EVALUATING INTERNET PROTOCOL VERSION 6 (IPv6) AGAINST VERSION 4 (IPv4)

Folorunso, S. O.
Department of Mathematical Sciences
Olabisi Onabanjo University
Ago – Iwoye, Ogun State.

ABSTRACT
This paper evaluates the performance of IPv6 against IPv4. IPv4 has address space shortages. The use of Classless Inter-Domain Routing (CIDR) and Network Address Translation (NAT) helped to address these shortages. However, Features built into IPv6 such as autoconfiguration, IPSec, Mobility, Multiple addresses for hosts and networks, Multicast communication make it well worth the cost, time and effort required to migrate to it. Performance metrics used in order to analyze the protocols are network delay, network drop, and throughput. Results showed that IPv6 is not better in terms of packet management than IPv4. The results also showed that IPv6 has higher delay, and packet drop than IPv4; though the margin between the values are however small. It was also found that IPv6 has a higher throughput. It is hereby concluded, that even though IPv4 is performing better, it will not solve the address limitation problem. This has made it inevitable to recommend IPv6 as a replacement for the IPv4.

Keywords: Latency, Throughput, PacketDrop, NAT, Mobility, Autoconfiguration.

1. INTRODUCTION

WLAN has being in existence for quite sometime, demand for services on it in recent times has shifted so much attention to it as cheaper and more comfortable means of accessing Internet services. The opportunities WLAN gives its users are boundless as it gives the power of mobility, simplicity, and yet enhanced productivity to its users. One of the services that can be deployed on WLAN is the Internet. This means with apt WLAN setup, users can access Internet services on the fly. Just like other LAN, WLAN uses the famous Open System Interconnection (OSI) reference model. It is the de facto standard for communicating between two different nodes (hosts) on a network. The OSI reference model has seven layers. However, the third layer (network layer) also known as Internet layer is the layer responsible for providing the protocol that makes it possible for one system to communicate with another system, linking systems together rather than just network interfaces; this is the layer concerned with delivery of data between two different nodes that may be on two different networks (Loshin, 2001).

This makes the network layer a very important layer on the WLAN network. Internet layer uses the Internet Protocol (IP) to carry out its operation. Presently, the Internet and numerous numbers of smaller, private networks use as their basic network infrastructure, the Internet Protocol version 4 (IPv4). IPv4 has been an incredibly successful protocol, able to scale from connecting hundreds or thousands of hosts on tens or hundreds of separate networks all the way up to linking the tens of millions of hosts estimated to be part of the global Internet (Loshin, 2001). However, IPv4's landmarks did not stop it from having its limitation amongst which is Address Space Limitation, Performance, Security, and Auto-configuration. IPv4 inadequacies have been observed and were published in the RFC 1287 (Request for Comment). Official recognition of these shortcomings can be dated as far back as 1991.

This led to the birth of IPv6 which attempts to solve IPv4's inadequacy. IPv6 is a relatively new protocol, though the specification had been submitted to and accepted by the Internet Engineering Task Force (IETF) as early as the end of 1995 (Loshin, 2001). Migration to IPv6 will relatively be gradual and will see co-existence and interaction with IPv4. Just before this migration exercise begins, IPv6 performance with regards to Internet traffics are of major concern and it needs to be investigated. It is not uncommon for Internet users to access multiple services on a network simultaneously. In fact, Internet users frequently browse web pages, simultaneously make internet calls, and at same time download files from the internet on the same network. These are common scenarios happening on a daily basis while going on the Internet.

How far IPv6 is going to fair with these heavy traffics will make a case for its adoption as the next Internet de facto protocol.

1.1 The Challenge

The migration to IPv6 is due to limitations and shortcomings of the IPv4 in terms of security, routing, auto configuration and address limitation. Now that Ipv6 is operation, there is a need to evaluate its performance on Internet traffics. This shall be done using performance metric tools such as Awk, Perl and Shell with appropriate simulated results.

2. PRELIMINARY STUDIES

2.1 Internet Protocol (IP)

Models that separate how data is treated as it passes from one system to another are often visualized as stacks of protocols to be used at different layers. The protocols implementation are also referred to as protocol stacks, and they represent the levels at which data can be manipulated and how that data is passed from one level up or down to next level. The standardized model adopted is the Open System Interconnection (OSI) model of networking. This basic reference model was devised originally to reflect all-inclusive model for internetworking. It has seven layers out of which Internet Protocol layer (Network Layer) is one of it. Previously, the widely used version of the IP is IPv4

(Internet Protocol version 4). But due to its limitations, there were moves to replace the old IP version. A typical IPv4 datagram is composed of a header and chunks of data (payload). The data in IP datagram, including data in the headers, is organized into 32-bit (four byte) words. Figure 2-1 shows how the IPv4 header fields are arranged.

2.1.1 Internet Protocol version 6 (IPv6)

In an attempt to solve the nagging ipv4 problems, IPv6 was introduced. Though, both have a lot in common but with few features changed in the datagram's header. In IPv4, all headers terminated on a 32bit boundary; in other words, the basic unit of measurement was four bytes as illustrated in Fig 2.3. In IPv6, header boundaries are placed at 64 bit boundaries, with IPv6 headers being a total of 40bytes long (Loshin, 1999). Route optimization is built into the ipv6 protocol to avoid triangle routing ,whenever a mobile host receives packets that was tunneled by the home agent, it sends binding update to the original sender. When working with mobile IP in ipv6, the care-of-address is used as the source address for the IP packets instead of the home address, the home address is then specified in the home address destination option. The use of care-of-address as the source address facilitates wireless multicasting since the Mobile host (as a sender) does not have to tunnel packets to home agents. The correspondent host can then communicate directly with mobile host. The IPv6 specifies the following fields for its header: A typical IPv6 header diagram is shown in fig. 2-2.

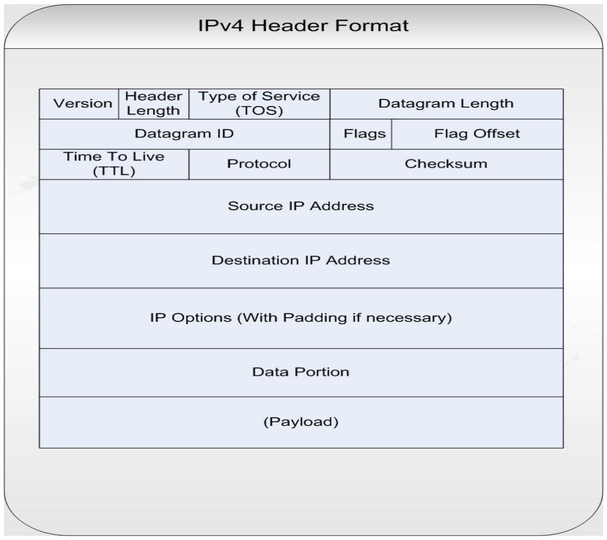


Fig 2-1 An IPv4 Header Format

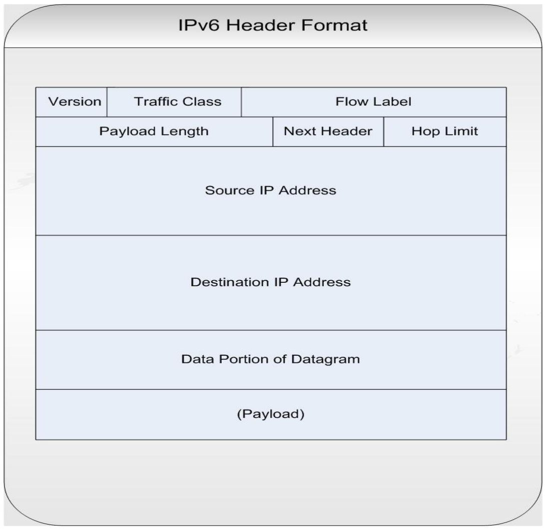


Fig 2-2 An IPv6 Header Format

- **Version**: This is a four-bit value for specifying the IP's version, and for IPv6 it must be equal to six.
- **Class**: An eight-bit value specifies that some form of "differentiated services" be provided for the packet. The latest IPv6 Internet draft referred to this class as Traffic class. The use of this field is defined separately from IPv6 and has not yet been specified in any RFC (Request for Comment) document. The default value is all zeroes.
- **Flow Label**: This is a 20-bit value used to identify packets that belong to the same flow. A node can be the source for more than one simultaneous flow. The flow label and the address of the source node uniquely identify flows. This field was originally set to 24bits (RFC 1883), but when the class field was increased in size to eight bits, the flow label was decreased to compensate.
- **Payload Length:** This is a 16bit field that contains an integer value equal to the length of the packets payload in bytes; that is, the number contained in the packets after the end of the IPv6 header. This means that IPv6 extensions are included as part of the payload for the purposes of calculating this field.
- **Next Header**: This field indicates what protocol is in use in the header immediately following the IPv6 packet. Similar to IPv4protocol field, the next header field may refer to a higher-layer protocol like TCP or UDP, but it may also indicate the existence of an IPv6 extension header
- **Hop Limit**: Every time a node forwards a packet, it decrement this eight bit field by one. If the hop limit reaches zero, the packet is discarded. Unlike IPv4, where the time-to-live field fulfills a similar purpose, sentiment is on packet lifetime for IPv6. This means that the function of timing-out old data should be accomplished in upper-layer protocols.
- **Source Address**: This is the 128-bit address of the node originating the IPv6 packet
- **Destination Address**: This is the 128-bit address of the intended recipient of the IPv6 packet. This address may be a unicast, multicast, or anycast address. If a routing extension is being used (which specifies a particular route that a packet must traverse), the destination address may be one of these intermediate node instead of the ultimate destination node.

Fig. 2.3 MAJOR DIFFERENCES BETWEEN IPv6 AND IPv4 (ARIN, 2011)

	Internet Protocol Version 4 (IPv4)	**Internet Protocol Version 6(IPv6)**
Deployed	1981	1999
Address Size	32 – bit number	128 – bit number
Address Format	Dotted Decimal Notation 192.149.252.76	Hexadecimal Notation: 3FFE:F200:0234:AB00:0123:4567:8901:ABCD
Prefix Notation	192.149.0.0 / 24	3FFE:F200:0234:: / 48
Number of Addresses	2^{32} = ~ 4,294,967,296	2^{128} = ~340,282,366,920,938,463,463,374,607,431,768,211,456

2.2 Internet Traffics

Internet traffics are regarded as a chunk of collective data passing over the Internet. Traffics on the Internet could be as a result of any of the Internet services offered. The collective passage of all protocol's data over the Internet is regarded as Internet traffic. However, different traffic exists for different application layer protocols. Traffics generated from the HyperText Transfer Protocol (HTTP) protocol are popularly regarded as HTTP or web traffics while those from the File Transfer Protocol (FTP) protocol are called FTP Protocol. For the purpose of this study, the following traffics will be examined: Voice Over Internet Protocol (VoIP), Simple Mail Transfer Protocol (SMTP), and HTTP traffics.

2.2.1 Voice over Internet protocol (VoIP)

Voice over IP (VoIP) can be described as the ability to make telephone calls and send faxes over IP-based data networks with a suitable Quality of Service (QoS) which utilizes bandwidth more efficiently by encoding voice data into small packets and transmitting the packets in a very high speed data network. The voice information is sent in digital form using discrete packets rather than via dedicated connections as in the circuit-switched Public Switch Telephone Network (PSTN) (Tyson and Valdes, 2005). Making a VoIP call requires converting a voice signal into a series of data packets which is known as voice packetization. This feature is achieved with the use of a codec. (coder-decoder), which converts an audio signal into a compressed digital form for transmission and then back into an uncompressed audio signal for replay.

2.2.2 Mail Traffic

Simple Message Transfer Protocol is a set of standards used for messaging applications. It is also the de facto standard for all mail transferred over the Internet. Just like other Application layer protocols, SMTP operates is another application layer protocol in the OSI model stack. SMTP runs only over TCP/IP networks and uses TCP/IP features to discover routes by which to deliver mail. Two hosts communicate over a TCP/IP using port 25. However, for both systems to communicate, they both must be running an SMTP program. Procedures and standard for SMTP mail are defined in RFC documents issued by the Internet Architecture Board (IAB).

2.2.3 Web Traffic

HTTP, Hyper Text Transfer Protocol is the command and control protocol used to manage communications between a Web browser and a Web server. HTTP is the mechanism that opens the related document when a link is selected on a web page, no matter where that document is located.

2.2.4 File Transfer Protocol (FTP) Traffic

FTP is also an application layer protocol which specializes in transferring packetize data on a network. It uses the TCP transport protocol in achieving this hence it requires an acknowledgement packet (Ack) to be sent to confirm a safe delivery of a packet. It also checks packet integrity on arrival. Any lost data will be resent to the destination host. It is usually dedicated for file download on the Internet.

2.3 Previous Works

2.3.1 Capacity Estimation of VoIP on Wireless Networks

A case study of VoIP over WLAN simulation is carried out at the Department of Electrical and Computer Engineering, University of Texas, Austin (Patel et al, 2003). The experiment was carried out on capacity estimation of VoIP Channels on Wireless Networks. In the experiment the QoS (Quality of Service) of VoIP was examined as well as the number VoIP calls a WLAN can support (without degrading the QoS) were concurrently investigated.

In the experiment acceptable QoS are defined based on International Telecommunication Union (ITU) recommendation G. 108 called E Model which defines a rating value R as shown in table 2.1. Yardstick used in measuring QoS are throughput, packet loss, packet delays, and jitter. In the experiment performed at the University of Texas, Austin, the voice quality was monitored while increasing the number of endpoints (nodes). Also determined was the maximum number of voice sessions possible with an acceptable QoS.

3. METHODOLOGY

In our study, a model is designed and NS2 simulation software is used to simulate the model. The proposed model to be used is broken down into disparate component models. The component models are Topology, Mobility, Traffic, and Network Load models. Firstly, a topology model is designed and used to define the proposed model structure (Architecture). The architecture consists of an access point with mobile nodes and three fixed server systems. Secondly, a mobility model is defined to emulate movements of wireless nodes in the topology.

The NS-2 simulation software is used to simulate IPv6 packets so that generated traffics can be encapsulated in the IPv6 format. Also, in the proposed model, traffics are designed by modeling real life traffics to achieve a reasonable and feasible result. Patterns of generating traffics too require special effort; therefore a realistic approach must be used to send traffics between nodes by emulating a real life network load. This is achieved by modeling a network load. Detailed explanation of each model is given below.

3.1 Topology

The topology modeled in this study is the infrastructure network. This network includes a base station connected to fix wired servers that render different network (Web, Email and VoIP) services to some wireless clients on the network. The Base Station (BS) acts as a transceiver station that passes data to and from the servers. Figure 3-1 shows a typical infrastructure network topology to be modeled for this study. The mobile hosts are labeled N_n where n represent the number of the host on the network i.e. (1, 2, 3 ………8).

3.2 Mobility

The simulation software to be used (Network Simulator 2 – NS2) provides a utility tool for generating randomized node positions at different point in time based on certain parameters supplied to it. The random points are based on the popular RNG (Random Number Generator) algorithm. With the NS2 tool, different positions will be generated for different mobile hosts within a specified geographical location. The NS2 tool used is called SetDest, a command line tool that takes argument on the Linux shell. SetDest output, by default, goes to the terminal. However, it can be redirected to a file for further usage. The output file from SetDest will serve as the model to forecast mobile host movement in network model.

3.3 Traffic Modeling

Three traffics (Web, VoIP, and Email) are of interests in our study. Models for each of the traffics to emulate its real life equivalent will be used. Modeling web traffics entail generating packets from a client to a web server which then in turn sends the apt packet back to the client. Also, the real life behavior of VoIP and email traffics will be emulated as close as possible. During performance evaluation, the total time it takes for packets to make a round trip will play an important role for the performance metrics.

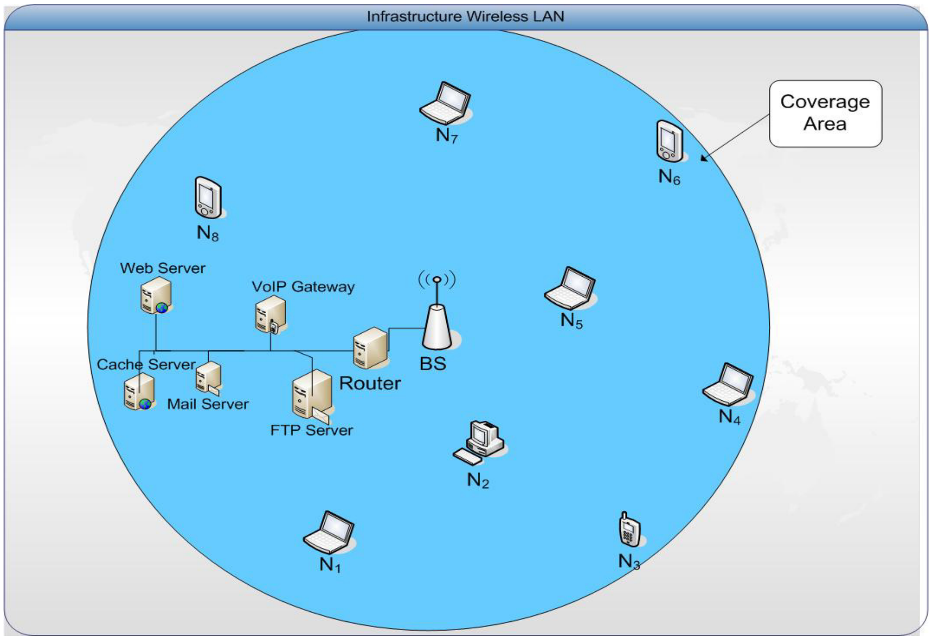


Figure 3.1 Topology Model

3.4 Network Load Modeling

For the purpose of our study, a model was designed to create different traffic on different nodes on the network. The aggregation of these traffics will form the load on the network. Realistic scenarios will be emulated where users can surf websites and simultaneously make Internet call. Also, cases such sending email and making Internet calls or surfing web sites will be simulated and evaluated for performance based on some chosen metrics.

3.5 Components of The Proposed Model

In studying the performance analysis of IPv6 in a wireless LAN with respect to web, VoIP, FTP and email traffics; the following components constitutes our model.

- ***Nodes:* -** Nodes are system units on the network. It can either be a server or a client.
- ***Channel (Link):* -**paths that connect nodes in a network together.
- ***Packet:* -** This is the fixed size smallest unit of communication containing information.

4. MODEL SIMULATION

Our simulation will be carried out on network simulators. The following simulators were used in our study, these simulators exist both on Linux and Windows Operating Systems.

OpNet

This is a leading commercial software for network simulation; it has support for windows and Linux, with a graphical interface

SSFNET

A scalable simulation framework with parallel discrete event simulators intended for modeling the internet at large scale.

GloMoSim

It is a simulator for wireless network, scalable to support thousands of nodes. The simulator uses layered approach to build different simulation layers.

Realistic and Large (REAL)

The real network simulator was developed by Keshev in 1988 as part of a network simulation test-bed (NEST) project.

Network Simulator 2

The first version of the network simulator was developed in 1995 and it was a variant of the REAL simulator which was written by Keshev. It is written in C++ and OTcl.

It allows for the analysis of network data by generating some trace files. There are two primary but distinct types of monitoring capabilities on NS-2. The first, called *traces*, record each individual packet as it arrives, departs, or is dropped at a link or queue. The other types of objects, called *monitors*, record counts of various interesting quantities such as packet and byte arrivals, departures, etc. Monitors can monitor counts associated with all packets, or on a per-flow basis using a *flow monitor.* There is also another method of analyzing network data, this time the physical movement of packets are visualized and monitored. The tool is popularly called Network Animator (NAM). Output for this tool is stored with a ".nam" extension.

4.1 Results and Discussions

This section shows results from the simulation. Results are generated for all traffic with 5, 10, 15, 20, 25, and 30 nodes. Also, results for IPv4 and IPv6 were generated separately. Details of all results are shown below. Each result table displays a specific type or combination of traffic with varying nodes with respect to a performance metrics.

All traffic Delay

Number of Nodes	**Delay (Secs)IPv4**	**Delay (Secs)IPv6**
5	1.07925	1.03845
10	2.08787	2.05668
15	3.05294	3.11763
20	4.12469	4.18367
25	5.14565	5.246
30	6.17638	6.20984

FTP Traffic Delay

Number of Nodes	**Delay(Secs)IPv4**	**Delay (Secs)IPv6**
5	0.0132829	0.0112383
10	0.0372721	0.0299649
15	0.0376026	0.0344459
20	0.0459902	0.0428603
25	0.0551253	0.0445773
30	0.0584549	0.0559291

HTTP Traffic Delay

Number of Nodes	**Delay (Secs)IPv4**	**Delay (Secs) IPv6**
5	0.00173346	0.00174796
10	0.00171106	0.00172555
15	0.00174731	0.001762
20	0.00176373	0.00177957
25	0.00177675	0.00180169
30	0.00195135	0.00195373

SMTP Traffic Delay

Number of Nodes	**Delay (Secs)IPv4**	**Delay (Secs) IPv6**
5	0.00618718	0.0264181
10	0.0173303	0.0013641
15	0.0618424	0.148565
20	0.137807	0.581423
25	0.250029	1.18519
30	0.672681	1.69538

VoIP Traffic Delay

Number of Nodes	Delay (Secs) IPv4	Delay (Secs) IPv6
5	0.016022	0.0168691
10	1.47313	1.43324
15	2.50927	2.60383
20	3.41582	3.56094
25	4.29702	4.4741
30	5.13595	5.35291

All Traffic Drop

Number of Nodes	Packet Drop IPv4	Packet Drop IPv6
5	0.319299	0.4266
10	0.599603	0.655527
15	0.710762	0.775803
20	0.795371	0.838011
25	0.830617	0.878176
30	0.859864	0.888793

FTP Traffic Drop

Number of Nodes	Packet Drop IPv4	Packet Drop IPv6
5	0.000261114	0.000340356
10	0.000483463	0.0003529
15	0.000767438	0.000833645
20	0.000930679	0.000791743
25	0.00054536	0.000732993
30	0.000920411	0.00104732

HTTP Traffic Drop

Number of Nodes	Packet Drop IPv4	Packet Drop IPv6
5	0.0625	0.0625
10	0.0306122	0.0306122
15	0.0410959	0.0410959
20	0.00502513	0.00502513
25	0.00803213	0.00803213
30	0.020202	0.020202

SMTP Traffic Drop

Number of Nodes	Packet Drop IPv4	Packet Drop IPv6
5	0.0678999	0.104862
10	0.0350606	0.151092
15	0.0548861	0.202498
20	0.136273	0.334839
25	0.118551	0.468189
30	0.212303	0.522556

VoIP Traffic Drop

Number of Nodes	Packet Drop IPv4	Packet Drop IPv6
5	0.0778527	0.0781468
10	0.206219	0.242046
15	0.469463	0.494055
20	0.601129	0.620046
25	0.68115	0.69669
30	0.734419	0.747715

All Traffic Throughputs

Number of Nodes	Throughput (Mbit/s) IPv4	Throughput (Mbit/s) IPv6
5	0.591331	0.576549
10	0.54756	0.542056
15	0.524382	0.53381
20	0.524615	0.529734
25	0.515092	0.527013
30	0.50572	0.513878

FTP Traffic Throughput

Number of Nodes	Throughput (Mbit/s) IPv4	Throughput (Mbit/s) IPv6
5	2.49313	2.55001
10	2.88503	2.92562
15	2.94957	2.92596
20	2.99839	2.94779
25	3.00699	3.04971
30	3.07465	3.07028

HTTP Traffic Throughputs

Number of Nodes	Throughput (Mbit/s) IPv4	Throughput (Mbit/s) IPv6
5	7.34694e-05	0.000146939
10	0.000155102	0.000310204
15	0.000228571	0.000457143
20	0.000323265	0.000646531
25	0.000403265	0.000806531
30	0.000475102	0.000950204

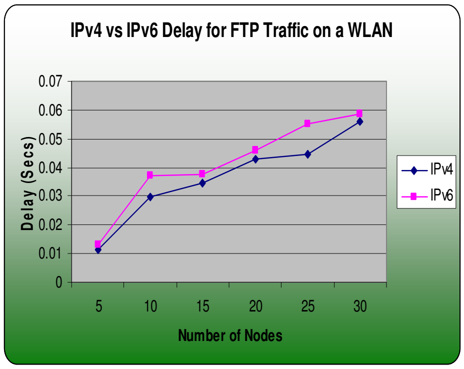
SMTP Traffic Throughput

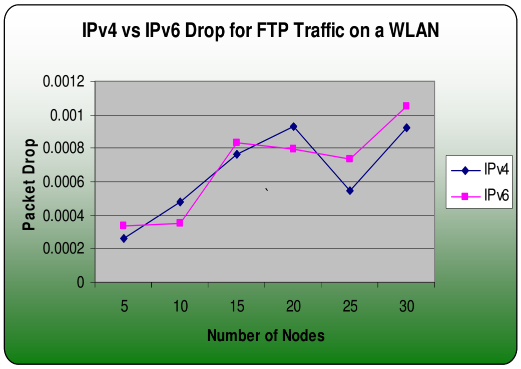
Number of Nodes	Throughput (Mbit/s) IPv4	Throughput (Mbit/s) IPv6
5	0.64672	0.68528
10	1.33912	1.59848
15	1.88136	2.284
20	2.10464	2.97136
25	2.12768	3.26792
30	2.09536	3.4536

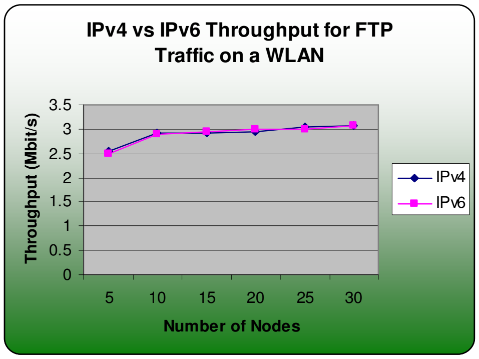
VoIP Traffic Throughput

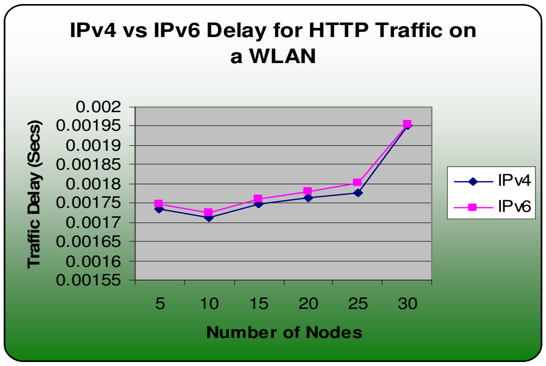
Number of Nodes	Throughput (Mbit/s) IPv4	Throughput (Mbit/s) IPv6
5	0.266946	0.269451
10	0.438567	0.46308
15	0.434689	0.459429
20	0.431184	0.45624
25	0.426391	0.451406
30	0.421521	0.44688

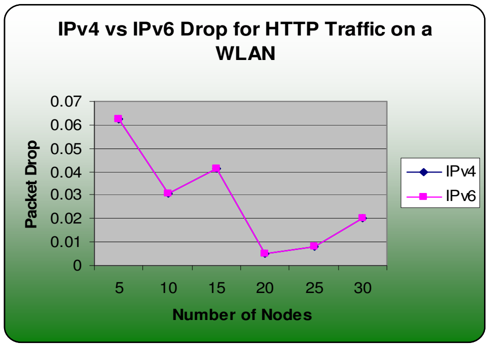
The following figures depicts IPv4 vs. IPv6 Throughput for VoIP, HTTP, FTP, and SMTP Traffic on WLAN

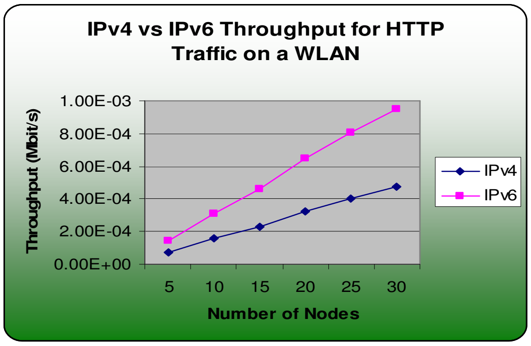


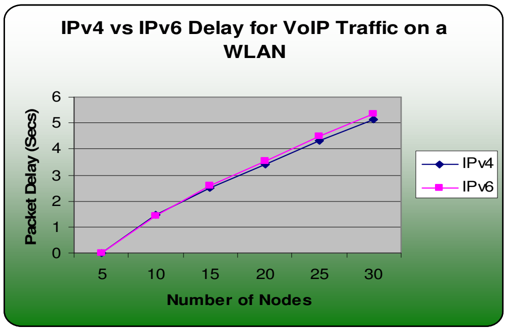


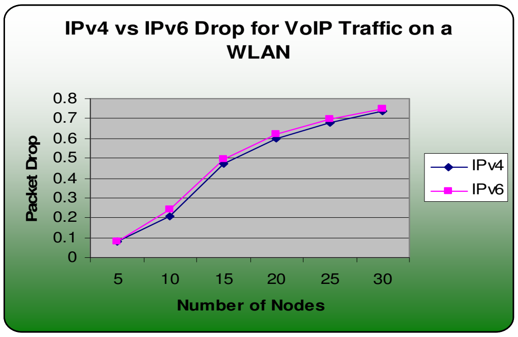












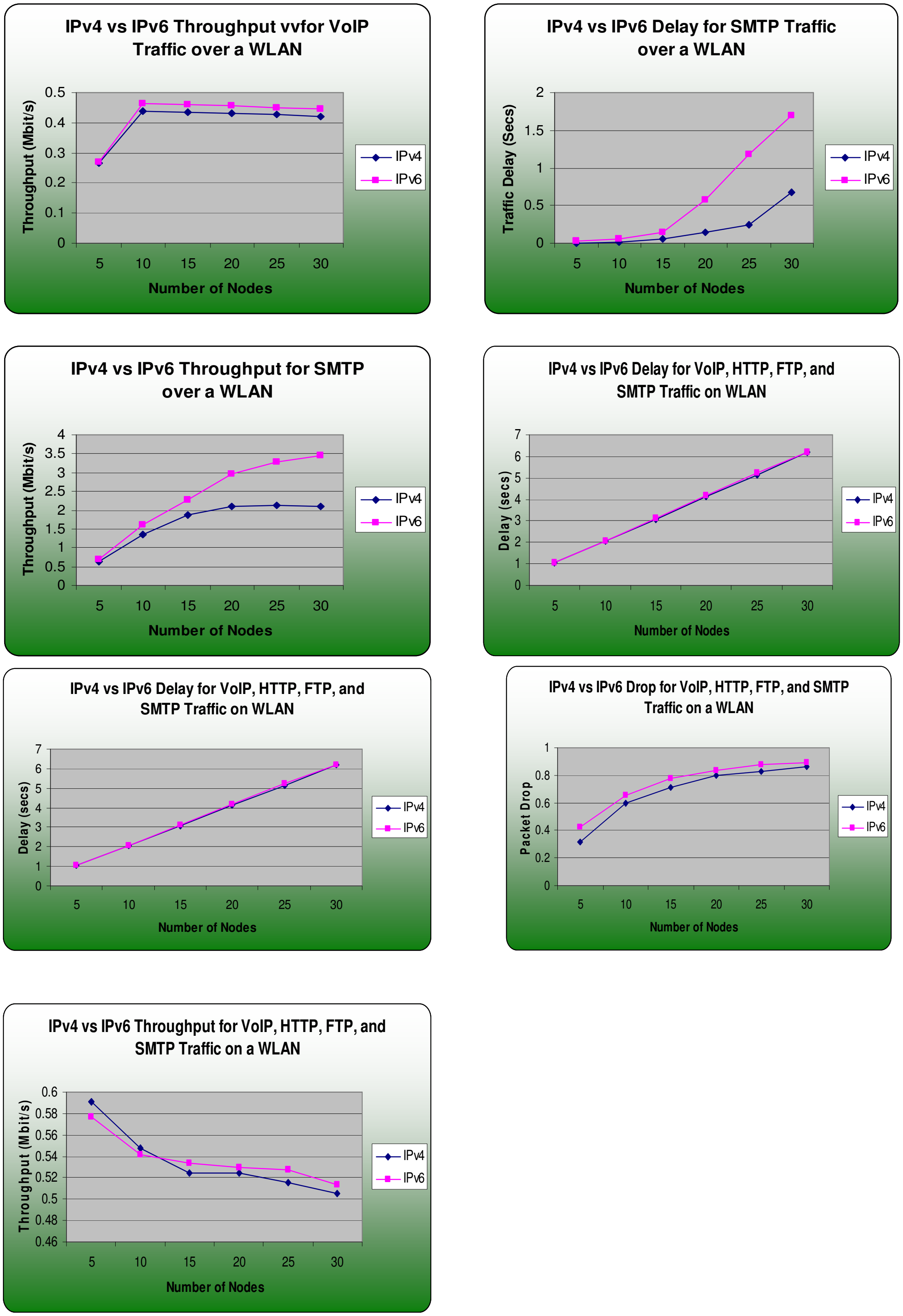


Figure 4-1: IPv4 vs. IPv6 Throughput for VoIP, HTTP, FTP, and SMTP Traffic on WLAN

5. CONCLUSION

In conclusion, IPv6 in terms of speed, packet management (packet loss), and throughput is not better than IPv4. IPv4 still performs better due to smaller header size. However, the differences between the performance reductions are not unacceptable. With better technology both on hardware and software platform, IPv6 can be better. IPv6 promises a brighter future with its features. Fortunately, IPv4 can be integrated with IPv6, which gives room for smooth changeover. Latency in IPv4 is lower than latency in IPv6, packet drop in IPv4 is lower than in IPv6. However, on the average, throughput for IPv6 is higher than that of IPv4. The technical functioning of the Internet remains the same with both versions and it is likely that both versions will continue to operate simultaneously on networks well into the future. To date, most networks that use IPv6 support both IPv4 and IPv6 addresses in their networks. Cisco (Townsley, 2011) and Google (Colitti, 2011) reported no significant issues during the test. Facebook (Lee, 2011)) called the results encouraging, and decided to leave their developer site IPv6-enabled as a result. (MacVittie, 2011). But the consensus was that more work needed to be done before IPv6 could consistently be applied. (MacVittie, 2011).

5.1 Future work Perspective

This simulation of IPv6 only used the header size feature and each traffic conducted differently. Further simulation should try and incorporation other feature such as the removal of broadcasting from IPv6, the evaluation of mobility over IPv6 (MIPv6) should be investigated against Mobility over IPv4 (MIPv4). And also evaluation of IPv6 (DHCPv6) against IPv4 (DHCPv4).

REFERENCES

1. American Registry for Internet Numbers (ARIN)(2011), http:// www.nro.net/wp-content/uploads/2011/02/IPv4-IPv6.pdf
2. Colitti, Lorenzo (2011). "World IPv6 Day begins 24 hours from now. Websites, start your engines.". *Official Google Blog*. http://googleblog.blogspot.com/2011/06/world-ipv6-day-begins-24-hours-from-now.html.
3. E. Altman, T. Jimenez (2003), 'NS Simulator for beginners' Unpublished Thesis, University de Los Andes, Merida, Venezuela and ESSI Sophia-Antipolis, France, pg 111.
4. K. Fall, Varadhan K. (2000), 'The NS manual (formerly ns Notes and Documentation)', UC Berkeley, LBL, USC/ISI, and Xerox PARC, pp 17, 18.
5. HTTP://wireless.utk.edu, 2006, 'Overview of Wireless Technologies', Internet Document, accessed on 18th April, 2007 (http://wireless.utk.edu/overview.html#intro)
6. J. Phillipe, 2003,'Modeling and Simulation Theory', Internet Document accessed on 10th May, 2007 (www.jean-phillipe.com/General/Model_Simulation/intro.html)
7. J. Tyson, R. Valdes, 2005, 'How VoIP Works', Internet Document, accessed on 15th May 2007 (www.howstuffworks.com/ip-telephony1.htm).
8. Lee, Donn (2011). "Exciting Results from World IPv6 Day". *Facebook Engineering's Notes*. http://www.facebook.com/note.php?note_id=10150198443513920.
9. Leong, K. (2002), 'Development of an ATM campus network Model Performance Analysis', PhD Thesis, Department of Multimedia Engineering centre, Nanyang Polytechnic, Bathesda.
10. MacVittie, Lori (2011) "IPv4 to IPv6 switch: When protocols collide" ZD Net; archived 20 June 2011 here by WebCite®
11. Mario Pei, 1977, 'The Lexicon Webster Dictionary', Vol 2, The English-Language Institute of America Inc.
12. Patel T.J., Ogale V.A, and Baek, S. (2003); 'Capacity Estimation of VoIP Channels on Wireless Network, The University of Texas, Austin.
13. Pete Loshin, 1999, 'IPv6 clearly explained', Morgan Kaufmann, San Francisco, CA pp 20, 23, 74.
14. S. Halford, K. Halford, 2002, 'OFDM Uncovered Part: The Architecture' Internet Document, accessed on 8th July 2007 (http://www.commsdesign.com/)
15. Spyros Sakellariadis, 1998, 'SMTP Mail basics', Internet Document; accessed on 15th May, 2007 (www.windowstlilibrary.com/content/212/01/1.html).
16. Townsley, Mark (2011). "World IPv6 Day: A Watershed Moment Towards a New Internet Protocol". *The Platform.* Cisco Systems. http://blogs.cisco.com/news/world-ipv6-day-a-watershed-moment-towards-a-new-internet-protocol/.