Assessment of the importance of Transiting from IPV4 to IPV6 in Nigeria

Ihekweaba Ogechi, Nweke Chisom B.

***Abstract*— Internet protocol is a set of technical rules that defines how computers communicate over a network. It is a network-layer protocol that contains addressing information and some control information to enable packet routing through a network. Transition from Internet Protocol Version Six (IPV4) to Internet Protocol Version Six (IPV6) has become unavoidable in the process of internet development because of many reasons. IPV6 is the next-generation internet protocol, intended as the follow-on to IPV4. It supports unlimited addresses, flexibility, robustness, enhanced security, better support for Quality of Service (QoS), higher performance, built-in multicasting, enhanced mobility etc. This paper assesses the importance of transiting from internet protocol version four (IPV4) to internet protocol version six (IPV6).**

***Index Terms*—IPV4, IPV6**

I. INTRODUCTION

Some years ago, the only kind of traffic that existed on the internet was that of emails or file transfers. In the early 1990s, it became evident that if the Internet will continue to grow at the rate it was growing, the IPv4 address space would be exhausted in few years time. Thus, work began on a new Internet Protocol, namely IPv6. To replace Internet Protocol Version Four (IPv4), a latest edition of the protocol is introduced and it is called Internet Protocol Version Six (IPV6)[1].

Presently IPv4 Internet is facing a sequence of tribulations including address exhaustion, routing scalability, broken end-to-end property etc. IANA (Internet Assigned Numbers Authority) had run out of global IPv4 address pool in Feb 2011, while simulations show that within 3 years all the RIRs (Regional Internet Registries) will drain their IPv4 address space [2]. Thus, the incessant demands for new IP address portion. IPv4 uses 32 binary bits to create a single unique address on the network. An IPv4 address is expressed by four numbers separated by dots. Each number is the decimal (base-10) representation for an eight-digit binary (base-2) number, also called an octet. IPv6 uses 128 binary bits to create a single unique address on the network. An IPv6 address is expressed by eight groups of hexadecimal (base-16) numbers separated by colons.IPv4 has a 20 byte header while IPv6 has 40 byte header. IPv6 provides a number of advanced features, and the massive increase in address space capacity is indisputably unique to IPv6 and represents the crowning objective for IP-address-hungry organizations. The main reason for a new version of the Internet Protocol was to increase the address space; IPv6 was designed with a 128 bit address scheme, enough to label every molecule on the surface of the earth with a unique address. IPv6 support scalability, multimedia transmissions, unlimited addresses, flexibility, robustness, enhanced security, better support for QoS, higher performance, built-in multicasting, enhanced mobility etc [3].

Manuscript received September 23, 2014.

Ihekweaba Ogechi, Department of Computer Engineering Michael Okpara University of Agriculture, Umudike, Abia state, Nigeria

Nweke Chisom B., Department of Computer Engineering Michael Okpara University of Agriculture, Umudike, Abia state, Nigeria

II. HISTORICAL BACKGROUND

At the end of the 1960's there was a great demand in various US universities and research centers for a network that should permit nationwide utilization of existing computer resources. In addition to that there was the desire for data exchange. Also, there was the interest in practical experiences, design, implementation, the use of network techniques in general and packet switching in particular. So the Advanced Research Project Agency, an US government organization, started developing a net called ARPANET [4]. From 1972 the Advanced Research Project Agency dealt with research projects of military interests and ARPANET were renamed DARPA. The first proposal was made in 1968. The contract was won in December 1968 by the company Bolt, Breakneck and Newman (BBN). The demands for file transfer, remote login and email were on top of the list for NCP (Network Control Protocol, the predecessor of TCP/IP). The first use of ARPANET was in 1971[5]. In 1973, a project was started, developing new lower layer protocols because the existing layers had become functionally inadequate. In 1974, Cerf and Kahn specified the following goals for the lower layer protocols, Independence from underlying network techniques and from the architecture of the host, Universal connectivity throughout the network, End-to-end acknowledgments, and Standardized application protocols. **I**n 1994, the Internet Engineering Task Force initiated development of the IPv6 suite of protocols, which were designed to replace IPv4. The IETF published the IPv6 standard in 1995.

Unlike IPv4, which has 32-bit addresses, IPv6 has 128-bit addresses. Thus, the new protocol increases the number of available IP addresses to 2**128** (about 3.4 x 10**38**) from IPv4's 2**32** (about 4.3 billion). IPv6 also offers other benefits. For example, the protocol specifies a new, simplified packet format designed to minimize header processing by routers. In addition, support for the IP Security standard is mandatory in IPv6 but optional in IPv4. Another advantage is that IPv6 hosts can auto-configure when connected to an IPv6 network. And the protocol's large address space enables multiple levels of hierarchy and greater flexibility in addressing and routing.

III. INTERNET PROTOCOL VERSION 4 (IPV4)

Internet Protocol version 4 (IPv4) is the fourth version of the Internet Protocol (IP) and it is the first version of the protocol to be widely deployed. It uses a 32 bit addressing and allows for 4,294,967,296 unique addresses [6]. It was the first that was widely used in modern TCP/IP. It provides the basic datagram delivery capabilities upon which all of TCP/IP functions and has proven its quality in use over a period of more than two decades. Figure1 shows a typical IPv4 Internet Edge Network

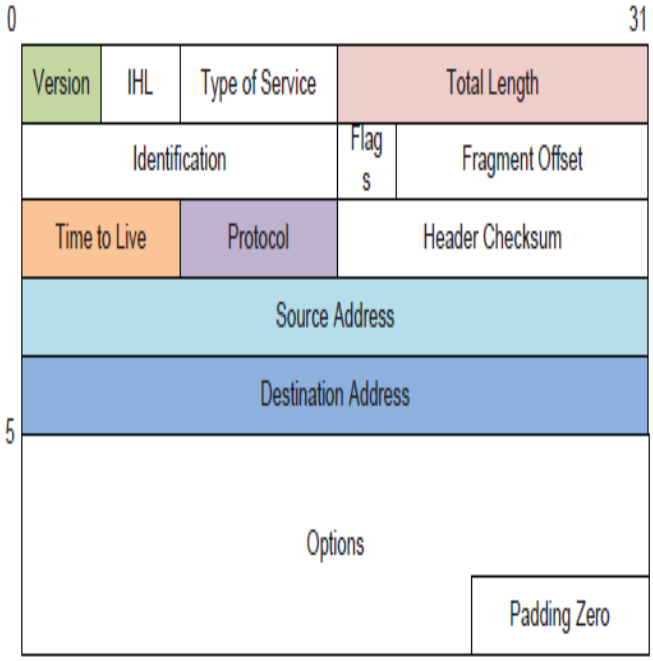

Figure1: IPv4 Internet Edge Network

A. *INTERNET PROTOCOL VERSION 6 (IPV6)*

Internet Protocol version 6 (IPv6) stands for Internet Protocol version 6 and also known as Ipng (IP next generation). It is the second version of the Internet Protocol to be used generally across the virtual world. IPv6 is developed as the next-generation network layer protocol, overcoming the problems in IPv4. Its 128-bit address format significantly enlarges the address space and will satisfy the address demands for a fairly long time. The length of the address also makes prefix aggregation fairly flexible, and subsequently achieves global addressing and routing in a hierarchical pattern. Forwarding efficiency is improved by simplifying the protocol header, as well as moving fragmentation to end hosts. In IPv6, flow label based QoS can be supported; stateless auto-configuration is invented to support Plug and Play feature. Besides, IPv6 has better mobility and security supports than IPv4 [7]. In general, IPv6 is a redesign of IPv4. It solves the problems in IPv4 and provides better IP service. It has been widely believed that IPv6 is the most mature and feasible solution for the next-generation Internet. Figure 2 shows an IPv6 transition environment

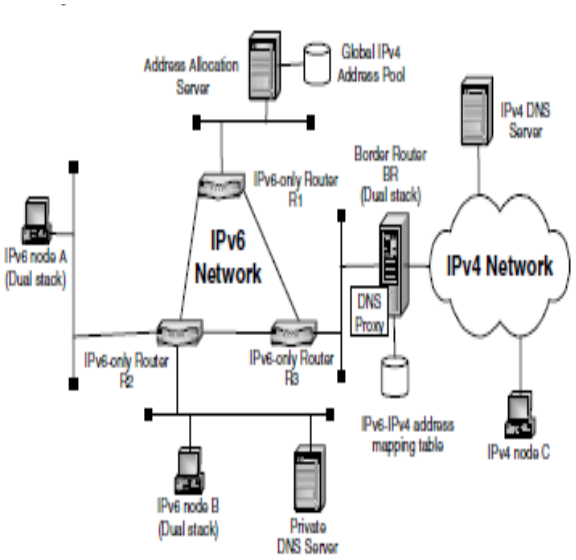

Figure2. An IPv6 transition environment

IV. LIMITATIONS OF IPV4

The limitations of IPv4 include:

A. *Address prefix allocation*

Because of the way that IPv4 address prefixes have been and are currently allocated, Internet backbone routers are routinely required to maintain unreasonably large routing tables of over 85,000 specified routes.

B. *Data security*

Private communication over a public medium like the Internet requires encryption services that protect the data being sent from being viewed or modified in transit. Although an add-on standard now exists for providing security for IPv4 packets (known as Internet Protocol Security or IPsec)

C. *Insufficient IP address space*

With only 32-bit capacity, IPv4 addresses have become relatively scarce, forcing some organizations to use Network Address Translation (NAT) to map multiple private addresses to a single public IP address. While NAT promotes conservation of the public address space, it does not support standards-based network layer security or the correct mapping of all higher layer protocols and can create problems when connecting two organizations that use the same private address space. The continued expansion of Internet-connected devices and appliances continues to put greater and greater stress on the public IPv4 address space [6].

D. *Quality of Service (QoS)*

While standards for QoS exist for IPv4, no identification of packet flow for QoS handling by routers is present within the IPv4 header. Instead, real-time traffic support relies on the IPv4 Type of Service (ToS) field and the identification of the payload, typically using a UDP or TCP port. However, the IPv4 ToS field has limited functionality and payload

identification using a TCP and UDP port is not possible when the IPv4 packet payload is encrypted.

E. Complexity of configuration

Most current IPv4 implementations must be either manually configured or use a stateful address configuration protocol such as Dynamic Host Configuration Protocol (DHCP). With more computers and devices using IP, there is a need for a Simpler and more automatic configuration of addresses and other configuration settings that do not rely on the administration of a DHCP infrastructure.

4.1. THE NEW FEATURES IN IPV6

The new features in IPv6 can be grouped into the following categories:

i. Address Size

IPv6 uses 128-bit addresses instead of the 32-bit addresses of IPv4. This is an increase of address space by a factor of 2. The address space provided by

IPv6 is large enough to accommodate continued growth of the Internet for many decades. There are enough addresses supported by IPv6 to provide an order of 6 * 10 23 unique addresses per square meter of the surface of the earth.

ii. Improved Options Mechanism

IPv6 options are placed in separate optional headers that are located between the IPv6 header and the transport layer header. Most of these optional headers are not examined or processed by any router on the packet's path. This simplifies and speeds up router processing of IPv6 packets compared to IPv4 packets.

iii. Address Auto-configuration

This capability provides for dynamic assignment of IPv6 addresses via stateful or stateless address auto configuration. DHCP is termed a stateful address configuration tool because it maintains static tables that determine which addresses are assigned to a new or moved station. A version of DHCP has been developed for IPv6. IPv6 also supports a stateless address auto-configuration service that does not require a manually configured server.

Stateless auto-configuration makes it possible for devices to configure their own addresses with the help of a local IPv6 router. Typically the device combines its

48-bit MAC address with a network prefix it learns from a neighboring router.

iv. Increased Addressing Flexibility

IPv6 includes the concept of any cast address, for which a packet is delivered to just one of a set of nodes. The scalability of multicast routing is improved by adding a scope field to multicast addresses.

v. Support for Resource Allocation

Instead of the type of service field in IPv4, IPv6 enables the labeling of packets belonging to a particular traffic flow for which the sender requests special handling. This aids in the support of specialized traffic, such as real-time video.

vi. Security Capabilities

IPv6 includes features that support authentication and privacy.

vii. The IPv6 Packet Format

The IPv6 datagram begins with a base header, which is followed by zero or more extension headers, followed by data. The only header required is that of the IPv6 header. This is of fixed size with a length of 40 octets compared to 20 octets for the mandatory portion of the IPv4 header.

4.2. PROPOSED TRANSITION MECHANISMS FROM IPV4TO IPV6 IN NIGERIA

The primary benefit of the transition comes from increased resources, not from radical protocol changes, as sometimes claimed. The original design goals of the new protocol were also very specific about enabling a smooth transition over the years and facilitating a long-term coexistence of IPv4 and IPv6.

Organizations with existing IPv4 networks needing to implement IPv6 face challenges in impacts, planning the transition and executing the migration to IPv6. Given the common organizational reliance on external communications for attracting new customers via the Internet, supporting dedicated partner links, home-based employees and providing Internet access for email, web browsing, etc., an overall plan should be compiled documenting the current environment, end users and the planned steps to IPv6 deployment.

Below are mechanisms to be employed while transiting from IPv4 to IPv6.

A. Dual Stack

Since IPv6 is a conservative extension of IPv4, it is moderately simple to write a network stack that supports both IPv4 and IPv6 while sharing most of the code. Such an implementation is called a dual stack. Most current implementations of IPv6 provide a dual stack. Figure 3 depicts the general protocol layers of a dual stack node. Figure 3 shows a typical Dual-stacked Network

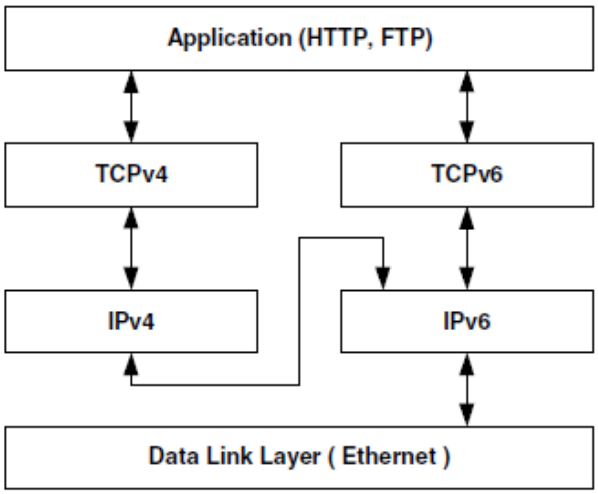

Figure 3: Dual-stacked Network

B. Tunneling

In order to reach the IPv6 Internet, an isolated IPv6 host or network must be able to use the existing IPv4 infrastructure to carry IPv6 packets. This is done using a technique known as tunneling, which consists of encapsulating IPv6 packets within IPv4, in effect using IPv4 as a link layer for IPv6. Figure 4 shows a typical IPv6 over IPv4 Tunneling

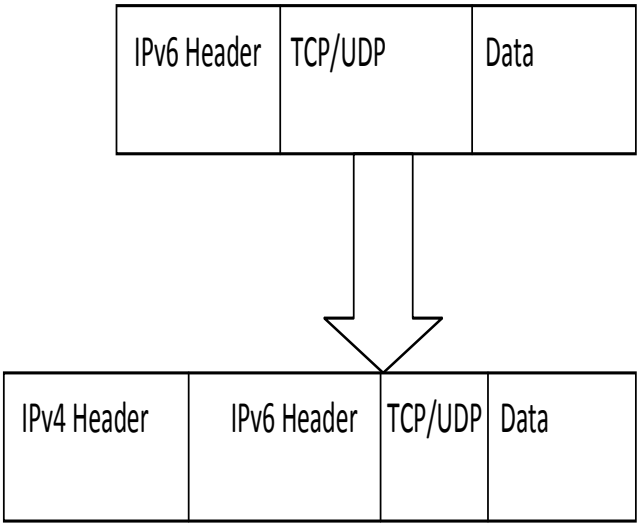

Figure 4: IPv6 over IPv4 Tunneling

i. Automatic Tunneling

Automatic tunneling refers to a technique where the tunnel endpoints are automatically determined by the routing infrastructure. Tunnel endpoints are determined by using a well-known IPv4 any cast address on the remote side, and embedding IPv4 address information within IPv6 addresses on the local side.

ii. Configured Tunneling

Configured tunneling is a technique where the tunnel endpoints are configured clearly, either by a human operator or by an automatic service known as a Tunnel Broker. Configured tunneling is usually more deterministic and easier to debug than automatic tunneling, and is therefore recommended for large, complex networks.

C. Proxying and Translation

When an IPv6-only host needs to access an IPv4-only service (for example a web server), some form of translation is necessary. The mainly commonly supported type of translation is the use of a dual-stack application-layer proxy, for example a web proxy. Techniques for application-agnostic translation at the lower layers have also been anticipated.

V. CONCLUSION

IPV6 is the next-generation internet protocol, intended as the follow-on to IPV4. It supports unlimited addresses, flexibility, robustness, enhanced security, better support for QoS, higher performance, built-in multicasting, enhanced mobility etc. This paper has x-rayed the importance of Transiting from internet protocol version four (IPV4) to internet protocol version six (IPV6).

REFERENCES

[1] RIPE NCC, "IPv4 - Running Out of Time?," 2003, http://www.ripe.net/internetcoordination/ ipv4-exhaustion/archive/ipv4- running-out-of-time

[2] G. Huston, "IPv4 Address Report," 2009, http://www.potaroo.net/tools/ipv4/index.html

[3] Jyh-Cheng Chen, O Caro, etal., 2000. "QoS Architecture for Future Wireless IP Networks" Twelfth Lasted International Conference on Parallel and Distributed Computing and Systems. Published In Website, Http://Citeseerx.Ist.Psu.Edu/Viewdoc/Summary?Doi=10.1.1.100.806Http://Citeseerx.Ist.Psu.Edu/Viewdoc/Summary?Doi=10.1.1.100.806.

[4] Chapman, D.B. and Zwicky, E.D. Building Internet Firewall, O' Reilly & Associates, Sebastopol, C.A, 199 5

[5] "Internet History Timeline," www3.baylor.edu/~Sharon_P_Johnson/etg/inthistory.h tm.

[6] Geoff Huston and Grenville Armitage, "Projecting future IPv4 router requirements from trends in dynamic BGP behaviour," in Proc. ATNAC, Dec 2006.

[7] S. Deering and R. Hinden, "RFC 2460. Internet Protocol, Version 6 (IPv6) Specification," 1998.

AUTHORS

Engr. (Mrs) Ogechi Ihekweaba is a lecturer in the department of Computer Engineering, Michael Okpara University Of Agriculture Umudike, Abia State, Nigeria. She holds a Bachelor degree (B.Eng) in Computer Science & Engineering, a Master's degree (M.Eng) in Computer Engineering and also at the verge of completing a Doctorate degree (PhD) in Computer Engineering. Her area of specialization is network security and computational intelligence. She is a COREN registered Engineer and has several publications.

Nweke Chisom B. received his B.Sc. degree in Computer Science from Michael Okpara University of Agriculture, (MOUAU) Umudike, Abia State Nigeria in 2012. His research interests are in the fields of Electronics Design and Embedded Systems, Computer Programming, Microcontroller based System, and Computer Maintenance etc.