



MSc Thesis

Thesis Title: **Designing and optimization of VOIP
PBX infrastructure**

By

Naveed Younas Rana

Student ID: **1133670**

Department of computer science and technology

University of Bedfordshire

Supervisor: **Dr. Ali Mansour**

Abstract

In the recent decade, communication has stirred from the old wired medium such as public switched telephone network (PSTN) to the Internet. Present, Voice over Internet Protocol (VoIP) Technology used for communication on internet by means of packet switching technique. Several years ago, an internet protocol (IP) based organism was launched, which is known as Private Branch Exchange "PBX", as a substitute of common PSTN systems. For free communication, probably you must have to be pleased with starting of domestic calls. Although, fairly in few cases, VoIP services can considerably condense our periodical phone bills. For instance, if someone makes frequent global phone calls, VoIP talk service is the actual savings treat which cannot achieve by using regular switched phone. VoIP talk services strength help to trim down your phone bills if you deal with a lot of long-distance (international) and as well as domestic phone calls. However, with the VoIP success, threats and challenges also stay behind. In this dissertation, by penetration testing one will know that how to find network vulnerabilities how to attack them to exploit the network for unhealthy activities and also will know about some security techniques to secure a network. And the results will be achieved by penetration testing will indicate of proven of artefact and would be helpful to enhance the level of network security to build a more secure network in future.

Author consent form

Author's name Naveed Younas Rana

Title of Thesis Designing and optimization of VOIP PBX infrastructure

Degree MSc Computer Networking

I have read and fully understand the rules and regulations of the University of the Bedfordshire concerning final thesis submission.

I AM AS FOLLOW:

- I am the Author of the following thesis.
- Work demonstration is originally designed and optimised
- I do accept University of Bedfordshire Policy concerning final thesis submission.

AUTHOR'S SIGNATURE:

Naveed Younas Rana

AUTHOR STUDENT ID:

1133670

date

23-05-2013

Acknowledgement

I would like to be appreciative for help and support of the very kind people around me, especially I would like to be thankful to my supervisor Dr. Ali Mansour for his greater guidance and for technical support as well in this project. Thanks for him to make it possible for successful completion of this project. He has offered me explicit support throughout. Report writing and network designing were a difficult challenges but I have done my job with his help successfully. His given feedback made me able to review my progress in writing dissertation. His support has been invaluable for me on academic level and I am extremely thankful for this.

Secondly, I would like to be thankful to Faisal Fayyaz Qurashi and be appreciative for his support and help in designing the network and overall throughout this project.

Abbreviations

Following are the important abbreviations:

VoIP	Voice over Internet Protocol
PBX	Private Branch Exchange
QoS	Quality of Service
PSTN	Public Switched Telephone Network
SIP	Session Initiation Protocol
TCP	Transmission Control Protocol
IPSec	Internet Protocol Security
FTP	File Transport Protocol
NAT	Network Address Translation
RTP	Real time Transport Protocol
ISP	Internet Service Provider
MPLS	Multiprotocol Label Switching
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
HTTP	Hypertext Transfer Protocol

Table of Contents

Abstract

Author concern form

Acknowledgement

Abbreviations

1	Introduction	9
1.1	Aim and objectives	9
1.2	Problem definitions	9
1.3	Methodology	10
1.3.1	Project requirements	10
1.3.2	Scenario	10
1.3.3	Expected Results	10
1.4	Organizing documentation	11
1.5	Summary	11
2	Literature Review	12
2.1	VoIP	12
2.1.1	History	13
2.1.2	Features	13
2.1.2.1	Infrastructure	13
2.1.2.2	Free calling	14
2.1.2.3	Quality	14
2.1.2.4	Flexibility	14
2.1.3	VoIP standards	14
2.1.4	VoIP requirements	15
2.2	IP PBX	15
2.2.1	Background	16
2.2.2	Architecture	17
2.2.2.1	IP	17
2.2.2.2	Hybrid IP	17
2.2.2.3	Linux	18
2.2.2.4	Windows	18
2.2.2.5	Real-time	18

2.2.3	Functionalities.....	18
2.3	QoS.....	19
2.3.1	Parameters.....	19
2.3.1.1	Packet loss.....	19
2.3.1.2	Jitter	19
2.3.1.3	Latency	19
2.3.2	Importance of QoS	19
2.3.3	Integrated services.....	20
2.3.4	MPLS traffic engineering.....	20
2.4	Security	21
2.4.1	Challenges and vulnerabilities	21
2.4.1.1	Denial of service attacks (DoS):.....	22
2.4.1.2	Access attack:.....	22
2.4.1.3	Modification attack:	22
2.4.1.4	Vishing:.....	22
2.4.1.5	Toll fraud:	22
2.4.1.6	Spam over internet Telephony (SPIT):	22
2.4.2	Firewall.....	23
2.4.3	Encryption	23
2.4.4	IPSec.....	24
2.5	Summary	24
3	Designing and optimization of network and results.....	25
3.1	Network design and tools	25
3.2	Network Requirements.....	25
3.3	Scenario and Results	25
3.4	Summary	39
4	Evaluation of QoS.....	40
4.1	Packets transmission.....	40
4.2	Jitter	40
4.3	Latency	41
4.4	Summary	42
5	Penetration testing	43
5.1	Spoofing	43
5.1.1	Spoofing attack	43

5.2	Inbound traffic capturing	47
5.2.1	Traffic Capturing	47
5.3	Solution	49
5.3.1	IP security	49
5.3.2	Wi-Fi Protected Access.....	49
5.4	Summary	50
6	Conclusion and future preference	51

References

Appendices

1 Introduction

It has been more than a few years; a system was launched known as Private Branch Exchange (PBX) as substitute of old telephone system. PBX system offers communication platform to perform tasks such as inbound calls and outbound calls, domestic or globally for less. PBX system is VoIP supported algorithm. Voice over Internet Protocol, mostly recognizable as VoIP, is used to transmit voice data over internet, using the same pattern in which we send and receive e-mail. VoIP services offers to make calls by exploiting existing broadband connection as a substitute of PSTN. VoIP technology transmits voice signals over the internet using packet switching technique by converting consumer's voice into packets. These packets travel through the internet from source (sender) to destination (listener), upon being collected; receiver or listener of these packets gets desired voice [VoIP deployment for dummies, 2009]. However, new elements with more advantageous features are introducing in VOIP infrastructure. Because of this emergence, VoIP technology has evolved towards various QoS questions and security threats. Mainstream of the VoIP service provider presume that introducing new features is sufficient to make good use of VoIP technology, and the consequences are, user's nitpick concerning poor voice quality and security assurance, are becoming more every day. In this project will be shown some effectual results concerning VoIP PBX issues which are based in actual environment.

1.1 Aim and objectives

Aims and Objectives part describes different stages concerning completion of this project.

Aim of this project is to identify vulnerabilities of the network based on VoIP technology and introducing basic techniques to secure the network in real time environment.

- To Understand VoIP tools in a real time environment by implementation
- To Design and optimize VoIP PBX infrastructure
- Configuration to Provide free domestic and global platform
- To Configure trunks for inbound or outbound routes
- Evaluation of different QoS parameters such as (Packet loss , Jitter and Latency)
- Pen-testing concerning VoIP security

1.2 Problem definitions

At the moment, inside communication industry, VoIP service is the most major tool which has significant impact and adopted by millions of users with furthermore mounting figure. In

present, it is possible for everyone to communicate with everyone globally by using VoIP services. Because of long list of advantageous features, flexibility and easy availability, the rate is also low. To exploit VoIP technology services, two major elements are considerable, a good QoS and voice Security. These elements rally round to encourage end-users to switch to VoIP technology to deal with their telephony activities every-day. Among these two nucleus elements, enhancement of security is the chief focus of this project. This paper will provide some efficient techniques from the past work and will be proposed a number of precious exercises.

1.3 Methodology

VMware, generally known as virtual operating system (OS), used in designing of VoIP based infrastructure in a live environment for the evaluation of QoS and security pen-testing of the VoIP calls.

1.3.1 Project requirements

- Personal Computer (PC)
- Virtual Machine (VMware)
- IP PBX (TrixBox 2.8.0.4)
- NETWORK Behaviour Monitoring Software
- Back-Track machine
- University Library Resources

1.3.2 Scenario

Choice of Scenario, a network is designed in live environment for the evaluation of QoS and pen-testing, concerning VoIP services performance and security.

1.3.3 Expected Results

- Designing of VoIP based network
- VoIP based call testing among different networks
- Inbound or Outbound call setup, domestic or international
- Evaluation of QoS by using network managing software
- Pen-testing concerning VoIP network vulnerability and security

1.4 Organizing documentation

Section 1: this section covers basics about the project. Such as, introduction, aims and objectives, methodology, problem definitions, basic project requirement, scenario and initial expected results.

Section2: this section covers Literature review. In this section report will provide brief introduction of Voice over Internet Protocol (VoIP), Private Branch Exchange (PBX), Quality of service (QoS) and its parameters (packet loss, jitter, Latency) and VoIP security.

Section 3: this section covers designing and optimization of network phase of this project.

Section 4: this section of the report will be highlighted expected results of evaluation of the QoS with description.

Section 5: this section based on penetration testing results of VoIP calls.

Section 6: this section will provide conclusion and some future preferences for better exploitation of VoIP technology.

1.5 Summary

Section one of this report covers basics about the project. Such as, introduction, aims and objectives, methodology, problem definitions, basic project requirement, scenario and initial expected results.

Next chapter is based on literature review and also will be providing detailed information relevant to previous work.

2 Literature Review

The description provided about the Following apparatuses is acquired from the previous research work:

2.1 VoIP

In past few years, Internet Protocol (VoIP usually is) has turn into a fit image than voice telephony technology of the industry. With additional features next generation VoIP telephony systems present term used to refer to. VoIP technology such as low cost and flexibility providers and end users, which is beneficial for both features promises to provide a great degree. VoIP packets on the Internet by changing his voice traffic signals. VoIP technology applications and protocols, especially a group of them on the internet to carry voice signals out who is responsible for the performance of specific tasks. VoIP services have changed the mode of telephonic conversation by providing empowerment to large, middle and small businesses to establish their personal telecommunication system with several added features like as, use of multi-carriers to save call charges and superior quality service. VoIP also contains feature to establish calls between PC to PC, PC to mobile, and mobile to PC etc. In general, VoIP service provider offers service at lower rates for making calls than old telephony companies.

In Voice over Internet Protocol (VoIP), technology has ability of transporting Voice packets by making use of Internet protocol (IP). VoIP technology service can easily attain by selection of required software and hardware and communication standards as the number of these are available. VoIP technology used to packetize the voice data and transport these packets using Internet [VoIP deployment for dummies, 2009]. The use of VoIP services is quickly growing up. Although, there are many active corporations that offer and implement VoIP services. For example, Microsoft Netmeeting and Skype application. VoIP services demand is getting increase everyday as VoIP costs is far less for the customer than the traditional telephone system in particular for international calls. One of the main advantages of VoIP services is, VoIP services provides superior Management for provider involved and also cost is very less as organisation could have single set-up for both data and voice as well, so it is beneficial for both customers and as well as service providers [Practical Implementations for Securing VoIP Enabled Mobile Devices, 2009].

2.1.1 History

Around Twenty years ago, to communicate with some person far than few steps expected pick-up the phone receiver and dial numbers. Those calls departed through Public Switched Telephone Network (PSTN). According to the demand, ever-increasing accessibility on fixed-rate broadband connections was the main source in 1990. To be created automatically an opportunity for an alternative to PSTN. Which was about to treat voice and as well as video signals as a data packets and transmit it using the Internet as a medium. This moved towards development and rose up as VoIP [An Introduction to Standards-Based VoIP: SIP, RTP, and Friends, 2010]. VOIP is fetching more popular than previous, and is sketching rapid mounting interest from all participants involved. It's been over a decade, Yahoo announced their latest edition of Yahoo, that provides facility to the consumer to establish voice calls anywhere globally over the internet, this was a big explosion inside telecommunication industry. Granting, to TM Global Knowledge, mainstream of telecom service transporter are engaged in the progression of hatful production of VOIP technology services [Security in the New Era of Telecommunication: Threats, Risks and Controls of VoIP, 2008]. The derivations of VOIP technology can be track reverse to ARPANET days. In early 1973, Internet associated person "Danny Cohen" from Information Sciences Institute, University of southern, California, build up and also put into practice a network called Network Voice Protocol (NVP). This network based on mechanism in which data converted into packetization to transport speech [An Introduction to Standards-Based VoIP: SIP, RTP, and Friends, 2010]. Network Voice Protocol established a technique to present "safe, low-bandwidth, real-time, high-quality, and full-duplex (to way communication) and digital voice communication on the internet and packetized data which can easily be delivered secure by using existing encryption elements. The modern-day VOIP technology is the progeny, and commercialized creation of Network Voice Protocol (NVP),[Security in the New Era of Telecommunication: Threats, Risks and Controls of VoIP,2008].

2.1.2 Features

A network based on VoIP technology, offers many more advantageous features over Public Switched Telephone Network (PSTN):

2.1.2.1 Infrastructure

It is very simple to create a small network if having both, Internet connection and PSTN, and there is a need of two devices for VoIP infrastructure at home or in office. One of these services carries IP packets and other transmits voice calls. Furthermore, there is a need

separate apparatuses all through the structure, includes phones sets, switch, etc. But in case of VoIP infrastructure, there is only need of joint infrastructure enthusiastic with IP service.

2.1.2.2 Free calling

Partially from the historical point of view, circuit switched telephone services are characteristically metered, while, broadband services are usually flat-rates. VoIP technology allows its users to exploit existing broadband connected to enable voice service at no supplementary insignificant cost, as long as they making calls other VoIP-enabled users.

2.1.2.3 Quality

VoIP technology, another greater feature of VoIP is superior voice quality. Over the circuit switched phone networks, only acceptable codec is G.711, which strictly restricted to audio fidelity. While, VoIP based phone system allows a wide range of codec and also negotiation in codec, consequently, VoIP offers a potentially feature rich calling opportunity.

2.1.2.4 Flexibility

Because VoIP technology deals with the packetization form of voice signals which is just an additional type of data, VoIP technology offers services that can be easily integrated efficiently with voice and video, instantaneous messaging, and also track to occurrence [VoIP security, 2007].

Key element is that we can have a number of features without deployment of VoIP technology universally. For example, an enterprise can create a small VoIP-based infrastructure inside and can integrate this with PSTN for outbound calls, (when someone make call from inside the enterprise to someone outside). It like, using of traditional PSTN services to transit calls between own sets nodes through switches over the Internet by using IPs, in consequences they exploiting the existing broadband connection for saving of costs [An Introduction to Standards-Based VoIP: SIP, RTP, and Friends,2010].

2.1.3 VoIP standards

This section of the report highlighting the most widely used VoIP standards:

Session Initiation Protocol and H.323

Session Initiation Protocol (SIP), a frequently used VoIP protocol to start the signalling process for VoIP calls to commence, modify and finish the call. The main apparatus of SIP is a proxy server to instigate the call process when a consumer phone up a number. Another factor of SIP protocol is the location server which used to locate the position of an end point or receiver. SIP offers various techniques beside the audio and video calls facilities. it offers

great opportunity such as audio and video conferencing, multimedia session and instant message conversation. Also, SIP uses for Uni-cast and multicast progression. Furthermore, it offers incredible features of changing address or ports numbers and also used to send invitation to new joining members. Therefore, anyone can attach or remove media tributary, call forwarding session, call holding, caller recognition, transfer to voice mail and billing process, [VoIP, wireless, P2P and new enterprise voice over IP 2008]. Session Initiation Protocol can work despite as a part of transport layer. It is also feasible in working with TCP and UDP. SIP is designed structure which is somehow alike to the design of HTTP. SIP is a transcript base protocol and it can be easily unmitigated to include newer features into it. Session Initiation Protocol is based on signals so the portrayal of the medium session is prepared by using other protocol such as the Session Description Protocol (SDP). Despite the session of the media is a VoIP, video streaming and video games, these description make this protocol more standardized as a signalling standardized protocols [Practical Implementations for Securing VoIP Enabled Mobile Devices, 2009].

H.323 is a comparable protocol to SIP which can be easily used to manage the signalling process in IP based networks. This protocol offer many services similar to Session Initiation Protocol. These Both protocols (SIP and H.323) provide similar features in different method. (Example), both protocols offer services such as put call on waiting, put call on forwarding to any other extension and call transfer [scalable VoIP mobility,2009].

2.1.4 VoIP requirements

Several companies have knowledge about the features rich importance of VoIP technology. In 1998, VoIP technology became gifted to make calls between phone-to- phone and PC-to-phone Internet broadband. In the last decade, VoIP technology has become very industry accepted as one has the precise equipment such as (hardware, software and broadband connection). An updated research [Practical Implementations for Securing VoIP Enabled Mobile Devices, 2009] shows that nowadays, the most of the voice calls are made by using Internet connection. In order to create a small indoor VoIP based network to make calls, one just needs a VoIP technology enabled devices and a good Internet connection or on the other hand also has other choice to buy or download software (softphone) to make a VoIP call using personal computer.

2.2 IP PBX

VoIP emerged as the method of communication technology, follow up traditional public telephone network (PSTN) to provide reliable changed as suspect. The potential to become a

credible alternative to PSTN is PBX. Effective Communication such as PBX and enable reliability to the organization to provide significant savings not only helps the exchange to a feature rich telephony. Been named as PBX with total privacy and their own low-cost communication infrastructure provides feature to create groups. PBX, IP PBX system as well known because supports a VoIP call. New technology based developments are being established in PBX's with mounting values [VoIP, wireless, P2P and new enterprise voice over IP 2008]. The PBX system is certainly varying with introducing of entirely solid state invention using Large Scale Integration (LSI) techniques. With the Changes because of the technology advancements, demands are also increasing every day. The use of VoIP technology by businessmen, the look further for more rich features, greater and flexible application, incredible low initial and operational costs, reliability and less continuation costs [Current Trends in PBX Power Supplies, 1978].

2.2.1 Background

Private Branch Exchange (PBX) is the term used for phone calls, since early 1960's this technology have been in use for reducing call expenses in businesses accordingly their needs, in terms of communication. Early Private Branch Exchange systems were adverted to as Private Automatic Branch Exchanges (PABX) and their implementations were started in early 1960's. The reason behind increase in demand of these systems, they were capable to streamline to industry manoeuvre and reduce costs of communication by offering them to create a personal telephone network to be dedicated to business necessities.

In start, PABX systems were innovatory contraption because they allowed businesses to create their own telephonic exchange for internal calls without use of public switched telephone network (PSTN). This technology placed offer which applies without a receptionist interaction to transfer internal calls from one extension to another inside the building. Private Automatic Branch Exchanges also approved external lines to be freed- up from internal traffic, as businesses required smaller number of lines. PABX also appreciably improved functionality of communication and condensed its expenses in terms of businesses requirements. In 1990's, Private Automatic Branch Exchanges (PABX) telephonic systems had begun to be known as Private Branch Exchange (PBX), a term which stick with even today. In those days, new Technologies were emerging in PBX systems and were easily available, but there was a drive back from the industry reputed tycoons and they didn't want to upgrade an entirely new infrastructure because it was on hands at far more expenses each time when Private Branch Exchange system improved.

By emergence and modification PBX systems turned out to be more flexible, and it provides aptitude to the final consumer to add or remove ports and also increase network capability and functionality. These days, Businesses can modify or increase communication era without having a new system each time with additional costs.

Features such as auto-receptionist, data integration, and increased level of telephonic communication applications have become necessary and packetization technology has become root of communication industry [history of PBX Phone Systems | Reviews, Comparisons and Buyer's Guides. 2013].

2.2.2 Architecture

Due to the rapid expansion phase of all communication technology based application and systems which also origin of vulgarisation of the Internet. Next age-group communication Networks will be having chief command on existing communications technologies. New communication based devices and applications will have covered conventional PSTN type of voice and data, in next few years. However, Next-Generation Networks will have greater advantageous features than present and traditional network systems based on communication. However, it is undoubtedly true to discard the existing networks for a newer one. IP PBX (term used for PBX which support IP) system founded on the soft-switch technology and has capability to be integrated with the existing data networks or telephone networks in enterprises internally. IP PBX system offers a standardized platform to support multimedia communication applications and devices attached and support audio, video and data [Design and implementation of IP PBX architecture based on V5 interface, 2011].

2.2.2.1 IP

IP based network architecture performs all of its switching process in Internet Protocol's world, so there lies no transcoding between Time Division Multiplexing (TDM) and IP. Because of scalability and no hardware requirement to packetize signal, IP based networks are considered more beneficiary than others. "Examples" (3 Com NBX, 3Com VCX, Asterisk, and Call Manager Cisco).

2.2.2.2 Hybrid IP

Hybrid IP network architectures convert media session among internet protocol (IP) and time division multiplexing (TDM). This means there is more sources are required for transcoding. Characteristically, Hybrid IP network architecture systems contain certain boundaries that how many IP phones can be placed. "Examples" (Avaya Comm Manager, Avaya IP Office, Nortel BCM, and Nortel Succession).

2.2.2.3 Linux

Linux operating system offers a well-built platform for IP PBX. However, Linux systems are pretty reliable exercise but its installation expenses are considerably higher. Examples are 3Com, VCX, Asterisks, and Alcatel etc.

2.2.2.4 Windows

Windows operating systems allow new technology based devices to be integrated with other applications more frequently. Maintain security patches in these platforms are quite difficult than other. Windows based Examples are “Cisco Call Manager, Nortel BCM,, Vertical Communications Instant Office, Toshiba Strata CS and Vertica Communications.

2.2.2.5 Real-time

In term of reliability, Real-time operating systems are familiar for completion of operations. However, many application servers are required sometimes to complete operation but these systems are not able to be easily integrated with other. Examples of companies using these type of Operating Systems include VX Works - 3Com NBX, Nortel Succession, Nortel Norstar, Nortel Meridian, and proprietary OS - Avaya Definite [Design and implementation of IP PBX architecture based on V5 interface,2011].

2.2.3 Functionalities

This section of the report contains discussion about a brief introduction concerning integration of voice and data Services and the responsibility of PBX system for providing such integration services for local enterprises. Conventionally in offices, the method was preferred for communication was verbal communication, either directly or by use of a telephone line. Nevertheless, the extensive development in communication technology has significant Result over communication based networks environment (LAN's) which are widely used to exchange the large multiplicity and ever mounting amount of data produced [scalable VoIP mobility,2009]. There were excellent reasons to join manage the functions of both voice and data over a one single integrated medium, VoIP based PBX systems have evolved and added effective features to manage voice and data transmission and organize them. Thus, PBX systems are quite recognizable in enterprises and regardless of the extensive use of computers are possible to remain in the predictable prospect.

Consequently, PBX systems are in a productive point to manage with data services as they grow, mainly as there were prediction of development in managing combined voice and data services such as storage of data, while engaged with most predominant traffic–speech

[Integrated switching system: a distributed star network for integrated voice and data traffic,1988].

2.3 QoS

VoIP is possible substitutes of PSTN, so it is not sufficient to be less expensive, easy to implement and easily manageable. It must have capability to provide superior call quality image or at least equally standardised to PSTN. So that it would be a motivation for clients to switch over VoIP. However, in present, VoIP lies in a row of top of the IP networks, but when transmission passes through different network stages such as gateway's boundaries, so it might gets some performance problems. The parameters of QoS are also affected by the delaying firewall and blocked premises of network for encryption. Such as,

2.3.1 Parameters

2.3.1.1 Packet loss

If packets get lost from the packetized data, during transmission that is known as packet loss. In IP based infrastructure, packet loss may occur due to deprived connection where medium become fails to transmit packets successfully. It is brutally consider as dreadful conditions of IP network.

2.3.1.2 Jitter

A fluctuation in delay timings during transmission of packets is called Jitter. It normally falls out when transmission of voice packets contains different measures in timing during call duration on the internet.

2.3.1.3 Latency

Latency, voice packet transmit duration from source to destination via internet is called Latency. Thus, by researchers, 150ms delay in packets transmission is countable as high quality service [VoIP, wireless, P2P and new enterprise voice over IP 2008].

Same Security measures are not able to be implemented in VoIP as the same was in conservative networks. Intrusion detection system, firewall and other security and network component are necessary to be use in VoIP based network.

2.3.2 Importance of QoS

VoIP is a real-time voice and data communication service which based on telephone or computer in network infrastructure or using internet for wide area communication. QoS provides usage, attributes and requirement level as per user request using H.323 and SIP framework series. To analyse of vulnerability measurement of security in VoIP based

network, the measurement of QoS parameters is a systematic level of process. Without improvement in Quality of QoS parameters, improve the security encryption levels and systematic quality is just not possible. Measurement process of QoS is divided into three parts, measurement of Quality, measurement of speed, and functional support [VoIP QoS (Quality of Service) Design of Measurement Management Process Model, 2010].

2.3.3 Integrated services

Integration of services to provide and improve the method of the QoS is depends upon flow of bandwidth reserving protocol. Integrated services system is being used as RSVP signalling method. A definite quality of service asks for the session of the user's session of network bandwidth when RSVP utilises. Supporting integrated services for QoS is a still have significant impact in IP networks. Various integrated services required their own QoS; a proper traffic management is required when congestion occurs between different nodes of the network to manage traffic. Voice is the term used for a session stream of voice from the sender to send the message by using RSVP case. Each path of the message recognises of its resources first before sending the message that each node assigned a new RSVP. Refreshing path of every node to route instant reservation in integrated services to keep the session on hold, must be sent gradually over the network. Once the user checked the path message sent and the user of the session were got involved and wishes to carry out and the message sent by the RSVP reservation will be sent back. RSVP reservation system is only single way, The reason of the process of bidirectional would be valid in and out.

Once session been established, each route of the session of integrated services system must be periodically maintained. Messages and RSVP route in between the routers must be sent periodically to avoid any mishap of the soft state time- out [VoIP, wireless, P2P and new enterprise voice over IP 2008].

2.3.4 MPLS traffic engineering

Wide area network (WAN) connection is a very expensive service for an Internet Service Provider (ISP) within the budget limit. By using MPLS traffic engineering, ISPs route traffic to the users on best offers and also provide best throughput and delay. By enabling MPLS traffic engineering, service provider provide services more efficiently and also it helps to reduce the network services cost.

However, many service providers rely over the overlay model. Layer 2 switching model uses to manage the transmission services in an overlay model. To get the precise control of bandwidth which used by the traffic, IPS use layer 2 transit layer explicitly. MPLS traffic

engineering system offers track to achieve a number of benefits as same as of the overlay model. For that purpose, neither we need to run a separate network nor need of any non-scalability of router interconnections. MPLS engineering contains following features:

Packet transportation by MPLS crossing of multi-hop Label Switched Path (LSP)

Signals and route capability

Understanding of topology and resources

Managing bandwidth is one of the core functions of the network and also it acts as a aggregation chore of QoS. MPLS traffic engineering system takes decision immediately for the new session without consulting multiple routers [MPLS Traffic Engineering – Cisco System. 2013].

2.4 Security

Security matters when privacy and discretion requires. In IP based network, alongside the QoS, network security also considers as an important factor that it would be a motivation for clients to switch over VoIP. Discretion and privacy are used to deliver consumer's anticipations to the contributor that data and calls are safe from outside attacks, such as eavesdropping attacks and call hijacking operations. Today, IP based networks covenant with innumerable clients and with their activities resourcefully. Though, behind the chain of feature rich benefits, IP network also escorted of security challenges. In IP networks, there is a number of challenges higher than old PSTN because of enormous user's data-base. IP network based on signals and they are not able to identify that client is genuine user or non-genuine eavesdropper. Other side, in PSTN system, attacker's physical access required to destroy infrastructure. In last few years, communication has been moving regularly toward the VoIP. However, security skills are not capable to run parallel. In this project we will discuss a number of security aspects concerning VoIP call security.

2.4.1 Challenges and vulnerabilities

Security concerns where privacy and confidentiality require. Security consider as a sensitive and essential part in every communication network because conversations within users or employees are privacy sensitive and good for company policy. That is the reason companies use firewall and higher level of security patches according to their importance of data, to make sure that nobody is eavesdropping or accessing the private data. though, it is quite unsafe to send unencrypted voice packets on the internet, the reason is over the internet, messages pass through several phases in terms to reach to the it's correct destination, in that

case if some of these systems are not in control fully or have low security patches enabled so computer hackers might eavesdrop or change the real data. To avoid misuse of our data, higher security encryption level must be enabled before data sent through the internet, to avoid unauthorized access [Practical Implementations for Securing VoIP Enabled Mobile Devices, 2009].

2.4.1.1 Denial of service attacks (DoS):

This kind of attacks works because security parameters of the system get exhausted or they are no more engaged in these types of attacks.

2.4.1.2 Access attack:

Attacks of this nature take place by an unauthorized person, who attempts to get access to confidential information, for which he has no authorisations. Sometimes, Access attacks can affect both privacy and accountability of security services.

2.4.1.3 Modification attack:

Modification attacks take place when unauthorized person attempts to amend or modify private and confidential data. These kinds of attacks affect both the reliability and accountability of the organisation [Practical Implementations for Securing VoIP Enabled Mobile Devices, 2009].

2.4.1.4 Vishing:

The process of spoofing of VoIP services and caller ID is called vishing. These kinds of attacks are often hidden behind such companies which do not exist actually. Players of these attacks try to get private information to theft money through internet. Most likely phishing attacks this kind of scams inculcated by phone call where they make known account holder's information.

2.4.1.5 Toll fraud:

Toll fraud attack is one of the most common attacks of the VoIP based networks. These attacks are concerning unauthorized call making by exploiting weak username and their password [Voice over IP security, 2010].

2.4.1.6 Spam over internet Telephony (SPIT):

This type of attack indicates alternative spam attack of an unwanted email. These type of attacks collecting from spontaneous e-mail user. Spam over Internet Telephonic attacks makes cause of disturbance of users by unsolicited emails and advertisement. SPIT can be a call from a call centre for the purpose of selling products. But it is leading towards

discomfortness of users [Detection and mitigation of spam in IP telephony networks using signalling protocol analysis, 2005].

2.4.2 Firewall

Organizations which are linked with internet, mostly like to use of Internet firewall to diminishing risk level of network, data theft, data demolition, and other security severances. One of the useful features of firewall is that it provides a central location for deployment of security. Internet firewalls, although, inflict an excessively plain inside and outside replica concerning security breaches that is not compatible with business needs, requires leading out insufficient expectations to external unit. Furthermore, firewalls security outer limits are not enough to secure a network entirely, because firewalls do not provide any protection from indoor attacks. Firewalls do not promise for any protection of sensitive information, which can be easily transmitted by inside permitted protocols. Today, Security firewalls in IP network is a staple requirement to secure voice. It is also even truth, if we say that firewalls are lie in first line to protect a computer, networks or even VoIP based networks. Processing of IP based network's transmission through firewall is already determined in programme rules. However, more multifarious sets of rule are featured in firewalls. Today, elimination of basics as firewalls, and as Internet evolving direct to applets, mobiles, and object frameworks, these problems likely will get worse [Domain and type enforcement firewalls,2000].

2.4.3 Encryption

Therefore, switching of communication medium to IP based infrastructure, is indicating several security threats such as Denial of Services (DOS), Call Hijacking, Eavesdropping attacks, Man-in-The-Middle attacks, and Phishing spam. In recent days, VoIP technology has become popular in communication era, uncertainty also concerns for VoIP security. In order to address these problems and prevent our network, a number of solutions concerning with security threats, have been programmed. Which also helpful to prevent user data and diminish the threat of attack, for example, Firewalls, Virtual Private Network (VPN) setup and Encryption keys [Is Implementation of Voice over Internet Protocol (VoIP) More Economical for Businesses with Large Call Centres, 2010]? Encryption method is the term used for furnishing data inaccessible by unauthorised persons. Encryption key exchange process works throughout encryption algorithm to convert plain-text into cipher-texts to encrypt by the sender and decrypt by the recipient of data. Though, there are couple of main classes of encryption keys: 1) Asymmetric, in this class, more than single set of keys employ

for encrypt and decrypt data. 2) Symmetric, in this category same key is used to encrypt and decrypt of data. Speed of Cipher encryption class can be counted a very vital part when approaching to encryption algorithm level in terms to find out strength or limitation. Speed is a confidential obstruct that supports bound such as data duration, how much is time taken by a plain-text or cipher-text, and key-length [Impact of Encryption on QoS in VoIP,2010].

2.4.4 IPSec

Internet protocol security (IPSec) is divided into two core components, Authentication Header (AH) and Encapsulating Security Payload (ESP). IPSec security protocol has ability to be integrated with the gateway operating system to present requisite confidentiality, integrity and availability to substitute data with external network. As explained above, IPSec consist two protocols named ESP and AH, for the safety of the IP traffic [The New Security Standard for the Internet, Intranets, and Virtual Private Networks, 2003]. AH provides data legitimacy, integrity and protection. Encapsulating Security Payload offers same feature as AH provide, and additionally it offers greater level of confidentiality. Internet Protocol Security (IPSec) works in two different modes. 1) Transport mode, IPSec offers security for upper layer protocols. 2) Tunnel mode, IPSec tunnel mode provides protection of the complete IP data-file. Tunnel mode works when target destination of data is dissimilar from the security termination point. In tunnel mode, whole data-file is encapsulated by a further IP packet, and the IPSec header is enclosed among the external IP header and the central IP header. When a network has safety gateways in a packet pathway, then security gateway use to decrypts outer header of the packet, and sends it to its destination IED accordingly internal IP header. Security associations describe that how IPSec enabled end-points Secure traffic. Security policies are used to classify that what traffic is to be protected by IPSec protocols. These security polices provides legibility to assign separate policies to different IP traffic, that is the reason that remote observation, maintenance issues and managing traffic can be secured with different IPSec policies independently [Implementation of IPSec in substation gateways,2012] .

2.5 Summary

This section covers Literature review. In this section report will provide brief introduction of Voice over Internet Protocol (VoIP), Private Branch Exchange (PBX), Quality of service (QoS) and its parameters (packet loss, jitter, Latency) and VoIP security.

Next chapter contains designing and optimisation phase and configuration steps.

3 Designing and optimization of network and results

3.1 Network design and tools

VMware, a virtual Operating System used for the completion of this project. VMware Version 8.0.2 is used for designing, configuration and implementation. This virtual operating system is user-friendly and easy to understand. Various advantageous features make this useful comparatively with other available virtual operating systems such as, Windows Virtual PC, QEMU and VirtualBox etc. These virtual operating systems can exploit by network developers and researchers for new inventions and as well as for testing purposes which can be developed in real time environment after successful experiments. For the research organisations, these tools are very useful in terms of saving money.

This project based on one single scenario. This Scenario is of a small scale enterprise setup for communication inside the organisation, receiving inbound calls from outside and making outbound calls from inside by using different devices with the same caller ID. Same setup design can be implemented in large scale enterprises by extension of tools and space according to the requirements. All this setup is been done in virtual environment using VMware tool.

3.2 Network Requirements

General requirements for this project are, personal computer (PC) or lab computer of University of Bedfordshire, VMware 8.0.2, TrixBox PBX 2.8.0.4, Soft-phones (X-lite and 3CX), VoIP PBX hosting (sipgate). All required components and features are available in VMware concerning completion of this project.

3.3 Scenario and Results

This Scenario is of a small scale enterprise setup for communication inside the organisation, receiving inbound calls from outside and making outbound calls from inside by using different devices with the same caller ID. An organisation, for which it is necessary to make and receive a large number of phone calls within the organisation or outside, every day, can implement or use VoIP services to save costs. Configuration steps are as follow:

Initial installation

First, VMware (virtual operating system) was installed on a computer. After that a TrixBBox CE (telephony platform) installed successfully in VMware. Give your login detail, and to access to the TrixBBox PBX server, go to command prompt of the TrixBBox and run command:

Comm.: `ipconfig >> enter`

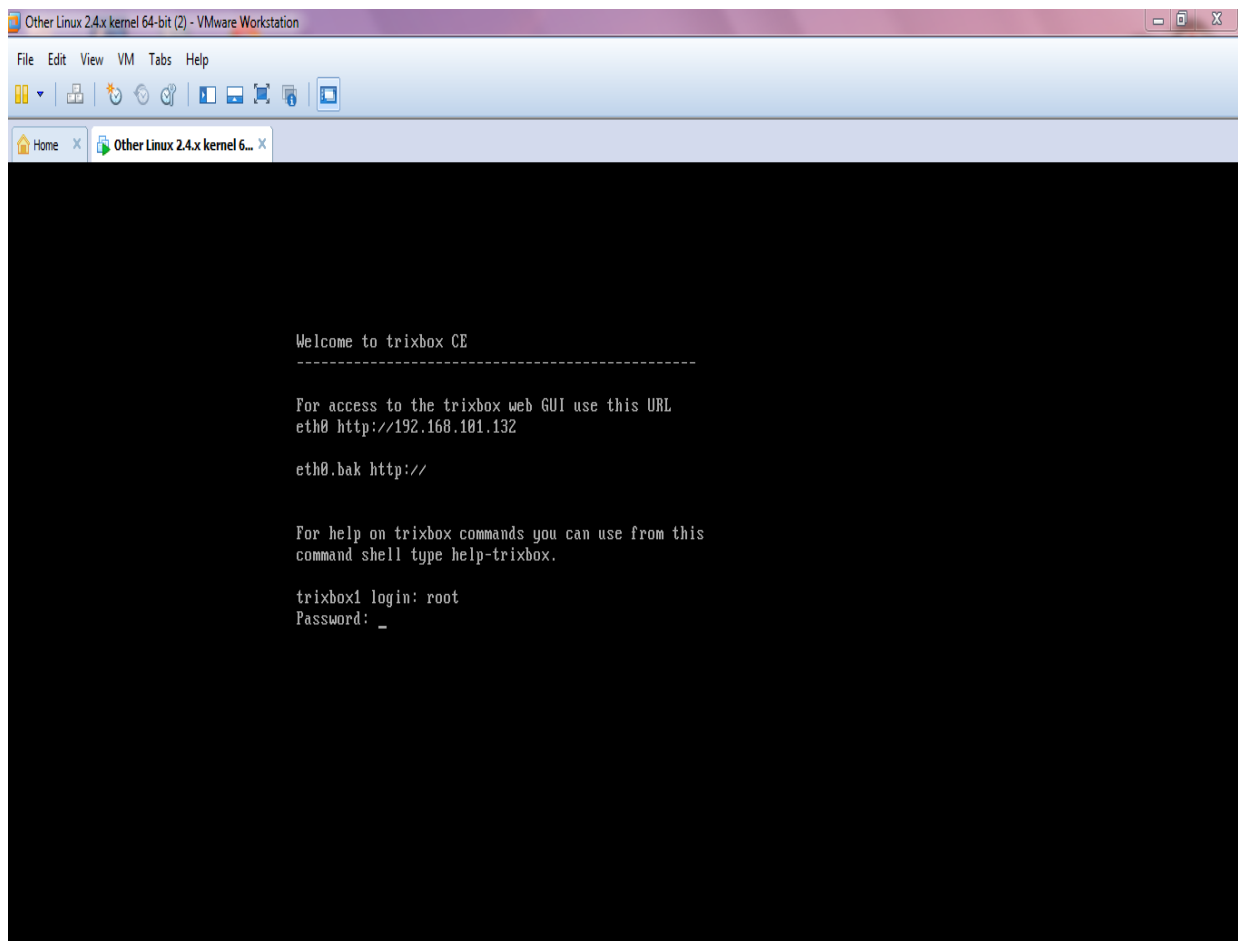


Figure 1: starting TrixBBox server

Above is the result which shows an IP address (192.168.101.132) to access of the TrixBBox PBX server. Write this IP address in your browser. Following page will be open:

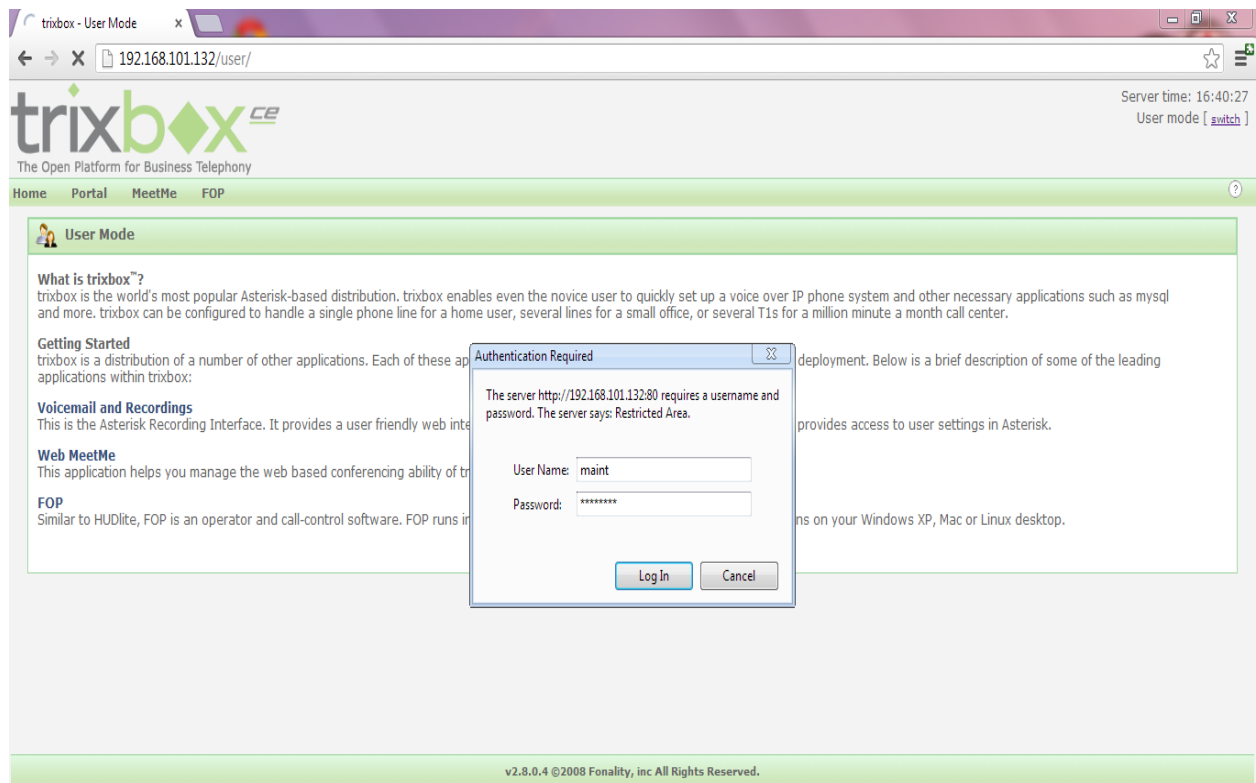


Figure 2: online access of trixbox

Click on the switch button showing on the top on right hand side, it will ask for user name and password, which is:

Username: maint

Password: password

This is default username and password. There is also an option available to change username and password according to your desire.

Create extensions

To create an extension, after logged in on TrixBBox PBX server:

Click PBX >> PBX setting >> click on extension on left hand side.

“Generic sip device” is showing in front of “Device” in the box.

Click on “Submit”

Following page will be open:

Write user Extension: 501 (example); any number can be user extension

Write Display Name: Naveed (example)

“SIP Alias” will be the same as user extension (it support direct users dialling internally)

Write password (Secret): 12345678; (any number or combination)

Click Submit >> then click on “Apply red bar configuration changes” will be shown at the top of the page.

The screenshot shows the 'Add SIP Extension' page in the FreePBX web interface. The browser address bar shows '192.168.101.132/maint/index.php?freepbx'. The left sidebar contains a navigation menu with categories like 'Setup', 'Tools', 'Admin', 'Basic', 'Inbound Call Control', and 'Internal Options & Configuration'. The main content area is titled 'Add SIP Extension' and contains several sections: 'Add Extension' with input fields for 'User Extension' (501), 'Display Name' (naveed), 'CID Num Alias', and 'SIP Alias' (501); 'Extension Options' with dropdowns for 'Outbound CID', 'Ring Time' (Default), 'Call Waiting' (Enable), 'Call Screening' (Disable), and 'Emergency CID'; 'Assigned DID/CID' with fields for 'DID Description', 'Add Inbound DID', and 'Add Inbound CID'; and 'Device Options' with a note 'This device uses sip technology.' and input fields for 'secret' (12345678) and 'dtmfmode' (rfc2833).

Figure 3: creating extension named <Naveed>

In the following page, result shows that “ naveed <501>” has been successfully created.

I have created two more extensions “ faisal<502> and faheem<503>” using same method. As showing in the page below.

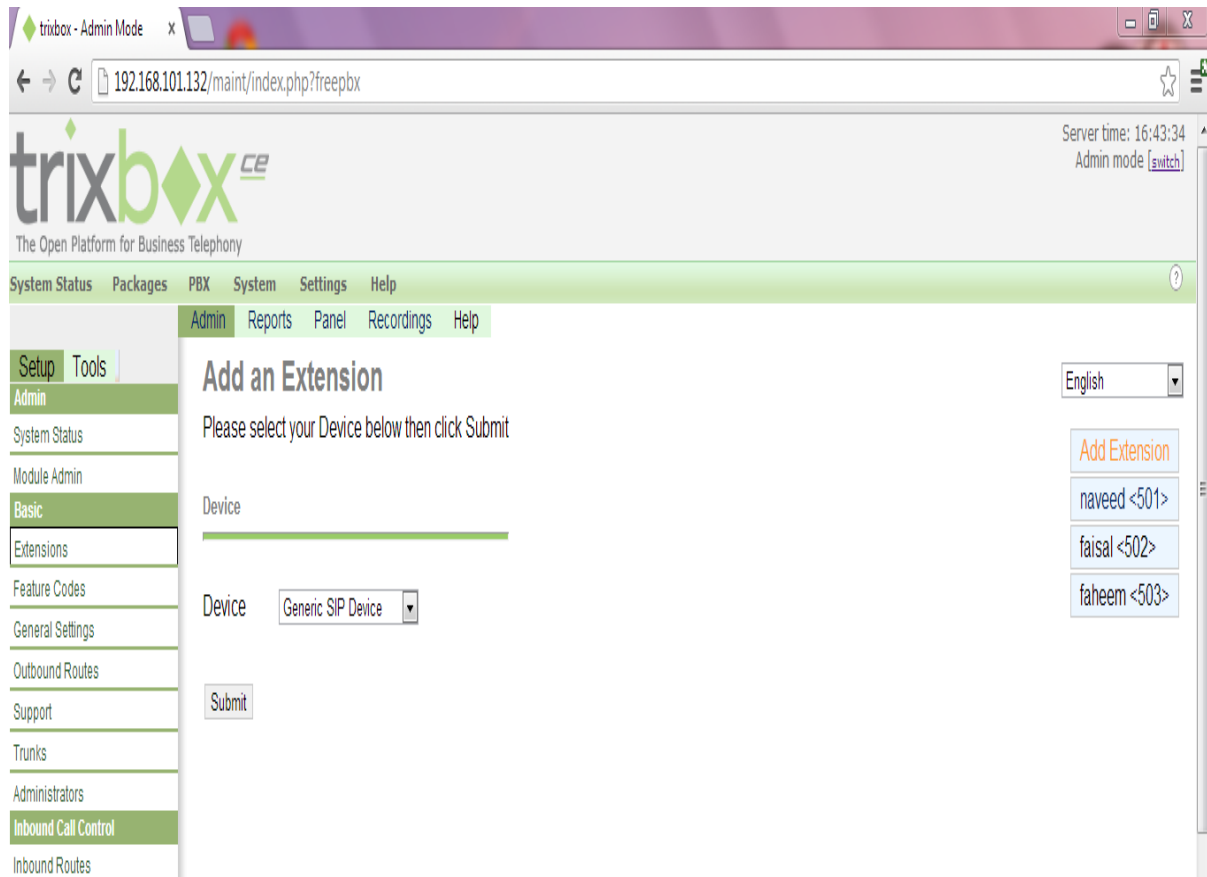


Figure 4: three extensions created

Soft phone

Next step is soft phone installation and their configuration. Such as X-lite and 3CX.

X-lite:

Click on softphone option >> account setting

Account name: Faisal >> user ID: 502>> Domain: 192.168.101.132

Password: 12345678 (secret) >> display name: 502

Click OK

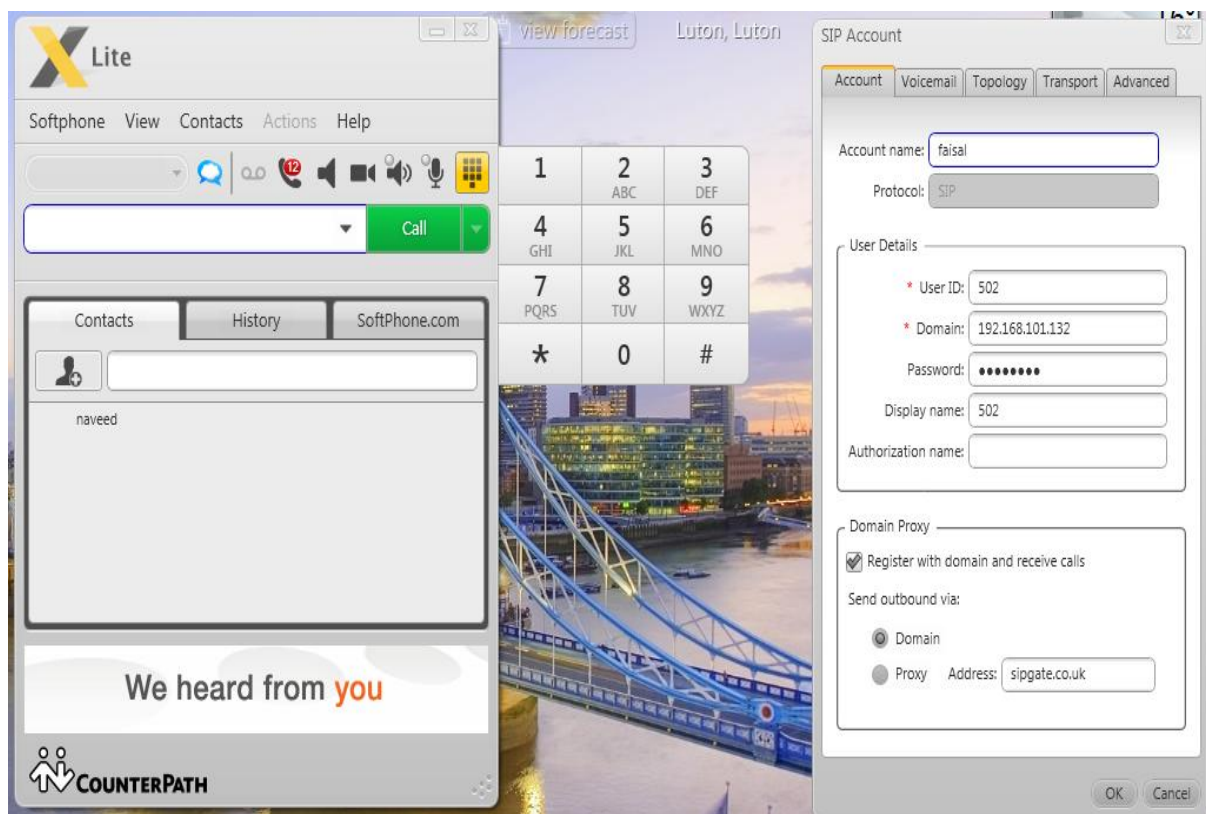


Figure 5: X-Lite softphone setting

SIP account (extension: 502) has been enabled on X-lite softphone.

3CX:

Install 3CX softphone on your computer.

Right click on the softphone screen >> click on the “account” icon

A menu will be open. Click on the “edit” option on the right hand side.

Another menu will open as following.

Enter account name: rana >> caller ID: 501 >> extension: 501 >> ID: 501

Password: 12345678 (secret) >>

I m in the office- local IP : 192.168.101.132

Click OK

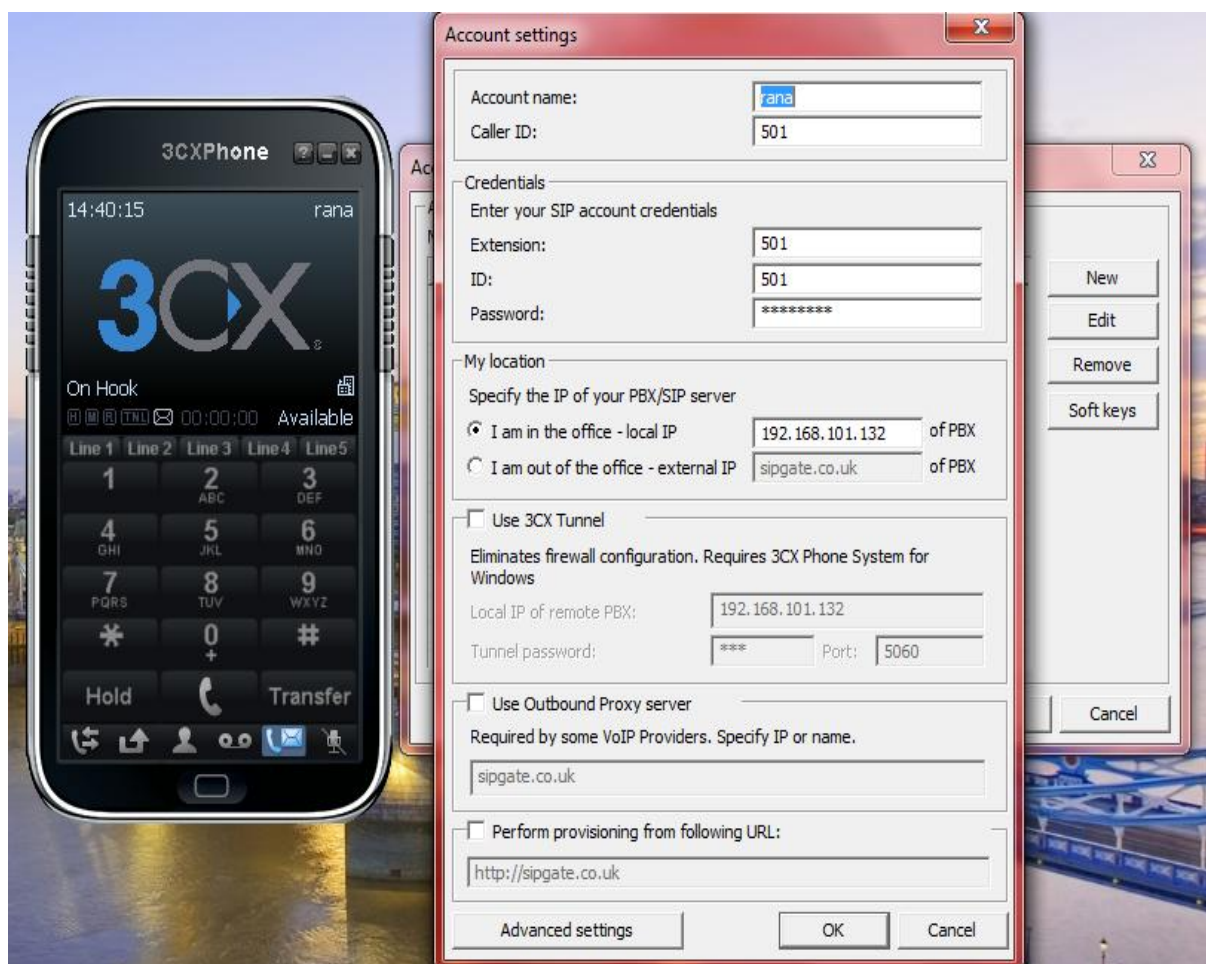


Figure 6: 3CX softphone setting

SIP account (extension: 501) has been enabled on 3CX softphone.

Test call

Following image is the result of successful VoIP call between two extensions <501> and <502>.

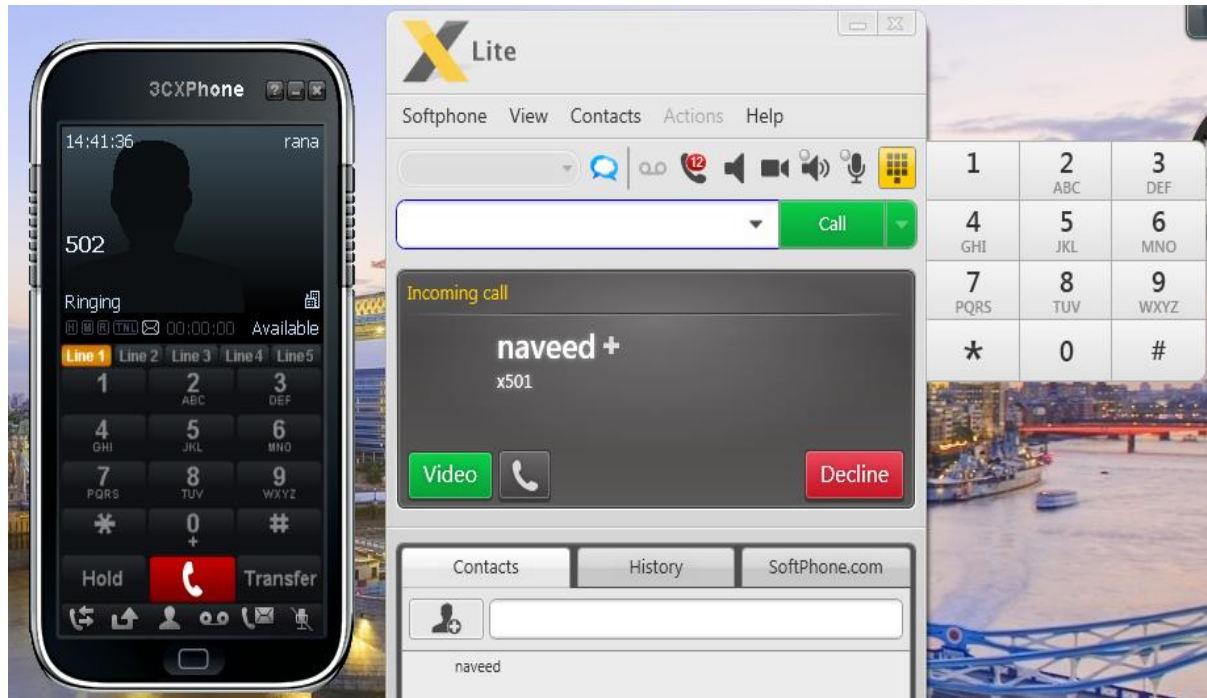


Figure 7: successful test call among extensions

Voice-mail setting

To setup a voice-mail service, go to PBX setting >> extensions >> get in extension “naveed <501>” >> scroll down to voice-mail and directory:

Select enable >> voicemail password. Use something you can type on a phone keypad like '123456'. Enter an e-mail address where you would like to receive your voice messages sent and click submit. Then click on the red apply bar at the top of the screen.

Status	<input type="text" value="Enabled"/>
Voicemail Password	<input type="text" value="123456"/>
Email Address	<input type="text" value="naveedyounasrana@yahoo"/>
Pager Email Address	<input type="text"/>
Email Attachment	<input checked="" type="radio"/> yes <input type="radio"/> no
Play CID	<input type="radio"/> yes <input checked="" type="radio"/> no
Play Envelope	<input type="radio"/> yes <input checked="" type="radio"/> no
Delete Voicemail	<input type="radio"/> yes <input checked="" type="radio"/> no
VM Options	<input type="text"/>
VM Context	<input type="text" value="default"/>

Figure 8: voice mail configuration

We can enable setting of voice-mail setup on any extension according to our desire and need.

Voicemail Result

Following result shows, voice mail sent from extension to email ID. (from faisal <502> to navedeyounasrana@yahoo.com)

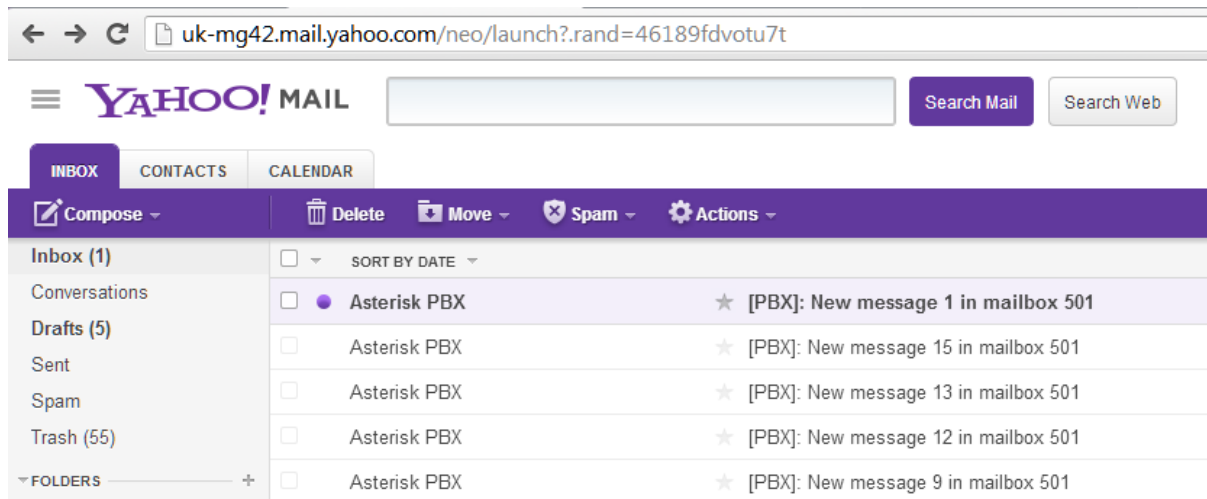


Figure 9: result of voice mail in e-mail ID

Inbound Trunks Configurations

For the Inbound Route configuration, First we need to select the service Provider for Inbound and outbound data. In this project, SIPGATE, VoIP DID provider, (www.sipgate.co.uk) is been chosen for inbound and outbound traffic.

To get registered with SIPGATE provider and select Virtual DID, consorting to the requirement, after registration with Virtual DID, here is the following secret information provided by sipgate.co.uk:

Example: Virtual Telephone Number: 01582809376 (Luton, England)

SIP-ID: 1711563

SIP Password: PYBNXCGF

Domain: sipgate.co.uk

Proxy: sipgate.co.uk

Stun: stun.sipgate.net:10000

Trunk setting

First Click on PBX >> go to PBX Setting >> Trunks :

A page will be open: choose option “Add SIP Trunk”

Following page will be open:

Fill up the space as following:

Trunk name: (e.g.” navedsipgate”)

PEER Details box (Write the following configuration)

Write Registration String as following

Click “Submit Changes”

Then click the red bar appearing on the top of the page

ADDITIONAL: ADD theses in peer details after the configuration shown:

Context=from-trunk >> Canreinvite=no >> authuser=1711563 >> allow=ulaw

← → ↻ 192.168.101.138/maint/index.php?freepbx

DISA
Languages
Music on Hold
PIN Sets
Paging and Intercom
Parking Lot
System Recordings
VoiceMail Blasting

Trunk Name: navedsipgate

PEER Details:

```
host=1711563@sipgate.co.uk  
type=friend  
secret=PYBNXCGF  
qualify=yes  
nat=yes  
insecure=invite  
fromuser=1711563  
dtmfmode=rfc2833  
disallow=all  
context=from-trunk
```

Incoming Settings

USER Context:

USER Details:

Registration

Register String:
1711563:PYBNXCGF@sipgate.co.uk/1711563

Submit Changes

Figure 10: inbound trunk configuration

Inbound routes

Click PBX >> PBX Setting >>

Click on “inbound routes”

Following page will be open:

Write the following configuration:

Click on “Submit”

Then click on “red bar” at the top of the page.

Extensions
Feature Codes
General Settings
Outbound Routes
Support
Trunks
Administrators
Inbound Call Control
Inbound Routes
Zap Channel DIDs
Announcements
Blacklist
CallerID Lookup Sources
Day/Night Control
Follow Me
IVR
Queues
Ring Groups
Time Conditions
Time Groups
Internal Options & Configuration
Conferences
DISA
Languages
Music on Hold
PIN Sets
Paging and Intercom
Parking Lot
System Recordings
VoiceMail Blasting

Edit Incoming Route

Description: naveed
DID Number: 1711563
Caller ID Number:
CID Priority Route: ☐

Options

Alert Info:
CID name prefix:
Music On Hold: Default
Signal RINGING: ☐
Pause Before Answer:

Privacy

Privacy Manager: No

Fax Handling

Fax Extension: default
Fax Email:
Fax Detection Type: None
Pause After Answer:

CID Lookup Source

Source: None

Set Destination

☐ Terminate Call: Hangup
☒ Extensions: <501> naveed
☐ Voicemail: <501> naveed (busy)
☐ Phonebook Directory: Phonebook Directory

Figure 11: inbound route configuration

Result for inbound

Following is the result of successful inbound call coming from “07869682170”.



Figure 12: successful inbound call result

Outbound trunks configuration

To make calls from IP phones to go out on a specific trunk. When having more than one trunk, need to setup outbound routes and dialling rules (dialling patterns) in order to specify which calls should go out on which trunk. Click PBX >> PBX Setting >> Trunks:

A page will be open: choose option “Add SIP Trunk”

Following page will be open:

Fill up the space as following:

Trunk name: (write Trunk Name, e.g.” navedoutbound”) >> PEER Details box (Write the configuration)

User detail >> user context >> Registration String as following

Click “Submit Changes”

General Settings

Outbound Caller ID:
Never Override CallerID: ☐
Maximum Channels:
Disable Trunk: ☐ Disable
Monitor Trunk Failures: ☐ Enable

Outgoing Dial Rules

Dial Rules:

Clean & Remove duplicates

Dial Rules Wizards:

(pick one) ▼

Outbound Dial Prefix:

Outgoing Settings

Trunk Name:
PEER Details:

`host=sipgate.co.uk
username=1711563
secret=PYBNXCGF
type=peer
insecure=very
qualify=yes`

Incoming Settings

USER Context:
USER Details:

`secret=PYBNXCGF
type=peer
context=from-trunk`

Registration

Register String:

Figure 13: outbound trunk configuration

Outbound route

Click PBX >> PBX Setting >>

Click on “outbound routes” left hand side

Following page will be open:

Write the following configuration:

Click on “Submit”

Then click on “red bar” at the top of the page.

The screenshot shows the 'Edit Route' configuration page for a route named 'naveedoutbound'. At the top, there is a red bar with a delete icon and the text 'Delete Route naveedoutbound'. Below this, the configuration fields are as follows:

- Route Name:** naveedoutbound (with a 'Rename' button)
- Route Password:** (empty text field)
- PIN Set:** None (dropdown menu)
- Emergency Dialing:** (checkbox, unchecked)
- Intra Company Route:** (checkbox, unchecked)
- Music On Hold?:** default (dropdown menu)
- Dial Patterns:** A text area containing '00.', '001.', and '011.'. Below it is a 'Clean & Remove duplicates' button.
- Dial patterns wizards:** (pick one) (dropdown menu)
- Trunk Sequence:** 0 SIP/naveedoutbound (dropdown menu with a trash icon). Below it is another empty dropdown menu and an 'Add' button.

At the bottom left, there is a 'Submit Changes' button.

Figure 14: outbound route configuration

Result for outbound

Following result shows a successful VoIP outbound call made from extension <501>.



Figure 15: successful outbound call

3.4 Summary

This section covers designing and optimization of network phase of the project with expected results exhibition.

Next chapter based on evaluation of QoS

4 Evaluation of QoS

VoIP lies in a row of top of the IP networks, but when transmission passes through different network stages such as gateway's boundaries, so it might get some performance problems. The parameters of QoS are also affected by the delaying firewall and blocked premises of network for encryption. The evaluation of QoS prerequisites is one of the decisive jobs that extent both the design and the run-time stage of QoS administration. The suppleness afforded by IP mobility in network system is often at odds with the confront of guarantee of stability of service and maintaining a settled stage of QoS [An Evaluation Mechanism for QoS Management in Wireless Systems, 2005]. VoIP is one of the most striking and imperative technology services these days in telecommunications era. Nevertheless, when VoIP packets are being elated via Internet, an amount of situations dissimilar from the traditional PSTN will be having influence on superiority of the call as supposed by clients. The QoS superiority of VoIP infrastructure based on many parameters, the bandwidth, packet loss, end-to-end delay and Jitter, type of codec employed distance of voice packets, and the size of the jitter-absorbing buffer [VoIP, wireless, P2P and new enterprise voice over IP 2008].

4.1 Packets transmission

If packets get lost from the packetized data, during transmission that is known as packet loss. In IP based infrastructure, packet loss may occur due to deprived connection where medium become fails to transmit packets successfully. It is brutally consider as dreadful conditions of IP network. As discussed earlier, below figure clearly show the successful and un-successful calls with their source and destination IP addresses, start and end times, status of the call with duration along with caller ID with Destination IP address. In addition, for the positive prospective, legitimate administrator can track the record and fix if any problems happen; in contrast, malicious user can easily launch the attack by using this information. Therefore, security is pre-requisite and will be discussed in detail in Section 5.

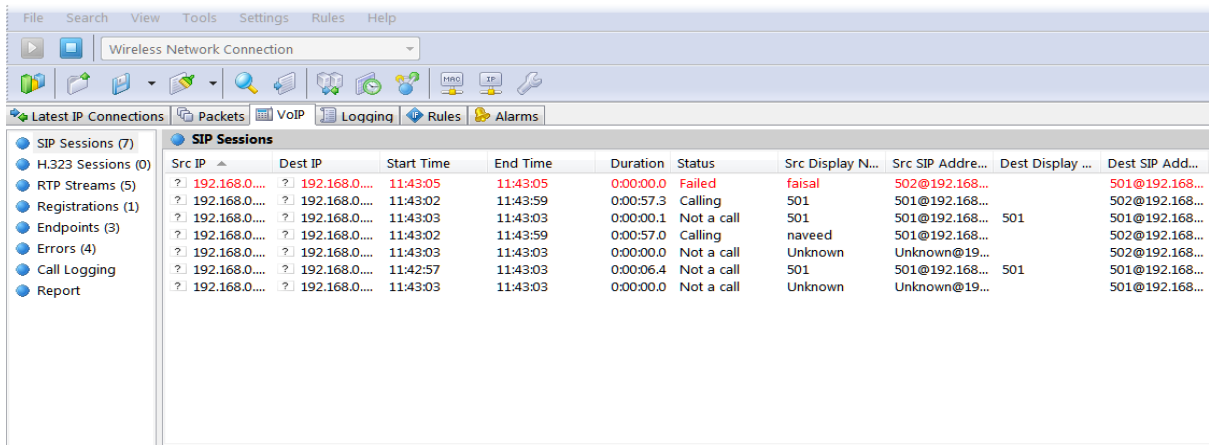


Figure 16: VoIP packet transmission query

4.2 Jitter

A fluctuation in delay timings during transmission of packets is called Jitter. It normally falls out when transmission of voice packets contains different measures in timing during call duration on the internet. Following result shows packet transmission per second at different amount of times. Jitter can occurs due to low bandwidth which does not support the entire network requirements or it might be the reason of insufficient component used inside the network.

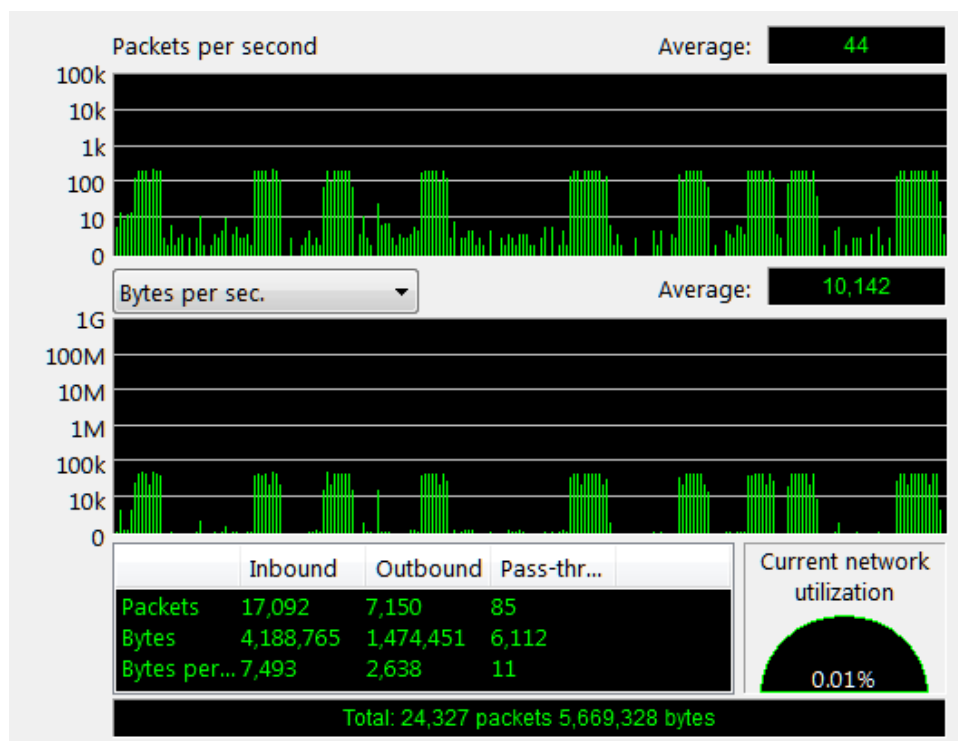


Figure 17: variations in delay timings

4.3 Latency

Latency, voice packet transmit duration from source to destination via internet is called Latency. Thus, by researchers, 150ms delay in packets transmission is countable as high quality service. This is a very important constituent for the service such as VoIP, where minimum commotion and package stability are the most important requirements [Improving the vertical handover latency for VoIP between WLAN and WiMAX networks, 2011].

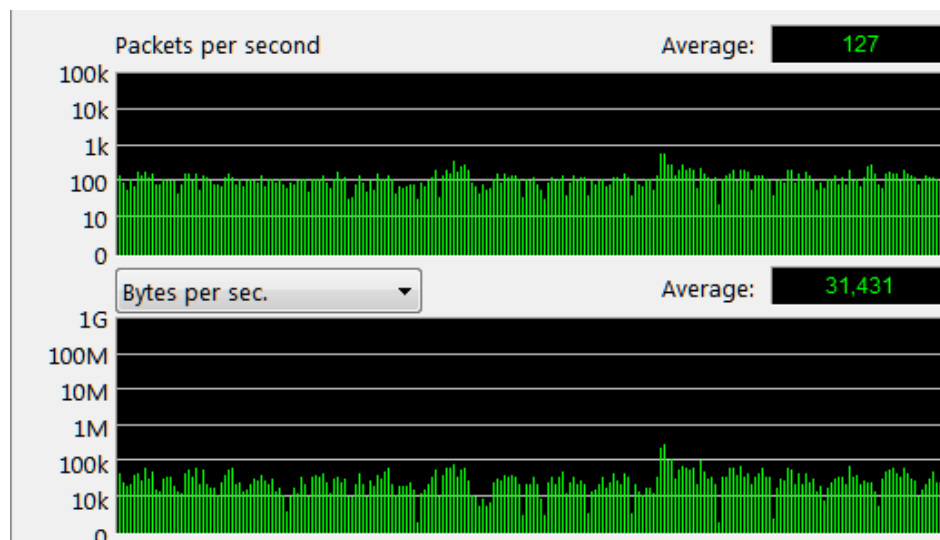


Figure 18: constant delay

4.4 Summary

This section of the report will be highlighted expected results of evaluation of the QoS with description.

Next chapter is contains penetration testing results which have been done by author himself.

5 Penetration testing

Penetration testing is also known as pen-testing in short, widely used to provide assurance of the security of the infrastructure. In early days, penetration testing were implemented physically and executed by tester consorting to company policy scheme, the procedure was typically complex in result and also was labour-intensive and required equipment to be well-known with all used tools. So it is very advantageous to employ an integrated system to illustrate the process which can easily be identified by computer system, then the computer can be used to alternative for testing equipment to perform pen-testing by using soft applications. Pen-testing is a well-known security risk to evaluate network vulnerability. It has been defined that pen-testing as security testing of the network; in which evaluator impersonate real-world threats to categorize processes for circumventing the security features of the applications, systems, or the networks. Basically this is the idea is to find out that how to get unauthorized entrée to its secret information and information systems [Network Penetration Testing Scheme Description Language, 2011].

5.1 Spoofing

Wireless networks are more susceptible for spoofing attacks than wired one, and spoofing success into the network allows to a large extent of other kind of attacks on the network. As more wireless networks or wireless sensor networks are deployed today, these kinds of networks are increasingly becoming targets for attacks such as malicious attacks. On account of accessibility and lack of security of wireless networks and wireless sensor networks, they are mainly vulturous to spoofing attacks, where attackers creates its fake individuality to pretence as another device of the network, or even creates multiple dishonest individualities. Spoofing attack is a serious challenge; it symbolizes real form of individuality conciliation and can make possible variety of data inoculation attacks, such as evil twin access point attacks. It is hence enviable to perceive the presence of spoofing attack and eradicate it from the network [Detecting and Localizing Wireless Spoofing Attacks, 2007].

5.1.1 Spoofing attack

For the spoofing attack we need a couple of things such as, VoIP server, client softphone and attacking machine inside the network.

X-lite soft phone used as a client which is registered with the server IP address.

Go to attacking machine >> open terminal >> **ifconfig** >> it will show same subnet as server is registered with. And also shows that we are on interface“**eth3**”.



```
root@bt:~# ifconfig
eth3      Link encap:Ethernet  HWaddr 00:0c:29:d6:d6:d5
          inet addr:192.168.101.135  Bcast:192.168.101.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fed6:d6d5/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:208 errors:0 dropped:0 overruns:0 frame:0
          TX packets:26 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:21608 (21.6 KB)  TX bytes:6826 (6.8 KB)
          Interrupt:19 Base address:0x2000

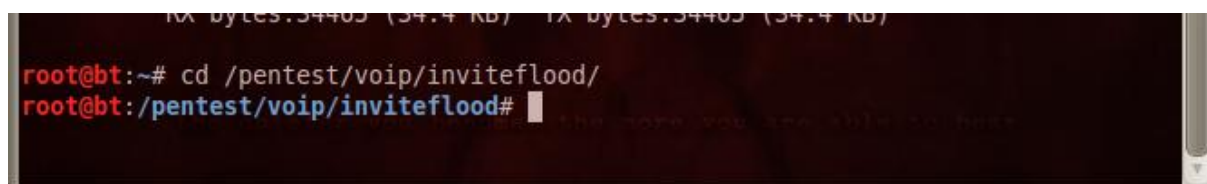
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:481 errors:0 dropped:0 overruns:0 frame:0
          TX packets:481 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:34465 (34.4 KB)  TX bytes:34465 (34.4 KB)

root@bt:~#
```

Figure 19: showing interface eth3

Get into the directory >> type command “**cd /pentest/VoIP/inviteflood/**”

Inviteflood is a backtrack tool for spoofing pen-testing.



```
root@bt:~# cd /pentest/voip/inviteflood/
root@bt:/pentest/voip/inviteflood#
```

Figure 20: showing directory

After getting into directory, >> get to the option >> type command

“**./inviteflood -h**”

Following result shows options.

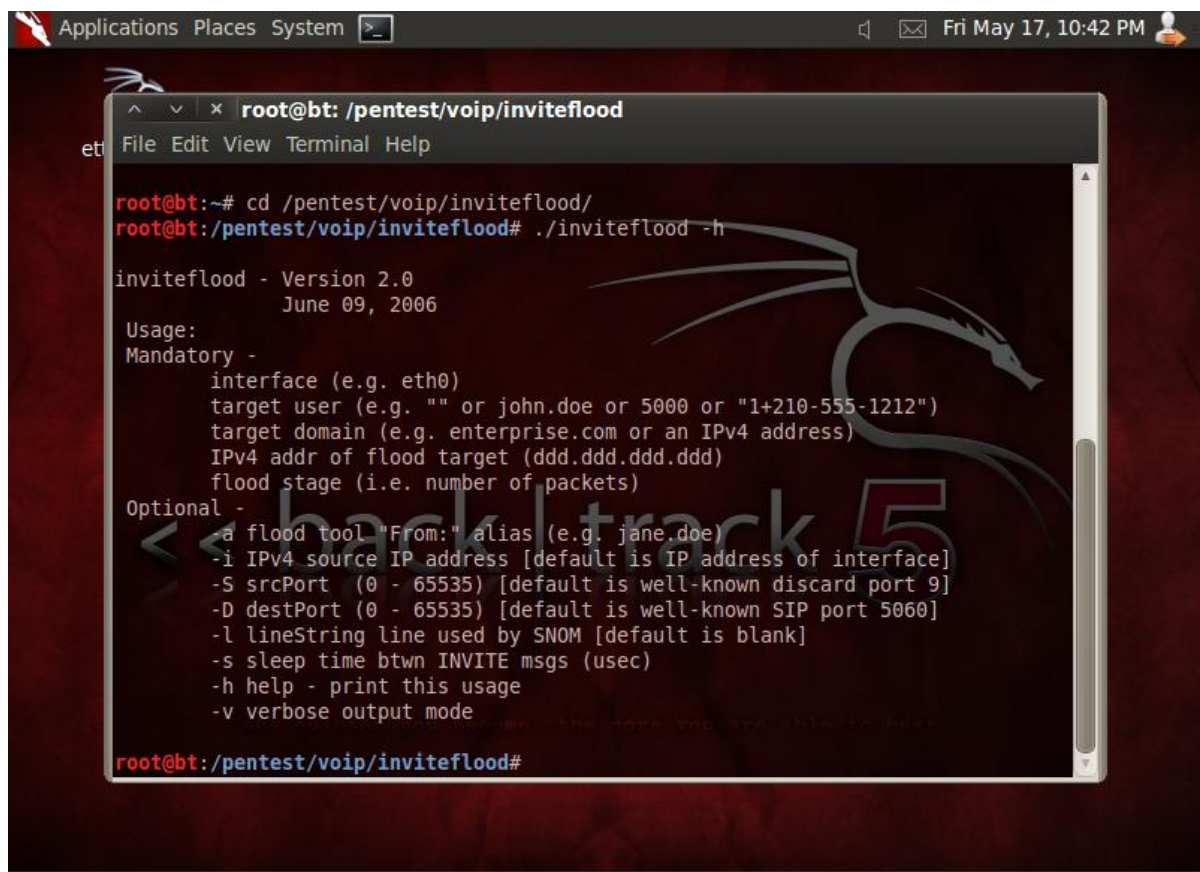


Figure 21: Inviteflood command options

Interface	eth3
Target user	faisal
Base-machine IP	192.168.101.1
IPV4	192.168.101.1
Flood stage	1 (number of packets)
Formalise user	-a ejaz
Spoofing IP	-I 100.100.100.100

After that type command:

./inviteflood eth3 faisal 192.168.101.1 192.168.101.1 1 -a ejaz -i 100.100.100.100

Press **Enter**



Figure 22: spoofing command

Following result shows a successful VoIP call by using fake ID “ejaz”

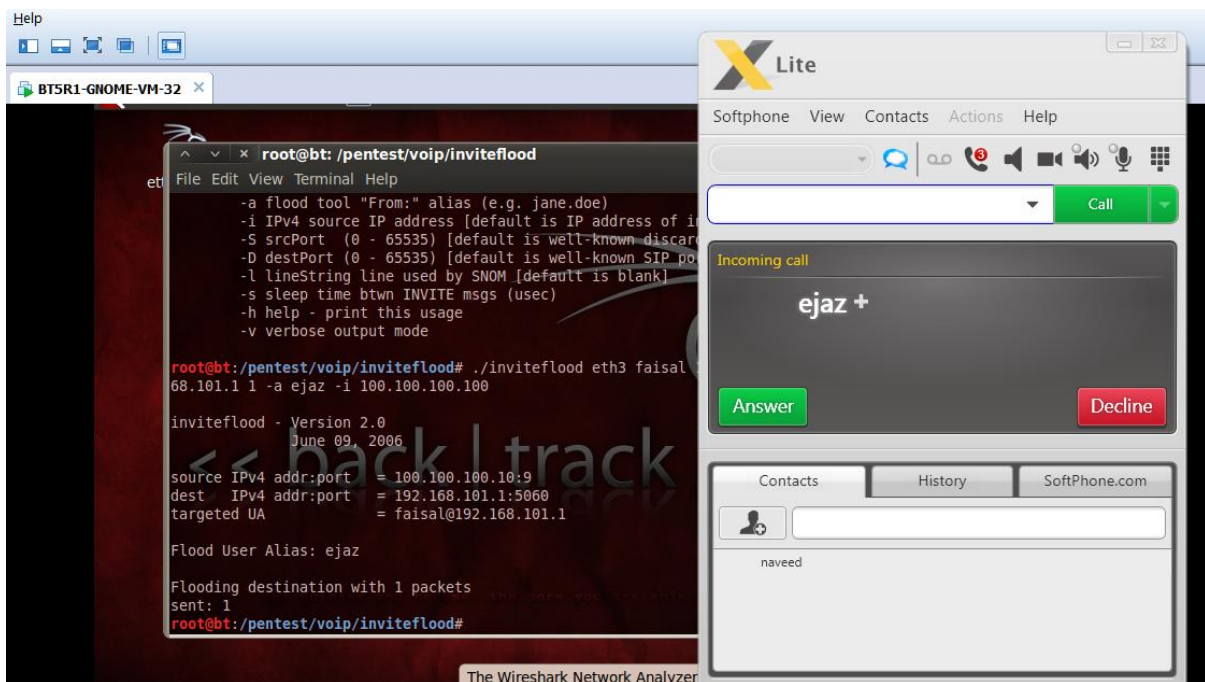


Figure 23: result of spoofing attack

5.2 Inbound traffic capturing

Traffic information has significant impact on network management; it is extensively used in formation of report of the traffic, personating the network, accountability and interference detection. To address these challenges, it is very imperative to understand traffic behaviour and traffic flow status of IP networks. Present communication system network holds a multiple choice of traffic, ordering from best-effort Email to real-time multimedia data streaming. Generally, the instant bandwidth requirement is not very simple to calculate, and this job becomes even trickier as the amount of end-user and network services boosts. On the other hand, the user professed communications superiority depends on predominantly on how healthy network can address these transformations in bandwidth timely demand [Monitoring, capturing and analysis of mission-critical traffic in experimental communication networks, 2006].

5.2.1 Traffic Capturing

For the traffic capturing we need a couple of things such as, VoIP server, client softphone and attacking machine “wireshark tool” inside the network.

To capture VoIP call traffic:

Go to attacking machine >> open Terminal>>wireshark>>press enter

Go to capture>> start>> type SIP in the box next to filter >> make call from your mobile number to VoIP provided number (07869682170 to 01582809376).

Following result shows capturing traffic, sip phone is ringing and also showing incoming caller ID.

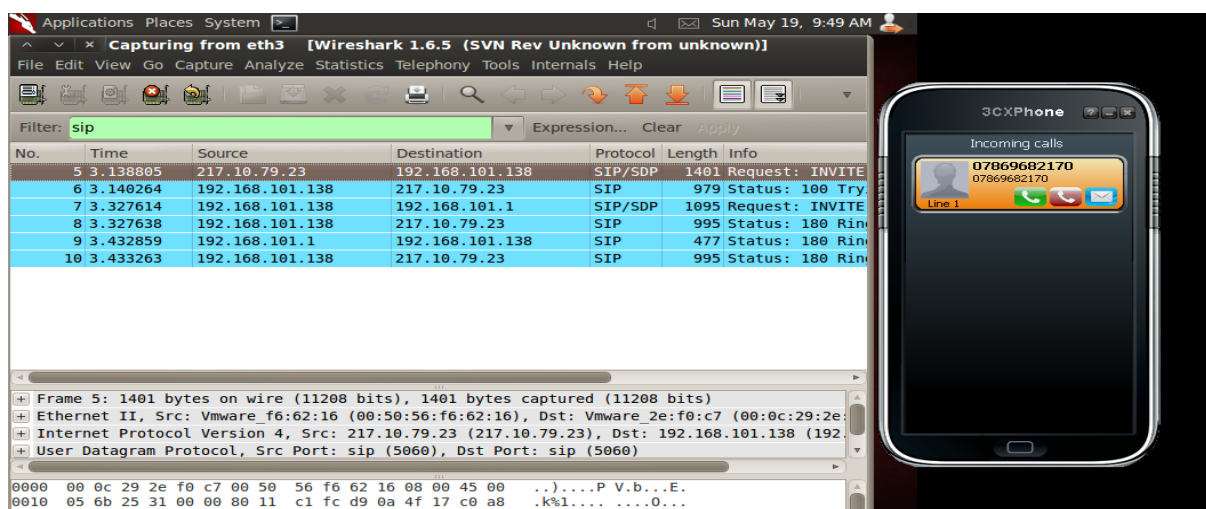


Figure 24: VoIP inbound call for traffic capturing

Pick up the phone; it will start capturing traffic over the VoIP network.

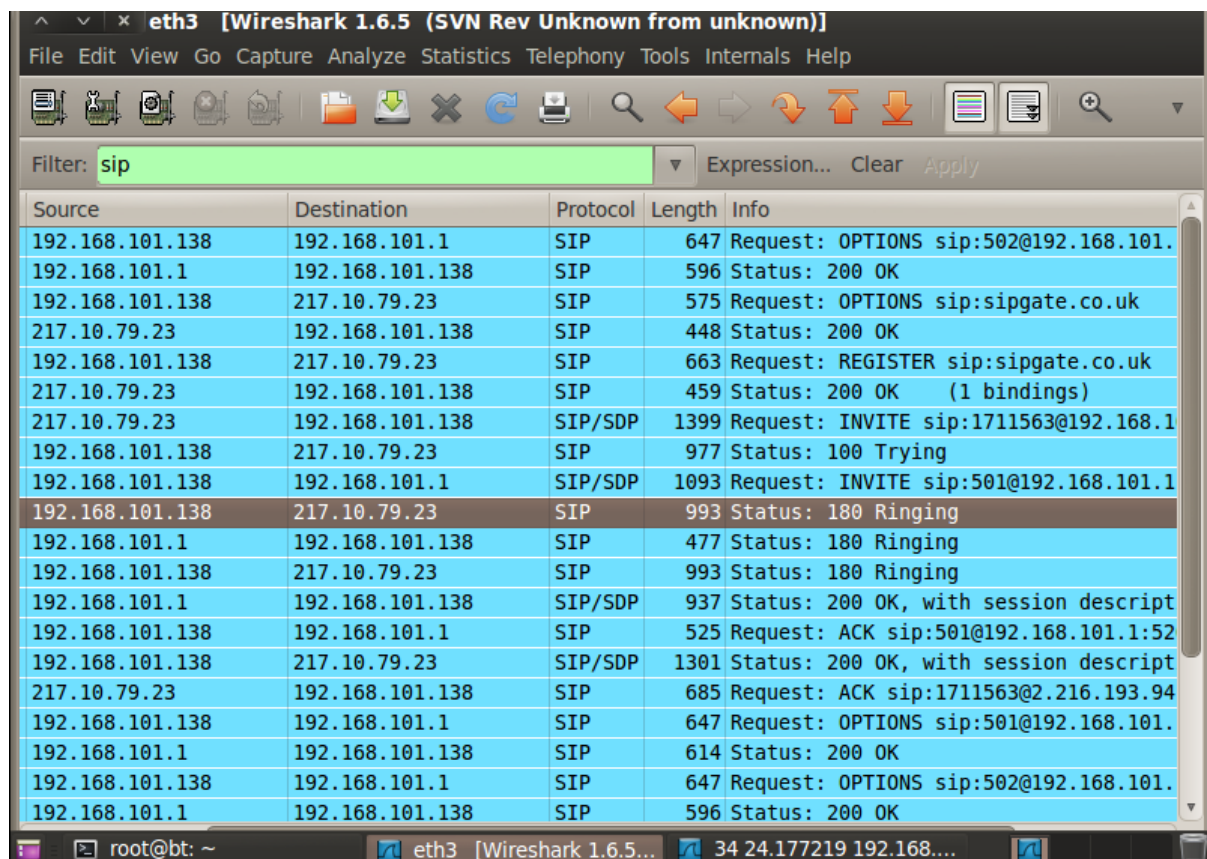


Figure 25: traffic capturing with wireshark

Double click on the first captured packet when you dialled number to make call. It will show following information results.

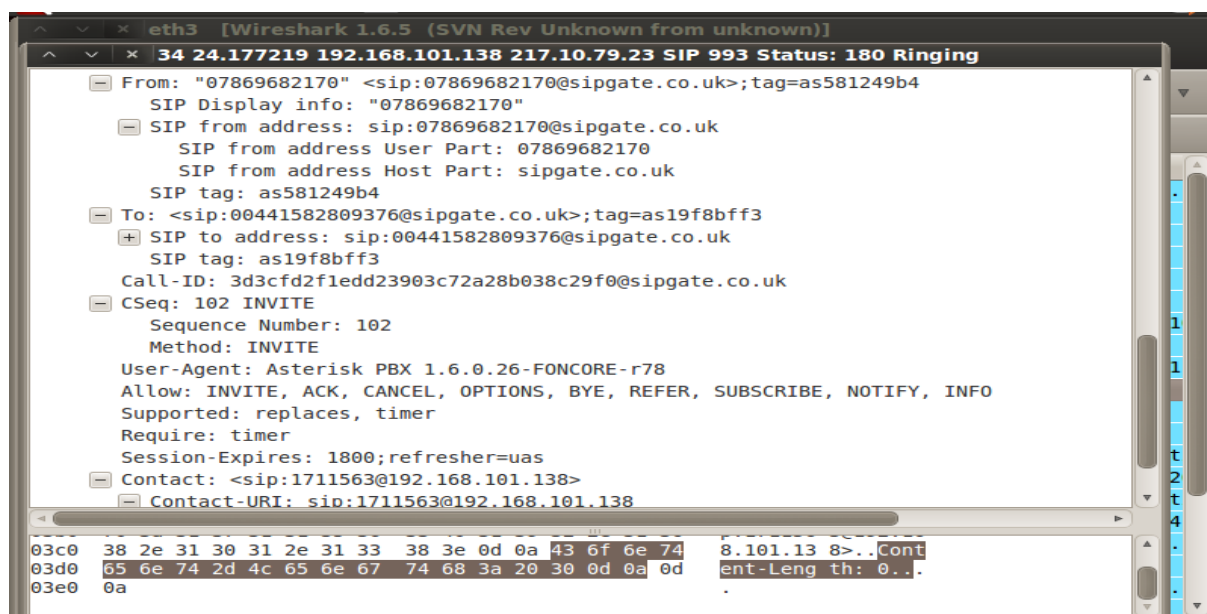


Figure 26: providing session detail

5.3 Solutions

5.3.1 IP security

The internet protocol Security (IPSec) has been widely used since it started providing validation and approval ability, which recommend to clients of the VoIP network a secure communication strait. An IPSec channel can be formed a consistent, point-to-point link in a connectionless net. Encrypted channels offer network, data, and address solitude by scuttle data. IPSec channels offer safety by encryption of complete voice packet and staple up further, mandatory header data [Quality effects of wireless VoIP using security solutions, 2004].

5.3.2 Wi-Fi Protected Access

“Wi-Fi Protected Access (WPA)” carries rough, tough encryption to Wireless-LAN (WLAN) communication, and also presents as partial view of imminent 802.11i security protocol. WPA augments wireless network safety measures by recuperating WEP's found key structure and allowing consumer confirmation on the network. WPA also gives consumer verification, which wasn't including in WEP. It also identifies the use of “Advanced Encryption Standard (AES)” as a supplementary substitute for WEP encryption. Wireless networks using WPA suffer from certain performance degradations [Quality effects of wireless VoIP using security solutions, 2004].

5.3.3 Firewall

Organizations which are linked with internet, mostly like to use of Internet firewall to diminishing risk level of network pen-testing, data theft, data demolition, and other security severances. One of the useful features of firewall is that it provides a central location for deployment of security. Internet firewalls, although, inflict an excessively plain inside and outside replica concerning security breaches that is not compatible with business needs, requires leading out insufficient expectations to external unit. Furthermore, firewalls security outer limits are not enough to secure a network entirely, because firewalls do not provide any protection from indoor attacks. Firewalls do not promise for any protection of sensitive information, which can be easily transmitted by inside permitted protocols. Today, Security firewalls in IP network is a staple requirement to secure voice. It is also even truth, if we say that firewalls are lie in first line to protect a computer, networks or even VoIP based networks. Processing of IP based network's transmission through firewall is already determined in programme rules. However, more multifarious sets of rule are featured in

firewalls. Today, elimination of basics as firewalls, and as Internet evolving direct to applets, mobiles, and object frameworks, these problems likely will get worse [Domain and type enforcement firewalls,2000].

5.4 Summary

This section based on penetration testing, results, and solutions of VoIP calls.

Next chapter is of conclusion about this project.

6 Conclusion and future preference

VoIP technology is one of the most widely using technologies which support to deal with communication from anywhere in the world. VoIP engineering is necessarily varying telephony industry, enabling not just less expensive calls but also providing more advantageous and rich features and more flexible services. Stablement, interoperable standards are key factor for VoIP consumption extensively. Increasing number of service provider is one of the reasons of VoIP technology to be cheaper comparatively with others. Although, challenges stay behind, VoIP technology already plays a key function in businesses communications and is rapidly varying the residential and consumer landscape of domestic and international communication affair. In this dissertation a network is designed and optimised in VMware operating system to evaluate QoS parameters and penetration testing from security point of view. Designing of the network is been done in VMware based on one single scenario. This scenario based on VoIP technology. After designing and implementation of the network, services were checked by making test calls and figure out their results. Network was integrated with network monitoring application software to evaluate the QoS. Main objectives were achieved in this project by doing penetration testing. Penetration testing based on different types of network attacks and results captured graphically to know the network vulnerabilities. These results achieved by penetration testing indicate of proven of artefact and solution provided would be helpful to enhance the level of network security to build a more secure network in future.

References

- Angelos D. Keromytis, voice over IP security, IEEE computer and reliability societies, 2010
<http://www.cs.columbia.edu/~angelos/Papers/2010/msp2010020076.pdf>
- Bordbar, B.; Anane, R.; Okano, K., "An Evaluation Mechanism for QoS Management in Wireless Systems," *Parallel and Distributed Systems*, 2005. *Proceedings. 11th International Conference on*, vol.2, no., pp.150,154, 22-22 July 2005
- Butcher, D.; Xiangyang Li; Jinhua Guo, "Security Challenge and Defense in VoIP Infrastructures," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on*, vol.37, no.6, pp.1152,1162, Nov. 2007
- Chan Yeob Yeun; Al-Marzouqi, S.M., "Practical Implementations for Securing VoIP Enabled Mobile Devices," *Network and System Security, 2009. NSS '09. Third International Conference on*, vol., no., pp.409,414, 19-21 Oct. 2009
- Dai, Zhiyong; Lv, Liangshuang; Liang, Xiaoyan; Bo, Yang, "Network Penetration Testing Scheme Description Language," *Computational and Information Sciences (ICCIS), 2011 International Conference on*, vol., no., pp.804,808, 21-23 Oct. 2011
- Garuba, M.; Jiang Li; Zhenqiang Yi, "Security in the New Era of Telecommunication: Threats, Risks and Controls of VoIP," *Information Technology: New Generations, 2008. ITNG 2008. Fifth International Conference on*, vol., no., pp.587,591, 7-9 April 2008
- Harle, D.A.; Kriaras, Y.; Smith, D. G., "Integrated switching system: a distributed star network for integrated voice and data traffic," *Integrated Multiservice Communication Networks, IEE Colloquium on*, vol., no., pp.6/1,6/4, 21 Nov 1988
- History of PBX Phone Systems | Reviews, Comparisons and Buyer's Guides. [ONLINE] Available at: <http://www.comparebusinessproducts.com/phone-systems/pbx/pbx-101/history-of-pbx-phone-systems>. [Accessed 2 May 2013].
- Holly Xiao; Zarrella, P., "Quality effects of wireless VoIP using security solutions," *Military Communications Conference, 2004. MILCOM 2004. 2004 IEEE*, vol.3, no., pp.1352,1357 Vol. 3, 31 Oct.-3 Nov. 2004
- Hunter, Patrick L., "Current Trends in Pbx Power Supplies," *Telephone Energy conference, 1978. INTELEC 78. International*, vol., no., pp.135,139, 25-27 Oct. 1978
- Jakimoski, K.; Janevski, T., "Improving the vertical handover latency for VoIP between WLAN and WiMAX networks," *Telecommunications Forum (TELFOR), 2011 19th*, vol., no., pp.377,380, 22-24 Nov. 2011
- Jeomgoo Kim; Inyong Lee; SiChoon Noh, "VoIP QoS(Quality of Service) Design of Measurement Management Process Model," *Information Science and Applications (ICISA), 2010 International Conference on*, vol., no., pp.1,6, 21-23 April 2010
- Joseph Epstein 2009, scalable voip mobility (integration and deployment)[online], Elsevier Inc., 30 Corporate Drive, Suite 400, Burlington, MA 01803, USA, Available from: [Accessed: 4.2013].

- MacIntosh, R.; Vinokurov, D., "Detection and mitigation of spam in IP telephony networks using signaling protocol analysis," *Advances in Wired and Wireless Communication, 2005 IEEE/Sarnoff Symposium on* , vol., no., pp.49,52, 18-19 April 2005
- Marshall, W.; Faryar, A.F.; Kealy, K.; de los Reyes, G.; Rosencrantz, I.; Rosencrantz, R.; Spielman, C., "Carrier VoIP Security Architecture," *Telecommunications Network Strategy and Planning Symposium, 2006. NETWORKS 2006. 12th International* , vol., no., pp.1,6, Nov. 2006
- MPLS Traffic Engineering – Cisco System. [ONLINE] Available at: http://www.cisco.com/en/US/docs/iso/12_0s/feature/guide/TE_1208S.html#wp14551[Accessed on, 2 may]
- N. Doraswamy and D. Harkins, IPsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks, 2nd ed. Upper Saddle River, NJ, USA: Prentice Hall PTR, 2003.
- Oostendorp, K.A.; Badger, L.; Vance, C.D.; Morrison, W.G.; Petkac, M.J.; Sherman, D.L.; Sterne, D.F., "Domain and type enforcement firewalls," *DARPA Information Survivability Conference and Exposition, 2000. DISCEX '00. Proceedings* , vol.1, no., pp.351,361 vol.1, 2000
- Radmand, P.; Talevski, A., "Impact of Encryption on Qos in Voip," *Social Computing (SocialCom), 2010 IEEE Second International Conference on* , vol., no., pp.721,726, 20-22 Aug. 2010
- samrat ganguly,sudeept bhatnagar 2008, VoIP,wireless, P2P and new enterprise voice over IP [online], john wiley & sons Ltd, chichester, west sussex, England.
- stephen p.olejniczak 2009, voip deployment for dummies [online], wiley publishing, Inc., 111 river street, hoboken, nj 07030-5774, www.wiley.com
- Sun Ming; Yan Jun-zhi, "Design and implementation of IP PBX architecture based on V5 interface," *Electronics, Communications and Control (ICECC), 2011 International Conference on* , vol., no., pp.795,797, 9-11 Sept. 2011
- Thomas porter, michael gough 2007, VoIP security [online], syngress publishing, Inc, 800 hingham street, rockland, MA 02370, Available from: [accessed: 4.2013]
- Weerathunga, P.E.; Samarabandu, J.; Sidhu, T., "Implementation of IPsec in substation gateways," *Information and Automation for Sustainability (ICIAfS), 2012 IEEE 6th International Conference on* , vol., no., pp.327,331, 27-29 Sept. 2012
- Wietgreffe, H.; Ajenjo, A.D.; Rogula, T., "Monitoring, capturing and analysis of mission-critical traffic in experimental communication networks," *Testbeds and Research Infrastructures for the Development of Networks and Communities, 2006. TRIDENTCOM 2006. 2nd International Conference on* , vol., no., pp.9 pp.,363,
- Yingying Chen; Trappe, W.; Martin, R.P., "Detecting and Localizing Wireless Spoofing Attacks," *Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON '07. 4th Annual IEEE Communications Society Conference on* , vol., no., pp.193,202, 18-21 June 2007
- Z. A. Barnes, "Is Implementation of Voice over Internet Protocol (VoIP) More Economical for Businesses with Large Call Centers," Bowie State University 2005
- Zourzouvillys, T.; Rescorla, E., "An Introduction to Standards-Based VoIP: SIP, RTP, and Friends," *Internet Computing, IEEE* , vol.14, no.2, pp.69,73, March-April 2010

Interim report

Table of Contents

1.	Introduction	2
2.	Aims and Objectives	2
3.	Literature review	2
3.1	Voice over internet protocol	3
3.2	Trixbox PBX	3
3.3	QoS (Quality of service)	3
3.3.1	Packet loss	3
3.3.2	Jitter	3
3.3.3	Latency/Delay	3
3.4	Security	4
4.	Problems definition	4
5.	Methodology	4
5.1	System requirements	4
5.2.	Scenario	5
5.3	Initial Results	5
5.3.1	Result	5
5.4	Future Result	5
6.	Conclusion and future work	6

1. Introduction

Several years ago, a system was introduced called “PBX” as an alternatives of traditional communication system to reduce cost. Private Branch Exchange (PBX) system is a telephony platform for inbound and outbound national or international calls for less. PBX system is Wi-Fi enabled and based on VoIP technology. Voice over Internet Protocol, familiar as VoIP, is the term used for transport voice signals over the internet, in the same manner in which people send or receive emails or web surfing. VoIP technology provides to its users to make call by exploiting internet broadband connection as an alternative of using Public Switched Telephone Network (PSTN). In VoIP technology, there is a condition apply of packetization of speaker’s voice for transmission over the internet. These packets are transmitted over the internet from speaker to listener, upon collection of these packets; receiver or listener gets expected voice data. Now-a- days, new ingredient with more advance features are being introduced within VOIP structural design. Consequences of these emergences, VoIP technology evolving rapidly toward various QoS issues and security risks. Majority of the VoIP service provider assume that providing more features is enough to exploit VoIP technology, as a result user’s complains about poor quality and security are getting increase. This project is based on real time debate regarding VoIP PBX issues and will show some results.

2. Aims and Objectives

Aims and Objectives session includes different phase concerning evaluation of QoS and penetration testing regarding VoIP PBX security.

Understanding of VoIP tools in a real time environment

Designing and optimization of VoIP PBX infrastructure

Providing free national and international telephony platform

Configuration of trunks for inbound and outbound call routes

Evaluate different parameters of QoS (Packet loss, Jitter and Delay)

Penetration testing regarding VoIP calls security

3. Literature review

The description of the Following apparatuses is based on analysis of previous research work:

3.1. Voice over internet protocol

In recent years, Voice over Internet Protocol (normally known as VoIP) has become a burst image of telephony technology in industry. VoIP is the term used to refer existing telephony system to the next generation with additional features. VoIP technology holds enormous promises to provide features which is beneficial for both providers and end-users, such as low cost and elasticity. VoIP transports voice signals over the internet by converting them into packets. VoIP technology is a cluster of particular applications and protocols, each of them is

liable to performs specific task to carry out voice signals over the internet. VoIP technology has changed the way of telecommunication by empowering large, medium and small enterprises to erect their own telecom system with additional features such as, use of multiple carrier to save call cost and good quality service. VoIP technology also includes feature to make call computer to computer, computer to mobile, and mobile to computer etc. generally, VoIP service providers offer lower rates to make calls than traditional telephony companies.

3.2. Trixbox PBX

When VoIP technology emerges into communication scene, enterprises are sceptical to provide reliability as traditional Public switched telephone network (PSTN). Private branch exchange (PBX), which has become a possible reliable alternative of PSTN. PBX is a feature rich telephony exchange which not only helps to enable efficient communication but provide reliability and significant savings to the organisations. As name shown, PBX provides feature to organisations to create their own private communication infrastructure with total privacy and less cost. PBX system supports a VOIP call that is because it's called IP-PBX as well.

3.3. QoS (Quality of service)

To VoIP, for being possible alternatives of public switched telephone network, it is not enough to be cheaper, easy to deploy and easy to maintain. It must provide better call quality or at least equally to PSTN. So that it can become a motivation to an end- user to switch to VoIP. VoIP is running in a queue of top IP networks, while transmission goes through network gateway's boundaries it might cause some performance issues. Such as,

3.3.1 Packet loss

After packetisation of data, if some packets get lost during transportation that is called packet loss. In an IP based network, packet loss can occur due to poor bandwidth where application medium fails to deliver voice packets successfully. It is severely considerable as degradation of voice application.

3.3.2 Jitter

Jitter is a variation between delay timings of voice packets. It occurs when voice packets face different amount of time over during call duration over the internet.

3.3.3 Latency/Delay

Delay is a voice packet travel time from source (sender) to destination (receiver) over the internet. By contributors, delay time imposed by speed of light. Therefore, till 150ms in packets delay is conceder as good quality service.

3.4. Security

Security concerns where privacy and confidentiality require. In case of VoIP based network, beside the Quality of Service, security is also an important element which plays effective role to motivate end users to switch to VoIP. Confidentiality and privacy are the terms used to refer end-user's expectation to the provider that their data/call is safe from attacks, such as eavesdropping and call hijacking. IP based network deal with innumerable end users and their communication activities efficiently. However, chain of benefits of an IP based network also accompanied of security threats. Comparatively, in IP based networks, number of threats is

much more than traditional PSTN because of huge user's base, which is accessible from any part of the world. IP networks based on signals and signals never know that user is friendly user or eavesdropper. On the other hand, in PSTN infrastructure, there is involve a physical access to spoil network infrastructure. In recent years, communication era moving frequently toward the VoIP technology but security expertise is not able run parallel. This project will discuss some aspects regarding VoIP security by penetration testing.

4. Problems definition

Today, in communication era, VoIP is the predominantly technology which is used by thousands of users with additionally everyday increasing numbers. Today, everyone can communicate with anyone by using VoIP technology in entire world. Because of list of features, flexibility and increasing number of service provider, the cost is also condensed to less. Regarding better exploitation of VoIP technology, two elements concern, Quality of service and Security. These two elements help to motivate end users to adapt to VoIP technology to compete with their everyday telephony activity. Also, these are good for Relationship between Vender and end-user, which generates good revenue for the company. Among these core elements, security is the main focus of project. This document will get some effective techniques from the available work and will suggest some valuable practice.

5. Methodology

VMware is a virtual operating system used for deployment of VoIP technology in real time environment for QoS and security testing Purpose.

5.1 System requirements

Personal Computer (PC)

VMware

TrixBos 2.8.0.4

NETWORK monitoring software

BackTrack machine

Library Resources

5.2. Scenario

A real time scenario is designed for evaluating QoS and penetration testing for VoIP call's performance and security.

5.3 Initial Results

Deploying VoIP based infrastructure

VoIP call testing between two different networks

5.3.1 Result

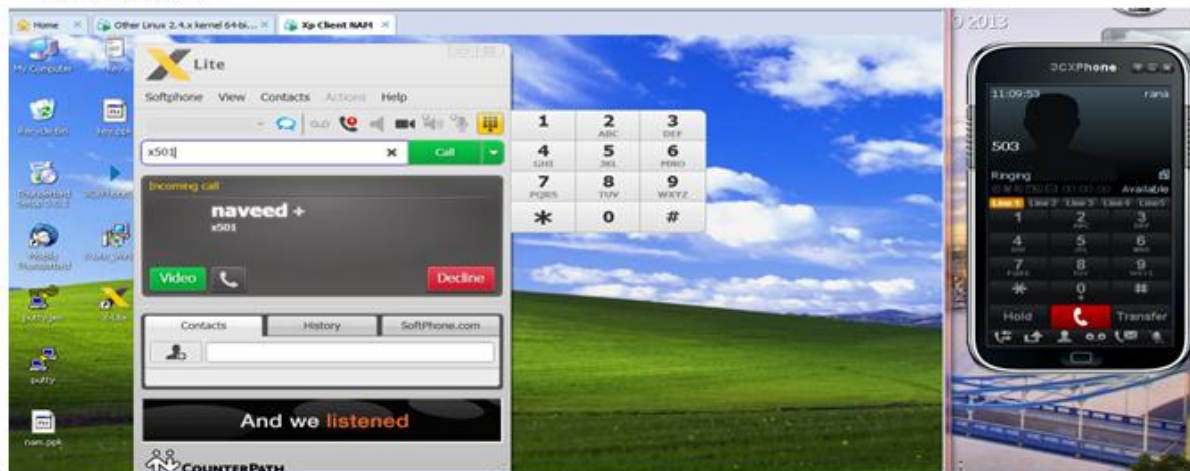


Figure 1: shows the successful live call testing among the two networks using Trixbbox, IP PBX fully configured and optimized by the author.

5.4 Future Result

Inbound and Outbound call testing, nation or international

Evaluation of quality of service (QoS) by using network monitoring software Penetration testing regarding VoIP security

6. Conclusion and future work

This report based on outline of the project. In this report, An indication is provided concerning to introduction , aims and objectives, literature review, problem definition, system requirements, scenario, chosen methodology, and expected results. Next, project work will be moving toward final report and will show accomplished results in real time environment.

References

1. Butcher, D.; Xiangyang Li; Jinhua Guo, "Security Challenge and Defense in VoIP Infrastructures," *Systems, Man, and Cybernetics, Part C: Applications and Reviews, IEEE Transactions on* , vol.37, no.6, pp.1152,1162, Nov. 2007
2. Marshall, W.; Farvar, A.F.; Kealy, K.; delos Reyes, G.; Rosencrantz, I.; Rosencrantz, R.; Spielman, C., "Carrier VoIP Security Architecture," *Telecommunications Network Strategy and Planning Symposium, 2006. NETWORKS 2006. 12th International* , vol., no., pp.1,6, Nov. 2006
3. samrat ganguly.sudeept bhatnagar 2008, VoIP.wireless. P2P and new enterprise voice over IP [online], john wiley & sons Ltd, chichester, west sussex, England.
4. stephen p.olejniczak 2009, voip deployment for dummies [online], wiley publishing, Inc., 111 river street, hoboken, nj 07030-5774, www.wiley.com
5. joseph epsein 2009, scalable voip mobility (integration and deployment)[online], elsvier Inc., 30 corporate drive, suite 400, burlington, MA 01803, USA, Available from: [Accessed: 4.2013].
6. Thomas porter, michael gough 2007, VoIP security [online], syngress publishing, Inc., 800 hingham street, rockland, MA 02370, Available from: [accessed: 4.2013]

asMSc Project Proposal Form
AY12/13, Semester I

Student Number	1133670
Student Name	Naveed Younas Rana
Degree Course	MSc computer networking
Supervisor Name	Dr Ali Mansour
Title of Project	Designing and optimization of VOIP PBX infrastructure
Description of your artefact	<p>This project is related to VOIP PBX. Trixbox, formerly known as "Asterisk@Home", is a CentOS Linux distribution that provides an open source telephony package based on the famous Asterisk Voice-over-IP PBX. In this project I will configure a trixbox iso then I will create a couple of extensions to make calls between these by using Softphone in a virtual machine, after these successful testing I will use backtrack machine for sniffing data packets and eavesdropping attacks. As an artefact, research and implementations of VOIP PBX will be obliging PBX users to better exploit this technology in their business risk free.</p> <p>The aim of this project is divided into two parts, 1) designing and optimization of VOIP PBX infrastructure virtually and 2) penetration testing and as well as presenting that how to make this secure from attacks, such as packet sniffing , etc.</p> <p>Promoting enhancement of security encryption levels and access control.</p> <p>Configuration VOIP PBX, security issues, effective security techniques,</p> <p>Dealing with security PBX security issues, Evaluation of different security encryption levels and effective security techniques</p>
What methodology (structured process) will you be following to realise your artefact?	<p>I am going to use Rapid Application Development methodology. I will follow of its phases (1: staff members discuss and agree on business needs, project scope, constraints, and system requirements., 2: understanding, modification, and eventually presentation and approvement of the system that meets their needs, 3: users continue to participate and can still suggest changes or improvements as actual screens or reports are developed and 4: including, testing, changeover to the new system, and user training. Compared with traditional methods,. As a result, the new system is built, delivered, and placed,)to achieve our goal.</p> <p>I am going to design a secure VoIP PBX infrastructure in virtual environment for testing purpose, using VM ware, trixbox ISO, softphone dialler, extensions, inbound and outbounds calls, network monitoring software installation for evaluation of load, latency, jitter,. Back track for attacks,.</p>

How does your project relate to your degree course and build upon the units/knowledge you have studied/acquired	As related to computer networking, designing, implementation, and evaluation of encryption security levels of VOIP PBX is strong side.	
Resources	Google, books, journals, ACM digital library, IEEE, Virtual machine, trixbox ISO, network monitoring , attacking machine (backtrack etc)	
Have you completed & submitted your ethics form?	yes	

FACULTY OF CREATIVE ARTS, TECHNOLOGIES AND SCIENCE

Form for Research Ethics Projects (CATSethicsform)

1. Student Name	Naveed Younas Rana
2. Student Number:	1133670
3. Degree Pathway:	MSc computer networking
4. Supervisor's name	Dr Ali Mansour
5. Supervisor Signature	<i>A. Mansour</i>
6. Working title of project	Designing and optimization of voIP PBX infrastructure

SECTION A Proposal

Please summarise below the ethical issues involved in the research proposal and how they will be addressed. In any proposal involving human participants clear explanation of how informed consent will be obtained, how confidentiality will be observed, how the nature of the research and the means of dissemination of the outcomes will be communicated to participants must be provided.

The diagram consists of two overlapping triangles. The left triangle is light green and contains the text 'Brief outline of project'. The right triangle is light red and contains the text 'List of ethical issues'. The triangles overlap in the center, with the green triangle on the left and the red triangle on the right.

SECTION B Check List

Please answer the following questions by circling YES or NO as appropriate.

1. Does the study involve vulnerable participants or those unable to give informed consent (e.g. children, people with learning disabilities, your own students)?
YES ☒ NO
2. Will the study require permission of a gatekeeper for access to participants (e.g. schools, self-help groups, residential homes)?
YES ☒ NO
3. Will it be necessary for participants to be involved without consent (e.g. covert observation in non-public places)?
YES ☒ NO
4. Will the study involve sensitive topics (e.g. obtaining information about sexual activity, substance abuse)?
YES ☒ NO
5. Will blood, tissue samples or any other substances be taken from participants?
YES ☒ NO
6. Will the research involve intrusive interventions (e.g. the administration of drugs, hypnosis, physical exercise)?
YES ☒ NO
7. Will financial or other inducements be offered to participants (except reasonable expenses or small tokens of appreciation)?
YES ☒ NO
8. Will the research investigate any aspect of illegal activity (e.g. drugs, crime, underage alcohol consumption or sexual activity)?
YES ☒ NO
9. Will participants be stressed beyond what is considered normal for them?
YES ☒ NO
10. Will the study involve participants from the NHS (patients or staff) or will data be obtained from NHS premises?
YES ☒ NO

If the answer to any of the questions above is "Yes", or if there are any other significant ethical issues, then further ethical consideration is required. Please document carefully how these issues will be addressed.

Signed (student):

Roma Nand

Countersigned (Supervisor):

A-Mansy

Date: *07/03/2013*

Date: *7/3/13*

VoIP PBX quality of service and security

Naveed Y. Rana, Faisal F. Qureshi, Dr. Ali Mansour

INTRODUCTION

Voice over Internet Protocol (VoIP) provides the existing and future small, medium and large organizations including home users to optimise their telephony systems with reduced cost. In addition, using the VoIP technology to receive free of cost incoming calls and make outbound national and international calls, text and videos calls with minimal cost.

OBJECTIVE

- ❖ To understand VoIP tools with Linux and Windows Operating Systems
- ❖ To implement FREE international and national calling platform for SME's
- ❖ To configure the trunks for inbound/outbound call routes
- ❖ To configure and manage VoIP messages forwarding to the E-mail address
- ❖ To improve the efficiency of the calls on the available bandwidth
- ❖ To investigate risks and threats of VoIP technology by penetration testing

FUTURE OF VOIP (2010-2015)

According to the Network Enhancers recent reports discussed the VoIP growth rates from 2010 to 2015 [1].

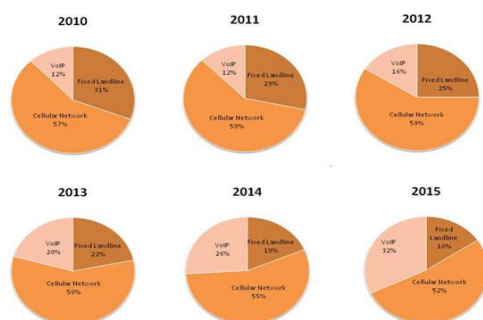


Figure 1: Growth Rate of VoIP in Communication Industry

Quality of Service (QoS)

- ❖ packet loss far less than one percent to avoid audible errors. Ideally, there should be no packet loss for VoIP.

❖ The ITU G.114 specification recommends less than 150 millisecond (ms) one-way end-to-end delay for high-quality real-time traffic such as voice.

❖ Jitter buffers (used to compensate for varying delay) further add to the end-to-end delay, and are usually only effective on delay variations less than 100ms. Jitter must therefore be minimized [2]

Why VoIP technology is better than standard PSTN?

- ❖ Economical
- ❖ Utilize the existing Bandwidth
- ❖ Free calling among the users
- ❖ Portability
- ❖ Less maintenance
- ❖ Automatic Billing & Recurring
- ❖ Web Access
- ❖ Easily manageable incoming and outgoing calls from your PC, laptop or even from your smart phone .

CYBERCRIMES MARKET SURVEY REPORT

For the past five years, the CSI—in conjunction with the FBI has published the results of such surveys in a report called [Computer Security Issues and Trends](#).

Types of cybercrimes

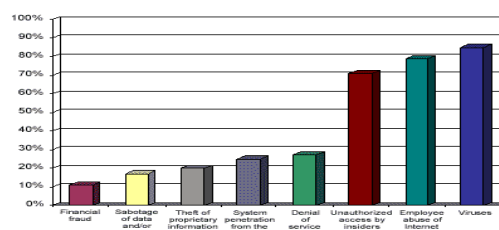


Figure 2: cybercrimes percentage

CONCLUSION

Security is on the minds of just about everyone in the IT world. But Network security such as VoIP is still a very big challenge for security researchers and scientist. Network security should be the main focus with increasing demand.

REFERENCES

- [1] www.google.com/network enhcers [Accessed on Mar. 19, 2013]
- [2] Byoungjin Kim; Hyewon Lee; Seongho Byeon; Kwang Bok Lee; Sunghyun Choi, "Enhancing QoS of voice over WLANs," *World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2012 IEEE International Symposium on a*, vol., no., pp.1,9, 25-28 June 2012.
- [3] www.techrepublic.com cybercrime [accessed on may. 22,2013]