Exploring Technical Deployments of IPv6 on University LANs

Shadreck Kudakwashe Mudziwepasi[1] and Shakes Mfundo Scott[2]

**[1] Computer Science Department, University of Fort Hare,
P Bag X1314, Alice, South Africa, 5700**

**[2] Computer Science Department, University of Fort Hare,
P Bag X1314, Alice, South Africa, 5700**

Abstract

The current version of the Internet Protocol version 4 (IPv4) addressing scheme is officially exhausted. Internet Protocol version 6 (IPv6) is the next generation internet protocol proposed by the Internet Engineering Task Force (IETF) to supplant the current IPv4. Every device connected to the internet is expected to support this new generation of the basic protocol of the internet. At the University of Fort Hare which is the test environment of this research work, the entire network infrastructure has over the years gone through various upgrade terminologies in an effort to promote continued provision of an enhanced integrated environment to its users. This, in some instances has actually seen the university having to go for private IPv4 address space to meet all its network address requirements due to shortage of IPv4 addresses, a phenomenon which forms the primary concern of introducing IPv6. The introduction of IPv6 is imminent, not only at this institution but in all institutions of higher learning around the country. IPv6 introduction will see the network benefiting in plenty of ways which include but not limited to infinite addressing space, advanced network performance, enhanced network security and improved quality of service. It is however very important to note that as a new type of technology, the specifics of IPv6 and its advanced implementation strategies can in a way add uniqueness to its introduction and deployment. Also, as is always the case, a new technology can present a huge project risk if its implementation is not executed properly. Therefore, we need a careful and strategic plan that takes into account the type of network on which deployment is to take place and provide possible solutions to any impending technical challenges expected to be faced. This paper hereby presents an exploration of the motivations for IPv6 deployment. It proceeds to provide possible solutions for technical challenges of IPv6 deployment and strategies for beginning a reliable, efficient and cost effective deployment of IPv6 on University Local Area Networks (LANs).

Keywords: IPv4, IPv6, Technical Challenges, Deployment, University LANs.

1. Introduction

Internet Assigned Numbers Authority (IANA) announced a few years ago that it had run out of IPv4 addresses. Even though we know that some large Internet Service Providers (ISPs) have reserved some address pool for the future, we also know in essence that requesting new IPv4 addresses from Local Internet Registries (LIRs) will be difficult and next to impossible due to high demands for these addresses in the face of the official IPv4 address exhaustion announcement. Shortage of network addresses has however not stopped the technological world from expanding and diversifying. More and more devices that require internet connection are being introduced onto the market daily. These include smart phones, netbooks etc. In the wake of this IPv4 address exhaustion, an option for most ISPs would be to use Network Address Translation (NAT). This works well for basic connectivity even though it however causes difficulties to many applications. There are also scenarios where large ISPs will trade with their unallocated IPv4 addresses. However these scenarios can be considered as only short term solutions. The only perspective solution of addressing the discrepancies of IPv4 is to deploy IPv6 [1]. Deploying IPv6 will in essence bring many new issues onto the table for consideration and scrutinization. These include the fact that techniques for IPv6 address assignment are implemented differently in various Operating Systems (OSs) and special configuration needs to be done for different kinds of OSs. Missing implementations of security tools such as Router Advertisements (RAs) Guard as well as Secure Network Discovery (SEND) can also be a serious issue to consider. In as far as Security and privatization is concerned, the new feature of privacy extensions makes user's identification more difficult [2]. This behaviour is different from the normal identification technique of assigning a unique user identification portal for any user in any network, a technique necessary for any network administrator. Thus, new ways to deal with this feature needs to be developed whilst at the same time also dealing with any other transition technique that raises security problems [3]. We also note that improperly configured OSs sending rogue RAs can also on the long run cause network malfunctioning [4].

These are only but a few examples of challenges that may be posed by the deployment of IPv6 on any network. There are also many other problems that network administrators are facing such as IP Security (IPsec), data tracking and monitoring etc. This paper aims to investigate and assess these and many more technical challenges that may be involved in IPv6 deployments in a specific type of network, the University LAN. A case study of the University of Fort Hare LAN (UFH LAN) will be used. In doing so, we hope to offer a smooth transition strategy to this new generation of internet addressing for this type of network. The results of such an investigation can then be used for any network in any particular institution of higher learning.

2. Background : The Driver for IPv6

IPv4 was created in the 1970's, well before the advent of the World Wide Web (www), home computers, and the internet as we know it today. In that decade, no one could foresee that the protocol's 32-bit address space, representing approximately 4.3 billion addresses, could possibly be too small for what was, at the time, just an experiment. But as early as 1992 there were concerns about the rapid depletion of what seemed in the 70s to be an enormous number of addresses. Much of this had to do with the way IPv4 addresses were categorized by prefixes into Class A, Class B, and Class C. Class A prefixes were 8 bits and supported 16,777,216 addresses each; Class B prefixes were 16 bits and supported 65,536 addresses each; Class C prefixes were 24 bits and supported 256 addresses each. There was the rapidly rising popularity of Internet Protocol (IP) networking enabled devices such that the thought of the eventual depletion of all IPv4 addresses led to people thinking about another version of the protocol. A new version of the protocol supporting a much larger pool of available addresses was needed. After considering a number of proposals, IPv6 was adopted.

3. Related Work

3.1 Current Status of IPv6 Deployment at Brno University of Technology (Czech Republic).

To date, most of the parts of the university already provides native IPv6 connectivity and a significant part of devices connected to the campus network can partially use IPv6. From the user's perspective, Brno University of Technology (BUT) campus network connects more than 2,500 staff users and more than 23,000 students. The top utilization is at student dormitories where more than 6,000 students are connected via 100 Mb/s and 1Gb/s links. It is a really big challenge to provide functional and stable IPv6 connectivity to that amount of users [1].

IPv6 related activities started at the university several years ago. In that time a temporary IPv6 network was created especially for testing purposes. Routing was performed on the PC based routers with routing software Extensible Open Router Platform (XORP) and outside connectivity to National Research and Education Network (NREN) was encapsulated inside tunnels. The IPv6 infrastructure was completely separated in order to minimize impact of IPv6 infrastructure to running IPv4 services. That means the IPv6 network was run on dedicated routers and cable/fiber infrastructure. There were not any critical services running on IPv6 in that phase. The significant change became in 2010 when the university started participating on Hewlett-Packard (HP) ProCurve beta testing program. This was mainly focused on IPv6 features in the HP ProCurve devices that are widely used on the BUT network. Due to pretty good results from this beta testing program, the decision to move the core of the network to dual stack was made in the middle of 2010. IPv6 was enabled on all devices in the core network. At the end of 2010 the topology of the IPv6 network started completely following the terminologies of the topology of the IPv4 network. At the same time, the university decided to get their own Provider Independent (PI) IPv6 address space to be able to use multihomed IPv6 connections. Today, the IPv6 and IPv4 network provide some notable common services at the university although not yet convincingly. Work is underway to investigate technicalities that prevented the process of transition from being smooth enough to see IPv6 network functioning just like the IPv4 network and offering all the essential services at wire speed [1].

3.2 Current Status of IPv6 Deployment at Oxford University (Australia)

The full deployment schedule is more complex and will change, but the list below gives an approximate guide to the work which is currently underway at the university [5]. The focus right now is on preparing the core services for IPv6 support duely in the following ways:

- Older switch hardware performing IPv6 functions in software will be replaced. This will imply a major backbone upgrade on all major devices e.g. replacement of routers to introduce routers that support IPv6 routing and switching in hardware.
- Routing of IPv6 will be enabled on the university backbone.
- Underlying core services software will be upgraded and tested.
- Supporting services e.g. Network Time Protocol (NTP) and Web Proxy (WP) will be upgraded to support IPv6 in readiness, despite not being reachable via IPv6 at the time of configuration [5].

- A test wireless network will be the first network to have IPv6 enabled, as it does not depend on the Internet Protocol (IP) Address Management systems and is separated from other production university network services [5].

It is intended that IPv6 will be ready for university IT support staff to deploy locally after the above measures and considerations have been put in place. However due to experiences shared by other universities in IPv6 deployment, work is also underway at this university to investigate all possible technicalities to be faced in the wake of the pending deployment exercise.

During the process of moving to IPv6, institutions of higher learning continue to encounter several problematic issues especially with regards to network security and data monitoring and this has hindered prospects of a smooth transition. These and other technical challenges are very essential and nowadays there are still not proper solutions for them, a phenomenon which forms the primary concern of carrying out this research.

4. Deploying IPv6 on the UFH LAN

4.1 The UFH LAN

The UFH LAN is a centralized LAN. It depends on one single main core station. This single main core station is the backbone. This backbone is based at the Technical Support Centre (TSC) and it is called a 6400 Core-Switch. This Core-Switch has a routing module and the whole university depends on this switch for its networking terminologies. This 6400 Core-Switch is connected to a Telkom line called TL1 and TL3, so Telkom is the main network supplier to the UFH LAN. UFH network administrators use fibre cables to distribute the network to other surrounding buildings on campus e.g. to the Library, Administration etc. There are other areas such as the Agriculture and Mathematics departmental buildings that have small core-switches. The core-switches in these buildings are used to make loops so as to transport the network to other buildings. Each department in the campus is has its own main switch which acts as a backbone of the department at stake. These switches are used to distribute the network to their hosts e.g. offices, using Category 5 (CAT 5) or Unshielded Twisted Pair (UTP) cable. In departments such as Computer Science, GIS etc, where there are computer laboratories, there are sub-switches that depend on these main departmental switches e.g. Computer Science Honours and Masters Laboratories. In these departments, each fibre cable goes from one serial interface to the other. Each switch must have its own domain, subnetted using Virtual Local Area Network (VLAN) according to the University's network policy. UFH has three campuses (Alice, Bisho and East London) which are connected together using a Hybrid Star Topology. The link between these campuses is made using Integrated Digital Services Network (ISDN) lines. We have a Demilitarized zone (DMZ) firewall on each campus which means that intruders and hackers are unable to access our intranet from outside the three campuses. Since the DMZ acts as a security tool, everything that comes from the outside world must first pass through it to access the UFH LAN of each campus. This therefore makes the UFH LAN a private network.

Fig 2 below clearly outlines the topological layout of the UFH LAN with the linkage between campuses and associated information clearly outlined.

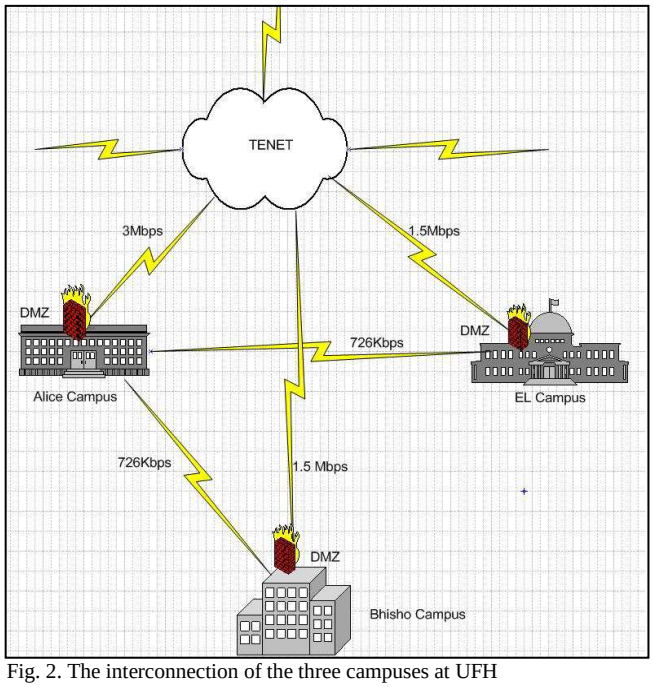

Fig. 2. The interconnection of the three campuses at UFH

The three serial cables that come out of the Tertiary Education Network (TENET) are extensions to the outside world, but there could be as many as we want. There are two main servers under the UFH LAN, one for the employees and one for the students. These servers operate different services e.g. login services, email services etc. The UFH LAN uses a class B network addressing scheme which runs under 172.20.*.*. However the problem with this addressing scheme is that it behaves like a class C address when it is subnetted. This is because when it is subnetted, its subnet masks start by 255.255.255.0 and so on as it has been subnetted into smaller networks, of which these smaller networks are as big as class C network addresses. It is also important to note that for the internet, there is a proxy server called the Microsoft Internet Security and Acceleration (ISA) server. This ISA server is

used to distribute the Internet to the whole campus. Also, in departments such as computer science and the library, there are servers connected to the main ISA server and they distribute the internet to various hosts devices in offices and laboratories

4.2 Planning for IPv6 Deployment at UFH

Creating a successful IPv6 implementation plan is in most ways no different from planning for the implementation of any new technology. A few overarching rules apply. These include but not limited to:

- Deploying the technology incrementally.
- Backing up the design assumptions with practical testing.
- Establishing sensible, liberal timelines.

There are, however, some factors that make an IPv6 implementation plan unique. Most of these involve the specifics of IPv6 and its implementation mechanisms.

Planning for IPv6 must also:

- Take into account the relative lack of extensive experience with the protocol
- The resulting depth of IPv6 deployment best practices.

The following subsections describe the components of an IPv6 implementation Plan that will help control risk and costs and ensure a successful completion [6].

4.2.1 Design

There are a lot of avenues that can be explored in this research project. Through exploring these, it is also important to note that each stage of deployment will come with its own package of technical challenges. A thorough investigation and assessment of these challenges is vital towards making the deployment process a success.

We will look at the following aspects of IPv6 deployment and expand our research based on them:

- IPv6 Basics
- Addressing
- Essential functions and Services
- Transition and Operational Reality
- Integration and Transition Routing and Network Management
- Multicast and Security
- Mobility and Applications

After an in-depth understanding of the afore-mentioned essential sections, we should be able to determine the steps to follow when deploying IPv6 on a university LAN. Departmental deployment will depend on the day-to-day work variations between different departments based on technological systems and operations. Finally such an exercise will delineate all possible technicalities or technical problems of IPv6 deployment to pave way for a smooth transition [7]

4.2.2 Inventory

A thorough inventory of the network is an essential first step to any network implementation planning. The inventory must provide a clear listing of what already supports IPv6 and give a clear description of everything that needs to be upgraded or replaced. The network inventory covers all aspects that IPv6 will address. These include:

- Routers, servers, hosts and the user applications.
- The OSs versions they run.
- Security, management and the office systems.

4.2.3 Methodology

There are basically three ways to deploy IPv6 on University LANs and these can be used for the UFH LAN. These are:

4.2.3.1 Core to Edge

IPv6 is implemented first in the routers forming the core of the network. We can take the core to be from within the LAN of the Alice campus and partake the deployment from therein within, usually using dual stacked interfaces and progressively expanding towards the edge of the network. This methodology has the advantage of implementing first where it is easiest, as most core router software either already supports IPv6 or can support it with a simple upgrade. These gains us more time to address the more difficult security and management implementations as the core is being converted. This method also tends to be the safest approach, allowing operations and engineering personnel time to become acquainted with the protocol before it reaches the users[1].

4.2.3.2 Edge to Core

IPv6 is implemented first at the edge of the network and then expanded toward the core. An edge is selected within the intranet of each of the three campuses and we deploy addresses towards the core. Manual tunnels such as GRE or MPLS are used to connect edge devices across the core during the interim. This approach is advantageous when IPv6 must be turned up relatively quickly for a customer requiring it or when a network must otherwise

demonstrate early IPv6 capability. It is also valuable when the core consists of legacy routers that either cannot support IPv6 but can support a tunneling technology or that can only be upgraded with difficulty [1].

4.2.3.3 IPv6 Islands

Certain segments throughout each LAN of the interconnected network, ranging from individual devices to complete sites, are converted. The islands can be interconnected with manual or automatic tunnels, or a combination of the two. As the implementation project progresses, the IPv6-capable islands grow until they begin to merge and toward the end of the project there are IPv4-only islands in the midst of an IPv6-capable ocean. This approach is useful when the network's existing IPv6 capabilities are scattered or when IPv6 must be quickly added to specialized systems throughout the network [1].

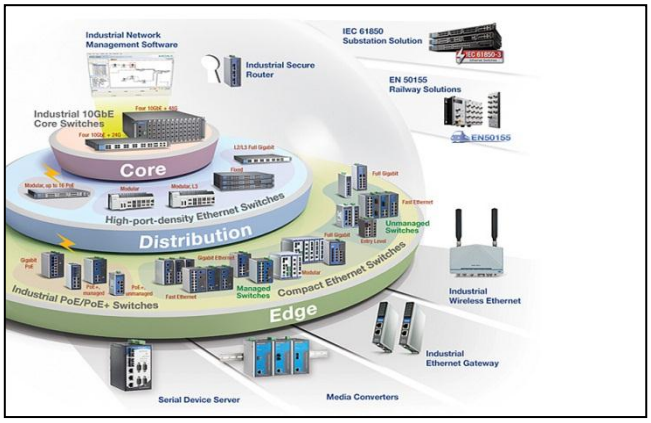

Fig. 3. The Core-Edge and Edge-Core Network Coverage on a wider network such as a University LAN [8].

5. Technical Challenges of IPv6 Deployment on CANs

Growing security, addressing issues and data tracking aspects discussed below present an overview of technical problems we are encountering whilst trying to deploy IPv6 protocol on University LANs.

5.1 Addressing issues

One of the basic problems is address assignment for the client systems. The mixture of various OSs requires a solution of automatic address assignment that is supported by most systems. The stateful autoconfiguration using Dynamic Host Configuration Protocol version 6 (DHCPv6) is very difficult to use today because of the lack of support in windows OSs, which is still the very widespread used OS, and older version of access control OSs. DHCPv6 does not support all configuration options e.g. option for default route, so the Stateless Address Auto Configuration (SLAAC) has to be used as well [9]. Unfortunately, the stateless autoconfiguration in some OSs turns on privacy extensions which means that the devices use random End User Identifier (EUI) named temporary IPv6 addresses. This is a brand new IPv6 feature that allows a node to automatically generate a random IPv6 address on its own.

5.2 Protection and Security

Vendors use slightly different terminology for individual types of protection but generally we can meet the following ones

5.2.1 DHCP Snooping

Some ports are explicitly defined in the switch configuration. Such ports are able to receive DHCP responses from DHCP (so called trusted port). It is assumed that somewhere behind the trusted port is a DHCP server and if a reply from a DHCP server arrives to a port having not been defined as trusted, the response is discarded right away [10]. Any DHCP server running on the client system (whether intentionally or by accident) does not threaten other clients on the network because the answers will not reach further than the access port for which this protection has been activated. DHCP snooping is usually prerequisite for other protection mechanisms such as IP lockdown or Address Resolution Protocol (ARP) protection [1].

5.2.2 Dynamic ARP protection, ARP inspection

DHCP snooping database contains MAC address – IP address – switch port combination. This database is then used on untrusted ports to inspect ARP packets. Other MAC addresses not recorded in the database are discarded. This eliminates attacks focused on creating fake records in the ARP table (poisoned ARP cache) [1].

5.2.3 Dynamic IP Lockdown

IP source guard: Another degree of protection is achieved by inspecting source MAC and IPv4 address on untrusted ports for all packets entering the port. This eliminates spoofing a source IPv4 or MAC address. Another often appreciated feature of this mechanism is the fact that the client cannot communicate over the network unless an IP address from the DHCP server is obtained [1]. Autoconfiguration should be considered.
The IPv6 autoconfiguration and neighbour discovery can be vulnerable to similar attacks as autoconfiguration in IPv4 networks [3]. Nowadays, network administrators of IPv6 networks are facing mainly a problem with rogue

router advertisements, which is similar to the problem of fake DHCP server in IPv4 networks. Many rogue advertises are generated by windows computers. This is a serious issue because computers propagate their own interfaces as a default gateway. Unfortunately this behavior can be in some conditions caused by properly used Internet connection sharing service. Described solutions for mitigating attacks in IPv4 networks are implemented in most of access switches on the market. IPv6 techniques for autoconfiguration are different so new solutions are necessary. Some security mitigation techniques in IPv6 networks to delineate the afore-mentioned technicalities are outlined below.

5.2.3.1 Source Address Validation Improvements (SAVI)

The SAVI method was developed to complement ingress filtering with finer-grained, standardized IP source address validation [10]. Framework has option for DHCP servers.

5.2.3.2 Secure Network Discovery (SEND)

This method tries to deal with autoconfiguration problem in a totally different way [11]. SEND is based on signing packets with cryptographic methods. Apart from a router it does not require support on the active network devices level. The validity verification itself through message certificate takes place at the end-user system. IPv6 address of the end-user system is a result of a cryptographic function, this means that we have another autoconfiguration method. Using SEND directly excludes using EUI 64 addresses and Privacy Extensions. SEND has one big advantage of not only solving the autoconfiguration problem but also other safety problems of the Network Discovery protocol (RFC2461). Another advantage is independent infrastructure; hence it can also be used in Wi-Fi networks for instance. The main shortcoming of SEND is the fact that it requires the support of public key infrastructure according to X 509. To make it work properly, one needs to install a certificate of the authority which issues router certificates [12].

5.2.3.3 RA Guard

Another alternative which however deals only with the issue of fake router advertisements is IPv6 Router Advertisement Guard [13]. It is a similar technique to DHCP snooping, but only for Router Advertisement packets. However, we note with concern that if the protective devices are to be truly purposeful, they must be placed as close to the end-user system as possible. In some cases, this could mean a complete replacement of network infrastructure which is a job that few will want to undergo so as to just implement IPv6. Affordable solutions which would at least alleviate efforts to paralyze the IPv6 auto configuration mechanism are as outlined below:

5.2.3.3.1 Access Lists on the switch

This solution assumes that we can configure IPv6 access lists on the active device. The aforementioned access list will block all ICMPv6 messages type 134 (RA messages line no. 2) and it will block traffic to the 546 target port (dhcpv6-client, line no. 3). The rules are subsequently applied to the inputs of ports to which the clients are connected (line no. 7). This can eliminate instances of rogue routers and DHCPv6 servers.

5.2.3.3.2 Passive Monitoring

Another option is detection of fake Router Advertisements. This will not protect us much from a well-crafted and targeted attack but it can at least detect incorrectly configured clients. We will need to use this solution if none of the options above can be used. For many networks it would be the only usable solution for a long time. All tools for detection of rogue RA work based on the same principle. They connect to the multicast group where the messages spread and thus enabling one to be able to monitor all messages appearing on the network. They can then tell the administrator about the undesirable status, call an automated action or even send a message canceling the validity of fake RA back to the network.

5.3 User tracking, monitoring and accounting

Long-term network monitoring, accounting and backtracking of security incidents is often achieved in IPv4 networks using NetFlow probes and collectors. This can be a problem if IPv6 is deployed and privacy extensions are allowed in the network. Same user can then communicate with different addresses. This means that addresses cannot be used as a unique identifier anymore. As part of deploying IPv6 we will try to develop extension to existing monitoring systems to allow easier tracking of users in an IPv6 network. The main idea of the extension is collecting and putting together data obtained from differed parts of the network [14].

5.4 Collecting and monitoring data

Data is collected using the Simple Network Management Protocol (SNMP) and stored in the central database where the network administrator can search data using the IPv6, IPv4 or MAC addresses as keys. A useful tool for pooling and storing information from switches and routers is Network Administration Visualized (NAV). SNMP pools the data from switches every fifteen minutes. The mapping between the IPv6 address and its corresponding MAC

address is downloaded from the router's neighbour cache. Port, Virtual Local Area Networks (VLAN) number and other information comes from the switch's Forwarding Database (FDB) table. Traffic statistics are obtained from NetFlow. NetFlow records alone are not sufficient for user surveillance and activity tracking because of the temporary IPv6 addresses as described in previous sections. Therefore, NetFlow records are extended by additional information called flow tags. The flow tag is added to a flow record after its creation, usually when the information is received and stored at the main database. The tag is a unique identifier of the user, because NetFlow records are generated for every single connection of the user, even with different IPv6 addresses. Flow tags can be used as keys to identify the activities of any user stored in the system. This is necessary because not all data is available immediately in the central monitoring system, for example, due to a delay caused by SNMP pooling.

6. Conclusion

Herein thoroughly outlined in this research project is an investigation and assessment of technicalities associated with transition mechanisms and techniques of deploying IPv6 on University LANs. The project offers an exhaustive analysis of possible challenges faced in various stages of IPv6 deployment ranging from basic addressing to the most important aspect of IP Security. We also explore possible mitigation strategies through an in-depth analysis of IPv4 and IPv6 from the basics to the most essential functions and services channeling through the transition and operational reality. In the context of the chosen case study, this project determines the steps to follow in deploying IPv6 in academic and non-academic departments of a University LAN. The combination of such departmental deployments will then in essence inform the actual university deployment analysis thereby resulting in successful deployments of IPv6 in institutions of higher learning.

7. Acknowledgement

I would like to thank my supervisor, who is also the Head of Computer Science Department at the University of Fort Hare, Mfundo Shakes Scott for his unwavering support and contributions throughout this research. Also, I would like to thank Jean Basson from the ICT unit at the University of Fort Hare for providing essential information about the University network setup and interconnection. I appreciate the information provided by Simon Angling from CCS IT training in East London, South Africa about IPv6 on Cisco devices and deployment techniques.

7. References

[1] T. Podermanski and M. Greg G,Deploying IPv6 in University Campus Network-Practical Problems,published article, November 2011,
url : http://www.fit.vutbr.cz/~poderman/pubs.php

[2] Krishnan. Privacy Extensions for Stateless Address Autoconfiguration in IPv6. RFC 4941, September 2007,
url : http://tools.ietf.org/html/rfc4941

[3] S. Frankel, R. Graveman, and J. Pearce. Guidelines for the Secure Deployment of IPv6. Technical Report 800-119, National Institute of Standards and Technology, 2010,
url : http:// csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf

[4] T. Podermanski: Security concerns and solutions with IPv6, GN3 IPv6 Workshop - Networking without IPv4?, [online], url : http://ow.feide.no/geantcampus:ipv6_mar_2011

[5] url:http://www.oucs.ox.ac.uk/network/addresses/ipv6/index.xml
[online], 2013-07-12

[6] Juniper NETWORKS: deploying IPv6: Issues and Strategies,iec organisation newsletter,february 2009
url : http:www.iec.orgnewsletterfebruary09_1juniperwhitepaper.pdf

[7] url : http://cs.ufh.ac.za/research/sites/cs.ufh.ac.za.research
/files/Honours_Projects_2013_v1-1.pdf: [online], 2013-07-12

[8] MOXA:Industrial-Network-Management-Software,[online],2013-07-10
url:http://www.moxa.com/Event/Net/2011/MXview/Edge_to_core_Network_Coverage.html

[9] S.Thomson, T.Narten, and T.Jinmei. IPv6 Stateless Address Autoconfiguration. RFC 4862, September 2007,
url : http://tools.ietf.org/html/rfc4862

[10] Wu, J., Bi, J., Bagnulo, M., Baker, F., and C. Vogt: Source Address Validation Improvement Framework", draft- ietf-savi- framework-04 (work in progress), March 2011

[11] J. Arkko, Ed., J. Kempf, B. Zill, P. Nikander: SEcure Neighbor Discovery (SEND). RFC 3971, Febuary 2011, url:http://tools.ietf.org/html/rfc3971

[12] R. Albright, Cisco System's Statement of IPR related to draft-ietf-v6ops-ra-guard-02, April 2009, url : http://www.ietf.org/ietf-ftp/IPR/cisco-ipr-draft-ietf-v6ops-ra-guard-02.txt

[13] E. Levy-Abegnoli, G. Van de Velde, C. Popoviciu, J. Mohacsi: IPv6 Router Advertisement Guard, RFC 6105, February 2011,
url : http://tools.ietf.org/html/rfc6105

[14] T.Narten, E.Nordmark, W.Simpson, and H.Soliman. Neighbor Discovery for IP version 6 (IPv6). RFC 4861, September 2007,
url : http://tools.ietf.org/html/rfc4941

Shadreck Mudziwepasi received his BSc degree in Computer Science and Mathematical Statistics at the University of Fort Hare in 2013. He is currently studying towards his honors degree in Computer Science at the same university. His research interests include networking, network security, e-diaries, wimax networks, scalable information retrieval and communications issues and has great focus on real-time embedded systems and coordination models for distributed systems.