International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 6 Issue 6 Ver. I ǁ 2018 ǁ PP. 44-57

Design And Simulation Of Internet Virtual Private Network For Large Enterprise Using Riverbed Modeler

N.S. Tarkaa[1],D.N. Nwabuike[2], P. C. Lifu[3]
[1 2 3]*Department of Electrical and Electronics Engineering, University of Agriculture, Makurdi, Nigeria*
Corresponding Author: N.S. Tarkaa

Abstract: *With the emergence of Internet Protocol (IP) as the networking technology for efficient and cost-effective convergent transmission of voice, data and video services, service providers have been transforming their legacy networks and building new ones. A major concern of most organizations is to interconnect their dispersed sites and remote workers through secure links while using the public Internet. Virtual Private Network (VPN) has evolved as one of the growing technologies that enable organizations to achieve this goal and additional service requirements benefits such as speed, cost-efficiency and scalability. Due to concerns of its efficacy for IP networks, various studies are being conducted for different scenarios and types of VPN applications using different approaches and tools. In this paper, a state-of-the-art network simulator, Riverbed Modeler, which comprises of a wide range of networking technologies and protocols is used to design and simulate a Site-to-Site VPN for a large enterprise. Firstly, an IP network comprising of three widely dispersed sites of the enterprise was designed without VPN. Then the network was configured with Site-to-Site VPN and simulation was carried out. The simulation results revealed some positive effects of VPN on the performance of the network.*

Keywords: *Internet Protocol, Network Simulator, Site-to-Site VPN, Tunneling Protocol, VPN Gateway.*

Date of Submission: 09-07-2018 Date of acceptance: 23-07-2018

I. INTRODUCTION

Virtual Private Network (VPN) is a very comprehensive term used to describe a communication network that uses any combinations of technologies to secure a connection tunneled through an otherwise untrusted network instead of using a dedicated connection such as a leased line [1]. A virtual connection is made between geographically dispersed users and networks over a shared or public network. Data is transmitted as if it were passing private connections directly connected.The network of many enterprises or business models today consists normally of many sites which are located very far away from each other due to the vast branches of the enterprise. Leased lines traditionally were used to provide connectivity among these customer sites. Over the years, though, customer networks grew up and it was realized that leased lines had become a very expensive solution and so had become a challenge for network scalability.Virtual Private Network (VPN) came as an alternative. It provided an attractive business model both for provider and customer and got attention. Customers could deploy low cost scalable networks using service provider's network infrastructure, whereas service providers had the capability to generate more revenue just by providing connectivity to many customers using a single backbone [1].

Nowadays, a key area of application of VPNs is Internet Protocol (IP) which has become the universal communications network technology for the efficient and cost-effective provision of voice, data and video services worldwide [2], [3]. Private enterprises with their own IP networks as well as major telecommunications organizations and IP telephony carriers that have developed IP backbones can provide service quality that competes with the traditional Public Switched Telephone Network (PSTN) [3].In using the IP technology through the Internet, more security and traffic control issues are encountered compared with the traditional PSTN [4].Today's VPN solutions overcome the security factor using special tunneling protocols and complex encryption procedures [5].Without VPNs, organizations like the government, the military, large private businesses and even individuals who need some secure access to local area networks for the provision of vital services efficiently and cost-effectively would be handicapped. But with VPN, a secure network access is provided using the Internet which logically connects together locations very far apart as one, and significantly costs less than privately owned leased lines.Although early VPNs required extensive expertise to implement, technology has matured to a level where deployment can be a simple and affordable solution for businesses of all sizes [1].

VPN transmits Data, voice calls and faxes by means of tunneling. Before a packet is transmitted, it is wrapped/encapsulated in a new packet with a new header. This header provides routing

information so that it can traverse a public network before it reaches its tunnel. When each packet reaches the tunnel end point, it is de-encapsulated/unwrapped and then forwarded to its final destination. Both tunnel end points need to support the same travelling protocol. Tunnelling protocols are operated at either the Open System Interconnection (OSI) layer two (Data link layer) or layer three (Network layer)[6]. The most commonly used tunneling protocols are the Internet Protocol security (IPSec), Layer 2 Tunnelling protocol(L2TP), Point-to-Point Tunnelling Protocol (PPTP) and Secure Sockets layer (SSL). A packet with a private non-routable IP-address can be sent inside a packet with a globally unique IP address thereby extending a private network over the Internet. Site-to-Site IPSec based VPN tunnels are set up across the cloud lab. It's travelling, deploying and management of resources are enabled throughout the cloud interface command line. To ensure data security through encryption and authentication algorithms, an open source IPSecVPN solution is implemented to ensure data confidentiality against third party intruders [7], [8].

Perhaps, due to concerns of its efficacy for IP networks, various studies are being conducted for different scenarios and types of VPN applications using different approaches and tools. Generally a good network simulator comprising of a wide range of networking technologies and protocols that help users to design different network topologies using various types of nodes such as end-hosts, hubs, network bridges, routers, optical link-layer devices, and mobile units would be essential [9]. Such a network simulator is said to belong to a family of commercial and complex simulators [9]. So in this paper, the IP network and VPN were designed and configured using a commercial and complex network simulator, Riverbed Modeler.Riverbed Modeler Academic Edition incorporates tools for all phases of a project, including model design, simulation, data collection, and data analysis [10]. Simulations in the Modeler are run by representing real world devices as nodes and links. The Modeler provides an environment on which attributes of these nodes and links can be configured and used as inputs in the simulation run, after which results are analyzed.

One related previous study also used this modeler but it focused on the design of MPLS VPN between two sites of an enterprise [6]. Another related previous study used Cisco Packet Tracer for design and implementation of different IPSec VPN types for a medium size office [11]. The differences between these previous studies and this study is that (1) they both used presumed traffic values, whereas in this study, systematically estimated traffic values were used, (2) the previous studies did not include the Internet, whereas this study involved configuration and simulation of an internet cloud, (3) the two previous studies both used medium size enterprises, whereas this study was based on a large-scale enterprise configuration.

This paper describes how the Riverbed Modeler Academic Edition was used to execute the VPN project. Firstly, a large enterprise IP network comprising three subnets and Internet cloud for the widely dispersed major cities of Makurdi, Otukpo and Gboko in Benue State of Nigeria was designed and simulated without VPN. Then the network was configured with Site-to-Site VPN and simulation was carried out. The results of the two simulations were compared and they revealed interesting results about the effects of VPN on the performance of the network.

The rest of the paper is organized as follows: VPNsare discussed in section 2. This is followed by the description ofRiverbed Modelerin section 3. Section 4 describes the IP network and VPN configuration and simulation process. The simulation results are presented in section 5. Lastly in section 6 is the conclusion.

II. VIRTUAL PRIVATE NETWORKS (VPNS)

2.1 Definition of VPN

A VPN is defined as a network that uses public network paths but maintains the security and protection of private networks. The Internet Engineering Task Force (IETF) provides the standardized definition of a VPN as a network in which connectivity among multiple private Wide Area Networks (WANs) is deployed using shared IP infrastructure with the same policies as a private network.A VPN is also described as an extension of a private intranet through a public network infrastructure to provide a secure, cost effective and reliable communication channel between two ends. The private tunnels provide help in this extension of the private intranet to enable the point-to-point communication for data exchange [6].

The VPN conceptis illustrated inFig. 1 [12]. Imagine two points A and B. A and B are connected through point C but everyone can see and hear everything that is happening between point A and B because everyone has access to point C. So a continuous impenetrable tube is run between A and B so that no one at point C can see or hear what is being passed down the tube. A and B now have secure communication. This is what is called Virtual Private Network (VPN). It is as if A and B are part of the same location [12].

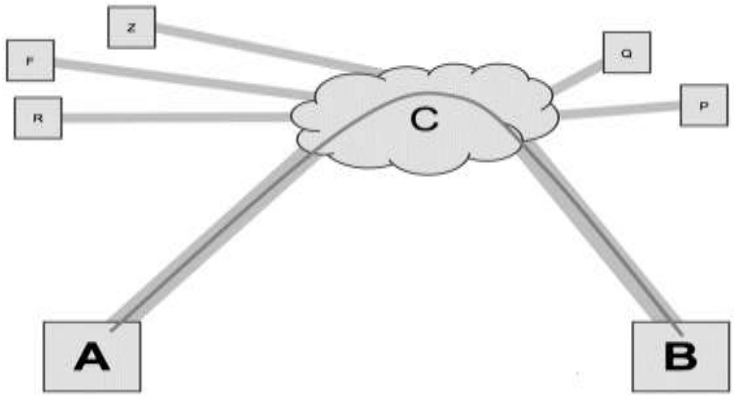


Figure 1: VPN Concept

2.2: Types of VPN

There are three broad categories of VPNs: host-to-host, site-to-site and remote access configurations [13].

2.2.1 Host-to-Host configuration

In host-to-host configuration, a VPN tunnel is established between two hosts that want to initiate a secure communication without relying on gateways[13].

2.2.2 Remote access VPNs

In remote access VPNs, every host must have VPN client software. Whenever the host tries to send traffic to the protected network, the VPN client software encapsulates and encrypts the data before it is sent over the Internet (or public infrastructure) to the target VPN gateway. Upon reception, the VPN gateway behaves in the same way as the site-to-site peer; decrypting and detaching the IP header before forwarding it to its private subnet. Remote access protocols are more varied. The point-to-point tunneling protocol (PPPTP) layer two tunneling protocols, (L2TP), SSL/TLS, IPsec are all used to deliver remote access VPNs [14].

2.2.3 Site-to-Site VPN

A Site-to-Site VPN is also called a Router-to-Router VPN and is mostly used in corporate based operations. For the fact that many companies have offices located both nationally and internationally, a Site-to-Site VPN is used to connect the network of the main office location to multiple offices. This is also known as an Intranet based VPN. The opposite is also possible with Site-to-Site VPN. Companies use Site-to-Site VPN to connect with other companies in the same way and this is classified as an Extranet based VPN. In simple terms, Site-to-Site VPNs build a virtual bridge that joins networks at various locations in order to connect them to the Internet and maintain a secure and private communication between these networks.

Similar to that of a PPTP VPN, Site-to-Site VPN works to create a secure network. However, there is no dedicated line in use allowing the various sites within a company connect to form a VPN. Also unlike PPTP, the routing, encryption and decryption is done by either hardware or software based routers on both ends.

The most commonly deployed secure protocol used in site-to-site VPN set up is the IPsec protocol according to Gupta M. et al., (2007). VPNs are largely deployed using IPsec protocol because of its ability to enhance productivity and communication thus increasing the flexibility of the network [7]. An example of Site-to-Site VPN is shown in Fig. 2 [15].

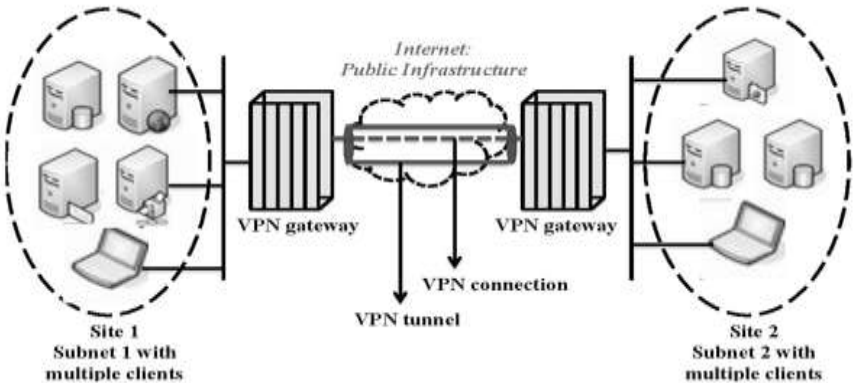


Figure 2: Example of Site-to-Site VPN

Further classifications of VPNs according to protocol and types are given in the following sections [7].

2.2.4 PPTP VPN

PPTP stands for Point-to-Point Tunneling Protocol. Like its name states, a PPTP VPN creates a tunnel and captures the data. PPTP VPN is the most commonly used VPN. PPTP VPNs are used by remote users to connect them to the VPN network using their existing internet connection. This is a useful VPN for both business users and home users. To access the VPN, users log into the VPN using an approved password. PPTP VPNs are ideal for personal use and business because they do not require the purchase and installation of extra hardware and features typically offered as inexpensive add-on software. PPTP VPNs are most widely used also because of its compatibility with Windows, Mac and Linux systems.Although PPTP VPNs seem to have many benefits, there is a disadvantage to this VPN. The disadvantage of using a PPTP VPN is that it does not provide encryption. Another disadvantage is that it relies on the PPP or Point-to-Point Protocol to implement security measures.

2.2.5 L2TP VPN

L2TP stands for Layer 2 Tunneling Protocol that was developed by Microsoft and Cisco. L2TP VPNs are VPNs that are typically combined with another VPN security protocol to establish a more secure VPN connection. An L2TP VPN forms a tunnel between two L2TP connection points and another VPN such as IPsec protocol encrypts the data and focuses on securing communication between the tunnels.L2TP is also similar to PPTP. The similarities exist in terms of their lack of encryption and that both rely on PPP protocol to do this. They begin to differ with regards to their data confidentially and data integrity. L2TP VPNs provide both whereas PPTP VPNs do not.

2.2.6 IPsec

IPsec is an abbreviation for Internet Protocol Security. IPsec is a VPN protocol used to secure internet communication across an IP network. A tunnel is set up in a remote site to allow access to your central site. An IPsec works to secure the internet protocol communication by verifying each session and individually encrypts the data packets throughout the connection. There are two modes in which an IPsec VPN operates. The two modes are transport mode and tunneling mode. Both modes are to protect data transfer between two different networks. During the transport mode, the message in the data packet is encrypted. In the tunneling mode, the entire data packet is encrypted. A benefit to using an IPsec VPN is that it also can be used in addition to other security protocols to provide a stronger security system.

Although an IPsec is a valuable VPN to have, a great disadvantage to utilizing this protocol is the expensive time consuming client installations that must occur prior to usage.

2.2.7 SSL and TLS

SSL stands for Secure Sockets Layer and TLS stands for Transport Layer Security. These two work as one protocol. Both are used to build a VPN connection. This is a VPN connection where the web browser serves as the client and user access is restricted to specific applications only instead of an entire network. The SSL and TLS protocol is utilized primarily by online shopping websites and service providers. An SSL and TSL VPN provide you with a secure session from your PC browser to the application server. This is because web browsers switch to SSL easily and require practically no action from the user. Web browsers already come integrated with SSL and TSL. The SSL connections have https in the beginning of the URL instead of http.

2.2.8 MPLS VPN

Multi-Protocol Label Switching or MPLS VPNs are best used for Site-to-Site type of connections. This is primarily due to the fact that MPLS are the most flexible and adaptable option. MPLS is a standards based resource that is used to speed up the distribution of network packets over multiple protocols. MPLS VPNs are systems that are ISP-tuned VPNs. An ISP-tuned VPN is when two or more sites are connected to form a VPN using the same ISP. However, the biggest disadvantage of using a MPLS VPN is the fact that the network is not as easy to set up compared to other VPNs. It is also not easy to make modifications. Therefore, MPLS VPNs are typically more expensive.

2.2.9 Hybrid VPN

A hybrid VPN combines both MPLS and IPsec based VPNs. Although these two types of VPNs are used separately at different sites. However it is possible to use both at the same site. This would be done with the intentions of using the IPsec VPNs as back up for the MPLS VPN.

IPsec VPNs are VPNs that require some piece of equipment on the customer side as mentioned previously. This equipment is usually in the form of a router or multipurpose security appliance. Through this router or

multipurpose security device, data is encrypted and form the VPN tunnel as discussed earlier. Comparatively, MPLS VPNs are utilized by a carrier, by means of equipment in the carrier's network.
In order to connect these two VPNs, a gateway is established to eliminate the IPsec tunnel on one side and charts it to the MPLS VPN on the other end while preserving the security that VPNs are intended to provide.
Hybrid VPNs are utilized by companies primarily because using MPLS for their sites would not be the most appropriate choice. There is a great amount of advantages that MPLS has over public internet connections, however the cost is high. Therefore using a hybrid VPN allows you to access the central site through a remote site. Hybrid VPNs are overall costly, however,they offer greater flexibility.

2.3 Making the Right Choice of VPN

In conclusion, making the right choice about which VPN is for you might be a difficult one. In order to determine which VPN is right for you, first determine what type of security that you would like to have. Choosing your VPN will vary depending on whether or not you are a student, small business owner, or own multiple corporate offices. Another idea that you should consider is how extensive your security should be in terms of whether or not to get something simple or more complex like a hybrid VPN. Cost is another factor that comes into play during this decision process. How much money are you willing and is worth spending on securing your internet connection? Once you are able to answer these questions, deciding on which type of VPN to choose will be easier. One idea that could be helpful is to do more research concerning this area. For individual users PPTP VPNs offer the best deals but for large offices or ones with complex requirements for connectivity, MPLS VPNs might be the best option [7].

2.4 How VPN Works

When making a VPN connection, there are two connections. The first connection is made to the Internet Service Provider. In connecting to the service provider, Transmission Control Protocol/Internet Protocol(TCP/IP) and PPP (Point-to-Point Protocol) are used to communicate to the ISP. The remote user is assigned an IP address by the ISP. The user logs into the company login. This second connection establishes the VPN connection and a tunnel is created with the use of PPTP (for example) after the user is authorized. The IP datagrams containing encapsulated PPP packets are sent. In normal connections, the company's firewall does not allow PPP packets from entering the network, thus, internet users are not able to access a private network. However, VPN services allow users who meet security criteria to be admitted. The VPN server disassembles the packet and transfers the packet to the destination computer located in the private network[6].

2.5 VPN Security Mechanisms

A secure VPN consists of two Internet-connected devices that, after having authenticated one another, exchange data over the Internet in a secure fashion. The four processes that comprise a secure VPN are tunneling, confidentiality, integrity and authentication. The four processes are described in the following sections [5].

2.5.1 Tunneling

This is the defining characteristic of a VPN as it allows packets to travel to destinations that would not ordinarily be reachable over the Internet. This allows existing Internet infrastructure to replace a dedicated intersite leased line or dial-up service. A VPN tunnel consists of two Internet-connected devices, one at either end. These tunnel endpoints both dispatch packets to the other endpoint and receive packets, sent by the peer, that are emerging from the tunnel. In order to send a packet down the tunnel it is first placed within another packet. This has the effect of creating a new outermost IP header whose source and destination fields are filled with the addresses of the sending and receiving tunnel endpoints. When this packet is received at the far end of the tunnel, the additional headers concerned with delivery via the tunnel are stripped away and the original packet is regenerated. This mechanism can be used to dispatch two types of packet over the Internet that would, by their very nature, ordinarily be undeliverable:

i. Invalid Protocols

Some sites may employ network-level protocols, such as AppleTalk or Novell's Internet Packet Exchange(IPX), on disparate LANs. The Internet, by definition, only routes IP packets and so other Layer 3 protocols cannot be carried in their native form. Encapsulating an IPX packet within an IP envelope would permit the two campuses to use the Internet rather than private leased lines to exchange Netware traffic.

ii. Invalid Addresses

Many sites employ IP addresses from the designated private ranges on their local networks. A college with several campuses, each using private IP numbers, could use tunneling to allow the campuses to exchange these packets via the Internet.

There are two broad classes of tunneling methods that work by either encapsulating Layer 2 frames, usually, Point-to-Point Protocol or Layer 3 packets.

2.5.2 Confidentiality

A VPN causes traffic local to an organization to be transmitted over infrastructure that carries general Internet traffic. It is essential to guard against the remote possibility that these packets could be intercepted and examined by some third party. Data confidentiality may be achieved by encrypting the payload of any packets that are destined for the remote end of a VPN tunnel (a separation of confidential traffic from public Internet traffic by carrying it along dedicated MPLS circuits is another way of achieving that). The encryption process is a compromise between the inevitable increase in transmission delays and the strength of the cryptographic cipher employed. There are two categories of encryption algorithm and both are used to secure packets that travel over a VPN:

i. Symmetric

These algorithms rely upon the two security endpoints agreeing upon a secret phrase that is used for all subsequent encryptions and decryptions. Although they operate quickly, the great drawback of these encryption algorithms is that the shared key must be agreed in advance over the insecure medium. If this initial exchange were conducted in plaintext, any third party that managed to intercept it would be able to decode all the subsequent encrypted data.

ii. Asymmetric

These algorithms do not require a secret phrase to be shared between the security peers. Each peer generates two keys, one of which (the Public Key) is published while the other (the Private Key) is kept secret. A message that has been encrypted with a peer's Public Key can only be decrypted by means of the partnering Private Key. Despite their great security, these algorithms are slow and therefore unsuitable for ongoing encryption of a stream of data such as IP packets.

A useful compromise between the speed of the symmetric algorithms and the security of the asymmetric type is readily achieved. A fast symmetric algorithm is used for securing the data stream with the shared secret (the Session Key) being encrypted using an asymmetric cipher. This means that transmission times for packets traversing the VPN are kept to a minimum without compromising security by exchanging the Session Key in plaintext. It is normal practice for the Session Key to be assigned a limited lifetime so that it must be periodically renewed. This further increases security, as an attacker would have insufficient time to discover the Session Key by means of some brute force attack before it expires and is replaced with a completely new key.

2.5.3 Integrity

It is vital that any data arriving at one of the endpoints of a VPN is guaranteed to have originated from the recognized security peer and not to have been modified en-route. Both of these assurances can be provided by use of digital signatures.

Passing a message through a mathematical function called a hash function produces a short, fixed-length digest. If even one bit of the original message is changed then a different digest will be produced. Data integrity can be assured by attaching a digest to an outgoing message. When a message that has been transmitted via a VPN is received, the recipient applies the hash function to the data that was sent and compares the resulting digest to one that was generated by the sender and attached to the message. If the two digests differ, the recipient endpoint will know the message has been modified.

The problem with this scheme is that the sender's digest that accompanies the message could easily be replaced with one that had been calculated from the modified data. The recipient would then be unaware that the sender's message had been changed. The digest can be guaranteed to have originated from the sender by instead using a keyed hash function that uses the message and a key as the input. A symmetric hash function is one where the key is a secret phrase that the two security peers have previously agreed upon. A slower, but more secure, asymmetric hash function employs the sender's Private Key. An on-going stream of data will be authenticated using the fast symmetric variant and the key will be the same one used for the symmetric encryption. Because only the two security peers know the key, third parties will not be able change the digest and the recipient can be confident that the message has not been changed en-route from the sender.

2.5.4 Authentication

By introducing VPN technology into the network, servers that would otherwise be shielded from the dangers of exposure to the Internet can be rendered vulnerable. It is absolutely essential therefore that measures be taken to ensure that only approved remote stations are able to inject packets via a tunnel into the local network. Two different techniques can be used to identify approved stations.A password is configured on both of the stations that are acting as the tunnel endpoints. The authentication process requires each endpoint to check that the peer's copy of the secret matches its own in the following way.

i. Certificate Authentication

A digital certificate is installed on each of the tunnel endpoints. Provided the two stations have been configured so as to trust the issuer of the peer's certificate, then authentication will occur. These certificates can either be purchased from a commercial Certification Authority (CA), or the organization can configure a server to generate its own local certificates.

If a number of remote users require access to the organization LAN, then issuing certificates (which can later be revoked if a staff member leaves the organization's employment) allows the network manager more control over who has access to the VPN facilities. For a single remote site, a shared secret is simpler as it does not require any supporting infrastructure and can be quite secure as the two tunnel endpoints can also be statically configured with the other's IP address as an additional identity check.

III. RIVERBED MODELER

Riverbed Modeler was originally OPNET Modeler. OPNET is the registered commercial trademark and the name of product presented by OPNET Technologies Incorporation. OPNET was released in 2006, and it was acquired by Riverbed Technology, an American IT company in 2012 [10]. The modeler is one of the most famous and popular commercial network simulators by the end of 2008. It is based on a mechanism called discrete event system which means that the system behavior can simulate by modeling the events in the system in the order of the scenarios the user has set up. Hierarchical structure is used to organize the networks. OPNET's software environment is called Modeler, which is specialized for network research and development. It can be flexibly used to study communication networks, devices, protocols, and applications [10]. Because of the fact of being a commercial software provider, the modeler offers relatively much powerful visual or graphical support for the users. The graphical editor interface can be used to build network topology and entities from the application layer to the physical layer. Object-oriented programming technique is used to create the mapping from the graphical design to the implementation of the real systems. Topology configuration and simulation results can be presented very intuitively and visually. The parameters can also be adjusted and the experiments can be repeated easily through easy operation through the GUI [10].

Riverbed Modeler inherently has three main functions: modelling, simulating, and analysis. For modelling, it provides intuitive graphical environment to create all kinds of models of protocols. For simulating, it uses 3 different advanced simulations technologies and can be used to address a wide range of studies. For analysis, the simulation results and data can be analyzed and displayed very easily. User friendly graphs, charts, statistics, and even animation can be generated by OPNET for users' convenience. According to the OPNET whitepaper, the modeler's detailed features include [10]:

- Fast discrete event simulation engine
- Lot of component library with source code
- Object-oriented modelling
- Hierarchical modelling environment
- Scalable wireless simulations support
- 32-bit and 64-bit graphical user interface
- Customizable wireless modelling
- Discrete Event, Hybrid, and Analytical simulation
- 32-bit and 64-bit parallel simulation kernel
- Grid computing support
- Integrated, GUI-based debugging and analysis
- Open interface for integrating external component libraries

Because of the consistent endeavor and operation of Riverbed Technology Inc., the modeler is becoming mature and its product maintain a high acknowledgement in the industry [10]. Moreover, the company always keeps an eye on the most recent users' requirements and keeps improving their product which make it very competitive compared with other commercial network simulators. The modeler's main advantage is that, being a commercial network simulator, it generally has complete and up-to-date documentations and they can be consistently maintained by some specialized staff in that company. Its main disadvantage lies in its non-open-source nature in that it has limited access for individuals and other organizations to contribute to its

rapid development and debugging of documentation [10].Common device models used for design of IP network in the Riverbed Modeler environment are as described in Table 1.

Table I:Main Device Models for Network Design in Riverbed Modeler

Models	***Name***	***Description***
Routers, Switches, Servers, Etc.	Variety in object palette	Sorted by manufacturer's name, type, protocols supported and other features.
Links	PPP SONET	The PPP SONET OC 3, OC 12, OC 24, OC48 and OC 192 point-to-point transmission links are used to connect two nodes running IP at speed of 155 Mbps, 622 Mbps, 2.5 Gbps and 10 Gbps respectively.
	Gigabits Ethernet	Ethernet duplex links represent Ethernet connections operating at various speeds. They are used for connection of co-located routers.
Utilities	Background Traffic	This node was used for configuration of traffic attribute used to generate background traffic utilization and the traffic modelling practice.
	Application Definition	Used for application specification, and voice encoder schemes.

IV. DESIGN OF IP NETWORK AND VPN CONFIGURATION

4.1 Block Diagram Formation

The block diagram of the proposed three-sites VPN is shown in Fig. 3.

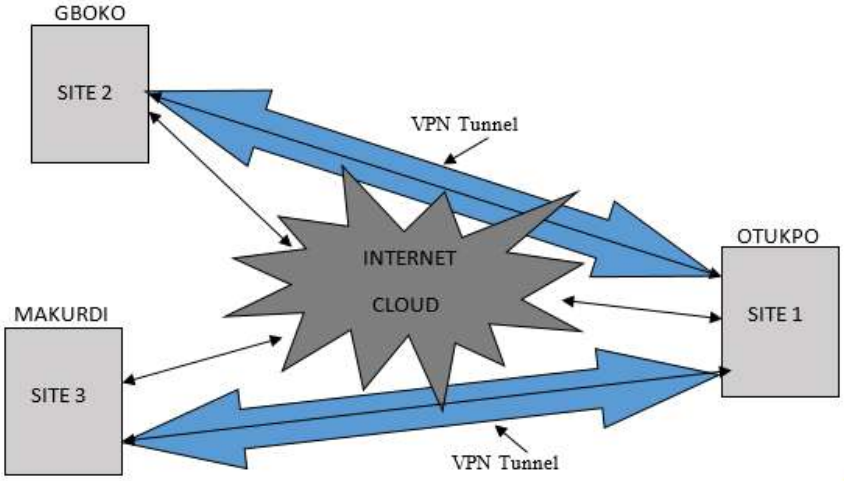


Figure 3: The block diagram of the proposed 3-sites VPN architecture

4.2 The Three Sites without VPN

First, the IP network was designed and configured in Riverbed Modeler environment without VPN. An Internet cloud in which three routers are interconnected by high-speed OC 48 (2488.32 Mbps) links serves as the Internet and connects three business Enterprise Subnets using PPP E1 (2.048 Mbps) links. Gboko and Makurdiserve as branch Subnets with a workstation each. Otukposerves as the Headquarter Subnet with three workstations. Three routers are connected across each workstation in Otukpo Enterprise Headquarters and these three routers are connected to a gateway router in the Subnet. The Routers and workstations in the Enterprise branch and Headquarter Subnets are interconnected usingPPP E1 (2.048 Mbps) links. The needed traffic is generated by configuring both the application, IP and profile configuration objects. After the configuration is completed, the performance of the Internet cloud is evaluated in terms of the three routers contained in it. The simulation is done in such a way that for the 'three sites without VPN' scenario, all the workstations at Gboko, Otukpo and Makurdi gain access to the Internet. And, the scenario is chosen and named as three sites without VPN scenario. The Enterprise headquarters, branches and Internet subnets are shown in Figs. 4, 5, 6 and7 respectively. Fig. 8 shows the complete view of three sites without VPN as configured in the modeler.

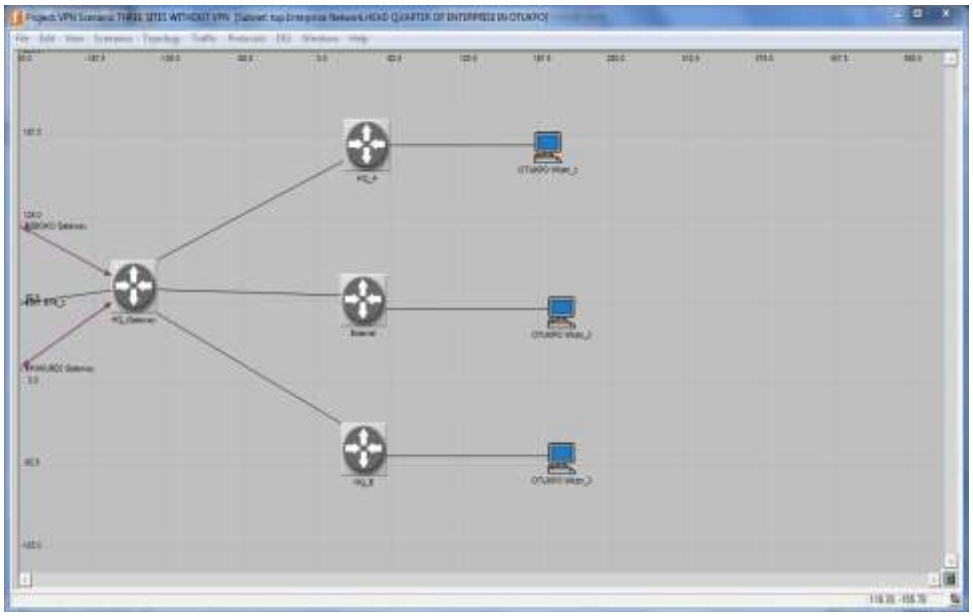


Figure 4: Otukpo headquarter subnet

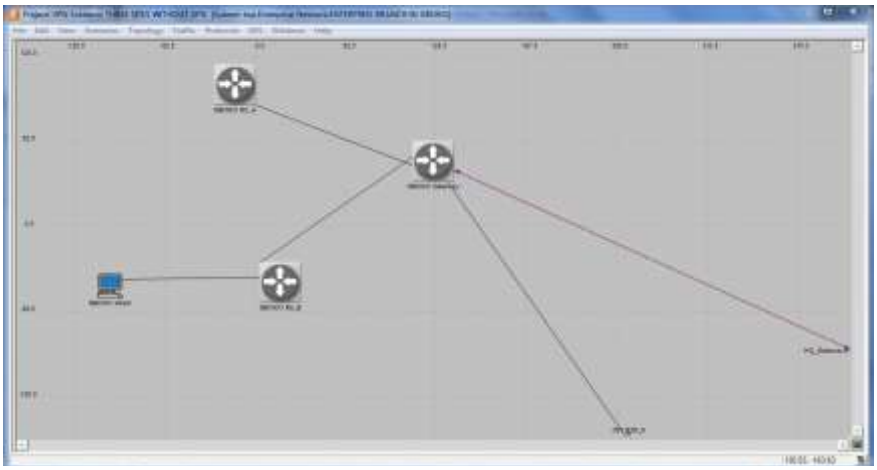


Figure 5: Gboko branch subnet

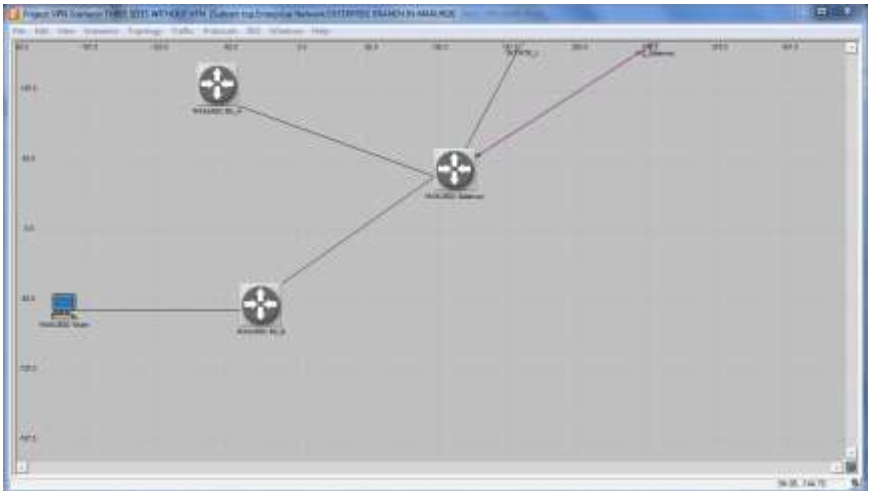


Figure 6: Makurdi branch subnet

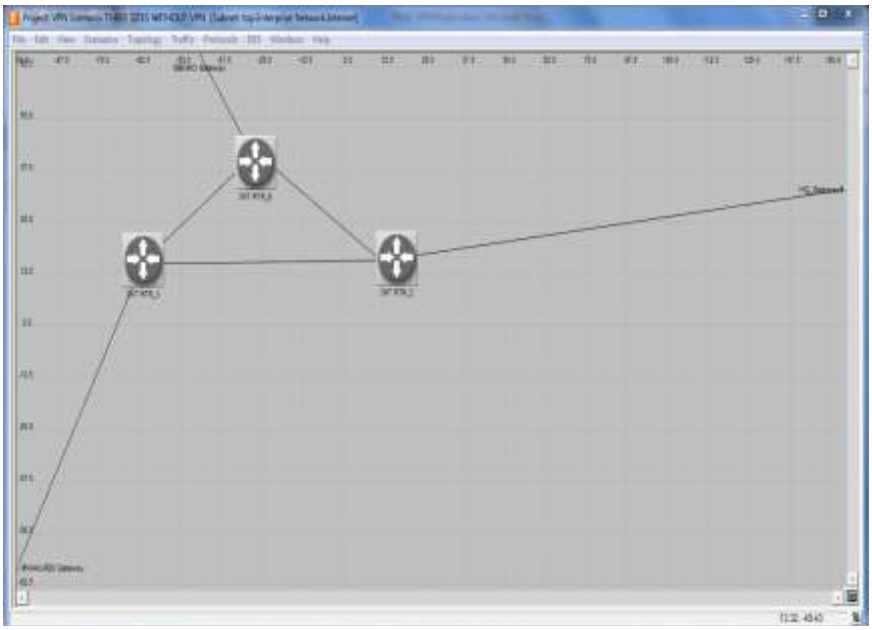


Figure 7: The Internet

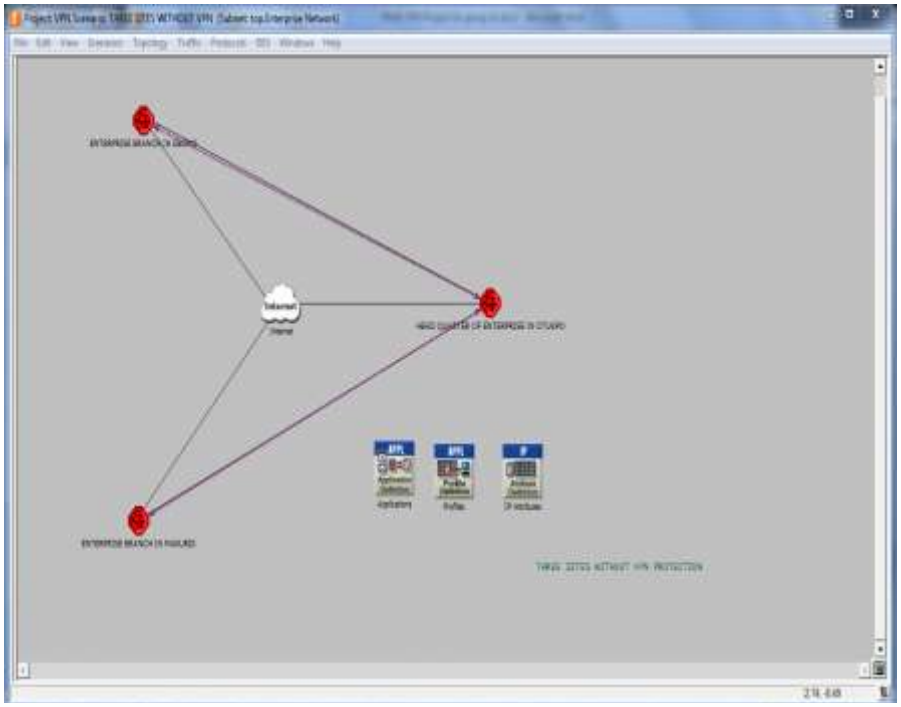


Figure 8: Complete view of three sites without VPN

4.3 The Three Sites with VPN

This scenario was designed by duplicating the previous scenario (that is three sites without VPN). To duplicate the first scenario and configure it as VPN protected, the procedureis described by thefollowing steps.

i. Double click on the VPN configuration in the object palette and drag it to the work space. Then Right click on it and set its name to VPN, then edit the attributes.

ii. Expand the profile configuration as shown in Fig. 9.

Fig. 10 shows the complete view of the three sites with VPN scenario as configured in the modeler.

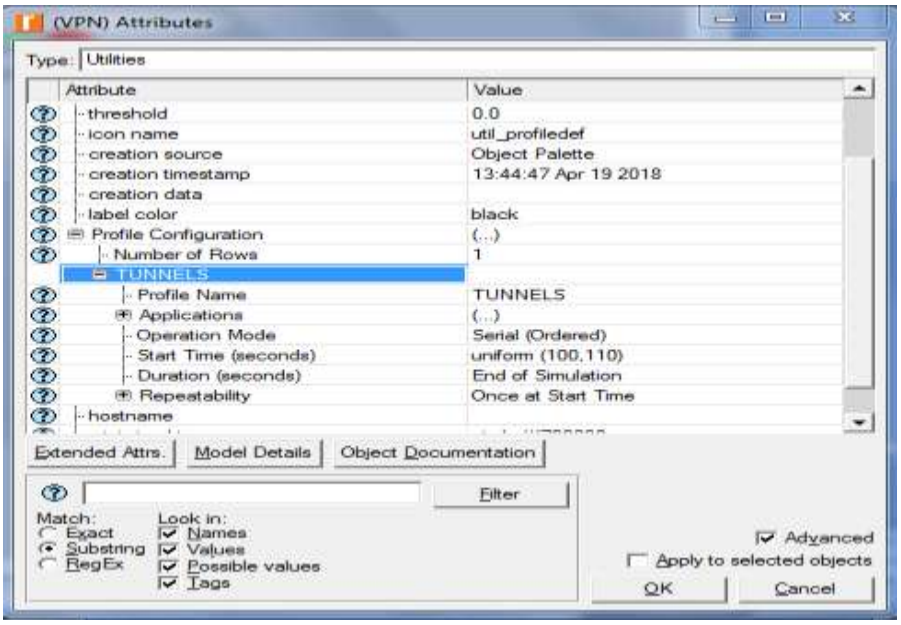


Figure 9: Profile window for VPN configuration

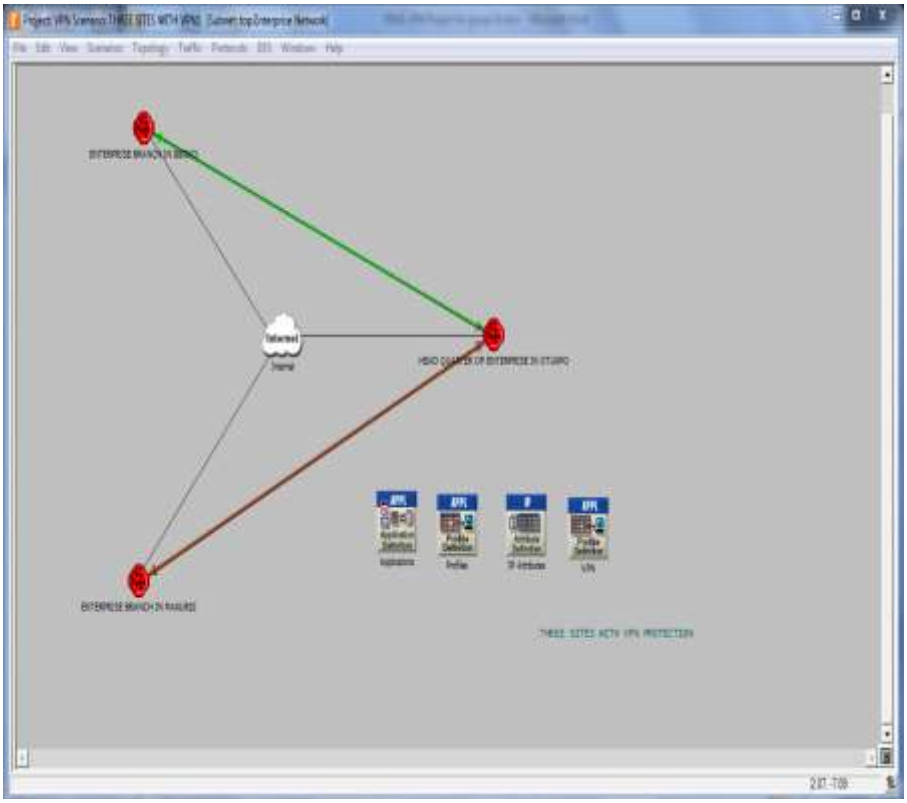


Fig. 10: Complete View of three sites with VPN

V. SIMULATION AND ANALYSIS OF RESULTS

After configuring of the two scenarios (that is 'three sites without VPN' and 'three sites with VPN'), theVoIP traffic was configured as shown in Fig. 11.For Gboko, the traffic is given as 7516 Erlangs while the call duration is 192 seconds. For Makurdi, the traffic is given as 7735 Erlangs while the call duration is 194 seconds and for Otukpo, the traffic is given as 5388 Erlangs while the call duration is 205 seconds. This is achieved by selecting the 'manage scenarios' option from the scenario menu. The given traffic parameters were gotten from a previous study [16].Then simulation was run for one hour.

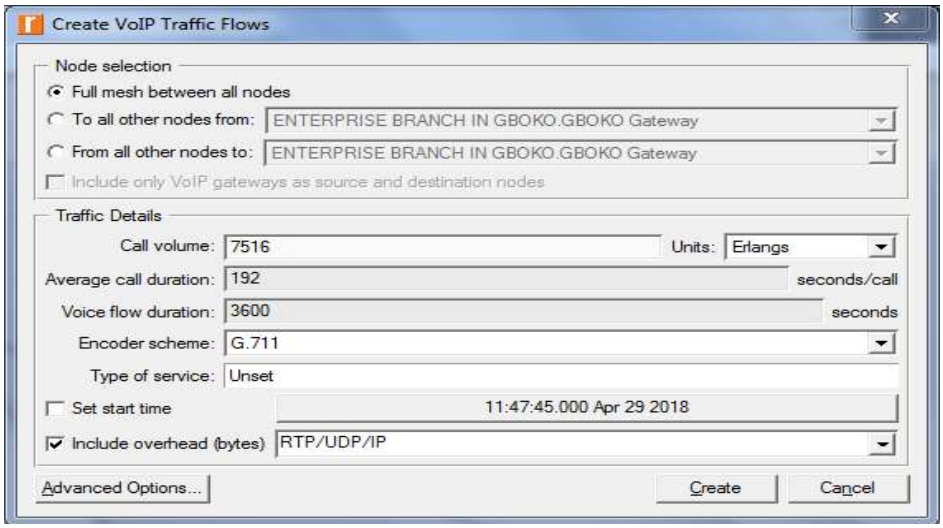


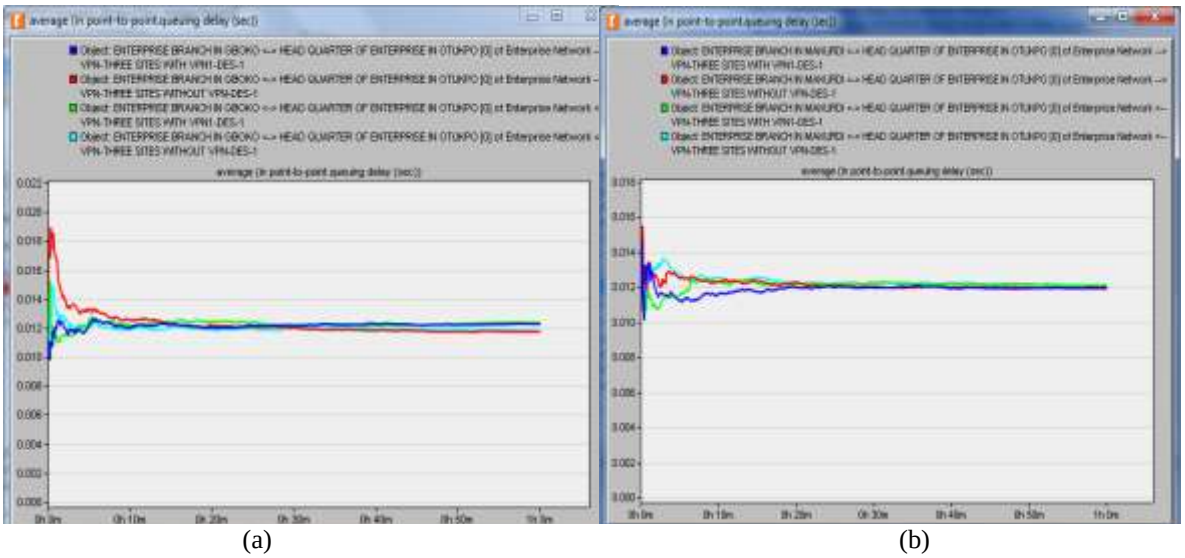
Figure 11: Pictorial view of the traffic configuration window

The performance metrics chosen for display of the simulation results were: packet queuing delay (in seconds) which benchmark is150ms; throughput (in bits per second); and bandwidth utilization (in percentage) which benchmark is100%.

5.1 Analysis of Packet Queuing Delay

Queuing delay is one of the key indicators used to ascertain the performance of the network. In this project, queuing delay refers to the statistics that represents instantaneous measurements of packet waiting times in the transmitter channel's queue. Measurements are taken from the time a packet enters the transmitter channel queue to the time the bit of packet is transmitted. It is measured in seconds. The delay may slightly vary based on the amount of traffic going through the network. Fig. 12 (a) and (b)represents the graphs obtained for queuing delay.

Queuing delay for both with and without VPN for sent and received packets to and from the Gateway of Enterprise Branch in Gbokoby the headquarters of Enterprise in Otukpois estimated to be approximately 0.012 seconds. It is 0.0125 seconds with VPN active and 0.012 seconds without VPN applied. Queuing delay for packets sent and received by Gateway of Enterprise Branch in Makurdi for both with and without VPN is also estimated to be approximately 0.012 seconds.Hence in average, the queuing delay of packets sent and received to the Enterprise branches gatewaysfrom the Headquarter Gateway in Otukpo is the same for both with and without VPN scenarios. Hence for a large enterprise network, the application of VPN does not affect the quality of service in the network.



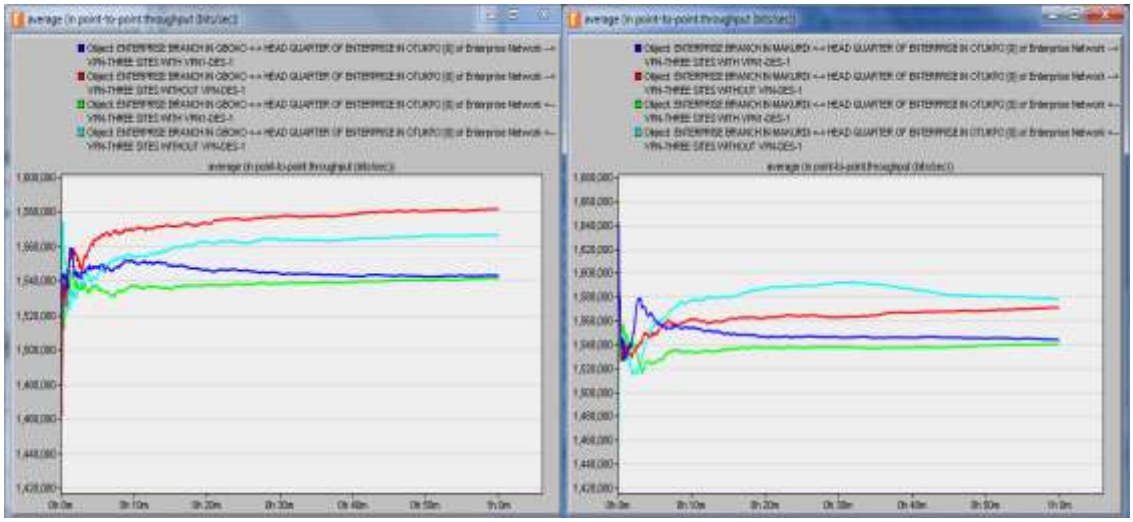
(a) (b)

Figure 12: Packet queuing delay sent and received to and from enterprise branch in (a) Gboko and (b) Makurdi by headquarter of enterprise in Otukpo for both with and without VPN

5.2 Analysis of Throughput

For this project, throughput is a statistic measured that represents the average number of bits successfully received or transmitted by the receiver or transmitter channel per unit time in bits per second. Its measurement might vary based on the different locations of the Enterprises. Fig. 13 (a) and (b)represents the graphs obtained for throughput.

The throughput for sent and received packets from the Enterprise headquarters in Otukpowith VPN for Enterprise branch at Gboko is approximately 1540000 bits per second while without VPN, it is approximately 1568,000 bits per second.For Enterprise branch in Makurdi, packet data throughput sent and received with VPN application is approximately 1540000 bits per second while without VPN, throughput sent is 1570000 bits per second and that received is 1580000. It can be seen that in this case too, there is no significant change in the values of throughput for sent and received traffic with and without VPN. Hence the application of VPN for the large enterprise network proved successful.

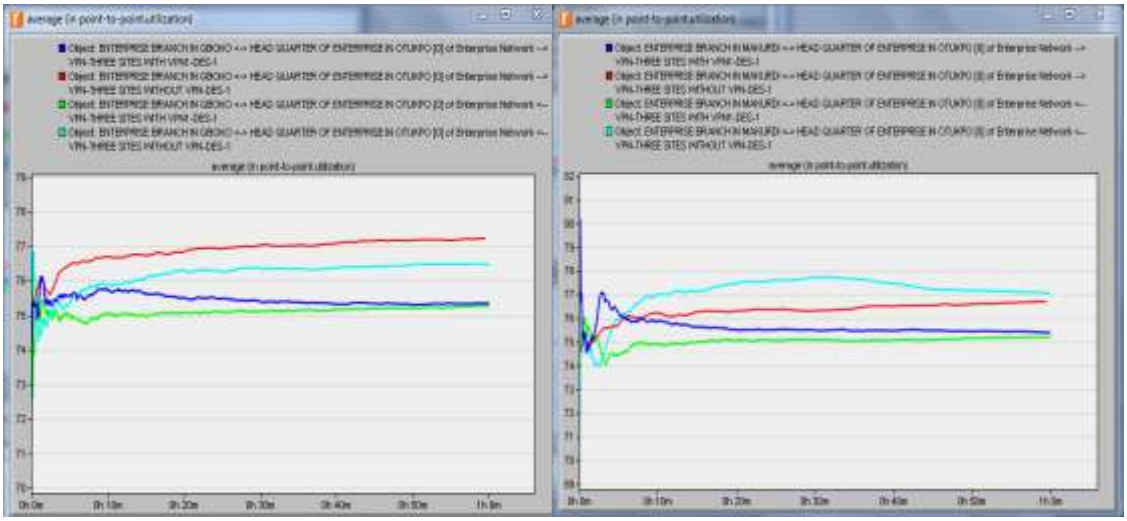


(a) (b)

Figure 13: Throughput sent and received to and from enterprise branch in (a) Gboko and (b) Makurdi by headquarter of enterprise in Otukpo for both with and without VPN

5.3 Analysis of Bandwidth Utilization

For this project, utilization is the statistic that represents the percentage of the consumption to date of an available channel bandwidth, where a value of 100 would indicate full usage. Fig. 14 (a) and (b)represents the graphs obtained for bandwidth utilization.



(a) (b)

Figure 14: Bandwidth utilization sent and received to and from enterprise branch in (a) Gboko and (b) Makurdi by headquarter of enterprise in Otukpo for both with and without VPN

Bandwidth utilization from Enterprise Headquarter in Otukpo to its branch in Gboko is the same for the sent and received packets with an approximate value of 75.3% with VPN. Then for without VPN scenario, its sent utilization has an average value of about 77% while its received has a value of about 76.5%.The Bandwidth utilization from Enterprise Headquarter in Otukpo to its branch in Makurdi is the same for the sent and received packets with an average value of 75.5% with VPN. While for without VPN scenario, its sent utilization has an average value of about 76.7% while its received has a value of about 77%.So in average, the network is seen to be well utilized in both scenarios. It can be seen that the application of VPN enhances the scalability of the network since it gives lower bandwidth utilization.

VI. CONCLUSION

VPN provisioning using legacy technologies including the PSTN have been available for a long time, but over the past few years IP and IP/Multiprotocol Label Switching (MPLS) based VPNs have become more and more popular. As it is usually the case whenever such transformation from legacy to IP based technologies occur, various studies are being conducted for different scenarios and types of VPN applications using different approaches and tools to evaluate its efficacy and effects in relation to IP network performance. This study considers the design and performance evaluation of an Internet based Site-to-Site VPN network for a large-scale enterprise using a state-of-the-art network simulator, Riverbed Modeler (Academic Edition). The network was optimally designed with IP/MPLS enabled routers and SONET PPP transmission links. The network was then duplicated in Riverbed Modeler environment and configured with VPN attributes thus creating two scenarios with and without VPN. Then, using systematically estimated traffic parameters from a previous study, the two scenarios were configured with VoIP traffic and simulated. The simulation results showed that the performance indication for the two network scenarios, that is, with and without VPN, were almost the same andgenerally efficient. Moreover, there was an indication of enhancement of network scalability with VPN. Thus this study has proved the efficacy and effectiveness of the application of VPN technology for a large Enterprise. The study proposes a methodology that may be used for optimal provision of VPN for large enterprises in particular.

REFERENCES

[1]. Gregory J.C., Virtual Private Network (VPN) security, SANS Institute GIAC Paper, January 4, 2001, www.giac.org/paper/gsec/380/virtual-private...

[2]. Dr. K.V. Prasad, *Principles of digital communication systems and computer networks* (Charles River Media Inc: Dreamtech Press, 2003, pp 176-180, 233-239).

[3]. Computer Desktop Encyclopaedia, The Computer LanguageCompany Inc. [Online]. Available: www.computing-dictionary. the freedictionary.com/IP+Telephony, *Integrating IP telephonywith the PSTN*. [Accessed: Jan. 7, 2013].

[4]. Angelos D.K., A comprehensive survey of Voice over IP security. Research in IEEE communications survey and tutorials, (New York, 2010).

[5]. An Overview of VPN technology. [Oneline]. Available: https://comunity.jisc.ac.uk/library/advisory-services/overview.vpn-technology.

[6]. Shahid Ali Bilal ZahidRana, *OPNET analysis of VoIP over MPLS VPN with IP QoS*, Master's thesis, School of Computing, Blekinge Institute of Technology SE – 371 79 Karlskrona Sweden, 2011.

[7]. Hurwitz, J., Bloor, R., Kaufman, M. and Fern, H. *Cloud computing for dummies*, 1st edition, pp 103-125, 2011.

[8]. What is a virtual private network? [Online]. Available: ptgmedia.pearsoncmg.com/…/1587051796/content.pdf. [Accessed July 2, 2018.

[9]. Jianli Pan, A Survey of network simulation tools: current status and future developments, November, 2008. [Online]. Available:http://www.cse.wustl.edu/~jain/cse567-08/index.html. [Accessed: March 2, 2017].

[10]. Introduction to Riverbed Modeler Academic Edition: Common procedures when using Riverbed Modeler Academic Edition. [Online]. Available: splash.riverbed.com/docs/Doc-4833. [Accessed: Aug. 6, 2017].

[11]. Bett Collins, *Design and implement a VPN (Virtual Private Network) for a medium office*, B.Sc. thesis, Department Of Electrical And Information Engineering, University Of Nairobi, Kenya, 2016.

[12]. VPN images. [Online]. Available: https://search.google.com/search?q=images+of+private+network&tbm. [Accessed: July 2, 2018].

[13]. Kent K., Frankel S., Lewkowski R., Ritchey R.W., and Sharma S.R., *Guide to IPsec VPNs*. (NIST Spec. Publ., pp. 800–77, 2005).

[14]. Cisco Remote-Access VPNs: business productivity, deployment, andsecurity considerations, (2015), [Online], Available: http://cisco.com/c/en/us/products/collateral/security/asa-5500-series-next-generationfirewalls/prod_white_paper0900aecd804fb79a.html.

[15]. VishaaviBandaru, Design and modeling of an IPsec VPN in virtualized environment. Virtual private network in the cloud, pg. 13, 2015.

[16]. Tarkaa N.S. and Ani C.I., Design of cost effective synthetic IP backbone topology for a developing economy. *American Journal of Engineering (AJER)*. 5(7), 2016.

N.S. Tarkaa"Design And Simulation Of Internet Virtual Private Network For Large Enterprise Using Riverbed Modeler" International Journal of Research in Engineering and Science (IJRES), vol. 06, no. 06, 2018, pp. 44-57.