Journal of Communication and Computer 16 (2021) 6-18
doi:10.17265/1548-7709/2021.01.002

A Secured Network Prototype for Enhanced Connectivity in Hospital Environment for Remote Patient Monitoring

Kennedy Amadasun[1], Michael Short[1], James Agajo[2], Kenneth U. Osigwelem[3], and Joel O. Egwaile[4]

1. School of Computing, Engineering & Digital Technologies, Teesside University, England, United Kingdom

2. Computing Engineering Department, Federal University of Technology, Minna, Nigeria

3. Computer Science Department, Alvan Ikoku Federal College of Education, Owerri, Nigeria

4. Department of Electrical/Electronic Engineering, University of Benin, Benin City, Nigeria

Abstract: With the developing stride in science and technology, effective healthcare delivering system is paramount. Healthcare service provider have taken pains over the past decades to implored Information Technology to render a better quality of service by setting up LANs & WANs Technology (Virtual Private Network) for securing connectivity between associate organizations and as well protecting patient's data for confidentiality and integrity. The aspiration of this research is to design a network prototype good enough for deployment in healthcare institution (Hospital) with cardinal points on assurance of data integrity and privacy, providing resilient link with high availability by avoiding single point of failure in the network and security between the network links. This work is aimed at deploying an impeccable network solution that is resilient and not susceptible with secure real-time access to patients' medical history and a nice access control polices for health centers in developing countries and as well a means of data development for every citizen.

Keywords: Network, data, infrastructure, hospital, security, VPN

1. Introduction

Availability is a crucial and paramount issue in network design and building whether is a network for small, medium, or large-scale enterprise for convenient communication, file sharing and other operations that rely on computer network [1]. Availability must be put into consideration to avoid down time and above all the networks must be secured, setting up a network with high availability is not enough because they are vulnerable to damages which could be intentionally or unintentionally. Despite these only few organizations have good knowledge of how much availability that is required. Factors like budget limitation, duration of time for completion, competency and experience are what determine a good network design and availability.

1.1 Research Aim

The aim of this research study is to produce well secured data transmission link with a functional network system connecting all clinics and hospitals to Federal Medical Centre with ability to fail-over.1.2 Research Objectives.

The objectives of this research study are as follows:

- To design and produce a prototype network which demonstrate a secure network for hospital.
- To embed in the network capability for end-to-end connectivity
- To inculcate high availability in the network.

Corresponding author: Kennedy Amadasun, School of Computing, Engineering & Digital Technologies, Teesside University.

1.3 Need for the Research

From present research it has been discovered that many patients lost their life in Nigeria because of lack of medical record of patient. Patients are treated without tracing the root causes of the ailment or critically examine the medication he/she has been on, which is unprofessional and awkward. Every patient is expected to have medical record that is highly secured and confidential .The fact that the data traffic is transfer via internet link (un-trusted network) between the hospital headquarter, branch and Nigeria National Health Insurance Scheme (NHIS) therefore it becomes very imperative to provide security for the traffic so as to upgrade the health well-being of the populace and safe guard high quality health care, with the incessant growth of the internet in our present day lives companies, businesses are moving towards internet services, the internet is also becoming vulnerable to hackers for malicious and fraudulent act, to avoid tempering with the information the necessary security measures need to be in place [2].

In case of patient referral to any of the hospital, medical history can be accessed at any given time. It therefore implies that for the medical data of patient to be access at any given time the network link must be up and running, and highly available to avoid down time. A safe failure (failover) is needed to be implemented to arrest the issue of down time.

1.4 Motivation

The main problem with computer systems and network is reliability. Reliability of a complex system is a big concern that leads to some components failure which is disastrous. The capability of a system to execute its desired functions for a specific time under pre-defined conditions is called reliability. The art that promotes computer reliability is the main point of growth that cut across academic sector and every industry. The intricacy in computer network deployment, security and fault tolerance has remained a choice for networking engineers to consider getting hold of network reliability so that high availability and secured network can be assured [3]. The Healthcare system keeps and controls very vital information that requires maximum level of confidentiality to protect patient’s privacy. The prime primary requirement in the health locality is a care delivery that is free from interference. When a patient cannot be treated due to poor facilities in the hospital and unavailability of medical professionals the patient is immediately transfer to hospital with better facilities and medical expert. There is need in sending patient’s medical data to the partner hospital, which is a common practice in the healthcare sector, but the data must be kept secured and confidential.

1.5 Contribution and Structure

This paper is organized as follows: Section II describes the research methodology adopted in the research. Section III IP addressing. Section IV Network Simulation. Section V concludes the work.

2. Research Methodology

2.1 Overview

In addition to a literature review, a critical assessment and interviews was carried out in Federal Medical Centre and other hospitals to observe the information technology network infrastructure and security on ground. Researching into existing secured network technologies that will be suitable for healthcare system because in health sector confidentiality of patient’s medical data is very important to assure complete privacy with respect to the patient’s medical record or data. In an institution where security and privacy are highly needed, it is necessary to make sure that the authorized officer gets access to the facilities that it is permitted to access within the network in the cause of its duty to deliver quality healthcare Having inspected all the infrastructure a simulation tool called cisco packet tracer was adopted due to the largeness of the network to demonstrate the process. The medical profession is extremely conscious of patient’s right to privacy, and steps has been taking by medical professionals to guarantee patient’s right to this privacy, so computer security is not compromise in the health sector [15]. To cope with security needs of a Computer-based Patient Record (CPR) in a health care system Network Access Control (NAC) needs to be introduced to determine who have the right to access the network and what resources in the network can he/she is able to access if permitted and who should be restricted from the network. In a health care network identification and authorization security polices need to be implemented on devices and users according to the functions they perform.

2.1.1 Terminal Access Controller Access Control System plus (TACACS+)

It employed AAA protocol to coordinate networking devices and alter identification of confidential code in a unify server. TACACS+ renders AAA services independently and differentiate authentication and authorization operations while in RADIUS both functions are combined. TACACS+ have the potentials to harmonize with any other services or integrate into its personal data storage, TCP protocol has been used for transportation and meanwhile all the packets are well encrypting except the header whereas only the confidential code is encrypted in RADIUS. Haven critically looked at all the protocols that can be employed to suit the requirement of any Healthcare system AAA protocols seems to be the best, but TACACS+ is preferable since it applies TCP for transport which guarantee a reliable communication between server and the user when compare to UDP. TACACS+ allow network manager to define commands which client can use and above all during transportation data cannot be sniff from packet because all the data are encrypted. Virtual Private Network (VPN) Technology. In our present-day world connecting of remote sites with internet infrastructure is increasing rapidly because of its flexibility and cost effective unlike other WAN technologies. The internet is a public network which is highly vulnerable and has the capacity to create a lot of security risk and challenges. However, data need to be reliably transmitted and secured, and to achieve a secure network VPN need to be implemented. VPN technology is the application of cryptography understanding in the open and public network to create a virtual private network (VPN). It uses a set of cryptographic systems which are message digest algorithm, digital signature, digital certificates, asymmetric encryption, and symmetric encryption [4]. While Jaha et al. (2008) [5]; Rossberg and Schaefer (2011) [6] refer to VPN as a network security technology that deliver secure data link communication between two networks over untrusted public communication framework like the internet in which each user has certificate that enable secure communication as shown in Fig. 1. VPN establish a tunnel which look like pipe that is encrypted connecting two points in an internet cloud, the tunneling protocol use to provide protection and data privacy is called the VPN IPsec.

2.1.2 Techniques of VPN Connection

Connection of VPN techniques in Remote access and Site-to-site VPN are divided into two. Provider Edge (PE) also known as Network-based VPN and Customer Edge (CE). In PE-based VPN the appliances implement the tunneling process encapsulation and decapsulation while the CE appliances have no VPN role to play, also on the other way round CE appliances execute all VPN roles of tunnel encapsulation at the customer end while thePE appliances is indisputable to the VPN tunnel and

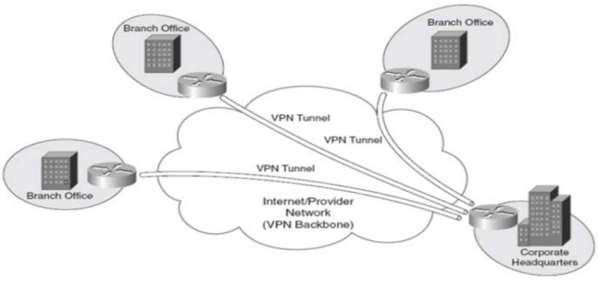


Fig. 1 VPN environment [7].

has no role to play in VPN tunneling. The main aim of adopting VPN technology is because of data security, an organization may be transmitting a sensitive data, taking healthcare as a good example a patient medical record can be transfer via the internet (public network) without getting disturbed about its integrity and privacy because all the transmitted data are encrypted to the extent whereby if attacker succeeded in sniffing the data packets it cannot read the information, it will be useless to him/her.

In hospitals patient's medical record are transfers from one remote end to another end or a bigger hospital as referral without undermining patient's medical record, now and days medical examinations/diagnosis report are transmitted to the medical consultant from the laboratory without been worried about the confidentiality and privacy.

2.1.3 Generic Routing Encapsulation (GRE)

GRE is a layer 3 proprietary protocol for engulfing network layer from any network layer protocol and it allows various protocols to be engulfed in IP tunnels. GRE is a virtual end-to-end connection but lacks protection and adaptability because during transportation in GRE packets are not coded nevertheless IPsec can be used with GRE tunnels to encode and makes it more reliable and protected [8].

2.1.4 Recommendation

GRE tunnel has the potentials to execute protocols that are not supported by IPsec. The GRE first uses the tunneling protocol to encapsulate the private IP packets and has the potentials to engulf multiple protocols over backbone single protocols which imply that every data traffic moving between the locations are enclosed in a GRE packet before the encapsulation process begins. GRE tunneling permit VPN across WAN, GRE tunneling is cost effective and simple to implement.

2.1.5 Internet Protocol Security (IPsec)

It is a tunneling protocol at the network layer (layer 3) of the OSI model initiated by IETF to control encryption, confidentiality, originality of data and authentication for fortifying integrity. It generates end to end traffic ensuring the originality of data packet confidentiality which implies that data such as payload, IP address, cannot be intercepted during transportation. The major aim is to achieve secure data communication across insecure medium. IPsec integrates a set of protocols to function together as a suite of protocols with each protocol effecting data security. The components of IPsec are Internet Key Exchange (IKE), Authentication Header (AH) and Encapsulating Security Payload (ESP) [9].

2.1.6 Internet Key Exchange (IKE)

It is an instrument used to liaise for other protocols. These protocols in the internet need security check to secure all data and data integrity. It implements security structure such as the Internet Security Association and Key Management Protocol (ISAKMP). Security Association (SA) is the fundamental of IPsec by setting arrangement of principles encoding tools. SA is a data formation which is utilized to store and secure all the privacy variables between devices. IKE comprises of two phases: phase 1 is for creating IKE SA to establish a secure authenticate communication link by creating a shared secrete key for encryption, and phase 2 is for IPsec SA whereby data flow is clarified and secured between the peers, an access lists is also configured to permit only wanted traffic and create crypto maps [10].

2.1.6 Authentication Header (AH)

It is the IPsec protocol that is responsible for data integrity and sender authentication for IP packets by attaching more fields to the IP header. AH can be used in transport or tunnel mode. In transport mode no new header is attached but the user PC remains the tunnel end point while in tunnel mode additional IP header is attached in the front of the packet.

AH has no encryption capacity for confidentiality it only provides authentication and integrity for IP packets. Encryption services are rendered by ESP, an RFC specification standard format for AH fields which consist of: Next header (8 bits), Payload length (32 bits/8bits), Reserved (16 bits), Security Parameter Index (32) while the data authentication consists of Integrity Check Value (ICV) [5].

2.1.7 Encapsulating Security Payload (ESP)

ESP is one of IPsec protocol in-charge of data confidentiality using the application of encryption and encapsulation. ESP encode the original information and appends additional ESP header field and trailer field to the packet before it has been transported. AH and ESP can be used in transport and tunnel mode. Payload data, authentication data, next header and pad length are IETF 2406 specified standard format for ESP.

2.1.8 IPsec Operation

IPsec protocols have two forms of operation to establish a secure communication route between communication network, the two forms are transport and tunnel mode. During Transport mode it gives end-to-end connectivity between IP hosts or devices such as router, VPN user or firewall, while in Tunnel mode a new IP header is attached to the packet for forwarding since the whole passenger IP packet will be enclosed and secured before transportation, in the operations the tunnel mode is Router-based, and the transport mode is PC-based [16]. Security is a paramount issue to be able to protect the network to mitigate the risk of being attack by black hackers. The effect of network been attack by invaders is destructive which can lead to data loss, interference with services and network outage. A lot of technique has been set up to complement the secured technology already recommended [11].

2.1.9 Existing Infrastructure

Uwa hospital has its headquarter, and branch located in Benin City municipal with approximately10 kilometers from each other.

In the headquarter there are two buildings, and each is a storey building with various department, Accident & Emergency, Pharmacy, Laboratory & Radiology and Administration & Accounts stretch across the floor of the buildings, at the branch the same arrangement structure was also carried out meanwhile the branch hospital only have just a storey building. The headquarters and the branch hospital attend to patients and admit them if the situation warrants it and if not getting better it is referred toFederal Health Centre (FHC) or Federal Medical Centre (FMC) which is an ally organization owned by the federal government with cutting-edge technology and in a referral situation the patient medical data will be forwarded to FHC in a secure mode.The available infrastructures the hospital has in their Information and Communication Technology (ICT) session is just computers that are used for the purpose of administration job such as directory, record, register, files and checklist for drugs and control in pharmacy department, this is what is also obtainable at the branch hospital.

2.2 Network Design Approach

There are various elements impeding the successful change to future commutations. These types of element hindering the changes are cause by top-down approach in computer network design. The general concept design requirement in the first case is the identification of all useful components for the design stage, merging the components as a single entity and design testing with respect to the client specification [14].

It must be realized that there is no perfect design network that will fit into your client network design because all projects have their own unique features, there is no two project that is the same although it might look similar, and so your client requirements need to be met according to specification. Networks are lively and evolve overtime to harbor the arising issues which imply that flexibility is a required milestone for a good design network. Having succeeded in the identification of the client requirement the next task is the suitable technology to implement the design.

2.3 Technical Design Requirement

Technical design requirements are simply the development of the client network plan to meet up all the specification required according to standard and at the end, the aims and objectives of the project is achieved. The design requirements are as follows:

- Performance

The performance of a network depends upon the bandwidth which is a function of the speed, throughput, latency, and capability. The quality of the network is one of the most important components of client satisfaction, and the network link requirement rate for internet and intranet should not be less than 100Mbit/s for data transfer and to enhance data traffic.

- Scalability

Scalability is also an important component that is becoming a driving force for network expansion due to new services such as multimedia services enhancement [12]. When designing a network expansion and growth in number of users and other applications must be put into cognizance for future purposes to avoid network redesign which may cause interruption to service availability.

- Availability

Since my client is a healthcare service provider, it is very important that the network needs to be highly available if possible, without a downtime and is one of the required features in the network design. Availability is one of the most demanding aspects of a network and it is usually a measurement of time taken for the network link to be up and running without the link going down or rather the ability for the network to perform a task without failure.

- Adaptability

Adaptability of network is the potentials of a network to perform with ease or effortlessly when there are changes because of application change or technology. A good network design should be able to adapt or accommodate changes with ease as we all know technology is not static but rather dynamic due to a lot of discoveries and invention in the area.

- Security

Security is one of the most important requirements by my client in the network design to anticipate unofficial disclosure of patient’s record. It is a basic requirement from my client that all network traffic going to the associate organization FHC either from the headquarters or branch must be secured and hidden from any unauthorized person and maintains its integrity and the security features implemented in the design are confidentiality service and integrity service through VPN while Authentication and Authorization was implemented at the user level. Presently security is becoming a leading feature in Communication Engineering due to the fact of vulnerability and malicious attack of network. Designing and building of network without security is like a man that is planning to fail.

- Affordability

The client budget in a project is the major determinant of the network design. The design must be limited to the budget of the client to make it affordable and meet up the required standard as shown in Figs. 4 and 5. In a situation whereby most recent and best devices are used in the design process during the deployment the total cost spend to actualize the project will be far much than the budget, so is always better to work with the frame of the budget allocated for the project.

- Manageability

It is a basic requirement to manage your network and it is necessary in any network design it support security checks, control, coordination, and monitory. In my client network a simple management tool is used called SYSLOG to observe events on the network from a management PC located at the hospital headquarter.

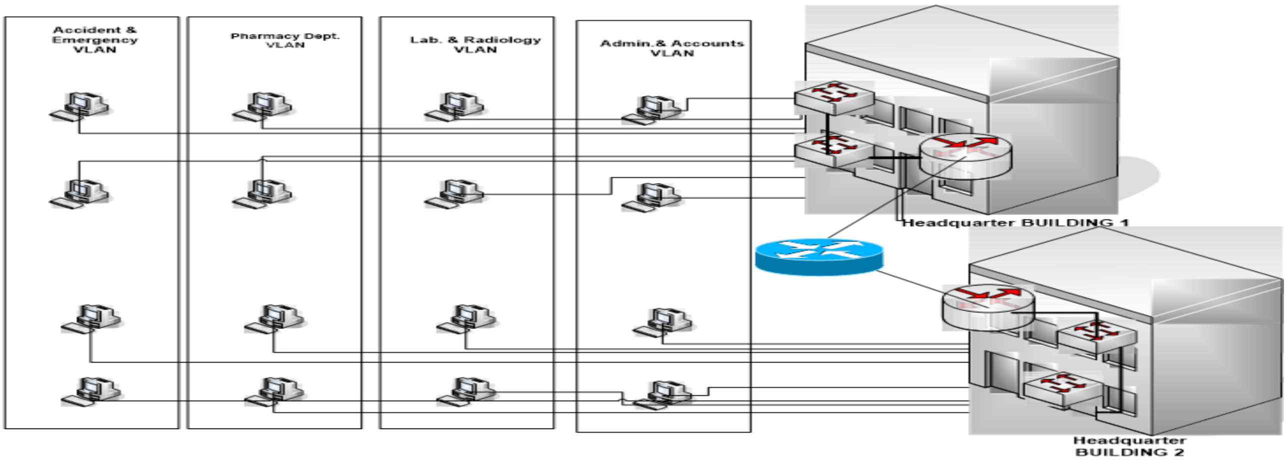


Fig. 2 Headquarter VLAN design.

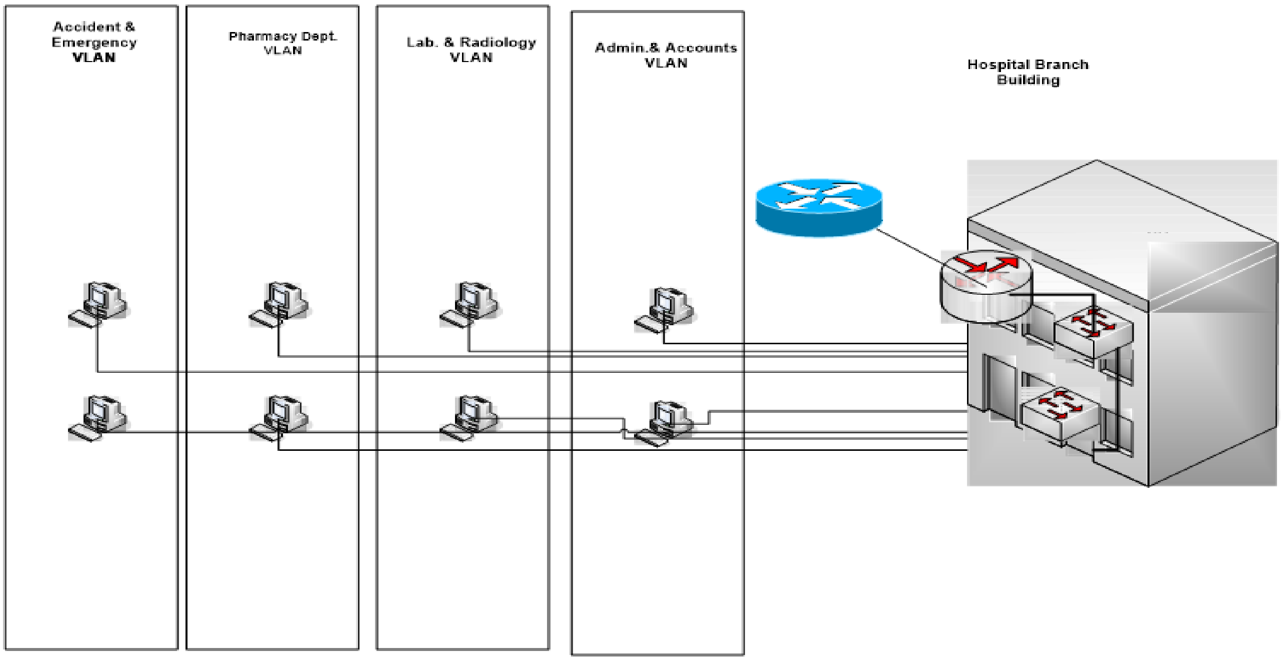


Fig. 3 Branch VLAN design.

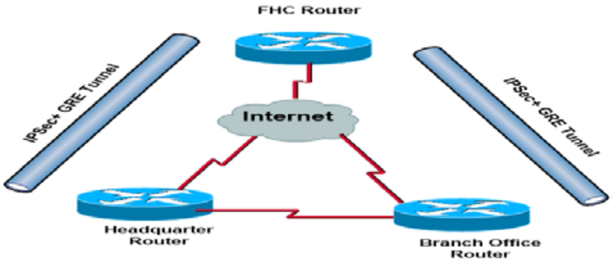


Fig. 4 Showing design model of the network.

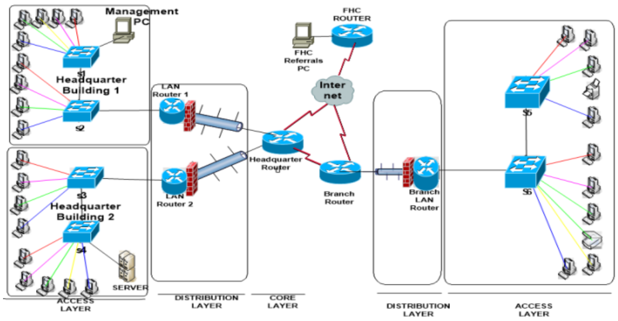


Fig. 5 Showing complete network design of Uwa hospital.

3. IP Addressing Scheme

With the development of public internet, IPv4 addresses are becoming reduced. In attempt to combat the shortage, some IPv4 has been selected as private addresses which cannot be route through the internet but can be installed in a LAN and public addresses so that it can be routed over the internet [17]. The IPv4 class B private address scheme was selected for my client network due to the fact the private addresses are free and cannot be route over the internet and as well to reduce cost. To be able to route private IP address over the internet, Network Address Translation (NAT) must be implemented on the private address utilizing public IP address. The Internet service provider will help my client with two or more public IP addresses for translation.

Private class C IP address 192.168.0.0 will be used in the network and the IP address must be sub netted correctly as shown in Tables 1-5 and using of Variable Length Subnet Masking (VLSM) is needed [13]. The IP addressing scheme for headquarter 192.168.1.0 was used which comprises of four subnets for the four VLANs. In Pharmacy subnet, I select /26 subnet which will give 62 usable hosts and my intention for selecting/26 is since when the number of users increases in future you do not need to redesign the network again, the network will always accommodate such increases, same reason for /26 subnet choosing for Accident & Emergency department. Admin & Accounts department is allocated /27 which will give 30 usable hosts while Laboratory & Radiology department was allocated /28 which will give 14 usable hosts for same reason above scalability.

In the second building of the headquarter 192.168.2.0 was allocated with four subnets as well. The following IP addresses was used for the configuration of routers and switches.

Table 1 IP addressing scheme for headquarters (building 1) 192.168.00

Subnet name (Department)	Subnet address	First usable host address	Last usable host address	Broadcast address	Subnet mask
Pharmacy	192.168.1.0/26	192.168.1.1	192.168.1.62	192.168.1.63	255.255.255.192
Accident &Emergency	192.168.1.64/26	192.168.1.65	192.168.1.126	192.168.1.127	255.255.255.192
Administration & Accounts	192.168.1.128/27	192.168.1.129	192.168.1.158	192.168.1.159	255.255.255.224
Lab & Radiotherapy	192.168.1.160/28	192.168.1.161	192.168.1.190	192.168.1.191	255.255.255.240

Table 2 IP addressing scheme for headquarters (Building 2) 192.168.00.

Subnet name (Department)	Subnet address	First usable host address	Last usable host address	Broadcast address	Subnet mask
Pharmacy	192.168.2.0/26	192.168.2.1	192.168.2.62	192.168.2.63	255.255.255.192
Accident &Emergency	192.168.2.64/26	192.168.2.65	192.168.2.126	192.168.2.127	255.255.255.192
Administration & Accounts	192.168.2.128/27	192.168.2.129	192.168.2.158	192.168.2.159	255.255.255.224
Lab & Radiotherapy	192.168.2.160/28	192.168.2.161	192.168.2.190	192.168.2.191	255.255.255.240

Table 3 IP addressing scheme for branch office (Building 1) 192.168.00.

Subnet name (Department)	Subnet address	First usable host address	Last usable host address	Broadcast address	Subnet mask
Pharmacy	192.168.5.0/26	192.168.5.1	192.168.5.62	192.168.5.63	255.255.255.192
Accident &Emergency	192.168.5.64/26	192.168.5.65	192.168.5.126	192.168.5.127	255.255.255.192
Administration & Accounts	192.168.5.128/27	192.168.5.129	192.168.5.158	192.168.5.159	255.255.255.224
Lab & Radiotherapy	192.168.5.160/28	192.168.5.161	192.168.5.190	192.168.5.191	255.255.255.240

Table 4 IP addressing scheme for serial and ethernet link.

Link name	Subnet address	First usable host address	Last usable host address	Broadcast address	255.255.255.252
FUC(S0/0/0) to (S0/2/0)	192.168.3.0/30	192.168.3.1	192.168.3.2	192.168.3.3	255.255.255.252
ISP(S0/0/0) to HEADQ(S0/0/0)	192.168.4.0/30	192.168.4.1	192.168.4.2	192.168.4.3	255.255.255.252
ISP(S0/0/1) to Branch(S0/0/0)	192.168.15.208/30	192.168.15.209	192.168.15.210	192.168.15.211	255.255.255.252
Branch core to dist.	192.168.15.192/30	192.168.15.193	192.168.15.194	192.168.15.195	255.255.255.252
HEADQ core to DISTR 1	192.168.1.208/30	192.168.1.209	192.168.1.210	192.168.1.111	255.255.255.252
HEADQ core to DISTR 2	192.168.1.192/30	192.168.2.193	192.168.2.194	192.168.2.195	255.255.255.252

Table 5 Other IP network addressing scheme.

Network name	Subnet address	First usable host address	Last usable host address	Broadcast address	Subnet mask
FHC	10.10.0.0/24	10.10.0.1	10.10.0.254	10.10.0.255	255.255.255.0
Tunnel 0	192.168.100.0/24	192.168.100.1	192.168.100.254	192.168.100.255	255.255.255.0
Tunnel 2	192.168.200.0/24	192.168.200.1	192.168.200.254	192.168.200.255	255.255.255.0

4. Testing and Evaluation of Network

A simulation software was used to test the design of the network, in Fig 6 and the simulation software is called Cisco Packet Tracer which is has a free version available on the internet at no cost. With the stimulation software small and medium sized network design can be stimulated with perfect visibility, it also offers a good support for Switching, LAN, Routing, TCP/IP, WAN, security protocols like IPsec, GRE, ISAKMP and a lot of others.

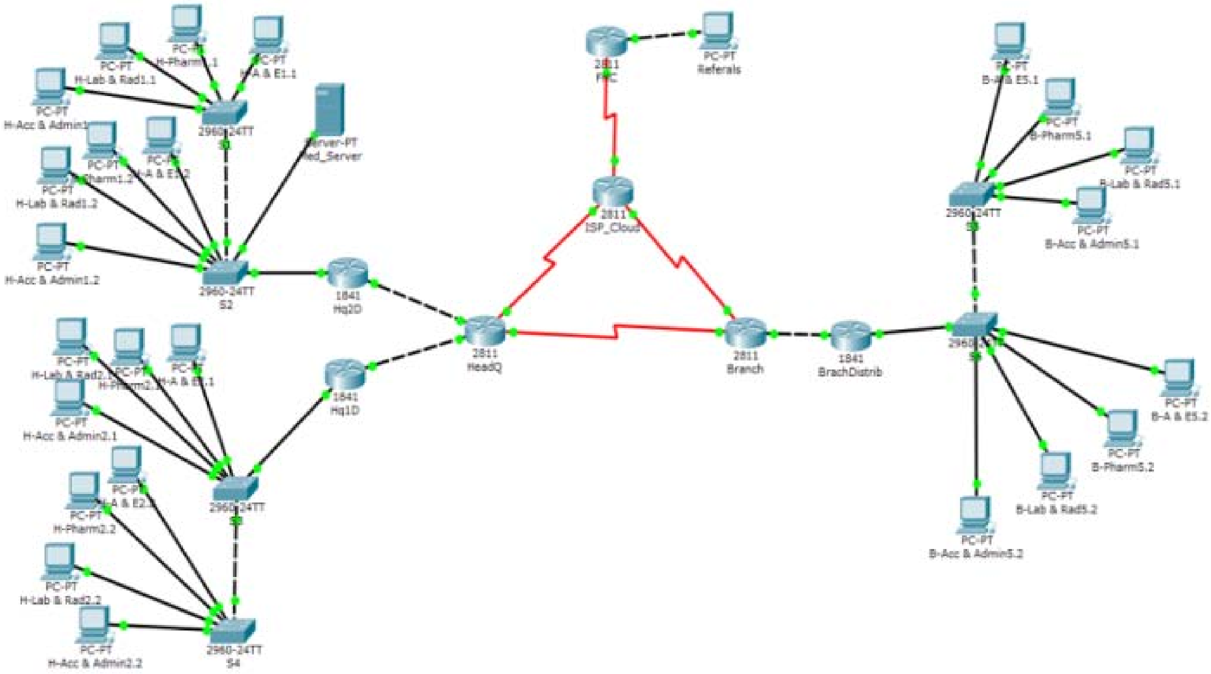


Fig. 6 Displaying network simulation prototype in Cisco Packet Tracer.

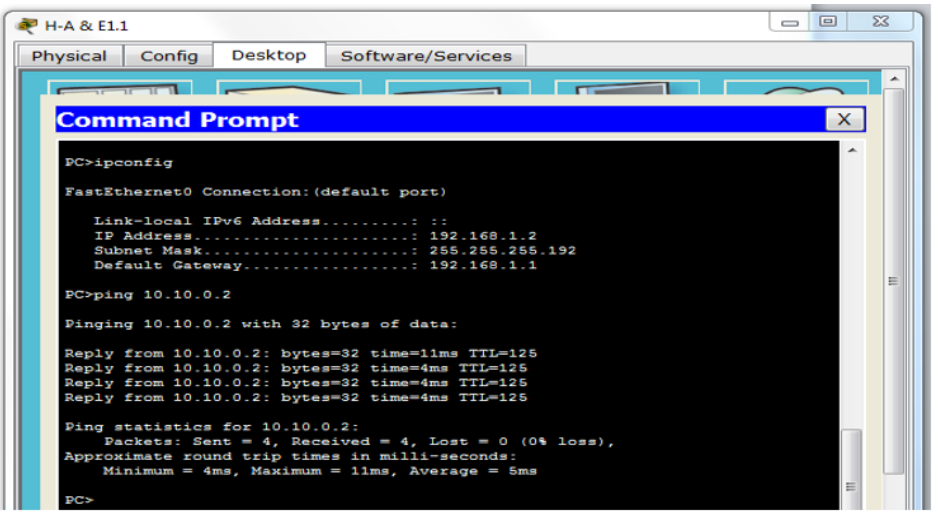
4.1 Simulation Process Test

4.1.1 Network Simulation

To commence with the test, process a Cisco packet tracer version 6.1 is installed and launch on the computer and the prototype network simulation can be loaded as follows by slotting in the compact disc and check out for the file name and open the screen shot for the network design comes up.

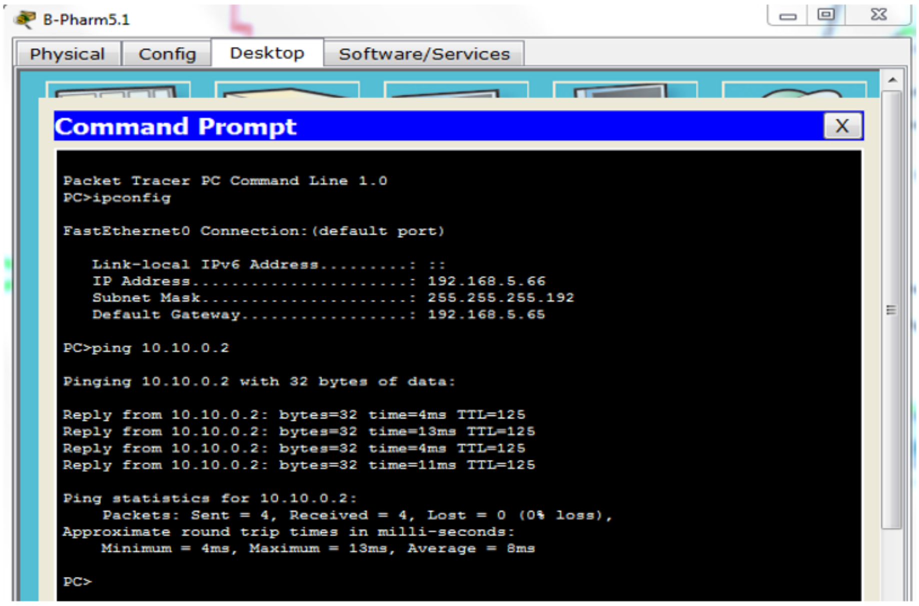
4.1.2 End-to-end connectivity

This test is proved by using a PC from any VLANs in any of the floor to establish connectivity with another PC in a different building or the FHC referral PC. The test is carried out by sending Internet Control Message Protocol (ICMP) packets through ping in Figs. 7 and 8.



```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: ::
   IP Address......................: 192.168.1.2
   Subnet Mask.....................: 255.255.255.192
   Default Gateway.................: 192.168.1.1

PC>ping 10.10.0.2

Pinging 10.10.0.2 with 32 bytes of data:

Reply from 10.10.0.2: bytes=32 time=11ms TTL=125
Reply from 10.10.0.2: bytes=32 time=4ms TTL=125
Reply from 10.10.0.2: bytes=32 time=4ms TTL=125
Reply from 10.10.0.2: bytes=32 time=4ms TTL=125

Ping statistics for 10.10.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 11ms, Average = 5ms

PC>
```

Fig. 7 Ping from A & E PC (Headquarter) to FHC PC.



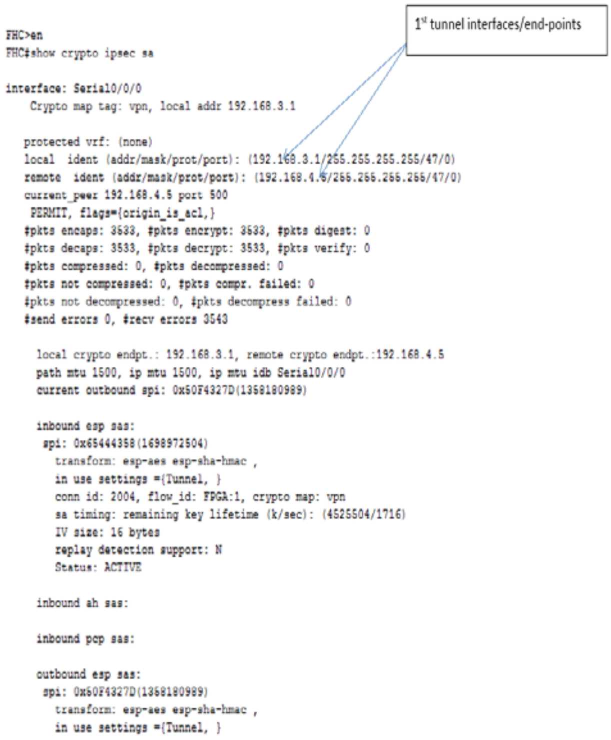
```
Packet Tracer PC Command Line 1.0
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.........: ::
   IP Address......................: 192.168.5.66
   Subnet Mask.....................: 255.255.255.192
   Default Gateway.................: 192.168.5.65

PC>ping 10.10.0.2

Pinging 10.10.0.2 with 32 bytes of data:

Reply from 10.10.0.2: bytes=32 time=4ms TTL=125
Reply from 10.10.0.2: bytes=32 time=13ms TTL=125
Reply from 10.10.0.2: bytes=32 time=4ms TTL=125
Reply from 10.10.0.2: bytes=32 time=11ms TTL=125

Ping statistics for 10.10.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 13ms, Average = 8ms

PC>
```

Fig. 8 Ping from Pharm PC (Branch) to FHC PC.

4.2 VPN Security Test

The test operation was performed on the routers where the VPN tunnels was established, the test started from FHC router head-end and type a command show crypto ipsecsa on the global interface mode of FHC router to prove that IPSec tunnel is up, the following parametric values: Security Parameter Index (SPI), PKtsdecaps, PKts decrypt, PKtsencaps and PKtsencrpt can never be zero and further status must display **ACTIVE**.

Below is the extracted screen shot from the VPN security test:



1st tunnel interfaces/end-points

```
FHC>en
FHC#show crypto ipsec sa

interface: Serial0/0/0
    Crypto map tag: vpn, local addr 192.168.3.1

   protected vrf: (none)
   local  ident (addr/mask/prot/port): (192.168.3.1/255.255.255.255/47/0)
   remote  ident (addr/mask/prot/port): (192.168.4.5/255.255.255.255/47/0)
   current_peer 192.168.4.5 port 500
    PERMIT, flags={origin_is_acl,}
   #pkts encaps: 3533, #pkts encrypt: 3533, #pkts digest: 0
   #pkts decaps: 3533, #pkts decrypt: 3533, #pkts verify: 0
   #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 3543

     local crypto endpt.: 192.168.3.1, remote crypto endpt.:192.168.4.5
     path mtu 1500, ip mtu 1500, ip mtu idb Serial0/0/0
     current outbound spi: 0x50F4327D(1358180989)

     inbound esp sas:
      spi: 0x65444358(1698972504)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
        conn id: 2004, flow_id: FPGA:1, crypto map: vpn
        sa timing: remaining key lifetime (k/sec): (4525504/1716)
        IV size: 16 bytes
        replay detection support: N
        Status: ACTIVE

     inbound ah sas:

     inbound pcp sas:

     outbound esp sas:
      spi: 0x50F4327D(1358180989)
        transform: esp-aes esp-sha-hmac ,
        in use settings ={Tunnel, }
```

In this extract all the parameters in bold italic imply that the tunnel is established meaning encryption and decryption is functional. The Security Parameter Index (SPI) values must not be zero and once it is zero it means the tunnel is not established.

pkts encaps: 2180, #pkts encrypt: 2180,

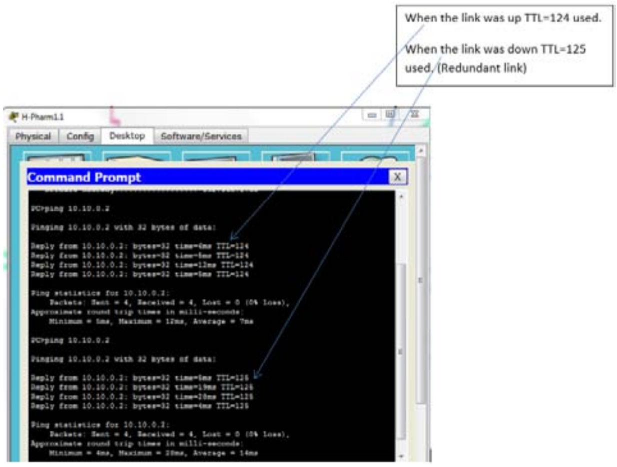
#pkts decaps: 2181, #pkts decrypt: 2181,

Moreover, the tunnel status also shows active.

4.3 High Availability Test

This test was done by first shutting down the tunnel interface of the Headquarter router by inputting the following command (a) enable, (b) configure terminal, (c) interface S0/0/0, (d) shutdown, then interface where the tunnel was established will be disable while the node in the network will automatically change from Green to Red which implies that the tunnel can no longer be accessible. The command *traceroute***(tracert)** is input from a user in any of the headquarter VLAN 192.168.1.66 or branch in Fig 2 and 3 via the command prompt to ascertain the flexibility and toughness of the network when the interface of the branch tunnel is turn off or fail, it was noticed that the route to the FHC PC referral took a hops 192.168.1.65 (default gateway), 192.168.1.210 (Headquarter core router gateway), 192.168.100.1 (tunnel head-end at the headquarter)and then proceed to its final destination 10.10.0.2 the route trace was completed successfully, below is a capture of the screen shot displaying it.To further support the proof pinging was done on the same user then the same tunnel interface link was up, and later it was shut down and another ping was done, it was still replaying meaning the redundant link has been used to access other part of the network. Below is the screen shot.

To buttress the high availability test further, a similar test was carried out, a user 192.168.5.3 from the branch Accident & Emergency VLAN in Fig 9 and 10 to FHC referral PC 10.10.0.2 the Branch tunnel interface was up for a little while and later it was shut down. Then the result obtained from trace route was also like the previous ones which imply that when the Branch tunnel interface fails there is a safe failover to the Headquarter tunnel interface.

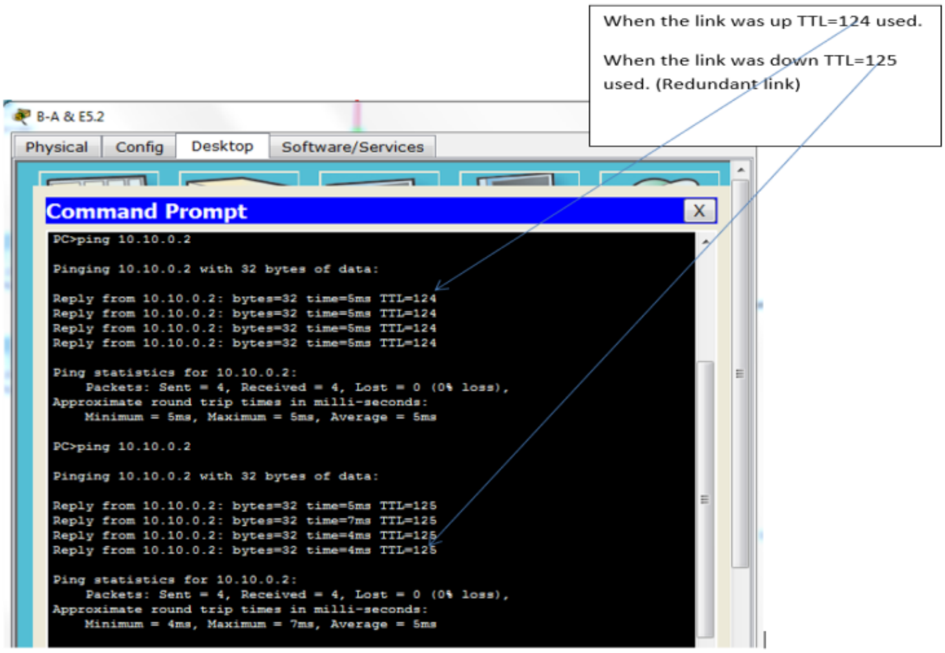


When the link was up TTL=124 used.

When the link was down TTL=125 used. (Redundant link)

```
PC>ping 10.10.0.2

Pinging 10.10.0.2 with 32 bytes of data:

Reply from 10.10.0.2: bytes=32 time=4ms TTL=124
Reply from 10.10.0.2: bytes=32 time=5ms TTL=124
Reply from 10.10.0.2: bytes=32 time=12ms TTL=124
Reply from 10.10.0.2: bytes=32 time=5ms TTL=124

Ping statistics for 10.10.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 12ms, Average = 7ms

PC>ping 10.10.0.2

Pinging 10.10.0.2 with 32 bytes of data:

Reply from 10.10.0.2: bytes=32 time=5ms TTL=125
Reply from 10.10.0.2: bytes=32 time=19ms TTL=125
Reply from 10.10.0.2: bytes=32 time=20ms TTL=125
Reply from 10.10.0.2: bytes=32 time=4ms TTL=125

Ping statistics for 10.10.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 20ms, Average = 14ms
```

Fig. 9 Screen shot displaying ping from HQ 1 to 10.10.0.2 when the link was up and later down.



When the link was up TTL=124 used.

When the link was down TTL=125 used. (Redundant link)

```
PC>ping 10.10.0.2

Pinging 10.10.0.2 with 32 bytes of data:

Reply from 10.10.0.2: bytes=32 time=5ms TTL=124
Reply from 10.10.0.2: bytes=32 time=5ms TTL=124
Reply from 10.10.0.2: bytes=32 time=5ms TTL=124
Reply from 10.10.0.2: bytes=32 time=5ms TTL=124

Ping statistics for 10.10.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 5ms, Maximum = 5ms, Average = 5ms

PC>ping 10.10.0.2

Pinging 10.10.0.2 with 32 bytes of data:

Reply from 10.10.0.2: bytes=32 time=5ms TTL=125
Reply from 10.10.0.2: bytes=32 time=7ms TTL=125
Reply from 10.10.0.2: bytes=32 time=4ms TTL=125
Reply from 10.10.0.2: bytes=32 time=4ms TTL=125

Ping statistics for 10.10.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 7ms, Average = 5ms
```

Fig. 10 Screen shot displaying ping from Branch to 10.10.0.2 when the link was up and later down.

5. Conclusion

In conclusion this research work carried out VPN security which is a basic network requirement where privacy, integrity and high availability is the order of the day. It is more relevant and suitable in a healthcare sector where patients need high degree of privacy and confidentiality of their medical record. The design network uses IPsec VPN and GRE to meet up the security measures as demanded by the client, VPN appears to have nice security features for organization network however is still susceptible to attacks even the most secured network on earth is vulnerable toattacks, a combination of IPsec VPN + GRE will offer a better solution to attacks.Fault tolerance is another essential factor that will guarantee high availability and toughness of a network which is highly needed in a healthcare sector due to emergency that arises at any given time, for a quality health service delivery to be sustained the network link must be resilient and highly available. Therefore, with the present development we can now concluded that the deliverable presented to the client was a successful one.

References

[1] Manghui, T., Liangliang, X. and Dianxiang, X. (2013). “Maximizing the Availability of Replicated Services in Widely Distribution System Considering Network Availability”.In: *IEEE International Conference proceedings on Software Security and Reliability (SERE) 2013 Gaithersburg*, MD 18th–20th June, pp. 178–187.

[2] Gong, G., Qiang, S. and Wang, J. (2009). “Information Security Measures and Regulation Research.” In: *IEEE International Conference Proceedings on Management Science and Engineering (ICMSE)*, Moscow 14th–16th Sept, pp. 2184-2189.

[3] Andrew, T. and Maarten, V. (2007). *Distributed Systems Principles and Paradigms*. Pearson Prentice Hall Inc.

[4] Chen, F., Wu, K., Chen, W. and Zhang, Q. (2013). “The Research and Implementation of the VPN Gateway Based on SSL.” In: *IEEE International Conference Proceedings on Computational and Information Sciences (ICCIS)*, Shiyang, China, 21st-23rd June, pp. 1376-1379.

[5] Jaha, A., Ben-shatwan, F. and Ashibani, M. (2008). “Proper Virtual Private Network (VPN) Solution.” In: *IEEE International Conference proceedings on Next Generation Mobile Applications, Services and Technology (NGMAST)*, Cardiff, UK, 16th–19th Sept., pp. 309-314.

[6] Rossberg, M. and Schaefer, G. (2011). “A Survey on Automatic Configuration of Virtual Private Networks.” *Computer Networks* 55 (8) 1684-1699.

[7] Zaharuddin, M. H. M., Rahman, R. A., and Kassim, M (2010). "Technical Comparison Analysis of Encryption Algorithm on Site-to-Site IPSec VPN." In: *IEEE International Conference proceedings on Computer Application and Industrial Electronics (ICCAIE)*, Kuala Lumpur, Malaysia 5th-8th Dec., pp. 641 -645.

[8] Bruno, A. and Jordan S. (2011). *CCDA 640-864 Official Cert Guide*, Cisco Systems.

[9] Dhall, H., Dhall, D., Batra, A. S. and Rani, P. (2010). "Implementation of IPSec Protocol." In: *IEEE International Conference Proceedings on Advance Computing and Communication Technologies (ACCT)*, Rohtak Haryana, India, 7th-8th Jan, pp. 176-181.

[10] Marwa, A., Malika, B. and Nacira, G. (2013). "Contribution to Enhance IPSec Security by a Safe and Efficient Internet Key Exchange Protocol." In: *IEEE International Conference Proceedings on World Congress Computer and Information Technology (WCCIT)*, 22nd-24th June, pp. 1-5.

[11] Baghaei, N. and Hunt, R. (2004). "Security Performance of Loaded IEEE 803.11B Wireless Networks." *Computers Communications* 27 (2004) 1746-1756.

[12] Amadasun, K., Short, M. and Crosbie, T. (2020). "Telecommunication Infrastructure Sharing: A Remedy for the Reduction of Network Operator Costs and Environmental Pollution?" In: *Proceedings of the 20th IEEE International Conference on Environment and Electrical Engineering (EEEIC 2020)*, Madrid, Spain, June 2020.

[13] Irving, P. (2010). *Computer Networks* (3rded.), Lexden Publishing Limited.

[14] Hassan, H., Eltoweissy, M., and Youssef, M. (2009). "Cell Net: A Bottom-Up Approach to Network Design." In: *Proceedings of the 3rd International Conference on New Technologies, Mobility, and Security*, pp. 433-438.

[15] Bottino, L. J. (2006). "Security Measures in Secured Computer Communications Architecture." In: *IEEE/AIAA 25th Digital Avionics Systems Conference*, pp. 1-18.

[16] Cisco (2007). Available at IPSec Negotiation/IKE Protocols - Configuration Examples and TechNotes – Cisco.

[17] Balchunas, A. (2007). "Static vs. Dynamic Routing." Available online at: http://www.routeralley.com/ra/docs /static_dynamic_routing.pdf.