Sudan University of Science and Technology

College of Graduate Studies

QoS Measurement for Real-Time Voice Traffic Over IPv4 and IPv6

قياسات جودة الخدمة لحركة البيانات الصوتية في الزمن الحقيقي علي الاصدار الرابع والسادس لبروتوكول الانترنت

A Thesis Submitted in Partial Fulfillment of Requirements

for the Degree of Master of Computer Engineering

Prepared by:

Hiba Hamed Ali Mohamed

Supervisor:

Dr. Ahmed Abdalla

May-2017

آيـة

قال تعالي:

بسم الله الرحمن الرحيم

(قُلْ كُلٌّ يَعْمَلُ عَلَى شَاكِلَتِهِ فَرَبُّكُمْ أَعْلَمُ بِمَنْ هُوَ أَهْدَى سَبِيلاً (84) وَيَسْأَلُونَكَ عَنِ الرُّوحِ قُلِ الرُّوحُ مِنْ أَمْرِ رَبِّي وَمَا أُوتِيتُمْ مِنَ الْعِلْمِ إِلَّا قَلِيلاً(85))

الاسراء الآية 84-85

صدق الله العظيم

Acknowledgment

First of all, I Am deeply grateful to Allah, My lord, who gave me the power and confidence to pursue this work and complete my MSC studies. I would first like to thank my family, especially my **sister Najat**, for the continuous her support have given me throughout time; I could not have done it without her.

Especially I would like to thankful to my supervisor **Dr.Ahmed Abdalla** his greater guidance and for technical support as well in this project. Thanks for him to make it possible for successful completion of this project. Great privilege and honor to work and study under his guidance. I am extremely grateful for what he has offered me.

I would like to thank Sudan University of science and technology 'data center office', University of Khartoum 'SudREN office' and SUDA CAD Academy for their cooperation to complete this thesis.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

ASCII	American Standard Code for Information Interchange.
CPL	Call Processing Language.
GNU	General Public License.
HL	Header Length.
HTTP	Hyper-Text Transfer Protocol.
IETF	Internet Engineering Task Force.
IPv4	Internet Protocol Version 4.
IPv6	Internet Protocol Version 6.
ITU	International Telecommunication Union.
MGCP	Media Gateway Control Protocol.
MTU	Maximum Transmission Unit.
NAT	Network Address Translation.
OSPFv2	Open Shortest Path First version2.
OSPFv3	Open Shortest Path First version3.
QoS	Quality of service.
RTP	Real Time Protocol.
SIP	Session Initiation Protocol.
SIP-CGI	SIP Common Gateway Interface.
SMTP	Simple Mail Transfer Protocol.
SUST	Sudan University of Science and Technology.
TCP/IP	Transmission Control Protocol/Internet Protocol.
TTL	Time-To-Live.
UDP	User Datagram Protocol.
U of K	University of Khartoum.
VOIP	Voice Over IP.
VPN	Virtual Private Network.

Abstract

Real time applications over IP network became widely used in different fields; video conference, online educational lectures, online call, online games and IP-TV.

The purpose of this study is to examine and analyze the impact of IP networks parameters; delay, jitter, and packet loss on the performance of real-time traffic “VOIP” sent across different IP networks; IPv6, IPv4 and compare the behavior of real-time traffic packets over IP networks. Experiments has been carried out in real operating networks environment: Prototype test network, Ideal operating network environment “controlled”, real operating network environment (University of Sudan- Dual-Stack) and real operating network environment (Khartoum University- Dual-Stack). Using Phonerlite application to generate real time traffic data between client’s hosts over IP (IPv4/IPv6) network. Examining delay, jitter, and packet loss for different packet sizes by using wireshark application and how these parameters can affect quality of real time traffice.

contrary expectations; results showed that the IPv4 network had a lower Delay and lower Jitter than IPv6 network. That is probably because IPv4 has a lower overhead than IPv6 therefore take less bandwidth to send the payload. IPv4 network had higher packet loss than IPv6 network; due to optimization of fragmentation.

Results obtained from this research may incourage researchers in the field to find solutions to problems of real-time traffic issues related to migration to IPv6.

المستخلص

التطبيقات في الوقت الحقيقي عبر شبكة IP أصبحت تستخدم على نطاق واسع في مختلف المجالات؛ مؤتمر الفيديو، والمحاضرات التعليمية عبر الإنترنت، والدعوة عبر الإنترنت، والألعاب عبر الإنترنت وIP-TV. والغرض من هذه الدراسة هو دراسة وتحليل أثر معلمات شبكات بروتوكول الإنترنت؛ تأخير، غضب، وفقدان الحزمة على أداء حركة المرور في الوقت الحقيقي "VOIP" المرسلة عبر شبكات IP مختلفة؛ IPv6، IPv4 ومقارنة سلوك حزم حركة المرور في الوقت الحقيقي عبر شبكات بروتوكول الإنترنت. وقد أجريت التجارب في بيئة شبكات التشغيل الحقيقية: شبكة اختبار النموذج، بيئة شبكة التشغيل المثالية "متحكم بها"، بيئة شبكة التشغيل الحقيقية (جامعة السودان ‘dual-stack ’) وبيئة شبكة التشغيل الحقيقية (جامعة الخرطوم ‘dual-stack’)

استخدم تطبيق phonerlite لتوليد بيانات حركة المرور في الوقت الحقيقي بين العميلين المضيفين عبر شبكة IP (IPv4 / IPv6). فحص التأخير والارتعاش وفقدان الرزم لأحجام الرزم المختلفة باستخدام تطبيق ويريشارك وكيف يمكن لهذه المعلمات أن تؤثر على نوعية حركة المرور في الوقت الحقيقي. علي غير المتوقع؛ أظهرت النتائج أن شبكة IPv4 لديها تأخير أقل وانخفاض غضب من شبكة IPv6. ويرجع ذلك على الأرجح إلى أن الإصدار IPv4 يحتوي على overhead أقل من IPv6 وبالتالي فإن عرض النطاق الترددي أقل لإرسال الحمولة النافعة. IPv4 لديه خسارة في الحزم اعلى من IPv6؛ بسبب التجزئة المثالية.

النتائج التي تم الحصول عليها من هذا البحث قد تحث الباحثين في هذا المجال على إيجاد حلول لمشاكل قضايا حركة المرور في الوقت الحقيقي المتعلقة بالهجرة إلى IPv6.

1.1 Background:

Quality of service is very important especially for applications which need high performance like real time application. Quality of service is important if the network capacity is insufficient, especially for real-time multimedia applications such as voice over IP, online games and IP-TV, since these often require fixed byte rate and are delay sensitive. It is also important for networks where the capacity is a limited resource, for example in cellular data communication. Quality of service sometimes refers to the level of quality of service[1].

There are some important parameters in QoS:

a. Delay: the time which retard between the sending voice signal and the moment of arrival to destination, along time of each packet to arrive to destination, some time because queuing mechanism and routing direction in congestion[1].

b. Jitter: It is the variation of the delay in the voice packages that are delivered to destination. This variable time difference may determine interruptions in the voice signal[1].

c. Packet loss: the router may fail or lose the packets. The receiving application may ask for information that dropped to be retransmitted again, possibly causing severe delays in the overall transmission [1].

Real-Time Challenge:

In multimedia networking, one can expect at least three difficulties, which are as follows:

(a) Compared with traditional textual applications, multimedia applications usually require much higher bandwidth[2].

(b) Most multimedia applications require the real-time traffic. Audio and video data must be played back continuously at the rate they are sampled. If the data does not arrive in time, the playing back process will stop and human ears and eyes can easily pick up the artifact. In addition to the delay, network congestion also has more serious effects on real-time traffic[2].

(c) Multimedia data stream is usually bursty. Just increasing the bandwidth will not solve the burstiness problem. For most multimedia applications, the receiver has a limited buffer. If no measure is taken to smooth the data stream, it may overflow or underflow the application buffer. When data arrives too fast, the buffer will overflow and some data packets will be lost, resulting in poor quality. When data arrives too slow, the buffer will underflow and the application will starve [2].

Voice over Internet Protocol (**Voice over IP**, **VoIP** and **IP telephony**) is a methodology and group of technologies for the delivery of voice communications and multimedia sessions over Internet Protocol (IP) networks, such as the Internet. The steps and principles involved in originating VoIP telephone calls are similar to traditional digital telephony and involve signaling, channel setup, digitization of the analog voice signals, and encoding. Instead of being transmitted over a circuit-switched network; however, the digital information is packetized, and transmission occurs as IP packets over a packet-switched network. They transport audio streams using special media delivery protocols that encode audio and video with audio codecs, and video codecs. Various codecs exist that optimize the media stream based on application requirements and network bandwidth; some implementations rely on narrowband and compressed speech, while others support high fidelity stereo codecs. Some popular codecs include μ-law and a-law versions of G.711, G.722, a popular open source voice codec known as iLBC, a codec that only uses 8 kbit/s each way called G.729, and many others[3].

1.2 Problem statement:

Real time voice traffic is sensitive to delay, jitter and packet loss. Next generation IP (IPv6) as new protocol, is designed and assumed to better support real-time voice traffic. However, the performance of IPv6 needs more realistic evaluations under real operating networks. There is a need to validate whether IPv6 compared to IPv4 does actually provide better performance and QoS to real-time traffic.

1.3 Proposed solution:

Measure quality of service of real time voice traffic generated by a 4-minutes Phonerlite application sessions over IPv4 and IPv6. Measurements are done several times on different testbeds with different topologies. To measure QoS of each session, Wireshark tool is used to calculate delay, jitter and packet loss parameters.

1.4 Aim & objectives:

The aim of this research is to evaluate and compare quality of service of real time voice traffic over IPv4 and IPv6.

Other indirect expected benefits of fulfillment of the study are:

- To reduce delay, jitter and packet loss in real time traffic.
- To enhance performance of real time traffic.

1.5 Research Outline:

This research is organized as follows:

- Chapter 1 gives an introduction to the research field and background of IPv6 as the successor to IPv4.
- In Chapter 2, an overview on IPv4 and its limitations and why there is a need to migrate to IPv6. Then there is an overview on IPv6, RTP, VoIP. This is followed by a literature review that summarizes the most related works on the topic.
- Chapter 3 shows the overall research methodology, explains and discusses general framework, the test bed used for evaluation and the selected VoIP application. It also discusses with details all experimental setups and steps, validation methods and rational constructions behind the selected methodology.
- Chapter 4 presents, discusses and justifies the different scenarios results of the carried out experiments.
- Chapter 5 concludes all the study and states the degree of objective fulfillment, and makes suggestion for future work.

2.1 Introduction

This chapter makes a review on IPv4 and its limitations and why there is a need to migrate to IPv6. Then there is an overview on IPv6, RTP, VoIP. This is followed by a literature review that summarizes the most related works on the topic.

2.2 Internet Protocol version 4 (IPv4):

Is the fourth version of the Internet Protocol (IP). It is one of the core protocols of standards-based internetworking methods in the Internet, It still routes most Internet traffic today, despite the ongoing deployment of a successor protocol, IPv6 [4]**.** IPv4 employs a 32-bit address, which limits the number of possible addresses to 4,294,967,296[5]. Because of the demand of the growing Internet, the small address space finally suffered exhaustion on 3 February, 2011[6], after having been significantly delayed by classful network design, Classless Inter-Domain Routing, and network address translation (NAT)[4]. IPv4 will eventually be replaced by IP Version 6 (IPv6), due to a shortage of available IPv4 addresses [5]. The following figure shows the ipv4 header**:**

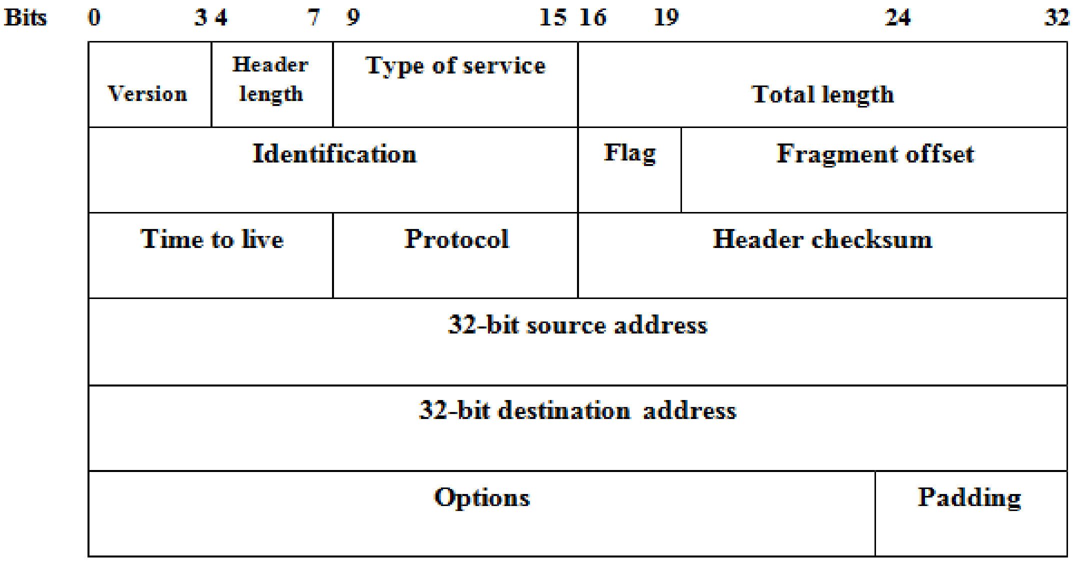


Figure (2-1) IPv4 header

2.3 Internet Protocol version 6 (IPv6):

IPv6 as IP next generation is the successor to IPv4. IPv6 not only solves the shortcomings problem of IPv4 address, but also benefits the QoS. Especially during network congestion. Flow label field in IPv6 packet header provides an efficient way for packet marking, flow identification, and flow state lookup [1].

2.3.1 IPv6 Header:

The IPv6 header is a streamlined version of the IPv4 header. It eliminates fields that are unneeded or rarely used and adds fields that provide better support for real-time traffic [7]; the following figure shows the ipv6 header [8]:

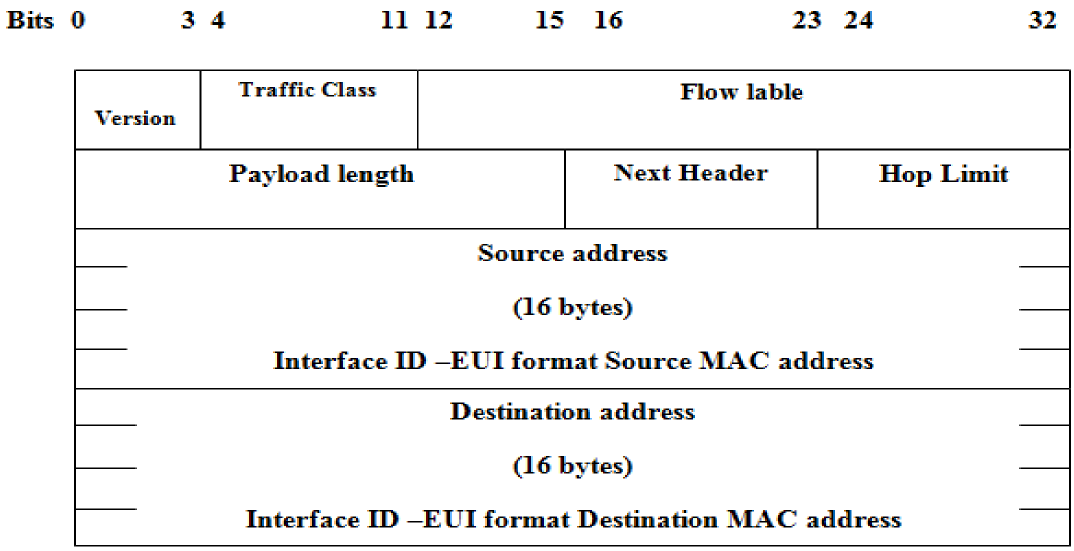

Bits 0 3 4 11 12 15 16 23 24 32
Version
Traffic Class
Flow lable
Payload length
Next Header
Hop Limit
Source address
(16 bytes)
Interface ID –EUI format Source MAC address
Destination address
(16 bytes)
Interface ID –EUI format Destination MAC address

Figure (2-2) IPv6 header

IPv6 header is much simpler than IPv4 header. The size of IPv6 header is much bigger than that of IPv4 header, because of IPv6 address size. IPv4 addresses are 32bit binary numbers and IPv6 addresses are 128 bit binary numbers. In IPv4 header, the source and destination IPv4 addresses are 32 bit binary numbers. In IPv6 header, source and destination IPv6 addresses are 128 bit binary numbers. IPv4 header includes space for IPv4 options. In IPv6 header, we have a similar feature known as extension header. IPv4 datagram headers are normally 20-byte in length. But we can include IPv4 option values also along with an IPv4 header. In IPv6 header we do not have options, but have extension headers [9]. The header fields and their meanings [10] are shown in the Table2-1.

Table 2-1: Description of IPv6 Header Fields.

Name of Field	**Length (bit)**	**Description**
Version field	4	Version No.
Traffic class field (priority)	8	This field is subsequently used by the originating node and the routers to identify the data packets that belong to the same traffic class and distinguish between packets with different priorities.
Flow Label field	20	This field used by the source to label a set of packets belonging to the same flow.
Payload length field	16	Shows the data length in the packet following the IPv6 packet header.
Next Header field	8	Specifics the type of header that follows the header of ipv6 header.
Hop Limit count	8	This field is decremented by one, by each node (typically a router) that forwards a packet. If the Hop Limit field is decremented to zero, the packet is discarded.
Sources address	128	Sender address.
Destination address	128	Recipient address.

2.3.1.1 Fields that are not kept in IPv6 Header:

- **HL field**

The HL field in the IPv4 header identifies the length of the IPv4 header. Because the Options field exists in the IPv4 header, the IHL field is mandatory to determine the length of the IPv4 header. However, the IHL field has 4 bits only (the minimum value is 5 in the unit of 4 octets), so the expandability of the options in the header is limited. The IPv6 header is composed of the basic header and the extension headers. The length of the basic header is fixed as 40 octets, so the IHL field is eliminated in the IPv6 header. The Identification field in the IPv4 header is assigned a value by the sender to identify the same group of fragments so as to help fragment reassembly. IPv6 packet fragmentation is implemented through the extension headers. Therefore, the Identification field is no longer needed in the basic header of an IPv6 packet[11].

- **Flags field**

The Flags field in the IPv4 header identifies whether the packet is a fragment and whether it is the last fragment. IPv6 packet fragmentation is implemented through the extension headers. Therefore, the Flags field is no longer needed in the basic header of an IPv6 packet. Fragment Offset field The Fragment Offset field in the IPv4 header identifies the position of the fragment in the original packet before the packet is fragmented. IPv6 packet fragmentation is implemented through the extension headers. Therefore, the Fragment Offset field is no longer needed in the basic header of an IPv6 packet[11].

- **Header Checksum field**

The Header Checksum field in the IPv4 header is used to check for errors in the IPv4 header. Generally, the link layer in the current networks is highly reliable with a check mechanism and the transmission layer has its own header checksum mechanism. Therefore, the Header Checksum field is excessive to some extent. Moreover, the computation of the Header Checksum field involves TTL and every intermediate Router need re-compute the TTL, so the forwarding efficiency is affected. Therefore, the Header Checksum field is eliminated in the IPv6 header (but checksum computation is mandatory in the UDP header) [11].

- **Options field**

The Options field in the IPv4 header is used to support the options. Its length is variable, but cannot exceed the length of the IPv4 header. The expandability of the Options field is limited. In the IPv6 packet, the extension headers implement this function and thus the Options field is no longer needed[11].

- **Padding field**

In the IPv4 header, the Padding field is used to ensure that the header ends with the 32-bit border to facilitate hardware to access the packet. In the IPv6 packet, the length of the basic header is fixed and thus the Padding field is no longer needed[11].

2.3.1.2 New fields in IPv6:

- **Flow Label field**

The Flow Label field is added in the IPv6 header. The source node can use this field to identify a specific data flow. The flow label is allocated by the source node [11].

2.4 VOIP signaling protocols:

Most VOIP signaling protocols run over TCP/IP networks, which provide a full reliable transfer of data packets between clients or between clients and servers. The transfer of real-time packets (RTP protocol) is carried over UDP, which does not provide a loss-less packets transfer between the two ends of the link, because resending lost packets is unnecessary since they usually arrive too late to be used in voice stream. VOIP uses signaling protocols such as Session Initiation Protocol (SIP) or H.323 for establishing, modifying and tearing down unicast or multicast session consisting of one several media streams[12].

Different standards are emerging to specify VOIP protocols. The following are the main standards used in this area: SIP, H323, and MGCP. A brief introduction is included hereafter for the two most popular protocols (SIP and H.323). Figure (2-3) gives a high-level view of the SIP and H.323 protocols and their interaction with the TCP/IP stack. Traditional VOIP protocols, such as Session Initial Protocol (SIP) and H.323 (ITU recommendation), work in a centralized manner[12].

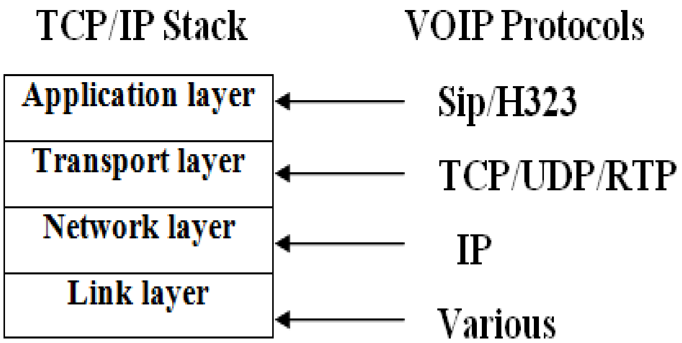


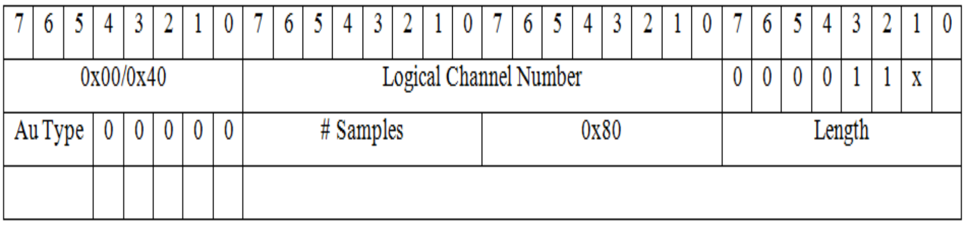
Figure (2-3): VOIP protocols over TCP/IP stack

The Session Initiation Protocol (SIP) is an ASCII-based, peer-to-peer application layer protocol that defines initiation, modification and termination of interactive, multimedia communication sessions between users[12].

SIP is developed by Internet Engineering Task Force (IETF) and is derived from Hyper-Text Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP).SIP is defined as a client-server protocol, in which requests are issued by the calling client and responded to by the called server, which may in itself be a client for other aspects of the same call. SIP is not dependent on TCP for reliability but rather handles its own acknowledgment and handshaking. This makes it possible to create an optimal solution that is highly adjusted to the properties of VOIP[12].

The ITU-T recommended H323 protocol show in figure (2-4) below suite has evolved out of a video telephony standard H.323 is known for quite complex signaling, high connection setup latencies, and implementation difficulties[12].

However, H.323 is widely implemented and is the primary common denominator for all VOIP[12].



7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0	7	6	5	4	3	2	1	0
0x00/0x40								Logical Channel Number																0	0	0	0	1	1	x	
Au Type			0	0	0	0	0	# Samples								0x80								Length							

Figure (2-4): H323 protocol

Logical Channel Number: The number of the H.245 logical channel 1.

Au Type: The audio codec to be used.

Samples: The number of samples -1 per audio packet as defined in ITU-T Rec.H.245.

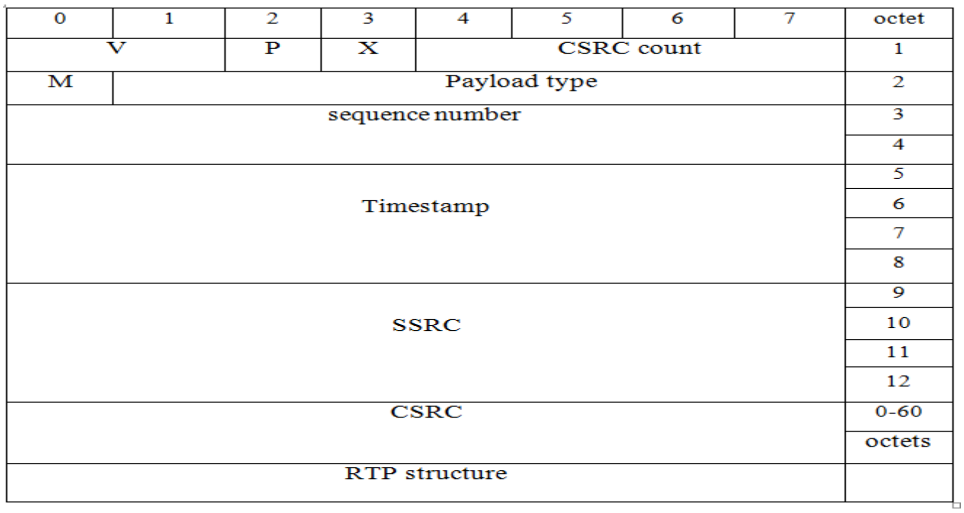
SIP and H.323 provide similar functionality: call control, call setup and teardown, basic call features such as Call waiting, Call hold, Call transfer, Call forwarding, Call return, Call identification, Call Park, and capabilities exchange. Each protocol exhibits strengths in different applications. H.323 defines sophisticated multimedia conferencing which can support applications such as white boarding, data collaboration, or video conferencing[12].

SIP supports flexible and intuitive feature creation with SIP and SIP-CGI (SIP Common Gateway Interface) and CPL (Call Processing Language). Third party call control is currently only available in SIP. Work is in progress to add this functionality to H.323[12].

2.5 Real Time Protocol:

The RTP is an application layer protocol that attaches itself to UDP to provide added benefits for real time application, applications typically run RTP on top of UDP. The RTP packets contain the audio and video elementary streams associated with the selected program and information about the standard used for the compression[12].

(RTP) was developed for the transportation of real time multimedia, such as VOIP service .Traditionally, VOIP application use the protocol stack of RTP/UDP/IP to convey voice data .UDP is a connectionless transport protocol widely used in multimedia services[12].



0	1	2	3	4	5	6	7	octet
V		P	X	CSRC count				1
M	Payload type							2
sequence number								3
								4
Timestamp								5
								6
								7
								8
SSRC								9
								10
								11
								12
CSRC								0-60
								octets
RTP structure								

Figure (2-5) real time protcol

V: Version. Identifies the RTP version.

P: Padding. When set, the packet contains one or more additional padding octets at the end which are not part of the payload.

X: Extension bit. When set, the fixed header is followed by exactly one header extension, with a defined format.

CSRC count: contains the number of CSRC identifiers that follow the fixed header.

M: Marker. The interpretation of the marker is defined by a profile. It is intended to allow significant events boundaries to be marked in the packet stream.

Payload type: Identifies the format of the RTP payload and determines its interpretation by the application. A profile specifies a default static mapping of payload type codes to payload formats. Additional payload type codes may be defined dynamically through non-RTP means.

Sequence number: Increments by one for each RTP data packet sent, and may be used by the receiver to detect packet loss and to restore packet sequence.

Time stamp: Reflects the sampling instant of the first octet in the RTP data packet. The sampling instant must be derived from a clock that increments monotonically and linearly in time to allow synchronization and jitter calculations. The resolution of the clock must be sufficient for the desired synchronization accuracy and for measuring packet arrival jitter (one tick per video frame is typically not sufficient)**.**

SSRC: Identifies the synchronization source. This identifier is chosen randomly, with the intent that no two synchronization source within the same RTP session will have the same SSRC identifier.

CSRC: contributing source identifiers list. Identifies the contributing source for the payload contained in this packet[12].

An RTP header includes a sequence number to help preserve the order of the transmitted packets. It also includes a timestamp, which is meant to provide information to the destination application so that it may compensate for problems such as delay or jitter if they arise[12].

RTP is protocol of choice for streaming media over the Internet and is widely used in VOIP application. RTP is typically run on top of UDP to make use of its multiplexing and checksum functions. TCP and UDP are two most commonly used transport protocol on the Internet .TCP provide a connection-oriented and reliable flow between hosts, while UDP provide a connectionless but unreliable datagram service over the Internet. UDP was chosen as the target transport protocol for RTP because of two reasons. First, RTP is primarily designed for multicast;

the connection-oriented TCP does not scale well and therefore is not suitable. Second, for real-time data, reliability is not as important as timely delivery. Even more, reliable transmission provided by retransmission as in TCP is not desirable. For example, in network congestion, some packets might get lost and the application would result in lower but acceptable quality. If the protocol insists a reliable transmission, the retransmitted packets could possibly increase the delay, jam the network and eventually starve the receiving application [12].

2.6 User datagram protocol UDP:

UDP is a simple, transport layer protocol that does not guarantee any reliability and in order delivery of the packets. It supports both multicasting and broadcasting. UDP is considered where the in time delivery of data is important rather than reliable delivery[13].

Source port address (16 bits)	Destination port address (16 bits)
Total length (16 bits)	Checksum (16 bits)

Figure (2-6) UDP Datagram Format

The description of each field in detail is as follows :

- **Source port address-** This field indicates the port of the sending process which sends the datagram.
- **Destination port address-** It indicates the port of the destination process to which the datagram is to be sent.
- **Length-** This field specifies the length (in bytes) of datagram which includes the header also.
- **Checksum-** This field is an optional 16-bit one's complement of the one's complement sum of a pseudo-IP header, UDP header,

and UDP data, where the pseudo-IP header contains source IP address and destination IP address, protocol, and UDP length[13].

2.7 Related Work:

In [14] Authors designed and simulated network by using OPNET Modeler to evaluate and compare the performance of IP (IPV4 and IPV6) by using four parameters (delay ,jitter, utilization and throughput) , and find out what is the best IP under particular application (Voice ,HTTP, Email) . After simulation Result, they find that the performance of IPV6 is much better than IPV4, the IPv6 protocol has better transmission efficiency and high throughput and the largest utilization per line rate are those traffic mixes with the most IPv6 traffic. The IPv6 has a higher Ethernet Delay than IPv4 because IPv6 has a larger header field. IPv4 has a smaller header field and the packet frame. Except in voice; in case of send traffic is equal but in receives IPV4 has larger delay when compare to IPV6. Another key aspect is the jitter, IPV6 showed less jitter than IPV4 protocol.

In [15] Authors discussed about IPV4 and IPV6 and use transition strategies of IPV6 and also compare their performance to show how these transition strategies affects network behavior . Result of this research shows that native Dual-Stack is the technology that companies should consider for their deployment. It keeps both IPv4 and IPv6 running at the same time. When the network is fully transitioned to IPv6, operators can stop supporting IPv4. The next best transition technology to deploy in the network is NAT64.

In [16] Authors demonstrated the two tunnels and show when to immigrate from IPv4 to IPV6.Then the risks of immigration are discussed. Result of this research shows Migrating from IPv4 to IPv6 in an instant is impossible because of the huge size of the Internet and of the great number of IPv4 users, and there will not be one special day on which IPv4 will be turned off and IPv6 turned on because the two protocols can coexist without any problems.

In [17] Authors compared and evaluated the performance of IPv4, IPv6 and tunneling (6to4) using OPNET 17.5. A computer simulation shows the theoretical comparison in terms of delay, throughput and packet loss. They use different network after the network implementation, start to configure the attributes for Ipv6, Ipv4, Tunneling (6to4) , Authors conclude that IPv6 has a higher Ethernet Delay than IPv4 because IPv6 has a larger header field , 6to4 the delay is higher than IPv4 because the packets are not transferred directly.. IPv4 has a smaller header field and the packet frame.

Delay6to4 < DelayIPv6 < DelayIPv4

The IPv6 has high throughput stated time if we compare it with tunnelling and IPv4.

IPv6< 6to4tunnel <IPv4

The IPv6 has high packet loss stated time if we compare it with tunneling and IPv4.

IPv6 < 6to4 tunnel < IPv4.

In [18] Authors investigate the characteristics of IPv6 packet traffic and the differences between IPv6 and IPv4 packet traffic in terms of spectral density, autocorrelation, distribution, and self-similarity of packet interarrival time and packet size.

They demonstrate that there are certain differences in terms of the mentioned traffic characteristics for both IPv6- and IPv4-related traffic. Packet interarrival time and packet size distribution fitting results prove that they should be modeled with different functions. While the beta distribution could model the empirical cumulative distribution of IPv4 packet size, the log logistic distribution gave more efficient results for

IPv6 packet size according to chi-square and Anderson-Darling test statistics. Various analysis results showed that the aggregated incoming traffic at different time scales exhibited very different characteristics in terms of power spectral density and autocorrelation. These variations deeply affect the self-similarity degree of aggregated traffic at different time scales for both protocol traffics. Lastly, we analyzed the interarrival times of incoming traffic loads per 10,000, 50,000, 100,000, and 500,000 received bytes in terms of IPv6 and IPv4 protocol traffic. The self-similarity results for the interarrival time series were quite different for the protocols. IPv6 packet traffic exhibited greater self-similarity degrees than IPv4. The results obviously show that IPv6 protocol traffic would cause more performance degradations in computer networks.

In [19] Authors presented the simulation results of the comparison of the two Internet Protocols, Internet Protocol version 4 and Internet Protocol version 6. The comparison criteria are the affect of each on the Ethernet load and Ethernet delay over four networks services http service, DB service, video conference service and IP telephony service. After simulation Result, they find that:

- When the network used IPv6 as addressing protocol there have to be more IP addresses rather than it used IPv4.
- The delay over the network severs when it used IPv6 less than IPv4.
- On the other hand the network load increased when the network used IPv6 rather than IPv4.

In [20] Authors aims to compare between OSPFv2 and OSPFv3, to explain the impact of the change in OSPFv3 packet format and the over load when OSPFv3 uses IPv6 packet instead of IPv4 packet format that was used by OSPFv2, and the comparison based on common OSPF packets that was sent in the same network. After simulation Result, the study resulted in the following findings:

- Packet sent in an IPv4 environment is smaller than the packet sent in an IPv6 environment. This is because in the IPv6 network, addressing is much larger than in IPv4. IPv4 header size is 20 bytes, whereas in IPv6 is 40 bytes.
- In OSPFv3, authentication has been removed from the OSPF packet header. OSPFv3 relies on the authentication mechanism of IPv6 to ensure integrity and validity.
- OSPFv3 does not require a Network mask to form an adjacency formation. Adjacency is formed on the link local as v6 runs on per link instead of per subnet.

In [21] Authors focused to compare and analyze IPv4 and IPv6 networks, study their characteristics and header formats , and addresses the issues that are prevalent in IPv4 and explains the reasons for seamless migration to IPv6 , also discusses about established migration techniques and highlights their drawbacks from security and performance point of view.

These techniques demand optimization in hardware and software like enhancing router software, operating systems etc. The similarities in two protocols help in implementing strong security policies to secure IPv6 and migration networks. It is expected that IPv4 and IPv6 hosts will need to coexist for a substantial time during the steady migration from IPv4 to IPv6, and the development of transition strategies, tools, and mechanisms has been part of the basic IPv6 design from the start.

In [22] Authors analyzed Ipv6 and Ipv4 Threat Comparisons, they focus on the attacks with Ipv4 and Ipv6 similarities and on the attacks with new considerations in Ipv6.

Authors conclude that IPv6 mandates usage of the IPSec protocol and also has flexible extension header options. In practice that could help, however does not solve all the security problems for the all requirements. Although IPv6 offers better security (larger address space and the use of encrypted communication), the protocol also raises new security challenges. It is far from being a panacea. For an improved protection in IPv6 networks it is recommended to implement security mechanisms for packet filtering (firewalls) and intrusion detection. All unneeded services should be filtered at the firewall. Nevertheless, security of IPv6 protocol and IPv6 networks can still be improved, but this fact should not be an obstacle to its acceptance, usage and further development.

In [23] the research groups analyzed IPv6 hacking techniques such as Man in the Middle, Smurf attacks their functionalities and how to protect each are in individual way. and propose a combined solution from the existing solutions , the solution for this attacks used firewall in middle and used VPN for monitoring the online processing. Used these things together in the internal firewall it is protect network very efficiency.

Table 2-2: show the summary of some papers

No	Author, Date	Methodology	Finding
1	G.y .Al-Gadi , Dr.Amin Babiker, A .Al-Gadi , (2014) .	• using OPNET Modeler . • evaluate and compare the performance of IP (IPV4 and IPV6). • using four parameters (delay ,jitter, utilization	IPv6 : • better performance. • better transmission. efficiency and high throughput • a higher Ethernet Delay , Except in voice. • less jitter than IPV4

		and throughput) ,	protocol.
2	Priya Bali , (2015)	• Transition strategies of IPV6. • compare their performance	• Native Dual-Stack. • NAT64.
3	A.M. Kapashi Dr. Amin Babiker Dr: Gasm Elseed Ibrahim3, (2015)	• Compared and evaluated the performance of IPv4, IPv6 and tunneling(6to4). • using OPNET 17.5.	• Ethernet Delay: Delay6to4 < DelayIPv6 < DelayIPv4. • throughput: IPv6 < 6to4tunnel < IPv4. • packet loss: IPv6 < 6to4 tunnel < IPv4.
4	Dr. Mustafa ElGili Mustafa (3, March 2015)	• comparison of the two Internet Protocols, IPv4 and IPv6 . • comparison criteria on the Ethernet load and Ethernet delay over four networks services http service, DB service, video conference service and IP telephony service	• The delay over the network severs when it used IPv6 less than IPv4. • On the other hand the network load increased when the network used IPv6 rather than IPv4.

3. Research Methodology

3.1 Introduction :

This chapter describes, discusses and justifies the research approach, methods and techniques used in this research work. General methodology frameworks followed by specific sub frameworks of all phases and way forward to achieve research objectives are presented and explained.

3.2 Overall Research Design:

Figure 3.1 shows a general framework of the research work. The following subsection describes each step of the research framework.

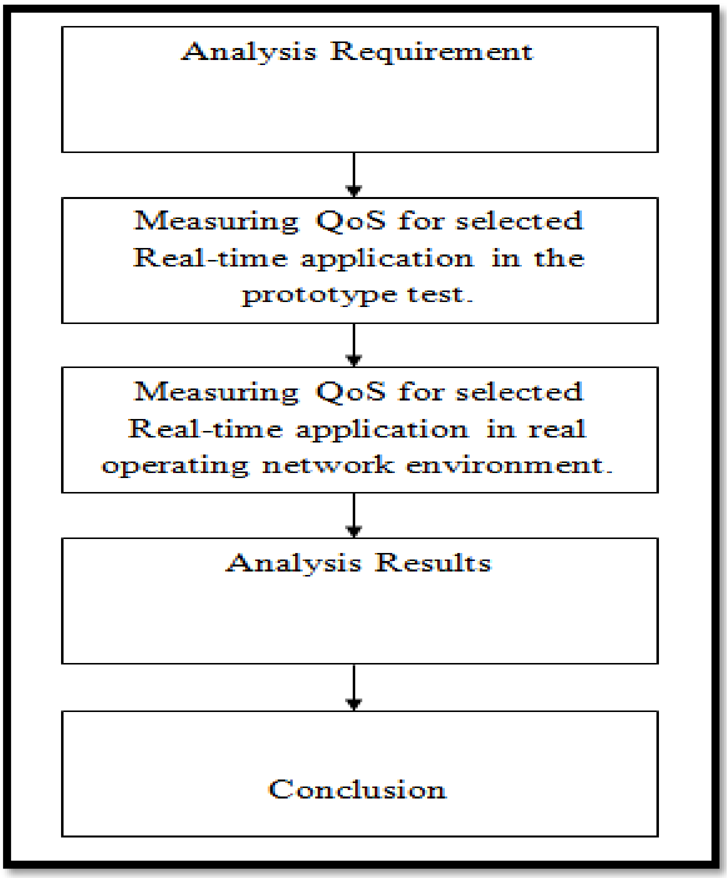

Analysis Requirement
Measuring QoS for selected Real-time application in the prototype test.
Measuring QoS for selected Real-time application in real operating network environment.
Analysis Results
Conclusion

Figure (3-1): Research Framework

3.3Analysis Requirement:

For analysis real time traffic there is a need to use various and different testbeds , tools (to generate and analysis traffic) and to select appropriate performance metrics.

3.3.1 Network Testbeds:

Two scenarios of IP network are evaluated by the same networks type topology. The first scenario based on the IPv6 configuration, the second scenario based on IPv4 configuration. When evaluating an IPv4 network, the IPv6 network is disabled. This means that the network is guaranteed from end-to-end IPv4 network. When evaluating an IPv6 network, the IPv4 network is disabled. This means that the network ensures either end-to-end IPv6 or end-to-end IPv4 network.

- The selected testbeds are:
  - Prototype test network.
  - Ideal operating environment “controlled”.
  - Real operating network environment (Sudan University).
  - Real operating network environment (University of Khartoum).

3.3.2 Tools:

Two traffic tools are Chosen:

- Phonerlite application: It is a clearly arranged application for Windows. It enables PC to be used for Internet telephony (VoIP) Voice over IP. And has the ability to support both versions of IP (IPv4 & IPv6). It is freeware; but it is not open source [24].

  It is used to generate voice data between client’s hosts over IP (IPv4/IPv6) network by using headsets, RTP/UDP/IP port 5060, and standard voice compressing codecs (opus, G.711 A-law, G.711 U-law, G.726-32, GSM, i LBC, Speex, Speex WB, G.722 WB, DTMF (OOB)). The bit rate is 64Kbit/s. User in phonerlite is configured as (sip:SIPPER@[IPv6]) for IPv6 networks “EX: sip:SIPPER@[2C0F:2000::1]” and it is configured as (sip:SIPPER@IPV4) for IPv4 networks “EX: sip:SIPPER@192.168.1.21”.

- Wireshark application is a network packet analyzer. It is free and open source software project, and is released under the GNU General Public License (GPL) [25]. It is used to analyze real time “VOIP” traffic behavior.

3.3.3 Performance Metrics:

Factors such as packet delay, jitter and packet loss can noticeably affect the quality of User Datagram Protocol (UDP) based services such as VOIP and video streaming.

- Delay, Jitter and packet loss Test:

Delay, jitter and packet loss tests are made by using wireshark application to find out the delay, jitter and packets loss of IP (IPv4/IPv6) network between clients. The wireshark tests are run over the packet sizes for a standard Ethernet MTU (1500 Byte). The clients will generate different packet sizes over UDP/IP (IP4/IPv6) for time 4 minutes and repeat the test ten times. After each successful run the received data is analyzed by using wireshark.

3.4 Prototype test implementation:

The initial test network is designed and implemented by using two clients running windows 7and a switch device.

The network topology of IP (IPv4/IPv6) and the connections of clients is shown in figure (3-2).

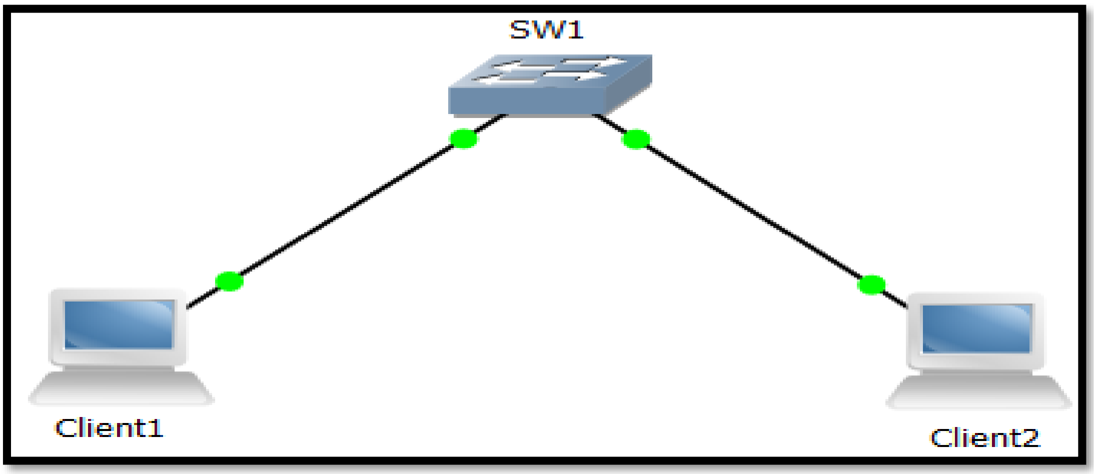


Figure (3-2): The proposed Network IP (IPv4/IPv6) prototype test.

3.5 Test in real operating network environment

3.5.1 Ideal network environment (Suda CAD Academy 'controlled')

- Real time (VOIP) performance over IP (IPv4/IPv6):

The IP (IPv4/IPv6) network is evaluated using proposed lab network. The lab topology of IP(IPv4/IPv6) network is designed and implemented using two Clients running windows 7, Cisco 1841 router " IOS 12.4", two switches Cisco Catalyst 2960 (layer 2) " IOS 12.2" and switch Cisco Catalyst 3560 (layer 3) " IOS 12.2",.

The network topology of IPv4 scenario and the connections of clients is shown in figure (3-3).

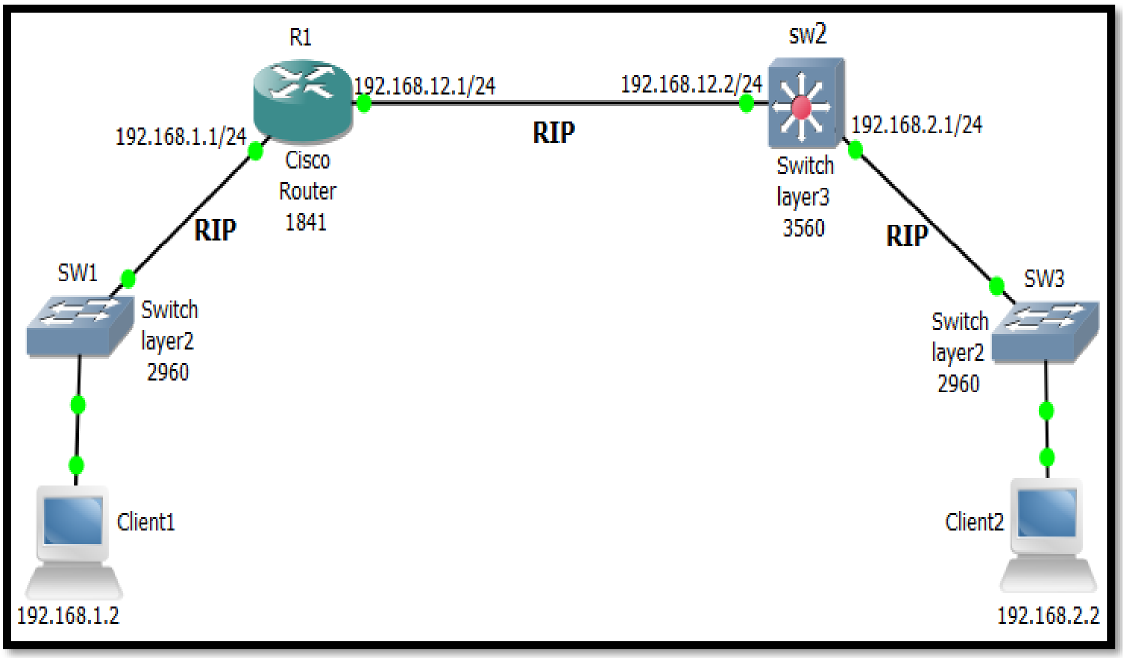


Figure (3-3): The proposed Network of Ipv4 Scenario ‘Suda CAD Academy’

The network topology of IPv6 scenario and the connections of clients are shown in figure (3-4).

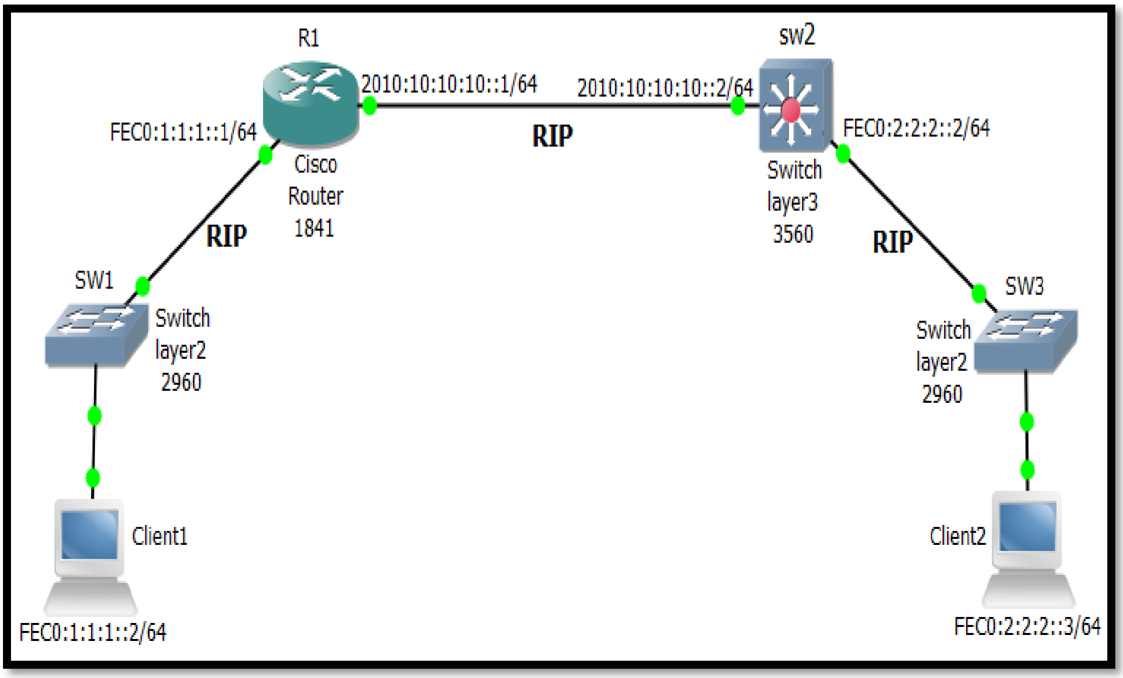


Figure (3-4): The proposed Network of Ipv6 Scenario ‘Suda CAD Academy’.

3.5.2 Real operating network environment (Sudan University):

The IP (IPv4/IPv6) is evaluated using a subnet of Sudan University of Science and Technology (SUST) network. The Tarffic is captured from Laser Building “Data Center Office” to Faculty of Computer Science Building “Western Server Office”. The traffic from client1 to client2 consists of 2 Clients with windows 7, two switches (layer 2) and switch (layer 3).

The network topology from client1 to client2 and the connections is shown in figure (3-5).

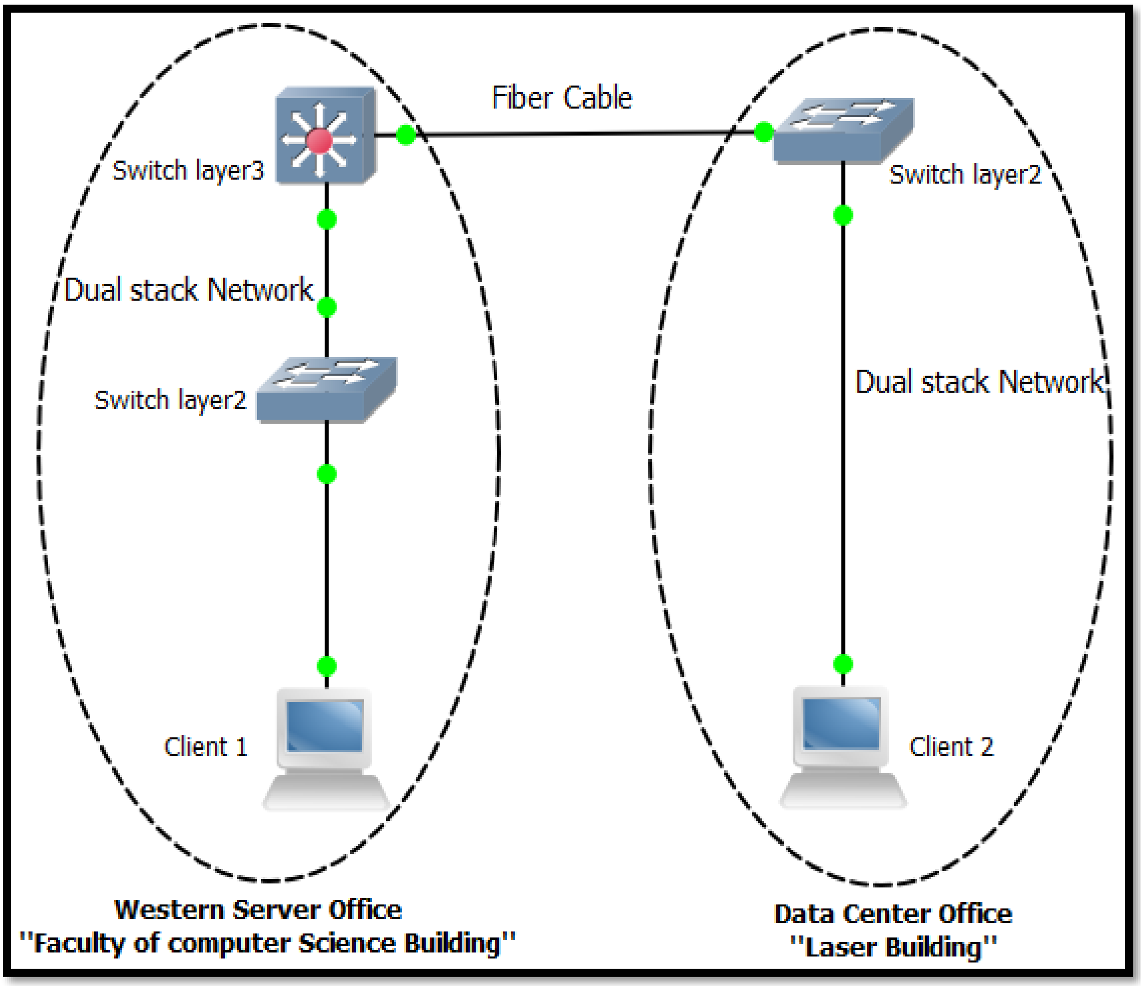


Figure (3-5): The Network of Ipv4 Scenario from Client1 to Client2 ‘Sudan University’.

3.5.3 Real network environment (University of Khartoum):

The IP (IPv4/IPv6) network is evaluated using a subnet of University of Khartoum network. The Traffic is captured from SudREN Office to University of Khartoum Office. The traffic from client1 to client2 consists of two Clients with windows 7, Firewall and Cisco Router (7200).

The network topology from Client1 to Client2 and the connections is shown in figure (3-6).

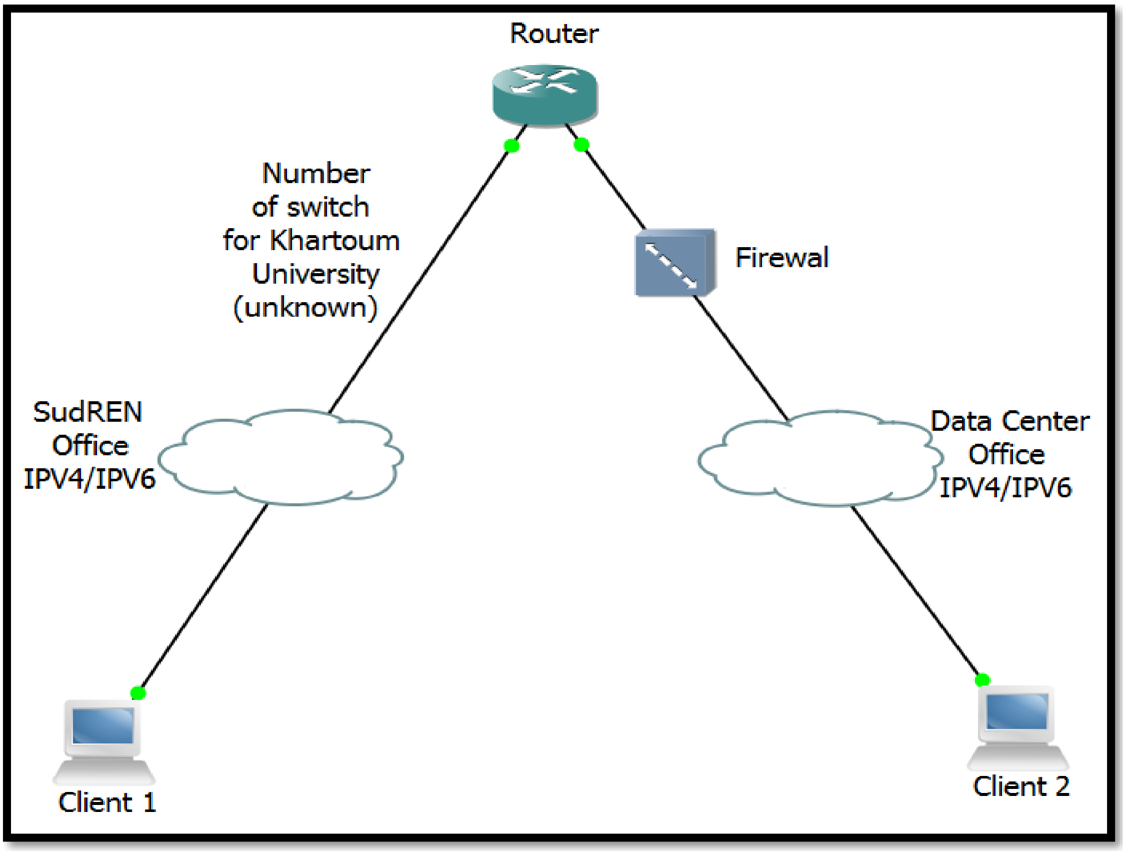

Router
Number of switch for Khartoum University (unknown)
Firewal
SudREN Office IPV4/IPV6
Data Center Office IPV4/IPV6
Client 1
Client 2

Figure (3-6): The Network topology from Client1 to Client2 'Khartoum University'

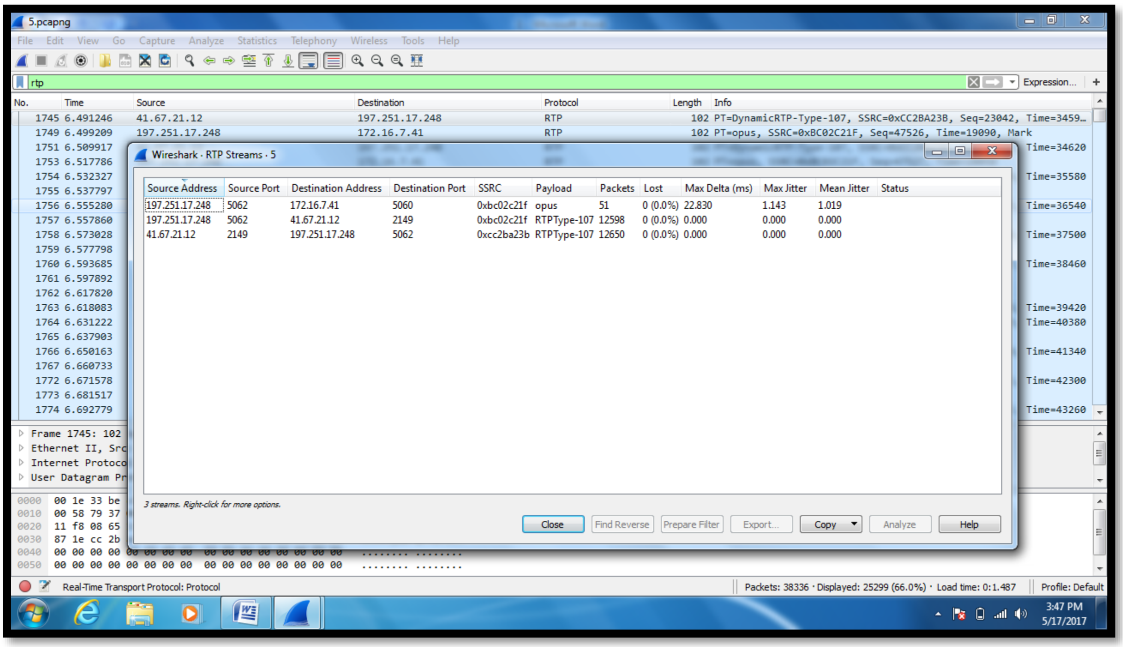
3.6 Analysis Results:

The analysis is done in two phases; wireshark application is used to calculate QoS metrics and Excel 2007 is used to calculate the average of metrics.

a) Wireshark analysis

Figure 3.12 shows snapshot of wireshark application . The following subsection describes each step of the research framework.

The interface appears; calculations of delay, jitter and packet loss in it. “Note: Delta= Delay”.


5.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
rtp
Expression…
+

```
No.       Time        Source            Destination       Protocol   Length  Info
     1745 6.491246    41.67.21.12       197.251.17.248    RTP           102  PT=DynamicRTP-Type-107, SSRC=0xCC2BA23B, Seq=23042, Time=3459…
     1749 6.499209    197.251.17.248    172.16.7.41       RTP           102  PT=opus, SSRC=0xBC02C21F, Seq=47526, Time=19090, Mark
     1751 6.509917                                                                                                            Time=34620
     1753 6.517786
     1754 6.532327                                                                                                            Time=35580
     1755 6.537797
     1756 6.555280                                                                                                            Time=36540
     1757 6.557860
     1758 6.573028                                                                                                            Time=37500
     1759 6.577798
     1760 6.593685                                                                                                            Time=38460
     1761 6.597892
     1762 6.617820
     1763 6.618083                                                                                                            Time=39420
     1764 6.631222                                                                                                            Time=40380
     1765 6.637903
     1766 6.650163                                                                                                            Time=41340
     1767 6.660733
     1772 6.671578                                                                                                            Time=42300
     1773 6.681517
     1774 6.692779                                                                                                            Time=43260
```

```
▷ Frame 1745: 102
▷ Ethernet II, Src
▷ Internet Protoco
▷ User Datagram Pr
```

```
0000  00 1e 33 be
0010  00 58 79 37
0020  11 f8 08 65
0030  87 1e cc 2b
0040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0050  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
```

Wireshark · RTP Streams · 5

Source Address	Source Port	Destination Address	Destination Port	SSRC	Payload	Packets	Lost	Max Delta (ms)	Max Jitter	Mean Jitter	Status
197.251.17.248	5062	172.16.7.41	5060	0xbc02c21f	opus	51	0 (0.0%)	22.830	1.143	1.019	
197.251.17.248	5062	41.67.21.12	2149	0xbc02c21f	RTPType-107	12598	0 (0.0%)	0.000	0.000	0.000	
41.67.21.12	2149	197.251.17.248	5062	0xcc2ba23b	RTPType-107	12650	0 (0.0%)	0.000	0.000	0.000	

3 streams. Right-click for more options.

Real-Time Transport Protocol: Protocol

Packets: 38336 · Displayed: 25299 (66.0%) · Load time: 0:1.487

Profile: Default

Figure (3-7): calculations of delay, jitter and packet loss in wireshark.

b) Excel 2007:

Excel 2007 used to calculate the average for each scenario and to drawing the graph for all tests in each scenario.

4. Result and Discussion

4.1 Overview

This chapter covers practical results of QoS for real time “VOIP” traffic which is represented in delay, jitter, and packet loss for different packets payload sizes over IP (IPv4/IPv6). The result of wireshark application shows that the payload size has delay, jitter and packet loss. The obtained results are organized in tables and plotted into graphs to show the performance of real time traffic over IPv4 and IPv6.

4.2 Results:

The networks types that are shown in chapter 3 are used to record experiments.

4.2.1 Result of Prototype network:

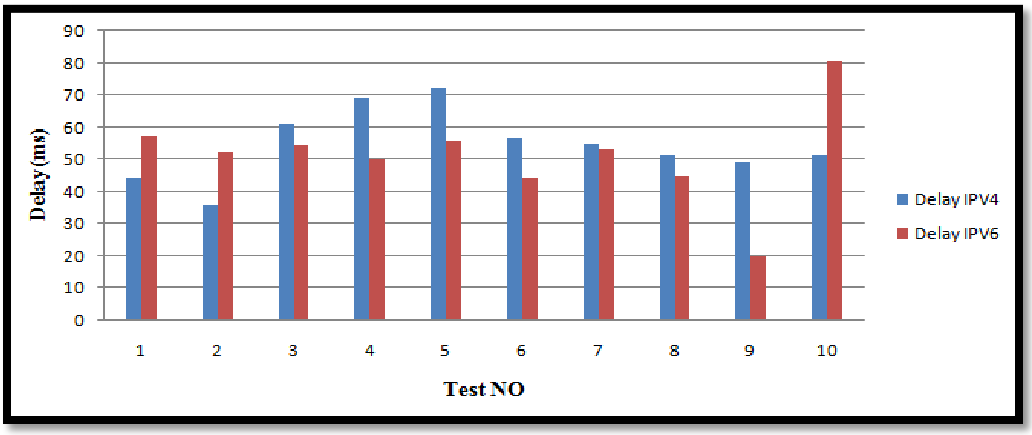
Figure (3-2) in chapter 3 will be used to monitor the results shown in the table (4-1).

Table 4-1: Delay, Jitter and packet loss over IP (IPv4/IPv6) by using wireshark application”Prototype test network”.

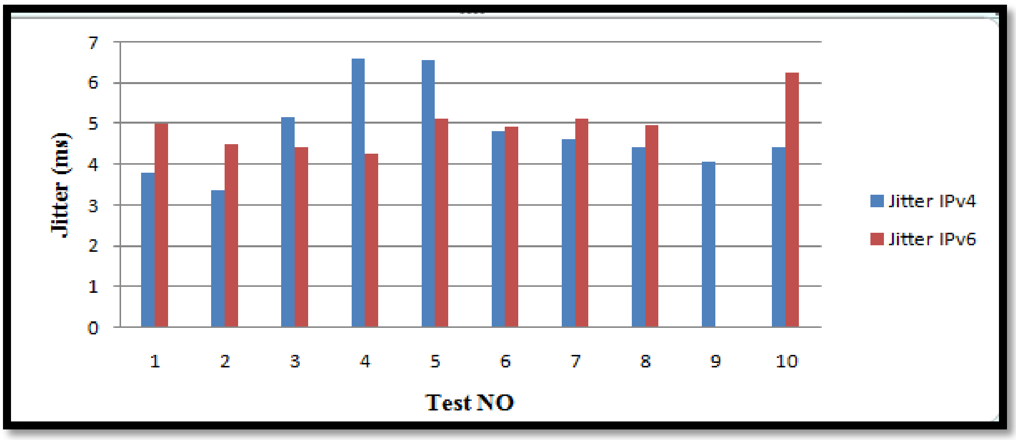
Test	Delay		Jitter		Packet loss	
-No	IPv4	IPv6	IPv4	IPv6	IPv4	IPv6
1	44.475 ms	57.091 ms	3.806	5	0(0.0%)	0(0.0%)
2	35.837 ms	52.318 ms	3.38	4.506	0(0.0%)	0(0.0%)
3	61.262 ms	54.636 ms	5.176	4.432	0(0.0%)	0(0.0%)
4	69.37 ms	50.15 ms	6.593	4.287	0(0.0%)	0(0.0%)
5	72.12 ms	55.963 ms	6.58	5.136	0(0.0%)	0(0.0%)
6	56.727 ms	44.315 ms	4.834	4.924	0(0.0%)	0(0.0%)
7	54.939 ms	53.301 ms	4.646	5.149	0(0.0%)	0(0.0%)
8	51.412 ms	44.828 ms	4.431	4.977	0(0.0%)	0(0.0%)
9	49.398 ms	20.017 ms	4.091	0.039	0(0.0%)	0(0.0%)

10	51.44 ms	80.473 ms	4.417	6.265	0(0.0%)	0(0.0%)
Ave	**54.698**	**51.3092**	**4.7954**	**4.4715**	**0**	**0**

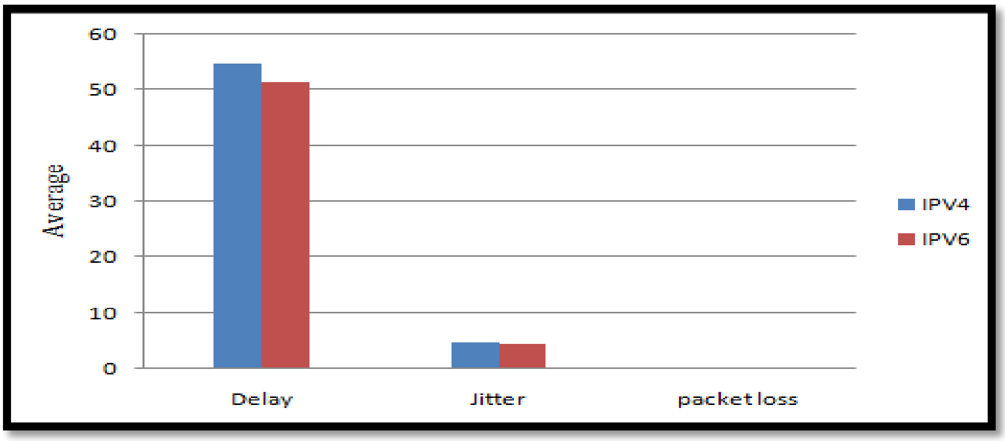
According to practical results of delay, jitter, and packets loss that are shown in tables (4-1); delay, jitter, and packets loss test for different packet payload sizes over IPv4 and IPv6 networks can be illustrated in figures (4-1). IPv4 represented in blue, IPv6 represented in red.



(A) Delay.



(B) Jitter.



(C) Average of Delay, Jitter and Packet loss.

Figure (4-1) the comparison of Delay, Jitter and packet loss of real time traffic over IP (IPv4/IPv6) for Prototype test Network.

In Figure (4-1): 'A and B' we observe that in most sessions, IPv4 has higher Delay and higher Jitter than IPv6. In 'C'; IPv4 has higher average Delay and higher average Jitter than IPv6; the reason we used just layer2. At layer2 unique identification is done via physical addressing scheme. There is no packet loss because we used ideal network.

4.2.2 Result of Ideal network (controlled):

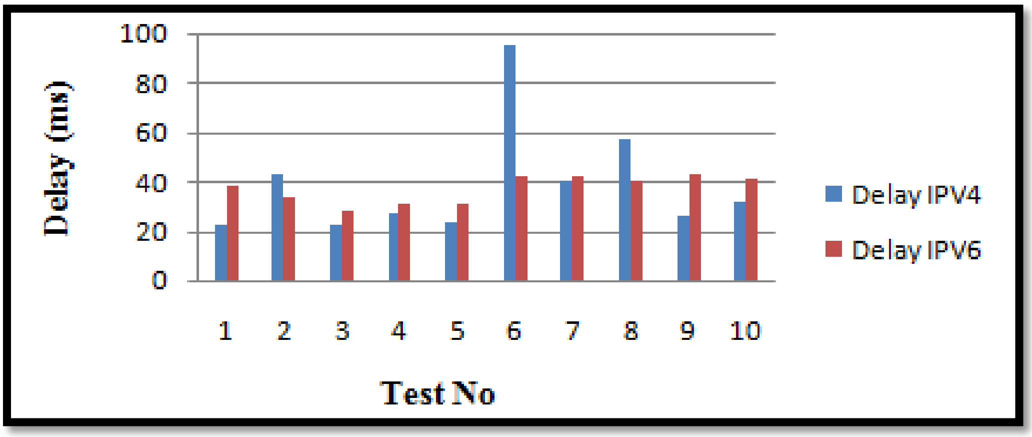
Figure (3-3) and (3-4) in chapter 3 will be used to monitor the results shown in the table (4-2).

Table 4-2: Delay, Jitter and packet loss over IP (IPv4/IPv6) by using wireshark application "Ideal network".

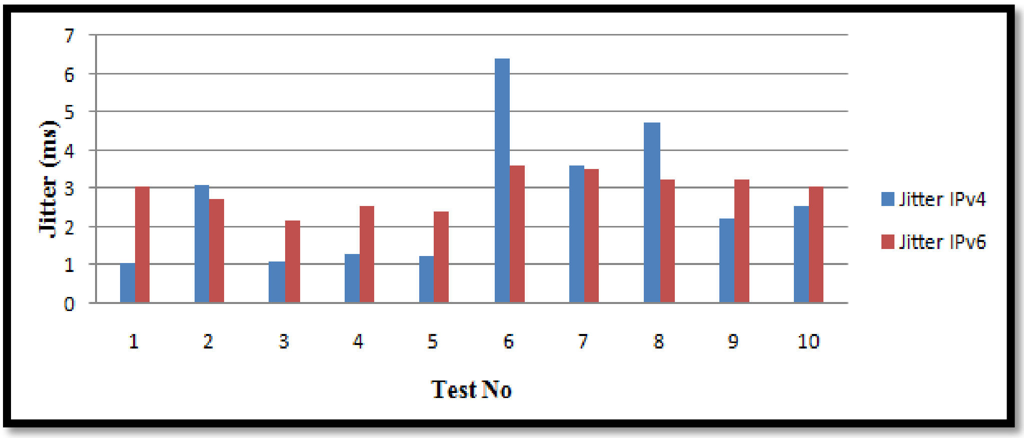
Test -No	Delay		Jitter		Packet loss	
	IPv4	IPv6	IPv4	IPv6	IPv4	IPv6
1	22.847 ms	38.567 ms	1.089	3.080	0(0.0%)	0(0.0%)
2	43.076 ms	33.904 ms	3.118	2.741	0(0.0%)	0(0.0%)
3	23.004 ms	27.874 ms	1.124	2.156	0(0.0%)	0(0.0%)
4	27.066 ms	31.289 ms	1.289	2.565	0(0.0%)	0(0.0%)
5	23.309 ms	31.261 ms	1.257	2.400	0(0.0%)	0(0.0%)
6	95.494 ms	41.838 ms	6.395	3.617	0(0.0%)	0(0.0%)

7	40.310 ms	42.645 ms	3.615	3.518	0(0.0%)	0(0.0%)
8	57.219 ms	40.580 ms	4.746	3.250	0(0.0%)	0(0.0%)
9	25.943 ms	43.181 ms	2.225	3.249	0(0.0%)	0(0.0%)
10	31.752 ms	41.697 ms	2.559	3.072	0(0.0%)	0(0.0%)
Ave	**32.7**	**36.8**	**2.3**	**2.9**	**0**	**0**

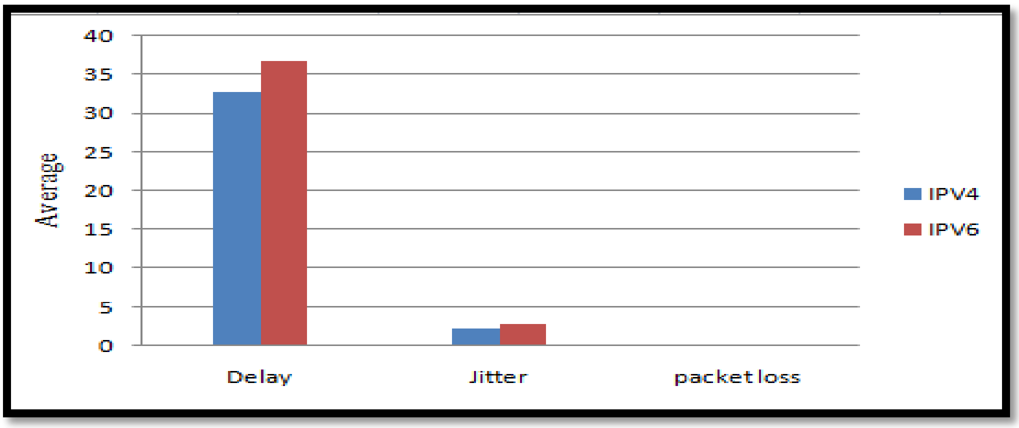
According to practical results of delay, jitter, and packets loss that are shown in tables (4-2); delay, jitter, and packets loss test for different packet payload sizes over IPv4 and IPv6 networks can be illustrated in figures (4-2).



(A) Delay.



(B) Jitter.



(C) Average of Delay, Jitter and Packet loss.

Figure (4-2) the comparison of Delay, Jitter and packet loss of real time traffic over IP (IPv4/IPv6) for Ideal network ”controlled”.

In Figure (4-2): ‘A and B’ we observe that in most sessions, IPv6 has higher Delay and higher Jitter than IPv4. In ‘C’; IPv6 has higher average Delay and higher average Jitter than IPv4. There is no packet loss because we used ideal network.

Note:

(When calculating the average; session 6 reading could not be taken due is considered an abnormal reading compared to reading the most of the sessions. This is because of a network error.).

4.2.3 Result of real operating network environment:

A) SUST:

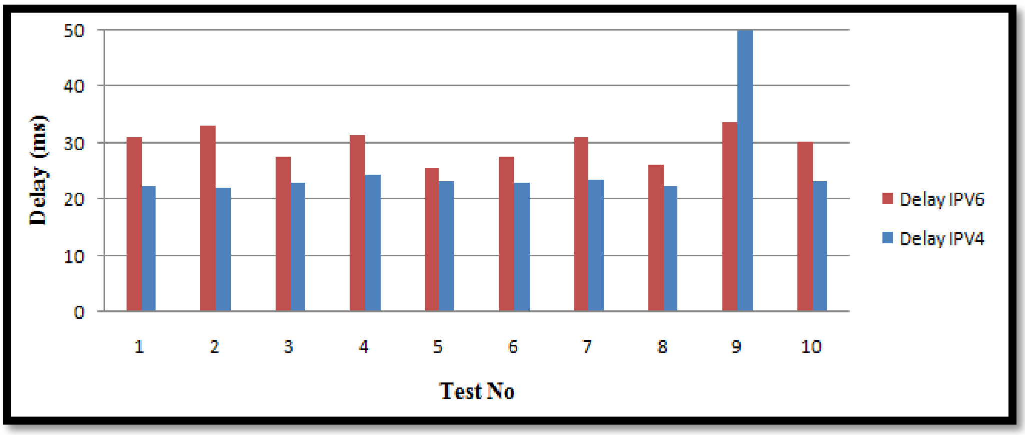
Figure (3-5) in chapter 3 will be used to monitor the results shown in the table (4-3).

Table (4-3): Delay, Jitter and packet loss over IP (IPv4/IPv6) by using wireshark application ”Sudan university network”.

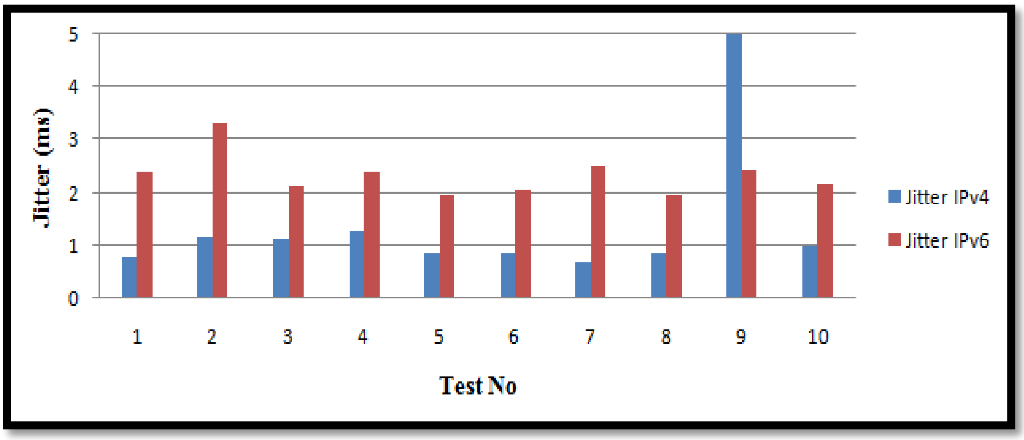
Test -No	Delay		Jitter		Packet loss	
	IPv4	IPv6	IPv4	IPv6	IPv4	IPv6
1	22.227 ms	31.002 ms	0.788	2.406	0(0.0%)	1(0.0%)

2	22.105 ms	33.003 ms	1.162	3.306	0(0.0%)	0(0.0%)
3	22.795 ms	27.487 ms	1.127	2.120	0(0.0%)	0(0.0%)
4	24.265 ms	31.447 ms	1.258	2.394	0(0.0%)	0(0.0%)
5	23.343 ms	25.623 ms	0.866	1.942	1(0.0%)	0(0.0%)
6	22.999 ms	27.673 ms	0.849	2.058	----	0(0.0%)
7	23.361 ms	31.002 ms	0.688	2.501	0(0.0%)	0(0.0%)
8	22.376 ms	25.966 ms	0.834	1.942	0(0.0%)	0(0.0%)
9	1354.027 ms	33.647 ms	84.279	2.426	1(0.0%)	0(0.0%)
10	23.268 ms	30.243 ms	0.994	2.155	0(0.0%)	0(0.0%)
Ave	**22.97**	**29.27**	**0.95**	**2.31**	**0**	**0**

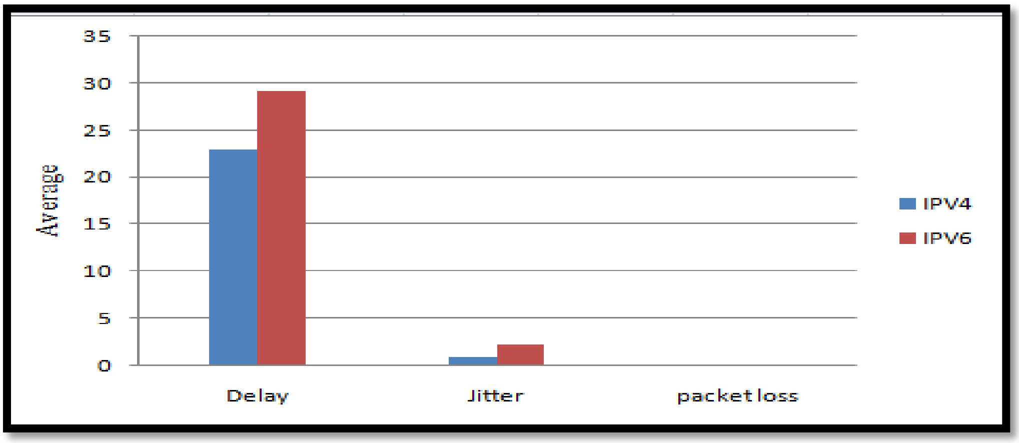
According to practical results of delay, jitter, and packets loss that are shown in tables (4-3); delay, jitter, and packets loss test for different packet payload sizes over IPv4 and IPv6 networks can be illustrated in figures (4-3).



(A) Delay.



(B) Jitter.



(C) Average of Delay, Jitter and Packet loss.

Figure (4-3) the comparison of Delay, Jitter and packet loss of real time traffic over IP (IPv4/IPv6) for Sudan university network.

In Figure (4-3): ‘A and B’ we observe that in most sessions, IPv6 has higher Delay and higher Jitter than IPv4. In ‘C’; IPv6 has higher average Delay and higher average Jitter than IPv4. There is no packet loss because distance from client 1 to client 2 is small.

Note:

- Session 6 packet loss reading could not be taken due to an error occurred in wireshark.

- When calculating the average; session 9 reading could not be taken due is considered an abnormal reading compared to reading the most of the sessions. This is because of a network error.

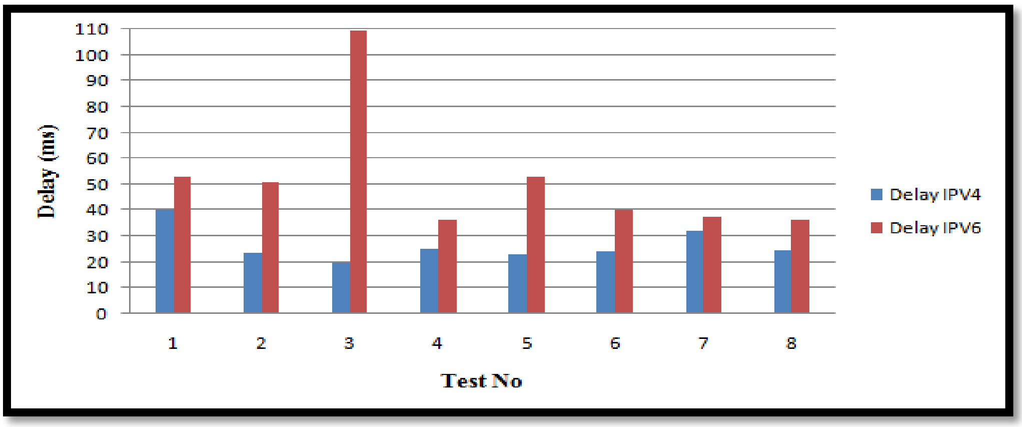
B) U of K and SudREN:

Figure (3-6) in chapter 3 will be used to monitor the results shown in the table (4-4).

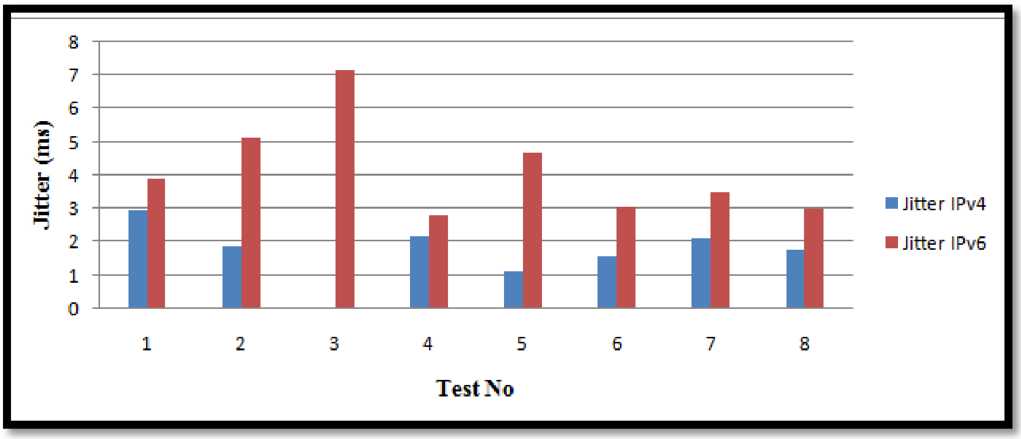
Table (4-4): Delay, Jitter and packet loss over IP (IPv4/IPv6) by using wireshark application ”university of Khartoum network”.

Test -No	Delay		Jitter		Packet loss	
	IPv4	IPv6	IPv4	IPv6	IPv4	IPv6
1	39.973 ms	52.957 ms	2.968	3.900	13(0.1%)	0(0.0%)
2	23.521 ms	51.076 ms	1.863	5.160	2(0.0%)	2(0.0%)
3	20.023 ms	109.559 ms	0.009	7.165	2(0.0%)	24(0.2%)
4	25.207 ms	36.339 ms	2.157	2.802	79(0.6%)	16(0.1%)
5	22.830 ms	53.070 ms	1.143	4.712	0(0.0%)	0(0.0%)
6	24.124 ms	39.928 ms	1.563	3.042	0(0.0%)	0(0.0%)
7	32.182 ms	37.621 ms	2.142	3.514	0(0.0%)	0(0.0%)
8	24.410 ms	36.335 ms	1.803	3.004	0(0.0%)	0(0.0%)
Ave	**26.53**	**52.11**	**1.71**	**4.16**	**0.09**	**0.05**

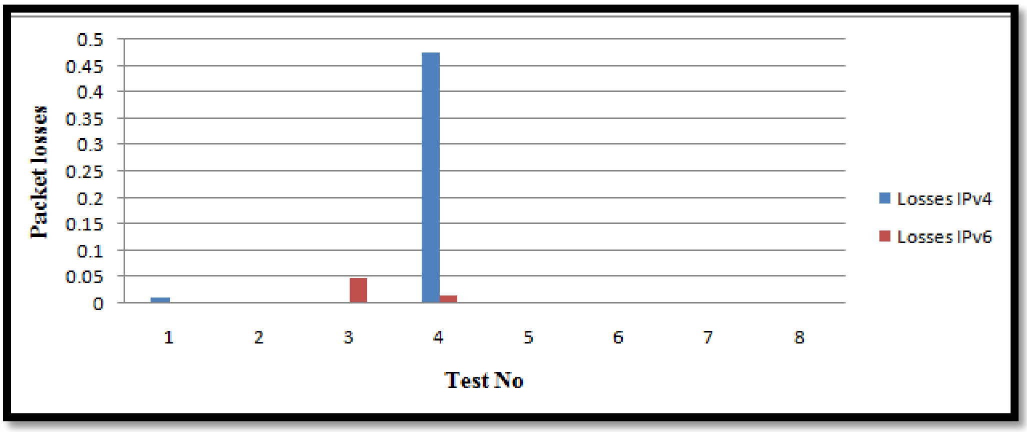
According to practical results of delay, jitter, and packets loss that are shown in tables (4-4); delay, jitter, and packets loss test for different packet payload sizes over IPv4 and IPv6 networks can be illustrated in figures (4-4).



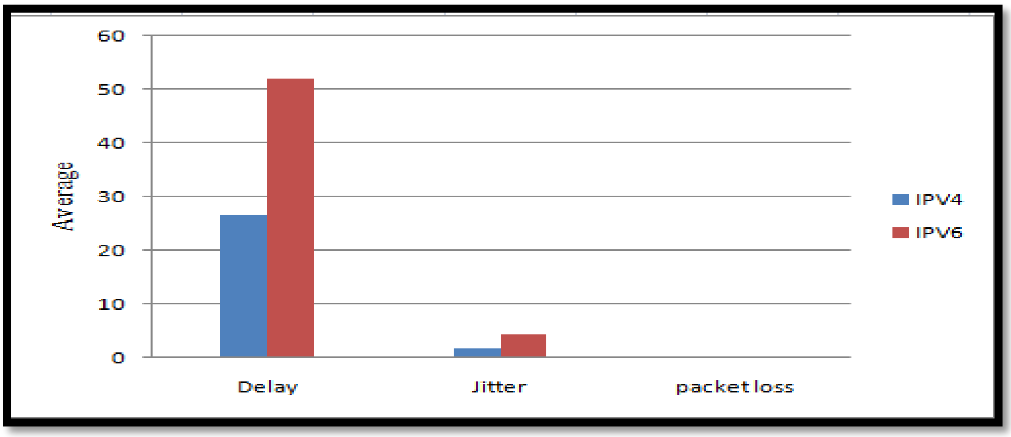
(A) Delay.



(B) Jitter.



(C) Packet loss



(D) Average of Delay, Jitter and Packet loss.

Figure (4-4) the comparison of Delay,Jitter and packet loss of real time traffic over IP (IPv4/IPv6) for university of Khartoum network.

In Figure (4-4): ‘A and B’ we observe that IPv6 has higher Delay and higher Jitter than IPv4. In ‘D’; IPv6 has higher average Delay and higher average Jitter than IPv4. In ‘C’ IPv4 has high packet loss than IPv6.

We conclude IPv6 has a higher Delay and higher Jitter than IPv4. That is probably because IPv4 has a lower overhead than IPv6 therefore take less bandwidth to send the payload (The data).

Packet sent in an IPv4 environment is smaller than packet sent in an IPv6 environment. This is because IPv6 header is larger than that of IPv4. IPv4 header size is 20 bytes, while IPv6 header is 40 bytes.

5.1 Conclusions:

Two network scenarios called IPv4 network and IPv6 network have been configured in different networks topology. Despite of the many benefits offered by IPV6, the results demonstrates that real time voice traffic over IPv4 network had a lower delay than IPv6 network. The Jitter outcome shows that the IPv4 network had a lower Jitter than IPv6 network. That is probably because IPv4 has a lower overhead than IPv6 therefore take less bandwidth to send the payload (The data).

Packet sent in an IPv4 environment is smaller than packet sent in an IPv6 environment. This is because IPv6 header is larger than that of IPv4. IPv4 header size is 20 bytes, while IPv6 header is 40 bytes.

The Packet loss analysis indicates that IPv6 produced least amount of packet loss compared to the IPv4 network.

5.2 Recommendations for Future Work:

For more accurate results of real time traffic :

1\ The tests can be performed on a number of applications instead of using the phonerlite application only.

2\ The traffic of real time passes over more number of Routers between the hosts over the IP (IPv4, IPv6) networks .

References:-

[1] E.Musbah 1, Kh.Bilal 2, A.Babiker A./N.Mustafa , Comparison of QoS Performance over WLAN, VoIP4 and VoIP6, International Research Journal of Management, IT and Social Sciences, pp(42 – 52),November 2015.

[2] M Natarajan, Multimedia and Data Transfer Technology: The Challenges and Delivery, DESIDOC Bulletin of Information Technology , Vol. 23, No.4, July 2003, pp. 19-26.

[3] Voice over IP, Wikipedia the free encyclopedia**,** last modified on 30 April 2017, at 00:09, available in https://en.wikipedia.org/wiki/Voice_over_IP.

[4] IPV4, Wikipedia the free encyclopedia**,** last modified on 27 December 2016, at 09:15, available in https://en.wikipedia.org/wiki/IPv4.

[5] A short introduction to IP Addresses, available: (https://www.paessler.com/support/kb/questions/50).

[6] IPv4 Address Report (This report generated at 28-Dec-2016 08:18 UTC).

[7] IP V6 Header**,** Taken from http://www.microsoft.com/windows2000/docs/ipv6.doc , available in http://euclid.nmu.edu/~rappleto/Classes/CS442/Notes/IPv6_Header.html

[8] IPv6 Datagram Packet Structure, mniSecu.com, available in http://www.omnisecu.com/tcpip/ipv6/ipv6-datagram-header-format.php**.**

[9] Comparison between IPv4 Header and IPv6 Header, mniSecu.com, available in http://www.omnisecu.com/tcpip/ipv6/comparison-between-ipv4-header-and-ipv6-header.php.

[10] IPv6 Header Deconstructed, IPV6.com, available in http://www.ipv6.com/articles/general/IPv6-Header.htm.

[11] IPv6 White Paper, 3 COM university.

[12] A.Sh Abdalrahman, Evaluation of Service of Quality of Voice over Internet Protocol, Sudan University of Science and Technology College of Graduate Studies, January 2015.

[13] Survey on Transport Layer Protocols: TCP & UDP, Santosh Kumar, Sonam Rai , International Journal of Computer Applications ,pp 20-25, 7, May 2012.

[14] G.Al-Gadi 1, Dr. A.Babiker A/N.Mustafa 2, A.Al-Gad , Comparison Between Ipv4 And Ipv6 Using Opnet Simulator , IOSR Journal of Engineering

(IOSRJEN) , pp (44-50), 8 August 2014.

[15] P.Bali, a Detail Comprehensive Review on IPv4-to-IPv6 Transition and Co-Existence Strategies, International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), pp (1429- 1432) , 4 April 2015.

[16] A.N Abu Ali, Comparison study between IPV4 & IPV6, International Journal of Computer Science Issues (IJCSI), pp (314-317), 1 May 2012.

[17] A.M Kapashi , Dr. A.Babiker A/ N.Mustafa Dr: G.Els Ibrahim, Performance Evaluation of IPv4 Vs Ipv6 and Tunnelling Techniques Using Optimized Network Engineering Tools (OPNET) , IOSR Journal of Computer Engineering (IOSR-JCE), PP (72-75) , Jan – Feb. 2015.

[18] Cebrail C¸ ˙IFL˙IKL˙I, Ali GEZER∗, Abdullah Tuncay ¨OZS¸AH˙IN , Packet traffic features of IPv6 and IPv4 protocol traffic , Turk J Elec Eng & Comp Sci , pp(727 – 749) , 25.08.2010 .

[19] Dr. M.Elg Mustafa , The Effect of IPv4 and IPv6 over Network and Application Servers Load and Delay , International Journal of Engineering and Technical Research (IJETR) , pp (227 – 230) , 3 March 2015.

[20] M.E Mustafa , Comparison between OSPFv3 and OSPFv2 , Creative Commons Attribution International License (CC BY), pp (43 – 48) , 11 March 2014 .

[21] J.L Shah , Next Generation Internet Protocol A Survey on Current Issues and Migration , International Journal of Computer Science and Mobile Computing , PP(490- 496) , 1 January- 2015 .

[22] Emre Durdag , Ali Buldu, IPV4/IPV6 security and threat comparisons , Procedia Social and Behavioral Sciences ,pp (5285–5291), 25 January 2010 .

[23] A.M Aslam Sujah, H.M Shadir, M.S.M Shakir, K. Jasandan, S. Kavitha, Dhishan Dhammearatchi ,Hacking Techniques in IPV6 Networks and Prevention Machanisams , International Journal of Scientific and Research Publications , pp (373-377) , 4 April 2016.

[24] phonerlite, available in http://phonerlite.de/index_en.htm .

[25] Chapter 1. Introduction to wireshark, available in https://www.wireshark.org/docs/wsug_html_chunked/ChapterIntroduction.html#ChIntroWhatIs.