

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/366231876>

Secure and Optimize VoIP Communication Using QoS Technologies and VPN

Article · December 2022

DOI: 10.5281/zenodo.7433359

CITATIONS

0

4 authors, including:



Bello A. Buhari

Usmanu Danfodiyo University Sokoto

28 PUBLICATIONS 26 CITATIONS

[SEE PROFILE](#)



Bello Bodinga

Usmanu Danfodiyo University Sokoto

8 PUBLICATIONS 1 CITATION

[SEE PROFILE](#)



Maniru Malami Umar

Usmanu Danfodiyo University Sokoto

13 PUBLICATIONS 13 CITATIONS

[SEE PROFILE](#)

Some of the authors of this publication are also working on these related projects:



A Survey of Security Vulnerabilities in P HP Applications among IT Professionals in Nigeria [View project](#)



Security [View project](#)

Secure and Optimize VoIP Communication Using QoS Technologies and VPN

Muhammad Zaharaddeen Bello¹, Bello Alhaji Buhari^{2}, Bello Aminu Bodinga², Maniru Malami Umar²*

¹*Government Day Secondary School Mabera, Sokoto, Nigeria.*

²*Department of Computer Science, Usmanu Danfodiyo University, Sokoto, Nigeria.*

Corresponding Author

E-Mail ID: buhari.bello@udusok.edu.ng

ABSTRACT

The use of Voice over IP (VoIP), which enables two users connected to Internet to have a voice conversation, plays a vital role on the performance of an enterprise companies. In this research we have focused in the Virtual Private Network (VPN) environment and how to run voice application over it. The Voice Over Internet Protocol (VOIP) is as a combination of IP networks, voice applications and voice calls which being replaced by the old service conversation and created their evolution at the technical and conceptual framework of phone. This technology is an innovative form of phone that can dramatically increase performance and capacities of telephone service for businesses and individuals around the world. But voice qualities, security, Jitters, Echo, Data loss are the pertaining problems associated with VoIP. To overcome this limitation in this research, we used Simulation method in Cisco packet tracer to secure this technology using VPN. This is because VPN establishes a secure, encrypted connection between a computer and the internet, providing a private tunnel for ones data and communications while he/she uses public networks. Thus, provide users with a secure communication platform and at the same time optimized the technology using QoS technologies so as maintained and assure service's performance and to avoid degradation of speech quality.

Keywords: VOIP, VPN, Secure Communication, Voice application, QoS.

INTRODUCTION

The proliferation of the Internet across geographic boundaries gave rise to the creation of a new application: Voice over IP (VoIP), that enables two users connected to Internet to have a voice conversation. Voice over IP technology refers to the concept of using the well-established IP networks (e.g. internet), as backbone for carrying real time voice communications. The voice transferred over the Internet exhibits different characteristics than voice transferred through the Public Service Telephone Network (PSTN) and requires certain provisions in the network. With a paradigm shift of IP networks from pure

data networks to a unified data and voice, multimedia network has significantly reduced the voice communications costs leading to a growing demand among end-users. Voice applications have different characteristics and requirements from those of traditional data applications. Because they are innately real-time, voice applications are highly sensitive to delays in speech and crispy sounds. Thus strict measures for QoS are needed to ensure the possibility of performing better VoIP calls with higher quality. In addition, the inherent problems with security in WLANs pose additional challenges in regard to VoIP that need to be addressed. Voice over internet Protocol is defined to

be the digitization and transmission of the analogue voice as a stream of packets which is carried out over a digital data network that can carry data packets using IP and other Internet related protocols. This network may be an organization's internal LAN, a leased network, the PSTN or the open Internet [1]. Recently, high speed Internet connections became inexpensive and reliable. This led to the spread of Virtual Private Network (VPN) connections instead of direct dial-up or leased line connections. They connect offices in different parts of the world and make corporate networks accessible for the employees anywhere using a single Internet connection.

They also help reserving the remaining IPv4 address space by making computers accessible without public IP addresses; however, they are still not practical for real-time, delay or speed sensitive applications. Online games, video streaming, and file sharing services are just a few of the numerous protocols that cannot be efficiently used with the current, point-to-point virtual private network protocols; however, recently many applications of peer-to-peer technologies proved to be efficient, fast and reliable. By combining peer-to-peer technologies with VPNs, it is possible to create faster VPN networks. There are many problems associated with VoIP Communications these include: Voice Quality Problem, Performance Problems, Bandwidth Saturation, Security Issues, Lack of Quality of Service which is concerned delay and packet loss are the major issues and Traffic Management problem.

The aim of this research is to secure and optimize VoIP communication using QoS technologies and VPN and its simulation on Enterprise Companies. This is because VPN establishes a secure, encrypted connection between a computer and the internet, providing a private tunnel for

ones data and communications while he/she uses public networks.

RELATED WORKS

Voice over Internet Protocol (VoIP) is one of the most important technologies in the world of communication. Around 20 years of research on VoIP, some Quality of Service (QoS) problems of VoIP are still remaining. During the past decade and with growing of wireless technologies, they discovered that many papers turn their concentration from Wired-LAN to Wireless-LAN. VoIP over Wireless LAN (WLAN) faces a lot of challenges, due to the loose nature of wireless network. Issues like providing QoS at a good level, dedicating capacity for calls and having secure calls is more difficult rather than wired LAN. Therefore, VoIP over WLAN (VoWLAN) remains a challenging research topic [12].

In recent studies consolidated and addressed all VoIP #, VPN and WLAN issues. In [3] the Author focused his study on introducing and implementing this technology in a converged network in Nigerian environment, which also showcased VoIP's numerous advantages and looked at issues likely to be encountered during its implementation.

In [4] both the Authors described VoIP system for the enterprise network (e.g. company, university) that have been developed based on Asterisk which is a kind of open source software to implement IP-PBX system. Through the development and evaluation, they have confirmed that VoIP system based on Asterisk is very powerful as a whole and most PBX functions to be required for the enterprise network can be realized.

In [5] Author Proposed Design and Implementation of a Voice over Internet Protocol (VoIP) over Local Area Network (LAN). The research aimed at installing and implementing a VoIP server to enable

voice communications between computers on the network. The method used by this system is basically two which comprises of installing the hardware tools and configuring the software component. The hardware tools that the system needs are Computer, VoIP Server, IP Phone, Router and Switches. Then configuring the software components this involves the conversion of a traditional computer into a VoIP asterisk server and installation of soft phones.

Then additional configurations to be done are configuring the IP phones, soft phones and asterisk server. Hence forth the system Increased productivity by allowing us to have our phone lines over our internet protocol network. And allow room for unified communications. It also allows users to have added features like voicemail and conferencing at no extra cost. However, the major limitation of this system is the security and Quality of service (QoS) of the voice packet which is transmitted over the private network.

The author in [6] designed an Internet Phone (VoIP) for Voice Security using the VPN. This paper suggests a new model of Internet telephone for eavesdrop prevention enabling VoIP (using SIP protocol) to use the protocol and establish the probability of practical use comparing it with Internet telephone. In this study, therefore, in order to prevent the wiretapping by the Internet phone, an Internet phone terminal was developed by using Virtual Private Network (VPN).

And it was analyzed for its performance and examined for its validity by applying PPTP (Point-to-Point Protocol) to the Internet phone terminal using SIP protocol stack in order to prevent wiretapping. Call length was set up to 10 seconds in order to measure the performance of internet phoneCall for preventing wiretapping in PPTP and SIP protocol implemented in

this study. Therefore, Control Connection message should be encrypted in order to make complete security of encryption and it would be better to use IPSec among VPN functions which have the authentication function.

In [7] Author measured the quality VoIP performance over Virtual Private Network technology. In his study he analyzed the VPN over open source application (e.g. Windows and Linux operating system), and hardware device (e.g. juniper) performance areas evolved with the quality of service delivered by VoIP conversation between branches. His study concluded that base on the findings, VoIP over VPN using software base contributes to higher delay, jitter and CPU utilization compare to VPN hardware base. It is therefore recommended to implement VoIP over VPN using hardware base in order to achieve a good quality service conversation.

The author in [8]proposed the Designing 802.11 WLANs for VoIP and Data This paper presents a procedure and its implementation in an experimental scenario for designing WLANs with VoIP support, using two of the most important current standards for WLANs: 802.11b and 802.11g.His Study Concluded that Designing a wireless network with 801.11b or g standards for VoIP and data as an extension of the wired one, it can only be feasible in small places (hot spots) with standstill clients, in short distances and with a low number of calls. However, the major limitation of this system is the security and Quality of service (QoS) of the voice packet which is transmitted over the private network.

In [9] the author focused on VoIP Security: Common Attacks and their Countermeasures this research paper Common threats and attacks within VoIP network are being discuss and also some

mitigation strategies that can be used in order to ensure security of VoIP network. He concluded that VoIP technology is gaining more popularity and it is expected to replace the traditional public switch telephone network (PSTN) in years to come. However, as the technology grows, the issue of its security grows as well. Security of information is very important since it is the greatest asset of an organization. Mitigation strategies which involve authentication and decryption of VoIP protocols, separating VoIP and data network, regular updates and upgrades of patches, complying with ISO27001 standard will help to strengthen security in a VoIP network.

Another study review is analysis of QoS enabled MPLS VPN VOIP network withripv2 routing protocol in [10]. In this paper, analyze the behavior of RIPv2 (Routing information protocol version 2) based MPLS VPN architecture by using intense VOIP traffic with help of OPNET simulation process and unique network architecture. At last, the conclusion is made that RIPv2 based MPLS VPN architecture has produce VPN delay, LSP delays andp2p Queuing delay so it is not best solution for the large network environment.

In [11] Author Proposed a Comparative Evaluation of Security Aspects of VoIP Technology This paper provides starting point for understanding the security facets of VoIP in a rapidly evolving set of technologies that are seeing growing deployment and use. The main goal is to provide a better understanding of the security background with respect to VoIP security facet toward directing future research and in other similar up-and-coming technologies.

The author in [12] provides A Survey on Voice over IP over Wireless LANs as a major concerned issue. Although, VoIP

can tolerate packet loss to some extent, it is very sensitive to delay factor. Jitter also plays a main role on voice quality therefore jitter buffer is introduced to smooth the play out of packets. Echo and throughput are also other factors that affect the quality of voice. Different techniques for voice QoS assessment were mentioned as well. Furthermore, WLAN is a bandwidth limited network which may limit the number of VoIP calls. Accordingly, this paper discussed capacity and its measurement technique as it is based on IEEE 802.11b standard with voice codes and millisecond packetization intervals. At the same time as security issues in VoIP poses a challenge, security issues and their available solutions are also investigated in this paper.

In the proposed Study the Design and implementation of VoIP over VPN using QoS technology will be seen using the simulation of the hardware using chosen networking tools.

METHODOLOGY

The simulation methodology is suitable for the success of this research. Simulation method is the process of creating and analyzing a physical model to predict its performance in the real world [18]. Simulation of a system is the operation of a model of the system. There are different kind of tools used to simulate a network tools like GNS 3 and CISCO packet tracer. For this research simulation the Cisco packet tracer will be used because of its simplicity than other tools and it require less memory to run the simulation.

Cisco Packet Tracer is a powerful network simulation program that allows students to experiment with network behavior and ask questions. Packet Tracer provides simulation, visualization, authoring, assessment, and collaboration capabilities to facilities the teaching and learning of complex environment where processes between various networking devices, such

as routers, switches, wireless access points, computer, links and applications are visible with animations and easy explanatory descriptions. Most importantly, packet Tracer helps students and instructors create their own virtual network worlds for exploration, experimentation, and exploration of networking concepts and technologies [19]. Cisco Packet Tracer version 7.2 is used for my simulation, which will support the VPN QoS and VoIP design. The simulation was performed using Windows based operating system core i5 4GB RAM 2.7GHZ processor speed.

REQUIREMENTS FOR THE PROPOSED VOIP

Cisco IOS Multiprotocol Label Switching (MPLS) which enables Enterprises and Service Providers to build next-generation intelligent networks that deliver a wide variety of advanced, a static route which is manually entered by an Administrator on a

Network Device to reach to a specific network or set of specific networks using its Exit Interface or next hop-router, a virtual private network (VPN) which is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures, IPsec which is a set of protocols and standards developed by the Internet Engineering and QoS technologies which are set of tools and techniques to manage network resources and are considered the key enabling technologies for the transparent convergence of voice, video, and data networks.

LOGICAL TOPOLOGY OF THE PROPOSED NETWORK

The figure 1 below illustrates the logical topology of the proposed network and its description using router to router connections.

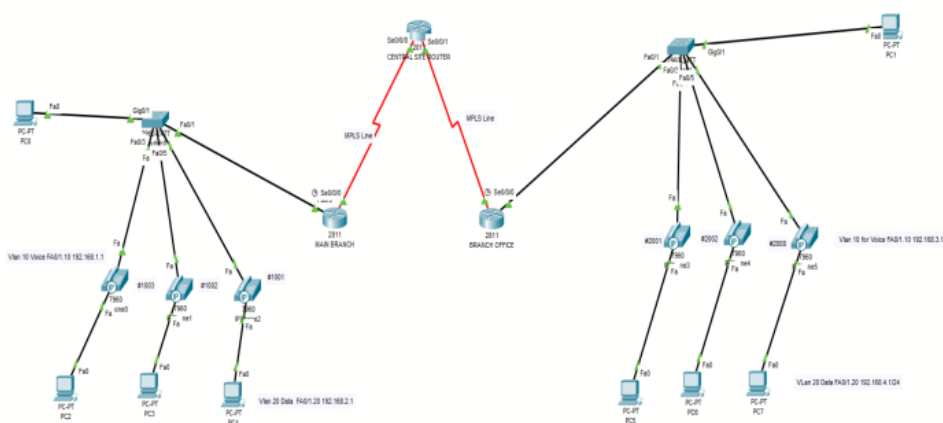


Fig.1:-Proposed network topology

Router to router is being used to design the IPsec VPN Considering the Topology of the enterprise, The Enterprise Company is said has three routers the central site router the main Branch router and extended network to the remote branch by adding another router to the City Campus therefore enabling us to choose the router to router encryption mode. That is configuring the IPsec parameters on the

router at the main branch and then configuring the IPsec parameter on the other router located at remote site router. IPsec VPN uses tunneling to establish a private connection through which all your data is passed through.

Unlike other protocols that function at application layer, IPsec operates at network layer and this allows it to encrypt

the entire packet. A variety of encryption algorithms are employed for this very purpose, but we can drill them down to two main mechanisms DES and AES, PureVPN's IPsec uses AES (Advanced Encryption Standard) along with other technologies to keep your data safe. And also, IKE mechanism is required between the IPsec peer to allow data exchange IKE uses the Internet Security Association and Key Management Protocol (ISAKMP).

A. Phases in Creating VPN

PHASE 1

Set up the access list permit on each router that will tunnel to allow the routers knows the IP address that are allow to follow that VPN tunnel

PHASE 2

Set up the isakmp policy on each router
Set up the isakmp key

PHASE 3

Create a transform-set from one router to other such that

PHASE 4

Create a crypto map on either router to bind phase 2 and 3 parameters

Apply crypto map on the interface

ANALYSIS AND DISCUSSION OF THE SIMULATED RESULTS

A. VPN Result Analysis and Discussion

Step 1: Activate securityk9 module.

The Security Technology Package license must be enabled to complete this activity.

```
License Info:
License UDI:
-----
Device#      PID          SN
-----
*0           CISCO2901/K9  FTX1S242U8D

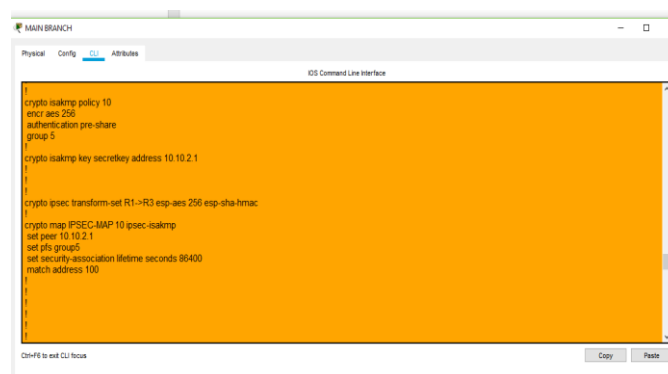
Technology Package License Information for Module: 'c2900'
-----
Technology    Technology-package    Technology-package
Current       Type                 Next reboot
-----
ipbase        ipbasek9             Permanent
security      securityk9           Evaluation
uc            None                 None
data          None                 None

Configuration register is 0x2102
```

Fig.2:-Activation of securityK9 module

Step 2: Configure IPsec Parameters on R1

This shows that the Ipsec parameters are configured on R1 having the encryptions and authentication mode activated and connection to R3 is secured.



```
crypto isakmp policy 10
encr aes 256
authentication pre-share
group 5

crypto isakmp key secretkey address 10.10.2.1

crypto ipsec transform-set R1->R3 esp-aes 256 esp-sha-hmac

crypto map PSEC-MAP 10 ipsec-isakmp
set peer 10.10.2.1
set pfs group5
set security-association lifetime seconds 86400
match address 100
```

Fig 3:-Configure Ipsec on Router one (R1) Main Branch

Step 3: Configure the Isec parameters on R3

This shows that the Isec parameters are configured on R3 having the encryptions and authentication mode activated and connection to R1 is secured.

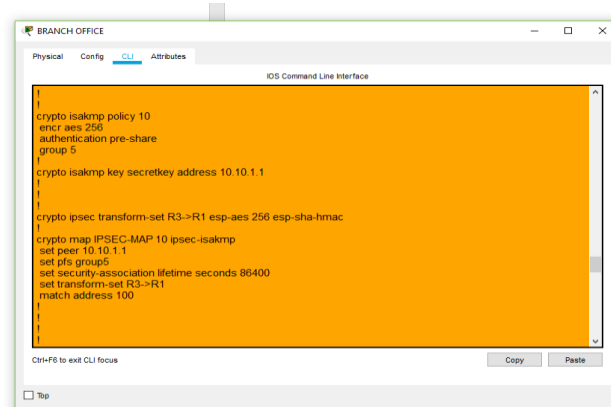


Fig.4:-Configure Isec on router three (R3) Branch Office

B. VoIP Discussion

First thing that needs to be done is to power the IP phones ON by clicking on the adapter extreme right end and drag it to its port and that will power on the phone and allow them to work fully.

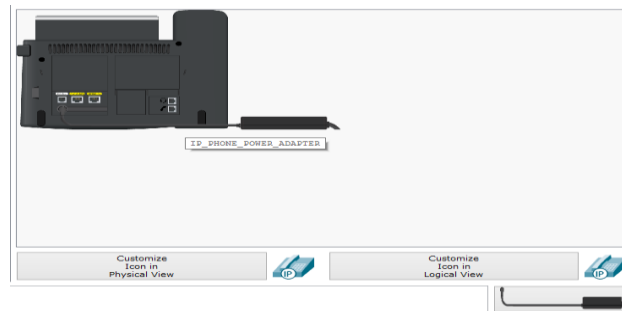


Fig.5:-Power the Phone On

Main Branch

On the main branch the IP phones connection have been established as the phones installed can communicate to each other as we can see phone number 1002 called phone number 2002 and the phones are connected.



Fig.6:-Call established at Main Branch

Branch Office (Remote Site)

On the other hand, the phones installed at city campus are also communicating to each other as phone number 2000 called phone number 1003 and the call is connected.



Fig.7:-Call established at Branch Office (Remote Site)

FINDINGS OF THE SIMULATED RESULTS

Based on the result obtained from the simulation we can see that every staff of the enterprise company can Communicate with each other, that is you don't have to be in the same branch. a staff from main branch can contact another staff at remote site (branch office) and this

communication is secured using VPN technology which means that if a staff is communicating with another staff from different branch then the router that connect the two branches that is the Central Host Router will not know the actual source and destination IP address of the packet as you can see from Figure 8 and 9 blow.

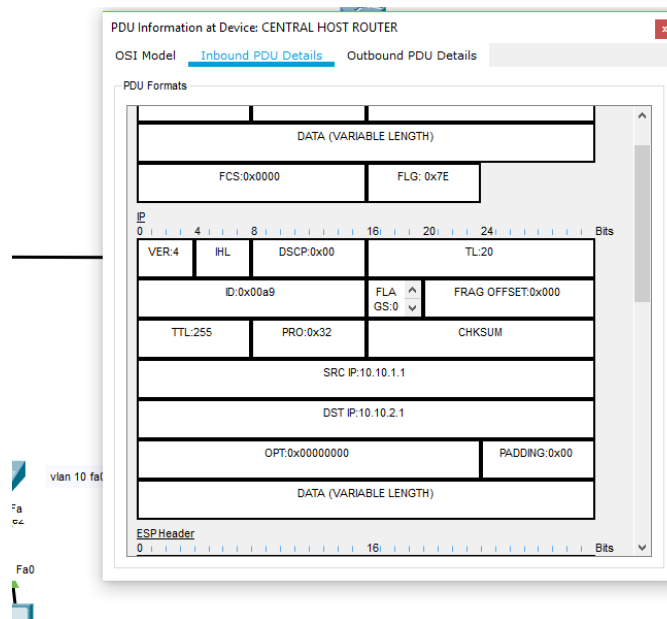


Fig.8:-The packet header where the Central Host Router sees the source IP address

This figure shows the packet header where the Central Host Router sees the source IP address as 10.10.1.1 and destination IP

address 10.10.2.1 which is not the actual Source and destination IP addresses of the packet.

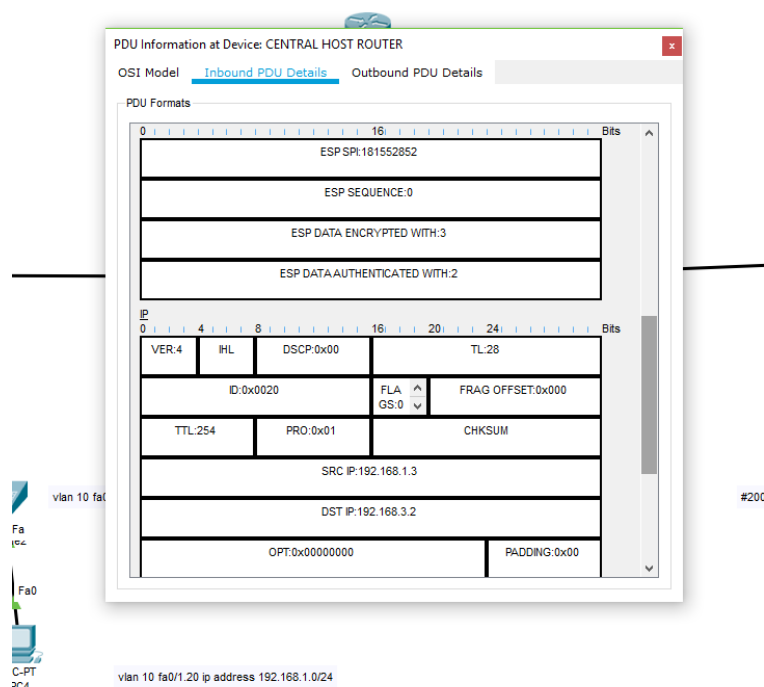


Fig.9:-The actual Source and destination IP addresses

This figure shows the actual Source and destination IP addresses which are 192.168.1.3 and 192.168.3.2 encrypted by the VPN tunnel.

CONCLUSION

In this study a research local area network linking the two branches of an enterprise company which are the main branch that is located in the city and the branch office located in a remote site was established. Security is very important as it plays a vital role is the safety of file transfer over the internet.

The mode securing that was used to help secure the link between the two branches of the enterpriser company was a Virtual Private Network (VPN).

The VPN itself has many technologies of securing a network connection in which

amongst the methods chosen is Internet Protocol security (IPsec), which provides enhanced security features such as better encryption algorithms and more comprehensive authentication. However, in this research a VoIP connection was established within the main Branch and the remote site respectively and all the phone can communicate with them on the same local network. And also, QoS technology was used in other to optimized service quality of the VoIP communication.

The VoIP technology is becoming the major means of Telecommunications globally because it establishes a secure, encrypted connection between a computer and the internet, providing a private tunnel for ones data and communications while he/she uses public networks, therefore, integrating VoIP into our Enterprise network must be encouraged.

The VoIP technology has cheaper call rate, reduction in operational cost for a combined network for voice and data, it is also easy to manage. The main disadvantage that is yet to be addressed fully for VoIP to be called a success is the inability to exchange phone call from one network to another due to the platform used and Quality of service of the voice packet which is transmitted over the private network. This technology when implemented by the Enterprise Company management over the already existing network with increased bandwidth will ease the communication lapse and increase security in their network.

REFERENCES

1. Gradwell P., VOIP Discussion at the BCS Specialist Internet Group, British Computer Society: London,(February 2006), Available at: <http://www.bcs.org/server.php?show=ConWebDoc.3556> [Last Accessed 13/03/019].
2. Dudman, J.(2006).*Voice over IP: what it is, why people want it, and where it is going*. JISC Technology and Standards Watch. pp 2-27.
3. Ayokunle O. O (2012), *Integrating Voice over Internet Protocol (VoIP) Technology as a Communication Tool on a Converged Network in Nigeria*, International Journal of Information and Communication Technology Research, 2(11), 829-837.
4. Al-Musawi B. Q. , Al-Shemmary E.J.(2012). *Low Cost VoIP Architecture Using Source Software Component in Tertiary Institutions*. Advances in Computer Science and its Applications, 2(1), 281-286.
5. Umar Wada (2013) *Design and implementation of a Voice over Internet Protocol (VoIP) over local area network (LAN)*. Federal University of Technology Minna, Nigeria.
6. Sang-Jo, Y., Seung-Sun, Y., Gil-cheol, P., and Tai-hoon, K. (2007).*Design of Internet Phone (VoIP) for Voice Security using the VPN*, International Journal of Multimedia and Ubiquitous Engineering. Vol. 2, No. 4, pp 55-65.
7. Ismail, M., N. (2013), *study the best approach implementation and codec selection for VoIp over virtual private network* the international Arab journal of information technology. Vol. 10, No. 2 pp 198-203
8. Lizzie Narváez Designing 802.11 WLANs for VoIP and Data IJCSNS International Journal of Computer Science and Network Security, VOL.7 No.7, July 2007
9. Abdullahi Mohammed VoIP Security: Common Attacks and their Countermeasures *International Journal of Computer Science and Information Security (IJCSIS)*, Vol. 15, No. 3, March 2017
10. Mr. Dhavalparmar, 2 dr. T. P. Patalia “analysis of qos enabled mpls vpn voip network with rip v2 routing protocol”. Journal of information, knowledge and research in computer engineering ISSN: 0975 – 6760 | NOV 12 TO OCT 13 | VOLUME – 02, ISSUE – 02.
11. Mohd Rahul A Comparative Evaluation of Security Aspects of VoIP Technology (IJCSIS) International Journal of Computer Science and Information Security, Vol. 11, No. 2, February 2013
12. Haniyeh Kazemitabar, A Survey on Voice over IP over Wireless LANs World Academy of Science, Engineering and Technology 71 2010
13. Adoption of VoIP <http://epubl.luth.se/1653-0187/2007/003/LTU-PB-EX-07003> SE.pdf
14. VoIP Wireless LAN Survey Final http://www.jaist.ac.jp/~razvan/publications/voip_survey_final.pdf

15. Generating synthetic VoIP Traffic for Analyzing Redundant Open BSD-Firewall
<http://research.iu.hio.no/theses/pdf/master2006/maurice.pdf>
16. Mason, Andrew G. Cisco Secure Virtual Private Network. Cisco Press, 2002.
17. VoIP White Paper
<http://voip.about.com/od/voipbasics/a/qos.htm>
18. M Ozaki, Y. Adachi, Y. Iwahori, and N. Ishii, Application of fuzzy theory to writer recognition of Chinese characters, *International Journal of Modelling and Simulation*, 18(2), 1998, 112-116.

Cite this article as: Muhammad Zaharaddeen Bello, Bello Alhaji Buhari, Bello Aminu Bodinga, & Maniru Malami Umar. (2022). Secure and Optimize VoIP Communication Using QoS Technologies and VPN. *Journal of Network Security and Data Mining*, 5(3), 1–11. <https://doi.org/10.5281/zenodo.7433359>