Best practice wireless network deployment configurations for ICTD service provisioning in MRAs

N. Ndlovu
Department Of Computer Science, Fort Hare University
Alice, South Africa
nndlovu@ufh.ac.za;

N. Jere
Department Of Computer Science, Fort Hare University
Alice, South Africa
njere@ufh.ac.za;

M. Thinyane
Department Of Computer Science, Fort Hare University
Alice, South Africa
mthinyane@ufh.ac.za

Abstract

Bringing information to marginalized communities in Africa has previously been a challenge for governments. This is because deployment of wired networks is expensive and not as profitable as in urban areas. Fortunately, the spread of wireless networking addresses this issue by allowing for the establishment of Internet connections in those areas at a much faster pace than anticipated. This major success has greatly changed the way people communicate, share information and also live by eliminating the challenges of distance and location. Consequently, almost all areas need to be connected as well so as to benefit from technological advancements and from participating in global knowledge systems.

This paper explains how wireless technologies (i.e. Worldwide Interoperability for Microwave Access (WiMAX) and Wireless Fidelity (WiFi)) can be merged and deployed to further extend the networks in marginalized communities. The field-site is the Siyakhula Living Lab (SLL) in Dwesa which is located in the Eastern Cape region, South Africa. Dwesa was chosen since it has a WiMAX and VSAT already deployed and also there is a need to further extend the network. The combination of WiMAX and VSAT presents a relatively new prototype where VSAT is used as a backhaul Internet connectivity technology for WiMAX sites covering many Digital Access Nodes (DANs) which in our case are schools. This network undergoes regular incremental updating and redesign to cater for the changing socio-technical factors. This paper provides a detailed overview of how WiFi technology is merged into this network. The main idea is to create WiFi hotspots by deploying access points around each and every school. These will cover the air space at the edges of the network, but being managed centrally at controllers. These WiFi hotspots created will provide high speed wireless access services for users within the coverage area. Schools which are close by can enjoy supplementary services like seamless switchover and load balancing.

This paper also provides an overview of security issues on a converged WiFi and WiMAX networks. The access points will provide network services for authenticated users within its coverage. ChilliSpot captive portal will be used as a wireless access controller for the wireless hotpot since it can provide better security as compared to the WPA. ChilliSpot is accepted as a better authenticating access controller in wireless networks especially WiFi

networks. ChilliSpot creates a virtual private network which uses a dialogue in granting and restricting users for Internet. Finally, the paper explains how this telecommunication network can facilitate the successful undertaking of the ICT4D intervention which will definitely boost the socio-economic lives of these community members.

Keywords: Digital Access Nodes, Information and Communication Technology for Development (ICT4D), Very Small Aperture Terminal, WiFi Protected Access.

1. Introduction

In recent years, a number of ICT4D projects have been and are still being implemented in the marginalised areas. They aim to realize the benefits of Information and Communication Technology (ICT)s in a range of sectors, from health, education, commerce and e-government to scientific capacity building, human rights and gender empowerment (Thinyane, 2006; Slay, 2006). However, these benefits are hindered by inadequate telecommunication infrastructure and human capacity in the marginalized areas. As a result, almost every government and non-governmental organisations are trying to leverage this information sharing setback (Goth, 2005). Recently, technology has been used to deliver information to marginalised areas. This approach has seen the livelihoods of the community members in these areas improving vastly. Wireless technology has recently taken the lead in such marginalised telecommunication deployments (Bage, 2004).

This paper presents a similar wireless network deployment in one of the marginalised areas of South Africa, Dwesa community. This network deployment provides Internet connectivity and also acts as a platform for other ICT4D application projects which are also being deployed in the area (Mandioma, 2006). Dwesa community is a deep rural area and it is located in the Eastern Cape region. The project undertaken in this area falls under the name Siyakhula Living Lab (SLL), (Thinyane, 2006; Slay, 2006). Rhodes and Fort Hare universities are the primary participants behind the success of this living lab.

This paper again presents an investigation on how various wireless access technologies mainly, WiMAX and WiFi can be converged and deployed in the area. It also gives information on how hotspots are created by deploying access points around the schools and investigate the benefits they brought to the entire community. Lastly, it aims to give an overview of security issues on a converged WiFi and WiMAX networks. The access points will provide network services for authenticated users within its coverage. ChilliSpot captive portal will be used as a wireless access controller for the wireless hotpot since it can provide better security as compared to the WPA.

The paper is structured as follows: The first part gives an overview of the SLL. On this part a brief description of the Dwesa community is presented and also the infrastructural constraints in the area. The next part defines wireless convergence and then afterwards, we give the alternative wireless convergence technologies. We then explain the current network situation of the SLL. This is followed by a brief explanation and presentation of the work that has been done so far in order to meet our initial objectives of conducting the project. Lastly, we conclude and give possible future extensions on the network that will achieve a reliable, high throughput and low latency network.

2. The Siyakhula Living Lab

The University of Fort Hare, together with Rhodes University embarked on an ICT4D project four years back the line. They primary aim of the project was to provide a research platform which will explore novel and innovative mechanisms to leap-frog socio-economic

development in marginalized communities of South Africa (Thinyane, 2006; Slay, 2006). The test bed was chosen in the marginalised community of Dwesa in the Eastern Cape region.

2.1 Dwesa Community Overview

The Dwesa community is located on the Wild Coast of the former homeland of Transkei, in the Eastern Cape Province of South Africa. The community is under the Mbashe Municipality which belongs to the Amatole region based in East London. Dwesa is a rural community isolated from the global telecommunication service with poor cellular coverage and inaccessibility. The area has a hilly terrain and its valleys characterised by rivers (Timmermans, 2004). Having such a terrain makes it difficult for any telecommunication company to deploy a network in an environment similar to this one. The majority of the inhabitants are poor people who rely on donations though they work for themselves to improve their living standards. The Dwesa inhabitants are typically subsistence farmers who depend mainly on the farming of the land for their livelihoods (Palmer *et al*., 2002). The Dwesa region also has a coastal nature reserve, an attraction particularly to South African tourists, who however visit almost exclusively during school holidays. Finally, there are arts and crafts entrepreneurs in Dwesa who serve the local markets with their artefacts (Timmermans, 2004). These entrepreneurs are mostly organized as groups.

2.2 Infrastructural Constraints

In terms of infrastructure the area is still underdeveloped. The road leading to the main town, Willovale is a rough earth road. It is difficult to drive in this area and it takes one approximately an hour to get to the town. The transport system is still at its infancy stage. There is no regular transport from Dwesa to town. Another issue affecting the area and the deployment of a telecommunication infrastructure is lack of electricity (Mandioma, 2006). Few places have electricity available. Places such as schools, few shops, few homesteads and clinic are the ones with electricity installed. This on its own has a negative impact on the use of technology and deployment of various ICTs around the area (Thinyane, 2006; Slay, 2006). As a result, very few people own cell phones. A certain amount is paid to get the cell phone battery recharged in places where there is electricity. A minimum of five rand is charged for full battery recharging. The telecommunication infrastructure is also very limited (Mandioma, 2006). There are very few telephone lines in the community, and the few public pay phones that had been installed in the community have been vandalized and damaged. Vodacom and MTN have provided a GSM network around the area since the GPRS and EDGE are unreliable and always unavailable (Anderson, 2001).

3. Definition of Wireless Convergence

Since we will be merging to wireless technologies WiMAX and WiFi in the SLL network, the term convergence in this context means combining the two technologies so as to have a high broadband data throughput rates, high reliability, low latency and more secure network. It is evident that wireless technologies such as WiMAX and WiFi are making it easier in the provision of the much needed telecommunications infrastructure in the marginalized and disaster struck areas worldwide (Gast, 2002). These technologies enable rapid low cost deployment of service and increases backhaul and last mile connectivity options (Morrow, 2004). WiFi has proven to be more flexible and mobile as compared to Ethernet wired network. Its major drawback is the security issue (Rensburg, 2006). On the other hand, WiMAX offers broadband wireless technology, which can support high-speed transmission of data, voice and video up to approximately 50km of direct line of sight. Initially, WiMAX was meant to address the drawbacks of WiFi such as low security, low-speed access and small area coverage (Mandioma, 2006).

Consequently, we proposed to deploy a converged wireless network in the SLL. WiMAX will be the backbone and WiFi will be used for hotspots deployment in the area. This idea will solve the rural Internet connectivity in a cost effective manner. The converged wireless networks are thought to offer a number of benefits (Computer Science Corporation, 2005), which are:

- Increased Security
- Flexibility and scalability
- Significantly reduced costs
- Effective communication
- Productivity Enhancements
- Simplicity
- Cost control

4. Alternative Wireless Convergence

A comparison of different wireless technologies that can be converged for rural Internet connectivity was done. However, in this paper we did not look much in the security aspects of these technologies after they have been combined. This comparison discussion will provide a clear picture on why some of these technologies are unsuitable to be converged for the provision of a reliable and always available communication link.

4.1 WiFi vs. WiMAX

The two technologies are almost similar. However, the major difference in these wireless access technologies is the communication range (Intel, 2005). In general, WiFi was designed for short range of approximately 100m and WiMAX can cover distances of close to 50km (Mandioma, 2006).This comparison can be shown best in Table 1 below.

WiFi	WiMAX
➢ Range :100 m, covers a coffee shop, one floor of an office building, one home ➢ Throughput: 11 Mbps ➢ Security: Limited ➢ QoS: Limited	➢ Range : 50 km, covers a small city with one base station ➢ Throughput: 72 Mbps ➢ Security: Multi-level encryption ➢ QoS: Dynamic bandwidth allocation, good for voice + video

Table 1: Comparison of WiFi and WiMAX (Rensburg, 2006)

4.2 WiFi vs. Bluetooth

Both technologies use 2.4GHz unlicensed radio spectrum. 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 a close proximity. Various devices such as phones, printers, personal digital assistance and modems and computers have Bluetooth built within them. The 16 bit Personal Identification Number (PIN) used for Bluetooth authentication and data encryption is not robust compared to the 80211i security enhanced protocol used in WiFi. Lastly, the low bandwidth and the low signal coverage of Bluetooth, makes it difficult and practical impossible to set up an effective and reliable network for remote applications (Crookston, 2004).

4.3 WiMAX vs. UMTS

Universal Mobile Telecommunications System (UMTS) is a general mobile wireless access technology with data speeds of 384 Kbps. This is very low as compared to that of WiMAX which can go to up to 70Mbps for coverage of 50km. Similarly, to other mobile technologies WiMAX have the same capabilities to transmit data and voice (Sweeny, 2004). The choice of using mobile technologies in transmitting voice is more expensive with VoIP/WiMAX as compared to WCDMA/HSDPA (Computer Science Corporation, 2005). The overall cost for the WiMAX equipment is much lower as compared to the UMTS, especially due to less usage of high tower structures. 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) is already there while the WiMAX requires a new infrastructure setup for it to operate (Morrow, 2004). UMTS is preferred for mobile communication compared to WiMAX because of its easy availability.

4.4 WiFi vs. UMTS

Both WiFi and UMTS offer mobility to end users (Morrow, 2004). They have similar characteristics. However, WiFi has a drawback of low distance coverage. The low coverage of WiFi limits its application around hotpots areas, but it enables user-friendly interface to be used as IP-based broadband access devices (Esmailzadeh, 2006a). In fact, WiFi and UMTS work rather better as complementary access technology (Esmailzadeh, 2006b).

5. Proposed Converged Wireless Network

The telecommunication infrastructure deployed in Dwesa currently comprises of four schools, Ngwane, Nqabara, Mpume and Mtokwane as shown in Figure 1 below.

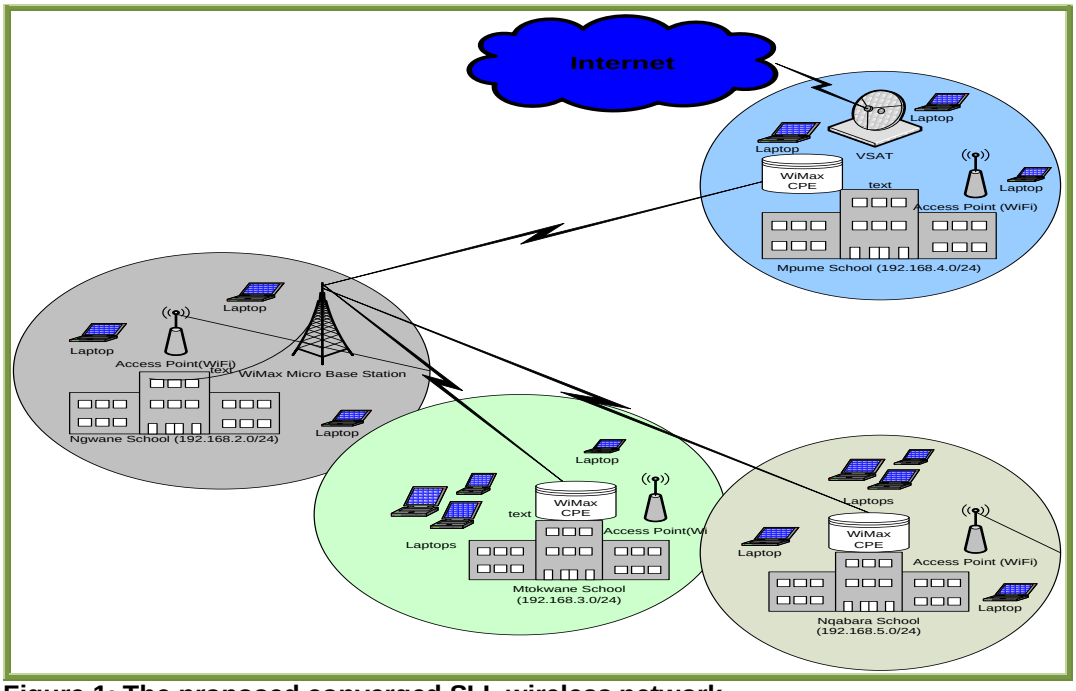

Figure 1: The proposed converged SLL wireless network.

Figure 1 above depicts the layout of the network. Four of the schools, which form the community Digital Access Nodes (DANs), are connected via a WiMAX network which allows higher throughput suitable to VoIP and multimedia applications and a larger range

to reach the remote regions within the community (Sweeny, 2004). The current and future updates to the network are elaborated in detail in the next paragraph.

A VSAT which offers backhaul Internet connectivity was installed at Mpume. Mpume Router/Server is connected to the VSAT through the VSATs' indoor unit. The indoor unit has a Dynamic Host Configuration Protocol (DHCP) server that was built and installed by Telkom. The Mpume Server/Router provides server capabilities within the network in the school. It also allocates DHCP addresses within the Mpume School Lab. Initially, we started by extending the existing network by setting up WiMAX Customer Premise Equipment (CPE) at Nqabara. Afterwards, we created WiFi hotspots by deploying access points around each and every school to cover the air space at the edges of the network, but manage them centrally at controllers. These WiFi hotspots created provide high speed wireless access services for users within the coverage area (Esmailzadeh, 2006b). As a result, we intended to make it possible for users in nearby schools like Ngwane and Mtokwane to access supplementary services like seamless switchover and load balance (Aitel, 2004; Young, 2004). These access points provide network services for authenticated users within its coverage.

For authenticating users a setup depicted in Figure 2 below was established;

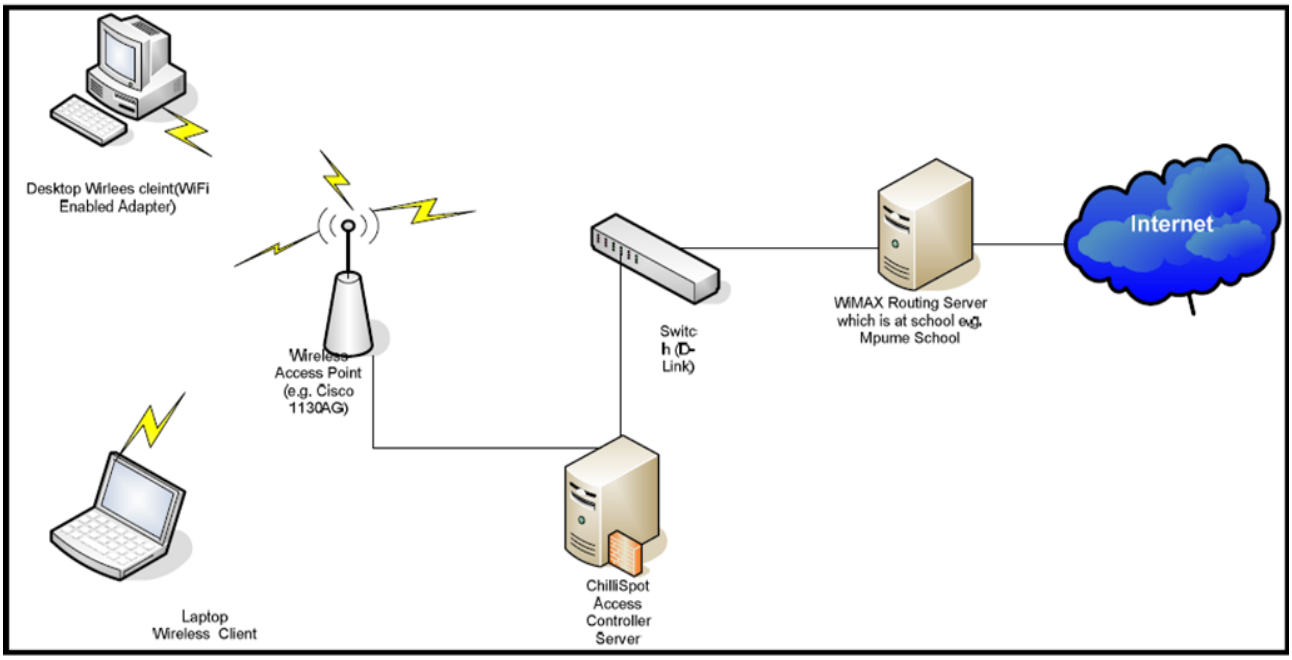

Figure 2: ChilliSpot Access Controller for a hotspot.

The ChilliSpot can be used as a wireless access controller for the wireless hotpot since it can provide better security compared to the WPA (Aitel, 2004; Young, 2004). The ChilliSpot application is accepted as a better authenticating access controller in wireless networks especially WiFi networks. The ChilliSpot as explained creates a virtual private network which uses a dialogue in granting and restricting users for Internet. The ChilliSpot has built-in DHCP capabilities in assigning Internet Protocol (IP) addresses to wireless clients.

6. Converged SLL Network Implementation

Having considered the different technologies of their advantages and disadvantages we chose WiMAX and WiFi. We used the two wireless technologies to deploy a converged

SSL network. The version of WiMAX that we used is BreezeMAX 3500 (802.16d) operating at 3.5GHz (Alvarion, 2005). It links the schools and it is the backbone of the network. VSAT is the backhaul (Everett, 1992). Below is a brief discussion of how this network was implemented. Software and hardware used is discussed.

6.1 The Implementation Requirement Components

Various components were utilized in the implementation of our converged SLL network. These components are both hardware and software. A detailed research on the different components and relevant information was done to successfully deploy our network.

6.1.1 Hardware

Various hardware components were used in this research. We used mainly the two versions of access points from Cisco and DLink. These are Cisco Aironet 1100 AP series, Cisco 1130AG and a DWL 2100 AP.

- ***Wireless Access Points*** – All these access points, Cisco Aironet 1100 AP series, Cisco 1130AG and a DWL 2100 AP support 802.11b, while the Cisco 1130 AG had additional support for 802.11a/g as well.
- ***Customer Premises Equipment (CPE)*** – It is also called Subscriber Unit (SU) and is usually installed at the organizational entity. It provides data connection to the Access Unit. In this research according to the Alvarion, (2005), the 10/100 Ethernet port connects to the user's data equipment, thereby providing bridging functionality, traffic shaping and can support up to 512 MAC addresses. SUs are comprised of two inseparable components; Indoor unit (IDU) that is powered from the mains and the Outdoor Unit (ODU) which contains the modem, radio, data processing and the management components of the SU (Sweeny, 2004).
- ***Micro Base Station (BS)*** - According to Alvarion, (2005), the BreezeMAX base station (BS) equipment is made available in two variants; chassis configuration and micro base station. We used the micro base station which has a functionality required to communicate with the SU and connect to the backbone (VSAT connection at Mpume) of the Internet Service Provider (ISP). It has additionally 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).
- ***Computers*** - We used two client computers, one desktop computer with slotted in D-Link wireless adapter and a WiFi enabled HP laptop, one server running the ChilliSpot and all the relevant packages and a switch.

6.1.2 Software

We used open source software since it is cost effective. Linux operating system was used. The version that we used is Ubuntu 9.04 Jaunty. Other different software like ChilliSpot and FreeBSD were downloaded for free on the Internet. The following list gives a summary of software that we used:

- ***FreeBSD*** - it is a UNIX like free operation system from AT&T Unit through the Berkeley Software Distribution (BSD). FreeBSD 6.1 was used as the operating

system for each WiMAX router at each school, where as the FreeBSD 6.2 was used on the Mpume School Access Concentrator.

- ***Ubuntu 9.04 Jaunty Operating System*** – This is the Linux operating system version that we used.
- ***ChilliSpot*** – It handles authentication, authorization and accounting for wireless users through its use of the free radius server (Beltrame, 2007).

6.2 Experimental Test-bed Implementation

In this paper, WiMAX and WiFi were defined as our converged wireless network technologies. We are going to give a brief description and explanation of the investigated test bed at Dwesa rural community as well as the network and the services, giving an insight into the installation and the configuration settings of the network.

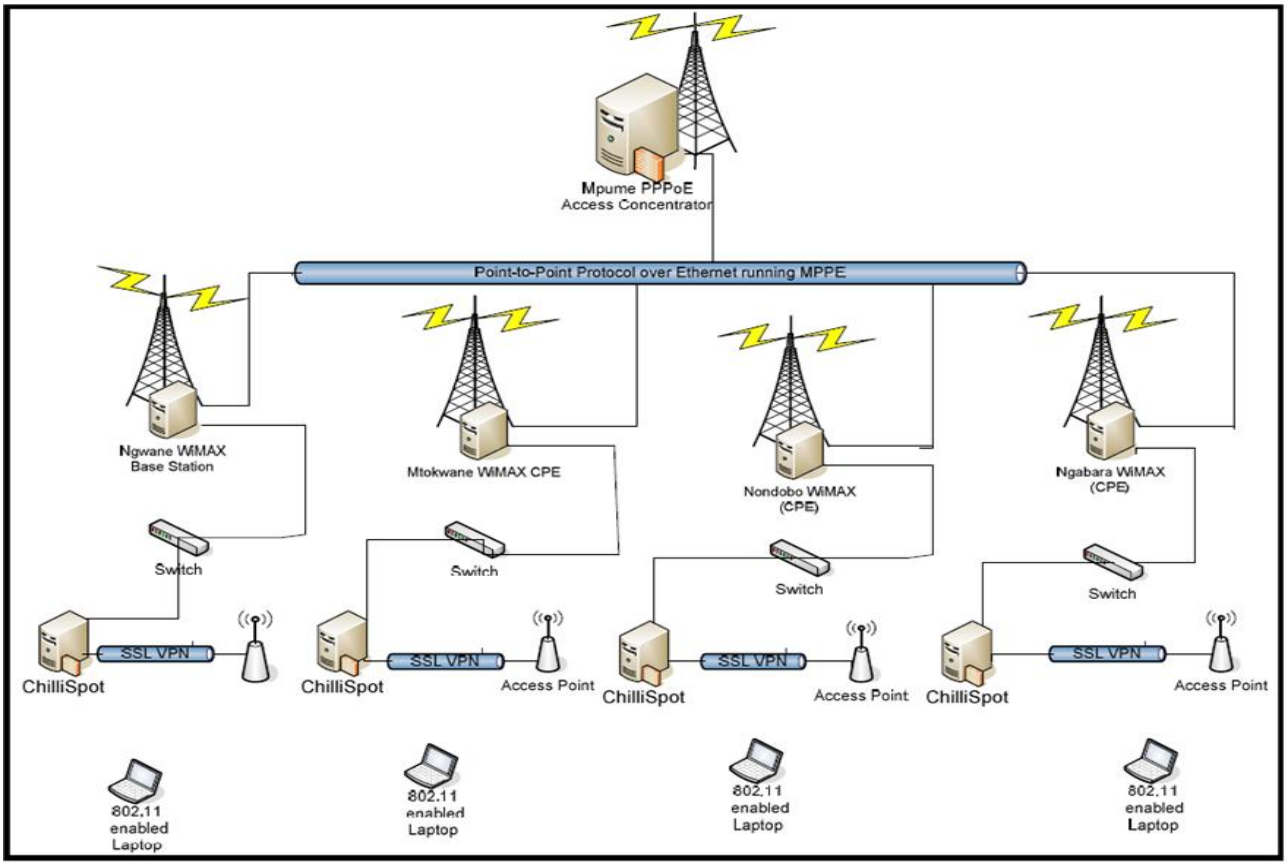

Figure 3: Dwesa test- bed implementation diagram.

The following points are explaining Figure 3 above and how the network implementation was done.

- ***Mpume Access Concentrator (AC)*** - This was installed at Mpume together with the VSAT. The computer used as an AC has an Intel Pentium III processor running a stable FreeBSD 6.2 operation system. It is connected to the router at Mpume and it creates communication tunnels on the WiMAX. The WiMAX SU located at Mpume is linked to the indoor data module that is connected to the router. As a result, signals reach the WiMAX system through this link. At Mpume there is a router with three network cards. The first one is for connecting to the VSAT. The second one

binds an IP address on the local area network at Mpume. Whereas, the third one connects to the backbone with the AC and binds the IP address 192.168.0.1.

- ***Subscriber Station/Units (SU)*** – These have been installed in all schools, with Nqabara SU having been installed recently. WiMAX SUs connects to a router which is installed at each and every 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 Ngwane. The BS has an Omni-directional antenna of 13 dBbi, which provides the signal to the other subscriber units attached to the network.
- ***Switch*** - A DLink switch was used to connect an AP and the wired network. The switch is designed to systematically eradicate traffic congestion.
- ***Wireless Access Controller (ChilliSpot Server)*** – It is used as a wireless access controller for the wireless hotpot since it can provide better security compared to the WiFi Protected Access (Wireless Security Corporation, 2008). It handles authentication, authorization and accounting for wireless users through its use of the free radius server.

6.3 ChilliSpot Implementation

Accordingly, to a “Howto” posted by Beltrame, (2007), a ChilliSpot has a number of requirements that should be considered when implementing it. Figure 4 below shows how the ChilliSpot was implemented in the SLL network.

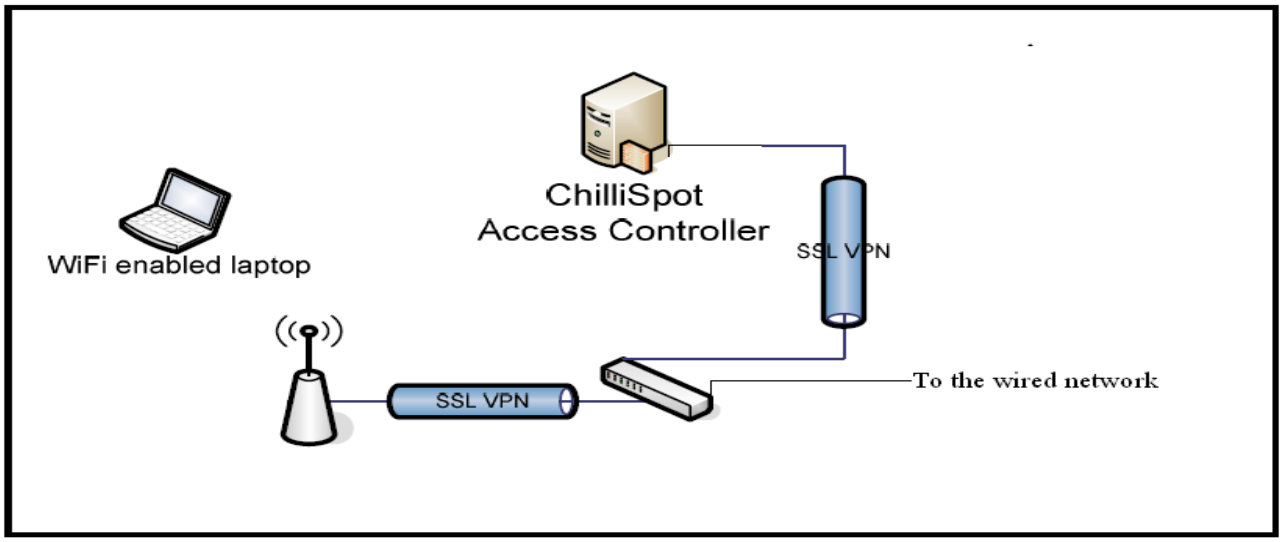

Figure 4: ChilliSpot implementation diagram.

The requirements are as follows:

- ***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 authentication of wireless clients, we had to use three conf files and edited them 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 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 */etc/raddb/radius.conf* file since it is the one that is used to authenticate the wireless users.

- ***Apache Configurations*** – We had to configure our web server Apache. SSL support 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, we changed the *uamsecret* in the hotspotlogin.cgi in the */etc/chilli.conf* to my *ndlovuwireless*

- ***MySQL Configurations*** – We had to configure our database to store the names and passwords for authorized users. An imported SQL schema was used, where a *radcheck* table used with the following fields; Username Attribute and Value. We created these fields using MySQL command line interface
  > INSERT INTO radcheck (Username, Attribute, Value) VALUES ('matwayi', 'Password','k@izer';

- ***ChilliSpot Configurations*** - We gave the machine 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 Chilli since it was used during the authentication process. The DNS server had an IP address of dns1 192.168.1.73. We then configured the access point to use the *dhcpif eth1.* We then configured the Universal Access Method (UAM) section, which denies wireless clients and certain urls to gain access to the network through the access point. For instance, to restrict wireless clients other resources like internet, files, a *uamserver* was used.
  uamserver https://192.168.1.73/cgi-bin/hotspotlogin.cgi

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

6.4 Security Considerations

Since different applications such as Internet services: email, SMS, file sharing etc, VoIP, an e-commerce platform with shopping mall, e-government, e-learning, e-health, e-judiciary and lastly a new approach on billing services for rural Internet will use the network, we made sure that security is our main priority. We started by securing each segment of the network using the inherent mechanisms considering the performance cost and effectiveness. The interactions of the wireless networks devices taking the vulnerabilities and threat impact through impact analysis, e.g. shared resources between the wireless networks link and users such as RADIUS servers was our main security consideration (Johnson, 2004; Walker, 2004). We also considered IPSec or VPN which are network independent mechanisms (Wireless Security Corporation, 2008). As the security mechanisms of these two wireless networks still could not provide robust and seamless security, therefore an access concentrator implementing Point-to-Point Protocol tunneling with MPPE security infrastructure was recommended (Alvarion, 2005; Walker, 2004).

7. Conclusion

Deploying a converged wireless network is a cost effective approach in providing Internet connectivity to the marginalised areas. As the research continues, we have noted that the convergence of WiMAX and WiFi wireless technologies may offer a solution to high-speed rural Internet connectivity. It may also provide ICTs a cost effective way of bridging the digital divide. Furthermore, this network deployment has lead to a number of projects being initiated, as well as the provision of Internet connectivity to a multi-purpose ICT platform (Thinyane, 2006; Slay, 2006). This platform is being used to build e-commerce applications that can eventually empower people. Services such as e-judiciary are being implemented in this network. Network security is still a major concern in such wireless network configurations. It must be priority that confidentiality, integrity and authentication be achieved on the converged network. From the initial findings, the inbuilt security mechanisms in WiFi and WiMAX still could not manage to offer a robust network solution in a converged infrastructure. As a result, we intend to overcome these security drawbacks in future and also evaluate the effectiveness and robustness of this extended converged WiMAX/WiFi network (Mandioma, 2007). The network would be monitored remotely and alerts used, in form of emails that will be sent to the administrators to notify them of any network failure occurrence or security loop-holes encountered (Johnson, 2004; Walker, 2004).

8. List of references

Aitel, D and Young, S. 2004. *The Hackers' Handbook: The Strategy behind breaking into and Defending Networks*, 1st ed. CRC Press.

Alvarion BreezeMAX 3500, 2005. *System Manual*. Available At: http://solomon.ipv6.club.tw/NCNU/WiMAX/alvarion.pdf (accessed 16 March 2010).

Anderson, C. 2001. *GPRS and 3G Wireless applications*, John Wiley and Son, Wiley Computer Publishing.

Bage, L. 2004. Rural development. *Key to Reaching the Millennium Development Goals*, Available At: http://www.ifad.org/events/op/2004/mdg.htm (accessed 16 March 2010).

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

Computer Science Corporation, 2005. *Converged Networks,* article, CSC press release. *Retrieved on the 2 January 2009.*

Crookston, R. 2004. *Bluetooth vs. WiFi,* Available At: http://www.verifonedevnet.com/VeriFone/Attachment/20040804/RetailTechnolog_407_28_316.pdf (accessed 21 March 2010).

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

Everett, L. 1992. *Introduction to VSATs, Very Small Aperture Terminals*, IEEE Telecom Series 28, Peter Peregrinus Ltd.

Gast, M. 2002. *802.11 Wireless Networks: The Definitive Guide*, O'Reilly, 494pages.

Goth, G. 2005, *Digital-divide efforts are getting more attention*, *Proceedings of the IEEE Internet Computing Conference*. 2005.

Intel, 2005. *Understanding WiFi and WiMAX as Metro- Access Solutions*. Available At: http://www.intel.com/netcomes/technologies/wimax/wimax__docs.html (accessed 16 March 2010).

Johnson, D. and Walker, J. 2004. *Overview of IEEE 802.16 Securities,* Security & Privacy. Magazine, vol. 2, Issue 3, The IEEE Computer Society Press.

Mandioma, M. Rao, K. Terzoli, A. And 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.

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

Palmer, R. Timmermans, H. and Fay, D. 2002. *From conflict to Negotiation: Nature based development on South Africa's Wild Coast*.

Rensburg, J. 2006. *Investigation of the deployment of 802.11 wireless networks*, MSc Thesis from University of Rhodes.

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

Thinyane, M. Slay, H. Terzoli, A. and Clayton, P. 2006. *A preliminary Investigation into the Implementation of ICTs in Marginalized Communities*, Proceedings of the South African Telecommunications Network Applications Conference, Western Cape, South Africa.

Wilson, J. 2004, *The Next Generation of Wireless LAN Emerges with 802.11n. Technology*, Intel Magazine.

Wireless Security Corporation, 2008.*VPN and IPSec: Imperfect Solution for Wireless Security.* Available at: http://www.scmagazineuk.com/wireless-security-2008 (accessed 16 March 2010).

9. Acknowledgements

We would like to thank the Telkom COE and other industry partners who are fully supporting the success of this big project. We would also like to thank the whole 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 perhaps, we would like to thank the Dwesa community for their cooperation and continual support of our research.