SOFTWARE PABX PILOT DEPLOYMENT IN CAMPUS NETWORK OF THE OPEN UNIVERSITY OF SRI LANKA

M. Punchimudiyanse[1*] J. P. P. Tharanga[1] and E. M. S. S. Edirisinghe[2]

[1] Department of Mathematics and Computer Science, The Open University of Sri Lanka
[2] Information Technology Division, The Open University of Sri Lanka

INTRODUCTION

A private automatic branch exchange (PABX) is an automatic telephone switching system within an institution used in their communication needs. Electronic PABX systems incur huge costs for upgrading and maintenance based on the number of telephone extensions. Generally, telephone service providers assist an institution in connecting its branch offices. Advancement of technology has paved way to have digital connectivity to the PABX systems from telephone service providers via E1/T1 links where multiple telephone connections provided through a single wired or wireless connection.

Corporate institutions are moving towards software based PABX systems that use session initiation protocol (SIP) and their voice calls are routed over computer networks connected to the Internet. This is termed as voice over Internet protocol (VoIP) technology. We present a pilot project that is carried out to deploy a SIP based PABX over the campus wide computer network of the Open University of Sri Lanka (OUSL). The OUSL has the largest distributed computer network belongs to a government university in Sri Lanka, which interconnects its six regional centers situated in different provinces of the country via VPN. The primary solution is to provide a software phone (soft phone) to a user PC and the secondary solution is to have intercom calls routed to Smart phones of employees via OUSL WIFI network. This PABX system is capable of reducing call costs by routing the intercom voice communications through a VPN and connecting IP phones for places that require physical phones.

TECHNICAL BACKGROUND

Session initiation protocol (SIP) is an application layer signaling protocol, which is capable of creating, maintaining, tearing down of sessions with multiple users. The first version of this SIP protocol is developed by Mark Handley, Henning Schulzrinne, Eve Schooler and Jonathan Rosenberg in 1996 (RFC2543). Then the SIP version 2 (RFC3261) is the current version published in 2002. The SIP protocol uses text-based messages in communications in performing five functions, namely, user location and registration, user availability, user capabilities, session setup and session management.

SIP can run over internet protocol (IP) version 4 and 6 and uses either user datagram protocol (UDP) or transmission control protocol (TCP). Most implementations use UDP and IP version 4 as UDP reduces the overheads in maintaining connections. Actual voice communication happens in peer-to-peer mode most of the time unless there is network address translation (NAT) between two clients.

A SIP client uses session traversal utilities (STUN) protocol to discover the public IP address if it is behind NAT. A STUN server helps the client behind NAT to set up calls through peer-to-peer IP connectivity using their respective public IP addresses. In corporate networks with firewalls controlling the in/out traffic, there can be restrictions to using STUN in making the call establishment difficult. The answer to that problem is using traversal using a TURN server (relays around NAT) server residing in the public side (Internet side) of the network, which provides media relaying service to clients when both SIP clients are using NAT.

ICE (Interactive Connectivity Establishment) protocol negotiates the mechanism of setting up

[*] *Corresponding author: Email -* ***malinda@ou.ac.lk***

a call between two parties using STUN and TURN. It enables successful traversal through NAT in UDP based multimedia sessions established with protocols like SIP, which has offered/answered model of communications. The real-time transport protocol (RTP) transports actual voice data between two clients after SIP protocol setting up the connection. A standard voice codec, such as a-law, u-law, GSM, Speex, g722, g723, g726 and g729 encodes the voice data of a SIP call. The Secure RTP protocol encrypts a voice call to prevent eavesdropping. The initial key negotiation for SRTP is through plain text, which is insecure. Hence, the line is secured using TLS (transmission layer security) or ZRTP (composed of Z and Real-time Transport Protocol), which is a cryptographic key-agreement protocol that negotiates the keys for encryption between two endpoints in a VoIP call. In order to use the voice encryption, all clients participating in a voice call should have the encryption support in their soft phones.

METHODOLOGY

We found that the Asterisk is the most popular free PABX engine that utilizes the SIP protocol. It also has a native protocol named inter-asterisk exchange (IAX) in addition to the SIP protocol. Software based commercial PABX system named 3CX is having a free version, which only supports two simultaneous voice calls. The FreePBX and Elastix are popular free web based frontends to the Asterisk based PABX systems. Both Freepbx and Elastix provide additional features, appliances, hardware components and set of IP phones for a fee. In this pilot project, we have installed both Freepbx and Elastix in two different virtual machines and compared the free features by connecting software phones and smart phones. We opted for the Elastix front-end because it gives more features free such as call center, operator panel and endpoint management interface.

We have carried out an e-mail based survey to find OUSL employee feedback on available resources, their interest in having an intercom and to get their participation in the pilot project. In the pilot setup, we have deployed Elastix PABX on a virtual machine with the intention of moving it to a physical machine to connect SIP trunks in the future. We have focused on giving a particular user the ability to publish their presence of information in the Elastix so that if a user is not interested in receiving calls at a particular time, (eg. Meeting, not at a desk, busy with important task) he/she can mark the presence status as busy. Then the PABX forwards incoming calls to his/her voice mail. We have set up two extension numbers per user, one extension is intended for soft phone application installed on user’s PC and the other extension is for user’s Smartphone. We have enabled the hunting, call waiting and call conferencing features for those two extensions. In the hunting feature, if the user is not answering the desk extension, call will be automatically forwarded to Smartphone extension, if the smart phone is not answered or marked as “Do not Disturb” then the call is forwarded to voice mail. We have configured TCP for calls over VPN and the rest utilizes UDP within OUSL central campus.

Software Phone Selection for PC and SmartPhones

In this research, the project team has tested several free software phones for the compatibility in different Operating systems; ease of installation by the end-user themselves, Simplicity and features available such as encryption and call conferencing facility. Out of those applications, we chose the soft phone X-Lite for a typical Windows and Mac user who needs maximum of 3 way call conferencing but X-lite lacks the call forwarding feature. The Yate-client is selected for the power users who need to have more than three way call conferencing and call forwarding (attended) features and the installation on Windows, Linux and Mac OS distributions. The Yate client lacks call split feature when we want to break a conference call to individual calls but X-lite has it. The Ekiga soft phone also can be used for Linux clients.

The Zoiper soft phone supports windows, Linux and Mobile platforms android, IOS and Windows mobile. However, Zoiper does not allow call transfer, call conference features on its free version. We used it as a compatible client for IOS, Android and Windows phone. For the phones with Android 4+ operating systems, we chose GS-wave as soft phone that has call encryption, 6 way conferencing and call transfer features. The Csipsimple soft phone is used as the android soft phone for a wider compatibility in the phones with older android versions.

RESULTS AND DISCUSSION

Our e-mail survey has received 82 responses indicating over 90% of the participants like to have their own intercom number. Over 80% of participants have an official PC connected to OUSL wired network, which is not shared with other users. Only 6% said "No" to receive intercom calls to their PCs while 48% said "YES" and 46% would like to try that out.

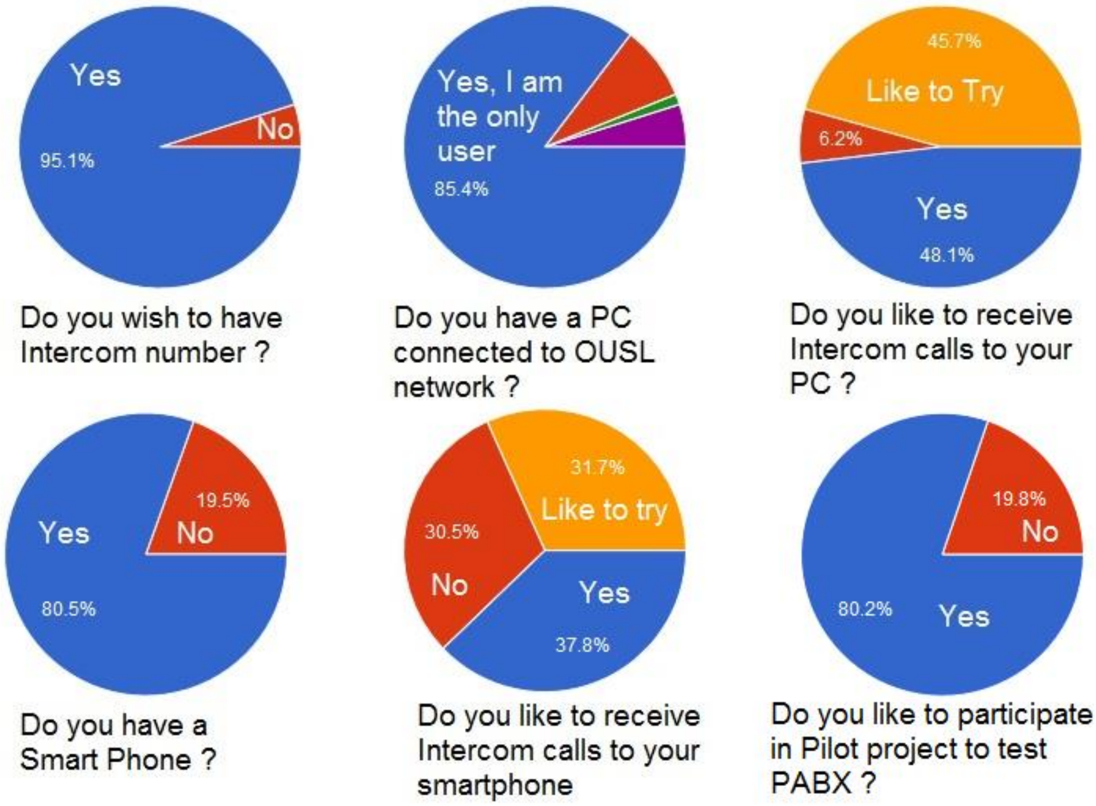

Figure 1. Outcome of the survey on intercom facilities for desktop PCs and Smartphones

The results of our survey also indicated that Smartphone density among the staff of OUSL is around 80%, while android OS dominated with around 85% and windows mobiles 12%. OUSL WIFI coverage is sufficient to cover almost every area in Colombo premises and providing user accounts to the needy users are underway. Intercom over WIFI is tested with users who have the WIFI connectivity and around 30% of people do not want to receive intercom calls via WIFI. 80% of the users have shown interest in participating in the pilot project, which is a huge motivational boost for us.

The OUSL campus network is protected by multiple firewalls and NAT is used only when traffic is routed to the Internet. Necessary ports are opened in firewalls to route traffic between the PABX and clients (PC and Smartphone) residing in different subnets while ensuring only RTP and SIP traffic is routed via those ports. Since NAT is not taking place, even the regional center clients could connect to PABX without ICE, STUN or TURN. The SIP over TCP and default public STUN servers accessible from the soft phones are proposed to connect the PABX and the clients through ADSL from the study centers of OUSL. We have created 30 extensions in the Elastix PABX system and tested for proper connectivity with both PC client and Mobile client via the WIFI network. We had a maximum of 12 simultaneous calls and a 4 way conference call with a mobile client. The System worked well with wired network while Smart phones worked well within the WIFI coverage area of fair signal strength. When the signal strength is low, high jitter and connection dropouts have occurred. Table 1 depicts the features that are tested for the proper functionality in the PABX.

Table 1. Features tested in the PABX System

Feature	Expected Result	Result
Two way call / Presence	One party calls an extension and it rings for pickup when soft phone status is available.	OK
Call waiting / forwarding	Alert a person in a call that they receive another call, forward calls blind mode and attended mode	OK
Call encryption	The call is encrypted and display a locked sign in mobile application	OK
Consultation	Keeping one call on hold and dial another number for getting a quick feedback	OK
Follow me service	Automatic forwarding of the call to Smartphone extension when PC extension is not answered, subsequently forward to voice mail when no answer to both extensions.	OK
Directory service	When first few letters of a name entered using the dial pad, PABX search and spell it out for dialing.	OK
Voice Mail	The call is forwarded to Voice mail when an extension is not answered. Indication and retrieval of voice mails	OK

CONCLUSIONS/RECOMMENDATIONS

The Software based PABX system is successfully tested within OUSL network and had no bandwidth issues in both wired and wireless networks with 12 simultaneous calls. Around 68kbps bandwidth is needed per voice call. High jitter, call dropouts occurred in places of poor WIFI signal strength. A campus wide deployment of this system is feasible and the outside telephone lines can be connected through SIP cards. If proper SIP trunks and number systems are negotiated, PABX systems in all the Sri Lankan universities can be linked via LEARN academic network.

REFERENCES

PaloSanto Solutions. (2016). *Elastix Installation Guide*. Retrieved from http://blogs.elastix.org/en/manuals/

Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., .. & Schooler, E. (2002). *SIP: session initiation protocol* (Vol. 23). RFC 3261, Internet Engineering Task Force.

Rosenberg, J., Mahy, R., Huitema, C., & Weinberger, J. (2003). *STUN-Simple Traversal of UDP Through Network Address Translators*.

Gupta, P., & Shmatikov, V. (2007, July). Security analysis of voice-over-IP protocols. In *Computer Security Foundations Symposium, 2007. CSF'07. 20th IEEE* (pp. 49-63). IEEE.