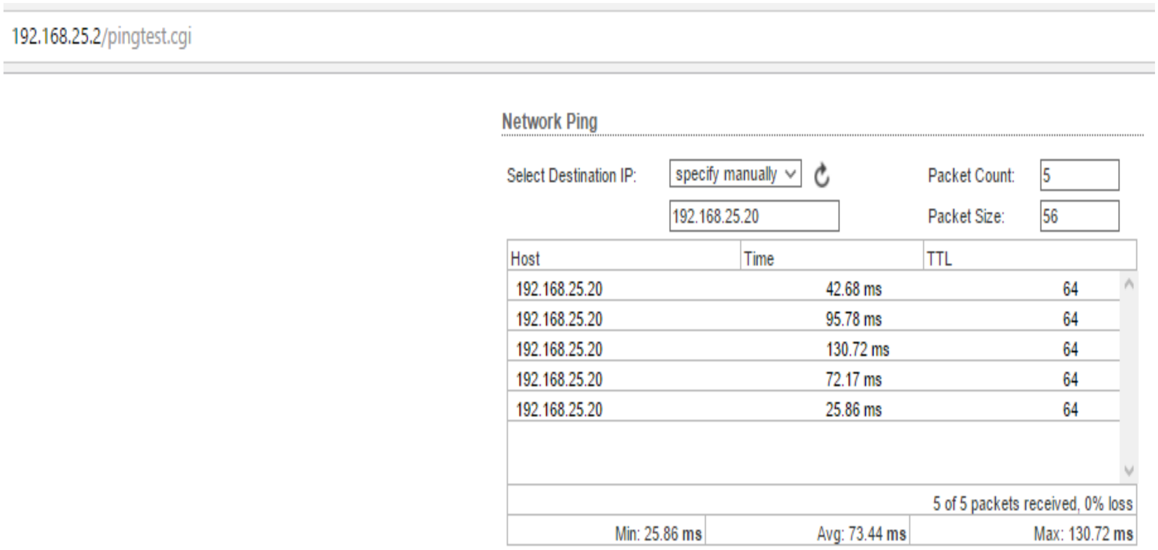


Figure 3.14: Screenshot of mobile phone pinged at the end of the ISSER Road[2]

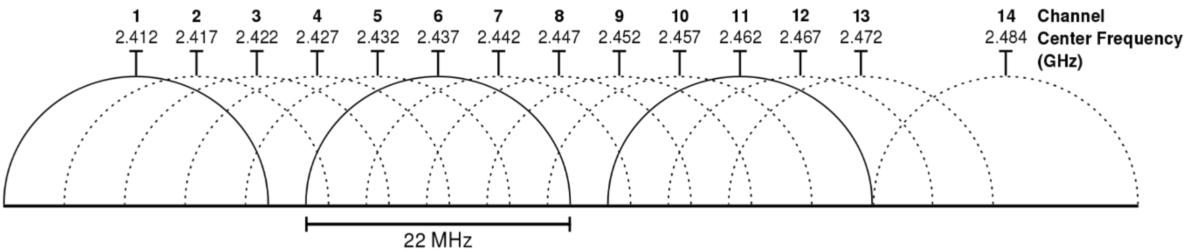


Figure 3.15: List of default channels in the 2.4GHz bank for UK country

3.5 The Asterisk Server

The Asterisk (*) as the name of the telephony system used for the VOIP-over-WLAN test bed is a symbol that represents a wildcard in computer programming languages. This name gives a revelation into the minds of the developer of Asterisk as a powerful open source telephony framework upon which anything of a telephony system can be installed. For that reason, this work installed Asterisk system for the test bed. Other examples of such telephony systems include Interactive Voice Response IVR systems, voicemail system, PBX, and VOIP system.

[2] www.asterisks.org
draalin.com/installing-asterisk-in-ubuntu/
(Using Ch 1 5 9 13 vs 1 6 11 on a 2.4Ghz/20MHz? - Ubiquiti Networks Community 2015)

3.5.1 Installing the Asterisk Server

The instructions for both pre-installation and general installation of the Asterisk system are detailed at http//:draalin.com/installing-asterisk-in-ubuntu/. The Asterisk telephony system runs on the Linux operating system platform. The Ubuntu 64bits (a distribution of the Linux operating system) was installed on a VMware workstation 12.0 player upon which the Asterisk 12.0 server was installed.

3.5.2 Configuring the Asterisk Server

The configuration of the Asterisk server was guided by the extensions numbers for the users of the VOIP-over-WLAN test bed. Four digits were considered as the extension numbers for the users on the test bed. Extension numbers starting with 1are for the technical operators of the test bed, 2 for the students of the Computer Science Department, UG, and 3 for the other

of the

e 3.15

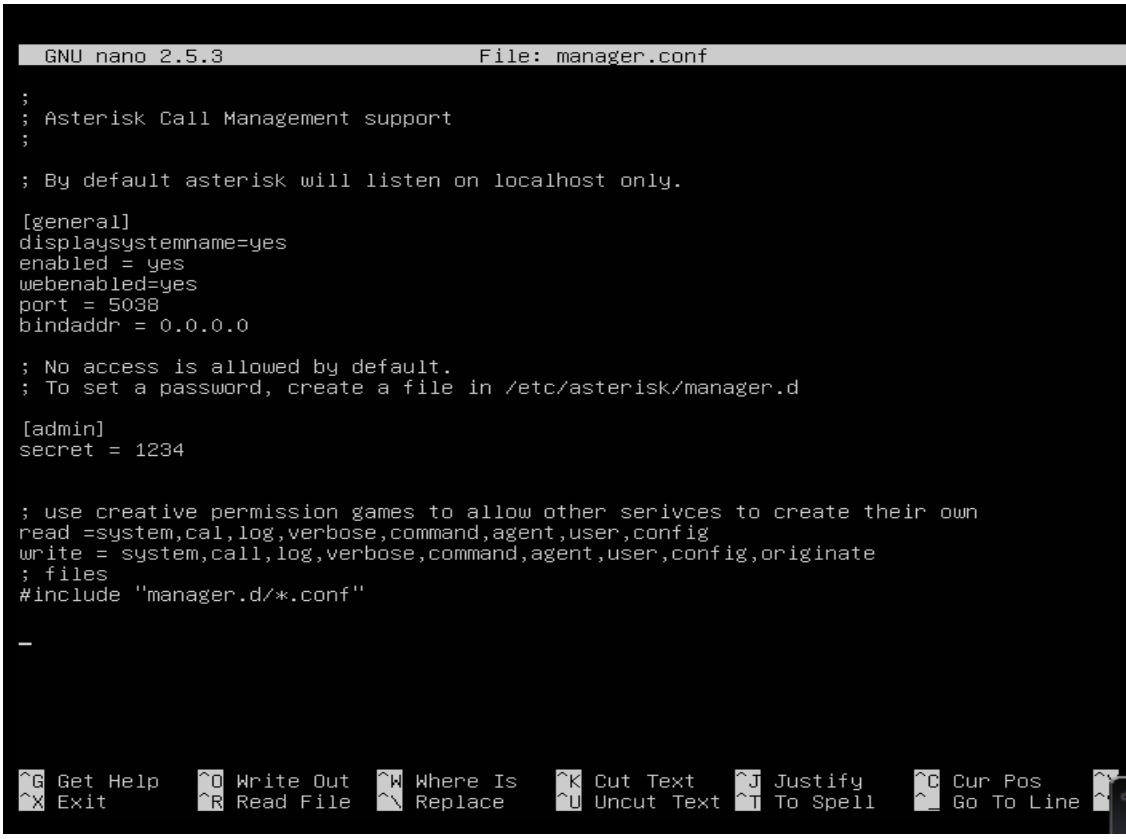


Figure 3.15: Screenshot of the Asterisk management configuration terminal

The main configuration of the Asterisk server is in three main stages. These are:

Users configurations: This describes the setup of the users of the VOIP system as shown in Figure 3.16.

SIP configurations: This also describes the setup of the SIP channels and registration of the SIP peers as shown in Figure 3.17.

Extensions configurations: This is the setup of the incoming and outgoing dial plans as shown in Figure 3.18.

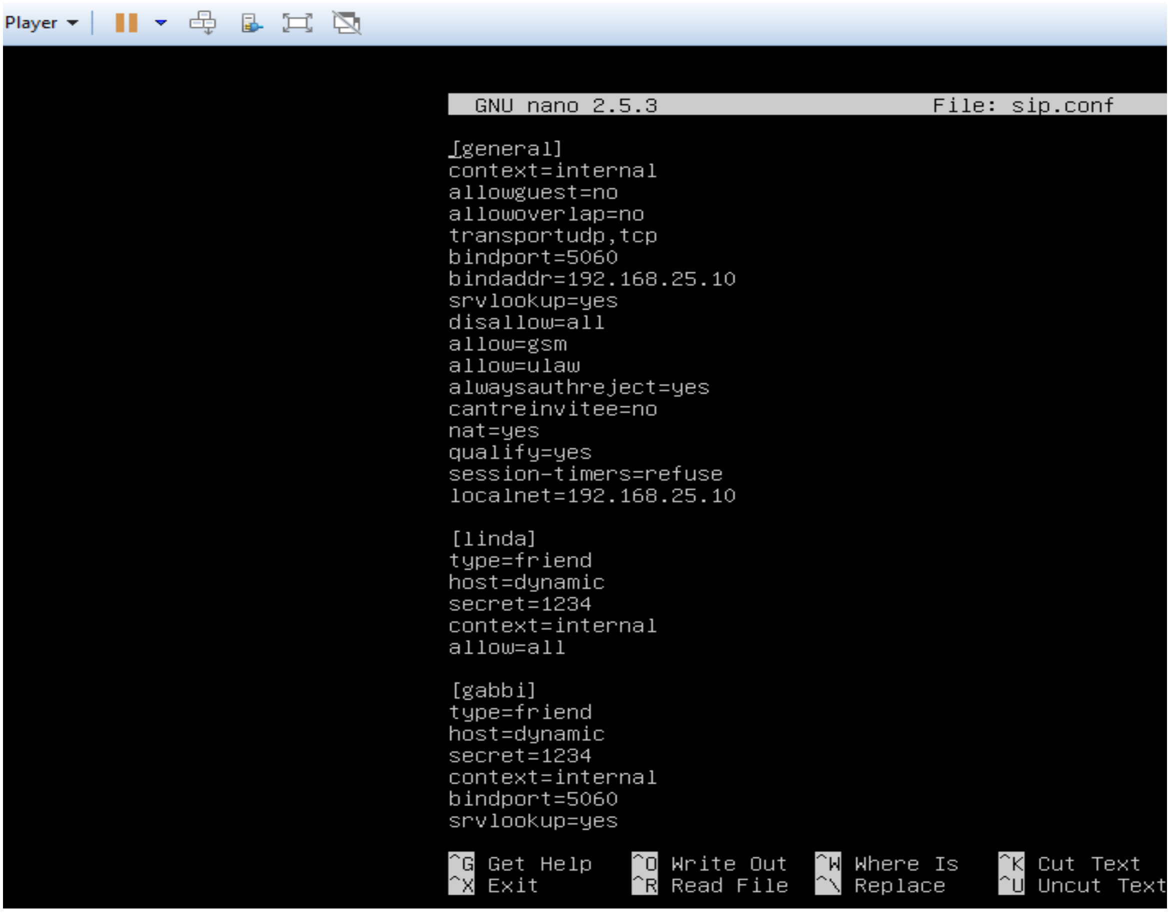


Figure 3.16: Screenshot of the SIP configuration terminal

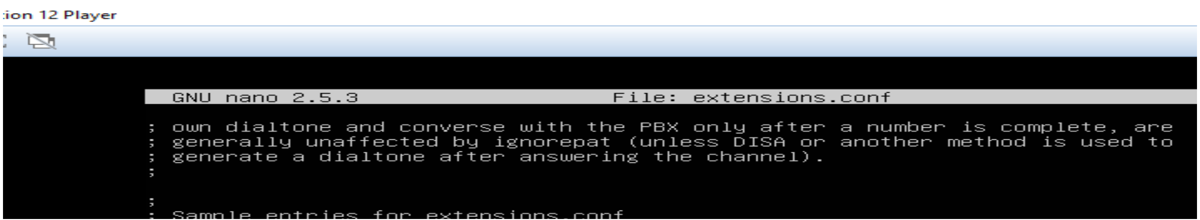


Figure 3.17: Screenshot of the Extensions configuration terminal

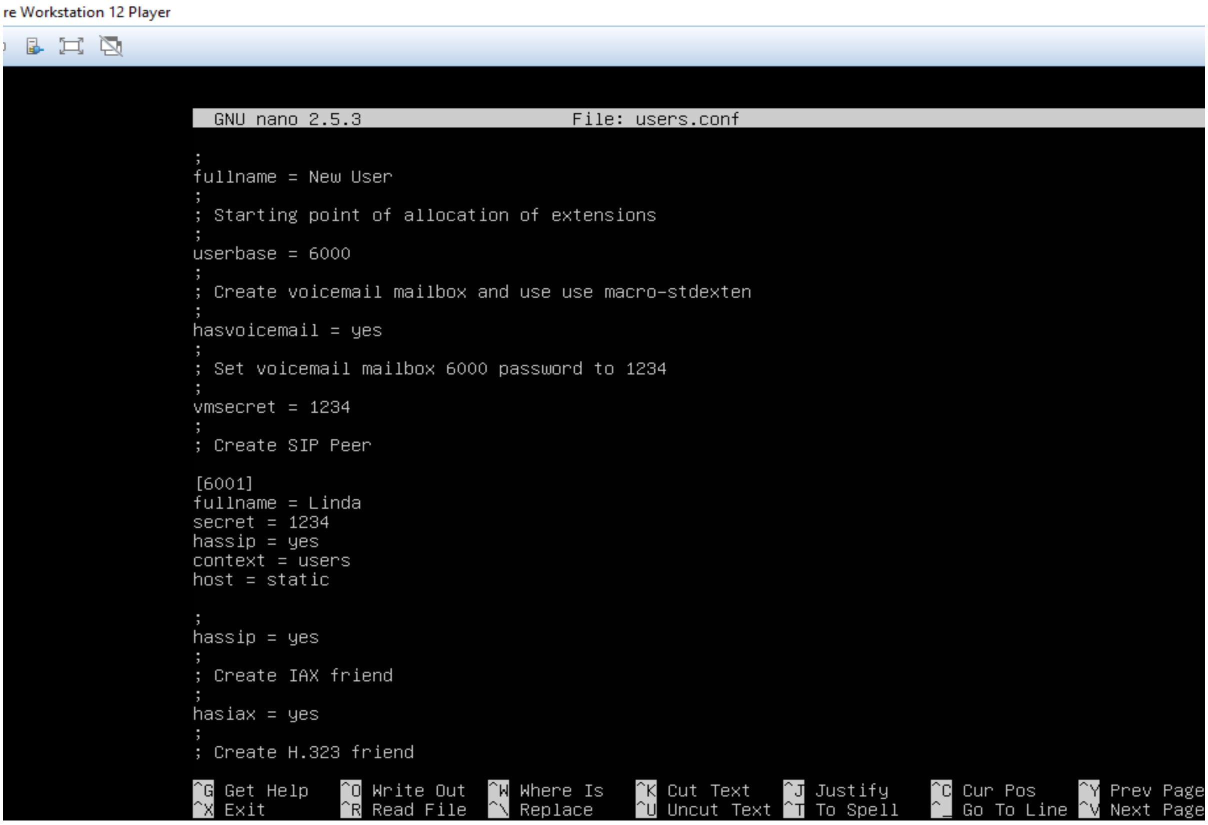


Figure 3.18: Screenshot of the Users configuration terminal

3.6 Softphone on Smart Phone

Several open source softphones are available on all android phones. However, ZOIPER was identified to be the best for this test bed since it supports both SIP and Inter-Asterisk

Exchange IAX operations of the Asterisk server, and compatible with all smart phones. Again, one could view statistics of the parameters displaying the measures of the voice quality of the VOIP calls.[3]

The ZOIPER software was downloaded from the Google[4]play store and installed on Android phones. The https//:www.zoiper.com>documentation website provides detailed instructions to the installation of the software. However, the following were also considered.

1. The user names, passwords, extension numbers of the various users configured in the Asterisk server, and the server information were configured on the client devices (mobile phones) to enable pass of authentication for VOIP communication to be established.
2. The necessary Coder / Decoder CODEC, signaling protocols, etc. were also considered.

Figure 3.19 shows a screenshot of ZOIPER configuration settings. After all the installations and configurations, the VOIP-over-WLAN test bed was ready, and VOIP calls were made between the server and client devices at the defined locations.

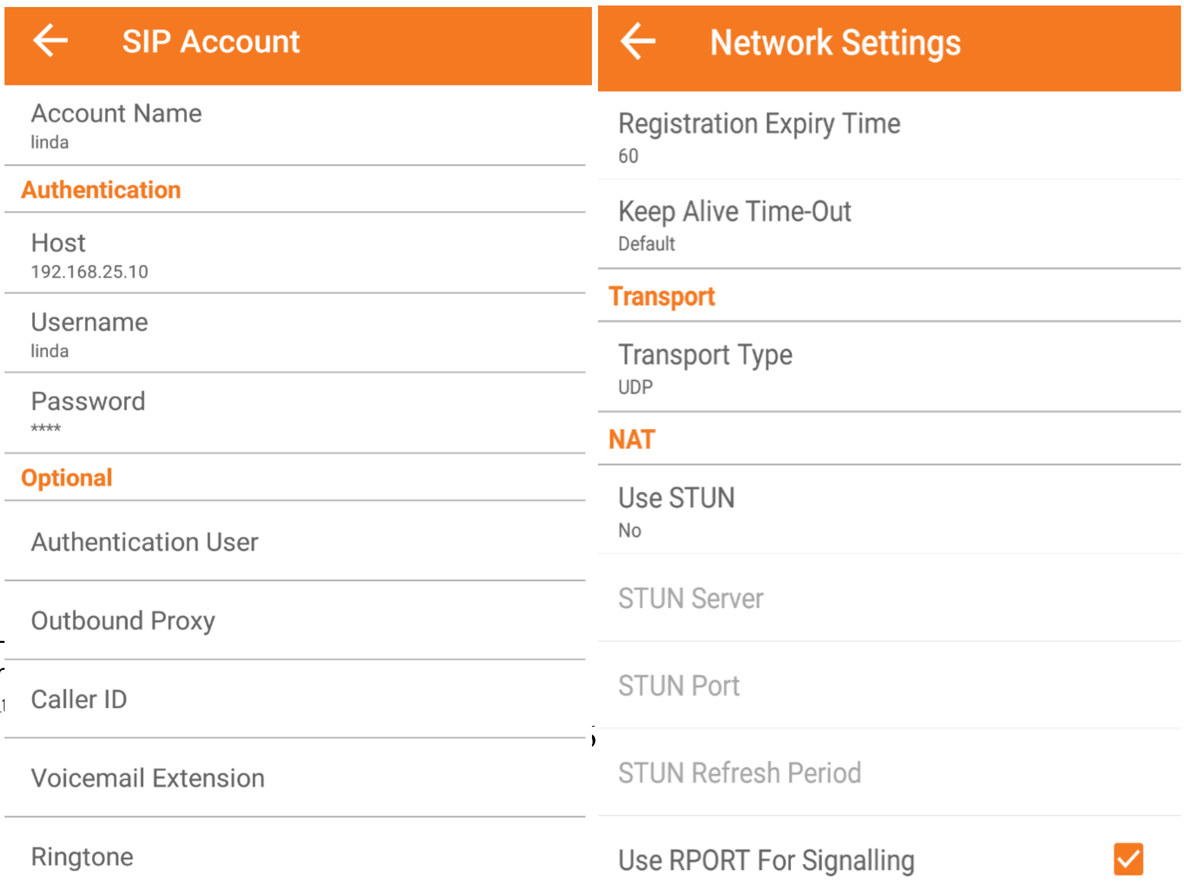


Figure 3.19 Screenshots showing configurations of ZOIPER

3.7 Chapter Summary

This chapter presented the design and implementation of the proposed VOIP-over-WLAN test bed at the Computer Science department. The various steps in the design of the WLAN together with the VOIP system were described. The researcher also explained the configurations and installations of the WLAN, PBX, softphone and the definitions of the operational terms. RF parameters that examine the state of the WLAN were measured. The next chapter will present and discuss the results of the study.

CHAPTER 4: RESULTS AND DISCUSSION

This Chapter presents and discusses the experimental results based on the objectives of the study. The results are presented in tables and graphs with respect to two RF surveys that were conducted, and are organized as follows: (1) the scanned frequencies in the wireless environment, (2) the averages of the scanned frequencies and their mean values of SNR, (3) the overall RF results of the surveys, and (4) the voice quality test corresponding to the respective surveys. Moreover, the Chapter presents the comparative analysis of the results, and the performance issues related to VOIP-over-WLAN are discussed.

4.1 Scanned Frequencies of the Wireless Environment

The scanned frequencies surveys of the wireless environment were the first exercise of the RF survey. Tables 4.1 and 4.2 show the summary results of the scanned frequencies of the wireless environment for Survey 1 and Survey 2 respectively. The exercise revealed the various WAPs and their respective channels, signal strengths, and signal to noise ratio to determine the best channel that could be chosen for the VOIP-over-WLAN test bed.

In Survey 1 (Table 4.1), 21 visible WAPs were identified with their various channels, signal strength, noise floor and signal to noise ratio. The channels used ranged from 1 to 13, and the channels 4, 7, 8, 10, and 13 were exceptional since none of the visible WAPs used them. The values of the signal strength of the WAPs are also ranged from -92dB to -16dB, and the noise floor values are from -98 to -97 with the SNR values ranging from 5dB to 81dB. The Survey 2 (Table 4.2) has only four channels that were seen to be in usage by the various WAPs with signal strength ranging from -28 to -91, noise floor values ranging from -97 to -98, and signal to noise ratio values are from 3dB to 69dB.

Table 4.1: The Scanned Frequencies of the Wireless Environment in Survey 1

SSID	CH	SS	NF	SNR
Eduroam	1	-90	-98	8
Management	1	-91	-97	6
Staff	1	-91	-97	6
Prof FD	2	-90	-97	7
CSCD-Library	3	-90	-97	7
MPhil	5	-68	-97	29
Management	6	-83	-98	15
Staff	6	-84	-98	14
Staff	6	-82	-98	16
Conf	6	-83	-98	15
Eduroam	6	-84	-98	14
Eduroam	6	-83	-98	15
Student	11	-16	-97	81
RobertsGuest Network	11	-90	-97	7
RobertsWiFi Network	11	-92	-97	5
Management	11	-91	-97	6
MA2016	11	-91	-97	6

Staff	11	-16	-97	81
Eduroam	11	-16	-97	81
Staff	11	-90	-97	7
MLE Unit	12	-90	-98	8

*SSID=Service Set Identifier, CH=Channel, SS=Signal Strength, NF=Noise Floor, and SNR=Signal to Noise Ratio

Table 4.2: The Scanned Frequencies of the Wireless Environment in Survey 2

SSID	CH	SS	NF	SNR
Staff	6	-95	-98	3
Eduroam	1	-30	-97	67
Staff	1	-31	-97	66
RIPS PhD	1	-72	-97	25
Management	1	-28	-97	69
Student	1	-30	-97	67
CSCD-Library	5	-88	-98	10
Hairvanity	6	-89	-98	9
King WiFi	6	-60	-98	38
Conf	11	-91	-98	7
WLAN-11G-GW	11	-60	-98	38

*SSID=Service Set Identifier, CH=Channel, SS=Signal Strength,
*NF=Noise Floor, and SNR=Signal to Noise Ratio

4.2 Mean Scanned Frequencies and SNR Values

Table 4.3 (Survey 1) and Table 4.4 (Survey 2) present the mean scanned frequencies and their mean values of SNR. It is clear from table 4.3 that in Survey 1 the channel 11, 6 and 1 are condensed with many WAPs, thus, it not appropriate for the VOIP system. The channels 2, 3, and 12 may be considered for the VOIP system, but they are overlapping channels and are easily identified with channel interferences. Survey 2 (Table 4.4) is not too different from what was observed in Survey 1 (Table 4.3). The channels 1, 6, and 11 are all populated, but channel 5 which is not much occupied has a less SNR value, thus, can be used for the VOIP system.

Table 4.3: The Average Channels and their Respective Average SNR in Survey 1

CH	NOU	AVGSS	AVGNF	AVGSNR
1	3	-90.6	-97.3	6.7
2	1	-90	-97	7
3	1	-90	-97	7
5	1	-68	-97	29
6	6	-83.16	-98	14.84
11	8	-74	-97	23
12	1	-90	-98	8

*CH=Channel, NOU=Number of Users, AVGSS=Average Signal Floor AVGNF=Average Noise Floor, AVGSNR=Average Signal to Noise Ratio

Table 4.4: The Average Channels and their Respective Average SNR in Survey 2

CH	NOU	AVGSS	AVGNF	AVGSNR
1	5	-38.2	-97	58.8
5	1	-88	-98	5

6	3	-81	-98	17
11	2	-75	-98	22.5

*CH=Channel, NOU=Number of Users, AVGSS=Average Signal Floor
AVGNF=Average Noise Floor, AVGSNR=Average Signal to Noise Ratio

4.3 The Overall RF Results of the Surveys

The overall RF results of the Survey 1 and Survey 2 are presented in Table 4.5 and Table 4.6 respectively with the parameters such as distance (D) covered by the signal in meters (M), round-trip time (RTT), packet loss (PL), signal strength (SS), signal-to-noise ratio (SNR), and client connection quality (CCQ). In Survey 1 (Table 4.5), at the Engineering Street (see the coverage area map Figure 2.4), all the parameters for the RF survey recorded the least values, and this may be attributed to its longest distance. The packet loss at all the locations of the coverage area (Figure 2.4) is zero.. The Research Lab recorded the highest value for all the RF parameters measured as it has the shortest distance. Survey 2 (Table 4.6) shows not much different from Survey 1 (Table 4.5) results. However, in Survey 2, the Software Lab presented the least SNR value of 23dBm.

Table 4.5: The Overall RF Results of Survey 1

Location	D (M)	Remarks (LOS)	Min RTT (ms)	Max RTT (ms)	Avg RTT (ms)	PL %	SS (dBm)	SNR (dBm)	CCQ %
Research Lab	10	Presence of florescent light, electrical cables and mobile phone operations	1.13	66.67	27.11	0	-36	63	100
Research Lab Entrance	15	Thick walls and glass windows and doors	1.61	111.06	44.58	0	-71	28	84
Car Park	30	Thick walls and glass windows and doors	1.84	128.74	61.33	0	-74	25	93
Software Lab	40	Tree branches, florescent light, electrical cables, mobile phones	25.86	130.72	73.44	0	-78	21	99
Engineering Street	60	Trees, Tall buildings, thick walls	1.9	212.39	103.15	0	-83	16	79

*D(M) = Distance in Metres, LOS = Line Of Sight, RTT=Round Trip Time
PL=Packet Loss, SS= Signal Strength, SNR = Signal to Noise Ratio, CCQ = Client Connection Quality

Table 4.6: The Overall RF Results of Survey 2

Location	D (M)	Remarks (LOS)	Min RTT (ms)	Max RTT (ms)	Avg RTT (ms)	PL %	SS (dBm)	SNR (dBm)	CCQ %
Research Lab	10	Presence of florescent light, electrical cables and mobile phone operations	1.27	35.77	11.33	0	-21	77	100
Research Lab Entrance	15	Thick walls and glass windows and doors	1.11	116.71	38.4	0	-52	46	99
Car Park	30	Thick walls and glass windows and doors	38.82	114.03	91.04	0	-53	46	99
Software Lab	40	Tree branches, florescent light, electrical cables, mobile phones	2.31	116.21	95.86	0	-75	23	95
Engineering Street	60	Trees, Tall buildings, thick walls	25.86	130.72	73.44	0	-68	31	92

*D(M) = Distance in Metres, LOS = Line Of Sight, RTT=Round Trip Time

PL=Packet Loss, SS= Signal Strength, SNR = Signal to Noise Ratio, CCQ = Client Connection Quality

4.4 Quality of Voice Test

The sample results of the quality of voice test for Survey 1 are represented in Figures 4.1–4.5, and Figures 4.6– 4.10 present the sample results of Survey 2. In Figures 4.1 – 4.10, the blue bar represents the jitter, red bar represents the latency, green bar for packet loss, and indigo bar represents the SNR values.

Example 1: voice quality test at Research LAB

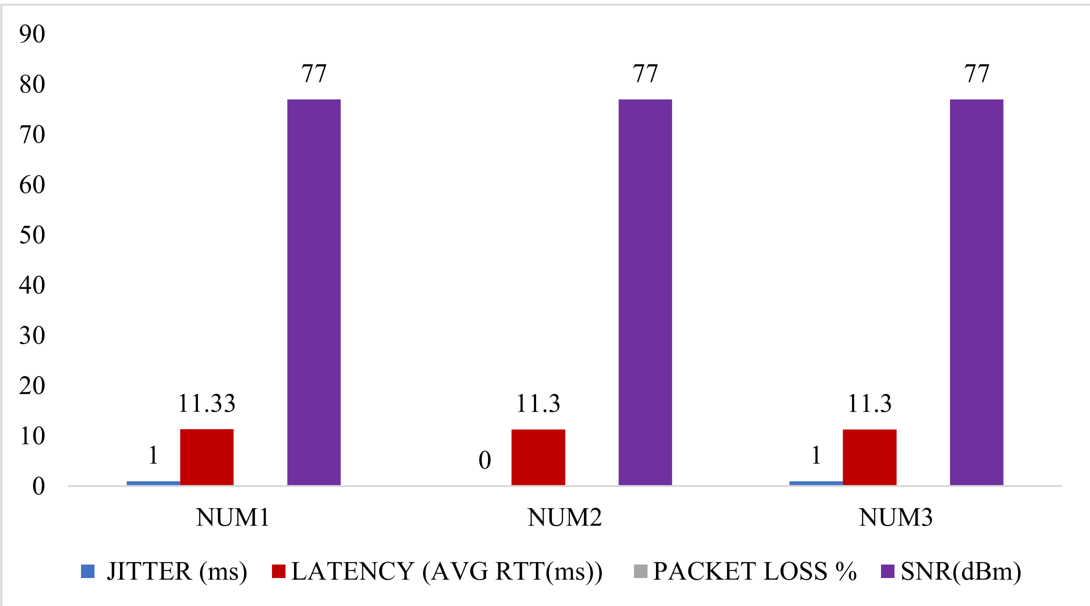


Figure 4.1: Voice quality test at the Research LAB

Three different calls were instantiated at the said location and the various metrics that measure the quality of voice transmitted were measured. Of the three different calls, 1ms was the highest jitter value recorded at the research lab during the VOIP calls and 0ms was the least jitter value recorded at the same location with 0% packet loss, 11.33 latency and 77dB for SNR value.

Example 2: voice quality test at Entrance of Research LAB

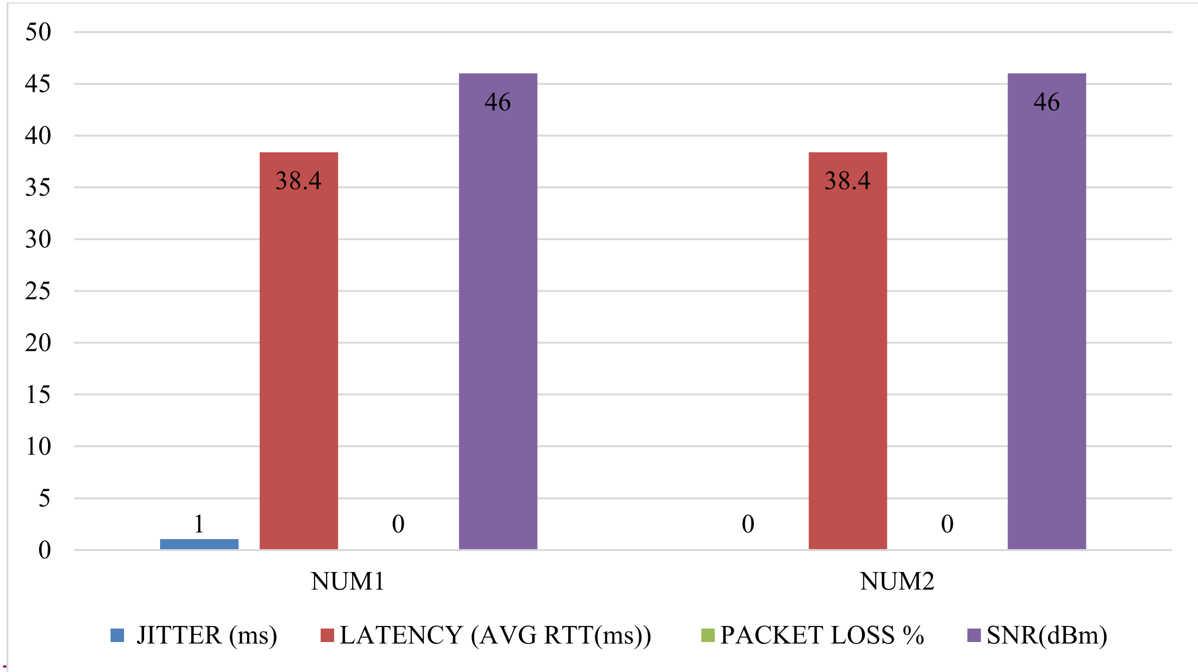


Figure 4.2: Voice quality test at the Entrance of Research LAB

Figure 4.2: Two main calls were instantiated at the entrance of the Research Lab and the various metrics that measure the quality of voice transmitted were measured. From the two different calls, 1ms was the highest jitter value recorded at the location during the VOIP calls and 0ms was the least jitter value recorded at the same location with 0% packet loss, 38.4latency and 46dB for SNR values. Jitter and packet loss values in figure 4.2 were not so different from that of figure 4.1.

Example 3: voice quality test at Software LAB

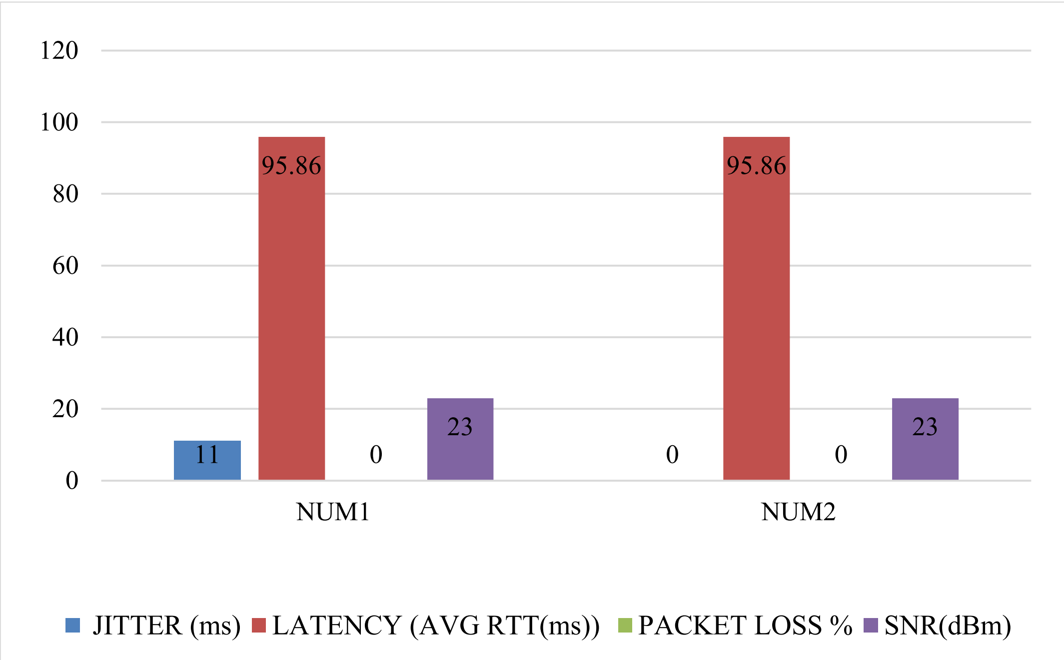


Figure 4.3: Voice quality test at the Software LAB

Figure 4.3: Again, two calls were instantiated at the software LAB and the various metrics that measure the quality of voice transmitted were measured. 11ms was the highest jitter value recorded at the location during the VOIP calls and 0ms was the least jitter value recorded at the same location with 0% packet loss, 95.86 latency and 23dB as SNR value.

Example 4: voice quality test at the car park location during the VOIP calls. 1ms was the least jitter value recorded at the same location with 0% packet loss, 91.04 latency and 46dB as SNR value.

Example 4: voice quality test at the Car Park

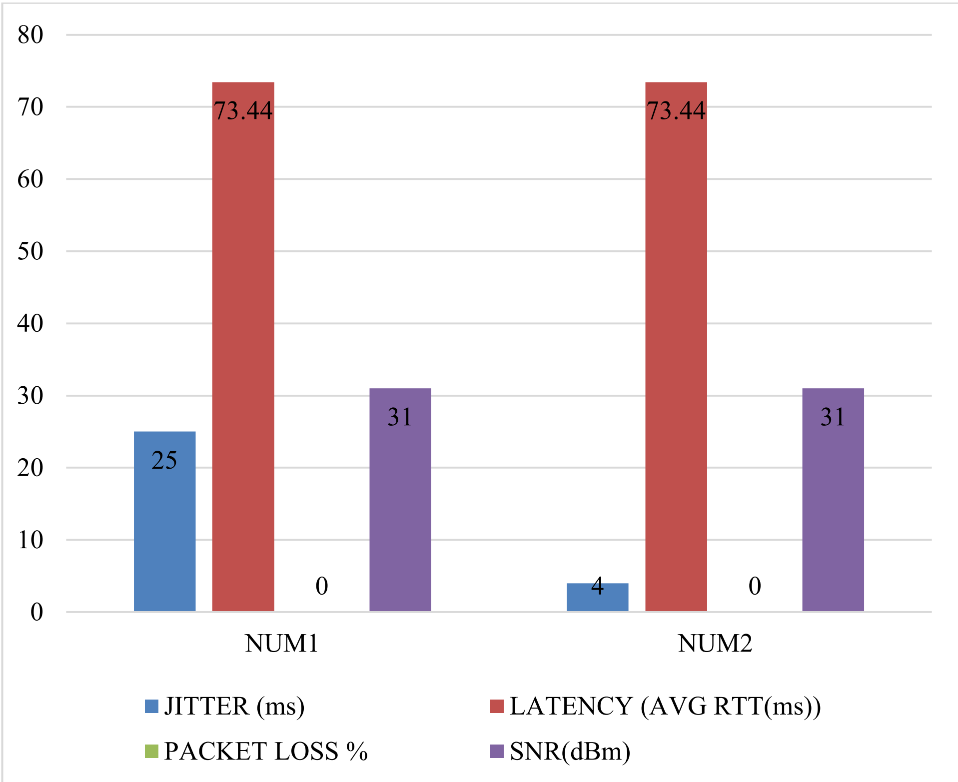


Figure 4.4: Voice quality test at the Car Park

Figure 4.4: All the two calls instantiated at the car park recorded 25 ms and 4ms jitter values. Other metrics recorded were 0% packet loss, 73 latency and 31 as SNR value.

Example 5: voice quality test at the Engineering Street

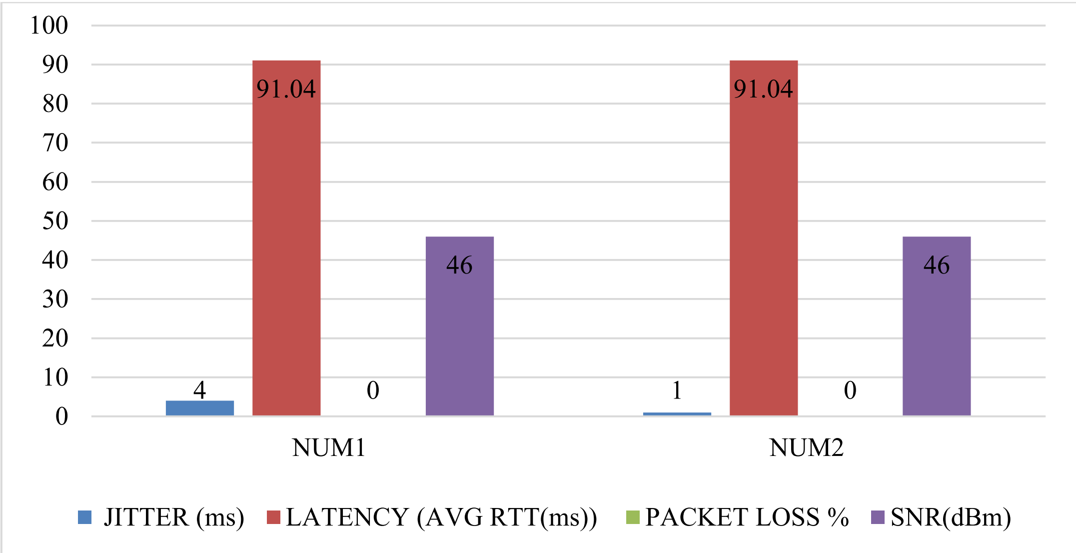


Figure 4.5: Voice quality test at the Engineering Street

Figure 4.5: All the call instantiated at the Engineering Street recorded the highest latency as 91.04dBm. Jitter values as 4ms and 1ms. Packet loss was 0% and SNR value was 46 for all the calls at the location.

4.5 Comparative Analysis of the Results

This section seeks to interpret the values of the descriptive statistical tables and figures earlier presented in this chapter. The goal of the study is to find out if the wireless environment of the Centre is ready for a VOIP system and if ready, how well would the inherent WLAN challenges be properly managed to efficiently support the VOIP system at the department.

Wireless Environmental Test

An environment to be assessed as conducive for additional WLAN to support VOIP system is dependent on parameters that measure the general performance of the WLAN in an area, the signal strength of the user devices, the noise floor of the area and the signal to noise ratio (SNR). It is known that the speed and viability of a wireless signals drop as more and more users use the same channel within the wireless environment. Other forms of interference to the performance of the WLAN in an environment are the various forms of channel interferences these are the co-channel, adjacent channel and overlapping channel interferences.

In the descriptive statistical table 4.1, the results of the scanned frequency exercise of the experiment present the researcher with the details about the wireless environment of the Centre. In the Table, a total of twenty-one (21) wireless access points (WAPS) were in operation at the Centre. This means that there were several users on the 2.4 GHz of the wireless LAN and this may cause the speed and viability of the wireless signal drop. However, attention to the channel distributions in table 4.3 of the first RF survey indicates that the non-overlapping channels (1, 6 and 11) were all occupied with many users and with a mean SNR value of 6.7, 14.84 and 23 respectively. Jim Geier tutorials on how to define minimum SNR values for signal coverage indicates the following:

Table 4.7: The General Acceptable Signal to Noise Ratio

S/N	SNR VALUES	EXPECTED PERFORMANCE AND QUALITY
1	>40dB SNR	Excellent signal, always associated; lightning fast.
2	25dB to 40dB SNR	very good signal; always associated; very fast.
3	15dB to 25dB SNR	low signal, always associated; usually fast.
4	10dB to 15dB SN	very low signal; mostly associated; mostly slow.
5	5dB to 10dB SNR	No signal, not associated; no go

Comparisons of these SNR values from Jim Geier in his tutorials to the scanned frequencies of the wireless environment at the Centre in table 4.1 indicates that only three WAPS were with excellent signal strength of 81dB SNR value, one access point was with 29dB SNR value to indicate very good signal strength, four were with low signal strength with 15dB SNR values and the rest of the WAPS were with very low and no signals. Reasons for very low SNR values may be due to some forms of interference: both in the sense of objects in the signal path and other operations of 2.4GHZ transmitters ("wireless networking - Wifi poor SNR, reasons and solutions: - Super User," 2010).

The corresponding channels to the excellent signal strength, very good and low signal strength are channel 11, 5 and 6 respectively. This signifies that the Centre is with many users on the 2.4GHZ wireless LAN but with many poor SNR values with most of the Wireless Access Points. WAPS with averagely good signal strength were all concentrated in channel 11 and 6, therefore, there is an existing non-overlapping channel which is channel 1 and the rest of the channels for an efficient and resilient WLAN performance.

Wireless LAN performance test

In the knowledge of identifying the general performance of the WLAN at the Centre, the techniques of WLAN performance measurement used resulted in the RF surveys statistically described in Table 4.5 and 4.6 for both first and second survey respectively. In these Tables are values of the determinants metrics that exhibits the overall WLAN performance at the various locations.

SNR value measured at the client device puts on view the general performance of the WLAN at the Centre. However, the underlining parameters that determine the good to bad values of SNR are the location and distance of the client device from the WAP, remarks on the LOS (Line of Site) between the WAP and the client device, signal strength and the noise floor.

The client device at the location of the Research Lab records the closest distance of 5m from the WAP and the Engineering Street with the furthermost distance of 90 meters from the WAP. The WAP supposedly operates within 100 metre square. The closeness of client device to the WAP mostly warrants excellent signal strength which may also result in an excellent SNR value to depict excellent WLAN performance (How to: Define Minimum SNR Values for Signal Coverage 2013). The signal strength attenuates as distance to WAP increases. In other words, the signal strength is a function of the distance between the client device and the WAP (Range & Capability, 2012;Sanguino & Roberts, 2011). With 90m closeness to the WAP as the farthest distance within the coverage area is an indication that the WLAN would perform very well at the Centre in general.

Presence of fluorescent lights, electrical cables and mobile phones operations at the Research and software Lab as remarks on the LOS adds onto the value of the background noise and other forms of interferences to reduce the received signal strength at the client device (Cisco 2007).The reason is that these materials mentioned earlier share the common 2.4GHZ band with the WLAN. In this case, records of the signal strength values at the various locations could have been better without these materials mentioned present at the labs. Again, signal strengths attenuate as it passes through materials (Cisco 2007). The presence of walls, metal pillars, glass windows at the Centre also causes some form of interferences to the radio signal. In general, the presence of these materials is an indication of troubles to the performance of the WLAN.

Table 4.8: The General Acceptable Signal Strengths

Signal Strength	Performance	Expected Quality	Required For
-30 dBm	Amazing	Max achievable signal strength. The client can only be a few feet from the AP to achieve this. Not typical or desirable in the real world.	N/A
-67 dBm	Very Good	Minimum signal strength for applications that require very reliable, timely delivery of data packets.	VoIP/VoWiFi, streaming video
-70 dBm	Okay	Minimum signal strength for reliable packet delivery.	Email, web
-80 dBm	Not Good	Minimum signal strength for basic connectivity. Packet delivery may be unreliable.	N/A
-90 dBm	Unusable	Approaching or drowning in the noise floor. Any functionality is highly unlikely.	N/A

The received signal strength of the client device is a good metric together with the noise floor indicates the SNR value that shows the general performance of the network (WiFi Signal Strength Basics | MetaGeek 2016). From the table above, a good signal strength value for VOIP ranges from -67dB to -30dB. However, the first survey result shown in Table 4.5 indicates -83dB to -36dB as a range of values for signal strength. These values on their own were not good for VOIP communication except that values for noise floor from the same survey were reasonably good resulting in good SNR values. Again, the second survey recorded encouragingly good values for signal strength ranging from -75 to -21 in Table 4.6

at the research lab location, a signal strength of -36dB and a noise floor value of -99 dB resulting in a signal to noise ratio (SNR) value of 63 (i.e. -36 – (-99) = 63) from table 4.5 specifies a good signal to the performance of the WLAN. The signal strength of negative values closer to zero and greater than the background noise is a good indication for the good performance of the network. Cause of low signal strength values in a wireless network is mostly due to the distance between the AP and the client devices, obstructions of constructions materials in the wireless environment and other interferences from 2.4GHZ devices (Reasons for a Low WiFi Signal | Chron.com 2015).

The SNR value is basically the difference in decibels between the signal strength and the noise floor (Cisco Systems 2015). Its value ranges from 0 to 120 (Fundamentals 2014; MILLER KAYLE 2010). SNR values from 5dB to 25dB only indicates the poor performance of the network whiles SNR values greater than 25dB and above indicates very good to the excellent performance of the network (How to: Define Minimum SNR Values for Signal Coverage 2013). In Table 4.6, SNR values ranges from 23dB to 77dB. The software lab records the least value of 23dB and the rest of the locations at the Centre records SNR values from 31 to 77. These values indicate a good performance of the WLAN. However, Table 4.5 showing RF survey results for the first survey also records SNR values ranging from 16dB to 63dB. 16dB at the Engineering Street specifies week performance of the WLAN at the said location. This indicates that the received signal strength in the second survey from table 4.6 exhibits an excellent performance of the network and Table 4.5 also puts on view a fairly good performance of the network. Excellent SNR values are mostly obtained when the signal strength is far greater than the background noise and with this data, transmissions would be without interferences (Fundamentals 2014). Poor SNR value is an indication of enablement of data corruption and re-transmissions to create a delay which also affects the general performance of the network (Cisco Systems 2015; How to: Define Minimum SNR Values for Signal Coverage 2013).

Average Round Trip Time (AVG RTT) is another important metric that specifies delay and latency value in the performance of the WLAN from the client device's point of view. It is the average travel time it takes for a packet to reach its destination from the source and to the destination from the source (two-way) (Ghoumid and Ameziane 2013). RTT can range from 0-300 milliseconds: few milliseconds under ideal conditions between closely spaced points to several milliseconds under adverse conditions between points separated by a large distance (El et al. 2013). Large milliseconds value of RTT causes echoes and overlapping noises in the system, hence the need to read at least the maximum tolerable value for RTT, 150ms for a one-way trip (Ghoumid and Ameziane 2013). All the various locations at the Centre recorded RTT values between 11.33ms and 103.15ms for both RF surveys. These values are far below the maximum tolerable value for RTT and are a good indication that there were not much delay in the system, specifying that the WLAN performance is also good. Courses of high RTT values may be to latency from the network devices, media path and various forms of delay (transmission delay, processing and queuing delay, propagation delay. etc.) (El et al. 2013).

Another metric to consider in the measurement of the performance of the wireless network is the Packet Loss. Packet loss is the failure of a number of data transmitted to reach the intended destination (Worldwide 2014). This is mostly caused by the inadequate signal strength of the client device (Modules and Diego 2016). Real-time communications systems normally tolerate 0-1% as a range of values of packet loss (Roychoudhuri and Al-Shaer 2005). In VOIP systems packet loss values greater than one results in mutilated received voice and this is noticeable by the receiver of the VOIP call (Wang 2013). From all the results of both first and second survey, packet loss of 0% is recorded at every location of the Centre. This means that all the data transmitted from the source to the destination reached the destination successfully. This is an indication of the excellent performance of the network.

Quality of voice test

For VOIP to be the possible alternative of the GSM communication services at the Centre, it is not enough to be cheaper, easy to deploy and easy to maintain. It must provide better call quality or at least call quality equal to the GSM calls to create enough motivation to an end-user to switch to VOIP. For this reason, voice quality test is a very important exercise to determine the success of any VOIP system deployed. After the deployment of the VOIP system on the WLAN, this exercise was performed to measure metrics that determine the voice quality transmitted in the VOIP system. The metrics measured are jitter, packet loss and delay.

Jitter as a metric to the measurement of the voice quality in the VOIP system refers to the variations of delay in receiving voice data packets (Cisco Systems 2006). This variation in delay is detrimental to voice quality and voice data in general and mostly occurs when voice packets face different amount of time over during call periods over the IP network (What is Acceptable Jitter? – Datapath.io – Medium 2014). This is mostly caused by network congestion, improper queuing or configurations errors (Cisco Systems 2006). In order for voice to be clear, successive voice packets must arrive at regular time intervals. Voice packets normally tolerate about 20ms jitter values (Cisco 2001; VoIP jitter tolerance - Learn how to Troubleshoot 2014). High jitter values greater than 30ms are unbearable to the end-user since it creates jerky voices which are glitches to the ear (VoIP jitter tolerance - Learn how to Troubleshoot 2014). The examples of calls in figure 4.1 to 4.5 records jitter values within the said range except that of the calls at the Engineering Street location which recorded jitter values of 25ms. In general, the jitter values recorded exhibits a very good performance of the VOIP system.

Packet Loss as describe in the previous section is the failure of the voice data to reach its intended destination from the source. VOIP can only tolerate up to a percentage of one (1%). Values greater than 1% create large gaps in the communication perceivable by the end-user. In the examples of voice quality tests presented in figure 4.1 to 4.5. All calls recorded 0% packet loss. This is as the result of the usage of the separated WLAN for the VOIP system.

Delay

This metric is normally said to be the travel time of the voice packet between the source and destination. Measuring of delay in any network system is a known complex task because of the varied forms of delay such as propagation, queuing, transmission etc in any communication system and the challenge of time synchronization between the sending and receiving nodes. This complex task is beyond the scope of the study. Hence, PING, an ICMP payload to determine the average RTT value and diving it into two gives us an approximation time of delay in the system. Delay time values ranging from 0 to 150ms is an acceptable range of values for the VOIP system and greater than the 400ms range of values are unacceptable for the general performance of the network. In the examples of voice quality tests presented in figure 4.1 to 4.5. All calls recorded less than 150ms for RTT values, meaning Delay time values in the mentioned figures are less than 75ms which falls within the acceptable range of values. This is as the result of the usage of the separated WLAN for the VOIP system.

Comparison of the VOIP system and GSM at the Centre

GSM and VOIP are both systems that enable communication in our world today. These systems are with their own benefits and disadvantages as well. VOIP is normally identified with voice quality and connectivity challenges. However, the test bed designed at the Department of Computer Science indicated an excellent connectivity and a very good voice quality which is the same as that of the GSM connectivity and quality of voice transmitted at the Department. This could be attributed to the fact that a private data network was used for the deployment of the VOIP system.

4.6 Performance Issues of VOIP-over-WLAN

The general performance of the VOIP-over–WLAN system was promising but not exceptional. The considerable issues that affected the performance of the system are discussed such as Line of Sight (LOS), obstructions from construction materials, and other forms of interferences are discussed here. **The line of Sight and Obstructions:** The presence of tall ornamental trees and other tree branches at the Centre did not enable excellence performance of the VOIP system.

Obstructions from construction materials: Tick walled and tall buildings present at the department affected the general performance of the VOIP system at the Centre.

Other forms of interferences: The presence of fluorescent light, electrical cables and mobile phones at the centre also affected the overall performance of the VOIP system.

4.7 Findings of the Study

The results of the study show that using WLAN for the VOIP has a great potential of providing free communications services. The results obtained at all the coverage area locations, with the exception of the Engineering Street which is the longest much distance from the WAPs, were promising. The RF Survey 2 results reveal that the WAPs present at the coverage area are either with low signal strengths, SNR values or are operating in different channels. This significant result from the survey gives an indication that the network performance is very good at all locations of the coverage area. Again, the RF Survey 2 recorded poor values for the network performance metrics especially at the Engineering Street, which is the longest distance from the WAPs.

Moreover, putting together the results of the two surveys, there is an indication that the network performance may be very poor when all the WAPs present are up with good signal strengths, SNR values and are operating on the three main non-overlapping channels at the coverage area. Finally, the result of the quality of voice test with VOIP calls gives an indication that the voice quality for the VOIP-over-WLAN system is very good.

4.8 Chapter Summary

In this Chapter, the researcher described the results of the experiments that measured and examined the readiness of the Centre for the VOIP system, the network performance metrics for the Wireless LAN and the voice quality test for the VOIP calls made at the Centre. The main goal of the experiments was to determine how well the VOIP system could perform on the Wireless LAN at the Centre and find out if the VOIP system could replace the already existing GSM as means of communication at the department. The experimental results show that VOIP-over-WLAN has potential in providing free means of communication at the Centre and can alternate the use of GSM. However, LOS, obstructions from construction materials and other forms of interferences issues affected the performance of the VOIP system at the Centre. The results of the study were discussed. Summary and future works are presented in the next Chapter.

CHAPTER 5: CONCLUSION

5.1 Summary

Communication on UG campus has experienced a significant revolution over the years till now. From PSTN, GSM, 3^{RD} and 4^{TH} (3G/4G) smart phones all provided by the Telecommunication Networks. The evolution of IP networks and VOIP systems has enabled free communication services on a converged data network with some known challenges, hence the birth of this research work which will enable the researcher to see how well the VOIP system will behave on a private data network (wireless).

5.2 Conclusion

This thesis provided an experimental study into the design and deployment of a VOIP-over-Wlan system at the Department of Computer Science on UG-Campus to first examine how well the VOIP-Over-Wlan system would be feasible to adopt on UG-Legon campus. Again, knowing the inherent challenges of wireless technology, the study sought to find out how well these challenges could be managed to support the VOIP system. Finally the study performed a comparative test on the performance of the VOIP-Over-Wlan system to GSM at the department.

First of all, the research sought to find out the main components of the VOIP-Over-Wlan system and the determinants factors that ensure quality performance of the system. It has been identified in Chapters 2 and 3 that the private wireless network and the VoIP system are the main components of the VOIP-Over-Wlan system and the determinants that ensure quality performance of the system are signal strength (SS) of the devices, signal to noise ratio (SNR), which goes a long way to indicate high Jitter, Latency and packet loss values.

Secondly, the research sought to find the extent of suitability of the wireless network to the VOIP application. With reference to the RF site survey reports in Chapter 3, it has been identified that the wireless LAN technology is most suitable for the VOIP application once the environment is with little or no forms of interferences.

Again, the study revealed the following as answers to the third research question.

i. One may not know when an additional wireless access points would be configured in the wireless environment, but configurations of more wireless access point in the environment may degrade the quality of the VOIP system.
ii. Broadcast collision is inevitable once a new wireless device is introduced without proper configuration.
iii. Speed reduces when more clients are introduced.
iv. Vulnerability of wireless systems in relation to security.
v. The wireless system could be connected but not working without working.

Finally, the inherent challenges of the wireless LAN for the system were managed by regular monitoring of the wireless environment of the VOIP system.

5.3 Recommendations

The completion of this research has proposed the use of dedicated frequency channel from National Communication Authority for the VOIP-Over-Wlan so that channel interference would not be a challenge to the system. This is necessary since the VOIP system comes with many benefits and these benefits could be maximized once the system is well designed and the wireless environment is well monitored and properly managed.

5.5 Further Work

The goal is to improve on timely monitoring of the wireless environment of the VOIP system. Future work may include studies on how the VOIP System would identify the inherent wireless network challenges and employ the needed technique to manage the challenges by itself.

REFERENCES

Airtel Ghana | Legacy Tariff.(2017). Retrieved May 16, 2018, from http://www.africa.airtel.com/wps/wcm/connect/AfricaRevamp/Ghana/Home/Personal/Voice and Text/tariff plans/Legacy Tariff.

Aigbe, P., &Akpojaro, J. (2014).Analysis of Security Issues in Electronic Payment Systems.*International Journal of Computer Applications*, *108*(10), 975–8887. https://doi.org/ 10.5120/ 18946-9993.

Arora, R. (2000). Voice over IP : Protocols and Standards. *Components*, 1–20.

Ayokunle, O. O. (2012). Implementing Security on a Voice over Internet Protocol (VoIP) Network : A Practical Approach, *7*(4), 24–30. https://doi.org/10.9790/0661-0742430

Banerji, S., &Chowdhury, R. S. (2013). On IEEE 802.11: Wireless Lan Technology. *International Journal of Mobile Network Communications & Telematics, 3*(4), 45 – 64. https"//doi.org/10.5121/ijmnct.2013.3405.

Behrouz A. Forouzan. (2013). Data *Communications and Networking*.

Benefits of Using VoIP Technology – (2015). Retrieved May 16, 2018, from http://www.precisinit.com/benefits-of-using-voip-technology/

Beuran, R. (2006). VoIP over Wireless LAN Survey.*Science And Technology*, 1 – 40.

Backs, P., &Pohlmann, N. (2008).Influence of Security Mechanisms on the Quality of Services of VoIP.*ISSE 2008 Securing Electronic Business Processes*, (2008), 341–346. https://doi.org/10.1007/978-3-8348-9283-6_36

Bansal, R. (1998). Wireless IP Telephony, *7*(2), 239–243.

Batchvarov, A. (2004). Security Issues and Solutions for Voice over IP compared to Circuit Switched Networks. *Communication*, 1–14.

BBC - Standard Grade Bitesize Physics - Communication using waves : Revision, Page 5. (2014). Retrieved May 18, 2018, from http://www.bbc.co.uk/bitesize/standard/ physics/ telecom unications/communication_using_waves/revision/5/

BehrouzA.Forouzan. (2013). *Data Communications and Networking*.

Beuran, R. (2006). VoIP over Wireless LAN Survey.*Science And Technology*, 1–40.

Beyh, S., &Kagioglou, M. (2004). Construction sites communications towards the integration of IP telephony. *International Journal of Information Technology in Construction*, *9*(April 2003), 325–344. Retrieved from http://www.itcon.org/2004/23

Bryant, R., Madsen, L., &Meggelen, J. Van. (2013). *Asterisk: The Definitive Guide: The Future of Telephony Is Now*.

Butcher, D., Li, X., &Guo, J. (2007).Security challenge and defense in VoIP infrastructures.*IEEE Transactions on Systems, Man and Cybernetics Part C: Applications and Reviews*, *37*(6), 1152–1162. https://doi.org/10.1109/TSMCC.2007.905853

Banerji, Sourangsu, and Rahul SinghaChowdhury. 2013. "On IEEE 802.11: Wireless Lan Technology." *International Journal of Mobile Network Communications & Telematics* 3(4): 45 – 64. http://www.airccse.org/journal/ijmnct/papers/34qwijmnct05. Pdf.

Consider Separating Your Data and VoIP Networks. (2012). Retrieved May 14, 2018, from http://www.sipvine.com/blog/bid/53855/Consider-Separating-Your-Data-and-VoIP-Networks.

Cisco. (2001). Quality of Service for Voice over ip, (I), 1 – 44.

Cisco. (2007). 20 Myths of Wi – Fi Interference: Dispel Myths to Gain High – Performing and Reliable Wireless. *Cisco. Com,* 1 – 9, Retrieved from http://www.ci.sco. com/c/en/us /products/collateral/wireless/spectrum-expert-wi-fi/prod-white-paper 0900 aecd 807395 a9.pdf.

Cisco Systems. (2006). Understanding Jitter in Packet Voice Networks (Cisco IOS Platforms) Jitter in Packet Voice Networks. Cisco Systems, 189o2. https://doi.org/18902.

Chen, C.-L. (2013). Combining the quality of services path first routing and admission control to support VoIP traffic. *Future Generation Computer Systems*, *29*(7), 1742–1750. https://doi.org/http://dx.doi.org/10.1016/j.future.2012.03.026

Cisco. (2001). Quality of Service for Voice over IP, (1), 1–44.

Cisco. (2007). 20 Myths of Wi-Fi Interference : Dispel Myths to Gain High- Performing and Reliable Wireless. *Cisco.Com*, 1–9. Retrieved from http://www. cisco.com/c/en/us/ products/collateral/wireless/spectrum-expert-wifi/prod_white_paper0900aecd807395a9.pdf

Cisco Systems. (2015). Wireless fundamentals: Signal-to-Noise Ratio (SNR) and wireless signal strength - Cisco Meraki, 1–3. Retrieved from https:// documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Wireless_fundamentals%3A_Signal-to-Noise_Ratio_ (SNR)__and_wireless_signal_strength

Communications, A., & Authority, M. (2006). AM radio issues, (January).

Dantu, R., Fahmy, S., Schulzrinne, H., &Cangussu, J. (2009). Issues and challenges in securing VoIP. *Computers and Security*, *28*(8), 743–753. https://doi.org/10.1016/j.cose. 2009.05.003

Davidson, J. (2006). Voice Over IP Fundamentals, 394. Retrieved from https://books.google.com/books?id=MLxfy6W8bxgC&pgis=1

El-metwally, E.S.E. (2012). Master's thesis summary Performance Evaluation of VoIP Quality Schemes Submitted by Name:, (January).

Egbenyon, D. (2011). Implementing QoS for VoIP in a Local Area Network (LAN).

Feng, Z. (2017). Introduction of Wi-Fi standardization and Interoperability Certification Test.

Gast, M. (2005). *802.11 wireless networks : the definitive guide*. O'Reilly.

Habib, B. M., &Bulusu, N. (2002).Improving QoS of VoIP over WLAN (IQ - VW) Project Research Paper Computer Communications University of Colorado at Colorado Springs, (December).

Help How to separate VOIP and data networks while only using one router? – Spiceworks. (2016). Retrieved May 14, 2018, from https://community.spiceworks.com/topic/469812-help-how-to-separate-voip-and-data-netwroks-while-only-using-one-router.

HKSAR.(2008). VPN Security, (February), 24.Retrieved from http://www.infosec. gov.hk/ english/technical/files/vpn.pdf.

Internet Telephony. (2018). Retrieved from https://www.nfon.com/en-de/cloud-telephone-system/resources/glossary/internet-telephony/

Hersent, O., Petit, J.-P., &Gurle, D. (2005).Beyond VoIP Protocols.*PhD Proposal*, *1*. https://doi.org/10.1017/CBO9781107415324.004

Ilyas, E., &Tomader, M. (2016).Study of the security aspect of networks based on SIP and H323 protocols, *16*(9), 69–75.

Jalendry, S., &Verma, S. (2015). A Detail Review on Voice over Internet Protocol (VoIP), *23*(4), 161–166.

Ji, M., & Technology, I. (2017). Designing and Planning a Campus Wireless Local Area Network, (May).

K.Mishra, B., K. Singh, S., & Patel, K. (2012). Performance Analysis of Various Codecs using RSVP on VoIP Quality of Service over Variable Bandwidth. *International Journal of Computer Applications*, *41*(7), 28–36. https://doi.org/10.5120/5555-7630

Kennedy, G. (2011). *Kennedy ' s Electronic Communication Systems*.

Kumar, A. (2006). an Overview of Voice Over Internet Protocol (Voip), *2*(1), 1–13.

Kumar, A. (2006). An Overview of Voice Internet Protocol (Voip), 2(1), 1 – 13.

K. Mishra, B., S. K. Singh, and Kalpana Patel. 2012. "Performance Analysis of Various

Codes Using RSVP on VoIP Quality of Service over Variable Bandwidth." *International Journal of Computer Application* 41 (7): 28 – 36.

Lammle, T. (2008).*CCNA: Cisco Certified Network Associate: Fast Pass*. Retrieved from https://books.google.com/books?id=PARCyPSSkF8C&pgis=1

Latif, T. (2007).MASTER ' S THESIS Adoption of VoIP.

Lazzez, A. (2013). VoIP Technology: Security Issues Analysis. *International Journal of Emerging Trends & Technology in Computer Science*, *2*(4), 1–9. Retrieved from http://arxiv.org/abs/1312.2225

McCabe, J. D. (2007). Network design, 385–431. https://doi.org/10.1016/B978-012370480-1/50011-6

Mehdi, G. (2009). Future of VoIP over Wireless in Economic Downturn.*Technology*, (November), 55.

Michigan, L. (2002). Yerkes Summer Institute 2002.

Mupparapu, M. (2008). Voice over Internet protocol for the orthodontic practice: A sensible switch from plain old telephone service. *American Journal of Orthodontics and DentofacialOrthopedics*, *133*(3), 470–475. https://doi.org/10.10 16/j.ajodo. 2006.09. 048

Mehdi, G. (2009). Future of VoIP over Wireless in Economic Downturn.*Technology,* (November), 55.

Mupparapu, M. (2008). Voice over Internet protocol for the orthodontic practice: A sensible switch from plain old telephone service. *American Journal of Orthodontics and DentofacialOrthopedics,* *133* (3), 470 – 475.https://doi.org/10.1016/j.ajodo.2006.09.048.

Nagar, R. A. M., & Delhi-, N. E. W. (2016).Multicolour Illustrative Edition Principles of.

NASA.(2010). Anatomy of an Electromagnetic Wave. Retrieved May 18, 2018, from https://science.nasa.gov/ems/02_anatomy

Nwebonyi, F. N. (2014). VOIP Security : Threats , And Counter Measures, *1*(6), 1–12.

Obidinnu, J. N., &Ibor, A. E. (2016).A survey of Attacks on VoIP networks and Countermeasures.*West African Journal of Industrial and Academic Research*, *14*(1), 28–38. Retrieved from http://www.ajol.info/index.php/wajiar/article/view/128074

Open Source VOIP Software - VoIP-Info. (2003). Retrieved September 7, 2018, from https://www.voip-info.org/open-source-voip-software/

Pain, H. J. (2005).THE PHYSICS OF VIBRATIONS Sixth Edition, 570.https://doi.org/10. 1002/0470016957

PBX Software - VoIP-Info. (203AD). Retrieved September 7, 2018, from https://www.voip-info.org/pbx-software/

Phithakkitnukoon, S., Dantu, R., &Baatarjav, E. A. (2008).Voip security — attacks and solutions.*Information Security Journal*, *17*(3), 114–123. https://doi.org/10.1080/193935 50802308618

Pros & amp; Cons: Keeping voice & data on separate networks. (n.d.).Retrieved May 14, 2018, from https://www.comparebusinessproducts.com/phone-systems/rpos--cons-keeping-voice--data-on-separate-networks.

Qadeer, M. A., Shah, K., &Goel, U. (2012). Voice - Video communication on mobile phones and PCs' using asterisk EPBX. *Proceedings - International Conference on Communication Systems and Network Technologies, CSNT 2012*, 534–538. https://doi.org /10.1109/ CSNT.2012.121

Rana, N. Y. 2013. (2013). MSc Thesis Thesis Title : Designing and optimization of VOIP PBX infrastructure By NaveedYounasRana Student ID : 1133670 Department of computer science and technology Supervisor : Dr . Ali Mansour, 1–63.

Sanguino, J., & Roberts, R. W. (2011). Wireless Communications Adapter For A Hearing Assistance Device. *The Journal of the Acoustical Society of America*, *129*(4), 2354. https://doi.org/10.1121/1.3582201

Scores, E. (2013). GRADUATE SCHOOL of NATURAL and APPLIED SCIENCES. *Gyte.Edu.Tr*,5.Retrieved from http://www.gyte.edu.tr/files/muhendislik fen_bilimleri/ application_form_for_international_graduate_students.pdf

Sinclair, J. (1997). *How radio signals work : all the basics plus where to find out more*. McGraw-Hill.

Stallings, W. (1997).*Data and computer communications*. Retrieved from http://tinnakorn.cs.rmu.ac.th/Courses/DataCommNetwork/Book/DataAndComputerCommunications8E.pdf

Toral-Cruz, H., Argaez-Xool, J., Estrada-Vargas, L., & Torres-Rom, D. (2011). An Introduction to VoIP: End-to-End Elements and QoS Parameters. *VoIP Technologies*, *ISBN 978-9*, 336. https://doi.org/10.5772/13520

Scores, E. (2013). GRADUATE SCHOOL of NATURAL and APPLIED SCIENCES. *Gyte.Edu.Tr,5.* Retrieved from http://www.gyte.edu.tr/files/muchendislik-fen-bilimleri /application-form-for-international-graduate-students.pdf.

Tariffs.(2004). Retrieved May 16, 2018, from https//www.mtn.com.gh/ personal/ mobile/ traiffs.

The Importance of VLAN Segmentation for Voice and Data.(n.d.).Retrieved May 14, 2018, from https://info.hummingbirdnetworks.com/blog/importance - of - vlan-segmentation-voice – data.

Toral – Cruz, H., Argaez – Xool, J., Estrada – Vargas, L., & Torres – Rom, D. (2011). An Introduction to VoIP: End – to – End Elements and Qos Parameters. *VoIP Technologies, ISBN978 – 9,*336. https:doi.org/10.5772/13520.

Types of Waves, Mechanical Waves & Electromagnetic Waves • SSP. (2014). Retrieved May 18, 2018, from https://www.smartsciencepro.com/types-waves-electromagnetic/

University of Ghana.(2016). Overview University of Ghana.Retrieved May 12, 2018, from http://webcache.googleusercontent.com/search?q=cache:http://www.ug.edu.gh/about/overiew&gws-rd=cr&ei= N9iZWI-1KczOjwPQmpq4Cg.

Using Ch 1 5 9 13 vs 1 6 11 on a 2.4 Ghz/20MHz? – Ubiquiti Networks Community. (2015). Retrieved July 31, 2018, from https://community.ubnt.com/t5/unifi-Wireless/Using-Ch-1-5-9-13 vs-1-6-11-on-a-2-4Ghz-20MHz/td-p1252133?lightbox-message-images-1252824=53910i86CE517C21C4AB18.

Vodafone Ghana I Vodafone Call rate / Tariff.(n.d.).Retrieved May 14, 2018, from https://support.vodafone.com.gh/customer/portal/articles/1857245-vodafonce-call-rate-tariff.

Voice, I., Protocol, I., Switched, P., Network, T., Voip, T., Protocol, I., …Gray, R. M. (1974). Chapter 1 VOICE OVER INTERNET PROTOCOL (VOIP), 1 – 35.

Voice over IP.(2018). Retrieved from https://www.nfon.com/en-de/cloud-telephone-system/resources/glossary/voice-over-ip/.

VoIP project, one network or two? – Luminet. (n.d.).Retrieved May 14, 2018, from http://luminet.ca/voip-project-one-network-or-work/.

Voice, I., Protocol, I., Switched, P., Network, T., Voip, T., Protocol, I., …Gray, R. M. (1974). Chapter 1 VOICE OVER INTERNET PROTOCOL (VOIP), 1–35.

Wei, X., Bouslimani, Y., &Sellal, K. (2012). VoIP based solution for the use over a campus environment. *2012 25th IEEE Canadian Conference on Electrical and Computer Engineering: Vision for a Greener Future, CCECE 2012,* 3- 7. https://doi.org/10.1109/CCECE.2012.6335009.

Wireless networking – Wifi poor SNR, reasons and solutions: - Super User .(n.d.).Retrieved July 28, 2017, from https://superuser.com/questions/208270wifi-poor-snr-reasons-and-solutions.

Worldwide, S. (2014). Troubleshooting Common Issues in VoIP.

Wadhwa, P. (2007). Design of PSTN-VoIP Gateway with inbuilt PBX & SIP extensions for Wireless medium PriyeshWadhwa Department of Computer Science and Engineering Indian Institute of Technology Bombay, (05329011).

Wang, W., Member, S., Liew, S. C., Member, S., & Li, V. O. K. (2005). Solutions to Performance Problems in VoIP, *54*(1), 366–384.

Woller, J. F., &Gebhardt, W. (2012).Th Wireless book Evolution and Communication, 214. Retrieved from http://www.steute.co.uk/fileadmin/ Downloads/ wireless/ Kataloge/9177-Wireless_book.pdf.