Implementation of Secured IP Telephony System

A Thesis submitted to the Daffodil International University in Partial fulfillment of the requirement for the Degree of Bachelor of Science in Electronics and Telecommunication Engineering

Submitted By
Md. Najmul Islam
ID: 101-19-1206

Mst. Dilruba Yeasmin Hera
ID: 101-19-1216

Shafee-Ul-Mahmud Chowdhury
ID: 101-19-1220

Supervised by
Dr. A. K. M. Fazlul Haque
Associate Professor and Head
Department of Electronics and Telecommunication Engineering
Daffodil International University

Department of Electronics and Telecommunication Engineering

Daffodil International University

APPROVAL

This thesis entitled "**Implementation Of Secured IP Telephony System**" by Md. Najmul Islam, Mst. Dilruba Yeasmin Hera and Shafee-Ul-Mahmud Chowdhury has been submitted to the Daffodil International University in partial fulfillment of the requirement for the Degree of Bachelor of Science in Electronics and Telecommunication Engineering. This thesis has been accepted as satisfactory by the honorable Members of the Board of examiners after its presentation that was held on 18th January 2014.

BOARD OF EXAMINERS

1…………………………………………..
Dr. A.K.M. Fazlul Haque, **(Chairman)**
Associate Professor and Head,
Department of Electronics and Telecommunication Engineering,
Daffodil International University

2. Taslim Arefin ……………………………………….
Mr. Md. Taslim Arefin **(Internal Member)**
Assistant Professor,
Department of Electronics and Telecommunication Engineering
University of Dhaka

3……………………………………….
Mrs. Shahina Haque **(Internal Member)**
Assistant Professor,
Department of Electronics and Telecommunication Engineering
Electronics and Communication Engineering
University of Dhaka

4. S. K. Aditya ……………………………………….
Dr. Subrata Kumar Aditya, **(External Member)**
Professor,
Department of Applied Physics,
Electronics and Communication Engineering
University of Dhaka

DECLARATION BY THE CANDIDATE

We do hereby declare that the research work incorporated in this thesis entitled "**Implementation of secured IP telephony system**" has been done by us under the supervision of A.K.M. Fazlul Haque, Associate Professor and Head, Department of ETE of Daffodil International University and that no part of this work has been submitted in any University or Institution for any degree.

1. Najmul ....

(Md. Najmul Islam)

ID: 101-19-1206

Department of Electronics and Telecommunication Engineering.

Daffodil International University

2. Dilruba ....

(**Mst. Dilruba Yeasmin Hera**)

ID: 101-19-1216.

Department of Electronics and Telecommunication Engineering.

Daffodil International University

3. Shafee ....

(**Shafee-Ul-Mahmud Chowdhury**)

ID: 101-19-1220

Department of Electronics and Telecommunication Engineering.

Daffodil International University

CERTIFICATE OF THE SUPERVISOR

I hereby certify that the thesis entitled "**Implementation of Secured IP telephony System**" submitted by Md. Nazmul Islam, Shafee-Ul-Mahmud Chowdhury and Mst. Dilruba Yeasmin Hera have been composed by him under my supervision.

To the best of my knowledge, it has not formed the basis for any degree or award elsewhere.

....

(Dr. A.K.M. Fazlul Haque)

Associate Professor and Head of the Department

Department of Electronics and Telecommunication Engineering

Daffodil International University

Dhaka 1205

Bangladesh

ACKNOWLEDGEMENTS

First off all we would like to express our cordial gratefulness to Almighty ALLAH for HIS kindness, for which we successfully completed our thesis within time and we also apologize to Him for our any kind of mistakes.

We would like to express our boundless honor and respect to our supervisor, **A.K.M Fazlul Haque**, Head of the Deapartment, Department of Electronics and Telecommunication Engineering, Daffodil International University. His dedicated efforts, wise advices and keen knowledge showed the path of achievement.

We would like to thank the graduate committee of **Professor Dr. M. Shamsul Alam** Professor and Dean, Faculty of Engineering, Daffodil International University, and **Dr. Subrata Kumar Aditya**, Professor Department of Applied Physics, Electronics and Communication Engineering , University of Dhaka.

We would like to also express my gratitude to our senior brother **Mahfuzur Rahman Mahfuz,** student of 19th batch of ETE department, for his keen interest and valuable advice. We will be obliged him forever.

We thank our parents for supporting us throughout all our studies at University. We also like to thank to other faculty members, the staffs of the Department of Electronics and Telecommunication Engineering and Faculty of Science and Information Technology, Daffodil International University.

And last but not the least we must acknowledgement with due respect the constant support and patience of our family member for completing this thesis report.

Md. Najmul Islam,
Shafee-Ul-Mahmud Chowdhury
and
Mst. Dilruba Yeasmin Hera

ABSTRACT

In this project, IP telephony feature and secured IP telephony system have been considered to setup the PBX system. IAX trunk is created and configured so that extension of one server can call to the extension of another server of same network. Elastix call center is also installed and configured so that campaign for incoming and outgoing calls could be made and which allowed the interaction between agents and telephony subscribers. Openfire and Spark have been installed and configured so that instant messaging between people could be made on same network, even network joined by a WAN, instant messaging also possible to external people by using the openfire gateway plug in. The packet passing over the network has also been analyzed by wireshark. And, finally, server has become secured in 3 levels by Bactrack and it is ensured the privacy of the system and no one can hack and destroy the system modify it as one want.

Content Pages

Approval	i
Declaration of Candidates	ii
Certificate of Supervisor	iii
Acknowledgement	iv
Abstract	v
Table of Content	vi
List of Figure	viii
List of Table	xi
Chapter 1: Introduction	01-02
1.1 General Introduction	01
1.2 Goal of the Research Work	01
1.3 Organization of the thesis	02
Chapter 2: Theory	03-11
2.1 IP telephony	03
2.2 Elastix	03
2.3 Asterisk	04
2.3.1 Used of Asterisk	04
2.3.2 Asterisk Dialplan	04

2.3.3 Protocol	05
2.3.4 Codec and Codec Translation	07
2.4 Softphone	08
2.5 Openfire	09
2.6 XMPP	09
2.7 Call Center	11
Chapter 3: Installation & Configuration	12-26
3.1 Soft Phone Configuration	12
3.2 IAX trunk setup	13
3.3 Outbound route configure	15
3.4 Openfire configure	16
3.5 Spark	21
3.6 Call center	23
Chapter 4: Packet Analysis	27-36
4.1 Packet Analysis	27
4.2 Wireshark	27
4.3 SIP packet Analysis	28
4.4 RTP packet Analysis	34
Chapter 5: Security	37-41
5.1 De active remote Login	37

5.1.1: Port number changing 37

5.1.2: Finding process of port number 38

5.1.3 Finding password of remote host 39

5.1.3 User binding: 40

5.2 User binding with IP 40

Chapter 6: Conclusion 42

Reference 43

List of Figure viii-xi

Figure 1: Soft Phone 09

Figure 2(a): Xlite soft phone 13

Figure 2(b): Xlite soft phone configuration 14

Figure 3: IAX trunk setup 15

Figure 4(a): Outbound Route configuration 16

Figure 4(b): Outbound route configuration 17

Figure 5(a): IM tab in Elastix Graphical User Interface 17

Figure 5(b): Openfire language selection 18

Figure 5 (c): Openfire Server settings 18

Figure 5(d): Openfire Database settings 19

Figure 5(e): Openfire Profile settings 19

Figure 5(f): Openfire Administrator account settings	20
Figure 5(g): Openfire Setup Complete Console	20
Figure 5(h): Openfire Administrator Login Console	21
Figure 5(i): Openfire Server information console	21
Figure 5(j): Openfire user creation	21
Figure 6(a): Spark user creation	22
Figure 6(b): Spark Start chat	23
Figure 6©: Spark chat	23
Figure 6(d): Spark Chat Bar	23
Figure 7(a): Queue configuration	24
Figure 7(b): Form configuration	25
Figure 7(c): Form configuration	25
Figure 7(d): Group Configuration	26
Figure 7(e): Agent configuration	26
Figure 7(f):Campaign configuration	27
Figure 7(g): Agent login console	27
Figure 8: Wireshark console	28
Figure 9: All packet showing	29
Figure 10: Type “sip” for filtering SIP packet	29

Figure 11: SIP packet filtered 30

Figure 12: Showing function of each layer of 557no SIP INVITE packet 30

Figure 13: Showing function of Frame 31

Figure 14: Showing information of Internet protocol version 31

Figure 15: Showing information of User Datagram Protocol 32

Figure 16: Showing information of Session initiation protocol 32

Figure 17: Showing information of Request-Line 33

Figure 18: Showing information of message header 34

Figure 19: Showing Information of Message Header 34

Figure 20: Capturing RTP packets all stream 35

Figure 21: Showing all information about RTP data stream 35

Figure 21: Capturing stream analysis 36

Figure 22: Showing Forward direction packet information 36

Figure 23: Showing reverse direction packet information 37

Figure 24: Command for going Configured file 38

Figure 25: Showing port number of ssh 39

Figure 26: Changing SSH port number 39

Figure 27: Showing all port number set as by default 39

Figure 28: After changing port number 40

Figure 29: running script 40

Figure 30: Allowing some authorized user 41

Figure 31: Allowing some authorized user 41

Figure 32: Service SSHD restarting 41

Figure 33: Command for entering host.allow file 42

Figure 33: Binding IP address 42

Figure 34: Allowing Host 42

Figure 35: Deny all unauthorized IP 42

List of table xi

Table 1: Codec 08

Chapter 1

Introduction

1.1 General Introduction

IP telephony feature has been installed. IP Telephony represents the next generation of telecommunication services. As the price for IP Telephony equipment decrease it rapidly becomes more cost competitive. In IP Telephony synergistic effects can also be produced by utilizing the existing knowledge base that exists within the telecommunication and computer networking community. Elastix is an open source PBX which has been used. Elastix is a command line program. This means that you have to open a command line interface (a DOSbox,a shell) and type in an appropriate elastix command. This also means that there is no graphical user interface. It is an Open source program. SIP refers to as Session Initiation Protocol, Widely used in IP telephony system. It is request-response method. Inter-Asterisk exchange (IAX) is a communications protocol native to the Asterisk private branch exchange (PBX) software, and is supported by a few other softswitches, PBX systems, and softphones. It is used for transporting VoIP telephony sessions between servers and to terminal devices.IAX now most commonly refers to IAX2, the second version of the IAX protocol. The original IAX protocol is deprecated **[1]**. Openfire is an instant messaging and groupchat server that uses XMPP server written in Java **[2]**. XMPP refer to as Extensible Messaging and Presence Protocol (XMPP) is a communications protocol for message-oriented middleware based on XML (Extensible Markup Language) **[3]**. Spark is an Open Source, cross-platform IM client optimized for businesses and organizations. It features built-in support for group chat, telephony integration, and strong security. It also offers a great end-user experience with features like in-line spell checking, group chat room bookmarks, and tabbed conversations **[4]**.

1.2 Object of our thesis

In this project secured IP telephony system has been considered and implemented so that hacker could not able to hacked the system or modify the system configuration. Security system configured in 3 level's through Backtrack. SIP INVITE packet and RTP packet over the network has been analyzed. Openfire has been configured combined with Spark for instant messaging. IAX trunk has been created between two servers of same network so that extension of one server can call extension of another server in same network such as intercom, it is costless and secured. Call center installed and configured for interacting between agent and telephone subscriber.

1.3 Organization of the thesis

There have already been cases of hackers taking over IP clients, due to lack of administration passwords in one case, and due to vulnerabilities associated with unauthenticated configuration server access in another. Like any application, a risk assessment of IP telephony needs to be done to assess its intrinsic value, to understand the implications of loss, and to formulate a security policy. We can start this assessment by making some key observations on telephony and data security in general.

In Chapter 2, basic theory has been discussed.

In Chapter 3, configuration and installation has been discussed.

In Chapter 4, SIP and RTP packet has been analyzed by Wireshark.

In Chapter 5, Security system has been implemented.

Chapter 2

Theory

2.1 IP telephony

Internet Protocol telephony apply the Internet Protocol's packet-switched connections for exchanging voice, fax and other terms of application as an alternative of dedicated circuit-switched connection of the Public Switched Telephone Network (PSTN). In short we can say that, IP-Telephony is the process of routing voice over the internet. By using the Internet, a call passes over the internet as packets of data on shared line and it’s avoiding the tax of the PSTN.

2.2 Elastix

Elastix is a composition of Open Source products and tools made simultaneously to become an integrated IP PBX.

2.2.1 Major component of Elastix

The major components that make up Elastix are given below

- ✓ **Asterisk** (currently v1.4) - the core PBX (Made by Digium)
- ✓ **vTigerCRM**® and **SugarCRM**® - CRM systems
- ✓ **A2Billing**® - Calling Card platform and billing application for Asterisk.
- ✓ **Flash Operator Panel** -a screen-based operator’s console
- ✓ **Hylafax**® - a software based FAX System
- ✓ **Openfire**® - Jabber Compliant Server for Instant messaging, presence management, SIP Phone
- ✓ **Conferencing -** control application
- ✓ **freePBX**® (embedded and standalone) - a web User Interface tool for Elastix.
- ✓ **A report system –** the part of Elastic (and freePBX) that provides CDR reporting.
- ✓ **A Maintenance system** - also part of Elastix, which provides low level interfaces to some components and real time system information

- ✓ **OSLEC** - Software Based Echo Cancellation
- ✓ **Postfix**® - a well known mail server.
- ✓ **Round Cube webmail –** Webmail Interface
- ✓ **CentOS**® - a version of Linux related to a very well known Enterprise Linux (but without the branding and support) **[6].**

2.3 Asterisk

Asterisk is “Open Source PBX software” which once installed in PC hardware along with the correct interfaces, can be used as a full featured PBX for home users. Asterisk is much more than a PBX. It allows real time connectivity between PSTN and VoIP networks.

2.3.1 Used of ASTERISK

- ✓ Extreme cost reduction.
- ✓ Telephony system control and independence.
- ✓ Easy and rapid development environment.
- ✓ Feature rich.
- ✓ Dynamic content on the phone.
- ✓ Flexible and powerful dial plan.
- ✓ Open source running on top of Linux.
- ✓ Asterisk architecture limitations.

2.3.2 Asterisk Dialplan

Heart of any Aserisk System is its dialplan which defines how Asterisk maintains inbound and outbound calls. It defines how Asterisk handles each and every call to the PBX. Most of the dial plan is enclosed in the extensions.conf file at the /etc/asterisk directory. The dialplan is made up of four main parts: contexts, extensions, priorities, and applications.

2.3.3 Protocol

Asterisk supports:

- ✓ SIP
- ✓ H.323
- ✓ IAX v1 e v2
- ✓ MGCP
- ✓ SCCP (Cisco Skinny)

Brief description of Asterisk Protocol is given below-

A) H.323

The H.323 standard is a basis method for the transmission of real-time audio, video, and data communications over packet-based networks. It specifies the components, protocols, and procedures providing multimedia communication over packet-based networks Packet-based networks include IP–based (including the Internet) or Internet packet exchange (IPX)–based local-area networks (LANs), enterprise networks (ENs), metropolitan-area networks (MANs), and wide-area networks (WANs). H.323 can be applied in a variety of mechanisms—audio only (IP telephony); audio and video (video telephony); audio and data; and audio, video and data. H.323 can also be applied to multipoint-multimedia communications.H.323 provides point to point or point to multipoint communication. The components of H.323 are-

- ✓ Terminal
- ✓ Gateway
- ✓ Gatekeeper
- ✓ Multipoint control unit

B) MGCP

MGCP – Media Gateway Control Protocol —is the most important protocol in next generation networks because it is responsible for implementing the migration from PSTN to IP telephony at large enterprises, ISPs, and carriers by converting today's TDM circuits into tomorrow's voice packets. MGCP is a protocol that operates between a Media Gateway (MG) and a Media Gateway Controller (MGC). Media Gateway - Terminates PSTN lines and packetizes media streams for IP transport **[7].**

C) Skinny Client Control Protocol

When Telephony systems are moving to a common wiring plant the end station of a LAN or IP-based PBX must be simple to use, familiar and relatively cheap. While the H.323 recommendations are pretty expensive, an H.323 proxy can be used to communicate with the Skinny Client using the SCCP. Skinny client control protocol uses the following items:

- ✓ TCP/IP to/from one or more Cisco Call Manager(s) to transmit and receive a stimulus.
- ✓ RTP/UDP/IP to/from a similar Skinny client or H.323 terminal for audio **[8].**

D) Inter Asterisk Extension Protocol

IAX is the Inter-Asterisk exchange protocol, which facilitates VoIP connections between servers, and between servers and clients that also use the IAX protocol. The protocol is highly optimized for VoIP calls where low overhead and low-bandwidth consumption are priorities. This pragmatic aspect makes IAX more efficient for VoIP than protocols that consider possibilities far beyond current needs and specify many more details than are strictly necessary to describe or transport a point-to-point call. Furthermore, because IAX is designed to be lightweight and VoIP-friendly, it consumes less bandwidth than more general approaches. IAX is a binary protocol, designed to reduce overhead, especially in regards to voice streams. Bandwidth efficiency, in some places, is sacrificed in exchange for bandwidth efficiency for individual voice calls. For example, when transmitting a voice stream compressed to 8 kbit/s with a 20 ms packetization, each data packet consists of 20 bytes. IAX adds 20% overhead, 4 bytes, on the majority of voice packets while RTP adds 60% overhead with 12 additional bytes per voice packet. IAX also uses the same UDP port for both its signaling and media messages, and because all communications regarding a call are done over at the same point-to-point path, NAT traversal is much simpler for IAX than for other commonly deployed protocols.

E) Session Initiation Protocol

The Session Initiation Protocol signaling protocol, for creating, modifying and terminating sessions. These sessions can be multimedia conferences, Internet telephone calls and similar application consisting of one or more media types as audio, video, whiteboard etc.SIP is a textual protocol based on the client-server model, with requests generated by one entity (the client), and sent to a receiving entity (the server) which responds them. A request invokes a method on the server and can be sent either over TCP or UDP. The most important SIP method, of the currently six, is the INVITE method, used to initiate a call between a client and a server. A SIP network is composed of four types of logical SIP entities. Following are the four types of logical SIP entities:

- **USER AGENT:** In SIP, a **User Agent** (UA) is the endpoint entity. as follows:
  - ✓ **User Agent Client (UAC)—**a client application that initiates SIP requests.
  - ✓ **User Agent Server (UAS)—**a server application that contacts the user when a SIP request is received and that returns a response on behalf of the user.
- **PROXY SERVER**: A Proxy Server is an intermediary entity that acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests are serviced either internally or by passing them on, possibly after translation, to other servers. A Proxy interprets, and, if necessary, rewrites a request message before forwarding it.
- **REDIRECT SERVER:** A **Redirect Server** is a server that accepts a SIP request, maps the SIP address of the called party into zero (if there is no known address) or more new addresses and returns them to the client. Unlike Proxy servers, Redirect Servers do not pass the request on to other servers.
- **REGISTRAR:** A **Registrar** is a server that accepts REGISTER requests for the purpose of updating a location database with the contact information of the user specified in the request **[9].**

2.3.4 Codec and codec translation

There are several codec available for Asterisk and these codec can be transparently translated from one to another. Some codec in Asterisk are supported only in pass-through mode, and these codec can’t be translated. The following codec are supported:

Codec	Codec Bit rate(Kbps)	Normal Ethernet Bandwidth(Kbps)	Approx. MByte user per hour
G.711	**64**	**87.2**	**39.24**
G.729	**8**	**31.2**	**14.04**
G.723.1	**6.4**	**21.9**	**9.86**
GSM	**13.2**	**28.7approx.**	**12.92approx.**
iLBC	**15.2**	**30.83approx.**	**13.87approx.**
G.723.1	**5.3**	**20.8**	**9.36**
G.726	**32**	**55.2**	**24.84**
G.726	**24**	**47.2**	**21.24**
G.728	**16**	**31.5**	**14.18**

Table 1: Codec

2.4 Softphone

A **softphone** is a software program for manufacturing telephone calls over the Internet using a general reason computer, rather than using dedicated hardware. Often a softphone is designed to act like a traditional telephone, sometimes appearing as an image of a phone, with a display panel and buttons with which the user can act together. A softphone is usually used with a headset connected to the sound card of the PC, or with a USB phone.

Figure 1: Soft Phone

2.5 Openfire

Openfire is an instant messaging and group chat server that uses XMPP server. Its written in Java and licensed under the Apache License. previously known as wildfire & jive messenger **[2].** Open fire is a free, open-source and full featured Jabber-based Instant Messaging server **[12].** This server allows for Instant Messenger programs to interconnect to each other via this server **[13].**Open fire is a real-time collaboration (RTC) server dual-licensed under the Open Source GPL. It uses the only widely adopted open protocol for instant messaging, XMPP (Extensible Message Presence Protocol). Open fire is easy to set up and administer, but offers rock-solid security and performance **[14].** One of most attractive Open fire's features is Instant Messaging Transports that provide connectivity to multiple external Instant Messaging services.. When we register to use a messaging transport (IM client), the user ID and password for that instant messaging service are stored in encrypted form on the XMPP server. When we delete or remove the transport from the XMPP client, these IM-based credentials are removed from the server as well **[15].**

2.6 XMPP

XMPP (Extensible Messaging and Presence Protocol) is a protocol based on Extensible Markup Language (XML) and desired for instant messaging (IM) and online presence detection. It functions two or more servers, and facilitates near-real-time operation. The protocol may eventually permit Internet users to send instant messages to anyone else on the Internet, regardless of differences in operating systems and browsers" **[16].** XMPP resulted out of the early XML streaming technology developed by the Jabber Open Source community and is now the leading protocol for exchanging real-time structured data. XMPP can be used to stream virtually any XML data between individuals or applications, making it a perfect choice for applications such as IM **[17].** The Extensible Messaging and Presence Protocol (XMPP) is an free technology for real-time communication, using the Extensible Markup Language (XML) as the base format for exchanging information. In summary, XMPP provides a way to send small pieces of XML from one entity to another in close to real time.[18]It supports different communicating methods, such as unicast , multicast and group talk fashion. Quite a few protocols and frameworks that support the IM service have been created already. In addition, Session Initiation Protocol based design, SIMPLE (SIP for Instant Messaging and Presence Leveraging Extensions) and IM extension also perform the same functionality.

- **Sequence of Interaction**

The sequence of the initial interaction between client and server is as follows:

1. The client connects to the server and sends credentials like the username and password.
2. The server authentication the received credentials against its user database and send a response to the client.
3. When authentication is successful, the client receives a response containing presence notification data. This is a collection of presence data from different buddies of the user, which the client authenticated to the server **[19].**

✓ Message: It is carried out in a "store and push" mechanism through which one entity pushes information to another, such as, exchange messages between two users .

<message from’ safi@ example.bd/laptop’
to=’hemel@.example.bd’ />
<body>Hello</body>
</message>

✓ Presence: When multiple entities receive information about a given entity it is broadcast to which they’ve subscribed, such as, entity’s availability.

<presence from=’safi @example.bd/laptop
to=’hemel@example.bd’ />

✓ Iq: It is a request-response mechanism, similar to HTTP, that lets entities make requests and receive responses from each other, for example: file transfer, roster retrieve.

<iq type=’get’
from=’safi @.example .bd/laptop’>
<query xmlns=’jabber:roster’/>
</iq

All primitive XML stanzas must reside in the <stream/> block, which stands for a XML stream. The meaning of these XML stanzas should be treated as the content of a XML stream. Spark web is an open source, web-based IM client. It featured built in support for group chat and strong security. It also offers a great end-user experience with features like group chat room bookmarks, and tabbed conversations.

2.7 Call Center

Objective of call center is to generate calls automatically to numbers that have been previously uploaded in a CSV file format. It also monitors calls received through a queue. To use the Call Center Module, we must have to select a few options and provide some necessary data. Here's the order in which it is recommend to enter this data.

1. Enter information for the agents.
2. Enter types of breaks (if necessary).

- **For incoming calls:**
  - ✓ You can upload a CSV file with customer information so this information can be displayed on your screen when a call is being received
  - ✓ Select the queue to be used for incoming calls
- **For outgoing calls:**
  - ✓ Create forms to collect information from customers that agents are calling.
  - ✓ Create outgoing campaigns that indicate telephone numbers to call, hours of calls, etc **[10].**

Chapter 3

Configuration & Installation

In this project softphone has been installed, extension created, trunk created, IVR created, IAX trunk configured, callcenter installed & configured, openfire installed & configured, spark installed & configured, wireshark installed & configured, backtrack installed & configured . We briefly described in this chapter why and how we have been configured IAX trunk, Call center, Openfire, Spark. Wireshark will describe in chapter 4 and backtrack will describe in chapter 5

3.1 Soft phone configuration

In our project we used Xlite soft phone. A soft phone is a software program that runs on a PC that emulates an IP telephone.

Figure 2(a): Xlite soft phone

The X-lite is the phone that will be configured to work with the extension made previously in Asterisk PBX. After installing Figure: 1 will appear on your screen. Than right clicked on Xlite monitor, an option appeared that is ‘SIP account setting”, clicked on that option than add page will appeared. After clicked on add button the configuration page will appeared.

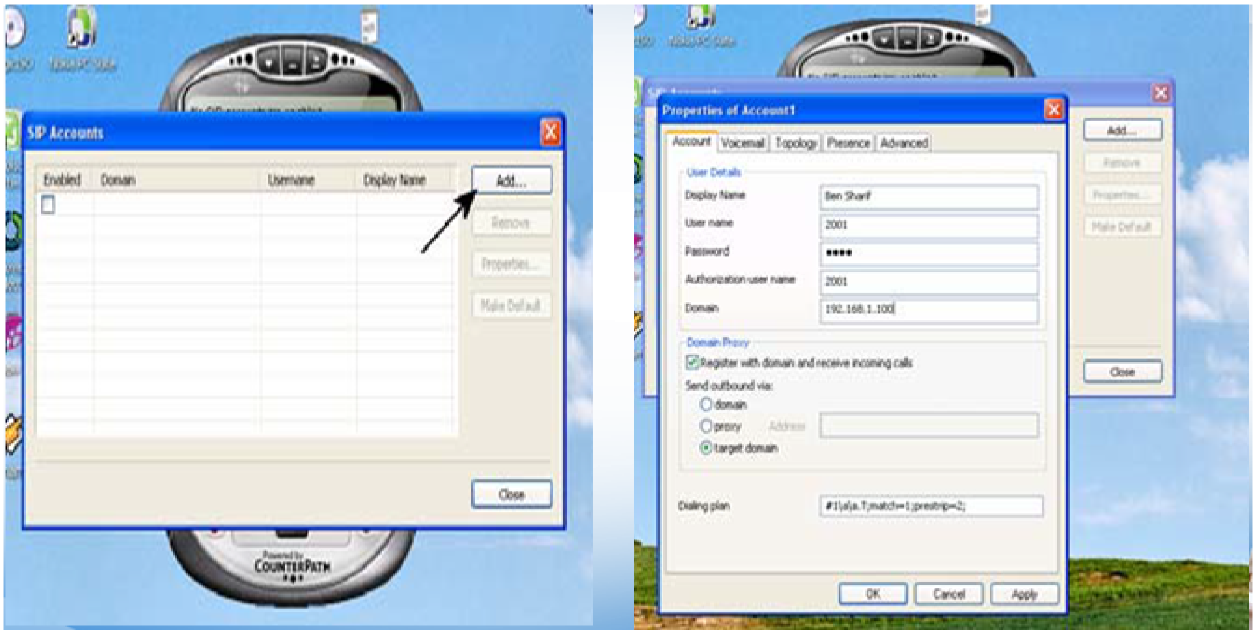


Figure 2(b): Xlite soft phone configuration

Now we have to configure account settings. On the display name we have to give a name which will show in the phone monitor, it could be anything as you want. Than user name, it will be the user extension number which we created on Elastix PBX server. After that password, It will be the user extension secret number. Authorization user name is not necessary. Than domain, domain will be the domain address actually the Elastix PBX server address where we create the extension.

3.2 IAX Trunk Set up

Suppose you have two branch of office, one branch in the Dhaka city and another branch are in the Chittagong city. You want that call cost between two branches will be low. Therefore we have two configure two asterisk servers in two branch office of same domain server and setup Inter Asterisk Exchange between two servers. Than call between two branches acts as intercom call and its toll free. After login in the Elastix server page, we will show PBX above, on the left side there will be trunk set up, after clicking on trunk set up some option will appear like “ SIP trunk setup", "IAX trunk setup" and so on, We will select IAX trunk set up, than Figure 3 will appear on your screen.

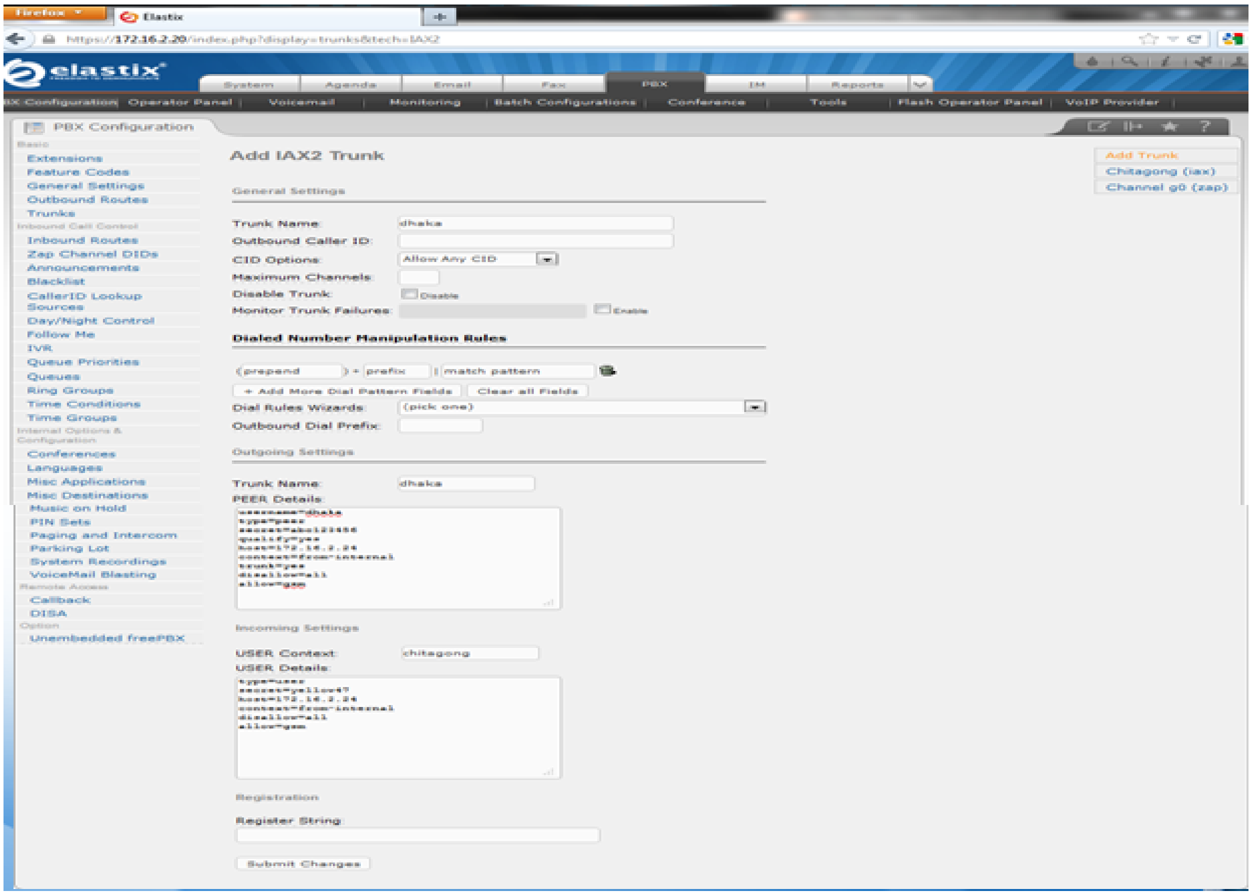


Figure 3: IAX trunk setup

Enter the details for IAX trunk. Only the settings below need to be modified - any other values can be left as default.

- ✓ **Trunk Name:** enter a name for the trunk
- ✓ **Outbound caller ID:** enter the telephone number that you wish for the trunk to present to the called party
- ✓ **CID Options:** set to Allow Any CID

In the **Dialed Number Manipulation Rules** section, delete match pattern and enter a period (.) instead. Now scroll down to **Outgoing Settings**. Now set the **Trunk Name** to anything like. In the **PEER Details** field enter:

“host=www.diu.edu.bd

user name=[as set by admin]

secret=[as set by admin]

type=peer

qualify=yes”

Click **Submit Changes**.

After that a page will appear where we have to click on “Apply Configuration Change Here”

3.3 Outbound route configure

On both systems, we need to setup an outbound route to tell it what to do when a caller in Dhaka wants to call an extension in Chittagong.

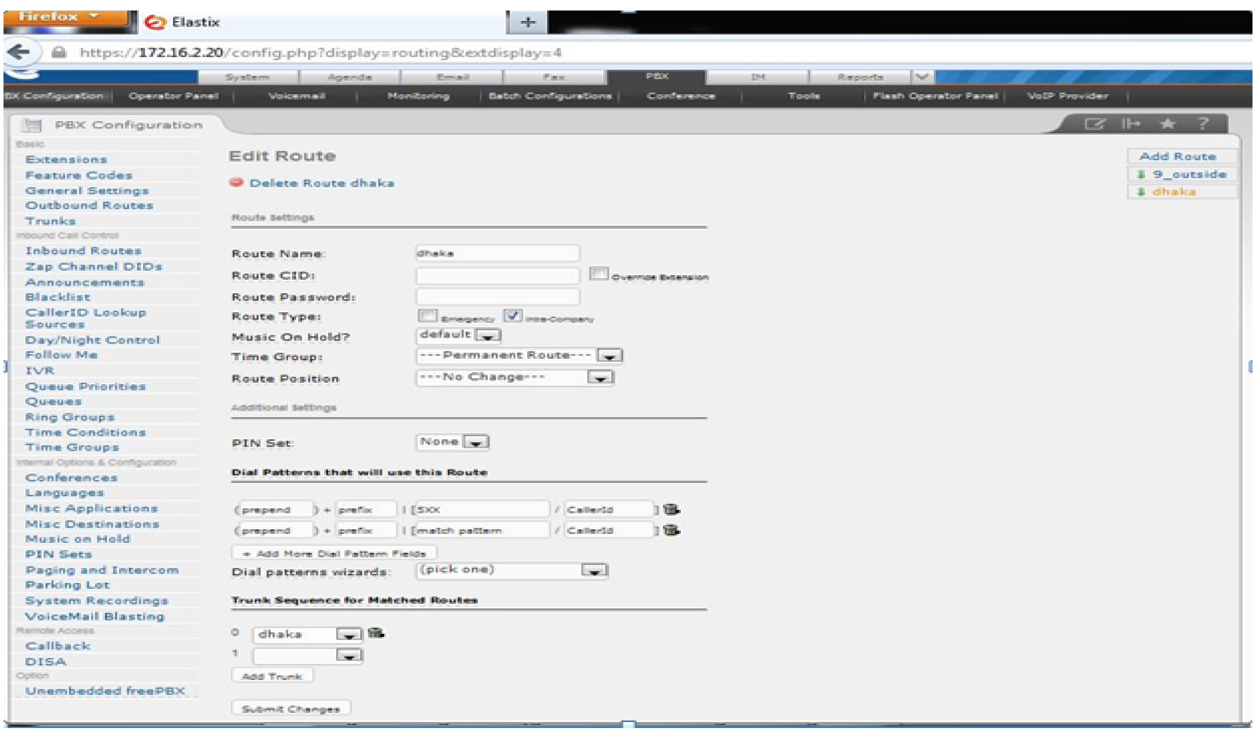


Figure 4(a): Outbound Route configuration

Enter a name for the route and within the **Dial Patterns that will use this Route** section change match pattern to a period. In the **Trunk Sequence for Matched Routes** section select the trunk we've just created in position zero using the dropdown box. Click **Submit Changes** to complete the configure. After that a page will appear where we have to click on "Apply Configuration Change Here"

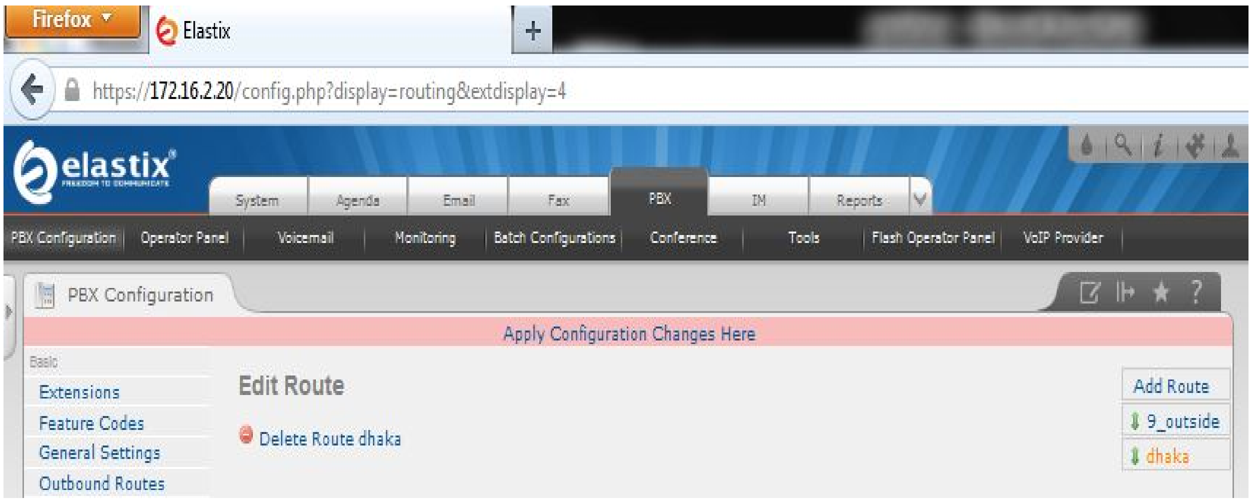


Figure 4(b): Outbound route configuration

3.4 Openfire configure

Openfire provides comprehensive group chat and instant messaging (IM) services using the XMPP protocol.

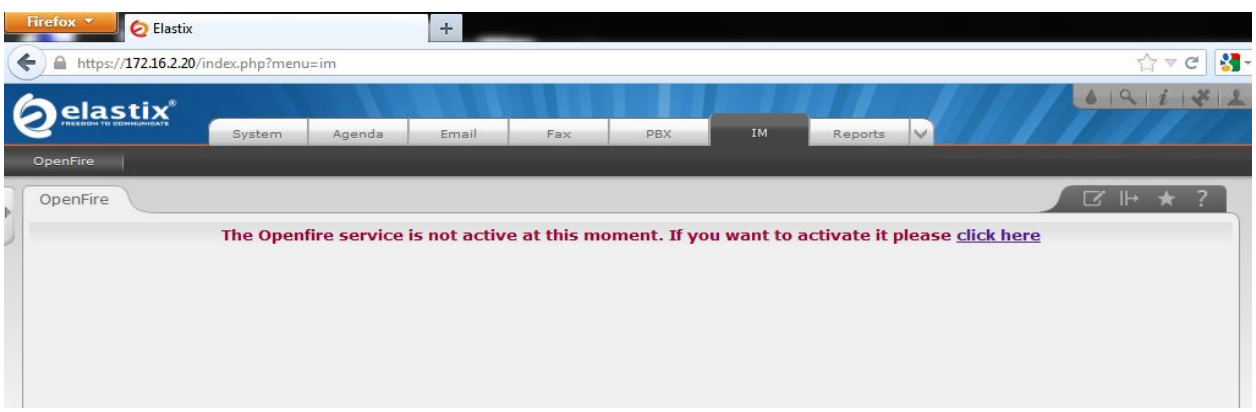


Figure 5(a): IM tab in Elastix Graphical User Interface

Go to IM tab in Elastix GUI and start the installation. Then we clicked the **click here** option. Then select the language & click **continue** button.

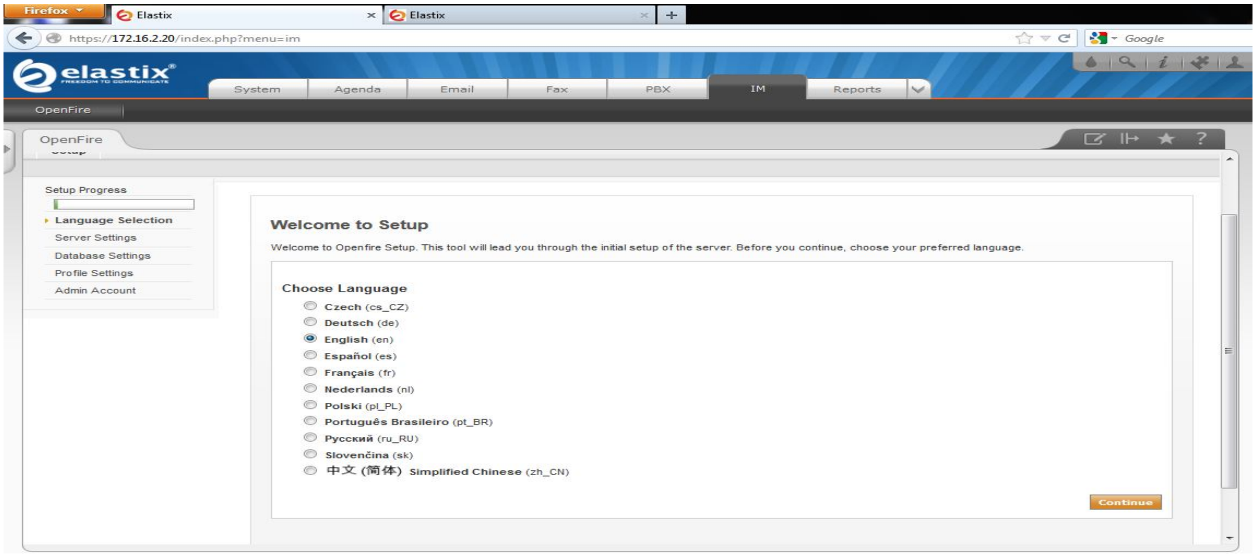


Figure 5(b): Openfire language selection

Now configure the **server settings** & go to next step click on **continue.**

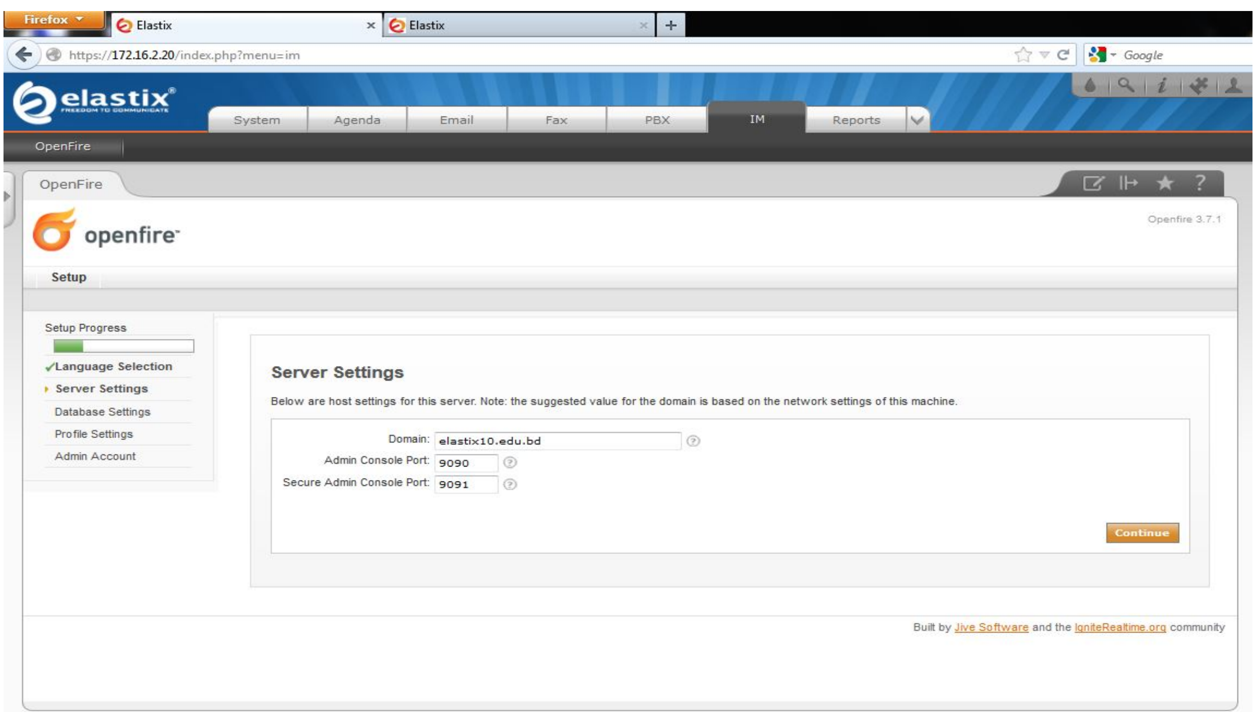


Figure 5 (c): Openfire Server settings

Then select the **Database settings** as **Embedded Database** & **continue.**

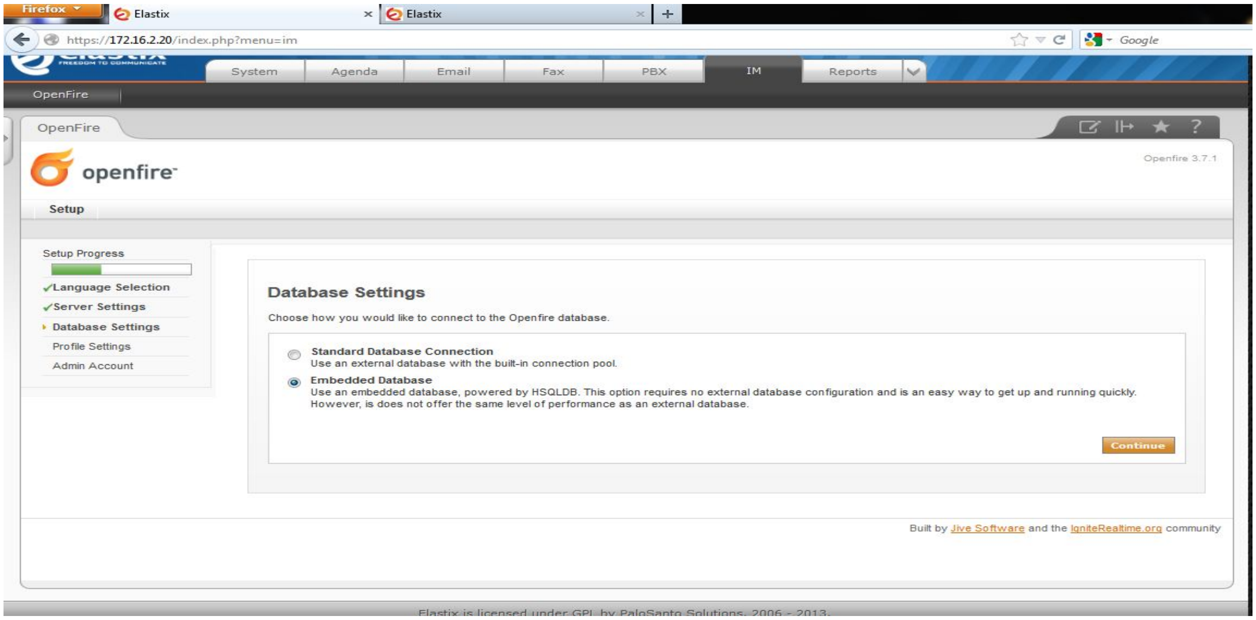


Figure 5(d): Openfire Database settings

Select Profile Settings as **Default** Server & **Continue**

.

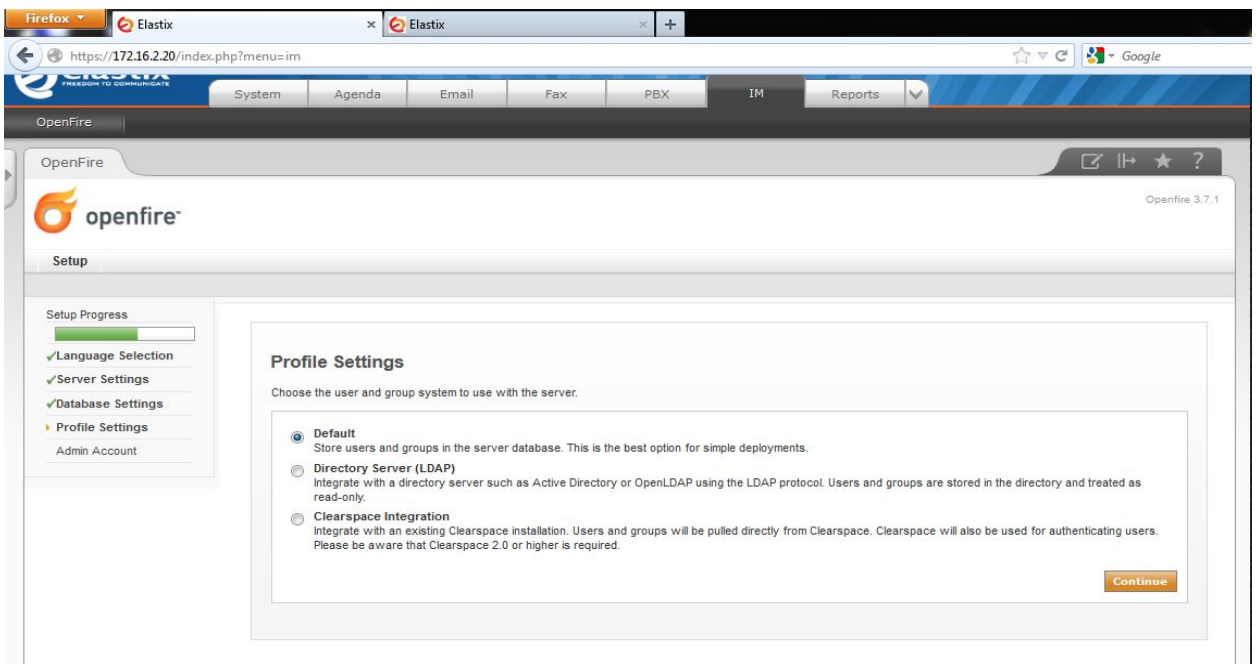


Figure 5(e): Openfire Profile settings

Now administrator account settings. Enter admin Email means the domain address which must have to be a valid domain address. After that we have to enter password and re enter the password again. Than clicked to continue

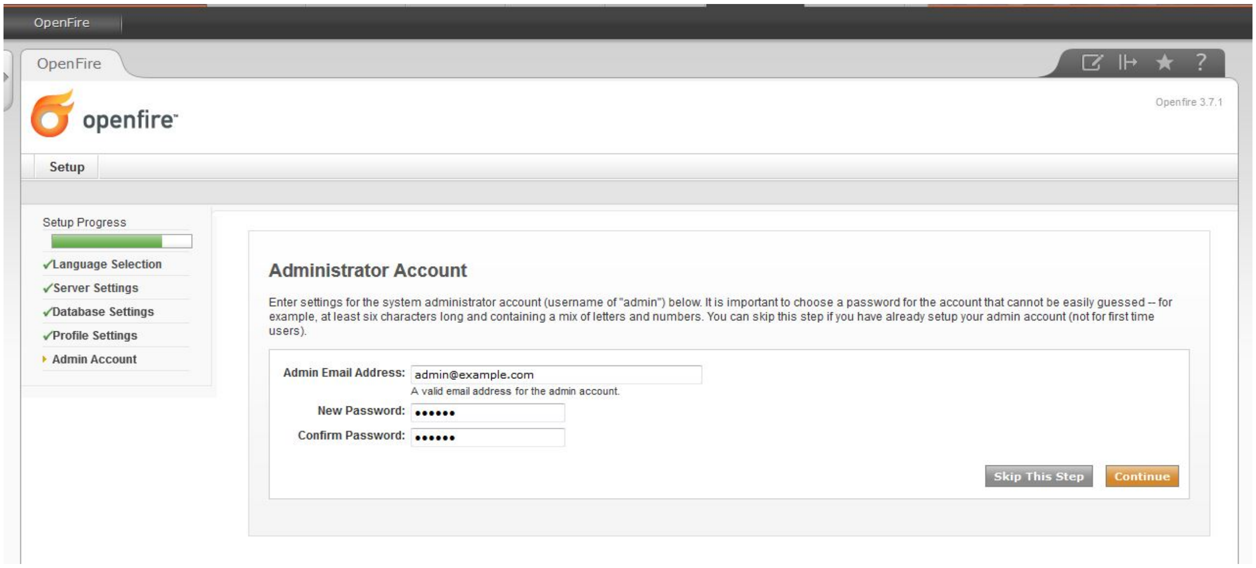


Figure 5(f): Openfire Administrator account settings

The **Openfire** setup is complete.

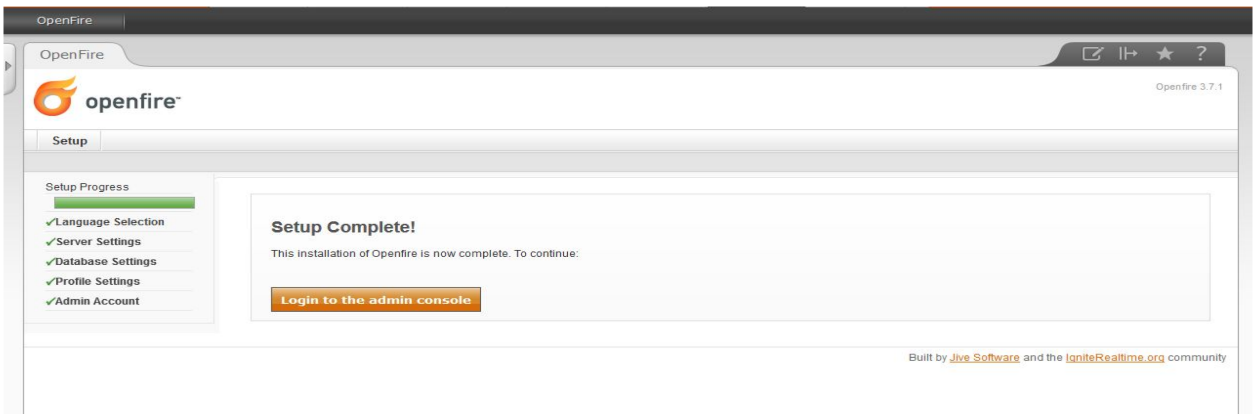


Figure 5(g): Openfire Setup Complete Console

Now login into the **Openfire** using username & password.

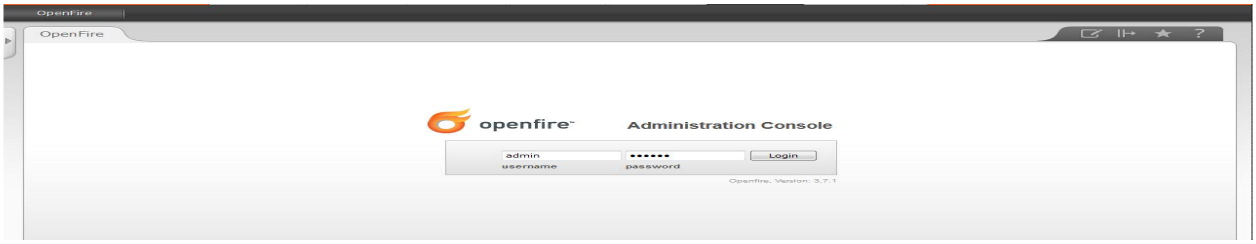


Figure 5(h): Openfire Administrator Login Console

Now see the **server information** go into the **server manager** option.

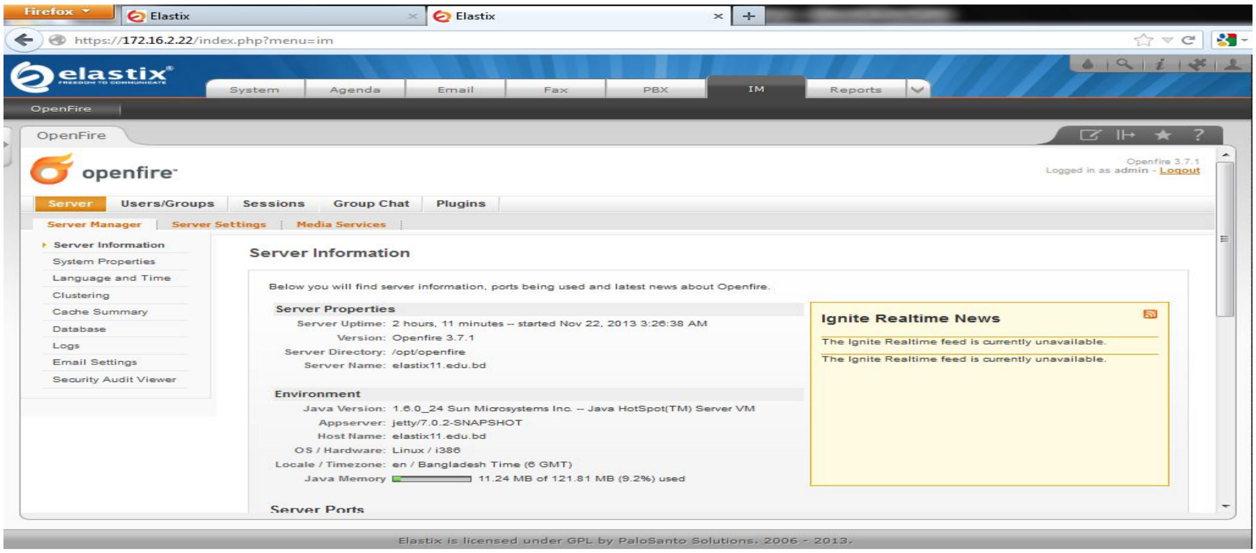


Figure 5(i): Openfire Server information console

Enter the **Servers/Groups** option & create **users**.

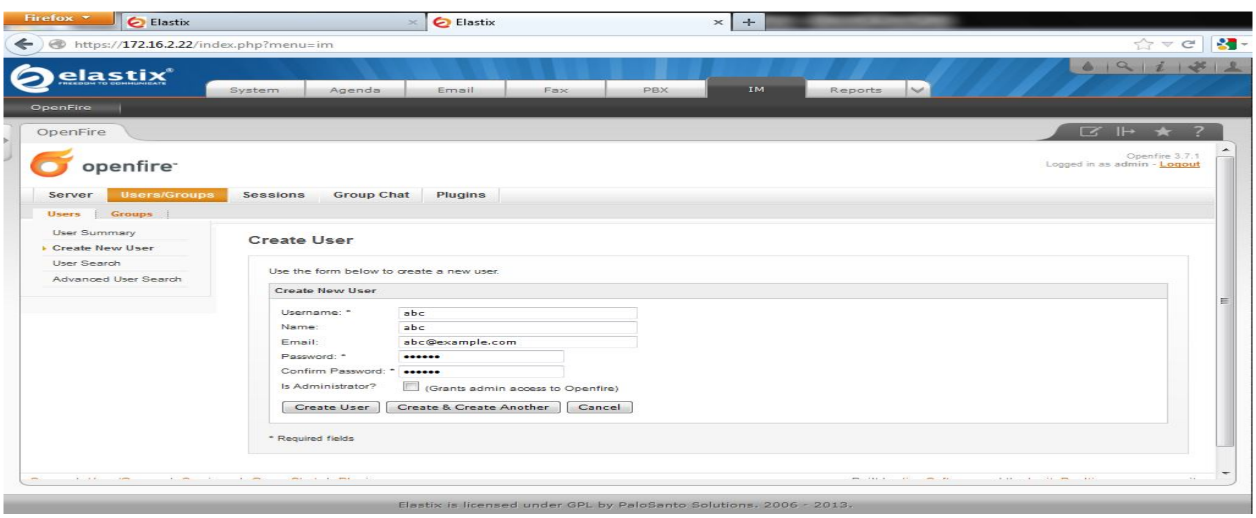


Figure 5(j): Openfire user creation

3.5 Spark

Spark is an Open Source, cross-platform IM client optimized for businesses and organizations. It features built-in support for group chat, telephony integration, and strong security. It also offers a great end-user experience with features like in-line spell checking, group chat room bookmarks, and tabbed conversations. Combined with the Openfire server, Spark is the easiest and best alternative to using un-secure public IM networks.

Figure 6(a): Spark user create

To configure the Spark Client, simply click on the account and fill in the following:

Username: Put desired username here.
Password & Confirm Password: Put desired password and confirm it here.
Server: Put Openfire Server IP here or domain if using a DNS infrastructure

Then click on **Actions** & enter **start a chat** option.

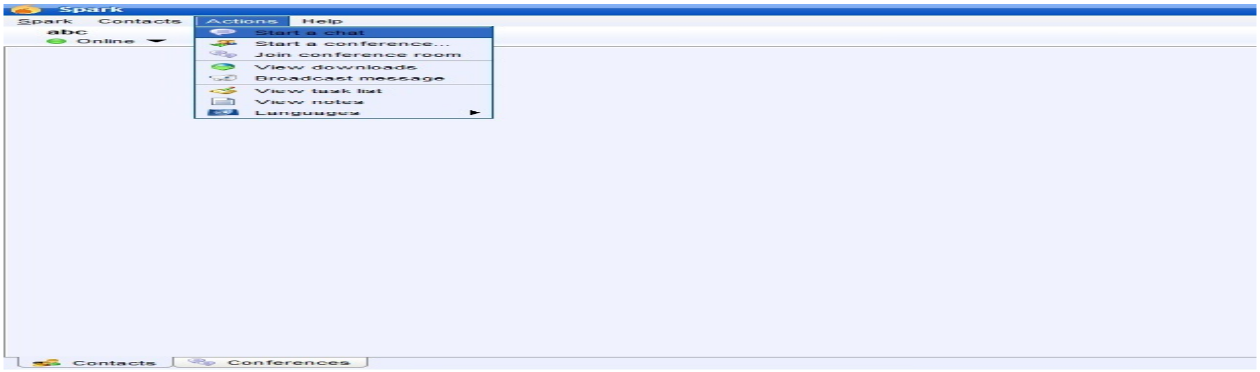


Figure 6(b): Spark Start chat

In the box enter an address of another user, with whom I want to do chat

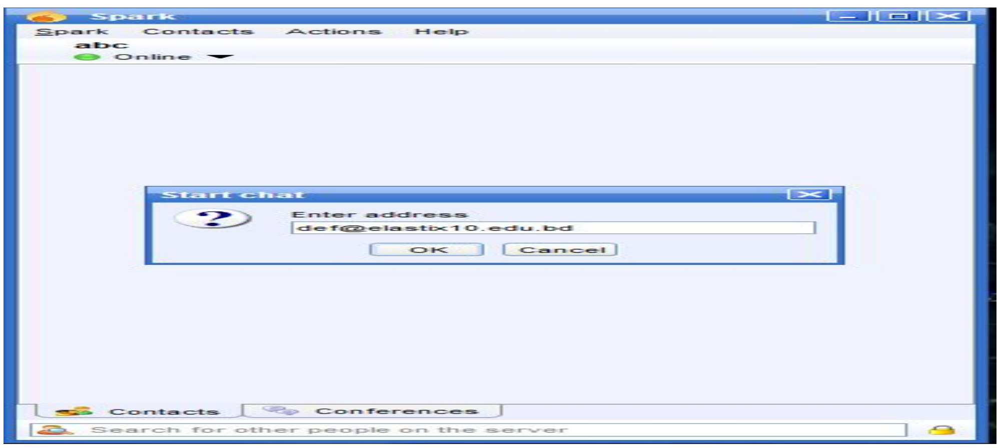


Figure 6©: Spark chat

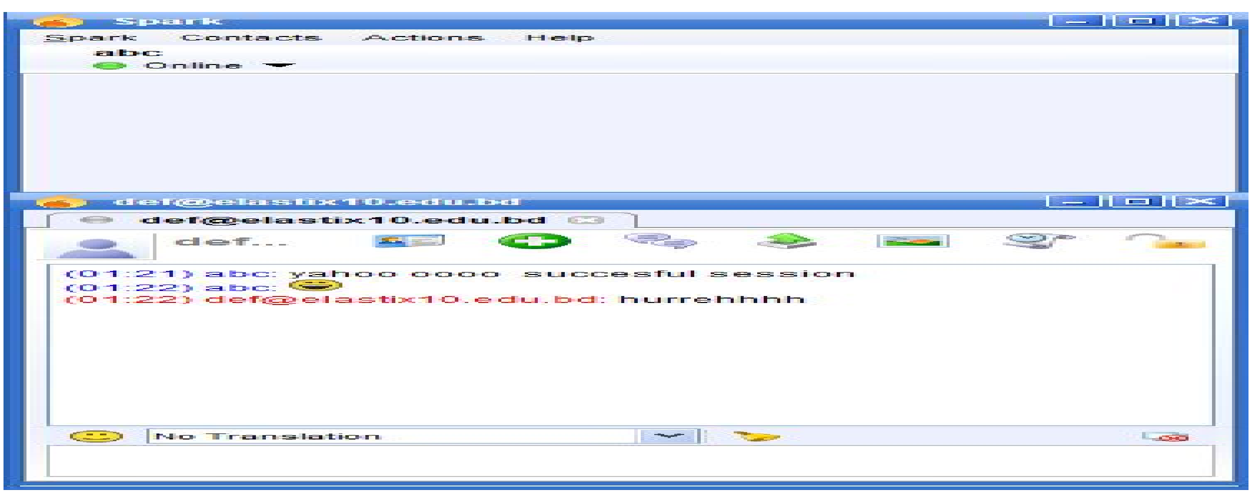


Figure 6(d): Spark Chat Bar

Then start chat using **Openfire** & **Spark**.

3.5 Callcenter

For call center configuration we have to configure some feature of call center Queue, Form, Group, Campaign and Agent Login.

Queue: Queues are designed for receiving calls in a call center. They allow monitoring of calls received by an agent and help to determine if a call was connected successfully or failed to be received.

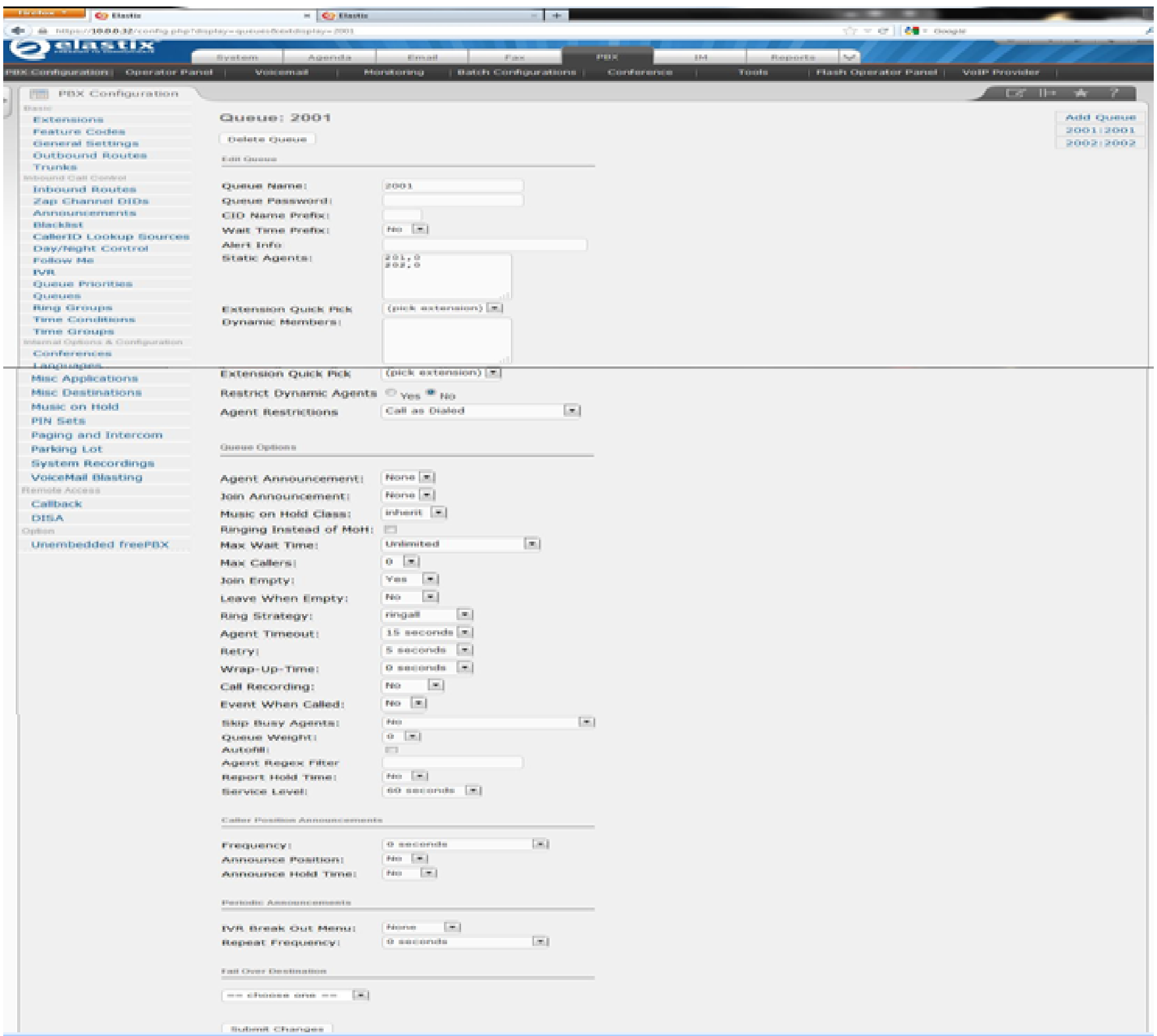


Figure 7(a): Queue configuration

Form: This window allows the creation of forms, which are created with the objective of collecting data to run a campaign and make calls from the agent console.

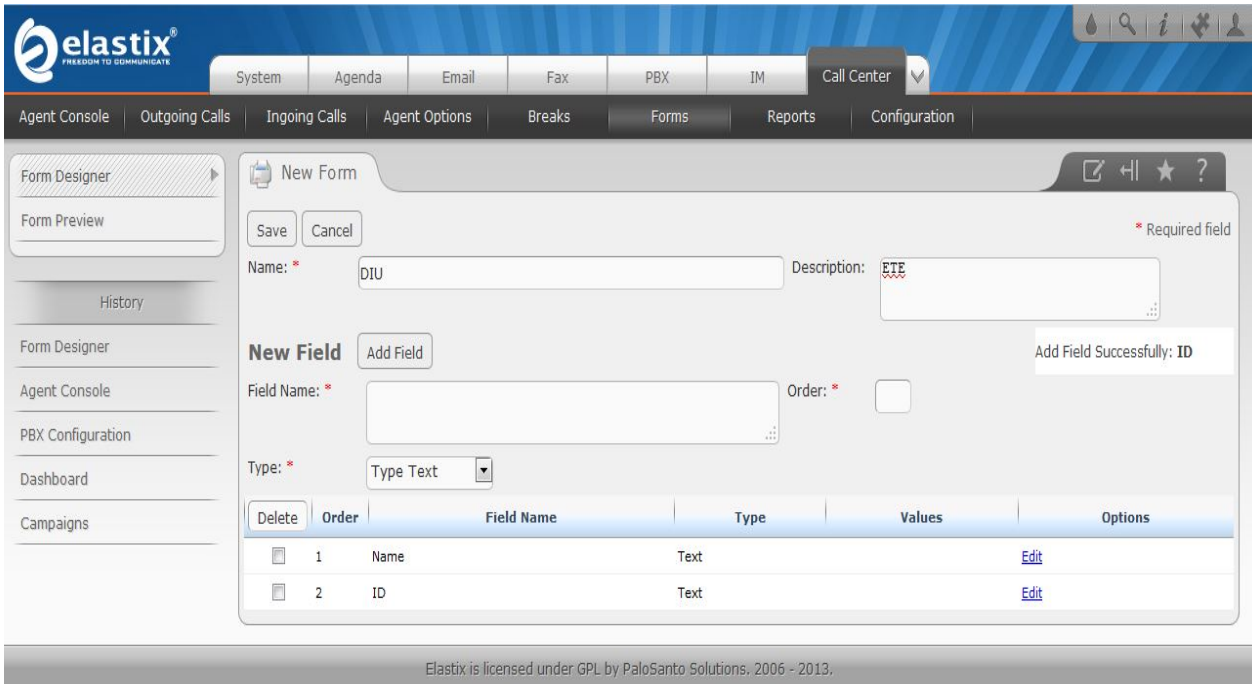


Figure 7(b): Form configuration

In the form window, we gave name DIU, you can give anything as you want. You can choose fields like as we choose ID, Level and Term. You can choose field type as we choose Text type and List type.

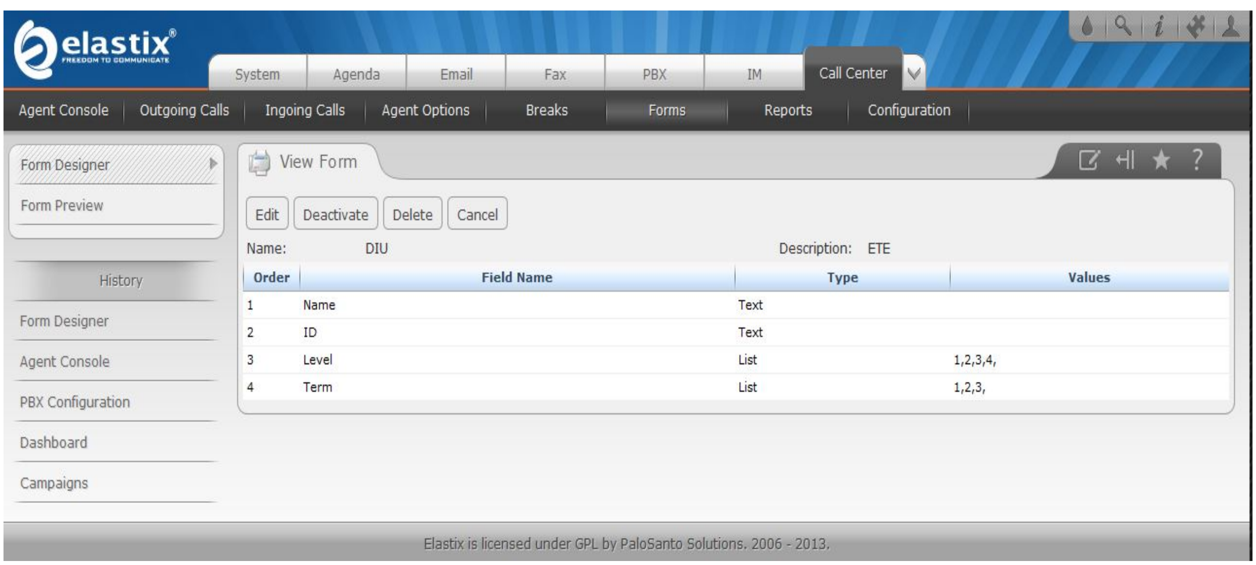


Figure 7(c): Form configuration

Group: Creation of users and agents is important for the operation of the call center. For security reason and control, must restrict the access for this user. It is necessary to create a group with restricted access to the interface. To create the group go to : System-> User-> Group ->Create new group.

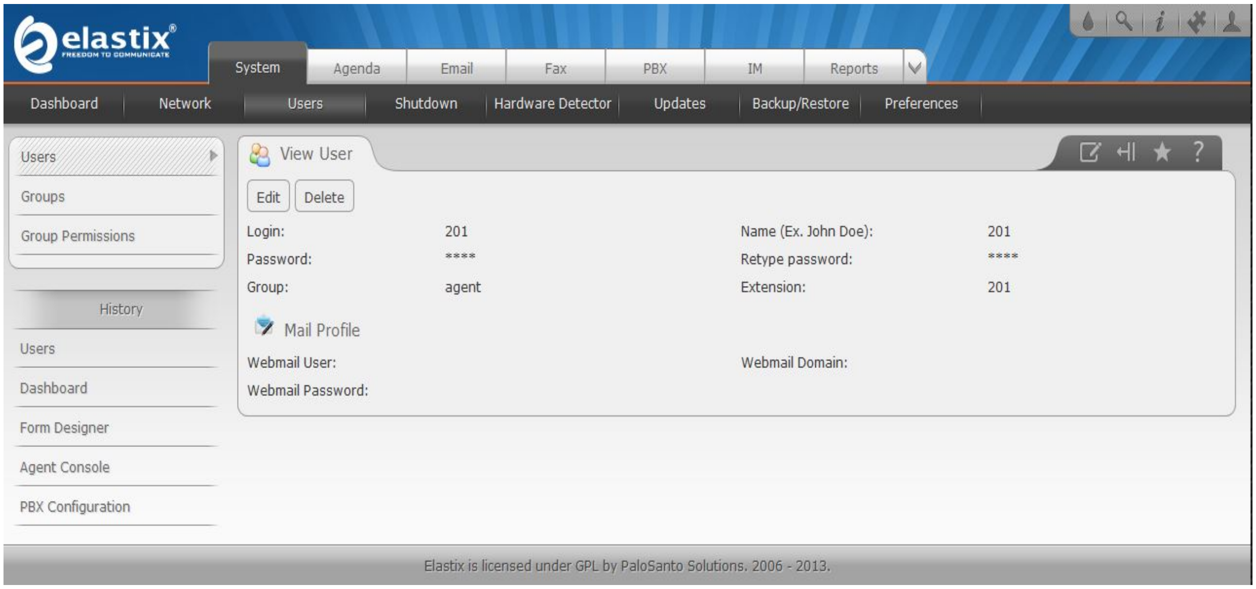


Figure 7(d): Group Configuration

Agent: This allows us to enter the data of the people going to operate the system and have been named agents. Each agent must have a number and password assigned in order to make or receive calls. In this window, Agent number will be the extension number which you create on PBX and password will be the extension secret password.

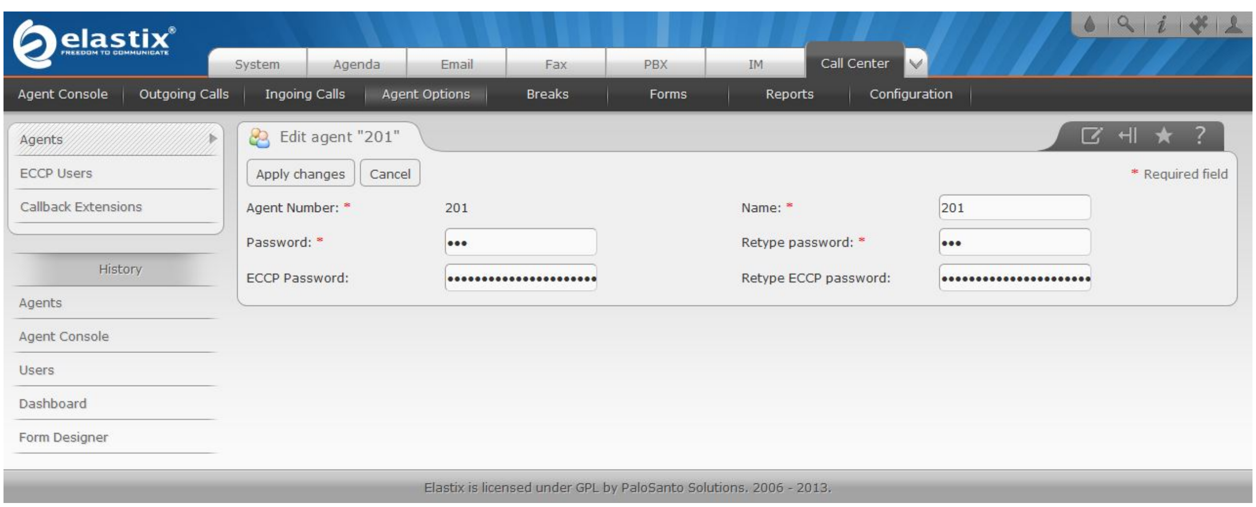


Figure 7(e): Agent configuration

Campaign: This section is used to create what is known as outbound campaigns, which is information that generates a series of calls automatically to telephone numbers that are uploaded in a CSV file.

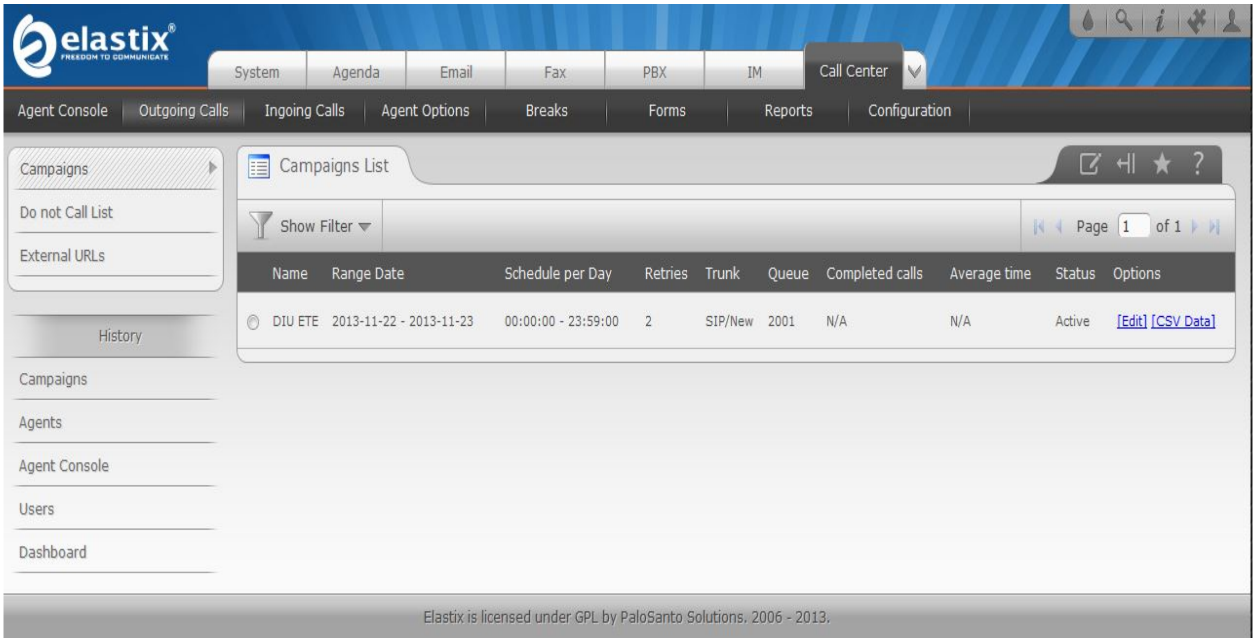


Figure 7(f): Campaign configuration

Agent login: The Agent Console provides agents the ability to conduct a Telephone Campaign (Default is surveys to telephone numbers), by an agent of the call center.

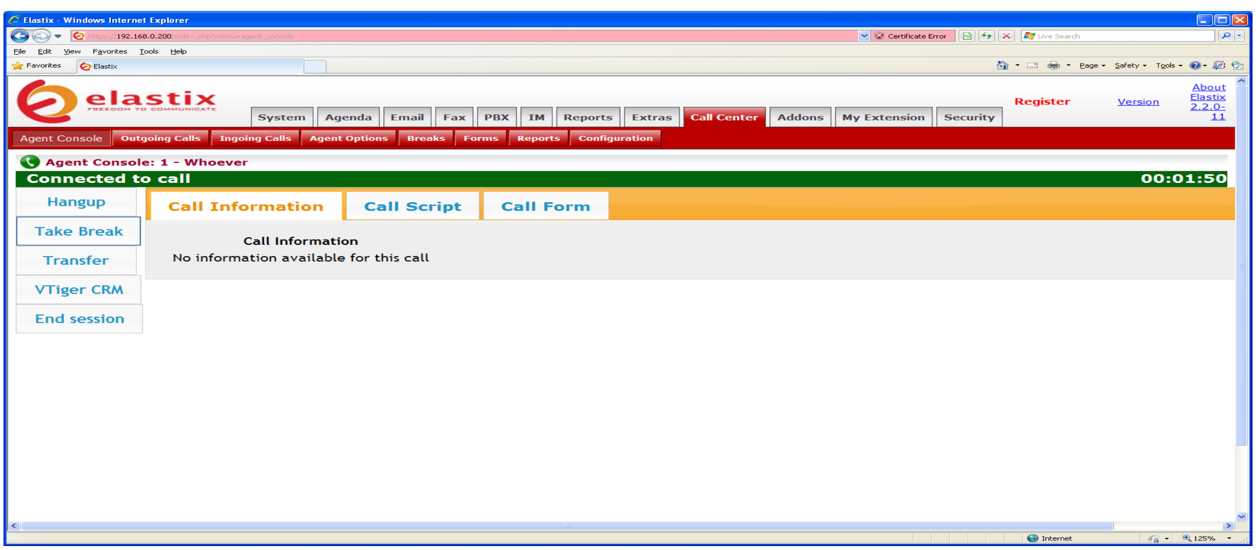


Figure 7(g): Agent login console

Chapter 4

Packet Analysis

4.1 At first we have to know actually what is packet analysis. Packet analysis is a process which describes the way of capturing and interpreting live data as it passes over a network. It's also refer to as protocol analysis and it's used for better understanding what is happening on the network. There are various types of packet sniffing programs, including both free and commercial ones. A few of the more popular packet analysis programs are tcp dump (a command-line program), Omni Peek, and Wireshark (both GUI-based sniffers).

4.2 Wireshark

In our project we used WIRESHARK, which is a protocol analyzer, or "packet sniffer" application, used for network troubleshooting, analysis, software and protocol development, and education. It allows the user to see all traffic being passed over the network by putting the network card into promiscuous mode. Wireshark is an open-source program.

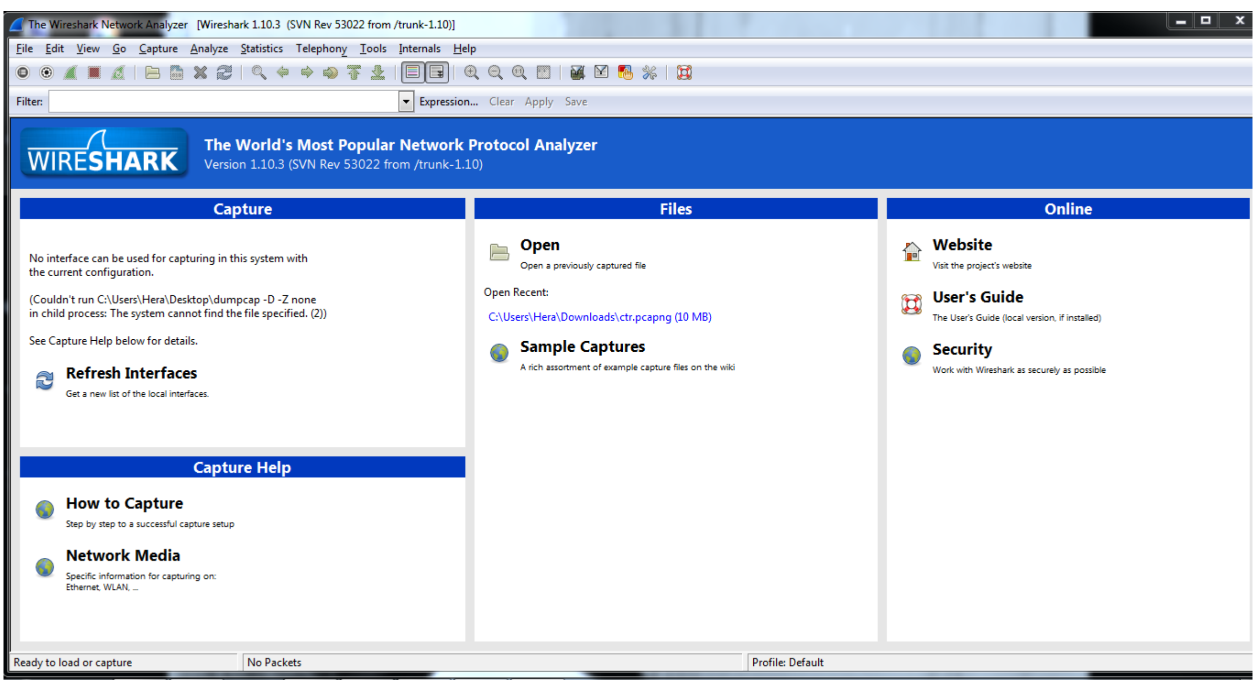


Figure 8: Wireshark console

At 1st Have to make call between two IP telephony in our network.

2ndly Have to go to the wireshark packet capture option.

3rd Click to Start

4th Start packet capturing

5th Stopped packets capturing. Go back to Wireshark, and from the Capture menu, select Stop to stop capturing packets. Then, look at the content of the captured packets

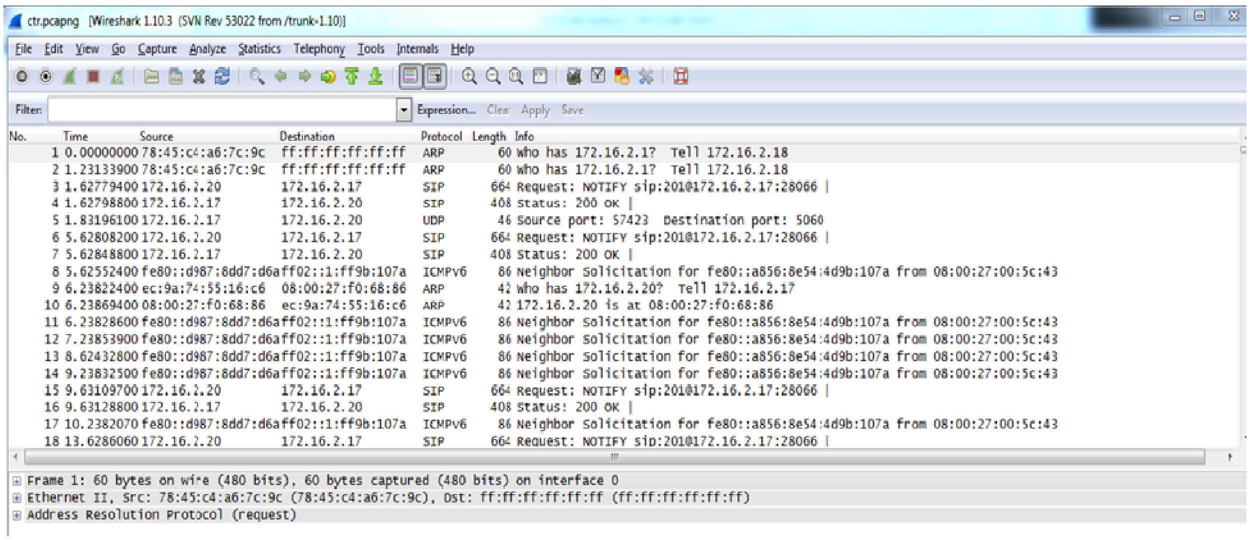


Figure 9: All packet showing

4.3 SIP packet Analysis

Now SIP packet will be captured through the Wireshark packet analyzer, therefore in the above "Filter " option have to write "sip" than clicked on to " Apply"

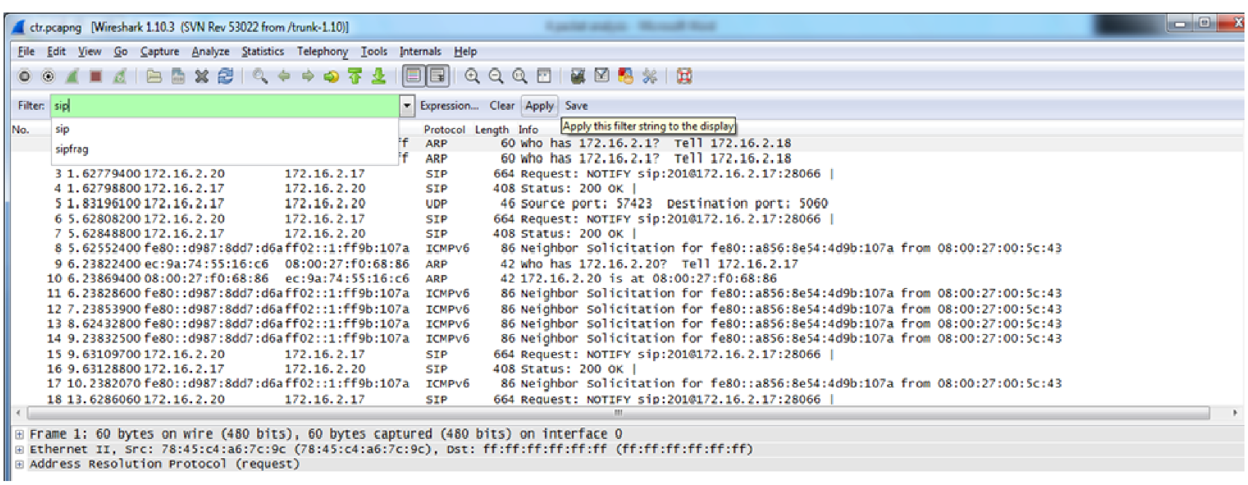


Figure 10: Type "sip" for filtering SIP packet

Than only SIP protocol packet will be shown in the console.

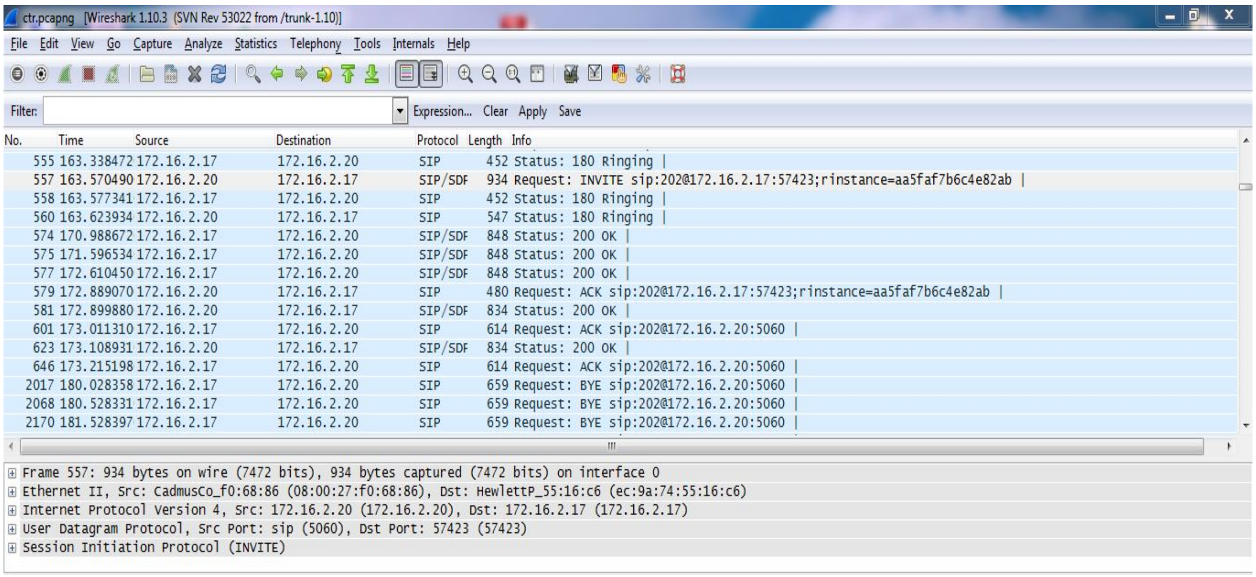


Figure 11: SIP packet filtered

As SIP is a request-response method. Let see 557 no packet, which is a SIP invite packet and its SIP request process. After double clicked on the 557 no packet below console will be appeared

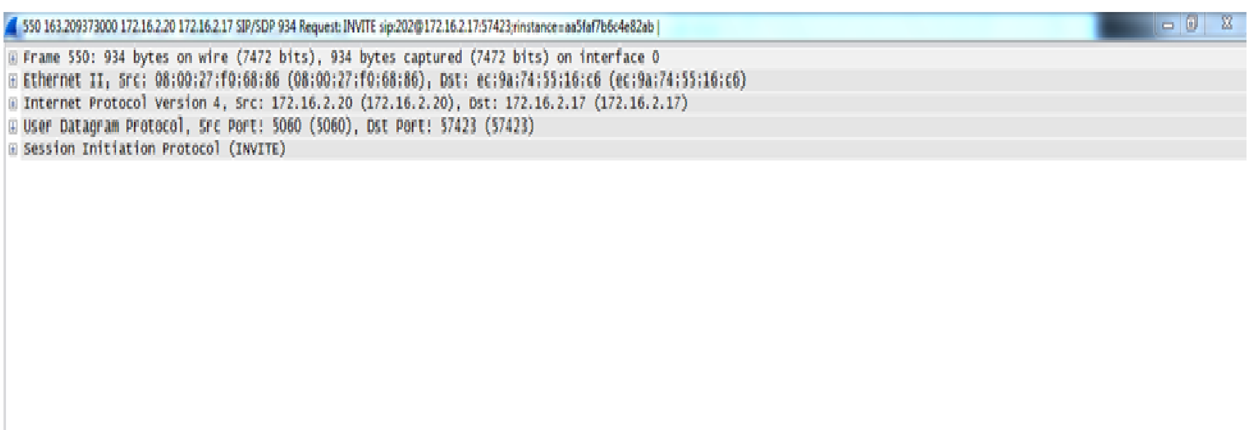


Figure 12: Showing function of each layer of 557no SIP INVITE packet

Lets clicked on the Frame, all information about Frame will be shown as shown in the below console

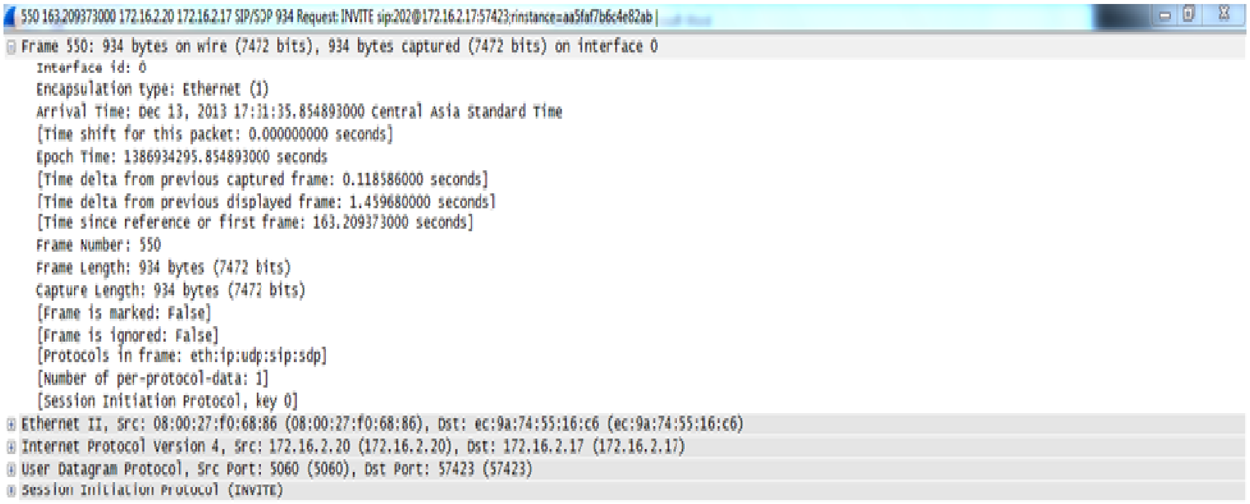


Figure 13: Showing function of Frame

As we show its 550 no Frame and Frame length is 934 bytes (7472 bits), and others information about frame you can see. Now let clicked on the Internet protocol version

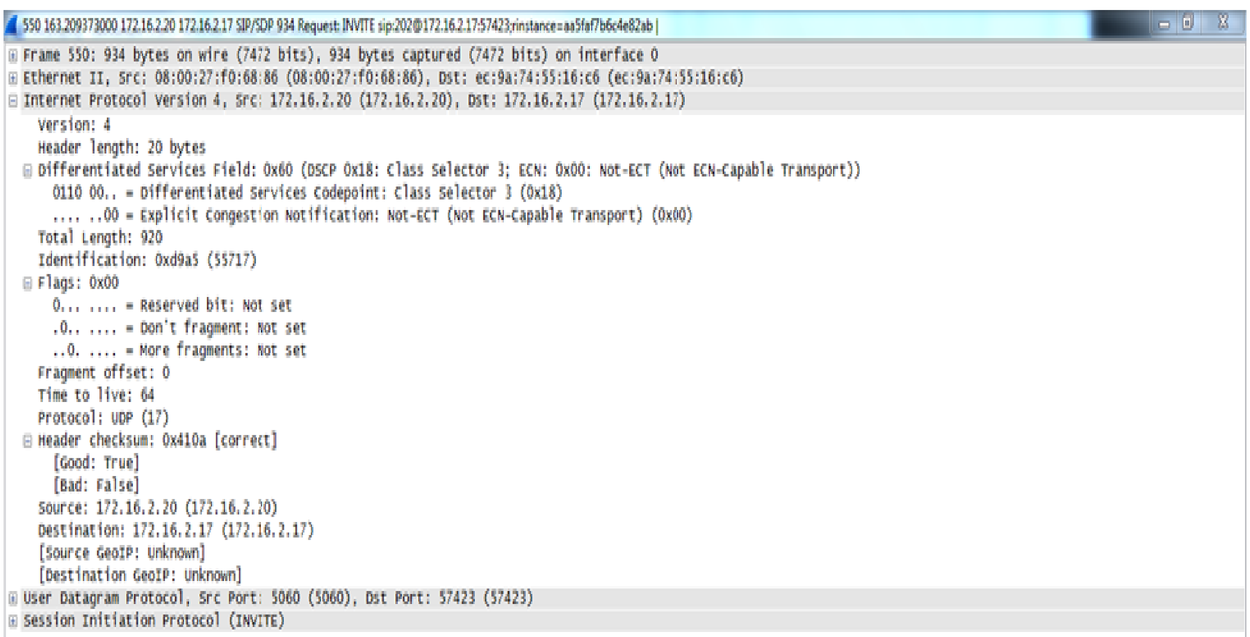


Figure 14: Showing information of Internet protocol version

Destination and Source address information showing in this console. Also Showing Flags information 0x00, time to live 64, protocol UDP (17) and others information. Now let's clicked on the User Datagram Protocol.

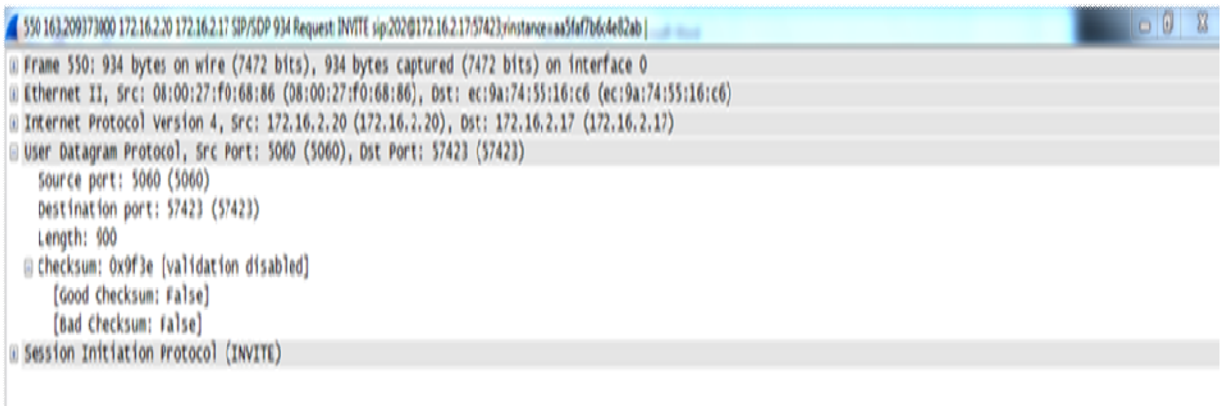


Figure 15: Showing information of User Datagram Protocol

Here, Source port and destination port information is showing, and checksum information is also showing. Let clicked on the Session Initiation Protocol.

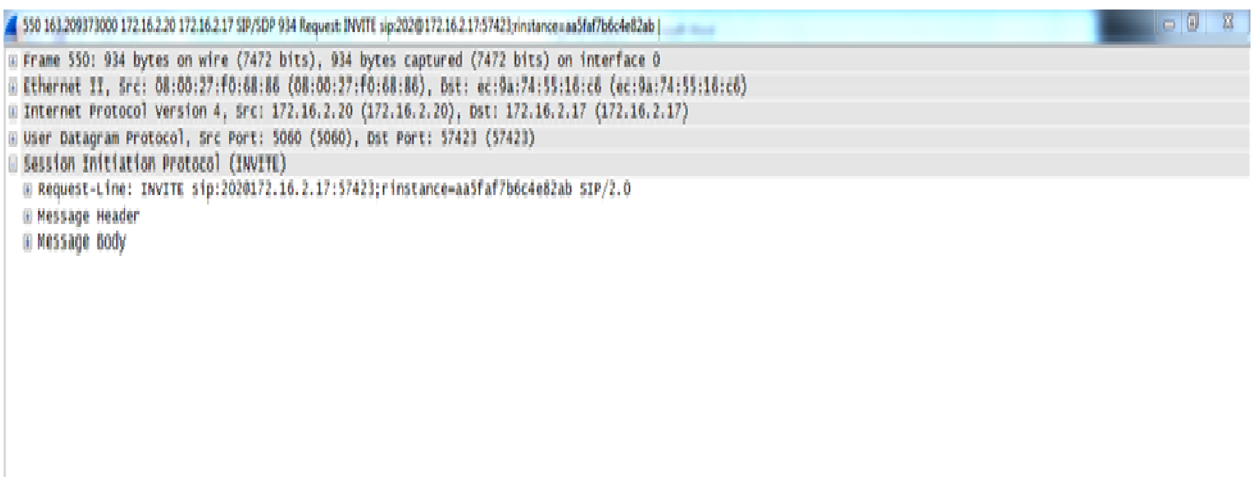


Figure 16: Showing information of Session initiation protocol

After clicking three options appeared, they are

- ✓ Request line information
- ✓ Message Header information
- ✓ Message Body information

Let see Request line information. As extension 201 (server is 172.16.2.20) is called 202, therefore Request –URI user part is showing 202, and server of 202 extension is 172.16.2.17, therefore Request- URI host part is showing 172.16.2.17.

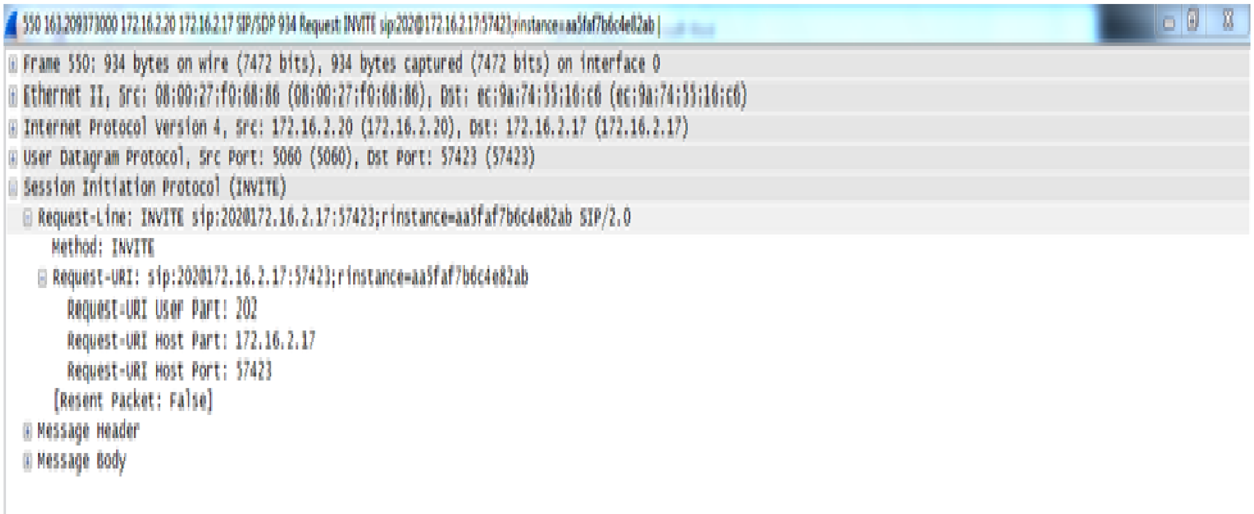


Figure 17: Showing information of Request-Line

Now let's see next option which is Message header.

As before mentioned that the extension 201(172.16.2.20) is calling extension 202(172.16.2.17). See in the above console all information is showing.

- ✓ Transport: UDP
- ✓ Sent by Address: 172.16.2.20
- ✓ Sent by Port: 5060
- ✓ Max forward:70
- ✓ SIP from Address: sip:201@172.16.2.20
- ✓ SIP address user part: 201
- ✓ SIP address Host part: 172.16.2.20
- ✓ SIP from tag:as498f3e20S
- ✓ SIP to Address: sip:202@172.16.2.17
- ✓ SIP adress user part: 202
- ✓ SIP adress Host part: 172.16.2.20
- ✓ SIP to URI parameter: rinstance-aa5faf7b6c4e82ab
- ✓ Date: Fri,13 Dec 2013, 04:55:57 GMT
- ✓ Sequence Number:102
- ✓ Method: INVITE

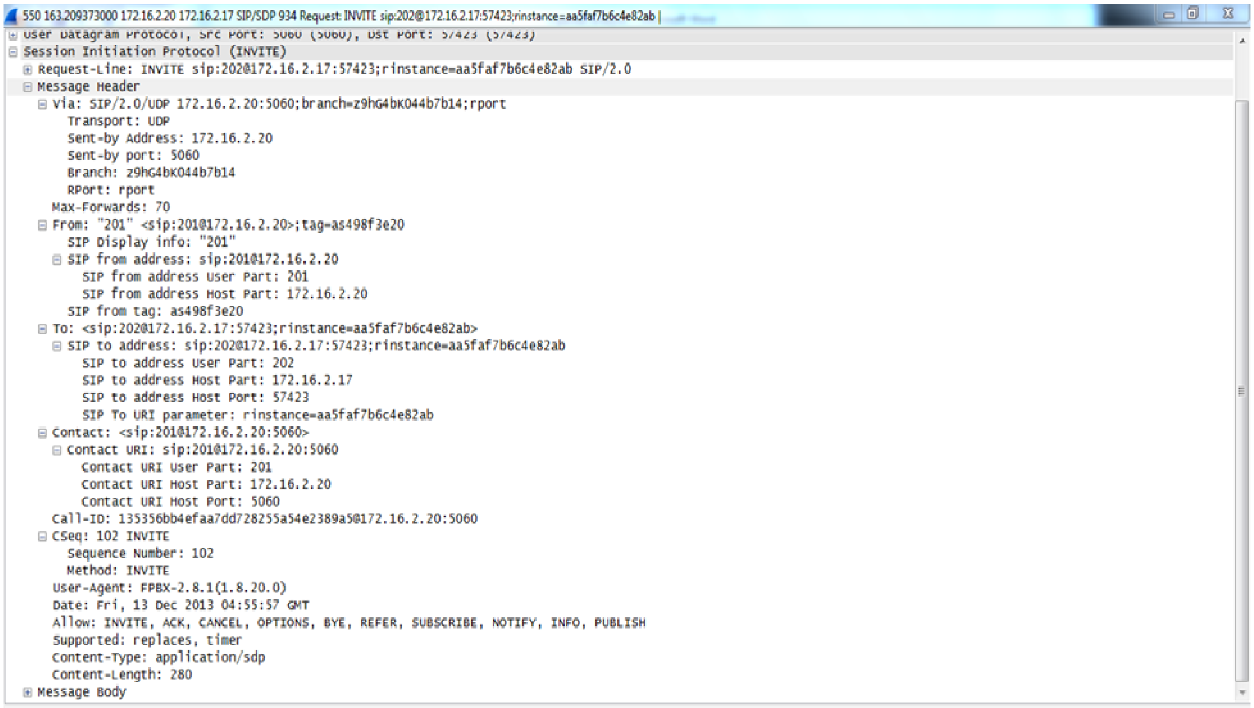


Figure 18: Showing information of message header

In the Message Body Option Session Description protocol Described.

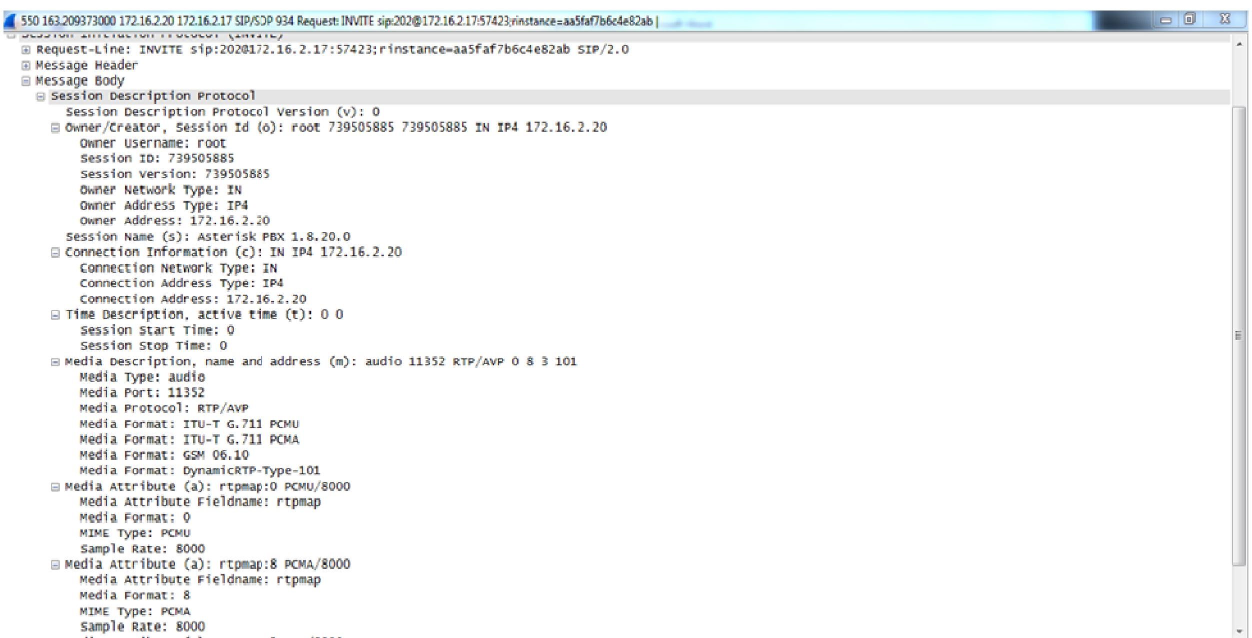


Figure 19: Showing Information of Message Header

In this analysis SIP INVITE packet analysis only just showed, in this way all packet analysis such as ACK,RINGING, BY and so on packet analyze could be done.

4.4 RTP packet Analysis

In same way RTP packet has been captured. RTP packet captured in two ways, at first “Showing all stream” than “stream analysis”

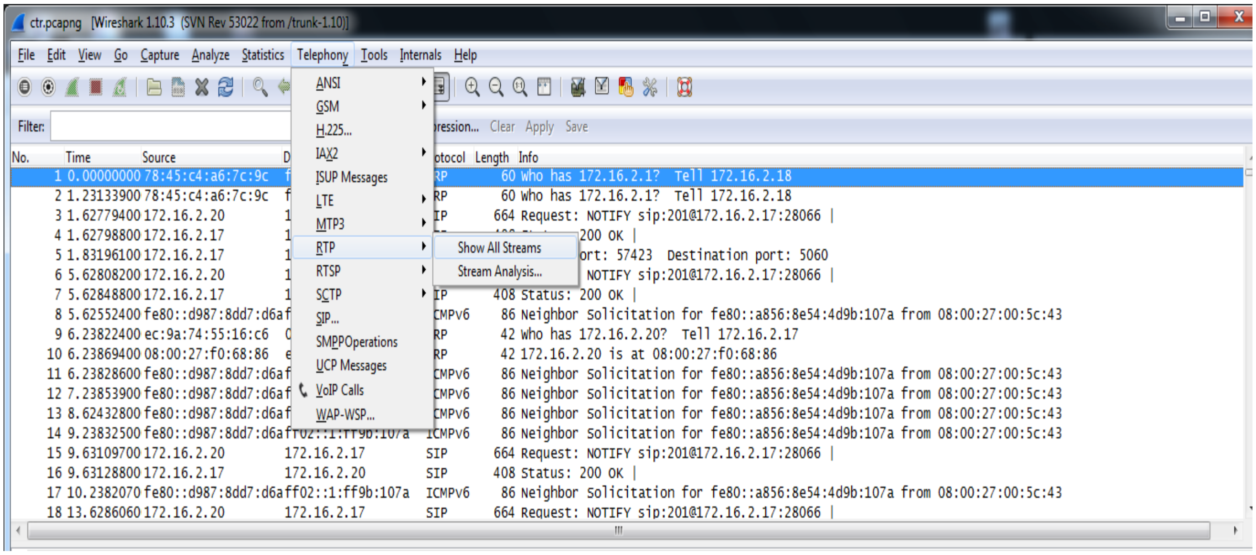


Figure 20: Capturing RTP packets all stream

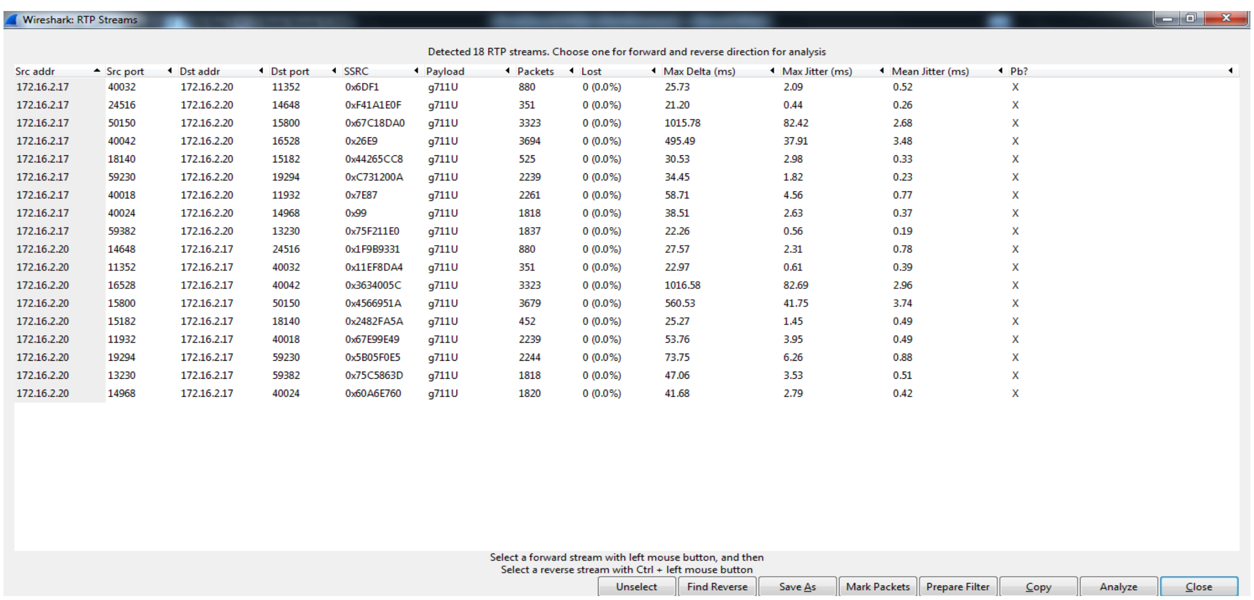


Figure 21: Showing all information about RTP data stream

In above console source address and destination address information is showing. Destination and source port information is also showing. Payload information is also showing. Payload is the part of the transmitted data which is the fundamental purpose of the transmission, to the exclusion of information sent with it (such as headers or metadata, sometimes referred to as overhead data) solely to facilitate delivery [11]. Showing Max Delta, max jitter and mean jitter information. The delta is the time difference between the current packet and the previous packet in the stream. **max delta** is the largest delta value.

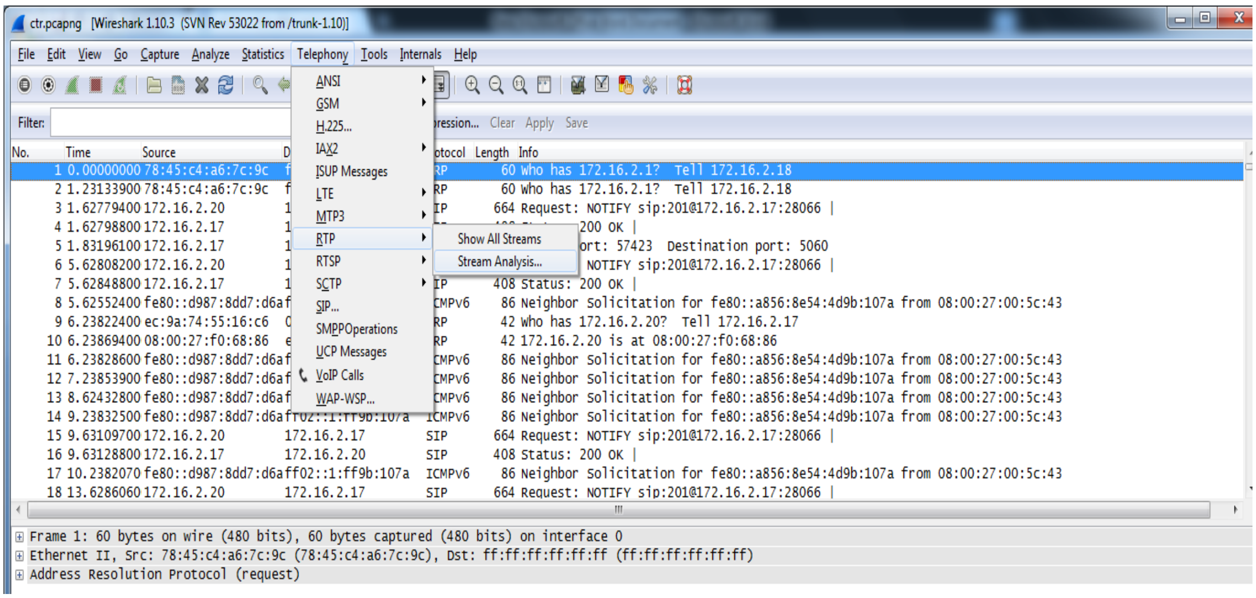


Figure 21:Capturing stream analysis

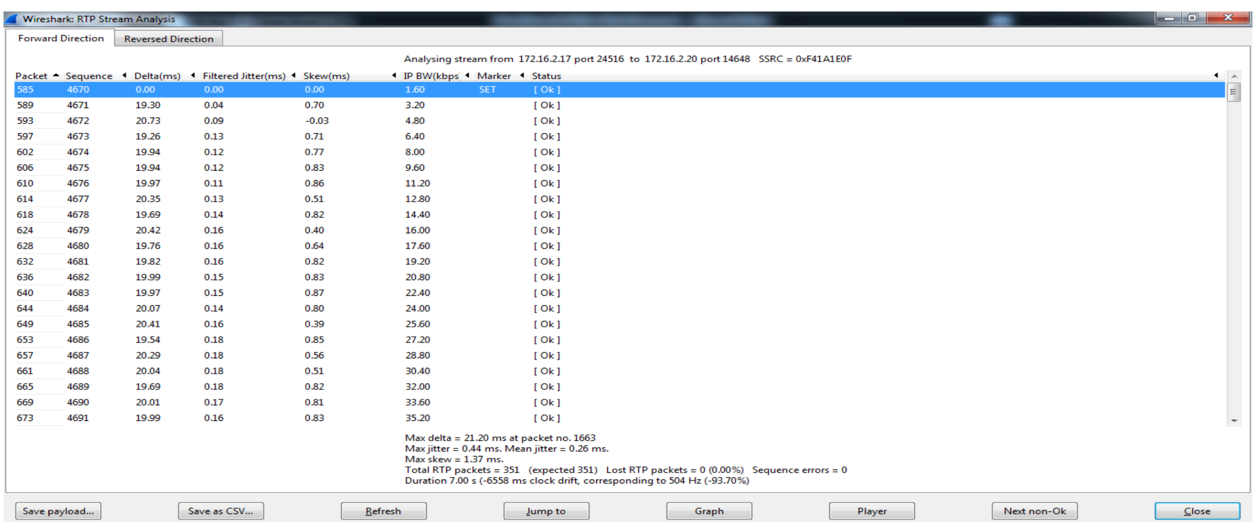
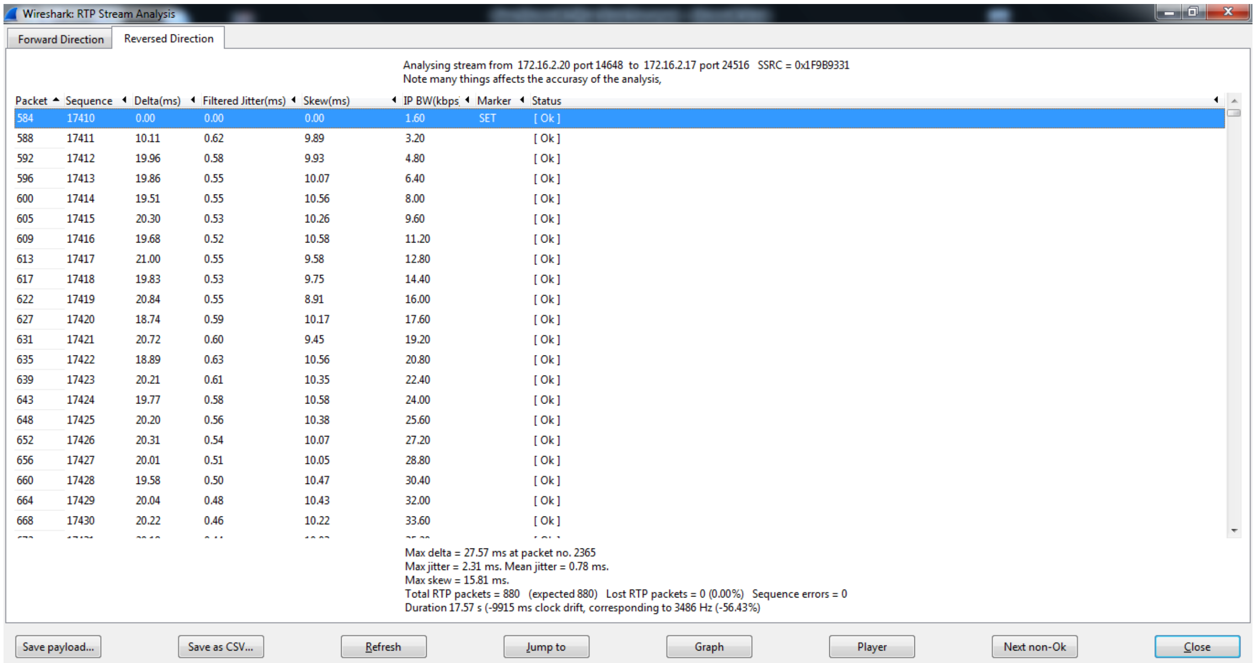


Figure 22: Showing Forward direction packet information



Wireshark: RTP Stream Analysis

Forward Direction | Reversed Direction

Analysing stream from 172.16.2.20 port 14648 to 172.16.2.17 port 24516 SSRC = 0x1F9B9331
Note many things affects the accurasy of the analysis,

Packet	Sequence	Delta(ms)	Filtered Jitter(ms)	Skew(ms)	IP BW(kbps	Marker	Status
584	17410	0.00	0.00	0.00	1.60	SET	[Ok]
588	17411	10.11	0.62	9.89	3.20		[Ok]
592	17412	19.96	0.58	9.93	4.80		[Ok]
596	17413	19.86	0.55	10.07	6.40		[Ok]
600	17414	19.51	0.55	10.56	8.00		[Ok]
605	17415	20.30	0.53	10.26	9.60		[Ok]
609	17416	19.68	0.52	10.58	11.20		[Ok]
613	17417	21.00	0.55	9.58	12.80		[Ok]
617	17418	19.83	0.53	9.75	14.40		[Ok]
622	17419	20.84	0.55	8.91	16.00		[Ok]
627	17420	18.74	0.59	10.17	17.60		[Ok]
631	17421	20.72	0.60	9.45	19.20		[Ok]
635	17422	18.89	0.63	10.56	20.80		[Ok]
639	17423	20.21	0.61	10.35	22.40		[Ok]
643	17424	19.77	0.58	10.58	24.00		[Ok]
648	17425	20.20	0.56	10.38	25.60		[Ok]
652	17426	20.31	0.54	10.07	27.20		[Ok]
656	17427	20.01	0.51	10.05	28.80		[Ok]
660	17428	19.58	0.50	10.47	30.40		[Ok]
664	17429	20.04	0.48	10.43	32.00		[Ok]
668	17430	20.22	0.46	10.22	33.60		[Ok]

Max delta = 27.57 ms at packet no. 2365
Max jitter = 2.31 ms. Mean jitter = 0.78 ms.
Max skew = 15.81 ms.
Total RTP packets = 880 (expected 880) Lost RTP packets = 0 (0.00%) Sequence errors = 0
Duration 17.57 s (-9915 ms clock drift, corresponding to 3486 Hz (-56.43%)

Save payload... | Save as CSV... | Refresh | Jump to | Graph | Player | Next non-Ok | Close

Figure 23: Showing reverse direction packet information

Chapter 5

Security

Now a day's IP telephony become a popular technology which provides many advance feature for communication. Many traditional telephony systems are replaced by IP telephony. Because IP telephony provides multi feature like, Multiple Extensions, Caller ID, Voice mail, IVR capabilities, Recording of conversations, IAX2 , Call-centre open-fire with hardware based telephones or software based. With this new technology comes a new challenge for both the defensive and offensive side of security. To protect the data we need security in the system server .If any unauthorized access in a server unwontedly, can make change everything of the system. A reachable hacker can attack the system server with various ways. So at first have to make secure the system server. In the project three layer securities has been given to the server to ensure the security of the server.

5.1 Deactivate Remote login

If anyone's wants to attack system server than attacker must have to reach to the target network. Most of cases, Attacker try to login to the system server remotely, so at first need to off the login system of the unauthorized remote user. To do this job some rules must be followed. When a user want to log in remotely to the server user use "SSH" technique either authorized or unauthorized. As every process are running in different port. When a user try to login remotely into server he sent a request to specific port number.

5.1.1 Port number changing

So, if change the port number of "SSH" then the probability of unauthorized user remote login will be reduced. For this job need to go to this configuration file of server.

Figure 24: Command for going Configured file

Then to change the port number of "SSH"

Figure 25: Showing port number of ssh

Figure 26: Changing SSH port number

Assume that anyhow attacker find the port number, Then he will accessible.

5.1.2 Finding process of port number

There are many way to find the port number which is assigned for which service. In this project port number have been tried to find by using backtrack run a command which helps to find the open port number. It gives two result depends on system server configuration.

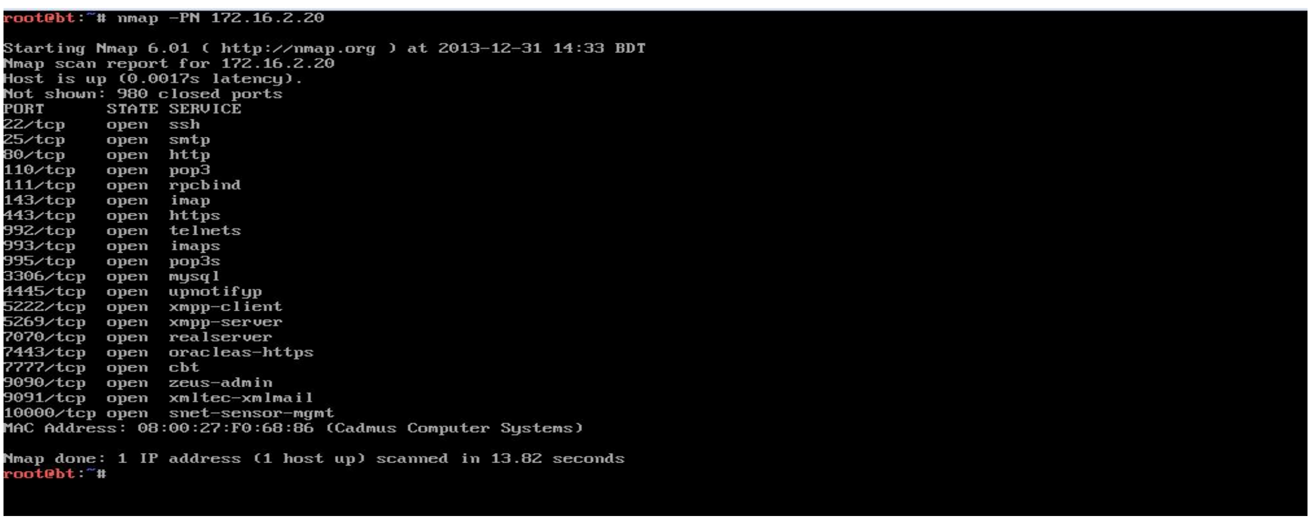


Figure 27: Showing all port number set as by default

Fig 28: After changing port number

5.1.3 Finding password of remote host

If hacker successfully find out the exact port number of "SSH" service, then server will be attacked by hacker with appropriate password of root in this way .That is hacker create a file "password. list" with approximate password and to know the password of remote host, hacker run the file Password. list with this command .

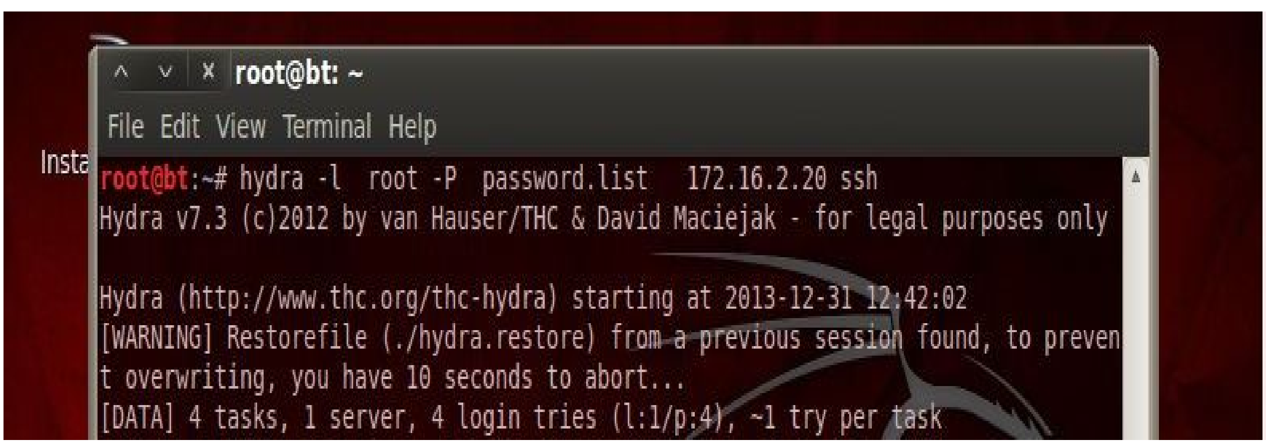


Figure 29: running script

5.1.3 User binding

If anyhow password is found then it's not secured, to make more secure system allow only some authorized user except "ROOT”. For this reason in the system, declare some authorized user only who can be accessible.

```
#LoginGraceTime 2m
#PermitRootLogin yes
PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
-- INSERT --
```

Figure 30: Allowing some authorized user

```
# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
allowuser  hera,safi,hemel
#PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
```

Figure 31: Allowing some authorized user

To apply changes in configuration file run this command

```
[root@elastix10 ~]# service   sshd restart
Stopping sshd:                                             [  OK  ]
Starting sshd:                                             [  OK  ]
[root@elastix10 ~]# _
```

Figure 32: Service SSHD restarting

5.2 User binding with IP

If any how attacker find the authorized user name, then it's easy for him to access the server. Now restrict the user by IP. Need to declare some authorized IP in "hosts.allow" file. That's why go to the configuration file of host.allow

Figure 33: Command for entering host.allow file

Then add the service name along with IP. Only who can get the permission

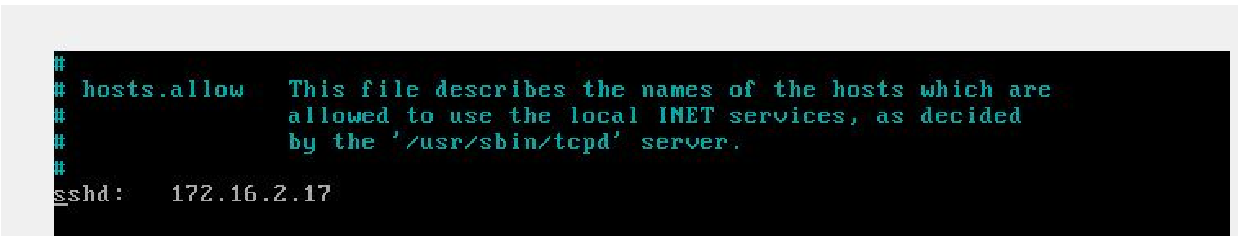


Figure 34: Binding IP address

Then need to go to the hosts to declare that all IP are access denied except only one are declared to access. You may declare two or three accessible IP as you want.

Figure 35: Allowing Host

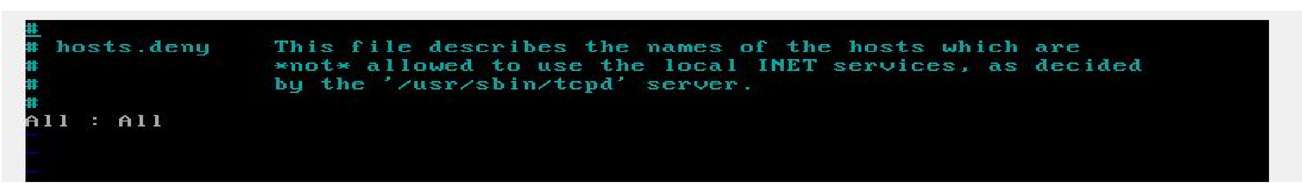


Figure 36: Deny all unauthorized user

If above security apply in any system server then it will be tougher to break the security.

Chapter 6
Conclusion

In this project, advanced feature of IP telephony system has been extracted. Considering cost free call, two asterisk servers created and IAX trunk configured so that extension of one server can called extension of another server as intercom. For Instant massaging or group chat in spark which combined with Openfire has been configured. For interaction between agent and telephone subscriber, Elastix call centre module is installed and configured. Packet passing over the network has been analyzed by Wireshark for understanding function of each layer. To ensure the security of the system, server has become secured in three labels.

Reference

[1] Inter Asterisk Exchange, Wikipedia [online]. Available: http://en.wikipedia.org/wiki/Iax

[2] Openfire, Wikipedia [online]. Available: http://en.wikipedia.org/wiki/Openfire

[3] XMPP, Wikipedia [online]. Available: http://en.wikipedia.org/wiki/Xmpp

[4] ignite Realtime [online]. Available: http://www.igniterealtime.org/projects/spark/

[5] Josephine Larsson &Ida Waller,” IP telephony – Future Investment or risk assessment?”, Master Thesis, Computer Science, Thesis no: MSC-2004-1,1June 2004

[6] Ben Sharif, Elastix- without tears, January 15, 2009

[7] http://web.uct.ac.za/depts/commnetwork/eee5026/note/eee5026-06-620mgcp.pdf

[8] http://www.ixiacom.com/pdfs/library/technology_guides/skinny.pdf

[9] http://www.radvision.com/nr/rdonlyres/51855e82-bd7c-4d9d aa8ae822e3f4a81f/0/radvisionsipprotocoloverview.pdf

[10] http://www.investrussia.org/elastix/elastix-callcenter.pdf

[11] Payload(computing), Wikipedia [online]. Available: http://en.wikipedia.org/wiki/Payload_(computing)

[12] Mayank Sharma, Openfire Administration, Chapter No. 6 "Effectively Managing Users"

[13] http://www.igniterealtime.org/builds/spark/docs/spark_user_guide.pdf

[14] http://www.igniterealtime.org/about/OpenfireScalability.pdf

[15] http://docweb.cns.ufl.edu/docs/d0211/d0211.pdf

[16] Install Openfire Server, PIAF Development Team, December, 2011

[17] http://www.igniterealtime.org/about/jive_xmpp_wp.pdf

[18] ftp://167.205.50.45/pub/download/ebooks/oreilly.xmpp.the.definitive.guide.may.2009.pdf

[19] http://web.sarathlakshman.com/Articles/XMPP.pdf