Demonstrating the Impact of 6to4 Tunneling on IPv4 and IPv6 Network Coexistence

E. Osa, S. Konyeha, and E. Evbuomwan

Abstract — In this work the impact of the 6to4 tunnels is considered. In order for traffic to flow from an Internet Protocol version 4 (IPv4) website to a native Internet Protocol version 6 (IPv6) website, an additional configuration must be added to the network, as this cannot be done by default. The Riverbed Modeler Academic Version 17.5 is used to build and evaluate network efficiency with optimized 6to4 tunnels. The performance of the network is assessed based on the traffic received and sent by Internet Protocol (Version 6), Voice Called Traffic and the Sent and Received Traffic of the configured applications. The flow of traffic from servers to workstations in native IPv6 sites shows the effect of the tunnel configured.

Index Terms — IPv4; IPv6; 6to4 Tunneling; Internet, Protocol.

I. INTRODUCTION

End devices and nodes in a network require an IP (Internet Protocol) address to communicate. The address range of IP version 4 currently in use is not enough to address the increasing IP address requests [1]. Some techniques have been developed to handle the problem of address depletion such as Network Address Translation (NAT), Classless Inter Domain Routing (CIDR), Variable Length Subnet Mask (VLSM), and Port Address Translation (PAT). Internet Protocol, Version 6 (IPv6) was conceived by the Internet Engineering Task Force (IETF) to resolve the expected IPv4 address exhaustion issue. IPv6 is meant to replace IPv4 in the long run [2]. The IPv6 was built to provide ample address space for the internet’s increased growth to the present and future demand. IPv6 raises the size of the IP address scheme from 32 bits in Version 4 to 128 bits [3]. However, IPv6 has a number of new features over IPv4. IPv6 is not backward compatible with IPv4 with these improved features. The implication is that IPv6 hosts cannot interact directly with IPv4 hosts normally, and vice versa. Many transfer techniques have been introduced to ensure a quick, gradual and autonomous transfer to IPv6 with existing IPv4 networks, each of which has its own method of operation. These techniques are usually categorized into three main groups namely: Dual-stack, Tunneling and Translation [4].

II. TUNNELING

In the Tunneling method, the header of the packet is altered as it traverses from one protocol to another. IPv6 packets can then convert to IPv4 packets so that IPv6 network hosts can be interconnected via IPv4 backbone using IPv6 tunnels. The two oldest tunnel mechanisms originally published in 1996 are the Manual and Automatic [5]. Automatic tunnels are designed by embedding IPv4 address information into the IPv6 address packet, the IPv6 address of the destination host provides the information on which IPv4 address packet should be tunneled to [6]. However, the latest specifications for tunnel mechanisms include the following:

- Configured Tunnels [RFC 4213].
- Tunneling IPv6 over UDP through NATs (Teredo) [RFC4380].
- Automatic Tunneling [RFC2893].
- IPv6 over IPv4 without Explicit Tunnels (6over4) [RFC2529].
- Generic Routing Encapsulation (GRE) [RFC2784].
- Connection of IPv6 Domains via IPv4 Clouds (6to4) [RFC3056].
- Anything in Anything (AYIYA).
- Peer-to-Peer IPv6 on Any Internetwerk (6bed4)
- Locator/ID Separation Protocol (LISP) [RFC6830].
- Intra-site Automatic Tunnel Addressing (ISATAP) [RFC5214].
- IPv6 Rapid Deployment (6rd) [RFC5969].
- Native IPv6 behind NAT 44 CPEs (6a44) [RFC6751].
- Subnetwork Encapsulation and Adaptation Layer (SEAL) [7].

In 6to4 tunneling, the aim is to help those devices that are IPv6-enabled and reside in an IPv4 network, connect to other devices of the same configuration and to the IPv6-enabled Internet. This involves a “simple tunnel” that encapsulates IPv6 packets into IPv4 packets (by utilizing the protocol number ‘41’). This represents the IPv6 configured tunnel over IPv4 [6].

The IPv6 capable system can be a single device with a 6to4 pseudo-interface that encapsulates IPv6 packets in IPv4 packets and decapsulates IPv6 packets in the opposite direction. In this case it is called a 6to4 device. It is also possible for multiple IPv6 devices to exist in an IPv4 network behind a 6to4 border router which performs the encapsulation of the IPv6 packets into IPv4 packets and the decapsulation in the opposite direction. These 6to4 IPv6 devices can communicate with other 6to4 IPv6 devices or IPv6 devices on a native IPv6 Internet connection. However, in the latter case, a 6to4 relay mechanism is required at the IPv4 Internet and IPv6 Internet borders. If a link exists between two IPv6-enabled devices that both use 6to4 tunneling, the path of

S. Konyeha, Department of Computer Science, Faculty of Sciences, University of Benin, Nigeria.
E. Evbuomwan, Department of Computer Engineering, Faculty of Engineering, University of Benin, Nigeria.

Published on September 30, 2020.
E. Osa, Department of Electrical and Electronic Engineering, Faculty of Engineering, University of Benin, Nigeria. (corresponding e-mail: edosa.osa@uniben.edu)

DOI: http://dx.doi.org/10.24018/ejece.2020.4.5.245

Vol 4 | Issue 5 | September 2020
travel for the encapsulated packet in the IPv4 network is set by the public IPv4 addresses of the two 6to4 hosts and routers. If a communication node resides in the native IPv6 internet, the packet must go through a 6to4 relay [8]. A simple way to identify an IPv6 6to4 address is that the first 16 bits are always 2002 (in hexadecimal as defined in RFC 3056). The next 32 bits will be the IPv4 address, following the RFC specification. Thereafter, a special IPv6 subnet [9] will be defined for the next 16 bits.

III. OPNET (RIVERBED MODELER)

OPNET (Optimized Network Engineering Tool) was introduced to the public in 1987 as the premier commercial communications network simulation tool [10], [11]. OPNET is considered to be highly useful due to its potential to simulate a wide variety of networking technologies. It allows an entire network to be modelled, including devices such as routers, switches, protocols, servers, and the specific applications that these devices support. OPNET models consist of three primary layers namely; process layer, node layer, and network layer. Generally, OPNET can perform three main functions such as modelling, simulating and analysis of networks. It provides a very simple but comprehensive graphical environment [12].

IV. RELATED WORKS

Different researches have considered the efficiency of transformation methods for IPv6. In [13] the 6to4 transition process and tunneling were empirically compared with the Windows 2000 operating system on a testbed setup. [14] demonstrated the ease of transmission of TCP data using 6to4 tunneling as opposed to native IPv4 and IPv6 networks. [8] experimented with the 6to4 form of transformation IPv6. For performance and stability testing Linux sit, FreeBSD stf, and NetBSD stf 6to4 relay implementations were selected. It defined the test environment and the measurement process. In [15] 6to4 tunneling is implemented over OpenSSH with more than one device. In this paper the routing of traffic from a 6to4 site via an ISP relay to a native IPv6 site is shown.

V. EXPERIMENT SETUP

In this experiment the OPNET (Riverbed) Modeled Academic Edition version 17.5 was used to run the network simulations with a specific tunnel configured as Tunnel 0. The network testbed containing the following objects was implemented as displayed in Figure 1:

- Application Config. node:
  
  This module specified the applications supported by the network. The specified application name was used when constructing user profiles on the Profile Config object.

- Profile Config. node:
  
  The profile module described how the users implement the applications described in the Application configuration module.

- Four ethernet4_slip8_gtwy routers: Routers A, B, C and D.

- Four ethernet workstations: Workstations A, B, C and D.

  - Two IP_32 Cloud objects: For the IPv4 and IPv6 backbones respectively.
  - Two ppp_server_adv: For the Email and File Transfer Protocol (FTP) applications.
  - One ethernet_server: For the Hyper Text Transfer Protocol (HTTP) application.
  - One ethernet_server_adv: For the Database application.
  - IP Attribute Config. Node. This sets the Ping Parameters for the network.

A. Traffic Description

There are two 6to4 sites in the network above namely, sites W and X respectively. The 6to4 tunneling is configured on routers A and C so that they can communicate with each other. However, in order to communicate with the native IPv6 site, Z, the traffic needs to be routed through an ISP relay (site Y). Packets traversing from site W or X to the native IPv6 site will first go to router B (Relay router) before they reach their eventual destination and vice versa.

B. Configuration

Tables 1 through 6 show the configuration for the various nodes in the network.

| Table 1: Application Configuration |
|-----------------------------------|
| Application Name | Description |
| Web               | Http (Heavy Browsing) |
| FTP               | Ftp (High Load) |
| Remote Login      | Remote Login (High Load) |
| Email             | Email (High Load) |
| Voice             | IP Telephony and Silence Suppressed |

| Table 2: Profile Configuration |
|--------------------------------|
| Profile | Application |
| FTP & Voice | FTP, Voice |
| Voice & Email | Voice, Email |
| Remote Login & FTP | Remote Login, FTP |
| Email & FTP | Email, FTP |
TABLE 3: ROUTER CONFIGURATIONS

| Parameters                      | A B C D  |
|---------------------------------|---------|
| Static Routing (Destination address/ Next Hop) | 2002::/Tunnel0 and 2002::/2005:1:3::1 |
| Interface Address               | 2002:192.0.10.1:a:1 2002:192.0.4.1:a:1, 2002:192.0.10.1:a:1 |
| Tunnel Address                  | 2002:192.0.1.1:a:1, 2002:192.0.1.1:d:1, 2002:192.0.1.1:e:2 |
| LoopBack Address                | 2002:192.0.1.1:a:1, 2002:192.0.1.1:d:1, 2002:192.0.1.1:e:2 |

TABLE 4: WORKSTATIONS CONFIGURATION

| Attribute                  | A B C D  |
|----------------------------|---------|
| Interface Address          | 2002:192:0:1:a:1 2005:1:1::1 2002:192:0:1:b::1 2005:2:2::2 |
| IPv6 Default Route         | 2002:192:0:1:1 2005:1:1::1 2002:192:0:1:1 2005:2:2::1 |
| Profile Name               | FTP & Voice Remote Login & FTP Voice & Email FTP & Email |

TABLE 5: IPV6 BACKBONE CONFIGURATION

| Attribute                      | Value |
|-------------------------------|-------|
| Destination Address/Next Hop  | 2002::/2005:1:3::1 |
| Interface Address             | 2005:1:3::2, 2005:2:1::2 |

TABLE 6: SERVERS CONFIGURATION

| Application | Email | Terminal | FTP | HTTP |
|-------------|-------|----------|-----|------|
| IPv6 Default Route | 2002:192:0.1:1 2002:192:0.1:1 | 2002:192:0.1:1 2002:192:0.1:1 | 2002:192:0.1:1 2002:192:0.1:1 | 2002:192:0.1:1 2002:192:0.1:1 |

C. Simulation Duration

The simulation process was run for 600 seconds and value per statistic set to 100. Four types of statistics were collected which include: IPv6 Traffic Received, IPv6 Traffic Sent, Voice Calling Party Traffic Sent and the various client application Traffic Sent and Received.

VI. RESULTS

Figures. 2 through 5 show the results for the simulation. However for brevity only selected results are displayed.

VII. DISCUSSION

For the nodes linked to the IPv4 cloud backbone as well as the IPv6 cloud backbone, there is IPv6 traffic flow across all locations within the network. This proves that there is some additional process, as IPv4 traffic cannot flow to a native IPv6 location, and vice versa by default. In this experiment the mechanism responsible is the 6to4 tunnel configured in the routers (i.e. Tunnel 0). Figure 4 shows that Workstation D sends and receives Email traffic, whereas the email server is located outside the native IPv6 site and Figure 5 shows that Workstation D sends and receives FTP traffic while the FTP server is located outside the native IPv6 network. This is because of design of the tunnel.
VIII. CONCLUSION

This simulation experiment was performed to demonstrate the impact of configuring 6to4 tunnel in a network that is made up of both IPv4 and IPv6 sites. It was shown that due to the configuration of tunnels it was possible for traffic to flow from non-native IPv6 sites to native IPv6 sites. Hence as the IPv4 depletion process is almost complete, Internet active organizations should consider the option of implementing 6to4 tunneling, as they migrate to an IPv4- IPv6 coexistence scenario.

ACKNOWLEDGMENT

This work was sponsored by the Telecommunications Unit of EDYSYS Solutions, Nigeria.

REFERENCES

[1] G. Huston. (May 2010), “IPv4 Address Report.” Available: http://www.potaroo.net/tools/ipv4/index.html. 2010.
[2] New Zealand IPv6 Task Force, 2010, “FAQs” [Online] Available: www.IPv6.org.nz.
[3] R. Hinden and S. Deering, “Internet Protocol Version 6 (IPv6) Addressing Architecture”, RFC 3513, April 2005.
[4] K. Bayan and A. Ahmad, Impact of IPv4/IPv6 Transition Techniques on Applications Performance. International Conference on Electronics, Information and Communication (ICEIC2017) At: Phuket, Thailand. 2017.
[5] R. Gilligan and E. Nordmark, ‘Transition Mechanisms for IPv6 Hosts and Routers’, RFC 1933, April 1996.
[6] E. Normark and R.E Gilligan, “Basic transition mechanisms for ipv6 hosts and routers,” RFC4213, 2005.
[7] S. Steffann, I. van Beijnum and R. van Rein, A Comparison of IPv6 over IPv4 Tunnel Mechanisms, Network Working Group, Internet-Draft, April 11, 2013.
[8] L. Gábor and R. Sándor, (2013). Performance Analysis and Comparison of 6to4 Relay Implementations International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 4, No. 9.
[9] Hexasoft, (2019). What is 6to4 tunneling? [Online] Available: www.IP2Location.com.
[10] F. Sally, (2020). Network Simulators. [Online] Available: http://www.icir.org/models/simulators.html.
[11] OPNET Technologies, Inc. (2004). “OPNET Modeller”.Available: http://www.opnet.com/products/modeler/chome.html.
[12] S.B Jyoti, G. Debonita and N. Shovon, 2014, OPNET: A New Paradigm for Simulation of Advanced Communication Systems, International Conference on Contemporary Challenges in Management, Technology and Social Sciences at M.G. Institute of Management and Technology, Lucknow, India. April 5th-6th, 2014.
[13] I. Raicu and S. Zeadally, “Evaluating ipv4 to ipv6 transition mechanisms,” in 10th International Conference on Telecommunications, ICT 2003, vol. 2. IEEE, 23 Feb.–1 March 2003, pp. 1091–1098.
[14] N. Bahaman, E. Hamid and A. Prabuwono, “Network performance evaluation of 6to4 tunneling,” in International Conference on Innovation Management and Technology Research (iICMTR), Malacca: IEEE, May 2012, pp. 263–268.
[15] I. Coonjah, P.C. Catherine and K.M.S Sojjaudah , “6to4 tunneling framework using OpenSSH,” IEEE 2015 International Conference on Computing, Communication and Security (ICCCS), Pamplemousses, Mauritius, 2015, pp.1-4.