Analysis of Packet Transmission Overhead of IPv4 and IPv6 through Simulation

Nitul Dutta
MEF Group of Institution, Rajkot, Gujrat, India-360003

Kushal Pokhrel
Sikkim Manipal Institute of Technology, Majhitar, India -737136

S.R. Biradar
MITS, Lakshmangarh, Sikar, Rajasthan, India- 332311

Kiran Gautam
Sikkim Manipal Institute of Technology, Majhitar, India -737136

Md. Abusafi
Jadavpur University, Kolkata, India

Shrijana Pradhan
Sikkim Manipal Institute of Technology, Majhitar, India -737136

Krishna Chakraborty
MEF Group of Institution, Rajkot, Gujrat, India-3600033rd

Saswati Bhattacharyee
Sikkim Manipal Institute of Technology, Majhitar, India -737136

ABSTRACT
Internet Protocol (IP) is becoming a dominant network layer protocol in the current network. Due to some limitations, mainly the shortage of address space in IP version 4 (IPv4), the newer version of the protocol named IPv6 is increasingly getting its popularity. But there is already a huge investment made towards the implementation of IPv4. Also, new applications have started developing using IPv6. So, there is a great confusion among users of IP based network whether to deploy IPv6 or stay back with IPv4. This paper is a general comparative study of both the versions of IP and intended to outline few scenarios that may be considered during the selection of IP version as a network layer protocol. The findings of this work are presented in the form of graphs which focus few positive sides of using IPv4. The advantages of IPv6 over IPv4 are tabulated to realize the benefits of using IPv6 as well. The conclusion drawn from the work carried out may be considered as a basis for the proper selection of the different versions of the protocol.

Keywords
IPv4, IPv6, Packet, Protocol, Security.

1. INTRODUCTION
Most of today's internet uses IPv4 as a network layer protocol [1]. Over twenty years old IPv4 is remarkably useful but in spite of that it suffers few problems which could not be tolerated. Most importantly there is a shortage of IPv4 addresses, as every device in the Internet that uses IPv4 (or IPv4 as well) needs a unique address. To resolve the problem of limited address range, a method called Network Address Translation (NAT) firewall was proposed to map multiple private addresses to a single public IP address [2]. Although NAT is a very powerful technique, it does not support standard network layer security and also creates complicated barriers to VoIP, and other services [3]. Due to inclusion of NAT, the routing tables of Internet backbone routers are becoming larger, since a separate routing table entry is needed for each network comprised of NAT. Another problem with IPv4 is the security. The security features are not integrated with IPv4, perhaps security is realized by means of some external security protocols. One example is the use of IPSec protocol as an encrypting mechanism for IPv4 traffic. But all of the IPv4 encryption methods are proprietary and no real standard encryption methods exist.

Internet Protocol version 6 (IPv6) is the next-generation Internet Protocol version designated as the successor to IPv4 [4]. IPv6 was defined in December 1998 by the Internet Engineering Task Force (IETF) with the publication of an Internet standard specification, RFC 2460. The main intention for the redesign of Internet Protocol was to resolve the foreseeable IPv4 address exhaustion. IPv6 has defined a larger address space than IPv4. This results from the use of a 128-bit address, whereas IPv4 uses only 32 bits. The IPv6 address space supports 2128 (about 3.4×1038) unique addresses. This expansion provides flexibility in allocating addresses and routing traffic and eliminates the need for NAT, which gained widespread deployment as an effort to alleviate IPv4 address exhaustion [5].

The actual confusion begins here. Having two different versions of the same popular protocol, users got confused regarding the protocol that should be adopted for their work with IP based network. As it is clear that during the span of more than twenty years, a huge investment is made by the investors to deploy IPv4 based network and applications, a sudden change in such a protocol is really a matter of thoughts. Famous golden rule in computer world says that "never touch a running system." If we apply this to IPv4 based network, then as long as they do what you need them to do, we should let them run. But when an IPv4 network hits the limits for some reason, IPv6 could be evaluated. Many case studies and deployments worldwide shows that IPv6 is mature enough to be used in corporate and commercial networks. But looking into the high investments already made in the past for IPv4 setups, it is vital to understand clearly the strength and weakness of both the versions of the protocols. Based on this, one in a state of confusion regarding the use of the newer or older version of the IP, can judge the requirement of the appropriate version of the protocol. Until the limit is reached where it becomes crucial to shift to IPv6, IPv4 can carry on serving as the network layer protocol. This paper is intended to give a brief idea of the fact what we may lose or gain by using either of the versions of the protocol.

Rest of the paper is organized as follows. A survey of related work along with our motivation is found in section II. Section III presents the simulation scenario in network simulator 2 (ns-2). A brief discussion of the simulation results are in section IV. In section V, few tables are presented to understand the benefits of using IPv6 over IPv4. Finally, section VI concludes the paper.

2. SURVEY OF RELATED WORKS

Since IPv6 is not yet mature enough, a lot of research is going on to study the behavior of the protocol. But comparatively there is less work that compares the performance of IPv4 and IPv6. Most of the research work in this area discusses the different transition mechanisms and compares their performance on IPv4 with respect to IPv6 based network. Few of such works are presented in this section. The work in [6] presents a comprehensive performance comparison of IPv6 and IPv4, including connectivity, packet loss rate and roundtrip time using a test bed. They have traced 585,680 in the packet-level with 133,340 million packets collected from 936 IPv4/IPv6 dual-stack Web servers located in 44 countries. Results show that IPv6 connections tend to have smaller RTTs than their IPv4 counterparts, but suffer higher packet loss rate at the same time. Also the tunneled paths do not show notable performance degradation compared with native paths. They have claimed their paper as the first performance study based on both large scale TCP and ICMP traffic measurement in real IPv6 Internet. Now-a-days, more attention is paid to the performance and operational issues of IPv6 networks. In [7], the main emphasis has been given to measure the IP's Quality-of-Service (QoS) provisioning of both the protocols. The gap of QoS between IPv4 and IPv6 has been broadly analyzed through a video-streaming application. Their experiments were performed using two different operating systems (OS) with different test-bed configurations. The QoS performance parameters that have been considered are delay, Jitter, throughput and packet loss. The target was to determine how efficiently IPv4 and IPv6 behave under these performance metrics. Their results show that the average delay observed in IPv6 is less than that observed in IPv4. Also in general IPv6 gives significantly lesser and somewhat constant jitter than IPv4. The results and conclusion show the comparison of IPv4/IPv6 dual-stack performance measures over three different network configurations and IPv6 supported host in hybrid network. They have concluded the paper with the observation that IPv6 has better performance over hybrid network compared to network bridge and isolated network through cross-cable on the dual-stack scenario. In [8], the authors discuss the IPv6-in-IPv4 tunnel discovery problem along with a proposal for a set of techniques to infer and validate tunnel end points by combining basic methods. Their experimental results show traffic traverse around 60% of the total path through IPv6 tunnel in the Internet. The authors of [9] argue that major hurdles to the perceived quality of the IPv6 Internet are created by poorly managed experimental IPv6 sites. With focuses on troubleshooting, they select a group of IPv4/IPv6 dual-stack nodes by DNS lookups, and study the IPv6: IPV4 RTT ratios by dual-stack ping with a path analysis using trace route from three different locations in Japan and Spain. In the work discussed in [10], the authors have adopted the DSTM to study network performance with few types of traffic sources: Voice-over-IPv4, FTP-overIPv6, and MPEG-4-over-IPv6. The performance is evaluated considering bandwidth, throughput, percentage of dropped packets, and mean end-to-end delay of each traffic flow for both IPv4 and IPv6. Through the simulations performed by using the Network Simulator 2 (ns-2), they have shown that when the traffic density of IPv6 session increases, the bandwidth of IPv6 session increases at the expense of the decrement of the bandwidth of IPv4 session. On the other hand, the increment of the traffic density of IPv4 session does not increase its bandwidth due to its lower priority. In addition, the increment of packet size of IPv6 traffic results in the increment of a little bit of the mean end-to-end delay, but it is not the case for IPv4 traffic. In [11], the authors have presented the impact of IPv6 transition mechanisms on user application. Through experimental results, they have shown that though performance overheads were minimal, with small, fragmented and translation packets degrades some performance. They have compared IPv4 versus IPv6 header overhead and header overhead between transition mechanisms. Their work also reflects CPU utilization of all these mechanisms and certain other performance aspects like throughput and round-trip time for several types of traffic. And it was intended to empirically analyze impacts on transition mechanisms compared with IPv4-only and IPv6-only network performance. In [12], the authors have analyzed more than 600 end-to-end IPv6 paths between about 26 test boxes of RIPE NCC over the past two years, and compared the delay and loss performance evolution in IPv6 with their IPv4 counterparts. They have presented and discussed the measurement methodology, and provided evidence that IPv6 network has a higher delay and loss evolution than IPv4. Finally, based upon their measurements, they have assessed the perceived quality of three real-life applications: VoIP, Video-over-IP and data communication services based upon TCP. They have found that for VoIP and Video-over-IP, the differences in delay and packet loss between IPv4 and IPv6 do not translate to the perceived quality domain but for applications based upon TCP, the differences in delay and packet loss between IPv4 and IPv6 have a strong impact on the realized throughput.

All of these papers lack a direct and prominent discussion of IPv4 and IPv6 performance. The novelty of this work is that there is very little exposure given by researchers to compare the behavior of the two versions of the protocol. So exploring this area with a wide variety of applications on different types of traffic was significant. Besides, we also want to show a comparative performance evaluation of these applications considering both IPv4 and IPv6 network. Our effort to understand the IPv6 performance and operational issues is not complete. Future research can help to evaluate the complete realization of the same so as to be nominated as the future generation internet layer protocol.

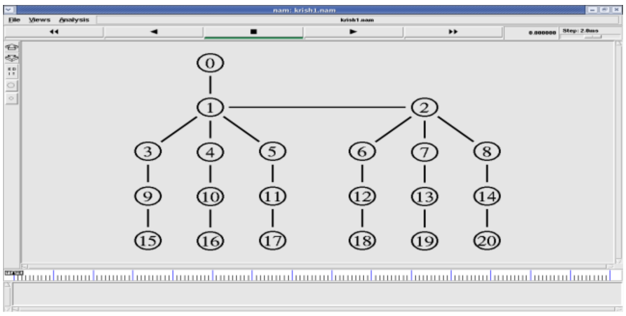

Figure 1. Simulation scenario

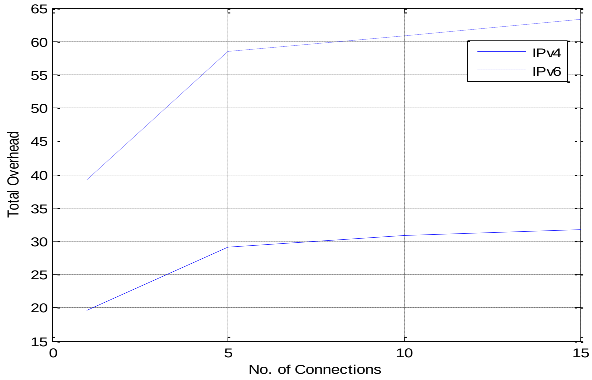

Figure 2. Signaling overhead versus number of connections

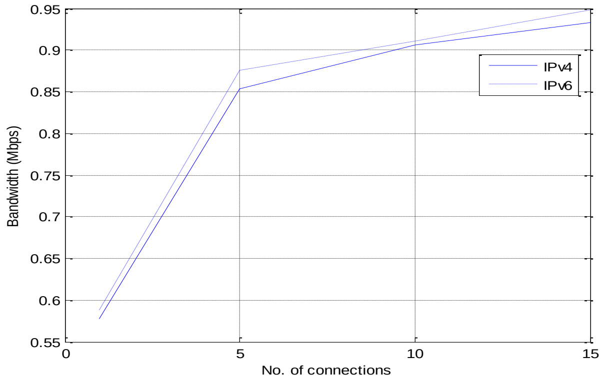

Figure 3. Bandwidth versus number of connections

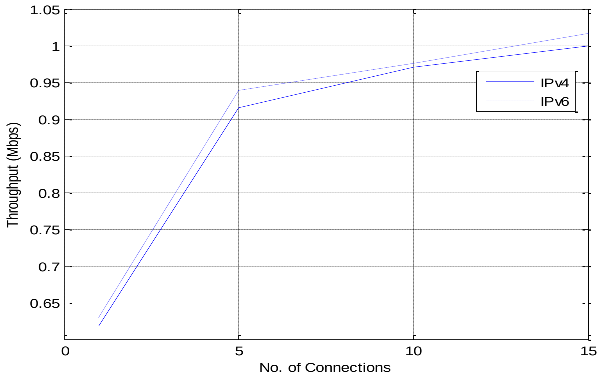

Figure 4. Throughput versus number of connections

3. SIMULATION SCENARIO

A simulation scenario as depicted in Figure 1 is created both for IPv4 and IPv6 based network. IPv4 scenario is created using ns-2.33 [13] and corresponding IPv6 based network is designed using MobiWan patch pack with ns-2.26. Despite of having higher versions of ns-2, the reason behind using ns-2.26 is to make use of MobiWan [14] patch pack. The MobiWan patch pack is primarily designed to simulate Hierarchical Mobile IPv6 but the structure of IPv6 is well implemented as well. Few modifications are done into the implementation of IPv6 in MobiWan to implement the scenario stated in this paper and tcl scripts are written to make use of the patch pack. Nodes are numbered using hierarchical addressing approach for both IPv4 and IPv6 scenarios. The node 0 is configured as source from where packets flow and passes through the route following nodes 1, 2, 6 and 12 to finally reach the destination node 18. The simulation is performed under different traffic conditions with a variation of 1, 5, 10 and 15 sessions using TCP as transport layer protocol. The same traffic conditions are used for both IPv4 and IPv6 network environments. Various performance parameters observed in the simulation are plotted and are compared in the next section.

4. DISCUSSION OF SIMULATION RESULTS

The performance of IPv4 and IPv6 network is analyzed in depth by computing certain parameters like packet overhead, bandwidth consumed, throughput and packet delivery ratio (PDR). The findings of these observations are plotted and their explanations are presented in the next few subsections. The intention of these graphs presented here is to have a comparative study of two versions of the IP and to understand the benefits and drawbacks of them for the deployment as a network layer protocol for next generation network.

4.1 Packet Transmission Overhead.

Figure 2 shows the overhead during packet transmission for both IPv4 and IPv6 for different number of FTP connections over TCP between source node 0 and destination node 18. The overhead is calculated as the extra bytes transmitted to successfully deliver all the data packets to the destination.

The packet transmission is always higher in IPv6 compared to IPv4. This is due to the size of the IPv6 header (40 bytes) is more than that of the IPv4 header (20 bytes). This is obvious due to the fact that if packet transmission is more, then overhead will also be high. The graph in Figure 2 shows that overhead in IPv4 is significantly higher than in IPv6.

4.2 Bandwidth Consumption

Figure 3 is the observation of bandwidth consumed by various FTP connections over TCP for IPv4 and IPv6 networks. We have computed the bandwidth considering the number of packets received at destination and the size of each packet for 150 seconds of simulation. The graph in Figure 3 shows that bandwidth consumed by IPv6 is higher than that of IPv4. This may also be expected because the size of the IPv6 header is more than that of the IPv4 header, and hence the required bandwidth.

4.3 Throughput

The graph in Figure 4 is the performance comparison of IPv4 and IPv6 networks from the achievable throughput in FTPs over TCP. The throughput is computed considering the number of packets received at destination during entire simulation time. It is found that IPv6 has higher throughput than IPv4. This a result of bigger size of data transmitted in IPv6 due to the larger header size.

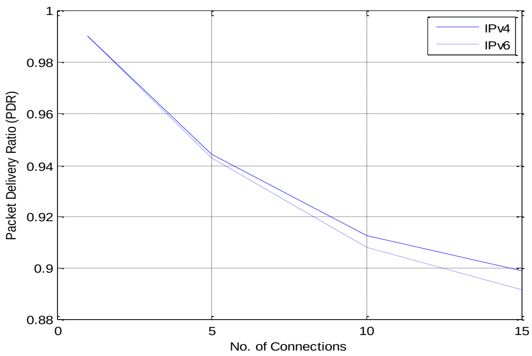

Figure 5. Packet Delivery Ratio versus number of connections

4.4 Packet Delivery Ratio

In the graph of Figure 5, packet delivery ratio (PDR) for various FTPs using TCP connections are shown. It is observed that when number of connections increases, the PDR decreases significantly. Again when the PDR for IPv4 and IPv6 networks is compared, it is found that IPv4 has higher PDR than IPv6 for more number of connections. For one connection there is no gap in PDR for both protocols. As the number of connections increase, the difference in PDR also increases between IPv4 and IPv6 networks. This is due to the fact that as the traffic flow increases, more packets are dropped. The limit when the packet dropping starts in IPv4 is less than that in IPv6. Therefore in IPv6, as the limit of packet drop reaches earlier, the PDR for same number of connections will be less in IPv4 as compared to IPv6. We have computed the PDR considering the number of packets received at destination by the number of packets sent at source.

TABLE I

Protocol	Address Space	Multicasting Supported	Network Layer Security	Triangular Routing in Mobile
IPv4	32	Optional	Optional	Yes
IPv6	128	Integrated	Integrated	No

TABLE II

Protocol	MTU Size Bytes	Header Size (Bytes)	Fragmentation Done at Router	Header Checksum Computed
IPv4	Atleast 68	20	Yes	Yes
IPv6	Atleast 1280	40	No	No

TABLE III

Protocol	Options Extensibility	Jumbograms
IPv4	Fixed 40 Bytes	64 KB of payload
IPv6	Size of the entire packet	As large as 4 GB

5. BENEFITS OF USING IPV6: A DISCUSSION

From the observation made in section 4, it is found that IPv4 is better in many situations. Despite this, now-a-days IPv6 is considered as the protocol for next generation IP based network. To have an understanding of the benefits of using IPv6 some of the parameters are compared in the form of tables in this section. These tables will help to focus the advantages of using IPv6 as network layer protocol.

From the Table I, it is found that the address space available in IPv6 is much higher than that of IPv4. So the problem of shortage of address space in IPv4 is eliminated for next few decades. Support of multicast as an in-built feature of IPv6 seems to be of a great help in most of the other IP related protocol designs. Multicasting puts extra burden on protocol designers when it is done using IPv4. Integrated security protocols in IPv6 help IPv6 users to develop new IP based protocol without the need of adding external security features. Triangular routing in mobile IPv4 introduces extra end-to-end packet delivery delay, which is highly inefficient. Triangular routing is eliminated in mobile IPv6 and hence decreases the end-to-end packet delivery delay up to a great extent.

A higher MTU, as mentioned in Table II, brings greater efficiency because each packet carries more user data while protocol overheads, such as headers or underlying per-packet delays remain fixed, and higher efficiency means a slight improvement in bulk protocol throughput. However, large packets can occupy a slow link for some time, causing greater delays to following packets and increasing lag (the term lag is used to refer to delays noticeable to the user) and minimum latency. Because of the larger MTU size and reasons given above, IPv6 offers higher throughput compared to IPv4. Again, although the size of the IPv6 header is more, but it is only due to the size of the source and destination address fields. Excluding source and destination addresses, IPv4 includes (20-8) = 12 bytes of information whereas, IPv6 includes (40-32) = 8 bytes of information. And it is obvious that larger information processing will consume more processing time. Hence, IPv6 suffers less header processing time compared to IPv4. Intermediate routers do not do fragmentation in IPv6 which reduces processing delay in these routers. Also header checksum, although included in IPv4, it is not necessarily useful for error detection and correction. So, absence of header checksum computation reduces some more processing time in IPv6.

Moreover, all the information carried inside a header is not always processed or needs to be processed. In fact, most of them are ignored by almost all intermediate routers as well as destination. So an optional header is introduced in IP headers. IPv6 has higher space allocated for optional header. If some additional information is required to be added to the header, IPv6 is more flexible compared to IPv4, since IPv6 can include more bytes as optional header. The use of jumbograms may improve performance over high-MTU networks. Network with any size of MTU up to 4GB can be utilized by IPv6. In such case, IPv6 will give better performance and also larger packet size will result in smaller overhead. From all the parameters shown in Table I, II and III, it seems that IPv6 is a favorable protocol for next generation IP based network.

6. CONCLUSION

At the end, by observing all the results and discussions, it can be concluded that IPv4 network gives better performance with respect to signaling overhead, bandwidth, throughput and packet delivery ratio over IPv6 network. Although in some performance areas, IPv4 gives better response, but still the significant reasons for adopting IPv6 is the need for more address space, security, and Quality of Service (QoS) features. Since IPv4 network is also essential where these special features of IPv6 are less important, therefore the need for the co-existence of both protocols is necessary. To make existence of both the versions of the protocol together, some mechanisms of interoperability is required. There are few transition mechanisms that exist for this purpose. These mechanisms may be used for the proper functioning of both the versions together and benefit the best from them. The research on these transition mechanisms are going on and is a hot area of research these days.

7. REFERENCES

[1] RFC 791 on "Internet Protocol Darpa Internet Program Protocol Specification," September 1981.

[2] D. Senie, "RFC 3235 on 'Network Address Translator (NAT)-Friendly Application Design Guidelines," January 29th, 2002.

[3] Introduction to IPv6 http://forums.techarena.in/guides-tutorials/ 1064417.htm

[4] S. Deering , R. Hinden, "RFC2460 - Internet Protocol, Version 6 (IPv6)," Specification December 1998

[5] http://en.wikipedia.org/wiki/IPv6.

[6] Yi Wang, Shaozhi Ye, Xing Li, "Understanding Current IPv6 Performance: A Measurement Study" Proceedings of the 10th IEEE Symposium on Computers and Communications (ISCC 2005)

[7] Mohiuddin Ahmed, Mohd. Adam Suhaimi, Quazi Shoyweeb, Md. Faisal, Shariq Haseeb, "Evaluating QoS performance of Streaming Video on both IPv4 and IPv6 Protocols", Proceedings of the 2007 Spring Simulation Multiconference vol. 1, pp. 109-116.

[8] L. Colitti, G. D. Battista, M. Patrignani, "IPv6-in-IPv4 tunnel discovery: methods and experimental results," IEEE Transactions on Network and Service Management, vol. 1, no.1. April. 2004.

[9] K. Cho, M. Luckie, and B. Huffaker, "Identifying IPv6 Network Problems in the Dual-Stack World," SIGCOMM'04 Network Troubleshooting Workshop, Portland, USA, 2004.

[10] T. Sanguankotchakorn et al., "Performance Evaluation of IPv6/IPv4 Deployment over Dedicated Data Links," Fifth International Conference on Information, Communications and Signal Processing, 2005.

[11] Myung-Ki Shin et al., "An Empirical Analysis of IPv6 Transition Mechanisms," Feb. 20-22, 2006, ICACT 2006.

[12] Xiaoming Zhou, Rob E. Kooij, Henk Uijterwaal, Piet Van Mieghem, "Estimation of Perceived Quality of Service for Applications on IPv6 Networks," PM²HW²N'06, October 6, 2006, Torremolinos, Malaga, Spain ACM 2006.

[13] The Network Simulator - ns, downloaded from http://www.isi.edu / nsnam/ns/

[14] "Mobiwan: ns-2 extensions to study mobility in Wide-Area IPv6 Networks", http://www.inrialpes.fr/planete/mobiwan