Available Online at www.ijecse.org **ISSN- 2277-1956**

PERFORMANCE ANALYSIS OF CONFIGURING IPV6 NETWORKS COMMUNICATING OVER IPV4

Dr. Preeta Sharan [1], Sarvotham Prasad R [2]
[1 2] *Department of Electronics and Communication Engineering,*
The Oxford College of Engineering, Bangalore.
[1] *Proffesor, Dept. of ECE*
[2] *3 Sem, Mtech. In Vlsi Design and Embedded Systems*

Abstract- IPv6 is designed to solve many of the problems of the current version of IP (known as IPv4) such as address depletion, security, auto-configuration, research and extensibility. The Proposed work deals with the IPv4-IPv6 tunneling method where performance & analysis of multimedia data communication using IPv4-IPv6 Mixed Networks is done. We are using TCP (Transmission Control Protocol) for the communication on the Connection Oriented Network. This paper presents a new implementation idea through which we can have a cost effective IPv4 – IPv6 mixed multimedia communication network

After Experimental Analysis it has been observed that performance of the tunneling Method is Superior Compared to the IPv4-IPv6 network. The time required to access the data at the destination is estimated and the values obtained during minimum attenuation are 260 seconds and maximum attenuation is 330 seconds. And the same using tunneling method is 270 seconds. The Video File takes 20 and 28 seconds for minimum and maximum attenuation. The tunneling method uses 270 sec for audio file and 25 seconds for the access of video file 270 sec for audio file.

Keywords - Dual stack protocol, IPv4, IPv6, Tunneling.

I INTRODUCTION

Multimedia is a popular application in Internet. Multimedia communication in Internet needs a large bandwidth. It is not easy to implement in the wireless network for the unstable radio bandwidth. With rapid growing of wireless and mobile technologies, portable wireless and mobile devices can access Internet ubiquitously. The integrating of Internet and the mobile communication provided the users to be able to access the Internet services anytime and anywhere is an important issue for mobile computing. That is, to overcome the unstable and limited bandwidth in the wireless network is the main issue for the wireless multimedia communication.

In order to support multi-media services in IP-based networks, it is important to assure service qualities, e.g., delay, since IP networks inherently provide best effort service. In general, modeling of IP-based networks supporting multi-media services is complex and thus QoS estimation is challenging. IPv6 security is in many ways the same as IPv4 security. The basic mechanisms for transporting packets across the network stay mostly unchanged, and the upper-layer protocols that transport the actual application data are mostly unaffected. However, because IPv6 mandates the inclusion of IP Security, it has often been stated that IPv6 is more secure than IPv4. Some significant differences, however, exist between IPv4 and IPv6 beyond the mandate of IP security. IPv6 includes a transition mechanism which is designed to allow users to adopt and deploy IPv6 in a highly diffuse fashion and to provide direct interoperability between IPv4 and IPv6 hosts.

II. IPv4 COMMUNICATION

In order to support multi-media services in IP-based networks, it is important to assure service qualities, e.g., delay, since IP networks inherently provide best effort service. In general, modeling of IP-based networks supporting multimedia services is complex and thus QoS estimation is challenging. IPv4 is the dominant addressing protocol

used on the Internet and most private networks today. With the current exponential growth in Internet users worldwide, combined with the limited address range of IPv4, the number of available public IPv4 addresses remaining is very limited. IPv4: 232 addresses equal 4.3 billion addresses (less than the global human population of 4.7 billion).

Because no further large allocations of IPv4 addresses are available, the ability of Asia-Pacific ISPs to allocate IPv4 addresses for new customers depends on the number of addresses they already hold, the rate at which they are using them for new services, and the ISP's capability to adopt address translation technologies, which may reduce their rate of address demand. These factors will be different for each ISP, so it is likely that ISPs across the industry will run out of IPv4 addresses across wide timeframe – some may run out within only a couple of years, others may be able to delay that exhaustion well into the future.

III. IPv6 COMMUNICATION

IPv6 was designed during the mid-1990s, when the Internet Engineering Task Force (IETF) realized that IPv4 address size constraints would soon be a major impediment to the continued growth of the Internet. IPv6 was first known as the Next Generation Internet Protocol (IPng) during development within the IETF. Since 1998, it has officially been known as IPv6. In the transition to IPv6, both IPv6 and IPv4 will co-exist until IPv6 eventually replaces IPv4.

The most obvious difference between IPv6 and IPv4 is the address size. IPv6 addresses comprise 128 bits, whereas IPv4 addresses comprise 32 bits. This difference results in a huge expansion in available IP address space:

- IPv6: 2128 addresses. Because the last 64 bits are used to allocate addresses within a subnet that leaves 264, which equals 18 billion subnet addresses.

Whilst IPv6 performs the same address function as IPv4, IPv6 is not backwardly compatible with IPv4. Therefore, an IP data session must use either IPv4 or IPv6 end-to-end. IPv6 and IPv4 can be used together with translation mechanisms such as Application Layer Gateways when the applications are known and supported end-to end.

IV. IPv6 OVER IPv4 TUNNELING

The term "tunneling" refers to a means to encapsulate one version of IP in another so the packets can be sent over a backbone that does not support the encapsulated IP version. For example, when two isolated IPv6 networks need to communicate over an IPv4 network, dual-stack routers at the network edges can be used to set up a tunnel which encapsulates the IPv6 packets within IPv4, allowing the IPv6 systems to communicate without having to upgrade the IPv4 network infrastructure that exists between the networks. A variety of tunneling mechanisms are available for deploying, they include:

- Configured Tunnels- when network administrators manually configure the tunnel within the endpoint routers at each end of the tunnel. Any changes to the network like renumbering must be must manually reflected on the tunnel endpoint. Tunnels result in additional IP header overhead since they encapsulate IPv6 packets within IPv4 (or vice versa).
- Automatic Tunnels - refers to a technique where the routing infrastructure automatically determines the tunnel endpoints. Tunnel endpoints are determined by using a well-known IPv4 anycast address on the remote side, and embedding IPv4 address information within IPv6 addresses on the local side.

V ARCHITECTURE AND IMPLEMENTATION

There are many methods to set up the combinational network. Tunneling is one of the methods used in common. IPv6 is the major network and An IPv6 tunnel is created over IPv4. Similarly, Tayga Tunnel is used to configure IPv6 over IPv4 in a mixed network.

Besides the technical details of IPv6, a very practical matter of IPv6 is: how will the public Internet, which is based on IPv4, be transitioned to IPv6? The problem is that while new IPv6-capable systems can be made "backwards compatible", already deployed IPv4-capable systems are not capable of handling IPv6 datagram's. Several options are possible. Probably the most straightforward way to introduce IPv6-capable nodes is a dual-stack approach, where IPv6 nodes also have a complete IPv4 implementation as well. Such a node, referred to as an IPv6/IPv4 node, has the ability to send and receive both IPv4 and IPv6 datagram's. When interoperating with an IPv4 node, an IPv6/IPv4node can use IPv4 datagram's, when interoperating with an IPv6 node, it can speak IPv6. IPv6/IPv4 nodes must have both IPv6 and IPv4 addresses. They must furthermore be able to determine whether another node is IPv6-capable or IPv4-only.

In the dual-stack approach, if either the sender or the receiver is only IPv4-capable, an IPv4 datagram must be used. As a result, it is possible that two IPv6-capable nodes can end up, in essence, sending IPv4 datagram's to each other.

An alternative to the dual-stack approach is known as tunneling. Tunneling can solve the problem noted above. The basic idea behind tunneling is illustrated in Figure 1. (The intervening set of IPv4 routers between two IPv6 routers is referred to as a tunnel.)

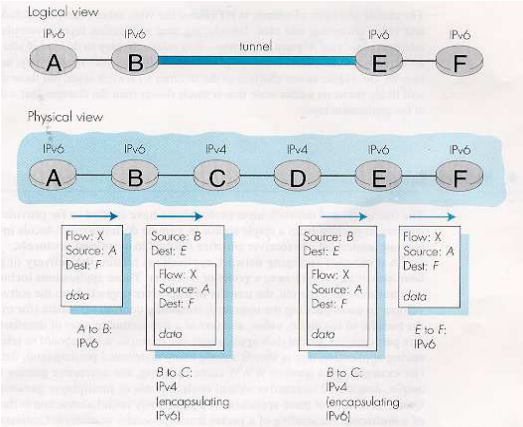


Figure 1: Tunneling

With tunneling, the IPv6 node on the sending side of the tunnel (router B) takes the entire IPv6 datagram and puts it in the data field of an IPv4 datagram. This IPv4 datagram is then addressed to the IPv6 node on the receiving side of the tunnel (router E) and sent to the first node in the tunnel (router C). The intervening IPv4 routers in the tunnel route this IPv4 datagram among themselves, just as they would any other datagram, blissfully unaware that the IPv4 datagram itself contains a complete IPv6 datagram.

The IPv6 node on the receiving side of the tunnel eventually receives the IPv4 datagram, determines that the IPv4 datagram contains an IPv6 datagram, extracts the IPv6 datagram, and then routes the IPv6 datagram exactly as it would if it had received the IPv6 datagram from a directly connected IPv6 neighbor.

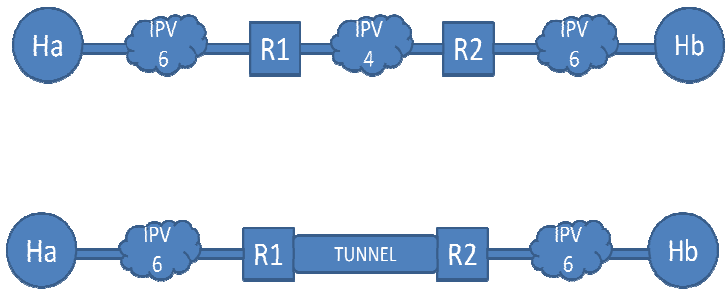


Figure 2 Implementation Diagram

To minimize any dependencies during the transition, all the routers in the path between two IPv6 nodes do not need to support IPv6. Basically, IPv6 packets are placed inside IPv4 packets, which are routed through the IPv4 routers. The following figure illustrates the tunneling mechanism through IPv4 routers. The implanted Diagram Of the Network is as shown above in Figure 2. The communication between IPv4 and IPv6 systems within a network is possible with the above mentioned process. But when it comes to the matter of server and client there are many things to note about communication, mapping of addresses etc.

VI. SIMULATION RESULTS AND ANALYSIS

We have considered four computers out of which two computers are host computers and remaining two are configured as Routers using nc commands on ubuntu-11.10 platform. Out of two hosts, one is configured as source hosts and the other is configured as destination hosts. From source hosts we are sending audio, text and video data in bulk and the links which are connected with this host to first router is carrying data in Gb ps.

The optical fiber cable of different lengths are considered and we have observed the effect of cable length, attenuation occurred when cable lengths are increased or decreased. Various optical components like couplers, multiplexers, attenuators are used to verify the results. Source Host1 data is multiplexed using a multiplexer, transferred through a bottleneck link and de-multiplexed finally to receive the output at destination host.

We are using TCP (Transmission Control Protocol) for the communication on the Connection Oriented Network.IPv4 and IPv6 Protocols are used in the respective networks defined before. The intermediate routers are configured with Dual Stack Protocols to use IPv4 and IPv6 simultaneously.

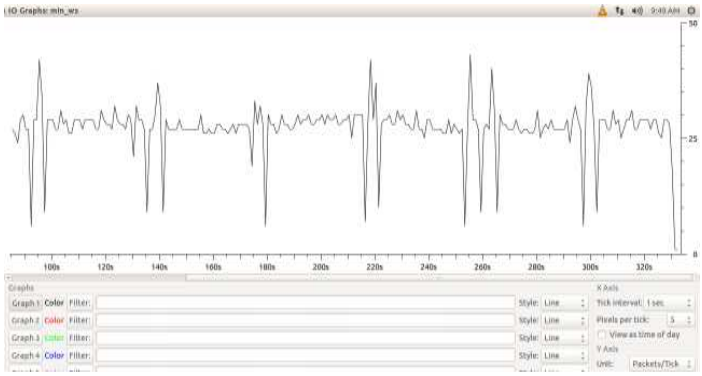
Configuring Linux (Ubuntu) system as router Creating Virtual Server using Apache server and transmitting multimedia data. Data transmission using Ethernet cable and Optical Fiber Cable Comparing and analyzing the performance of Mixed Networks.

(i) Using Minimum and Maximum attenuation (Audio)

Initially the whole network was configured to be mixed IPv4-IPv6 multimedia data communication network and the multimedia data like: audio, video are transmitted from server to client. And Using the OFC cables with an attenuator. The resulting analysis is as shown below:

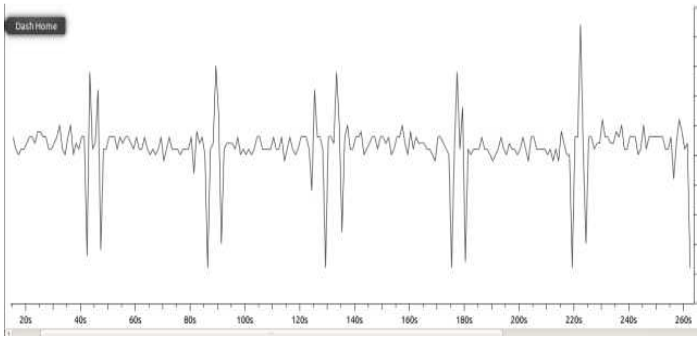
a) Minimum Attenuation

Figure 3. (a) Minimum attenuatione (b) Maximum attenuation (c) Video File Minimum and (d) Maximum Attenuation



(a)

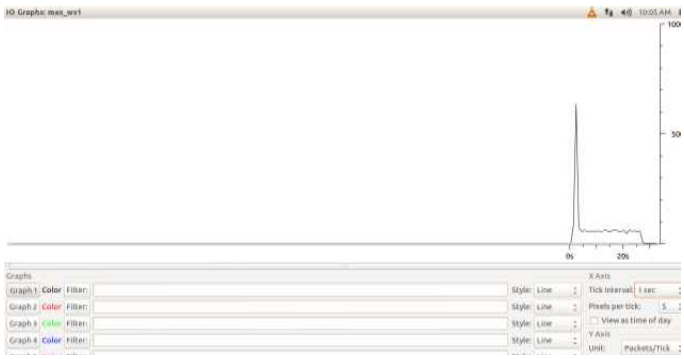
b) Maximum Attenuation



(b)

c) Video File Minimum and Maximum Attenuation

(C)



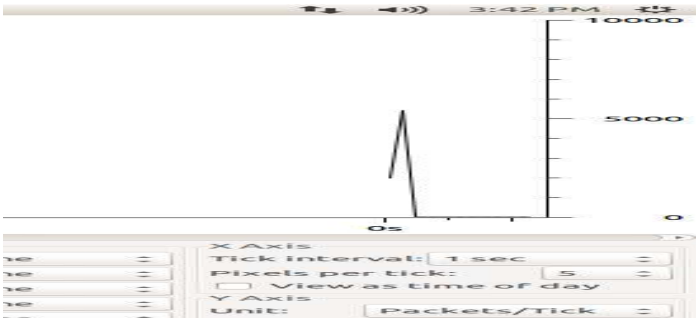
(d)

(ii) Using Tunneling Method

Initially the whole network was configured to be IPv4-IPv6 server client for multimedia data communication network and the multimedia data like: audio, video. In this method the tunnel is established between the systems. The resulting analysis is as shown below:

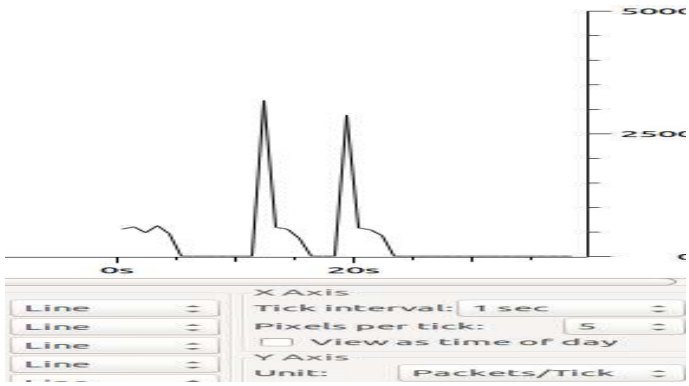
a) Audio File

Figure 4.Ttunneling method (a) Audio File (b)Video File



(a)

b) Video File



(b)

The Following Table 1 Shows the Comparison of the Different methodologies used and the use of OFC for real time multimedia communication. Here the Data requires the time for getting accessed and downloaded at the destination system. So it is calculated using the wireshark tool at the destination system. Hence the tabulated values are listed below.

Table -1 Experiment Result

Multimedia	File Size (Mb)	Time Taken For Accessing The Data At the Destination (Sec)		
		Minimum Attenuation	Maximum Attenuation	Using Tunnel Method
Audio	8.4	260	330	270
Video	26.2	20	28	25

VII CONCLUSION

We see that, now-a-days each and every company is replacing their IPv4 server to IPv6 servers. The process of replacing IPv4 server to IPv6 servers is cost effective. IPv6 is deployable in a production environment. Not only does it solve the shortage of addresses, but it also promises a number of enhanced features which are not an integral part of IPv4. The transition between today's IPv4 Internet and a future IPv6-based one will be a better process during which both protocol versions will coexist. Though the benefits of IPv6 are well understood, the cost of overhauling the existing IPv4 infrastructure is prohibitive for many network operators and service providers.

We have succeeded in configuring the computers as routers and perform different analysis using these routers. The comparison between the use of Mixed Network and the IPv4-IPv6 network has been done. The Audio and Video files are transferred with the apache server. The results obtained for minimum and maximum attenuation for audio files are 230 and 330 seconds respectively. For tunneling method the audio and video files are accessed at the destination of duration 270 and 25 seconds respectively. The results are analyzed using Wireshark Network analyzer.

For the present world in which the IPv4 addresses are being getting empty, the transition of each system address into IPv6 address helps not to replace the older systems**.**

VIII ACKNOWLEDGMENT

I am very thankful to VGST (Vision Group on Science and Technology), Government of Karnataka for the Funding of this Project. With their support and Helping in setting up of the lab in The Oxford College of Engineering., Bangalore.

REFERENCES

[1] Chapter 4 Making the Transition from IPv4 to IPv6 (IPv6 Administration Guide).
[2] "IPv4 to IPv6 Transition – *Update 2011*" A white Paper, September 2011.
[3] Alexander F. Yaroslavtsev, Tae-Jin Lee, Min Young Chung, Hyunseung Choo. "Performance analysis of IP-Based Multimedia Communication Networks to support Video Traffic", Institute of Mining, Siberian Branch of the Russian Academy Of Science Novosibirsk, Russia. ICCS 2004, LNCS 3036, pp. 573-576, 2004. Springer- Verlag Berlin Heidelberg 2004.
[4] Long-Sheng Li,Shr-Shiuan Tzang, Gwo-Chuan Lee and Young-Yu Yang (2011), "*Performance Analysis of an Efficient Multicast Scheme for the Multimedia Communications in NEMO"*, Tamkang Journal of Science and Engineering, Vol. 14, No. 3, pp. 191200.
[5] Lucia Bello (2012), *"The Case for Ethernet in Automotive Communication"*, University of Catania, Italy.
[6] Alexander F. Yaroslavtsev1, Tae-Jin Lee2, Min Young Chung2, and HyunseungChoo (2004),"*Performance Analysis of IP-Based Multimedia Communication Networks to Support Video Traffic"*, M. Bubak et al. (Eds.): ICCS 2004, LNCS 3036, pp. 573–576, 2004. Springer-Verlag Berlin Heidelberg 2004.

[7] Website links https://security.appspot.com/vsftpd.html http://help.ubuntu.com/10.01/serverguide/ftp-server.html http://linux.die.net/man/5/vsftpd.conf
[8] GaborLencse, SandorRepas, *"Performance Analysis and Comparison of Different DNS64 Implementations for Linux, OpenBSD and FreeBSD"*,Department of Telecommunications SzechenyiIstvan UniversityGyor, Hungary. IEEE AINA 2013, Barcelona, Spain.
[9] Ferdinando, Samaria, Harold Syfrig, Alan Jones and Andy Hopper, *"Enhancing Network Services through Multimedia Data Analysers"*, ORL, Olivetti & Oracle Research Laboratory24 Trumptington St Cambridge CB2 1QAUnited Kingdom.
[10] Handout "Transition from IPv4 to IPv6", ", IEEE Workshop on Wireless Multimedia Data Netowroks, PESIT, Bengaluru, INDIA.