The effects of Security mechanisms on VoIP communication Quality of Service

by

Macdonald Mauye (R122032F)

Submitted in partial fulfilment for the degree of

BSC (HONS) TELECOMMUNICATIONS

Department of Applied Physics &Telecommunications in the Faculty of Science & Tech.

Midlands State University

Gweru, Zimbabwe

November 2015

Supervisor: Dr. A Nechibvute

[HTEL 438 Dissertation]

CHAPTER 1

INTRODUCTION

1.1 Background

Voice over Internet Protocol (VoIP) is one of the most important technologies in the world of communication.Mass business sector VoIP telephony started in 2004 with the presentation of VoIP calling arrangements which allowed endorsers of make calls generally as they would with traditional phone organization administrations [1]. VoIP is the steering of voice conversation over the Internet or some other IP-based system [2]. The voice information streams over a broadly useful parcel exchanged system, rather than customary devoted circuit-exchanged voice transmission lines.Lower phone bills, virtual offices, centralized management, rapid deployment, toll bypass, network consolidation and service convergence are a few of its benefits [3]. System union that is network consolidation empowers the transmission of information, voice, and video over than one single system [3].

The reconciliation enormously diminishes setup and upkeep costs. The conventional phone system POTS (Plain Old Telephone Service) or the PSTN (Public Switched Telephone Network) was excessive and was overseen by just a couple organizations and inefficiently [3].VoIP deployments capitalize on the inefficiency andare increasing steadily [4]. To transport voice over a data network, the human voice must be “packetized”. Voice packetization involves appending headers with routing information to thevoice data. Multiple voice samples are combined into packets and the voice packets areswitched and sent though the network one-by-one[5]. The process ofpacketization compresses the callers’ voice signal, transfers it over the IP network and it isthen decompressed at the other end[6].

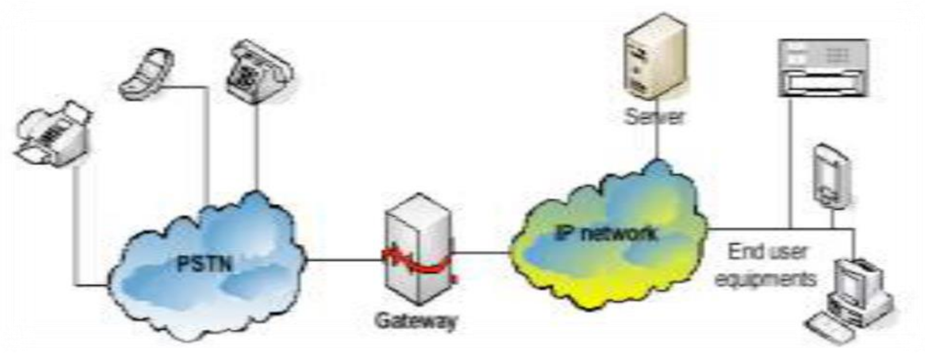


Fig. 1.1: A general VoIP network [2]

The major components of a general VoIP network are illustrated in Figure 1.1 [2]. The gateway converts signals from the traditional telephony interfaces to VoIP. The server provides management and administrative functions to support the routing of calls across the network [2].In the process of saving money and increasing efficiency, two crucial portions of any infrastructure, voice and data, were combined thus security threats become more complex and it’s mandatory to carefully consider effective security measures. There are numerous threats to a VoIP network that is the systems administration gadgets, the servers and their working frameworks, the protocols, the phones and their softwares are all vulnerable [2]. The Quality of Service (QoS) necessity of VoIP leaves less working space for conceivable efforts to establish safety. An exceptionally secure VoIP framework that cannot convey great voice quality is not alluring.

1.2 Opportunities and Challenges of VoIP

VoIP as compared to the traditional Public Switching Telephone Network (PSTN) phone systems has numerous advantages. The major advantages being its bandwidth efficiency, cost effectiveness, easy convergence of data and voice network. VoIP uses IP networks that has the flexibility of allocating bandwidth as needed and reserve the unallocated bandwidth for data. Flat rate plans offered by VoIP providers offer an unlimited number of minutes to make calls on both long and short distances thus reduced communication costs of an organization. The flexibility of VoIP in it being integrated with other applications gives rise to the easy of telephony management. The use of VoIP also comes with phone portability as users are provided with number mobility as the number can be used virtually anywhere. As there exists number portability, there is increased mobility since remote workers are allowed the same access as corporate office employees. Convergence of data and voice network allows for use of the same infrastructure and hence also permits going wireless thus reducing cable management. Companies can increase its flexibility while reducing overhead costs as consolidation of voice and data technical staff implies maintaining one maintenance team.

Like any new technology VoIP comes short on certain important aspects the major one being security. As a new technology it has many proprietary standards thus making it difficult to implement security. New complex security threats are also introduced as it's an emerging technology. Power outages may hinder a phone call being made hence VoIP availability is unreliable. The VoIP protocols in use currently offer no physical caller's location to emergency operator services. As with any phone system quality of service must be maintained and with VoIP data travelling over an IP network is susceptible to delay and loss due to routing, network latency and security in place hence there is a major challenge in maintaining a good quality of service.

The results obtained in this research will give an insight into which security architectures greatly affect the VoIP quality of Service (QoS). They will also help into effectively building a converged network for medium enterprises that is cost effective and eliminates redundant hardware, communications facility and support staff.

1.3 Research Purpose and Context

Voice over Internet Protocol (VoIP)   is a set of protocols that enables the internet to be used as a transmission medium for voice calls. Many organizations are opting to implement VoIP for its major advantage of being able to be consolidated on one network with data, reducing costs and resulting inlower system aggregate expense of possession. Nonetheless, numerous directors erroneously expect that since VoIP travels in packets simply like data, existing network structure and tools can be utilized without change yet not just does VoIP acquire all information system security dangers, it presents new vectors for dangers related with the intricate protocols connected with VoIP. These new threat vectors arises the need for a carefully considered and assessed integrated network with the most feasible security in account.

However, implementation of security measures has to be undertaken with great importance as security measures may aid to the depreciation of VoIP quality of service. In many cases companies end up spending more money due to improperly implemented security giving rise to poor quality of service which in turn cripples all business dealings as communication is the backbone of all businesses, thus suffering greater expenses than the intended reduction of expenditure. This background has motivated the current researcher to find the impact of security measures implemented to Quality of Service.

1.3.1 Aim and Objectives

The aim of this project is to research on the impact of securing a VoIP network to Quality of Service offered by the VoIP network.

The main objectives of the project are:

i. To design and simulate a typical network and deploy VoIP technology.
ii. Evaluate specified security measures impact on VoIP Quality of Service (QoS) experimentally.
iii. To deduce ways of decreasing the effects of security mechanism on the QoS.

1.4 Dissertation outline

The report is made up of 5 chapters:

Chapter 1

It is an introduction to the research. It states the issues to be addressed within the report later on.

Chapter 2

It gives the literature review and theoretical aspects. In this chapter, the student will be reviewing current literature done by other scholars. Constructive description of equipment being used in this project is done in this chapter. The chapter also looks at the theoretical aspects; these include the finer detail on the topic being discussed.

Chapter 3

This chapter seeks to explain in detail the methods or the way and steps taken for the project to be carried out.

Chapter 4

Results obtained in the research are analyzed and explained in detail in this chapter. The analysis may involve comparison of other authors' work, expected results and the actual results that were found from doing the project practically.

Chapter 5

This chapter gives the overall analysis and conclusion pertaining the findings from the research. It also encompasses recommendations intended to various stakeholders using and offering the VoIP communication technology.

References

[1] J. B. Meisel and M. Needles, "Voice over Internet Protocol development and public policy implications," pp. 3-15, 2005.

[2] R. M, "IJERST," [Online]. Available: http://www.ijerst.com. [Accessed January 2015].

[3] "Voice Over IP," November 2010. [Online]. Available: http://www.qaddisin.com. [Accessed 26 March 2015].

[4] G. K, "Latency-qos-voice-ip," [Online]. Available: http://www.riverstonenet.com/pdf/qos.pdf. [Accessed 25 March 2015].

[5] F. J. Cobley and A. A. Coward, "Voice over IP versus Voice over Frame Relay," *International Journal of Network Management,* vol. 14, pp. 223-230, 2004.

[6] E. Morris, "IP telephoney ready to explode into the corporate world," *Communications News,* vol. 5, pp. 96-97, 2001.

CHAPTER 2

LITERATURE REVIEW

2.1 Voice over Internet Protocol

Voice over IP (VoIP) is a communication technology allowing voice and multimedia transversal over the internet that is an open or private IP system. VoIP has been an overall innovation since its rise in the late 90s, as a new IP service. The reason for this being its flexibility, low setup costs and services, portability, ability to expand and also its mobility. Despite it having many advantages over the traditional PSTN, the VoIP technology suffers most from challenging issues in terms of security and quality of service (QoS). Its design initially addressed provision of best effort service but the IP network technology cannot support the stringent QoS requirements of voice traffic resulting in QoS problems for voice communications over IP networks.

2.2 Overview of VoIP Technology

VoIP, otherwise called IP Telephony, is the real-time transmission of voice signs utilizing the Internet Protocol (IP) over the public Internet or a private information network [1]. The principal general phone trade was set up in New Haven in 1878. Early phones were rented in sets to endorsers. About the same time the transistor was developed. Dr. Shannon's the inventor formed the basis of the entire digital communications revolution, from cell phones to the Internet.15 years later, in 1963, AT&Tutilized Dr. Shannon's ideas and made "Touchtone" dialing. This advancement of innovation permitted calls to be exchanged digitally and, later, empowered all way of automated menus and usefulness that wiped out the requirement for human administrators [2]. In 1984 home clients were permitted to quit renting their telephones from AT&T and permitted to buy their own telephones.These progressions lead to a rush of new outlines and capacities for the home telephone [3].In 1968 the Internet was initially created by

ARPANET (Advanced Research Projects Agency Network) [1].Developed in the 1970s, and in parallel to the Internet, were time-offer PC systems. In 1989, Tim Berners-Lee and a gathering of specialists at CERN (a global logical association situated in Geneva, Switzerland) madehypertext transfer protocol (HTTP) and a text format code called hypertext markup language [1]. They likewise concocted an all-inclusive asset identifier (later universal resource locator, or URL) to recognize document locations. These developments shaped the establishment of the World Wide Web [2].Although the phone and Internet were essential to the presence of VoIP, another innovation is firmly related, and generally as critical. In 1972 Dr. Vint Cerf was the man who developed Transmission Control Protocol/Internet Protocol (TCP/IP) – the specialized protocol that characterizes the type of net information packets and how they travel to their destinations. From most records, VoIP began in February of 1995 by a little organization in Israel called Vocaltec. It brought to market the first internet phone software called the Internet Phone. The Vocaltec programming compacted the voice signal, made an interpretation of it into digital packets, and conveyed it over the Internet. The innovation arrangement functioned admirably as long as both the guest and the recipient had the same equipment and software. Although sound quality was poor and nowhere near that of conventional equipment at the time [4].

2.2.1 VoIP Fundamentals

VoIP uses an IP or a packet switched network as a transmission medium.A VoIP phone is a device on the user end used to capture the analog voice and converting it into digital packets that are then transmitted across a network. VoIP telephones can change digital packets in analogue voice streams .To perform this transformation and transfer of voice stream a VoIP telephone utilizes particular arrangement of VoIP conventions and voice codecs [5].

VoIP communication typically consists of two phases consisting of different protocols. The first is the signaling protocol and the second is the communication protocol.The flagging stage is for the most part for call setup, for example, acquiring the callee's IP address. After a ring is set, the guest then begins corresponding with the callee over the IP system [6]. The signaling phase is generally for call setup, such as obtaining the callee’s IP address thus establishing a session between the two. After a call is set up, the caller then starts communicating with the callee over the IP network guided by media transport protocol specifying the rules and formats of the actual voice packets [7], thus the communication phase.

A VoIP telephone is a phone set designed particularly for use in a voice over IP (VoIP) framework by changing over standard phone sound into a computerized format that can be transmitted over the Internet, and by changing over approaching digital signals from the Internet to standard phone sound [8].There are generally 3 types of VoIP phones namely PSTN phones, hardphones, and softphones.

(a) PSTN phones

Typically they are not VoIP phones but can however be used to make VoIP Calls with the use of a phone adapter known as (ATA) Analogue Telephone Adapter that converts voice from analogue to digital.

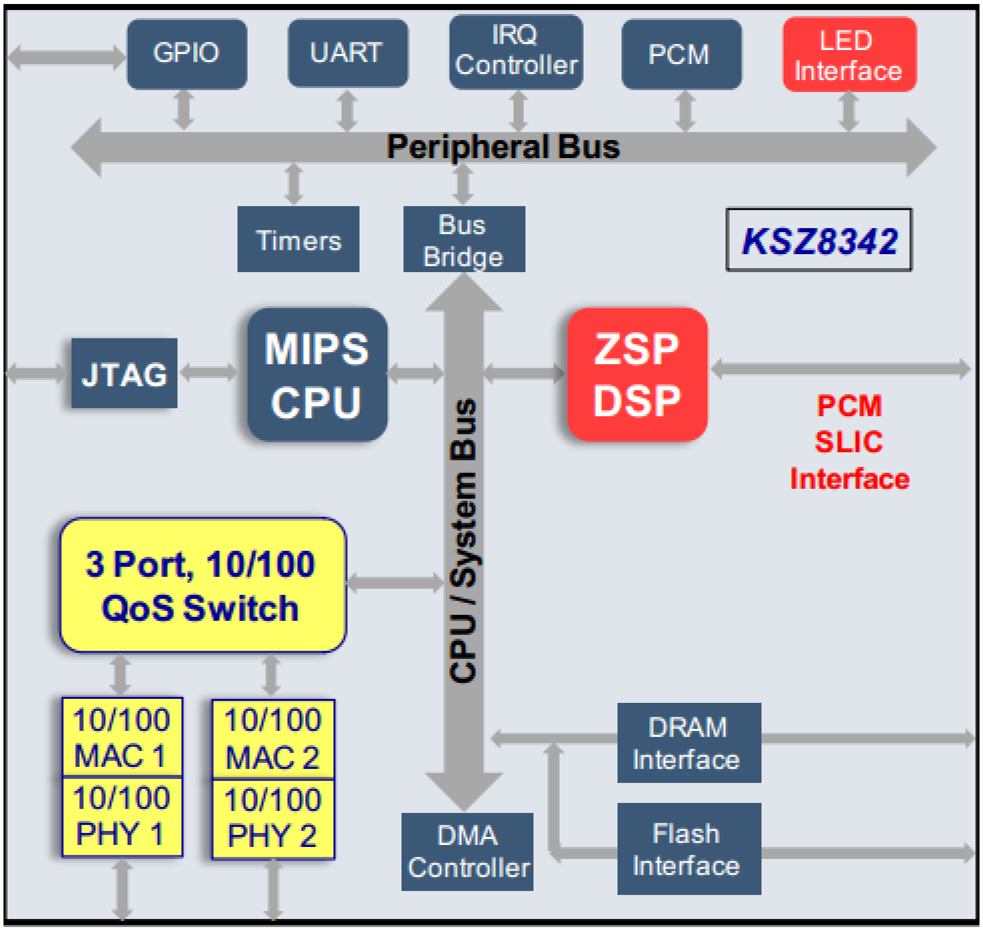


Figure 2.1: A block diagram of the ATA adapter [9].

(b) Hardphone

It’s identical to a PSTN phone but understands IP standards on its own. It does not require an analogue to digital convertor as it can do this on its own. It requires an internet connection. The following are a list of various types of hardphones:

i. Ethernet
ii. cordless
iii. WLAN or Wi-Fi
iv. Voice/video
v. softphone

The term softphone refers to a telephone capability implemented on an ordinary PC, using only special software and a microphone/headset that plugs into the PC’s audio ports [10].Hence a softphone can also be referred to as VoIP phone in form of software.it is able to make computer calls to basic PSTN/IP handsets.

2.2.2 VoIP Services

The VoIP technology is made up of four different distinct services: signaling, encoding, transport, and gateway control [11].A signaling protocol is responsible for controls and call management, it includes elements such as call set up, clear down, and call forwarding. E.g. H.323, SIP, and skinny. During the conversation the audio voice is digitized/encoded into packets which are in turn transmitted over the IP network towards the destination.

(a) Encoding

Since the IP network transmits digitized packets voice in its pure form cannot be transmitted hence there’s need for it to be converted into digital form. A voice codec is used to convert analogue voice into digital and back again, and may compress and decompress the data for more efficient transmission. A codec determines bandwidth usage and quality of voice thus higher quality voice service usually require higher bandwidth. Codecs also enhance the security of packets being transmitted and prevent any unauthorized illegal access [12].Examples of popular audio codecs include G.711, G.729 and G.722 [11].

(b) Transport

The transport protocols carry voice packets generated from the codec. The codec must allow the receiver to detect any losses in packets and also provide timing information [13].There are many mechanisms deployed but RTP is widely used. Real Time Protocol is a protocol that uses source IDs to collect packets from the same source, and it has a field identifying the payload so that the receiver can deduce which codec was used in creating the voice packet [11]. It is a standard to transport real-time audio and video data. Examples of transport protocols includes RTP, RTCP (Real Time Control Protocol), SRTP (Secure Real Time Protocol), and SRTCP (Secure RTCP).

(c) Gateway control

It is used for communication between the separate components of a decomposed VoIP gateway. Decomposed VoIP gateways consists of Media Gateways (MGs) and Media Gateway Controllers (MGC), and appear to the outside as a single VoIP gateway [10].MGs concentrate on the audio signal interpretation capacity, performing transformation between the audio signals carried on phone circuits and data packets transversed over the Internet or other packet networks. A single MGC can control multiple MGs, which leads to cost reductions when deploying larger systems [10].

2.2.3 VoIP Security

As VoIP is a new technology it doesn't have a security standard thus resulting in different security mechanism being deployed on differing VoIP protocols.

(a) Eavesdropping

Because VoIP transmitters voice packets with or without encryption there is a risk of someone listening to the conversation. For this type of attack the unauthorized person has to be between the 2 end points. The attack uses a packet sniffer to capture voice packets and then interpret the meaning[19].

(b) Spoofing

This type of attack has the attacker acting/pretending to be someone he's not. Usually done for toll fraud, gaining access to messages and obtaining private information e.g. PIN numbers. SIP proxy can be accessed and the configuration on call forwarding changed in an attempt to commit toll fraud [19].

(c) Denial of Service

DoS uses 2 types of attacks to collapse the entire VoIP system [14]. The first being sending a lot of distorted or broken packets to flood the system thus making it slow or crashing it. The second involves sending a flood of well-formed packets to exhaust resources[19],[20]. The DoS attack occurs both in the application and or transport layer. At the application layer it floods by sending a bunch of call invitations or registration requests at the signaling channel.

(d) Spam over VoIP

VoIP is vulnerable to spam also known as SPIT (Spam over Internet telephony) [14]. This type of attack can also disable the whole VoIP system. The user receives lot of unwanted calls and also the spam can attack the gateway and degrade the QoS [19].

2.3 VoIP Protocols

These are protocols required to make the VOIP products from different vendors to interoperate. The main focus is on SIP and H.323, which are signaling protocols. The signaling protocols are responsible for setting up a VoIP call, which includes tasks like pinpointing users and negotiating parameters between the end devices. Table 1 below lists the most popular signaling protocols.

Table 2.1: VoIP protocols [7]

Protocol	**Organization**	**Type**
H.323	ITU-T	Signaling
Session Initiation Protocol (SIP)	IETF	Signaling
MGCP	ITU-T	Signaling
Megaco/H.248	ITU-T/IETF	Signaling

2.3.1 H.323 Standard

This is the ITU-T's (International Telecommunications Union) standard that users should abide by while providing VoIP services. This recommendation provides the technical requirements for voice communication over LANs or WANs while giving no guarantee of quality of service (QOS) being provided by LANS [13]. It is often referred to as umbrella standard as it references a number of other standards that support multimedia communications.It was initially created for interactive media conferencing for LANs yet later reached out to Voice over IP. The standard incorporates both point to point interchanges and multipoint conferences.

(a) Components of H.323

H.323 characterizes 4 noteworthy segments to be specific Gateways, terminals, guardians, and multipoint control units (MCUs).

(i)Terminals

These are endpoints that give continuous, two way correspondences. All H.323 terminals need to bolster H.245, Q.931, Registration Admission Status (RAS) and Real Time Protocol (RTP) [13]. H.245 permits the utilization of channels, Q.931 is for ring flagging and set, and RTP is continuous transport convention that conveys voice packets while RAS is for cooperating with the gatekeeper. Examples of terminals incudes IP phones which are telephones with a built in codec and embedded H.323 software, a network interface card (NIC) and a protocol stack [15].Also PC phones which are termed softphones which capitalizes on computer installed software and having on one NIC card dedicated to only processing VoIP packets.

(ii) Gateways

A gateway is an endpoint on the network providing real time, 2-way communications between terminals on the network and other devices on a switched based network or to another gateway.

They provide services that cannot be decentralized and implemented by end points [16]. They translate different transmission formats into the required formats and also between audio and video codecs. Gateways are the interface between the PSTN and the Internet [13].Gateways are discretionary in that terminals in the same neighborhood that is LAN can speak with one another straightforwardly. When they have to correspond with different terminals on an alternate system, then they convey by means of gateways utilizing H.245 and Q.931 protocols.

(iii) Gatekeepers

It's the most vital component of the H.323 system and acts as a manager.it is the central point for all calls within its realm (a realm being the aggregation of the gatekeeper and the endpoints registered with it) and provides services to the endpoints registered. These gatekeepers are an optionally but widely used component of a VoIP network [17].

Some of the gatekeeper's functions are as follows:

i. Address translation where the alias address is translated to the transport address.
ii. Admission control that is granting access or denying access based on call authorization, source and destination address or some other criteria.
iii. Call signaling where it may decide to finish a call motioning with the endpoints and may handle the call signal itself.
iv. Call approval in this manner when it can reject calls taking into account approval failure through utilization of H.225 flagging.
v. Bandwidth management that is control of terminals simultaneously accessing the network.
vi. Call management where the gatekeeper maintains a list of ongoing H.323 calls. This data may be utilized to show that a terminal is occupied, and give data to the bandwidth administration function.

(iv) Multipoint Control Units (MCU)

The MCU is an endpoint on the network giving the capacity to three or more terminals and portal to take part in a multipointconference [13].it consists of a mandatory (MC) controller and optional multipoint processor (MP). The MC decides the normal abilities of the terminals and the MP performs multiplexing of media streams under the control of the MC.

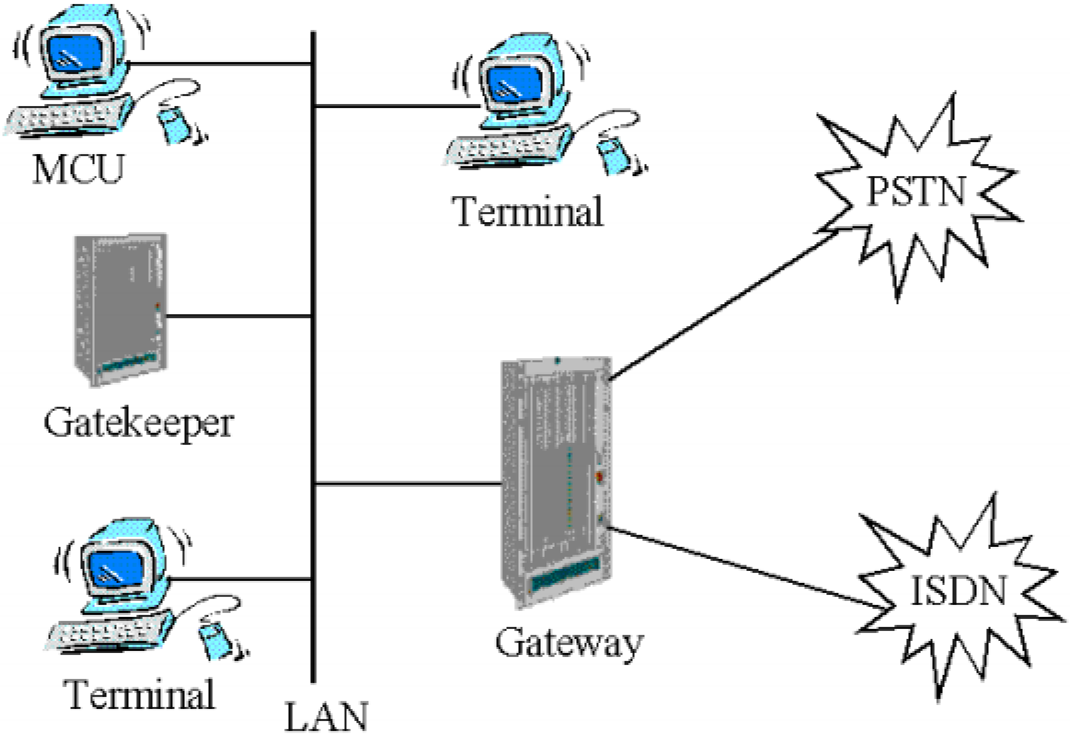


Fig 2.2: Components of H.323 [13]

(b) H.323 Protocols

H.323 characterizes the information stream arrangements and protocols that endpoints terminals actualize keeping in mind the end goal to correspond with each other. It also defines the control and management protocols used between terminals, gateways, gatekeepers and MCUs. Figure 4 below shows the protocol stack implemented by H.323 endpoints (terminals and gateways) in a VoIP network.

Table 2.2: Protocol stack implemented by H.323 endpoints [13].

Audio Application	Video Application	Terminal Control and Management			
Audio codecs G.711 G.729 G.723.1	Audio codecs G.711 G.729 G.723.1	Real-Time Control Protocol	H.255.0 Registration, Admission, And Status	H.255.0 Call Signaling	T-120 Data
Real-Time Protocol					
User Datagram Protocol (UDP)			Transmission Control Protocol (TCP)		
Internet Protocol (IP)					

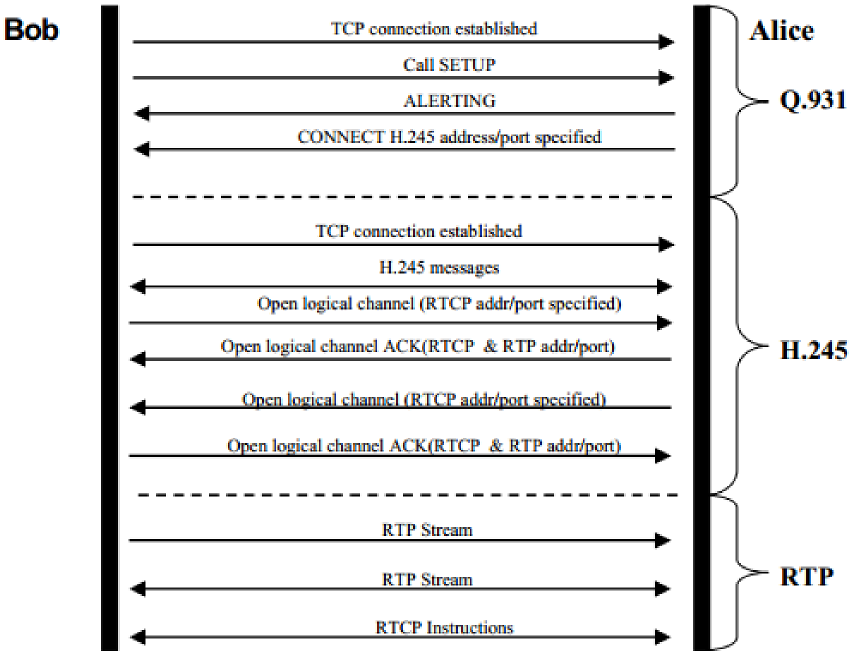
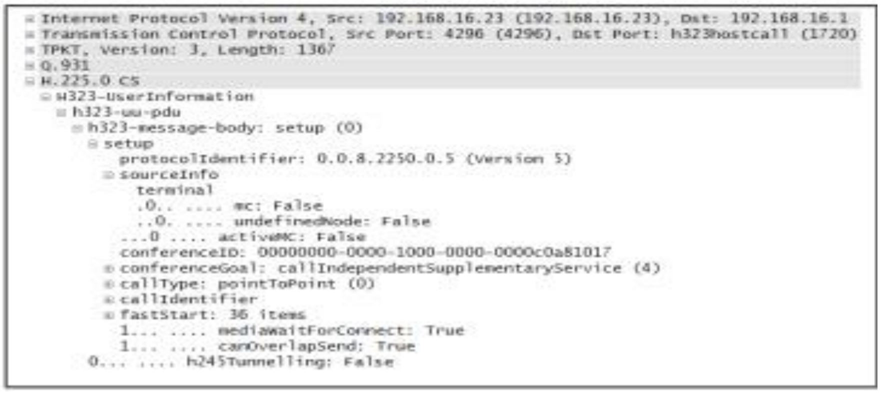

Bob
Alice
TCP connection established
Call SETUP
ALERTING
CONNECT H.245 address/port specified
Q.931
TCP connection established
H.245 messages
Open logical channel (RTCP addr/port specified)
Open logical channel ACK(RTCP & RTP addr/port)
Open logical channel (RTCP addr/port specified)
Open logical channel ACK(RTCP & RTP addr/port)
H.245
RTP Stream
RTP Stream
RTCP Instructions
RTP

Fig 2.3: H.323 Call Setup Process [17]

Figure 2.3 above portrayed the complex way VoIP call setup in light of H.323 can be set up. The H.323 suite has distinctive conventions connected with more complex types of correspondence including H.332 (expansive meetings), H.450.1, H.450.2, and H.450.3 (supplementary administrations), H.235 (security), and H.246 (interoperability with circuit exchanged administrations) [18].The utilization of these additional conventions and/or efforts to establish safety adds to the intricacy of the H.323 setup process thus this complexity aids to the difficult compatibility of H.323 with NATs and firewalls.



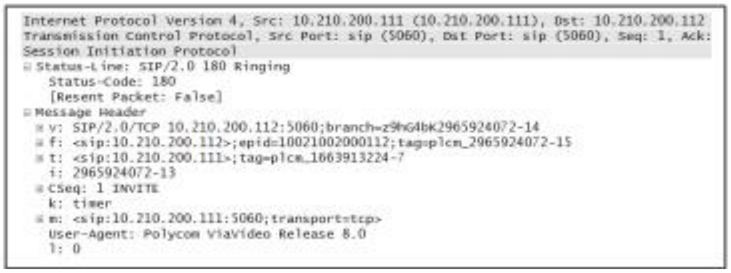
```
⊞ Internet Protocol Version 4, Src: 192.168.16.23 (192.168.16.23), Dst: 192.168.16.1
⊞ Transmission Control Protocol, Src Port: 4296 (4296), Dst Port: h323hostcall (1720)
⊞ TPKT, Version: 3, Length: 1367
⊞ Q.931
⊟ H.225.0 CS
  ⊟ H323-UserInformation
    ⊟ h323-uu-pdu
      ⊟ h323-message-body: setup (0)
        ⊟ setup
            protocolIdentifier: 0.0.8.2250.0.5 (Version 5)
          ⊟ sourceInfo
              terminal
              .0.. .... mc: False
              ..0. .... undefinedNode: False
            ...0 .... activeMC: False
            conferenceID: 00000000-0000-1000-0000-0000c0a81017
          ⊞ conferenceGoal: callIndependentSupplementaryService (4)
          ⊞ callType: pointToPoint (0)
          ⊞ callIdentifier
          ⊞ fastStart: 36 items
            1... .... mediaWaitForConnect: True
            1... .... canOverlapSend: True
        0... .... h245Tunnelling: False
```

Fig 2.4: H.323 packet [11]

Figure 2.4 above shows the H.323 packet and sub protocols in a H.323 session.

2.3.2 Session Initiation Protocol

It was developed by IETF and it’s a nonproprietary standard. The format of SIP messages is close to that of Hypertext Transfer Protocol (HTTP) [24]. SIP is the most common signaling protocol used by most companies including Vonage, Cisco and Skype. SIP is considered simpler than H.323 [11].



```
Internet Protocol Version 4, Src: 10.210.200.111 (10.210.200.111), Dst: 10.210.200.112
Transmission Control Protocol, Src Port: sip (5060), Dst Port: sip (5060), Seq: 1, Ack:
Session Initiation Protocol
⊟ Status-Line: SIP/2.0 180 Ringing
    Status-Code: 180
    [Resent Packet: False]
⊟ Message Header
  ⊞ v: SIP/2.0/TCP 10.210.200.112:5060;branch=z9hG4bK2965924072-14
  ⊞ f: <sip:10.210.200.112>;epid=10021002000112;tag=plcm_2965924072-15
  ⊞ t: <sip:10.210.200.111>;tag=plcm_1663913224-7
    i: 2965924072-13
  ⊞ CSeq: 1 INVITE
    k: timer
  ⊞ m: <sip:10.210.200.111:5060;transport=tcp>
    User-Agent: Polycom ViaVideo Release 8.0
    l: 0
```

Fig 2.5: SIP packet [11]

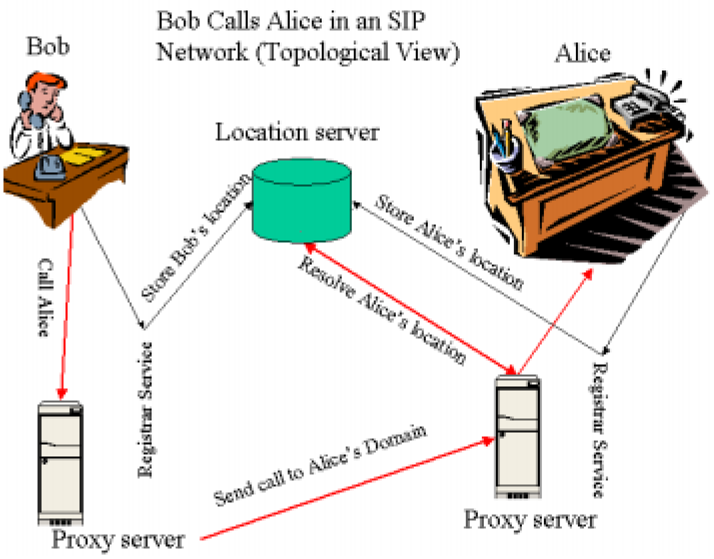


Fig 2.6: SIP Architecture [10]

(a) Components of SIP

(i) User Agents

It's an end system acting on behalf of the use. It comprises of 2 parts i.e. the client and a server. The user agent client (UAS) the client portion is used to initiate a SIP request while the user agent server (UAS) receives requests and return responses.

(ii) Network Servers

There exists 3 servers within a network that is registration, proxy and redirect servers. The registration server receives updates about current locations of users. A proxy server forwards requests received to the next hope server with more information of the called party. A redirect server determines the next hop server and returns the address to the client instead of forwarding the request [10].

(iii) SIP Messages

SIP defines a lot of messages which are used for dialogue between the client and the SIP server. These are:

INVITE: for inviting a user to call

BYE: for termination of communication between two endpoints

ACK: for reliable exchange of information between two parties

OPTIONS: for gathering information about the possibilities of a call

REGISTER: provides information about the user location to the SIP registration server

CANCEL: for terminating the search of a user

SIP relies on the real time protocol (RTP) to move voice packets between two endpoints. SIP is used extensively to trunk between systems. It operates on the application layer to initiate user sessions for multimedia transmissions such as voice, video, chat, gaming and virtual reality [11].It can be carried out by UDP, TCP and STCP [19]. SIP is designed to set up and tear down media sessions, for user location and capabilities, availability, and session-handling information.

A SIP network is composed of end points, proxy, redirect server, location server and registrar [19]. The user tells the registrar of their location. This information is saved in the external location saver and proxy servers extract the intended address information. They then contact the corresponding location server and forward the packets to the end points. The redirect server just sends the information back to the original sender.

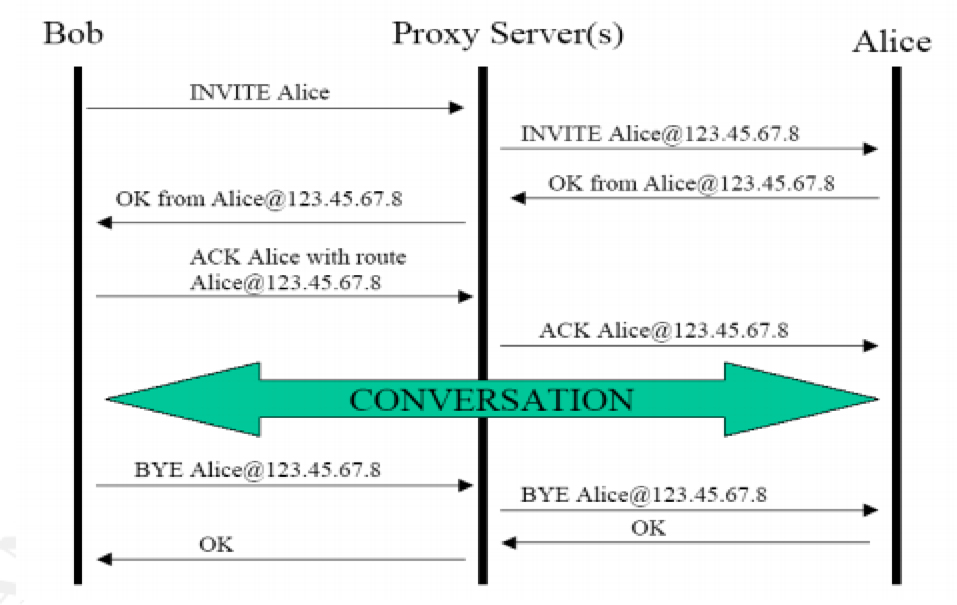


Fig 2.7: SIP protocol [19]

The SIP protocol is modelled around the 3-way handshake method of TCP. Figure 9, above is an example with a proxy and 2 endpoints. Unlike H.323, SIP does not define its own security profile. It can use HTTP digest authentication, TLS, IPsec and S/MIME (Secure/Multipurpose Internet Mail Extension) for security [20].

2.3.3 Contrast between H.323 and SIP Protocols

Table 2.3: Comparison between H.323 and SIP [19].

H.323	**SIP**
Loop detection is difficult	Loop detection is comparatively easy
Hundreds of elements	Only 37 headers
Complex protocol	Comparatively simpler
Binary presentation for its messages	Textual representation
Requires full backward compatibility	Doesn’t require full backward compatibility
Not very modular	Very modular
Not very scalable	Highly scalable
Complex signaling	Simple signaling
Large share of the market	Backed by IETF

2.3.4 Media Gateway Control Protocol (MGCP)

MGCP, developed by IETF controls gateways in an IP network [7]. It has 2 components that is the call agents and gateways. It acts in a master slave manner in which the call agent sends signaling, control, and processing commands to the gateway. The gateway acts as a slave and executes the commands sent by the call agent. It's a control protocol, permitting a central controller to monitor events in IP phones and gateways and instructs them to send media to specific addresses. The protocol is used to manage signaling and control activities for VoIP network gateways such as H.323, SIP and SS7 signaling [7].

2.3.5MEGACO/H.248

It's derived from MGCP and expected to be accepted widely in the industry [19]. It has improvements including support of multimedia and multipoint conferencing. It was as a result of a combined effort between the IETF and ITU-T. Megaco has basically the same architecture as MGCP.

2.4 Security Methods

2.4.1 NAT

Network address translation (NAT) is a router function that enables private IP networks that use nonregistered addresses to connect to the internet [21]. NAT is a method allowing communications between hosts on a private network to those on a public network i.e. the internet [22] . NAT works completely on the network level.

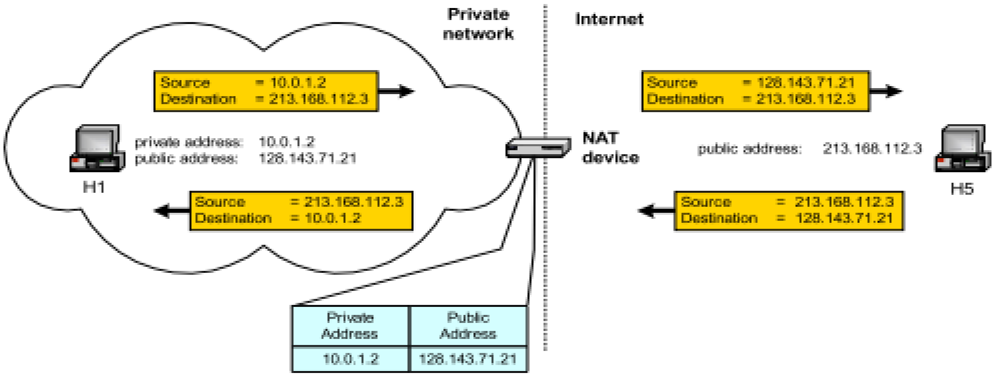
2.4.1.1 Types of NAT

(a) Dynamic NAT – it maps private addresses to internet address pool. The global addresses come from a pool of addresses that one configures [22].

(b) Static NAT – it maps a particular global address with a particular private address. It's used when one wants to ensure that the software always maps the same global address to a given private address.

(c) NAT Overload / Port Address Translation (PAT) – translates the outbound traffic of clients to unique port numbers off of a single global address. It is necessary when the number of internal clients exceeds the available global addresses [23].

2.4.1.2 Basic NAT operation


Private network
Internet
Source = 10.0.1.2
Destination = 213.168.112.3
Source = 128.143.71.21
Destination = 213.168.112.3
private address: 10.0.1.2
public address: 128.143.71.21
H1
NAT device
public address: 213.168.112.3
H5
Source = 213.168.112.3
Destination = 10.0.1.2
Source = 213.168.112.3
Destination = 128.143.71.21

Private Address	Public Address
10.0.1.2	128.143.71.21

Fig 2.8. Basic NAT operation [22].

Fig.3 above computer H1 has IP address 10.0.1.2. It sends a packet to a computer H5, IP address 213.168.112.3, on the internet. The firewall (NAT device) cannot forward the packet to the internet with source address thus it assigns a valid internet address 128.143.71.21. The NAT device replaces the original source address with a static internet address [22] [24].

2.4.1.2 Benefits of NAT

a) Hiding the specific addresses and addressing structure of the internal network that is security.

b) Addresses the issue of conserving ipv4 addresses.

c) Allows movement to another network service provider, simple as it only requires a redesign of the NAT gadget.

d) Helps in load adjustment/ balancing of servers.

2.4.2 FIREWALLS

These are gadgets or programs that control the stream of system activity that is traffic between networks or hosts that utilize varying security stances [25]. They are used in enterprise networks to restrict connectivity to and fro the internal networks. Firewalls contain content filtering features and intrusion prevention (IPS) system technologies.Firewalls are placed often on network boundaries thus such firewalls would have both internal and external interfaces.

2.4.2.1 Features of firewalls

The following are some of the most important firewall features:

a) Packet filtering – firewalls that perform packet filtering are also known as statelessinvestigation firewalls, as they do not stay informed regarding the condition of every stream of movement that goes through the firewall. This implies they cannot associate multiple requests within a single session to each other.

b) Stateful inspection – it tracks state of connections and blocking packets that deviate from an expected state i.e. improving on the functions of packet filters. Stateful examination catches packets at the network layer and reviews to figure out whether they are permitted by a current firewall standard and it stays informed concerning each connection in the state table.

c) Deep packet inspection – improves on stateful analysis by adding basic intrusion detection technology. This permits a firewall to acknowledge or deny access taking into account how an application is running over the system.

d) Application-proxy gateways –it is a feature for advanced firewalls that combines lower layer access control and upper layer functionality [25]. It doesn’t allow direct connection between two hosts but uses a proxy agent that acts as an intermediary for them to communicate.

e) Unified threat Management – it’s a combination of multiple firewall features. A typical unified threat management system consists of a firewall, malware detection and eradication, sensing and blocking of suspicious network probes, etc. [25].

2.4.3 Problems of NAT and Firewalls

While NAT and firewall play an important role in securing the VoIP communication network there are some drawbacks in implementing these mechanisms. These problems are namely:

- Connections can be initiated from the private network to the internet, but not the other way around thus made worse as SIP controls separate media streams and subsequently transports addresses.
- Firewalls usually deny access to port numbers connected with VoIP.
- Some even assess the bundle substance to recognize and dismiss VoIP traffic.
  RESULT: VoIP users behind NATs and Firewalls do not benefit the end-to-end connectivity necessary for VoIP.

2.4.4 Effects of Security on VoIP

VoIP security methods discussed previously are all likely to affect its performance by aiding in the increase of jitter, latency and or packet loss. Firewalls as well as NAT introduce end-to-end delay to packets sent over the network as they filter by inspecting each and every packet that transverses the network. Security mechanisms also introduce call setup delays due to identification and authentication mechanisms. It is necessary to investigate the overall effects of these on the system.

2.5 VoIP Quality of Service (QoS)

The way of IP innovation shows certain transmission issues to data packets sent by means of an IP network system, for example, packet deferral, jitter, and packet loss [26]. QoS is characterized as the capacity of the network to give better or "extraordinary" support of chosen clients and applications, to the potential drawback of otherusers and applications [26].QoS is used as a measure of a VoIP network performance. Delay variations i.e. jitter and latency are the QoS terms effected by complications of VoIP resulting from delay due to the firewall and call setups being blocked for encryption purposes. Many security measures implemented in the old and conventional data networks are not applicable in these VoIP networks due to its time critical nature [26]. QoS technology enables allocation of priority service to voice for VoIP. The main factors that affect QoS are latency, jitter and packet loss.

2.5.1 QoS Parameters

VoIP QoS is measured by suggestions in view of distinctive parameters like deferral, packet loss and jitter. These parameters can be manipulated in such a way that the VoIP QoS can be improved. The parameters are briefly discussed below:

Latency

It is the delay effect of a packet from the source to the destination and is a general problem in all telecommunications networks. In VoIP it relies on the postponements made by encoding, packet creation, physical network and directing delays, playback and unraveling decoding [14]. The codec used to encode the sign gives out the encoding deferral while network postponement is the entirety of transmission, transmission and queuing delay.Packet creation delay is time taken in creating an RTP packet from the encoded voice stream. Playback is a result of the buffer and decoding delay being time the system takes to remodel the original signal at the receiver. Voice cannot tolerate too much delay. The maximum amount of latency that can be tolerated is 150 milliseconds (0.15 sec) but is preferred be 100 milliseconds (0.10 sec) [27].Equation (1) shows the calculations of delay where Average delay (D) is expressed as the sum of all delays (di), divided by the total number of all measurements (N) [28].

$\mathrm{D} = \sum_{i=1}^{N} di/N$ ……………………………………………..equation 2.1

Jitter

It’s the delay due to variations in packet delivery and occurs as a result of improper queuing and network congestion [29]. As information is broken down into packets before transversal into the network, they are transported in parts with different routes. As they arrive at the destination they are reassembled but due to different network utilization some arrive late and some lost and hence the original message is altered thus jitter. The voice jitter delay tolerance is about 75 milliseconds (0.075sec) but is preferred be 40milliseconds (0.040sec).

Equation (2) shows calculation of jitter (j). Both average delay and jitter are measured in sec. Thus, if (*di*) values are equal, then D = *di* and *J* = 0 (i.e. there's no jitter) [28].

J = $\sqrt{\frac{1}{(N-1)}\sum_{i=1}^{N}(di-D)(di-D)}$…………………………equation 2.2

Packet loss

Packet loss occurs usually because of network congestion. UDP (user datagram protocol) is the transport level usually used by VoIP networks which is a connectionless protocol so packets are lost as there is no retransmission involved. Similarly if a packet isn't received on time it's discarded by the system. Voice traffic can tolerate less than a 3% loss of packets (15 is optimum) before callers feel at gaps in conversation [14].

Equation (3) shows calculation of packet loss ratio of the number of lost packets to the total number transmitted. Where N = total packets transmitted during a specific period and N*l*= number of packets lost the same period [28].

Loss packets ratio = $\left(\frac{Nl}{N}\right)\times 100\%$ ………………………..equation 2.3

Echo

It is the hearing of one's own sound [30]. The voice travels from one endpoint to another through varying equipment and trunk lines. The echo will not occur on the digital end rather it occurs at the analogue end of the network. This is when it has to be sent from one set of hybrid wires to a four trunk line [30].

Mean Opinion Score (MOS)

MOS is a standardized scale for judging the quality of voice. The MOS is primarily derived from the r factor. It also can be generalized from user responses about a given service .i.e. it is the human perception of the voice quality of service. It's expressed according the following scale [30]:

Table 2.4: MOS scale

Quality of Voice	Value
Excellent	5
Good	4
Fair	3
Poor	2
Bad	1

The ITU recommended values for good quality as in table 2.4 below are used to evaluate and provide a range of performance grades from excellent to poor for different VoIP networks.

Table 2.5: ITU Recommended Values for VoIP Quality [32]

Delay	< 150ms	>150ms < 300ms	> 300ms
Jitter	<20ms	>20ms < 50ms	> 50ms
Packet Loss	<1%	>1% < 5%	> 5%
Performance	Excellent	Good	Poor

References

[1] Consumer Electronics Association, "www.ce.org," 6 november 2004. [Online]. Available: http://www.ce.org/publications/books%5references/digital%5famerica/history/telecom.asp. [Accessed 12 june 2015].

[2] P. F. Cobley and A. Coward, "Voice over IP versus Voice of Frame Relay," *International Journal of Network Management* , vol. 14, pp. 223-230, 2004.

[3] M. Edwards, "IP telephony ready to explode into corporate world.(Industry trend or event)," *Communications News,* vol. 5, pp. 96-97, 2001.

[4] "VoIP insights," [Online]. Available: http://www.voipinsights.com/voip history.html. [Accessed 7 July 2015].

[5] [Online]. Available: http://www.voipsupply.com/voip-phone. [Accessed 7 July 2015].

[6] K.-C. LAN and T.-H. WU, *JOURNAL OF INFORMATION SCIENCE ENGNEERING,* vol. 28, pp. 723-737, 2012.

[7] L. Tse, "FEASIBILITY STUDY OF VOIP INTERGRATION INTO THE MYSEA ENVIRONMENT," NAVAL POSTGRADUATE SCHOOL MONTEREY, Carlifornia, 2005.

[8] "Techtarget,"[Online].Available:http://www.searchunifiedcommunications.techtarget.com/definition/VoIP-phone. [Accessed 7 August 2015].

[9] [Online]. Available: https://www.grandstream.com/index.php/products/ip-voice-telephony/consumer-analog-telephone-adaptors. [Accessed 7 August 2015].

[1] R. D. Kuhn, T. J. Walsh and S. Fries , "Recommendations of the National Institute of Standards and Technolodgy," *Security Considerations for Voice over IP systems,* pp. 800-858.

[11] B. Hartpence, Packet Guide to Voice over IP, Sebastopol: O'Reilly Media, 2013.

[12] ziffdavis corp, "VoIP for beginners," ziffdavis, 2012.

[13] R. Arora, "Protocols and Standards," [Online]. Available: http://www.arora@cis.ohio-state.edu. [Accessed 9 August 2015].

[14] T. M. Ashraf, N. J. Davies and V. Grout, "An Investigation into the Effect of Security on Perfomance in a VoIP Network," Centre for Applied Internet Research (CAIR), Wrexham.

[15] "Combining VoIPwith Policy based QoS," [Online]. Available: www.extremenetworks.com.

[16] R. Daniele and C. Catania , "Voice over IP Service for Intergrated Communications," May 1999. [Online]. Available: http//computer.org/internet/. [Accessed 7 June 2015].

[17] K. Siddiqui and S. Tajammul, "Comparison of H.323 and SIP for IP Telephony Signalling," in *IEEE 4th International Multioptics Conference*, Lahore, 2001.

[18] "DataBeam Corp," [Online]. Available: http://www.databeam.com/h323/h323primer.html.. [Accessed 9 June 2015].

[19] X. Jianqiang, "Security Issues and Countermeasures for VoIP," *InfoSec Reading room*, 2007.

[20] J. Hallock , "evolution and Trends in Digital Media Technolodgies," Digital Media University of Washington, Washington, 2004.

[21] "Chapter 11: Nating," in *Network Address Translation*.

[22] "virginia.edu," [Online]. Available: http://www.cs.virginia.edu./-itlab/book/slides/module17-nat.pt. [Accessed 20 august 2015].

[23] A. Balchunas, 2013. [Online]. Available: http://www.routeralley.com.. [Accessed 20 August 2015].

[24] "Visual Telephone Systems and Equipment for local Area Networks," ITU-T, Switzerland.

[25] K. Scarfone and P. Hoffman, "Guidlines on Firewalls and Firewall Policy Recommendations," *Computer Security Division Information Technology,* pp. 20899-8930, 2009.

[26] A. Lazzez and T. Slimani, "Deployment of VoIP Technology : QoS Concerns," Taif University, Saudi Arabia.

[27] A. Qinxia, "Analyzing the characteristics of VoIP traffic . Thesis Msc Dept of Comp scie," University of Saskatchewan, Canada, 2007.

[28] N. F. Tawfeeq, "Network congestion and quality of service analysis using OPNET," Al-Nahrain University, 2009.

[29] A. A. Syed and M. llyas, in *VoIP Handbook*, CRC Press, 2009, p. 370.

[30] H. Schulzrinne and J. Rosenberg, "A comparison of SIP and H.323 for internet telephony," in *International Workshop on Network and Operating System support for Audio and Video*, Cambridge, 1998.

[31] C. E. Irvine, T. D. Nguyen, D. J. Shifflet, T. E. Levin, J. Khosalim, C. Prince , C. P. Clark and M. Gondree, "MYSEA: the Monterey Security Architecture," Naval Postgraduate School, Carlifornia.

[32] S. Vadivelu, "Evaluating the Quality of Service in VoIP and comparng various encoding techniques," University of Bedfordshire, Bedfordshire, 2011.

CHAPTER 3

RESEARCH METHODS AND TECHNIQUES

3.1 Introduction

When Voice over internet protocol (VoIP) is made accessible to the general public it is of interest that its performance is taken into greater account. Technologies designed for limited use often have a downside of not scaling up to users satisfaction. Therefore VoIP providing high Quality of Service (QoS) is mandatory for it to be a replacement of Public Switched Telephone Network (PSTN). However, deployment of VoIP in the Internet network has no guarantees on the availability of good QoS since the internet works on a best effort basis. As the internet is a public resource, privacy considerations becomes a major importance particularly from the business use perspective. Information can be obtained on VoIP sensitivity to its key parameters of QoS through lab simulations.

This chapter gives an overview on the details of the experimental procedures and assumptions undertaken to measure the extent to which security affects the quality of VoIP calls. It details all steps in gathering data from experiments, questionnaires and the analysis of data to construct results that answers the research question and are meaningful in the research context.

3.2 Overview of QoS Parameters

Technically QoS is more than the client's perspective rather it consists of other parameters that is jitter, delay, packet loss, echo and bandwidth. The performance of VoIP is measured through QoS [1]. Researchers have come out with parameters to be observed in order to ensure VoIP QoS. QoS has categories for its parameters namely Timeliness, Bandwidth and Reliability.

In the research, three QoS parameters were selected from two categories namely Timeliness and Reliability. For timeliness the investigation focused on delay and jitter. Delay is defined as the average amount of time taken by a packet to transverse a network from its source to its destination. Also jitter is defined as the amount of fluctuations in packet access [2]. Packet loss was taken into account for the Reliability parameter. Packet loss being defined as the packets that do not arrive at the intended destination. The main justification of such choice being that the study focuses on differing VoIP communication in different network environments, hence it’s much practical to consider reliability and time.

There are several works carried out by other authors in the field of VoIP QoS. Delay introduced to a network due to security implementations was done by [3] [4] [5]. VoIP performance measurement using QoS parameters has been done by [6], while [7] focuses on the effects of QoS mechanisms affecting QoS performance.

3.3 Experimental Procedure

In analyzing the QoS performance parameters of VoIP communications the experiments were carried out in a lab and partially in a real time environment. The researcher chose to undertake the experiments at Entire Office Systems located at 22 Seke road Graentside due to a number of issues. Firstly as a company providing VoIP it was of greater advantage to work hand in hand with the experts. Considering also that the company had a lab with all equipment it was easy to minimize costs and use their premises and equipment as the equipment is expensive to obtain individually.

Also because Entire Office Systems provides services to other companies it was an advantage as the researcher could get access to doing a real time experimental VoIP calls between the company and any one of the clients in this case Delta Beverages located approximately 500metres away.

In undertaking the experiment, bandwidth and queuing algorithms were chosen as the independent variables and is justifiable from previous literature on QoS in VoIP. The dependent variables were chosen to be jitter, packet loss and delay. Therefore, in the research context QoS is defined from these dependent variables.

3.3.1 VoIP Network Design

The experiment was conducted in 2 scenarios. The first involved lab experiments and the second were data collected through questionnaires. A test network depicting a LAN, a WAN and the internet are used to conduct a VoIP communication test. The LAN was represented by two computers connected with a crossover cable as in figure 3.1 below.

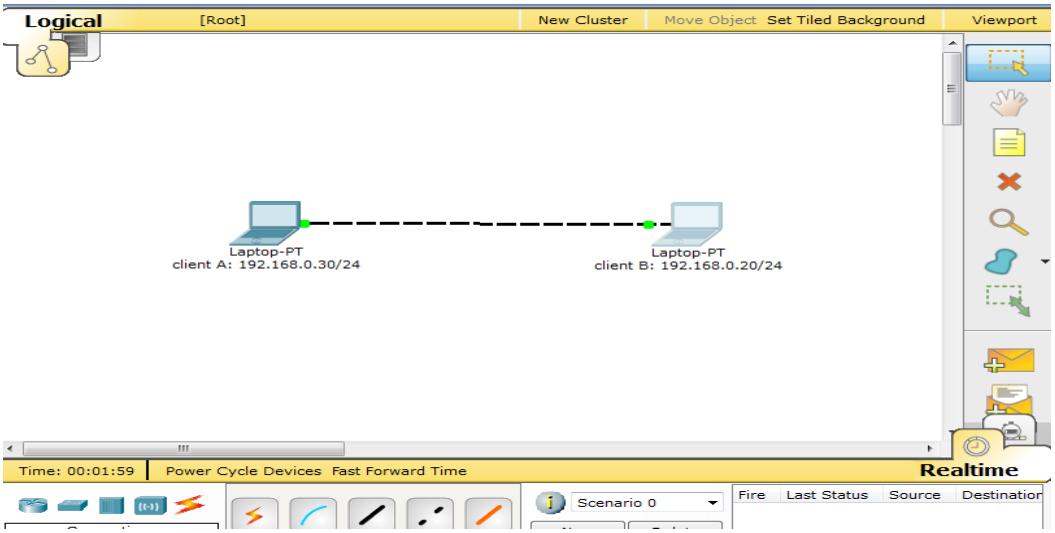


Fig 3.1: LAN topology

The LAN setup was reconfigured by adding one 2960 Cisco switch and two 2960 Cisco switches incrementally. The setup in figure 3.1 automatically puts the machines in the same local area network (LAN). The WAN setup was designed and implemented in a lab as the LAN. The WAN configurations included one which involved one router and the other which included two routers as in figure 3.2. Both configurations had two groups consisting of two computers and an Aria LIP8002 IP phone per group. These were connected via Cisco 2901 routers. A serial link connected the routers in a scenario as in figure 3.2 and enabled communication between the two through the use of a ping command after router configurations. The configurations are given in appendix 1. The Ethernet interfaces of the routers were configured that the computers from the different LANs could communicate to each other. The WAN design is as in figure 3.2 below:

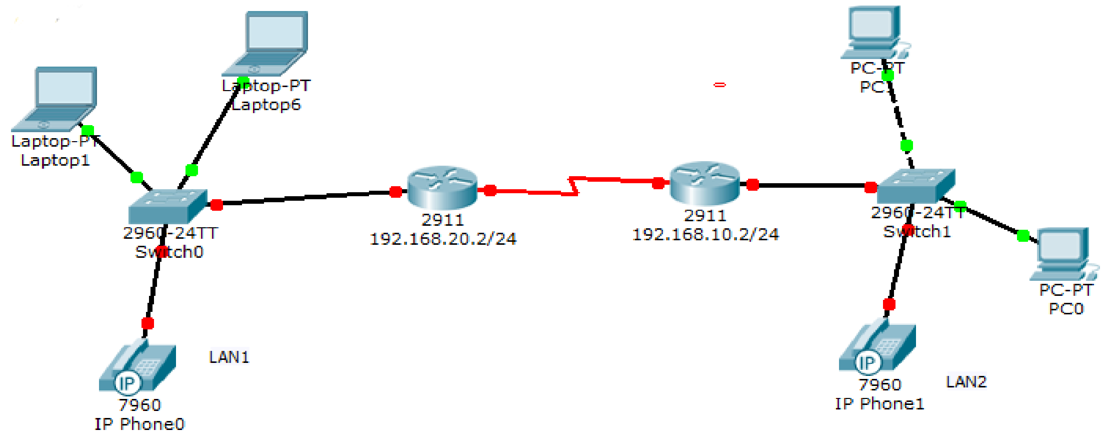


Fig 3.2: WAN test Network topology

The lab based configuration is as follows:

1. 100Mbps bandwidth for the LAN.
2. 100Mbps for the WAN.
3. 70Mbps for the real time experiment.

For the real time setup Entire Office Systems network were used as the LAN1 and Delta Beverages network was used as LAN2. The network topology is simplified as in figure 3.3 below:

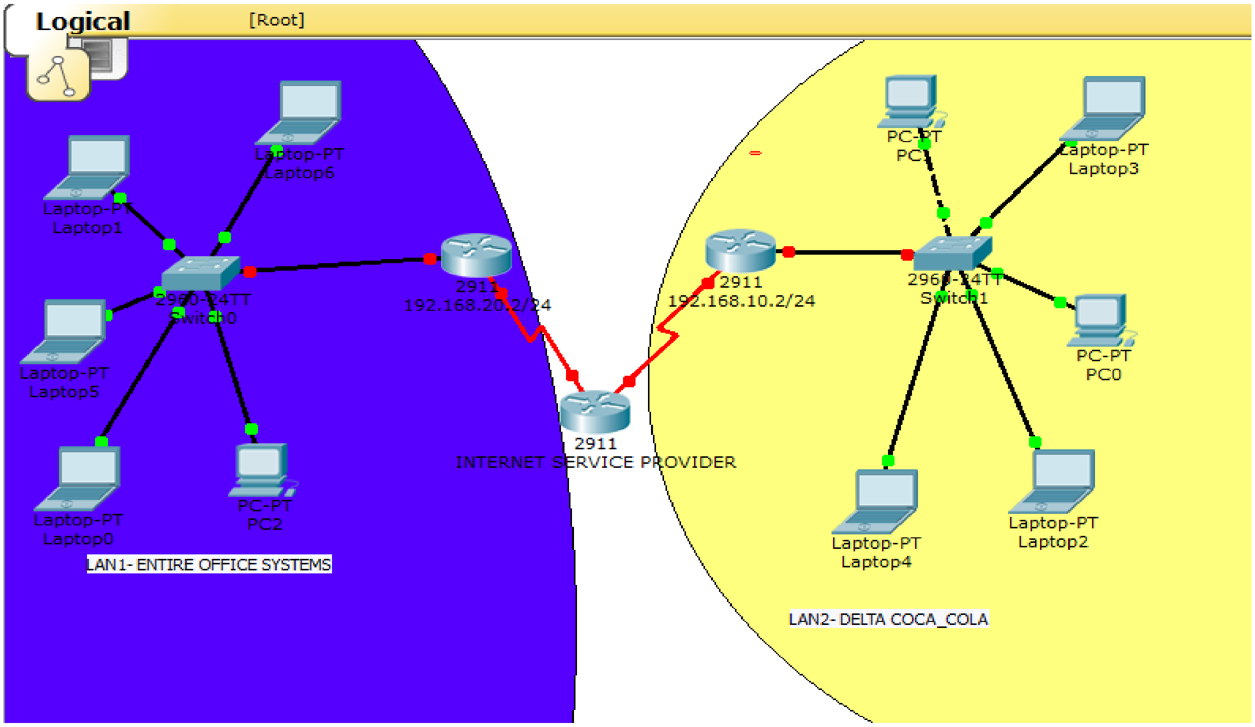
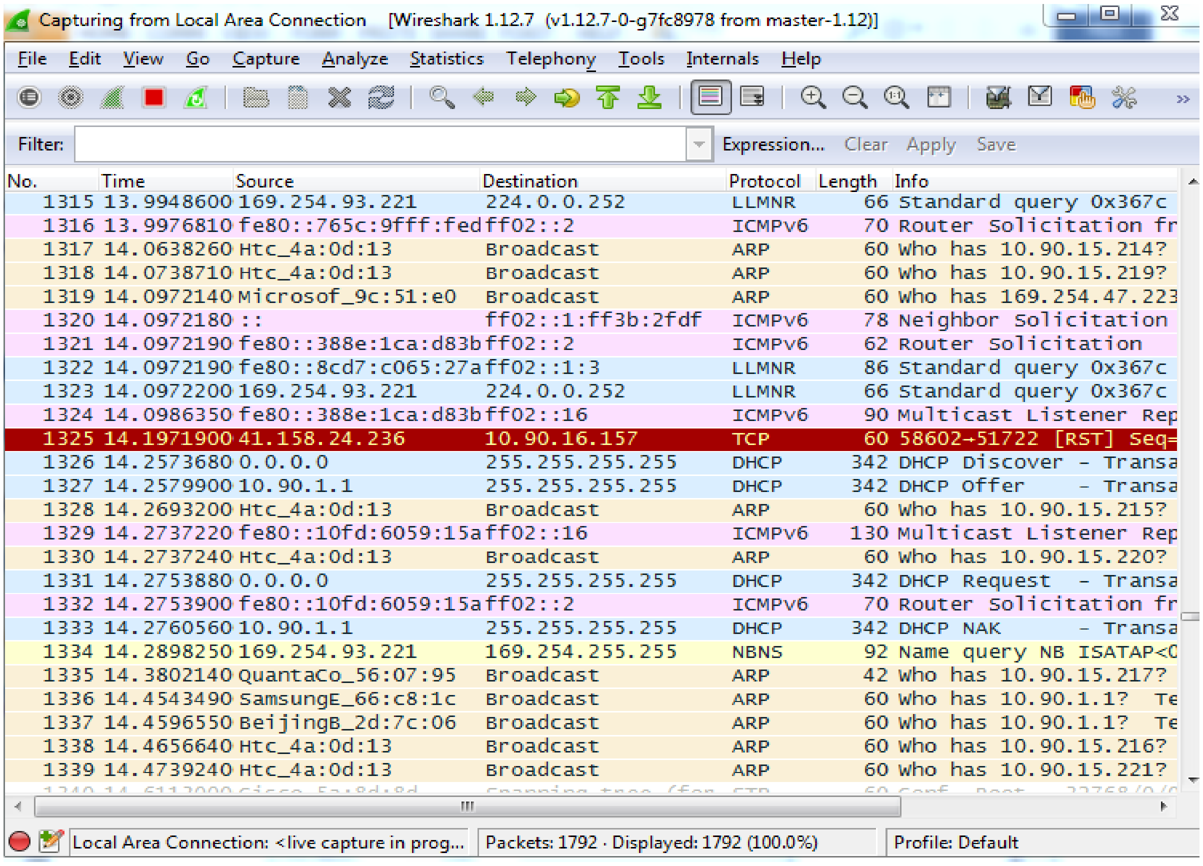


Fig 3.3: WAN real time topology.

The two networks were able to ping each other. The experiment applied internet infrastructure to transmit VoIP voice data.

3.3.2 Voice Traffic Capture

The impact of implementation of encryption algorithms measurements were deducted from different scenarios from the test network with differing bandwidth speeds. The design used softphones i.e. SJPhones as the conferencing software, wireshark as the packet sniffer, VQManager as the QoS metric analyzer. Each packet travelling between sender and receiver was capture using wireshark as shown in figure 3.4.



File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

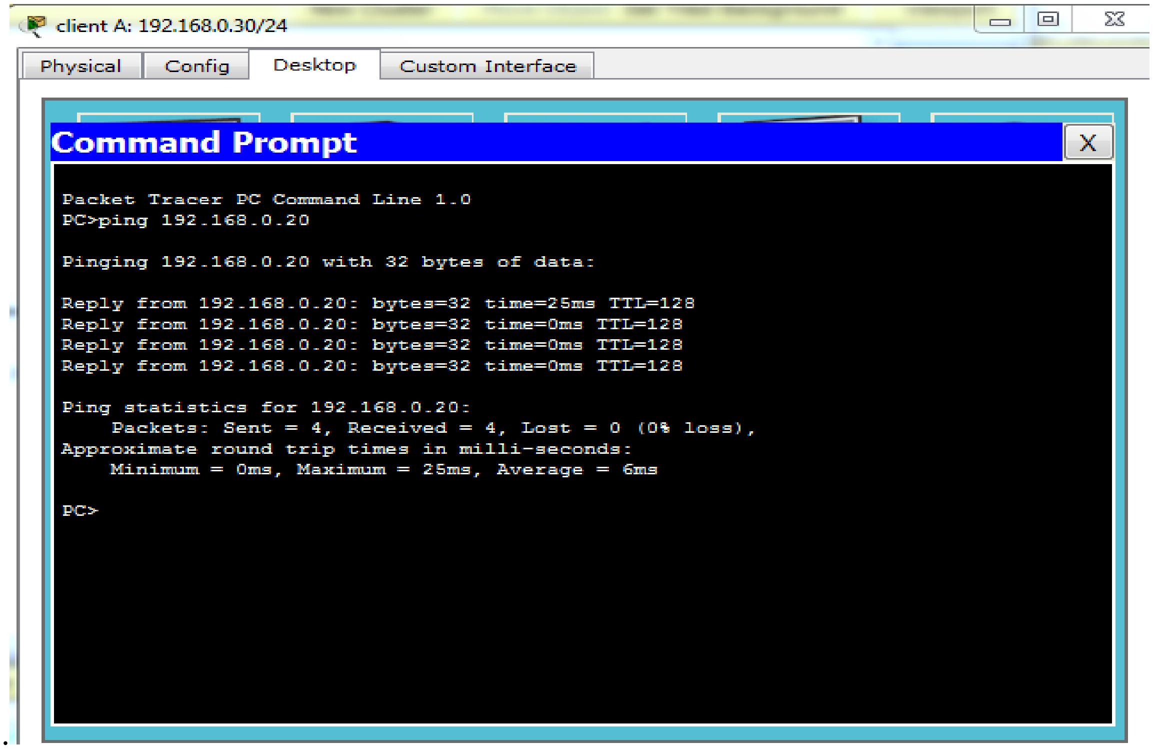
Capturing from Local Area Connection [Wireshark 1.12.7 (v1.12.7-0-g7fc8978 from master-1.12)]

No.	Time	Source	Destination	Protocol	Length	Info
1315	13.9948600	169.254.93.221	224.0.0.252	LLMNR	66	Standard query 0x367c
1316	13.9976810	fe80::765c:9fff:fed	ff02::2	ICMPv6	70	Router Solicitation fr
1317	14.0638260	Htc_4a:0d:13	Broadcast	ARP	60	Who has 10.90.15.214?
1318	14.0738710	Htc_4a:0d:13	Broadcast	ARP	60	Who has 10.90.15.219?
1319	14.0972140	Microsof_9c:51:e0	Broadcast	ARP	60	Who has 169.254.47.223
1320	14.0972180	::	ff02::1:ff3b:2fdf	ICMPv6	78	Neighbor Solicitation
1321	14.0972190	fe80::388e:1ca:d83b	ff02::2	ICMPv6	62	Router Solicitation
1322	14.0972190	fe80::8cd7:c065:27a	ff02::1:3	LLMNR	86	Standard query 0x367c
1323	14.0972200	169.254.93.221	224.0.0.252	LLMNR	66	Standard query 0x367c
1324	14.0986350	fe80::388e:1ca:d83b	ff02::16	ICMPv6	90	Multicast Listener Rep
1325	14.1971900	41.158.24.236	10.90.16.157	TCP	60	58602→51722 [RST] Seq=
1326	14.2573680	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transa
1327	14.2579900	10.90.1.1	255.255.255.255	DHCP	342	DHCP Offer - Transa
1328	14.2693200	Htc_4a:0d:13	Broadcast	ARP	60	Who has 10.90.15.215?
1329	14.2737220	fe80::10fd:6059:15a	ff02::16	ICMPv6	130	Multicast Listener Rep
1330	14.2737240	Htc_4a:0d:13	Broadcast	ARP	60	Who has 10.90.15.220?
1331	14.2753880	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transa
1332	14.2753900	fe80::10fd:6059:15a	ff02::2	ICMPv6	70	Router Solicitation fr
1333	14.2760560	10.90.1.1	255.255.255.255	DHCP	342	DHCP NAK - Transa
1334	14.2898250	169.254.93.221	169.254.255.255	NBNS	92	Name query NB ISATAP<0
1335	14.3802140	QuantaCo_56:07:95	Broadcast	ARP	42	Who has 10.90.15.217?
1336	14.4543490	SamsungE_66:c8:1c	Broadcast	ARP	60	Who has 10.90.1.1? Te
1337	14.4596550	BeijingB_2d:7c:06	Broadcast	ARP	60	Who has 10.90.1.1? Te
1338	14.4656640	Htc_4a:0d:13	Broadcast	ARP	60	Who has 10.90.15.216?
1339	14.4739240	Htc_4a:0d:13	Broadcast	ARP	60	Who has 10.90.15.221?

Local Area Connection: <live capture in prog... | Packets: 1792 · Displayed: 1792 (100.0%) | Profile: Default

Fig 3.4: Wireshark packet capture.

The output from wireshark captured packets' payload data is used to find the lost packet ratio and timestamps for latency and jitter. Also a ping command as much as a packet payload data and timestamps from wireshark can calculate two of the factors affecting QoS. Below is a snippet of a ping command showing the delay for a packet sent over the data network, size of the packet and number of packets lost.



```
Packet Tracer PC Command Line 1.0
PC>ping 192.168.0.20

Pinging 192.168.0.20 with 32 bytes of data:

Reply from 192.168.0.20: bytes=32 time=25ms TTL=128
Reply from 192.168.0.20: bytes=32 time=0ms TTL=128
Reply from 192.168.0.20: bytes=32 time=0ms TTL=128
Reply from 192.168.0.20: bytes=32 time=0ms TTL=128

Ping statistics for 192.168.0.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 25ms, Average = 6ms

PC>
```

Figure 3.5: Ping command output.

VoIP communication was initiated between two different computers on the test networks according the following procedures:

a) No security: Both clients were running SJPhone software, wireshark packet sniffer and the windows firewall was disabled. No encryption was used. This setting was the base /benchmark.

b) Firewall only: both clients were running SJPhone software, Wireshark packet sniffer and the windows firewall was enabled. No encryption algorithms were in use.

c) Windows firewall and encryption algorithm: both clients were running SJPhone, VQManager, with windows firewall enabled and OpenVPN with different encryption/decrypting VoIP calls between both parties.

3.4 Qualitative Research: Questionnaires

The system of questionnaires was used as part of the data collection method. The questionnaires were distributed randomly to workers with direct use of the VoIP service on both Entire Office System (LAN1) and Delta Beverages (LAN2). Given the design and distribution of the network, open ended questionnaires were used and the findings were used to compare the experimental data and the user experience. Attached in Appendix 2 is a sample of the questionnaires distributed partially to Entire Office Systems and Delta Beverages.

3.4.1 Comparison between open and closed ended questionnaires

Table 3.1: Open ended questionnaires [8]

ADVANTAGES	DISADVANTAGES
Opportunity to probe	Time consuming
Useful in hypothesis testing	Demands more effort
Flexible and freedom to answer	costly

Table 3.2: Closed ended questionnaires [9]

ADVANTAGES	DISADVANTAGES
Easy to process	Low flexibility
Fast to gather data	Biased towards researcher's view
No extended writing	Too crude
Makes comparisons easy	May irritate respondents

From the above comparisons it can be seen both types have drawbacks. The researcher resorted to open ended questionnaires as it allowed him to capture user experience with the technology more precisely. The random system of issuing out the questions was done so as to eliminate any biases that might come from giving people with a deep technical background. However the survey sample was that of a small number. This number was chosen as the research tried to have the questionnaire respondents being people who used the VoIP communication on a daily basis rather than giving to a someone who used a phone as little as twice a week.

References

[1] C. .. Hardy, "Measuring and Evaluating packet switched Voice," McGraw-Hill.

[2] D. H. . A. Mohammed, . H. D. A. Ali and J. H. Mohammed, "The Affects of Different Queuing Algorithms within the Router on QoS VoIP application Using OPNET," *International Journal of Computer Networks & Communications (IJCNC)* , vol. Vol.5, no. No.1, 2013.

[3] P. Radmand, J. Singh, M. Domingo, J. Arnedo and . A. Talevski, "The Impact of Security on VoIP Call Quality," Curtin University, Perth, Australia.

[4] A. Lazzez, "Securing VoIP Systems: A QoS-Oriented," *IJCSI International Journal of Computer Science Issues,* vol. Volume 11, no. Issue 6, 2014.

[5] . A. H. Mohammed and A. H. Ali, "Effect of some Security Mechanisms on the Qos VoIP Application using OPNET," *International Journal of Current Engineering and Technology,* vol. Vol.3, no. No.5, 2013.

[6] A. M. Amin, "VOIP PERFORMANCE MEASUREMENT USING QoS," in *The Second International Conference on Innovations in Information Technology (IIT'05)*, Perak Darul Ridzuan.

[7] M. S. Islam and S. . N. Mehdi, "How Different QoS Mechanisms Affect VoIP," Halmstad University, 2010.

[8] B. Hancork, An Introduction to Qualitative Research, Trent Focus Group, 1998.

[9] W.L.Neuman, "Social Research Methods: Qualitative and Quantitative Approaches," in *The free Space,* Allyn and Beacon, 2001.

[10] C. Cheyanne and M. Rogers , "Designing of Results," in *Qualitative or Quantitative Research,* p. 56.

[11] "SJ Labs," 2006. [Online]. Available: http://www.sjlabs.com. [Accessed July 2015].

CHAPTER 4

RESULTS AND ANALYSIS

4.1 Introduction

This chapter gives the overall perspective that is a detailed analysis of the results collected from the experiment. These results were presented in graphical and tabular form. Graphs were included to present a better view and readable results. Results presented are limited to the scenarios indicated in the previous chapter.

4.2 LAN and WAN Laboratory Measurements

For the laboratory environment Tables 4.1, 4.2 and 4.3 summarizes the measurements obtained for a LAN configuration incrementing the switch numbers. Table 4.4, 4.5 and 4.6 has WAN configurations incrementing the router number. Based on the experiments, the jitter, packet loss and delay values have been organized in form of bar graphs, representing each topology scenario against the perceived averaged value of the parameters. Data from the study was collected using Wireshark network monitoring software and the ping command from the Microsoft command line. The delay was obtained from the ping command results whereas jitter was calculated from the differences between the inter arrival time of the RTP packets. Packet loss values are represented in percentage of the total lost RTP packets from the total being transmitted.

4.2.1 Procedure

(a) Settings for Case I: Peer-to-peer connection.

The simulation is taken over an 8 minutes period taking the readings at an interval of 1 minute. Two PCs are connected directly to each other using a cross over cable. A SJphone softphone is installed on both PCs. The first simulation involves making a call to the other PCs with default windows firewall turned off. From both PCs wireshark is turned on and used to capture the packets transversing from one PC to the other. Then for the second scenario the firewall is turned on and just as before a communication is established calling the other part capturing readings.

Table 4.1: Showing parameters for a peer-to-peer connection used in the simulation studies.

Time(min)	**Jitter(ms)**		**Delay(ms)**		**Packet loss (%)**	
	No security	**firewall**	**No security**	**firewall**	**No security**	**firewall**
1	00.00	00.00	01.00	01.00	00.00	00.00
2	00.00	00.00	00.00	01.20	00.00	00.00
3	00.00	01.00	01.00	01.50	00.00	00.00
4	00.00	00.00	00.00	02.00	00.00	00.00
5	00.00	01.00	00.00	00.00	00.00	00.00
6	00.00	01.00	00.50	01.00	00.00	00.00
7	00.00	00.00	01.00	00.00	00.00	00.00
8	00.00	01.00	01.00	00.00	00.00	00.00

(b) Settings for Case II: 4PCs and one Switch.

Incrementing from Case I, a switch is added in that model and also 2 more PCs are included. This is done so as to increase traffic in the scenario. In this case instead of the PCs connecting direct to each other a switch is used that they connect from there. Just as above the simulation starts with firewall turned off and network activity being captured by firewall. A ping command is sometimes issued so as to compare the wireshark results and the ping results.

Table 4.2: Showing parameter measurements for LAN with one switch used in the simulation studies.

Time(min)	Jitter(ms)		Delay(ms)		Packet loss (%)	
	No security	**firewall**	**No security**	**firewall**	**No security**	**firewall**
1	00.00	02.00	10.00	10.00	00.00	1.00
2	00.00	02.30	14.00	15.00	00.00	1.00
3	03.00	01.75	19.00	20.00	00.00	1.00
4	04.00	01.50	20.00	16.00	00.00	1.00
5	10.00	12.00	28.00	16.00	00.00	0.20
6	09.00	04.50	34.00	21.00	00.00	1.00
7	06.00	11.00	15.00	15.00	00.00	1.10
8	05.00	07.50	12.00	19.00	00.00	1.90

(c) Settings for Case III: 2 switches and 4 PCs

From Case II another switch is added into the topology. Simulations are as before starting with no firewall and measuring with firewall turned on.

Table 4.3: Showing parameter measurements for LAN with two switches used in the simulation studies.

Time(min)	Jitter(ms)		Delay(ms)		Packet loss (%)	
	No security	**Firewall**	**No security**	**Firewall**	**No security**	**Firewall**
1	17.00	00.00	10.00	00.00	1.00	2.20

2	13.00	10.00	14.00	60.00	0.00	1.00
3	15.00	15.00	19.00	45.00	0.50	1.30
4	15.00	74.00	20.00	70.00	0.90	1.90
5	16.00	70.00	28.00	08.00	1.10	1.00
6	13.00	35.00	34.00	10.00	0.50	2.00
7	14.00	21.00	15.00	12.00	0.00	1.50
8	14.00	19.00	12.00	30.00	0.90	0.80

(d) Settings for Case IV: WAN connection with 1 router, 4 PCs and 2 IP phones.

Case IV simulates a wide area network (WAN) different from Case I-III above simulating a local area network (LAN) hence, instead of switches being used routers are used. Just as the procedure in Case I above the WAN procedure is the same. Having 2 PCs on both ends and starting capturing with no security incrementing to having a firewall. NAT is introduced as it couldn’t be implemented in scenarios above because it’s only implemented in routers. Measurements involve no security, firewall and NATing in that order taking calculations as in tables to follow.

Table 4.4: Showing parameter measurements for WAN topology using one router.

Time(min)	**Jitter(s)**			**Delay(s)**			**Packet loss (%)**		
	No security	**Firewall**	**NAT**	**No security**	**Firewall**	**NAT**	**No security**	**Firewall**	**NAT**
1	00.00	10.00	16.00	00.00	10.00	24.00	0.00	1.00	0.50
2	01.00	15.00	17.00	10.00	05.00	17.00	0.00	1.00	1.00
3	01.00	18.00	11.00	10.00	10.00	29.00	0.90	1.90	0.40
4	20.00	06.00	30.00	00.00	20.00	23.00	0.00	0.80	1.50

5	11.00	10.00	16.00	20.00	30.00	16.00	1.00	1.20	0.90
6	01.00	20.00	20.00	22.00	40.00	23.00	0.20	1.50	0.30
7	00.00	34.00	19.00	14.00	20.00	16.00	0.10	1.80	0.80
8	23.00	31.00	21.00	00.00	10.00	29.00	0.00	1.20	1.00

(e) Settings for Case V: 2 Routers, 4 PCs and 2 IP phones.

Just as in Case IV above the topology was maintained but another router is added. The IP phones basically are so as to increase the traffic in the network. The measurement procedure is also just as above.

Table 4.5: Showing parameter measurements for WAN topology using two routers used in the simulation studies.

Time(min)	**Jitter(s)**			**Delay(s)**			**Packet loss (%)**		
	No security	**Firewall**	**NAT**	**No security**	**Firewall**	**NAT**	**No security**	**Firewall**	**NAT**
1	10.00	45.00	10.00	40.00	86.00	87.00	1.00	4.00	5.00
2	19.00	25.00	12.00	40.00	86.00	86.00	1.20	4.20	5.20
3	28.00	40.00	25.00	41.00	87.00	86.00	1.10	5.00	5.00
4	23.00	39.00	39.00	40.00	82.00	86.00	0.90	5.10	4.90
5	22.00	33.00	45.00	42.00	86.00	85.00	1.00	4.90	5.30
6	20.00	34.00	32.00	41.00	85.00	87.00	1.10	4.00	5.10
7	16.00	29.00	28.00	41.00	87.00	85.00	1.00	5.00	5.00
8	13.00	29.00	23.00	40.00	86.00	88.00	1.00	4.10	4.90

4.2.2 QoS averaged measurements

Based on the results obtained in Section 4.2.1 averaged calculations of the parameters can be obtained in order to be able to represent them graphically.

Table 4.6: Summary of averaged parameters for all cases

Case	**Settings**	**Jitter (ms)**	**Delay (ms)**	**Packet loss (%)**
I	No security	00.00	00.50	00.00
	firewall	00.00	00.75	00.00
II	No security	04.625	03.120	00.000
	Firewall	04.763	16.500	01.025
III	No security	14.625	10.00	00.613
	Firewall	18.500	25.00	01.463
IV	No security	07.125	09.500	00.275
	Firewall	18.000	18.125	01.300
	NATing	18.750	22.125	00.800
V	No security	18.875	40.625	01.038
	Firewall	34.25	85.625	04.537
	NATing	25.500	86.250	05.050

4.2.3 Summary of Results

(a) No Security

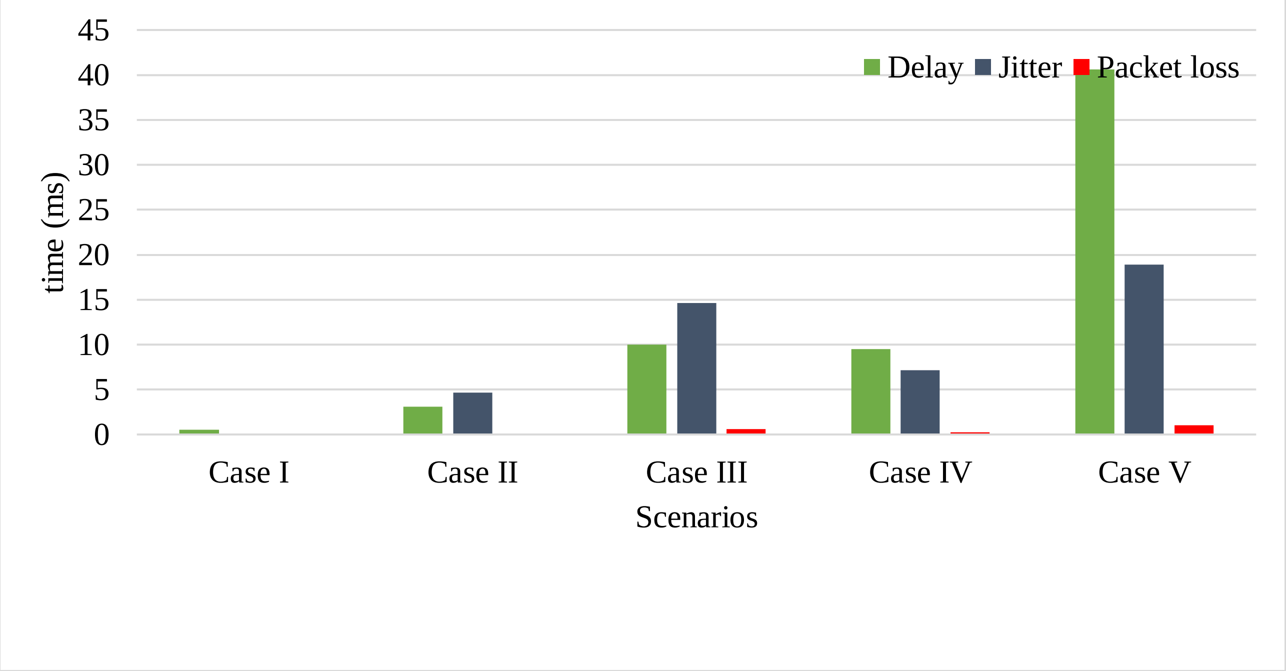


Figure 4.2: Parameters variations with no security.

Jitter represents the difference in the time taken by packets to reach the destination. This variation is as a result of traffic congestion, time variations and/or route changes. The figure 4.1 above reveals that the degree of jitter is increased as we move from Case I – V by changing the network topology and increasing the traffic levels. However in a LAN i.e. Case I (100Mbps) the amount of jitter is zero for the configuration without security and no switch.

In Case V configurations the network is bigger as it involves an increase in traffic from an addition of another PC and an IP phone on both ends.). The degree of jitter is slightly increased to a little less than 10ms for the configuration without any security. This can be attributed due to delays caused by a changed network topology and bandwidth as compared to Cases I-III. For Case V the jitter value for firewall implemented increased to approximately 35ms when the network condition involved two routers, which is the greatest degree of jitter among all scenarios.

(b) Firewall

As firewalls are a main line of defense against intrusion. The firewall characteristic of packet filtering introduces delay in that every packet passing through it needs to be checked. This adds an extra delay for all transmitted packets, which is the sum of queuing delay on the firewall input and the needed time to check the packet. Thus there is a noticeable increase on delay on the WAN configuration as shown in figure 4.4. The delay can also be found with NATing when the packets are remodeled and being added to it a new header. A firewall also acts as a bottleneck on the network because every packet has to be checked before being allowed to pass through. Therefore the noticed increase in packet loss on figure 4.2 when firewall was introduced.

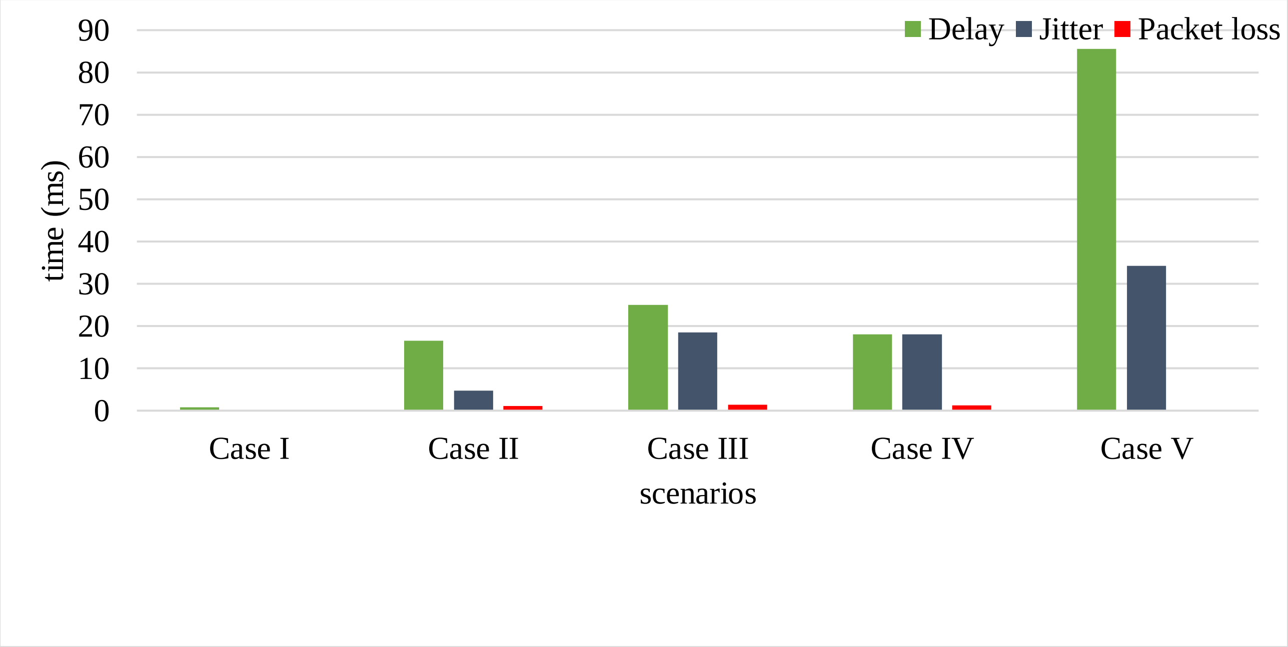


Figure 4.3: Parameter variations with a firewall.

For Cases I-III measurements obtained with security and incrementing the number of switches gives a rise in jitter values this however is so because the packets will now be transversing a longer path i.e. a changed route. Thus from the graph above jitter levels for all scenarios are fairly a bit higher as compared to those in figure 4.1. The jitter values obtained show that a firewall security mechanism exhibits higher values as compared to both no security and NATing mechanism. Since in the experiments firewalls were directly installed on PCs it was seen that for two routers the jitter value was higher. This is most probably caused by higher variations in packet arrival time due to the firewall. However the degree of jitter or all the experiment gives a good voice quality it doesn’t disrupt the conversation to an extent that it won’t be clear.

Delay is the average time taken by a packet to transverse the network from source to destination. For a network to be efficient its delay should have less delay value. It can be deduced that the network performance is inversely proportional to delay. From figure 4.2 above the firewall degrades QoS as it introduces delay increasing from a little less than 10ms up to approximately 30ms.It is noted that the results from the delay analysis of all Cases shows lower values as compared to the standard of 300ms by ITU. This is acceptable since the results obtained from a controlled lab environment, with a single VoIP communication, less traffic being transversed in the network and an entire unshared 100Mbps bandwidth. According to [1], delay values from 150ms and above are detectable by humans and impair the conversation quality thus in context of the obtained measurements the voice heard on both ends is of good quality. As expected in Case II and III firewalls increased delay in both conditions that with two switches added it had a delay higher than when there was one switch.

(c) NAT

From table 4.1 above it can be noted that Cases I- III have no NAT measurements as NATing is a router configuration and the Cases have switches in their topologies.

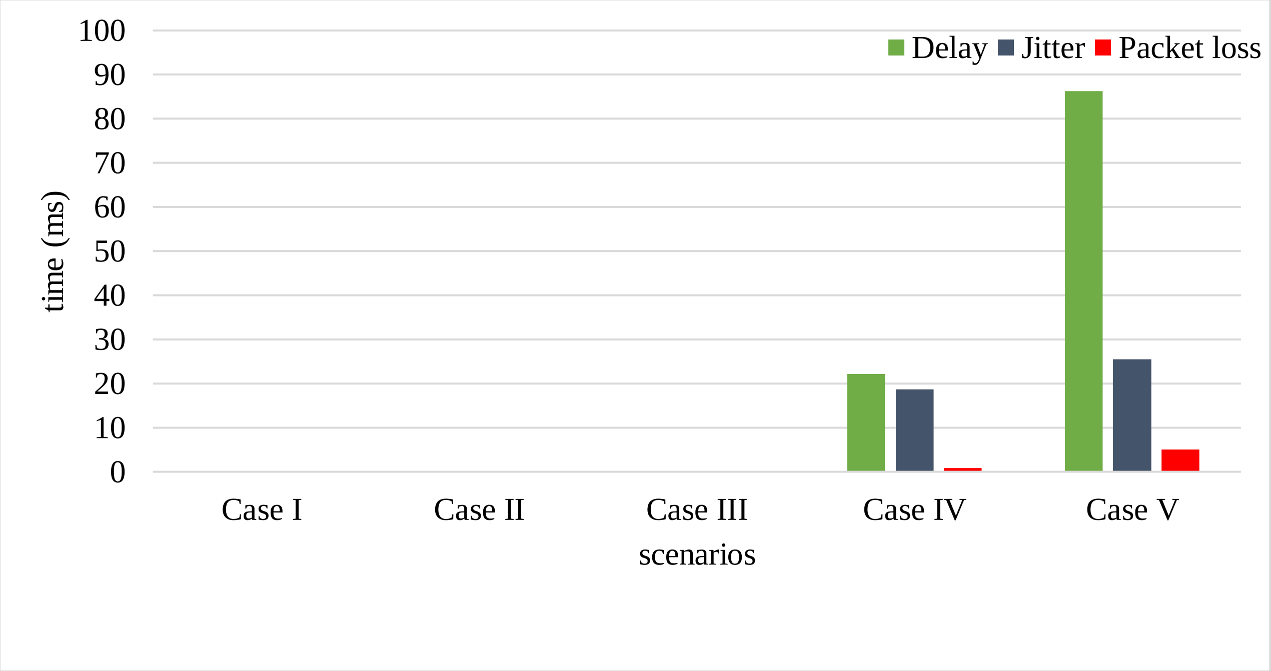


Figure 4.4: Parameter variations with NAT implemented.

Packet loss is defined as packets dropped by the network that is those which does not reach the intended destination thus causing loss of communication in the conversations and in severe cases transmitting of packets not in order hence a distorted message. In relation to the packet loss analysis, the scenarios where no security was implemented constantly produced relatively low packet loss rates. As expected and given from other experiments involving QoS parameters by other authors i.e. [2], [3] the packet loss for firewall and NATing are high and almost the same but less than the 5% threshold.

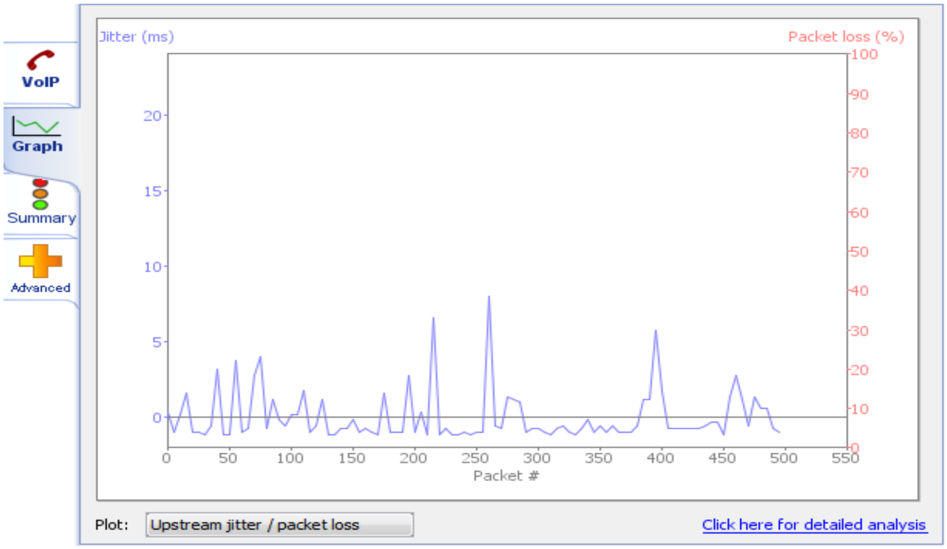
The packet loss values for Cases I-III in all figures above were very low thus barely imposing an impact in the voice communication. From figure 4.3 above, Cases IV and V can be used in the approximations that packet loss, jitter and delay increase with respect to increase in traffic and the growth of the network. It is clear from the above figures that where there is no security involved the QoS parameters are less as compared to that when security mechanisms are in place.

4.3 Simulation output of real time WAN experiment

The real time experiment assumed same bandwidth allocation for both LANS. Using the traceroute command the number of routers were found to be 6. The Graphs and summary of the parameters were obtained using OnSIP software. From the experiment firewalls were installed on both ends and the time when the measurements were taken was in the morning thus probably affected the results as there was little traffic as compared to if it was during pick working hours in the afternoon.

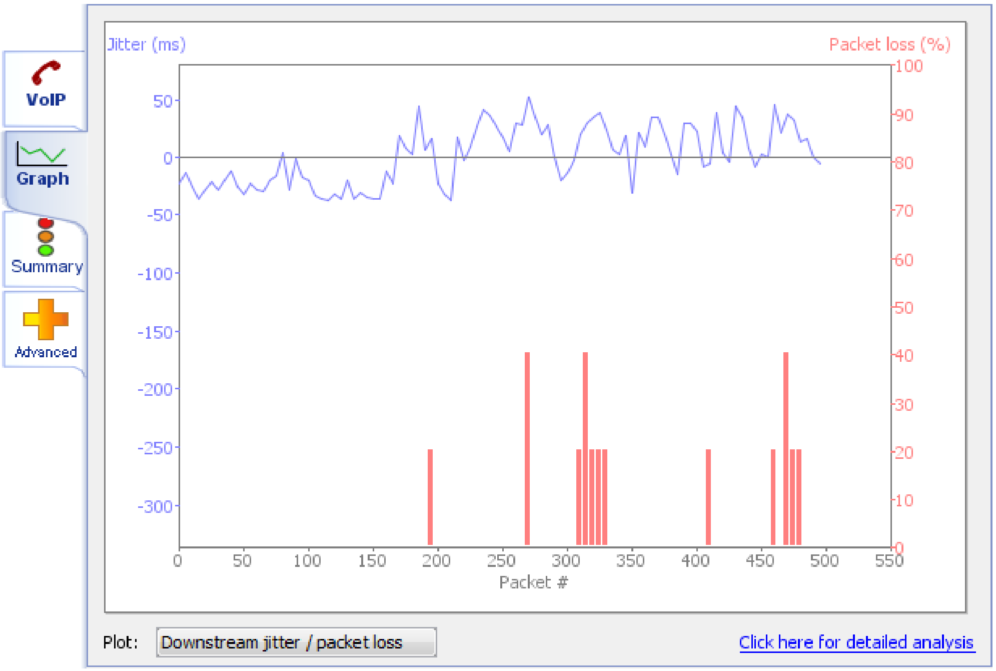
As can be seen in figures below the degree of jitter was at 27.5% for a real world environment. This was a little less than the degree of jitter that was expected as compared to the controlled lab experiments. The lower value can be attributed to lower traffic level and time of day.

Figures 4.7 and 4.8 shows the packet loss to be between 0 to 10% and figure 4.9 summaries it to be 4.5% that is packets discarded. Even though the packet loss was closest to the recommended packet loss for VoIP, call degradation is rarely noticed. From the experiment the call was clear and could be understood easily by both clients involved. This experiments show that increasing the number of routers thus giving a different network structure and also implementing simple security mechanism like firewall and NAT does not affect the quality of the call.



Plot: Upstream jitter / packet loss

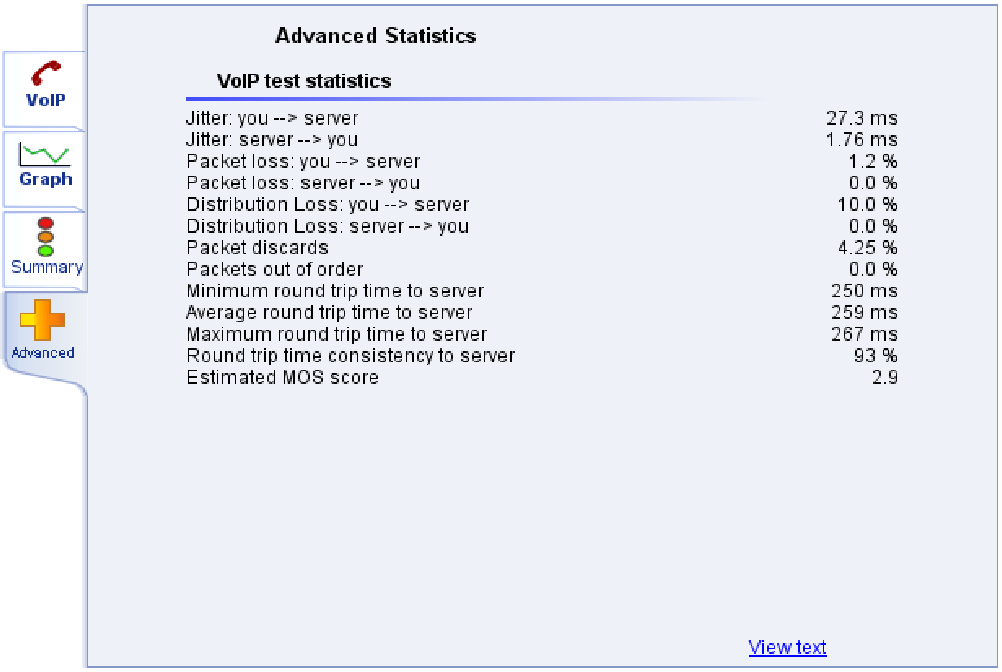
Figure 4.4: Simulated graph of upstream jitter and packet loss.



Plot: Downstream jitter / packet loss

Click here for detailed analysis

Figure 4.5: Simulated graph of downstream jitter and packet loss.



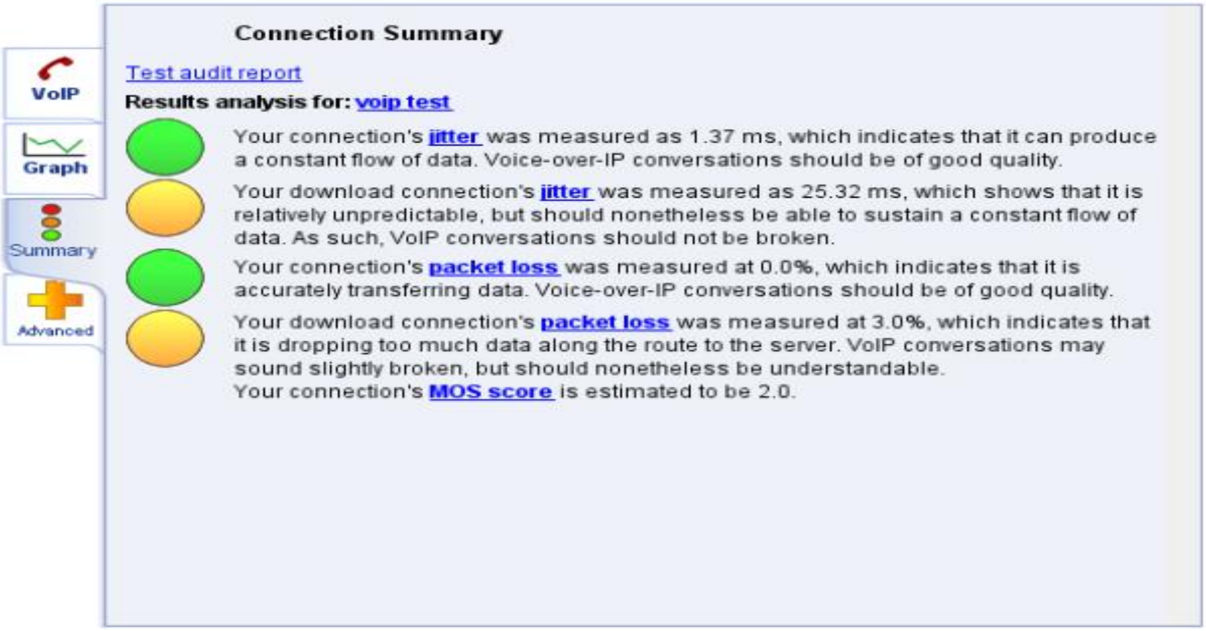
Advanced Statistics

VoIP test statistics

Jitter: you --> server	27.3 ms
Jitter: server --> you	1.76 ms
Packet loss: you --> server	1.2 %
Packet loss: server --> you	0.0 %
Distribution Loss: you --> server	10.0 %
Distribution Loss: server --> you	0.0 %
Packet discards	4.25 %
Packets out of order	0.0 %
Minimum round trip time to server	250 ms
Average round trip time to server	259 ms
Maximum round trip time to server	267 ms
Round trip time consistency to server	93 %
Estimated MOS score	2.9

Figure 4.6: Statistical data for the overall experiment.

From the statistical data jitter values is seen to be 27.3 ms and packet loss is less than 5 % the standard ITU value thus the VoIP communication is excellent.



Connection Summary

Test audit report

Results analysis for: voip test

Your connection's jitter was measured as 1.37 ms, which indicates that it can produce a constant flow of data. Voice-over-IP conversations should be of good quality.

Your download connection's jitter was measured as 25.32 ms, which shows that it is relatively unpredictable, but should nonetheless be able to sustain a constant flow of data. As such, VoIP conversations should not be broken.

Your connection's packet loss was measured at 0.0%, which indicates that it is accurately transferring data. Voice-over-IP conversations should be of good quality.

Your download connection's packet loss was measured at 3.0%, which indicates that it is dropping too much data along the route to the server. VoIP conversations may sound slightly broken, but should nonetheless be understandable.

Your connection's MOS score is estimated to be 2.0.

Figure 4.7: Showing the data summary.

4.4 Results of Survey

The survey was carried out by handing out random sample questionnaires to both the employees of Entire Office Systems (E.O.S) and Delta Beverages. The results gathered gave an insight into the performance of the VoIP communication using a WAN network and their perception of voice clarity, jitter and delay values.

The sample was chosen to be for 10 people i.e. 5 from both companies involved. Given the limited time the researcher had for result collection the number chosen for the sample had to be small hence 10 seemed appropriate. Also, E.O.S is a private company consisting of a less than 12 people with 8 of them being technicians there was going to be a biased in the results obtained if everyone was given the questionnaires.

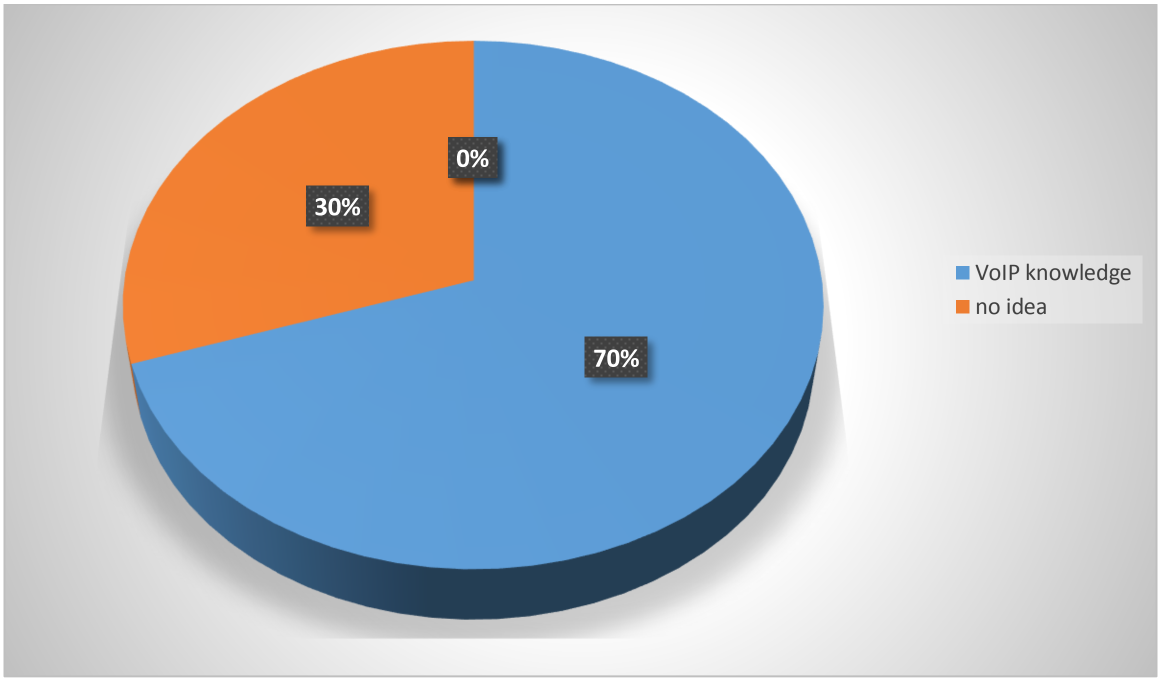
4.3.1 Summary of Survey Results

Table 4.7: Showing summary of survey measurements.

Questions	**Response**
VoIP Knowledge	7 /10
SIP Provider	liquid
Availability	9/10
Clarity	8/10
Delay (average)	1.2ms

From the survey result analysis 7 out of the 10 people showed a positive response in the knowledge of VoIP. Tabulated below is the percentage distribution of the findings.

Table 4.8: illustrating distribution of knowledge of VoIP among the sample.



From the above summaries obtained within a 10 people random sample 7 out of these people posed a general knowledge of VoIP. Given that the sample was of the people using the real time environment with which results were obtained earlier on it was expected that the findings be in sync. However the delay reported was averaged to be 1.2ms which is barely noticeable and does not affect the voice communication clarity. Besides the common problem of power cuts it was found that the VoIP communication was always available 90% of the time. Also these power cuts, echoes in conversation and crosstalk were the only disruptions reported on by the respondents. Unless there was a network failure or high traffic the clarity of the conversation was good.

4.5 Conclusion and Discussion of Findings

From the experiments carried out it can be seen that bandwidth and network structure affected the QoS metrics either positively or negatively. The real time experiment's time can be said to give different and higher values of QoS metrics if it were taken during the day when high traffic volumes are experienced. The survey showed a little deviation as expected from the obtained real time experimental results. The sample of survey reported a little delay hence jitter from the measured values thus implying that the perceived Voice quality was tolerable. From the experiment of LAN using switches it can be seen that the switches had no direct impact on either of the three metrics rather it just added in the reconfiguration of the network structure. As switches involve many separated collision domains as expected increasing traffic had a no impact. Rather the one broadcast domain they depict can be assumed to be the one adding up to the firewall delay and inducing the measured delay as in figure 4.3.

Routers contain one collision domain and many broadcast domains. This collision domain provided a room for traffic congestion and packet loss. The configuration of networks including routers thus directly added in jitter, delay and packet loss values for WAN going up as compared with the LAN set up. Firewalls and Nating however were found to have a little less interference in the Voice Quality of Service of the VoIP communication.

References

[1] Y. Amir, C. Danilov, D. Hedqvist and D. Terzis, "Using Overlay Networks to Improve QoS," CNDS, 2004.

[2] A. Amin, "VOIP PERFORMANCE MEASUREMENT USING QoS," in *The Second International Conference on Innovations in Information Technology (IIT'05)*, Perak Darul Ridzuan.

[3] I. N. A. a. A. A. Miloucheva, "Automated Analysis of Network QoS Parameters for VoIP over IP Application," in *Inter-Domain Performance and Simulation Workshop (IPS)*, 2004.

CHAPTER 5

CONCLUSION

5.1 Introduction

The presented research attempted to study the effects of security on VoIP communication Quality of Service (QoS). Section 5.1 gives an overall perspective of the activities and obtained results obtained during the experiments. Section 5.3 presents recommendations to relevant stakeholders, and for further research are presented.

5.2 Summary of Major Findings

a) This research revealed that the VoIP communication QoS is dependent on bandwidth, network topology and security mechanisms. Also jitter and packet loss are directly proportional in that the degree of variation in jitter implies the same degree of variation in the packet loss.

b) VoIP communication in a LAN environment has an excellent QoS whereas on a WAN the QoS is below excellent as the VoIP communication environment would be complex with introduction of high traffic, external network accesses and increased network topology implying greater transversal distance for voice packets.

c) The 3 parameters being measured had a degree not higher than the ITU standard. Jitter, delay and packet loss values were the least in the case of peer-to-peer communication in all scenarios. This doubled in cases were switches and routers were introduced in the topology. However due to different bandwidth use and traffic density a topology having routers that is Case IV and V had degree of jitter highest and also a greater percentage of packet loss.The QoS of VoIP communication is decreased with the introduction of network congestion/high traffic density owing to the relatively higher packet loss. Even so no degradation in call quality was found and the security mechanisms did not adversely affect the network QoS. The ration of lost packet in the real world environment is 4.25% which is less than lost packet ratios in the lab at 5.050% maximum, but improves as when 100Mbps bandwidth is used in Cases I-III.

5.3 Implication of findings & Recommendations to stakeholders

Given the findings obtained in the research a number of recommendations has been put together for the parties involved. The key stakeholders being the VoIP service providers and the clients i.e. companies acquiring the VoIP service. In the research the primary stakeholders were Econet and E.O.S. Econet being the service provider and E.O.S was the retailer of this service selling it to other companies. While the recommendations are primarily for the stakeholders, the research findings can be generalized to other stakeholders. In light of the findings presented in section 5.2, the following are some of the recommendations to be taken into account.

5.3.1 Recommendations to VoIP Service providers

(a) As it is important to secure sensitive company information as well as clients information putting up security should be considered carefully. Security mechanism should not affect the quality of the service hence for service providers offering the VoIP service stateful firewalls and also priority queuing for voice packets is advisable as it takes the voice with the highest priority [1], [2].

(b) Providers can also do assessment tests on client's network infrastructure to come up with the best signaling protocol to offer as not all VoIP signaling protocols work differently depending on the network setting and also the environment in which the VoIP is to be used.

5.3.2 Recommendations to Companies acquiring VoIP service

(a) Most companies would prefer to run a converged network of both data and voice. This has a strain on the voice quality if not properly implemented hence to reduce this stain that is delay and jitter the routers can be configured with queuing methods that offer highest priority to voice packets. Also buffers can be used within the network topology so as to reduce the degree of jitter, packet loss and delay [3].

(b) Most company administrators mistakenly assume that the same security mechanism for data network works also when it's on a converged network. This is entirely a misleading assumption as VoIP comes with new complex threats therefore it is highly recommended that network security upgrades be carried out for instance putting in place encryption algorithms , creation of Virtual Local Ares Networks (VLANs) to separate data and voice[4].

(c) Most security mechanisms can come costly for many companies thus a unified system can be put in place that is use of a Session Boarder controller (SBC) [1], [2]. These are dedicated appliances that offer NAT/firewall security schemes, protocol internetworking and Admission control. Therefore SBCs allow use of firewall/NAT security while avoiding their effects on QoS.

(d) Also companies can acquire a larger network bandwidth to increase processing speed, buffering capacity and transmission capacity of the network.

5.4 Further Research

In carrying out this research, some challenges were encountered. These led to the research only giving out an idea of how the VoIP network behaves with regards to the measured parameters that is jitter, delay and packet loss. However, given enough time the research could be extended to have been carried out over different times of the day, carried out over different network topologies and carried out with differing VoIP protocols in order for one to have a clear picture of the scenario.

Generally many companies which adopt VoIP have security policies in place that made it difficult for the researcher to have to investigate the scenarios at primary level. For calculating the parameter values wireshark packet capture software was used. However using this software limited the dependent variables only to jitter, delay and packet loss. For future researches there is need to use softwares such as OPNET and VQ manager as they have room for different parameters to be considered.Carrying out the lab tests over a number of few topologies restricted the research but allowed a thorough unbiased result collection. With enough space and equipment future researches could be taken on a much larger scale and having different remote sites to test a WAN topology.

The test results obtained were consistent with the expectations however having a small survey sample gave an insight into the end user’s experience with the system in place. In further researches, a larger crowd would give a little less biased experience and a room for averaging and generalizing the findings. Further researches and testing needs to be performed in order to reach more conclusive results. It is needed to identify other factors that may affect voice quality, such as routing protocol, congestion, different codec and type of network to determine the effects these have upon the QoS in VoIP.

References

[1] M. H. a. J. A. Schormans, "LIMITATIONS OF PASSIVE & ACTIVE MEASUREMENT METHODS," Queen Mary, University of London, London.

[2] H. Fischer J Martin, "A Method for Analyzing Congestion in Pareto and Related Queues," The Telecommunications Review, 2000.

[3] B. Stringfellow, "Secure Voice Over IP," 20 August 2001. [Online]. Available: http://www.sans.org//rr/voip/sec voice.php. [Accessed 20 october 2015].

[4] N. G. G. J. K. M. N. K. J. Augustin Jebakumar1, "Security and Privacy Preservation over Interconnected Networks," *International Journal on Recent and Innovation Trends in Computing and Communication,* vol. 2, no. 3, pp. 641- 644, 2014.

[5] T. J. W. a. S. F. D. Richard Kuhn, "Security Considerations for Voice over IP Systems: Recommendations of the National Institute of Standards and Technologies.," *NIST Special Publication* , pp. 800-58, 2005.

[6] J. R. a. H. Schulzrinne, "SIP Traversal through Residential and Enterprise NATs and Firewalls," *Internet Draft, Internet Engineering Task Force,* 2001.

[7] a. B. C. Vinod Joseph, "“Deploying QoS for Cisco IP and Next-Generation Networks: The Definitive Guide," Morgan Kaufmann, 2009.

Appendix 1: Sample Open ended Questionnaire

Midlands State University

Department of Physics and Instrumentation

BSc Telecommunications Research Questionnaire

By Macdonald Mauye doing a research on The Effects of Security on VoIP Communication Quality of Service.

1. How would you rate your knowledge about VoIP technology? (1 being the worst and 5 being the excellent)……………………………………………………………………..

   ………………………………………………………………………………………..

   ………………………………………………………………………………………..

2. How often do you use VoIP technology? ....

   ………………………………………………………………………………………..

   ………………………………………………………………………………………..

3. Which SIP service provider are you connected with? ....

   ………………………………………………………………………………………..

   ………………………………………………………………………………………..

4. How often is the SIP service available? ....

   ………………………………………………………………………………………..

   ………………………………………………………………………………………..

5. How do you rate the voice clarity? (1 being the worst and 5 being the excellent)……..

   ……………………………………………………………………………………….

   ……………………………………………………………………………………….

6. Do you experience any delay in speech? If yes approx. how much seconds? ………...

   ……………………………………………………………………………………….

   ……………………………………………………………………………………….

7. Is there any disturbances experienced during calls? If yes clarify…………………….

   ....

   ………………………………………………………………………………………

Completed by

…………………………………………..............
(Signature)

Appendix 2: Configuration for WAN using two routers

Configurations for 1st router

```
Router > enable //
Router # conf t //
Router (config) # hostname CASE_V1 // naming router for CASE V
CASE_V1 (config) # enable secret 0000 // configuring password for login
CASE_V1 (config) # interface g0/0 //
CASE_V1 (config) # ip address 192.168.10.1 255.255.255.0 // assigning an ip address to a router interface
CASE_V1 (config) # no shut //
CASE_V1 (config) # interface serial 0/0 //
CASE_V1 (config) # 192.168.20.1 255.255.255.254 //
CASE_V1 (config) # no shut
CASE_V1 (config) # exit
```

Configurations for 2nd router

```
Router > enable //
Router # conf t //
Router (config) # hostname CASE_V2 // naming the second router CASE_V2
CASE_V2 (config) # enable secret 0000 // configuring password for login
CASE_V2 (config) # interface g0/0 //
CASE_V2 (config) # ip address 192.168.30.1 255.255.255.0 // assigning an ip address to a router interface
CASE_V2 (config) # no shut // turning up the interface
CASE_V2 (config) # interface serial 0/0
CASE_V2 (config) # 192.168.20.2 255.255.255.254 // assigning an ip address for the other network
CASE_V2 (config) # no shut // turning the interface up
CASE_V2 (config) # exit
```