A Preview of IPv6 and the Challenges of its Adoption in Nigeria

Okereke George Emeka, Nwagwu Honour Chika, Abhadiomhen Stanley, Echezona Stephenson
Department of Computer Science
University of Nigeria
Nsukka, Nigeria
E-mail: honour.nwagwu@unn.edu.ng

ABSTRACT

There is need for the adoption of the Internet Protocol version 6 (IPv6). This is because of the near exhaustion of IPv4 addresses and other associated benefits. In this work, we explore the reasons for the introduction of IPv6 and we compare the two internet protocols notably the IPv4 and IPv6. We discuss the worrisome state of IPv6 adoption in Nigeria. An evaluation of peer reviewed journal and various online documented resources is the research methodology adopted in this work.

Keywords: IP, IPv4, IPv6, IPsec, Internet, Network, Addresses

1. INTRODUCTION

Each host on a network (such as the internet) identifies and communicates with another through the use of internet protocol (IP). The Internet Protocol was introduced to industries in 1981 [1]. Its function is moving datagrams through an interconnected set of networks. The IP versions in use are the Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) with later being a new and improved version of the former. The development of an improved IP version (the IPv6) was as a result of the near exhaustion of IPv4 addresses, which when projected into the future, cannot accommodate the increasing number of internet users.

Consequently, the Internet Engineering Task Force (IETF) initiated the design and development of IPv6 in 1994. The IPv6 is also known as IP Next Generation or IPng [2]. IPv6 uses a128-bit address size compared with the 32-bit system used in IPv4 and will allow for enough address spaces for the entire devices owned by different individuals on earth. Given that there are growing numbers of devices which are connected to the Internet in Nigeria and Africa at large, and with the pool of available IPv4 addresses which are quickly running out, there is need for African mobile communication companies, government institutions and other organisations to adopt the IPv6-128-bit system. Also, unlike in IPv4-based internet system, the IPv6-128-bit system provides for multiple levels of hierarchy and other added advantages.

Section 2.0 of this work provides a comparative analysis of IPv4 and IPv6 based systems. There are however, challenges limiting cooperate organisations from adopting IPv6 in Nigeria. These challenges include the overhead cost and inadequate incentives and directions from Nigerian government. These factors are discussed in section 3.0. Interestingly, the Nigerian government have impressively, initiated the IPv6 council to encourage the adoption of IPv6 but this measures is not so fruitful given that Nigeria ranks very low in GoogleIPv6 ranking. This work ascribes this failure to the lack of a roadmap by African countries on the move to IPv6 adoption. It provides some recommendations on the way forward. It also discusses the approaches to adopting IPv6 in section 3.0. Section 4.0 presents the conclusion of this work.

2. A COMPARATIVE ANALYSIS OF IPV4 AND IPV6 BASED SYSTEMS

Several works had been carried out on IPv4 and IPv6. They include [3,4,5,6,7,8] among others. We briefly review these works in this section and our comparative analysis will be based on these previous works and our own experience over the years. The IPv4 uses a 32-bit address system. This address system is capable of feeding 2^{32} (i.e. 4,294,967,296 or 4.3 billion) devices. This number is limited considering the vast number of mobile devices available on earth today. It results in easy depletion of these IPv4 addresses. The IPv6 was developed in 1999 to serve as the next IP. IPv6 has the following peculiar attributes as against IPv4:

Available address space: The number of mobile devices currently in the world is increasing daily. It is evaluated by GSMA intelligence [1] to be at about 7.22 billion at the time of this write-up. Unlike IPv4, IPv6 has 128-bit (16-byte) source and destination IP addresses. There are 2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456 (that is 340 undecillion) IPv6 available addresses for devices. The IPv6 can therefore provide enough IP addresses for all devices in the world, today and even beyond. The large address space of IPv6 has been designed to allow for multiple levels of sub-netting and address allocation from the Internet backbone to the individual subnets within an organization. The main limitation of IPv4 lies in the exhaustion of its available address spaces.

Format of the Header: [3] carried out a comparison between the headers of IPv4 and IPv6 in which the following observations were made: IPv6 header is much simpler when compared to IPv4 header, because the length of IPv6 header is fixed, it uses an extension header instead of the IPv4 fragmentation fields, IPv6 eliminates the checksum field available in IPv4, and it uses a smaller option field size than IPv4 header as observed by [4] Again IPv6 header size is128 bits while that of IPv4 is 32 bits, showing that IPv6 header size is very much bigger than that of IPv4 header size. Some fields like Internet Header Length (IHL) and identification flags which are available in the IPv4 header are absent in IPv6 header. IPv6 header uses a 4-bit Time-to-Live (TTL) field while IPv4 header uses 8-bit TTL field. The comparison showed that the fields version, source and destination addresses are present in both IPv4 and IPv6. The fields IHL, identification, flags, fragment offset, Header checksum, option and padding are all absent in IPv6. The following IPv4 field names and positions changed in IPv6. Type of service in IPv4 changed to Traffic class in IPv6; Total length in IPv4 changed to payload length in IPv6; Time to live in IPv4 changed to Hop limit in IPv6 while IPv4 protocol field changed to Next header field in IPv6. And finally Flow label is in new field in IPv6 and is completely absent in IPv4 systems.

Available Security: Security is one major improvement of the IPv6 over IPv4. As security is a serious consideration in IT world today, IPv6 has made some security improvement over the IPv4 which has very little security implementation in place. For example, [5] stated that the IPSec is implemented in IPv6 through the use of the Encapsulating Security Payload (ESP) extension header and the Authentication Header (AH). It has the ability to determine the origin of any attack as noted by [6]. IPsec as developed by the Internet Engineering Task Force (IETF) is a group of protocols which provide encryption and authentication at the network layer for IP networks. It offers authentication and/or encryption of traffic at the IP level. IPSec is optionally available for implementation with IPv4 but a basic requirement in IPv6 implementations. Despite the security enhancements in IPv6, there are still different types of attack which can potentially affect networks which have fully deployed IPv6. This means that some of the attacks prevalent in IPv4 networks can also be evident in IPv6 networks. The following are some of the examples of these common threats:

[1] https://www.gsmaintelligence.com/

The sniffing attacks
This is the process of getting the data transmitted over the network. This makes confidential data transmitted as plaintext over the network available for compromise by an attacker or intruder running sniffing attack. Proper implementation of IPSec architecture is one of the ways of circumventing sniffing attack [7,8].

Application layer attacks
[9] observed that attacks targeted at the application layer such as worms, buffer overflow, web application and viruses cannot be prevented even as we migrate from IPv4 to IPv6. IPv4 and IPv6 are both network layer based protocol whereas application layer attacks target the OSI model's application layer.

Flooding attacks
Brute force attack is one of the most common attacks present in the IPv4 networks. IPv6 is also vulnerable to this type of attack as identified [10]. It means flooding a network device such as a router or a host with enormous quantities of traffic thereby making the affected device unable to process the large network data and then becomes unreachable. If the targeted network device is being flooded by traffic emanating from various hosts at the same time this attack can be classified as a Distributed Denial of Service attack (DDoS).
Other forms of attacks common to both IPv4 and IPv6 include Man-in-the-middle attack, Rogue devices, and the Reconnaissance attacks.

Network Address Translation (NAT): Network Address Translation (NAT) is the process where a network device usually a firewall or router, assigns a public address to a computer (or group of computers) within a local network. The primary use of NAT is to restrain the number of public IP addresses an organization or company must use, for both economy and security sake [11]. The private addressing scheme works well for computers that only have to access resources inside the network, like workstations demanding access to file servers and printers. Routers inside the private network can route traffic between private addresses with no trouble. However, to access resources outside the network, using Internet as example, these computers will be given a public address in order for responses to their requests to return to them. Internet requests that demand Network Address Translation (NAT) are quite elusive but occur swiftly that the end user hardly detects what happened behind the scene. Unlike the IPv4, IPv6 has no need for NAT because the address space allocated for it is large enough.

Loopback Address Format: One of the noticeable differences that exist between IPv4 and IPv6 is the appearance of the IP addresses. IPv4 uses dotted decimal to separate four pairs of numbers e.g. "192.168.1.1" known as octet, while IPv6 uses hexadecimal numbers that are separated by colons e.g. "fe80::d4a8:6435:d2d8:d9f3b11". The loopback address (both in IPv4 and IPv6) is an address which represents the local address of a computer. The loopback addresses are vital to programmers for development and testing of network applications notwithstanding the absence of network configurations.
Loopback address IPv4: A complete network is reserved as loopback address in IPv4. Today most operating systems use local to represent IPv4 address loopback. IPv6 address lookback use 0000:0000:0000:0000:0000:0000:0000:0001/128 which is usually written as::1/128 in abridged form.

Configuration: In computing, IPconfig command (internet protocol configuration) in Microsoft Windows is a console program that displays all TCP/IP network configuration and their current values. This can also modify DHCP and DNS settings. The IPconfig command is often used in conjunction with the command line switch '/all' to produce a more detailed information about the network. This results in more detailed information than IPconfig alone.

In IPv4, the IPconfig command only supports manual configuration or Dynamic Host Configuration Protocol (DHCP) whereas IPv6 supports automatic configuration along with plug and play capability.

Mobile Support: Mobile IP (MIP) is an IETF standard communications protocol. This protocol was designed to enable mobile device users to move from a particular network to another with its IP address remaining permanent. The IETF RFC 5944 describes the mobile IP for IPv4 while IETF RFC 4721defines its extensions. IPv4 supports MIP that ranges from 1G to 3G phones while IPV6 supports MIP that ranges from 4G and above phones.

Transmission: TCP/IP is a combination of two different protocols; the Transmission Control Protocol (TCP) and the Internet Protocol (IP) with the former running on top of the later. The basic functions of the Internet Protocol IP in transmission include the provision of addressing, communication and routing. It also carries TCP data. Transmission Control Protocol (TCP) on the other hand offers the measure to guarantee a reliable transfer of computer data over a TCP/IP network. The Internet Protocol (IP) fragments data from program which is encapsulated inside the IP datagram and sent across a network. In other to transfer data reliably over the Internet, TCP/IP set of protocols is employed. There are broadcast addresses for all devices in IPv4 while the IPv6 only uses a multicast group.

Support: IPv4 makes use of 0.0.0.0 as unspecified address while IPv6 makes use of :: as unspecified address.
A comparative analysis of the IPv4 and IPv6 is presented in table 1. The table clearly shows the superiority of IPv6 over IPv4.

Table 1: A Comparative Analysis of IPv4 and IPv6

S/n	Attributes	IPv4	IPv6
1.	Available Address Space	Uses 32-bit address system capable of supporting 2^{32} or 4.3 billion devices.	Uses 128 address system capable of supporting 2^{128} or 340 undecillion devices.
2.	Size of Header Information	Uses header field length of 20-60 bytes along with other header options.	Uses header field length of 40 bytes. It has no other header options.
3.	Available Security	Poor security because IPSec is optional.	Better security because of built-in IPSec which is mandatory.
4.	Mobile Support	Supports mobile IP in the range of 1G to 3G devices.	Supports mobile IP devices above 4G.
5.	Transmission Capabilities	Broadcasts addresses for all devices.	Uses only a multicast group.
6.	Configuration	IPconfig command only supports manual configuration or Dynamic Host Configuration Protocol (DHCP).	Supports automatic configuration along with plug and play capability.
7.	Network Address Translation (NAT)	NAT is used to support address limitation as it is projected that IPv4 addresses might get exhausted in the future because of the increasing number of internet users.	Has no need for NAT because the address space allocated for IPv6 is large enough and can accommodate the increasing number of internet users.
8.	Loopback Address Format	Uses 127.0.0.0 as loopback IP address, i.e. dotted decimal called octet.	Uses ::1 as loopback IP address, i.e. hexadecimal numbers separated by colons.
9.	Support Capabilities	Uses 0.0.0.0 as unspecified address.	Uses :: as unspecified address.

3. CHALLENGES OF ADOPTING IPV6

There are challenges limiting cooperate organizations and government institutions from adopting IPv6 in Nigeria. These challenges include the overhead cost and inadequate incentives and directions, among others. These challenges are discussed herein as follows:

Overhead cost for IPv6

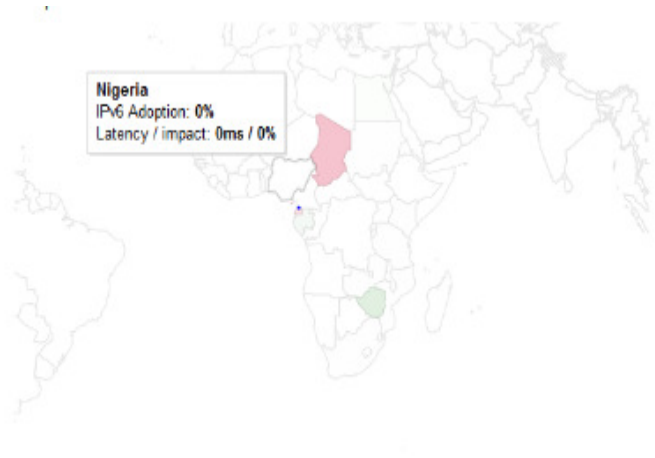
Older devices in a company may lack support for an IPv6 address and this could create network-communication issues when the company tries to change to IPv6 address protocol. As stated above, IPv4 supports MIP that ranges from 1G to 3G phones while IPV6 supports MIP that ranges from 4G and above phones. Also, unlike the IPv4, IPv6 has no need for NAT because the address space allocated for it is large enough. It is therefore essential to evaluate the available resources to check and address any compatibility issues if a new addressing protocol is to be adopted. Also, an organization which adopts an approach of running IPv6 along with IPv4 will need a dual-stack configuration to enable the usage of both the IPv4 address and the IPv6 address in the same network. These will involve additional trainings to staff. Consequently, there is an increase in costs of any organisation which adopts a new IP address system. A move from running operations with IPv4 to IPv6 necessitates the audit, review, reconfiguring and testing of the entire technology infrastructure of a company as explained in [2].

Inadequate incentives and directions from Nigerian government

The government of Nigerian initiated and inaugurated an IPv6 council[2]. This council is given the responsibility to promote the deployment and coordination of IPv6 uptake with support from industry, education, research communities and government agencies. Even so, Nigeria ranks very low on the ranking of countries that has adopted IPv6 in Africa and in the world at large. It has a 0% IPv6 adoption rating and a latency/impact scale of 0% according to Google rating as evident in the diagram in Figure 1. Google[3] ranks Nigeria at 215 out of 262 ranked countries in 2018. It is noted in [13] that organizations in developing countries are lagging behind in the migration from IPv4 to IPv6. Figure 1a explicitly shows the backwardness of African Countries notably Nigeria when compared to European Countries in Figure 1b.

[2] http://ipv6council.ng/

[3] https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption

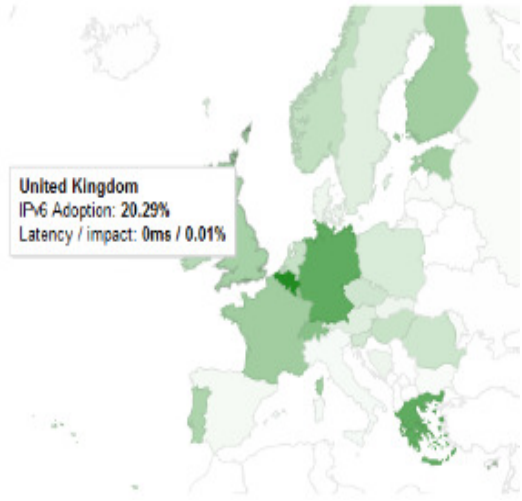


Regions where IPv6 is more widely deployed (the darker the green, the greater the deployment) and users experience infrequent issues connecting to IPv6-enabled websites.

Regions where IPv6 is not widely deployed and users experience significant reliability or latency issues connecting to IPv6-enabled websites

Regions where IPv6 is no deployed IPv6

Fig. 1a: Google statistics of Per-Country IPv6 adoption in Africa as adopted from GoogleIPv6



Regions where IPv6 is more widely deployed (the darker the green, the greater the deployment) and users experience infrequent issues connecting to IPv6-enabled websites.

Regions where IPv6 is no deployed IPv6

Fig 1b: Google statistics of Per-Country IPv6 adoption in Europe as adopted from GoogleIPv6

4. RECOMMENDATIONS AND CONCLUSION

The authors of this work are of the opinion that Nigerian government is not providing adequate incentives and directions on the adaptation of IPv6 to its government agencies and organisations. This is because there appears to be latent policies that do not spur Nigerian organizations to implement IPv6. In addition, there are indeed, no road maps to ensure that organizations in Nigerian adopt the new technology. Most developed countries adopted roadmaps towards the migration of IPv4 to IPv6 as evident in [14, 15]. Indeed, IPv6 has been adopted as an industry strategy backed by government policies in some of the developed countries, spurring focused research and development for IPv6 technology and applications as explained in [15]. Consequently, the authors of this work recommend that Nigerian government should mandate the IPv6 council to produce a white paper on a roadmap towards adopting IPv6. The roadmap should have deadlines for government agencies and parastatals to migrate to IPv6. The white paper should propose that Nigerian government runs web servers for public access to its own information and such web servers should adopt IPv6. It is also recommended that taxes on IPv6 associated devices should be removed to incite private organisations to migration to IPv6.

Conclusively, there is a serious need to allocate unique IP addresses to millions of mobile and computer users and this cannot be realized through the adoption of IPv4 in Nigerians. It is evident that the adoption of IPv6 is far from widespread in Africa, notably in Nigeria. This work has related the need for the adoption of IPv6 to the imminent exhaustion of the IPv4 addresses. Also, the adoption of IPv6 will enable the attainment of end-to-end IPsec based on IPv6 thereby allowing easy detection of cyberspace and other technology related crimes. The Nigerian people cannot afford to slow down business growth as a result of inability of IP providers to assigned IP address. A call is consequently made in this work to academic researchers and the media to create the publicity that will advert this imminent disaster.

REFERENCES

1. J. Postel. (1981). RFC791: Internet Protocol–DARPA internet program protocol specification. [Online], Available at https://tools.ietf.org/html/rfc791 [Last accessed on 12th April, 2018].
2. Deering, S. E. (1998). Internet protocol, version 6 (IPv6) specification. [Online], Available at https://tools.ietf.org/html/rfc2460 [Last accessed on 12th April, 2018]
3. IETF *"RFC4301: Security Architecture for the Internet Protocol".* Accessed January 20, 2018
4. J. Thomas. (2018). *Comparison between IPv4 Header and IPv6 Header*. http://www.omnisecu.com/tcpip/ipv6/comparison-between-ipv4-header-and-ipv6-header.php Accessed January 15, 2018.
5. R. Thayer, N. Doraswamy and R. Glenn. (2016). *IP Security Document Roadmap*. IETF. doi:10.17487/RFC2411. RFC 2411. Accessed January 21, 2018.
6. P. Hoffman (2015). *Cryptographic Suites for IPsec*. IETF. doi:10.17487/RFC4308. RFC 4308. Accessed January 21, 2018.
7. S. Kent. (2015). *IP Authentication Header*. IETF. doi:10.17487/RFC4302. RFC 4302. Accessed January 21, 2018.
8. S. Kent and R. Atkinson. (2015). *IP Authentication Header*. IETF. Doi:10.17487/RFC2402. RFC 2402. Accessed January 21, 2018.
9. *P. Willis (2015). Carrier-Scale IP Networks: Designing and Operating Internet Networks. IET. p. 267. ISBN 9780852969823.*
10. D. McDonald, B. Phan, and C. Metz. (2015). RFC 2367, *PF_KEYv2 Key Management API.* Accessed January 21, 2018.
11. *I. V. Beijnum (2014). "After staunch resistance, NAT may come to IPv6 after all". Ars Technica.* Accessed February 1, 2018.
12. Spindel M (2018). IPv6 Adoption: Challenges and Options [Online] Available at http://www.datacenterjournal.com/ipv6-adoption-challenges-options/ Last accessed on the 17th April, 2018.
13. Dawadi, B. R., Joshi, S. R., & Khanal, A. R. (2015). Service Provider IPv4 to IPv6 Network Migration Strategies. *Journal of Emerging Trends in Computing and Information Sciences*, *6*(10).
14. Department of Business Innovation and Skills (2010), IPv6 Rollout in the UK, A BIS departmental Report. [Online] Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/78236/10-1229-ipv6-rollout-in-the-uk.pdf Last accessed on 13th April, 2018.
15. Eslambolchi Hossein (2012) IPV6 MIGRATIION AND ITS CONTINGENCIES, COMPLEXITIES AND IMPLICATIONS. [Online] Available at http://2020vp.com/ipv6-migratiion-and-its-contingencies-complexities-and-implications/ Last accessed on 17th April, 2018.

WEB Links (Footnotes)

1. https://www.gsmaintelligence.com/
2. http://ipv6council.ng/
3. https://www.google.com/intl/en/ipv6/statistics.html#tab=per-country-ipv6-adoption&tab=per-country-ipv6-adoption