EasyChair Preprint

№ 9793

Network Security and Management of Medium Enterprise Business Network

Ayodele Ajala and Thaier Hamid

February 28, 2023

Network Security and Management of Medium Enterprise Business Network

Ajala, Ayodele Oladimeji. Aoa1crt@bolton.ac.uk, Dr Thaier Hamid. Th5@bolton.ac.uk

MSc Cloud and Network Security,

School of Art and Creative Technology, University of Bolton

***Abstract*—The advent of technology and inclusion in our daily lives and medium sized business enterprises have become apparent as most business cannot function without the use of technology. This has brought about vulnerabilities and security loopholes.**

Secured communication is essential for businesses with numerous branches. The use of Dynamic Multipoint Virtual Private Network (DMVPN) technology has brought an advancement to the communication; however the link will not be well secured. The advent of IP security (IPsec) has however secured the communication link with the use of encryption for Intrusion Prevention Systems (IPS).

This paper illustrates the integration, deployment and configuration of well secured communication links between business branches while considering DMVPN and securing the aforementioned link with IP security (IPsec) while simulating it in a virtual environment using the GNS3 simulator.

***Index Terms*—Local Area Network (LAN), Dynamic Multipoint Virtual Private Network (DMVPN), IP security (IPsec), Intrusion Prevention System (IPS)**

I. Introduction

Medium sized organisations play a very vital role in the economy of any country. Their importance cannot be overlooked as they thrive to become large scale business organisations. Most people categorize Small Scale businesses and Medium Scale businesses together as SMEs which is believed are obviously miles apart in the business hierarchy ranking. According to the research conducted by Ndiaye in 2018, he demystified the whole opinion of researchers classifying the small and medium business enterprise into the same category [1]. Considering the staff strength, a small business enterprise is usually between 0 to 99 persons while a medium sized business enterprise is between 100 to 999 persons working for the organisation.

Moreso, putting into consideration of the different types of network designs available for a Medium Scale Business such as the multihoming required from the Internet Service Providers (ISPs), routers with firewall (FW) capabilities in different locations, Dynamic Multipoint Virtual Private Network (DMVPN) running across the branches, ethernet headquarters and the management and security software to be utilized, there are quite several security vulnerabilities to be considered in this research.

However, technological advent in as much as enabling medium businesses to thrive in the present-day economy can be the downfall of any organisation if adequate security measures are not put into place from the lowest in the Open Systems Interconnection Model (OSI model) which is the Physical layer to the highest which is the application layer. Although, this model explains the framework of the network standard worldwide, this research will only be considering the network layer and Data Link layer. Often, network security issues at layer 2 which is the Data Link layer are not given the same attention as those at higher levels; instead, they concentrate on the device's security for the overall management system [2].

Despite several research already carried out in Local Area Network (LAN) security and enterprise network security, most studies merge both the small and medium business enterprises together when considering the security vulnerabilities and management of network security. There is a huge difference between the small and medium business organisation when considering the Network security and vulnerabilities.

A.

1) Statement of the problem : Connecting multiple business sites have become an issue for medium-sized business enterprises with the increase in the number of security breaches in the technical world. Businesses have become vulnerable to sniffing as attackers keep coming up with different means to attack businesses for personal gains which makes it necessary for medium-sized businesses to increase the security not only within their Local Area Network but also between different office locations [3].

Multiprotocol Label Switching (MPLS) is intended to handle network concerns such as network speed, traffic engineering, Quality of Service (QoS) management, scalability, as well as broadband management, and service demands for the next generation of IP headquarters networks. MPLS Virtual Private Network (VPN) has several amazing characteristics such as high-speed switching, QoS performance, flow control, scalability, and management, among others. However, it is also in a state of insecurity. The network layer tunnelling protocol provides a standardised, dependable, and scalable security method [4]. Label Switching with Multiple Protocols MPLS was first proposed to increase forwarding speed. In comparison to standard IP routing, it just analyses IP headers at the network's edge, rather than examining IP headers in each hop, reducing processing time.

MPLS also enables various key characteristics such as traffic separation, the development of VPNs, Virtual Leased Lines (VLLs), and Virtual Private LAN Services (VPLS). It

Ayodele Oladimeji Ajala is with School of Arts and Creative Technology, The University of Bolton , Deane Road, Bolton, BL3 5AB, United Kingdom, e-mail: ajala_ayodele@yahoo.com

works well in determining the best route to take to reach the destination with minimal downtime. In the event of a problem, the entire network will not be brought down. It operates on layer 2.5, which implies it supports both layer 2 and layer 3 of the Open System Interconnection (OSI) reference Model [5].

Depending on the situation, VPN has become one of the solutions provided. It is a private network connection to a public network. It works by utilizing tunneling and encryption methods. It also demands a series of protocol modifications capable of providing secure communication, data integrity, and confidentiality. The protocol is IP Security (IPsec), which is current model tunneling method used on VPNs [8]. The purpose of this study is to investigate and use the GNS3 network simulator to create IPsec on a VPN.

ISPs employ similar procedures to better secure their client edge routers that give Internet access in a situation where Internet access is supplied to the customer over the MPLS link. Furthermore, the Internet Service Provider (ISP) routing protocols contain built-in procedures that are often activated, increasing the security level even further.

Aims and Objectives: The purpose of this study is to review medium-sized business network security considering the MPLS, VPN, IPsec an,d the DMVPN and the pitfalls o the interconnection for medium-sized business etwork, the MPLS and VPN connections for secured communication between the branches while developing a standard to develop extensive recommendations for data-link network security for threat mitigations for attacks.

This research will also help in developing recommendations for data-link network security extensively while considering IPsec L2VPN and L3VPN while generating a comprehensive approach considering network vulnerability using GNS3 to fully understand security approaches for a medium-sized busi- ness network.

Outlined below are the objectives of this research study:

To critically evaluate secured communication models that can enhance network protection for a medium-sized business enterprise by using a virtual simulation.

To evaluate a method for vulnerability assessment considering the

To determine vulnerability measures against problems between the communication links of head office and the branch offices.

To develop recommendations for network security extensively while considering VPN, IPsec and

To compare different communication protocols and the latency between different branches.

3) Research Questions and Hypothesis : This research aims to observe the network security vulnerability in a medium- sized business enterprise while considering the connections and communication loopholes between the different business locations with IP security into consideration while considering the DMVPN while generating a comprehensive approach considering network vulnerability using GNS3 to fully understand security approaches for a medium-sized business network. This research will also answer some basic questions such as:

What is dynamic multipoint virtual private network (DMVPN)?

What are the advantages and disadvantages of using DMVPN?

Under which circumstances can MPLS be used?

What are the advantages and disadvantages of VPN and DMVPN, the deployment, configuration, and troubleshooting of DMVPN and IPsec technologies?

How will medium-sized organisations benefit from the use of MPLS, the concept of IPsec, the deployment, topology, use-case scenarios and troubleshooting of these technologies and to discuss the future impact of MPLS while considering SD-WAN technology which is widely being used at the moment?

4) Significance of the study : This study is used to break down the use-case scenarios for MPLS, the integration, configuration, and troubleshooting of this major technological concept as well as DMVPN and IPsec. Many researchers have focused in recent years on SMEs' network security vulnerabilities, the security challenges faced in the OSI model from the application layer all the way through the physical layer, and the security measures required to successfully run DMVPN, IPSEC, and VPN across multiple branches. The usage of IPsec VPN, which greatly benefits users, creates several challenges for the network service unit and the use unit when performing security audits on network transmission content [9].

5) Scope and limitation of the study : This project is aimed to help medium-sized business organisations integrate and implement higher network security between different locations hence improving the overall network layer security and reducing network vulnerabilities. The goal of the DMVPN over Dynamic IPsec Tunnels functionality is to provide a solution that supports connectivity across overlapping addresses in client site where a remote customer site must be dynamically identified using NHRP while simultaneously safeguarding internet traffic between routers using IPsec. However, due to time and financial constraints, this research will be conducted in a virtual environment using the GNS3 simulator and cisco IOS versions uploaded on multilayer switches to emulate the business head office and branches.

II. THEORETICAL CONTRIBUTION

In the past couple of years, a lot of researchers have focused on network security vulnerabilities of SMEs, the security challenges faced in the OSI model from the application layer all through the physical layer, and the security measures needed in place to successfully run dynamic multipoint virtual private network (DMVPN) across multiple branches. In this research, the solutions and limitations of the researchers will however be discussed and how this paper will help investigate such limitations.

A.

1) Security Issues with Medium Businesses : According to the research conducted by [3], they reviewed the structures and challenges of security policies on small and medium enterprises. The researchers highlighted how small and medium business enterprises do not care or show less effort to information security thereby making them targets of cyber-attacks [3]. The researchers also analysed the perspective of such firms, examined the structure of an information security strategy, and determined its most significant and least important features. However, they considered both small and medium business enterprises as the same entity which are two different entities as I will be discussing in this paper. The security approach for a small business enterprise will not totally be the best approach for a medium-sized business enterprise considering the staff strength and different locations for offices.

The research work done by [11] in his book titled: Information Security Breaches; Avoidance and Treatment Based on ISO27001, the author explored the security breaches, the avoidance and the treatment of network security issues. The author also discussed the confidentiality, integrity, and availability and explored difference recovery plans in case of a security vulnerabilities [11]. This research however, does not discuss the forms and mode of secure communication between the headquarters and the branches which will be investigated in this research.

2) IPsec over DMVPN : The research work done by [13] considered the study of DMVPN alongside IPsec which were configured in a couple of branches. The researchers also did quantitative and qualitative research on the impact of DMVPN in remote locations well considering the voice over Internet Protocol (VOIP), the jitter, and the latency [13]. The researchers also quantified an evaluation result using the voice-over IP and video conferencing between the branches. In their conclusion, it was drawn that IPsec increased the header by 9% but this does not affect the quality of service as the overhead alongside the data ahead will be transmitted. However, for future works, the researchers will be considering MPLS over the wireless network as this was only done across the wired network.

In the research work of [6], IPsec was implemented on nexus switches alongside Software Defined Network (SDN) using site to site and host to site VPNs. The goal was to determine how the P4-IPsec would be configured, the performance of the security details with the Internet Key Exchange (IKE), setting up new tunner end points and evaluating the results [6]. However, their research was limited in the 3rganizatio of the implementation as the prototypes used didn't use the DMVPN technology or the IPsec in SDN.

The MPLS protocol was created to improve and control network traffic flow amongst service provider networks and commercial wide area networks. The Internet Engineering Task Force (IETF) proposes it for effective system traffic routing, switching, and forwarding [5].

4) DMVPN and IPsec : According to the research carried out by [4], they proposed running DMVPN across multiple business branches. They also configured GRE over IPsec for the business branches which will run as the tunnel between the offices. HSRP was used for redundancy, and this was all developed on GNS3 [16] In their research DMVPN was integrated to secure the communication between the branches and headquarters. However, MPLS was not considered in this research which will be considered in this paper. They also used Wireshark to capture the packet flow between the head office and the branches to analyse the packet headers. Using Wireshark is however not a proactive security measure as the damage will already be done by the intruder. The software is also limited to TCP/IP which is basically a transport layer protocol hereby limiting the research to just a layer in the OSI model. This will be addressed comprehensively by considering other layers in the OSI model and, proactive measures to prevent security vulnerabilities.

Also, according to [7], the DMVPN network performance was considered based on different routing protocols and IP security encryption. The critically analysed the different routing protocols such as EIGRP, OSPF, and are RIPv2 at different DMVPN phases, that is, phase one and phase two while considering the latency, jitter, packet loss, and throughput [7]. Their result depicted different latencies for different DMVPM phases while considering the routing protocols, but as it is not advisable to run more than one routing protocol across the network to prevent issues such as high overhead and high CPU utilization, their result was inconclusive on the preferred routing protocol. However, in this paper, the static route will be used across the network.

[18] in their research determined the throughput, jitter, and packet loss associated with the use of three different routing protocols. They configured each routing protocol in the DMVPN phases 1 through 3 while comparing the parameters of each routing protocol [18]. However, MPLS was not considered in their research while only three parameters were considered. It was discovered that RIP version 2 had the highest latency while the EIGRP had the best jitter value.

The combination of the above research and the limitations will be examined in this research and how a medium sized organization can benefit from proactively preventing vulnerabilities spanning across MPLS, DMVPN and IPsec to enable the business enterprise to thrive while maintaining a well-secured network across the business enterprise intercommunication.

III. METHODOLOGY

This research will be using the experimental approach as a research methodology. The experimental research is a type of research used to undertake a discovery test a hypothesis or demonstrates a known fact. This, however, will be conducted in a simulated environment using the GNS3 simulator to test the DMVPN hypothesis.

The DMVPN connection alongside the IPsec will also be demonstrated in the simulated environment to understand the network security challenges of a medium sized business enterprise. Masruroh et al, (2018) conducted an experimental approach to compare the performance of

DMVPN using 3 different protocols. In their observation, they recorded the parameters such as throughput, jitter, and packet loss. They also compared the routing protocols with respect to the DMVPN phase one call mark phase two, and phase three respectively [18].

IV. IMPLEMENTATION AND TESTING

IPsec may be used in either transport or tunnel modes. Transport mode secures IP traffic transferred between two network sites (host-to-host scenario). Tunnel mode secures IP traffic in branch-to-headquarters communication of branch-to-branch communication situations [6]. The communication between the medium-sized business enterprise headquarters and branches we will be over the DMVPN. This configuration, however, will be divided into four different stages the first stage being the configuration of the multipoint GRE tunnel, the second stage will involve the configuration of the Next Hop Resolution Protocol (NHRP), the third stage will involve the routing protocols such as our Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF) or Border Gateway Protocol (BGP), while the last page will involve securing the tunnel using IP security. For the purpose of this research, we will be running the static route as the use of routing protocols increases the complexity. The static route has an administrative distance of 1 while other routing protocols have higher administrative distances when compared to the static route.

The static route has a faster convergence time when compared to other routing protocols such as the OSPF which is the industry standard with an administrative distance of 110, EIGRP which is Cisco proprietary with an administrative distance of 90 and RIP which has a maximum of 15 hops and also an administrative distance of 120 [10]. Table 4.1 indicates the different configuration stages:

Table 4.1 Configuration Stages

Configuration Stage	**Configuration Process**
1	Multipoint GRE
2	Next Hop Resolution Protocol
3	Routing Protocol (OSPF, EIGRP, RIP and static routes)
4	IPsec over DMVPN

A.

1) *Multipoint GRE :* A GRE tunnel connects to a wide range of network layer protocols by encapsulating and forwarding packets across an IP network. DMVPN employs multi-point GRE encapsulation and dynamic routing protocols, removing many of the support concerns associated with conventional VPN systems [16].

GRE tunnels are considered overlay networks since they are built on top of an existing transport network, also known as an underlay network. When the router wraps the packet for the GRE tunnel, it adds additional header information to it.

Table 4.2: IP Addresses

Location	**LAN IP /24**	**WAN IP /32**	**Tunnel ID**	**Tunnel IP /24**
Headquarters	192.168.0.0	11.11.11.10	1	172.16.0.11
Branch 1	192.168.1.0	1.1.1.10	1	172.16.0.1
Branch 2	192.168.2.0	2.2.2.10	1	172.16.0.2
Branch 3	192.168.3.0	2.2.2.10	1	172.16.0.3

From table 4.2 above, the IP addresses follow the same nomenclature for easy troubleshooting by the network administrator. The first usable IP address for each LAN network IP was used as the local area network IP in the simulation. However, a loopback IP address was used to represent the local network IP address so as to simulate the reachability from the headquarters to each of the four branches and also the communication between each of the branches.

For wide area network communication, public IP addresses are usually provided by the Internet service providers but for this simulation, private IP addresses were used and also, and reachability was ensured using open shortest path first protocol before the tunnel link can be established. The use of the same tunnel identification was encouraged for easy troubleshooting by the administrator.

2) Next Hop Resolution Protocol (NHRP) :

NHRP, like Address Resolution Protocol (ARP) or Reverse ARP, is a layer 2 resolution protocol and cache. The Headquarters router serves as the server, while its branch routers function as clients. The Headquarters keeps a unique NHRP database with all configured branches' public IP addresses. Each branch records its public IP address with the headquarters and searches the NHRP database for the destination branches' public IP addresses in order to construct a VPN tunnel [7]. This makes communication between the different branches and the headquarters easier as they will seem directly connected thereby reducing the need for different tunnel interfaces across the business network.

The third and fourth configuration stages which are the static route configuration and the configuration of IPsec over the DMVPN network will be discussed alongside the implementation in this research.

2) *The DMVPN network:* Before we go into the setting of our routers, we'll go over how the DMVPN is supposed to function. This can aid in understanding of how DMVPN

works in this network:

- Each branch has a constant IPSec connection to the headquarters but not to any other network branch. Each branch identifies with the NHRP server as a client.
- The headquarters router functions as the NHRP server.
- When a branch needs to transmit a packet to a recipient (private) subnet on another branch, it requests the NHRP server for the destination (target) branch's actual (outside) address.
- When the originating branch knows the destination branch's peer address, it can start a dynamic IPSec tunnel to the destination branch.
- The multipoint GRE (mGRE) interface is used to build the branch-to-branch tunnel.
- When there is communication between the branches, the branch-to-branch links are formed on demand. Following that, packets can skip the headquarters and use the branch-to-branch tunnel.
- IPSec is used to encrypt any data passing via the GRE tunnel.

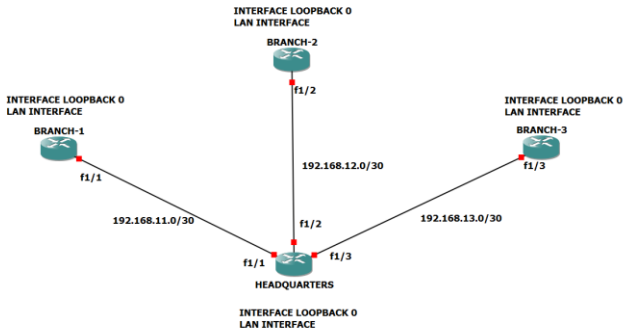

Figure 1: Topology showing the physical interfaces

Figure 1 above illustrates the communication between the headquarters and the branches. Interface fast Internet 1/1-3 All connected to branches 1 – 3 respectively for the wide area network communication. This topology is usually referred to as the headquarters and branch network as it depicts the communication between the branches going through the headquarters.

Advanced network communication is usually between the ISP as the cloud network serves as the mode of communication between the branches, but this is not usually the case as the tunnel between the branches can communicate between each other without traversing the headquarters network.

Type of device and version: Cisco IOS Software, 3750 Software (C3750-JK9O3S-M), Version 15.2(19), RELEASE SOFTWARE (fc1)

A. *Basic Configuration for DMVPN* : During the initial configuration, it was stated that the headquarters router will act as the hub device while the branch routers will be configured as the spoke devices. Because of the simulation however, the interface connecting directly with the spoke devices from the hub and other spoke devices will act as the internet IP addresses which will be the Non-Broadcast Multi Access network (NBMA) with public IP addresses. This will however be simulated with private IP addresses for intercommunication between the hub and spoke routers as depicted in Appendix 4.1

B. *RIP routing protocol for DMVPN* : RIP version 2 is used for the dynamic configuration between the hub and spokes devices. However, the hub local area network depicted by using the loopback address was unable to reach the spoke devices loopback address, hence auto-summary was disabled and the NBMA addresses advertised were used as a /24 address range. This resolved the connectivity issue as the DMVPN was formed over the RIPv2. The commands are illustrated in Appendix 4.2 as the latency is observed to be higher when using RIPv2 as compared to the static routes.

C. *OSPF routing protocol for DMVPN*: Because OSPF is a link-state protocol, it is not very scalable when it is used for the configuration of DMVPN. All devices will have to be configured in the same area to have a complete Link State Database (LSDB) while the branches will be configured as either stub areas or totally stubby areas. However, for this research, the point to multipoint network type will be utilized and all devices will be configured in area zero. This reduces the number of prefixes in the DMVPN network to only the required prefixes thereby enhancing the latency and improving the throughput.

D. *EIGRP routing protocol for DMVPN*: Just like RIP, EIGRP is also a distance vector and is susceptible to issues like the split horizon, hence the remote LAN will not be able to communicate. The no split-horizon command is therefore used to prevent this from happening. The NBMA network is advertised in the EIGRP process and also the LAN network to enable all-around communication between the headquarters device and the branch office device.

E. *Static routing protocol for DMVPN*: The use of a static route enables us to point each route to the required destination. Though the number of static routes increases as the network increases, the processor consumed using static routes is minimal. However, this is not an effective solution when the business enterprise grows and can get more stressful for the network administrator.

```
HEADQUARTERS#sh ip nhrp
172.16.0.1/32 via 172.16.0.1, Tunnel0 created 00:31:03, expire 01:35:36
  Type: dynamic, Flags: unique registered
  NBMA address: 192.168.11.2
172.16.0.2/32 via 172.16.0.2, Tunnel0 created 00:16:38, expire 01:59:57
  Type: dynamic, Flags: unique registered
  NBMA address: 192.168.12.2
172.16.0.3/32 via 172.16.0.3, Tunnel0 created 00:13:12, expire 01:59:54
  Type: dynamic, Flags: unique registered
  NBMA address: 192.168.13.2
HEADQUARTERS#
```

Figure 2: NHRP server connection to clients

The Figure 2 above explains that the NHRP server will be one of the routers. All the other routers will function as NHRP clients. NHRP clients connect to the NHRP server and publish their public IP address. In its cache, the NHRP server maintains record of all public IP addresses. When one router wishes to tunnel anything to another, it will ask the NHRP server for the other router's public IP address. Because NHRP employs this server and client approach, a

headquarters and branches topology makes appropriate for multipoint GRE. Our headquarters router will function as the NHRP server, with all other routers acting as branches. The IP address of the headquarters router will be specified statically on the branches routers while the headquarters router will accept branches routers dynamically. To establish their public IP addresses with the hub, the routers will send an NHRP registration request message. The NHRP server, the hub, will build a connection between the public IP addresses and the tunnel interface IP addresses. After a few seconds, spoke1 chooses to communicate something to spoke2. It must determine the destination public IP address of spoke 2, therefore it will submit an NHRP resolution request to the Hub router, inquiring about the public IP address of spoke 2. The Hub router searches its cache for an item for spoke 2 and sends the NHRP resolution reply to spoke1 along with spoke2's public IP address [20].

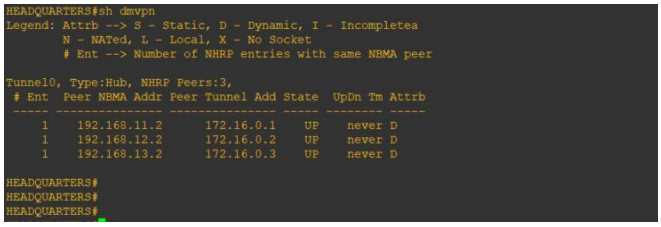

Figure 3: Headquarters DMVPN connections to branches

Figure 3 explains the DMVPN connections between the headquarters and the business branches. The underlay network is the open shortest path first communication between the headquarters and the branches while the overlay network is the tunnel configured between the devices. Dynamic Multipoint Virtual Private Network has 3 phases. All traffic in Phase 1 DMVPN travels through the Hub. DMVPN Phases 2 and 3 build spoke-to-spoke tunnels and transfer traffic directly, skipping the Hub. The ensures faster communication between the business branches.

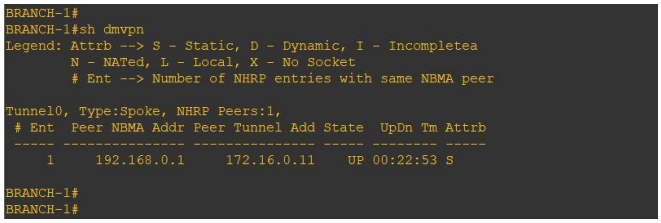

Figure 4: DMVPN communication from Branch 1 to Headquarters

Figure 4 above shows the NBMA address of the headquarters, the tunnel address which is 172.16.0.1 of the headquarters router, the uptime, and the attribute which is observed to be static.

Figure 4 can also be used to analyse the DMVPN attributes which are static, that is the use of static routes for inter communication between the devices, dynamic attribute which indicates the use of dynamic routes such as OSPF, EIGRP and RIP which will be considered in this research to compare the latencies and provide information for the business enterprise. The number of NHRP entries can also be determined and in this case, just a direct entry from the headquarters router to the branch router. However, this will not be the same case when the DMVPN entries are observed from the headquarters router. Each branch device will be shown in the entry as the headquarters acts as the hub for the communication while the branch devices acts as the spoke.

DMVPN allows each spoke to dynamically construct a VPN connection to each other spoke, allowing direct communication without having to route all traffic through the main Hub. This saves bandwidth, time, and money [10].

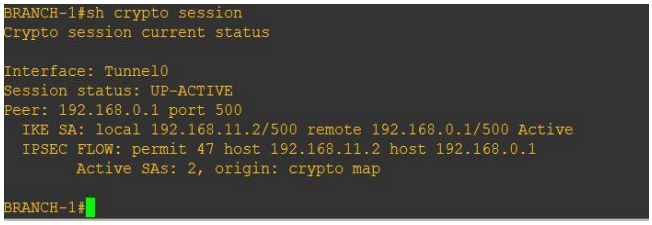

Figure 5: Branch Tunnel Security Configuration.

Figure 5 above shows the crypto session from the first branch office to the headquarters. This contains information such as the interface which is the tunnel 0 interface, the session status which is up and active, the peer and the port in which the peering occurred which are 192.168.0.1 and port 500 respectively. It also contains the local address, the remote address, the port and the port number, the IPSEC flow and the number of active sessions.

V. EVALUATION

This section analyses the experimental research and the result acquired from the simulation of the routers to depict the network security between business branches while mainly focusing of the intercommunication using the hub and spoke technology and securing the link with IPsec.

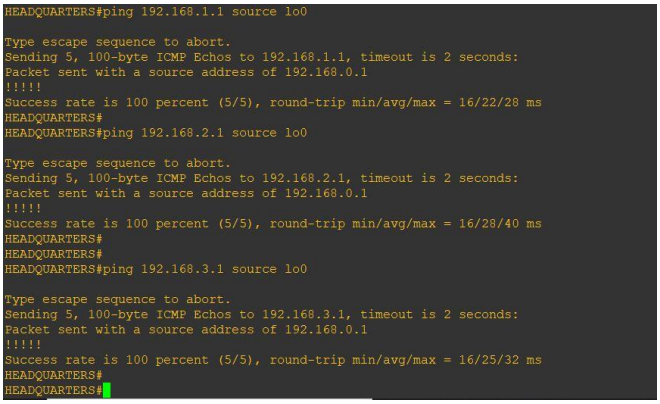

Figure 6: Ping and Latency Test

The Figure 6 above shows the local area network to local area network (LAN-to-LAN) communication between the headquarters and the business branch. This is to ensure the link is fine and the latency is low to ensure secured and smooth functioning of the business. Site-to-Site secure tunnels are used to securely transmit data, files, audio or video between two or more locations. The VPN tunnel is established across the public Internet network and encrypted with a variety of modern encryption algorithms to ensure the secrecy of data exchanged between the two or more locations.

Figure 7: Graph showing the average Latency for each Protocol

Figure 7 above illustrates the average latency from the business headquarters to each of the specific branches while using the static route, EIGRP, OSPF, and RIP. It can be observed that the use of static routes had the lowest latency while RIP has the highest latency. The usage of static routes minimises the latency between the devices, nevertheless, is not scalable. A more robust and scalable routing system will be necessary as the corporate operation develops, which is the main aim.

Achieved Objectives

During this research, all the aims and objectives stated have been considerably achieved in due time.

VI: REFERENCES

[1] N. Ndiaye, A. R. Lutfi , N. Ruslan and N. Adam , "Demystifying small and medium enterprises' (SMEs) performance in emerging and developing economies," Science Direct, vol. 18, no. 4, pp. 269-281, 2018.

[2] B. Mahmood, W. Shahid, M. Mohsin, S. Muhammad and A. Akber, "Network Security Issues of Data Link Layer: An Overview," 2020.

[3] f. Almeida, I. Calvalho and F. Cruz, "Structure and Challenges of a Security Policy on Small and Medium Enterprises," KSII Transactions on Internet and Information Systems. Korean Society for Internet Information (KSII), p. 3837, 2018.

[4] M. Zhang and T. ZhongPing, "Application Research of MPLS VPN," Fourth International Conference on Computational and Information Sciences, 2012.

[5] M. Farhan, M. Asif, M. B. Ahmad and K. Maqsood, "A Comparative Analysis of Unicast Routing Protocols for MPLS-VPN.," Lahore Garrison University Research Journal of Computer Science and Information Technology, pp. 43-49, 2019.

[6] F. Hauser, M. Haberle and M. Menth, "P4-IPsec: Site-to-Site and Host-to-Site VPN," IEEE Access, 2020.

[7] H. Marah, J. Khalil, A. Elarabi and M. Ilyas, "DMVPN Network Performance Based on Dynamic Routing Protocols and Basic IPsec Encryption," International Conference on Electrical, Communication, and Computer Engineering (ICECCE), pp. 1-5, 2021.

[8] D. E. Kurniawan, H. Arif, N. Nelmiawati, A. H. Tohari and M. Fani, "Implementation and analysis ipsec-vpn on cisco asa firewall using gns3 network simulator," Journal of Physics, p. 23–24, 2018.

[9] G. Wang, Y. Sun, Q. He, G. Xin and B. Wang, "Content Auditing Method of IPsec VPN," IEEE Third International Conference on Data Science in Cyberspace, 2018.

[10] cisco.com, "cisco," 2022. [Online].

[11] K. Michael , Information Security Breaches : Avoidance and Treatment Based on ISO27001, 2 ed., Vienna: IT Governance Ltd, 2014.

[12] M. Pulkkinen, A. Naumenko and K. Luostarinen, "Managing information security in a business network of machinery maintenance services business – Enterprise architecture as a coordination tool," Journal of Systems and Software, vol. 80, no. 10, pp. 1607-1620, 2007.

[13] C. Simatimbe and S. Lubobya, "Performance Evaluation of an Internet Protocol Security (IPSec) Based Multiprotocol Label Switching (MPLS) Virtual Private Network.," Journal of Computer and Communications, vol. 8, no. 1, pp. 100 - 108, 2020.

[14] S. Tongkaw and A. Tongkaw, "Multi-VLAN Design over IPSec VPN for Campus Network," IEEE Conference on Wireless Sensors (ICWiSe), pp. 66-71, 2018.

[15] L. Nowosielski, R. Wielemborek, D. Laskowski and M. Wnuk, "Confidentiality of data in backbone networks based on scalable and dynamic environment technologies," IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), pp. 68-71, 2015.

[16] T. Alam, C. Refat, A. Imran, S. Rashid, M. Kabir, R. Tarek and A. Gafur, "Design and Implementation of a Secured Enterprise Network using Dynamic Multipoint VPN with HSRP Protocol," International Conference on Innovations in Science, Engineering and Technology (ICISET), pp. 367-371, 2018.

[17] H. Chen, "Design and implementation of secure enterprise network based on DMVPN," International Conference on Business Management and Electronic Information, pp. 506-511, 2011.

[18] S. U. Masruroh, P. K. H. Widya, A. Fiade and I. R. Julia, "Performance Evaluation DMVPN Using Routing," The 6th International Conference on Cyber and IT Service Management, 2018.

[19] V. Marojevic, I. Guvenc, M. Sichitiu and R. Dutta, "An Experimental Research Platform Architecture for UAS Communications and Networking," IEEE 90th Vehicular Technology Conference (VTC2019-Fall), pp. 1-5, 2019.

[20] networklessons.com, "networklessons," 2022. [Online].

[21] firewall.cx, "firewall," 2022. [Online].

Ayodele Oladimeji Ajala School of Art and Creative Technology The University of Bolton
Deane Road, Bolton, BL3 5AB http://www.bolton.ac.uk