Investigating Wireless Network Deployment Configurations for Marginalized Areas

Submitted in fulfilment of the requirements

for the degree of Masters in Computer Science in the

Faculty of Science and Agriculture at the

University of Fort Hare

By

Nkanyiso Ndlovu

University of Fort Hare

Together in Excellence

Declaration

I, Nkanyiso Ndlovu [Student Number: 200509070], hereby confirm that the work presented in this thesis is my own original work and has not been submitted, in its entirety or in part, to any other educational institution for any other degree. All information extracted from other sources is acknowledged as such.

Requests for permission to copy or make use of materials in this thesis, wholly or partly, should be addressed to:

_____

Nkanyiso Ndlovu

October 2011

Dedication

To my brother, who has always told me that "*a goal without a plan is just a wish*". Ngiyakuzwa webafo ukuba uthini. Lastly, I dedicate this thesis to Magumz and PK. Continue to be what you are to me. Iswazi lwakho mzali made a difference.

Acknowledgements

Firstly, my thanks go out to my brother '*Adolf*' for his encouragement, faith, motivation and support. I would like to thank the Telkom Centre of Excellence and the following industry partners: THRIP, Tellabs, Telkom, Saab Grintek, Easttel and Khula Technologies, who have provided the much needed financial support which ensured the success of this big project. I would also like to thank the entire group of Dwesa researchers from both the University of Fort Hare and Rhodes University for the work that they have put in to make this project happen. Most importantly, I would like to thank the Dwesa community, Alfredo Terzoli and Mamello Thinyane for their cooperation and continual support of this research.

Abstract

Wireless technologies, such as Worldwide Interoperability for Microwave Access (WiMAX) and Wireless Fidelity (WiFi), are making it easier to provide the much needed telecommunications infrastructure in marginalized areas worldwide. These technologies enable the rapid deployment of network services as well as their redistribution throughout these marginalized areas. The ability to bring Internet connectivity to previously underserviced and marginalized areas has the potential to leap-frog socio-economic development and improve participation in the global knowledge economy. This study investigated how wireless access technologies, such as WiMAX and WiFi, can be integrated and used to deliver ubiquitous distributed Internet connectivity with increased capillarity in rural areas. The research was undertaken within an ICT for Development (ICT4D) intervention called Siyakhula Living Lab (SLL) which is based in the Eastern Cape province of South Africa. The research further eliminated the accessibility constraints associated with long distances and remoteness from the Digital Access Nodes (DANs) and provided increased penetration in the network in contrast to the traditional Telecentre model which has been used extensively in ICT4D interventions. This was achieved by deploying WiFi hotspots around the DANs and extending the existing SLL WiMAX backbone to increase the network footprint to neighboring communities. The technical result of the research has been the provision of increased capillarity on the network and service redistribution throughout the entire Dwesa community. Consequently, this has given local community members an opportunity to access network services easily and ubiquitously. Finally, the research investigated and presented the benefits of such wireless network deployment configurations on ICT4D activities in marginalized areas.

Key Words – ***Rural Connectivity, Global Knowledge Economy, ICT for Development, Siyakhula Living Lab, WiFi, WiMAX***

Publications

Ndlovu, N. Thinyane, M. Terzoli, A. 2009. ***Deployment and Extension of a Converged WiMAX/WiFi Network for Dwesa Community Area South Africa***. Proceedings of SATNAC 2009 Conference, Royal Swazi Spa, Swaziland

Ndlovu, N. Thinyane, M. 2010. ***Investigating Wireless Network Deployment Configurations for Rural Marginalized Areas (Dwesa Case Study).*** Proceedings of ZAWWW-2010 Conference, UKZN, Durban, South Africa

Ndlovu, N. Dumani, K. Hlungulu, B. Ngwenya, S. Samalenge, J. Thinyane, M. Terzoli, A. 2010. ***Technology Solutions to Strengthen the Integration of Marginalized Communities into the Global Knowledge Society (Dwesa Case Study).*** Proceedings of IST-Africa, 2010 Conference, ICC, Durban, South Africa

Ndlovu, N. Jere, N. Terzoli, A. 2010. ***Wireless Network Deployment Configurations: Dwesa Marginalized Area as a Case Study.*** Proceedings of SAICSIT 2010 Conference, Bela Bela, South Africa

Ndlovu, N. Jere, N. 2010. ***A Mobile Phone Approach in Delivering Healthcare Information to Marginalized Areas.*** Proceedings of SATNAC 2010 Conference, Spier Estate, Stellenbosch, South Africa

Ndlovu, N. Jere, N. Terzoli, A. 2011. **Can Wireless Network Deployment Configurations in Rural Schools Deliver Ubiquitous Internet Connectivity & Help Uplift Education Standards in MRAs?** Proceedings of SACLA 2011 Conference, Zimbali Resort, Durban, South Africa

Ndlovu, N. Jere, N. Terzoli, A. 2011. **Best Practice Wireless Network Deployment Configurations for ICT4D Service Provisioning in MRAs.** Proceedings of ZAWWW 2011 Conference, Wits University, Johannesburg, South Africa

Contents

List of Figures

List of Tables

List of Acronyms and Abbreviations

AC	Access Concentrator
AES	Advanced Encryption Standard
AH	Authentication Header
AK	Authentication Key
BS	Base Station
CIA	Confidentiality Integrity and Availability
CPE	Customer Premises Equipment
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
DAN	Digital Access Node
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
EAP	Extensible Authentication Protocol
EDGE	Enhanced Data Rates for GSM Evolution
FOSS	Free and Open Source Software
GPRS	General Packet Radio System
GSM	Global Systems for Mobile Communication
ICMP	Internet Control Message Protocol
ICT	Information and Communication Technology

IPSec	Internet Protocol Security
ISP	Internet Service Provider
LOS	Line of Sight
MAC	Media Access Control
MBS	Micro Base Station
MJSS	Mpume Junior Secondary School
MPPE	Microsoft Point-to-Point Encryption
MTJSS	Mtokwane Junior Secondary School
NHS	Nqabara High School
NJSS	Ngwane Junior Secondary School
NLOS	Non Line of Sight
NPS	Nondobo Primary School
ODU	Outdoor Unit
OFDM	Orthogonal Frequency Division Multiplexing
PPPoE	Point-to-Point Protocol over Ethernet
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
SLL	Siyakhula Living Lab
SSL	Secure Socket Layer
SU	Subscriber Unit

TCP	Transmission Control Protocol
TCP/IP	Transmission Control Protocol/Internet Protocol
TEK	Temporal Encryption Key
UMTS	Universal Mobile Telecommunication Service
VoIP	Voice over IP
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal
WEP	Wired Equivalent Privacy
WiFi	Wireless Fidelity
WiMAX	Worldwide Interoperability for Microwave Access
WLAN	Wireless Local Area Network
WPA	WiFi Protected Access

1 Chapter One: Introduction

This chapter introduces the research project and provides an overview of the study. Section 1.1 below outlines the background of the study, and discusses the previous and present state of wireless telecommunication networks in rural areas. Thereafter, the problem to be addressed when planning and deploying particular networks in order to achieve rural Internet connectivity is highlighted. Section 1.4 presents various methods and approaches that would be used in conducting the research. This is followed by an overview of the structure of the rest of the thesis.

1.1 Background of Rural Telecommunication Networks

Recent research has shown that the growth of deployed wireless networks contributes significantly in offering digital cellular communication (Agbinya, 2003). Such technological advancements allow the continuous flow of information, both in and out of marginalized communities in both developed and developing countries. Popular technologies, such as Worldwide Interoperability for Microwave Access (WiMAX) and Wireless Fidelity (WiFi), enable the rapid, low cost deployment of wireless networks in rural areas (Agbinya, 2003). This ability to bring Internet connectivity to previously underserviced and marginalized rural areas bridges the gap between those who actively participate in the global knowledge economy and those who have been marginalized and excluded from participating (Agbinya, 2003). These technologies have also influenced the exploration of novel and innovative mechanisms to leap-frog socio-economic development in marginalized rural areas (Ndlovu *et al.*, 2010c).

This research encourages new and innovative technologies that can be merged and deployed in rural areas whilst maximizing the benefits and flexibilities that wireless telecommunications offer. Wireless technologies are categorized into different standards and types. WiFi, WiMAX and Bluetooth all fall under the IEEE 802.x wireless networks (Van Hoorik *et al.*, 2007), whereas the Very Small Aperture Terminal (VSAT) is categorized under satellite technologies and the Universal Mobile Telecommunications System (UMTS), Enhanced Data Rates for GSM Evolution (EDGE), Third Generation (3G) and High-Speed Downlink Packet Access (HSDPA) are categorized as mobile telecommunications technologies. They can be further categorized

according to the way in which they transmit signals, the range of their coverage and throughput, as well as their frequency band of operation (Van Hoorik *et al*., 2007). Due to the mobility, flexibility and cost savings when installing, moving or reconfiguring a Wireless Local Area Network (WLAN), wireless technologies have proven to be an infrastructure alternative in introducing rural Internet connectivity where fixed lines are not feasible (Agbinya, 2003). As a result, this research seeks to provide ubiquitous access to network resources and to increase capillarity to the Siyakhula Living Lab (SLL) network. The SLL is located in the Dwesa community, situated in the Eastern Cape province of South Africa. It is situated in the former homeland of the Transkei (Ndlovu *et al.*, 2010a). The Dwesa community has approximately 15000 inhabitants who are distributed into 2000 households. Further details pertaining to the research context and the SLL network are presented in Chapter Five.

1.2 Statement of the Problem

The main problem with the SLL's network deployment is that it is relatively centralized and allows community members to access network resources only in central places like schools. However, this becomes a problem when schools are closed because the community cannot access the resources. Additionally, some community members feel that they are left out because they have to travel long distances to access these facilities. The situation becomes worse during holiday periods because they do not have any access and, as a result, they feel that they are not fully benefiting from this innovative, i.e. the SLL project. The main research question is *"Can decentralization of the SLL network resources through inter connectivity and the deployment of WiFi hotspots, improve the social and cultural livelihoods of people in rural areas?"* This main question can be expanded into the following problem questions:

- What type of information pertaining to rural areas should be acquired prior to planning a wireless network?
- Which access technologies can be merged so as to deploy a cost effective, ubiquitous and reliable wireless network suitable for rural areas?
- How best can the deployed wireless network be managed for effective utilization in rural areas, taking into consideration access control?

- Do these innovations and outcomes truly contribute to improving the social and cultural livelihoods of people in rural areas?

1.3 Objectives of the study

This research aims to provide ubiquitous distributed Internet connectivity while, at the same time, increasing capillarity to the SLL network. It seeks to address the abovementioned problems by redistributing the network facilities through the concept of hotspot deployment and the addition of an extra SLL WiMAX Digital Access Node (DAN). This will allow the Dwesa community to access network resources at any time of the day. As a result, the research has to identify and merge technologies that are the most cost effective, more secure, sustainable, and easily deployed (in similar or in most rural terrains). This research also aims to deploy a more secure wireless telecommunication infrastructure that contains minimal loopholes in terms of security and prevents any unscrupulous users from gaining access to the network. Below is a summarized list of the additional objectives of this research:

- To investigate the marginalized rural context in terms of the terrain and wireless network deployments related to this research.
- To investigate WIMAX and WiFi features and their security shortfalls. Thereafter, to merge these technologies for wireless telecommunication network deployment for the SLL.
- To deploy WiFi hotspots around each and every Digital Access Node (DAN) and add an extra WiMAX DAN to the SLL network.
- To determine the results from the experiments conducted in this research and present the benefits of this network to the community.
- To recommend any new ideas gained from this research.

1.4 Methodology

The research focuses on the deployment of a more secure WiMAX/WiFi network that effectively provides resources to the marginalized areas of the Dwesa community. The different research approaches that are used are:

- A detailed literature review which was conducted so as to fully understand the advantages and disadvantages of WiMAX and WiFi as well as to gain background knowledge and understanding into a converged wireless telecommunication network.
- The study of the marginalized rural context was investigated through observation and regular visits to the Dwesa community, which was the test bed in this research. Similar case studies, in other areas of southern Africa, were taken into consideration so as to deploy a network with no or minimum problems.
- Questionnaires were created and villagers interviewed in order to determine what they expected from the deployment of this initiative.
- A case study approach was used to conduct the on-the-ground deployment of an extra WiMAX DAN and additional WiFi hotspots.
- The research then recommended the protocols and mechanisms used to secure the WiMAX/WiFi network after obtaining the results from the experiments conducted on the network.

1.5 Thesis Organization

Chapter 2: Rural Telecommunications Networks. This Chapter provides an overview of the different characteristics and the context of rural marginalized areas. The major reason for this is the need to enhance the background knowledge of how different rural telecommunication networks, similar to that studied in this research, are deployed. It provides the key aspects which define what rural telecommunications networks are. Finally, the Chapter explores various case studies similar to this research and elaborates on their importance to this research.

Chapter 3: Access Technologies for Achieving Internet Connectivity. This Chapter explains different access infrastructure technologies at the physical layer as well as their media of data transmission. It provides essential knowledge appropriate for selecting the media of data transmission during the network design stage. Lastly, the Chapter looks at the required components for both hardware and software including the chosen technologies.

Chapter 4: Controlling Access within IEEE 802.xx Networks. This Chapter discusses security issues on the chosen IEEE 802.xx technologies. It provides a detailed discussion of IEEE 802.11 security (WiFi) and possible mechanisms for controlling wireless access. Afterwards, it explains WiMAX security issues and concludes by giving the best possible authentication methods which could be implemented in the SLL network.

Chapter 5: Implementation of WiFi/WiMAX in the SLL Network. This Chapter provides the implementation and deployment configuration details used when setting up the WiFi/WiMAX SLL Network. It explains how the access nodes where configured and also gives in detail the procedures of determining the suitable positions for deploying the DAN.

Chapter 6: Testing Strategies and Evaluation of Results. This Chapter provides experimental results and an evaluation of the performance costs of the proposed implementation of hotspots.

Chapter 7: Conclusions and Future Work. This Chapter concludes the research by summarizing the findings and the possible future work which can be conducted in relation to the SLL network. It provides various recommendations which can be followed when deploying wireless telecommunication networks for rural areas.

1.6 Summary

This chapter presented a background of the research and rural telecommunication networks. In addition, the problem statement was outlined. Section 1.3 outlined the objectives of the research. Afterwards, a detailed outline of the methodology used to conduct the investigation on a converged wireless network was presented. Finally, a brief outline of the organization of the thesis is given. Chapter Two, below, presents an overview of rural telecommunication networks and provides the key aspects which help define what rural telecommunications networks are. The Chapter shows the need to deploy rural communication networks such as these as well providing various examples of similar on-going rural-network-building projects.

2 Chapter Two: Rural Telecommunication Networks

This chapter is an overview of the different characteristics and the context of marginalized rural areas. This contextualization is based on the need to enhance the background understanding of how different rural telecommunication networks, similar to this research, are deployed. In section 2.4, the research provides the key aspects which help define what rural telecommunications networks are. It also shows the importance of deploying such rural telecommunications networks and provides examples of deployed and on-going rural network building projects similar to this one.

2.1 Why Deploy Rural Telecommunication Networks?

One of the major problems in rural telecommunications deployment is the ability to provide a *"technological solution*" whilst at the same time providing a "*working and sustainable solution*" (Westerveld, 2004). Rural areas in developing countries are primarily characterized by inaccessible geographical terrains and adverse climates. This kind of environment makes the deployment of such networks difficult and de-motivating to many telecommunication companies and service providers (Conradie *et al.,* 2003). Their fear is the loss of revenues and very little returns while requiring large investments. As a result, this is a major setback to both technological and economic developments and, at the same time, hinders social developments within rural communities (Westerveld, 2004).

However, the best possible comprehensive solutions can be brought in so as to address and resolve these problems due to a higher demand for Internet connectivity in rural areas worldwide (Wertlen, 2007). Getting marginalized rural areas connected to the entire world will definitely enhance the livelihoods of rural community members and help in their participation in global knowledge systems (Conradie *et al.,* 2003). This is the primary objective of building rural telecommunications because it leverages and closes the digital divide. The research presents a brief discussion of the general trends in the impact of the Internet on the communities in Section 2.2 below.

2.2 Visualizing a Rapidly Changing Region Through the Use of the Internet

Several initiatives have been, and continue to be, implemented across the world to tackle the major barriers to bridging the digital divide. These include the use of the Internet and other ICTs (Wellenius, 2002). This is seen as a substantial step in the alleviation of different paramount social-economic problems at the same time; in the transformation of society and the realization of a truly free and democratic world society (Wellenius, 2002). The use of technology in bridging this gap is a fundamental advancement because it brings with it mutual understanding and the elimination of differentials of power within communities both in developing and developed countries worldwide (Huggins, 2002). Figure 2.1 below shows the Internet penetration rates around the world.

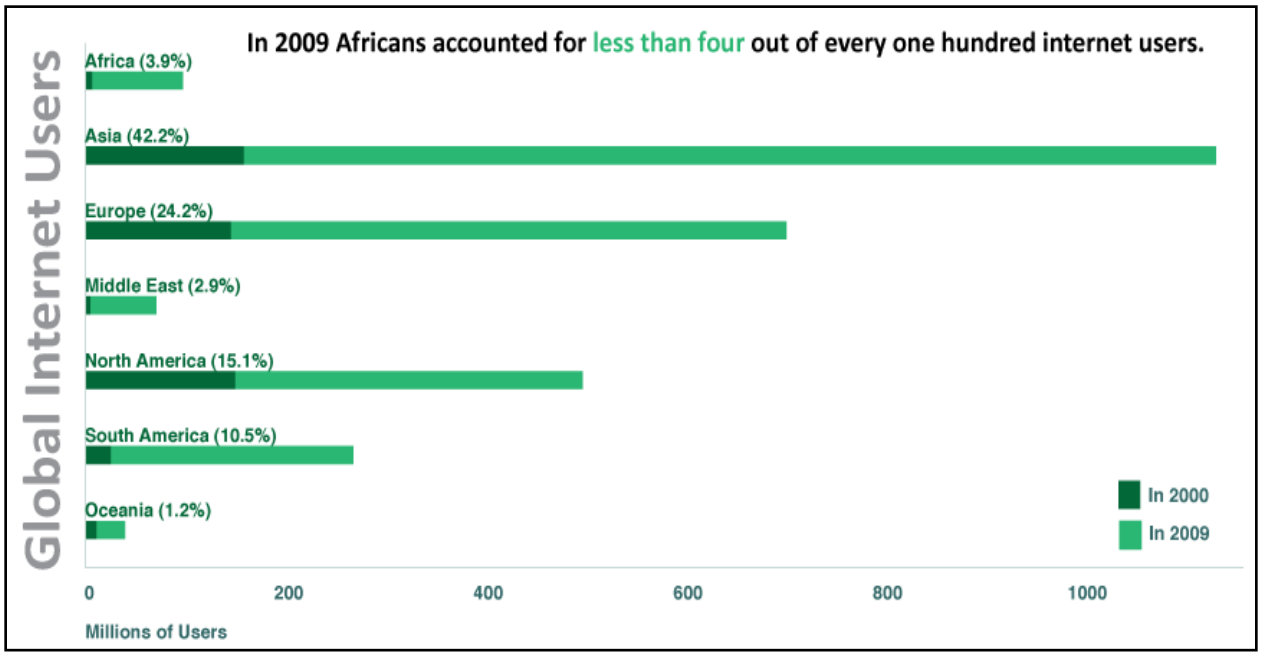


Figure 2.1: Internet users in the world by region adapted from Internet World Stats (2009).

Figure 2.1 above shows that Africa still lags behind in terms of Internet connectivity. The reason for this might be that most African countries are still developing and Internet usage is still in its infancy. This shows that there are very few people who have access to the Internet. Asia has higher Internet penetration rates than Africa. In Asia, many people have access to the Internet and, as a result, the digital divide in these areas is very narrow in comparison to Africa. The huge

difference in Internet access is undesirable because it shows that people of different communities have unequal opportunities to benefit from technology in their daily lives (Jung *et al*., 2001). A direct and mutual correlation exists between the Gross Domestic Product (GDP) per capita of a country and use of telecommunication services such as the Internet (Corrocher *et al.*, 2002). As a result, the use of telecommunication influences both the financial and social well-being of a population (Corrocher *et al.*, 2002). There are a variety of arguments as to why closing the digital divide is essential. The following are some of the key arguments (Marine *et al*., 2004; Wellenius, 2002):

2.2.1 Economic Equality

According to Wellenius (2002), the provision of Internet to marginalized rural communities improves the economic well being of the people. Some people think that it is more of a basic necessity for citizens in developing countries where each and every government strives to guarantee the provision of Internet to its people. The Internet provides important information on the career, safety, health and civic life of people (Wellenius, 2002). Last, but not least, it helps in the administration and electronic offering of social welfare services. Some might argue that the telephone or the cell phones are better options. Surprisingly, these technologies can work together and telephonic services have recently been offered through the Internet as Voice over Internet Protocol (VoIP) services (Ndlovu *et al.*, 2009; Wellenius, 2002).

2.2.2 Social Mobility

Some people believe that the use of the Internet has brought a significant change in the manner in which education transpires and is being conducted (Marine *et al*., 2004; Wellenius, 2002). They believe that computers and computer networks have improved the different ways of learning and the education system as a whole. Without such offerings, the digital divide will continue to exist since people, mostly children, in a lower socio-economic position will not fully benefit or will eventually be left out (Wellenius, 2002). As a result, it will be of great help if governments intervene and provide support so as to proffer equal opportunities.

2.2.3 Economic Growth

The deployment of telecommunication information infrastructure in the rural areas is seen as a great step in economic expansion (Huggins, 2002). Local farmers will be able to attain viable and valuable market information and marketing effectiveness which are crucial in assisting them in reaching profitable markets. Some believe that the Internet will improve the timely access to information which is beneficial to economic decision making on farms (Wellenius, 2002). Even industries will be able to enter into competitive markets with other industries with the use of these information technologies. The sharing of information through increased Internet connectivity and the exploitation of the latest technologies will be a shortcut to production improvements in most developing countries (Marine *et al*., 2004; Wellenius, 2002).

2.2.4 Democracy

Democracy can be delivered in a number of ways. Some people believe that the previously underserviced marginalized rural areas will finally get a chance to participate in the general elections in their areas if they have Internet connectivity (Goth, 2005). Internet connectivity can be used to obtain information related to government and national activities to assist people when events, such as elections, occur so that they can participate in these events. The deployment of these wireless networks in the rural areas, so as to bridge the gap, will definitely have an influence on decision making processes (Csaki *et al.*, 2003; Servon, 2002).

2.2.5 Education

As technology advances, various innovations are emerging so as to deliver improved education in rural areas. Both governmental and nongovernmental organizations are working projects to translate powerful ideas about education and technology to powerful results that can be used to improve rural school education (Hawkins, 2002). Extending the idea of School of One and Learn-O-Vision to the rural schools, which uses technology to provide innovate instruction models, would definitely uplift the standards of rural education (Kozma, 2003). However, many obstacles exist in bringing the potential of education to scale (Hawkins, 2002). These include limited Internet connectivity and professional knowhow in rural areas. As a result, a majority of

rural telecommunication innovations strive to answer this question. In education, how can and should rural Internet connectivity be used to close the gap rather than exacerbate it?

2.2.6 Health Care

In developing countries, there exists a gap in the healthcare service delivery between urban and remote rural areas (InfoDev/ARD/SASKI, 2007). Mostly, the rural areas are the ones which are under-serviced because medical specialists are reluctant to work in those areas. As a result, rural clinics depend on specialists, who normally reside in urban areas, for diagnosis of any complicated medical conditions (Kovacs *et al.,* 2000). This requires a physician to visit or sending information to urban hospitals. This result delayed treatment as well as poor medical follow-up which contribute to high mortality rates in rural areas. However, innovative systems have been developed such as remote diagnostics of fetal heart rate monitoring and other applications that can be accessed through the Internet (Kovacs *et al.,* 2000). Unfortunately, Internet connectivity is limited in rural areas so as to support these applications. As a result, this motivates the deployment of a telecommunication infrastructure that provides different services which are always available, easily accessible and uses cheap existing resources (Di Lieto et al., 2008).

2.3 Rural Telecommunications Network Deployment Challenges

There are different factors that need to be considered when deploying wireless telecommunication networks for rural areas. These factors can be social, cultural, political, environmental or economic factors. The following section of the research presents a brief discussion of the environmental and economic factors affecting rural areas.

2.3.1 Rural Environments and Limitations

This section explores the motive behind conducting this study in a marginalized rural area. We elaborate upon the actual rural shortcomings and provide more knowledge regarding the actual needs of the research. An explanation of how the technology has influenced the development of rural areas is also put forward, after which the future of wireless telecommunications networks

for rural areas is discussed. The proper planning and selection of appropriate technology needs to be considered prior to deploying a wireless telecommunication network in rural areas where half of the world's inhabitants were living by the year 2005 (Bocquier, 2005). The research also mentions some of the problems that may indirectly be caused by the lack of telecommunications infrastructure (Bocquier, 2005):

- Lack of reliable electricity and other public facilities such as usable water and proper toilets.
- Transport is another major problem and this setback makes it difficult to transport goods around and outside the area.
- Most villagers engage in informal, self skilled jobs which bring in a low income. As a result, communication services are not affordable and communities are thus forced to de-prioritise their communication needs.
- Public social infrastructure is not fully developed and, as a result, the villagers have to walk long distances to acquire government and health services.
- Lack of an appropriate business model that will be financially and technically sustainable.
- Lack of technical and business skills for local entrepreneurs due to the fact that many villagers have low educational levels and the communities have high illiteracy rates.
- Low levels of economic activity with few job opportunities. The existing economic structure may be based on agriculture, fishing or handicrafts.
- Lack of working capital for small businesses such as those involved in the sale of clothes, fishing equipment, soft drinks kiosks, carpentry, education support, acquisition of school training aids/materials, production of local brew.
- The settlements are dispersed and, as a result, the deployment of a wired network is difficult. Topological inconsistence is another contributory factor. Some places are mountainous, hilly and further separated by valleys.

From the above factors, one realizes that there are many related cases and communities in most parts of South Africa who share these characteristics. An area called Dwesa in the Eastern Cape Province was identified as a location which displayed these characteristics of an underdeveloped

marginalized rural area. The prominence of the abovementioned factors in the Dwesa area indicates that there is a need to bring Internet connectivity to this locale. This will enable the communities to gain access to local ICT activities. More information on the research site is provided in Chapter Five of this study.

2.3.2 Rural ICT4D Applications

The use of technology, to facilitate the rapid exchange of information, has uplifted the socio-economic status of many rural communities in Africa and worldwide (Conradie *et al.,* 2003). Despite this, developing countries still experience problems in areas such as health, economy and education. The chances are high that ICTs will continue to play an important part in achieving Millennium Development Goals (MDGs) such as the eradication of poverty, combating serious diseases like HIV/AIDS, improving education and health facilities (Conradie *et al.,* 2003). ICTs have made it possible for people to have improved access to information and for ease of communication (Marine *et al*., 2004).

In recent years a number of ICT4D projects have been, and are still being, implemented in rural areas. They aim to realize the benefits of ICT in a range of sectors, from health, education, commerce and government to scientific capacity building, human rights and gender empowerment (Thinyane *et al.,* 2007). However, these benefits are hindered by inadequate infrastructure and the human capacity to support ICT. The following are relevant examples of some ICT rural applications which have been carried out in different places for rural requirements:

- ***Human Rights and Democracy:***

In most African countries, and some developing countries worldwide, fellow citizens are deprived of their rights which include human or political rights (Zhira, 2008). This is evident in countries like Zimbabwe, where citizens are denied their freedom of speech and expression because of political instability (Zhira, 2008). An ICT initiative called the Kubatana Trust was developed and deployed in Zimbabwe. Its primary aim was to strengthen the use of e-mail and Internet strategies in local non-governmental organizations (NGOs) and civil society

organizations (William, 2008). A centralized, electronic source is used to make human rights and civic education information available to the general public and Zimbabwean citizens at large. With this technological advancement, international and local communities are able to read and stay updated about the current situation in their countries (Zhira, 2008). This is an actual example of the benefits of ICT, which is technology designed to enable communication and the electronic capture, processing and transmission of information *(*Heeks, 2005b).

- ***Commerce:***

Different farmers, either fruit or vegetable, are now able to use their mobile phones to get updated information regarding the current market prices of their products (Marine *et al.*, 2004). This is possible because of an ICT initiative which is practiced in one of the developing countries of Africa, Senegal. A private French telecommunications company, called *Manobi*, is in charge of this technological advancement initiative which uses Wireless Application Protocol (WAP) enabled mobile phones to obtain up-to-date market prices for fruits and vegetables from different markets and locations (Rashid *et al.*, 2009). Various data collectors immediately update the main central database from their respective locations or markets. They also give real time related rates or market prices for these products which the producers have no access to or will only receive later, once things have changed (Marine *et al*., 2004; Rashid *et al.*, 2009). This is indeed a major boost to the commerce of Senegal.

- ***Health:***

Another example of a rural ICT application is being pioneered in Mali. It is called the Keneya Blown tele-medicine project. Its main focus is connecting all hospitals, clinics and health institutions around that country, thereby creating an online network (Bagayoko *et al.*, 2006). Currently, its primary users are physicians but it is open to other healthcare workers for consultation purposes and contributing to human health in their areas. Furthermore, it now incorporates medical tele-teaching where medical information can be conveyed to a patient in Bamako, Mali by a specialist or physician in England and vice versa (Bagayoko *et al*., 2006).

- ***Economic empowerment:***

The demand, by women, for equal rights and opportunities around the world has seen a non-governmental organization called Grameen Bank providing them with low cost loans (Tracey *et al.*, 2007). Grameen Bank is a village based organization and it is found in Bangladesh (Cavaye *et al.*, 2000; Tracey *et al.*, 2007). After acquiring these loans, women use them to purchase and setup mobile phone exchanges around their villages which currently have only a few landlines (Tracey *et al.*, 2007). For every call one makes in the Village Pay Phone, they charge up to three times more than a normal call will be charged in an urban public phone box (Cavaye *et al*., 2000). The income they obtain is used to send their children to school and colleges around the country. This business practice has greatly improved their livelihoods. Recently, the service has been decelerated and disrupted by the introduction of cheap cell phones which many villagers have acquired (Tracey *et al.*, 2007).

- ***Distance education:***

Learn-O-Vision (Herselman, 2003) was developed by Mr. D. Oosthuizen to provide rural schools with all the facilities of a first-rate educational institution. He realized the need for such a facility after watching the news bulletin showing a school located in Garankuwa which had no classrooms; this resulted in teaching and learning taking place under trees (Hawkins, 2002). The system components of Learn-O-Vision comprises of a solar-powered computer system, television, video machine and a writing and flannel board housed in a portable and secure box (Herselman, 2003). Moving it around is a simple task because it has wheels. In front of the box, there are flaps which can be opened out and which act as a writing board with the video machine and television in front (Herselman, 2003). The computer operates on battery power and beeps for ten seconds if one does not switch it off. The computer is stored at the back of the unit. The unit can alternatively operate on electricity but it currently runs on solar powered batteries. The two solar panels provide the power to charge the batteries and when fully charged, they can last the entire day. The Learn-O-Vision unit will eventually evolve to give rural schools access to the Internet and make distance education possible (Kozma, 2003; Herselman, 2003). With the possibility of distance education, the system will allow rural learners to watch and learn through educational tapes by using the video machine and watching academic programs on the television.

Eventually, such a system will definitely improve the standards of education in rural schools (Kozma, 2003).

- ***Community and business development:***

Various applications have been developed which allow rural community members in remote tourist outposts to sell their crafts (Jacobs *et al.,* 2006). Such applications are called point-of-sale applications (Csaki *et al.*, 2003; Jacobs *et al.,* 2006). Some applications allow the dissemination of information about government programs, subsidies and administrative matters through multilingual and localized websites (Csaki *et al.*, 2003; Corrocher *et al.,* 2002). These cases show how ICTs are important in different societies. Therefore, ensuring proper telecommunication networks in these areas is critical (Conradie *et al.,* 2003).

2.3.3 Economic Issues in Rural Areas

In order to facilitate the understanding of the economic relativity of network nodes in wireless telecommunication network deployment and the choice of proficient economic parameters for modeling, the research briefly discusses the economic issues affecting rural areas in general.

Before deploying a network in the rural areas, network planners tend to ask themselves one important question: Which social member is responsible for paying for rural communications? In order to answer this question, a value chain has to be considered; this is illustrated in Figure 2.2 below.

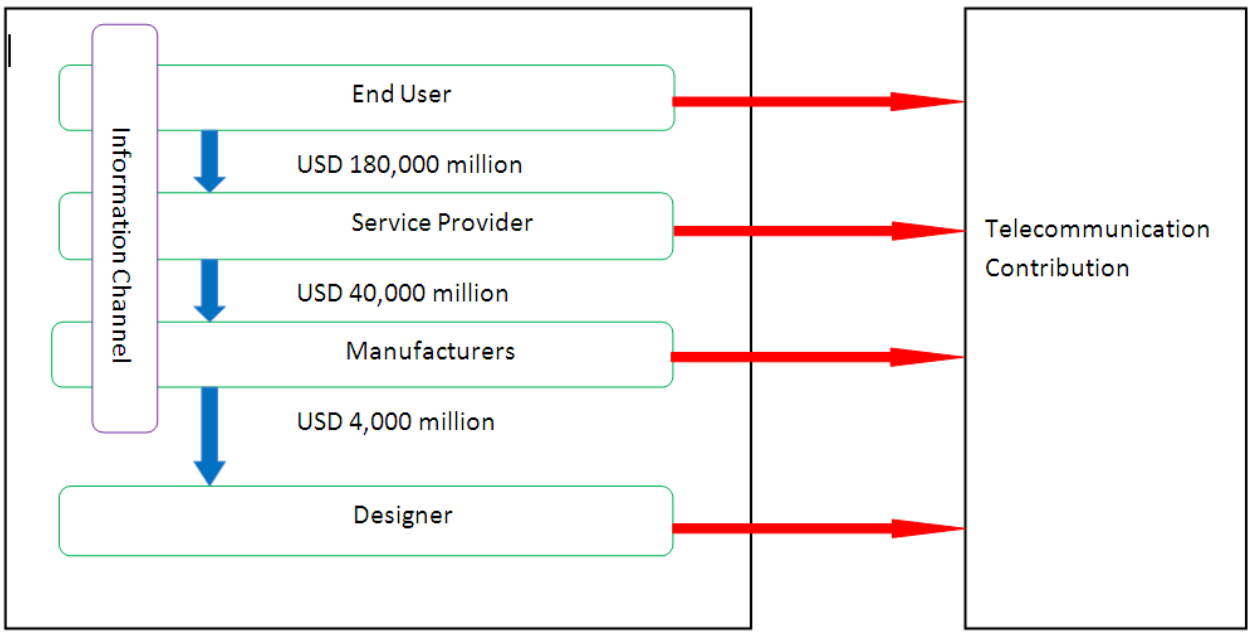


Figure 2.2: Value chain of network construction and contribution (Lu et al., 2006).

Figure 2.2 shows that the initial stage of network construction is when a manufacturer develops a telecommunication infrastructure such as DLink or Cisco wireless routers from the information acquired from the designer. These products are then bought by service providers who use them in the deployment of a wireless network in the rural areas. This happens concurrently with the information channels notifying customers of products and services to ensure profits (Lu *et al.*, 2006). Having deployed the telecommunication network, the end user utilizes the network resources after paying their bills. The services that they are entitled to, range from voice and video to data. As a result, telecommunication carriers profit from the taxes paid for all enterprises. However, it is difficult to determine the exact number of services and the number of products that have to be purchased, but an ideal model for part of the relative values is illustrated in the value chain below (Agbinya, 2003).

This value chain is modeled according to the European market but it can be applied to any rural network setup regardless of whether it is a developed or developing country. All four members in the chain fit in regardless of the nature of the network to be deployed. Figure 2.2 shows large amounts of cash flow from the end users to the service providers. Manufacturers make their profits through a suite of tariff mechanisms which can be either cost of capital or return on

service provision or tax (Lu *et al.,* 2006). Every member of the chain contributes to the telecommunication industry because of their membership to the chain. As a result, such a value chain can also be applied in the South African telecommunications industry (Lu *et al.,* 2006). In Section 2.4 below, the research explores the various initiatives used in some parts of the world to establish rural Internet connectivity.

2.4 Models for Rural Internet Connectivity in Developing Countries

It is now possible to bring Internet connectivity to the rural areas, even though there are undesirable conditions, through the use of wireless communications. Therefore, particular attention must be paid in planning and deploying these networks. The following aspects can be considered as research procedures or steps in setting up networks in rural areas (Agbinya, 2003):

- Evaluate and determine the physical situations of that particular rural area. Thereafter, implement the policy of how, why and when wireless rural telecommunications are to be deployed.
- Provide a clear picture of why there is a need to deploy a wireless network in the research area.
- Choose the appropriate technology according to the findings made in the initial survey and evaluation of the physical aspects of rural areas.
- Define models intended for the rural Internet connectivity.
- Proper tools must then be created for developing and expanding the telecommunications networks.

The following are related projects which exhibit a similar approach to the steps of the research procedure above, and thus form the basis of the discussion of business models for rural Internet connectivity in developing countries.

2.4.1 Manguzi Wireless Network

Manguzi village is located in the KwaNgwanase district in the northern KwaZulu-Natal province of South Africa (Smith, 2000). This area forms part of the Maputaland region and it is 15

kilometers south of the Mozambique border en route to the Ponto Do Ouro border post. Figure 2.3 below shows the Manguzi area.

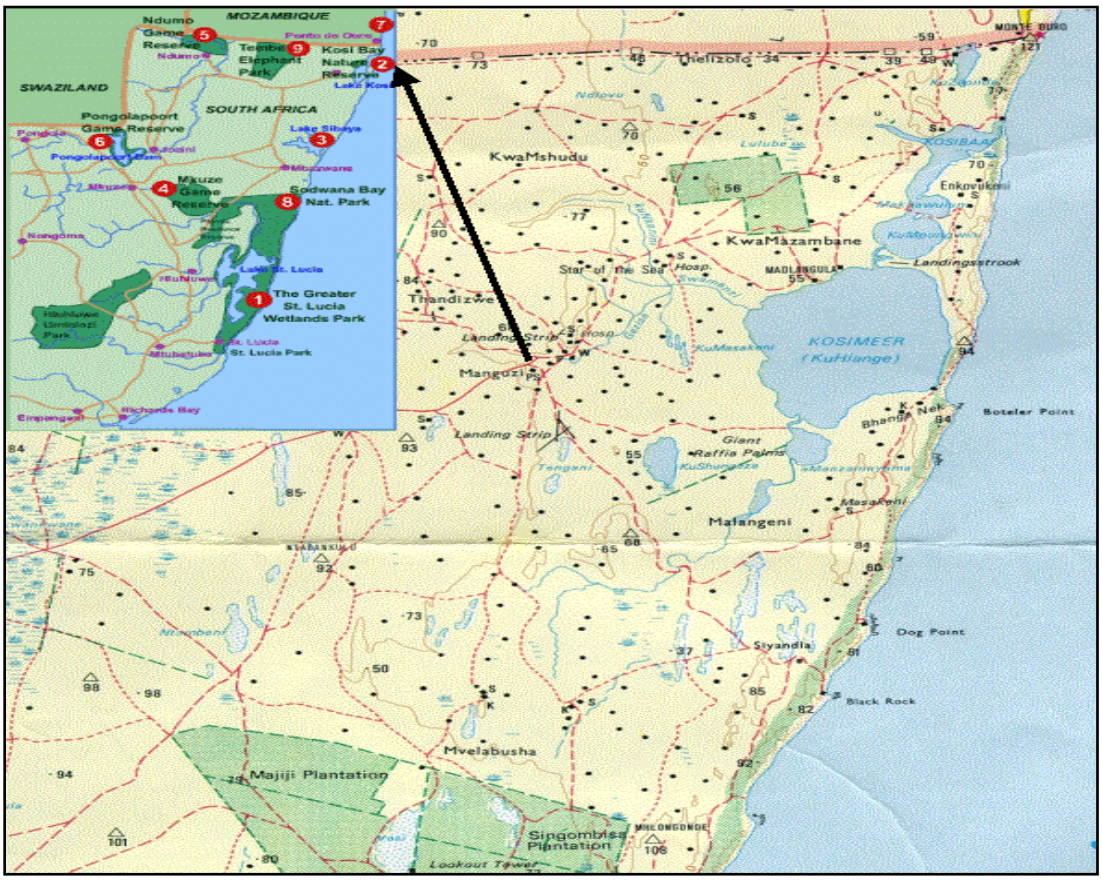


Figure 2.3: Map of Manguzi and its environs (Smith, 2000).

About 100,000 inhabitants live in this 60 square kilometer area and the majority of them are poor peasant farmers (Smith, 2000). The climate in the area is mainly tropical and subtropical which makes it one of the most popular ecotourism places in South Africa. In the past, the Manguzi area has been infested with mosquitoes and tsetse flies (Mandioma *et al.*, 2006). The area became malaria prone which derailed the tourism industry in the area. This is the main reason why Maputaland is still relatively sparsely populated and underdeveloped (Mandioma *et al.*, 2006; Smith, 2000). However, the Kosi Bay nature reserve is one of the biggest tourist resorts around the area which is renowned for its remoteness and unspoiled beauty (Smith, 2000). According to Smith (2000), different projects are being undertaken in the area to support ecotourism. Among these is the introduction of ICTs in the form of a Telecentre.

❖ **Constraints and Motivation**

One of the headmasters in the area approached CSIR icomtek to connect his school to the Telecentre. The idea was to enable students to use the facilities for educational purposes, specifically the Internet (Smith, 2000). However, there were a number of factors which made such this deployment difficult. These included (Smith, 2000):

- Limited funds were available for the installation of the infrastructure. This was due to the low employment rate of about 15%. The area is mainly agriculturally based and under traditional ethnic authority.
- Only three schools out of seventy one in the surrounding area of Manguzi had electricity. Most of the schools did not have telephone lines to connect to the Internet.
- A cheap solution was needed. A solution that was not going to incur monthly costs.
- The telecommunications infrastructure was underdeveloped, with services such as ISDN, VSAT and leased lines not being available. Cellular coverage was unreliable.
- None of the traditional telecommunications infrastructures were suitable.
- Telecommunications politics such as the Telkom monopoly played a critical part as well.

The introduction of ICTs in the Manguzi community facilitated access to opportunities and information (Smith, 2000). As a result, the children were able to conduct their research, communicate with others and equip themselves in terms of career options and empowerment (Smith, 2000). This project aimed to create a local ICT capacity by training young people, nominated by the community, to support and manage the Telecentre and schools network. Afterwards, they were able to train other members of the community to make productive use of the facilities (Smith, 2000). Figure 2.4 below shows the community and school children utilizing these facilities.

Figure 2.4: Students and community members during educational training (Smith, 2000).

- **Manguzi Wireless Internet Implementation**

CSIR icomtek established connectivity in this area by first initiating it at the local community centre (Smith, 2000). This became a Telecentre and it provided different services amongst which is Internet access (web browsing and e-mail), using a dial-up link. The main objective was to provide Internet connectivity which, in turn, supports local economic development. This has been operational since September 1998. The Telecentre comprises of two parts (Smith, 2000):

- A local area network with eight Windows 98 personal computers and a FreeBSD file server. These machines are connected to the Internet and offer different services like word processing, scanning, printing and photocopying. Internet is provided through a dial-up analog connection.
- Five telephone booths and a fax machine are housed in a phone shop. This shop provides phone and fax services to the community.

The initial step was to obtain community buy-in and co-operation (Smith, 2000). It is vital to have community support and participation when launching such a project. Two schools were identified to participate. The schools are Shayina Secondary School with 1002 students and Maputa Senior Primary School with 450 students. The schools were nominated on the basis of

the availability of electricity and their proximity to the Telecentre (3-5 km). This made it easy to access both sites during the installation and testing phases (Smith, 2000). Various traditional methods were explored before the final method on how to connect the schools was chosen. Table 2.1 below provides a summary of the methods and the comments given.

Table 2.1: Link options investigated for Internet connectivity (Smith, 2006).

Option	Comment
Telephone lines	Not available
Cellular telephone	Coverage not ubiquitous and reception very unreliable.
Two-way VSAT	Installation and monthly costs too expensive.
Spread spectrum radio solutions	Requires line-of-sight but the two schools are not visible from the Telecentre. License required.
ISDN	Not available
Satellite Internet Broadcast	High-speed Internet downloads via satellite uses telephone line for the back channel to the Internet. No license required.
Low Frequency Radios	Normally used for telemetry - are limited to very low bit-rates. Attractive option because a partner company had a license and line-of-sight is not a problem.

The network was further extended to two local schools (Maputa HP and Shayina HS) which were connected through the use of a radio link (Smith, 2000). This project utilized the combination of radio and satellite broadcasting technologies to provide Internet access, e-mail and learning resources to schools in a very remote marginalized area (Smith, 2000). According to Smith (2000), satellite receivers are usually capable of receiving data at much higher rates than those made possible via normal telephone lines. The equipment required at each site is indicated in the Table 2.2 below:

Table 2.2: Equipment used in each site.

Schools	Telecentre
Radio and DSB dish	Radio
Yagi antenna	Omni-directional antenna
Satellite receiver card	Connection to Telecentre LAN

Figure 2.5 shows the radio converged with the satellite broadcast for the system implemented and deployed in Manguzi.

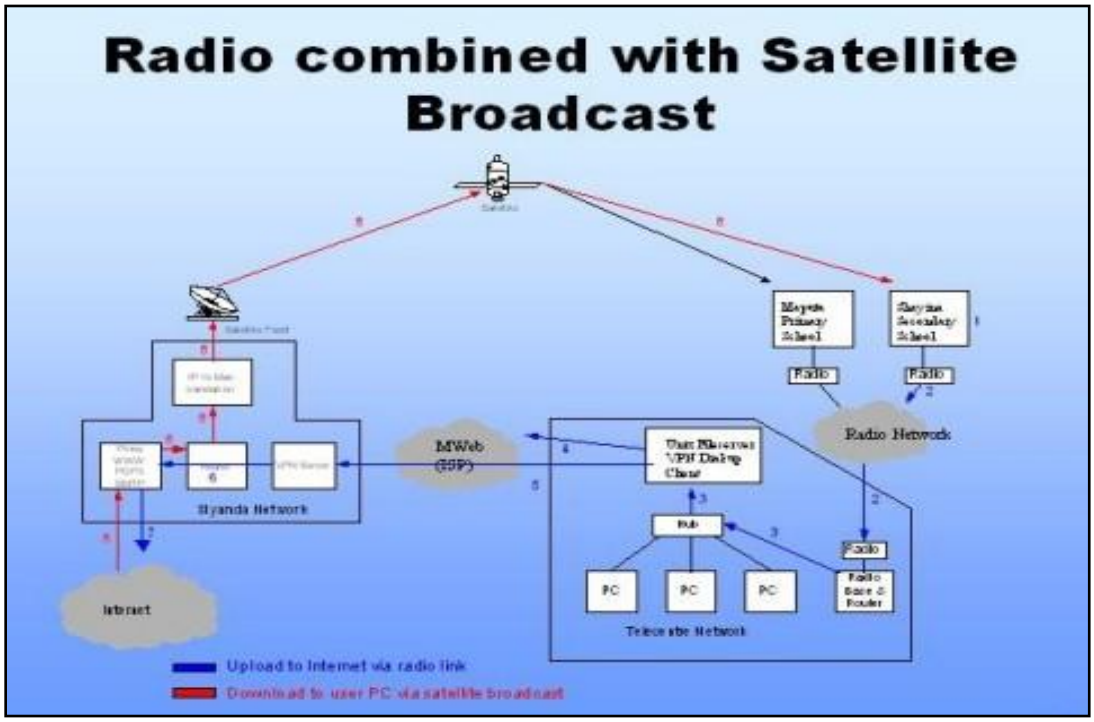


Figure 2.5: Manguzi connectivity setup (Smith, 2000).

A radio with an antenna as well as a satellite receiver card and DSB dish is connected to a computer (Ryan, 2000). A small local area network in the Telecentre serves as the hub of the network because it already has Internet connectivity. A computer acting as a router was connected to the Telecentre network (Smith, 2000). A radio is then connected and an Ethernet card installed in this router. When one tries to connect to the Internet from one of the schools, the request is transmitted to the Telecentre via the radio link. At the Telecentre a Unix fileserver dials on demand to execute the request (Smith, 2000). The requested information is then

downloaded directly to the user's PC using satellite broadcasting technology. The asymmetric nature of the data requirements of Internet applications makes the solution viable (Smith, 2000).

- **Achievements**

The main reason for deploying this facility was to help Manguzi participate in the global knowledge society (Smith, 2000). The community can now access services such as word processing, desktop publishing, send and receive e-mail, surf the Web and perform numerous other activities (Smith, 2000). These services are offered at the Telecentre. Teachers are also able to utilize this ICT advancement in facilitating the education of learners in the area. According to Smith (2000), various difficulties were faced during the launch of the project; poor community support and the politics surrounding access provision were the main problems faced. Additionally, technical support was an issue and therefore proper planning needed to be done before the deployment (Smith, 2000). However, the team gained a lot of knowledge about the different social and cultural aspects that accompany the introduction of ICT in rural South Africa. Even though the project was more challenging than expected, this project increased their knowledge capacity on the innovative use of technology (Smith, 2000).

2.4.2 Macha Wireless Network

LinkNet and its partners at the Meraka Institute (South Africa), TNO (Netherlands) and the Global Research Alliance established an ICT initiative in the rural area of Macha (Matthee et al., 2007). They brought rural Internet connectivity to the area (Matthee *et al*., 2007; Van Hoorik *et al*. 2007). Macha is a village located in the Southern Province of Zambia, 75km from the nearest town of Choma (Van Hoorik *et al.* 2007). Most of its community members are peasant farmers. The area has electricity problems which made it difficult to deploy the telecommunications network. The main objective in deploying this facility was to enable local health institutes to operate more effectively and give local people the opportunity to communicate and explore new ideas (Matthee *et al.,* 2007; Van Hoorik *et al.,* 2007).

❖ **Technical Solution Implemented**

A VSAT was used as the backhaul connectivity to the Internet (Matthee *et al.*, 2007). A wireless local area network (WLAN) consisting of computers and other user devices was connected to the VSAT to obtain an Internet connection. The use of wired connections was minimized because of their high installation costs and sensitivity to physical damage. The current network consists of (Matthee *et al.*, 2007):

- two VSAT satellite connections
- a number of servers
- switches
- routers

Figure 2.6 below illustrates the network topology.

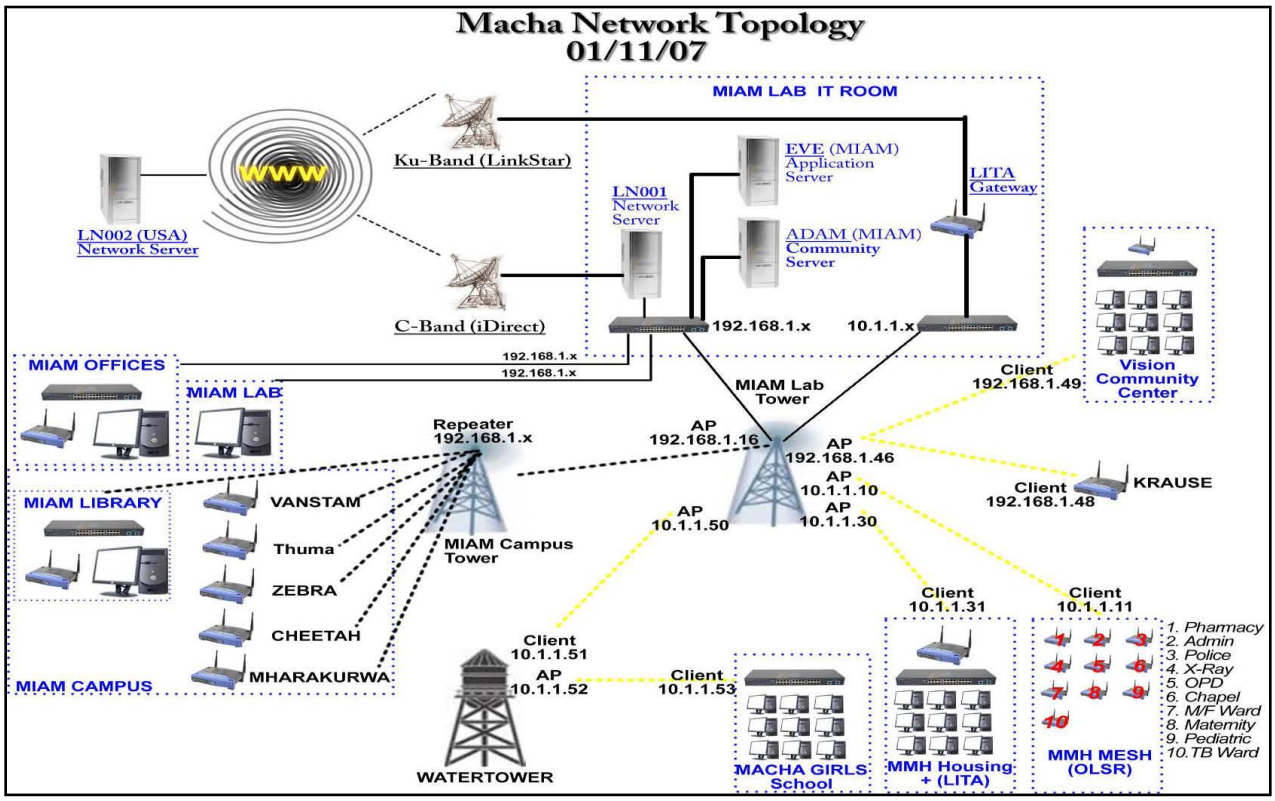


Figure 2.6: Macha network topology (Matthee et al., 2007; Van Hoorik et al. 2007).

The Macha network is divided into a three layer WLAN (IEEE 802.11g) network (Matthee *et al.*, 2007; Van Hoorik *et al.*, 2007). This kind of architecture allows the Internet connection to be shared throughout the community. The top layer is the wireless wide area backbone that interconnects several wireless local area backbones to the middle layer. The clients' access layer, which is the bottom one, has hotspots. Different users access the Internet through this layer.

- **Achievements**

Community members who assisted in deploying this network learnt a great deal about the use of wireless technology (Matthee *et al.*, 2007). The use of the technology required skill and proper planning (Agbinya, 2003). Successful deployment of the Macha network left institutions such as the medical research institute, the hospital and schools connected to the Internet (Matthee *et al.*, 2007; Van Hoorik *et al.*, 2007). An Internet cafe was setup to provide community members with the Internet. They can now access their e-mails, chat, e-learning, buy goods such as second-hand cars from Japan, learn new agricultural techniques and acquire educational material (Matthee *et al.*, 2007).

2.4.3 Long Distance WiFi Aravind Eye Hospital

Researchers from Intel and the University of California at Berkeley, with support from the National Science Foundation, came together and initiated a project called Aravind Eye Hospital (Ramani *et al.*, 2006). It consisted of five hospitals which were interconnected and aimed at providing quality eye care services, at a reduced cost, to its rural poor patients in South India (Dandona *et al*., 2010). A WiFi network which covers long distances, offers high bandwidth and provides point-to-point connections to the Aravind hospitals has seen rural vision centers being interlinked as well (Ramani *et al.*, 2006). Consequently, villagers are now able to have video consultations with the doctors. This project has actually eliminated the problem of patients walking long distances just for regular checkups (Dandona *et al*., 2010).

Since WiFi covers short distances, one tends to wonder how this project was made possible. Actually, they modified the software; specifically the WiFi media access control (MAC) protocol (Dandona *et al*., 2010). The combination of the modified WiFi software, with directional

antennas and routers, is able to send, receive and relay signals (Ramani *et al.,* 2006). This technological advancement has made it possible to achieve network speeds of up to 6 Mbps, at distances up to 40 miles (Ramani *et al.,* 2006). Various projects using a similar technique have emerged. A good example is in Ghana where the University of California at Berkeley also played a major role in the final deployment. Finally, this project is economical and cost effective since the equipment used is cheap and 50 rural clinics are now linked to five big hospitals (Dandona *et al*., 2010).

2.4.4 Tsilitwa Tele-Health Project, Eastern Cape

The Council for Scientific and Industry Research (CSIR) embarked on an ICT innovation in order to improve rural health in the Tsilitwa area of the Eastern Cape Province (Makitla *et al.,* 2010). This pilot project utilizes solar energy to support a low cost communication platform (Callghan, 2009). The advantage of solar energy is that it is renewable. This platform facilitates the improvement of the healthcare and local economic development of the Tsilitwa community (Makitla *et al.,* 2010; Paton, 2003). A wireless infrastructure was setup to connect a school, clinic, hospital, police station and a community Telecentre within a 15km diameter cell. The police station and hospital are located within the Sulenkama village, whereas the clinic is in Tsilitwa (Makitla *et al.,* 2010). The wireless technology developed by CSIR provides voice communication via Voice over IP throughout the cell. Since the two villages are in Non Line of Sight (NLOS), a repeater was deployed between them. The repeater boosts the signal coverage range (Agbinya, 2003). Figure 2.7 below shows the network setup.

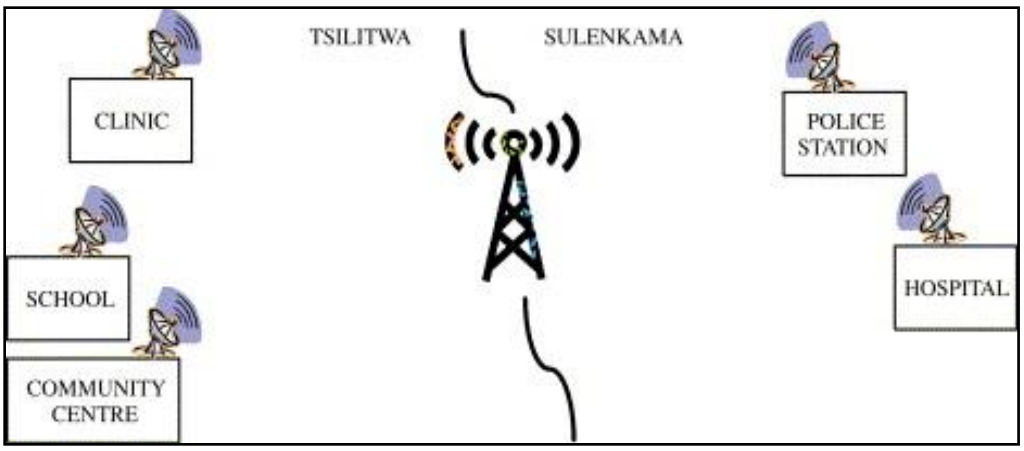


Figure 2.7: Tsilitwa network connectivity adapted from Makitla et al. (2010).

In every digital access node, an omni-directional antenna was installed. A VoIP phone and a desktop were then placed in the computer room. These are used during tele-consultation between a nurse at Tsilitwa Clinic and a doctor at Sulenkama hospital. The audio and video demonstrations use GSM technology. The sustainability of this project is through the use of cost effective intranet communication and the provision of information services (Makitla *et al.*, 2010).

2.4.5 The Village Area Network (VAN)

An ICT was implemented in The Dominican Republic, in a small village called Bohechio (Best, 2003; Ndlovu *et al.*, 2010b). The project's main objective was to improve the economic development of rural communities. The services and opportunities were rendered to the community to improve the living standards, as well as its medical and educational standards (Marine *et al.*, 2004). An area of one square kilometer is covered by this VAN (Best, 2003). There is a Telecentre which was setup and its services are spread throughout the village by use of outdoor antennas and routers which route the WiFi signals to most parts of the village. The wireless network uses IEEE 802.11b standards.

A VSAT and fixed telephone connection were installed and deployed in the Telecentre. External radios and antennas are mounted on the mast tower and the radio links connect to the Telecentre where there is a VSAT. The VSAT acts as an Internet backhaul. The antennas which were

mounted on the municipality building link up with the VSAT on point-to-point connection. The antennas then provide a VAN wireless network to the entire community which spreads to a radius of 1km to the surrounding areas at speeds of up to 11Mbps (Agbinya, 2003). A network topology which uses WiFi, and has services like VoIP implemented, has been successfully deployed. This links the medical clinic and the school. Figure 2.8 below illustrates this VAN network topology.

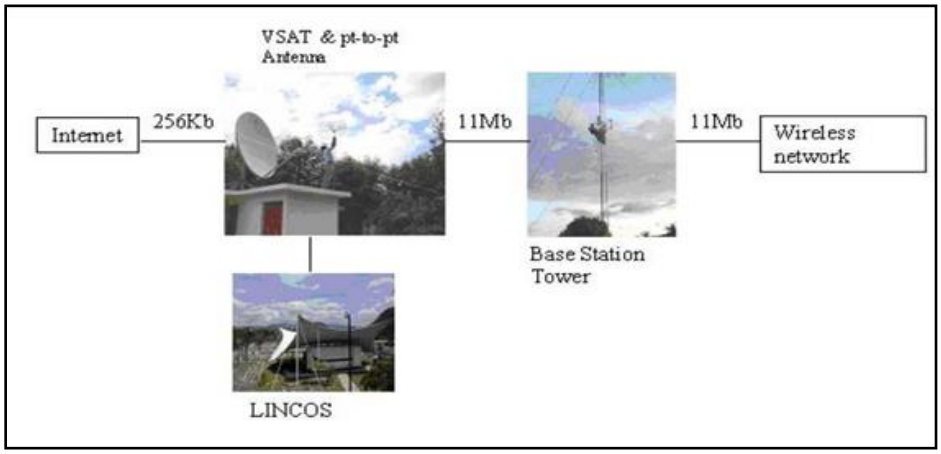


Figure 2.8: Village area network topology (Best, 2003).

The success of the VAN project has attracted other service providers who have joined and deployed their services in the area. As a result, the educational and medical sector of this area continues to improve on a daily basis (Best, 2003; Ndlovu *et al.*, 2010b).

2.4.6 CRCnet: Connecting Rural Communities using WiFi

The WAND group at the University of Waikato embarked on an ICT project. Their aim was to serve and connect rural communities with a low population and low income returns (Brown, 2004). Various wireless networks operating within the Industrial Scientific and Medical (ISM) bands were used for connection purposes. CRCnet used WiFi technology because of its low cost equipment and their desire to integrate it in the existing interface resources. This project uses open source software such as Squid Report Generator (SRG) (Surana *et al.*, 2008). SRG is a log file analyzer for the Squid web proxy. It was chosen because it is flexible and fast. The way in which SRG was created makes it easier to integrate into other authentication systems. If

requested, SRG reports right down to the level of individual files needed. CRCnet developers started from scratch by integrating SRG into other authentication systems rather than modifying an existing program. The reason for this is that the other existing report generators were not giving them what they needed (Brown, 2004). They used another open source monitoring and reporting solution called Distributed Arpwatch (Darpwatch).

This case shows that it is a cost-effective way for network deployment when free and open-source software (FOSS) is used in the establishment of networks and, at the same time, FOSS allows the localization of software that enables people in disadvantaged rural areas to easily conceptualize ICT for development. Again, it elaborates upon the theory of designing and implementing a wireless network in rural areas (Lu *et al.*, 2006). Attention and proper planning should be made before deciding which technology to use. WiFi was chosen by CRCnet because it uses low bandwidth.

2.5 Discussion of the Models

Manguzi Wireless Internet gives an overview of wireless telecommunication network deployment in an area similar to Dwesa. It also shows how different technologies can be integrated so as to offer reliable and efficient Internet connectivity. This is relevant to this study since it plans to merge different technologies such as WiFi, WiMAX and VSAT so as to create a low cost and flexible solution for the Dwesa community. Manguzi Wireless Internet shares the same motivation as this research.

The second case study, the Macha Wireless Network, was deployed in one of the marginalized rural areas of Zambia. The area has electricity problems and an unreliable transport system. These are similar problems as those faced in the area under investigation in this research. A proper survey of the area needs to be done before deploying a telecommunication infrastructure in similar places. This case study provides further knowledge of how to go about surveying the Dwesa rural area so as to deploy a reliable and efficient network.

The third and fourth case studies explain the kind of applications that can be deployed once we have deployed our network. We can provide the Dwesa community with applications such as

telemedicine, e-learning and VoIP services. However, the research conducted on the Tsilitwa Project elaborates on alternative power sources which could be used. It shows that solar energy, which is a renewable resource, can serve as a backup alternative in case of electricity outages. It also sets up a structural reference.

The fifth project explains the relevance of telecommunications development to the level of economic performance. This case study will serve as a model in deciding the economic parameters that need to be used when deploying a telecommunication infrastructure in rural areas.

The VAN project's main objective was to improve the economic development of rural communities. The VAN uses VSAT and WiFi, whereas this research includes WiMAX as the backbone and VSAT as the backhaul. The last case study assists us in choosing the various technologies to use and explains the importance of using FOSS. Open source software usage is seen as a viable option in resolving real technical problems such as Quality of Service (QoS). As a result, this research uses open source developmental software.

2.6 Summary

In this chapter, various rural characteristics resembling those of the Dwesa community were explained. The chapter focused on the importance of delivering rural Internet connectivity using various technologies irrespective of whether they are wired or wireless. Different rural telecommunications projects, similar to this research, were explored to help comprehend the core of this research. The importance of Internet connectivity in marginalized rural areas was also highlighted. Three paramount factors need to be considered when deploying rural networks; these include harsh rural environments, economic issues in a wireless network chain and the type and choice of technology to be used. However, wireless access technologies dominated in all projects deployed in rural areas. Since the main focus of this research was to build a cost effective and sustainable telecommunication network for the Dwesa rural community, various technologies needed to be considered. In the next chapter the characteristics of both wireless and wired technologies are presented along with a discussion of how they can be merged to provide efficient and reliable rural Internet connectivity.

3 Chapter Three: Access Technologies for Achieving Internet Connectivity

Generally, a telecommunication network can be defined as a connection of two or more telecommunication devices, such as computers, with the aim of transferring information (Agbinya, 2003). The telecommunication devices should share the same protocols so that they are able to transfer information. The flow of information in the form of voice, data, and video requires a medium which could be either wired or wireless (Mandioma, 2007). This medium is labeled ICT infrastructure and allows information to be passed in the form of a pulse of light for fiber optic cables, an electrical signal for copper cables and microwave, infrared, radio frequency or laser for wireless media (Herselman, 2003). Any form of equipment that supports the provision of telecommunication services; for example, antenna, towers and satellites, falls under the ICT infrastructure. For proper media selection during the design of a network, the appropriate knowledge and understanding of different advantages and limitations of various access technologies is required (Wong *et al.*, 2006). This allows for the deployment of a reliable and cost effective network. This chapter looks at different access infrastructure technologies at the physical layer, looking at all media of data transmission. It also provides essential knowledge appropriate for selecting the media of data transmission during the network design stage.

3.1 Communications Media for ICT Infrastructure

Wireless communications allow signals to be sent from one point to another through the use of electromagnetic waves (motion of electric fields) as a medium for data transmission (Mandioma, 2007). These waves fall under the electromagnetic spectrum, which extend through a wide range of frequencies and wavelengths. The electromagnetic spectrum is divided into two parts. One part is controlled by licensing regulators and the other is kept open for general unlicensed use. The ISM band falls under the unlicensed portion of the electromagnetic spectrum. South Africa follows these regulations and wireless communication is therefore illegal unless you are the holder of a carrier's license and own the spectrum in which you operate (Mandioma, 2007; Wertlen, 2007). The technologies discussed in the following section are critical if the regulations

permit for their use in South Africa. Section 3.1.1 below, explains the previously used wireless technologies as well as the recent ones.

3.1.1 IEEE 802.11 (WiFi)

Wireless Fidelity (WiFi) connects to the Internet at speeds up to 54Mbps (Best, 2003). WiFi enabled devices use radio technologies based on the IEEE 802.11 standard to communicate data anywhere within the range of an access point and they operate in the unlicensed spectrum (Best, 2003; Ndlovu *et al.,* 2010a). Several IEEE 802.11 components have to interact to create a wireless LAN (Gumaste *et al.*, 2004; Wong *et al.,* 2006). The coverage area, also known as the basic service set (BSS), is the basic building block of an IEEE 802.11 LAN. Within the coverage area of BSS, stations (a station is any device that contains an IEEE 802.11 conforming MAC and PHY interface to the wireless medium) may communicate directly with other stations within the BSS (Best, 2003; Gumaste *et al*., 2004). Should a station leave the BSS, direct communication will cease (Gumaste *et al.,* 2004). A station has to be dynamically associated with an access point (AP) so as to become part of the coverage area (Belloti *et al*., 2001). APs are single servers and provide access to the distribution system. This allows data to move from the coverage area of the AP to the distribution system, via the AP (Baghaei *et al*., 2004). The following is a list of WiFi specifications (Best, 2003; Gumaste *et al.,* 2004):

- Uses 802.11 networking standards.
- Operates in short distances of about 100m.
- Communicates in the 2.4, 3.6 and 5 GHz frequency bands.
- Its bit transmit rate is up to 540Mbps.
- Easily susceptible to access by unauthorized users who could use the access as a free Internet connection.

To address the issues of wireless local area coverage, the IEEE 802.11 standard was modified. This resulted in the standard operating at different frequencies which are incapable of interfering with each other (Best, 2003; Gumaste *et al.,* 2004). The new standards, based on IEEE 802.11, are differentiated from each other through the use of an alphabetic suffix. These standards are

802.11, 802.11a, 802.11b, and 802.11g. Table 3.1 below shows the specifications of each standard.

Table 3.1: Wireless LAN standards chart (Gumaste et al., 2004).

IEEE 802.11 standard	Specifications
802.11	The original WLAN standard; supports 1 to 2 Mbps.
802.11a	High-speed WLAN standard for 5 GHz band; supports 54 Mbps.
802.11b	WLAN standard for 2.4 GHz band; supports 11 Mbps.
802.11d	International roaming: automatically configures devices to meet local RF regulations.
802.11e	Addresses quality-of-service requirements for all IEEE WLAN radio interfaces.
802.11f	Defines inter-access-point communications to facilitate multiple-vendor distributed WLAN networks.
802.11g	Establishes an additional modulation technique for the 2.4 GHz band; supports speeds up to 54 Mbps.
802.11h	Defines the spectrum management of the 5 GHz band.
802.11i	Addresses the current security weaknesses for both authentication and encryption protocols; the standard encompasses 802.1X, TKIP, and AES protocols.
802.11n	Provides higher throughput improvements; intended to provide speeds up to 500 Mbps.

Advantages

- Low cost and easy deployment (Best, 2003; Gumaste *et al.,* 2004).
- Supports hotspot establishment which will allow community members to access the Internet 24 hours a day (Best, 2003).
- Less financial pressures due to minimal infrastructural deployment as compared to wired technology (Best, 2003; Gumaste *et al.,* 2004).
- 802.11b and 802.11g standards are able to frequency hop.

- It uses an unlicensed radio spectrum. This means that there is no need for regulatory approval prior to use (Gumaste *et al.,* 2004).
- It supports roaming (Belloti *et al*., 2001).
- Ability to deploy networks without the use of cables reduces network deployment and expansion costs (Best, 2003).
- WiFi has global standards which allow its users to work in different countries worldwide.
- Its products are extensively available on the market. Different access points and user's network interfaces are able to interoperate at a very basic service level (Best, 2003).

Disadvantages

- Unsuitable for distances exceeding 100m because it was initially designed to be a LAN network standard (Best, 2003).
- Poor when it comes to offer backhaul connectivity. This becomes a problem particularly with our mission of connectivity for a disadvantaged rural area (Best, 2003).
- Interference affects the ISM band (Baghaei *et al*., 2004).
- Inconsistency in spectrum assignments and operational limitations worldwide.
- Degradation in performance because of the existence of other devices such as Bluetooth, microwave ovens, cordless phones, or video sender devices and many others which all operate at the unlicensed 2.4GHz spectrum used by WiFi (Best, 2003).
- Wired equivalent privacy (WEP) encryption has been shown to be breakable even when it has been correctly configured (Lu *et al.,* 2006).

WiFi presents a number of limitations such as short range coverage, high interference and low signal strength as the distance increases. An alternative has to be considered to overcome these shortfalls of WiFi. In the next section, WiMAX technology is discussed since it is considered an alternative to WiFi.

3.1.2 IEEE 802.16 (WiMAX)

WiMAX stands for Worldwide Interoperability for Microwave Access (Sweeny, 2004). WiMAX usually provides last mile connectivity to many networks. It provides significant bandwidth which is shared among users efficiently (Best, 2003; Wong *et al.,* 2006). It follows the IEEE 802.16 standards of wireless technology (Sweeny, 2004). This broadband wireless access technology supports and provides radio coverage of approximately 70km to users (Sweeny, 2004). There are a variety of applications supported by WiMAX such as video, voice, data and entertainment services. The traffic flow of these applications can be unidirectional, asymmetrical, symmetrical or change with time (Best, 2003; Wong *et al.,* 2006).

WiMAX was initially published in 2002 and then later approved in June 2004 by IEEE (Sweeny, 2004). This version of WiMAX, which is the 802.16d, is the fixed WiMAX standard IEEE 802.16-2004. It supports point-to-multi-point (PMP) and point-to-point (P2P) broadband wireless access and its product-profile utilizes the OFDM 256-FFT system profile (Sweeny, 2004). Current deployments use this standard. However, the mobile WiMAX standard, the 802.16-2005 (also known as 802.16e) was approved by IEEE in December 2005. This standard has added features such as mobility and allows for fixed wireless and mobile NLOS applications, by enhancing the Orthogonal Frequency Division Multiple Access (OFDMA) (Wong *et al.,* 2006). It operates on frequency bands of 2 to 11 GHz-licensed bands and allows for the roaming of WiMAX compliant equipment (Sweeny, 2004).

IEEE 802.16f – This is also known as Management Information Base for Fixed Services. Actually, it is an amendment and has improved enhancements to IEEE Standard 802.16-2004. It defines a management information base (MIB) for the MAC and PHY and associated management procedures (Wong *et al.,* 2006).

IEEE 802.16g – This is the amendment of the IEEE Standard 802.16-2004 which is still under development and it is also known as the Management Plane Procedures and Services. It provides enhancements to the MAC and PHY management entities of IEEE Standard 802.16-2004, as amended by P802.16e, to create standardized procedures and interfaces for the management of conformant 802.16-devices (Wong *et al.,* 2006). WiMAX uses OFDM. As a result, it has wide

bandwidth and has the ability to carry very high data rates. A summarized list of the characteristics and features of WiMAX are provided below (Sweeny, 2004):

- Has wide signal coverage, with a theoretical maximum range of approximately 70km, with a direct line of sight.
- Has a higher speed of broadband service.
- Has a theoretical maximum bandwidth of 75Mbps.
- Provides up to 3Mbps broadband speeds without the need for a cable.
- Is based on the IEEE 802.16 standards (also called Broadband Wireless Access).
- Enables the delivery of last mile wireless broadband access.

Advantages

- Since the aim of this research is to provide Internet connectivity to a deep rural area, WiMAX is a good option for backhaul connectivity and offers cheap, fast broadband connectivity to rural and other underserved areas (Best, 2003; Wong *et al.*, 2006).
- Offers good quality of service (QoS) for applications such as VoIP which will be deployed in our network (Sweeny, 2004).
- It is designed to be a MAN/WAN technology. Since it covers a wide area, it is ideal for rural connectivity (Wong *et al.*, 2006).
- Easy to install and deploy in rural areas where wired technology is difficult to deploy. Using this technology overcomes problems associated with connectivity in remote, disadvantaged areas (Best, 2003).
- It is more reliable and cost effective in areas where traditional xDSL is unsuitable due to a small number of customers per digital subscriber-line access multiplexer (DSLAM).
- Operates efficiently in non line of sight (Sweeny, 2004).

Disadvantages

- As the distance becomes significantly long, LOS is required for long-distance connections. Backhaul connectivity becomes a problem in such situations (Sweeny, 2004).
- Few companies offer pre-WiMAX products in South Africa. As a result, the products have to be shipped into the country which makes them costly (Best, 2003).
- WiMAX offers lower data rates in comparison to other wired technologies like optical fiber (Wong *et al.*, 2006).
- The signal strength can be affected by buildings, trees and atmospheric conditions, such as rain. This degrades the performance of WiMAX (Wong *et al.*, 2006).

However, the use of wireless cellular systems can be taken into consideration. It is noted that none of the technologies discussed above are ubiquitous. Section 3.1.3 below is a discussion of wireless cellular systems. This kind of technology can be beneficiary to the South African community since it is ubiquitous.

3.1.3 Wireless Cellular Systems

The three groups of wireless cellular systems include First Generation Technologies (1G), Second Generation Technologies (2G) and Third Generation Technologies (3G) (Best, 2003). There is a fourth one under study and it is the Fourth Generation Technology (4G). Firstly, 1G was started in the 1940s and was mainly based on Advanced Mobile Phone Service (AMPS) technology (Andersson, 2001). The AMPS provided roaming telephone services and were based on Frequency Division Multiple Access (FDMA) technology. They also provided limited data rates of less than 10 Kbps (Andersson, 2001).

However, during the 1990s, 2G emerged and it was based on digital mobile technologies which made use of Code Division Multiple Access (CDMA), Time Division Multiple Access (TDMA) and Global System for Mobile Communications (GSM) (Andersson, 2001). 2G also offered limited data rates of up to 20 Kbps (Andersson, 2001). GSM was deployed mainly in European countries and South Africa, whereas various parts of the USA used the TDMA and CDMA.

Between the 2G and 3G, an intermediate technology emerged called the 2.5G. The 2.5G technology embraced technologies such as General Packet Radio Service (GPRS), Enhanced Data rates for GSM Evolution (EDGE) which is 2.75G and CDMA. The 2.5G technologies were more of a converged voice and data centric just like 3G (Andersson, 2001).

Finally, there was an emergence of 3G which is mainly based on International Telecommunications Unions (ITU) and International Mobile Telecommunications-2000 (IMT-2000). Technologies such as the Universal Mobile Telecommunications System (UMTS), CDMA-2000 and Time Division Synchronous Code Division Multiple Access (TD-SCDMA) all fall under the 3G umbrella. In South Africa, Vodacom, Cell-C and MTN offer 3G which provides data rates of up to 100 Kbps (Andersson, 2001). However, 3G can support data rates up to 2Mbps. A new technology has been proposed and is envisaged to offer higher data rates, support global roaming and multiple classes of service with variable end-to-end Quality of Service (QoS). 4G will be based on a pure-IP architecture and pure packet switched. Figure 3.1 below shows the wireless cellular systems generations and how they have evolved.

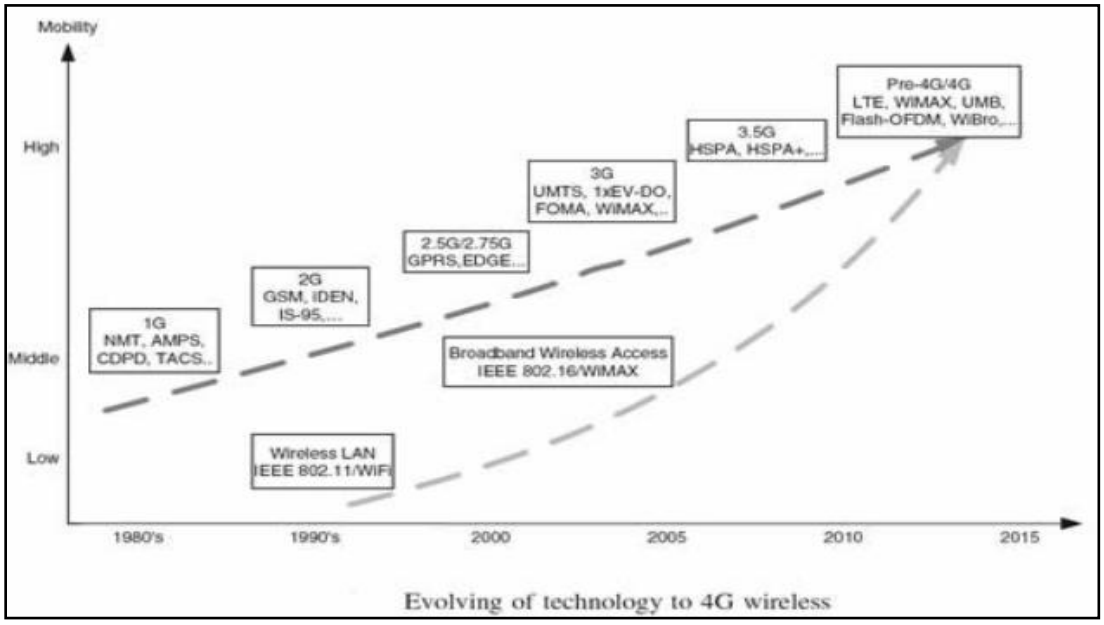


Figure 3.1: Wireless cellular systems generations (Halonen et al., 2003).

Advantages

- In South Africa, it is readily available. MTN, Cell-C and Vodacom provide 90% coverage. This technology can be used for rural connectivity (Andersson, 2001).
- 3G can provide converged voice and data applications. As a result, various applications such as voice and data will be provided in one network (Halonen *et al*., 2003).
- There is no need to deploy infrastructure from scratch since the bulk of the cellular phone infrastructure has previously been deployed (Andersson, 2001).

Disadvantages

- Rural coverage is very low since 3G services are mainly available in large cities like Johannesburg, Cape Town and Durban (Andersson, 2001)
- An alternative is GPRS which offers very low data rates up to 384 Kbps. This is low when compared to some of the wireless and wired technologies (Andersson, 2001).
- The technology requires a mobile phone with 3G capabilities and it is not certain that this is always available (Halonen *et al*., 2003).

Having outlined the general specifications of different wireless cellular systems, the next section delivers a short discussion of the General Packet Radio Service (GPRS), which is a more specific 2.5G standard with maximum data transmission at 50Kbps. This technology is seen as a forerunner for the so-called 3G mobile Universal Mobile Telecommunications System (UMTS).

3.1.4 GPRS

This is a packet based technology which is ubiquitous and is used for sending and receiving high-speed data across the GSM network (Andersson, 2001). Since it is radio technology, it adds packet-switching protocols at a shorter set-up time for ISP connections. It supports flexible data transmission rates, typically up to 20 or 30 Kbps. With GPRS, several devices can now be deployed. This was not possible with the traditional GSM (Andersson, 2001). This is due to the fact that the traditional GSM has limitations in speed (9600bps), message length of the Short Message Service (160 characters), dial up time and costs (Andersson, 2001). As a result, it can

only be used in applications such as point of sale terminals, vehicle tracking systems, and monitoring equipment which can be deployed. However, GPRS does not guarantee any level of quality but operates within a best possible attempt scenario (Andersson, 2001). The unused portions of the GSM network are used by the GPRS to transmit and receive data packets (Andersson, 2001).

Advantages

- It does not require the setting up of permanent structures. This reduces deployment costs (Andersson, 2001).
- Allows mobile phones to have Internet access and large amounts of information can be transferred to and from the mobile device over the Internet.
- As long as one is within the radius of the GPRS, the mobile phone can be used to access the Internet (Halonen *et al.,* 2003).
- It can be used as backup connectivity technology because of its portability and fast data cards, which plug directly into the laptop.
- Users only get charged for transmitting and receiving data. As a result, they can stay connected forever and not get charged (Halonen *et al.,* 2003).

Disadvantages

- GPRS uses the cellular network's GSM band to transmit data and, as a result, other network related functions and calls cannot be used as long as the connection is active (Andersson, 2001).
- It is not convenient for real time data transfer when using point to multi-point systems especially when the time rate exceeds 10 minutes (Halonen *et al*., 2003).
- The number of circuit-switched connections is less than the packet switching connections and, as a result, GPRS packet loss phenomena occur (Andersson, 2001).

Different wireless technologies have been discussed and it has been shown how they could be used to achieve the much anticipated rural Internet connectivity. However, power line

communication (PLC) is one of the wired technologies often used and investigated in South Africa. Section 3.1.5, below, discusses PLC technology and explains its advantages and shortfalls.

3.1.5 Power Line Communication (PLC)

Power Line Communication allows a broadband data signal to be transmitted over electricity lines together with an electric current (Tongia, 2004; Locher, 2002). The technology is cost effective since data signals are transmitted in a pre-existing electricity or power line infrastructure. As a result, there is no need for new infrastructure installations (Dostert, 2001). This concept is also known as broadband over power lines. High and medium voltage PLC offers transmission rates of up to 64Kps and has been used primarily for point-to-point data communication. Power utility industries started utilizing this technology long ago, dating back to 1920. They used it primarily to communicate with and monitor their power networks (Dostert, 2001). Street lights and other minor services could be switched on and off through the use of PLC. However, PLC technology has improved greatly through the integration of complex frequency modulation processes such as OFDM (Orthogonal Frequency Division Multiplexing), semi-conductor chips and improved transmission rates of up to 1Mbps. This makes it an alternative for last mile Internet connectivity to other technologies such as Ethernet cable networks and DSL services (Tongia, 2004; Locher, 2002).

Modern PLC uses its sophisticated modems to transmit and receive data at a higher frequency than the 50Hz to 60Hz used for AC power. As a result, the two signals are able to coexist on the same line (Dostert, 2001). Research shows that the technology keeps on advancing with data transmission rates having reached up to 4.5Mbps and 14Mbps. Some researchers have quoted data rates of up to 45Mbps being achieved. Carrier frequencies in which PLC operates affects its coverage distance (Dostert, 2001). A frequency of 2.4MHz can cover a range of 150m to 250m whereas for 8.4MHz the typical distance can be 100m to 200m. Consequently, the use of repeaters can help to regenerate the PLC signal for better coverage on the low-voltage power line (Tongia, 2004). The repeaters also relay communication between neighboring units, including a medium voltage node and low-voltage head-end, another repeater and Customer Premises Equipments (CPEs). PLC is cheaper than broadband services offered over DSL (Dostert, 2001).

In South Africa, PLC offers the opportunity to deliver telecommunication services to remote and low tele-density areas. A pilot PLC project was deployed in the Tshwane Metro at the Rooiwal area, just outside Pretoria. The aim of the project is to provide landline access to almost all of South Africa's poor residents by delivering voice and data services through existing electricity lines. Currently, more than 130 homes are connected on the PLC network as part of the investigation into frequency interference (Mandioma, 2007). All those connected have a fully-fledged VoIP installation. Rooiwal homes connect to the Internet via Telkom through a point of presence (POP) in the City of Tshwane network operating centre, with the municipality's fiber optic line and all homes having a working VoIP installation.

Advantages

- It is cost effective since it uses existing infrastructure and remote rural areas with a power-line grid can get connected to the Internet (Dostert, 2001).
- It is easy and simple to set-up since it has plug-and-play. There is no need for new complicated cable and wiring installations (Tongia, 2004; Locher, 2002).
- For rural users, it can offer all-in-one facilities such as telephone, cable television and high-speed Internet connectivity (Dostert, 2001).
- It does not depend on frequency and line voltage of current (Tongia, 2004).

Disadvantages

- It is difficult to implement because 32.1% of the disadvantaged rural areas of South Africa remain outside an electricity grid line (Mandioma, 2007)).
- Surges in voltage or by electrical appliances create significant interference in power lines.
- The electricity grid becomes a giant transmitter which radiates waves that interfere with wireless communications. This is caused by the usage of high frequency signals needed for data transmission (Tongia, 2004; Locher, 2002).
- Grid electricity suppliers, such as Eskom, experience copper cable theft (Mandioma, 2007).

- PLC regulations are not standardized and the high bandwidth is still in its infancy (Tongia, 2004).

Having looked at the wireless options and one of the wired technologies available in South Africa, for rural Internet connectivity, an extensive wireless network comparison is given in Section 3.2 below. Wireless technology proves to be more realistic and convenient for this research. The reason for this is the fact that the study seeks to bring Internet connectivity to a deep rural area of South Africa using cost effective and reliable technologies or tools. In Section 3.2 below, a comparison of the different wireless technologies is given.

3.2 Wireless Networking Comparison

This section offers a comparison of different wireless technologies that can be converged for rural Internet connectivity. This comparison provides a clear understanding of why some of these technologies are unsuitable to be merged for the provision of a reliable and constantly available communication link.

3.2.1 WiFi vs. Bluetooth

WiFi and Bluetooth technologies use the 2.4GHz unlicensed radio spectrum (Yu *et al.*, 2006). Bluetooth can cover a range of approximately 10m. Due to short range coverage, it is suitable for data file transfer from one device to another in close proximity. Various devices such as phones, printers, personal digital assistance, modems and computers have built-in Bluetooth receivers. The 16bit Personal Identification Number (PIN) used for Bluetooth authentication and data encryption is not as robust as the 80211i security enhanced protocol used in WiFi (Yu *et al.*, 2006). Lastly, the low bandwidth and low signal coverage of Bluetooth, makes it difficult and practically impossible to set up an effective and reliable network for remote applications (Yu *et al.*, 2006).

3.2.2 WiFi vs. UMTS/3G

WiFi and UMTS/3G technologies offer mobility to end users (Morrow, 2004). They have similar characteristics. However, WiFi has a drawback of low distance coverage compared to 3G. The low coverage of WiFi limits its application around hotspot areas, but it enables user-friendly interfaces to be used as IP-based broadband access devices (Esmailzadeh, 2006a). In fact, WiFi and UMTS work better as complementary access technology (Ndlovu *et al.*, 2010a; Esmailzadeh, 2006a).

3.2.3 WiMAX vs. UMTS/3G

Universal Mobile Telecommunications System (UMTS) is a general mobile wireless access technology with data speeds of 384Kbps (Morrow, 2004). This is very low compared to that of WiMAX which can go up to 75Mbps for coverage of 50km. Similarly, compared to other mobile technologies, WiMAX has the capability of transmitting data and voice (Wong *et al.,* 2006; Sweeny, 2004). The choice of using mobile technologies in transmitting voice is more expensive with VoIP/WiMAX compared to WCDMA/HSDPA (Computer Science Corporation, 2005). The overall cost for WiMAX equipment is much lower in comparison to that of UMTS, especially due to the less frequent usage of high tower structures. The UMTS cellular system has an advantage over WiMAX in that its infrastructure for 3rd Generation mobile network (3G), HSPDA, GPRS and Evolutionarily Distinct and Globally Endangered (EDGE) already exists while WiMAX requires a new infrastructure to be set up for it to operate (Morrow, 2004). UMTS is preferred for mobile communication, when compared to WiMAX, because of its easy availability (Ndlovu *et al.,* 2010a).

3.2.4 VSAT vs. WiMAX

VSAT can be used for backhaul Internet connectivity in remote rural areas. WiMAX can then act as the backbone for the provision of a point-to-multi-point service to surrounding areas such as schools and clinics (Meldrum, 2003). However, in such a connection, there is a need to use Ethernet or WiFi technologies as end user access technologies. This type of convergence shows that different access technologies such as VSAT, WiMAX and WiFi can be merged to provide

ever present Internet access in remote rural areas. This aim of this research is to achieve ubiquitous Internet access in a remote rural area. The main disadvantage of using VSAT is the high cost of installation and maintenance. However, it has high security levels which are achieved through the use of VPN/IPSec as its security mechanisms (Meldrum, 2003).

3.2.5 WiMAX vs. GPRS

GPRS and WiMAX can be used to provide Internet access to underserved rural areas. WiMAX can be used as an access network and GPRS as the core network (Sweeny, 2004). Since GPRS is a packet switched network, it is easier to use than the GSM core network. It operates using the priority system and voice has a higher priority. This kind of technology is useful in providing best effort communication in rural areas (Wong *et al.*, 2006). However, a WiMAX network is set up using point-to-point connections between nodes. A PC acting as a server which provides Internet to the rest of the WiMAX network will be connected to one of the nodes. As a result, the GPRS network will act as the core network in this scenario (Sweeny, 2004).

3.2.6 WiFi vs. WiMAX

WiFi and WiMAX technologies have many similarities (Morrow, 2004). However, the major difference in these wireless access technologies is the communication range (Wong *et al.*, 2006). In general, WiFi was designed for a short range of approximately 100m and WiMAX can cover distances of close to 70km (Wong *et al.*, 2006). They are compared in Table 3.2 below.

Table 3.2: Comparison of WiFi and WiMAX (Wong et al., 2006).

WiFi	**WiMAX**
➢ Range :100 m, covers a coffee shop, one floor of an office building ➢ Throughput: 11 Mbps ➢ Security: Limited ➢ QoS: Limited	➢ Range : 70 km, covers a small city with one base station ➢ Throughput: 75 Mbps ➢ Security: Multi-level encryption ➢ QoS: Dynamic bandwidth allocation, good for voice and video

3.3 Converged Wireless Infrastructure

According to Ndlovu *et al.* (2010a), the term convergence in this context means combining two or more technologies so as to achieve high broadband data throughput rates, high reliability, low latency and a more secure network. The converged wireless networks are thought to offer a variety of benefits including increased security, more flexibility and scalability, significantly reduced costs, effective communication and simplicity (Ndlovu *et al.*, 2010a).

3.3.1 Criteria of Choosing Technologies for Rural Areas

Various factors have to be considered when one chooses technologies for rural areas. The following are some of the aspects that can be taken into consideration:

- The costs of the infrastructural implementation and operation have to be low so that the deployed wireless network is affordable to the community in rural areas.
- The suitability, strength and weakness of the technology have to be taken into account. The rural areas require a user friendly and constantly available wireless network.
- The technology has to be effective, simple and, at the same time, more secure.
- Flexibility and scalability are to be used together with other technologies.
- The implementation of the technology must be independent of basic infrastructure such as electricity, running water and tarred roads.
- The technology must provide coverage over a large area irrespective of the nature of rural environments. Wireless networks seem to be an option.

The following Table 3.3 gives the qualitative comparison of some of the technologies discussed above.

Table 3.3: Summary of Qualitative Comparative Features

Attribute	WiFi	WiMAX	3G (1xEVDO)	HSDPA/HSUPA	Bluetooth
Base Standard	!EE 802.11	IEE 802.16d/e-2005	IMT-2000	WCDMA	BSIG IEEE 802.15.2
Duplex Method		TDD^3	FDD	FDD	FHSS
Uplink Multiple Access	OFDMA	OFDMA	CDMA	CDMA , CDM-TDM	UMTS W-CDMA
Channel BW	2.4GHz	Scalable: 5, 7, 8.75, 10MHz	1.25 MHz	5MHz	2.402 – 2.48Ghz
Frame Size		5ms TDD	1.67ms DL 6.67ms UL	2ms DL 2.10 ma UL	
Modulation DL	QPSK	QPSK/16QAM/64 QAM	QPSK/8PSK/16QAM	QPSK/16QAM	DQPSK
Modulation UL	QPSK/16QAM	QPSK/16QAM	BPSK/QPSK/8PSK	BPSK/QPSK	8DPSK
Coding	Turbo	CC, Turbo	Turbo	CC, Turbo	N/A
H-ARQ	Multi-Channel Asynchronous CC	Multi- Channel Asynchronous CC	Fast 4- Channel Asynchronous CC	Fast 6- Channel Asynchronous CC	Asynchronous Connection-Less
Scheduling	Fast Scheduling in DL and UL	Fast Scheduling in DL and UL	Fast Scheduling in DL	Fast Scheduling in DL	Adaptive frequency hopping
Handoff	Network initiated Handoff	Network Optimized Hard Handoff	Virtual Soft Handoff	Network initiated Hard Handoff	N/A
Beam forming	Yes	Yes	No	Yes (Dedicated Pilots)	Yes
DL Peak Over the Air Data Rate	54Mbps	46Mbps, DL/UL=3^4 32Mbps, DL/UL=1 (!0 MHz BW)	3.1Mbps	14Mbps	2.1 Mbps
UL Peak Over the Air Data Rate	11Mbps	7Mbps, DL/UL=1^5 4Mbps, DL/UL=3 (!0 MHz BW)	1.8Mbps	5.8Mbps	723.1 kbps

3.3.2 Chosen Technologies

VSAT and WiMAX are classified as service provider technologies and VSAT offers backhaul connectivity. WiMAX will be the backbone of the network (Best, 2003). WiMAX can be converged with a variety of technologies such as WiFi and other mobile technologies. However, in this research we chose WiFi as the access technology. This is evident in the wireless comparison discussion which clearly illustrates the potential capabilities of WiFi. WiFi can offer much higher data rates and is cheap. The problem with 3G is that it operates within the licensed spectrum and, as a result, accumulates monthly costs (Andersson, 2001). It is crucial to understand the security issues of a converged WiFi and WiMAX and the ways in which these need to be incorporated and adopted so as to deploy a reliable and cost effective network in Dwesa. This research made use of a combination of WiFi, WiMAX and VSAT technologies.

3.4 Important Considerations

The following facts and considerations have to be taken into account prior to embarking on the construction of a wireless network for marginalized areas (Agbinya, 2003):

- ***Cost of support versus the cost of planning*** - Maintaining a badly designed network and appropriate planning prior to the deployment of a wireless network presents a trade-off in terms of cost. As a result, the appropriate planning and selection of equipment is essential prior to the deployment of wireless networks in rural areas.
- ***Telecommunications Regulations*** - Appendix B shows the specific regulations for each country in Africa regarding WiFi equipment. The use of the 2.4GHz and 5.8GHz bands is regulated by a regulatory body in each country. This goes for the maximum power output for wireless equipment as well, which is also regulated.
- ***Wireless network planning (channels)*** - Channels 1, 6, and 11 are the only three non overlapping bands in the IEEE 802.11 b/g standards.
- ***Ethernet network planning (subnets)*** - When deploying wireless networks, IPv4 addresses are assumed but IPv6 can also be used. However, this research will use IPv4 addresses.

- ***Interference of signals*** - The signals can be obstructed and experience interference. As a result, obstructions such as trees and plants should be taken into consideration. Objects like water on the leaves, roofs as well as reinforcements in concrete walls, negatively affect signal strength. Before the deployment of wireless networks, one has to make sure that access points will not be obstructed by any object in order to avoid interference.
- ***Lightning*** - Before deploying wireless equipment outdoors, appropriate protection from lightning is essential. Wireless equipment is susceptible to lightning damage. As a result, lightning protection is of paramount importance, especially for outdoor deployments.

3.5 Requirement Components

Both hardware and software will be of much use and critically needed during the implementation phase. These components will support and provide WiFi and WiMAX. In Section 3.5.1 below, the different software components are briefly discussed, as well as the hardware used during the deployment of this network.

3.5.1 Software

In this research, Free and Open Source Software (FOSS) is used. Since the Linux operating system is a FOSS, the study opted to use the Ubuntu 9.04 Jaunty version. Other software used included the ChilliSpot and FreeBSD which were downloaded for free from the Internet. The following discussion offers a summary of the software that was used:

- ***Ubuntu 9.04 Jaunty Operating System*** **–** This is the version of Linux used at the time of the implementation of the WiFi/ WiMAX SLL network.
- ***FreeBSD*** **–** This software version was released by Berkeley Software Distribution (BSD) and is a UNIX-like free operation system from AT&T Unit. Each router at each Digital Access Node (DAN) operates using the FreeBSD 6.1 version. Whereas the access concentrator at Mpume Junior Secondary School (MJSS) has the FreeBSD 6.2 version installed. We present a full discussion on the FreeBSD in Chapter Five.
- ***Backtrack 4.0*** **–** This is used for auditing and managing wired or wireless networks. This networking security suite is a Linux based operation system. Backtrack was downloaded

from the Internet since it is a FOSS as well. Its features include an update kernel running with several patches. During an attack, it can support many wireless drivers to build a raw and packet injection. Backtrack has many built-in security tools which include RFMON, kismet, nmap, etherape and wireshark (formerly known as ethereal).

- ***ChilliSpot* –** This software uses a Free radius server to handle the authentication, authorization and accounting for wireless users (Beltrame, 2007).

3.5.2 Hardware

Different brands of hardware were used for this research. The access points that were used were drawn from the two popular Cisco and DLink brands. In this regard, a brief description of the hardware components that were used in this research is provided here:

- ***Wireless Access Points (AP)* –** Access points which support IEEE 802.11b include the Cisco Aironet 1100 AP series, Cisco 1130AG and a DWL 2100 AP. Whereas, the Cisco 1130 AG had additional support for 802.11a/g.
- ***Customer Premises Equipment (CPE)* –** This is also known as the Subscriber Unit (SU). CPEs are usually installed as the organizational entity. According to Alvarion (2005), for this research, the user's data equipment is connected through the 10/100 Ethernet port; this provides data connection to the Access Unit. This, on its own, provides bridging functionality; traffic shaping and can support up to 512 MAC addresses. Generally, CPEs consist of two inseparable components. There is the Outdoor Unit (ODU) which contains the modem, radio, data processing and the management components of the SU and the Indoor Unit (IDU) which is powered from the mains (Sweeny, 2004).
- ***Micro Base Station (BS)* –** This comes in two variants which are chassis configuration and a micro base station. A micro base station was deployed in the Ngwane Junior Secondary School (NJSS) access node and has the capability and functionality of communicating with the CPEs. It can connect to the backbone (VSAT connection at MJSS) of the Internet Service Provider (ISP). It has built-in additional functions such as traffic classification and connection establishment, policy based data switching, service

level agreement management and alarm management, more than BreezeMAX modular Base Station (Alvarion, 2005).

3.6 Summary

This chapter presented the optional technologies available in South Africa for connecting the rural areas and delivering an ever present Internet access. Both wired and wireless technologies were discussed and their capabilities and weaknesses exposed. Wireless technologies proved to be more advantageous than wired ones in terms of offering rural Internet connectivity. This was evident in the study's comparison of wireless technologies and the outline of the requisite components for implementation. The actual implementation of the selected technologies for this research will be discussed later in the study. However, it is important to know how to control access and understand the security issues of the technologies chosen for this research; this is discussed in the next chapter.

4 Chapter Four: Controlling Wireless Access within IEEE 802.xx Networks

This chapter focuses on security issues related to the chosen IEEE 802.xx technologies. Poor configurations and encryption are key sections to the deployment of a vulnerable wireless network. As a result, strong encryption has to be performed to secure a wireless network and avoid attacks such as packet sniffing. In Section 4.1 below, the research provides a detailed discussion of IEEE 802.11 security (WiFi) and the possible mechanisms for controlling wireless access. Lastly, it explains WiMAX security issues and concludes by suggesting possible authentication methods which can be implemented in the SLL network.

4.1 IEEE 802.11 Security (WiFi)

Security is one of the key aspects that need to be considered when implementing WLANs. Several security solutions exist and can be implemented when deploying WLANs. These range from Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Virtual Private Network (VPN) to 802.11i (Vines, 2002). They vary in terms of security levels and each method has its own advantages and disadvantages that need to be fully understood before implementation (Vines, 2002). Furthermore, each method attempts to address issues of Confidentiality, Integrity and Authentication (CIA) (Karygiannis *et al.*, 2002). However, they introduce vulnerabilities in the network during this process and, therefore, their weaknesses need to be understood. Figure 4.1 below shows the evolution of the WLAN security, with the WEP being initiated in 1999.

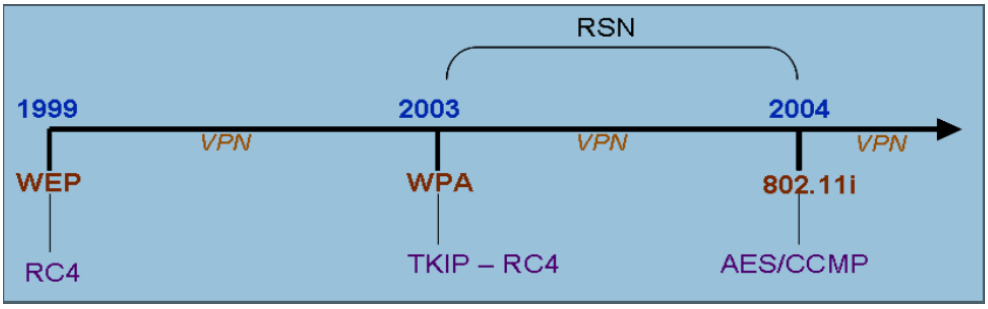


Figure 4.1: Time-line of the evolution of wireless security (Karygiannis et al., 2002).

In 2003, WiFi Alliance introduced the WPA to provide a temporary solution to wireless security through the use of an RC4 algorithm (Karygiannis *et al.*, 2002). However, some institutions were still using VPNs as an alternative (Stanton, 2005). Finally, in June 2004, a very strong encryption scheme called 802.11i was introduced. Again, the Robust Security Network (RSN) used for authentication purposes was introduced as well (Karygiannis *et al.*, 2002). In Section 4.1.1 below, the study discusses the security technologies, exposing their advantages and disadvantages.

4.1.1 Wired Equivalent Privacy (WEP)

This is commonly known as WEP. This kind of technology is widely deployed even though it was ratified in 1999 (Scholz, 2002). It failed to provide authentication, integrity and confidentiality because of its vulnerabilities (Vines, 2002). It uses two methods for authentication: mainly the open system and the shared key authentication. According to Vines (2002), in shared key authentication, WEP generates encryption keys. These encryption keys are used by both the source and destination to encrypt and decrypt frames sent. WEP can operate at different levels; for example 40 bit, 56 bit, 126 bit and the 256 bit. WEP can provide automatic encryption since it is possible for the WEP keys to be assigned to any client, on connection, automatically (Scholz, 2002). Figure 4.2 below shows WEP Encryption.

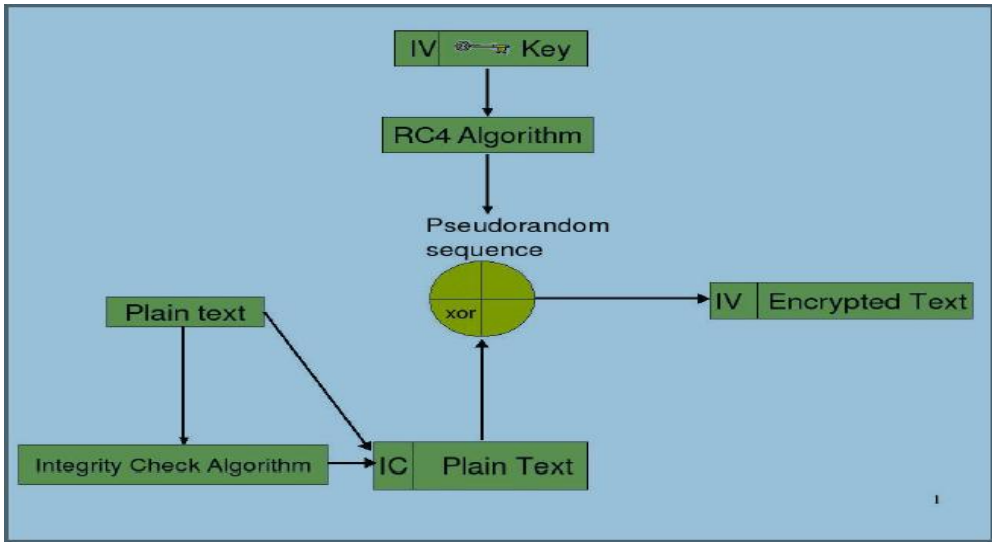


Figure 4.2: WEP encryption adapted from Karygiannis et al.(2002).

When WEP is implemented in a network and a client tries to connect with an invalid key or without a key, the client is denied access to the network until valid keys are used (Matsunaga *et al.,* 2003). However, the keys used in WEP can easily be calculated and acquired with the aid of specialized software. Having calculated the key, one is able to access the network even though he/she is not authorized to (Matsunaga *et al.,* 2003). This presents some loopholes and vulnerabilities within the WEP technology which makes it unsuitable for implementation in scenarios where sensitive data is being handled (Matsunaga *et al.,* 2003).

4.1.2 WiFi Protected Access (WPA)

Since WEP has numerous loopholes, WiFi Alliance and IEEE introduced WPA in 2003 to act as a temporary solution to the weak security offered by WEP (Vines, 2002). This kind of technology has to be implemented in mobile devices and WLAN infrastructure which supports 802.1x EAPOL. WPA supports authentication for enterprise and home users. It uses the Remote Authentication Dial-In User Service (RADIUS) and Extensible Authentication Protocol (EAP) for an enterprise environment; this makes use of an 802.1x server. However, in the case of home usage, pass-phrases, or passwords, are manually entered onto all devices and a Pre Shared Key (PSK) is used in place of a RADIUS server (Scholz, 2002).

In WPA, the Temporal Key Integrity Protocol (TKIP) uses the dynamic key allocation protocol for each packet (Matsunaga *et al.,* 2003). The TKIP scrambles the keys and uses a larger 48 bit key IV, which takes a long time to duplicate. The TKIP is based on the original shared key and proper storage or disposal of the original key must be done to boost security. In an enterprise environment, a pair wise key for a specific session is created by the authentication server once a client has been authenticated. For integrity purposes, a message is discarded if it has been tampered with. This is done through the use of the receiver and transmitter which compare it to detect a tampered packet (Matsunaga *et al.,* 2003). A strong mathematical function is used by the supplicant and authenticator to calculate the message integrity check.

Again, the supplicant and authenticator are authenticated to each other through the EAP method in order to prevent the client from connecting to rogue access points in the network (Scholz, 2002). However, denial of service attacks are possible in WPA because EAP-Start, Logoff and

failure messages used by 802.1x are not protected and can thus easily forge messages (Stanley *et al.*, 2005). Also, the option of using a shared key presents a loophole since this key is open and can be used in the entire network. A network tool called coWPAtty can be used to comprise the network protected using WPA and gain access (Andrew *et al.*, 2004).

4.1.3 Virtual Private Networks

This security technology was not initially designed as wireless security but to offer security to mobile users connecting to an intranet over a public external network (Stanton, 2005). Widely used VPN technologies include Secure Socket Layer (SSL) and IP Security (IPSec) (Stanton, 2005). In order to use IPSec, all wireless clients have to acquire the client software installed in them first. This allows them to get connected to the company's private network (Stanton, 2005). If one intends to connect two private networks over the Internet, then IPSec offers the best solution. To use SSL, an application has to be HTTP enabled since this technology operates at the Application Layer (Stanton, 2005). SSL becomes the best solution when one wants to connect to a private network remotely.

One of the major drawbacks of VPNs is that layer two, where wireless networks broadcast, is unencrypted (Scholz, 2002). This is due to the fact that VPN encrypts data traffic at layer three. Again, VPNs are not interoperable and can reduce the throughput of a network by 15% (Stanton, 2005). Reduction in throughput is caused by strong encryption, tunneling and packet overhead (Scholz, 2002).

4.1.4 Robust Security Network

This security architecture was developed by IEEE and it primarily negotiates algorithms that will be used to communicate between clients and access points (AP). The components of the robust security network are shown in Figure 4.3 below.

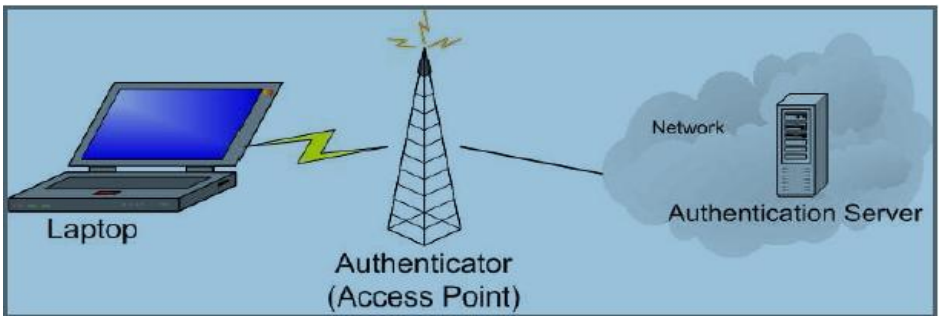


Figure 4.3: RSN components.

This method classifies the three elements as follows and it is shown in Figure 4.3 above (Vines, 2002):

- ***Supplicant*** – This is a client intending to get connected to the network.
- ***Authentication Server*** – This can be a server; for example, a RADIUS server used to authenticate clients.
- ***Authenticator*** – This is an intermediate access point between the client and the authentication server which basically relays messages between the two.

The above entities of RSN use the EAP to communicate during authentication (Stanley *et al.*, 2005). The supplicant and the authenticator have to agree upon security parameters before authentication can occur (Stanley *et al.*, 2005). Figure 4.4 below shows how the authentication process occurs.

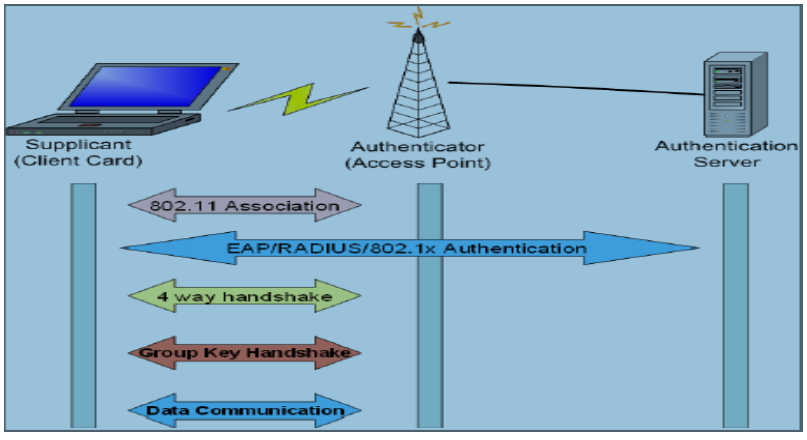


Figure 4.4: Authentication process.

A Master Session Key (MSK) is generated during authentication and, as a result, the client and authentication server become mutually authenticated. This allows the client to be authenticated and connected to the AP but it will not be granted access to the network (Scholz, 2002). This is due to the control port of the IEEE 802.1x which remains blocked (Stanley *et al.*, 2005). Having looked at how the authentication process occurs in RSN, we now look at another security solution that can be implemented in wireless networks. The next section of this chapter offers a brief explanation of IEEE 802.11i security technology.

4.1.5 IEEE 802.11i

This security mechanism was developed in 2004 (Scholz, 2002). It is similar to WPA but has been improved in terms of security. Before authentication, the supplicant and the authenticator agree on certain parameters that will be used in the authentication process. This stage is insecure and it is called the association (Scholz, 2002). During the authentication stage, a four way handshake is performed for key management. The supplicant, authenticator, and the authentication server use the EAP over LAN (EAPOL) key frames for the exchange of information between themselves (Stanley *et al.*, 2005). After this process, a secure communication is established. However, CCMP and TKIP are used by this mechanism to establish the data confidentiality protocol.

IEEE 802.11i has its vulnerabilities just like any other wireless security mechanism. It usually experiences Denial of Service (DoS) attacks, where an attacker forges the De-authentication or Disassociation messages (Vines, 2002). These, in turn, will cast a client away from a WLAN. Another possible attack is the Man in the Middle Attack. However, as an increase in the security level of this method, both the supplicant and the authenticator need to verify and check if the incoming messages are from the correct source (Vines, 2002).

4.2 IEEE 802.16 Security (WiMAX)

As seen in Section 4.1, security is critical when deploying WLANs which applies to IEEE 802.16 standards. WiMAX is an example of the IEEE 802.16 standard and seeks to provide CIA (Hasan, 2006). The fixed WiMAX uses Data Encryption Standard (DES) algorithm with a 56 bit

key. However, DES can be cracked easily (Hasan, 2006). The recently introduced 802.16e standard now uses the Advanced Encryption Standard Counter with CBC-MAC (AES-CCM) encryption algorithm which is more secure than the DES (Hasan, 2006). This standard uses CBC-MAC for integrity purposes and X.509 certificates for authentication.

Like any other security mechanism, this mechanism displays some vulnerability. The subscriber unit can be susceptible to spoofing or replay attacks because this method cannot provide mutual authentication between a subscriber and the Base Station (BS) (Hasan, 2006). Again, the 802.16 can be susceptible to jamming or scrambling which are both physical layer attacks. Attacks such as the Man in the Middle can also be a threat since the MAC headers are not encrypted (Scholz, 2002). This allows for the management frames to be sent exposed. Finally, the introduction of the 802.16e curbs the security flaws which were previously experienced by the older version of 802.16.

4.3 Possible Authentication Solutions Which Can Be Implemented

Various methods are being devised to control wireless authentication and use. As a result, these hardware or software solutions are now widely used in WLANs. They can either be implemented in access points or deployed in servers as captive portals. In Section 4.3.1 below, the study briefly describes the possible methods that can be used as control and authentication measures in WLANs.

4.3.1 MAC Address Filtering and Device List Authentication

MAC address filtering is a low level and small scale security mechanism which uses MAC address to authenticate users wishing to access network resources in WLANs (Scholz, 2002). MAC address is used because of its uniqueness of devices in the network; this method avoids easy cracking (Scholz, 2002). This mechanism is mainly implemented in WiFi networks. As for WiMAX networks, the Device List Authentication is used (Hasan, 2006). This mechanism allows the Subscriber Unit (SU) to send data across the network after it has been assigned to the Micro Base Station. MAC address filtering is more secure than WEP because it requires some administrative rights and high powered devices to compromise it (Vines, 2002). As for the

Device List Authentication, the quick Time Division Multiplexing between a Micro Base Station and the SS requires an attacker to be in possession of a sophisticated device to compromise it (Vines, 2002). However, both MAC address filtering and Device list authentication are prone to the Denial of Service (DoS), masquerading, data modification and impersonation attacks. Below, the research elaborates on the method used and followed, according to Vines (2002), so as to compromise the MAC address filtering and bypass this security precaution in a lab environment.

Aircrack-ng was used for sniffing the traffic and MacMakeUp to change the MAC address which are all FOSS. The process started by sniffing packets around by monitoring all channels on interface *eth1* and logging them to a file with the Prefix after *–w*. This was done using the command below:

airodump-ng -c 0 -w Prefix eth1
The following information appeared on the screen and was logged and sent to a file.

BSSID, First time seen, Last time seen, Channel, Speed, Privacy, Power, # beacons, # data, LAN IP, ESSID
*00:**: XD: 24:**:**, 2010-02-13 10:11:02, 2010-02-13 10:17:20, 7, 55, OPN, 14, 225, 63, 192.168. 5. 2, AIRTIES*
Station MAC, First time seen, Last time seen, Power, # packets, BSSID, ESSID
*00:**:Y3: XD: **:**, 2010-02-13 10:11:02, 2010-02-13 10:17:20, 17, 89, 00:**: XD: 24:**:**, AIRTIES*

From this information, it was deduced that *00:**:Y3: XD: **:** is the client connecting to the network and has been added to the Allow list. The MacMakeUp was opened and an interface selected before entering the above MAC address without the colons. This cycles the interface and the next time we were able to connect to the network without a problem. According to this tutorial, by Vines (2002), it was realized that MAC filtering is not reliable and can be bypassed at any time.

4.3.2 EAP Mechanism

For security purposes, EAP is considered to be a better solution than WEP (Stanley *et al.*, 2005). However, it is prone to attacks such as Man in the Middle (MIM) and dictionary attacks (Stanley *et al.,* 2005). These attacks can compromise the security mechanism even though mutual authentication and replay attack resistance have been provided by EAP-LEAP. MIM attack still becomes a problem when implementing EAP-TTLS and EAP-PEAP as security solutions within WLAN (Stanley *et al.,* 2005).

However, there are EAP methods which are common and usually used, just like EAP-MD5 (Stanley *et al.,* 2005). This method provides low-level security, although it is characterized by many loopholes which disqualify it from being recognized as a standard authentication mechanism. One of its shortfalls is the ability to be cracked because of the weak shared key and the one way hash algorithm (Stanley *et al.,* 2005). During MIM attacks, an attacker can falsely pose as a legitimate access point (rogue access point). As a result, EAP-LEAP is often a better option to consider because it offers mutual authentication and dynamic WEP keys (Stanley *et al.,* 2005).

4.3.3 IPUnplugged Internet Access Control

This method, or mechanism, acts as a platform for supporting many authentication methods whilst providing a flexible architecture for wireless Internet access (Wang *et al.*, 2005). It is usually called the IPUnplugged IAC; IAC is the abbreviation for Internet Access Control. IAC operates with a roaming gateway which can be deployed locally or distributed all over the nodes so that it can be accessed over the Internet (Wang *et al.,* 2005). This roaming gateway server performs the Authentication, Authorization and Accounting (AAA) just as a RADIUS server does (Zhang *et al.*, 2002). If a user tries to log in, he/she is directed to the roaming server. The roaming server acts as a captive portal (Wang *et al.,* 2005). However, a client requires only a web browser such as Internet Explorer or Mozilla Firefox to supply his credentials. There are no extra requirements for the client. Various authentication methods can be implemented with IAC, such as Credit Card billing, Mobile IP authentication and the famous username / password method (Wang *et al.,* 2005).

4.3.4 NoCatAuth Gateway and Authentication Server

This software is often categorized under the captive portals and is mainly used by community wireless networks. NoCatAuth is open source software and can be freely obtained from the Internet (Wang *et al.,* 2005). It uses DHCP to assign incoming users with an IP address and then restricts network access until the user has been granted permission (Wang *et al.,* 2005). Users tend to vary and can be administrator, guest or paying customer. NoCatAuth functions just like any other captive portal by redirecting traffic. When a user attempts to open a web page before being validated, he/she is rerouted to the portal login page. This is done through rewriting the destination of all port 80 traffic in the firewall (Wang *et al.*, 2005).

However, the majority of APs control access to a network by use of WEP or MAC address filtering and these are configured differently (Scholz, 2002). NoCatAuth uses IPTables which is a firewall package included with Linux (Scholz, 2002). This method controls network access dynamically. NoCatAuth comprises of the gateway and authentication server. In gateway mode, the firewall rules are rewritten as the users connect and disconnect. Since no other firewall will be in place, this method is the better of the two. In authentication mode, NoCatAuth uses the RADIUS, file or the SQL database table to control the storage and retrieval of user password and accounts (Wang *et al.*, 2005).

When one is using NoCatAuth, it is easy for one to block IP ports and domains when necessary. This offers good IP port security and secures network resources from unauthorized connections through various ports and domains (Wang *et al.,* 2005). Additionally, NoCatAuth allows for each AP in the network to use its own gateway (Wang *et al.,* 2005). As a result, there will be many gateways and one authentication server in the network. The authentication server does not necessarily have to be located on the same network but can be an Internet source. Both NoCatAuth components can be installed in one machine although it is not recommended (Wang *et al.,* 2005). If one is using different machines for the gateway and the authentication server it is advisable, easier and secure for multiple gateways to use a single authentication server (Vines, 2002). Section 4.3.5 below describes another captive portal widely used in wireless networks. This captive portal is called the ChilliSpot access controller.

4.3.5 ChilliSpot as a Wireless Access Controller

Recently, access to wireless networks was most frequently controlled through the use of captive portals. ChilliSpot is another example of a captive portal which is commonly used as an access controller (Lee *et al.*, 2008). It supports a web-based login and has a free RADIUS server which handles Authentication, Authorization and Accounting (AAA) (Zhang *et al.*, 2002). ChilliSpot uses the web server which, in turn, uses the hashed challenge/response mechanism over a SSL (Lee *et al.*, 2008).

This SSL makes it difficult for attacks such as a dictionary attack to invade this ChilliSpot mechanism. Furthermore, ChilliSpot is capable of creating a VPN, which is an IP tunnel (Vines, 2002). This IP tunnel provides better security because all usernames and passwords are sent through this channel after being encrypted using the SSL. Figure 4.5 below shows how ChilliSpot operates.

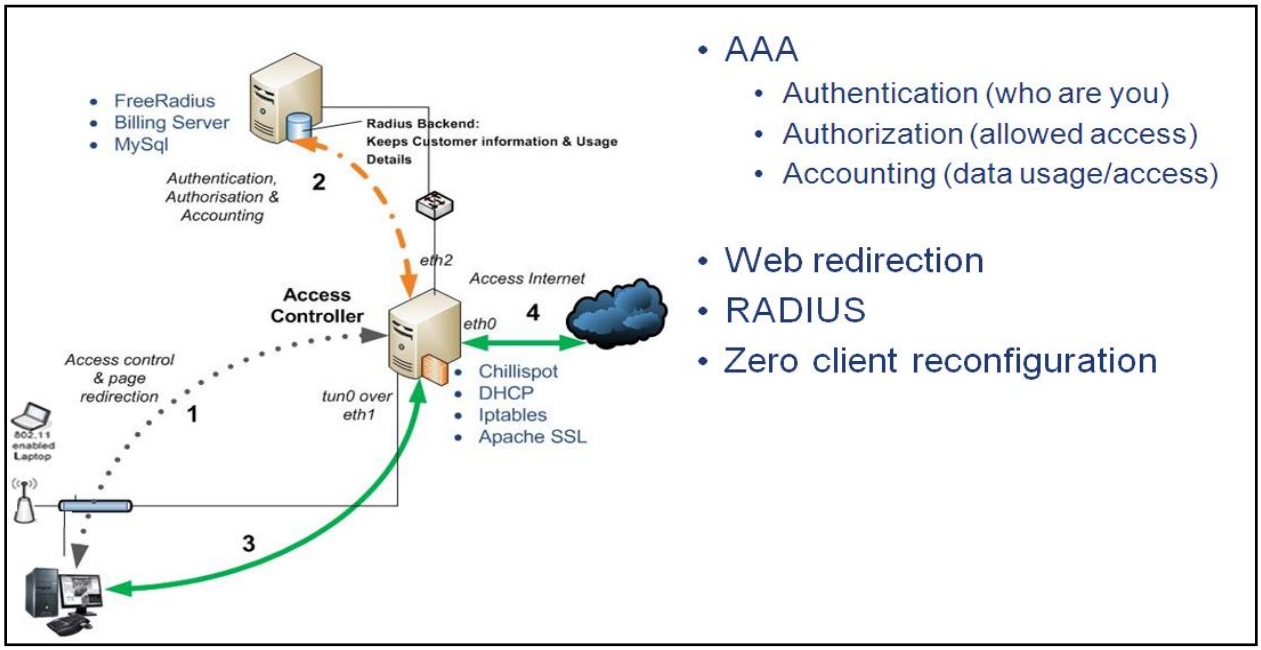


Figure 4.5: ChilliSpot as an access controller (Vines, 2002).

ChilliSpot is considered to be one of the best captive portals that can be deployed in wireless networks in marginalized areas (Vines, 2002). The ChilliSpot has many advantages and is

suitable for deployment in the SLL network. As a result, it was opted it to be deployed in the SLL network. In Section 4.3.6 below the security mechanism which can be deployed in the WiMAX backbone is described, since the SLL will be using both WiFi and WiMAX technologies to achieve connectivity.

4.3.6 Point-to-Point Protocol over Ethernet running (PPPoE)

This method can be used to authenticate and encrypt wireless traffic and is mainly used by Internet Service Providers (ISPs) (Scholz, 2002). It can offer a safe security mechanism even though it also requires extensive knowledge or expertise to configure it. PPPoE Clients are authenticated through the use of a remote Access Concentrator (AC) on a third party PPPoE Server (Mishra *et al.*, 2002). PPPoE Clients' credentials will be communicated via a MPPE encrypted tunnel after authentication has been created (Hasan, 2006). Basically, the PPPoE interface is created on a physical Ethernet device. It mainly transports packets between two peers and builds PPP sessions and encapsulates PPP packets over an Ethernet device. Multi-point relationships are not supported by this security mechanism.

However, MPPE is prone to DoS and dictionary attacks (Hasan, 2006). As a result, the Internet Protocol Security (IPSec) could be an option since it offers better security in comparison to PPPoE. IPSec uses the Encapsulation Security Protocol (ESP) and the Authentication Header (AH) protocols to ensure secure communication between hosts (Hasan, 2006). Again, IPSec uses the transport and tunnel modes for encryption and tunneling is the more secure between the two. Tunneling encrypts both the header and the payload (Hasan, 2006).

4.4 Summary

This chapter offered a discussion of various security mechanisms and methods which can be deployed in the SLL network. Various security mechanisms for both WiFi and WiMAX technologies were focused on since they are the technologies chosen for deployment. Security mechanisms that are viable with WiFi were initially discussed; these range from WEP, WPA, EAP and Captive Portal mechanisms. Thereafter, IEEE 802.16 security mechanisms were discussed. This was done to determine the best possible solution to be deployed on the WiMAX

backbone of the SLL network. It was noted that ChilliSpot presented the best solution and would be ideal for deploying in the WiFi access technology. The ChilliSpot is used as an access controller in this study and PPPoE configured on the WiMAX backbone to provide security. In Chapter Five, the actual implementation of the merged WiFi/ WiMAX SLL network is presented. The detailed installations and configurations of WiFi and WiMAX are also provided.

5 Chapter Five: WiFi/WiMAX Telecommunications Network Deployments

This Chapter begins by discussing the research site. The existing SLL network structure, which was initially deployed in 2006 when the project started, is then elaborated on. The SLL is basically a research platform that leverages the synergies of the multi-stakeholder, multi-disciplinary, user-driven innovation environment. In Section 5.3, the implementation of WiFi/WiMAX Digital Access Nodes (DAN) in the SLL network is elaborated on. This is followed by a brief explanation of the details of the implementation of a wireless access controller which acts as an authentication solution in the WiFi/WiMAX SLL network. In Section 5.6, an overview of the current state of the SLL network is presented.

5.1 The Research Context

The University of Fort Hare, together with Rhodes University is undertaking an Information and Communication for Development (ICT4D) intervention. This intervention is called the Siyakhula Living Lab and is located in Dwesa, a rural area in the Eastern Cape Province of South Africa. An overview of the Dwesa rural area is provided in the next section.

5.1.1 An Overview of the Community

Dwesa is a rural community isolated from the global telecommunication service by poor cellular network coverage and inaccessibility (Timmermans, 2004). It is located on the Wild Coast of the former homeland of Transkei, in the Eastern Cape Province of South Africa (Mandioma et al., 2006; Palmer *et al*., 2002). The community is under the Mbashe Municipality which belongs to the Amatole district; their main office is based in East London.

The population density is very low in the Eastern Cape Province and most of the settlements are dispersed (Timmermans, 2004). The current Dwesa population is approximately 15000 people and its population density is 96 people per square kilometer, with a land area of about 42 square kilometers. The majority of the inhabitants are poor people who rely on donations and grants

from the government, although they are able to work for themselves, in-order to get extra money. The inhabitants of Dwesa are typically subsistence farmers who depend primarily on farming the land for their livelihoods (Palmer *et al*., 2002).

The Dwesa terrain is hilly, with numerous rivers and streams (Timmermans, 2004). Such a terrain makes it difficult for any telecommunications company to deploy a network in the area. The Dwesa region also has a coastal nature reserve; an attraction for South African tourists who visit almost exclusively during school holidays. The nature reserve is a channel for the promotion of tourism, although government social welfare grants seem to be the main source of income for the local community (Siyakhula project, 2007). However, the area is characterized by extensive infrastructural constraints. Section 5.1.2 below elaborates on the constraints faced by the Dwesa community.

5.1.2 Infrastructural Constraints

Dwesa is still underdeveloped in terms of infrastructure and experiences vast constraints. Firstly, the road network consists mainly of gravel or earth roads which are still underdeveloped. From this area, the nearest possible town is Willowvale which is about 52km away (Timmermans, 2004). Until recently, the area lacked basic infrastructure such as electricity in homes. The schools, a few homesteads and the clinic were the only places with electricity installed although Eskom has recently embarked on a rural electrification scheme. According to Ndlovu *et al.* (2010c), this has a direct influence on the availability and utilization of technology in the community. However, the majority of community members have cell phones (Ndlovu *et al.*, 2010c). This is shown in the results obtained from a baseline study undertaken in 2008 to identify the actual figures and numbers of people with access to a cell phone. Furthermore, a working business model has been adopted by the schools and shops which have electricity (Siyakhula project, 2007). This working business model allows for an arrangement to be made wherein people bring their cell phones to be charged for a small fee. Previous attempts by both the government and NGOs to install solar panels in the schools, in order to supply electricity, have been unsuccessful. As a result, most of these solar panels are not utilized anymore due to theft and vandalism. This has lead to a very limited telecommunication infrastructure (Siyakhula project, 2007). The community is characterized by very few telephone lines and the few public

pay phones that are installed in the community have been vandalized and damaged. The country's leading mobile operators Vodacom and MTN have provided the availability of a GSM network in the community. However, even though GPRS and EDGE technologies are also present in the area, their connectivity is sometimes erratic and not always available (Ndlovu *et al.*, 2010c). There also exists a need to equip this rural community with ICT infrastructure and the deployment of the e-commerce platform and communication platform as well (Palmer *et al.*, 2002; Siyakhula project, 2007). This is an ideal location for conducting this research and the following section focuses on the SLL network which was initially deployed when the project started in 2006.

5.2 The Traditional SLL Network

The SLL project was pioneered in 2006 and there were only four digital access nodes (DANs) deployed at that time. The network topology of the SLL is illustrated in Figure 5.1 below.

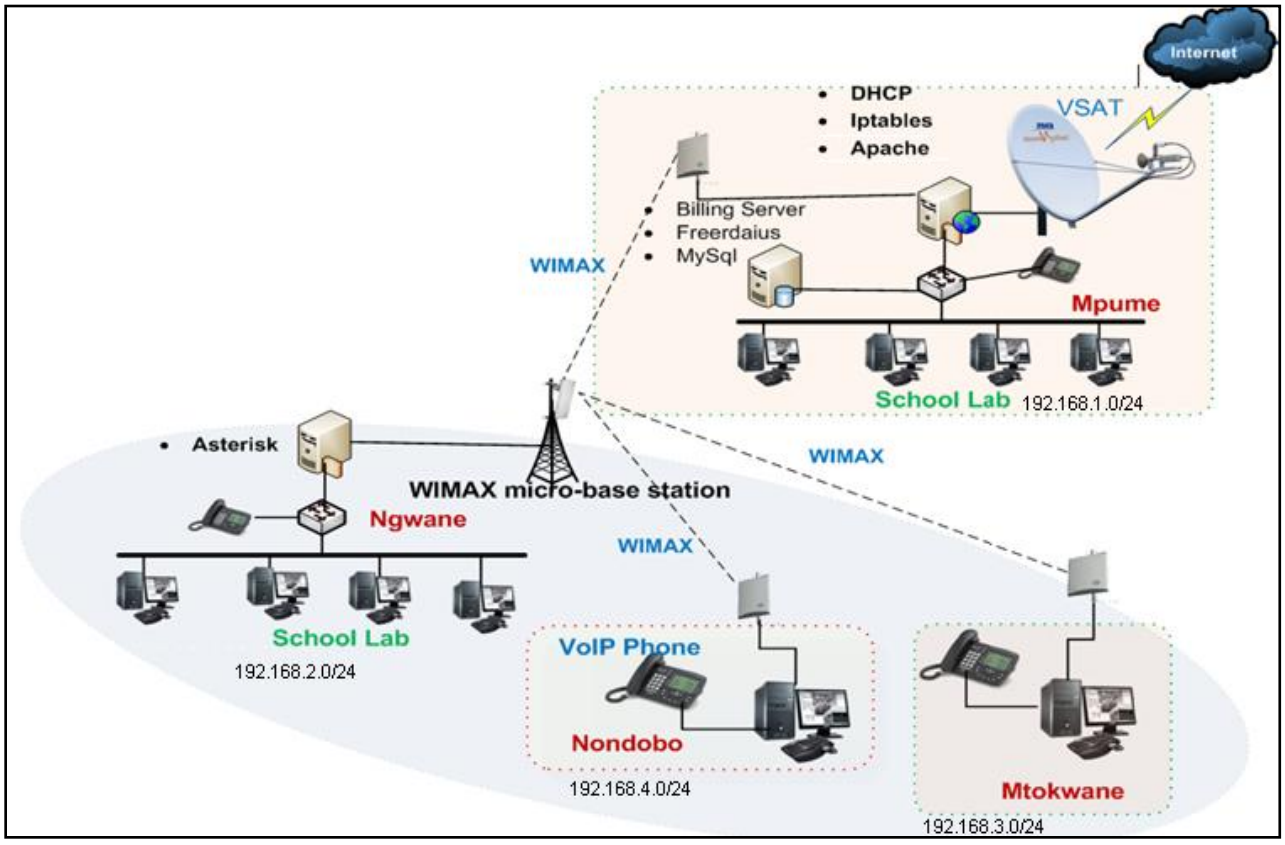


Figure 5.1: Traditional SLL network topology.

Figure 5.1 depicts the SLL telecommunication infrastructure that was initially deployed when the project started. There were originally 4 schools connected. The following section explains the network infrastructure and how the network was initially deployed as shown in Figure 5.1:

- ***VSAT*** **–** One of the schools, Mpume Junior Secondary School was the site where the Telkom VSAT was deployed. The site was chosen for its good security to house the VSAT and for easy accessibility by network administrators. VSAT offers backhaul Internet connectivity to the SLL network.
- ***Access Concentrator*** **-** This was installed at Mpume Junior Secondary School (MJSS) together with the VSAT. The computer used as an AC has an Intel Pentium III processor running a stable FreeBSD 6.2 operating system. It is connected to the router at Mpume and it creates communication tunnels on the WiMAX. The WiMAX SU located at MJSS is linked to the indoor data module connected to the router. As a result, signals reach the WiMAX system through this link. At MJSS there is a router with three network cards. The first one is for connecting the VSAT. The second one binds an IP address on the local area network at MJSS, which is 192.168.1.0/24. Whereas, the third one connects to the backbone with the AC and binds the IP address 192.168.0.1.
- ***Micro Base Station*** **-** According to Alvarion, (2005), the BreezeMAX base station (BS) equipment is made available in two variants: chassis configuration and a micro base station. The micro base station used in this research has the functionality required to communicate with the SU and connect to the backbone (VSAT connection at MJSS) of the Internet Service Provider (ISP). It has additional features like traffic classification and connection establishment, policy based data switching, service level agreement management and alarm management, more than BreezeMAX modular Base Station (Alvarion, 2005). The base station was deployed at Ngwane Junior Secondary School (NJSS) and it has a line of sight with the VSAT at MJSS. The base station has an outdoor AU-ODU unit and an omni-directional antenna which was mounted outside the building at NJSS. A tripod stand was used to mount the outdoor units with a clear LOS to remote access points. Figure 5.2 below shows a Micro Base Station unit which was housed in the lab together with a 24 port switch.

Figure 5.2: Micro base station indoor unit.

- ***Subscriber Units (SUs)*** **-** These have been installed in all the schools. The SUs were first added into the micro base station before being powered. This avoids the base station locking them out. WiMAX SUs connect to a router which is installed at each school. The router runs FreeBSD 6.1 with an Intel Pentium III processor. All the SUs are added to the network at the Base Station which is located at NJSS. The BS has an Omni-directional antenna of 13 dBbi, which provides the signal to the other subscriber units attached to the network. The IP addresses of the local area network for each school is given in Figure 5.1 above and more details are found in the SLL networking document provided in the appendices.
- ***Switch*** **-** A DLink switch was used to connect an AP and the wired network. The switch is designed to systematically eradicate traffic congestion.

The network was mainly established through the use of a networking document written by the following COE researchers: Ingrid Sieborger and Barry Irwin, but modified but Nkanyiso Ndlovu (refer to Appendix C). Section 5.3 below explains the installation and deployment of another WiMAX BreezeMAX 3500 System DAN in Nqabara High School.

5.3 Nqabara Digital Access Node (DAN) Integration and Implementation

Since this is an on-going project, propositions to further extend the network have always been there ever since the beginning of the project. The main objective is to eventually extend the SLL network segment to the Nkwalini community area about 25km from Ngwane DAN. The deployment of a DAN in Nqabara High School (NHS) was done in two stages. NHS is located

about 2.1km away from the base station. It was initially left out because of the shortage of the CPEs and access points. However, from the observations made during the field trips and the interviews conducted in the Nqabara area, the researchers realized the need to connect the school because a large number of community members were willing to partake in and benefit from the SLL network. The first stage included adding the SU to the base station at Ngwane Junior Secondary School (NJSS) whereas the second stage was the actual site installation of WiMAX SU at NHS. These stages are briefly explained below.

- **Stage 1**

Since the version of WiMAX, which is the BreezeMAX 3500 System, is managed at the micro base station; we started by first adding the subscriber units on the micro base station before moving on to deploy the access point at NHS. The system is managed at the base station for improved security reasons. The base station was connected through the management port using a laptop and a crossover cable. The aim of conducting this operation was to:

- Add the SU's MAC address to the base station database before deploying it. This procedure allows the SU to be permanently added to the micro base station.
- Enable a communication link between the SU and the base station by setting up a specific subscriber profile.

The moment the researchers completed adding the SUs to the micro base station, it was noticed that the signal strength was now 9/9, meaning that the base station and the SU were connected and ready to communicate.

- **Stage 2**

In Nqabara High School, an initial survey was conducted so as to determine the proper position where the SU was to be mounted. Afterwards, the equipment was assembled by following a user manual which came with the equipment. Appropriate attention was given and steps taken into account to ensure that the equipment was assembled properly. The school is approximately 2.1km away, in the line of sight of NJSS which hosts the micro base station. Hence, it was

convenient to find a suitable position that would be in the line of sight (LOS) of the base station. Finally, the SU was mounted outdoors on the wall which gave a 7/9 on the Link quality LEDs after the SU was switched on. This position has a partially blocked LOS. However, this was the best possible position since it did not give 9/9 on the Link quality LEDs indicating saturation of the signal which is not advisable according to the BreezeMAX system manual (Alvarion BreezeMAX 3500). A tripod stand was used to permanently mount the SU outdoors as shown in Figure 5.3 below which was taken during the site installation of the SU at NHS.

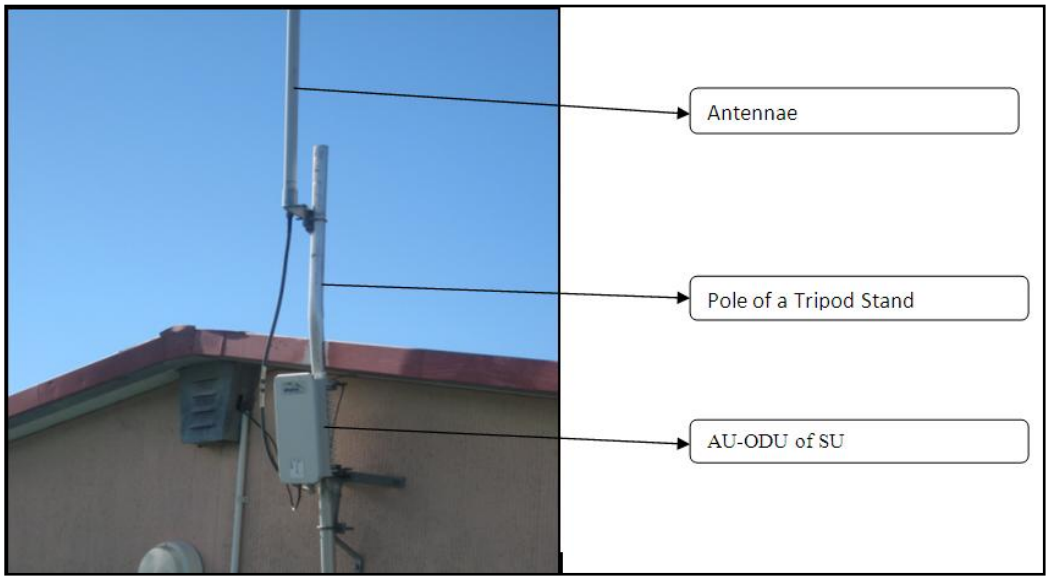


Figure 5.3: Site installation of SU at NHS.

PPPoE was configured on the WiMAX backbone to provide security. Each DAN has a PPPoE router installed which communicates with the PPPoE Access Concentrator at MJSS. The PPPoE Access Concentrator in turn uses the MPPE protocol to create permanent virtual tunnels which are used to authenticate and encrypt network traffic. PPPoE protocol offers high reliability and low cost in high speed Internet connections. Having successfully established a DAN in a school further away from the base than any other DANs, the performance evaluation of this DAN was vital. Section 5.4 below, elaborates on the implementation and deployment of WiFi hotspots around every DAN in the network.

5.4 Hotspot Implementation

WLAN presents unique characteristics and, as a result, good practices have to be taken into account when deploying and managing these wireless hotspots. WLAN life cycle together with these practices has to be followed. Good practices involve:

- ***Availability****:* This involves providing access to LAN resources wirelessly to clients. Consequently, availability means the user has access to the network resources 24/7. The user is given the highest priority when it comes to access to network resources. Therefore, it is of paramount importance, when one deploys a WLAN, that users always have access to the network resources.
- ***Reliability:*** Since various applications such as VoIP and video streaming will be utilizing the network, it is vital for the WLAN to offer reasonable throughput and consistent communication under determined circumstances so that these applications are always available. A WLAN with poor quality of service (QoS) is considered useless to users of the network.
- ***Security:*** When deploying a network, security is vital because the usage of network resources has to be controlled. However, security of a WLAN offers CIA.

Figure 5.4 below shows how a network administrator and a user value these practices. A user is seen to be more concerned with the availability, whereas the administrator seeks to provide secure access to information and network resources. During implementation, the security of the entire network was considered a priority. Focus was placed on providing a secure network while offering the availability of network resources to users as well.

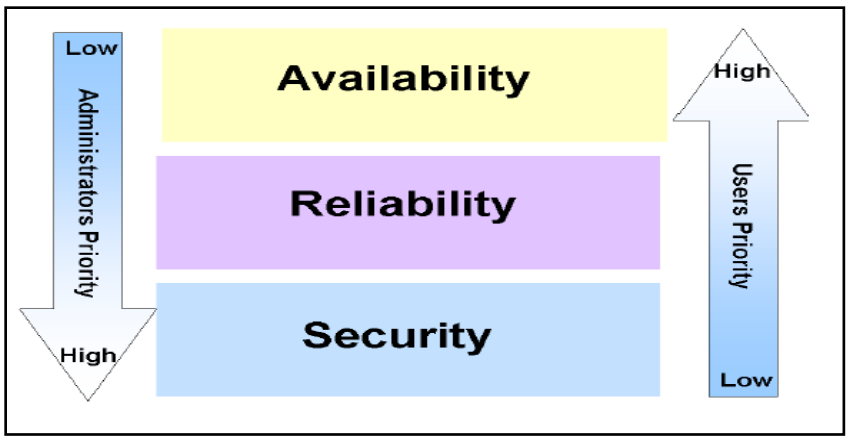


Figure 5.4: Best practices categories.

5.4.1 Preliminary Hotspot Planning

A WLAN life cycle was followed in deploying the hotspots. This stage involved the site survey, selection of equipment ranging from the types of antennas and the kind of access points to be used. In this research, DLink DWL-2100AP access points were used. Afterwards, performance evaluation tests were conducted before permanently deploying them in the SLL. The experiments and results of these tests are presented in Chapter Six of this study.

The study opted to use either channel 1, 6 or 11 within the frequency band since they offered the least amount of interference to one another. In planning, the environmental factors were considered since they affect signal strength as well as the method of assigning IP addresses to our network. After carefully planning the network, the access points were deployed in their respective positions so as to offer capillarity and ubiquitous Internet connectivity, starting at MJSS to the rest of the DANs.

5.4.2 Deployment of Hotspots

Based on the network plan and the knowledge acquired from the literature review, the actual physical deployment of access points and antennas was performed. Each hotspot was setup to provide Internet access and other network services wirelessly to the community surrounding each

DAN. The whole process started by configuring the AP at MJSS. Figure 5.5 below shows the hotspot setup at MJSS.

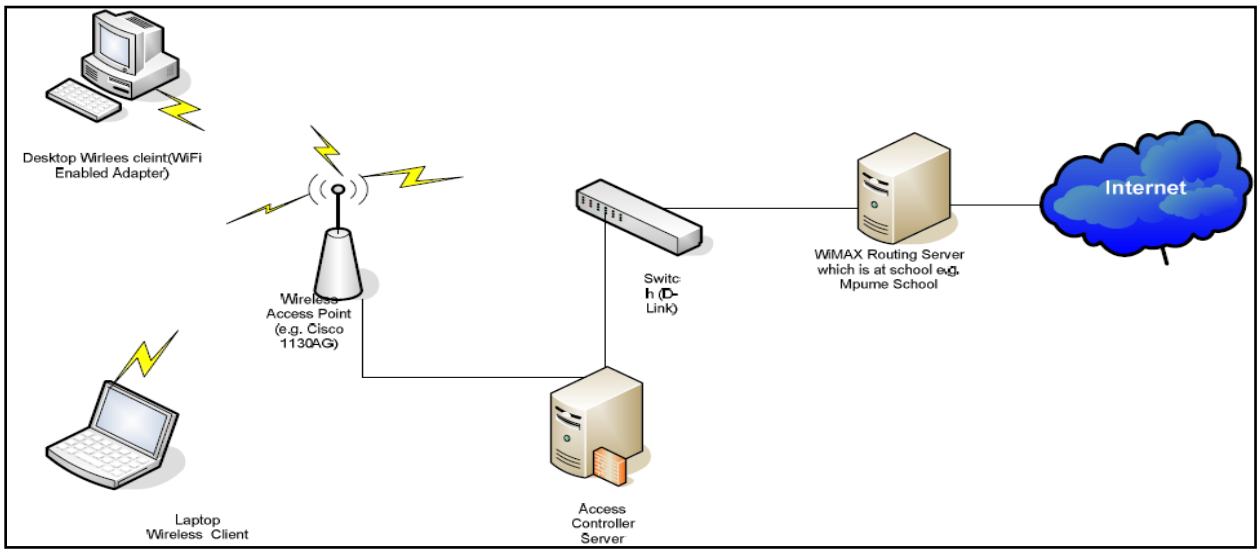


Figure 5.5: MJSS hotspot setup.

This particular hotspot configuration consisted of:

- WiMAX Routing Server with two network interface cards (NICs) running Linux. The server provides IP addressing through DHCP, firewall, masquerade and forwarding between the Internal and External NIC's through IPTables and lastly, top level domain name caching through the use of Berkeley Internet Name Daemon (BIND).
- 24 port switch and AP.
- The access controller server with ChilliSpot implemented has two NICs i.e. *eth0* and *eth1*. The first one connects to the AP and the other to the switch.

The access points used are all configurable from a web browser and the MJSS access point was given the SSID of Mpume. Both WEP and WPA were disabled since ChilliSpot access controller was to be implemented later on. In this research, the geographical location was set to South Africa and IPTables implemented through the use of a Bourne Again SHell (BASH) which was executed directly through the use of the following command: *Sh ./firewall.sh.* Hotspots were configured and implemented to all other DANs in the network following a similar procedure.

Afterwards, a security measure was devised and implemented to control the use of network resources. Section 5.4.3 below provides a brief explanation of how the access controller was implemented in the SLL network as an authentication solution.

5.4.3 Writing an Authentication Solution

An authentication server may provide a variety of services including Authentication, Authorization and Accounting (AAA). However, it is not as simple as expected because it can consist of certain applications which utilize other services. The authentication servers are best used for controlling the time or bandwidth clients are allowed on the network. Additionally, this applies to when a user unexpectedly disconnects or does not respond when he/she is out of coverage. This is difficult, or practically impossible, to handle when one uses firewall rules and web servers which only allow authorized clients to use the network resources.

Authentication solutions allow the users to consume network resources whilst they keep checking if they are still in the network. This is done through the addition of user details to a list which is constantly checked to find whether one is still logged in. If not, the rules are applied depending on the user details that are supplied and the user is automatically removed and requested to re-authenticate the next time he/she tries to access the network. As a result, ChilliSpot was chosen and implemented in the hotspots since it uses web-based management unlike NoCatAuth which only has a web-based status page making it difficult to administer.

5.5 Adding ChilliSpot Wireless Access Controller to the Hotspot

A tutorial on how to implement ChilliSpot was followed so as to setup a security measure that allows authorized users to be authenticated prior to accessing network resources wirelessly. ChilliSpot was chosen because of its advantages as discussed in Chapter Four. According to a "How to" posted by (Beltrame, 2007), a ChilliSpot has a number of requirements that should be considered when implementing it. Figure 5.6 below shows how the ChilliSpot was implemented in the SLL network.

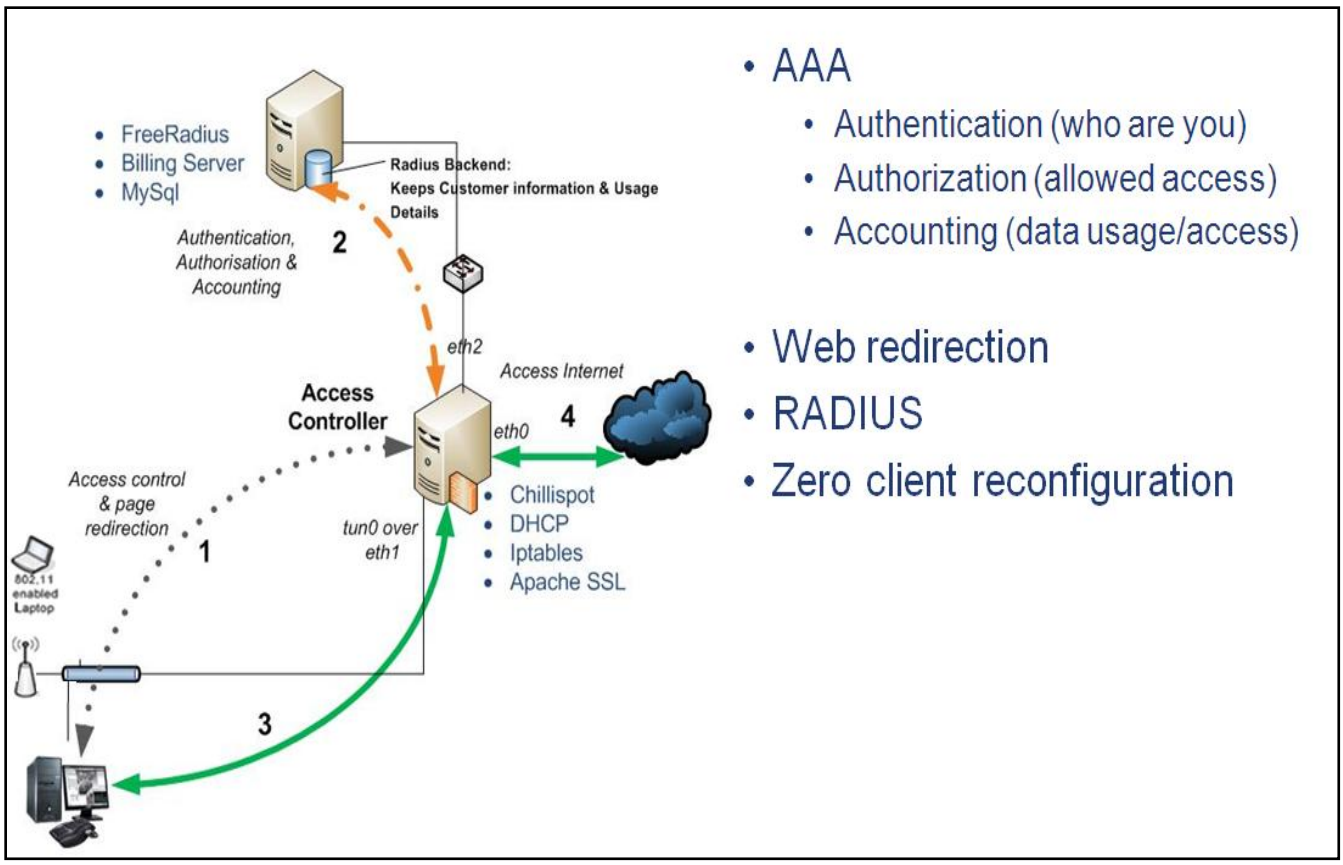


Figure 5.6: ChilliSpot implementation diagram.

The ChilliSpot implementation requirements and the basic configurations that we did in the software are given below:

- ***ChilliSpot Software requirements*** - The minimum software requirements needed to be installed are: ChilliSpot 1.0, Freeradius 1.0.x, Apache 2.x, and MySQL 5.x. (Beltrame, 2007) put an overall kernel requirement of the machine to be used to be not less than 2.6.x.

- ***Kernel Configurations*** – A kernel was manually configured to support TUN/TAP inside the kernel. A command which was used to compile the *tun* module was: *modprobe tun*

- ***Network and Firewall configurations*** – For security reasons we configured a firewall. The machine running the ChilliSpot had two network cards, *eth0* and *eth1*. *eth0* was

configured to connect to the Internet only and *eth1* connected to the switch or to the Access Point. The firewall which was used was called Firestarter. Since the *eth0* is connected to the internet, the *eth1* was set to be a local network connection interface. The DHCP option was not used.

- ***Freeradius Configurations*** – In configuring the Freeradius which is used for the authentication of wireless clients, three conf files were used and edited as follows: The */etc/raddb/clients.conf* to share the secret key with the ChilliSpot for authentication was modified to *:*

  client 127.0.0.1 {

  secret = abc123%d

  shortname = localhost }

  The second part was to make sure that the Freeradius server is able to utilize the MySQL and, as a result, we edited */etc/raddb/sql.conf*. The last part was to edit the */etc/raddb/radius.conf* file since it is the one used to authenticate wireless users.

- ***Apache Configurations*** – A web server Apache which supports SSL was configured to encrypt the username and password as the wireless client communicates with the server. The following editing was done to the SSL directive in the */etc/conf.d/apache*. A virtual host bound to http://192.168.1.73/ a content of *uamhomepage* variable in */etc/chilli.conf* file was setup. Lastly, the *uamsecret* in the hotspotlogin.cgi in the */etc/chilli.conf* was changed to my *ndlovuwireless*

- ***MySQL Configurations*** – MySQL database was configured to store the names and passwords for authorized users. An imported SQL schema was used, where a *radcheck* table was used with the following fields; Username Attribute and Value. The fields were created using the MySQL command line interface.

  > INSERT INTO radcheck (Username, Attribute, Value) VALUES ('matwayi', 'Password','k@izer';

- ***ChilliSpot Configurations*** - The machine was given an IP address of 127.0.0.1 with a secret *matwayi.* The secret used in Freeradius server */etc/clients.conf* file is the same used in the ChilliSpot since it was used during the authentication process. The DNS server had an IP address of dns1 192.168.1.73. The access point was then configured to use the *dhcpif eth1*. The Universal Access Method (UAM) section was configured as well and denies wireless clients and certain urls access to the network through the access point. For instance, to restrict wireless clients other resources like internet and files, a *uamserver* was used.

  uamserver https://192.168.1.73/cgi-bin/hotspotlogin.cgi 11

  The *uamserver* uses a SSL configured script which will display the login interface and manages the login. If a wireless client tries to browse for Internet and if not within the uamallowed list will be redirected to the login *uamhomepage*

  uamhomepage https://192.168.1.73/

  A shared secret between the ChilliSpot and the hotspotlogin.cgi was set to be *uamsecret ndlovuwireless.*

Figure 5.7 below shows how an access controller provides authentication to users who try to access the network services.

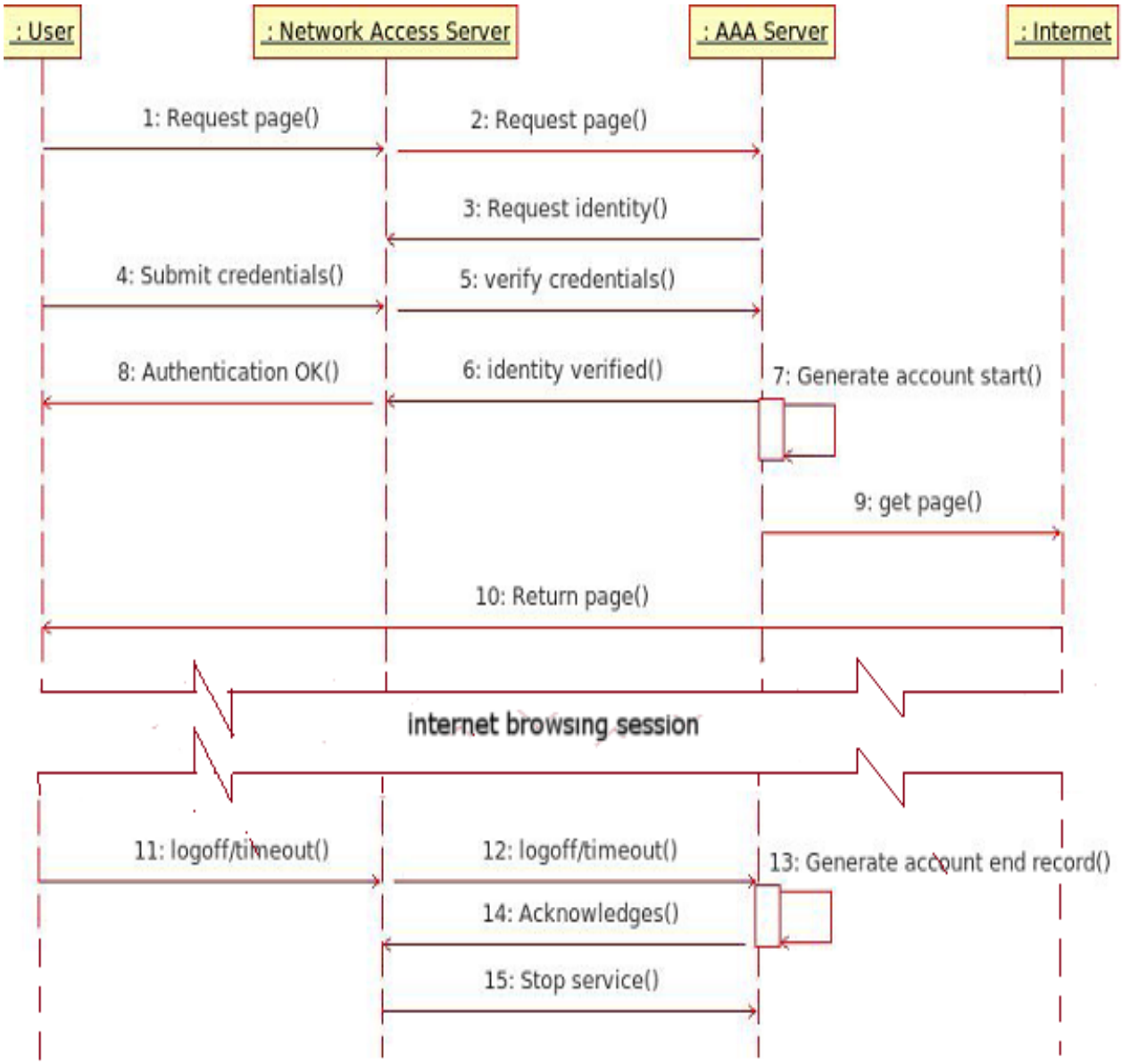


Figure 5.7: A user accesses the network sequence diagram (Ngwenya et al., 2009)

5.6 Overview of the Current Deployed SLL Network

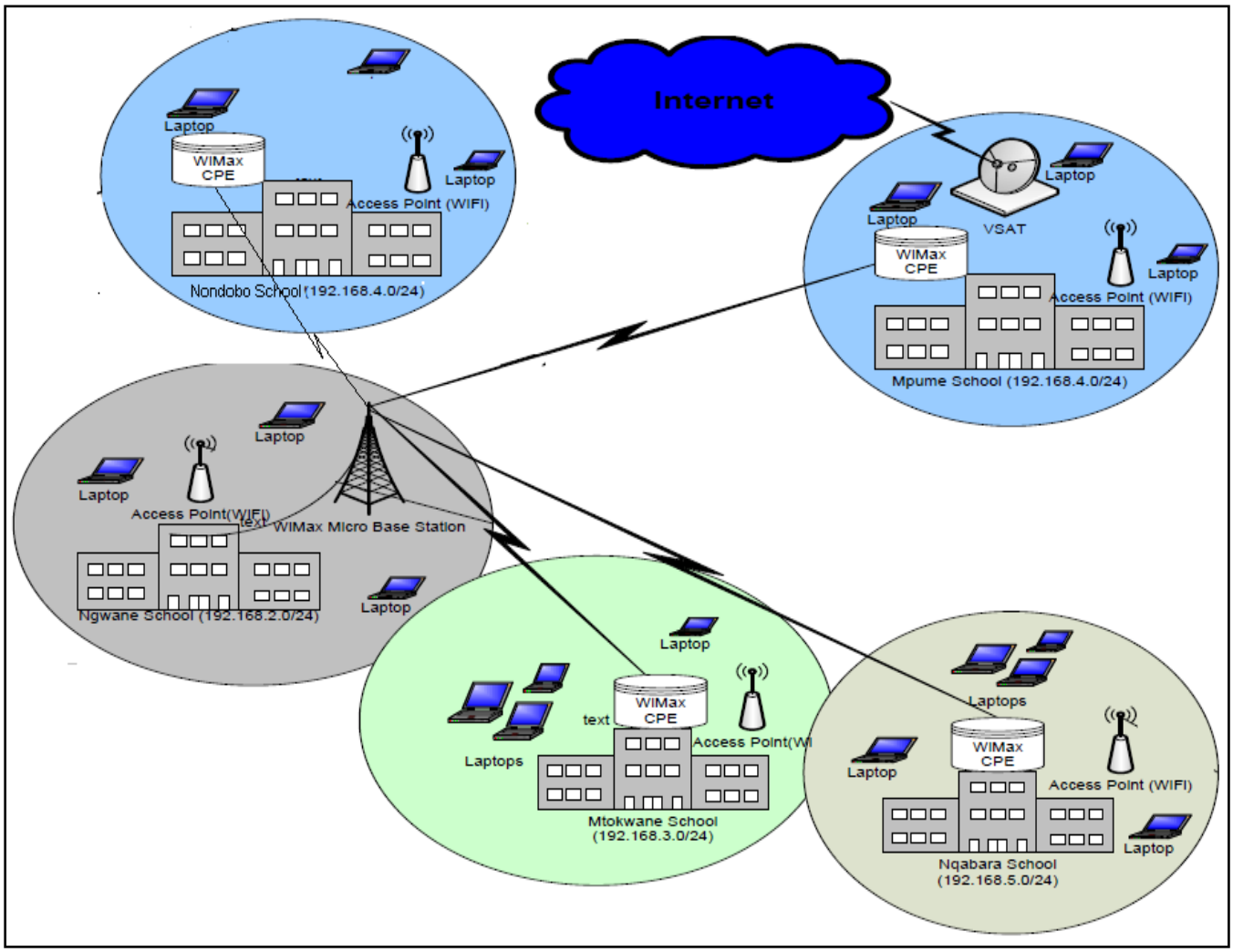


Figure 5.8: The current SLL network with hotspots around each DAN.

Figure 5.8 above shows the current overview of the SLL network after all the deployments have been successfully completed. As evident in Figure 5.8, we see that Nqabara DAN was successfully added to the SLL WiMAX backbone. Furthermore, it is evident that each DAN in the SLL network has WiFi hotspots. This means that users, and the community, can now access network resources wirelessly as long as they are within the coverage range of about 100m from each school in the network. The equipment and the deployed DANs were tested for functionality and various network performance evaluation experiments were conducted. In Chapter Six, the experiments and findings are presented.

5.7 Summary

This chapter described the research site and its various characteristics as well as its infrastructural constraints. It showed why Dwesa community area was chosen as an ideal site to conduct this research. Thereafter, an explanation of the traditional SLL telecommunication infrastructural network is given; this was followed by the actual physical deployments for both the WiMAX DAN at NHS and the deployment of WiFi hotspots around each DAN. The research highlighted that PPPoE was used as a security mechanism in the WiMAX backbone and how the ChilliSpot access controller was implemented so as to provide authentication in the WiFi hotspots. Finally, a general overview of how the network has changed and its current state after the successful completion of all deployments is provided. In Chapter Six, an explanation of the experiments and findings after various experiments were conducted is given. These range from network performance evaluation experiments to usability testing which is available in the appendices to network performance evaluation tests. A presentation on the social networking findings after the evaluation of the users' responses to the questionnaire is given as well. The questionnaire is also available in the appendices.

6 Chapter Six: Testing Strategies and Evaluation of Results

This chapter presents the experiments and results obtained after we conducted performance evaluation tests on the WiMAX DAN. It explains the performance evaluation tests and their outcomes. Thereafter, it presents the social findings and the cultural influences brought about by the introduction of this ICT4D initiative in the Dwesa area. The chapter concludes with a summary.

6.1 NHS WiMAX DAN Performance Evaluation Parameters Tested.

Since extra WiMAX DAN was added in the SLL network, it was necessary to conduct a network performance test on the WiMAX backbone and determine the effects of adding the NHS DAN to the SLL network. Acquiring this information, through experimental tests, is vital for future planning purposes especially when an extension of the network is necessary. Consequently, through the assessment of throughput, reliability and latency, the quality of a network, in terms of data transfer, can be determined and evaluated. Throughput of a network is the actual amount of data which can be transferred from one point to another in a network at a given time whereas latency consists primarily of path, queue and transmission delays. Throughput is measured in bits per second (bps). According to (Fruth *et al*, 2005), a simple equation, such as 6.1 below, can be used to calculate throughput.

$$P = \frac{s}{t} \qquad (6.1)$$

$$where: P = Throughput$$
$$s = File\,size$$
$$t = Transfer\,time$$

Throughput can be measured through two aspects which are the downloading and uploading times. File Transfer Protocol (FTP) applications can be used to conduct downloading times. However, performance experiments which determine the traffic overhead cost in terms of the downloading time and Round Trip Time (RTT) of the Internet Control Message Protocol (ICMP) packet for latency can be used. The average downloading time can be defined as the time the

initial requested file packet is sent until the time the last file packet is fully received by a client during the transmission and the following equation 6.2 is used to calculate downloading time (Mujinga, 2005). Network administrators are required to understand the concept of downloading time as it allows them to determine the negative impacts of downloading on network performance. This will allow them to manage the network properly and provide optimal performance to users.

$$Average\ Downloading\ Time = \frac{1}{n}\sum_{i=1}^{n} \left(t_{ri} - t_{si}\right) \tag{6.2}$$

Where :

$i = packet number$

$n = number\ of\ packets$

$t_{si} = the\ initial\ recorded\ time$

$t_{ri} = the\ last\ time\ recorded\ when\ the\ last\ file\ frame\ is\ received$

RTT is basically the time taken for a packet to be transferred from one machine to another and then back to the initial sending machine. To determine delay time using round trip time (RTT), we opted to use a ping test. A ping test enables us to calculate the minimum, maximum, average and standard deviation of the RTT of a machine which is pinged remotely and a script is run. Equation 6.3 is used to calculate RTT (Mujinga, 2005).

$$AverageRTT = \frac{1}{n}\sum_{i=1}^{n} t_i \tag{6.3}$$

Where:

$t_i = the\ return\ trip\ time\ trip\_i$

$n = the\ number\ of\ trips\ recorded$

From this, it was possible to determine and measure the round trip latency by looking at the values returned by the script as well as the reliability. Packet delivery reliability is deduced from the number of packets that are returned. Ping uses the ICMP packets to reach the target host and involves listening for ICMP replies to determine whether a particular host is reachable across an

IP Network (Foldoc, 2005). The results obtained were recorded to a CSV file and later exported to Excel for analysis and graphing.

6.1.1 Throughput Evaluation Performance Only

The initial experiments were conducted relative to the base station at NJSS. NHS is located 2.1km away from the base station at NJSS. From an omni-directional antenna at NHS to the base station at NJSS, there is a partially blocked LOS. The LOS is blocked by trees and other obstructions, including rugged terrain. The tests were conducted in two parts. Firstly, a signal level evaluation test was performed. This involved mounting the SU two meters above the ground and then determining the signal level strength. On letting the SU face the base station, a signal level of 7/9 on the Link quality LEDs was achieved. As a result, the SU was permanently mounted outside the building on top of the roof.

Afterwards, a ping test was performed. This involved running the Perl scripts on the FreeBSD routers. The script at NJSS, where the base station is located, sends 10 packets to the SU at NHS and then records the results. At NHS, another script was ran which does the file transfer by coping a file at NHS router and recording the average time taken to complete such a transfer. Both scripts were able to automate these processes since they were run in crontab. The file transfer script was allowed to execute every 10 minutes and then the other one every 5 minutes. The ping test gave an average round-trip time of 32.0859 ms and a transfer result of 916Kbps. Figure 6.1 below was generated using Wireshark during the month of August 2010.

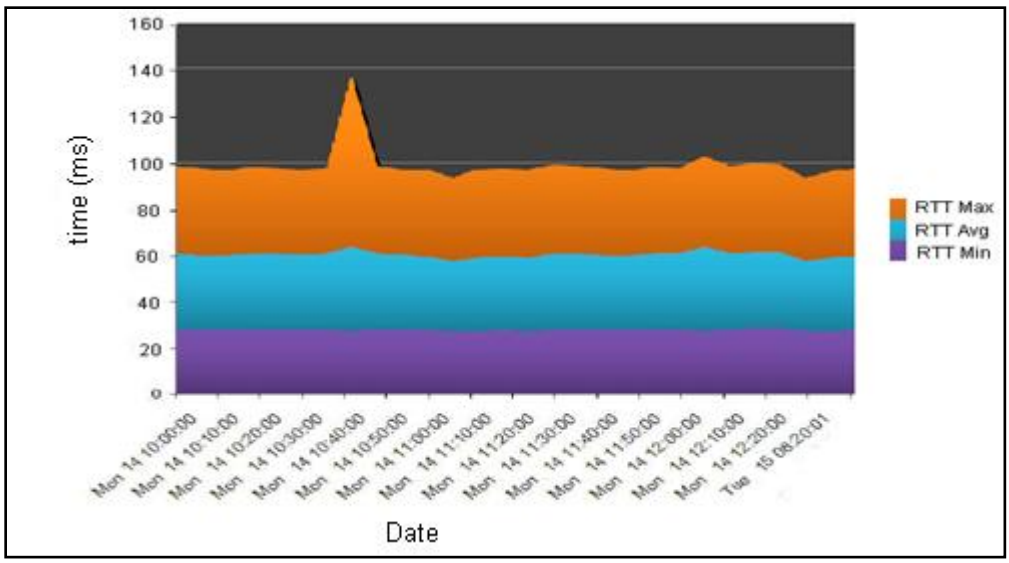


Figure 6.1: Ping test to the NHS SU from a computer connected to the base station at NJSS.

Minimum RTT: 27.23*m*sec;
Average RTT: 32.09 *m*sec;
Maximum RTT: 36.94 *m*sec;
Average Throughput: 3.63 *Mbps*.

Equations 6.1 and 6.3 above were used to compute the values for the minimum, average and maximum RTT respectively. The results shown in Figure 6.1 illustrate a throughput of 3.63Mbps with a distance of 2.1km apart. This low throughput might have been influenced by the long distance of separation between NHS DAN and the base station at NJSS. NHS DAN is the furthest of the access nodes from the base station in the network and may affect the throughput. Another factor which can be taken into account is the LOS, since it is partially blocked. This causes the interference of the signal from the base station to the access node at NHS and for that reason a lower throughput turnover. An outlier in Figure 6.1 shows that throughput varies with signal levels.

6.1.2 Throughput versus File Size Evaluation Performance

In Section 6.1.2, the research aimed to evaluate the WiMAX performance from NJSS to NHS in terms of latency and throughput of this DAN. As a result, latency and throughput were measured

from the NJSS network to the NHS network by creating files of different sizes. The sizes ranged from 1KB to 8MB and they we eleven in total. These files were then transferred in the network. Thereafter, equations 6.2 and 6.3 were used to compute the calculations and obtain the results. After analyzing our results the graphs were generated using the Wireshark network analyzer showing both latency and throughput for each file transferred. Figure 6.2 shows throughput measured in Mbps on the vertical axis plotted against file size measured in MB on the horizontal axis of the files ranging from 0.001MB to 8MB and they were eleven.

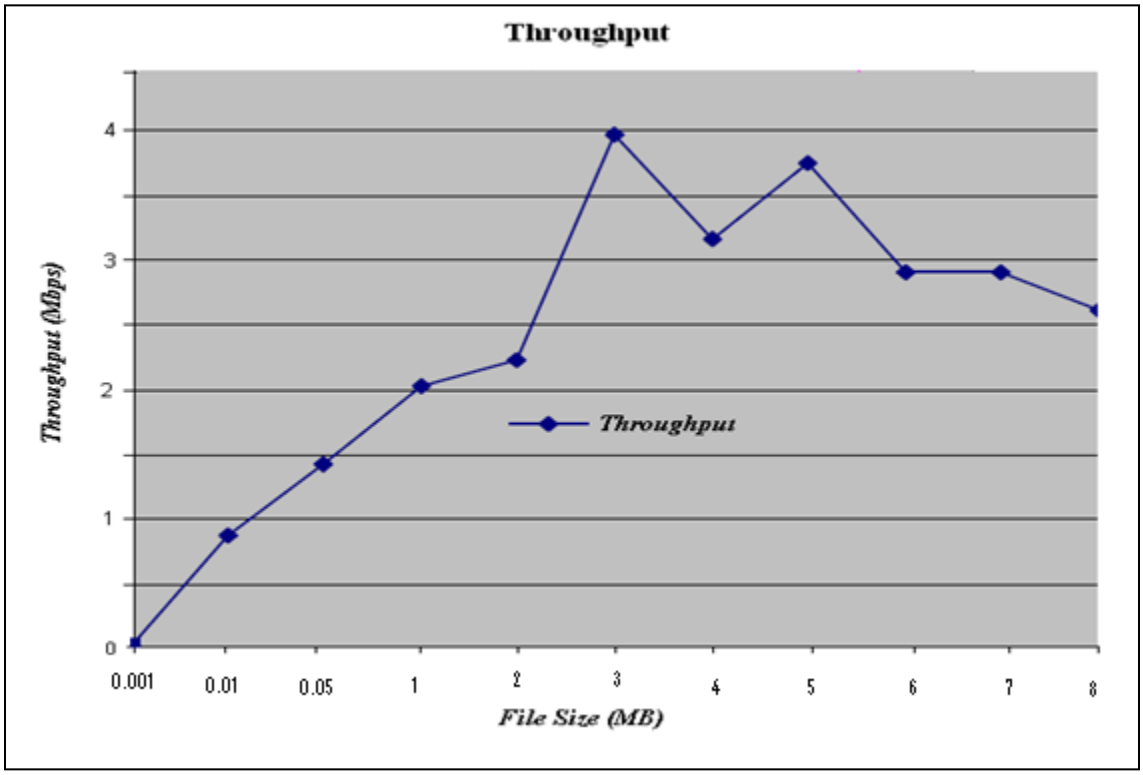


Figure 6.2: Throughput measured against file size.

Figure 6.2 illustrates that there is a slow increase in throughput as a file of 0.001MB is transferred until it reaches 1MB. During this phase, throughput is directly proportional to the size of a file being transferred. During a transfer of file size 3MB to 5MB throughput reaches a maximum. This is the peak point after which it drops as the file size increases. This trend in throughput behavior can be caused by a number of factors, including:

- During transfer of small files, the WiMAX holding capacity has not yet been reached and some of the bandwidth remains unused. Consequently, transferring small files means less traffic congestion and bandwidth utilization.
- Throughput starts to decline after all the bandwidth has been utilized and the link cannot support the load in it. This, in turn, slows the transfer rate. However, it was discovered that, in some cases, throughput was lower than expected although the transfer rate was high.

Having evaluated the throughput of the NHS DAN, the latency on this node was evaluated afterwards. The results are shown in Figure 6.3, below, which illustrates latency on the vertical axis (measured in seconds) plotted against file size on the horizontal axis.

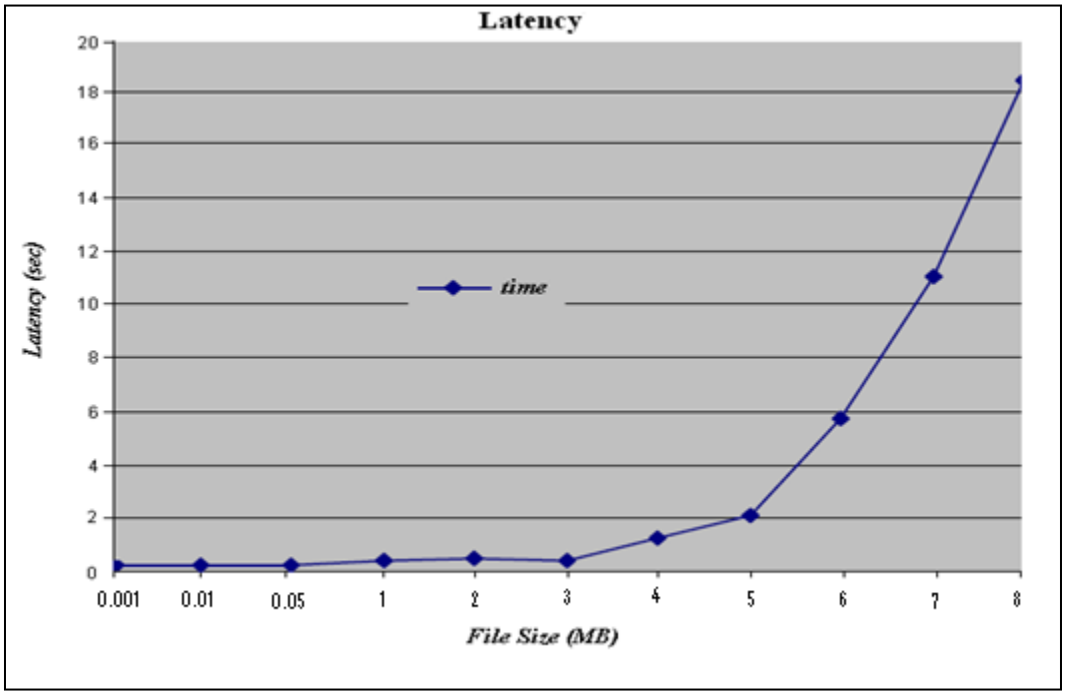


Figure 6.3: Latency measured against file size.

Figure 6.3 shows an expected behavior of files smaller than 4MB which experience a low latency below 2 seconds. This implies that the smaller the file the faster it is transferred in the network. The major reason for this behavior is because of lower congestion in the WiMAX network when

small files are being transferred. This can be attributed to unused bandwidth which is still available for usage and the load capacity of the link that has not been reached.

However, it was noted that as the files increased from 5MB, there was more latency experienced in the network. The other reason, besides limited bandwidth, might be the way the transfer script operates. The transfer script has many operational processes including the reading of contents into the buffer and then fetching them back for disk writing. After disk writing, the verification of a complete content reading is done before a success message is finally given. The verification process contributes quite significantly to high latency because it is not part of disk writing and it uses a large amount of bandwidth.

From the results that were obtained for the throughput and latency of the NHS DAN, it was possible to compute the optimal load of this node. The optimal load was computed using equation 6.4 below. Figure 6.4 below shows the optimal load of the WiMAX DAN.

$$Optimalload = Maximum\frac{(Throughput * \alpha)}{Delay} \quad (6.4)$$

Where the network factor = 1 in this scenario

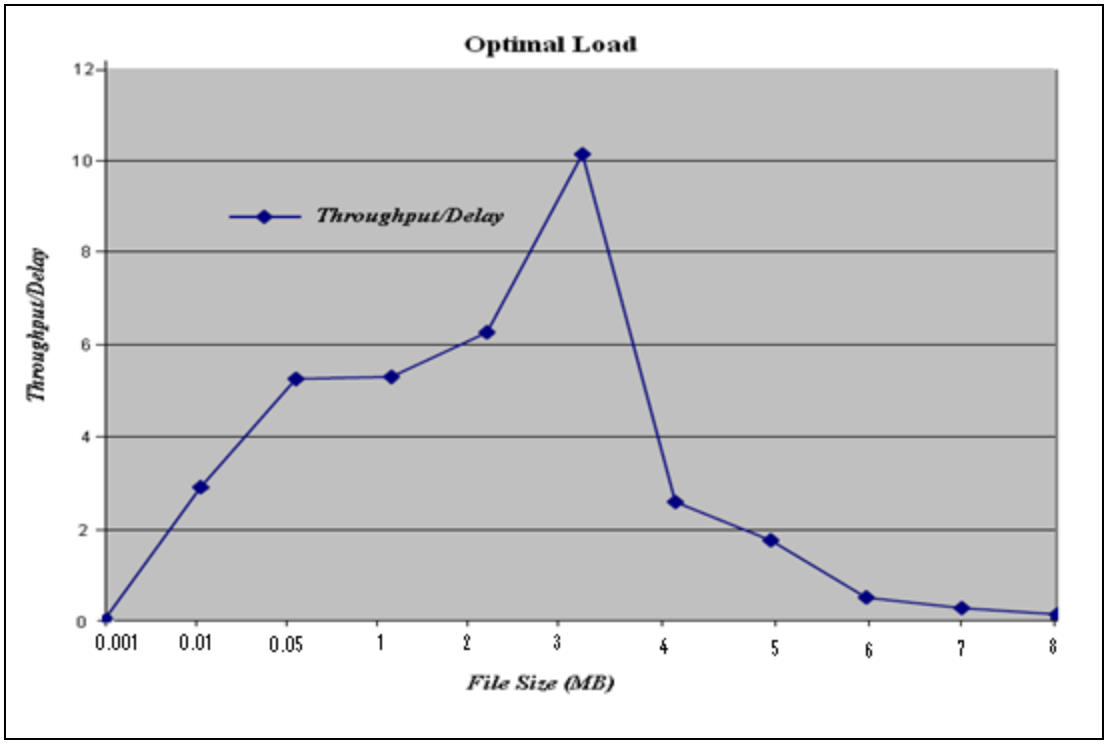


Figure 6.4: Optimal link load of the NHS WiMAX DAN network.

Figure 6.4 shows that the throughput/delay starts by increasing sharply until files of size 0.05MB are transferred. Thereafter, it gradually increases until a peak is reached at 3MB. This is the point where the optimal load can be transferred on this node without experiencing any high latency. Afterwards, there is a decline in throughput/delay as the file sizes continue to increase. This is due to the high latency experienced and minimum bandwidth available. Having tested the WiMAX backbone loop and looked at its performance, hotspots testing followed.

6.2 WiFi Hotspot Testing and Performance Evaluation

In this section, functionality testing procedures on each hotspot are presented. A HP Compaq wireless laptop was used to connect to the hotspot and disconnect from it. This involved a connection test and a network performance evaluation when a ChilliSpot access controller was added.

6.2.1 Connectivity Test

This involved pinging the AP and other clients on the LAN wirelessly. The ping application determines whether two hosts are communicating and checks if a connection is established between them. It can also be used in FTP applications as an initial troubleshooting technique during the failure of communication. Firstly, all security mechanisms such as WPA, WEP and Mac Address restrictions were turned off so as to avoid complications. The SSIDs for each DAN were first checked for availability before issuing the following command in the terminal *iwconfig* so as to ascertain what the laptop's WiFi card is called. Afterwards, a connection test was performed to find out if there is a working Internet connection by checking if the domain exists and can be reached through typing the following command:

ping -n 192.168.5.50 -c 4

This command sent out 4 pings to the internet address 192.168.5.50 and the following output was shown.

PING 192.168.5.50 (192.168.5.50) 56(84) bytes of data
64 bytes from 192.168.5.50: icmp_seq=1 ttl=52 time=86.6 ms
64 bytes from 192.168.5.50: icmp_seq=2 ttl=52 time=94.5 ms
64 bytes from 192.168.5.50: icmp_seq=3 ttl=52 time=84.3 ms
64 bytes from 192.168.5.50: icmp_seq=4 ttl=52 time=86.0 ms

These results showed that the wireless card is working and it was possible to ping an Internet address. The domain name was checked by pinging "yahoo.com" which is an internet address. The command *ping yahoo.com -c 4* was used. The experiment produced positive results because it was possible to ping the address. This showed that the DNS is working and our network is functioning properly. This procedure was performed in all DANs in the network and all our hotspots proved to be working fine. Section 6.2.2 below presents the results of the ChilliSpot access controller testing.

6.2.2 ChilliSpot Access Controller Testing

In this section, an experiment was conducted to test the ChilliSpot for bugs. The reason for this was to find out if it contains any bugs; this was done on a debian Linux shell as illustrated below.

```
root@DT:/# sudo /usr/local/sbin/chilli --debug --fg
ChilliSpot version 1.1.0 started.
chillispot[3926]: ChilliSpot 1.1.0. Copyright 2002-2005 Mondru AB. Licensed under GPL. See http://www.chillispot.org for credits
Waiting for client request...
```

This ChilliSpot testing checks for faults in the code and is run in debug mode. The status of the ChilliSpot can be determined from this and the results show that the program was successfully installed and was awaiting requests from clients. As a result, clients trying to access the network resources through a WiFi enabled device would be redirected to this access controller and requested to login with valid credentials. The network topology was setup, as shown in Figure 6.5 below, so as demonstrate how our deployed network functions and provides restricted access to resources.

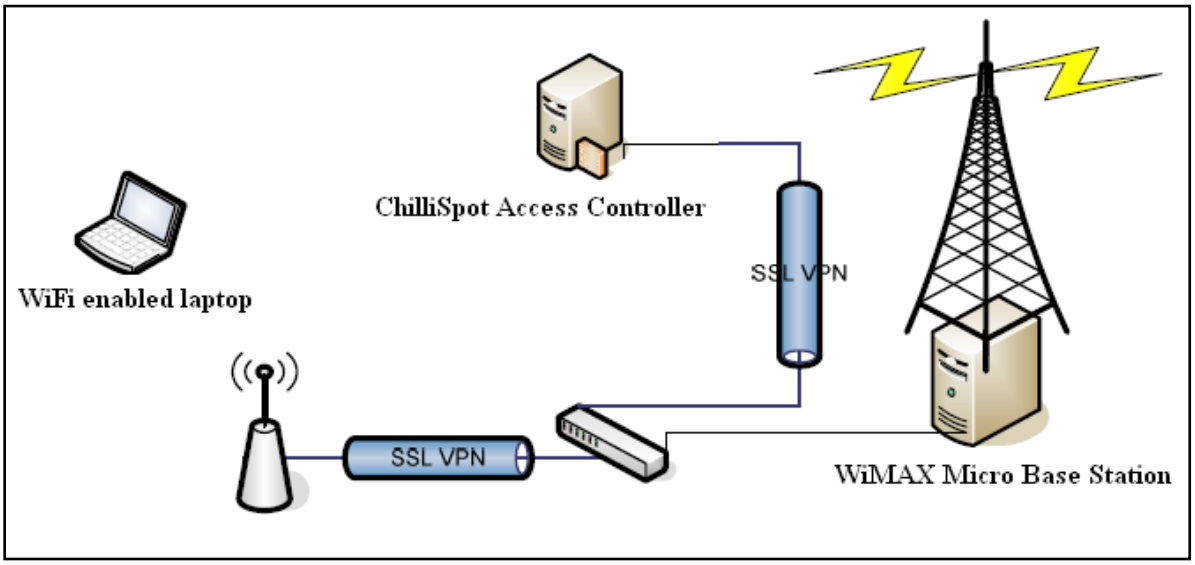


Figure 6.5: Users access the network resources through WiFi enabled devices.

Figure 6.5 above shows how a user is redirected to the ChilliSpot captive portal and requested to authenticate prior to accessing the Internet. In this experiment, proxy settings were deactivated. Figure 6.6 below shows the user being requested to enter their credentials which are a valid username and password.

Figure 6.6: Login page

Since an account for Matwayi had previously been created, the following login credentials were used to log into the system: username: *matwayi* and password *kaizer*. Matwayi was successfully logged in and was able to access the Internet. This is illustrated in Figure 6.7 below.

Figure 6.7: Successful login by user.

However, if the user is unauthorized, they are denied access to the network resources and are requested to login again with valid credentials. This is shown in Figure 6.8 below.

Figure 6.8: Login Failed

Figure 6.8 above shows unauthorized clients being denied access and requested to login with valid credentials. In Section 6.2.2 below, a brief presentation of the performance evaluation, with ChilliSpot installed, is given.

6.2.3 Performance Evaluation with ChilliSpot Installed

Once it was established that the network operated successfully, various tests were carried out with ChilliSpot installed. Firstly, general experiments which involved establishing whether a connection could be maintained and that the browser was redirected upon first launch were conducted. The details of these general hotspot testing experiments are given in the appendices section. Afterwards, performance evaluation tests, so as to determine the impact of ChilliSpot on network performance, were conducted. The reason for this was to determine the traffic overhead cost in terms of the downloading time throughput and RTT of ICMP packet (latency).

FTP applications were used to conduct downloading times for throughput performance and a ping application was used to determine delay time using RTT. RTT of the ICMP experiment was performed so as to determine packet delay overhead costs. The main idea was to measure RTT and downloading time. Each experiment was conducted three times and then the average determined later on.

A. Packet Delay

Various applications of different sizes such as web browsing, e-judiciary, e-health and VoIP services are utilizing the network and, as a result, ICMP packets of different sizes were chosen to represent these applications. ICMP packets ranging from 64bytes to 65536bytes were used to measure the performance metric of packet delay. This experiment was performed through the use of a ping application and it involved a ping on:

i. Two wireless clients on the NJSS WLAN.
ii. A wireless client at NJSS and the router at NHS.
iii. MJSS Access Concentrator (AC) and the wireless client at NJSS.

The network topologies for the conducted tests are given in the appendices. The outcomes of the experiment are presented in a graph as shown in Figure 6.9 below.

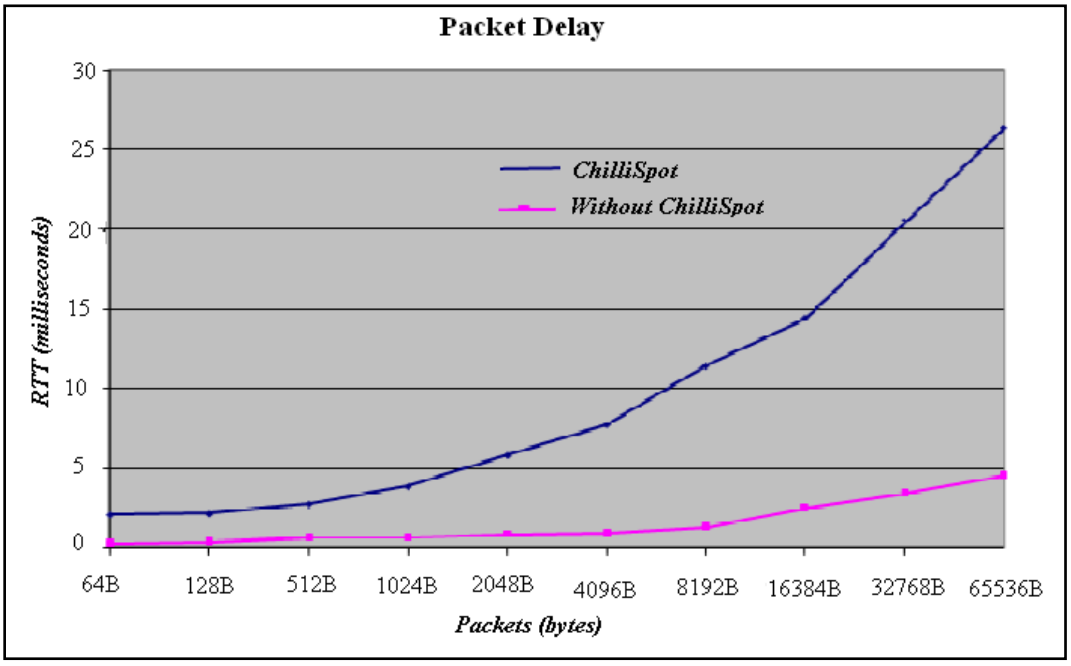


Figure 6.9: The packet delay on ICMP with and without ChilliSpot.

Figure 6.9 shows that RTT is directly proportional to the packet size. Generally, RTT increases with increase in packet size because transmission delay increase with packet size (Transmission

= Packet length/Link speed). In other words, a smaller packet takes a smaller amount of time to reach its destination and loop back in comparison to a larger packet. The reason might be that smaller packets require small bandwidth to be transferred. The graph also shows that the RTT with ChilliSpot implementation took a longer time to loop back when compared to the RTT without a ChilliSpot protocol implemented. The reason for this can be that some of the bandwidth is utilized by the ChilliSpot which, as a result, creates load congestion in the network and therefore higher RTT.

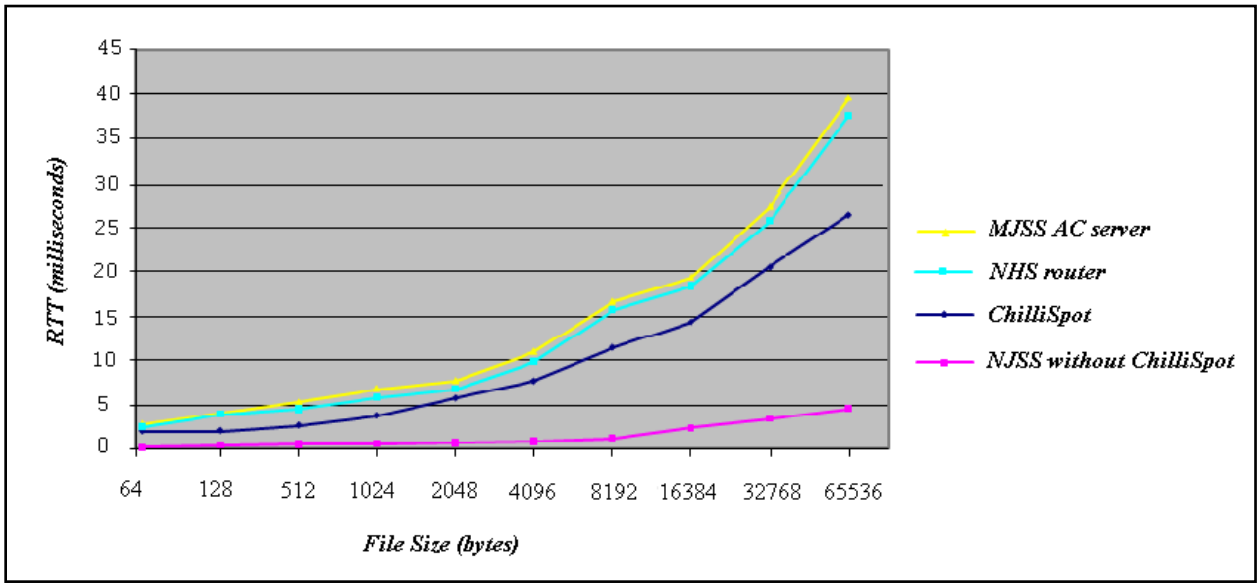


Figure 6.10: Packet delay with other DANs included.

Figure 6.10 shows lower packet delay for NJSS DAN in comparison to the MJSS AC server and NHS router. Different factors, such as distance between the DANs, line of sight (LOS) and the number of hops between the hosts might have influenced this behavior trend. There are many hops between NJSS DAN and NHS DAN. This is the same with NJSS DAN and MJSS AC. As a result, the RTT delay is high because the packets take longer to move to and from their destinations. This explains why the MJSS AC server has a higher RTT compared to other DANs. Other factors like distance and LOS contribute to the high RTT and the long delay in the packet looping back to the sending host. PPPoE with MPPE running on the NHS router and MJSS AC server may also contribute to the high RTT unlike that of the NJSS WLAN.

Afterwards, a downloading time on FTP experiment was conducted; this is presented in Section B below.

B. The Downloading Time on FTP

The aim of this experiment was to determine the throughout performance when a ChilliSpot access controller is installed. FTP was used to show the general downloading time in relation to file size. Different file sizes were transferred across the network and these ranged from 50KB to 10MB. Figure 6.11 below shows the results that were obtained after performing the experiment.

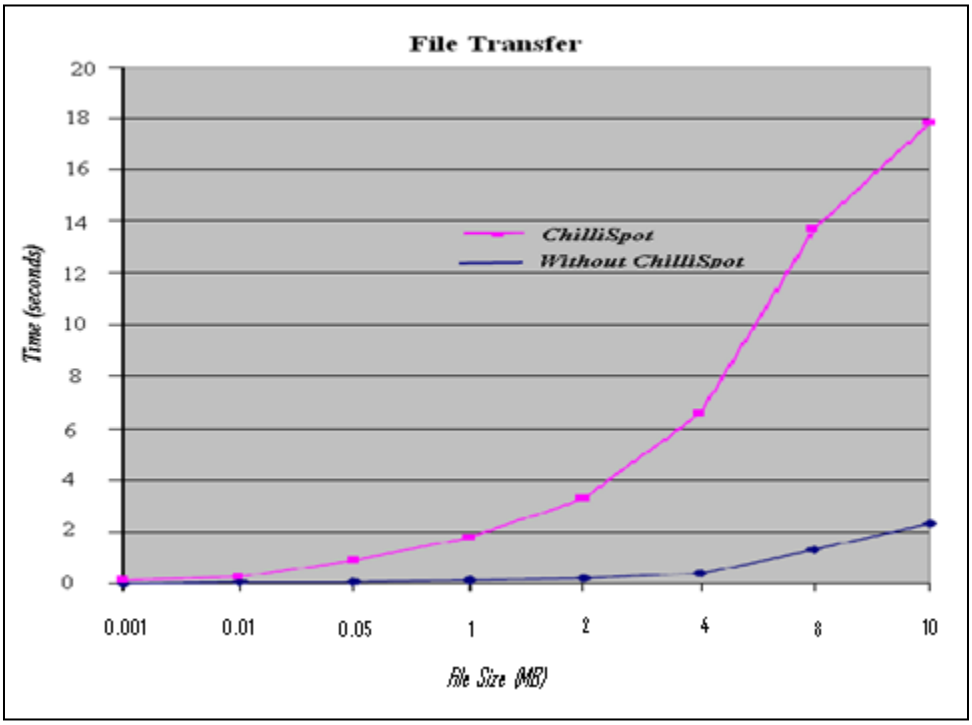


Figure 6.11: FTP downloads with and without a ChilliSpot.

Figure 6.11 above shows that the transfer of files less than 1MB is below 2 seconds. This basically means a faster downloading time. As the file size increased from 1MB to 10MB, we see that the time of transfer increased. This implies a delay of some sort. Generally, it is evident that transferring files with ChilliSpot implemented takes longer time that it would in a scenario in which it is not implemented. The major reason for this might be the SSL in its encryption of the web-based login and the Freeradius server in its authentication which utilizes some of the

bandwidth. As a result, insufficient bandwidth is available for downloading a file and this takes longer. It can be concluded that the addition of a ChilliSpot access controller reduces throughput in the network although it is vital in terms of controlling access to the network and its resources, on a larger scale.

6.2.4 Internet Responsiveness

This experiment was conducted to determine the way in which the Internet responded in terms of speed during different times of the day, including weekends. Weekends were included in this test because the addition of hotspots meant that community members can access network resources wirelessly even over weekends and during holidays. The total throughput on the gateway interface per hour and the percentage of local traffic was taken into account. This was done at Mpume J.S. School server. This was done early in the morning, at approximately 06h00, when network usage was low. Figure 6.7, which was generated from the Wireshark, shows the total number of requests per hour and the average bandwidth experienced.

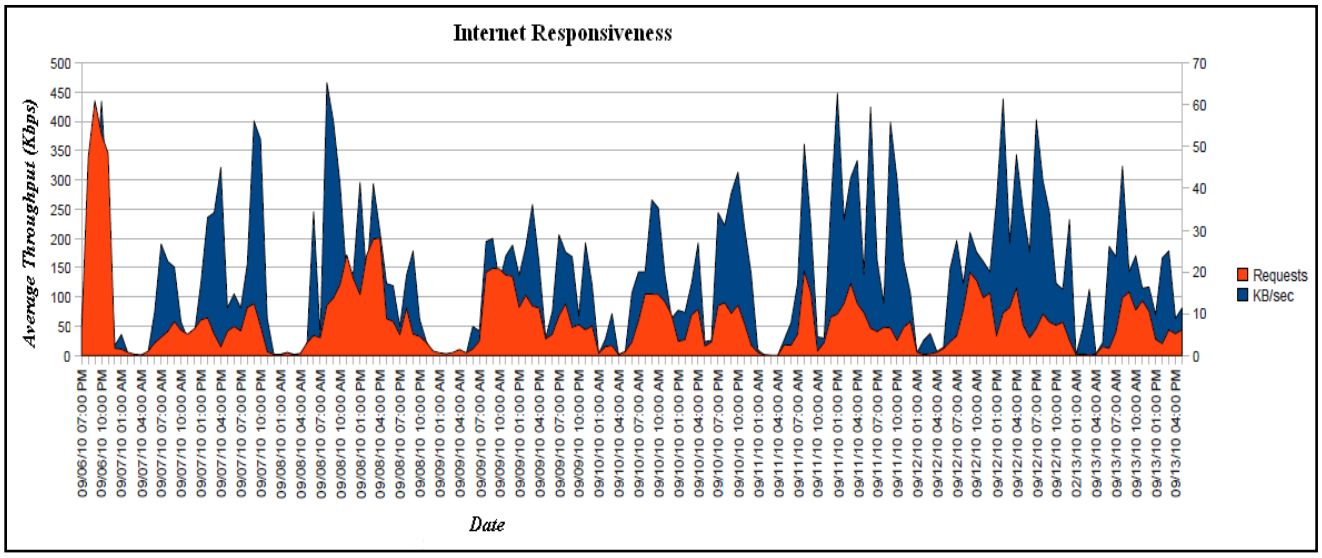


Figure 6.12: Plot of the total throughput for the satellite link over 8 days.

Figure 6.12 illustrates the average throughput experienced in Kbps and the total number of requests per hour over a period of 8 days. The total throughput follows an uneven pattern. The period in which the network is not in full use is short and occurs from 01h00 to 04h00, almost

daily. The major reason for this is that the users can stay up late and others wake up early to access the resources. However, it is evident that from 08h00 to 23h00, the average bandwidth usage is high with maximums reaching 450Kbps at times. This might be due to the introduction of hotspots which have allowed users to access the network at any time of the day. The deployment of hotspots has indeed brought ubiquitous Internet access to the Dwesa community. Section 6.2.5 below presents the methodology used in evaluating and explaining the Internet usage trends brought about by the deployment of WiFi hotspots.

6.2.5 Internet Usage Analysis

The successful deployment of hotspots has increased network resource redistribution because they are accessible at any time, if one is within the coverage range. However, it was critical to determine whether the introduction of WiFi hotspots had an impact in the Internet and resource usage of the SLL network; it also wished to determine whether the bandwidth of 3000 Mb with 128 Kbps uplink and 512 Kbps downlink allocated on a monthly basis is affected or needed to be upgraded. An experiment on the Internet usage analysis was conducted to determine these anticipations.

Generally, this experiment involved the monitoring and capturing of Internet traffic on the incoming and outgoing interfaces of the gateway server. An application called ACgui in Figure 6.13 below is used to show the status of the interfaces of the servers in the SLL network.

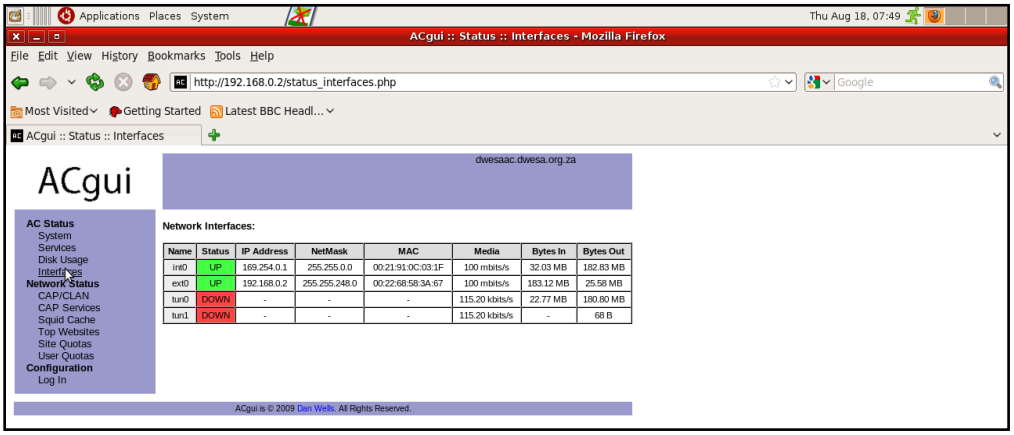
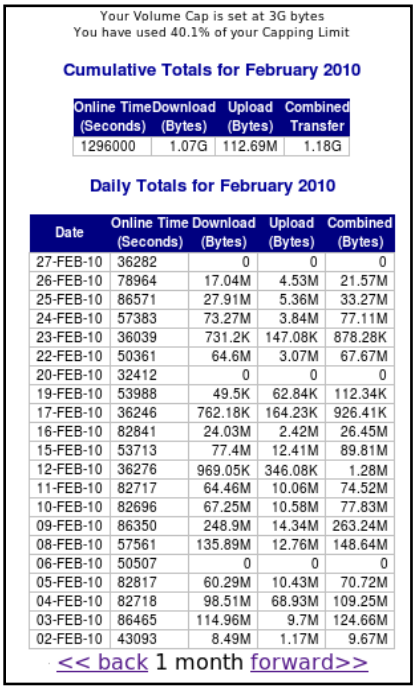


Figure 6.13: ACgui showing the status of interfaces of the server

An Internet usage experiment was done before and after the deployment of WiFi hotspots. Afterwards, a comprehensive analysis and comparison was conducted to determine any significant changes in bandwidth usage. Generally, this method presents accurate results, if followed properly, and observations conducted over a long period of time. In this experiment, the time frame was set for a period of six months prior to and after deployment. Figure 6.14, below shows the Internet usage pattern for February 2010.



Your Volume Cap is set at 3G bytes
You have used 40.1% of your Capping Limit

Cumulative Totals for February 2010

Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined Transfer
1296000	1.07G	112.69M	1.18G

Daily Totals for February 2010

Date	Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined (Bytes)
27-FEB-10	36282	0	0	0
26-FEB-10	78964	17.04M	4.53M	21.57M
25-FEB-10	86571	27.91M	5.36M	33.27M
24-FEB-10	57383	73.27M	3.84M	77.11M
23-FEB-10	36039	731.2K	147.08K	878.28K
22-FEB-10	50361	64.6M	3.07M	67.67M
20-FEB-10	32412	0	0	0
19-FEB-10	53988	49.5K	62.84K	112.34K
17-FEB-10	36246	762.18K	164.23K	926.41K
16-FEB-10	82841	24.03M	2.42M	26.45M
15-FEB-10	53713	77.4M	12.41M	89.81M
12-FEB-10	36276	969.05K	346.08K	1.28M
11-FEB-10	82717	64.46M	10.06M	74.52M
10-FEB-10	82696	67.25M	10.58M	77.83M
09-FEB-10	86350	248.9M	14.34M	263.24M
08-FEB-10	57561	135.89M	12.76M	148.64M
06-FEB-10	50507	0	0	0
05-FEB-10	82817	60.29M	10.43M	70.72M
04-FEB-10	82718	98.51M	68.93M	109.25M
03-FEB-10	86465	114.96M	9.7M	124.66M
02-FEB-10	43093	8.49M	1.17M	9.67M

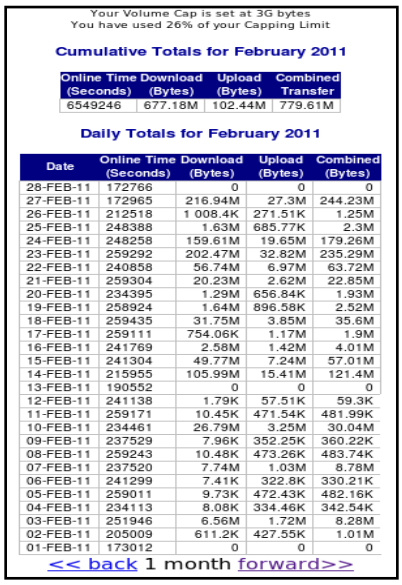
<< back 1 month forward>>

Figure 6.14: Internet usage in February 2010.

Figure 6.14 shows Internet usage for the month of February 2010. During school holidays and weekends, there was little Internet usage as compared to working days. The main reason for the trend was that only administrators and school teachers have access to the Internet during weekends and holidays. Other community members had no access at all, since the school labs were closed. Community members only had access to the Internet when schools were opened for a specified period. This was a problem, especially when they wanted to access SLL resources beyond that specified period and in cases of emergency.

After deploying WiFi hotspots, a similar experiment was conducted over a period of six months. The idea was to compare Internet usage patterns for both experiments and determine whether or

not to increase the bandwidth allocation. Figure 6.15, below, shows the Internet usage pattern for the month of February 2011.



Your Volume Cap is set at 3G bytes
You have used 26% of your Capping Limit

Cumulative Totals for February 2011

Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined Transfer
6549246	677.18M	102.44M	779.61M

Daily Totals for February 2011

Date	Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined (Bytes)
28-FEB-11	172766	0	0	0
27-FEB-11	172965	216.94M	27.3M	244.23M
26-FEB-11	212518	1 008.4K	271.51K	1.25M
25-FEB-11	248388	1.63M	685.77K	2.3M
24-FEB-11	248258	159.61M	19.65M	179.26M
23-FEB-11	259292	202.47M	32.82M	235.29M
22-FEB-11	240858	56.74M	6.97M	63.72M
21-FEB-11	259304	20.23M	2.62M	22.85M
20-FEB-11	234395	1.29M	656.84K	1.93M
19-FEB-11	258924	1.64M	896.58K	2.52M
18-FEB-11	259435	31.75M	3.85M	35.6M
17-FEB-11	259111	754.06K	1.17M	1.9M
16-FEB-11	241769	2.58M	1.42M	4.01M
15-FEB-11	241304	49.77M	7.24M	57.01M
14-FEB-11	215955	105.99M	15.41M	121.4M
13-FEB-11	190552	0	0	0
12-FEB-11	241138	1.79K	57.51K	59.3K
11-FEB-11	259171	10.45K	471.54K	481.99K
10-FEB-11	234461	26.79M	3.25M	30.04M
09-FEB-11	237529	7.96K	352.25K	360.22K
08-FEB-11	259243	10.48K	473.26K	483.74K
07-FEB-11	237520	7.74M	1.03M	8.78M
06-FEB-11	241299	7.41K	322.8K	330.21K
05-FEB-11	259011	9.73K	472.43K	482.16K
04-FEB-11	234113	8.08K	334.46K	342.54K
03-FEB-11	251946	6.56M	1.72M	8.28M
02-FEB-11	205009	611.2K	427.55K	1.01M
01-FEB-11	173012	0	0	0

<< back 1 month forward>>

Figure 6.15: Internet usage in February 2011.

6.15 shows Internet usage in February 2011, which is a depiction of the usage for 28 days including weekends. An interesting point of observation is the Internet usage during weekends. This is a new development because it was difficult to access Internet during weekends in 2010, prior to the deployment of hotspots, if one had no access to privileges. However, over some weekends, they was no Internet usage because the servers were switched off or power disruptions were experienced. The comparison provided in Figure 6.16 shows the usage statistics before and after the deployment of hotspots.

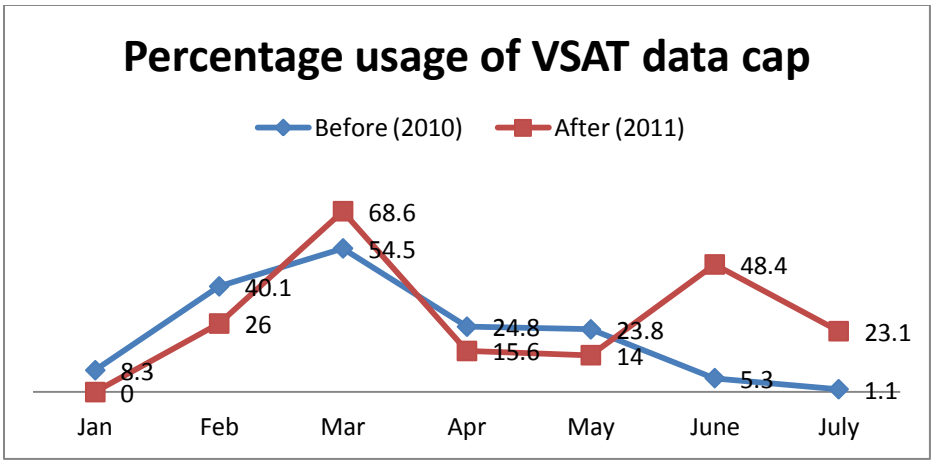


Figure 6.16: Percentage usage of VSAT data cap [Feb - July (2010 & 2011)]

Figure 6.16 shows a comparison between 2010 and 2011. During the 2010 period, schools which are the main points of access were closed during weekends and holidays. The percentage usage of bandwidth was very low during the June and July 2010 school holidays. Generally, most of the Internet users, during 2010, relied on accessing resources through the school labs which closed at 15h00 everyday and were closed during weekends. The 2011 spell started with no Internet at all because of the SLL network failure. From October until November 2010, the network had been inconsistent and failed most of the time. The problem was technical and required experts to address it. In February 2011, we saw an increase in Internet usage. During this month, the network operated properly and most users could access the resources, even during weekends, because of the availability of WiFi hotspots. However, in March 2011 an outlier was evident in the results graphs; the Internet usage increased greatly to 68.6%. This is a period when training sessions were conducted to train users on how to use WLAN and create user accounts on the access controller for authorized users. Many users needed to register first so that feasible results would be achieved in the end. This caused a high usage of the Internet even during weekends. The ensuing months followed a trend similar to that of 2010, even though there was a slight increase in figures.

However, it was critical to determine whether the introduction of WiFi hotspots had an impact on Internet and resource usage of the SLL network. This was done through the analysis of data for both periods: the 2010 spell when the WiFi hotspots were unavailable and the period after the

deployment of hotspots in 2011. A paired samples T-test was used and the statistical results are given in the appendices. Table 6.1 below shows the paired samples test section.

Table 6.1: Paired Samples Test

		Paired Differences				
		95% Confidence Interval of the Difference				
		Lower	Upper	t	df	Sig. (2-tailed)
Pair 1	A2010 - B2011	-35.6140109	4.3806776	-2.007	5	.101

Table 6.1 above shows the paired samples T-test with a probability value of 0.101. The addition of WiFi hotspots was anticipated to increase the Internet usage and bandwidth. Statistically, this expectation is denoted with a probability value of less than 0.05. Thereafter, one can conclude that there is a significant difference between the two scores. In this experiment, a probability value of 0.101 was obtained and was substantially greater than the specified alpha value of 0.05. Therefore, it was concluded that there was no significant difference between the two scores i.e. 2010 (M = 9.6, SD = 6.439) to 2011 (M = 25.2166, S = 21.87), t (5) = -2.007, $p>0.05$. As a result, the addition of WiFi hotspots had no effect on the Internet usage and bandwidth allocated. The main reason for these results was that the Dwesa community is not fully accustomed to the concept of hotspots. An informal interview with the community members and feedback from the questionnaire showed that the majority still prefer accessing resources through the schools' labs, which have desktop computers installed. Through observation, it was noted that although the introduction of hotspots has not increased Internet usage, it has emerged as a convenient way to access resources when school labs are closed (weekends and holidays).

Having completed all the necessary functionality tests in each DAN in the network and affirmed that everything was working, an investigation was conducted to determine the benefits brought about by the addition of these hotspots, in terms of accessing the resources and some other applications. This was done through the evaluation of responses to a questionnaire completed by

community members. Section 6.3 below presents the findings and achievements obtained from this research.

6.3 Findings

The establishment of this ICT4D initiative in Dwesa, through the extension of the existing SLL network and hotspots deployment, has facilitated the access of opportunities and information. This innovative telecommunications infrastructure deployment has been successful because various services are now offered to the community in order to improve their socio-economic livelihoods. The next section elaborates on how this network deployment has influenced the social and economical development of the Dwesa community and its members.

6.3.1 Social and Economical Development

The introduction of hotspots has added capillarity to the network and has allowed the Dwesa community to have ubiquitous Internet connectivity. This means that they can access Internet at any time of the day, including weekends and holidays when schools are closed. This was practically impossible before this development. In the next section, we present the results obtained from the responses to the questionnaire which was answered by community members. The questionnaire allowed community members to express their views and opinions regarding the deployment of this ICT4D initiative.

A. Computer and Internet Literacy Evaluation

Figure 6.17 below shows computer and Internet literacy evaluation statistics. The results were derived from the responses to the questionnaire by community members (teachers, students and local villagers). 25 participants, randomly selected by choosing 5 participants per DAN, were evaluated.

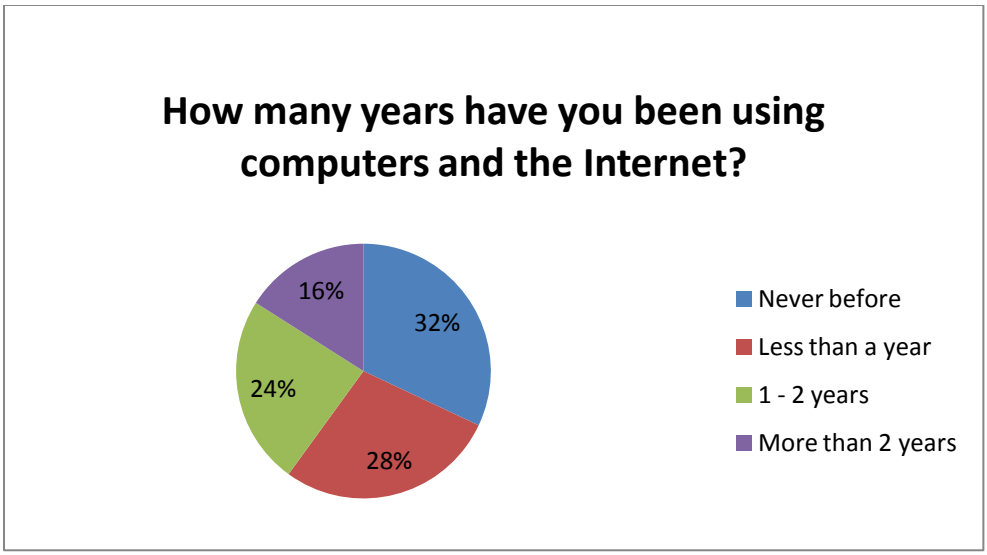


Figure 6.17: Computer and Internet literacy evaluation.

Figure 6.17 shows that 32% (eight) of the participants have never used the Internet before. Although the project was initiated in 2006, the main reason for this large a percentage of computer illiteracy can be attributed to the way in which community members had previously accessed SLL network resources. The access nodes, which are schools in this case, are closed soon after 16h00 and over weekends. It inconveniences the users so much that others lose interest in computers. However, 28% (seven) of the participants have been using the Internet for less than a year now. Lastly, 16% (four) of participants have used the Internet for more than two years. This percentage of participants definitely constitutes those who have been involved with the SLL project ever since it started. The eight participates who have never used computers and the Internet cannot be included in the next set of evaluation questions since it requires information from those who are computer literate.

B. Network Resource Accessing Methods

The following section provides the results obtained from the remaining 17 participants who have used the Internet and computers before. Participants were asked about the method they use to access the Internet. Figure 6.18 below shows the responses received from the participants.

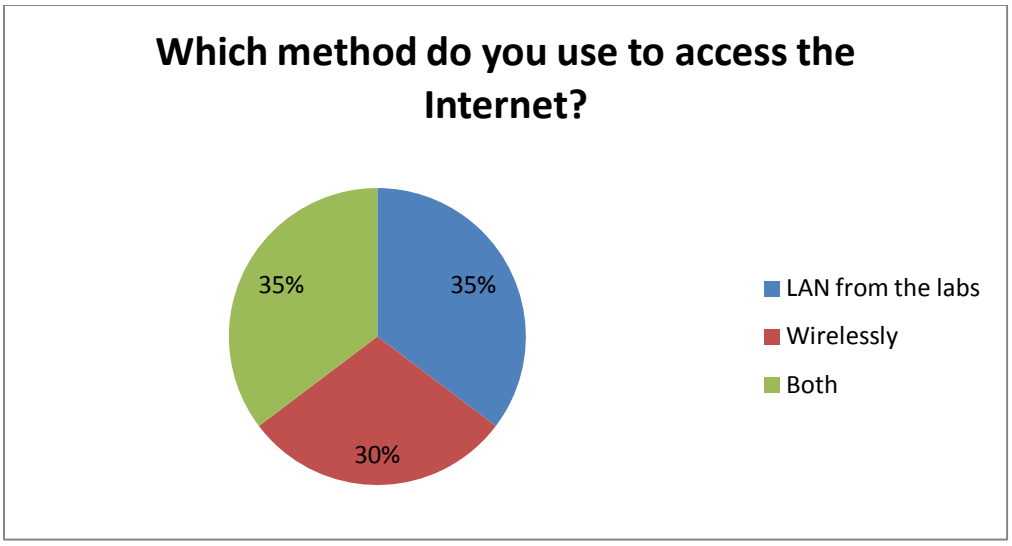


Figure 6.18: Accessing the SLL network resources.

Figure 6.18 shows that 35% (six) of the participants prefer to access the Internet through the local area network at DAN. The reason for this might be that they do not have WiFi enabled devices to connect wirelessly. However, 30% (five) of the participants prefer to use their WiFi enabled devices and connect wirelessly. This means that they can access network resources at any time of the day as long they are within range. These results show that villagers are also able to access e-services repositories wirelessly at any time, even in case of an emergency. 35% (six) of participates use either method. One can access the network resources wirelessly, even if outside the school premises, within the coverage zone.

C. Applications Frequently Accessed

The objective of this section was to determine the most common sites which users prefer to access. 17 participants responded to the questionnaire, and Figure 6.19 below shows their responses.

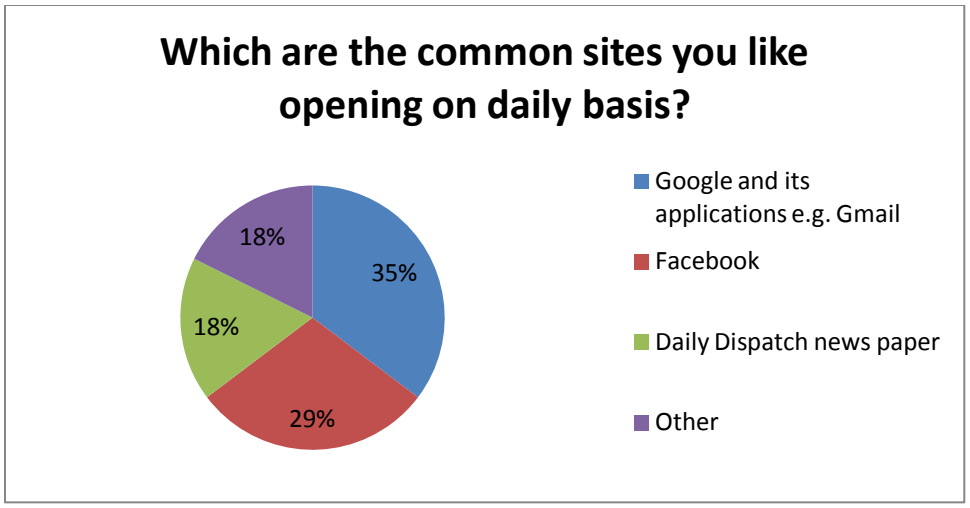


Figure 6.19: Commonly accessed applications and sites

Figure 6.19 shows that 29% (five) of the participants prefer to open their Facebook accounts. The community members are able to use applications such as Facebook at any time of the day. This allows them to communicate with relatives and friends who are far away. As a result, social networking and communication standards in the area have greatly improved. This is due to a decrease in the need for community members to travel long distances to send a message to their relatives. On the other hand, 35% (six) of the participants use Google and its applications, like Gtalk for chatting and Gmail for emailing purposes. The other reason why they prefer to use Google is for research and education. This would definitely improve the education standards in the area. 18% (three) of the participants preferred to open newspapers and keep themselves updated as to current affairs. As a result, this facility is anticipated to greatly improve community information distribution and collection.

Furthermore, ACgui has been installed in the SLL network. Figure 6.20 below is an extract from ACgui showing part of the top 50 websites that were frequently accessed during the month of August 2011.

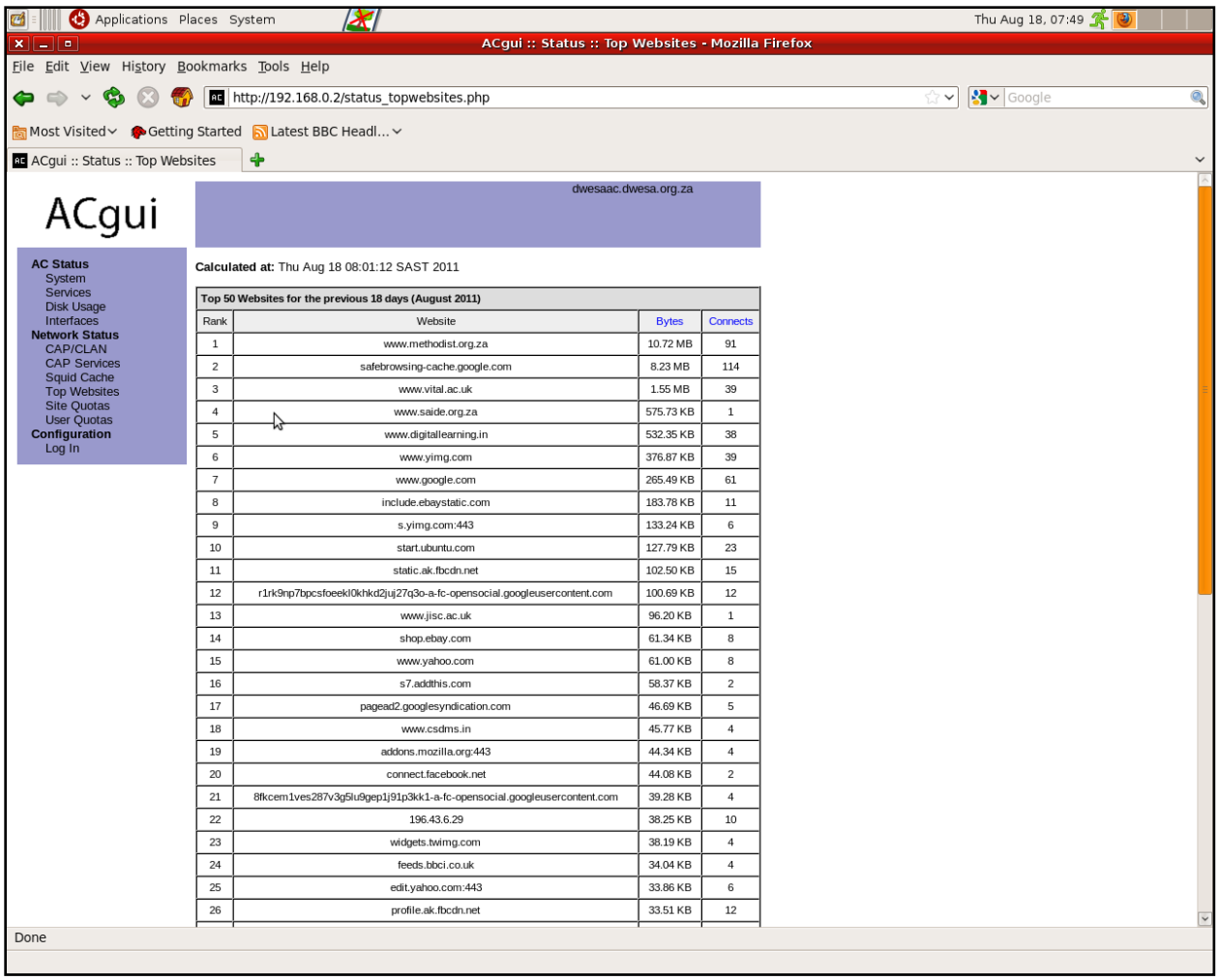


Figure 6.20: Top 50 websites accessed in August 2011

Figure 6.20 shows that websites like www.yahoo.com and www.google.com are part of the top 50 accessed sites and this corresponds positively with the feedback from the questionnaire. Additionally, in each school there is a VoIP telephony facility which has been deployed and it operates locally within the SLL network. This service is free of charge and only functions locally. Additionally, there is on-going training in schools; this is still progress. During this educational training, teachers and community members are taught new concepts and technological advancements related to the computer industry. Every month, researchers from both Rhodes and Fort Hare conduct training for one or two weeks; the duration of this depends on community attendance. Community members are trained on how to sustain the SLL project and have total ownership of the project. They are also encouraged to make full use of the Internet for research purposes and e-learning. Through this initiative, the level of computer literacy has

greatly improved in the area. This is evident from the feedback to the questionnaire which shows that 72% of the participants are computer literate and only 32% are illiterate.

During regular visits to the SLL for computer training exercises, the use of social networking applications was demonstrated to the community members. They were taught how to create accounts and use Gtalk, Facebook and Skype. Skype is a communications application which allows audio, text and video communication in real time worldwide and at no charge (Arjona et al., 2007). An informal interview with the participants was conducted afterwards and Figure 6.21 below shows the feedback obtained.

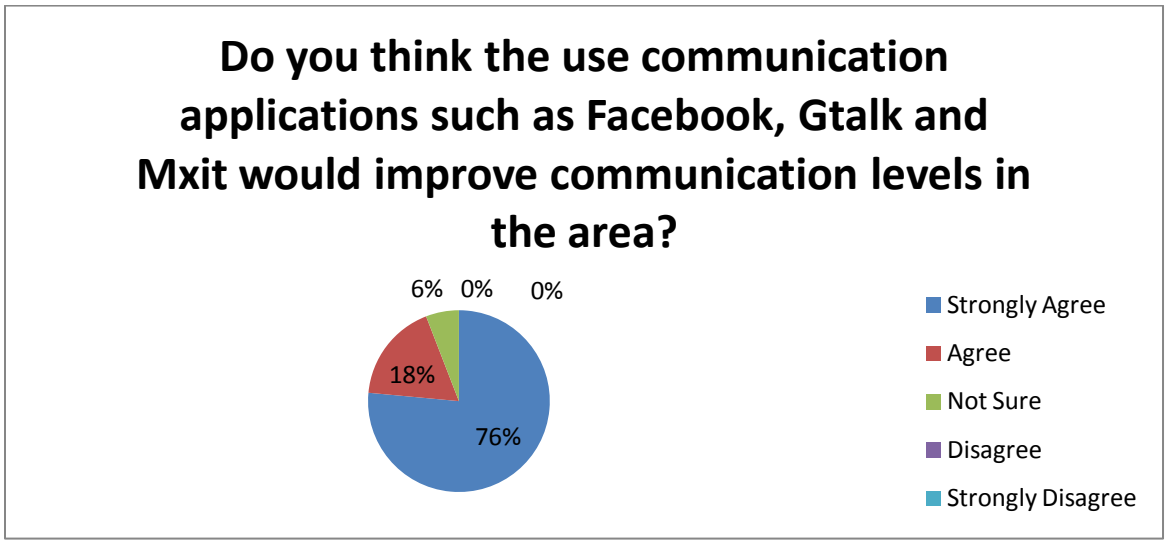


Figure 6.21: Interview responses on social networking applications

Figure 6.21 shows the responses of 17 participants who were interviewed after using the Skype application during the training session. 94% (sixteen) of the participants agreed that the usage of these social networking applications would improve the way they communicate in future. They expect to benefit from the usage of these applications since they would be accessible at any time. 6% (one) of the participants were not certain and felt that it depends on who has access to a wireless device.

Finally, the responses from community members showed that they understood the benefits and usage of hotspots. This was determined through feedback from a questionnaire to which 25 participants, five per DAN, responded. Figure 6.22 below shows their responses.

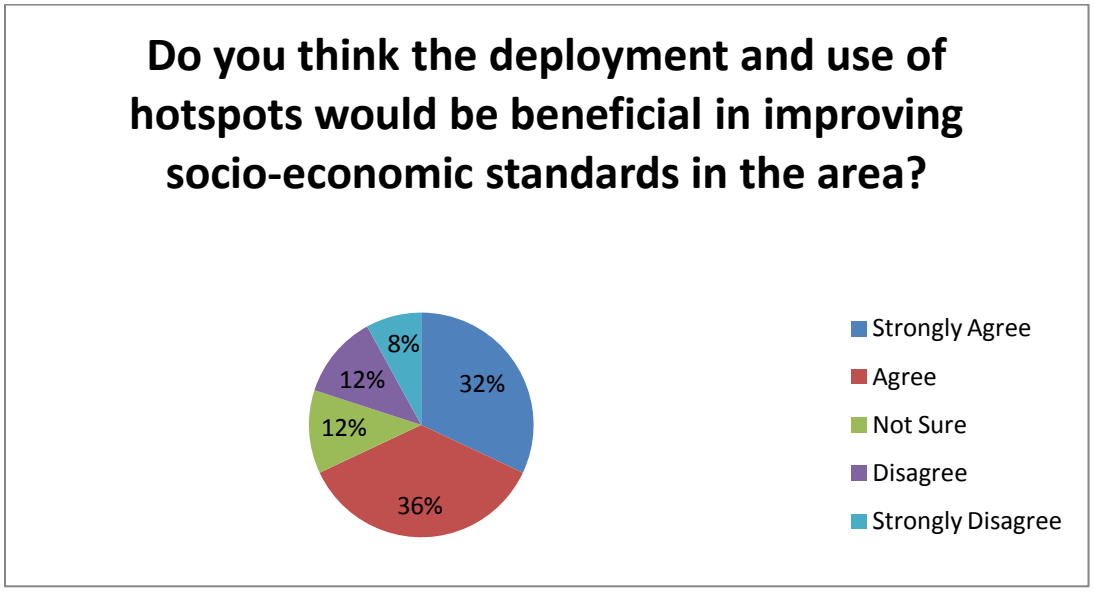


Figure 6.22: Socio-economic empowerment.

Figure 6.22 show that 68% (17) of the participants expect both social and economical benefits from the establishment of this initiative. They would be able to access various applications such as Facebook, e-commerce and other online applications such as e-banking even over weekends and during the holidays. This was impossible before the deployment of hotspots. 12% (three) of the participants were not certain because they were not familiar with hotspots and needed some training first. However, 20% (five) of the participants disagreed because they are computer illiterate and do not necessarily see the need of such initiative.

6.3.2 Cultural Influence by ICTs

There is also an Art and Craft Center in the Dwesa area where community members create crafts and arts based on their culture and tradition. An online application known as "An Online Shopping mall for Dwesa-Cwebe" was developed by one of the researchers to help the community members market their products and allow for the online shopping of their arts and

crafts worldwide (Njenje, 2007). This application allows customers to view and buy the arts and crafts online. The WiFi hotspot signal coverage at NHS can reach the Nqabara Craft center. A connectivity test, similar to one in Section 6.2.1, showed positive results and indicated that Internet connectivity was achievable. Internet availability means that community members are now able to complete their sales and transactions at the center. This would save them time, as they no longer need to go to the schools just to see if there are any sales made or if anyone requires a particular craft. These artifacts can be accessed at www.dwesa.com. However, the community has been alerted to what can be achieved by implementing ICTs, or not, so as to avoid conflicts which arise through rural tribal authority politics combined with our particular legislation and historical inequalities in the provision of resources. Refer to the appendices for regulatory and legislation rules for each country in Africa. Section 6.5 below, presents a summary of this chapter and introduces the conclusion and future work which has to be done to sustain and improve the SLL.

6.4 Summary

This Chapter presented various performance evaluation experiments that were conducted on the WiMAX backbone of the newly added NHS DAN. The performance evaluation experiments of each newly deployed WiFi hotspot in the network are given as well. This was done after connectivity and functionality testing were performed. Thereafter, a detailed explanation of the behavior of certain applications utilizing the network, soon after the hotspots were deployed, is presented. The levels of computer and Internet literacy and the feedback regarding the applications that community members prefer to access were presented. Finally, an explanation of the outcomes and findings of deploying this innovative ICT4D project in the Dwesa community was presented. These include the social and cultural benefits brought about by this initiative. In Chapter Seven, the final chapter of this study, this research is concluded by outlining its achievements and providing recommendations for future development and sustainability.

7 Chapter Seven: Conclusion

This Chapter presents a summary of the findings of the work undertaken in this project. It provides an overview of the achievements and limitations experienced during the deployment and extension of the SLL network. An explanation of how this initiative contributes to the rural community and the telecommunications sector is also presented. The final section of this chapter offers possible suggestions for research extension that can be conducted in future.

7.1 Goals Achieved

The primary objective of this research was to redistribute the SLL network services and address the problems faced by the Dwesa people when accessing these resources. They had to travel long distances to acquire services and mainly accessed them centrally in schools. This was a major problem when schools closed because the community had no access to these services at all. However, this problem was addressed through the provision of a telecommunication initiative which provided ubiquitous Internet and resource access. This also led to various access technologies being assessed in Chapter Three and their security capabilities investigated in Chapter Four. The main reason why security was taken into consideration is the issue of limiting unauthorized users from accessing network resources. Through the literature survey, various technologies were investigated in Chapter Three and WiFi, together with WiMAX technologies, were chosen because they are interoperable and can easily be merged to provide a cost effective and secure telecommunications network. WiFi hotspots were deployed around each and every DAN in the network. This has increased capillarity on the SLL network; this has led to the SLL network resources being distributed and accessible at any time. Users in this research were learners, teachers and community members. As a result, users now benefit from this innovation through the availability of various applications, including:

- Ubiquitous Internet access which is mainly used for accessing emails and chatting. The feedback from a questionnaire (Section 6.3.1(b)) showed that the learners, teachers and community members can now access various applications such as emails, Gtalk and

Facebook at any time through their WiFi enabled devices such as cell phones and laptops. This is expected to improve communication levels and social networking in Dwesa.

- The network resources are controllable because an access controller has been deployed. Users are required to authenticate prior to accessing the network resources. Through the literature survey (Section 4.1), various security mechanisms were investigated in Chapter Four and it was found that ChilliSpot was a better option in terms of controlling access to the SLL network. However, network performance tests (Section 6.2.3) showed that ChilliSpot has its own setbacks like high latency and packet delay on network performance.
- The community can use social networking and communications applications such as Facebook, Gtalk, Skype and IM for communication. Through the feedback gained from the questionnaire (Section 6.3.1(c)) and informal interviews (Section 6.3.1(c)) with the villagers, it was noted that the villagers are keen to use such applications and appreciate their benefits.
- Through observations during the regular field trips and from the questionnaire feedback (Section 6.3.1(c)), it was noted that community members regularly opened portal sites like Google and Yahoo. These are search engines used for research purposes. With ubiquitous Internet access in the SLL network, the education standards are anticipated to improve.
- From the observations made during connectivity testing, it was noted that community members would be able to access their sales whilst at the craft center or at home as long as they are within the coverage zone. This will save them time. WiFi embedded digital cameras would be used to take pictures of their artifacts and upload on the www.dwesa.com website.
- Since the inception of the SLL in 2006, several projects have been developed, and some are still being undertaken. Some of the projects that have been deployed and which can benefit from the availability of the wireless network include:
  - ❖ An e-commerce platform which enables members of the Dwesa community (SMMEs) to advertise and sell their art and crafts to the world market.
  - ❖ An e-government portal which aims to provide a platform for the people of Dwesa to access Government services online.

The following projects would also be accessible wirelessly once deployed:

- ❖ An e-judiciary portal which delivers online Judiciary services to the Dwesa community.
- ❖ A help desk system for the collaborative sharing of knowledge for the continuous assessment of project activities in Dwesa.
- ❖ An e-health portal for the Dwesa community to access health information and facilities online.
- ❖ A web services (synchronous and asynchronous) portal for communication. This portal is a one-stop shop that provides web services such as Electronic Mail, Short Message Services (SMS), and Multimedia Message Services (MMS) to foster communication in Dwesa.

It is evident, from the findings above, that the concept of deploying WiFi hotspots in urban areas, airports and hotels can be extended to rural areas. Coupling WiFi and WiMAX has made the delivery of convenient and affordable broadband connectivity a reality for rural communities in South Africa. This project has lead the way for major investments using ICT in marginalized regions, with most of the projects initiated involving Dwesa community members. In the next section of this chapter, the research questions posed in Section 1.2 of the thesis are revisited and answered.

7.2 Research Question Resolutions

In brief, the research questions outlined in Section 1.2 are answered in the same order in which they were first presented, and in accordance with the full scope of this research:

- ***What type of information pertaining to rural areas should be acquired prior to planning a wireless network?***

Prior to deploying wireless telecommunication for rural areas, network planners need to take into consideration various elements pertaining to rural communication. As elaborated in Chapter Two, this information includes the rural environment and an in-depth understanding of barriers to the deployment of telecommunication services in rural areas. In this research, relevant

information was collected through cross literature analysis, observations and oral interviews (Section 5.3) with the rural inhabitants and via community interaction during regular field trips in order to acquire vital information regarding the most important requirements for wireless communications.

- ***Which access technologies can be merged so as to deploy a cost effective, ubiquitous and reliable wireless network suitable for rural areas?***

In this research, coupling WiFi and WiMAX was reckoned the best choice after investigating various access technologies (Chapter Three). This was done in an attempt to determine and select the most cost effective, reliable and constantly available technology. The case study approach (Section 2.4) was critical as well because it helped in identifying related wireless telecommunication networks. A high level of awareness of all the appropriate wireless technologies that can be deployed in rural areas, and the criteria for choosing the most appropriate for a particular research area, has to be taken into account as explained in Chapter Three. Table in Chapter Three, shows a qualitative comparison of various access technologies, which made the selection of appropriate technologies for this project simpler. This step is vital when planning wireless telecommunication for rural areas. Various network performance tests (Section 6.1) were conducted on the WiMAX DAN first, so as to determine the reliability, throughput and latency of the node.

- ***How best can the deployed wireless network be managed for effective utilization in rural areas taking into consideration the method of accessing network resources?***

For a wireless network to be effective, reliable, ubiquitous and secure, access to it has to be controlled. In this research, through the implementation of a ChilliSpot access controller, the network resources were effectively managed. This was achieved through requesting authentication prior to accessing the Internet, as elaborated in Section 6.2.2. This avoids the abuse of network resources by unauthorized users. As can be ascertained from Chapter Four, wireless telecommunication security is vital and has to be given high priority. However, the network performance tests that were conducted (Section 6.1) showed that the ChilliSpot access controller creates high latency and increased packet delay in the network.

- ***Do these innovations and outcomes contribute to improving the social and cultural livelihoods of people in rural areas?***

Yes, they do contribute both socially and culturally, as elaborated in Section 6.3.1(b). The responses gained from the questionnaire show the various communications applications that are commonly used by Dwesa community members. These applications are mainly social networking and communications applications which make information distribution within the community simpler. Again, having a craft centre within the coverage zone is anticipated to benefit the community with viewing their sales whilst at the centre. This would save them time. This research aimed to provide the ICT industry with information related to the deployment of wireless telecommunication networks in rural areas. However, this research (Section 6.2.5) showed that the addition of WiFi hotspots into the SLL network does not affect the Internet and resource usage. The allocated bandwidth of 3G is still sufficient enough and there is no need to increase the bandwidth at present.

7.3 Limitations

This research focused primarily on deploying WiFi as user access technology and WiMAX as the backbone. The research did not go into detail regarding the investigation of ways of providing services across WiMAX and WiFi networks when users move between them. Unfortunately, this was impossible to accomplish because it required multi-mode subscriber devices that can communicate on both WiMAX and WiFi networks. Continual network failure and time constraints limited the completion of some of the experiments.

7.4 Future Work

Integrating various wireless access technologies has proved to be the solution to delivering convenient and affordable broadband connectivity for rural areas. As a result, it is recommended that an investigation into new versions of WiFi i.e. IEEE 802.11n and 802.16e-2005 Mobile WiMAX, which employs MIMO antenna mechanisms and can share the same antennas be performed, in conducted. This reduces component costs. Furthermore, an investigation of the evaluation of Internet usage after users become accustomed to the usage of WiFi hotspots is

critical. This information is vital for future network planning purposes and bandwidth allocation for the SLL network.

8 References

Agbinya, J. I. 2003. *Principles of communication networks*. Dept. of Computer Science, University of the Western Cape.

Andersson, C. 2001. *GPRS and 3G Wireless applications*. John Wiley and Son, New York.

Andrew, A. Vladimirov, K.V. Gavrilenko, A.A. 2004. *Wi-Foo: The Secrets of Wireless Hacking,* Pearson/ Addison Wesley, Boston.

Arif, A.A. 2001. *Learning from the Web: are students ready or not?* Educational Technology & Society, Citeseer Publishers, vol. 4.

Arjona, A. Takala, S. 2007. *The Google Muni Wifi Network--Can it Compete with Cellular Voice?* Telecommunications, AICT 2007, The Third Advanced International Conference, vol. 17.

Bagayoko, C.O. Muller, H. Geissbuhler, A. 2006. *Assessment of Internet-based tele-medicine in Africa (the RAFT project),* Computerized Medical Imaging & Graphics, Elsevier, vol. 30.

Baghaei, N. Hunt, R. 2004. *Review of quality of service performance in wireless LANs and 3G multimedia application services,* Computer Communications, vol. 27.

Bellotti, F. Gloria, A. D. Grosso, D. Noli, L. 2001. *WLESS-frame: a simulation-based development environment for 802.11 stations,* Computer Networks, vol. 36.

Beltrame, 2007. ChilliSpot Website, *Authentication Web server*. Available At: http://www.chillispot.info/features.html (accessed 16 March 2010).

Best, M. 2003. *The Wireless Revolution and Universal Access*. Trends in Telecommunications Reform Journal, vol. 1.

Bocquier, P. 2005. *World Urbanization Prospects: an alternative to the UN model of projection compatible with the mobility transition theory*, Demographic Research Journal,vol.12.

Borsos, K. 2004. *Economic issues of telecommunication development in Hungary*, IEEE Journal on Selected Areas in Communications, vol.12.

Brown, M. 2004. *Topology management in rooftop wireless networks*, School of Computing and Mathematical Sciences, University of Waikato.

Cavaye, J. Lawrence, G. 2000. *Regional and Rural Development – Fulfilling a Partial Approach, Keynote address*, SEGRA Conference, Ballarat, Victoria.

Computer Science Corporation. 2005. *Converged Networks*, article, CSC press release. (accessed on 2 January 2010).

Conradie, D. P. Morris, C. Jacobs, S.J. 2003. *Using information and communication technologies (ICTs) for deep rural development in South Africa*, Communication, Routledge, vol.29.

Corrocher, N. Ordanini, A. 2002. *Measuring the Digital Divide: a Framework for the Analysis of Cross-Country Differences.* Journal of Information Technology, vol. 17.

Csaki, C. de Haan, C. 2003. *Reaching the Rural Poor: A Renewed Strategy for Rural Development*. World Bank Publications.

Dandona, L. Dandona, R. Shamanna, B.R. Naduvilath, T.J. Rao, G.N. 2010. *Developing a model to reduce blindness in India: the International Centre for Advancement of Rural Eye Care*, Indian Journal of Ophthalmology, Medknow, vol. 46.

Di Lieto, A. De Falco, M. Campanile, M. Torok, M. Gabor, S. Scaramellino, M. Schiraldi,

P. &Ciociola, F. (2008). *Regional and international prenatal telemedicine network for computerized antepartum cardiotocography*, Journal of Telemedical Health, vol. 14,

Dostert, K. 2001. *Powerline Communications*. Prentice-Hall Inc, Upper Saddle River.

Esmailzadeh, R. 2006. *Broadband wireless communications business: An introduction to the costs and benefits of new technologies*. John Wiley and Sons, West Sussex.

Foldoc ,2005, *The free online dictionary of computing. Ping online computer dictionary*. Available from: http://foldoc.org/?query=ping&action=Search (accessed March 2010).

Goth, G. 2005. *Digital-divide efforts are getting more attention*, Journal of IEEE Internet Computing Conference, NJ, USA, vol. 9

Gumaste, A. Antony, T. 2004. *First Mile Access Networks and Enabling Technologies*. 800 East 96th Street, Indianapolis, IN 46240 USA: Cisco Press.

Halonen, T, Romero, J Melero, J, 2003. *GSM, GPRS and EDGE Performance: evolution towards 3G/UMTS*, Second Edition, John Wiley and Sons, The Atrium, Southern Gate, Chichester, West Sussex .

Hasan, J. 2006. *Security Issues of IEEE 802.16 (WiMAX)*. School of Computer and Information Science, Edith Cowan University, Australia, Citeseer Publishers.

Hawkins, R. 2002. *Ten lessons for ICT and education in the developing world*. The Global Information Technology Report 2001- 2002, Citeseer Publishers.

Heeks R, 2005a. *ICT and the MDGs: on the wrong track?* I4D, vol. 3.

Heeks R, 2005b. WSIS: *What did it achieve for ICTs and development?* DIG e-Development Briefing, IDPM, Manchester vol.11.

Herselman M.E. 2003. *ICT in Rural Areas in South Africa*, Informing Science and Information Technology Conference Proceedings, Pori, Finland, Citeseer Publishers.

Huggins, R. 2002. *The Digital Divide and ICT Learning in Rural Communities: Examples of Good Practice Service Delivery, Local Economy*, Taylor & Francis, vol. 17.

InfoDev/ARD/SASKI, (2007) *Using Information and Commmunication Technologies (ICT) to support Rural Livelihoods: Evidence, Strategies, Tools. A Workshop for World Bank* Staff June 5, 2007. Available from: *http://www.infodev.org/livelihoods*. (accessed 10 April 2011).

Internet World Stats, 2009. *South Africa, Internet Usage and Marketing Report*. Available At: http://www.internetworldstats.com/ (accessed 16 March 2010).

Jacobs, S. J. Herselman, M. E. 2006. *Information Access for Development: A Case Study at a Rural Community Centre in South Africa*, Informing Science and Information Technology Conference Proceedings, Manchester, England, vol. 3.

Jung, J.Y. Qiu, J.L. Kim, Y.C. 2001. *Internet Connectedness and Inequality: Beyond the 'Divide'*, Communication Research, vol. 28.

Karygiannis, T. Owens, L. 2002. *Wireless Network Security 802.11, Bluetooth and Handheld Devices*, The National Institute of Standard and Technology Special Publication 800-48, Technology Administration U.S. Department of Commerce.

Kovács, F.; Török, M. &Hábermajer, I. (2000*). A rule-based phonocardiographic method for long-term fetal heart rate monitoring,* Proceedings of *IEEE Trans. Biomed Conference.* London, England

Kozma, R. B. 2003. *Technology and Classroom Practices: An International Study.* Journal of Research on Technology in Education, International Society for Technology in Education, vol. 36.

Lee, Y.Y. Chen, I. Y. Kuo, S.Y. Liu, H.H. Leu, Y.R. 2008. *Implementation of OpenWrt-based IP PnP gateway*, Proceedings of the International Conference on Mobile Technology, Applications, and Systems, ACM.

Löcher, J. 2002. *Survey of the present-day state of the power line telecommunication, PLT technology*, Proceedings of the IEEE postgraduate Conference in Budapest, Hungary.

Lu, J. H. Chuang, J. C. I. 2006. *Wireless networking architecture and signaling for rapid deployment of rural communications.* Proceedings of the International Conference on Communication Technology, vol. 2.

Makitla, I. Makan, A. Roux, K. 2010. *Broadband provision to underprivileged rural communities*, CSIR 3rd Biennial Conference, CSIR.

Mandioma, M. Rao, K. Terzoli, A. Muyingi, H. 2006. *A Feasibility Study of WiMax Implementation at Dwesa-Cwebe Rural Areas of Eastern Cape of South Africa*, Proceedings of the IEEE TENCON Conference, Hong Kong, China.

Mandioma, M. Terzoli, A. Muyingi, H. 2007. *Rural Internet Connectivity: A Deployment in Dwesa-Cwebe, Eastern Cape, South Africa*. Master's thesis, University of Fort Hare.

Marine, S. Blanchard, J. M . 2004. *Bridging the digital divide: An opportunity for growth for the 21st century,* Alcatel Telecommunications Review. ALCATEL

Matsunaga, Y., et al. 2003. *Secure Authentication System for Public WLAN Roaming*. WMASH.

Matthee, K. Mweemba, G. Pais, A. V. Rijken, M. van Stam, G. 2007. *Bringing connectivity to rural Zambia using a collaborative approach.* Information and Communication Technologies and Development, 2007. ICTD 2007, IEEE International Conference.

Mishra, A. Arbaugh, W. A. 2002. *An initial security analysis of the ieee 802.1x standard*. Technical Report CS-TR-4328, University of Maryland.

Morrow, R. 2004. *Wireless network coexistence*. 1st edition, McGraw-Hill, New York.

Mujinga M (2005): *IPSec Traffic Overhead Analysis in Dual Stack IPv4/IPv6 Transition Mechanisms,* Msc Computer Science Thesis, University of Fort Hare.

Ndlovu, N. Thinyane, M. Terzoli, A. 2009. *Deployment and Extension of a Converged WiMAX/WiFi Network for Dwesa Community Area South Africa*. Proceedings of SATNAC 2009 Conference, Royal Swazi Spa, Swaziland.

Ndlovu, N. Thinyane, M. 2010a. *Investigating wireless network deployment configurations for rural marginalized areas (Dwesa Case Study).* Proceedings of ZAWWW-2010 Conference, UKZN, Durban, South Africa.

Ndlovu, N. Dumani, K. Hlungulu, Ngwenya, S. Samalenge, J. Thinyane, M. Terzoli, A. 2010b. *Technology Solutions to Strengthen the Integration of Marginalized Communities into the Global Knowledge Society (Dwesa Case Study).* Proceedings of IST-Africa, 2010 Conference, ICC, Durban, South Africa.

Ndlovu, N. Jere, N. 2010c. *Wireless Network Deployment Configurations: Dwesa Marginalized Area as a Case Study.* Proceedings of SAICSIT 2010 Conference, Bela Bela, South Africa.

Ngwenya, S. Thinyane, M. Terzoli, A. 2009. *Internet Charging schemes for ICT4D projects*. Proceedings of the 12th Annual conference on World Wide Web applications, University of Kwazulu Natal, 21-23 September 2010, Durban, South Africa.

Paton, S. 2003. *What Comes First, the Emu or the Egg? The Essential Interconnection between Healthy Rural and Remote Communities and a Healthy Landscape,* National Landcare Conference, Darwin.

Ramani, K. V. Mavalankar, D. 2006. *Health system in India: opportunities and challenges for*

improvements. Journal of Health Organization and Management. Emerald Group, vol. 20.

Rashid, A. T. Elder, L. 2009. *Mobile phones and development: An analysis of IDRC supported projects*, The Electronic Journal of Information Systems in Developing Countries, vol.36.

Rhyn, P. 2005. *Origins of Satellite Communication Satellite Communication and VSAT, Quantum's Demystifying Satellite Communications*, APRESS, 2006.

Senior, J. M. 1992. *Optical Fibre communications*: Principles and Practice, 2nd ed. Prentice-Hall, UK.

Scholz, G. R. Grumman, N. 2002. *An architecture for securing wireless networks.* The Internet Protocol Journal (IPJ), vol. 5.

Servon, L. 2002. *Bridging the Digital Divide: Technology, Community and Public Policy*, USA, Blackwell.

Smith, R. 2000. *Overcoming Regulatory and Technological Challenges to Bring Internet Access to a sparsely populated, Remote Area: A case study.* First Monday Journal, vol. 5.

Spanbauer, S. 2001. *5 Reasons we (still) love Dial-up*. PC World, New York.

Stanley, D. Walker, J. Aboba, B. 2005. *Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs*. RFC4017, March Published as IETF.

Stanton, R. 2005. *Securing VPNs: comparing SSL and Ipsec.* Computer Fraud & Security.

Surana, S. Patra, R. Nedevschi, S. Ramos, M. Subramanian, L. Ben-David, Y. and Brewer, E. 2008. *Beyond pilots: keeping rural wireless networks alive,* Proceedings of the 5th USENIX symposium on networked systems design and implementation, USENIX Association.

Sweeny, D. 2004.*WiMAX operators manual: Building 802.16 Wireless Networks.* 2560 Ninth street, Suite 219, Berkley, CA 94710: Apress.

Tongia, R. 2004. *Can broadband over powerline carrier (PLC) compete?* A techno-economic Analysis Telecommunications Policy, vol. 28.

Tracey, P. Phillips, N. 2007. *The distinctive challenge of educating social entrepreneurs: A postscript and rejoinder to the special Issue on entrepreneurship education*, Academy of Management Learning and Education, ACADEMY OF MANAGEMENT, vol 6.

Van Hoorik. P. Mweetwa F. 2007. *Use of Internet in rural Zambian areas*. Proceedings of the International Symposium on Sustainable Solutions with focus in Africa. Delft University.

Vines, R. D. 2002. *Wireless Security Essentials: Defending Mobile Systems from Data Piracy.* USA: Wiley.

Wang, J. Du, H. 2005. *Setting up a Wireless Local Area Network (WLAN) for a healthcare system*, International Journal of Electronic Healthcare, Inderscience, vol. 1.

Wellenius, B. 2002. *Closing the Gap in Access to Rural Communication: Chile 1995-2000*, info Journal, MCB UP Ltd. vol. 4.

Wertlen, R. R. 2007. *An Overview of ICT Innovation for Developmental Projects in Marginalised Rural Areas*, Citeseer Publishers.

Westerveld, R. 2004. *Cost effective rural communications using fixed cellular radio access*. B. Kiplagat and M. Werner (Eds.) Telecommunications and Development in Africa, Amsterdam: IOS Press.

William, De M. 2008. *Cross Cultural Trespass Assessing African Anti-corruption Capacity*, International Journal of Cross Cultural Management, vol. 8.

Wong, K. L. Chou, L. C. 2006. *Internal composite monopole antenna for WLAN/WiMAX operation in a laptop computer*, Microwave and Optical Technology Letters, Wiley Online Library, vol. 48.

Yu, S. N. Cheng, J. C. 2006. *A wireless physiological signal monitoring system with integrated bluetooth and WiFi technologies*, Engineering in Medicine and Biology Society, 27th Annual International Conference of the IEEE-EMBS

Zhang, J., et al. 2002. *Virtual Operator based AAA in Wireless LAN Hotspots' with Ad-hoc Networking Support*. Mobile Computing and Communications Review, vol. 6.

Zhira, M. 2008. *Uncovering the Reality of State Violence in Western Zimbabwe*. Past Imperfect, vol. 10.

9 Appendix A - Program Listings

1. The Ping Test Program

This program was used to ping another computer on a network. This was done so as to obtain data about the latency and reliability between the two computers on the network.

```
#!/usr/bin/perl -w
#ping.pl is a program used for performing ping test
use strict;
my $dst = $ARGV[0];
my $date = `/bin/date`; # this instruction fetches the date
chomp($date);
my $output = `/sbin/ping -c 10 -q $dst`; #this instruction sends the ping packets and
#records the output of ping and saves to appropriate variable
my ($received, $min, $avg, $max, $stddev);
if ($output =~ m/, (\d+) packets received/) {
        $received = $1;
        if ($output =~ m# = ([\d\.]+)/([\d\.]+)/([\d\.]+)/([\d\.]+) ms#) {
                $min = $1;
                $avg = $2;
                $max = $3;
                $stddev = $4;
        }
}
else {
        $received = $min = $avg = $max = $stddev = 0;
}
printf("%s,%d,%f,%f,%f,%f\n", $date, $received, $min, $avg, $max, $stddev);
```

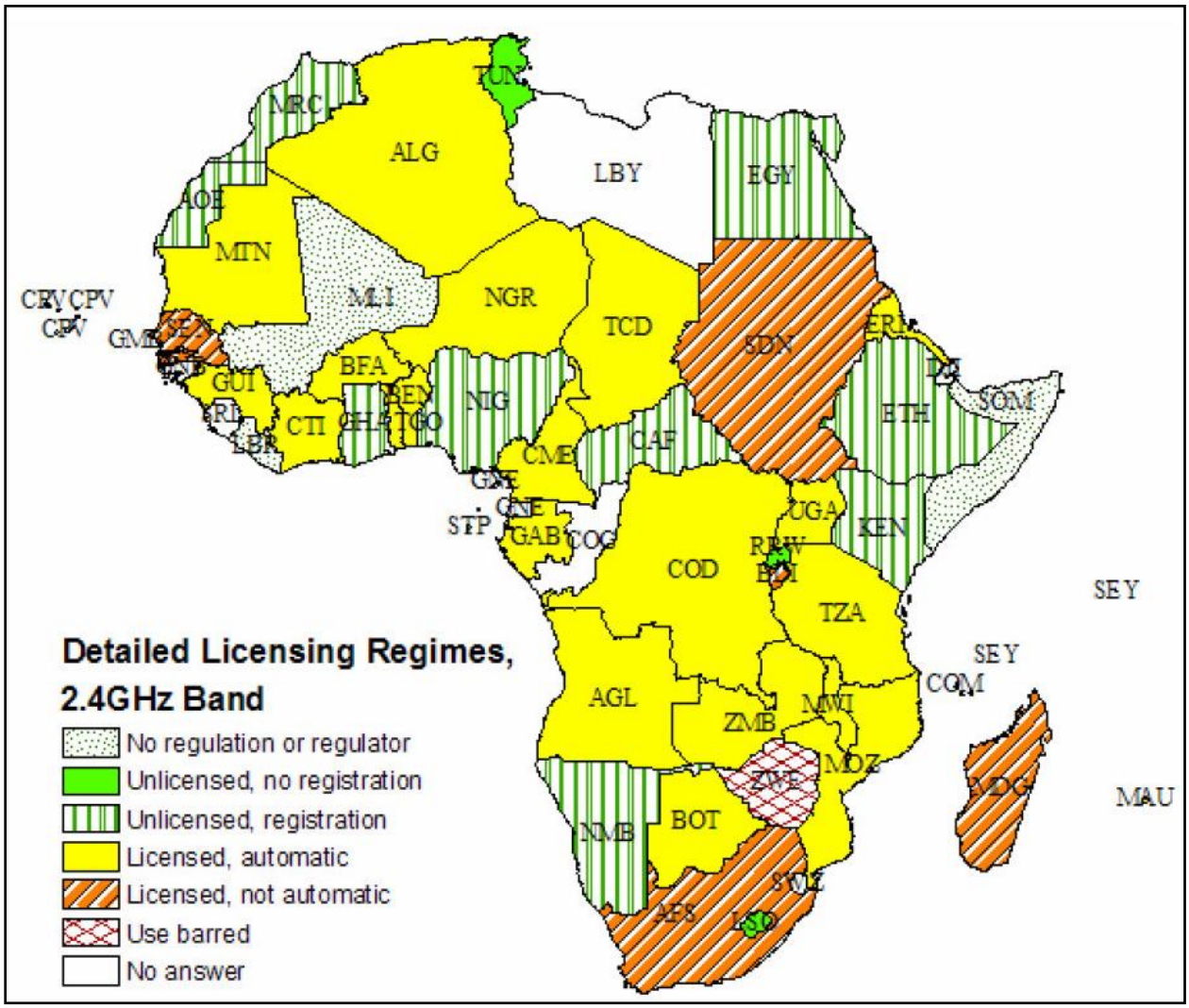
2. The Transfer Test Program

The transfer test was done to test data transfer from one machine to another over a network. The test was conducted so as to obtain data about the available throughput and reliability of the network.

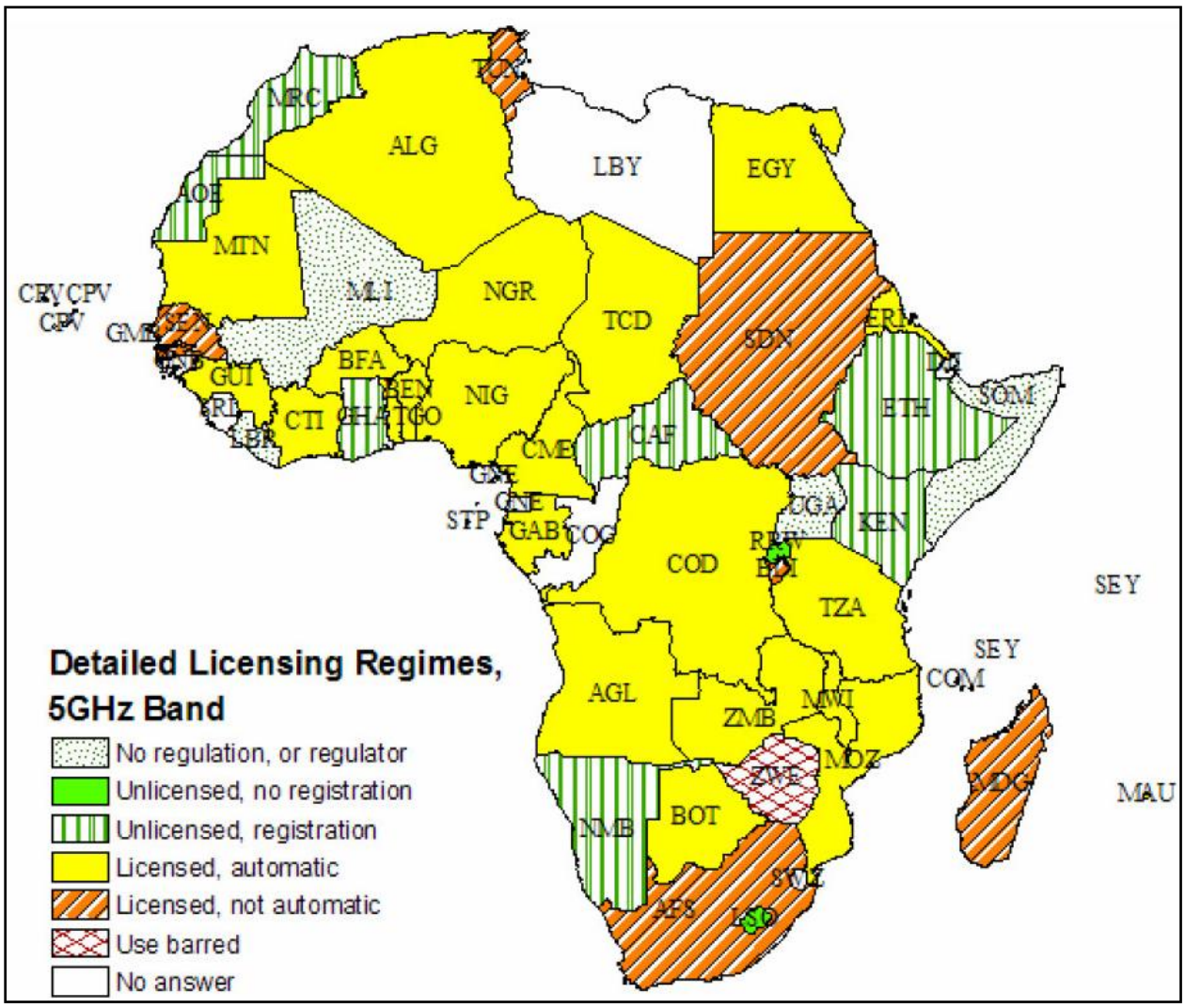
```
#!/usr/bin/perl -w
# transfer.pl is the program used to transfer files
use strict;
my $url = 'http://172.20.56.62/~kaizer/transferdata';
my $date = `/bin/date`;
chomp($date);

#fetches the test file from the url and records the time it took to do so
#this file is run by cron and cron pipes the results of the script to a csv
#file which can be used to calculate throughput later on

my $output = `/usr/bin/time /usr/bin/fetch -qd $url 2>&1`;
my $real;
if ($output =~ m/\s([\d\.]+)\sreal/) {
        $real = $1;
}
else {
        $real = 0;
}
printf("%s,%f\n", $date, $real);
```

10 Appendix B - Wireless Regulations in Africa

The two maps below show the licensing regulations for different African countries with respect to the 2.4 and 5GHz bands. Significant diversity in terms of wireless regulations exists across the African continent, as shown by these maps.



Map of licensing regimes – detailed categories for the 2.4GHz Band



Map of licensing regimes – detailed categories for the 5GHz Band

Countries which use the 2.4GHz and 5GHz both require a registration to be done prior to use. This is shown, in the Figures above, where we see 15% of the countries using the 5GHz and 19% using the 2.4GHz allowing unlicensed use only if one has registered. However, there are exceptions such as Rwanda, Lesotho and Tunisia which have all adopted the USA style which requires no license or registration.

Source: Licence-Exempt Wireless Policy: Results of an African Survey, Isabel Neto,

http://www.inta.gatech.edu/michael_best/wireless.pdf

11 Appendix C - Hotspot Testing

1. General Hotspot Experiments

Association to AP:	SSID:	MJSS	NHS	NJSS	MTJSS	NPS
		mpume	nqabara	ngwane	mtokwane	nondobo
	SSID Broadcast:	Yes				

	Approx. Distance	Speed
General Network Coverage:	10 metres	11 Mbps
	105 metres	11 Mbps
Channel:	6	
IP Address: e.g. association to MJSS AP	192.168. 1.50	
DNS Address:	10.0.0.0/8	
Default Gateway:	192.168.1.1	
Subnet mask:	255.255.255.0	
Access to internet: http://www.dwesa.org/	Yes, had to authenticate first	
Access to secure web service: https://webmail.ufh.ac.za/	Ok, was able to check emails	
Connect to Google Talk chat:	Yes	

2. ChilliSpot Based Experiments

Welcome page is displayed on first visiting ChilliSpot site:	Yes
Successful Login	Yes
Failed Login – Invalid Password:	Error message indicating incorrect password is displayed.
Failed Login – Invalid Username:	Error message indicating incorrect username is displayed.

Failed Login – Missing username / password:	Error message referring to missing username / password is displayed.
Failed Login – Both username and password missing:	Error message indicating missing username and password is displayed.
Logout:	OK, returns to welcome screen
Help – Logged out:	Relates to Logged out only
Help – Logged in:	Relates to Logged in only
Settings Displayed:	On first starting and when clicking
Locations can be inserted:	Yes, and Insert detected works
Username change:	OK – *ndlovu*
Password change:	OK – *wireless*
Gateway Settings viewed:	Yes
Gateway Settings refreshed:	Yes, no update
Gateway Settings displayed for editing	Yes
User Accounts displayed if using DBI and MySQL:	Yes – MySQL running locally
Account can be added:	Yes – matwayi added
Account can be edited:	Yes – matwayi changed to skura
Detected Settings can be inserted:	Yes
Homepage can be visited:	Yes – http://www.chillispot.info/chilliforum
Account can be deleted:	Yes – nobert removed
Gateway Settings viewed:	Yes
Gateway Settings displayed for editing:	Yes
ChilliSpot can be restarted	Yes
ChilliSpot can be stopped	Yes

Use Cases

1. **General Configuration:**
   a) Log into ChilliSpot with the credentials:
      I. username: *matwayi*
      II. password: *k@izer*
   b) Select the settings option
   c) Configure Gateway and RADIUS server
   d) Save changes
   e) Select View Gateway Settings
   f) Select View RADIUS server Settings
   g) Log out of ChilliSpot

2. **Advanced Gateway Configuration:**
   a) Log into ChilliSpot with the credentials:
      I. username: *matwayi*
      II. password: *k@izer*
   b) Select Edit Gateway Settings
   c) Change the Setting GatewayName to: siyakhula
   d) Change the Setting HomePage to: http://www.gmail.com
   e) Save changes
   f) Select Control ChilliSpot
   g) Click the Re-start button
   h) Log out of ChilliSpot

3. **Advanced RADIUS Configuration:**
   a) Log into ChilliSpot with the credentials:
      I. username: *matwayi*
      II. password: *k@izer*
   b) Select Edit RADIUS Settings
   c) Change the Setting HomePage to: http://www.yahoo.com

d) Change the LoginGreeting to: Welcome to Dwesa captive portal

e) Save changes

f) Select Control ChilliSpot

g) Click the Re-start button

h) Log out of ChilliSpot

4. Add user:

a) Log into ChilliSpot with the credentials:

I. username: *matwayi*

II. password: *k@izer*

b) Select User Accounts

c) Click Add a user

d) Add a new user with the credentials:

I. Username: *ndlovu*

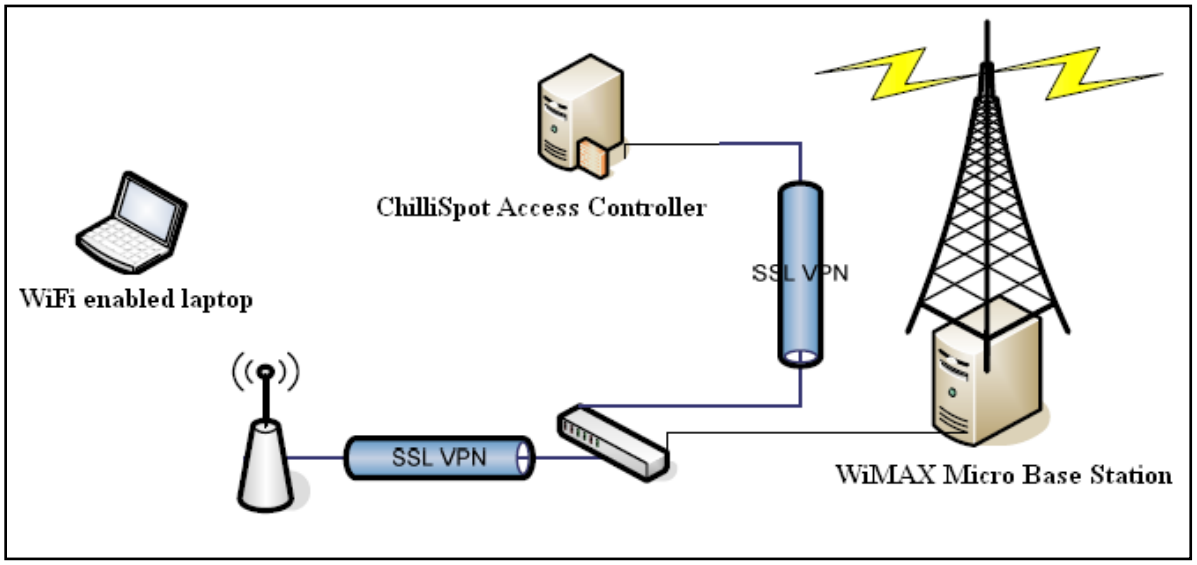
II. Password: *wireless*

III. Name: Hotspot_Testing

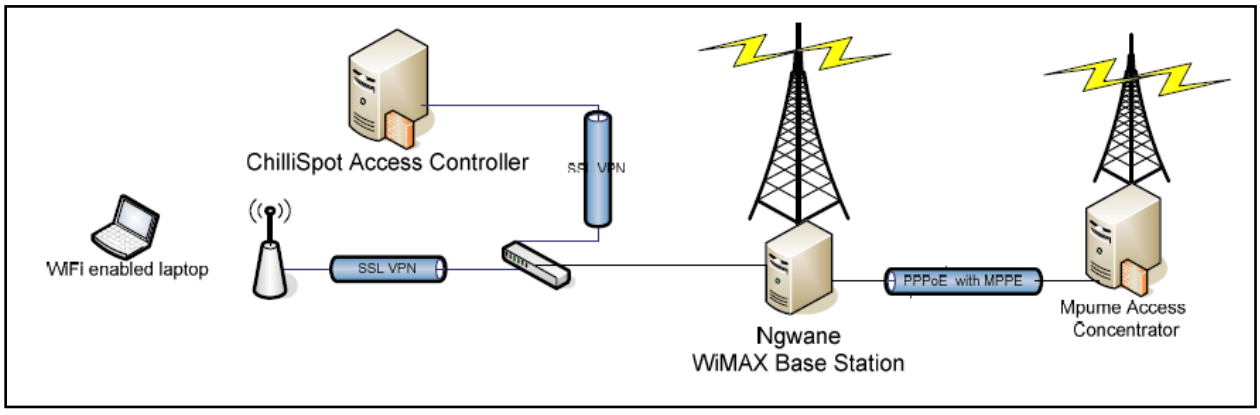
e) Save changes

f) Log out of ChilliSpot

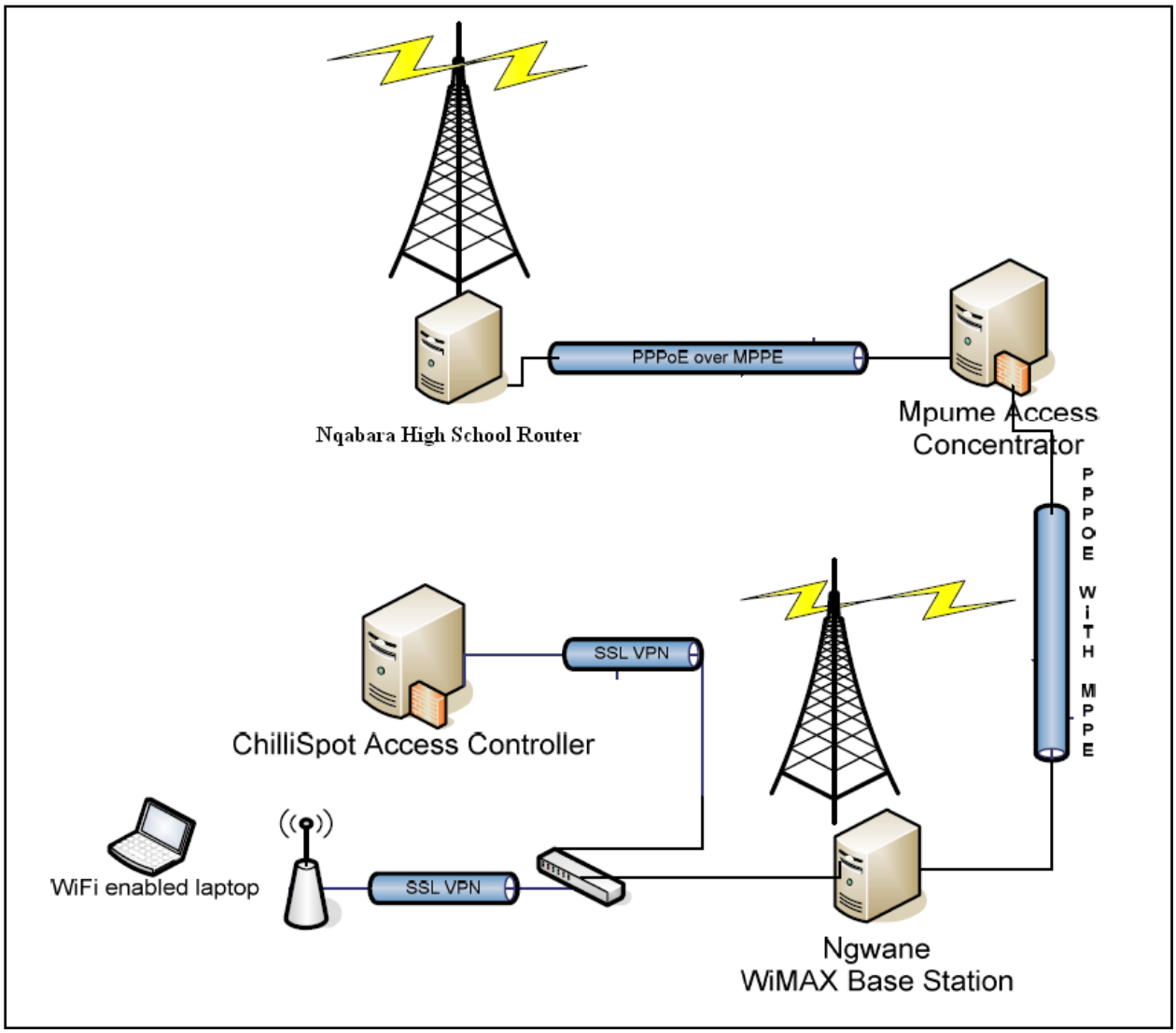
12 Appendix D - Network Topologies for the Conducted Tests



i. A network topology for two wireless clients on the NJSS WLAN.



ii. A network topology for MJSS Access Concentrator (AC) and the wireless client at NJSS.



iii. A network topology for a wireless client at NJSS and a router at NHS.

13 Appendix E - Statistical Analysis of Internet Usage

T-Test Distribution

GET DATA /TYPE=XLSX /FILE='\\al-tsc-cl01-fs\NNdlovu$\KAIZER.xlsx' /SHEET=name 'Sheet1' /CELLRANGE=full /READNAMES=on /ASSUMEDSTRWIDTH=32767. T-TEST PAIRS=A2010 WITH B2011 (PAIRED) /CRITERIA=CI (.9500) /MISSING=ANALYSIS.

Notes

	Output Created	20-Jul-2011 10:32:21
	Comments	
Input	Active Dataset	DataSet1
	Filter	<none>
	Weight	<none>
	Split File	<none>
	N of Rows in Working Data File	6
Missing Value Handling	Definition of Missing	User defined missing values are treated as missing.
	Cases Used	Statistics for each analysis are based on the cases with no missing or out-of-range data for any variable in the analysis.
	Syntax	T-TEST PAIRS=A2010 WITH B2011 (PAIRED) /CRITERIA=CI(.9500) /MISSING=ANALYSIS.
Resources	Processor Time	0:00:00.031
	Elapsed Time	0:00:00.125

[DataSet1]

Paired Samples Statistics

		Mean	N	Std. Deviation	Std. Error Mean
Pair 1	A2010	9.600000	6	6.4395652	2.6289415
	B2011	25.216667	6	21.8711149	8.9288453

Paired Samples Correlations

		N	Correlation	Sig.
Pair 1	A2010 & B2011	6	.556	.252

Paired Samples Test

		Paired Differences		
		Mean	Std. Deviation	Std. Error Mean
Pair 1	A2010 - B2011	-15.6166667	19.0553317	7.7793066

Paired Samples Test

		Paired Differences				
		95% Confidence Interval of the Difference				
		Lower	Upper	t	df	Sig. (2-tailed)
Pair 1	A2010 - B2011	-35.6140109	4.3806776	-2.007	5	.101

Daily Usage Statistics

Year: 2010

Your Volume Cap is set at 3G bytes
You have used 8.3% of your Capping Limit

Cumulative Totals for January 2010

Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined Transfer
1036800	219.6M	28.41M	248.01M

Daily Totals for January 2010

Date	Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined (Bytes)
29-JAN-10	32566	1 020.43K	352K	1.34M
28-JAN-10	82708	32.31M	3.4M	35.7M
27-JAN-10	86550	4.24M	1.36M	5.6M
26-JAN-10	86427	57.35M	9.87M	67.22M
25-JAN-10	57349	6.35M	1.15M	7.51M
23-JAN-10	32574	0	0	0
22-JAN-10	79186	4.13M	818.88K	4.93M
21-JAN-10	61040	72.32K	40.28K	112.61K
20-JAN-10	36225	2.28M	506.21K	2.78M
19-JAN-10	75526	6M	1.16M	7.16M
18-JAN-10	61049	12.42M	1.75M	14.17M
17-JAN-10	68628	286.02K	319.62K	605.64K
16-JAN-10	46819	0	0	0
15-JAN-10	57353	29.56M	1.63M	31.2M
14-JAN-10	29035	1.17M	350.56K	1.51M
13-JAN-10	86165	8.35M	1.48M	9.83M
12-JAN-10	57600	21.46M	2.77M	24.23M

<< back 1 month forward>>

Your Volume Cap is set at 3G bytes
You have used 40.1% of your Capping Limit

Cumulative Totals for February 2010

Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined Transfer
1296000	1.07G	112.69M	1.18G

Daily Totals for February 2010

Date	Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined (Bytes)
27-FEB-10	36282	0	0	0
26-FEB-10	78964	17.04M	4.53M	21.57M
25-FEB-10	86571	27.91M	5.36M	33.27M
24-FEB-10	57383	73.27M	3.84M	77.11M
23-FEB-10	36039	731.2K	147.08K	878.28K
22-FEB-10	50361	64.6M	3.07M	67.67M
20-FEB-10	32412	0	0	0
19-FEB-10	53988	49.5K	62.84K	112.34K
17-FEB-10	36246	762.18K	164.23K	926.41K
16-FEB-10	82841	24.03M	2.42M	26.45M
15-FEB-10	53713	77.4M	12.41M	89.81M
12-FEB-10	36276	969.05K	346.08K	1.28M
11-FEB-10	82717	64.46M	10.06M	74.52M
10-FEB-10	82696	67.25M	10.58M	77.83M
09-FEB-10	86350	248.9M	14.34M	263.24M
08-FEB-10	57561	135.89M	12.76M	148.64M
06-FEB-10	50507	0	0	0
05-FEB-10	82817	60.29M	10.43M	70.72M
04-FEB-10	82718	98.51M	68.93M	109.25M
03-FEB-10	86465	114.96M	9.7M	124.66M
02-FEB-10	43093	8.49M	1.17M	9.67M

<< back 1 month forward>>

Your Volume Cap is set at 3G bytes
You have used 54.5% of your Capping Limit

Cumulative Totals for March 2010

Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined Transfer
1131266	1.44G	166.38M	1.6G

Daily Totals for March 2010

Date	Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined (Bytes)
27-MAR-10	29056	0	0	0
26-MAR-10	86261	1.3M	275.8K	1.57M
25-MAR-10	57483	266.28M	17.64M	283.92M
24-MAR-10	28880	100.03M	45.6M	145.63M
23-MAR-10	57893	168.06M	14.59M	182.66M
20-MAR-10	28914	0	0	0
19-MAR-10	86301	1.92M	459.8K	2.37M
18-MAR-10	57585	39.67M	7.59M	47.25M
12-MAR-10	39679	36.93M	5.91M	42.84M
11-MAR-10	79371	127.19M	12.92M	140.11M
10-MAR-10	86185	491.05M	23.72M	514.77M
09-MAR-10	86405	28.4M	4.49M	32.9M
08-MAR-10	82869	43.9M	6.91M	50.81M
07-MAR-10	57491	0	0	0
05-MAR-10	39859	35.78M	4.75M	40.53M
04-MAR-10	82662	44.51M	5.42M	49.93M
03-MAR-10	79335	67.12M	10.62M	77.74M
02-MAR-10	57344	51.63M	9.67M	61.31M
01-MAR-10	7693	1.9M	593.8K	2.48M

<< back 1 month forward>>

Your Volume Cap is set at 3G bytes
You have used 24.8% of your Capping Limit

Cumulative Totals for April 2010

Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined Transfer
2066442	638.33M	106.05M	744.38M

Daily Totals for April 2010

Date	Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined (Bytes)
30-APR-10	209121	5.72M	957.8K	6.66M
29-APR-10	259317	40.65M	5.7M	46.35M
28-APR-10	222883	62.56M	14.68M	77.24M
27-APR-10	172705	0	0	0
26-APR-10	172846	0	0	0
25-APR-10	173093	0	0	0
24-APR-10	172463	0	0	0
23-APR-10	208790	0	0	0
22-APR-10	190662	265.59M	36.06M	301.65M
21-APR-10	75663	92.78M	19.76M	112.55M
20-APR-10	82902	128.57M	21.62M	150.19M
19-APR-10	39597	17.58M	2.33M	19.91M
16-APR-10	29022	0	0	0
15-APR-10	57378	24.89M	4.95M	29.84M

<< back 1 month forward>>

Your Volume Cap is set at 3G bytes
You have used 23.8% of your Capping Limit

Cumulative Totals for May 2010

Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined Transfer
7134974	620.84M	92.47M	713.3M

Daily Totals for May 2010

Date	Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined (Bytes)
31-MAY-10	223030	27.24M	5.17M	32.41M
30-MAY-10	230913	0	0	0
29-MAY-10	255398	0	0	0
28-MAY-10	248470	3.3M	516.91K	3.8M
27-MAY-10	259135	68.53M	20.5M	89.03M
26-MAY-10	259266	96.14M	17.49M	113.63M
25-MAY-10	259037	49.86M	7.43M	57.29M
24-MAY-10	255892	70.64M	9.85M	80.49M
23-MAY-10	258980	0	0	0
22-MAY-10	259071	629.43K	85.49K	714.92K
21-MAY-10	259552	186.3K	126.8K	313.1K
20-MAY-10	258631	8.55M	1.06M	9.61M
19-MAY-10	255965	6.14M	1.11M	7.25M
18-MAY-10	259477	7.71M	1.07M	8.78M
17-MAY-10	222656	6.16M	742.44K	6.89M
16-MAY-10	172904	0	0	0
15-MAY-10	209054	0	0	0
14-MAY-10	259245	214.15M	17.23M	231.38M
13-MAY-10	255503	8.83M	1.57M	10.4M
12-MAY-10	255625	13.96M	2.25M	16.21M
11-MAY-10	258830	13.95M	1.16M	15.11M
10-MAY-10	230590	12.7M	2.84M	15.55M
09-MAY-10	172458	0	0	0
08-MAY-10	173037	0	0	0
07-MAY-10	223429	1.94M	508.08K	2.44M

Your Volume Cap is set at 3G bytes
You have used 5.3% of your Capping Limit

Cumulative Totals for June 2010

Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined Transfer
5911158	134.52M	24.85M	159.37M

Daily Totals for June 2010

Date	Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined (Bytes)
30-JUN-10	172973	0	0	0
29-JUN-10	172709	0	0	0
28-JUN-10	172758	0	0	0
27-JUN-10	172850	0	0	0
26-JUN-10	172654	0	0	0
25-JUN-10	172615	0	0	0
24-JUN-10	173061	0	0	0
23-JUN-10	172650	0	0	0
22-JUN-10	172823	0	0	0
21-JUN-10	172831	0	0	0
20-JUN-10	172595	0	0	0
19-JUN-10	172961	0	0	0
18-JUN-10	172781	0	0	0
17-JUN-10	172673	0	0	0
16-JUN-10	173029	0	0	0
15-JUN-10	172795	0	0	0
14-JUN-10	172829	0	0	0
13-JUN-10	172759	0	0	0
12-JUN-10	172557	0	0	0
11-JUN-10	172973	0	0	0
10-JUN-10	205320	0	0	0
09-JUN-10	226754	4.56M	1.29M	5.86M
08-JUN-10	215887	3.37M	745.55K	4.09M
07-JUN-10	255950	19.08M	2.96M	22.04M
06-JUN-10	259000	0	0	0
05-JUN-10	259427	157.31K	174.9K	332.21K
04-JUN-10	258872	3.96M	1.74M	5.7M
03-JUN-10	259355	18.64M	4.59M	23.23M
02-JUN-10	255669	41.95M	7.09M	49.05M
01-JUN-10	259048	42.65M	6.1M	48.75M

<< back 1 month forward>>

Year: 2011

Your Volume Cap is set at 3G bytes
You have used 0% of your Capping Limit

Cumulative Totals for January 2011

Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined Transfer
5356427	0	0	0

Daily Totals for January 2011

Date	Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined (Bytes)
31-JAN-11	172734	0	0	0
30-JAN-11	172734	0	0	0
29-JAN-11	172972	0	0	0
28-JAN-11	172522	0	0	0
27-JAN-11	172998	0	0	0
26-JAN-11	172701	0	0	0
25-JAN-11	172934	0	0	0
24-JAN-11	172425	0	0	0
23-JAN-11	173119	0	0	0
22-JAN-11	172805	0	0	0
21-JAN-11	172621	0	0	0
20-JAN-11	172830	0	0	0
19-JAN-11	172963	0	0	0
18-JAN-11	172784	0	0	0
17-JAN-11	172679	0	0	0
16-JAN-11	172829	0	0	0
15-JAN-11	172664	0	0	0
14-JAN-11	172928	0	0	0
13-JAN-11	172781	0	0	0
12-JAN-11	172686	0	0	0
11-JAN-11	172765	0	0	0
10-JAN-11	172859	0	0	0
09-JAN-11	172981	0	0	0
08-JAN-11	172707	0	0	0
07-JAN-11	172985	0	0	0
06-JAN-11	172797	0	0	0
05-JAN-11	172580	0	0	0
04-JAN-11	172849	0	0	0
03-JAN-11	173003	0	0	0
02-JAN-11	172471	0	0	0
01-JAN-11	172721	0	0	0

<< back 1 month forward>>

Your Volume Cap is set at 3G bytes
You have used 26% of your Capping Limit

Cumulative Totals for February 2011

Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined Transfer
6549246	677.18M	102.44M	779.61M

Daily Totals for February 2011

Date	Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined (Bytes)
28-FEB-11	172766	0	0	0
27-FEB-11	172965	216.94M	27.3M	244.23M
26-FEB-11	212518	1 008.4K	271.51K	1.25M
25-FEB-11	248388	1.63M	685.77K	2.3M
24-FEB-11	248258	159.61M	19.65M	179.26M
23-FEB-11	259292	202.47M	32.82M	235.29M
22-FEB-11	240858	56.74M	6.97M	63.72M
21-FEB-11	259304	20.23M	2.62M	22.85M
20-FEB-11	234395	1.29M	656.84K	1.93M
19-FEB-11	258924	1.64M	896.58K	2.52M
18-FEB-11	259435	31.75M	3.85M	35.6M
17-FEB-11	259111	754.06K	1.17M	1.9M
16-FEB-11	241769	2.58M	1.42M	4.01M
15-FEB-11	241304	49.77M	7.24M	57.01M
14-FEB-11	215955	105.99M	15.41M	121.4M
13-FEB-11	190552	0	0	0
12-FEB-11	241138	1.79K	57.51K	59.3K
11-FEB-11	259171	10.45K	471.54K	481.99K
10-FEB-11	234461	26.79M	3.25M	30.04M
09-FEB-11	237529	7.96K	352.25K	360.22K
08-FEB-11	259243	10.48K	473.26K	483.74K
07-FEB-11	237520	7.74M	1.03M	8.78M
06-FEB-11	241299	7.41K	322.8K	330.21K
05-FEB-11	259011	9.73K	472.43K	482.16K
04-FEB-11	234113	8.08K	334.46K	342.54K
03-FEB-11	251946	6.56M	1.72M	8.28M
02-FEB-11	205009	611.2K	427.55K	1.01M
01-FEB-11	173012	0	0	0

<< back 1 month forward>>

Your Volume Cap is set at 3G bytes
You have used 68.6% of your Capping Limit

Cumulative Totals for March 2011

Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined Transfer
5490247	1.81G	204.22M	2.01G

Daily Totals for March 2011

Date	Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined (Bytes)
31-MAR-11	71962	14.08M	3.04M	17.12M
30-MAR-11	86247	9.3M	2.37M	11.67M
29-MAR-11	64754	11.82M	7.57M	19.39M
28-MAR-11	68385	2.14M	669.37K	2.79M
27-MAR-11	86400	399.2K	740.48K	1.11M
26-MAR-11	86400	1.63M	713.7K	2.33M
25-MAR-11	61424	22.12M	3.73M	25.85M
24-MAR-11	68302	4.58M	810.48K	5.37M
23-MAR-11	82698	10.72M	4.13M	14.85M
22-MAR-11	65040	5.24M	3M	8.23M
21-MAR-11	68136	471.15K	630.82K	1.08M
20-MAR-11	86400	395.54K	738.71K	1.11M
19-MAR-11	227064	396.14K	616.13K	1 012.28K
18-MAR-11	255433	2.89M	716.96K	3.59M
17-MAR-11	223440	32.27M	6.55M	38.81M
16-MAR-11	259480	65.46M	11.31M	76.77M
15-MAR-11	234184	47.31M	7.08M	54.39M
14-MAR-11	258755	55.09M	6.75M	61.84M
13-MAR-11	237924	1.6M	559.29K	2.15M
12-MAR-11	259433	495.95K	722.92K	1.19M
11-MAR-11	255440	32.99M	4.2M	37.19M
10-MAR-11	259252	346.42M	16.56M	362.98M
09-MAR-11	258986	482.62M	27.78M	510.4M
08-MAR-11	241329	214.73M	24.46M	239.19M
07-MAR-11	259066	366.92M	25.4M	392.31M
06-MAR-11	240988	5.66M	6.25M	11.91M
05-MAR-11	259470	6.69M	15.09M	21.79M
04-MAR-11	258959	37.4M	15.33M	52.74M
03-MAR-11	234203	69.07M	6.6M	75.67M
02-MAR-11	197935	2.12M	267.8K	2.38M
01-MAR-11	172758	0	0	0

<< back 1 month forward>>

Your Volume Cap is set at 3G bytes
You have used 15.6% of your Capping Limit

Cumulative Totals for April 2011

Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined Transfer
1782252	400.57M	68.36M	468.93M

Daily Totals for April 2011

Date	Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined (Bytes)
30-APR-11	86400	1.58M	1 005.06K	2.56M
29-APR-11	61274	234.78K	555.14K	789.92K
28-APR-11	64847	1.72M	646.04K	2.35M
27-APR-11	64739	336.79K	614.4K	951.19K
26-APR-11	68340	688.78K	884.79K	1.54M
25-APR-11	86400	293.46K	734.78K	1M
24-APR-11	61226	396.76K	889.82K	1.26M
23-APR-11	64947	1.73M	654.22K	2.37M
22-APR-11	64777	545.96K	711.35K	1.23M
21-APR-11	86543	1.8M	896.2K	2.68M
20-APR-11	68107	107.1M	18.45M	125.55M
19-APR-11	86400	2.21M	1.08M	3.28M
18-APR-11	61239	2.62M	1.29M	3.91M
17-APR-11	43347	92.95K	219.22K	312.17K
16-APR-11	68214	427.05K	699.84K	1.1M
15-APR-11	61480	11.5M	1.03M	12.53M
14-APR-11	64781	58.24M	7.52M	65.76M
13-APR-11	86275	97.46M	16.11M	113.57M
12-APR-11	86296	26.15M	3.84M	29.99M
11-APR-11	46768	25.77M	3.39M	29.17M
06-APR-11	18094	0	0	0
05-APR-11	68306	3.91M	801.12K	4.69M
04-APR-11	86400	475.96K	807.28K	1.25M
03-APR-11	61472	8.39K	21.04K	29.43K
02-APR-11	86386	3.16M	742.2K	3.89M
01-APR-11	79194	52.19M	5.03M	57.21M

<< back 1 month forward>>

Your Volume Cap is set at 3G bytes
You have used 14% of your Capping Limit

Cumulative Totals for May 2011

Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined Transfer
2019697	345.03M	75.42M	420.45M

Daily Totals for May 2011

Date	Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined (Bytes)
31-MAY-11	86598	24.72M	3.49M	28.21M
30-MAY-11	46568	3.72M	775.62K	4.47M
29-MAY-11	18064	265.67K	0	265.67K
28-MAY-11	68336	2.03M	141.28K	2.17M
27-MAY-11	86400	7.66M	1.67M	9.34M
26-MAY-11	86400	41.24M	5.6M	46.85M
25-MAY-11	86400	36.02M	4.99M	41.02M
24-MAY-11	86400	27.02M	5.14M	32.16M
23-MAY-11	61206	376.84K	606.84K	983.67K
22-MAY-11	64894	3.12M	6.83M	9.95M
21-MAY-11	75729	2.59M	6.18M	8.77M
20-MAY-11	82681	12.9M	1.44M	14.34M
19-MAY-11	61090	12.07M	2.6M	14.67M
17-MAY-11	43388	4.35M	1.32M	5.68M
16-MAY-11	43012	16.38M	2.8M	19.18M
14-MAY-11	32525	3.29K	2.56K	5.85K
13-MAY-11	82851	5.03M	1.17M	6.2M
12-MAY-11	86996	21.5M	4.03M	25.54M
11-MAY-11	86022	18.33M	6.46M	24.79M
10-MAY-11	61190	27.12M	3.62M	30.74M
09-MAY-11	86269	42.2M	6.41M	48.61M
08-MAY-11	86279	2.15M	884.41K	3.01M
07-MAY-11	68399	418.77K	640.59K	1.03M
06-MAY-11	86400	13.05M	1.83M	14.88M
05-MAY-11	18146	12.28K	22.1K	34.39K
04-MAY-11	86520	2.12M	1.12M	3.24M
03-MAY-11	68134	15.77M	2.75M	18.53M
02-MAY-11	86400	863.91K	1.99M	2.83M
01-MAY-11	86400	2.01M	992.26K	2.98M

<< back 1 month forward>>

Your Volume Cap is set at: 3G bytes
You have used 48.4% of your Capping Limit

Cumulative Totals for June 2011

Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined Transfer
6515999	1.3G	121.47M	1.42G

Daily Totals for June 2011

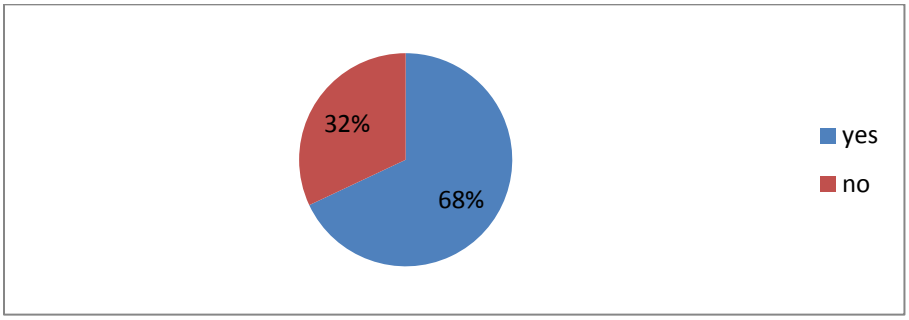
Date	Online Time (Seconds)	Download (Bytes)	Upload (Bytes)	Combined (Bytes)
30-JUN-10	29032	6.18M	794.79K	6.96M
29-JUN-10	76073	84.81M	13.2M	98.01M
28-JUN-11	68172	13.8M	4.77M	18.57M
27-JUN-11	86400	780.82K	945.17K	1.69M
26-JUN-11	61233	2.03M	825.45K	2.84M
25-JUN-11	64860	35.84M	6.09M	41.92M
24-JUN-11	64850	66M	7.8M	73.8M
23-JUN-11	68257	64.74M	11.09M	75.83M
22-JUN-11	86400	19.34M	3.77M	23.11M
21-JUN-11	86400	44.78M	8.54M	53.32M
20-JUN-11	61491	700.54K	718.19K	1.39M
19-JUN-11	172961	21.16M	2.35M	23.51M
18-JUN-11	172781	191.23M	17.38M	208.6M
17-JUN-11	172673	216.94M	27.3M	244.23M
16-JUN-11	173029	49.5K	62.84K	112.34K
15-JUN-11	172795	32.83K	45.03K	77.87K
14-JUN-11	172829	176.5M	11.86M	188.36M
13-JUN-11	172759	274.15M	18.59M	292.74M
12-JUN-11	172557	40.81M	4.79M	45.6M
11-JUN-11	172973	969.05K	346.08K	1.28M
10-JUN-11	205320	270.15M	17.08M	287.23M
09-JUN-11	226754	4.56M	1.29M	5.86M
08-JUN-11	215887	3.37M	745.55K	4.09M
07-JUN-11	255950	19.08M	2.96M	22.04M
06-JUN-11	259000	0	0	0
05-JUN-11	259427	157.31K	174.9K	332.21K
04-JUN-11	258872	3.96M	1.74M	5.7M
03-JUN-11	259355	18.64M	4.59M	23.23M
02-JUN-11	255669	41.95M	7.09M	49.05M
01-JUN-11	259048	42.65M	6.1M	48.75M

<< back 1 month forward>>

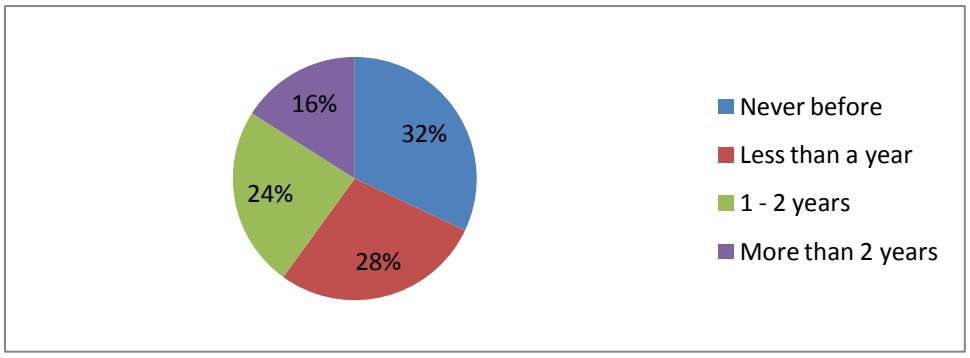
14 Appendix F - The Questionnaire and Feedback

This questionnaire is meant to completed by community members (i.e. teachers, students and local villagers) at Dwesa rural area. The aim of the questionnaire is to collect data pertaining to user feelings regarding the introduction of hotspots on their social and cultural livelihoods. We want to determine how this development has influenced the way they live and ascertain the benefits they gain through accessing the SLL network resources using hotspots.

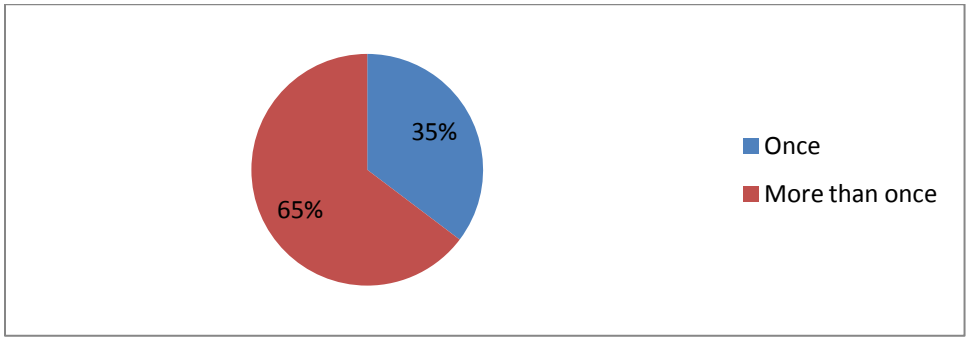
1. **Have you ever used computers and the Internet before?**
    1. Yes
    2. No



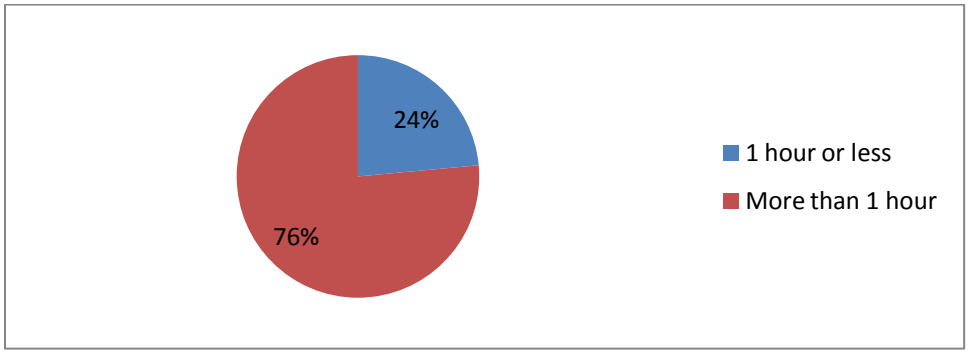
2. **How many years have you been using computers and the Internet?**
    1. Never before
    2. Less than a year
    3. 1 - 2 years
    4. More than 2 years



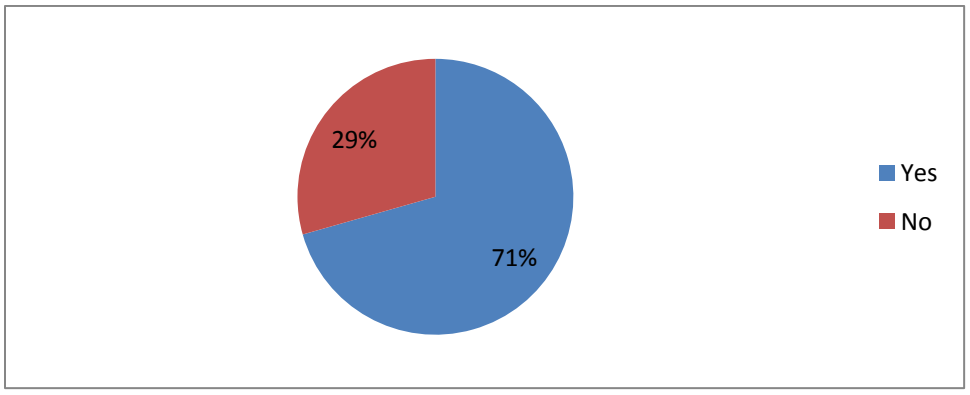
3. **How frequently do you use the Internet per week?**
    1. Once
    2. More than once



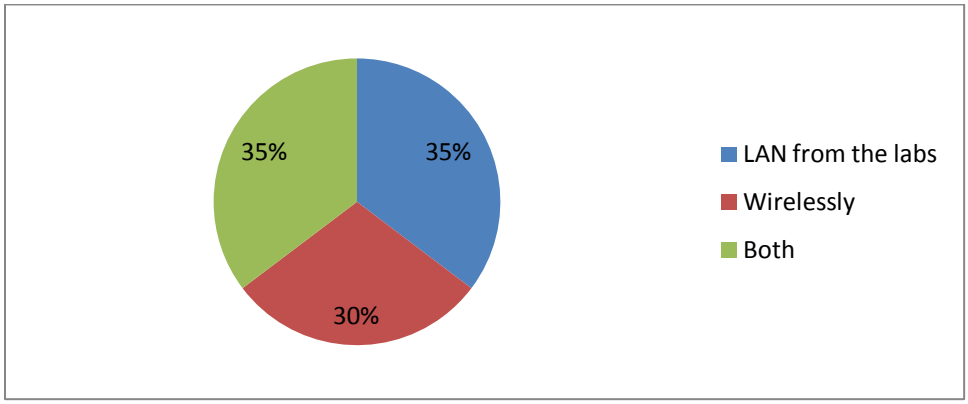
4. **How long do you use the Internet per day?**
    1. 1 hour or less
    2. More than 1 hour



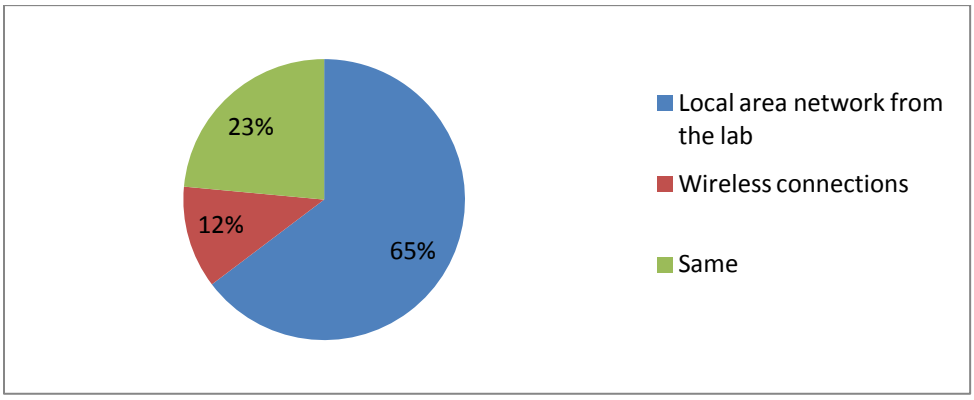
5. **Do you use the Internet and some other deployed applications during weekends?**
    1. Yes
    2. No



6. **Which method do you use to access the Internet?**
    1. LAN from the labs
    2. WiFi connections using a laptop or WiFi enabled cell phone
    3. Both

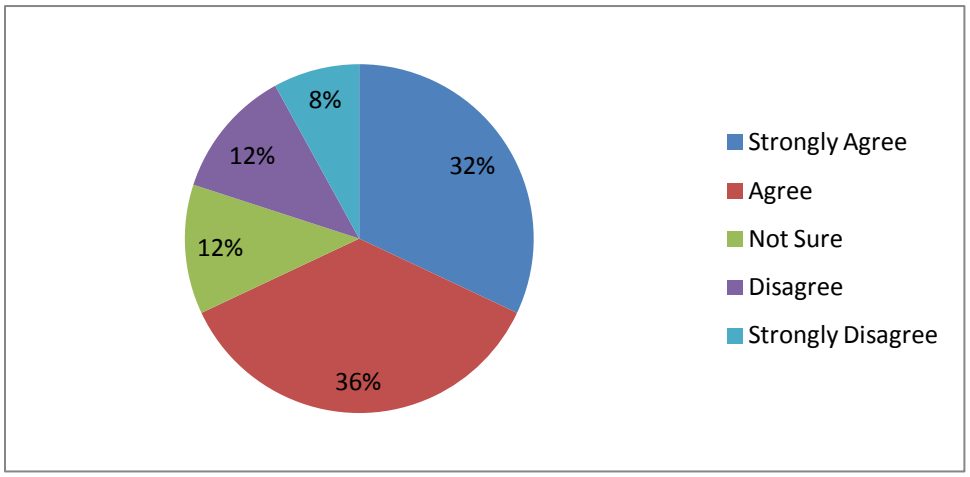


7. **Which method is faster when accessing sites and accessing other applications such as e-commerce, e-government?**
    1. Local area network from the lab
    2. Wireless connections
    3. Similar



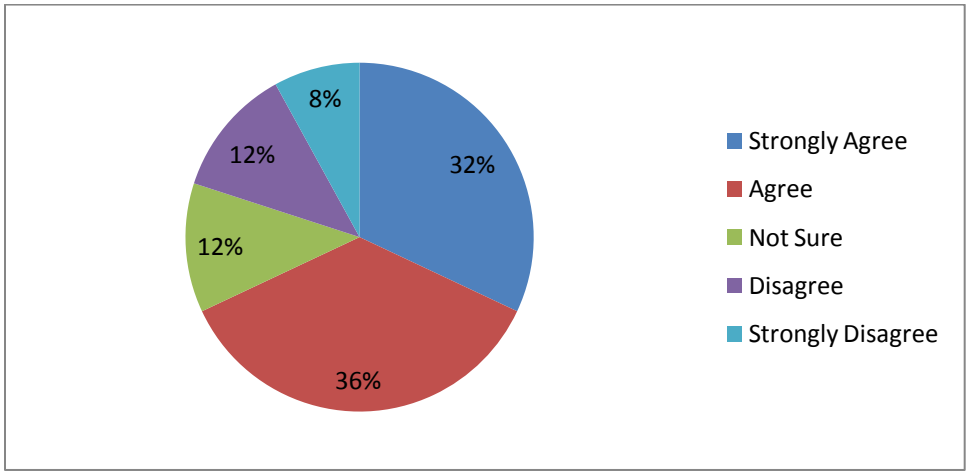
8. **Do you think the introduction of WiFi hotspots would interest you more in using computers and the Internet more often?**
    1. Strongly Agree
    2. Agree
    3. Not Sure

4. Disagree
5. Strongly Disagree



9. Is the deployment and use of hotspots beneficial in terms of the improvement of socio-economic standards?

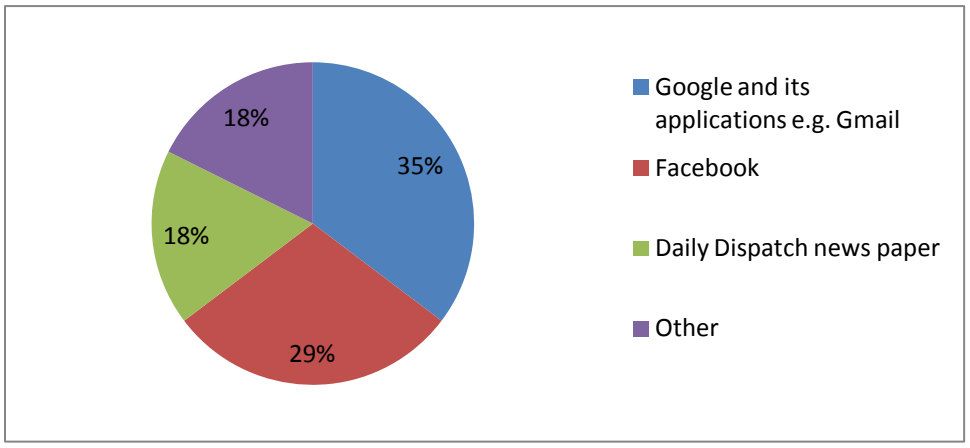
1. Strongly Agree
2. Agree
3. Not Sure
4. Disagree
5. Strongly Disagree



10. Which are the common sites you like opening on a daily basis?

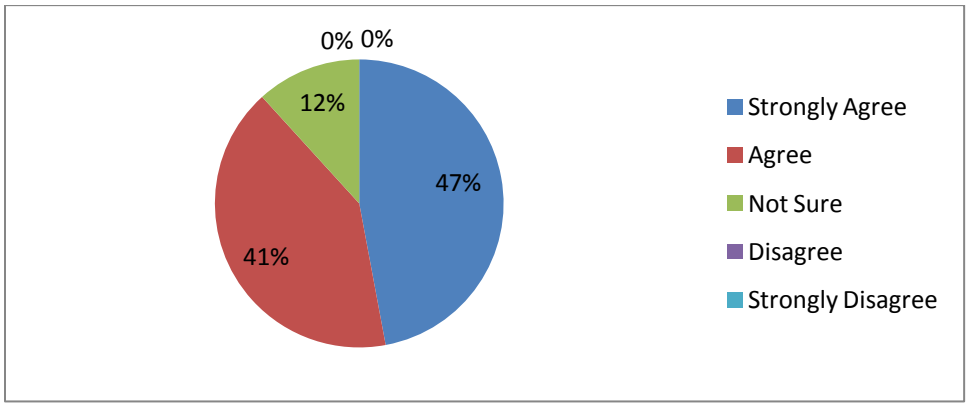
1. Google and its applications e.g. Gmail
2. Facebook

3. Daily Dispatch newspaper
4. Other



11. Do you think the introduction of WiFi hotspots would improve the learning and education standards in the area?

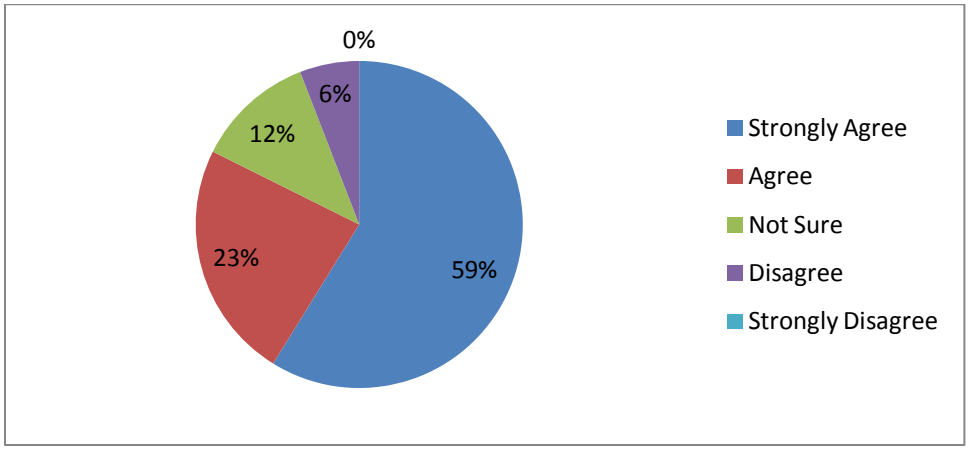
1. Strongly Agree
2. Agree
3. Not Sure
4. Disagree
5. Strongly Disagree



12. Do you think that using hotspots is convenient and would be critical especially for people who want to utilize the resources after school hours and during the weekends?

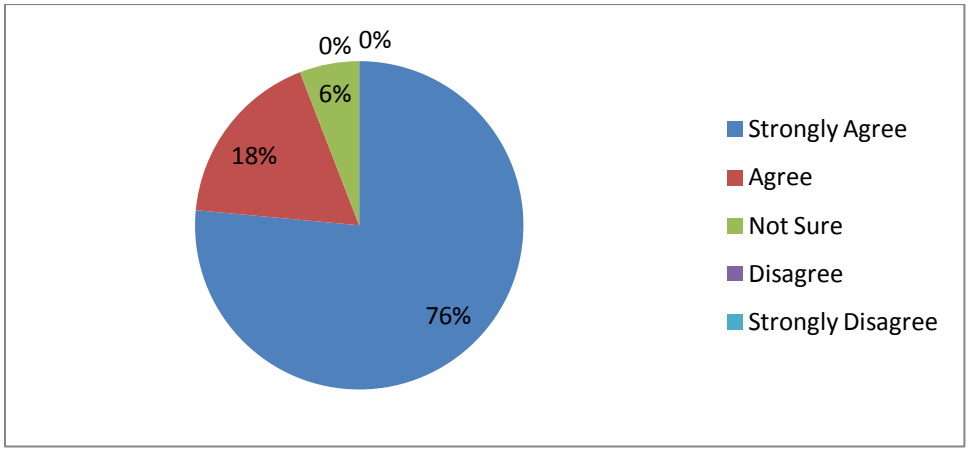
1. Strongly Agree
2. Agree

3. Not Sure
4. Disagree
5. Strongly Disagree



13. Do you think the use of social networking applications, such as Gtalk, would improve communication levels in the area?

1. Strongly Agree
2. Agree
3. Not Sure
4. Disagree
5. Strongly Disagree



More on Dwesa Projects @

http://siyakhulall.org