ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

Comparison between IPv4 and IPv6 QOS Based On Opnet Modeler

Mutasim Abdel Gaffar Mohamed Ali[1], Amin Babiker Abdel Nabi Mustafa[2]

1. MSc. Student, Department of Computer Engineering ,Faculty Of Engineering , Neelain, Khartoum, Sudan

2. Associate Professor, Department of Computer Engineering ,Faculty Of Engineering, Neelain, Khartoum, sudan

Manuscript Info

Manuscript History:

Received: 25 September 2014
Final Accepted: 29 October 2014
Published Online: November 2014

Key words:

(QOS), delay.opnet.IPv4, IPv6,

Corresponding Author

Mutasim AbdelGaffar Mohamed ali

Abstract

This paper present study of different (QOS) based on simulative and analytical methods in IPv4/IPv6 networks. This research aims to find out what internet protocol is better under the specific application .in doing so four different network loads in both scenarios are considered. In the context of network load, the importance of varying network load is realized while configuring and simulating the network models. For instance, a medium network load, high network load then a worst possible network load are considered to understand the impact on the delay in IPv4/IPv6 networks. Two Network models are defined which allow us to compare the Obtained results. In addition, IPv4 network model is used and extended in terms of configuring IPv6 network model as. The simulation has been carried out using Optimized Network Engineering Tool (OPNET).

Introduction

The internet protocol provides for transmitting blocks of data called datagrams from sources to destinations, where sources and destinations are hosts identified by fixed length addresses. The internet protocol also provides for fragmentation and reassembly of long datagrams, if necessary, for transmission through "small packet" networks. The internet protocol implements two basic functions: addressing and fragmentation.

-The internet modules use the addresses carried in the internet header to transmit internet datagrams toward their destinations. The selection of a path for transmission is called routing.

-The internet modules use fields in the internet header to fragment and reassemble internet datagrams when necessary for transmission through "small packet" networks.(1)

-The internet protocol uses four key mechanisms in providing its service:-

Type of Service, Time to Live, Options, and Header Checksum.

Type of service:-

The Type of Service is used to indicate the quality of the service desired. The type of service is an abstract or generalized set of Parameters which characterize the service choices provided in the networks that make up the internet. This type of service indication is to be used by gateways to select the actual transmission parameters for a particular network, the network to be used for the next hop, or the next gateway when routing an internet datagram (2).

Time to Live:-

The Time to Live is an indication of an upper bound on the lifetime of an internet datagram. It is set by the sender of the datagram and reduced at the points along the route where it is processed. If the time to live reaches zero before the internet datagram reaches its destination, the internet datagram is destroyed. The time to live can be thought of as a self-destruct time limit.

Option:-

The Options provide for control functions needed or useful in some situations but unnecessary for the most common Communications. The options include provisions for timestamps, security, and special routing.

Header checksum:-

The Header Checksum provides a verification that the information used in processing internet datagram has been transmitted correctly. The data may contain errors. If the header checksum fails, the internet datagram is discarded at once by the entity which detects the error.

Function Description:-

The function or purpose of Internet Protocol is to move datagrams through an interconnected set of networks. This is done by passing the datagrams from one internet module to another until the destination is reached. The internet modules reside in hosts and gateways in the internet system. The datagrams are routed from one internet module to another through individual networks based on the interpretation of an internet address. Thus, one important mechanism of the internet protocol is the internet address.

Addressing:-

Addresses are fixed length of four octets (32 bits) figure (1). An address begins with a network number, followed by local address (called the "rest" field). There are three formats or classes of internet addresses: in class a, the high order bit is zero, the next 7 bits are the network, and the last 24 bits are the local address; in class b, the high order two bits are one-zero, the next 14 bits are the network and the last 16 bits are the local address; in class c, the high order three bits are one-one-zero, the next 21 bits are the network and the last 8 bits are the local address(3).

Internet Protocol version 4 (IPv4) is one of the key foundations of the Internet, which is currently serving up to four billion hosts over diverse networks. Despite this, IPv4 has still been successfully functioned well since 1981. Over the last couple of years, the massive growth of the Internet has been evident requiring an evolution of the whole architecture of the Internet Protocol. There-fore, in order to strengthen the existing architecture of Internet Protocol, IETF has developed Internet Protocol version 6 (IPv6) . IPv6 offers a significant improvement of IPv4 when it comes to the unlimited address space, the built-in mobility and the security support, easy configuration of end systems, as well as enhanced multicast features, etc.

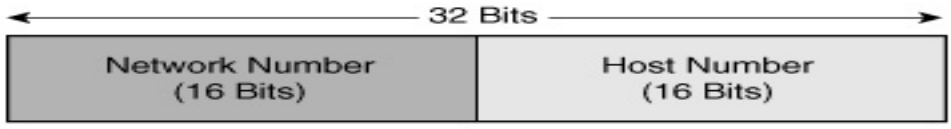


Figure No (1).IP Address Structure

IPv6 Address Format:-

As defined in RFC 1884 and later revised in RFC 2373, IPv6 addresses are 128 -bit identifiers for interfaces and sets of interfaces, not nodes. Three general types of addresses exist (4) (5):

Uncast—an identifier for a single interface. A packet sent to a uncast address is delivered to the interface identified by that address.

Anycast—an identifier for a set of interfaces that typically belong to different nodes. A packet sent to an anycast address is delivered to the nearest interface in the anycast group.

Multicast—an identifier for a set of interfaces that typically belong to different nodes. A Packet sent to a multicast address is delivered to all interfaces in the multicast group. To write 128-bit addresses so that they are more readable to human eyes, the IPv6 architects abandoned dotted-decimal notation in favor of a hexadecimal format. Therefore, IPv6 is written as 16-hex digits, with colons separating the values of the eight 16-bit pieces of the address (6).

IPv6 addresses are written in hexadecimal: **1080:0000:0000:0000:0008:0800:200C:417A** Leading 0s in each 16-bit value can be omitted, so this address can be expressed as follows: **1080:0:0:0:8:800:200C:417A**, Because IPv6 addresses, especially in the early implementation phase, might contain consecutive 16-bit values of 0, one such string of 0s per address can be omitted and replaced by a double colon. As a result, this address can be shortened as follows:

Under current plans, IPv6 nodes that connect to the Internet will use what is called an aggregatable global unicast address. This is the familiar counterpart to the IPv4 global addresses. Like CIDR - Enhanced IPv4, aggregatable global uncast addresses rely on hierarchy to keep Internet routing Tables manageable. IPv6 global uncast addresses feature three levels of hierarchy(7):

Public topology—the collection of providers that offer Internet connectivity.

Site topology—the level local to an organization that does not provide connectivity to nodes outside itself.

Interface identifier—The level specific to a node's individual interface.(3)This three-level hierarchy is reflected by the structure of the aggrgatable global uncast address, which includes the following fields:

Format Prefix (FP) field, 3 bits—The 3-bit FP is used to identify the type of address-uncast, multicast, and so on. The bits 001 identify aggregatable global uncast.

Top-Level Aggregation Identifier (TLA ID) field, 13 bits—The TLA ID field is use d to identify the authority responsible for the address at the highest level of the routing hierarchy. Internet routers necessarily maintain routes to all TLA IDs. With 13 bits set aside, this field can represent up to 8192 TLAs.

Reserved (Res) field, 8 bits—IPv6 architecture defined the Res field so that the TLA or NLA IDs could be expanded as future growth warrants. Currently, this field must be set to 0(8).

Next-Level Aggregation Identifier (NLA ID) field, 24 bits—The NLA ID field is used by organizations a assigned a TLA ID to create an addressing hierarchy and to identify sites.

Site-Level Aggregation Identifier (SLA ID) field, 16 bits—The SLA ID is used by an individual organization to create its own local addressing hierarchy and to identify subnets.

Interface ID field, 64 bits—The Interface ID field is used to identify individual interfaces on a link. This field is analogous to the host portion of an IPv4 address, but it is derived using the IEEE EUI-64 format. When this field is on LAN interfaces, the Interface ID adds a 16-bit field to the interface mac addresses local use address, which is specific to a network segment, figures no (2).

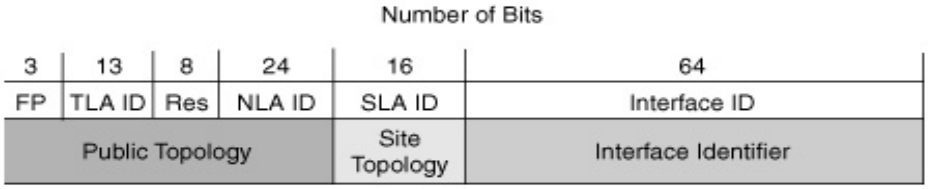


Figure No (2). IPv6 Address Format

I. IPV4&IPV6 HEADER COMPARISON

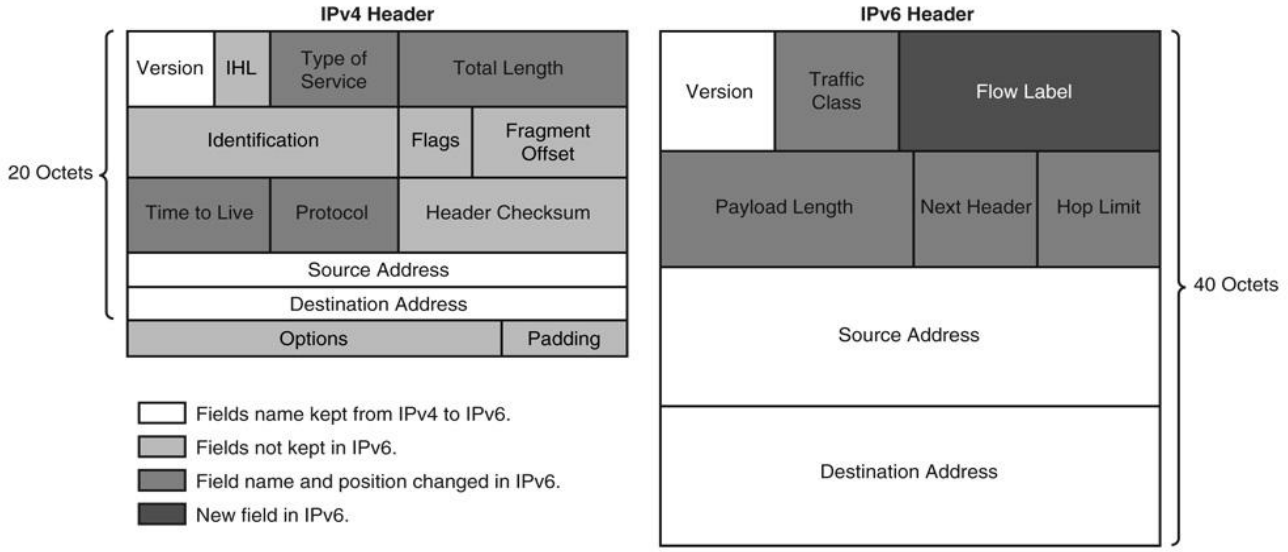


Figure (3). The differences between the headers of IPv6 and IPv4

The differences between the headers of IPv6 and IPv4 can be observed in the figure (3) (9)above.

• The length of the header is enlarged from 20 bytes (IPv4) to 40 bytes (IPv6).

• The number of bytes of each IP address in the header also increases, as IPv4 has 4 bytes for each address, and IPv6 has addresses of 16 bytes, what means that a very great part of the whole header is only used to represent the IP addresses.

• The number of header fields is reduced from 12 to 8.

• The options field is disappears from the base header, so the header length field is no longer needed, as the header will always have the same length.

The reason why the number of fields is decreased is the unnecessary redundancy, because, for example, the checksum , whose mission is ensure the integrity of the header, is also realized by other mechanisms of formation of packets (IEEE 802 MAC, framing PPP, ATM adaptation layer,…). Apart from this, the consequences of having errors in the IP header are not very important, so it is not dangerous to eliminate the checksum field(10).

The fragment offset header is also eliminated, because in IPv6 the fragmentation of the packets is completely different to the IPv4 fragmentation, what means that this field is absolutely useless. In IPv6 the routers do not fragment/defragment the packets, which can only by done end-to end. Instead of having the options field, IPv6 uses the "extension headers" that support more functionalities, and that are added to the main header only if needed. With this, we ensure that the length of the base header will always be the same (40 bytes), what implies a greater facility to be processed by the routers and the switches, even by hardware, what means greater pretentions.

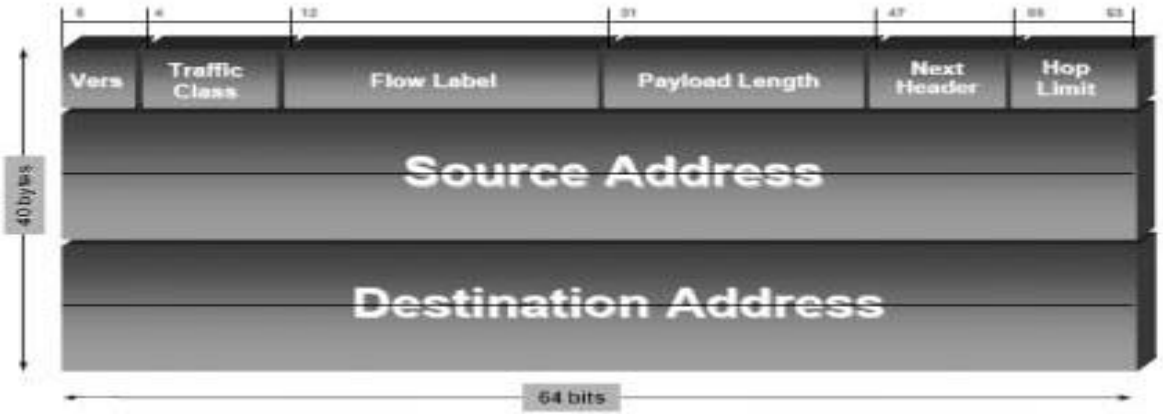


Figure no (4) Ipv6 base header

The header IPv6 fields above and their meanings figure no (4) are the following:-

• Version: This field indicates what version of IP protocol is being used. Its value will be 6, as we are using IPv6. Its length is 4 bits.

• Traffic Class: In this field is indicated what kind of traffic is being dealt and what its priority is. The length of this field is 8 bits. There are 2 types of traffic, in the first type, the user expects an answer in case of congestion (e.g. TCP), and in the second one, in case of congestion, the packets are discarded. For each of these types of traffic there are 8 possible priorities, from 0 to 7, being 7 the highest priority, and 0 the lower.

• Flow Label: This label is used when the user needs that the packets are handled by the routers in a special way, as high quality services or real time. Its length is 20 bits. Flow is a group of packets with similar values in their headers that need a special handling(11).

• Payload Length: The value of this label indicates the length in bytes of the data that follows the IP header. Its length is 16 bits, so the maximum size of the packet is 64 Kbytes. If the information is bigger than that, is possible to use an extension header of 32 bits that would allow packets up to 4.3 million bytes.

• Next Header: This label indicates the type of extension header that follows the base header. It has a length of 8 bits, and its information is coherent with the value of the field protocol in IPv4

.**Format of IPv6 packet:-the** figure no (5) shows the structure of the IPv6 packet. We can see that the format is more homogeneous than the IPv4 one, and the handling of options is improved, as we can use a concrete extension header for each special function we need (12).

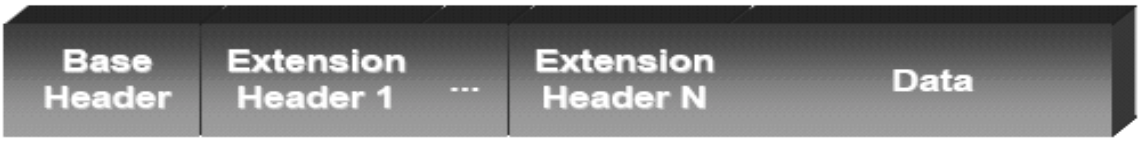


Figure no (5) Structure of the IPv6 packet

Extension Headers:-

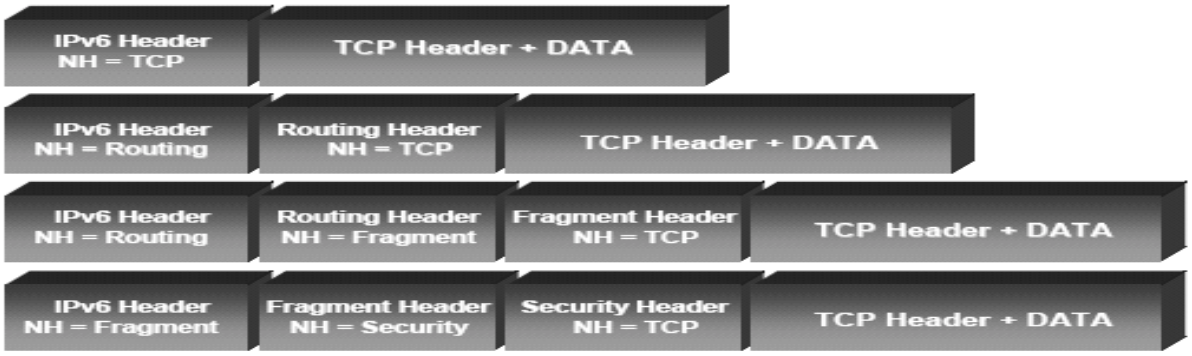


Figure no (6) extension headers

II. JUSTIFICATION OF THE METHOD OF STUDY

This section briefly discusses the different possible methods of research on networks and explains the choice of simulation as the appropriate method of study for the purpose of this work. Likewise, this section justifies the use of OPNET as the selected simulator and provides information on the procedures followed in order to reduce the possibility of simulation errors. Three methods are available for packet-level performance evaluation in IP networks which include: mathematical/analytical analysis, direct measurement and computer simulation. After thoughtful consideration, simulation and mathematical were found to be the suitable method of study in this work Many papers addressed the issue of comparison between ipv4 and ipv6 however most of them addressed the topic in terms of the theory only (13).

Network architecture:-

This section discusses about the following network components used in the suggested network models running on OPNET. Figure no (7).

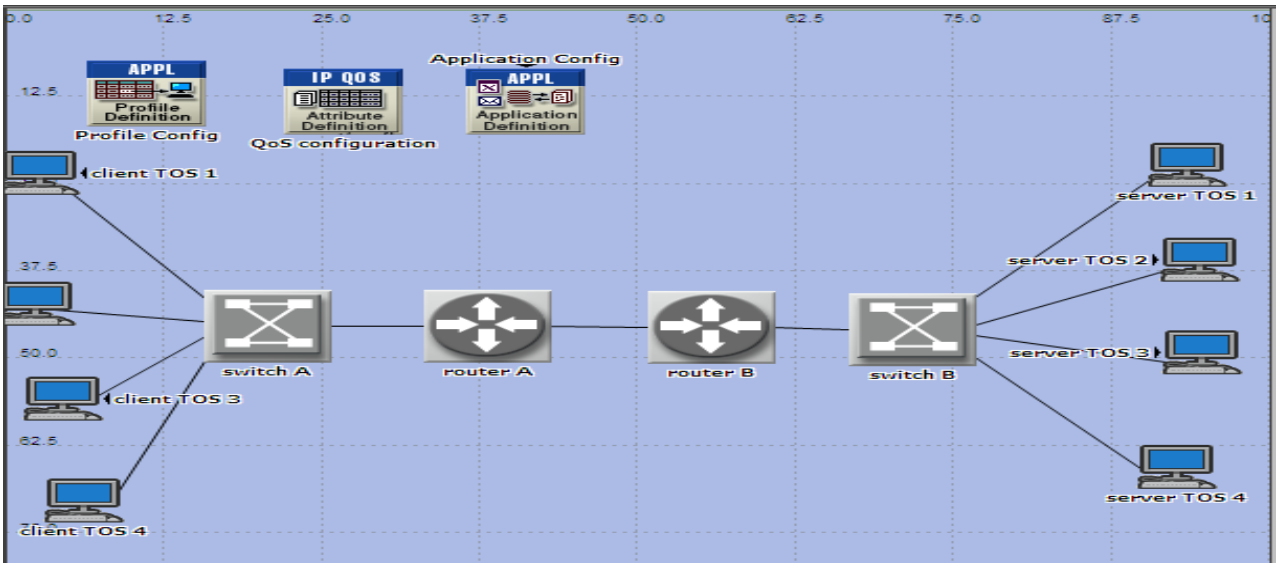


Figure no (7).IPv4&IPv6 Network Architecture

III. EXPERIMENTAL RESULTS

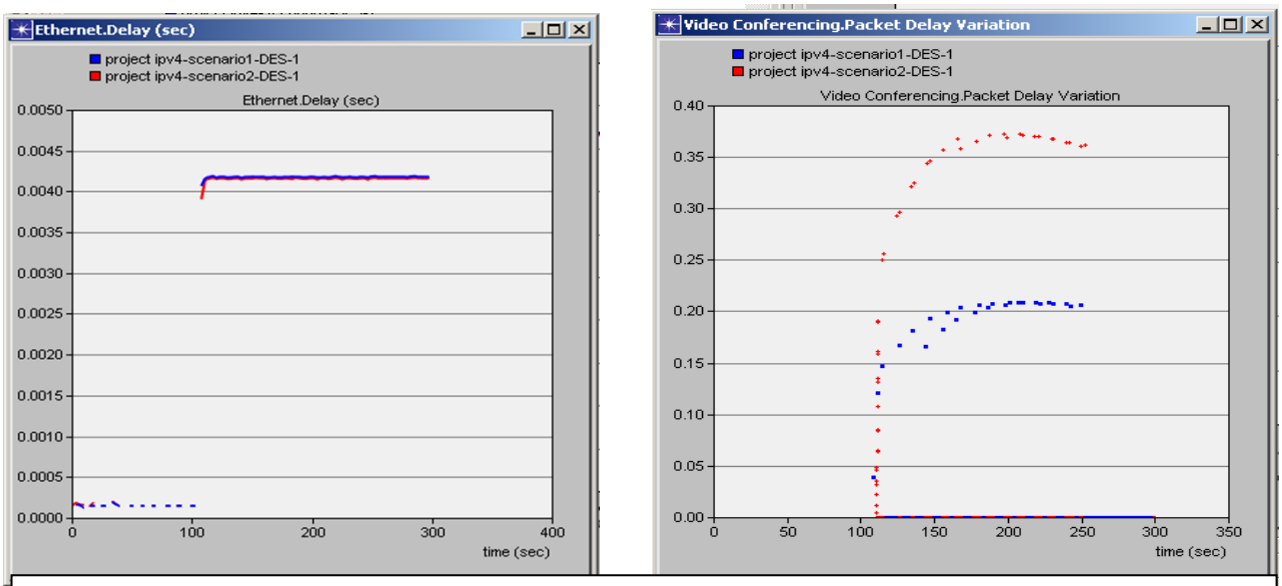
Network configuration:-

The network is composed of four pairs of video clients. Each pair uses a distinct TOS (Type of Service) for data transfer. The link between the two routers is a "potential" bottleneck.

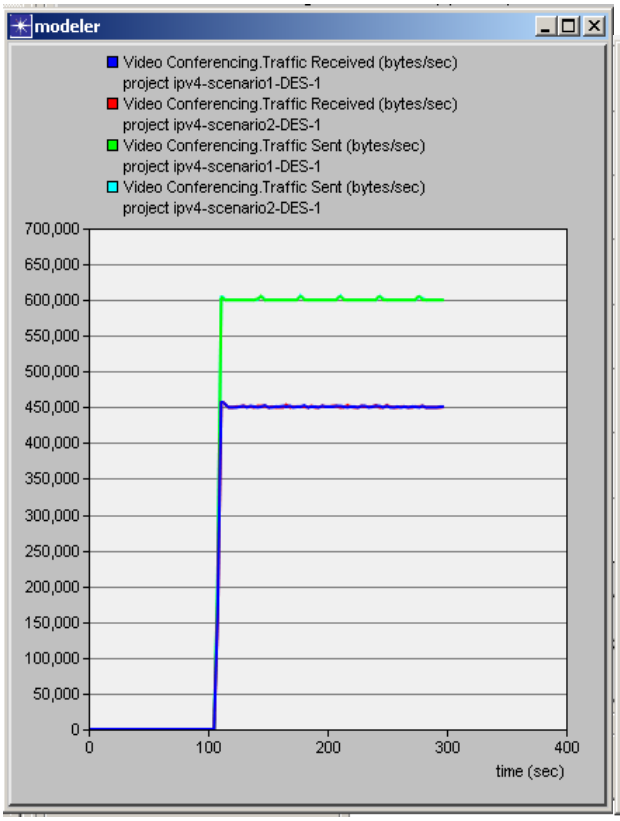
Results:-

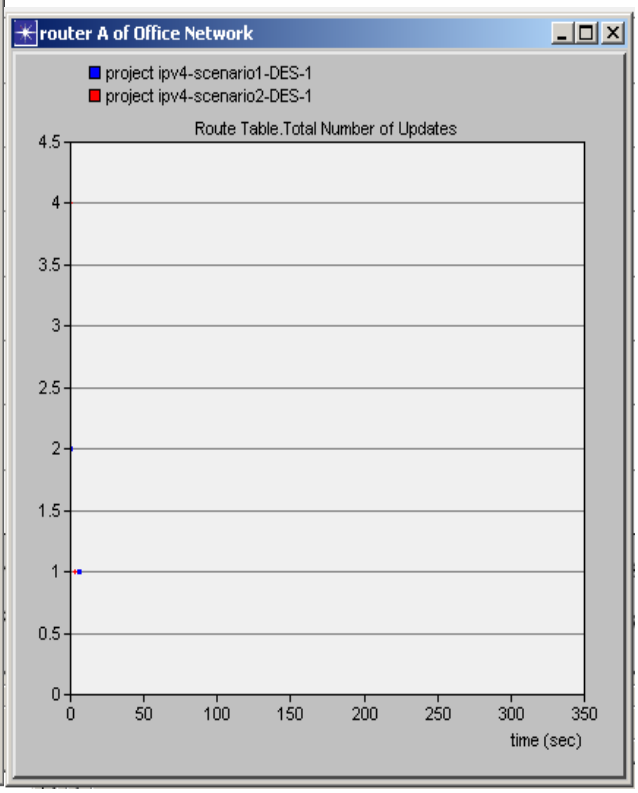
Traffic is queued in "router A" because of the bottleneck. Since "router A" has unlimited buffer capacity no packets get dropped.

The application response time keeps on increasing as the packets get queued indefinitely without ever getting dropped.

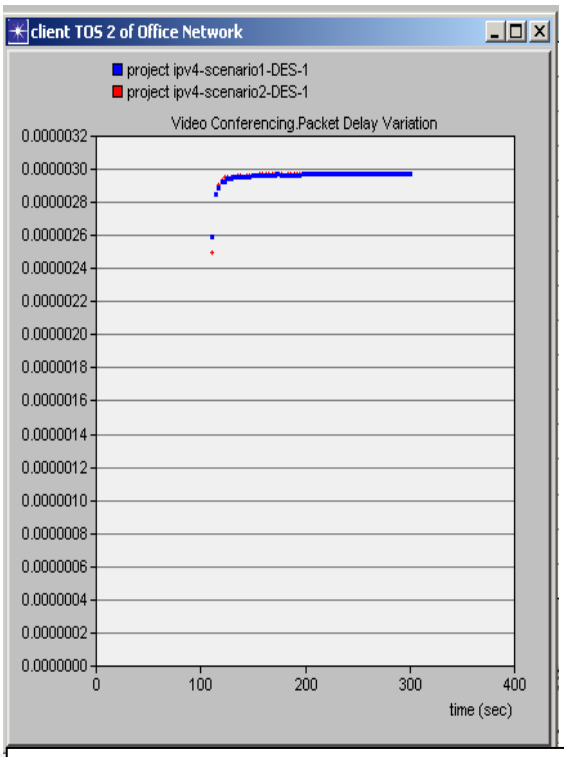


(a) (b)

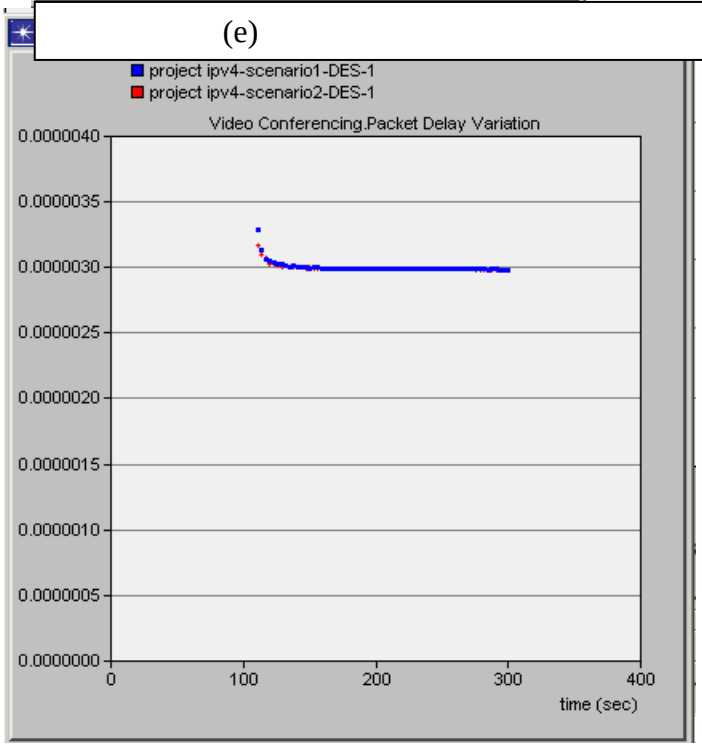

modeler
Video Conferencing.Traffic Received (bytes/sec)
project ipv4-scenario1-DES-1
Video Conferencing.Traffic Received (bytes/sec)
project ipv4-scenario2-DES-1
Video Conferencing.Traffic Sent (bytes/sec)
project ipv4-scenario1-DES-1
Video Conferencing.Traffic Sent (bytes/sec)
project ipv4-scenario2-DES-1
700,000
650,000
600,000
550,000
500,000
450,000
400,000
350,000
300,000
250,000
200,000
150,000
100,000
50,000
0
0
100
200
300
400
time (sec)


router A of Office Network
project ipv4-scenario1-DES-1
project ipv4-scenario2-DES-1
Route Table.Total Number of Updates
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
0
50
100
150
200
250
300
350
time (sec)

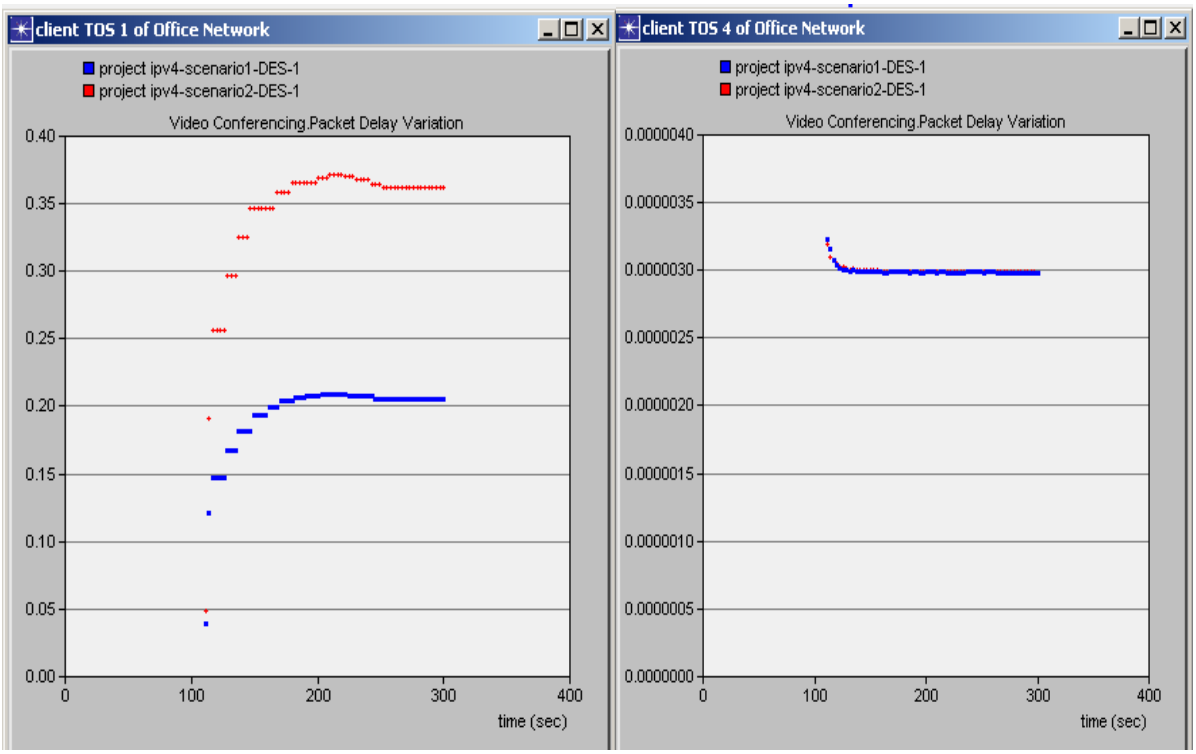
(c) (d)


client TOS 2 of Office Network
project ipv4-scenario1-DES-1
project ipv4-scenario2-DES-1
Video Conferencing.Packet Delay Variation
0.0000032
0.0000030
0.0000028
0.0000026
0.0000024
0.0000022
0.0000020
0.0000018
0.0000016
0.0000014
0.0000012
0.0000010
0.0000008
0.0000006
0.0000004
0.0000002
0.0000000
0
100
200
300
400
time (sec)

(e)


project ipv4-scenario1-DES-1
project ipv4-scenario2-DES-1
Video Conferencing.Packet Delay Variation
0.0000040
0.0000035
0.0000030
0.0000025
0.0000020
0.0000015
0.0000010
0.0000005
0.0000000
0
100
200
300
400
time (sec)

(f)



(g) (h)

Fig.no (8). Opnet analysis result (a) Ethernet delay (b) video conferencing .packet delay (c) video conferencing sent and receiver (d) Route Table. Total Number of updates (e) client 2 video conference .packet delay (f) client 3 video conference .packet delay(g) client 1 video conference .packet delay(h) client 4 video conference .packet delay

Discussion result:-

-In Fig no (8) (a) we find the Ethernet delay is semi equal between two version (ipv4&ipv6).this for all application

- In Fig no (8) (b) we find the different between two version when video conference application packet delay variation .IPv4 is low delay comparison with IPv6
- In Fig no (8) (c) find jitter when nodes sent and receive packet.

6000.000 sent byte-450.000 byte = 150.000byte .this jitter for all network.

- In Fig no (8) (d) route table number of update one to two updates every second
- In Fig no (8) (e) client TOS no (2) video conference (standard traffic) packet delay variation is 0.0000030 almost equal
- In Fig no (8) (f) client TOS no (3) video conference (excellent effort traffic) packet delay variation is 0.000003 IPv4 is delay is increase but ipv6 is go decreases.
- In Fig no (8) (g) client TOS no (1) video conference (background) packet delay variation IPv4 delay is very minimum than IPv6 (IPV4. 0.22) and (IPV6 it is near 0.40)
- In Fig no (8) (h) client TOS no (4) video conference (streaming) packet delay variation IPV6 is better than IPV4

IV. CONCLUSION

In this thesis paper, we have evaluated the Ethernet delay different based on simulation and analytical methods in IPv4/IPv6 networks. Two network scenarios called IPv4 network and IPv6 network have been simulated. The simulation has been carried out by using OPNET. Comparative investigation of Ethernet delay based on simulative

and analytical approaches was carried in both network scenarios. Based on this research, research question was aimed to understand and investigate what is difference in the delay is experienced in IPv4 and IPv6 network or what is best for user from (QOS) site. The simulation result in low load note ipv4 is low delay than ipv6, in medium load the delay is very low between them in high load the delay is equal. Although IPv6 more delay than IPv4 .but the IPv6 load Amax of header and security to treatment all network failure and problems.

REFERENCES

[1]- Md.Tarig Aziz, Mohamed Saiful islam, md.nazmul islam khan. throughput performance evolution of video /voice traffic in ipv4/ipv6 network. international journal of computer applications. December 2, 2011, p. 1
[2]- berger, arthur. comparison of performance over ipv6 versus ipv4. march 2011.page no 1.2
[3]-Press, cisco. Advanced Ip addressing management. s.l.: cisco system, 2004, pp. 52-55.
[4]-Ali, amer nizar Abu. Comparison study between ipv4&ipv6. International journal of computer science issue. May 1, 2012.
[5]-Parra, Jesus Ibanez. Comparison of ipv4and ipv6 network including concepts for deployment and interworking. InfoTech .seminar advanced. 2004.
[6]-Minoli, John. Moss and Daniel. Handbook of ipv4 to ipv6 transition. 2009.
[7]-davies, joseph. understanding ipv6. s.l. : microsoft press, 2003.
[8]-K.salah.Pealyam, M.buhari. Assessing readiness of Ip networks to support desktop video conferencing using Opnet.
[9]-k.salah.pealyam, and m.buhari. 2008. journal of network and computer application Vo.1.31 no 4,pp 921-943.
[10]-http://www.opnet.com/solution/network_rd/modeler.html. [Online].available, opnet .opnet modeler 14.5.
[11]- 3513, RFC. Internet protocol version 6(ipv6) addressing architecture.
[12]- RFC2462. internet protocol version 6 (ipv6) specification
[13]-Huitman. ipv6: the new internet protocol. s.l. : prentice. Hall, 1995.