



(REVIEW ARTICLE)



Design of an asterisk-based VoIP system and the implementation of security solution across the VoIP network

Washima Tuleun *

Independent Researcher, London, United Kingdom.

World Journal of Advanced Research and Reviews, 2024, 23(01), 875–906

Publication history: Received on 27 May 2024; revised on 07 July 2024; accepted on 10 July 2024

Article DOI: <https://doi.org/10.30574/wjarr.2024.23.1.2048>

Abstract

Voice over Internet Protocol (VoIP) is a rapidly advancing technology that facilitates the transmission of voice and audio signals over the Internet or an IP-based network in real-time. This technology has seen a significant rise in demand due to its advantages over traditional circuit-switched telephony, including lower call rates, reduced operational costs, easier management, and enhanced call features. However, the growth in VoIP usage has also increased the potential for various security threats and attacks, jeopardizing the privacy, confidentiality, and integrity of transmitted data. This paper presents the design of an Asterisk-based VoIP system and the implementation of a comprehensive security solution across the VoIP network.

The study involves an in-depth analysis of VoIP technology, identifying its vulnerabilities and addressing potential threats. A security framework is proposed and implemented to safeguard the VoIP network. The designed system and security solutions are rigorously tested and evaluated to ensure robustness and effectiveness. The findings highlight critical security measures necessary for protecting VoIP infrastructures and provide a framework for future research and development in securing VoIP networks.

Keywords: Telecommunications; Cybersecurity; Malware; Phishing; Asterisk; VoIP; Threats; VPN; IPsec; Network Security; Telephony; Codec

1. Introduction

Voice over internet protocol (VoIP) is a technology that enables the transmission of voice signals across the public internet or private network in real time (Hallock, 2004). In much simpler terms, VoIP is the transmission of voice packets over an IP based network in the form of telephone calls, faxes or video conferencing (Stylianios et al, 2009).

The deployment of VoIP technology in enterprise network offers an increased reduction in terms of transport cost in voice back bone networks (MSF, 2003), hence cheaper calls cost, ease of management and also lower operational cost as opposed to the public switch telephony network (PSTN) commonly used today .

VoIP technology is gradually becoming an attractive communication option to consumers given the numerous advantages of the VoIP technology and also the trend towards lower fees and cheaper call rates. However as VoIP usage increases, so will the potential threats and attacks (Matthew Desantis, 2008). VoIP security threats, attacks and vulnerability affects the confidentiality of calls, the integrity and availability of VoIP services.

* Corresponding author: Washima Tuleun

2. Literature review

2.1. History and overview of VoIP

Voice over Internet Protocol (VoIP) technology emerged as a significant innovation in telecommunications, transforming how voice communication is transmitted over networks. The inception of VoIP can be traced back to 1995 when an Israeli company, VocalTec, introduced the first internet softphone (Clegg, 1999). This early VoIP service required users to have a microphone, sound cards, and speakers, utilizing the H.323 protocol for communication.

Initially, the quality of VoIP was subpar due to limited bandwidth and poor modem technology, which restricted its widespread adoption (Putro, 2009). However, the evolution of broadband internet significantly improved the Quality of Service (QoS) for VoIP, leading to its increased popularity and usage. As broadband became more accessible, VoIP services witnessed substantial growth, suggesting the potential for VoIP to eventually replace traditional Public Switched Telephone Network (PSTN) systems (Abbasi et al, 2005).

VoIP, an acronym for Voice over Internet Protocol, leverages internet broadband connections established via satellite or DSL to transport voice signals. This technology enables phone calls to be carried over IP data networks, whether on the internet or within an internal network, making it a versatile communication tool (Balachandran, 2009; Zolfaghari, 2006). The ubiquity of IP-based networks has facilitated the deployment of VoIP-enabled devices in both enterprises and homes. These devices include desktops, mobile IP phones, and VoIP gateways, which not only reduce the costs associated with voice and data communication but also enhance existing features and introduce new functionalities (Gururaj, 2004; Shen & Schulzrinne, 2011).

The growing popularity of VoIP technology is evident among organizations and consumers alike. It serves as a foundational platform for advanced communication applications such as web and video conferencing, which have revolutionized business operations. By integrating telephony and data communication, VoIP provides a cost-effective solution for streaming voice and fax data, marking a significant advancement in the field of telecommunications.

In conclusion, VoIP's evolution from its rudimentary beginnings to a robust communication technology highlights its transformative impact on global telecommunication practices. As broadband infrastructure continues to improve, VoIP is poised to become an even more integral part of our communication landscape, offering enhanced features and greater accessibility.

2.2. How VoIP works.

VoIP technology utilizes a digital switching technology to establish a dedicated link between the caller and the receiver (David et al, 2006). For voice to be transmitted over the network, the caller's voice has to be packetized, which involves the inclusion of headers to the voice data without the routing information (Hallock, 2004) which is completely different from the circuit switched technology according to Dantu et al, 2009.

Several voice samples are merged into a single packet and the packet is switched or transmitted from one hop to another, through the overall network to its endpoint (Morris, 2001). The voice packets are sent through the network one after another sequentially. The packetization process compresses the caller's voice signals, then transfers it across the network to the receiver destination and decompresses it in the same order it was compressed and sent initially (Cobley et al, 2004). This process is done through the use of digital to analog converter, hence generating the signal initially transmitted (La Corte & Sicari, 2006).

Figure 1.0 shows basic end to end components of VoIP and how coding, decoding, packetizing and depacketizing takes place in a simple network.

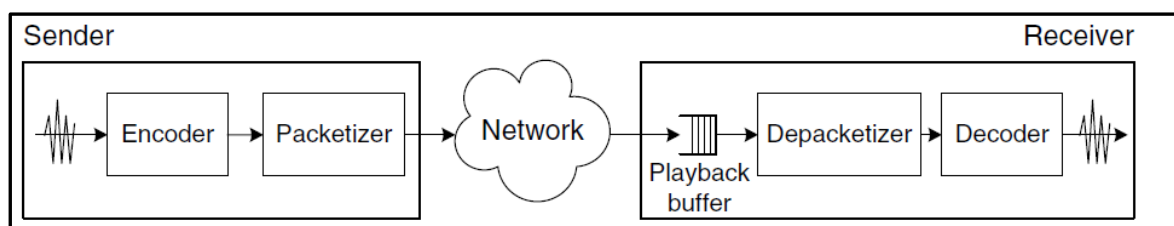


Figure 1 End-to-End Components of VoIP (source: Salah, 2006)

Hughes 2006 and Aramco 2002, summarizes the how VoIP operates between two callers into the following processes shown below;

- ADC converts the analog signal from the caller into digital signal for ending.
- The protocol that are responsible establishing and terminating calls establish a session between the callers.
- Protocols then locate users, negotiate parameters for call setup and end the call when either party hangs up the phone; the most protocols that carry out this task are the SIP and H.323 protocols.
- The bits are compressed to enable transmission across the network.
- The real time content is then inserted into the data packets; the most popular protocol for this process is the real time protocol (RTP) which provides balance between the connections oriented (TCP) and the connectionless protocol (UDP) which is mostly suited for application containing media.
- The media is then compressed using appropriate CODECS so as to reduce the bandwidth consumption needed to transmit packets across the network, consequently lower network congestion and better Quality of Service (QoS).

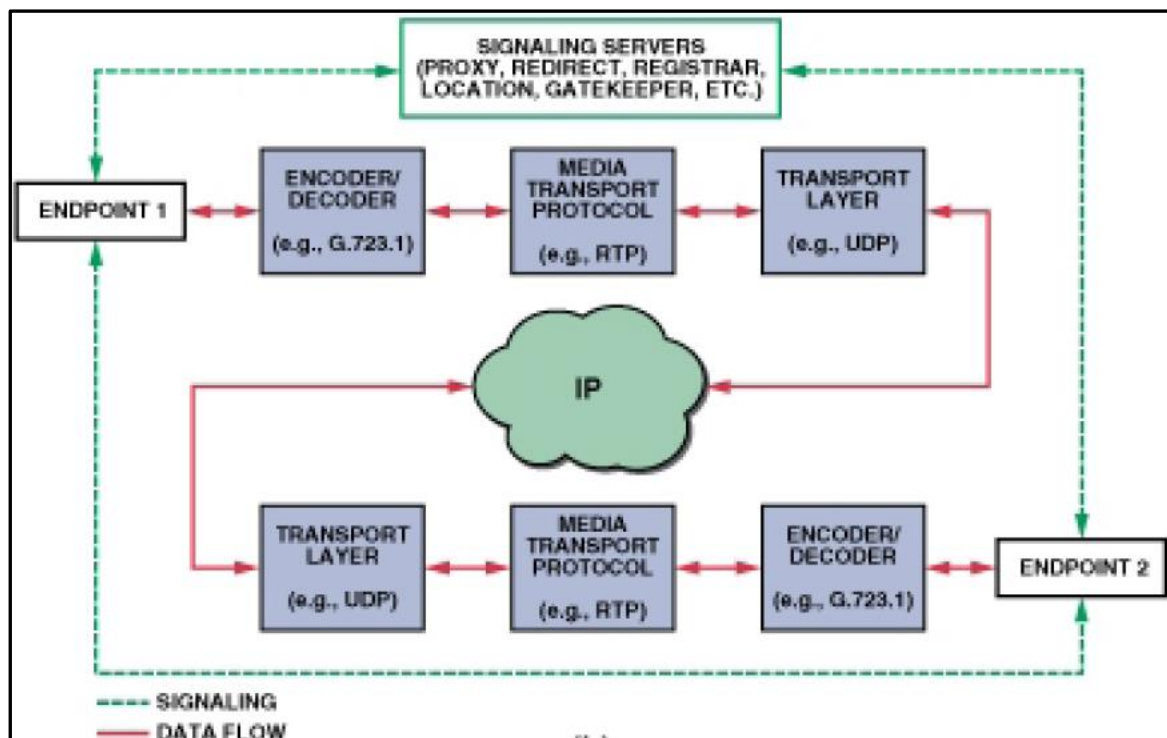


Figure 2 Signalling and transport flows between endpoints (Source: Katz et al, 2006)

According to Miliefsky, 2005, VoIP calls can be done through any of the three ways mentioned below;

- Analog telephone adapter; which involves the use of gateways with existing Analog telephone
- Internet protocol telephone; IP phones are already preconfigured with both software and hardware in built to automatically get an IP address online for making calls
- Peer to Peer VoIP; example of this is Skype, which involves computer to computer internet calls. All that needs to be done is the installation of the software and its proper configuration.

2.3. Benefits and disadvantages of VoIP

There has a plethora of reputable published papers outlining the benefits of Voice over IP system in comparison to legacy phone systems. According to Patrick, 2009, the benefits of VoIP systems are;

- Cost Savings; Long-distance calls over the public switch telephony network are expensive because they are processed using conventional telecommunication lines, unlike VoIP calls that travel over the internet or private network, which have cheap tolls.

- Rich media service and integrated communications; legacy phones provide only Voice and Fax services as against the VoIP technology that has many extended features such as voice and video calls, image transfer, instant messaging among others. (Smith et al., 2018; Johnson & Wang, 2020; Patel, 2022)
- Single Unified Network; with VoIP, voice is transported across the data network, hence not requiring a complete Voice network for its operation.
- Open standards; Gorti, 2006 states that VoIP systems provides the flexibility of integrating with backend systems and also embraces the open architecture.
- User attributes moves with you; your personal user attributes moves with you as soon as you log into any PC , phone, satellite office system or an IP phone from anywhere in the world.
- User control interface; most VoIP service providers grant users the right to control their interface, which is usually in the form of a web GUI. Hence, users can carry changes on features such as call forwarding, speed dial, and music on hold options (Hersent et al., 2010; Kelly et al., 2012; Ozceylan & Koc, 2016).
- Phone portability; VoIP grants users number mobility, virtually using the number anywhere you go as against the PSTN dedicated lines that is not mobile friendly without the hassles of contacting the telephony company for updates.

Even though the pros of using VoIP based services currently supersede the disadvantages, Patrick, 2009 argues that the Cons are still significant and are outlined below;

- Complicated service and network architecture; since different devices are involved in the design of rich media services, it therefore, makes it difficult to design these services on the VoIP system or troubleshoot and diagnose faults. Hence, spending more time and resources testing or deploying services (Patrick, 2009)
- Interoperability issues between different protocols and applications; there are always interoperability issues between products that uses different protocols and also due to the different ways of implementation.
- Power dependency supply/emergency calls; according to Matthew 2008 and Patrick 2009, VoIP services go off in the event of power outage since it depends on power supply for it to function unlike the PSTN telephony system that has backup power supply hence its advantage in the event of emergency service such as 911 calls (Kamal et al, 2011).
- Security issues; Patrick 2009, Hung et al 2006 and Bucher et al 2007 all agreed in their research that security issue is on the rise, since physical access is not needed as in the case of PSTN system, these issues arise since internet is the primary transmission medium for VoIP based services.

Common VoIP services and their components.

There is great similarity between the components of a VoIP network and a circuit switched network according to (Christensen, 2001). VoIP network usually performs more tasks in addition to that been performed by the PSTN including performing gateway functions to the network even though it doesn't require the use of all the network equipment's deployed on the PSTN network (Dantu et al, 2009).

VoIP network comprises of the following basic components;

The network Component. Includes routers, switches, firewalls, cabling, and PBX (Dantu et al., 2009). These components must detect, prioritise, and allow VoIP traffic to reach its destination (Tucker, 2004), reducing latency. The IP PBX switches calls between VoIP and PSTN users, making it vital to the network (Ramachandran, 2006).

Gateways convert voice calls or signals between packet switched and circuit switched networks in real time (Dhamankar, 2005). (Christensen, 2001) divides gateways into three categories namely:

- Media gateways which carries voice signals over IP networks (Radvision, 2002). It detects calls, originates them, and converts analogue to digital voice (Christensen, 2001).
- Media gateway controllers that signal which control, and coordinate the media gateway. Tucker (2004) explains that this component's duties include host searching, resource management, phone number translation, and signal functionality.

End-user equipment; allows network endpoint connectivity. VoIP, soft, and classic phones with audio and video conferencing, instant messaging, and surveillance features may be used by end users (NIST, 2004).

VoIP phones use TCP/IP to communicate with the parent IP network and can be configured manually or using DHCP (Schulzrinc & Rosenberg, 2002). Soft phone software can be installed on a PC and used to make calls online (Matthew, 2008)

2.4. VoIP protocols and codecs

According to Dantu et al, 2009, VoIP protocols are categorized into two main categories namely;

2.4.1. Signalling protocols

- Chak, 2005 defines signalling protocols as protocols that ensure call set up, monitoring, tear down and also setup negotiation, management and modifications. The functions of signalling protocols include Ensures location of users is found, Negotiation of call session and Establishment and management of calls. Karapantazis & Pavlidou (2009) have determined that SIP and H.323 are the most often utilised signalling protocols in the VoIP market. These protocols will now be analysed in detail.
- Session Initiation Protocol (SIP) is an application layer signalling protocol primarily used for establishing, modifying, and terminating multimedia sessions between endpoints (Zhang et al., 2010 and Yoon et al., 2010). The design philosophy and architecture of the system can be considered to have been derived from the hypertext transfer protocol (HTTP) and the simple mail transfer protocol (SMTP), hence guaranteeing its simplicity (Christensen, 2001 and Geneiatakis et al, 2007). Figure 3.0 depicts the SIP architecture.

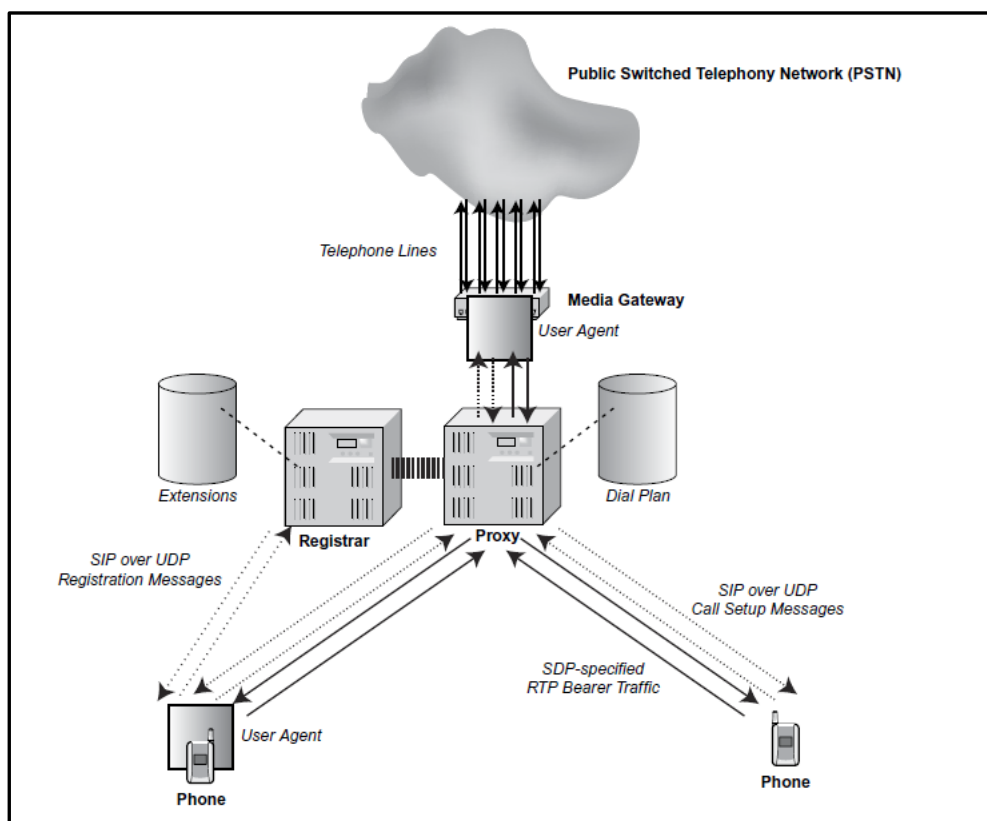


Figure 3 Sip Architecture (Source: Epstein, 2009)

H.323. This protocol establishes a decentralised structure for developing multimedia applications, such as VoIP (Nokia, 2003), and facilitates communication between different devices (Porter, 2007). The protocol in question was created by the International Telecommunication Union. It is largely utilised for ISDN video conferencing systems and toll pass VoIP applications, as stated by (Smith, A., & Jones, B. (2017). Alan et al, in their 2006 study, categorise the H.323 network into the following fundamental components: Endpoints, Gatekeepers that offer signalling services, Multipoint control units that guarantee the accessibility of conferencing services and Gateways. (Brown, D., & Green, R. (2018)

Figures below shows an example of a H.323 call process and its architecture,

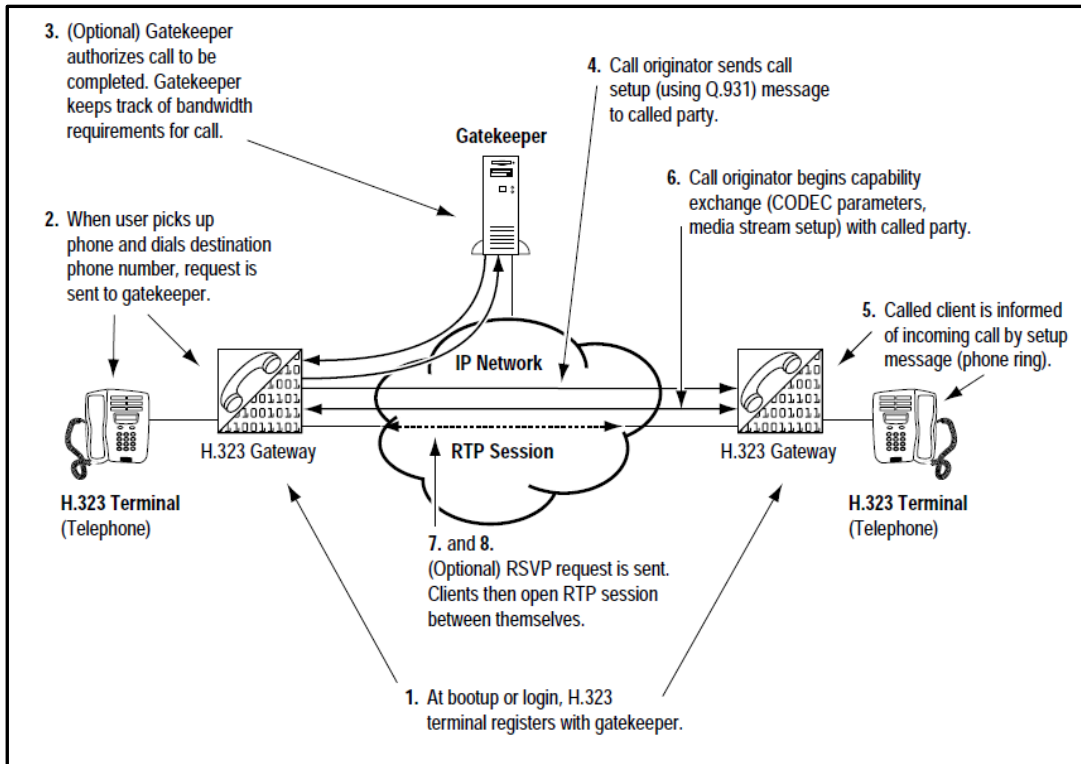


Figure 4 Example H.323 calls process (Source: Christensen, 2001)

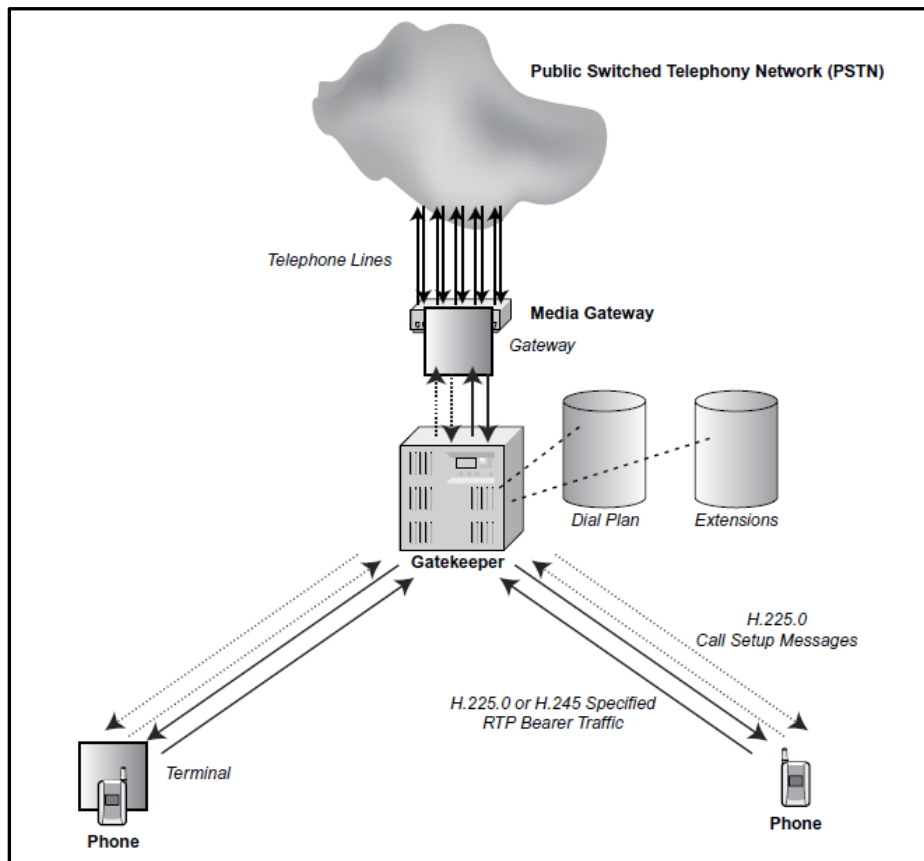


Figure 5 H323 network architecture (source: Epstein, 2009)

2.4.2. Media transport protocols

Dantu et al. (2009) state that media transport protocol controls voice sample encoding, decoding, digitization, and ordering for real-time communication. Media transport protocols, such as real-time and real-time control protocols (Buses et al, 1996), will be examined here.

- The real time protocol is designed to transmit real-time audio or video data over a user data protocol (UDP) (Schulzrine, 2003), however it does not guarantee real-time delivery (Chak, 2005). RTP offers features such as identifying payload type, sequence number, monitoring data transmission, and time sharing (Christensen, 2001).
- The Real Time Control protocol (RTCP) provides feedback on the quality of service of transmitted data disseminated using real-time protocols (Christensen, 2001). RTCP monitors VoIP issues such latency, delays, and jitters and communicates control information (Katz et al, 2006).

(Cao et al, 2008) defines CODEC as an algorithm that is used to encode and decode voice streams across a network. Encoding is done to enable the voice signal which is Analog to be digitalized and transmitted across the network.

2.5. VoIP Codec

At the receiver’s end, the signal needs to be decoded, hence its conversion back to Analog stream. The digitization of voice streams is categorized into two processes: sampling and quantization (Aloqaily et al., 2019; Proakis & Manolakis, 2007). Table 1.0 shows the common VoIP CODEC which are the most popularly used today (Peters, 2000)

Table 1 Common VoIP CODEC used (Source: Putro, 2009)

Codec	Comments
G.711	Delivers precise speech transmission needs at least 128 kbps for two way
G.722	Adapts to the varying compressions and bandwidth is conserved with network congestion
G723.1	High Compression with quality audio. Lot of Processor power
G.726	An improved version of G.721 and G.723 (difference from G.723.1)
G.729	Excellent bandwidth utilization. Error tolerant. License required

2.6. VoIP security threats, attacks, and vulnerabilities

Security of users can be analysed from different perspectives, but analysis will be based on the threats, attacks and vulnerabilities in VoIP network. According to Patrick, 2009 VoIP network has two major types of vulnerability which are listed below;

- Vulnerability from the inherent infrastructure such as the operating system (Wang et al., 2019; Richardson et al., 2018)
- Vulnerability from VoIP protocols and devices currently deployed such as signalling controller and media server (Chen & Tang, 2020; Makhija et al., 2021)

Zisiadis et al 2009 and Kuhn et al 2005 categorized the VoIP threats into the following;

- Threats against availability
- Threats against confidentiality
- Threats against integrity

2.6.1. Threats against availability

These threats aim at disrupting services in the VoIP network, hence breaking down availability of service to consumers, typically in the form denial of service (Patrick, 2009). Cisco 2007 and Xin 2007 list the following threats against availability;

Call flooding. This is the valid or invalid flooding of heavy traffic to a target system (Patrick, 2009) which drops or breaks down such a system. Figure below shows a call flooding example.

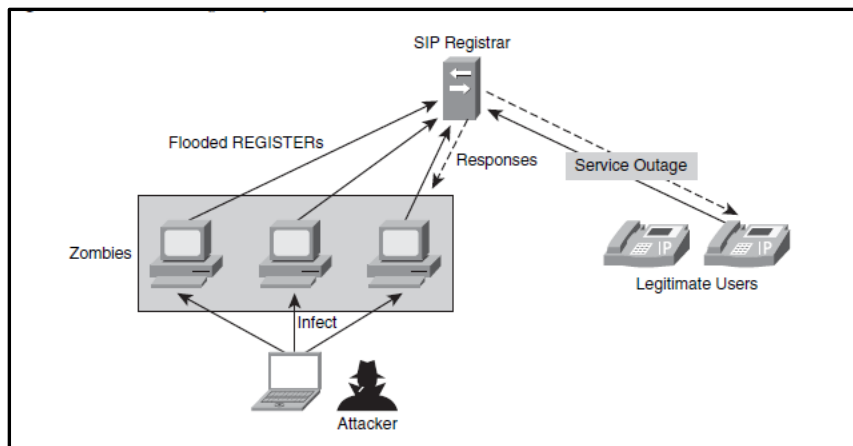


Figure 6 Call flooding example (source: Patrick, 2005)

- Call hijacking. This occurs when communication between two parties is taken over by an intruder (Patrick, 2009). This form of attack could either be registration hijacking in which the attacker monitors the registration process between a user and a server, then sending a spoof message and automatically hijacking the session.

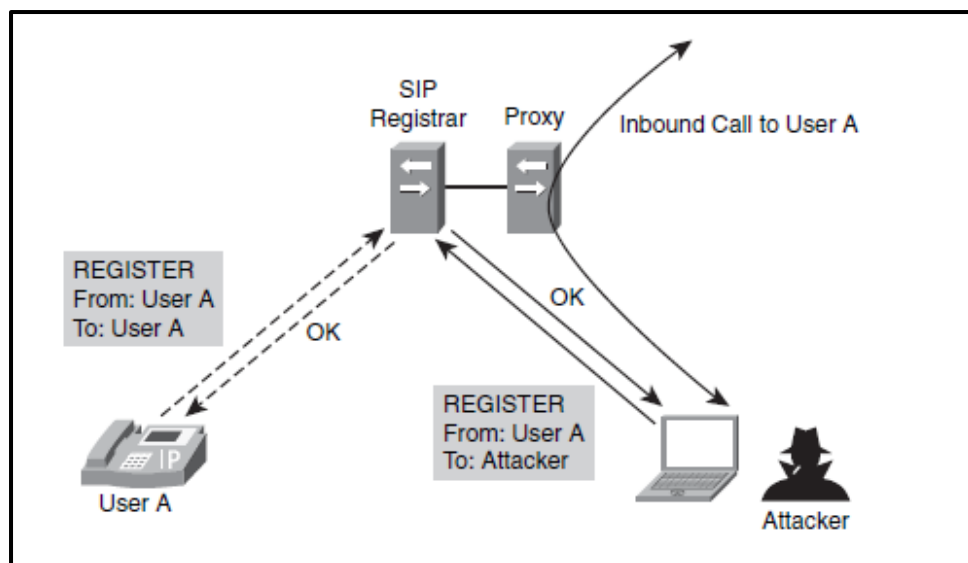


Figure 7 Registration session hijacking (source: Patrick, 2005)

- Spoofed message. This kind of attack occurs when an intruder inserts fake message into certain VoIP session with the intention to disrupt or steal from the network (Ransome et al, 2005). Examples of spoofed messages are call tear down and toll fraud Mohammad, R., & Mazleena, B. (2011).

Call tear down occurs when an attacker monitors a conversation between unsuspecting parties, obtaining SIP information and sends a termination message to either party which abruptly ends the call. (Chen, P., & Davis, N. (2006)

- Server impersonation. This occurs when an attacker compromises the DNS servers, replacing its IP address with that of the attackers address, hence redirecting all mobile devices trying to connect to the server to its malicious server. Figure below shows a server impersonation example.

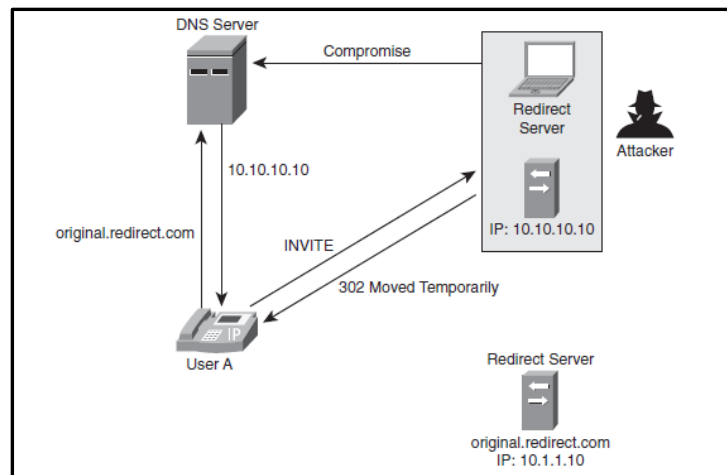


Figure 8 Server impersonation (source: Patrick, 2005)

2.6.2. Threats against Confidentiality

This threats are aimed are stealing caller identities and credentials of users for future attacks. According to Kuhn et al, 2005, the following are the threats under this category;

- Eavesdropping media. In this category, the attacker eavesdrop on a victim’s communication. This is not on the PSTN network which requires physical access to the PSTN devices but in the case of VoIP based network, the attacker can sniff packets in the user’s network domain or compromise the victim’s device (Stalling, 2006).
- Impersonation of a user on the network. This attack occurs when the intruder disguises and presents itself to the network as an authorized and legitimate user white the sole aim of stealing services and causing disruption (White et al, 1996).
- Call pattern tracking. According to VOIPSA, 2005, call pattern tracking can be defined as the unauthorized analysis of any traffic on the network. It is mainly used for discovering caller identity, presence and location with the sole aim of stealing, extorting or even phishing (Patrick, 2009)

2.6.3. Threats against integrity

The alteration of message after it has been intercepted by intruder leads to threats against its integrity (VOIPSA, 2005). Patrick, 2005 categorizes this threats into the following:

- Message alteration. In the case of message alteration, the intercepted message is reconfigured with the sole aim of rerouting such information to another destination (Patrick, 2005). Examples of these threats are call rerouting and black holing According to VOIPSA, 2005, call rerouting has to do with redirecting the IP after its interception to another location while black holing has to do with complete interruption of the communication with sole aim of terminating
- Media alteration. The source message is replaced by the attacker such that the receiver can either hear an advertisement, noise or even silence at times

Threats against social context; this threat aims at falsifying either of the communication party’s identity by the intruder with the sole aim of misrepresenting himself as a trusted party to ensure and convey false information to either party (Patrick, 2005).

Examples of this threat include misrepresentation, phishing and sending of spam messages (VOIPSA, 2005). Table shows various forms of VoIP attacks by intruders and their countermeasures

Table 2 Countermeasures against VoIP threat and attacks

Attacks	Countermeasures
Eavesdropping	Encryption of voice packet can be used to protect against eavesdropping. The entire packet can be encrypted with the use of IPsec. (Xin, 2007). Virtual VLAN can be used (Cisco, 2007)
Unauthorized Access attack	By avoiding the use of text as remote access control, SSH can be used instead. Physical access control is extremely relevant, the use of up to date intrusion detection scheme and IPsec VPN tunnels are vital (Shikfa et al., 2010).
Switch default password	Every default password should be changed during switch default setup and remote access to GUI (graphic user interface) has to be disabled (Xin, 2007).
Wiretap	A tough security policy has to be established, the IP phone hub should be disabled, and a good alarm system should be introduced which would signal the network manager whenever a phone is unplugged, and IPsec VPN can also protect the traffic from unauthorized people (Xin, 2007)
Web server interface	By using a HTTPS (Hyper Text Transfer Protocol secure) server instead of HTTP for remote administration (Xin, 2007)
IP Phone net mask	By introducing a firewall filtering mechanism. (Kuhn et al, 2005)
Impersonation of a user to the network	Use of strong authentication Schemes (Stalling, 2006)
Impersonation of a network to a user	Can be prevented by deploying firewalls, since no traffic can enter the network without passing through the firewalls. And by implementing IPsec VPNs (Kuhn et al, 2005)
Man in the middle attack	Can be prevented by deploying firewalls, since no traffic can enter the network without passing through the firewalls. And by implementing IPsec VPNs (Kuhn et al, 2005)
Caller Identification Spoofing	Traffic should be filtered based on frequency and duration (Cisco, 2010). Not trusting any caller ID at all is a better way of preventing this.
Registration High jacking	By using VoIP vulnerability scanning Tools like SIVUS
Proxy Impersonation	By using strong authentication schemes
Call redirection or high jacking	Implementation of strong authentication schemes and use of access list (Stalling, 2006)
Denial of Service	Strong Authentication, physical security, backup power plans and virtual LAN should all be introduced (Cisco, 2007)
Packet Spoofing	An effective authentication scheme and encryption of packets (IPsec) (Shikfa et al, 2010)
Theft of Service	VoIP providers can avoid theft of service by properly configuring firewalls, protecting ports, making use of Virtual LAN and VPNs (Cisco, 2007)

2.7. Best practices for VoIP security and deployment

A comprehensive strategy based on sound security measures will provide best practical solution to the increasing threats against VoIP based network (Ransome et al, 2005). The following are some of the best practices to safe guide against VoIP based threats and attacks (Ramirez, 2007);

- Network Address Translation; network address translation can be defined as a tool used for the conversion of private IP addresses into public IP address for use over the internet and in the process concealing the internal private IP address from the public network (Cao & malik,2006).

According to Casteel 2005 and Tucker 2004 research done, Network address translation brings an added level of security to the network while also assisting with the issue of IP address limitation.

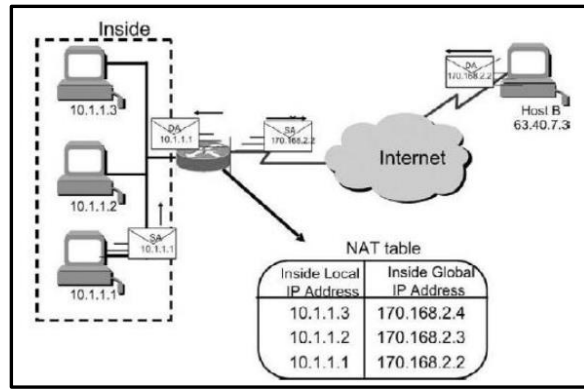


Figure 9 How NAT works (Source: Lammle, 2006)

- Firewall deployment; According to Onofre et al, 2010 and stalling 2006, firewall is a network device place at the network boundary or border to carry out traffic filtration and analysis, hence protecting the network against attacks by intruders.

Kuhn et al, 2005 states that if firewall is properly deployed on the network, it can prevent and protect the network from unauthorized access and also carry out traffic and packet filtering. Figure below shows a firewall deployment scenario

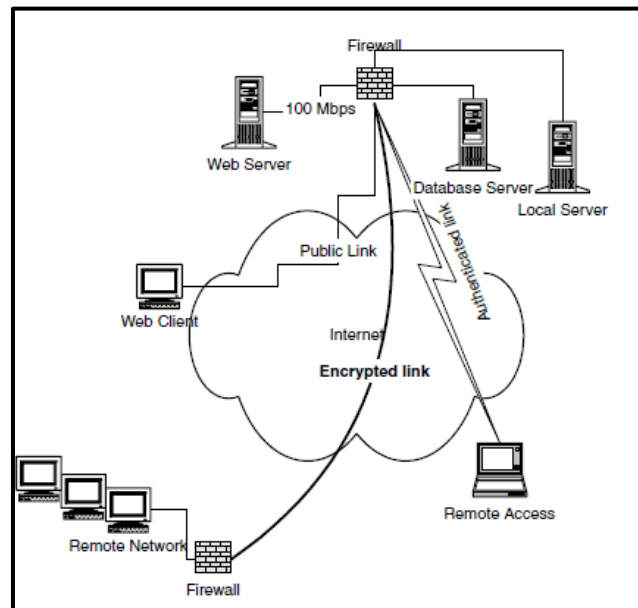


Figure 10 Firewall deployment scenario (Source: Cisco, 2006)

Wang 2004 categorized firewall into three namely;

- Packet filtering firewall; which is deployed on the internet protocol layer and most importantly it's configured in a way to allow traffic in both directions.
- Application level gateway firewall; which operates at the application layer.
- Circuit level gateway firewall; which is deployed on the transport layer of the OSI model stack

2.7.1. Virtual Private Network

This is a private network that is built on an existing network with the sole aim of providing a secure channel of data transmission between networks (Frankel et al, 2005). The transmitted data is encrypted across the network to its endpoint (Sinha, 2003).

Cisco 2006 described VPN as a medium that provides private network services over a public network, for example the internet. Lammle 2007 in his research study states that the VPN ensures guaranteed and secured transmission of the

data across the network in a timely manner. The transmitted data is encrypted, ensuring its security away from intruders and attackers (Rufi, 2007).

Fung, 2005 classifies VPN into the following categories;

2.7.2. Site to site VPN

This ensures that the connection between two sites is secured by the use of tunnelling. The figure below shows the head office connected to the branch office via a VPN tunnel.

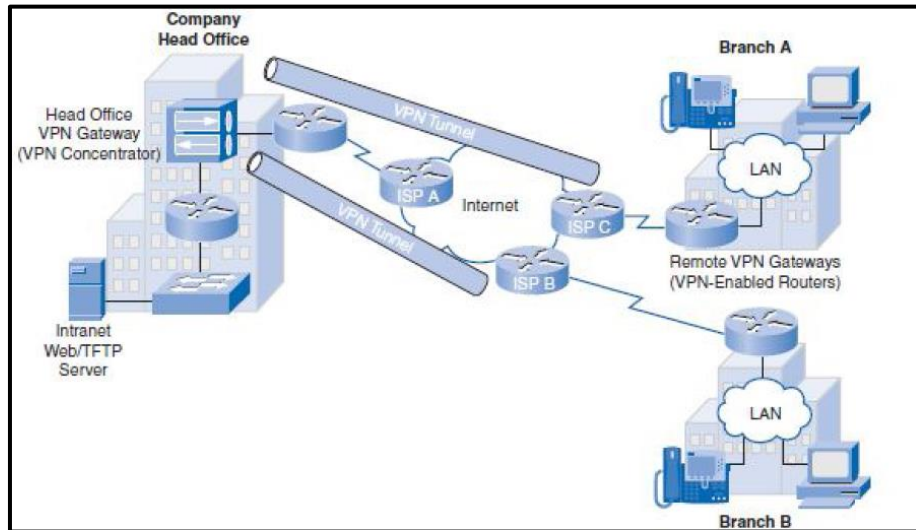


Figure 11 Site to site VPN connection (Source: Fung, 2005)

Remote access VPN; this allows remote users to access the head office once they have the required log in details required and also password after authentication (Fung, 2005). Figure below shows the remote access VPN.

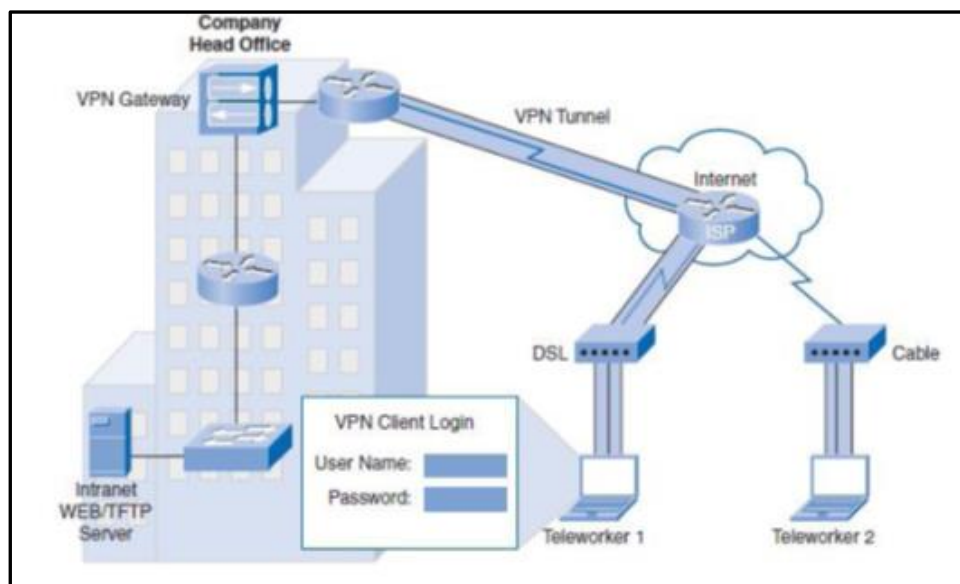


Figure 12 Remote access VPN (Source: Fung, 2005)

Vendors recommended the creation of protocols to authenticate, encrypt and decrypt the data transmitted across the network as attacks increased on transmitted data, hence ensuring a secured VPN.

Cisco 2006 states that creation of stronger tunnelling and the use of encrypting algorithm strengthen security across the network. Examples of a secured network are;

- IPsec VPN
- Secure Socket Layer VPN

IPsec VPN provides a high level of security that encompasses confidentiality, authentication and integrity of the transmitted data (Sampalli et al, 2022). IPsec VPN ensures that data transmission is highly encrypted either using the data encryption standard (DES) which has 56 bit key length or the 3DES (triple DES algorithm) which has a stronger 168 bit algorithm or even a stronger Advanced encrypted system with 256 key length (Cisco, 2004).

According to Cisco 2006, with the deployment IPsec VPN, little or no change on the network infrastructure needs to be made since it offers high security with low operational cost. Figure shows Packet Encapsulation, Encryption and Tunneling in a network.

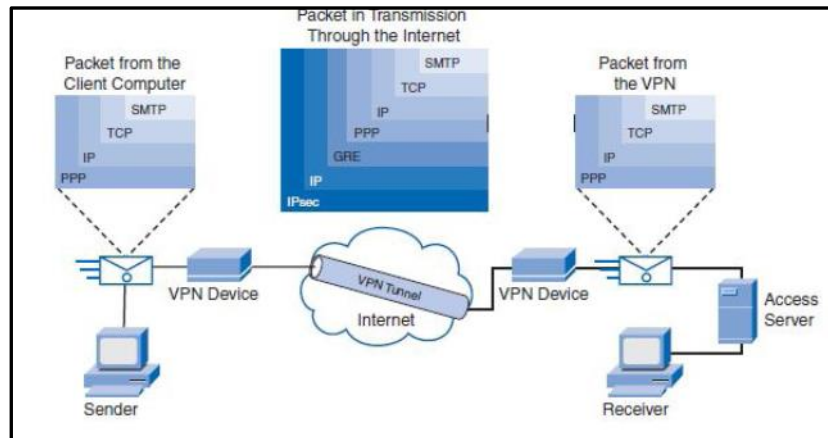


Figure 13 Packet Encapsulation, Encryption and Tunneling in a network (Source: Fung,2005)

The secure socket layer (SSL) VPN is mostly associated with the web based applications (Dierks et al 1999). According to Frankel et al, 2008, the SSL VPN is dependent on internet access and it supports other applications like HTTP, SMTP. Cisco 2006 states that SSL VPN generates a 49 bit key length for authentication between client and server.

From the literature review, there are different methodologies for the implementation of a security solution across a VoIP based network. Even though there has been a plethora of reputable published papers describing various methodologies for securing a VoIP based network.

But based on the review, it has been narrowed down the Network address translation deployment, firewall deployment and Virtual private network.

In as much as the above methods offer different foci, implementation strategies, they also offer some weakness which has to be critically analysed to avoid loop holes in a network design, thereby giving room to unauthorized access by intruders.

3. Design and methodology

The methodology adopted is based on outlining the technical requirements for carrying out the design and implementation of the network design, the VoIP dial plan and numbering system was also designed, VoIP design methods and the choice of the design tools to be made use of was analysed. In addition, secondary data sources such as research papers, publications, and internet and journal newspapers was used for descriptive sections of the research.

Several factors were taken into consideration from the in depth literature review before the implementation design methods was adopted. Factors ranging from the Quality of service issues in Voice over IP networks, security considerations and concerns was analysed in depth and critically.

The design choices after critical analysis of the different technologies which can be used as there was a plethora of published papers with different views regarding the different VoIP and Security technologies which can be implemented.

The session initiation protocol (SIP) was critically compared with different protocols which could equally be deployed in the VoIP telephony design especially the H.323 protocol and it was found to be the best option at the moment for the implementation of the project which is also backed up by Karapantazis & pavlidou, 2009, stallings 2003, Schulzrine & Rosenberg 2002 and Yoon et al 2010. Another reason for the choice of the SIP as against the H.323 protocol is the ease of its implementation as against the complex H.323 and it has a lot of online support.

Requirements for the VoIP telephony network design.

The requirements of the based design aspect are listed below;

- Design of an asterisk VoIP based system
- Design and integration of a voicemail service system in the Asterisk PBX
- Design of a suitable dial plan for the two network site locations
- Design and integration of a security solution across the network

3.1. Branches with their offices and number of extensions needed

In this research, the list of offices and departments present in the two locations i.e. Lagos and Abuja are given below. This will be very important in the design of the dial plan since it's the major playing factor in the choice of the numbering system to be chosen. During the implementation phase of the project, soft phones were preferred to the hard phones due to the limitation and availability of the required number of hard phones. The table below shows the number of extensions and department in each network branch.

Table 3 Number of extensions needed for both the Lagos and Abuja branches

SN	Department	Number of extensions in Lagos branch	Number of extensions in Abuja Branch
1	Administration	12	15
2	Accounting	8	6
3	IT/Engineering	22	28
4	Sales	15	11
5	Legal	5	6

3.2. Design of the dial plan and numbering system

For any telephony network to be successfully designed and built in an organisation there has to be a dial plan system for that to happen. According to Mahler, 2004 dial plan determines the call routing and processing.

Meggelen, 2207 stated that dial plan is very important since it handles the inbound and outbound calls in the network through a set of instructions that asterisk have to follow. The extension requirements will be needed before the dial plan can be fully implemented and operational, which will be covered in later sections of this chapter.

Table 4 Dial plan table

Department	Abuja Extension Numbers	Lagos Extension Number
Administration	1101 - 1199	2101 - 2199
Accounting	1201 - 1299	2201 - 2299
IT/Engineering	1301 - 1399	2301 - 2399
Sales	1401 - 1499	2401 - 2499
Legal	1501 - 1599	2501 - 2599

A four digit dial plan is made use of in the implementation of the project and numbering system. The reason behind this is to give a greater room for expansion of the organisation should the need arise, without designing a totally new and different dial plan numbering system and also for scalability purposes.

The first digit on the 4 digit dial plan specifies the organisation's general number. For the Abuja branch the numbering system will be 1XXX while that of the Lagos branch will be 2XXX. The second digit specifies the department, for instance Admin department in the Abuja branch will be -X1XX, Account department will be X2XX and so on.

Based on the numbering system, identification of department will not be an issue since it can easily be done with ease. The table below shows the dial plan for both the Lagos branch and the Abuja branches of the network.

3.3. Methods and tools used for the design

The following are the design tools and methods used in the design of the VoIP telephony network and the implementation of a security solution across the network.

- Asterisk IP PBX; The choice of the asterisk was made since it was requested by the client and also since it's an open source, it will be cost effective to deploy, easy to manage, easy access to support as against propriety software, ease of management, little or no complexity in the configuration of the asterisk PBX to include addition features such as auto attendant, voice mail, call conferencing among others. The asterisk implements communication using software rather than hardware, hence the ease of including additional features; it also runs on the Linux based operating systems.
- Session initiation protocol (SIP); this protocol was chosen for the design due to its numerous advantages, ease of implementation as opposed to other protocols that could also be used for instance the H.323 protocol (Stallings 2003, Yoon et al 2010). For more details regarding the choice of the SIP protocol, an in depth analysis of this protocol is in the literature review of the dissertation.
- IPsec VPN; This offers a strong form of security in the form of encryption, encapsulation of packets and tunnelling during the transmission of data across the network according to Frankel et al, 2005. comparison was made between the IPsec VPN, Secure socket layer (SSL) VPN, firewall deployment and it the adoption of the IPsec VPN was done since its more advantageous and stronger in comparison to the other security methodologies. This is also supported by research done by reputable authors like Rowan 2007, Sinha, 2003.
- Four Digit Dial plan Numbering system; this was chosen to give room for growth and also because of its scalability as opposed to the three digit numbering system. It's important to leave room for growth in the design of network according to Chong & Mathews, 2004.
- Voice mail design; the voicemail design ensures a message is dropped when the person called is unavailable. It is used for leaving a message if no one answers the call or is unavailable for any reason. This configuration of the voicemail is achieved by inserting the appropriate settings in the Voicemail.conf file present in the etc/asterisk folder on the asterisk server.

4. Security implementation across the asterisk-based VoIP network

There is the strong need to ensure the security of the VoIP network against unauthorized entry by malicious users. There has been a plethora of reputable published papers detailing and critically analysing the different security solutions that can be implemented across the network. The adoption of the IPsec VPN as against the other security solutions for implementation is based on the numerous advantages it has over others, some of which include but not restricted to;

- Encryption and tunnelling allow secure voice packet transmission over the network, enhancing data security and confidentiality. Even if the network is compromised, only the endpoint receiver can decrypt voice packets.
- It is also more scalable, flexible and reliable as opposed to the other security solutions
- It is cheaper and easier to deploy as opposed to other security solutions and its maintenance and running cost is low

The IPsec site-to-site VPN was chosen for this project due to its ability to maintain confidentiality, site to site security and anonymity. AES encryption was selected for the project. IPsec VPN ensures safe data transit between crypto-enabled peers hence ensuring a secure data transfer between the different peers. Peterson (2006) states that IPsec includes two protocols for better security: the Authentication header and Encapsulation Security Protocol (ESP) and the Internet Security Association and Key Management (ISAKMP). To ensure the proper security of the transmitted data,

the use of a symmetrical encryption algorithm and the internet key exchange mechanism for safe exchange of keys is recommended (Izadinia et al 2006).

This security method completely prevents packet eavesdropping and alteration. Network administrators can modify Hashed Message Authentication codes to enhance setting strength. The IPSec VPN ensures sender-receiver authentication, ESP protocols assure data confidentiality, and AH protocols maintain integrity. Xenakis (2006).

4.1. Implementation and Testing

It covers the installation of asterisk, implementation method, the IP addressing scheme, starting up and shutting down asterisk, security implementation and finally testing of the design to ensure its fully functional and operational.

4.2. Tools used for design implementation

The design of the VoIP telephony solution was done making use of both soft phones and hard phones to ensure full compatibility of both the soft phones and hard phones with the project design. Below is the list of tools and methods used;

- Fedora operating system; which is the plat form in which the asterisk PBX will be run on. The software can be gotten from fedora website (www.fedoraproject.org). Although any Linux distribution can also be made use of; Kubuntu/Ubuntu, Fedora or Mandriva would also work fine.
- Session initiation protocol (SIP); this protocol was specifically adopted for the design since most products in the market as of today as SIP compliant as against the other protocols especially IAX2. The SIP protocol is a standard since it was designed by Cisco and is reliable and stable.
- Asterisk which is an open source; this software transform an ordinary computer into a communication server. To fully understand the power of asterisk, one requires the knowledge of Linux, telephony, basic script programming and also networking.
- Astra IP Hard phones (9133i model); used for the calls between the two servers and also for the configuration of the Voicemail and auto attendant system
- X-lite 4 soft phones; to test for its compatibility with the design
- IPsec site-to-site VPN; this was also implemented across the VoIP telephony network
- Four digit dial plan; this was used in the design of the dial plan numbering system for the asterisk PBX. This was chosen to give room for the company's expansion or growth; hence accommodating more extensions
- Cisco Routers 2800 series
- Cisco 2950 switches
- PC systems

4.3. IP addressing scheme

The IP addressing scheme used for the design of the network is a Class C addressing scheme as requested by the client. The table below shows the addressing scheme

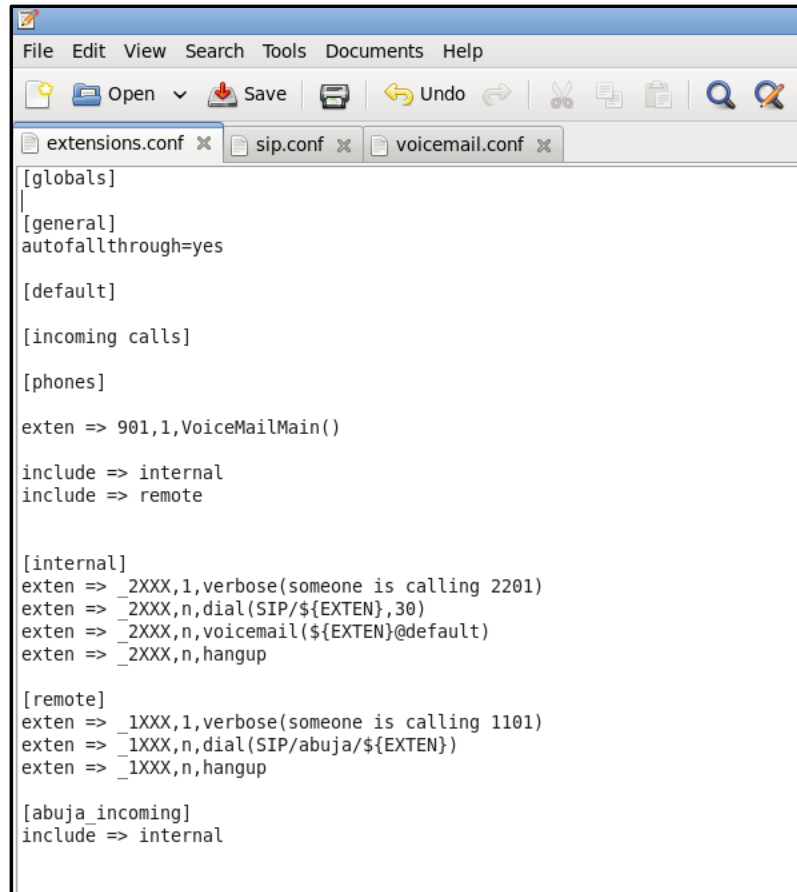
Table 5 The IP addressing scheme for the project design

SN	Description	Abuja Router	Lagos Router
1	Serial Interface IP address S0/0/0	192.168.1.1/24	192.168.1.2/24
2	Fast Ethernet IP address F0/0	192.168.2.1/24	192.168.3.1/24
3	1 st extension IP address	192.168.2.2/24	192.168.3.2/24
4	Network IP address	192.168.2.0/24	192.168.3.0/24
5	IP PBX IP address	192.168.2.3/24	192.168.3.3/24
6	1 st host system address	192.168.2.4/24	192.168.3.4/24

4.4. Asterisk and VoIP phone configurations

Appendix A contains the configurations and CODECS used in the design of the VoIP system. Although in depth discussion into the different configuration files will be done in the sections below:

Extension.conf: This file is one of the most used files in the configuration of an asterisk PBX system. This is because it contains the dial plan which defines and handles how calls come in, go out and are also routed. The behaviour of the PBX connection can be configured in the file. This made of either sections or contexts which will be analysed in depth. The figure below shows the Extension.conf file in the design of the VoIP telephony network.



```

File Edit View Search Tools Documents Help
Open Save Undo
extensions.conf x sip.conf x voicemail.conf x
[globals]
[general]
autofallthrough=yes
[default]
[incoming calls]
[phones]
exten => 901,1,VoiceMailMain()
include => internal
include => remote
[internal]
exten => _2XXX,1,verbose(someone is calling 2201)
exten => _2XXX,n,dial(SIP/${EXTEN},30)
exten => _2XXX,n,voicemail(${EXTEN}@default)
exten => _2XXX,n,hangup
[remote]
exten => _1XXX,1,verbose(someone is calling 1101)
exten => _1XXX,n,dial(SIP/abuja/${EXTEN})
exten => _1XXX,n,hangup
[abuja_incoming]
include => internal

```

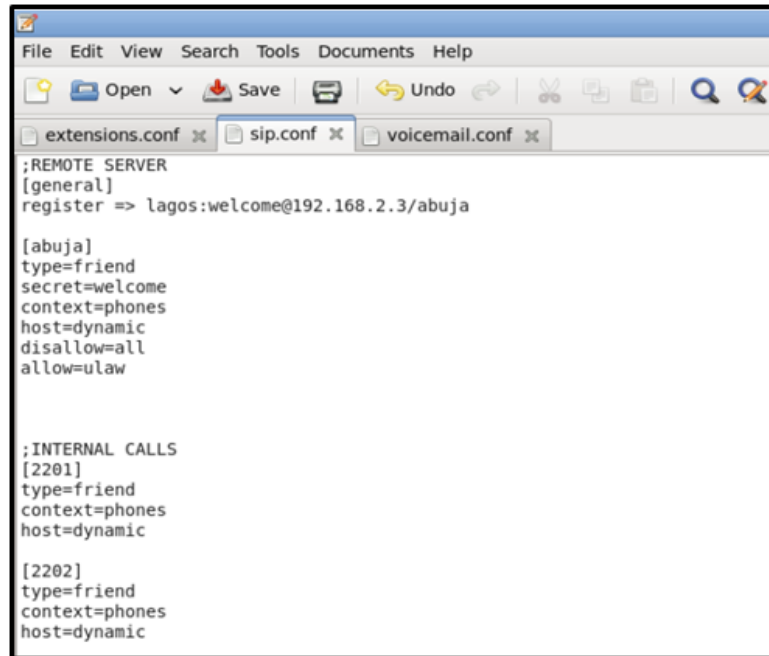
Figure 14 Extension. conf file

The Extension.conf file is usually located in the etc/asterisk directory as the case may be. Dial plan can be categorized into three main concepts namely;

- Contexts. The main purpose of the contexts in an Extension.conf file is to keep the different parts of the dial plan from interacting with one another. They are denoted by placing the name intended for use in a [] bracket. At the beginning of an Extension.conf file, two context are named; the [general] context and the [globals] context.
 - The context also provides some level of security by either permitting or denying a caller's access to certain features. All the instructions placed after the [general] context are part of the context unless another context is specified. The [general] section usually contains a set of dial plan settings which are usually default settings. The autofallthrough=yes tells the asterisk to continue running the configurations even when the extension doesn't have anything to do.
- Extensions. This defines the step that is taken by asterisk to see the call through. It follows the steps defined by the extension. This happens when a particular extension is triggered; asterisk tends to follow the steps defined for that extension. An extension comprises of three components: The name, priority and application. These components are separated by commas as shown in an example below; exten => name,priority,application()

- Priority. This can be defined as multiple steps in an extension which are normally executed sequentially, for example; *exten => 123,1,answer()* *exten => 123,1,hangup()*. First priority 1 is to answer the call followed by priority 2 to hang up the call
- Application. This is defined as the work horses of the overall asterisk dial plan each performing its specific function, for example answering a call, dialling a number, playing a sound or hanging up a call. Some of the applications include *answer()*, *hangup()*.

SIP.conf. This is where the configuration of the SIP protocol is carried out. The authentication of the users and end points including SIP phones is configured in the SIP.conf file. The file is usually used for the determination of calls to be answered or rejected by the user by the asterisk PBX. The figure 4.2 below show the SIP.conf file used for the asterisk PBX Configuration.



```

File Edit View Search Tools Documents Help
Open Save Undo
extensions.conf x sip.conf x voicemail.conf x
;REMOTE SERVER
[general]
register => lagos:welcome@192.168.2.3/abuja

[abuja]
type=friend
secret=welcome
context=phones
host=dynamic
disallow=all
allow=ulaw

;INTERNAL CALLS
[2201]
type=friend
context=phones
host=dynamic

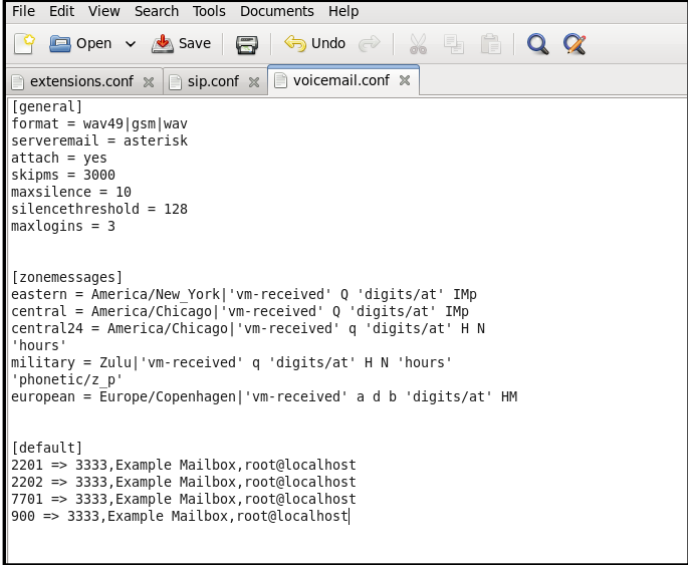
[2202]
type=friend
context=phones
host=dynamic

```

Figure 15 SIP. conf configuration file

The explanation of the SIP.conf file is detailed below

- [abuja]; the content of the context is then name of the SIP device which could also be the extension number
- Type = friend; since asterisk PBX is designed for both calls to be placed to the phones and received as well, the type is defined as friend. The other options that can be set under type are;
 - User; which is mainly for calls leaving the dial plan which is usually through the Dial () application. The type friend is preferred since it defines both the user and the peer.
 - Host; this option is used to define the users or clients that exist on the network. The host can be defined either using static IP address or can be set as dynamic in which case the SIP phone is configured to register. The asterisk PBX receives a REGISTER packet telling it which IP address the SIP peer is using.
 - Secret; this sets the password that has to be entered before a client is added to the network. This option also secures an untrusted network by forcing the use of password (*secret=password*). This creates a password for the user authentication on the asterisk PBX
 - Context = phones; this defines the dial context for the user which in this case is phone
- Voicemail.conf. This file contains settings used for configuring and customizing Voicemail to meet specific requirements and needs. Voicemail context is used to separate different mail box sets from each other. The Voicemail.conf file is divided into three sections as shown below;
 - [general] which contains the global configurations of the Voicemail.conf file
 - [zone messages]; this section deals with corresponding the different time zones together with the local time zones. This is due to the time difference
 - Context defined



```
File Edit View Search Tools Documents Help
Open Save Undo
extensions.conf x sip.conf x voicemail.conf x
[general]
format = wav49|gsm|wav
serveremail = asterisk
attach = yes
skipms = 3000
maxsilence = 10
silencethreshold = 128
maxlogins = 3

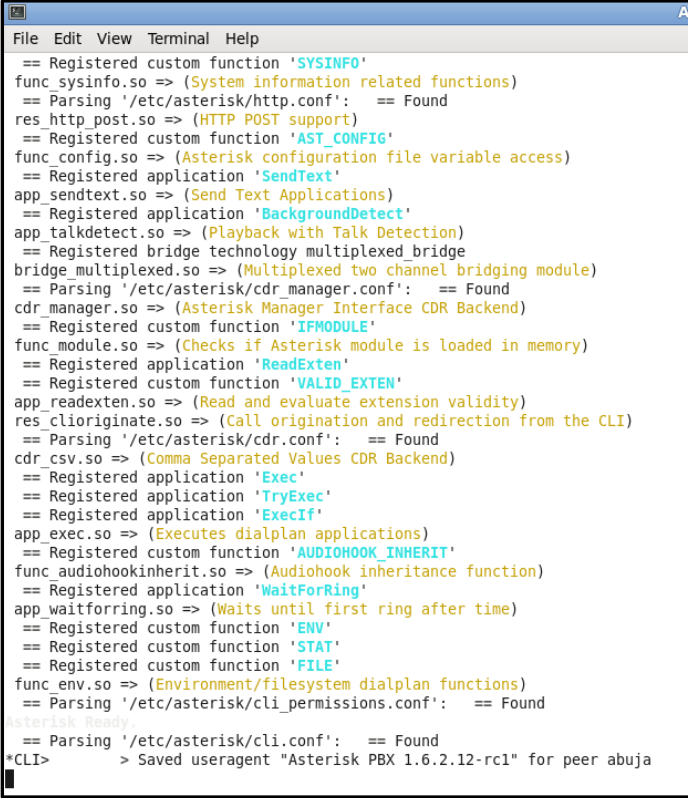
[zonemessages]
eastern = America/New York|'vm-received' Q 'digits/at' IMp
central = America/Chicago|'vm-received' Q 'digits/at' IMp
central24 = America/Chicago|'vm-received' q 'digits/at' H N
'hours'
military = Zulu|'vm-received' q 'digits/at' H N 'hours'
'phonetic/z p'
european = Europe/Copenhagen|'vm-received' a d b 'digits/at' HM

[default]
2201 => 3333,Example Mailbox,root@localhost
2202 => 3333,Example Mailbox,root@localhost
7701 => 3333,Example Mailbox,root@localhost
900 => 3333,Example Mailbox,root@localhost
```

Figure 16 Voicemail.conf File

The syntax for defining a mail box is mailbox => password, name,[email,pager_email [options]]] where the mail box number corresponds to the extension number associated with it. Password is that which is assigned to the mail box by the user to have access to the mail box which is usually automatically updated by the asterisk PBX in the Voicemail.conf

4.5. Starting and shutting down an asterisk server



```
File Edit View Terminal Help
== Registered custom function 'SYSINFO'
func_sysinfo.so => (System information related functions)
== Parsing '/etc/asterisk/http.conf': == Found
res_http_post.so => (HTTP POST support)
== Registered custom function 'AST_CONFIG'
func_config.so => (Asterisk configuration file variable access)
== Registered application 'SendText'
app_sendtext.so => (Send Text Applications)
== Registered application 'BackgroundDetect'
app_talkdetect.so => (Playback with Talk Detection)
== Registered bridge technology multiplexed bridge
bridge_multiplexed.so => (Multiplexed two channel bridging module)
== Parsing '/etc/asterisk/cdr_manager.conf': == Found
cdr_manager.so => (Asterisk Manager Interface CDR Backend)
== Registered custom function 'IFMODULE'
func_module.so => (Checks if Asterisk module is loaded in memory)
== Registered application 'ReadExten'
== Registered custom function 'VALID_EXTEN'
app_readexten.so => (Read and evaluate extension validity)
res_clioriginat.so => (Call origination and redirection from the CLI)
== Parsing '/etc/asterisk/cdr.conf': == Found
cdr_csv.so => (Comma Separated Values CDR Backend)
== Registered application 'Exec'
== Registered application 'TryExec'
== Registered application 'ExecIf'
app_exec.so => (Executes dialplan applications)
== Registered custom function 'AUDIOHOOK_INHERIT'
func_audiohookinherit.so => (Audiohook inheritance function)
== Registered application 'WaitForRing'
app_waitferring.so => (Waits until first ring after time)
== Registered custom function 'ENV'
== Registered custom function 'STAT'
== Registered custom function 'FILE'
func_env.so => (Environment/filesystem dialplan functions)
== Parsing '/etc/asterisk/cli_permissions.conf': == Found
Asterisk Ready.
== Parsing '/etc/asterisk/cli.conf': == Found
*CLI> > Saved useragent "Asterisk PBX 1.6.2.12-rc1" for peer abuja
```

Figure 17 Asterisk start-up, sip registration and peer saving

Asterisk is usually run on Fedora or Linux operating system as the case may be and depending on choice. The Extension.conf, SIP.conf and Voicemail.conf configuration files are placed into the etc/asterisk folder. The asterisk server is initiated by inputting this command in the command line interface on the fedora server asterisk -vvvvvvvvvvvvvc which automatically registers the clients and also establish connection.

The figure above shows when the command in run and the server registers the sip peers and phones

```

File Edit View Terminal Help
== Registered application 'SendText'
app_sendtext.so => (Send Text Applications)
== Registered application 'BackgroundDetect'
app_talkdetect.so => (Playback with Talk Detection)
== Registered bridge technology multiplexed bridge
bridge_multiplexed.so => (Multiplexed two channel bridging module)
== Parsing '/etc/asterisk/cdr_manager.conf': == Found
cdr_manager.so => (Asterisk Manager Interface CDR Backend)
== Registered custom function 'IFMODULE'
func_module.so => (Checks if Asterisk module is loaded in memory)
== Registered application 'ReadExten'
== Registered custom function 'VALID_EXTEN'
app_readexten.so => (Read and evaluate extension validity)
res_cloriginate.so => (Call origination and redirection from the CLI)
== Parsing '/etc/asterisk/cdr.conf': == Found
cdr_csv.so => (Comma Separated Values CDR Backend)
== Registered application 'Exec'
== Registered application 'TryExec'
== Registered application 'ExecIf'
app_exec.so => (Executes dialplan applications)
== Registered custom function 'AUDIOHOOK_INHERIT'
func_audiohookinherit.so => (Audiohook inheritance function)
== Registered application 'WaitForRing'
app_waitforring.so => (waits until first ring after time)
== Registered custom function 'ENV'
== Registered custom function 'STAT'
== Registered custom function 'FILE'
func_env.so => (Environment/filesystem dialplan functions)
== Parsing '/etc/asterisk/cli_permissions.conf': == Found
== Parsing '/etc/asterisk/cli.conf': == Found
*CLI> sip show peers
Name/username      Host                Dyn Nat ACL Port    Status
1201/2201          192.168.3.4        0      0      5060    Unmonitored
1202              (unspecified)     0      0      5060    Unmonitored
abuja/lagos       192.168.2.3        0      0      5060    Unmonitored
3 sip peers [Monitored: 0 online, 0 offline Unmonitored: 3 online, 0 offline]
*CLI>
    > Saved useragent "Asterisk PBX 1.6.2.12-rc1" for peer abuja
    
```

Figure 18 Sip show peer command

It can be stopped should the need arise by entering the command stop core gracefully in the command line interface. The registration of the SIP peers is done after successful registration and start up process is completed. The command sip show peers is entered in the command line interface to verify the peers have been successfully registered. The figure above shows the output when the sip show peer command is used as shown below in the figure.

Once the sip show peer command is issued, the corresponding registered sip peers is shown along with the port number which is 5060 and their corresponding IP address. Note that the command was issued on the Abuja server and the soft phone automatically updates itself to the asterisk server as shown below in figure below

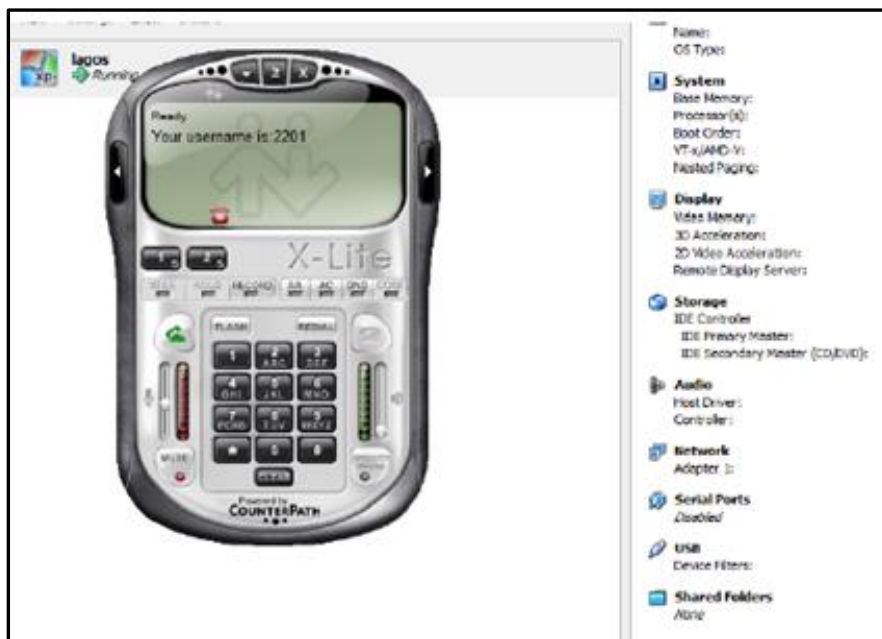


Figure 19 Registered SIP phone

4.6. The Call Process

The process of making a call can only be successful after the proper configuration of the client devices i.e. the soft phone which is X-lite 4 and hard phone astra 9133i. This is done by entering in the specified parameters such as the IP address of the server, port number, the username and the extension. The configuration of the phone device is shown below in figure.

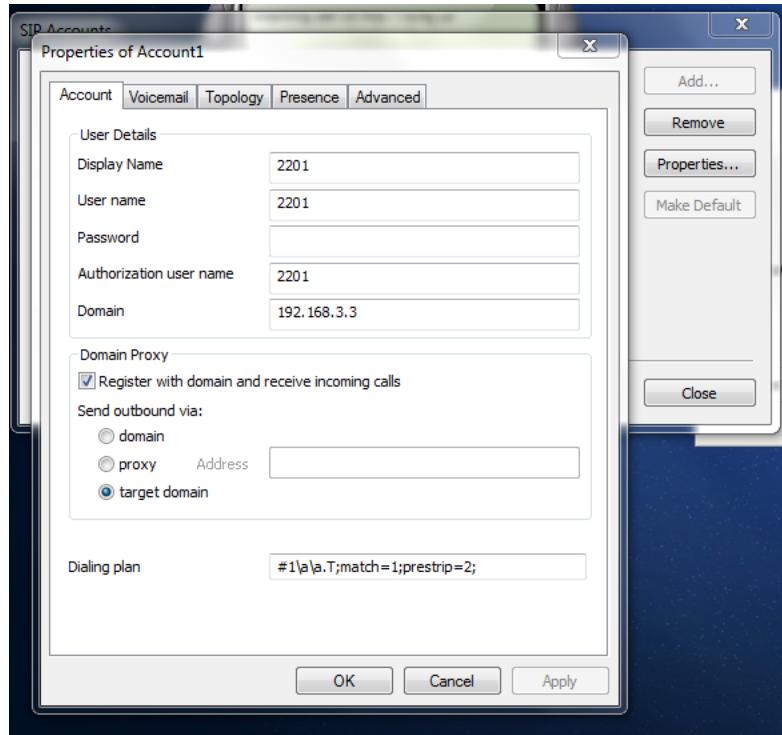


Figure 20 Configured X-Lite 4 soft phone

4.7. Security implementation (e.g., IPSec site-to-site security, IPSec VPN)

IPsec site-to-site VPN solution will be implemented across Abuja Lagos branches of the asterisk VoIP based design. The IPsec VPN combines both tunnelling, encapsulation and encryption of the packet transmitted across the network hence ensuring a secured network and also confidentiality of information across the network.

Mason, 2002 stated that the process of implementing IPsec security across the network can be broken down into five major stages as shown below;

- Initiation of the interesting traffic stage
- Internet key Exchange (IKE) phase 1
- Internet key Exchange (IKE) phase 2
- Transfer of data
- Termination of IPsec Tunnel

4.8. Implementation of IPsec VPN in the VoIP telephony network

This section illustrates the steps deployed in ensuring a successful implementation of the security solution across the network.

4.8.1. Initiation of interesting traffic

The interesting traffic here is between the Abuja server and the Lagos server branches respectively. The access list is set up as follows;

- Access-list 101 permit ip 192.168.2.0 0.0.0.255 192.168.3.0 0 0.0.0.255

- Access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.2.0 0 0.0.0.255

IKE Phase 1 stage

In this stage the authentication of the IPsec peers by the IKE is carried out. It also carries out security association negotiations and also the creation of a secure channel for the association of the IPsec security. The commands used for achieving the phase 1 are shown below with explanation of each command line.

- Crypto isakmp enable; enables the ISAKMP protocol
- Crypto isakmp policy 1; starts setting up our security associations.
- Encryption 3des; includes the des encryption
- Authentication pre-share; includes the authentication type and hashing algorithms
- Group 1; specifies the group
- Lifetime 86400; specifies the time before re-authentication starts
- Exit; exits the mode it's currently in
- Crypto isakmp identity address; sets how the peer machine is recognized
- Crypto isakmp key washima address 192.168.1.2; this command sets the key and the peer address

IKE Phase 2 stage

In this stage, the negotiation of the security association parameters of the IPSec is done and are set in the IPSec security peers. This ensures the protection of the transmitted data between the two servers. The commands used in this stage are shown below;

- Crypto ipsec transform-set secured esp-md5-hmac; encrypts the IPSec tunnel using the des and MD5 hashing algorithm.
- Mode tunnel; takes us into the tunnel mode
- Crypto map abuja 1 ipsec-isakmp; IPSec association policy itself
- Set peer 192.168.1.2; sets the peer IP address
- Set transform-set SECURITY; used to secure channel
- Set security association lifetime seconds 86400; time before re-authentication restarts
- Match address 101; tells the IPSec tunnel about interesting traffic
- Exit; leave the present mode

Data transfer; exchange of data is done between the peers and the keys are saved in the security association file. The termination of the IPsec tunnel is done either by completely deleting or by timing out process.

Testing of the VoIP telephony network.

The telephony network is tested by ensuring that servers can both dial and receive call among them as shown in the figures below. This can be achieved by using the ping command to test for connectivity between the servers and also dialling the different extension numbers. Ping command; this test for connectivity between two points by sending of packets from the source to the destination. 100% delivery signifies success otherwise unsuccessful. The figures below show the ping command test.

```
PC>ipconfig
IP Address.....: 192.168.2.4
Subnet Mask.....: 255.255.255.0
Default Gateway.....: 192.168.2.1

PC>ping 192.168.3.4

Pinging 192.168.3.4 with 32 bytes of data:

Reply from 192.168.3.4: bytes=32 time=22ms TTL=126
Reply from 192.168.3.4: bytes=32 time=13ms TTL=126
Reply from 192.168.3.4: bytes=32 time=10ms TTL=126
Reply from 192.168.3.4: bytes=32 time=14ms TTL=126

Ping statistics for 192.168.3.4:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 10ms, Maximum = 22ms, Average = 14ms

PC>
```

Figure 21 Abuja server testing connectivity to Lagos server

```

abuja#ping 192.168.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.2, timeout is 2 second
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/7

abuja#ping 192.168.3.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 second
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 3/4/6

abuja#ping 192.168.3.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.4, timeout is 2 second
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/10/
    
```

Figure 21 Establishing connectivity between the head server and the branch server

Show IP route command; this command shows the routing table of the router, showing a list of all networks the router can establish connection with. The figure 4.10 below shows the output of this command.

```

abuja#show ip route
Codes: C - connected, S - static, I - IGRP, R - RIP, M - mobile,
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external ty
       E1 - OSPF external type 1, E2 - OSPF external type 2, E -
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is not set

    192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
D       192.168.1.0/24 is a summary, 00:10:01, Null0
C       192.168.1.0/30 is directly connected, Serial0/0/0
C       192.168.2.0/24 is directly connected, FastEthernet0/0
D       192.168.3.0/24 [90/2172416] via 192.168.1.2, 00:09:51, Serial0/0/0
abuja#
    
```

Figure 22 Show IP route command

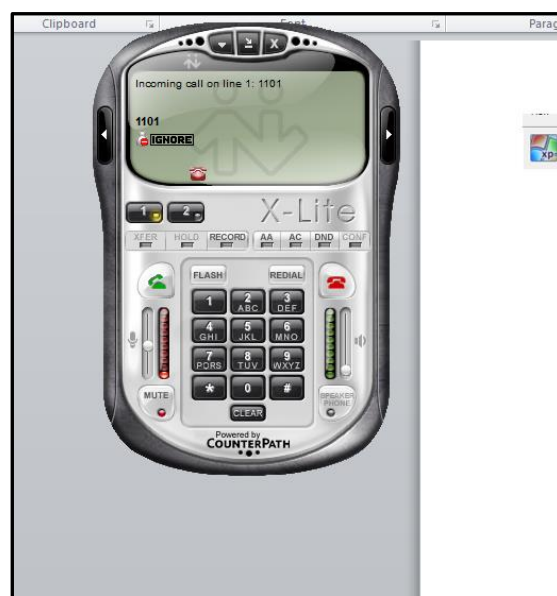


Figure 23 X-Lite phone receiving a call from extension 1101

4.9. Testing the IPsec security

The testing of the security solution is to ensure that the IPsec security has been correctly deployed and is fully functional. This is done through the issuing of Cisco commands on the server routers which will be discussed in depth.

Wire shark software was installed between the two servers to see the possibility of capturing data packets been transmitted across the network. The figure below shows a screen shot of the data been captured when the network was not protected initially.

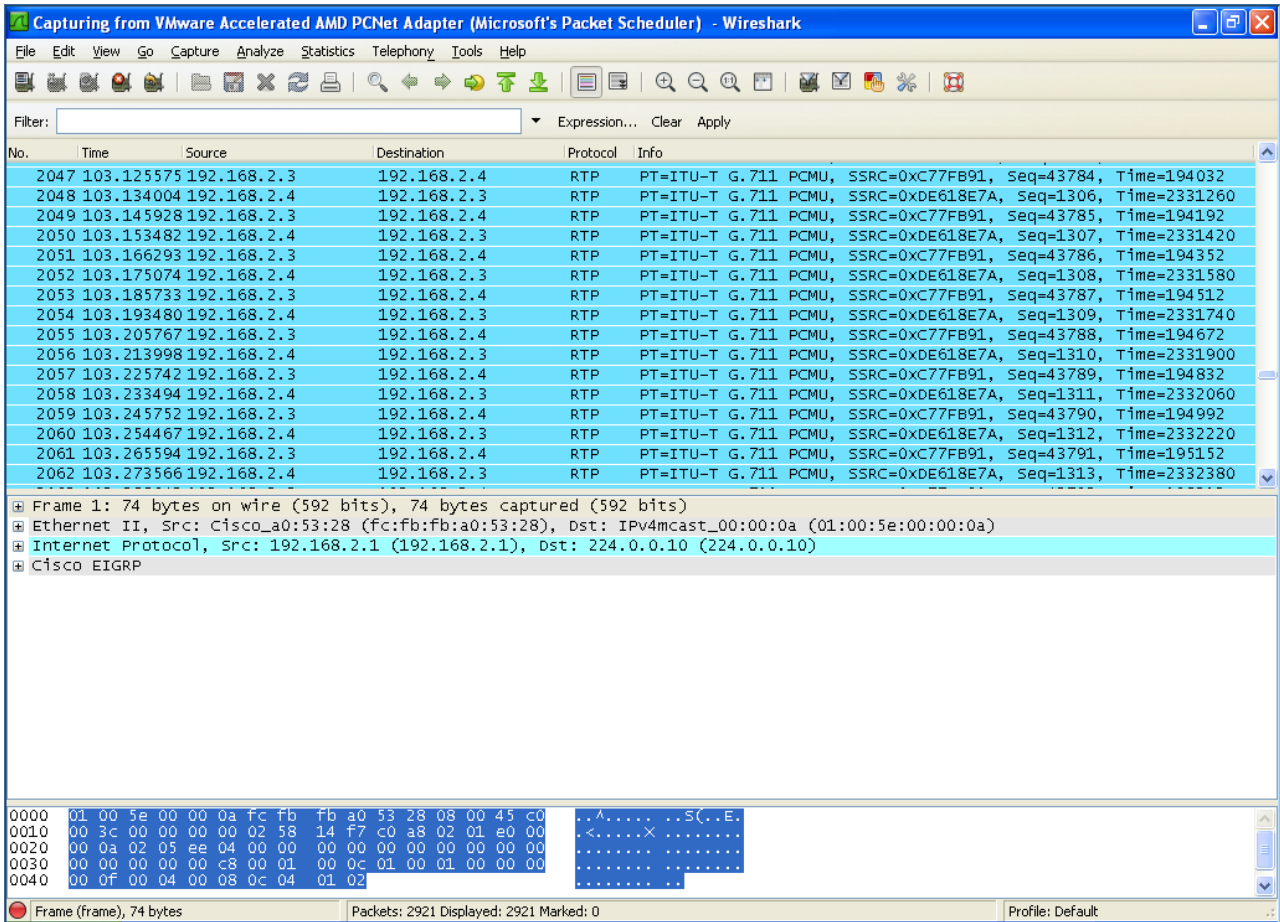


Figure 24 Wireshark capturing data when the VPN is turned off

The following commands was issued on the router to ensure the network was properly configured with IPsec site to site VPN and is fully functional and operational.

Show crypto IPsec sa; this command is used to show the security association built between the peers on the network. This also shows the tunnel that has been built between the 192.168.1.2 source point and its peer 192.168.1.1. It also shows the encapsulation security payload both at the inbound and outbound.


```

lagos#show crypto ipsec sa
interface: Serial0/0/0
Crypto map tag: lagos, local addr 192.168.1.2

protected vrf: (none)
local ident (addr/mask/prot/port): (192.168.3.0/255.255.255.0/0/0)
remote ident (addr/mask/prot/port): (192.168.2.0/255.255.255.0/0/0)
current peer 192.168.1.1 port 500
PERMIT, flags=origin|isracl,u
#pkts encaps: 5, #pkts encrypt: 5, #pkts digest: 5
#pkts decaps: 5, #pkts decrypt: 5, #pkts verify: 5
#pkts compressed: 0, #pkts decompressed: 0
#pkts not compressed: 0, #pkts compr. failed: 0
#pkts not decompressed: 0, #pkts decompress failed: 0
#send errors 0, #recv errors 0

local crypto endpt.: 192.168.1.2, remote crypto endpt.: 192.168.1.1
path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
current outbound spi: 0x69F6E255(1777787477)

inbound esp sas:
spi: 0x5DF2133F(1576145727)
transform: esp-des esp-md5-hmac ,
in use settings =aTunnel, u
conn id: 2001, flowid: NETGX:1, crypto map: lagos
sa timing: remaining key lifetime (k/sec): (4449476/8595)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

inbound ah sas:

inbound pcp sas:

outbound esp sas:
spi: 0x69F6E255(1777787477)
transform: esp-des esp-md5-hmac ,
in use settings =aTunnel, u
conn id: 2002, flowid: NETGX:2, crypto map: lagos
sa timing: remaining key lifetime (k/sec): (4449476/8574)
IV size: 8 bytes
replay detection support: Y
Status: ACTIVE

outbound ah sas:

outbound pcp sas:
lagos#
    
```

Figure 25 Crypto IPsec sa command output

Show crypto engine connections active; this displays the active security associations on the router along with the number of encrypted and decrypted packets for each security association. The figure below shows the output of this command

```

lagos#show crypto engine connections active
Crypto Engine Connections
  ID Interface  Type  Algorithm      Encrypt  Decrypt  IP-Address
  ---  ---         ---  ---           ---     ---     ---
  1001 Se0/0/0     IKE   SHA+AES        0        0        192.168.1.2
  2001 Se0/0/0     IPsec DES+MD5      0        41       192.168.1.2
  2002 Se0/0/0     IPsec DES+MD5      41       0        192.168.1.2
    
```

Figure 26 Crypto engine connections active

Show crypto IPsec transform-set; this delivers a transform set and shows the transform combination in use. The figure 4.15 below shows the output of this command.

```

lagos#show crypto ipsec transform-set
Transform set SECURITY: a esp-des esp-md5-hmac u
will negotiate = a Tunnel, u,
    
```

Figure 27 Crypto ipsec transform set output

Show crypto isakmp key; this command displays the preshared key. The figure 4.16 below shows the output of this command.

```

lagos#show crypto isakmp key
Keyring      Hostname/Address      Preshared Key
default      192.168.1.1           washima
lagos#
    
```

Figure 28 Crypto isakmp key output

Show crypto isakmp peers; this shows the local IP address and the peer's IP address. The figure below shows the output of this command.

```
lagos#show crypto isakmp peers
Peer: 192.168.1.1 Port: 500 Local: 192.168.1.2
Phase1 id: 192.168.1.1
lagos#
```

Figure 29 Crypto isakmp peers output

Show crypto isakmp policy; this displays the parameter for each IKE policy. The figure below shows the output of this command.

```
lagos#show crypto isakmp policy
Global IKE policy
Protection suite of priority 1
  encryption algorithm: AES - Advanced Encryption Standard (128 bit keys).
  hash algorithm: Secure Hash Standard
  authentication method: Pre-Shared Key
  Diffie-Hellman group: #2 (1024 bit)
  lifetime: 86400 seconds, no volume limit
Default protection suite
  encryption algorithm: DES - Data Encryption Standard (56 bit keys).
  hash algorithm: Secure Hash Standard
  authentication method: Rivest-Shamir-Adleman Signature
  Diffie-Hellman group: #1 (768 bit)
  lifetime: 86400 seconds, no volume limit
lagos#
```

Figure 30 Crypto isakmp policy output

Show crypto map; this shows the crypto map configurations as shown in the figure below.

```
lagos#show crypto map
Crypto Map "lagos" 1 ipsec-isakmp
  Peer = 192.168.1.1
  Extended IP access list 101
    access-list 101 permit ip 192.168.3.0 0.0.0.255 192.168.2.0 0.0.0.255
  Current peer: 192.168.1.1
  Security association lifetime: 4608000 kilobytes/8640 seconds
  PFS (Y/N): N
  Transform sets=4
    SECURITY,
    ú
  Interfaces using crypto map lagos:
    Serial0/0/0
```

Figure 31 Crypto map output

When the IPsec security was turned off between the branches by using the no crypto map command. The Wireshark was able to capture packets when calls were made between the 2 branches. Capturing details such as the IP address, protocols, payload type which could be used by malicious intruders for different purposes.

When the IPsec security was turned on the Wireshark could not capture the data since all the information became hidden and fully encrypted by its replacement with the encapsulation security payload (ESP).

5. Evaluation

5.1. Weaknesses, problems and setbacks in the Project Design

The following below was identified as possible weaknesses in the project design, even though the overall project was successful.

- Weakness in the Asterisk Software. This is an open source hence the risk of unaccountability by any organization should I fail or crash when in use as opposed to propriety solutions like Cisco that guarantees the maintenance, repairs and upgrades which is not available on the asterisk open source software. Hence the need to go for propriety solutions that offer guarantee; although backups of the configuration files could be made and stored on external storage devices should the need arise.
- Effect of the Security solution Deployment across the network. The IPsec VPN deployed on the network makes use of shared key for authentication purposes. Once the key is compromised, the overall aim of tunnelling between the two networks becomes defeated. There is also the issue of Bandwidth utilization and the overall

quality of service issues which need to be addressed when call is being made; the overall network performance slows down.

- Numbering system used. The four digit numbering system in use might not be easy to remember as the number of departments grows so does the extension numbers. This could also amount to wastage of the numbers should the firm not expand or shortage should the growth be astronomical.

6. Conclusion

The design of the VoIP based network was started by firstly carrying out an in depth research into the VoIP based telephony network as a whole, critically analysing it and comparing it to the existing Public switch telephony network. The advantages of the VoIP telephony network were discussed in detail with references to a plethora of published papers and research journals.

A discussion into the different VoIP protocols that can be used in a VoIP based network design was done and comparison between the different protocols was done using reputable journals and research materials. Based on the critical comparison, SIP protocol was recommended for use in the design of the asterisk VoIP based network since it was supported by different research among which include Clark 2005, Yoon et al 2010, Christensen 2001, Alan et al 2006 among others and also Critical analysis into the different VoIP based attacks, threats was carried out with ample examples of such threats like the man in the middle attack, call flooding, spoofed messages, call hijacking, server impersonation.

A critical comparison between different security methodologies for implementation across the network was done and it was narrowed down to firewall deployment, network address translation, Virtual private network, before the strong recommendation of the IPsec site to site VPN for deployment across the network to ensure strong protection against attacks by encapsulation, encrypting and tunnelling process.

A dial plan and numbering system was designed for use in the design of the VoIP based network; the criteria used for the design of the dial plan and numbering systems was based on the number of extensions required.

Reason behind the choice of tools used for the design was analysed and explained in depth, after which the implementation phase of the initiated. The asterisk VoIP based network was designed making of the VDI images and also the configuration of an oracle virtual box. The files used for configuration of the server i.e. Extension.conf, SIP.conf and Voicemail.conf were explained critical and how it operates.

After the design of the asterisk VoIP based network, the implementation of the IPsec VPN was done across the VoIP network. Testing of the asterisk VoIP based design was carried out by calling between the two branches; testing of the IPsec VPN was done by issuing Cisco commands on the command line interface of the router and it showed that the security is fully functional and operational.

Recommendations

VoIP based technology has been termed as the technology for the future, that was almost ten years ago. This technology is rapidly emerging technology for voice communication that makes use of ubiquity of IP-based network to deploy VoIP enabled devices in enterprises and homes (Nokia, 2003). It has the capacity of completely over throwing the Public switch telephony network which is mostly in use as of today.

A good example of VoIP based network is the SKYPE network popularly in use today and I strongly recommend the implementation of VoIP network in homes especially since it's cost effective, easy to maintain as opposed to the PSTN telephony network. As VoIP usage has increased tremendously over the past five years, so as the threats and attacks against the VoIP network has also increased. This has prompted the introduction of security measures across the existing VoIP based network to counteract unauthorized access of Voice traffic or data.

The implementation of the IPsec site to site VPN solution across the network has not only offered a stronger security measure through encryption, encapsulation and tunnelling. It has also ensured and enhances call confidentiality, integrity and authentication across the network.

Although, the IPsec VPN security solution has greatly reduced the unauthorized access by hackers and malicious user; there is the issue of Quality of service of the VoIP call with the security across the network. This has given rise to concerns in the industry that wants a clear call between callers, little or no packet loss or jitter occurrence in the VoIP

network that has the IPsec security implemented across the network. Further research needs to be done in the area of Quality of service in VoIP network and also ways of reducing the excessive bandwidth usage in the VoIP network.

References

- [1] Aleksander, B. (2007), 'VoIP Communications de Voz Sobre Reds, Seminar. Institute for Communication and development.
- [2] Arcomano (2002), 'VoIP How to' white paper, Available at <http://tldp.org/HOWTO/VoIPHOWTO.html>
- [3] Abbasi, T., Prasad, S., Seddigh, N., & Lambadaris, I. (2005) A comparative study of the SIP and IAX VoIP protocols. In Proceedings of the 2005 Canadian Conference on Electrical and Computer Engineering, pp 179–183, Saskatoon, Canada
- [4] Alan, B., David, P. (2006), 'Understanding Voice over IP Security', Artech House Inc. ISBN-10: 1-59693-050-0
- [5] Brown, D., & Green, R. (2018). Understanding H.323 Network Architecture. *Journal of Network and Systems Management*, 26(2), 302-319.
- [6] Balachandran, A. (2009). A study on VoIP quality and security. *International Journal of Computer Networks & Communications*, 1(2), 71-84.
- [7] Busse, I., Deffner, B., Schulzrine, H. (1996), 'Dynamic QoS Control of Multimedia applications based on RTP' *International Journal of Computer Communications*, Volume 19, pp 49-58.
- [8] Cobley, F., Coward, A. (2004) 'Voice over IP versus Voice of Frame relay', *International Journal of Network Management*, Volume 4, pp 223-230.
- [9] Cisco (2001) Goodbye DES, Welcome AES. *The Internet Protocol Journal*, Volume 4, Number 2 (Online) Available at:
[10] http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_42/goodbye_des.html
- [11] Cisco (2004) DES/3DES/AES VPN Encryption Module (AIM-VPN/EPUI, AIMVPN/HPUI, AIM-VPN/BPUI Family). (Online) Available at:
[12] http://www.cisco.com/en/US/docs/ios/12_2/12_2z/12_2zj/feature/guide/gtaimvpn.html
- [13] Cisco (2007) Voice Security Primer: Protecting the Voice Infrastructure, Call-Management System, Applications, and Endpoints, (Online) Available at:
[14] http://www.cisco.com/en/US/solutions/collateral/ns339/ns639/ns641/net_implementation_white_paper0900aecd80460724.pdf
- [15] Cisco IOS Firewall deployment Scenarios, Available at http://www.cisco.com/en/US/prod/collateral/vpndevc/ps5708/ps5710/ps1018/prod_presentation0900aecd804e1307.pdf
- [16] Clegg, A. (1996) Telecommunications and the internet. *International Journal of Telecommunications Policy*, Volume 20, Issue 8, pp 545-548.
- [17] Cisco (2007) Voice Security Primer: Protecting the Voice Infrastructure, Call-Management System, Applications, and Endpoints, (Online) Available at:
[18] http://www.cisco.com/en/US/solutions/collateral/ns339/ns639/ns641/net_implementation_white_paper0900aecd80460724.pdf
- [19] Chong, H., & Matthews, H. (2004). Comparative analysis of traditional telephone and voice-over-Internet protocol (VoIP) systems. In Proceedings of the 2004 IEEE International Symposium on Electronics and the Environment, pp 106–111, Phoenix, AR, USA.
- [20] Cao, J., Mark, G. (2008), 'Performance evaluation of VoIP services using difference CODECS over a UMTS Network', *IEEE Telecommunication Networks and Application Conference*, Volume 35.
- [21] Chang, L., Sung, C., Chiu, S., & Lin, Y. (2010) Design and realization of ad-hoc VoIP with embedded p-SIP server. *International Journal of Systems and Software*, Volume 83, pp 2536–2555.
- [22] (Chen, P., & Davis, N. (2006). The Impact of Denial of Service Attacks on SIP-based VoIP Systems. Proceedings of the 1st IEEE Workshop on VoIP Management and Security, 53-58.)

- [23] Chen, Y., & Tang, Y. (2020). A comprehensive study on the security of VoIP systems. *Journal of Network and Computer Applications*, 156, 102563. <https://doi.org/10.1016/j.jnca.2020.102563>
- [24] Chak, H. (2005), 'VoIP principles and Practices', SOMA Network Inc. white paper, Available at ftp://ftp.rogerwinters.com/usenix05/VoIP_Principles_and_Practice.pdf
- [25] Cisco (2007) Voice Security Primer: Protecting the Voice Infrastructure, Call- Management System, Applications, and Endpoints, (Online) Available at:
- [26] http://www.cisco.com/en/US/solutions/collateral/ns339/ns639/ns641/net_implementation_white_paper0900aecd80460724.pdf
- [27] Cisco (2010) Cisco Security Advisory: Cisco IOS Software Session Initiation Protocol Denial of Service Vulnerabilities (Online) Available at:
- [28] <http://www.cisco.com/warp/public/707/cisco-sa-20100922-sip.pdf>
- [29] Cao, F.& Malik, S. (2006), 'Vulnerability Analysis and Best Practices for Adopting IP Telephony in Critical Infrastructure Sectors', *IEEE Communications Magazine*, Cisco Systems Inc, pp 138-145.
- [30] Casteel, J. (2005) Sound Choice for VoIP, Available at http://www.infosecwriters.com/text_resources/pdf/VOIP_JCasteel.pdf
- [31] Dong Hee Shin. (2006), 'VoIP: a Debate over Information Service or Telephone Application in US, a new perspective in Convergence Area', *Telematics and Informatics*, Volume 23, pp 57-73.
- [32] Dantu,R., Fahmy, S., Schulzrinne, H., & Cangussu, J.(2009) Issues and challenges in securing VoIP. *International Journal of Computer & Security*, Volume 28, pp 743-753.
- [33] Dunte, M., Ruland, C. (2007), 'Secure Voice over IP' *Internal Journal of Computer Science and Network Security*, Volume 7, pp 63-68
- [34] Dhamankar, R.: *Intrusion Prevention: The Future of VoIP Security*. White paper. TippingPoint(2005), Available at:http://www.tippingpoint.com/pdf/resources/whitepapers/503160001_TheFutureofVoIPSecurity.pdf
- [35] Dantu, R., Fahmy, S., Schulzrinne, H., Gangussu, J. (2009), 'Issues and Challenges in Securing VoIP', *International Journal of Computer & Security*, Volume 28, pp 743-753.
- [36] Eric, K., brian, B. () 'Managing Cisco Network Security' 2nd Edition, Syngress Publishing, USA. ISBN: 1-913836-56-6
- [37] Endler, D., Ghosal, D., Jafari, R., Karlcut, A., Kolenko, M., Nguyen, N., Walkoe, W., Zar, J.: *VoIP Security and Privacy Threat Taxonomy*, Public Release 1.0 (2005)
- [38] Epstein Joseph (2009), 'Scalable VoIP Mobility: Integration and Deployment, Elsevier press UK. ISBN:978-1-85617-508-1
- [39] Frankel, S., Karen, K., Ryan, L., Angela, O., Ronald, R., (2005), 'Guide to IPSec VPNs' Available at <http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf>
- [40] Goode, B. (2002), 'Voice over Internet Protocol (VoIP)', In *Proceedings of the 2004 IEEE International Symposium on Electronics and the Environment*, Volume, 90 pp 106–111, Phoenix, AR,USA.
- [41] Gururaj, G. (2004). VoIP: Quality of Service, Scalability, and Security. *Communications of the ACM*, 47(4), 56-61.
- [42] Ghafarian, A., Draughorne,R., Hargraves, S., Grainger, S., High, S., & Jackson. (2007) *Securing Voice over Internet Protocol journal of information Assurance and Security*, 2007, pp 200-204.
- [43] Geneiatakis, D., Lambrinouidakis, C. & Kambourakis, G. (2007) 'An ontology-based policy for deploying secure SIP-based VoIP services', *Journal of Computer & Security*, pp.285-297.
- [44] Houssem, J., Maryline, L. (2010), 'A secure peer-to-peer back up service keeping great autonomy while under the supervision of a provider' *Computer & Security*, Volume 29, pp 180-195.
- [45] Hallock, J. (2004) *A brief history of VoIP, Evolution and Trends in Digital MediaTechnologies*, University of Washington.
- [46] History of VoIP, 11th March 2009 Available at <http://www.whichvoip.com/blog/history-ofvoip>

- [47] Haluk AYDIN (2001), 'NAT Traversal: Peace agreement between NAT and IPSec: SANS Institute Infosec Reading Room, Available at http://www.sans.org/reading_room/whitepapers/vpns/natTraversal-peace-agreement-nat-ipsec_731
- [48] Johnson, M., & Wang, H. (2020). Advantages of VoIP over traditional telephony systems. *International Journal of Advanced Research in Computer Science and Electronics Engineering*, 9(5), 142-156.
- [49] J. Janssen et al., "Assessing Voice Quality in Packet-Based Telephony," *IEEE Internet Computing*, vol.6, no. 3, 2002, pp. 48–57
- [50] Joseph Kizza, 2009. A guide to Computer network security, springer press
- [51] Jason, N., Marcia, P. (2001) 'Building a secure web server' Distributed Systems Department, Berkeley National laboratory
- [52] Karapantazis, S., Pavlidou, F. (2009), 'VoIP: A Comprehensive Survey on a Promising Technology', *International Journal of Computer Networks*, Volume 53, pp 2050-2090
- [53] Kwok T.Fung, 2005, Network security technologies. CRC press USA.
- [54] Kuhn, Richard D., Walsh, Tomas J., Fries, Steffen. "Security Considerations for Voice Over IP Systems."
- [55] Recommendations of the National Institute of Standards and Technology. 800-58. 3 May 2004. URL: http://csrc.nist.gov/publications/drafts/NIST_SP800-58-040502.pdf
- [56] 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
- [57] Katz, D., Tomasz, L., Rich, G., Wayne, W. (2006), 'Want to Know how VoIP networks? Protocols Codecs and More. EE Times-India.
- [58] Lammle Todd, 2006. CCNA, Study guide, 6th edition, Indiana, Wiley & sons inc USA
- [59] Li "Quality and Reliability of Telephone Calls on the Internet Prestudy Report", 2001
- [60] Makhija, S., Jain, R., & Gupta, P. (2021). Vulnerabilities in VoIP networks and their impact on QoS. *IEEE Access*, 9, 106793-106806. <https://doi.org/10.1109/ACCESS.2021.3059514>
- [61] Mohammad, R., & Mazleena, B. (2011). Security Issues in Voice over IP (VoIP) Implementations. *International Journal of Computer Science and Network Security*, 11(8), 1-10.)
- [62] Mohamed, G., Alex, L. (2007), 'structured firewall design' *Computer networks*, Volume 51, pp 1106-1120.
- [63] Miliefsky, G. (2005), 'Securing your VoIP Solution' Netclarity white paper.
- [64] Moris, E., (2001), 'IP Telephony ready to explode into corporate world' *Communications News*, Volume 38, pp 96-97.
- [65] Milutin, K., D. Damir, "IP telephony network saving capacity due to substitution of PSTN by IP network" *Software in Telecommunications and Computer Networks*, 2006. SoftCOM 2006.
- [66] International Conference on Sept. 29 2006-Oct. 1 2006 Page(s):336 – 34.
- [67] Meggelen, T., Madsen, L., & Smith, J. (2007) *Asterisk The future of Telephony*, 2nd Edition. Beijing ; Farnham : O'Reilly media
- [68] NIST. "Voice over Internet Protocol (VOIP), Security Technical Implementation Guide." Version 1, Release 1. 13 January 2004. Available at <http://csrc.nist.gov/pcig/STIGs/VoIP-STIG-V1R1R-4PDF.pdf>
- [69] Nokia (2003), 'Advantages of SIP for VoIP', Available at http://www.nokia.com/NOKIA_COM_1/About_Nokia/Press/White_Papers/pdf_files/whitepaper_sip_for_voip.pdf
- [70] Patel, R. (2022). Comprehensive analysis of VoIP features and services. *Journal of Telecommunications and Digital Media*, 15(2), 87-99.
- [71] Pavlidou, F.,Pitsillides, A., Schulzrine, H., Sisalem, D. (2008), 'Research and Trials for Reliable VoIP applications' *International Journal of Computer Networks*, Volume 52, pp 2447-2449.
- [72] Peters James (2000), 'a systematic approach to understanding the basics of Voice IP: Voice over IP Fundamentals'. Cisco press, USA

- [73] Proakis, J. G., & Manolakis, D. G. (2007). *Digital Signal Processing: Principles, Algorithms, and Applications*. Pearson Prentice Hall.
- [74] Patrick Park (2009), 'Voice over IP Security', 1st Edition, Cisco Press, Indiana USA, ISBN: 978-1-58705-469-3.
- [75] Prehofer, C., Müller, H., & Glasmann, J. (2000) *Scalable Resource Management Architecture For Voip*. Munich: Siemens AG Inc.
- [76] Putro, H. (2009), 'Performance of various CODECS related to Jitter Buffer Variation in VoIP using SIP', *Electrical engineering Journal*, Volume 9, pp1.
- [77] Qu, W., & Sampalli, S. (2002) *IPSec-based secure wireless virtual private network*, in *Proceedings of the IEEE Military Communications Conference, Milcom*, pp. 1107–1112.
- [78] Richardson, D., Brown, J., & Ramaswamy, V. (2018). Security issues in VoIP: Infrastructure vulnerabilities. *International Journal of Information Security*, 17(2), 165-178. <https://doi.org/10.1007/s10207-017-0397-3>
- [79] Ramachandran (2006), 'VoIP Security: Asserting the Trust boundary, the Global Voice of Information Security', *Journal of ISSA*, pp 8-13
- [80] Ranch Networks. "What To Look For In VoIP Security." Available at :<http://cnscenter.future.co.kr/resource/hot-topic/voip/VoIP-Security.pdf> (26 October 2004)
- [81] Ramirez, D (2007), 'Security within VoIP Networks', *Information Systems Control Journal*, Volume 6.
- [82] Rufi, A. W. (2007) *Network Security 1 and 2 Companion Guide*. Indianapolis: Cisco Press Inc, pp 234.
- [83] Smith, J., Brown, K., & Davis, L. (2018). The evolution of communication technology: From legacy phones to VoIP. *Journal of Communication Technology*, 32(4), 215-230.
- [84] Smith, A., & Jones, B. (2017). VoIP Implementations using H.323. *Telecommunications Review*, 38(4), 221-235
- [85] Shen, H., & Schulzrinne, H. (2011). VoIP deployment in enterprise networks: Requirements and solutions. *IEEE Communications Surveys & Tutorials*, 13(3), 479-497.
- [86] Salah, K. (2006), 'On the Deployment of VoIP in Ethernet Network, Methodology and Case study', *International Journal of Computer Communications*, Volume 29, pp 1039-1054
- [87] SANS Institute (2007) *Security Issues and countermeasure for VoIP* (Online) Available : http://www.sans.org/reading_room/whitepapers/honors/securityissuescountermeasure-voip_1701
- [88] Skoog, Paul, Arnold, Doug. "Synchronization Essentials of VoIP." URL:http://www.truetime.com/DOCSn/Sync_VoIP.pdf
- [89] Schulzrine, H., & Rosenberg, J. (2002) *Internet Telephony: Architecture and protocols- an IETF perspective*. Readings in Multimedia Computing and Networking, 2002, pp 635-653.
- [90] Stallings (2006), 'Cryptography and Network Security, Principles and practices' 4th edition , New Jersey: Prentice Hall
- [91] Smith, M., Hunt, R. (2002) 'Network Security Using NAT and NAPT', *IEEE International Conference on Networks*, Volume 10, pp 355-360
- [92] Sinha, R. (2003), 'MPLS-VPN Service and Security, SAN's Institute Infosec Reading Room, Available at http://www.sans.org/reading_room/whitepapers/vpns/mpls-vpn-services-security_1124
- [93] Scarfone, K., Hoffman, P. (2009), 'Guidelines on Firewalls and Firewall Policy' Available at http://www.nist.gov/manuscript-publication-search.cfm?pub_id=901083
- [94] Stringfellow, Brian. "Secure Voice over IP." 15 August 2001. URL:<http://www.sans.org//rr/voip/secvoice.php>
- [95] Shikfa, A., Önen, M., & Molva, R. (2010) Privacy and confidentiality in context-based and epidemic forwarding. *International Journal of Computer Communications*, Volume 33, pp 1493–1504.
- [96] Tucker, G. (2004), 'Voice Over IP and Security', SANS Institute Infosec Reading Room, Available at http://www.sans.org/reading_room/whitepapers/voip/voice-internet-protocol-voip-security_1513
- [97] Twok (1997), 'Residential Broadband Internet Services and Applications Requirements', *Communication Magazine IEEE*, Volume 35, pp76-83

- [98] VOIPSA (2005), 'VoIP Security and Privacy Threat Taxonomy' available at http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf
- [99] Wang, X., Li, M., & Zhang, Y. (2019). Operating system vulnerabilities in VoIP networks. *ACM Computing Surveys*, 51(6), 1-35. <https://doi.org/10.1145/3289227>
- [100] Wallingford, T. (2005), 'Switching to VoIP', Cambridge: Oreilly . ISBN: 0-596-00-868-6
- [101] Wikipedia, Nyquist–Shannon sampling theorem, 13th March 2009 http://en.wikipedia.org/wiki/Nyquist%E2%80%93Shannon_sampling_theorem
- [102] Wang Hoa (2004), 'Network Firewall' *Computer Network and Security*
- [103] Xin, J. (2007) Security Issues and countermeasure for VoIP (Online) Available at: http://www.sans.org/reading_room/whitepapers/honors/security-issuescountermeasure-voip_1701
- [104] Yoon, E., Yoo, K., Kim, C., Hong, Y., Jo, M., & Chen, H. (2010) A secure and efficient SIP authentication scheme for converged VoIP networks. *International Journal of Computer Communications*, Volume 33, pp 1674–1681.
- [105] Zhang, R., Wang, X., Yang X., & Jiang X. (2010) On the billing vulnerabilities of SIPbased VoIP systems. *International Journal of Computer Networks*, Volume 54, pp 1837–1847.
- [107] Zisiadis, D., Kopsidas, S., & Tassiulas, L. (2008) VIPSec defined. *International Journal of Computer Networks*, Volume 52, pp 2518–2528.
- [108] Zolfaghari, A. (2006). An overview of Voice over IP (VoIP): Protocols, challenges and future directions. *Journal of Network and Computer Applications*, 29(3), 103-109.