CONTENTS

LIST OF TABLES

LIST OF FIGURES

EXECUTIVE SUMMARY

The inherent limitation in the address capacity of the Internet Protocol version 4 (IPv4) necessitated the development and current migration to the Internet Protocol version 6 (IPv6).When the IETF published the IPv4 specification in 1981, the U.S population was under 250,000,000, and the world population was around 4.5 billion. IPv4 had been a very robust and successful protocol as it facilitated the expansion of the communications technology moving it from the circuit-switched platform to the packet-switched platform. The advantages of this technology supported the advancement of both data and voice communication (which was mostly circuit-switched) by enabling the development of the Voice over IP for voice transmission over data networks.

However, the development of new technologies and the continuous increase in the number of devices requiring access to the data networks created a need for more internet protocol addresses. Some of these technologies include the Internet of Things which estimates that over 50 Billion devices would be connected to the Internet by 2020. The 5G technology also predicts that more devices would require internet access resulting in an estimate of over 200 Billion IP addresses being needed by the year 2020. The address requirements far exceed the 4.3 Billion address limit of the IPv4 and this was the foundation for the development of the IPv6.

The IPv4 utilized 32 bits for generating the number of addresses while the IPv6 utilized 128 bits to create the IP addresses. The outcome of this bit differential resulted in the generation of 340 Trillion, Trillion, Trillion IP addresses for the IPv6.

This research study utilized an extensive review of relevant literature and the reports of the Internet Assigned Numbers Authority and the regional IP address management organizations. The report then focused on AFRINIC the organization responsible for managing IP addresses in Africa. Selected finding includes the fact that Africa is the only continent which still has IPv4 addresses. It revealed that there is a steady decline in the available IPv4 addresses in Africa. The research findings also reveal the fact that there is a new market for the resale of IPv4 addresses with these addresses being sold for $30 per address.

Cyber security analysis for the IP addresses were also reviewed and the key findings include that fact that there is a need to manage the migration process from the IPv4 to the IPv6 as these migration paths have the capacity to introduce security vulnerabilities on the network which can be utilized by persons with malicious intent. One key outcome of this large IPv6 address number span is the fact that the IPv6 can meet the IP address needs of future communication technologies. The technology has an inbuilt security architecture known as the IPSec which when combined with the large number of addresses eliminate the need for Network Address Translation and thus, enable the implementation of an End to End IP security for the networks. Besides the large IP address bank and IPsec, the IPv6 has several other features which makes it the winning technology for future communication systems. Inspite of the advantages of the IPV6 networks, its adoption will be driven by independent decisions of the individual network operators. For network operators that need to grow, such as mobile networks, IPv6 deployment can make economic sense as it can provide a path out of the operational complexities and costs of large-scale NAT.

This study concludes with key migration pathways and recommendations for a smooth and secure migration to IPv6 taking into account all the possible security gaps and use case scenarios to ensure the deployment of a secure IPv6 network.

CHAPTER ONE

PROJECT BACKGROUND

1.1 Introduction

The advent of IPv6 and the gradual exhaustion of the IPv4 addresses has driven various countries to develop roadmaps for the migration from IPv4 to IPv6 addresses, The lower internet penetration in Africa made her the last continent with some IPv4 addresses but the need to be connected to the global information highway and be shielded from the impact of the IPv4 exhaustion means that Nigeria must also be prepared to migrate to IPv6. This study is the first step in the preparations for migration to IPv6.

1.2 Research Focus

The focus of this research was to explore the benefits of the adoption of IP-based Telecommunications and ICT infrastructure and the evolution of the Telecommunication and Information Technology to the current global standard in the 21st century. The research also explored the key benefits of the all IP ICT infrastructure while discussing the challenges of the technology. It was also to address key issues around the cybersecurity challenges of the IP technology and proffer solutions for mitigating these challenges.

1.3 OBJECTIVES

1. *To identify how IP Architecture structure (IPv4 & IPv6) is implemented and its vulnerabilities.*

2. *To analyze how IP-based Technology help in the prevention of cyber-attacks by means of protecting service providers and end users (cyber security).*

3. *To determine how IP-based Technology enforces permissible-use policies to prevent unauthorized network use and to achieve policy implication.*

4. *To determine how IP-based Technology economics and its financial structure is the driving factor for its rapid acceptance.*

5. *To determine how IP-based Technology aids electronic marketing and distribution channels.*

1.4 SCOPE

1. *To identify the chances of spoofing and denial of service (DOD) and other dynamic, temporary user access through a firewall.*
2. *Recommend regulation on the use of Access Control List (ACLs) that performs packets filtering to control the flow of packets through a network.*

CHAPTER TWO
METHODOLOGY

2.1 Research Methodology And Work Plan

The methodology utilized in undertaking this study comprises of an extensive review of the relevant literature from the IEEE and other related databases. This was complemented by the review of relevant case studies showcasing the applications of the Internet Protocol in communication networks. The research utilized the results of the simulation of data communication and cyber security studies to further support the research findings and conclusions. Summary of the research methodology is shown in Table 1.

*Table 1: **Research Methodology***

Research Approach	**Research Objectives**	**Research Materials and Methods**	**Sources**	**Contribution to Research Aim/Focus**	**Analysis Type**
Define the problem	Project scoping and review of the scope of work	Project Terms of Reference	Contract Document	Research Direction	
Gather Information	Literature Review	Relevant literature	ITU and IEEE journals and papers	Provide Background information on IP implementation and evolution of Information Technology	Qualitative
Develop and Generate Solution	1.To identify how IP Architecture structure (IPv4 & IPv6) is implemented and its vulnerabilities.	Literature Review on IP structure Study and Analysis of IPv4 and IPv6 Implementation and Vulnerabilities	Relevant Journals and Simulation Software	The benefits of adoption of IP6 and IPv6. IPv4 and IPv6 Architecture and Implementation	Qualitative and Quantitative
	2.To analyze how IP-based Technology help in the prevention of cyber-attacks by means of protecting service providers	Study of cybersecurity strategies for IP based networks Simulation of IP technologies, Cyber Attacks and Cyber security	Short course on Cyber security strategies Simulation Software for cybersecurity analysis and training on	Challenges of current Information Technology standards	Qualitative and Quantitative

	and end users (cyber security).	protection strategies	simulation package		
	3.To determine how IP-based Technology enforces permissible-use policies to prevent unauthorized network use and to achieve policy implication.	Study permissible use policies used to prevent unauthorized network use and policy implementation strategies Simulate IP based network and permissible use policies to prevent unauthorized network use and policy implementation	Simulation Software. Related case studies and relevant ITU and IEEE Literature	Recommend regulation on the use of Access Control List (ACLs) that performs packets filtering to control the flow of packets through a network	Qualitative
	4. To determine how IP-based Technology economics and its financial structure the driving factor for its rapid acceptance.	Study the economics of IP based technology and its financial structure. Show the characteristics of technologies that enable the acceptance of that technology in telecommunication systems Show a mapping of how the technology economics and financial structure support the rapid acceptance of the Technology	Selected Case Studies Selected Journals and Conference papers from the IEEE and ITU	Key benefits of the all IP ICT infrastructure while discussing the challenges of the technology and conclude with the development of a conceptual framework for the continuous advancement of the technology in the face of the current cybersecurity challenges	Qualitative
	5. To determine how IP-based Technology aids electronic marketing and distribution channels.	Study and analyze the relationship between IP based technology and Electronic Marketing	Selected Journals and Conference papers from the IEEE and ITU	Key benefits of the IP-based Technology	Qualitative

CHAPTER THREE

GLOBAL IP ADDRESS MANAGEMENT

3.1 Internet Assigned Numbers Authority

IP addresses are managed by the **Internet Assigned Numbers Authority** (IANA) and this organization delegates Internet resources to the Regional Internet Registry (RIR).[1] The RIRs delegate these Internet resources to their customers following laid down policies. Their customers include Internet service providers and end-user organizations.[2] The RIRs are an integral part of the Number Resource Organization (NRO) which was formed to represent their collective interests, undertake joint activities and coordinate their activities globally. The NRO in collaboration with the Internet Corporation for Assigned Names and Numbers (ICANN)[3] established the Address Supporting Organization (ASO) which undertakes coordination of global IP addressing policies within the ICANN framework[4].

3.2 Number Resource Organization

The **Number Resource Organization** (**NRO**) [5]was set up on the 24th of October 2003 and the goal was to unite all the RIRs. The four existing RIRs at the time entered into a memorandum of understanding (MoU) in order to undertake joint activities such as joint technical projects and policy coordination. AFRINIC later joined in April 2005.

The NRO's main objectives are to[6]:

- Protect the unallocated IP number resource pool
- Promote and protect the bottom-up policy development process of the Internet
- Serve as a focal point for the Internet community to provide input on the RIR system

3.3 Regional Internet Registry

The allocation of Internet addresses is managed by the Regional Internet Registries for the different regions[7]. The internet number resources include the IP addresses and Autonomous

[1] IANA. https://www.iana.org/
[2] IANA https://www.ripe.net/participate/internet-governance/internet-technical-community/iana
[3] ICANN-ASO. https://aso.icann.org/about/
[4] Address Supporting Organization (ASO) Review. https://www.icann.org/resources/reviews/org/aso
[5] NRO. https://www.nro.net/
[6] Number Resource Organization. https://www.internetsociety.org/resources/deploy360/2012/number-resource-organization/
[7] Regional Internet Registries. https://www.nro.net/about/rirs/

System (AS) numbers. An Autonomous System is a network with internet protocol addresses under the control of one organization or one administrative entity.[8] These networks are under the control of one or more network operators with a single administrative domain. The ASN is usually subject to a common clearly defined routing policy.[9]

The regional Internet registry system evolved over time, eventually dividing the responsibility for management to a registry for each of five regions of the world as shown in figure 1.

The regional registries are[10]

1. The African Network Information Center (**AFRINIC**) which serves Africa
2. The American Registry for Internet Numbers (**ARIN**) which serves Antarctica, Canada, parts of the Caribbean, and the United States.
3. The Asia-Pacific Network Information Centre (**APNIC**) which serves East Asia, Oceania, South Asia, and Southeast Asia
4. The Latin America and Caribbean Network Information Centre (**LACNIC**) which serves most of the Caribbean and all of Latin America.
5. The Réseaux IP Européens Network Coordination Centre (**RIPE NCC**) serves which Europe, Central Asia, Russia, and West Asia.

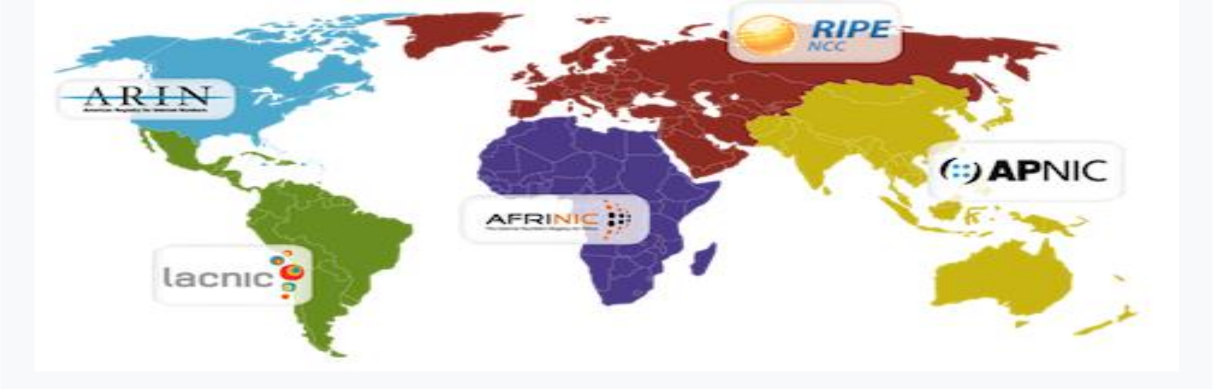


Figure 1. Map of regional Internet registries[9]

3..4 Local Internet registry

A **local Internet registry** (**LIR**) is the last mile in the IP address allocation. It is an organization that has been allocated a block of IP addresses by a RIR, and that assigns most

[8] The Internet Registry System. https://www.ripe.net/participate/internet-governance/internet-technical-community/the-rir-system

[9] History of the Regional Internet Registries. https://www.apnic.net/about-apnic/organization/history-of-apnic/history-of-the-regional-internet-registries/

[10] History of the Regional Internet Registries. https://www.apnic.net/about-apnic/organization/history-of-apnic/history-of-the-regional-internet-registries/

parts of this block to its own customers. Internet service providers, enterprises, or academic institutions make up most of the LIRs.

3.5 IPv4 address Exhaustion.

The African Network Information Center (AFRINIC) is currently the only regional internet registry that is still using the normal protocol for distributing IPv4 addresses[11]. A LIR is entitled to additional allocations when it has utilized about 80% of all its address space.[12] As of November 2018, AFRINIC had a minimum of 1024 IPv4 addresses while by November 25, 2019, RIPE NCC announced that it had fully run out of IPv4 addresses and called for greater progress on the adoption of IPv6[13][14]

These IPv4 usage statistics from the registries as at 2019 indicates the following:

1. APNIC exhausted its addresses on the April 15th 2011
2. RIPE NCC exhausted its addresses on the 14th of September 2012
3. ARIN reached the final /8 address amount on the 23rd of April 2014
4. LACNIC ran out of addresses on the 10th of June 2014
5. AFRINC's supply is expected to be exhausted in a couple of years

[11] AFRINIC IPv4 Exhaustion. https://www.afrinic.net/exhaustion

[12] Phases of IPv4 Exhaustion. https://www.lacnic.net/1039/2/lacnic/phases-of-ipv4-exhaustion

[13] Next Generation Internet: IPv4 Address Exhaustion, Mitigation Strategies and Implications for the U.S. An IEEE-USA White Paper 2009. https://ieeeusa.org/wp-content/uploads/2017/07/IEEEUSAWP-IPv62009.pdf

[14] BT begins trial of IPv6 as IPv4 address exhaustion looms. https://arstechnica.com/information-technology/2015/07/bt-begins-trial-of-ipv6-as-ipv4-address-exhaustion-looms/

The global IPv4 exhaustion graph is shown in figure 2

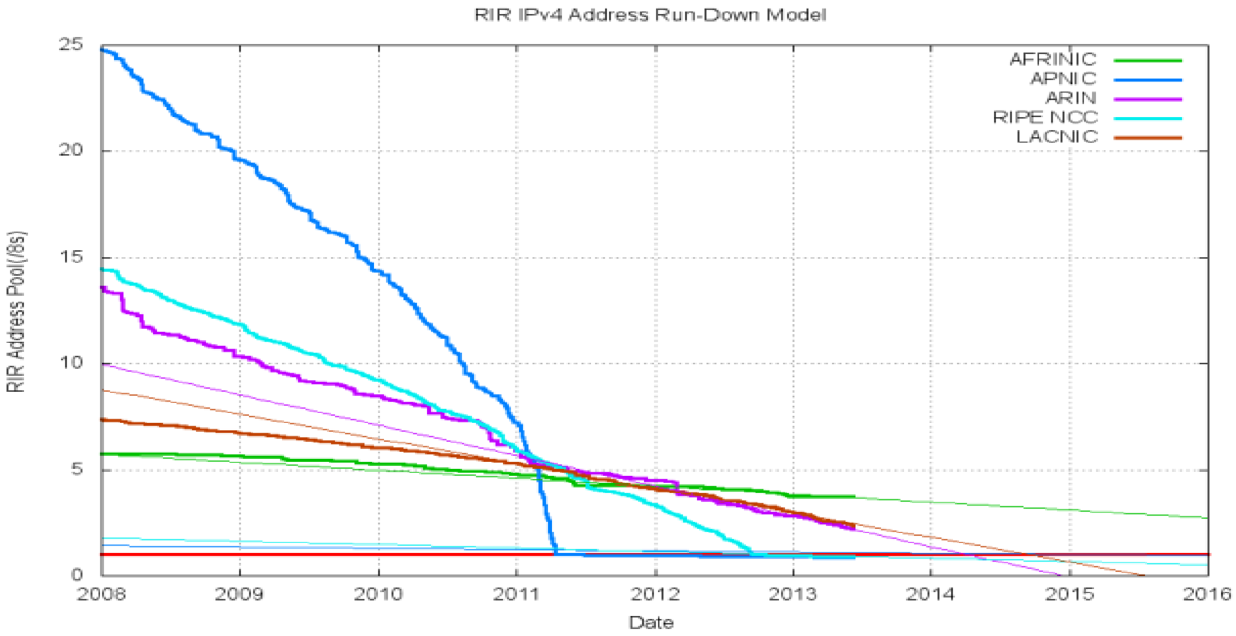


Figure 2. Global IPv4 Exhaustion graph.[15]

[15] BT begins trial of IPv6 as IPv4 address exhaustion looms. https://arstechnica.com/information-technology/2015/07/bt-begins-trial-of-ipv6-as-ipv4-address-exhaustion-looms/

CHAPTER FOUR
IPV6 DEPLOYMENT STATUS

4.1 Global Deployment of IPv6

Among the early adopters of the IPv6 address system were Universities. Virginia Tech deployed IPv6 at a trial location in 2004 and this installation was later expanded across the campus. The traffic grew to a point where over 82% of their network traffic used IPv6. Another institution which experimented with IPv6 was Imperial College London. An experimental network was deployed in 2003 and by 2016, the total IPv6 traffic on their networks averaged between 20% to 40%. The key driver of this growth at Imperial College was the high energy physics collaboration with CERN the European organization for Nuclear Research, which had all its IP traffic through IPv6.[16].

IPv6 continued to increase such that by 2011, all major operating systems in use on personal computers and server systems had production-quality IPv6 implementations. The migration from 3G to 4G also led to a sharp increase in IPv6 deployment in cellular telephones as voice transmissions were packaged as a voice over IP (VoIP) service that would leverage IPv6 enhancements. Verizon, a cellular operator in the US In 2009 released a technical specification for devices to operate on its "next-generation" networks. The specification mandated IPv6 operation according to the *3GPP Release 8 Specifications (March 2009)*, and deprecated IPv4 as an optional capability[16].

The Internet backbone was another infrastructure that supported the growth of IPV6. As at 2018 only 25.3% of the about 54,000 autonomous systems advertised both IPv4 and IPv6 prefixes in the global Border Gateway Protocol (BGP) routing database. An extra 243 networks advertised only an IPv6 prefix. Internet backbone transit networks with IPv6 support were available in every country, except for parts of Africa, the Middle East and China. Some major European broadband ISPs deployed IPv6 in mid-2008 for the majority of their customers. 86% of British Sky Broadcasting customers were provided with IPv6, while Deutsche Telekom in Germany had 56% deployment of IPv6, XS4ALL in the Netherlands had 73% deployment and in Belgium the broadband ISPs VOO and Telenet had73% and 63% IPv6 deployment

[16]State of IPv6 Deployment 2018. Key points. Internet Society https://www.internetsociety.org/resources/2018/state-of-ipv6-deployment-2018/

respectively. Comcast, an ISP in the United States the broadband had an IPv6 deployment of about 66%. She reported an estimated 36.1 million IPv6 users, while AT&T reported 22.3 million IPv6 users. [17][15]

The following are some statistics of IPv6 global deployment.

- **Over 25% of all Internet-connected networks advertise IPv6 connectivity**.
- Google reports **49 countries deliver more than 5% of traffic over IPv6**, with new countries joining all the time.
- Google reports **24 countries whose IPv6 traffic exceeds 15%**.

Figure 3 shows the global deployment of IPv6 indicating countries with greater than 15% deployment.

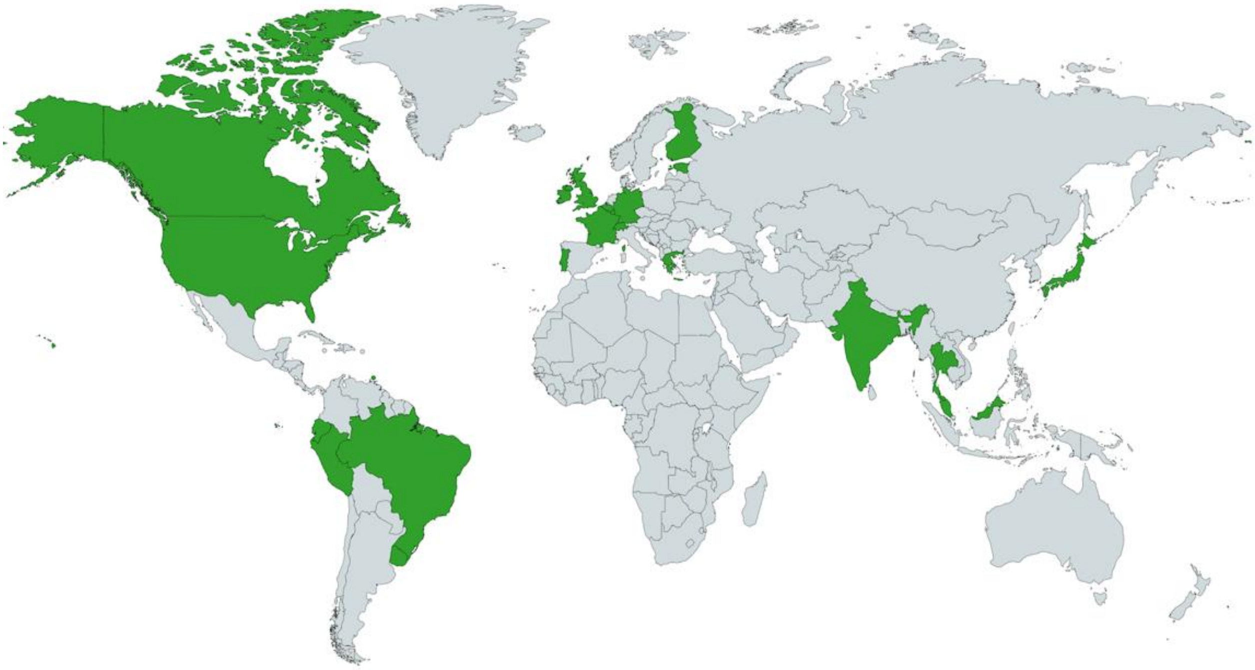


Figure 3. Countries with IPv6 deployment greater than 15%[18]

The adoption of IPv6 is also being driven by major mobile communication operators. Examples include where NTT – has about 7% IPv6 deployment, KDDI has 42% and Softbank has 34% deployment. In India Reliance JIO has 87% and the USA, Verizon Wireless has 84%, Sprint has 70%, T-Mobile USA has 93%, and AT&T Wireless has 57%. Many national mobile

[17] Stephen Ugwuanyi, Fouead Attaran, Syeed Hussaini, Ahmed Merehil. The State of IPv6 Deployment: A global Review. International Journal of Scientific & Engineering Research, Volume 8, Issue 4, April-2017

[18] State of IPv6 Deployment 2018. Key points. Internet Society https://www.internetsociety.org/resources/2018/state-of-ipv6-deployment-2018/

networks have very high levels of IPv6 deployment and some of these national networks are taking steps to run IPv6-only networks to simplify network operations and reduce costs.

Figure 4 shows web content access data from Alexa top 1000 websites in 2018 shows that 28% of these sites are access from IPv6, an increase from 23% in 2017.

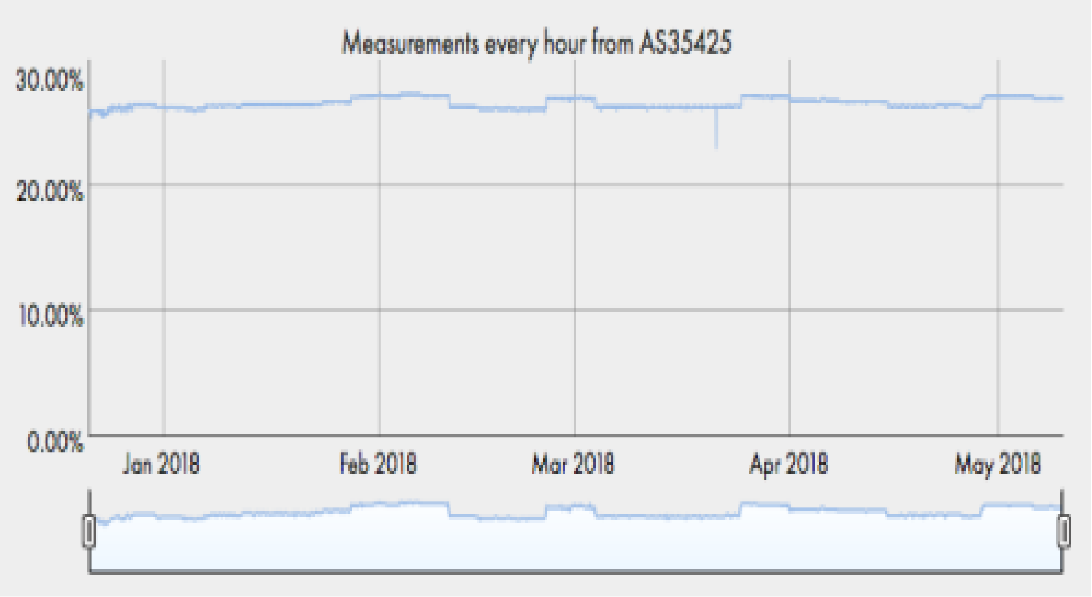


Figure 4. Percentage of Alexa Top 1000 websites reachable over IPv6.[19]

Belgium was the first country in the world to regularly deliver more than 50% of traffic to major content providers over IPv6 while nearly half of all IPv6 users on the planet today are in India where an estimated 270 million users have IPv6 connectivity to the Internet. Among the G20 nations, 13 of them deliver more than 5% of their traffic to Google over IPv6 while 7 of the G20 countries namely China, Indonesia, Italy, Russia, South Africa, Spain and Turkey have less than 5% IPv6 deployment. This is shown in Figure 5.

[19] State of IPv6 Deployment 2018. Key points. Internet Society https://www.internetsociety.org/resources/2018/state-of-ipv6-deployment-2018/

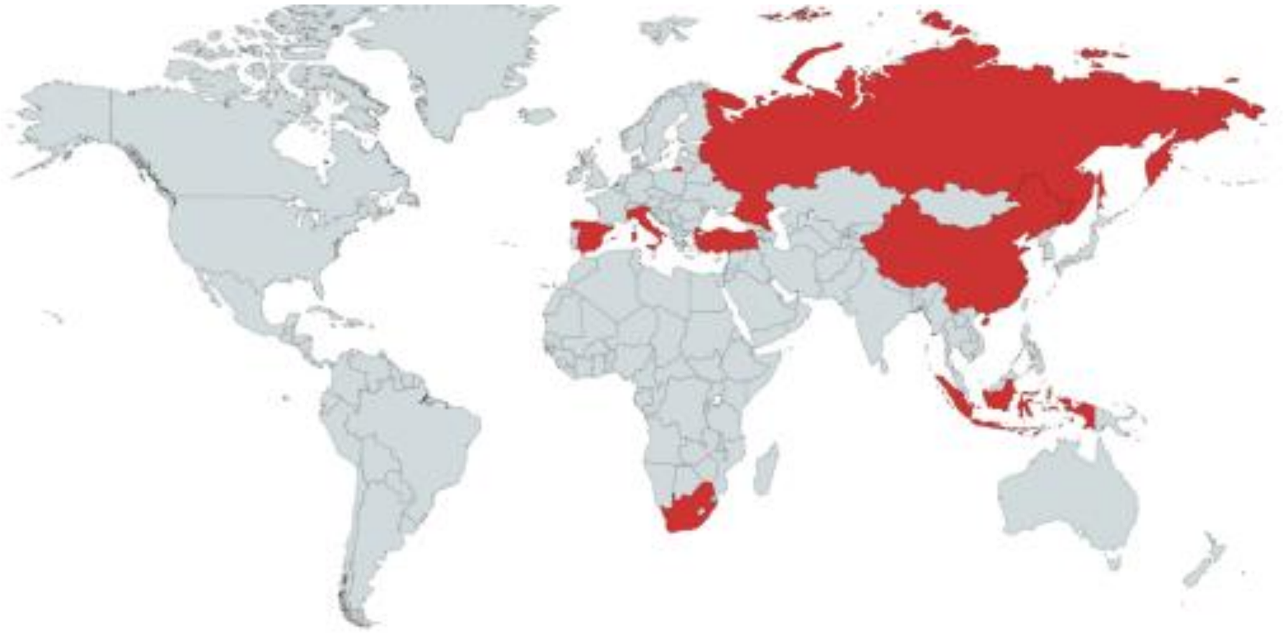


Figure 5. G20 countries with less than 5% IPv6 deployment. [20]

4.2 Operator case studies.[20]

1. Reliance JIO

Reliance JIO commenced deployment of IPv6 after its local Internet registry ran out of IPv4 address space. The company was faced with the option of buying IPv4 but took a business decision to migrate IPv6. As of February 2017, Reliance reported that about 90% of its LTE customers are using IPv6, representing about 80% of their traffic. This is driven, largely by their principal content partners, Google, Akamai, and Facebook, who began took a decision to deliver their content only using IPv6 in that network. Between September 2016 and June 2017, a space of nine months, Reliance activated over 200 million subscribers with IPv6 connectivity.

2. Verizon Wireless

Verizon began to proactively deploy IPv6 even though they had an existing IPv4 network. The company was facing network challenges due to IPv4 conflicts resulting in high network management costs and complexity. The company opted for IPv6 deployment as a solution and it simplified their network and reduced their network operating costs. Over 80% of traffic from Verizon Wireless to major online content providers now uses IPv6.

[20] State of IPv6 Deployment 2018. Key points. Internet Society https://www.internetsociety.org/resources/2018/state-of-ipv6-deployment-2018/

3. T-Mobile USA

T-Mobile is another mobile operator in the US that is in the process of turning off IPv4 within their mobile network and migrating to IPv6-only network configuration.

4. Facebook

Facebook is also in the process of turning IPv4 off within their datacenters; IPv4 and IPv6 from outside comes to their load balancers, and behind them it is only IPv6. The effect has been operational improvements and innovation in their software.

Other companies, including *LinkedIn* and *Microsoft*, have similarly stated an intention to turn IPv4 off within their networks.

The global deployment of IPv6 shows an increasing trend. Table 1 shows the list of countries and operators with IPv6 deployed in their networks. It also shows their deployment rank and the percentage of IPv6 deployment in their networks.

Table 2. Summary of IPv6 Global Deployment IPv6 percentage deployments in their networks.[21]

Rank	Participating Networks	Percentage IPv6 Deployment
1	Comcast	66.3%
2	Reliance JIO Infocomm LTD	86.09%
3	KDDI	42.22%
4	SoftBank	33.77%
5	ATT	65.95%
6	Charter Communications	31.65%
7	Verizon Wireless	85.51%
8	T-Mobile USA	93.69%
9	Vivo	42.00%
10	Deutsche Telekom AG	56.06%

Table 2 shows the number of IPv6 Users and their ISP. From this data, India’s Reliance Jio is ranked number 1 for the number of IPv6 users on its network while Comcast of the US is ranked number 2. The other rankings are shown in table 2.

[21] State of IPv6 Deployment 2018. Key points. Internet Society https://www.internetsociety.org/resources/2018/state-of-ipv6-deployment-2018/

Table 3. IPv6 User population and ISP

From the data shown in the tables 1 and 2, the key drivers for IPv6 deployments include the operational simplification that comes from removing overlapping address space from the network, the reduced operational costs of managing such complex networks, and the minimization of shocks to networking business that arise when additional address space is unavailable or requirements to deploy IPv6 arrive with a short time horizon.

Studies have also shown that many networks have IPv6 on their backbone but not to their end-users. Akamai reports that of the top 55 networks they interconnect with more than half have IPv6 deployment greater than 2% and these networks account for half of the residual IPv4 traffic that Akamai sees. Greater deployment efforts from this relatively small number of networks could yield huge increases in overall IPv6 deployment measured globally.

Google statistics show that over 30% of all traffic on google sites are over IPv6. Some countries are also being reported to have over 50% of all traffic going to google going over IPv6. Figure 6 shows the global IPv6 adoption which is seen to be on the increase[22].

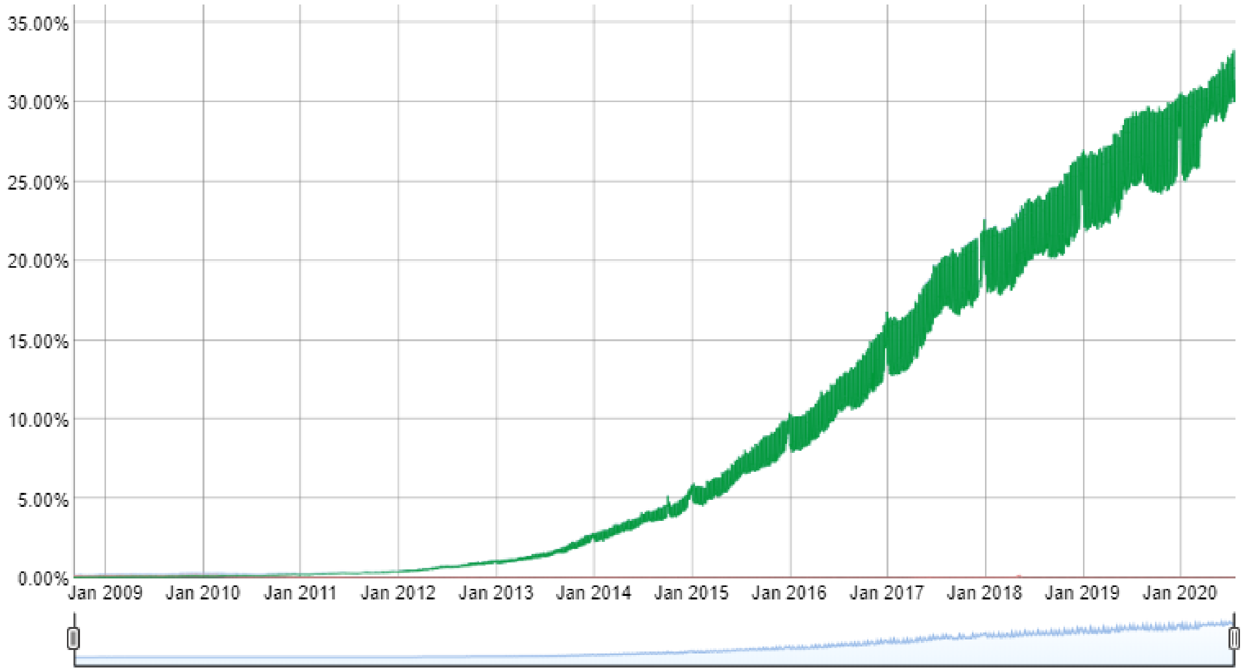


Figure 6. Global IPv6 Adoption[23]

[22] State of IPv6 Deployment 2018. Key points. Internet Society https://www.internetsociety.org/resources/2018/state-of-ipv6-deployment-2018/

[23] Global IPv6 Adoption. https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption.

A survey of major ISPs asking for the main incentive for IPv6 deployment showed that sustained customer and network growth were their key drivers for IPv6 rollout. Other incentives for IPv6 deployment are listed below

Network efficiency: IPv6 supports much larger packet size, and therefore makes network faster.

Business Agility: No more NAT and network management with big companies having to use a fragmented network in terms of addresses.

Competitive Differentiation

- Content that use a high bandwidth such as Google maps is no longer limited by the number of ports and TCP connections it opens.
- Having the MAC address inside the IPv6 address allows ISPs and mobile operators to control much more easily traffic coming from connected devices and also to provide a more personalized service to customers.

Figure 7 shows a global increase in the deployment of IPv6-enabled websites

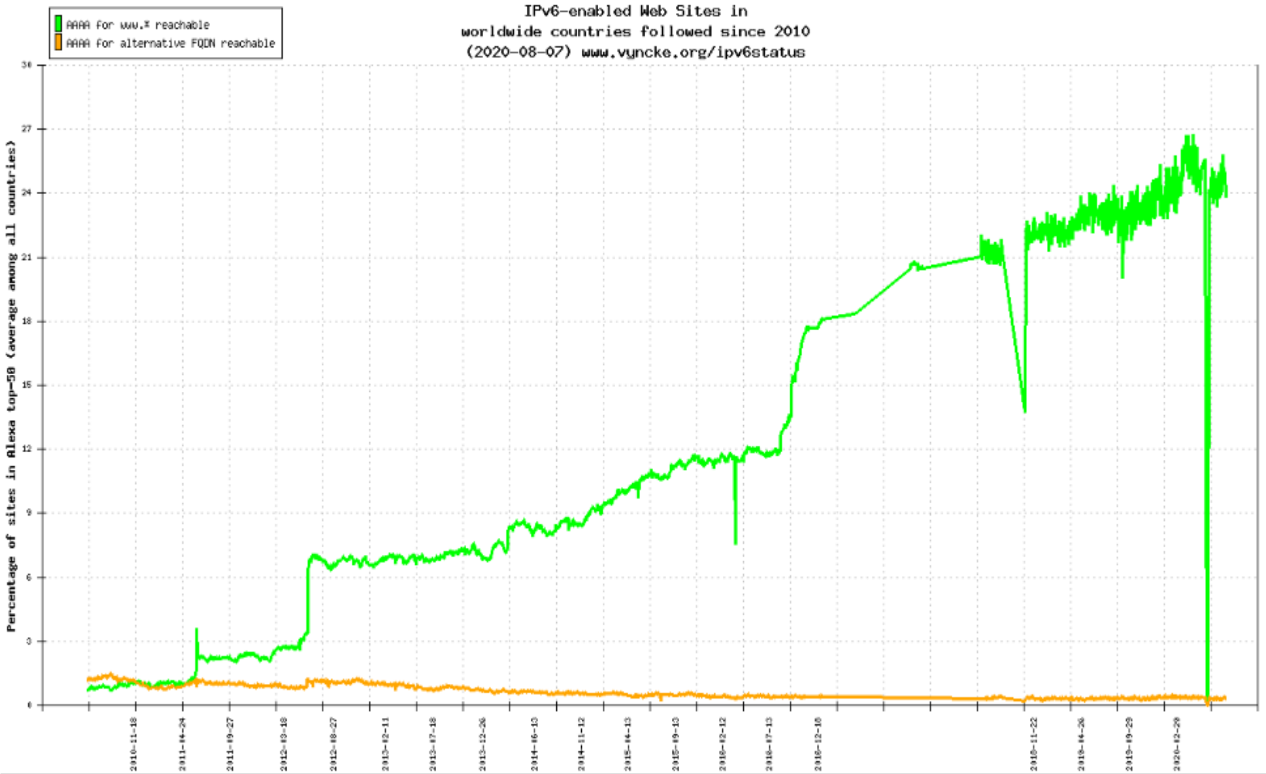


Figure 7. IPv6 -enabled website deployment. [24]

[24] IPv6 Deployment Aggregated Status. https://www.vyncke.org/ipv6status/

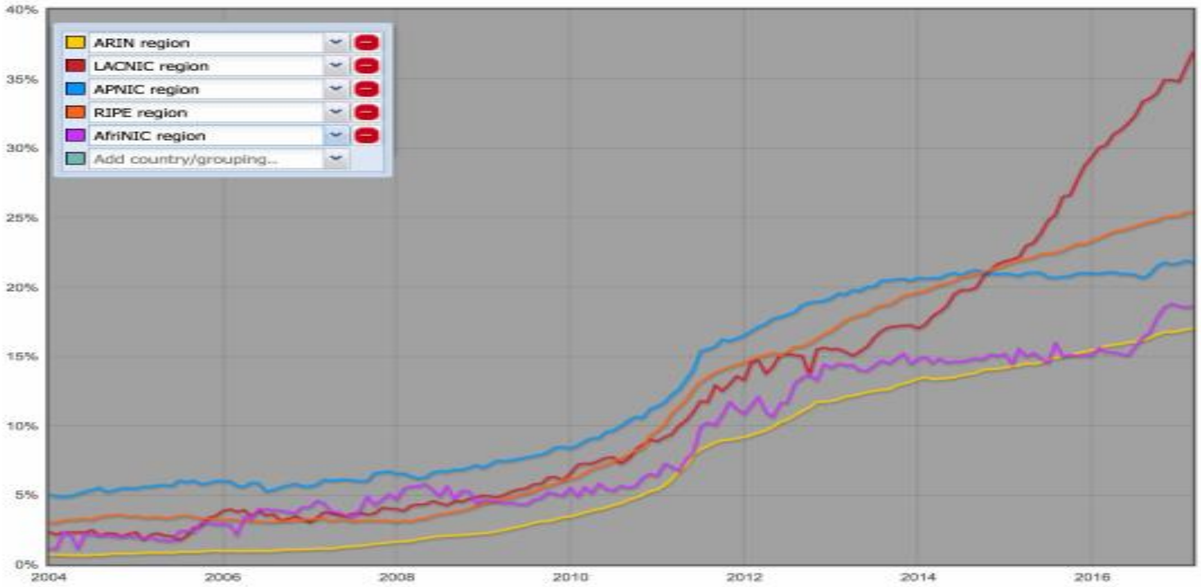


Figure 8. IPv6 routing support[24]

One critical factor for the increasing adoption and penetration of the IPv6 is the increasing support the protocol enjoys from all major Internet protocols. Figure 8 shows this trend across all the regions. Figures 9 and 10 shows this increasing trend in the number of Global IPv6 addresses and IPv6 users

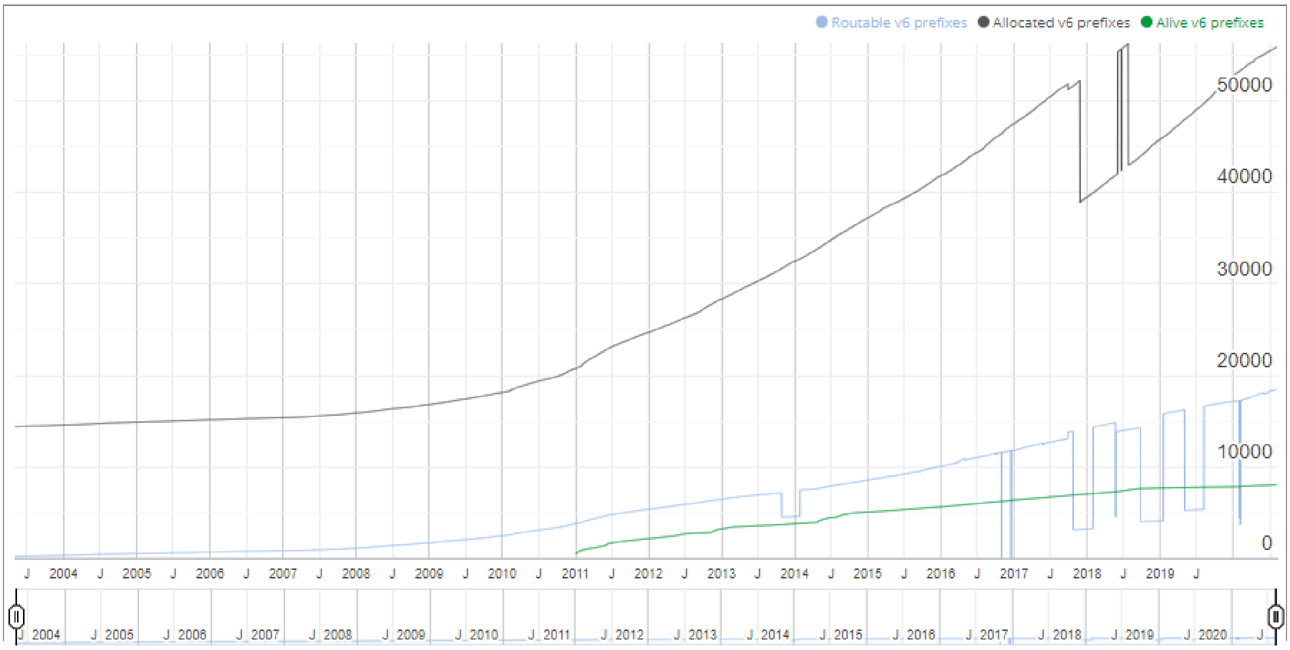


Figure 9. World IPv6 addresses [25]

[25] IPv6 Deployment Aggregated Status. https://www.vyncke.org/ipv6status/

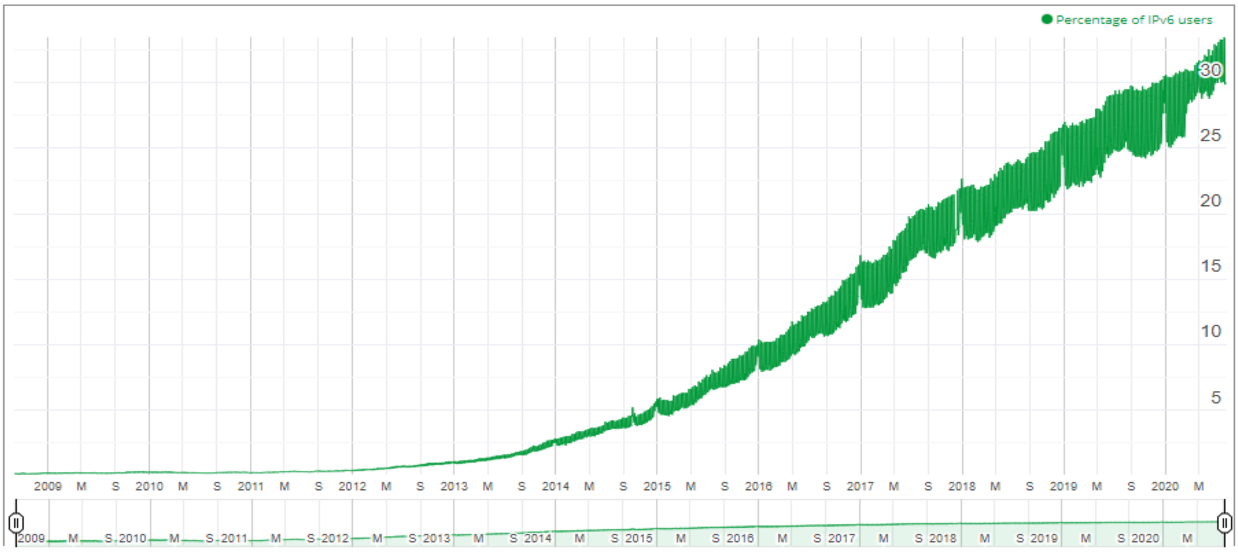


Figure 10. Percentage of Global IPv6 Users[26]

[26] CISCO. 6lab - The place to monitor IPv6 adoption. https://6lab.cisco.com/stats/cible.php?country=world&option=prefixes

CHAPTER FIVE
IPV6 DEPLOYMENT IN AFRICA

5.1 IPV6 Management in Africa

AFRINIC is the Regional Internet Registry (RIR) for Africa and the Indian Ocean and ensures fair management and distribution of Internet number resources in the African region. Set up in 2005, AFRINIC has been managing a pool of Internet Number Resources and delegating them to organizations that could justify the need to receive the resources. The management of the resources is done in accordance with resource policies and these policies are consolidated in the policy manual. The AFRINIC community proposed and supported the IPv4 Soft Landing policy to address the scarcity of IPv4 in the AFRINIC service region. This policy aims to guide AFRINIC membership regarding the exhaustion of AFRINIC's IPv4 address space, ensure better management of the IPv4 pool in the scarcity period for a smooth transition to IPv6. [27]

In February 2011, the IANA (now known as Public Technical Identifiers - PTI) allocated two large blocks of IPv4 address space to APNIC, causing the global IPv4 pool to deplete to a critically low level. This triggered the "Global Policy for the Allocation of the Remaining IPv4 Address Space". Each RIR then received one /8 each, which is around 16.8 million IPv4 addresses, depleting IANA's pool of available IPv4 address space and setting the ball rolling for global IPv4 exhaustion.

As at 24 September 2015, four of the five RIRs - APNIC, ARIN, LACNIC and the RIPE NCC - have exhausted their free pools of IPv4 and began allocating IPv4 address space from the final /8 they received from the IANA. The timelines for the management of the remaining IPv4 addresses from AFRINC is shown below.

- On 16 January 2017, AFRINIC announced that it is approaching Stage 1 of its IPv4 Exhaustion process.
- On 31st March 2017, AFRINIC announced the start of Phase 1 of the Soft-landing policy for IPv4 Exhaustion.
- On 19th August 2019, AFRINIC announced that it is approaching Phase 2 of the Soft-landing policy for IPv4 Exhaustion

[27] AFRINIC IPv4 Exhaustion statistics. https://stats.afrinic.net/ipv4/exhaustion

5.2 Soft Landing Policy

In a bid to ensure a smooth transition to IPv6, AFRINIC developed a policy known as the soft-landing policy which is aimed at ensuring the members have access to address space after the IPv4 pool is depleted. The key target of this policy is to help in maintaining IPv4 networks while deploying IPv6 networks – This is a practice that characterizes the transition period.[28]

5.2.1 IPv4 Exhaustion Phases

During the Exhaustion Phase, the following allocation and assignment guidelines are applicable. They apply to both LIRs and End Users, and to all IPv4 address, space allocated, assigned, or otherwise managed by AFRINIC during the transition to and after the beginning of the Exhaustion Phase, regardless of whether or not such IPv4 address space is a part of the Final /8. The exhaustion phase is divided into two parts: Phase 1 and Phase 2. This is shown in Table 3.

Table 4. AFRINIC IPv4 Exhaustion Phases[29]

Phase	Description
Current (at the time the soft-landing policy was ratified)	AFRINIC has IPv4 address space available in its free pool. It can assign IPv4 address space to its members according to justified need as documented in the current policy. AFRINIC has transitioned past this phase
Phase 1 - AFRINIC has transitioned to this phase since 31 March 2017	AFRINIC will enter Phase 1 when an otherwise valid request for IPv4 address space from an LIR or end-user to AFRINIC either:(a) cannot be fulfilled with the IPv4 address space available in the AFRINIC pool (with the exception of the final /8), or(b) can be fulfilled, but would leave the AFRINIC IPv4 address pool empty (with the exception of the final /8).
Phase 2 - AFRINIC has not yet reached this phase	Phase 2 begins when AFRINIC has no more than one /11 of non-reserved IPv4 space available in the final /8.

[28] AFRINIC IPv4 Exhaustion statistics. https://stats.afrinic.net/ipv4/exhaustion
[29] AFRINIC IPv4 statistics. https://stats.afrinic.net/ipv4/

5.2.2 IPv4 Allocation in Africa.

The allocation of IPv4 addresses in Africa is represented by the Pie chart shown in figure 11.

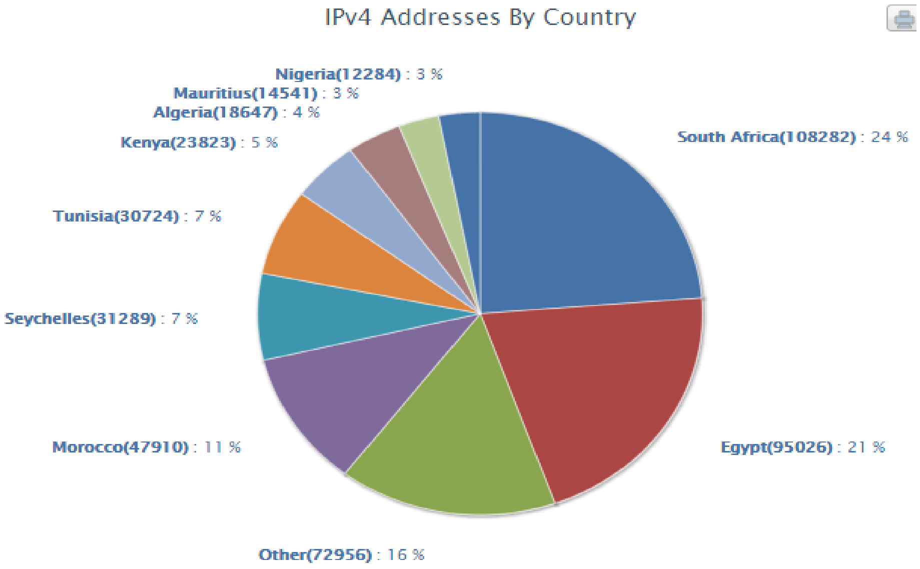
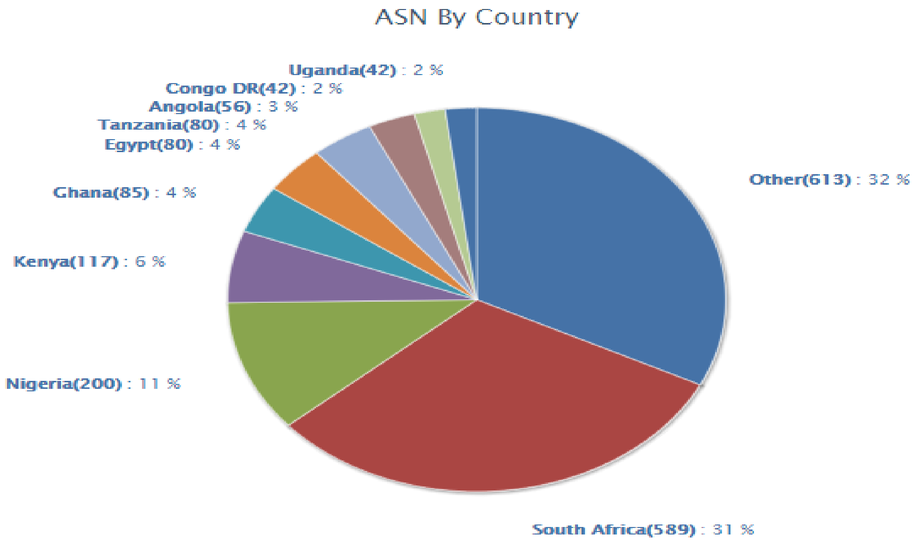


Figure 11. IPv4 Distribution in Africa[30]

This distribution shows South Africa to have the highest number of IPv4 addresses with 24% or a total of 108282 addresses followed by Egypt with 21% or a total number of 95,026 addresses. Nigeria shares the 8th position with 3% of the total IPv4 addresses or total number of 12284 IPv4 addresses.



[30] AFRINIC IPv4 statistics. https://stats.afrinic.net/ipv4/

Figure 12.IPv4 ASN allocation in Africa[31]

The distribution of the IPv4 Autonomous System Numbers is shown in Figure 12. South Africa again had the highest number of 589 or 31% with Nigeria having the second highest number with 200 or 11%. The ASN is an indication of the IP addresses assigned to corporate organizations and this data shows that Nigeria had the second largest number of corporate bodies with ASN allocations in Africa. The exhaustion of the IPv4 addresses is represented in the chart shown in figure 13. This chart shows that over 80% of the IPv4 allocated to AFRINIC has been allocated and the IPv4 addresses remaining are below 20%

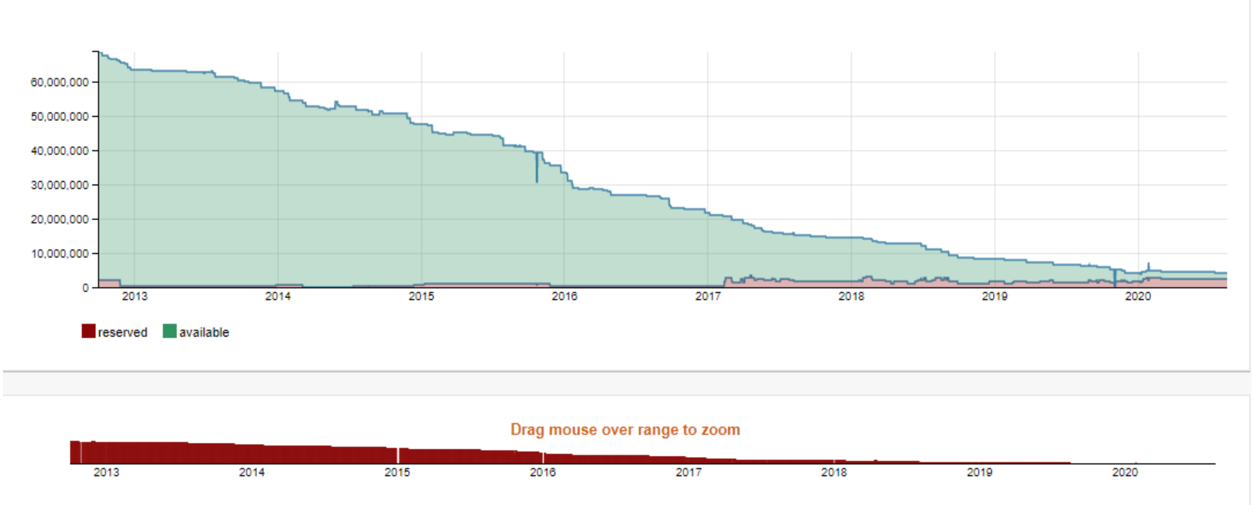


Figure 13. IPv4 Exhaustion in Africa[32]

5.2.3 IPv6 Allocation in Africa

There are currently 51 countries in Africa with IPv6 addresses. The top 5 of these African countries listed below.[33]

1. South Africa (325 prefixes),
2. Nigeria (81),
3. Kenya (58),
4. Tanzania (50),
5. Ghana (35)

The allocation of IPv6 addresses in Africa has commenced with the trends showing a correlation to the IPv4 allocation. The concentration of the IPv6 addresses already allocated is

[31] AFRINIC IPv4 statistics. https://stats.afrinic.net/ipv4/
[32] AFRINIC IPv4 Exhaustion statistics. https://stats.afrinic.net/ipv4/exhaustion
[33] AFRINIC IPv6 statistics. https://stats.afrinic.net/ipv6

represented in Figure 14 with South Africa having the highest number of IPv6 addresses issued. Over three hundred IPv6 addresses have already been issued in South Africa. Figure 15 shows the industry allocations for the IPv6. This chart shows that both the ISPs and telecommunication companies are almost at par in terms of IPv6 address allocation. While the Internet Service Providers have the highest number of allocations at 49.62%. the Telecommunication operators have 48.31% of the Total IPv6 address allocation to date. The increasing penetration of 3G and 4G networks coupled with the pending migration to 5G will lead to an increase in the IPv6 allocations to the Telecommunications industry.

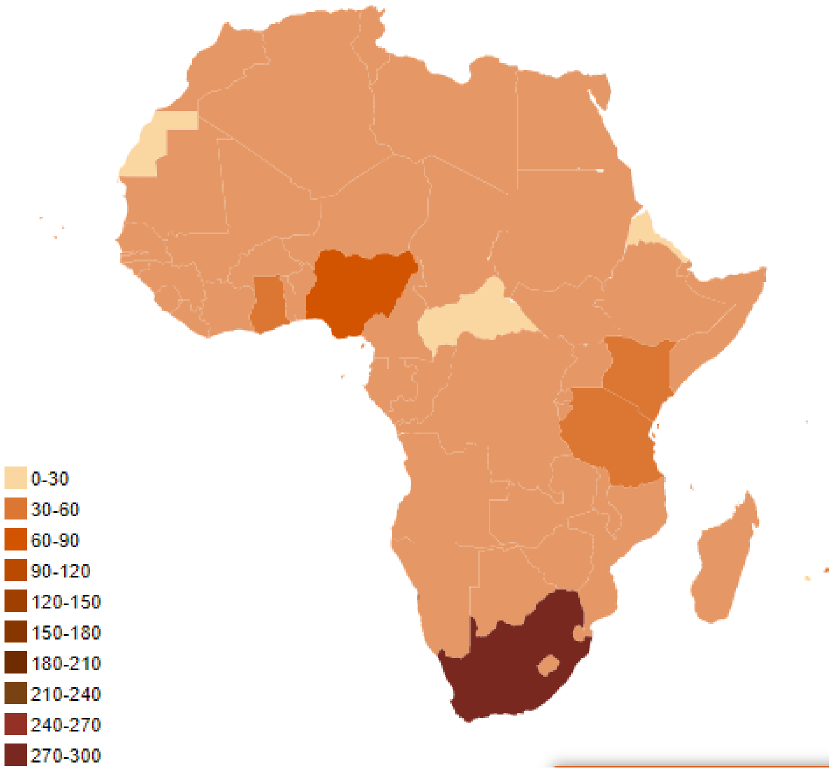


Figure 14. IPv6 addresses Issued by member countries in Africa[34]

[34] AFRINIC IPv6 statistics. https://stats.afrinic.net/ipv6

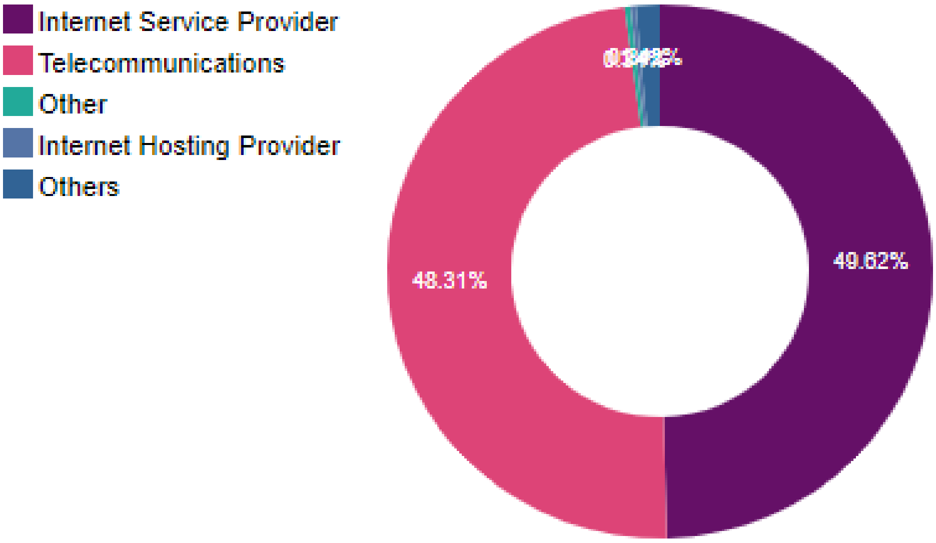


Figure 15. IPv6 addresses Issued to member industries[34]

5.2.4 IPv6 in Nigeria

There is a total of 81 IPv6 address allocations in Nigeria. The IP industry in Nigeria is predominantly sustained by the Carrier-grade NAT (CGN) routers. CGN also known as CGNAT is an approach to IPv4 network design where end sites are configured with private network addresses that are translated to public IPv4 addresses by middlebox network address translator devices embedded in the network operator's network. Limitations of the CGN include the lack of support for the end-to-end security principle as with all NAT systems, significant security, scalability, and reliability problems and it does not solve the IPv4 address exhaustion problem when a public IP address is needed, such as in web hosting. While the CGN provides some benefits with enabling the reuse of Private IPv4 addresses, its inherent challenges listed above makes it an unsustainable replacement for IPv6. Figure 16 shows the percentage of IPv6 users in Nigeria.

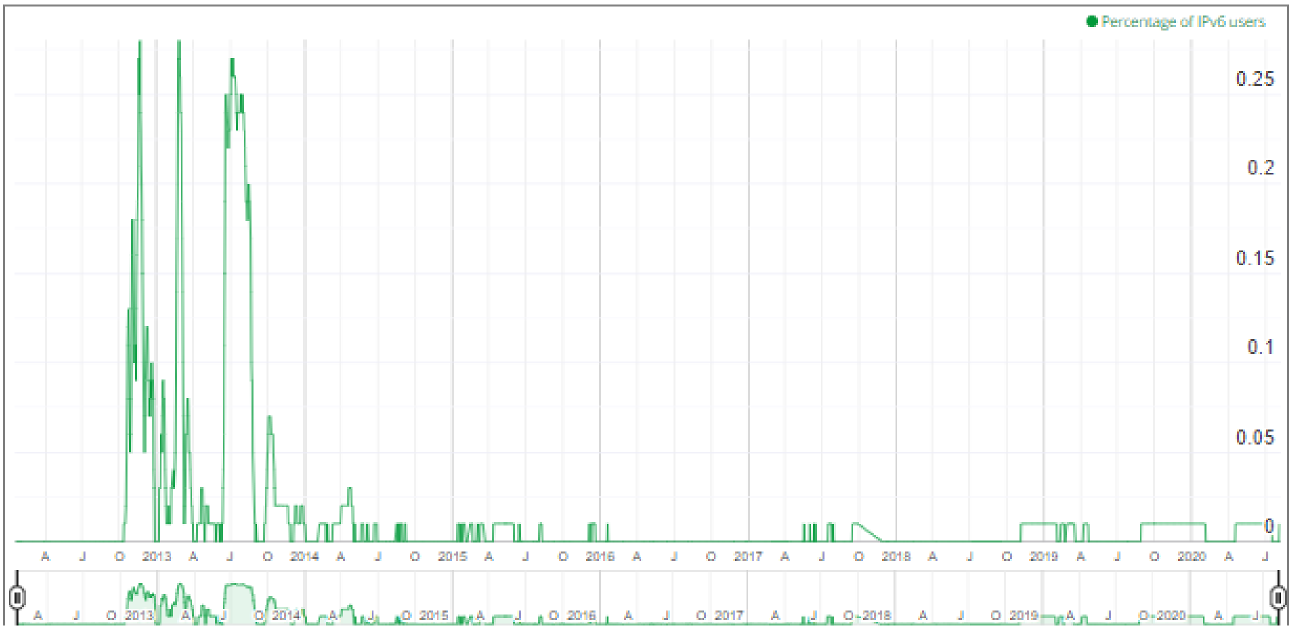


Figure 16. Percentage of IPv6 Users[35]

Figure 17 shows the trend of IPv6 enabled web servers in Nigeria. This projection shows an increase in the IPv6 deployment..

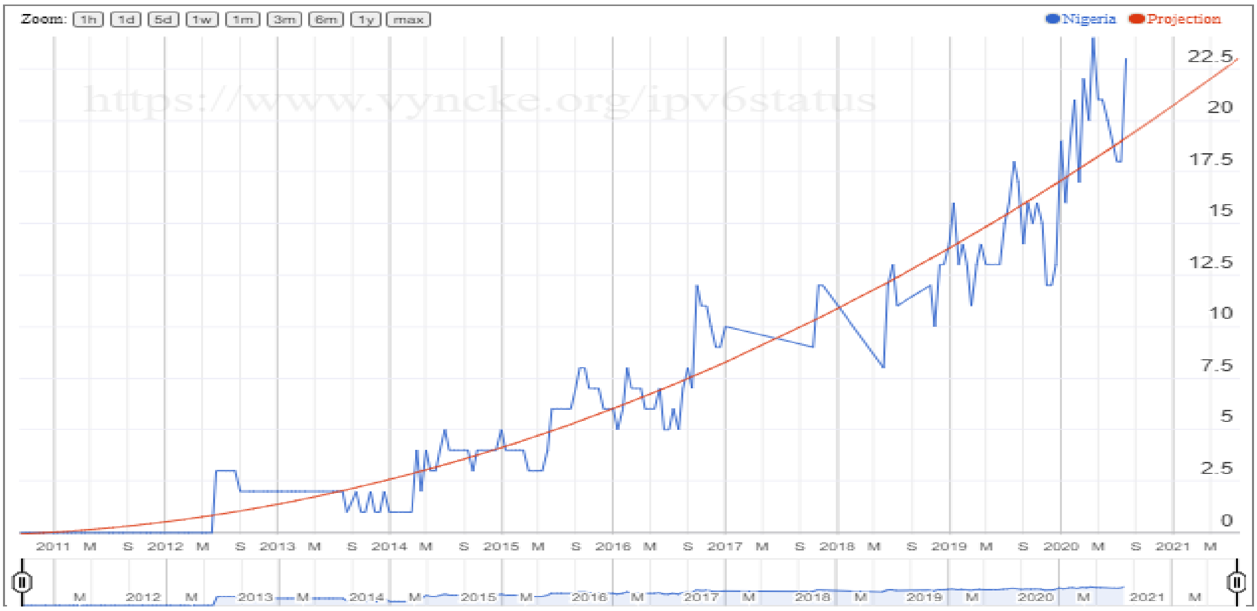


Figure 17. Projection of IPv6 IPv6-Enabled Web Servers in Nigeria Source [36]

Figure 18 shows the IPv6 allocations in Nigeria. ISPs have the greatest allocations with 77.78% while Education with 7.41% and Telecommunication with 5.56% are second and third respectively.

[35] IPv6 Deployment Aggregated Status. https://www.vyncke.org/ipv6status/
[36] IPv6 Deployment Aggregated Status. https://www.vyncke.org/ipv6status/

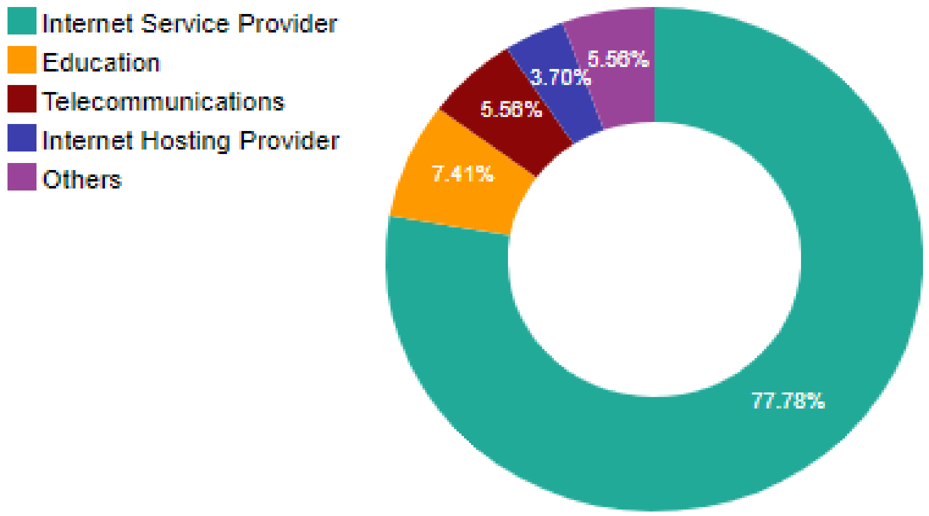


Figure 18. IPv6 addresses by Industries in Nigeria [37]

[37] AFRINIC IPv6 statistics. https://stats.afrinic.net/ipv6

CHAPTER SIX

ECONOMICS IMPLICATION OF IPV6 DEPLOYMENT IN NIGERIA

6.1 Introduction

Transitioning from IPv4 to IPv6 has a wide range of Economic Implications. These implications vary depending on the transition route adopted for the migration. These parameters impact on the deployment costs and adoption time as several factors have to be considered before these decisions will be taken. The following section discusses some of the economic parameters that will determine the transition choices.[38]

1. Compatibility options. There will be cases where some operators will either remain with the IPv4, others will deploy IPv6 networks and a third group will deploy any of the available IPv4 to IPv6 transition mechanisms. Operators must offer full compatibility with all other networks and as many endpoints and applications as possible. The options for these three basic network choices include

- Remain on IPv4 (do nothing)
- Run both IPv4 and IPv6 (implement dual stack and NAT)
- Run native IPv6 among compatible parts of their own network with some kind of NAT technology at the boundaries to make it compatible with IPv4

Amongst these viable alternatives, there is no difference in the network benefits obtained; all three approaches gain access to essentially the same "Internet" regardless of the transition approach.

2. Operators must also consider the costs of maintaining compatibility as these costs will be borne solely by the operators deploying IPv6.

3. Network growth is the critical driver of IPv6. The relative cost of network growth is the factor that most affects deployment decisions. This also means that the incentive to invest is determined by the potential for growth hence networks that have no need to grow have no incentive whatsoever to deploy IPv6, and can be expected to lag until the end game.

[38] The Hidden Standards War: Economic Factors Affecting IPv6 Deployment Brenden Kuerbis and Milton Mueller, Internet Governance Project, Georgia Institute of Technology, School of Public Policy. Research Project # 138078Project sponsor: Internet Corporation for Assigned Names and Numbers Final draft (February 2019)

4.Decisions for IPv6 are made independently at the AS level based on each AS's distinctive assessment and configuration. It is not a coordination game, not until the very end (an end that may never be reached).

5.Networks that deploy IPv6, will realize efficiency benefits when a greater portion of their Internet traffic can be diverted to an IPv6-only network. In this limited respect, the IPv6 deployment decisions of different network operators have some influence on each other. But one network operator's migration to IPv6 creates no variation in demand-side economies of scope, and no discernable difference in the Internet service offered.

6.As the IPv4 Internet continues to grow, and IPv4 brokerages and exchanges make unused or underutilized number blocks available, the slack in the IPv4 number space will be progressively eliminated. The resulting supply constraints on IPv4 numbers will lead to higher prices for IPv4resources, which can narrow the cost penalty for IPv6 deployment.

6.2 IPv4 Prices and Resource Transfers

The supply of IPv4 numbers plays an important role in the IPv4 - IPv6 competition. From an economic point of view, however, resources never just "run out;" instead, as their supply diminishes, they become increasingly expensive, and consumption patterns adapt to scarcity with greater conservation and new forms of substitution.

Network operators have adapted to the tighter supply of IPv4 addresses in two ways.

1. One is by using NAT, a conservation technique that uses a private (non-globally routable) IPv4 address space to connect local hosts, and passes traffic to the Internet by translating the many private addresses into a smaller number of globally routable IPv4 addresses. NATs are the reason why 20 billion connected devices on the modern Internet can be served by about 2 billion active IPv4 addresses.

2. The other adaptation is a secondary market for IPv4 number blocks, which allows networks that need more IPv4numbers to buy them from networks with an excess supply. This is made possible in part by the structure of the IPv4 address classes where a company acquires a Class A or B addresses with up to 16 Million network capacity (Class A) and doesn't utilize all the network address capacity. The incentives provided by the secondary market have led to the identification of millions of unused or underutilized IPv4 numbers by brokers such as IPv4 Market Group and exchanges such

as Addrex and HilcoStreambank. Hilco provides an online auction platform for the sale of IPv4 address blocks, including blocks registered in ARIN, RIPE, and APNIC, and ranging in size from /24 to /17.[39]

This transfer and sale of IPv4 addresses has led to the doubling of the median price per address over the last four years, from around $8.00in 2014 to $17.00 in 2018.

6.3 Deployment Incentives for Network Operators

Deployment decisions for network operators are discrete and independent. IPv6 deployment patterns, therefore, are best tracked at the AS level. The data show that there are a few markets where one or two major AS's have converted as much as 90% of their network to IPv6 while other major AS's in the same market have no discernable deployment at all. Data also shows that IPv6 deployers enjoy no competitive advantage when that happens, although there do seem to be cost efficiencies for large operators in expanding their network via IPv6.

While the aggregate trend for IPv6 over the past 7 years is upwards, the deployment trajectory is best understood as an accumulation of discrete decisions by individual network operators to convert all or part of their networks. Consequently, it is not unusual to see plateaus in deployment, at the country level and the AS level.

Plateaus occur when network operators complete a commitment to deploy IPv6 in part of their network and remain at that level. Further expansion requires another investment decision. There is no clear evidence indicating thatIPv6 deployment creates a major competitive advantage, so the negative correlation between market concentration and IPv6 deployment probably exists for two reasons:

1) the presence of more players in a market increases the likelihood that one of them will make an arbitrary deployment decision;

2) a more open market permits the entry of new firms (such as India's Reliance Jio) with newer infrastructures, which have a more favorable cost structure for IPv6.

For network operators that need to grow, such as mobile networks where the software and hardware ecosystem is mostly converted, IPv6 deployment can make economic sense. It

[39] KACZMAREK Hugo. Internet IPv6 Adoption: Methodology, Measurement and Tools
ECOLE POLYTECHNIQUE PROMOTION 2009 Research Internship Report

mitigates a major constraint on growth and can provide a path out of the operational complexities and costs of large-scale NAT.

The rising price of IPv4 numbers provides an additional stimulus to deploy IPv6. However, the need for deployers to maintain backwards compatibility with non-deployers eliminates many network effects that would create pressure to convert to IPv6. Enterprise networks don't need to grow much and/or may still be lodged in a slower-moving software and hardware ecosystem tied to IPv4.

When the IPv6 -only traffic ratio among IPv6 deployers reaches a given threshold, the IPv4 address requirements of those companies begin to decline. These operators can therefore release their IPv4 address resources into the market that would alleviate shortages and facilitate continued low levels of growth for legacy IPv4 networks.

The rising price of IPv4 numbers and the operational costs of NAT do in fact stimulate IPv6 deployment. But for static networks that already hold the IPv4 number resources they need, that is not a problem.

While the challenges with the NAT and the rising prices of IPv4 stimulates IPv6 deployments among fast growing networks, their IPv4 requirements will reduce thus leading to the availability of more IPv4 addresses for networks not ready to migrate to IPv6.

Given the vast number of countries with no discernable IPv6 deployment, their concentration in developing countries, and the presence of many enterprise networks that do not need to grow, it is difficult to envision a clean convergence on IPv6 any time in the near future. The wisest course of action for the global Internet technical community is to look forward to a mixed IPv4-IPv6 world for so many years to come and plan accordingly.

6.4 Impact Of IP-Based Technology On Electronic Marketing And Distribution Channels

Distribution channels are avenues utilized by companies to sell their products and services to their customer base. These channels are either direct, meaning that the customers are able to interact with their customers directly or indirect, meaning intermediaries perform activities on behalf of the company to reach customers. In the marketing strategy development phase, Companies must specify the channels it would use. Companies can choose to use either a single channel or multiple channel strategy.

The composition of a typical marketing channel includes the manufacturer, wholesaler, retailer and the consumer. Depending on the scale and nature of the business, the manufacturer may bypass the intermediate institutions to reach the consumer directly as shown in Figure 33.

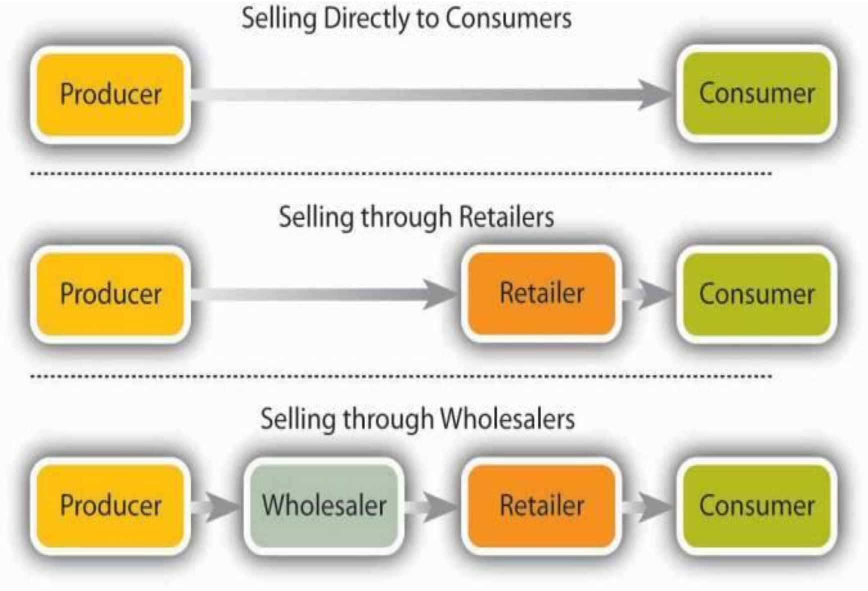

Selling Directly to Consumers
Producer
Consumer
Selling through Retailers
Producer
Retailer
Consumer
Selling through Wholesalers
Producer
Wholesaler
Retailer
Consumer

Figure 19. Typical Marketing Channels[40]

The information revolution has greatly impacted and changed the way business is done. The internet and online purchasing are the greatest change that has affected the structure of these marketing channels. This has led to the development of the Electronic Marketing Channels

6.4.1 Electronic Marketing channels

This can be defined as the use of the Internet to make products and services available so that the target market with access to computers or other enabling technologies can shop and complete the transaction for purchase via interactive electronic means. Some of these examples include the E-Commerce sites such as Amazon, eBay, Konga, Jumia etc. Other platforms being currently used include the social medial platforms such as YouTube, Twitter, Facebook etc. Sellers are able to advertise products to all their followers or connections and also utilize the pay on delivery approach to complete such transactions. This has led to a new industry of YouTube content developers who develop content and post of their channels on these

[40] Effect of Technology on Marketing Channel Design. T1 2016 MPK732 MARKETING MANAGEMENT (CLUSTER A). Deakin Business School

platforms. They earn income by having paid adverts inserted on their videos. Their income and revenues are determined by the number of persons that watch the videos or follow their channels.

Advantages of Electronic Marketing Channels

1. Global Scope and Reach.

2. Convenience/rapid transaction processing

3. Information processing efficiency and flexibility

4. Data-based management and relationship capabilities

5. Lower sales and distribution costs

Disadvantages of Electronic Marketing Channels

1. Lack of contact with actual products and delayed possession

2. Fulfillment logistics not at internet speed or efficiency

3. Clutter, confusion and cumbersomeness of the internet

4. Non-purchase motives for shopping not addressed

5. Security concerns of customers. Examples of this include buying products from unknown firms that exist only in cyberspace, and discomfort with sending credit card numbers over the Internet.

6.4.2 Impact of IP-Based Technology on Electronic Marketing and the Marketing mix

The fundamental paradigm of modern marketing management defines a marketing mix which comprise of product, price, promotion, place (distribution). This mix is still applicable with or without the internet. Electronic marketing channels however have come to change the blend of the marketing mix by enabling the Place (distribution) to assume a larger role relative to the other three variables for more and more firms. The Internet has the capacity to reduce potency of the first 3 Ps. This is done in the following manner:

Product – Due to the high volume of information flow capacity of the Internet, product differentiation can be negated. Users can identify alternatives very quickly thus reducing the dominance of some popular products.

Price – Internet allows mass price comparison, potentially eliminating price advantages of manufacturers. There are several platforms on the internet that aggregates similar products and enable the buyers compare prices of the different products together and make choices based on the price

Promotion – The company size becomes insignificant as users have access to several other similar products as such it will level the playing field so large firms will not have a significant promotional advantage.

Place (distribution) – The integration of a robust distribution platform by ecommerce firms increase their customer reach and helps to build relationships with customers via superior electronic marketing channels. This may provide a competitive advantage to those ecommerce platforms. Amazon has been able to integrate a robust distribution system its marketing platform thus creating a high level of trust with the customers.

CHAPTER SEVEN

RESULTS AND FINDINGS

7.1 Results and Key Findings

Objective One

To identify how IP Architecture structure (IPv4 & IPv6) is implemented and its vulnerabilities.

Key Findings

1. *The need for more IP addresses and the exhaustion of the IPv4 address space led to the development of the IPv6 address scheme. However, incompatibility of the IPv6 with the IPv4 has slowed down the adoption of the IPv6. While the adoption is inevitable, there are several pathways being adopted to make this migration possible. IPv6 is not foreseen to supplant IPv4 instantaneously so both protocols will continue to operate simultaneously for some time. IPv6 transition mechanisms are needed to enable IPv6 hosts to reach IPv4 services and to allow isolated IPv6 hosts and networks to reach each other over IPv4 infrastructure.*

2. *Shortage of IPv4 address will make it difficult for Internet Service Providers (ISPs) to connect new customers to the Internet. The delays with the migration to IPv6 has resulted in the ISP's developing a number of creative approaches to conserve IPv4 addresses and operate their IPv4-only networks for many years to come. Some of the transitions will cause all residential Internet traffic to be backhauled through a regional device which will add latency to Internet connections and result in performance degradation as all the individual subscribers will struggle for connections through the regional devices with millions of other subscribers.*

Key IPv6 Transition Mechanism[41]

1. Dual-stack IP implementation

Dual-stack IP implementations is one of the most robust IPv6 migration paths. It provides complete IPv4 and IPv6 protocol stacks in the operating system of a computer or the network device. These stacks run on the common physical layer such as the Ethernet. The

[41]Transition Mechanisms. https://www.ripe.net/publications/ipv6-info-centre/deployment-planning/transition-mechanisms

implementation of the Dual stack allows the simultaneous operation of IPv4 and IPv6 networks. A device with dual-stack implementation in the operating system has an IPv4 and IPv6 address, and can communicate with other nodes in the LAN or the Internet using either IPv4 or IPv6.Dual stack would also be required to be implemented on all routers between the host and the service for which the DNS server has returned an IPv6 address. Dual-stack clients should only be configured to prefer IPv6 if the network is able to forward IPv6 packets using the IPv6 versions of routing protocols. When dual stack networks protocols are in place the application layer can be migrated to IPv6.While dual-stack is supported by major operating systems and network device vendors, legacy networking hardware and servers don't support IPv6.

2. ISP customers with public-facing IPv6

Internet Service Providers (ISPs) are increasingly providing their business and private customers with public-facing IPv6 global unicast addresses. However, if in the local area network (LAN) IPv4 is still used, and the ISP can only provide a public facing IPv6, the IPv4 LAN addresses are translated into the public facing IPv6 address using NAT64, a network address translation (NAT) mechanism. A significant percentage of ISPs in all regional Internet registry (RIR) zones have obtained IPv6 address space. While some ISPs still allocate customers only IPv4 addresses, many ISPs allocate their customers only an IPv6 or dual stack IPv4 and IPv6.

ISPs report the share of IPv6 traffic from customers over their network to be anything between 20% and 40%, but by mid-2017 IPv6 traffic still only accounted for a fraction of total traffic at several large Internet exchange points (IXPs). AMS-IX reported it to be 2% and SeattleIX reported 7%.

A 2017 survey found that many DSL customers that were served by a dual stack ISP did not request DNS servers to resolve fully qualified domain names into IPv6 addresses. The survey also found that the majority of traffic from IPv6-ready webserver resources were still requested and served over IPv4, mostly due to ISP customers that did not use the dual stack facility provided by their ISP and to a lesser extent due to customers of IPv4-only ISPs.

3. Tunneling

Tunneling is a process of encapsulating IPv6 packets in IPv4 packets. It is designed to enable IPv6 packets to be transmitted using IPv4 network backbone.

One of the frequently used tunneling protocols is the 6to4. Teredo tunneling was also frequently used for integrating IPv6 LANs with the IPv4 Internet backbone. Teredo tunneling allows IPv6 local area networks to tunnel over IPv4 networks, by encapsulating IPv6 packets within UDP. The Teredo relay is an IPv6 router that mediates between a Teredo server and the native IPv6 network. It was expected that 6to4 and Teredo would be widely deployed until ISP networks would switch to native IPv6, but by 2014 Google Statistics showed that the use of both mechanisms had dropped to almost 0.

4. IPv4-mapped IPv6 addresses

Hybrid dual-stack IPv6/IPv4 implementations recognize a special class of addresses, the IPv4-mapped IPv6 addresses. These addresses are typically written with a 96-bit prefix in the standard IPv6 format, and the remaining 32 bits written in the customary dot-decimal notation of IPv4.

Addresses in this group consist of an 80-bit prefix of zeros, the next 16 bits are ones, and the remaining, least-significant 32 bits contain the IPv4 address. Because of the significant internal differences between IPv4 and IPv6 protocol stacks, some of the lower-level functionality available to programmers in the IPv6 stack does not work the same when used with IPv4-mapped addresses. Some common IPv6 stacks do not implement the IPv4-mapped address feature, either because the IPv6 and IPv4 stacks are separate implementations

Objective Two

To analyze how IP-based Technology help in the prevention of cyber-attacks by means of protecting service providers and end users (cyber security).

Key Findings

A number of security implications may arise from the use of IPv6. Some of them may be related with the IPv6 protocols themselves, while others may be related with implementations flaws. Some of the security flaws for IPv6 implementation include: [42]

[42] Guidelines for the Secure Deployment of IPv6. Recommendations of the National Institute of Standards and Technology. Sheila Frankel Richard Graveman John Pearce Mark Rooks. National Institute of Standards and Technology NIST. Special Publication 800-119. Dec 2010

1. Shadow networks

Device manufacturers and operating system developers have already begun to implement IPv6 in their devices and nodes as a default. This is capable of inadvertently creating shadow networks which will enable IPv6 traffic to flow into networks that has only IPv4 security management principles in place.

These shadow networks can also be launched during system upgrades when the newer upgrades enable IPv6 by default while the older ones didn't. Failing to update the security infrastructure to accommodate IPv6 can lead to IPv6 traffic bypassing it. These Shadow networks have occurred on business networks in which organizations replaced Windows XP systems without default IPv6 stack with Windows 7 systems which had the IPv6 stack enabled by default. Some IPv6 stack implementors have therefore recommended disabling IPv4 mapped addresses and instead using a dual-stack network where supporting both IPv4 and IPv6 is necessary.

2. IPv6 packet fragmentation

The use of packet fragmentation has been found to create an opportunity for hackers to evade network security controls. To counter this loop hole, the first fragment of an IPv6 packet must contain the entire IPv6 header chain. Additionally, the use of fragmentation of packets have been depreciated in Neighbor Discovery and discouraged for use in the Secure Neighbor Discovery (SEND).

The IPv6 transmission mechanisms which are meant to provide temporary pathways for the co-existence of both IPv4 and IPv6 also has its security vulnerabilities. The IPv6 packets have to be able to coexist with the IPv4 traffic on the IPv4 network resulting in a number of security implications for these networks.

3. IPsec

Internet Protocol Security is a suite of protocols and a framework of open standards developed by the Internet Engineering Task Force (IETF) and provides cryptographically-based security to network traffic. It ensures integrity, confidentiality and authentication of data *communications over IP networks. The flexibility of the IPsec which is one of its unique selling features has also resulted in several problems. One of these problems is the fact that it is not mandatory for network operators to implement IPv6 on their networks. This has the potential of creating networks without the required protection for IPv6 packets.. Poor maintenance which is a bane of security network also affects IPsec and can easily lead to a critical system failure.*

IPsec may be used in three different security domains:

1. *virtual private networks,*

2. *application-level security and*

3. *routing security.*

The most predominant application of IPsec at this time is in VPNs. IPsec must be combined with other security measures to be effective for deployment in application-level security or routing security domains. This requirement has limited the deployment of IPsec in these two domains.

The mechanisms employed by the IPsec for imposing security on IP Packets are

1. *Encapsulating Security Payload (ESP) protocol, which defined a method for encrypting data in IP packets. The ESP header provides encryption, data encapsulation and data confidentiality. This can also be defined as a security protocol for encrypting the entire IP packet (and authenticating its content). Data confidentiality is made available through symmetric key.*

2. *Authentication Header (AH) protocol, is a method for digitally signing IP packets. The AH provides authenticity and integrity for the packet. The authentication is provided through the use of keyed hash functions, also known as MACs (message authentication codes). The AH protocol also prohibits illegal modification and has the option of providing antireplay security.*

The AH can establish security between multiple hosts, multiple gateways, or multiple hosts and gateways, all implementing AH.

This can be defined as a security protocol for authenticating the source of an IP packet and verifying the integrity of its content

3. The Internet Key Exchange (IKE) protocol is used to manage the cryptographic keys used by hosts for IPsec.

4. IPsec operation

IPsec has two modes of operation and they are, the transport mode and the tunnel mode.

In the ***Transport mode****, all cryptographic operations must be performed directly by the source and destination hosts. Encrypted data is sent through a single tunnel that is created with L2TP (Layer 2 Tunneling Protocol). Data (ciphertext) is created by the source host and retrieved by the destination host. This mode of operation establishes end-to-end security.*

In the ***Tunnel mode****, which is usually used for communication between secured network gateways, IPsec tunnel mode enables hosts behind one of the gateways to communicate securely with hosts behind the other gateway. All the cryptographic processing is done by special gateways and both the source and destination hosts. In this mode, tunnels are created in series between the different gateways thus enabling the establishment of a gateway-to-gateway security. A typical example is a case where system users in the branch office can securely connect with any system in the main office if both the branch office and main office have secure gateways to act as IPsec proxies for hosts within the respective offices. The IPsec tunnel is established between the two gateway hosts, but the tunnel itself can carry traffic from any host inside the protected networks. Tunnel mode is useful for setting up a mechanism for protecting all traffic between two networks, from disparate hosts on either end.*

Regardless of the model of operation of the IPsec, there is a need to provide all the gateways with the ability to verify and authenticate the packet at both ends and all invalid packets must be dropped.[43]

5. Implementing IPsec

The support for IPsec has been included in most mainstream operating systems available from the late 1990s. These include desktop and server operating systems, as well as router and other network security appliances. While these older systems are designed with support for some version of IPsec, enterprises should deploy IPsec using operating systems that are current and

[43] D.Shalini Punithavathani and K.Sankaranarayanan. IPv4/IPv6 Transition Mechanisms European Journal of Scientific Research. ISSN 1450-216X Vol.34 No.1 (2009),

up to date on security patches. It is worthy to note that while older systems that support older versions of IPsec appear to enable secure IPsec circuits, they may not in fact be keeping data secure and be exposing the networks to security risks.

6. Security Implications of IPv6 on IPv4 Networks

Most popular Operating systems implement some form of IPv6 support. While some organizations have commenced the rollout of IPv6, other have opted to delay the rollout of the IPv6. This has resulted in the coexistence of both the IPv4 and the IPv6 traffic across the internet. In a bid to be able to accommodate these two protocols, several migration options are currently being implemented and these implementations has the potential of introducing security breaches on legacy IPv4 networks. This following operational practices can help to prevent security exposure in enterprise networks resulting from unplanned use of IPv6 on such networks.

These practices are only suitable for enterprise networks which are business specific in nature and not for general purpose internet access.

A typical security risk occurs when IPv6 enabled devices are deployed on enterprise networks intended to be IPv4-only, the existing IPv6 transition/coexistence technologies could be leveraged by local or remote attackers for a number of (illegitimate) purposes. Examples of this include

1. *A Network Intrusion Detection System (NIDS) might be set up to detect attack patterns for IPv4 traffic, but might be unable to detect the same attack patterns when a transition/coexistence technology is leveraged for that purpose.*
2. *An IPv4 firewall might enforce a specific security policy in IPv4, but might be unable to enforce the same policy in IPv6.*
3. *A NIDS or firewall might support both IPv4 and IPv6, but might not be configured to enforce on IPv6 traffic the same controls/ policies it enforces on IPv4 traffic.*
4. *Some transition/coexistence mechanisms could cause an internal host with otherwise limited IPv4 connectivity to become globally reachable over IPv6, therefore resulting in increased (and possibly unexpected) host exposure.*

Some transition/coexistence mechanisms (notably Teredo) are designed to traverse Network Address Port Translation (NAPT) devices, allowing incoming IPv6 connections from the Internet to hosts behind the organizational firewall or NAPT (which in many deployments provides a minimum level of protection by only allowing those instances of communication that have been initiated from the internal network).

5. *IPv6 support could, either inadvertently or as a result of a deliberate attack, result in Virtual Private Network (VPN) traffic leaks if IPv6-unaware VPN software is employed by dual-stacked hosts.*

In general, most of the aforementioned security implications can be mitigated by enforcing security controls on native IPv6 traffic and on IPv4-tunneled IPv6 traffic. Among such controls, is the enforcement of filtering policies to block undesirable traffic.

While IPv6 widespread/global IPv6 deployment has been slower than expected, it is nevertheless happening; and thus, filtering IPv6 traffic (whether native or transition/coexistence) to mitigate IPv6 security implications on IPv4 networks should (generally) only be considered as a temporary measure until IPv6 is deployed.

7. Security Implications of Native IPv6 Support[44]

Most popular operating systems include IPv6 support that is enabled by default. With this, even if a network is expected to be IPv4-only, much of its infrastructure is likely to be IPv6-enabled. Hosts are likely to have at least link- local IPv6 connectivity, which might be exploited by attackers with access to the local network. Additionally, unless appropriate measures are taken, an attacker with access to an "IPv4-only" local network could impersonate a local router and cause local hosts to enable their 'non-link-local' IPv6 connectivity (e.g., by sending Router Advertisement messages), possibly circumventing security controls that were enforced only on IPv4 communications.

Native IPv6 support could also possibly lead to VPN-traffic leakages when hosts employ VPN software that, not only does not support IPv6, but does nothing about IPv6 traffic.

[44] Guidelines for the Secure Deployment of IPv6. Recommendations of the National Institute of Standards and Technology. Sheila Frankel Richard Graveman John Pearce Mark Rooks. National Institute of Standards and Technology NIST. Special Publication 800-119. Dec 2010

To prevent these breaches, networks should enforce, the same security policies currently enforced on IPv4 traffic also on native IPv6 traffic. However, in those networks in which IPv6 has not yet been deployed and where enforcing the aforementioned policies is deemed as infeasible, a network administrator might mitigate IPv6-based attack vectors by means of appropriate packet filtering.

8. Filtering Native IPv6 Traffic

Some layer-2 devices might have the ability to selectively filter packets based on the type of layer-2 payload. When such functionality is available, IPv6 traffic could be blocked at those layer-2 devices by blocking, for example, Ethernet frames with the Protocol Type field set to 0x86dd. However, blocking IPv6 at layer-2 might create problems that are difficult to diagnose, inclusive of intentional or incidental use of link-local addressing (as in Multicast DNS/DNS-based Service Discovery) sites that enforce such a filtering policy should keep that possibility in mind when debugging the network. Attacks based on Stateless Address Autoconfiguration (SLAAC) can be mitigated with technologies such as Router Advertisement Guard (RA-Guard). In a similar way, DHCPv6-based attacks can be mitigated with technologies such as DHCPv6-Shield However, both RA-Guard and DHCPv6-Shield are incapable of mitigating attack vectors that employ IPv6 link-local addresses, since configuration of such addresses does not rely on Router Advertisement messages or DHCPv6-server messages. Administrators considering the filtering of native IPv6 traffic at layer-3 devices are urged to pay attention to the general considerations for IPv6 traffic filtering

9. Security Implications of Tunneling Mechanisms.

Tunneling mechanisms if not properly managed can lead to serious security lapses in the networks. These lapses range from increased host exposure, evasion of security controls, protocol-based vulnerabilities, and/or the corresponding code might contain bugs with security implications.

Of all the available tunneling mechanisms, the so- called "automatic tunneling" mechanisms (such as Teredo, Intra- Site Automatic Tunnel Addressing Protocol (ISATAP), and 6to4) are of particular interest from a security standpoint, since they might be employed without prior *consent or action of the user or network administrator. Tunneling mechanisms should be a concern not only to network administrators that have consciously deployed them, but also to those who have not deployed them, as these mechanisms might be leveraged to bypass their security policies.*

Some mitigation strategies include applying the common security practice of only allowing traffic deemed as "necessary" (i.e., the so-called "default deny" policy). Thus, when such policy is enforced, IPv6 transition/coexistence traffic would be blocked by default and would only be allowed as a result of an explicit decision.

It is recommended that, in addition to the enforcement of filtering policies at the organizational perimeter, the corresponding transition/coexistence mechanisms be disabled on each node connected to the organizational network when the transition mechanism is not in use. This would not only prevent security breaches resulting from accidental use of these mechanisms, but would also disable this functionality altogether, possibly mitigating vulnerabilities that might be present in the host implementation of these transition/coexistence mechanisms.

IPv6-in-IPv4 tunneling mechanisms (such as 6to4 or configured tunnels) can generally be blocked by dropping IPv4 packets that contain a Protocol field set to 41. Security devices such as NIDS might also include signatures that detect such transition/coexistence traffic.

(a)Filtering 6in4

This is probably the most basic type of tunnel employed for connecting IPv6 "islands". It is also called "6in4", in which IPv6 packets are encapsulated within IPv4 packets. These tunnels typically result from manual configuration at the two tunnel endpoints. 6in4 tunnels can be blocked by blocking IPv4 packets with a Protocol field of 41.

(b) Filtering 6over4

This specifies a mechanism known as 6over4 or 'IPv6 over IPv4' which comprises a set of mechanisms and policies to allow isolated IPv6 hosts located on physical links with no directly connected IPv6 router to become fully functional IPv6 hosts by using an IPv4 domain that supports IPv4 multicast as their virtual local link. This low-level deployment of multicast deployment in most networks is the reason for the low uptake of this transition technology. 6over4 encapsulates IPv6 packets in IPv4 packets with their Protocol field set to 41. As a result, simply filtering all IPv4 packets that have a Protocol field equal to 41 will filter 6over4. A more *selective filtering which blocks 6over4 Neighbor Discovery traffic directed to multicast addresses can be implemented. This will prevent SLAAC, address resolution, etc.*

(c) Filtering 6rd

6rd builds upon the mechanisms of 6to4 to enable the rapid deployment of IPv6 on IPv4 infrastructures, while avoiding some downsides of 6to4. 6rd can be blocked by blocking IPv4 packets with the Protocol field set to 41.

(d) Filtering 6to4

6to4 is an address assignment and router-to-router, host- to-router, and router-to-host automatic tunneling mechanism that is meant to provide IPv6 connectivity between IPv6 sites and hosts across the IPv4 Internet. All IPv6-in-IPv4 traffic, including 6to4, could be easily blocked by filtering IPv4 packets that contain their Protocol field set to 41. This is the most effective way of filtering such traffic. If 6to4 traffic is meant to be filtered while other IPv6-in-IPv4 traffic is allowed, then more fine-grained filtering rules could be applied.

(e) Filtering ISATAP

ISATAP is an Intra-site tunneling protocol, and thus it is generally expected that such traffic will not traverse the organizational firewall of an IPv4-only network. Nevertheless, ISATAP can be easily blocked by blocking IPv4 packets with a Protocol field of 41.

(f) Filtering Teredo

Teredo is an address assignment and automatic tunneling technology that provides IPv6 connectivity to dual-stack nodes that are behind one or more Network Address Port Translation (NAPT) devices, by encapsulating IPv6 packets in IPv4-based UDP datagrams. Teredo is meant to be a 'last-resort' IPv6 connectivity technology, to be used only when other technologies such as 6to4 cannot be deployed (e.g., because the edge device has not been assigned a public IPv4 address). To prevent the Teredo initialization process from succeeding, and hence prevent the use of Teredo, an organizational firewall could filter outgoing UDP packets with a Destination Port of 3544.

The most popular operating system that includes an implementation of Teredo in the default installation is Microsoft Windows. Microsoft Windows obtains the Teredo server addresses (primary and secondary) by resolving the domain name teredo.ipv6.microsoft.com into DNS A *records. A network administrator might want to prevent Microsoft Windows hosts from obtaining Teredo service by filtering, at the organizational firewall, outgoing UDP datagrams (i.e., IPv4 packets with the Protocol field set to 17) that contain in the IPv4 Destination Address any of the IPv4 addresses that the domain name teredo.ipv6.microsoft.com maps to (or the IPv4 address of any well- known Teredo server).*

Additionally, the firewall would filter incoming UDP datagrams from any of the IPv4 addresses to which the domain names of well-known Teredo servers (such as teredo.ipv6.microsoft.com) resolve.

(g) Filtering Tunnel Broker with Tunnel Setup Protocol (TSP)

The tunnel broker model enables dynamic configuration of tunnels between a tunnel client and a tunnel server. The tunnel broker provides a control channel for creating, deleting, or updating a tunnel between the tunnel client and the tunnel server. Additionally, the tunnel broker may register the user's IPv6 address and name in the DNS. Once the tunnel is configured, data can flow between the tunnel client and the tunnel server.

TSP can use either TCP or UDP as the transport protocol. In both cases, TSP uses port number 3653, which has been assigned by the IANA for this purpose. As a result, TSP (the Tunnel Broker control channel) can be blocked by blocking TCP and UDP packets originating from the local network and destined to UDP port 3653 or TCP port 3653.

(h) Filtering AYIYA

AYIYA ("Anything In Anything") allows the tunneling of packets across Network Address Port Translation (NAPT) devices. While the specification of this tunneling mechanism was never published as an RFC, it is nevertheless widely deployed. AYIYA can be blocked by blocking TCP and UDP packets originating from the local network and destined to UDP port 5072 or TCP port 5072.

From the finding of this study, there is a continuous increase in the IPv6 deployments with a number of hosts preferring IPv6 connectivity whenever it is available. This is likely to cause IPv6-capable hosts to attempt to reach the ever-increasing number of popular destinations via IPv6, even if this IPv6 connectivity relies on an "IPv4-only" network. Additionally, it should be noted that when filtering IPv6 traffic, it is good practice to notify the source of the packet when that packet is dropped.

This is to enable the source to take the timely required action in response to the dropped packet. For example, a firewall could signal the packet drop by means of an ICMPv6 error message (or TCP RST segment if appropriate), such that the source node can react as appropriate either to resend the message of notify the administrator of the loss of that packet.

Objective Three

To determine how IP-based Technology enforces permissible-use policies to prevent unauthorized network use and to achieve policy implication.

Key Findings

Permissible-Use Policies For Network Protection

Permissible use policies are policies set up by the administer which defines what a system (Client or Server) is permitted to do on the network.[45] *These policies help to improve network configuration and control and ultimately improve network operations. The policies lead to the development of a Policy driven network in which most of the router settings are fully automated. It also provides enforceable authorization policies for servers by preventing non approved applications from accessing the network while at the same time providing a real time monitoring of policy violations.*

Some of these policies include

1. *Restriction to the functions of a Web server. These restrictions range from the type of file transfer the server is authorized to make to the network the servers are not permitted to access*

2 *The Websites client applications are allowed to access when they are connected to the official company servers.*

These policies will be determined by the individual companies however, one key requirement is that when any user attempts to breach any of the policies by running the restricted

[45] Nakamoto. G, Durst. R, Growney C, Andresen. J, Ma. J, Trivedi. N, Quang. R and Pisano D. Identity-Based Internet Protocol Network. MITRE Corporation 2012

applications, such applications will be automatically blocked without the requirement human intervention or the need for a system reconfiguration.

Objective Four

To determine how the economics and financial structure of IP-based technologies contribute to the rapid acceptance of the technology.

Key Findings

1. Economic Implications of Transitioning from IPv4 to IPv6

Transitioning from IPv4 to IPv6 has a wide range of Economic Implications. These implications vary depending on the transition route adopted for the migration. The transition route impacts on the deployment costs and adoption time as several factors have to be considered before these decisions can be taken. The following section discusses some of findings on the economic parameters that will determine the transition choices.[46]

1. *Compatibility options. There will be cases where some operators will remain with the IPv4, others will deploy IPv6 networks and a third group will deploy any of the available IPv4 to IPv6 transition mechanisms. Operators must offer full compatibility with all other networks and as many endpoints and applications as possible. The options for these three basic network choices include*

    - *Remain on IPv4 (do nothing)*
    - *Run both IPv4 and IPv6 (implement dual stack and NAT)*
    - *Run native IPv6 among compatible parts of their own network with some kind of NAT technology at the boundaries to make it compatible with IPv4*

[46] The Hidden Standards War: Economic Factors Affecting IPv6 Deployment Brenden Kuerbis and Milton Mueller, Internet Governance Project, Georgia Institute of Technology, School of Public Policy. Research Project # 138078Project sponsor: Internet Corporation for Assigned Names and Numbers Final draft (February 2019)

Amongst these viable alternatives, there is no difference in the network benefits obtained; all three approaches gain access to essentially the same "Internet" regardless of the transition approach.

2. *Operators must also consider the costs of maintaining compatibility as these costs will be borne solely by the operators deploying IPv6.*

3. *Network growth is the critical driver of IPv6. The relative cost of network growth is the most significant factor that affects deployment decisions. This also means that the incentive to invest is determined by the potential for growth hence networks that have no need to grow have no incentive whatsoever to rush to deploy IPv6.*

4. *Decisions for IPv6 are made independently at the AS level based on each AS's distinctive assessment and configuration. It is not a coordination game, not until the very end (an end that may never be reached).*

5. *Networks that deploy IPv6, will realize efficiency benefits when a greater portion of their Internet traffic can be diverted to an IPv6-only network. In this limited respect, the IPv6 deployment decisions of different network operators have some influence on each other. But one network operator's migration to IPv6 creates no variation in demand-side economies of scope, and no discernable difference in the Internet service offered.*

6. *As the IPv4 Internet continues to grow, and IPv4 brokerages and exchanges make unused or underutilized number blocks available, the slack in the IPv4 number space will be progressively eliminated. The resulting supply constraints on IPv4 numbers will lead to higher prices for IPv4resources, which can narrow the cost penalty for IPv6 deployment.*

2. *IPv4 Prices and Resource Transfers*

The supply of IPv4 numbers plays an important role in the IPv4 - IPv6 competition. From an economic point of view, however, resources never just "run out;" instead, as their supply diminishes, they become increasingly expensive, and consumption patterns adapt to scarcity with greater conservation and new forms of substitution.

Network operators have adapted to the tighter supply of IPv4 addresses in two ways.

1. *One is by using NAT, a conservation technique that uses a private (non-globally routable) IPv4 address space to connect local hosts, and passes traffic to the Internet*

by translating the many private addresses into a smaller number of globally routable IPv4 addresses. NATs are the reason why 20 billion connected devices on the modern Internet can be served by about 2 billion active IPv4 addresses.

2. *The other adaptation is a secondary market for IPv4 number blocks, which allows networks that need more IPv4numbers to buy them from networks with an excess supply. This is made possible in part by the structure of the IPv4 address classes where a company acquires a Class A or B addresses with up to 16 Million network capacity (Class A) and doesn't utilize all the network address capacity. The incentives provided by the secondary market have led to the identification of millions of unused or underutilized IPv4 numbers by brokers such as IPv4 Market Group and exchanges such as Addrex and HilcoStreambank.*

This transfer and sale of IPv4 addresses has led to the doubling of the median price per address over the last four years, from around $8.00in 2014 to $17.00 in 2018. These prices crossed $20 in 2019 and as at 2020, some address blocks have been reported to sell at $30 for the /23 address

3. *Deployment Incentives for Network Operators*

1. *Deployment decisions for network operators are discrete and independent. IPv6 deployment patterns, therefore, are best tracked at the AS level. The data shows that there are a few markets where one or two major AS's have converted as much as 90% of their network to IPv6 while other major AS's in the same market have no discernable deployment at all. Data also shows that IPv6 deployers enjoy no competitive advantage when that happens, although there do seem to be cost efficiencies for large operators in expanding their network via IPv6.*

2. *While the aggregate trend for IPv6 over the past 7 years is upwards, the deployment trajectory is best understood as an accumulation of discrete decisions by individual network operators to convert all or part of their networks. Consequently, it is not unusual to see plateaus in deployment, at the country level and the AS level.*

3. *Plateaus occur when network operators complete a commitment to deploy IPv6 in part of their network and remain at that level. Further expansion requires another investment decision. There is no clear evidence indicating that IPv6 deployment creates a major competitive advantage, so the negative*

correlation between market concentration and IPv6 deployment probably exists for two reasons:

a) the presence of more players in a market increases the likelihood that one of them will make an arbitrary deployment decision;

b) a more open market permits the entry of new firms (such as India's Reliance Jio) with newer infrastructures, which have a more favorable cost structure for IPv6.

4. *For network operators that need to grow, such as mobile networks where the software and hardware ecosystem is mostly converted, IPv6 deployment can make economic sense. It mitigates a major constraint on growth and can provide a path out of the operational complexities and costs of large-scale NAT.*

5. *The rising price of IPv4 numbers provides an additional stimulus to deploy IPv6. However, the need for deployers to maintain backwards compatibility with non-deployers eliminates many network effects that would create pressure to convert to IPv6. Enterprise networks don't need to grow much and/or may still be lodged in a slower-moving software and hardware ecosystem tied to IPv4.*

6. *When the IPv6 -only traffic ratio among IPv6 deployers reaches a given threshold, the IPv4 address requirements of those companies begin to decline. These operators can therefore release their IPv4 address resources into the market that would alleviate shortages and facilitate continued low levels of growth for legacy IPv4 networks.*

7. *The rising price of IPv4 numbers and the operational costs of NAT do in fact stimulate IPv6 deployment. But for static networks that already hold the IPv4 number resources they need, that is not a problem.*

8. *While the challenges with the NAT and the rising prices of IPv4 stimulates IPv6 deployments among fast growing networks, their IPv4 requirements will reduce thus leading to the availability of more IPv4 addresses for networks not ready to migrate to IPv6.*

9. *Given the vast number of countries with no discernable IPv6 deployment, their concentration in developing countries, and the presence of many enterprise networks that do not need to grow, it is difficult to envision a clean convergence on IPv6 any time in the near future. The wisest course of action for the*

global Internet technical community is to look forward to a mixed IPv4-IPv6 world for so many years to come and plan accordingly

Objective Five

To determine how IP-based Technology aids electronic marketing and distribution channels.

Key Findings

The information revolution has greatly impacted and changed the way business is done. The internet and online purchasing are the greatest change that has affected the structure of these marketing channels. This has led to the development of the Electronic Marketing Channels.

1. Electronic Marketing channels

1. This can be defined as the use of the Internet to make products and services available so that the target market with access to computers or other enabling technologies can shop and complete the transaction for purchase via interactive electronic means. Some of these examples include the E-Commerce sites such as Amazon, eBay, Konga, Jumia etc. Other platforms being currently used include the social media platforms such as YouTube, Twitter, Facebook etc. Sellers are able to advertise products to all their followers or connections and also utilize the pay-on-delivery approach to complete such transactions. This has led to a new industry of YouTube content developers who develop content and post these contents on their channels on these platforms. They earn income by having paid adverts inserted on their videos. Their income and revenues are determined by the number of content views or followers of their channels.

CHAPTER EIGHT

CONCLUSION AND RECOMMENDATIONS

8.1 Conclusion

This study has been able to review the role of IPv6 as a wining Technology for Communications Technology Deployment. It provided a background of the state of global IP addressing management and the hierarchy of IP address administration. The report also presented a comparative analysis of the IPv4 and the IPv6 highlighting the key advantages of the IPv6. It further discussed the key security features and the transitions mechanisms for a smooth migration to the IPv6 protocol. The economic implications of the IPv6 transition was also covered in the study. The study concludes with a recommendation for the smooth transmission to IPv6, the security strategies for a safe IPv6 deployment and operation and the use of Access Control lists to manage the cyber security risks associated with IPV6 deployment.

8.2 Recommendations

The recommendations from this study are organized under key IPv6 deployment issues

IPv6 Cyber security Vulnerabilities[47]

IPsec is considered an integral part of IPv6. This creates an assurance of security however, there are two conditions which can weaken the security ratings of IPv6.Although the IETF mandates that all IPv6 nodes have IPsec available, the actual use of IPsec is optional. If all communications between two IPv6 nodes are encrypted then the network (which is usually trusted because it is centrally managed) becomes blind and cannot inspect the traffic or enforce a security policy.

Recommendation 1

IPsec on IPv6 should be reserved for the same cases as in IPv4: remote access virtual private networks (VPNs) or site-to-site VPNs.

[47] Guidelines for the Secure Deployment of IPv6. Recommendations of the National Institute of Standards and Technology. Sheila Frankel Richard Graveman John Pearce Mark Rooks. National Institute of Standards and Technology NIST. Special Publication 800-119. Dec 2010

Network Security Vulnerabilities for IPv6 Transition Mechanisms

1. Dual Stack

A dual-stack network is as secure as its weakest protocol family. This is called fate-sharing; for example, if the IPv6 access is not protected while the IPv4 is controlled, then the malicious user will use IPv6 for the attacks.

Recommendation 2

It is really important to have congruent security policies for IPv4 and IPv6.

2. Tunnels

Tunnels can be convenient to transport IPv6 over an IPv4-only network. They can also be misused by the attacker to inject or to sniff IPv6 packets, to gain unauthorized access to an IPv6 network, and even to launch an amplification attack by looping between two tunnels.

Recommendation 3

When tunnels are used to send sensitive traffic over a public network, they should be secured by adding IPsec authentication and confidentiality that can prevent both the injection/sniffing attacks and unauthorized access. This is a specific case where IPsec is useful.

3. Latent Threat

The fact that modern hosts can be attacked over IPv6 even when connected to an IPv4-only network is called the IPv6 latent threat. Most recent host OSs have IPv6 enabled by default and some of them even try very hard to establish tunnels when there is no native IPv6 connectivity. If the host has not secured its IPv6 access (for example it has only an IPv4 firewall configured), then a link-local attacker can launch an attack on this host by sending a Router Advertisement [RA] message to trigger IPv6 stateless auto-configuration on the target, or an offline attacker can attack its victim over an automatic tunnel.

Recommendation 4

Robust training on the security implementations for IPv6 networks and traffic

IPv6 Deployment in Nigeria

The basic assumption is that, for the foreseeable future, organizations will either operate dual stack networks or accommodate both IPv4 and IPv6 networking through other means.

However, the eventual goal is to transition to an IPv6 only network, or at least an IPv6-centric one.

Recommendation 5

The IPv6 deployment should follow the NIST guidelines for a secure information system life cycle and should include the following stages[48]

- Initiation Phase
- Acquisition/Development Phase
- Implementation Phase
- Operations/Maintenance Phase
- Disposition Phase.

The framework calls for a phased approach or a gradual transition from IPv4 to IPv6. The use of a phased implementation will enable an organization to implement IPv6 with as little disruption to the current environment as possible.

Recommendation 6

Existing users should be unaware of the new protocol until they require its use. The phased approach will minimize the effect on day-to-day operations.

There are two main approaches to transition deployment:

- Pervasive IPv6 deployment
- Sparse IPv6 deployment.

In a **pervasive deployment**, the organization enables dual (IPv4/IPv6) stack equipment rapidly throughout the entire enterprise. This scenario is appropriate when an organization has mostly new equipment that supports both IPv4 and IPv6. After the organization validates core services and translation mechanisms are functioning properly, IPv4 is disabled on all equipment, leaving an IPv6 dominant network.

In a **sparse IPv6 deployment**, organizations enable groups or islands of IPv6 equipment in an IPv4 dominant network. After most of the edge devices transition to IPv6, the network core transitions to either dual stack or IPv6 only. A sparse IPv6 deployment requires supporting both IPv4 and IPv6 traffic throughout the duration of the deployment life cycle. This approach

[48] KACZMAREK Hugo. Internet IPv6 Adoption: Methodology, Measurement and Tools
ECOLE POLYTECHNIQUE PROMOTION 2009 Research Internship Report

makes extensive use of IPv4/IPv6 and IPv6/IPv4 tunneling. This scenario is appropriate when an organization has a large installed base of older equipment or services that cannot transition to IPv6.

Software and Hardware Upgrades

Software or applications may be more important than equipment when selecting a transition approach. Upgrades for hardware and embedded operating systems can be quicker than custom or off the shelf applications. Many vendors may not be able or willing to upgrade software to support IPv6 and many organizations do not have the expertise in house to upgrade the code base. The more legacy applications and custom code an organization supports (either developed in house or highly customized off the shelf software) the greater the risk that the software will not support IPv6.

Recommendation 7

Transition planners must address software related issues in the approach to IPv6 transition.

Organizations not yet ready for IPv6 Deployment

It has been established that the decision to migrate to IPv6 would be taken at individual company levels as such, organizations that are not yet deploying IPv6 globally should implement the following recommendations:

Recommendation 8

1. Block all IPv6 traffic, native and tunneled, at the organization's firewall. Both incoming and outgoing traffic should be blocked.
2. Disable all IPv6-compatible ports, protocols and services on all software and hardware.
3. Begin to acquire familiarity and expertise with IPv6, through laboratory experimentation and/or limited pilot deployments.
4. Make organization web servers, located outside of the organizational firewall, accessible via IPv6 connections. This will enable IPv6-only users to access the servers and aid the organization in acquiring familiarity with some aspects of IPv6 deployment.

Key Recommendations for the Phases for IPv6 Migration

It has been recommended that the migration to IPv6 follows the NIST standard. There are however a number of recommendations that should be followed in the implementation of the different phases of the IPv6 migration.

Recommendation 9

1. Initiation Phase

The initiation phase is concerned with requirements gathering. It is important for an organization to understand its current environment before deploying IPv6. By understanding the current environment, the correct transition approach can be selected, and an organization can ensure that it maintains security parity between its IPv4 and IPv6 environment.

2. Acquisition / Development Phase

The acquisition and development phases are concerned with taking the requirements gathered during the initiation phase and developing the IPv6 enterprise architecture. When developing the IPv6 environment, the current enterprise architecture should be considered. The acquisition/development phase will work with three different architectures:

- the ―as is (IPv4 based enterprise architecture),
- the ―to be (IPv6), and
- the transitional architecture that bridges the IPv4 and the IPv6 architectures.

During the development phase, an organization should plan for an IPv6 evaluation pilot. The goals of an IPv6 pilot are to test IPv6 configuration and design assumptions against existing equipment, test and evaluate new IPv6 equipment and begin training staff.

3. Implementation Phase

The implementation phase involves the secure installation and configuration of IPv6 equipment, tunnels, and translation mechanisms. The deployment stage differs depending on which deployment scenario is used (IPv6 pervasive deployment or IPv6 sparse deployment). In both scenarios, the actual IPv6 roll out should follow a phased deployment.

4. Operations / Maintenance Phase

The operations phase often begins concurrently with the implementation phase. During operations, the focus should be on the secure operation of a dual stack or mixed IPv6/IPv4 environment. One of the most difficult challenges facing the operations staff in a mixed IPv6/IPv4 environment is keeping the two environments synchronized.

5. Disposition Phase

A migration from IPv4 to IPv6 results in displacement or retirement of equipment. Equipment that do not IPv6 are retired, while other equipment is transferred to IPv4 islands or to other organizations. Organizations must plan for the secure disposition of this obsolete equipment, ensuring that no confidential data is released. Organizations place themselves at great risk for exposing confidential information when disposing of obsolete equipment. Organizations should adopt a proactive approach to media sanitation.

a). Equipment removed from the network should be sanitized before the replacement equipment is installed. This reduces the window of vulnerability and greatly decreases the risk of information disclosure. Installers should provide proof of sanitation, including a certificate of destruction with serial numbers and asset tags.

b) Security risks are inherent during the initial deployment of a new protocol such as IPv6, but mitigation strategies exist and many of the residual risks are no different from those that challenge existing IPv4 networks. The mitigation strategies should be followed.

c) IPsec is a major component of IPv6 security and should be deployed, wherever possible, to secure IPv6 networks. Transition mechanisms allow existing IPv4 networks to coexist and interoperate with IPv6 networks, systems, and services. These transition mechanisms cover a wide range of technologies and transition scenarios. Organizations should plan their deployment and account for the full lifecycle of equipment from inception to disposal.

Bibliography

[1] IANA. https://www.iana.org/

[2] IANA https://www.ripe.net/participate/internet-governance/internet-technical-community/iana

[3] ICANN-ASO. https://aso.icann.org/about/

[4] Address Supporting Organization (ASO) Review. https://www.icann.org/resources/reviews/org/aso

[5] NRO. https://www.nro.net/

[6] Number Resource Organization. https://www.internetsociety.org/resources/deploy360/2012/number-resource-organization/

[7] Regional Internet Registries. https://www.nro.net/about/rirs/

[8] The Internet Registry System. https://www.ripe.net/participate/internet-governance/internet-technical-community/the-rir-system

[9] History of the Regional Internet Registries.https://www.apnic.net/about-apnic/organization/history-of-apnic/history-of-the-regional-internet-registries/.

[10] Regional Internet Registry. https://www.ripe.net/about-us/what-we-do/regional-internet-registry

[11] AFRINIC IPv4 Exhaustion. https://www.afrinic.net/exhaustion

[12] Phases of IPv4 Exhaustion. https://www.lacnic.net/1039/2/lacnic/phases-of-ipv4-exhaustion

[13] Next Generation Internet: IPv4 Address Exhaustion, Mitigation Strategies and Implications for the U.S. An IEEE-USA White Paper 2009. https://ieeeusa.org/wp-content/uploads/2017/07/IEEEUSAWP-IPv62009.pdf

[14] BT begins trial of IPv6 as IPv4 address exhaustion looms. https://arstechnica.com/information-technology/2015/07/bt-begins-trial-of-ipv6-as-ipv4-address-exhaustion-looms/

[15] State of IPv6 Deployment 2018. Key points. Internet Society https://www.internetsociety.org/resources/2018/state-of-ipv6-deployment-2018/

[16] Stephen Ugwuanyi, Fouead Attaran, Syeed Hussaini, Ahmed Merehil. The State of IPv6 Deployment: A global Review. International Journal of Scientific & Engineering Research, Volume 8, Issue 4, April-2017

[17] IPv6 @Virginia Tech. Virginia Tech University. http://ipv6.cns.vt.edu/

[18] Global IPv6 Adoption. https://www.google.com/intl/en/ipv6/statistics.html#tab=ipv6-adoption.

[19] IPv6 Deployment Aggregated Status. https://www.vyncke.org/ipv6status/

[20] CISCO. 6lab - The place to monitor IPv6 adoption. https://6lab.cisco.com/stats/cible.php?country=world&option=prefixes

[21] AFRINIC IPv4 statistics. https://stats.afrinic.net/ipv4/

[22] AFRINIC IPv4 Exhaustion statistics. https://stats.afrinic.net/ipv4/exhaustion

[23] AFRINIC IPv6 statistics. https://stats.afrinic.net/ipv6

[24] INTERNET PROTOCOL. DARPA INTERNET PROGRAM. PROTOCOL SPECIFICATION. Sept 1981

[25] F.Gont Request for Comments: 6274 Security Assessment of the Internet Protocol Version 4. Internet Engineering Task Force (IETF) June 2011

[26] Aluko T.S, Olusanya O.J, Oloyede O.E , Ebisin A.F. Comparative Analysis between Internet Protocol Version 4 & 6 (IPv4 and IPv6) International Journal of Scientific & Engineering Research, Volume 5, Issue 8,August-2014

[27] Internet Protocol Version 4 (IPv4) https://www.ibm.com/support/knowledgecenter/SSLTBW_2.1.0/com.ibm.zos.v2r1.hald001/ipversion4.htm

[28] Firdous Ahmad Khan, Falak Reyaz Wani, Mohammad Ahsan Chishti Performance Analysis of Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) over MPLS. International Journal of Computing and Network Technology @ 2014: Scientific Publishing Center, University of Bahrain. Int. J. Com. Net. Teach. 2, No. 3 (Sep. 2014)

[29] Microsoft pays Nortel $7.5 million for IPv4 addresses. https://www.networkworld.com/article/2228854/microsoft-pays-nortel--7-5-million-for-ipv4-addresses.html

[30] IPv4 addresses could soon be valued at $200 apiece. https://www.networkworld.com/article/2228857/expert--ipv4-addresses-could-soon-be-valued-at--200-apiece.html

[31] IoT trends 2018 for businesses to watch. https://medium.com/@mobidev.biz/iot-trends-2017-2018-fda47490a3de

[32] Jim Mckeeth. The Internet of Things and You. A Developers Guide to IoT. https://www.slideshare.net/jimmckeeth/the-internet-of-things-and-you-a-developers-guide-to-io-t

[33] S. Deering ,R. Hinden Internet Protocol, Version 6 (IPv6) Specification Internet Engineering Task Force (IETF) July 2017

[34] IPv6 Security Brief. Cisco Whitepaper. https://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enterprise-ipv6-solution/white_paper_c11-678658.html

[35] IPv6 Transition Mechanisms. https://www.ripe.net/support/training/videos/ipv6/transition-mechanisms

[36] Transition Mechanisms. https://www.ripe.net/publications/ipv6-info-centre/deployment-planning/transition-mechanisms

[37] D.Shalini Punithavathani and K.Sankaranarayanan. IPv4/IPv6 Transition Mechanisms European Journal of Scientific Research. ISSN 1450-216X Vol.34 No.1 (2009),

[38] Chuck Sellers. IPv6 Transition Mechanisms and Strategies. https://www.rmv6tf.org/wp-content/uploads/2012/11/Chuck-Sellers-090421-IPv6-Transition-Mechanisms-Sellers1.pdf

[39] Guidelines for the Secure Deployment of IPv6. Recommendations of the National Institute of Standards and Technology. Sheila Frankel Richard Graveman John Pearce Mark Rooks. National Institute of Standards and Technology NIST. Special Publication 800-119. Dec 2010

[40] James Cox. Access Control List (ACL) – What are They and How to Configure Them! January 2020. https://www.ittsystems.com/access-control-list-acl/#:~:text=An%20Access%20Control%20Lists%20...%20There%20are%20four,protect%20a%20network%20using%20only%20the%20source%20address.

[41] The Hidden Standards War: Economic Factors Affecting IPv6 Deployment Brenden Kuerbis and Milton Mueller, Internet Governance Project, Georgia Institute of Technology, School of Public Policy. Research Project # 138078Project sponsor: Internet Corporation for Assigned Names and Numbers Final draft (February 2019)

[42] KACZMAREK Hugo. Internet IPv6 Adoption: Methodology, Measurement and Tools. ECOLE POLYTECHNIQUE PROMOTION 2009 Research Internship Report

APPENDIX

TERMS OF REFERENCE

PROPOSAL FOR A CONSULTANCY STUDY ON INTERNET PROTOCOL (IP); THE WINNING TECHNOLOGY IN CURRENT TELECOMMUNICATIONS WORLD

1.0 INTRODUCTION

The Internet requires Internet Protocol (IP) which is an assigned unique number identifying an address or location of an Internet connection via web server, Smartphone, mail server, or laptop etc. The unique number (IP) is assigned to every Internet enabled device to identify the device when connected to the Internet. There are two versions of IP that currently coexist in the global Internet: IP version 4 (IPv4) and IP version 6 (IPv6).

There are other alternatives to IP that are being used to interconnect networks. These include but are not restricted to the following:

1. AppleTalk
2. Connectionless-mode Network Protocol (CLNP)
3. Internetwork Packet Exchange/ Sequence Packet Exchange (IPX/SPX)
4. Chaosnet
5. Digital Equipment Corporation Network (DECnet)

The telecom industry has undergone drastic changes over the last few decades, from a service only able to deliver voice capabilities, to a service where voice is one of a large number of features delivered across a network. These changes have accumulated to the point where another major change is imminent, a change to an all- IP infrastructure. One of the benefits of IP is easy access. Since IP is travelling in data packets over the internet, your phone will work no matter where you plug it on the Local Area Network (LAN), where TDM and other alternatives can only be used when a specific cable is present. Under TDM, the major offers from telecom providers had to do with voice, for example, three way calling and call waiting, but switching to IP could add value added services such as instant messaging, video calling between sites and dialing from a website. According to researchers, once large carriers realize the potential to make “new money” by converting to IP the transition will begin to increase.

The intended research focuses on benefits of adoption of IP-based Telecommunications / ICT infrastructure and how telecommunication and Information Technology has evolved as the global standard in 21st century which is inevitably unignorably.

An IP-based ICT infrastructure offers market flexibility, optimal control and significant savings by accessing increased bandwidth without incurring huge costs. The IP-based applications have become of crucial importance to the political, economic, social and technological development of any country, particularly developing countries, as communities globally seeks maximize the use of Internet and other ICT Infrastructure to provide global coverage of telecommunications in developing countries.

Internet protocols are at the heart of Internet's accomplishment of its aim and purpose. The importance of Internet facilitation and accessibility is the set of Internet Protocol's availability to communities globally to grant access to wide variety of hosts (Internet enabled Devices) in a complex and fully distributed fashion. IP focuses on data transfer and transaction, with innovation that allows images and limited multimedia (voice and video). The challenge in the future might be that the new innovation of Internet Protocols (IP) may not grant low end users' access to develop, but it will continuously facilitate the enriching of information transferred.

This research project will provide

1. An overview analysis of why IP as the wining technology in telecommunications and ICT world.
2. How Telecommunication and Information Technology has evolved till date becoming a state-of-art technology.
3. It will discuss its challenges and
4. Propose a conceptual framework of how IP will continue to vigorously thrive as a cutting-edge technology in the midst of cyber warfare (Cyber Security).

2.0 OBJECTIVES

6. To identify how IP Architecture structure (IPv4 & IPv6) is implemented and its vulnerabilities.
7. To analyze how IP-based Technology help in the prevention of cyber-attacks by means of protecting service providers and end users (cyber security).
8. To determine how IP-based Technology enforces permissible-use policies to prevent unauthorized network use and to achieve policy implication.
9. To determine how IP-based Technology economics and its financial structure the driving factor for its rapid acceptance.
10. To determine how IP-based Technology aids electronic marketing and distribution channels.

3.0 SCOPE

3. To identify the chances of spoofing and denial of service (DOD) and other dynamic, temporary user access through a firewall.
4. Recommend regulation on the use of Access Control List (ACLs) that performs packets filtering to control the flow of packets through a network.

4.0 DELIVERABLES

The consultant will deliver the following documents in accordance with the agreed timelines as indicated in the work plan:

1. An Inception Report to be submitted within four weeks of acceptance of Letter of Award.

This Inception Report will detail

(i) the study approach/methodology and

(ii) work plans with timelines including review meetings, in-house or out of office trainings where necessary, presentation periods following the submission of draft interim/progress reports and draft final reports.

2. In the event that the Inception report is unacceptable, the Commission reserves the right to cancel the award.
3. Interim/Progress report before and after completion of field survey.
4. Draft final report.
5. Final report.
6. The Consultant shall submit five (5) copies of each of the approved final report and two electronic copies in Microsoft Office software format.
7. A publishable Executive summary of the Final Report.

5.0 TIME FRAME

The study shall be executed within twenty weeks (20) effective from the date of award. An Inception Report must be submitted within four weeks of acceptance of Award.

6.0 PAYMENT

1. 15% payable on submission of Inception Report acceptable to the Commission and presentation of e-payment account details.
2. 25% payable on submission of Interim Report acceptable to the Commission.
3. 30% payable submission of Draft Report acceptable to the Commission.

4. 30% payable on submission and presentation of Final Report acceptable to the Commission.

7.0 ADMINISTRATIVE ARRANGEMENTS AND RESPONSIBILITIES

While this study is underway the Consultant shall;

Report directly to the Research and Development Department of the Commission and shall be responsible for alerting the Commission on all major issues pertinent to the successful execution and completion of the study.

The Consultant is expected to be available until the completion of the studies.

8.0 CONDUCT OF THE CONSULTANT

1. The Consultant shall be expected to carry out the assignment with the highest degree of professionalism and integrity.
2. The Consultant shall conduct their duties in an open and transparent manner and shall not hinder nor prevent the Commission from executing this or any other transaction included as part of industry development.
3. The Consultant will study all the guidelines and policies of the Commission with respect to the Industry development initiatives and will be expected to ensure that the transaction is concluded with very strict adherence to such policies and regulations.
4. The Consultant shall not take any material decision pertinent to this study without the express permission of the Commission.
5. The Consultant shall not discuss, publish, or reveal any information regarding the study without the Commission’s approval.