Volume 2 No. 11, November 2012 ISSN 2223-4985

International Journal of Information and Communication Technology Research

http://www.esjournals.org

Integrating Voice over Internet Protocol (VoIP) Technology as a Communication Tool on a Converged Network in Nigeria

Osanaiye Opeyemi Ayokunle
Department of Telecommunications Engineering, Federal University of Technology, Minna, Niger State, Nigeria

ABSTRACT

Telecommunications in recent years has been undergoing a rapid growth all over the world. Prominent among the advancements of telecommunication is the evolution of modern converged network that provides the trio of data, voice and video network on a single network platform. The converged technology uses the internet as a medium to transmit data, voice and video packets using packet switching. This comes with numerous benefits by providing add-ons to both the service providers and users. The VoIP technology has been widely accepted and has received a boost in most western countries like the US and UK where users are now migrating from the legendry Public Switch Telephony Network (PSTN) to VoIP because of the numerous benefits it offers but unfortunately the business environment in Nigeria is yet to key into this promising technology. This study therefore focuses on introducing and implementing this technology in a converged network in Nigerian environment. It will also showcase VoIP's numerous advantages and look at issues likely to be encountered during its implementation. It is hoped that it will help to serve as a tool in decision making process by converging the VoIP network with the already available data network.

Keywords: *VoIP, PSTN, SIP, Converged Network, Asterisk, QoS, Security.*

1. INTRODUCTION

New IP applications in the communication world are aiming towards the need for all IP converged network which tends to provide a better structure and reduce implementation and management support cost, VoIP is therefore not an exception. Voice over Internet Protocol which is also referred to as IP telephony was described by [1] as a revolutionary technology with the potential of completely overturning the world's telephone system. VoIP can still be referred to as a relatively new technology and common with every new technology, some countries and firms will quickly adopt while some will wait to see how it's being implemented in other countries before adopting, some others will completely ignore it.

A model was developed by [2] to categorize new technology adapters. The model highlighted five categories which were based on the time of adoption as: innovators, early adopters, early majority, late majority, and laggards. It can be said that the Nigerian government and other telecommunication service providers operating in Nigeria might not be ready for another massive investment into this technology based on the resent investment on mobile and cellular service. Published information within the UK and US has shown that the increase in usage and investment in this technology is growing at an alarming rate. This study therefore aims to introduce VoIP as a technology in a converged network, identify its features and issues, implement a VoIP system using the open source asterisk on a Linux platform and then make recommendations as regards to the Nigerian market.

1.1 Introduction to VoIP Technology

Voice over Internet Protocol (VoIP) which is also referred to as internet telephony is a technology that transmits voice signal in real time using the internet protocol (IP) over a public internet or private data network. [3]. In a simpler term, it converts voice signal which is analog to a digital signal in your telephone before compressing and encoding it into long strings of IP packets for upward transmission over the IP network to the receiver. At the receiving end, the received IP packets reassembles in order before decompressing and processing through the use of a Digital to Analogue Converter (DAC) to generate the initial signal transmitted. [4] .Its existence is basically based on two fundamental technologies, the telephone and the internet.

[5] Identified the sharing of existing infrastructures (convergence) between both data and voice application as some of the VoIP benefits in reducing implementation, management and support cost.

1.2 VoIP in Nigeria

VoIP in Nigeria can be traced to the early days of cyber cafes where cyber café operators offered cheap international calls when compared to the popular GSM and PSTN network. Few people that were aware of this technology then keyed into it at a cost. This cost can be said to be the poor voice quality which was as a result of the limited bandwidth available. As time went on, the Skype technology which is another VoIP platform where voice packets can be transmitted became popular among internet users both at home and in offices. To use this Skype technology, an internet facility must be available and there is also the need to install the Skype setup on both the transmitting computer and the receiving computer. This will then enable not only voice calls but also video and conference call as long as the computers have a webcam.

With the rate at which the technology developed, one would have thought the major telephone operators and the government would have seized the opportunity to key into this fast growing technology but that has not being the case. This study therefore describes how VoIP can be implemented in a converged network in Nigeria.

2. CONVERGED NETWORK

According to [6], the principal aim of converged network architecture is to integrate different type of network technology in a heterogeneous network. The common feature among these technologies was then identified as the end-to end packet delivery function they all offer.

The converged network can also be termed as a Next Generation Network (NGN) that carries data, voice and video traffic in a packet based network. It function by serving as a communication medium using broadband and QoS enabled transport technologies in which different service that are related in functions are independent from underlying transport technologies. The converged network provides consistent and ubiquitous service to users by supporting generalized mobility.

2.1 VoIP Network Components

The VoIP systems can come in different forms. Its basic structure is functionally similar to that of PSTN that allows it to communicate with the second party at the other terminal of the connection which is either a VoIP system or traditional analog telephone. Its basic form can be grouped into three; [7]

1. End users devices
2. Network Components
3. VoIP Gateway/Gatekeepers that interface with traditional telephone network.

2.1.1 End User Devices

The end user devices in a VoIP setup consists of VoIP phones and soft phones that provides an interface in which voice users interact with other users as well as the system. They use TCP/IP protocol to communicate with IP network that has an IP address for subnet on which they are installed. VoIP phones are usually auto-configured by a DHCP. The DHCP server tells the phone where the configuration server is located which sometimes is identical to a call processing server.

A soft phone on the other hand runs on software application on computers. They can also be installed on mobile devices and have the same base features as VoIP phones. [8]

2.1.2 Network Components

The main component in there is the IP PBX. The IP PBX which simply stands for IP private exchange box is a telephone switching system situated within the enterprise that switches calls between VoIP users on a local line while enabling users to share some certain number of external phone lines. [9]. IP PBX can be used to switch calls between a VoIP and PSTN user just like the conventional PBX does. It has an advantage of converging data and voice network which provides flexibility and reduced long-term operational and maintenance cost for an organization. Other network components include switches and routers.

2.1.3 Gateway/Gatekeepers

In VoIP, a gateway is a device that converts voice calls in real time between the PSTN and the IP network. [10] Its main function includes voice packetization, compression/decompression, call routing and control signalling. It may also additionally serve as an interface to external controllers taking the gatekeepers or soft switches, network management system and billing system. The gatekeeper on the other hand is a centrally controlled entity that performs management functions such as authentication, address mapping and bandwidth management in a VoIP solution for multimedia application such as video conferencing. Gatekeeper performs other numerous functions like providing intelligence to the system, authorization and authentication service, address resolution and logging of call detail record. Gatekeeper also controls bandwidth, provides interfaces to existing legal system and monitors network for engineering purpose.

Figure 1 below gives an illustration of the VoIP network component.

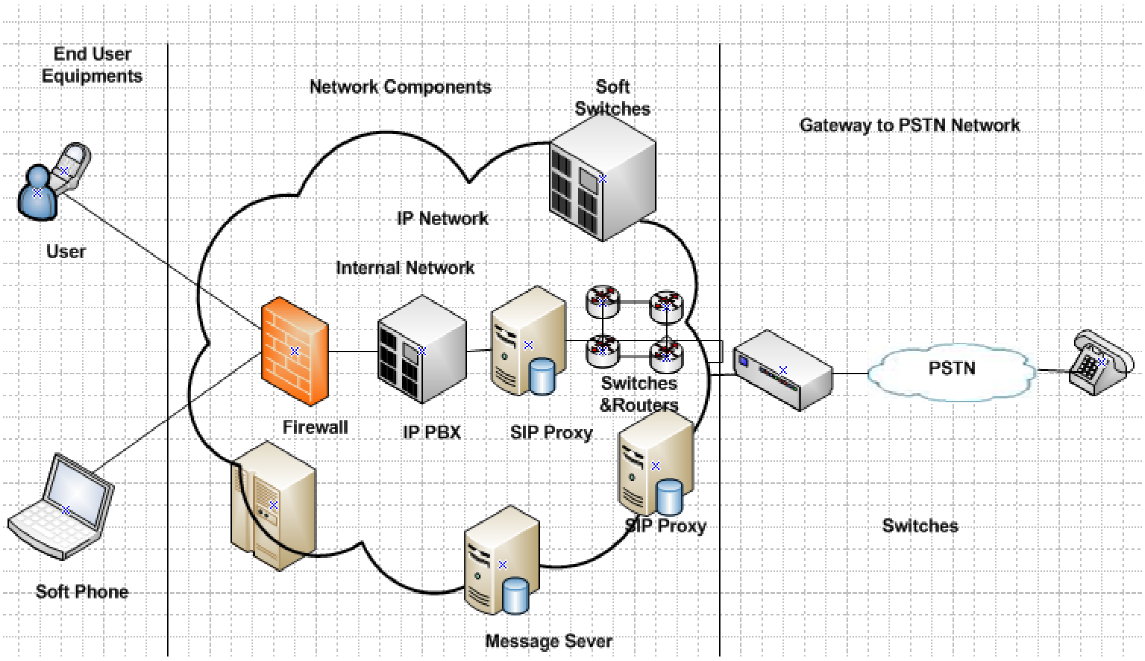


Figure 1.VoIP network component [7]

3. VOIP ARCHITECTURE

The major goal of the VoIP technology is establishing and managing communication sessions for transmitting both voice and data over a standard IP network.[11].Some additional data format like video text or images may also be supported by VoIP transmission. During this process, a stable and reliable transmission is maintained and the session can be put to end when any of the parties decides to.

According to [12] the two widely used protocols throughout the world today are the H323 and SIP protocol. They are functionally similar but competing protocols from two different organizations. The SIP was developed by the Internet Engineering Task Force (IETF) while the International Telecommunication Union (ITU) developed H323). [13] For the purpose of this study and our VoIP deployment, SIP protocol will be used.

3.1 Session Initiation Protocol (SIP)

Session Initiation Protocol (SIP) is an ASCII based application layer protocol; it was developed initially in 1999 by Internet Engineering Task Force (IETF) Multiparty Multimedia Session Control Group (MMUSIC) for multimedia conferencing over IP. This was later updated by SIP WG in 2002 [12]. SIP protocol can be used to initiate, maintain and terminate a call session between two or more end points. Just like any other VoIP protocol, SIP is designed to handle signalling and session management function within a packet telephony network. [1] The signalling function enables the transmission of information across boundaries while the control feature of an end-to-end call is performed by the session management.

SIP it similar to HTTP (Hyper Text Transfer Protocol) as it inherits its message structure used during multimedia session for setting up, cancelling and terminating real time session across an IP network by two or more participants. [14] Some of the benefits it offers include call/session control, extensibility and inherent user mobility. [15]

The major driving force behind SIP is to enable VoIP [16]. SIP is currently receiving a wide acceptance and will soon be the standard IP signalling mechanism for both multimedia and voice calling service .[16] As time goes on the older Private Branch Exchanges (PBXs) and network switches will be outdated and replaced with SIP enabled network model that is packet switched and IP based [17]

3.2 Comparison of VoIP and PSTN Services

In trying to compare the VoIP technology and the legendary PSTN, a table that compares the properties of each of this technology is drawn below.

Table 1: Comparison of VoIP and PSTN Services Source: [18]

Property	**PSTN service**	**VoIP service**
Switching	Circuit Switched. Bandwidth are used here even when information is not being transmitted	Packet Switched. No reservation of bandwidth, network resources are not used when packets are not transmitted.
Protocol	Uses SS7 signal protocol	Uses SIP, H323, RTP and several other transmission protocol to transmit data
Service	Traditional services like Phone calls, voice mail box, faxes, caller ID etc	Provides almost all traditional service and others like video, data and multimedia services
Quality	Quality here is guaranteed based on 64kbps bandwidth reservation	No bandwidth reservation and the quality can be affected by high traffic but quality can also be better than the PSTN with sufficient bandwidth
Infrastructure	Segmentation of infrastructure is necessary	Both data and voice share the same infrastructure
Power supply	Telephone lines transmit power of 48V which the Telephone uses even during power outage.	No independent power supply, alternative power is normally arranged.
Access	Limited	Open architecture with almost no restriction
Emergency	Caller may be localized during the case of an emergency as each client has their subscriber line.	No built emergency mechanism.
Security	Reasonably secured	Unsecured due to its open nature
Cost	High due to additional infrastructure and management	Relatively low as existing data network can be used for transmitting voice

It can be observed from the table above that the VoIP technology is still undergoing some improvement especially in terms of quality of service and security. Different QoS method has been developed and implemented that will prioritize real time traffic like the voice and video over the data traffic to grantee quality delivery of packets. The importance of security on the VoIP network cannot be overemphasised. All VoIP users require Confidentiality, Integrity and Availability (CIA) when this technology is being put to use. This two major factor has been looked into, with the major improvement on security being the encryption of voice packet over both public and private network.

One major attraction to VoIP technology when compared to the PSTN is the reduced cost and the other several add-ons it offers.

4. VOIP REGULATIONS

VoIP technology has received diverse reactions and response from countries all over the world, while some country totally embraced this technology, others completely banned it. For those that embraced it, some do not have any concrete regulation guiding it while others came up with some set of regulations guiding its deployment and usage. The Regulation of this technology in Nigeria is described below;

Nigeria: According to InfoDev an ICT regulation toolkit, Nigerian Communications Commission (NCC) on 11 February 2005 revealed its planed approach in regulating VoIP [19]. This was followed by series of consultative forum and workshops held by the industry study group on VoIP and its impact on international gateways and international access. Some common terms were agreed and the following guidelines were announced for Voice over IP regulatory conduct;

- VoIP is an eminent technology that provides voice telephony service and is not itself a distinct service.
- The Commission is authorized to and should continue to regulate the service and not the technology. This enables the industries practitioners to choose the technology to use in providing services that are authorized to provide.
- Consequently, the deployment of VoIP in Nigeria will be controlled by the commission and the necessary equipment needed for its deployment will be type-approved by the commission.

5. SECURING VOIP

Voice over IP being a mission-critical real time application has a low tolerance to delay and packet loss. This means several security solutions applicable to traditional telephony and data network in their present form are not applicable to VoIP [20] Intrusion detector systems (IDS), firewalls and other component must be designed specifically for VoIP so as to emulate and enjoy the security level being enjoyed by PSTN without affecting the voice quality of service. [21]

[22] identified segregation of traffic and protection of network components as the main security requirement of a secured VoIP network. Due to the fact that UDP packet does not guarantee service delivery, network components must prioritize voice traffic over data. VoIP components must be dedicated as regards to its performance and security. All unused ports must be disabled and the hardware components physically secured.

[23] in his publication summarized the countermeasures required in other to secure the VoIP network, this is presented below;

5.1 Countermeasures with VoIP Network

Some of the countermeasure required to secure the VoIP network are;

- **Physical security:** The hardware, equipment and the network component used to provide VoIP service must be physically secured.
- **Segmentation:** In other to isolate attacks, voice and data traffic must be separated using **virtual local area network (VLAN**). Virtual LAN on switches helps to logically separate the network rather than having a different physical network.
- **Encryption of traffic:** The VoIP traffic must be managed through secure connection in other to avoid intruders from capturing and modifying call contents and session information.
- **Duplicate TCP/IP service:** It is better to have a separate server for voice and data network in the case of Domain Name Server (DNS) and Dynamic Host Configuration Protocol (DHCP). This goes a long way in solving DoS attack aiming the service on one of the two networks.
- **Hardening:** Hardening of applications and operating system is essentials so as to protect the network.
- **Traffic filtering:** Unauthorized traffic must be filter using **VoIP-aware firewalls** in-between routers and switches. The network must therefore allow only expected traffics on individual VLANs screening out unnecessary ones. An example is the denial of SIP traffic on a data network and the blockage of DHCP request in-between IP phones.

The flow chat presented in figure 2 below illustrates the management of VoIP traffic during transmission in a secured network.

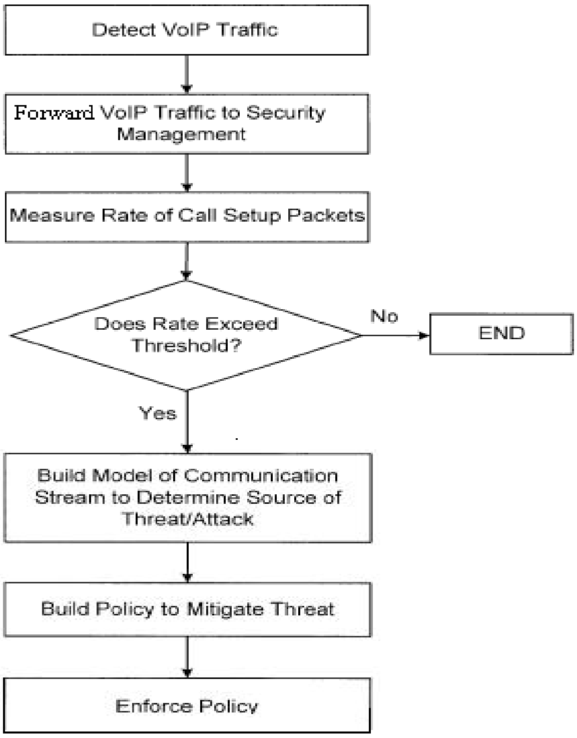

Detect VoIP Traffic
Forward VoIP Traffic to Security Management
Measure Rate of Call Setup Packets
Does Rate Exceed Threshold?
No
END
Yes
Build Model of Communication Stream to Determine Source of Threat/Attack
Build Policy to Mitigate Threat
Enforce Policy

Figure 2 Flow chat on how to manage security

Source: [24]

5.2 Effect of security on QoS

Due to the real time nature of voice, the security implemented on the traditional Data network is not applicable to it because of its low tolerance to delay and packet loss.

In deploying security on the VoIP network, the quality of service (QoS) must be put into consideration.] identified QoS as essential in the operation of the VoIP network. [25] then admitted that there will be degradation in the QoS of voice after implementing security on the VoIP network. [26] identified blocking or denying of call setup that leads to delay and latency as one of the consequence of implementing security on VoIP.

[27] then provided a solution to the worrying security deployment by recommending some specially made security solutions for voice traffic consisting of an inbuilt QoS mechanism. He also made other recommendations like encrypting packets at end point, using a Secured Real Transport Protocol (SRTP) for transmitting voice and video application and providing a reasonable amount bandwidth that will be sufficient for the intended applications.

5.3 Implementing Voice over Internet Protocol (VoIP) using open source Asterisk

When planning to implement VoIP in a converged network, choosing an approach will depend on factors like budget, technology expertise, implementation risk and cost of deployment. In our implementation scenario, VoIP will be implemented between two offices in different location. The Lagos office which is the Head office and the Abuja office (branch office).

In this report, an open source Asterisk will be implemented on a converged network but before then, an assessment will be made on the existing network.

5.3.1 Network Assessment

Before introducing a VoIP to an existing network, a thorough network assessment must be carried out on the organisation or company’s infrastructure. With this assessment, potential issues and problem can be identified before implementing the VoIP technology.

5.3.2 Detail Design

Table 2: IP Addressing and Telephone Extension Allocation

Description	Head Office (Lagos)	Abuja Office
IP address for VoIP network	192.168.2.0	192.168.1.0
Telephone Extension Numbers	2XXX	3XXX
IP PBX assigned IP address	192.168.2.2 255.255.255.0	192.168.1.2 255.255.255.0
Serial interface	192.168.10.1 255.255.255.0	192.168.10.2 255.255.255.0

5.3.3 Asterisk

Asterisk is an open source Voice over IP solution invented by Mark Spencer of Digium Inc in 1999. Because it can run conveniently on mid range PC hardware and its open nature as compared with other commercial VoIP deployment, it has become a choice of VoIP users. Asterisk runs on Linux platform and was released under GNU General Public Licence.

Asterisk runs on UNIX operating system and can be accessed through the command line interface (CLI). Various version of Asterisk has been developed after it was released in 1999 with the latest being Asterisk 1.8 released in 2010. It has more than 200 notable new features which include new security features, more than 200 enhancements, integration with IPv6 and lots more [28] Asterisk supports protocol like IAX, SIP, H323, SCCP and MGCP but SIP protocol was used in this implementation.

5.3.4 Requirements for building Asterisks

When designing the VoIP technology to be introduced into the network, the right requirements should be specified so make the right choices when acquiring both software and hardware to manage the money invested. Among major questions identified by [29] that must be asked are;

1. How many users will the IPBX support?
2. Do you have high performance server?
3. What type of operating system will your server run on?
4. Will your VoIP solution be attached to either digital or analog phones?
5. Do you need to connect either ordinary telephone line or PSTN trunk line to the system?

5.3.5 Configuring Asterisk

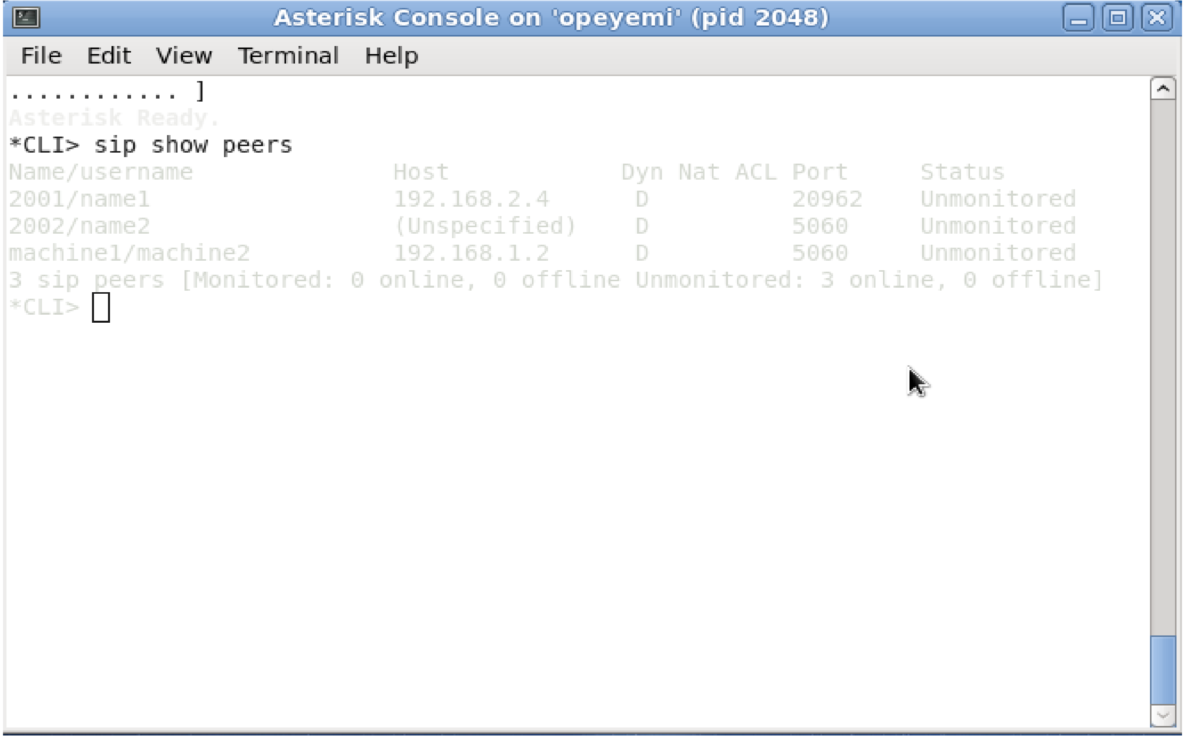
In configuring Asterisk, two different approaches can be deployed; these can be either configuration method by manually editing or the GUI using point and click. The manual editing was used for this implementation.
During the configuration process, the following files where manually edited;

Sip.conf: In this file the various sip clients were defined in their context for the Asterisk PBX.

Extensions.conf: This file defines how calls are handled and routed within and outside the Asterisk box. The dial plan for various users is also defined in their context that determines how they interact in the Asterisk.

Voicemail.conf: This file defines an interaction interface with callers when the intended receiver is not available to receive the call.

To check the status of the configured users, its extension number, IP address, port number and status, the command used is ***#sip show peers***; this is illustrated in figure 3



```
............ ]
Asterisk Ready.
*CLI> sip show peers
Name/username              Host            Dyn Nat ACL Port     Status
2001/name1                 192.168.2.4      D          20962    Unmonitored
2002/name2                 (Unspecified)    D          5060     Unmonitored
machine1/machine2          192.168.1.2      D          5060     Unmonitored
3 sip peers [Monitored: 0 online, 0 offline Unmonitored: 3 online, 0 offline]
*CLI>
```

Figure 3: Screen shot of Asterisk command line interface showing the configured SIP users

After the configured user's status was checked, a call was place between the two branches using both the IP Phones and the soft pones. The call was initiated and received successfully.

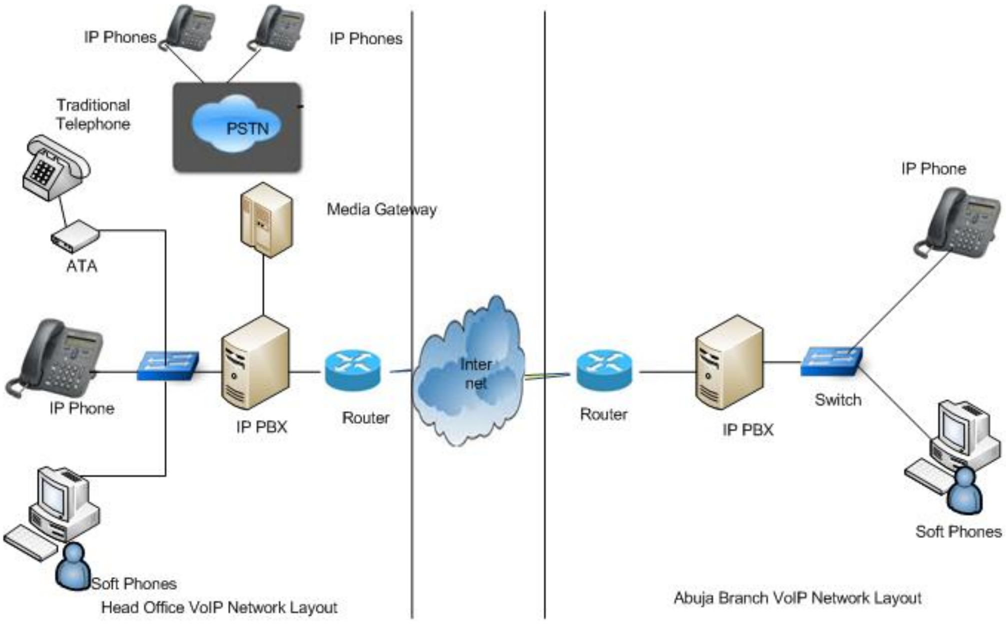


Figure 4: VoIP network

6. CONCLUSION

The VoIP technology has been predicted to be the future to Telecommunications globally; therefore integrating it in a converged network in Nigeria must be encouraged. The VoIP technology has cheaper call rate, easier IT management and reduction in operational cost for a combined network for voice and data which gives it an edge over the PSTN. It will only be considered as being successful and replace the traditional PSTN when both the security and quality of service of the voice packet which is real-time transmitted over the public and private network is specially addressed.
This technology when implemented by telecommunications operators in Nigeria over the already existing Data network with adequate bandwidth and security will go a long way in easing communication.

REFERENCES

[1]. Ansari ,S. & Khan, A. (2007) 'Voice over Internet Protocol Security problems in Wireless Environment' *Journal of Engineering and Sciences*, 1(2),pp. 82-85.

[2]. Moore, G. (1991) *Crossing the Chasm*, Harper Business, New York

[3]. Hallock, J. (2004) *A brief history of VoIP, Evolution and Trends in Digital Media Technologies*, University of Washington.

[4]. La Corte, A., & Sicari, S. (2006), 'Assessed quality of service and voice and data integration: a case study', *Computer Communications*, 29(11). pp. 1992-2003.

[5]. Ranganathan, M. & Kilimartin, L. (2003) 'Performance analysis of secure session initiation protocol based VoIP networks', *Computer Communications* 26(6), pp. 552-565.

[6]. Argyroudis, p., McAdoo, R., Toner, L., & O'Mahony, D. (2007) 'Analysing the Security Threats against Network Convergence Architectures'. *Third International Symposium on Information Assurance and Security*, IEEE computer society, pp. 241-246

[7]. Dantu,R., Fahmy, S., Schulzrinne, H., & Cangussu, J.(2009), 'issues and challenges in security VoIP' *Computer & Security*,28(8), pp .743-753.

[8]. Desantis,M. (2008) , *Understanding Voice over Internet Protocol (VoIP)*, US-CERT.

[9]. Ramachandran, (2006) VoIP Security: asserting the trust boundary, 'The Global Voice of Information Security', *ISSA Journal* pp.8-13.

[10]. Dhamankar, R. (2005), *Intrusion Prevention: The Future of VoIP Security*, White paper by Tripping Point.

[11]. Amarandei-Stavila, M. (2005) *Voice over IP Security A layered approach*, xmco partners.

[12]. Karapantazis, S. & Pavlidou, F. (2009) 'VoIP: A comprehensive survey on promising technology', *Computer Networks*, 53(12), pp.2050-2090

[13]. Ansari,S. , Khan ,K. , Rehana,J. , Lisa,J. , & Kaisar, S. (2009) 'Different Approaches of Interworking between SIP and H323' *International journal of Computer Science and Network Security*, 9(3),pp.232-239.

[14]. Geneiatakis, D., Lambrinoudakis, C. & Kambourakis, G. (2007) 'An ontology-based policy for deploying secure SIP-based VoIP services', *Computer & Security*, 2006(27), pp.285-297

[15]. Wisely, D. (2001)'SIP and conventional internet application' *BT Technology journal*, 19(2), pp.107-118.

[16]. Stallings W., (2003) 'The Session Initiation Protocol', *The internet protocol journal*, 6(1), pp.5-38

[17]. Borthick, S. (2003) *SIP for the Enterprise: Work in Progress, Business Communications Review*.

[18]. Lawecki, P (2007) 'VoIP Security in Public Network': A Master's Thesis submitted at Pozan University of Technology.

[19]. InfoDev (2010) ICT regulation tool kit.[Online] Available at http://www.ictregulationtoolkit.org/en/PracticeNote.aspx?id=2595, , last updated 22nd May 2012, [accessed: 11th July 2012]

[20]. Ghafarian, A., Draughorne,R., Hargraves, S., Grainger, S., High, S., & Jackson. (2007) 'Securing Voice over Internet Protocol' *journal of information Assurance and Security*, 2(2007), pp 200-204.

[21]. Diab,W. , Tohme,S., & Bassil. C.(2008) *VPN Analysis and New Approach for Securing VoIP Communication over VPN Network*. In: Fourth international conference on network and service (ICN 2008), Gosier, Guadeloupe, March 16-March 21, 2008, pp.73-78.

[22]. Edelson, E. (2005) 'Voice over IP: security pitfalls', *Network Security*, 2005(2), pp.4-7.

[23]. Ramirez.,D (2007) 'Security Within VoIP Networks', *Information Systems Control Journal*, Vol 6

[24]. Sankaran, N.,Raghunath, R.& Sanjay, R . (2010) 'Replacing Conventional Telephones by VoIP: Their Major Constraints & Solutions', *International Journal of Computer Applications*, 1(12), pp.66-70.

[25]. Chen ,X. , Wang,C. , Xuant, D. , Li,Z. ,Min,Y. , & Zhao,W. (2003), 'Survey of QoS Management on VoIP', *in proceeding of the 2003 international conference on Computer Networks and Mobile Computing*, Institute of Chinese Academy of Sciences.

[26]. Elbayoumy,A. & Shepherd,S. (2007) 'A Comprehensive Secure VOIP Solution' *International Journal of Network Security* , 5(6), pp.233-240.

[27]. Kuhn, D.,Thomas, J. ,Walsh, Steffen, F.(2005) National Institute of Standards and Technology; NIST Recommendations of NIST concerning VoIP security; *Security Considerations for Voice over IP Systems*.

[28]. www.digium.com/en [assessed 9th Aug, 2012]

[29]. Wicaksana, I., Febrinata, A., Trihasta, D.& Fajaryanti, j. (2008) 'VoIP and Conventional PABX together based on Open Source Asterisk', *Workshop on Open Source and Open Content (WOSOC)*, 1-3 December 2008, Bali- Indonesia, pp. 57-62.