ASSESSMENT OF COMPATIBILITY OF DEVICES IN THE ADOPTION OF INTERNET PROTOCOL VERSION 6 TECHNOLOGY IN THE FINANCE INDUSTRY.

KIGUTI IAN MUSILA

ICT-G-4-1444-21

A RESEARCH PROJECT SUBMITTED TO THE SCHOOL OF COMPUTING AND INFORMATICS IN PARTIAL FULFILMENT OF THE REQUIREMENT FOR THE AWARD OF THE DEGREE OF BACHELOR OF SCIENCE IN COMPUTER SCIENCE OF GRETSA UNIVERSITY.

APRIL 2024

DECLARATION

DECLARATION

This research project is my original work and has not been presented for the award of any degree or any similar purpose in any other university.

Signature…………………………… Date 29/11/2024.……………………

Kiguti Ian Musila

ICT-G-4-1444-21

Supervisor: This research project has been submitted with my approval as university supervisor

Signature…………………………… Date……02/11/2024.,

Sharon Mose
Computing and Informatics
Gretsa University

i

Table of Contents

List of Tables

List of Figures

Abbreviations and Acronyms

IPv4- Internet Protocol version 4

IPv6- Internet Protocol version 6

MN- Mobile Node

RIPE- Regional Internet Registry

ISPs- Internet Service Provider

IoT- Internet of Things

NAT- Network Address Translation

ICMPv6- Internet Control Message Protocol version 6

DHCPv6- Dynamic Host Configuration Protocol version 6

SLAAC- Stateless Address Autoconfiguration

DNS- Domain Name Server

IETF- Internet Engineering Task Force

Operational Definition of Terms

Adoption- The act of taking up and choosing to use.

Readiness- the state of being fully prepared

Internet- a global computer network providing a variety of information and communication facilities, consisting of interconnected networks using standardized communication protocols.

Mobility Management- to design local and regional solutions customized to fit the community's needs, resources, and vision.

ABSTRACT.

For the effective functioning of devices on the internet, there needs to be an IP address. IP addresses are identifiers of devices on the network. There have been several versions of the Internet protocol addressing system beginning from IPv0 to IPv6. IPv0 to IPv3 were unassigned. To set regulations for computer networks operating on the idea of data exchange, the well-known IPv4 was created in 1983. The IPv6 is a 128-bit addressing scheme with the following features: auto and renumbering address configuration, end-to-end connection integrity, an inbuilt security feature called IPSEC, address configuration in hexadecimal, fragmentation is only performed by the sender, encryption, and authentication are additional features. These characteristics add complexity to IPv6 and make its implementation challenging. With all of these readily available, it follows that Kenyan technology's infrastructure and resources are lacking. The technical readiness of ISPs, network operators, and service providers is a critical variable. The availability of IPv6-compatible infrastructure, network equipment, and software are necessary to successfully adopt IPv6. This research analyzed the state of IPv6 technology implementation and the readiness of the Kenyan financial industry in the adoption of IPv6 technology in terms of; the network protocols in place, mobility management protocols, and configuration models in place. The researcher undertook descriptive research on ABSA Bank Nairobi Branch for the study. The research involved IT administrators, IT engineers, and the IT support staff which is approximated to be 100. According to Yamane's formula for estimating sample size the sample size of this research will be 67 IT professionals. A Questionnaire and an interview guide were used for data collection. Statistical packages for social sciences was used for data analysis.

CHAPTER ONE: INTRODUCTION

1.1 Background.

In response to the rapid growth in world-class infrastructure and facilities, the Kenyan government released a blueprint (Kenya Vision 2030) to help Kenya plan a speedy cover-up. Among the deliverables in the blueprint is to ensure that all Kenyans can access technological services. For this to occur, the IPV6 addressing system has to be adopted. IP is a protocol that allows computers or devices to communicate with one another over a network. Now, IPv4 is the first version of IP to be used. Officially released in 1983, it is still the most known version used to identify network devices. However, this has not been the case as a simulation of the IPV6 technology is below the expected margin. The difference between the two is that IPv4 uses 32-bit addresses, whereas IPv6 uses a 128-bit address. The main reason the internet is shifting from IPV4 to IPV6 is that v4 had around 4.3 billion addresses compared to the human population of 7 billion. These addresses were getting depleted while there were still more devices requiring addresses. The first IPv6 operational network, called 6BONE, which was used to test IPv6 implementations and gain operational experience was established in 1997 by RIPE. The worldly adoption of IPV6 has been slow for the past 20 years until 2015 when Countries in Europe assimilated this use. As Kenyan ISPs are on the run to launch the 5th generation of the internet acceptance of the IPV6 is crucial.

The Communications Authority of Kenya (CAK) in 2022 released a report to roll out the IPv4 to IPv6 migration strategy. The CAK says that should Kenya delay in full adoption of IPv6, then serious technological challenges may befall the country's ICT sector, including lack of internet access, and lag in tech advances. Specifically, with the advent of IoT devices, most manufacturers are developing IPv6 devices because the IoT devices will be numerous, will each require access to the internet, and will therefore call for IPv6 usage. Kenya will not be able to take advantage of the

IoT devices as a result. According to IPv6 adoption rates for Kenya are currently around 8%, below 10%. This migration is expected to be done in July which is at the beginning of a new financial year. The Kenyan finance industry is expected to be on the frontline of the effective adoption of this technology. This research tackled the Compatibility, Trialability, and readiness of financial institutions in this migration having less than six months to roll out.

1.2 Statement of the Research Problem

With the depletion of IPv4 addresses, there is a need for a solution, which led to the emergence of IPV6. This has made it compulsory for the adoption of this new internet. According to the report released by the CAK in 2022, Kenya has very few IPv4 addresses remaining. Kenya's readiness for this transition is in question.

1.3 Purpose of the study

This study seeks to assess the compatibility of devices in the adoption of IPV6 technology in the Kenyan finance industry.

1.4 Conceptual framework

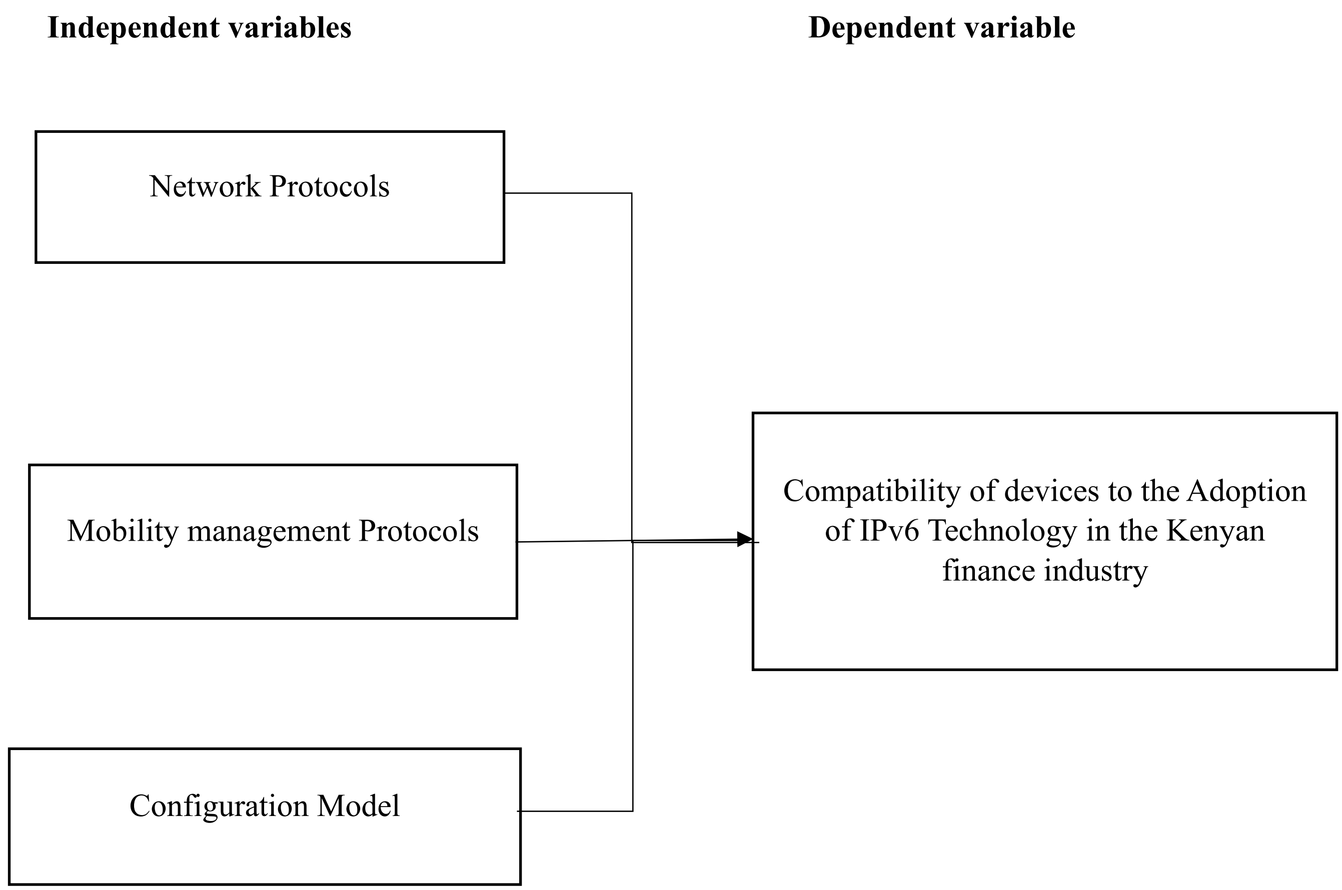


Figure 1: Conceptual Framework

1.5Research questions

The research was guided by the following questions

1) How does the network protocols affect the adoption of IPv6 technology in the Kenyan Finance Industry?
2) What are the mobility management protocols in place for the adoption of IPv6 technology in the Kenyan Finance Industry?
3) What effect does a configuration model have on the adoption of IPv6 technology in the Kenyan Finance industry?

1.6 Objectives of the Study

1.6.1 General objective

1. To assess the compatibility of devices in the adoption of IPv6 technology in the Kenyan Finance Industry.

1.6.2 Specific objectives

1) To determine the effect of network protocols in the adoption of IPv6 in the Kenyan Finance Industry.
2) To determine mobility management protocols in place for the adoption of IPv6 in the Kenyan Finance Industry.
3) To determine the configuration models in place for the adoption of IPv6 in the Kenyan Finance Industry.

1.7 Hypotheses of the Study

The following null hypotheses were used as a guide to the study:

H_{01}: There is no relationship between network protocols and Kenya's readiness for the adoption of IPv6 in the Kenyan Finance Industry.

H_{02}: There is no relationship between mobility management protocols and Kenya's readiness for the adoption of IPv6 in the Kenyan Finance Industry.

H_{03}: There is no relationship between a configuration model and Kenya's readiness for the adoption of IPv6 in the Kenyan Finance Industry.

1.8 Significance of the Study.

The study investigated the efforts that have been made in preparation for the adoption of IPv6 technology in the Kenyan Finance Industry. The findings from the study will help other institutions/industries such as the defense and agriculture departments what is expected in terms of the adoption of this network. ISPs will also need this evaluation to put in place measures that will help in the best service delivery to IPv6 clients. The government will also adjust policies governing address systems by the use of these findings.

1.9 Delimitations of the Study

They majorly focused on network protocols, mobility management protocols, and configuration models concerning the adoption of IPv6 technology. For easy compatibility with new technology, the underlying architecture determines its success factor. This research was constrained to network protocols, mobility management protocols, and configuration models since they are the underlying architectures in this field.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

The adoption of IPV6 technology is essential to facilitating communication between devices on the internet as ISPs switch from 4G to 5G. Since the majority of banking services are conducted online in Kenya, the financial sector is particularly important to the networking of devices. However, the technology's implementation might exclude roughly 90% of clients in the financial sector. In Kenya, there are roughly 8% of electronic devices that can operate on the IPV6 network, according to a report published by the Communications Authority of Kenya in 2022. Since a sizable portion of clients won't be able to access basic services, this poses a threat to all financial institutions. When it comes to adopting new technology, the financial sector is consistently one step ahead of other sectors and one of the most secure companies in Kenya. Carrier networks and ISPs were among the first to begin deploying IPv6 on their networks, with mobile networks spearheading the effort. UL & BII (2015) claim that network address translation (NAT) with IPv4, which transforms private IP addresses into public IP addresses, is partially to blame for the delay in the adoption of IPv6.

According to Alexandra Huides et al (2023), an increasing number of organizations are using IPv6 in their settings as a result of the expiration of public IPv4 space, the shortage of private IPv4 space, particularly in large-scale networks, and the demand to accommodate IPv6-only customers. There is no universal solution and there are best practices for planning and deploying IPv6, nevertheless, AWS customers can apply to convert their present cloud networks to IPv6. According to Alexandra Huides et al (2023), the IPv6 adoption strategy depends on the driving force behind it. With the long-term objective of entirely converting to an IPv6-only network, you might have an immediate aim such as addressing private IPv4 exhaustion or the capacity to provide IPv6 service endpoints by government mandate. The four primary forces and related adoption strategies are as follows:

• Private IPv4 exhaustion — The objective is to offer new nodes and issue routable IP addresses without IP overlap and without the difficulty of locating contiguous and useable IP addresses. Establishing IPv6-only routing across dual-stack network segments to enable IPv6 stack communication. interoperability layers, such as dual-stack load balancers, between IPv6 and IPv4.

The objective is to support IPv6-only clients connecting to your public endpoints. Public IPv4 exhaustion. The Internet of Things devices have IPv6 addresses, and the IPv4 interoperability layer is not provided by the network for IPv4. In IPv4 networks, other devices could be operational.

In dedicated IPv4-only or IPv6-only deployments, it is optional to provide separate endpoints for IPv4 and IPv6, according to Alexandra Huides et al (2023).

• Compatibility with networks that exclusively use IPv6. The objective is to enable communication from your IPv4-only network to IPv6-only nodes. Because the majority of endpoints operate in dual-stack mode and offer an interoperability layer, this use case is less common. The creation of IPv6-only subnets as part of dual-stack VPCs. Maintain an interoperability layer by utilizing DNS64 and the AWS NAT Gateway's built-in NAT64 functionality. Because dual-stack adoption is frequently impractical, IPv4 networks must support backward compatibility.

• Required IPv6 endpoints — The objective is to support compatibility with nodes connecting to your services that can only use IPv6 and to prevent the accumulation of technical debt in new services. Make a plan and finish the migration of older services that lack specialized IPv6 or dual-stack support.

2.2 Network protocols

The implementation of IPv6 technology in the financial industry is influenced by various network protocols. These network protocols will be discussed in IPv6 Protocol support, routing protocols, transport layer protocols, application layer protocols, and internet standards and interoperability.

1. IPv6 Protocol Support: IPv6 relies on specific network protocols designed to support its unique features and requirements. In the financial industry, where secure and reliable communication is paramount, the availability and support of these protocols are essential for IPv6 readiness.

According to Wu et al (2013) ICMPv6, the Internet Control Message Protocol version 6, is used for diagnostic and error reporting in IPv6 networks. It facilitates the exchange of network status and error information, allowing network administrators to identify and troubleshoot issues promptly. In the financial industry, where network reliability and quick response times are crucial, the proper functioning of ICMPv6 is vital.

According to Narten et al (2007), the Neighbor Discovery Protocol (NDP) is responsible for address resolution, neighbor discovery, and stateless autoconfiguration in IPv6 networks. It plays a critical role in ensuring the efficient use of IPv6 addresses and enabling seamless communication between devices. In the financial industry, where a large number of devices are interconnected, NDP ensures that devices can discover and communicate with each other effectively.

According to Wu et al (2013) Dynamic Host Configuration Protocol version 6 (DHCPv6) is in charge of managing and allocating IPv6 addresses on a dynamic basis. It facilitates effective address distribution, lessens the need for manual configuration, and enhances the scalability of

IPv6 networks. DHCPv6 ensures that devices in the financial industry can obtain valid IPv6 addresses and network configuration parameters accurately.

The support and proper implementation of these protocols are essential for financial institutions to ensure the availability, reliability, and security of their network infrastructure in an IPv6 environment.

2. Routing Protocol: Routing protocols govern the exchange of routing information and the decision-making processes used by network devices, which are essential to the operation of computer networks.

According to Jia et al (2019), the Border Gateway Protocol (BGP) is a routing protocol used in the financial industry to exchange routing information between different autonomous systems. With the introduction of IPv6, BGP with IPv6 address families enables the exchange of IPv6 routes, allowing financial institutions to extend their networks into the IPv6 realm. According to Jia et al (2019), and Wu et al (2013) proper support and implementation of BGP with IPv6 address families are vital for the seamless integration of IPv6 into existing network infrastructures.

3. Transport Layer Protocols: Transport layer protocols such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are essential for inter-host communication between programs.

   According to Long Hoang (2019), TCP ensures packet delivery, flow control, and congestion control to deliver dependable, connection-oriented communication. UDP, on the other hand, enables lightweight, connectionless communication, making it appropriate for real-time applications. According to Long Hoang (2019), an industry should test and validate the compatibility of their applications with IPv6 transport protocols. This includes verifying that TCP and UDP can establish connections and transmit data reliably over IPv6, ensuring that in an IPv6 environment, all transactions and sensitive data are sent securely.

4. Application Layer Protocols: Application layer protocols, such as HTTP, DNS, SMTP, and others, are used by various financial services and applications.

According to Long Hoang (2019), Hypertext Transfer Protocol (HTTP) is the cornerstone of data transmission via the Internet. Web-based applications are widely used by financial organizations to offer online banking services, financial data, and consumer portals. A successful industry-wide transition to IPv6 depends on ensuring that these apps and the underlying HTTP protocol can function without restriction over IPv6.

According to Bagnulo et al (2011), a Domain Name System (DNS) does the conversion of domain names to IP addresses. Financial institutions heavily rely on DNS for host resolution, service discovery, and email delivery. According to Wu et al (2013) vital to ensure that DNS services are fully IPv6 compatible, allowing financial institutions to resolve IPv6 addresses and access IPv6-enabled resources securely.

By confirming the readiness and compatibility of application layer protocols, institutions can ensure that their important financial services and applications are fully operational in an IPv6 environment, delivering a good user experience and maintaining high levels of security. Financial institutions should prioritize the use of equipment and software that comply with IPv6 standards and specifications. This ensures that all components of the network infrastructure work seamlessly together, enabling secure and efficient operation in an IPv6 environment.

2.3 Mobility management protocols

Mobility Management (MM) is the process of securing an organization's data on employee mobile devices, whether employee-owned or corporate-issued. Mobility Management solutions typically do have a broad range of services made to keep an organization's intellectual property and customer personally identifiable information (PII) safe and secure while combining with other enterprise IT systems and applications. According to J Lee et al (2023), mobility management enables:

- The ability to handle the highest number of devices by a single platform with support for a wide range of devices, both mobile and stationary. the ability to safely store all data on devices, whether it be corporate or personal, and the option to selectively remove business data without destroying personal employee information.
- Use app stores to restrict which programs can be installed on corporate devices and speed up the deployment of business applications in a secure way.
- Before granting access to sensitive information or intellectual property, enforce compliance by making sure remotely operated devices are using the secure infrastructure.
- Offer analytics, make use of data, and use reporting to find patterns that might hint at potential data breaches or exfiltration or that could result in greater usage.

According to Lee et al (2023), our daily digital ecosystems are expanding more swiftly thanks to mobile wireless ecosystems. Mobility management protocols are the fundamental elements of mobile wireless ecosystems. Mobile social networking, mobile collaboration computing, and mobile shopping will be possible with a well-integrated mobility management system. Several mobility management protocols have been designed to provide mobility services. The Internet Engineering Task Force (IETF) has been concentrating on supporting mobility at the network layer.

Fast Mobile IPv6 (FMIPv6) and Hierarchical Mobile IPv6 (HMIPv6) by N. Dutta & H. Sama (2021) are two modifications that have been made since the Mobile IPv6 (MIPv6) protocol was published to improve MIPv6 performance. Balfaqih (2020) claims that an analysis of the performance of the IPv6 mobility management protocol during the creation of the MIPv6 extensions has been incorporated into the improvement's creation. For instance, Yan & Lee (2019) and Balfaqih et al (2020) conducted comparative performance assessments of MIPv6, FMIPv6, HMIPv6, and a combination of FMIPv6 and HMIPv6, which specify the characteristics and performance indicators of each mobility management protocol. Although host-based mobility management protocols are deployable in wireless mobile communication infrastructures, Lee et al. (2023) state that communication service providers and standards development organizations have realized that these conventional solutions for mobility services are not suitable. In particular, for telecommunication service, a mobile node (MN) is required to have mobility functionalities at its network protocol stack inside, so modifications of the host-based mobility management protocols. According to Dutta & Sama (2021), it raises the cost and complexity of operation for the MN. Additionally, the host-based mobility management methods result in operators having no control because the MN is in charge of managing mobility support. According to Gundavelli (2008), as a result, the 3rd Generation Partnership Project has pushed for a new way to enable mobility service within the IETF. According to the MN, the entire PMIPv6 domain appears as a single connection because of the network-based mobility service offered by mobility service provisioning organizations. According to Balfaqih et al (2020) Fast Proxy Mobile IPv6 (FPMIPv6), an extension protocol to PMIPv6 was created to improve handover performance by lowering handover delay and preventing packet loss. Due to the significant differences in the protocol format and behavior, IPv4 and IPv6 are not interoperable. To further support IPv6, an ISP has to create an essentially parallel, independent network. As to end hosts, modern computer operating systems have already implemented dual-protocol stacks for access to both networks. The coexistence of IPv4 and IPv6 networks raises several general issues in different aspects. According to Shah et al (2019), Network devices like routers, firewalls, and various servers have to upgrade their hardware and software to support IPv6 features. Extra re-source dispatching mechanisms are needed in an overlapped environment, to allocate shared resources (link bandwidth, FIB entries, etc.) to each network and guarantee service for both. According to Wu et al (2013), a new QoS strategy for IPv6 should be developed to leverage the flow label field explicitly. A traversing problem happens when two or more native IPv4/IPv6 hosts are separated by a network that uses the other address family and thereby is not IPv4/IPv6-capable. According to Shah et al (2019), transition mechanisms are required for crossing the heterogeneous network. If IPv4 networks or hosts are separated by an IPv6 network in the middle, IPv4-over-IPv6 traversing is required; if IPv6 networks or hosts are separated by an IPv4 network, the problem then is IPv6-over-IPv4 traversing. According to Balfaqih et al (2020) New protocols in the IPv6 suite such as Neighbor Discovery and DHCPv6 may raise new security risks and thereby need to be evaluated. For end hosts, applications require intelligence to decide which protocol stack to use when the remote end may be reachable by both IPv4 and IPv6.

2.4 Configuration Models

In IPv6, configuration models define the process and mechanisms through which IPv6 addresses and network parameters are assigned to devices on a network.

1. Stateless Address Autoconfiguration (SLAAC):

According to Gont et al (2021), Stateless Address Autoconfiguration (SLAAC) is a core IPv6 configuration mechanism that enables devices to configure their IPv6 addresses automatically without the need for a centralized server. According to Mahmoud et al (2022), SLAAC takes advantage of the unique interface identifier (IID) derived from the device's MAC address or other identifiers, combined with a network prefix advertised by a router through ICMPv6 Router Advertisement (RA) messages. When a device joins an IPv6 network, it listens for RA messages containing a network prefix. Using the received prefix, the device combines it with its interface identifier to generate a globally unique IPv6 address. According to Gont et al (2021), SLAAC also through the RA messages, supplies the relevant data for further network parameters, such as the default gateway and DNS server.

2. Dynamic Host Configuration Protocol version 6 (DHCPv6):

DHCPv6 is an extension of the familiar DHCP protocol used in IPv4 networks. According to Xie et al (2021), DHCPv6 allows for the central administration and dynamic distribution of IPv6 addresses and network settings. It works with a client-server architecture, where DHCPv6 servers give DHCPv6 clients configuration data. According to Farrer (2022), it enables centralized control and administration of address allocation, allowing network administrators to enforce specific address assignment policies. DHCPv6 permits the assignment of extra network parameters as well, including domain names, DNS server addresses, and other configuration settings.

3. Combination of SLAAC and DHCPv6 (SLAAC+DHCPv6):

The SLAAC+DHCPv6 configuration model combines the benefits of both SLAAC and DHCPv6. According to Gont et al (2021), in this model, SLAAC is used for address configuration, while DHCPv6 is employed for additional network parameter assignment. This model allows network administrators to have greater flexibility in managing network parameters while still benefiting from the automatic address configuration provided by SLAAC.

4. Manual Configuration:

Manual configuration entails giving devices IPv6 addresses and network settings by hand. This approach is appropriate for networks with a small number of devices or where precise control over address assignment is required. The most in-depth level of management is offered via manual setup, which also enables network managers to assign specific addresses to devices as necessary. But it requires a lot of work and is prone to mistakes made by people. It might also reduce the network's capacity for scaling and automation.

5. Dynamic Address Assignment from a Pool:

Dynamic address assignment from a pool is a configuration model where devices are assigned IPv6 addresses from a predefined pool. In this model, a pool of available IPv6 addresses is maintained, and devices are assigned addresses from this pool as they join the network. Dynamic address assignment allows for efficient address utilization and simplifies address management by automatically reclaiming addresses when devices leave the network.

CHAPTER THREE: RESEARCH METHODOLOGY

3.0 Introduction

In this section, the researcher discusses the research's methodology, which will cover the study's research design, study area, target population, sample size, measurement of variables, research instruments, validity, and reliability, data collection method, data analysis, and logistical and ethical considerations.

3.1 Research design

A research design is an arrangement of conditions for the collection, measurement, and analysis of data in a manner that aims to combine relevance to the research purpose with economy and procedure. In this research, the researcher will use a descriptive research design. Frost et al (2019) assert that this research design tries to systematically obtain information to describe a phenomenon, situation, or population.

3.2 Study area

The research was conducted in ABSA Bank, Nairobi Branch as a representation of financial institutions. The technology in this branch has the upper hand and has the highest number of IT professionals in ABSA banks within the region.

3.3 Target population

The target population for this research was IT professionals; IT technicians, IT administrators, network consultants, network administrators, and the IT support staff within the branch. The target population was about 80 professionals as documented in the bank's employee records at the beginning of this year.

3.4 Sample size

The sample size is the measure of the number of individual samples used in an experiment.

This research will have a sample size of 80 according to Yamane’s formula.

Yamane’s formula states that:

$n=N/(1+N(e)^2)$

n is the sample size

N is the target population

e is the margin of error

$n = N / (1 + N(e)^2)$

$n = 80 / (1 +80(0.05)^2)$

$n = 80 / (1+ 80(0.0025))$

$n =80 / (1 + 0.2)$

$n = 80 / 1.2$

$n =67$

3.5 Measurement of variables

Table 1: Measurement of variables

Variable	Indicator	Measurement scale	Questions
Network protocols	Protocol support Scalability	Nominal	4
Mobility Management Protocols	Scalability and load balancing	Nominal	4
Configuration model	Type of configuration	Nominal	4

3.6 Research instruments

The researcher used questionnaires and interviews as primary research instruments. The researcher will use questionnaires to obtain general views and background information. Interviews will be used to fetch more clarity on the information covered in the questionnaires.

3.7 Validity of measurements

The validity of measurements refers to how accurate a measure is. In this research, the validity of the measurements involved checking the data collected in questionnaires related to the real world.

3.8 Reliability of measurements

This is about the stability and consistency of the measurement that will be used by the researcher. The researcher used internal consistency to measure the reliability of measurement from respondents' responses.

3.9 Data Collection Techniques

The study used primary data, which will be the only kind of data gathered. The questionnaires contained both open-ended and closed-ended inquiries. Open-ended questions allow for unstructured free-form remarks, allowing respondents to express their thoughts in an unbiased manner. The answers given by the responders were limited by closed-ended questions. Closed-ended questions were used to shield respondents' answers from the effects of the environment. This gave the entire population perfectly focused data that is well-targeted. The data that was obtained will be clarified through interviews.

3.10 Data analysis.

Hypothesis	Hypothesis test	Statistical method
There is no relationship between network protocols and Kenya's readiness for the adoption of IPv6.	Chi-square test	Assessing whether there is a significant relationship
There is no relationship between mobility management protocols and Kenya's readiness for the adoption of IPv6.	Fisher's exact test	A contingency table to check on the readiness of each protocol
There is no relationship between a configuration model and Kenya's readiness for the adoption of IPv6	Chi-square test	Assessing the contribution of a configuration

3.11 Logistical and ethical considerations

The researcher ensured that the respondents are informed and they give it willingly. Any confidential information collected was handled carefully so as not to compromise the respondent's ethics.

CHAPTER FOUR: FINDINGS AND DISCUSSION.

4.1 Introduction

In this chapter findings of data collected in the assessment of compatibility of devices in the adoption of internet protocol version 6 technology in the finance industry in Absa Bank Nairobi branch. The analysis of this data and its discussions will be made in this chapter and will be categorized according to the research questions and the objectives concerning the assessment of compatibility of devices in the adoption of Internet protocol version 6 technology.

4.2 Demographic Information

The research was targeted at 67 personnel who were handed questionnaires. A total of only 60 questionnaires were received from the respondents which amounted to 97% while that that wasn't received was 3%. Out of the received data, 30.8% was received from the female gender while 69.2% was male.

Table 2: Gender tabulation

Gender * Level Crosstabulation

Count

		Level					Total
		1	2	3	4	5	
Gender	Male	14	6	8	7	5	40
	Female	6	6	2	4	2	20
Total		20	12	10	11	7	60

4.2.1 Response Rate

Out of the 67 questionnaires returned 60 were found to be filled and could be useable for the research.

Table 3:Response Rate

	Frequency	Percent
Non response	7	10.5
Filled and returned	60	89.5
Total	67	100

4.2.1.1 Gender

Table 4: Gender Representation

Gender	Frequency	Percent
Male	46	69.2
Female	21	30.8

A larger percentage of respondents in the research were male as accounted for in the table above.

4.3Network Protocols

The research sought to determine which Internet protocol version 6 network protocols in the Kenyan finance industry had been established as compatible with the current devices.

4.3.1 Internet Protocol Version 6 Protocol Support

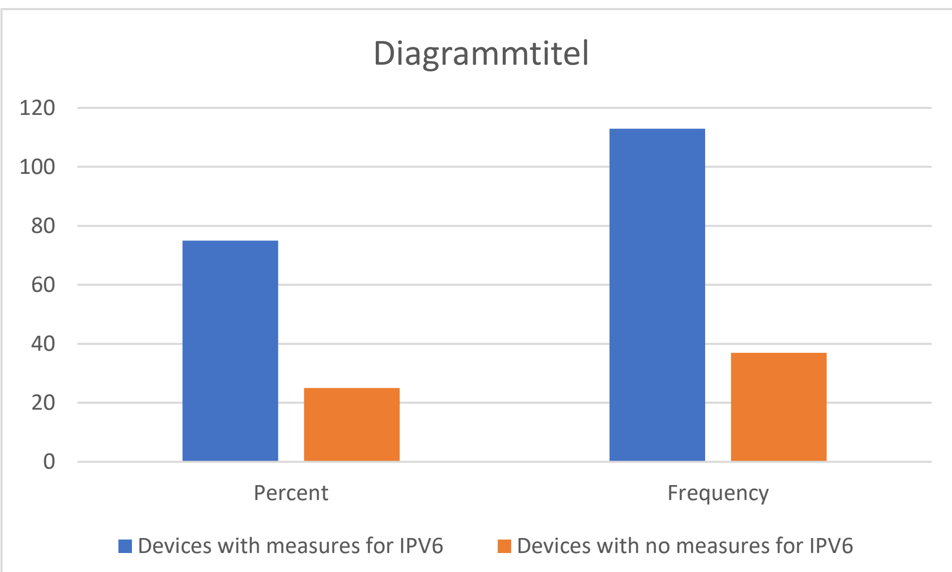
The questionnaire requested the IT officials in the equity bank to state to which level they thought the protocol support they had was in preparation for this new addressing system and their responses are documented in the table below. From the data below most of the respondents thought that the institution had a very low level of Internet protocol version 6 protocol support. On the other hand, 7 respondents thought the institution had the required protocol support

The research also sought to understand if devices have protocol support measures that the institution put in place in preparation for this adoption. This section entailed having a specific group of protocols in question. The data is tabulated below.

Table 5:Devices with measures

	Frequency	Percent
Devices with measures in place for IPV6	113	75
Devices with no measures in place for IPV6	37	25

Figure 2:Graph on devices with measures on IPV6



4.4Mobility Management Protocols

The researcher sought to find the mobility management protocols that had been selected if they were compatible with the new addressing scheme. The researcher was interested in checking if this new scheme was going to tamper with the desired output of the selected mobility management protocols. The research then was interested in handling and supporting devices with this new addressing system, the restrictions it would have, the new authentication mechanisms that would fall in line with it, and analysis of its complexity. The researcher collected data and illustrated it as below.

Table 6:Mappable devices

Total Number of devices	Number of IPV4 devices that can be mapped to IPV6	Number of devices already using IPV6	Number of devices that can only support IPV4
150	60	40	50

After conducting the results in a Fisher's Exact test, the following table was generated.

Fisher's Exact Test Results:

Table 7: Fishers test table

	IPV4 Devices	IPV6 Devices
Mappable to IPV6	60	0
	0	40

p-value = 4.576e-55

With such a small p value there is indeed an association between devices mapped on the on the IPV6 network hence the rejection of the null hypothesis.

4.5 Configuration models

The research sought to investigate the choices of configuration models in terms of both automatic configuration and manual configuration. The results were tabled below.

Table 8:Devices on different configuration models

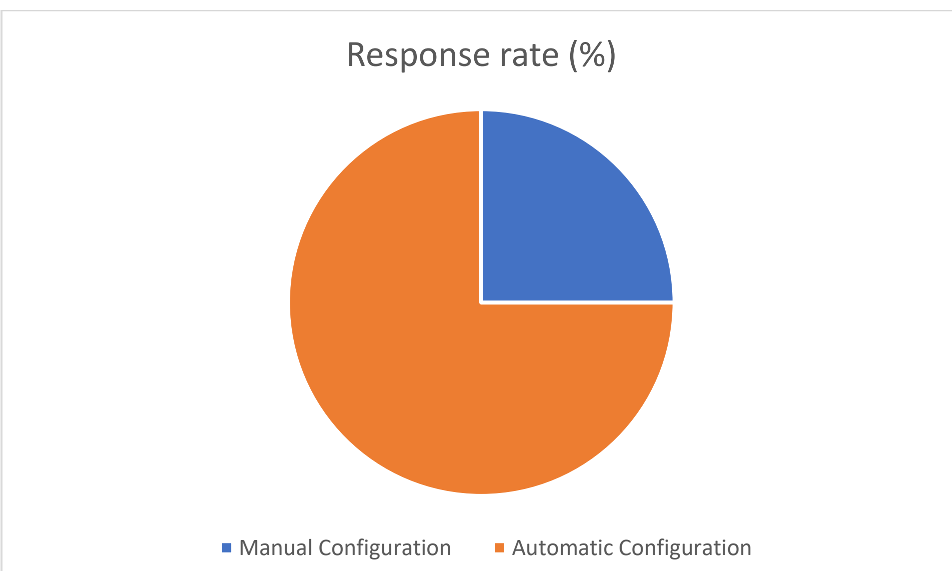
Number of devices that can only support manual configuration	Number of devices that can support automatic configuration	Number of devices that can support both Manual and automatic configuration
35	75	40

The research further sought to find out the response rate of devices that could only allow automatic configuration and those that could allow manual configuration.

Table 9:Type of configuration

	Response rate (%)
Manual Configuration	**25**
Automatic Configuration	**75**
Total	**100**

Figure 3:Representation on the configuration model



4.6 Correlation Representation

Table 10: Familiarity table

	Very familiar	Familiar	Neutral	Not familiar
How familiar are you with the IPV6 technology	13	15	14	18
How familiar are you with IPV6 network protocols	21	11	12	16
How familiar are you with devices working on the network	10	19	15	16
How familiar are you with mobility management in place	15	16	13	16
How familiar are you with configuration models used	15	17	17	11

The researcher chose to use the IT support team proficiency team in the correlation since this team familiarity was deemed very important in the adoption of IPV6 in ABSA bank Nairobi branch. The results above were submitted to chi square tests since they are the methods the researcher wanted to use in determining the relationship between the independent variables and the dependent variable. The table below shows the count of IT professional's familiarity, the expected count used in determining the Pearson chi square and their respective percentages.

Table 11: Chi test table

			Very familiar	Familiar	Neutral	Not Familiar	Total
Technology		Count	13	15	14	18	60
		Expected Count	13.0	15.0	14.0	18.0	60.0
		% within Technology	0.0%	0.0%	0.0%	0.0%	100.0%
		% within IPV6 Technology	21.7%	25.0%	23.3%	30.0%	100.0%
	Network devices	Count	10	19	15	16	60
		Expected Count	10.0	19.0	15.0	16.0	60.0
		% within Technology	16.7%	31.7%	25.0%	26.6%	100.0%
		% within IPV6 Technology	16.7%	31.7%	25.0%	26.6%	100.0%
	Configuration Model	Count	15	17	17	11	60
		Expected Count	14.9	18.6	15.8	10.7	60.0
		% within Technology	25.0%	28.3%	28.3%	18.4%	100.0%
		% within IPV6 Technology	24.8%	31.0%	26.4%	17.8%	100.0%
	Mobility management	Count	15	16	13	16	60
		Expected Count	14.3	17.3	13.6	14.8	60.0
		% within Technology	25.0%	26.6%	21.7%	26.7%	100.0%
		% within Ipv6 Technology	23.8%	28.8%	22.7%	24.7%	100.0%
Network protocols		Count	21	11	12	16	60
		Expected Count	21.0	11.0	12.0	16.0	60.0
		% within Technology	35.0%	18.3%	20.0%	26.7%	100.0%
		% within IPV6 Technology	100.0%	100.0%	100.0%	100.0%	100.0%

From this table majority of the IT professionals were not familiar to the IPV6 technology which was around 30%. For Network devices, configuration model, network protocols and mobility management majority of the team knew about them.

Chi-Square Tests

Table 12:Network protocols Chi test

	Value	Df	Asymptotic Significance (2-sided)
Pearson Chi-Square	12.000[a]	9	.213
Likelihood Ratio	11.090	9	.270
Linear-by-Linear Association	2.100	1	.147
N of Valid Cases	60		

From the table above found during comparison of Network protocols and the adoption of IPV6 a value of 12.000 was found using nine degrees of freedom and an Asymptotic significance of .213 was found. The results show that network protocols are not significant in the adoption of IpV6. Another finding concluded was that there was little or nothing that the IT team in ABSA bank would do to change that since Network protocols were IPV6 stack controlled. The team could only make sure that devices on the network should be IPV6 interoperable.

Chi-Square Tests

Table 13: Configuration model chi test

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	103.544[a]	9	<.001
Likelihood Ratio	112.300	9	<.001
Linear-by-Linear Association	51.822	1	<.001
N of Valid Cases	60		

The table above was made during the comparison of configuration models and adoption of IPV6 in ABSA Bank Nairobi branch. The results were a Pearson Chi-square of 103.544 and an Asymptotic significance <.001 which imply the results are statistically significant. The value is big since most of the devices have options of either choosing between manual and automatic configuration. The automatic devices will either choose SLAAC or DHCPv6 according to the infrastructure of the device.

4.7 Regression analysis

Ridge Regression Coefficients[a]

Alpha		Standardizing Values[c] Mean	Std. Dev.	Standardized Coefficients	Unstandardized Coefficients
1.000	Intercept[b]	.	.	2.524	2.575
	[Network_protocols=1]	.381	.486	-.186	-.383
	[Network_protocols=2]	.167	.373	-.012	-.031
	[Network_protocols=3]	.214	.410	-.019	-.047
	[Network_protocols=4]	.238	.426	.241	.565
	[Configuration_model=1]	.310	.462	-.238	-.515
	[Configuration_model=2]	.238	.426	.037	.086
	[Configuration_model=3]	.310	.462	.128	.277
	[Configuration_model=4]	.143	.350	.101	.288
	[Mobility_management=1]	.310	.462	-.238	-.515
	[Mobility_management=2]	.214	.410	-.117	-.285
	[Mobility_management=3]	.238	.426	.131	.307
	[Mobility_management=4]	.238	.426	.241	.565

a. Dependent Variable: Technology

b. The intercept is not penalized during estimation.

c. Values used to standardize predictors for estimation. The dependent variable is not standardized.

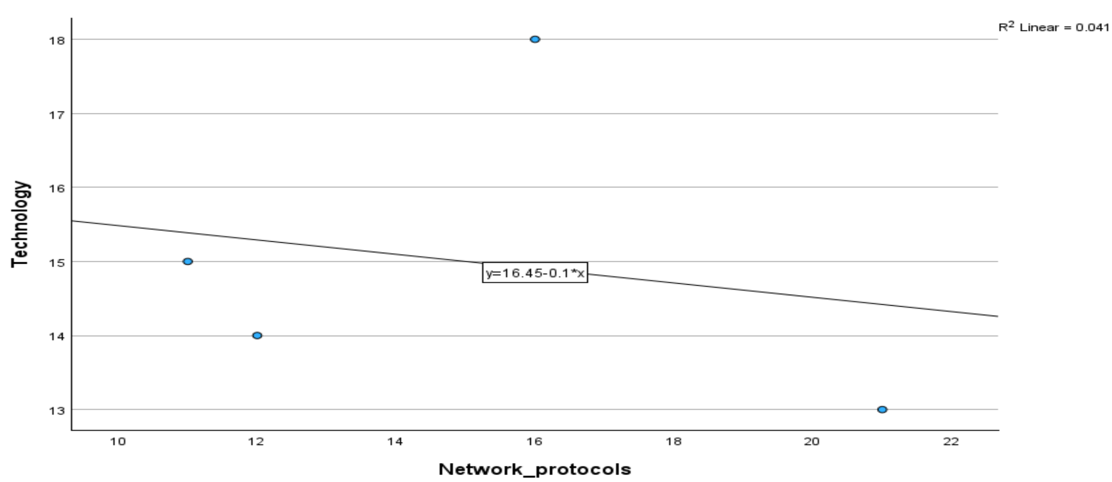
Model Summary[a,b]

Alpha	Training R Square	Holdout R Square
1.000	.928	.919

a. Dependent Variable: Technology
b. Model: Network_protocols, Configuration_model, Mobility_management

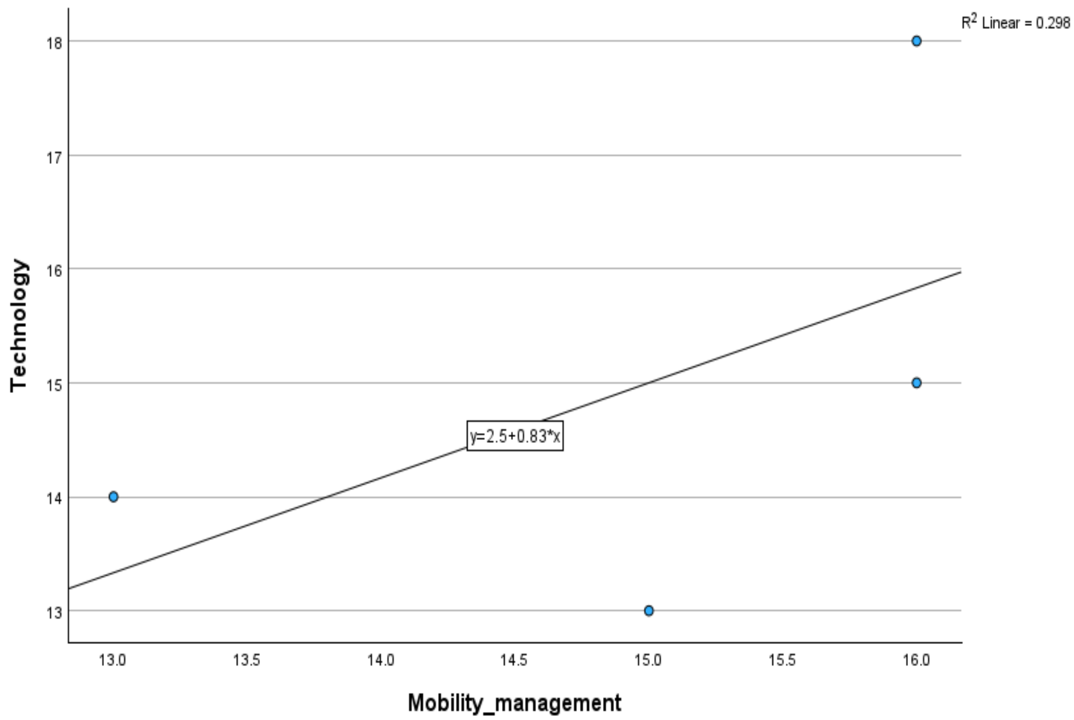
This regression model with the specified independent variables (Network_protocols, Configuration_model, Mobility_management) performs very well, with high R-squared values indicating strong explanatory power both in the training and holdout datasets. This suggests that the model effectively captures the relationship between the independent variables and the dependent variable Technology which represents adoption of IPV6.

Figure 4: Graph on Regression for technology and network protocols



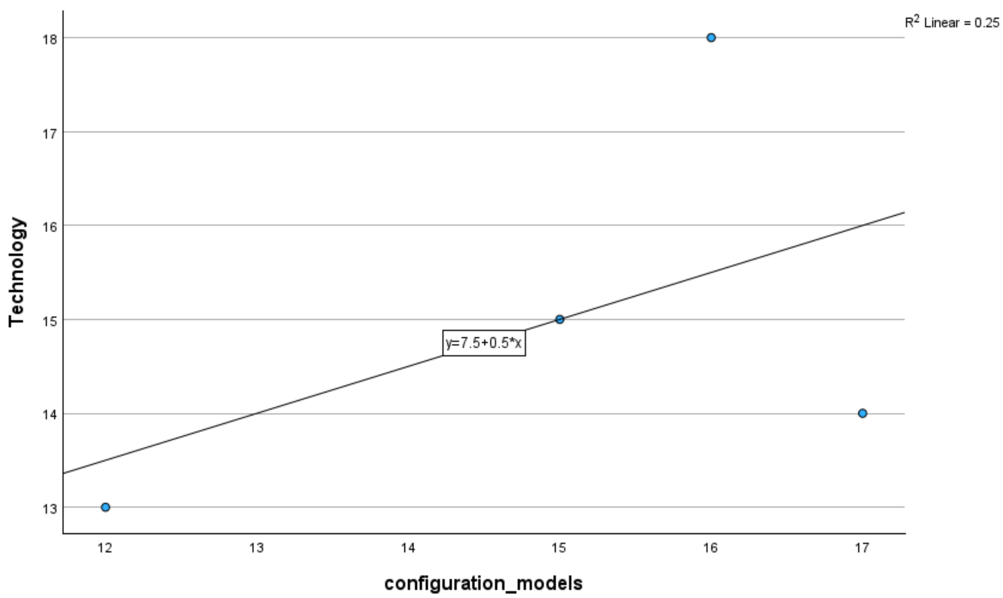
According to the graph above the regression coefficient r^2 linear for technology with network protocols is 0.041 which is a relatively smaller value andindicates that there is little or no relationship between network protocols and technology. The graph also is a line with a negative slope.

Figure 5: Graph for regression between technology and mobility management



According to the graph above the regression coefficient r^2 linear for technology with mobility management protococols is 0.298 which is a relative value and indicates that there is relationship between mobility management protocols and technology. The graph also is a line with a positive gradient**.**

Figure 6:Graph for Regression between technology and configuration model



According to the graph above the regression coefficient r^2 linear for technology with configuration models is 0.25 which is a relative value and indicates that there is a significant relationship between configuration models and technology. The graph also is a line with a positive slope.

CHAPTER 5: SUMMARY, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

In this chapter the researcher is going to focus summary of the findings on the compatibility of devices in the adoption of Internet Protocol Version 6, the conclusions from the research and the possible recommendations on this area. The study used the Kenyan finance industry as an area of interest and Absa Bank Nairobi Branch as its area of study.

5.2 Summary

With the Literature review focused on previous researches, journals related to the compatibility of devices in an IPV6 addressing system environment this research aimed to relate it to adoption in the real world with the finance industry as a case study.

5.2.1 Network Protocols

The researcher guided on the first hypothesis that stated there is no relationship between network protocols and Kenya's readiness for the adoption of IPv6 in the Kenyan Finance Industry; the researcher aimed at investigating the protocol support that had been made in support of this new addressing system and found out that very little protocol support could be provided by the institution under study. This might be that the devices that were being manufactured were using the OSI model which had protocols in its layers it difficult for the IT professionals to have any changes to make.

5.2.2 Mobility Management Protocols

From the findings guided by the hypothesis there is no relationship between mobility management protocols and the readiness for the adoption of IPV6 in the Kenyan Finance Industry it was evident that mobility management protocols had an impact in the adoption of IPV6. Different number of Mobility management protocols which were already in place seemed not to map to the new mobility management protocols that would have to accompany the new addressing system.

5.2.3 Configuration Models

From the findings of this research there was a partial relationship between configuration models and the adoption of IPV6. This was attributed by a significant number of devices that could not map onto the internet automatically using IPV6 addresses. These devices required manual configuration.

5.3 Conclusions

Many older devices, including personal computers, are compatible with IPv4 only.

Some routers and servers do not support IPv6, which means that IPv6-compatible devices might have difficulties connecting to the IPv4 network.

The transition from IPv4 to IPv6 poses challenges due to varying levels of device compatibility.

Ensuring that equipment (such as routers, servers, and personal devices) is IPv6-compatible is crucial for successful adoption.

Current versions of major computer operating systems, including those on mobile devices, built-in support for IPv6.

More recent networking equipment, such as switches, routers, and cable modems, include support for IPv6.

5.4 Recommendations

The Kenyan finance industry to train its IT personnel on IPV6 protocol support since a significant number was not familiar with it.

Upgrading most of the network devices to be mappable to the IPV6 network.

Make a roadmap to help in the future for scalability of more devices on the IPV6 network via the institution's network.

REFERENCES

Alexandra Huides, Evgeny Vaganov, Freddy Hartono, Madhura Kale, Matt Lehwess, Rohit Aswani, Severin Gassauer-Fleissner, Viktor Goldberg (2023). IPv6 on AWS Best practices for adopting and designing IPv6-based networks on AWS. Amazon.

Balfaqih M, Balfaqih Z, Shepelez V, Alharbi SA, Jabbar WA (2020). An analytical framework for distributed and centralized mobility management protocols. Journal of Ambient Intelligence and Humanized Computing.

Balfaqih Z (2020) Design and Development of network simulator module for distributed mobility management protocol. Journal of Ambient Intelligence and Humanized Computing.

D Gu, J Su, Y Xue, J Li, Z Luo & B Yan (2020). Modeling IPv6 from biological evolution. Comp Comms.

Eugene Tikhonov, Donat Schneps-Schneppe, Dmitry Namiot (2021), "Delay Tolerant Network protocols for an Expanding Network on a Railway." Sakheer, Bahrain. IEEE.

F. Gont J. Žorž & R. Patterson (2021). Reaction of IPv6 Stateless Address Autoconfiguration (SLAAC) to Flash-Renumbering Events. Internet Engineering Task Force (IETF).

I Farrer (2022), A Yang Data Model for DHCPv6 configuration model. Internet Engineering Task Force (IETF) RFC 9243

Jia, S.; Luckie M.; Huffaker, B.; Elmokashfi, A.; Aben, E.; Claffy, K.; Dhamdhere, A (2019). Tracking the deployment of IPv6: Topology, routing, and performance. Comput. Netw. 165, 1–15

JL Shah, HF Bhat & AI Khan (2019). Towards IPv6 Migration and Challenges. International Journal of Technology Diffusion. 10(2).

Mahmood A. Al-Shareeda, Selvakumar Manickam, Murtaja Ali Saare, Nazrool Bin Omar (2022) Sadetection: Security Mechanisms to Detect SLAAC Attack in IPv6 Link-Local Network. Al-Shareeda. 46(9)

N Dutta & HKD Sama (2021). Efficient mobility management in IP networks through three-layered MIPv6. Journal of Ambient Intelligence and Humanized Computing.

OI Khalaf & GM Abdulsahib (2021). Design and performance analysis of wireless IPv6 for Data Exchange. Journal of Information Science and Engineering. Vol 37 Issue 6

P Wu, Y Cui, J Wu, J Liu & C Metz (2013). The transition from IPv4 to IPv6; A State of Art Survey. IEEE Communication Surveys and Tutorials. 15(3).

S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury & B. Patil, (2008). Proxy Mobile IPv6, Aug.

T Narten, E Nordmark, W Simpson & H Soliman (2007), Neighbor Discovery for IP version 6 (IPv6), IETC RFC 4861.

Wanjuan Xie, Junhua Yu, Guoqiang Deng (2021). A Secure DHCPv6 System Based on MAC Address Whitelist Authentication and DHCP Fingerprint Recognition. Guiyang, China. IEEE

Z Yan & YH Lee (2019). Mobility Capability Negotiation for IPv6-Based Ubiquitous Mobile Internet. Computer Networks

APPENDICES

APPENDIX I: RESEARCH QUESTIONNAIRE

The main aim of this study is to assess Kenya's readiness for the adoption of IPv6 technology in the Kenyan Finance Industry.

Instructions

You are kindly requested to indicate your level of agreement or disagreement as honestly as possible.

Kindly do not reveal your identity on the questionnaire.

The information gathered will remain confidential to the researchers. Share it with high levels of honesty.

Section A: General questions

1. What is your gender?
   a. Male
   b. Female
   c. Others
2. What is your position? (Engineer, Technician, Administrator, etc.)
   ………………………………………………………………………………………………
3. How long have you been working in this industry?
   ………………………………………………………………………………………………
   ……………………………
4. How would you rate the reliability and availability of the IT infrastructure and systems in supporting the daily operations of this financial firm?
   - Excellent
   - Good
   - Fair
   - Poor
5. Are you satisfied with the level of technical support provided by the IT team?
   - Very satisfied
   - Satisfied
   - Neutral
   - Dissatisfied
   - Very dissatisfied
6. How would you rate the effectiveness of our data backup and disaster recovery procedures?
   - Highly effective
   - Effective
   - Somewhat effective
   - Ineffective
   - I don't know

7. Do you feel adequately trained and informed about the technological policies and practices in this financial firm?
   ……………………………………………..
8. On a scale of 1 to 5, how confident are you in terms of preparation for adopting IPv6?
   - 1: Not confident at all
   - 2: Slightly confident
   - 3: Moderately confident
   - 4: Very confident
   - 5: Extremely confident

9. Are you familiar with the IT governance framework and compliance requirements about the IPv6 in this financial firm?
   - Yes, very familiar
   - Yes, somewhat familiar
   - No, not familiar

10. How well do you think the choices of network protocols in the adoption of IPv6 adhere to regulatory and compliance standards?
   - Fully compliant
   - Mostly compliant
   - Partially compliant
   - Non-compliant

Section B. Specified questions

Give the most appropriate answer based on your opinion. This information will remain confidential to the researcher.

1) In your view does the adoption of a new technology have consequences for the users? Yes/ No?
   Explain……………………………………………………………………………
   ……………………………………………………………………………….
2) About IPv6 technology which network protocol is best suited to handle a large number of users?
   ....
   ....
3) Does the choice of protocol limit the number of users?

   ....
4) Are all network protocols in the IPV4 stack compatible with those in IPv6?

....

5) What factors are considered when choosing Mobility management protocols?

………………………………………………………………………………………

6) Which measures are effective in ensuring Smooth mobility management?

…………………………………………………………………………………………

……………………………………………………………………………………………..

7) How does the configuration model in IPv4 differ from that in IPv6 in the finance industry?

…………………………………………………………………………………………

8) What measures should be put in place for a seamless transition of configuration models?

……………………………………………………………………………………………...

APPENDIX II: RESEARCH BUDGET

ITEM	COST
Printing	2000
Transport	2000
Accommodation	7000
Food	6500
Miscellaneous	3200
Total	20700

Table 14: Research budget

APPENDIX III: WORK PLAN

Table 15: Work plan

TIME ACTIVITY	MAY	JUNE	JULY	OCTOBER	NOVEMBER
Correcting presented proposal					
Preparing questionnaires					
Data collection					
Data analysis					
Report writing and submission					