VoIP Based College Campus Communication Model

Dr. Darshankumar C. Dalwadi[1], Ronit Rout[2]
[1,2]Birla Vishvakarma Mahavidyalaya Engineering College
Vallabh Vidyanagar
Anand, Gujarat
darshan.dalwadi@bvmengineering.ac.in
routronit89@gmail.com

***Abstract*—**Voice over Internet Protocol (VoIP) technology is the future of Voice Communication. Through VoIP, one can enjoy seamless audio and video calls of high quality. Along with providing video calls, it can be used to provide other functionalities such as transferring the calls, routing the calls through different trunks, enabling Call Taping and many other functions by just a click of a button. VoIP provides an efficient method of connecting International as well as National Calls at much lower prices. VoIP is secure as it follows Session Initiation Protocol which can be used with any underlying transport layer protocol like TCP, UDP or SCTP. SIP can be further be encrypted with Transport Layer Security (TLS) when being when messages are sent over an insecure network. For the transmission of voice and video, SIP uses Real Time Protocol (RTP) and Secure Real Time Protocol (SRTP). This connectivity model deals with various aspects of VoIP Communication which involves designing the logical network topology, Session Initiation Protocol (SIP), VoIP Security issues and troubleshooting various problems using Wireshark.

***Keywords*—** *VoIP, SIP, Wireshark, Peer to Peer Connectivity, Security*

I. INTRODUCTION

With enhancement in communication technologies, the world is moving towards high speed Packet Switched voice communication model. The Voice over Internet Protocol (VoIP) is one of the recent trends and is putting its foot in GSM communication model as well. VoIP provides seamless voice communication functionality and providing tremendous supplementary services such as Instant Messaging, Presence Status Display, and connectivity across the globe. This VoIP based College Connectivity Model is based on these services provided by VoIP, which in turn will increase collaboration and reliability of the existing communication system. Institutions like our own are relying on conventional communication technologies such as Public Switched Telephone Networks (PSTN) and GSM for fulfilling its communication needs. These techniques are limiting the collaborative behavior of communication. Hence, multiple application and interfaces are required to address the communication requirements [1].

It is sometimes required that a certain group of faculties are assigned some particular task. The task is different from those tasks assigned to other groups. So, the concerned faculties assigned the same task are required to be in a group connectivity so that they can actively exchange information and that too securely. The information they exchange is only meant for that particular group and need not be shared with other groups. This system helps in connecting the different members through VoIP.

Different groups can be made through this model on the basis of IP addresses and just by changing some settings, we will be able to send messages to other groups (broadcasting) and to other departments as well. If a particular faculty is moving to some other group, then just changing the previous IP address in the previous network to the new IP address in the new network and the work is done. So, this system offers flexibility, scalability and security at the same time.

At this point of time, one may ask "What's wrong with WhatsApp? WhatsApp offers all these features." The reason is, WhatsApp becomes too personal which is not required in a college environment. Some amount of transparency is required in this environment. Some messages need to be private and some messages need to be broadcasted to all departments or concerned authorities of different departments. In WhatsApp, we need to first save the phone number and then we can send messages to that person. If the person changes the phone number, the new phone number should be saved and only then we can send messages [2].

WhatsApp requires all kind of details including the mobile number. It may be possible that sometimes, someone would like to keep the mobile number confidential due to some reason. And WhatsApp necessarily requires the mobile number. As an example, the Principal need not share his/her mobile number with the students. When he/she wants to do some announcement without his mobile number, they how can this be accomplished? For such problems VoIP becomes handy. It allows us to send messages or any other media and does not require our personal details [3].

It is highly secure and therefore there is little transparency. Groups need to be formed and the members are added on through their phone numbers. Whereas in this system, grouping is done on the basis of IP addresses [4]. Different departments are allotted a set of different IP addresses that can be used. Every node in that network is allocated a unique IP

address that can be used to get connected to a network and exchange information. The administrator can facilitate the allocation, grouping and the later movement of IP addresses from one work group to another.

Basically, this system connects different nodes in different networks which can then be used to exchange information either privately to different members or can even be broadcasted to all the groups across all the networks by suitably changing the network ID and the host ID.

II. IMPLEMENTATION OF VoIP

A. *Network Architecture*

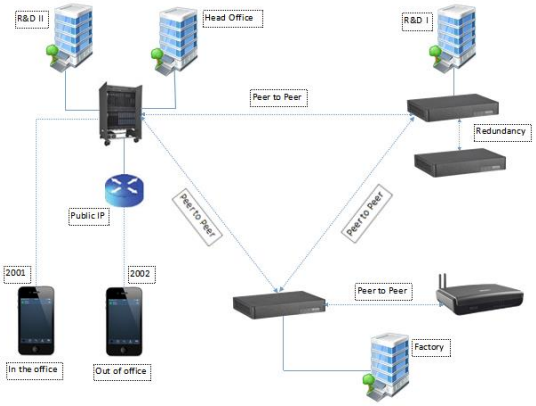

Fig. 1 The overall network topology of the system

Fig. 1 shows two buildings R&D II and Head Office are connected to a single large PBX (Private Branch Exchange). R&D I is connected to another small PBX. Factory is connected to the third PBX. All the three PBXs are connected to each other using peer to peer connectivity. Each PBX has many different phones connected to it for calling purposes.

If we are connected to LAN, then the PBX supports internal calling (in office). For external calling, the entire system should be connected to WAN through a public IP.

B. *Block Diagram of the Network*

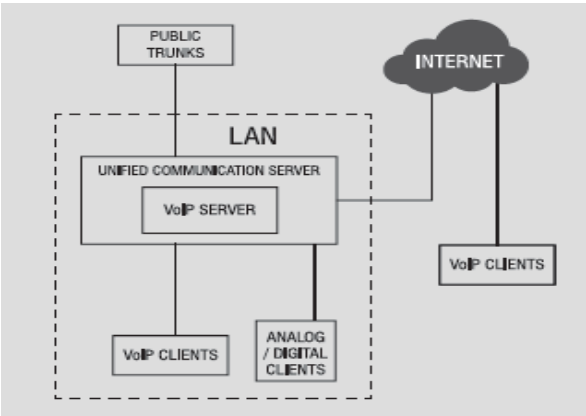

Fig. 2 Block diagram showing connectivity of Server and Client

In Fig. 2, VoIP Server is a part of the Unified Communication Server which serves Communication, Messaging, Mobility and other features thereby increasing productivity. The Unified Communication Server is connected to the Internet [5].

VoIP Clients are connected directly to the Unified Communication Server as well as to the Internet through which they can get registered on the Server. Both Analog and Digital Clients are supported by the Unified Server and are directly connected to it. The entire Server is connected to Public Trunks through which external calling is accomplished. The Unified Communication Server, VoIP Clients and Analog / Digital Trunks are connected on Local Area Network (LAN).

C. *Hardware / Software Analysis*

UNIFIED COMMUNICATION SERVER

Flexible device usage and round-the-clock connectivity is the need of the hour for the workforce in order to have consistent in-office experience while working from home, between appointments or while on the move. Unified Communication Server serves four important elements that are Collaboration, Communication, Messaging and Mobility. Other features include video and voice calling, conferences, Email Integration, Presence Status and various other features. It is designed to overcome geographical, communication device and user-accessibility barriers with a single platform.

VoIP SERVER

The VoIP Server or IP-PBX is the part of the VoIP phone system which is used for data processing and also for answering incoming request. A VoIP server can either be a software or a hardware. In its software form it is easy to operate and saves the maintenance cost. A server has a huge capacity in terms of memory and disk storage. This enormous capacity of the server enables it to work fast. It performs well even when multiple clients try to connect to the server simultaneously.

To increase its utility further one can add different features like video conferencing, IVR (Interactive Voice Response). With a VoIP Server connection one can configure extensions, set call forwarding and other low cost VoIP Services which all are included in this model.

Most important functions of VoIP Servers are:

ROUTING:

A VoIP Server manages the call routing. It searches for two endpoints and finds the best path to pass the pieces of information from one end to the other. Different algorithms help to determine the shortest, secure and the fastest path.

MULTIPLE PROTOCOLS:

In VoIP, the communication is established through various types of protocols. Different modules that support different protocols may be added.

CLIENT MANAGEMENT AND OTHER FUNCTIONS:
It manages various clients that use the VoIP service. It supports other features like Caller ID, Caller ID Blocking, Call Forwarding, Call Return, Call Waiting, Call Rejection etc.
VoIP CLIENT:
A VoIP client may simply be a smart phone, soft phone or any other device with Internet connectivity, dialing pad, User ID and other features. It supports network statistics, voice security, video conferencing and other features.

III. SESSION INITIATION PROTOCOL (SIP)

The Session Initiation Protocol (SIP) is a signalling protocol which works at the Application Layer. Used to create, modify, and terminate a multimedia session over the Internet Protocol. A session is nothing but a simple call between two endpoints. An endpoint can be a smart phone, a laptop, or any device that has the capacity to send and receive multimedia over the Internet. It is defined by IETF (Internet Engineering Task Force) standard. It is defined in RFC 3261. SIP takes the help of SDP (Session Description Protocol) which describes a session and RTP (Real Time Transport Protocol) used for delivering voice and video over IP network [6]. SIP can be used for two-party (unicast) or multiparty (multicast) sessions.

A. SIP Architecture

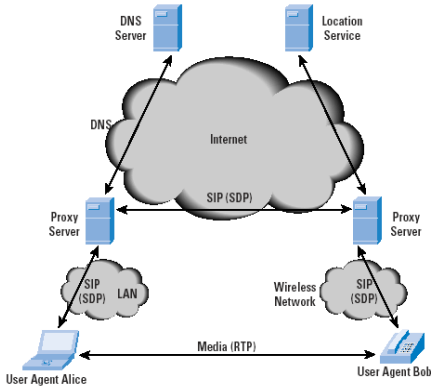

Fig. 3 Session Initiation and connection between client and server

From Fig. 3, the client (Alice) uses SIP to set up a session with the server (Bob). The Session Initiation uses SIP and may also employ proxy servers to forward requests and responses. The media between the two is sent using RTP (Real Time Protocol). The client is connected to proxy server using SIP over LAN. The Session Description Protocol (SDP) is used for describing multimedia communication sessions for the purpose of session announcement, session invitation and parameter negotiation. The server is also connected to a proxy server using SIP over wireless network [7]. SIP often uses User Datagram Protocol (UDP) for performance reasons and has its own security mechanisms, but may also use TCP. SIP messages often use Transport Layer Security (TLS) for travelling.

IV. SOLUTION PROVIDED

VoIP based College Connectivity Model is comprising of an inhouse VoIP Communication Server which hosts the VoIP based clients which can be installed either as a desk phone or as soft clients on Smart phones or PCs. These Clients can provide the unified communication in which the various communication techniques such as calls, video calls, conferences, SMSs, IMs, Presence Sharing, Voice mail from a single portal, call transfer, call forward for different time zones, prescheduled conference. The cost involved in calling between two parties/ branches is minimal and communication is reliable.

V. SALIENT FEATURES

The communication is **unified** and is single portal operated for voice calls, video calls, Instant Messaging, SMSs, Voice Mail etc. The communication remains intact **across the globe**. The system is equipped with various **call handling features** and functionality such as call transfer, call forward, hold, message broadcast etc. which are not available in various IM applications available in the world currently. The model saves the **calling cost** as it works on Wi-Fi in the internal network and moves to mobile data once the caller moves out of the office. The call parameters such as **Voice Codecs** can be configured and managed by admin unlike other IM Platforms. There are various **security protocols** compatible with the Unified Communication Server. **Call Transfer** functionality so that any call can be transferred at any given point of time. **Call Forward** – When dialled no. **is busy** or **when no reply** or **unconditional call forward** so that all calls can be forwarded to a particular number or a group of numbers if the dialled number is busy or is not replying. **Call Parking** feature to park calls (hold calls) in different orbits and give priority to other important calls and once they are over, continue with the previous calls. **Call Pickup** feature which enables to pick the call through another mobile if the first mobile is damaged or the buttons are not working or in case of no response (in a hung state). **Call Forward** according to three different time zones: **Working hours, Break hours** and **Non-working hours**. Each time zone can have different call forward features set. **Room Monitoring** feature that enables someone to listen to all conversations going in a room. **Barge- in** feature to break into ongoing conversation by having the timer set and assigning higher priority to some phones the two phones will be connected and the phone which was earlier in speech with the first extension will be put on hold. **Call Supervision** feature to check the last external number that has been dialled

by another phone. **DND (Do Not Disturb)** functionality to F deny access to all phones during certain period of time. **Dial-in Conference** to schedule conference by entering Conference ID and Conference Password. Other Conference users can join in the conference by entering the ID and password. **Prescence Status** to show the current status of any user like Present, Away, in a meeting, out of office, absent. **Soft Keys** functionality to monitor the status of another phone and calling them by a double click or sending messages to a particular group. **Auto Call Back** feature to automatically setup the call between two phones once they are free without repeated checking and redialling. **Voice Mail** feature to send, listen, record, delete voice mail messages to multiple people.
BLF (Busy Lamp Field) functionality to check whether a phone is busy, or on hold or DND mode from some other phone. **Sending messages** and **video call** functionality to facilitate mobility. **Raid** feature to interfere between a call and make it into a three party speech (3 party conference). **Multi-party video conferencing** supported of high quality. **Auto Redial** feature to redial a number if the number is busy. We need not dial the number every single time and therefore it saves a lot of time.

VI. WIRESHARK

Wireshark is a free application used to capture and view the data packets traveling from and to on the network. It provides the ability to drill down and read the contents of each packet and is filtered to meet specific needs. It is commonly used to troubleshoot network problems and to develop and test software. This open-source protocol analyzer is widely accepted as the industry standard. This free software lets us analyze network traffic in real time, and is often the best tool for troubleshooting issues on the network.

VII. NETWORK ANALYSIS USING WIRESHARK

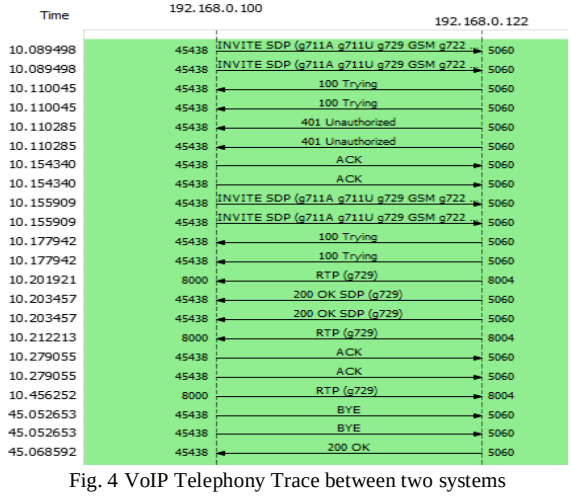

Fig. 4 VoIP Telephony Trace between two systems

Fig. 4 shows packet trace of VoIP telephony from IP 192.168.0.100 (System A) to 192.168.0.122(System B) which are connected using Peer to Peer Connectivity. First System A sends INVITE SDP with Codecs to System B. System B tries connecting back to System A but there is an authorization error. System A acknowledges (ACK) it and again sends INVITE SDP request with the preferred codecs. System B again tries to connect to System A. This time System B is able to connect to System A and Real Time Protocol (RTP) is initiated which is used for the delivery of voice and video. System B confirms SDP request of System A (OK) and then again initiates RTP packets. System A acknowledges it and after the speech is over sends a termination request (BYE). System B confirms the termination request (OK).

VIII. SECURITY ISSUES IN VoIP

The majority of VoIP traffic is sent over the Internet and if it is not encrypted, anyone with access to the network can listen in to telephone calls and this is one of the most serious threats in the VoIP environment. Interception of audio calls and signaling messages which can be decoded can allow the person intercepting the phone call to listen in to phone calls.

Hackers are able to impersonate a user, assume the identity of a caller and obtain sensitive and confidential business or client information. A middle man could intercept a VoIP call so that person ends up speaking with the impersonator rather than an actual business. This leaves personal information, credit card details open to theft from the interceptor. A more technical attack would involve sending a large volume of inauthentic packets to a VoIP server which will cause an overload and takes the service offline for genuine people. Once a hacker has gained access to a VoIP system, they can do anything on the network, from making and receiving calls through to transferring calls before they ring and recording and taping calls. Standards for securing VoIP are available in the Secure Real-time Transport Protocol (SRTP) and for analog telephony adapters, as well as for some soft phones. IPsec is available to secure point-to-point VoIP at the transport level by using opportunistic encryption. Government and military organizations use various security measures to protect VoIP traffic, such as voice over secure IP (VoSIP), secure voice over IP (SVoIP), and secure voice over secure IP (SVoSIP). The distinction lies in whether encryption is applied in the telephone endpoint or in the network. This connectivity model uses SIP V2.0 which is highly secure as compared to its predecessor. Moreover, the system supports SIP over SSL and SIP over TLS both for the purpose of encrypting the data and to keep the data secure. It should be complemented with a high quality Firewall to avoid any unauthorized access.

A. Abbreviations and Acronyms

VoIP : Voice over Internet Protocol.
TCP : Transmission Control Protocol.
UDP : User Datagram Protocol.
SIP : Session Initiation Protocol.

SSL : Secure Socket Layer.
TLS : Transport Layer Security.
RTP : Real Time Protocol.
SRTP : Secure Real Time Protocol.
LAN : Local Area Network.
SDP : Session Description Protocol.

ACKNOWLEDGMENT

In the accomplishment of this project successfully, many people have best owned upon me their blessings and the heart pledged support, this time I am utilizing to thank all the people concerned with this project.

Primarily, I would thank the almighty for being able to complete this project with success. Then I would like to thank my Principal Dr. Indrajit N. Patel for giving me an opportunity to work in a leading organization and learn some of the most important things theoretically as well as practically before moving forward with this project. Next I would like to thank my guide : Dr. Darshankumar C. Dalwadi, my project guide whose valuable guidance have been the ones that helped me patch this project and make it a success. Their suggestions and instructions have served as the major contributor towards the completion of the project.

Then I would like to thank my parents and seniors who have helped me with their valuable suggestions and their guidance has been very helpful in various phases of the completion of the project.

REFERENCES

[1] S. Young, D. Kershaw, J. Odell, D. Ollason, V. Valtchev, and P. Woodland, ‘’The HTK book’’, version 3.1, pp. 1-277, 2006.

[2] X. Menéndez-Pidal, J B. Polikoff, S M. Peters, J E. Leonzio, H T. Bunnell, ‘’The Nemours Database of Dysarthric Speech’’, J. IEEE, in press.

[3] M. Nebra, ‘’ Apprenez à créer votre site web avec HTML5 et CSS3- Learn how to create your website with HTML5 and CSS3’’, pp. 1-248, June 2013.

[4] Pitts J. M., Wang X., Yang Q., Schormans J.A.,“Excess- Rate queuing theory for M/M/1/RED with application to VoIP QoS”, IEEE Electron. Lett., 2006, 42, (20), pp. 1188– 1189.

[5] Pitts J. M.,Schormans J. A., “Configuring IP QoS mechanisms for graceful degradation of real-time services”, IEE MILCOM, Washington, DC, October 2006.

[6] Yang Q., Pitts J. M., “Guaranteeing enterprise VoIP QoS with novel approach to DiffServ AF configuration’. IEEE Int. Communication Conf. (ICC’07), Glasgow, UK, 24–28, June 2007.

[7] YANG Q., “Scalable quality of service in converged IP Networks: PhD thesis, Queen Mary, University of London, July 2007.