PERFORMANCE EVALUATION OF INTERNET PROTOCOL SECURITY (IPSEC) OVER MULTIPROTOCOL LABEL SWITCHING (MPLS)

by

Jessy Chisenga Mwape

A dissertation submitted in partial fulfilment of the requirements for the award of the degree of Master of Engineering in Information and Communication Technology Security

The University of Zambia

April, 2024

DECLARATION

I, Jessy Chisenga Mwape, do hereby declare that, this dissertation on **Performance Evaluation of Internet Protocol Security (IPsec) Over Multiprotocol Label Switching (MPLS)** is my own work and has not been submitted for the award of degree at any University.

Signed: …….

Date: ……

CERTIFICATE OF APPROVAL

This dissertation submitted by Jessy Chisenga Mwape has fulfilled the requirements for the award of the degree of Master of Engineering in Information and Communication Technology Security at the University of Zambia.

Supervisors

Supervisor: …….Signature: …… Date: ……

Co-Supervisor: ……..….Signature: ……..Date: ……

Examiners

Examiner 1: …….. Signature: …… Date……..

Examiner 2: …..…… Signature: …… Date……..

Examiner 3: ….……. Signature: .…… Date……..

Chairperson

Board of examiners……. Signature …… Date ……

Abstract:

For nearly two (2) decades, Multiprotocol Label Switching (MPLS) has provided Wide Area Network (WAN) solutions for enterprises and large organizations to manage their multiple networks in different locations. Real time networks have been affected negatively by high latency due to inefficient WAN technologies and security solutions. The popularity of Multi-protocol Label Switching (MPLS) continues to increase with Internet and Data Service providers (ISP) in Zambia. MPLS provides network efficiency through traffic engineering and Quality of Service, however, by default, it does not provide any mechanism for authentication and encryption of the data as it travels through the public network provided by Internet service providers. In order to resolve the security concerns in MPLS, this study has deployed the Internet Protocol Security (IPsec) over MPLS in order to provide additional layer of security to data during transmission. The method used to conduct this research is experiments. The research is conducted in a live environment where the service provider network implements MPLS and IPsec is deployed on Customer edge routers. Three (3) Customer Edge routers over the ISPs MPLS public network were deployed in different locations and configured with policy based IPsec. Data was collected before IPsec deployment and after IPsec deployment in order to analyze the performance metrics such as packet lengths, round trip times, authentication and encryption. The study captured and analyzed 15,362,356 packets. It has been established that using MPLS provides minimal security to data through the use of labels. This label feature both separates traffic streams and provides efficient use of network resources as IP addresses are not used to route traffic in the MPLS environment. It is worth noting that implementing IPsec over MPLS improves the security of the network and data. The study has shown that IPsec and MPLS are better together because the security risks associated with transmitting data over MPLS are resolved by IPsec. IPsec provides data privacy and security per connection for network traffic crossing the perimeter. Further, the authentication of peers and data provides the mechanism of identification and verifying the IPsec peers and validating the authenticity of the data send against the one received.

Key words: MPLS, Labels, Provider Edge (PE, Customer Edge (CE), IPsec, authentication, encryption, security

This research is dedicated to my children Peter Lazarus Mukasa and Daniel Musonda Mukasa who have given me a deep sense of responsibility and belonging.

Acknowledgements

This research would not have been possible without the help of Jehovah, my God and Father in heaven and many people. I am extremely thankful for the life and measure of health granted to me. Many thanks to my supervisor Dr. Charles Lubobya, and co-supervisor Mr. George Ziba who worked with me tirelessly, offerring guidance and support through numerous reviews and alignments of the research subject in order to make sense of the chaos. Also, many thanks to the University of Zambia for providing the facilities and resources for conducting the research. Thank you to the Enterprise teams from various companies and agencies for the resources, financial and technical support during MPLS and IPsec network deployment, troubleshooting and rollout tests. And finally, to my husband Peter Mukasa Snr, my children Peter Lazarus Mukasa Jnr and Daniel Musonda Mukasa, mother Rhoda Kunda Munshya, my siblings Evans Sabwa Sikazwe, Sydney Mutonta Mwape, Alice Musonda Mwape, Myrah Kunda Mwape and Sandrah Mutinta Mwape, my friend turned sister Ms. Foster Chimoto, other relatives and many friends who endured the long nights and gave emotional support, no amount of words can express my gratitude for you.

Table of Contents

List of Figures

List of abbreviations

MPLS:	Multi-protocol Label Switching
IPsec:	Internet Protocol security
L2:	Layer 2
L3:	Layer 3
IETF:	Internet Engineering Task Force
AH:	Authentication Header
ESP:	Encapsulation Security Payload
RFC:	Request for Comments
IKE:	Internet Key Exchange
P:	Provider router
PE:	Provider Edge router
CE:	Customer Edge router
LSR:	Label Switch Router
UDP:	User Datagram Protocol
TCP:	Transport Control Protocol
ICMP:	Internet Control Message Protocol
BGP:	Border gateway protocol
OSPF:	Open Shortest Path First
TE:	Traffic Engineering
QoS:	Quality of Service
QoE:	Quality of Experience
WAN:	Wide Area Network

LAN:	Local Area Network
LFIB:	Label Forwarding Information Base
OSI:	Open Systems Interconnection
LDP:	Label Distribution Protocol
LSP:	Label Switched Path
TDP:	Tag Distribution Protocol
RSVP:	Resource Reservation Protocol
CML:	Cisco Modelling Labs
IOS:	Internetworking Operating System
IPv4:	Internet Protocol version Four
AES:	Advanced Encryption Standard
MTU:	Maximum transmission unit
MAC:	Media Access Control
DoS:	Denial of Service
SHA:	Secure Hash Algorithm
MD5	Message-Digest algorithm (method 5)

CHAPTER ONE

INTRODUCTION AND BACKGROUND

1.1 Introduction

The popularity of Multi-protocol Label Switching (MPLS) continues to increase with Internet and Data Service providers (ISP) in Zambia. For industry players, investors and researchers who have any kind of stake in the MPLS dynamics and strategies, this research will provide in-depth analysis of the technology's implementation at Layer 2 (L2) and Layer 3 (L3) of the Open System Interconnection (OSI) model. It will also lay bare the opportunities available for providing more security on the MPLS enabled infrastructure using Internet Protocol Security (IPsec). As the demand and complexity of network connectivity increases, the need for integrating and securing several services continues to unfold. The research will analyze and evaluate the performance of IPsec on MPLS architecture and explore the potential impact these approaches will have on network security and efficiency.

1.2 Background

In order to fix the issues surrounding routing for internet traffic the Internet Engineering Task Force (IETF) formed a working group in 1997 to create standards. There was great need for routers to scale more efficiently and improve on speeds to meet the increasing bandwidth demand. The MPLS Protocol became widely adopted because it could work in multiprotocol environments and its ability to support legacy network technologies. The MPLS standard architecture and Label stack encoding specifications are defined in the Request for Comments (RFC) 3031 and 3032. These documents are managed by the Internet Engineering Task Force (IETF). The documents specifies the MPLS architecture, the label stacks and encoding to be used by routers in the MPLS environment produces packets that are labeled. [1] [2] Using the MPLS backbone, Layer 2 (L2) and Layer 3 (L3) virtual private networks (VPN) can be employed to route several types of traffic on the network. MPLS VPN standards are defined in RFC4364.The document specifies the Service Provider method to provide VPN for its customers through their backbone network. The RFC4364 obsoletes RFC2547 which defined the use of MPLS VPN to

forward packets while using Border Gateway Protocol (BGP) to distribute routes over the backbone. [3]

The standards of IPsec were initially defined in RFCs 1825-1829 and the protocol is commonly implemented in IPv4 networks. However, the standards were updated in RFC 2401-2412. This framework provides integrity, confidentiality and authentication of data. In 2005, the new IPsec superset standards of these preceding ones were defined in RFCs 4301-4309 which saw the abbreviation ***IPSec*** changed to ***IPsec***. The "standard provides network encryption (confidentiality), digital certification (integrity), and device authentication (authentication)." [4] With the continuous improvements being made to IPsec standards, the IPsec Maintenance and Extensions Working Group (IPsecme) continues facilitating for discussions, clarifications and IPsec extensions. The group is also a focus point for other Working Groups of the IETF that use IPsec in their own protocols. The working group is currently working on adding a mode to IKEv2 that will have "similar or better quantum resistant properties to those of IKEv1". [5] Additionally, the growing number of constrained networks use cases have showed interest to reduce the ESP overhead through compression of its fields and there are possible draft documents to this effect. [5] In order to meet the growing demand for traffic flow confidentiality, the Working Group has concluded that the standard of adding a null padding to ESP payload is very inefficient and is developing alternative solutions that are efficient on use of network resources.

In an enterprise network IPsec can be used to provide router security for data that transverse the public network.

1.3 Statement of the problem

Many Banking, Finance Services and Insurance (BFSI) organizations and government departments in Zambia dependent on Information systems that need to be secured to protect the integrity, confidentiality, and availability of sensitive information for the authorized users. To transmit data between their different branches, these organizations connect to the public MPLS infrastructure for the internet service providers which offers no security for the data as it traverses the public network. To resolve this problem, this study will deploy IPsec over the MPLS infrastructure and evaluate its performance in

terms of authentication and encryption to mitigate the security risks associated with transmitting data over a Wide Area Network (WAN).

1.4 Aim

The aim of this research is to improve the reliability and performance of network traffic for organizations that use the MPLS infrastructure while securing the data with IPsec as it traverses the public network.

1.5 Objectives

The objectives of this research are to:

1. Design and implement the IPsec over MPLS network and analyze the MPLS and IPsec characteristics in terms of label switching, encapsulation and encryption;
2. Assess the security limitations of MPLS and the role of IPsec in resolving them; and
3. Investigate the impact of implementing IPsec over MPLS in terms of performance and security on enterprise networks.

1.6 Research Questions

1. **What is MPLS and IPsec operation and what schemes and techniques are used to implement these two protocols on an enterprise network?**

   The answer to this research question will enlighten the features and characteristics of MPLS. The literature review will investigate the MPLS architecture and Traffic Engineering techniques, IPsec operation, encapsulation and encryption on an enterprise network. The methodology will highlight the peer-to-peer MPLS model and the tunnel mode implementation of IPsec.

2. **What are the specific security limitations of MPLS and how does the integration of IPsec address these limitations?**

   The answer to this research question will enlighten the features and characteristics of MPLS that make it vulnerable to risks associated with Wide Area Networks. The discussion will analyze Wireshark captured packets and determine the vulnerabilities of the harvested data when MPLS is implemented without IPsec.

3. **What are the perceived benefits of implementing IPsec over MPLS in an enterprise network, and how do these benefits contribute to enhanced network security and performance?**

   As the demand for efficient and secure delivery of network services by enterprises increase, continuous research on improvements to network security is a must. Identifying encryption, authentication and integrity of data as major factors and motivation for combining MPLS and IPsec on the network will be highlighted in the answer to this research question. Additionally, this will highlight how TE and data hiding mechanisms improves the security posture of Enterprises and WANs.

1.7 Significance of Study

Investigating the performance efficiency of IPsec on MPLS architecture is significant in the Zambian context as it provides valuable insights into the potential enhancements that can be achieved in network performance and security. This knowledge can help Zambian organizations and service providers optimize their network infrastructure and ensure efficient data transmission, particularly in sectors such as telecommunications, banking and government where secure and high-performance networks are essential for delivering services to the public.

Understanding the vulnerabilities of the MPLS and the effectiveness of IPsec as a security solution can help organizations in Zambia make informed decisions regarding their network security strategies. This knowledge can contribute to safeguarding sensitive data, protecting critical infrastructure and maintaining the integrity of communications in various sectors including finance, healthcare and government.

Overall, this study's significance lies in its potential to contribute to the development of secure and efficient network infrastructures In Zambia, and thereby fostering a resilient digital ecosystem that supports economic growth, innovation and the protection of sensitive information.

1.8 Scope of Research

The research will preview the challenges of traditional IP networks that are resolved by MPLS, investigate the MPLS label architecture and IPsec architecture, deployment

strategies and get the best Network performance and security based on Cisco hardware networking software. There are several VPN technologies that operate on different layers of the Open Standard Interconnect (OSI) model, however, in this research, the IPsec over MPLS implementation will be analyzed from layer 3 perspective. The research will focus on MPLS security using ingress and egress filtering, the separation of the control plane and data plane. The research will also explore the security strategy of defense in depth in combining MPLS and IPsec to provide data security through encryption and packet labelling.

1.9 Limitations of the study

The factors that have affected the generalization of the findings of this research are discussed below:

1. **Small sample size**: The access to live (production environment) data is limited to one ISP using Huawei Equipment on the Enterprise MPLS Core network. The harvested and analyzed data packets are also not for all the links on that environment but for a selected few due to company policies.
2. **Methodology of the study limited to cisco vendor devices**: Configurations are done on Cisco vendor equipment, hence the research configuration syntax discussed in Chapter 3 cannot be implemented as shown in this research on other vendor equipment. While the Cisco IOS and CML is able to deliver thousands of wide network features and service orchestration to meet the unique needs of Enterprise networks, there are other vendor equipment that have not been explored in this research.
3. **Limited access to information**: Accessing information from service providers who have implemented MPLS Service on their Enterprise Core Networks was difficult. Service providers are hesitant to give out information and approve the conducting of experiments by University Students on the production environment due to policy, service level agreements and privacy issues. Insufficient information on the IPsec/MPLS implementation on these live environments has affected the information discussed in this research.

1.10 Ethical Considerations

Early researchers predominantly utilized quantitative study methods, however, more diverse methodologies have arisen from the work-integrated learning models. During this research, the importance of ethical conduct in considering the issues around informed consent, confidentiality and conflict of interest have been considered. All participants to the research have been given information on the significance and scope of the research. Additionally, while engaging in the research the impact of the information and results obtained will have on the current implementation models of IPsec over MPLS and future research has been outlined. The confidentiality of the information gathered from Internet service providers has also been considered and well

1.11 Organization of Research

The research is structured in five (5) chapters namely, Background to the study, Literature review, Methodology, Data Collection and analysis, and Discussion and Conclusion. Chapter 1 discusses the background to the MPLS technology and IPsec protocol, the standards, guidelines and information for use of the two technologies. The objectives, problem statement, research questions and limitation to the study are also covered in Chapter 1. Chapter 2 reviews the literature related to MPLS and IPsec study. The literature review past and related work done by other researchers' offers an in-depth analysis of the IPsec and MPLS papers for operation, architecture, implementation strategies and modes of operation. The literature review also looks at the gaps that are resolved in this research. Chapter 3 looks at the methodology used to conduct this research. This chapter will discuss the Layer 3 implementation of the IPsec between two end nodes over an MPLS network. Two research methods namely; observation and experiments are used in this research. The experiments will be performed using the Cisco Modeling Labs (CML) simulation software. Chapter 4 will look at the Data Collection and Analysis. Wireshark will be used to capture and analyze the IP packets harvested from the MPLS live network and between IPsec end-nodes that have been configured using CML. Chapter 5 will discuss the conclusions drawn from this research. It will also look at the remaining gaps and the possible future research.

CHAPTER TWO

LITERATURE REVIEW

2.1 Multi-protocol Label Switching (MPLS) Architecture

MPLS is a protocol independent transport technique which uses label switching to direct traffic from one node to another on the network. Instead of developing long complex IP routing tables, MPLS uses labels. MPLS is not bound to any specific underlying technology and can be implemented across various networking protocols. It functions similarly to bookmarks as MPLS-enabled routers are informed about the location of specific prefixes in the routing table through the MPLS protocol. Every prefix entry in the routing table is assigned a specific number or label which is communicated to other MPLS enabled neighbor routers to know the label for each prefix for the purpose of routing an IP packets properly and quickly. [6] MPLS routing is different from regular hop-by-hop IP forwarding of packets.

The label is a 4 byte identifier which identifies the path in between endpoints on the MPLS network. The MPLS labels are inserted between the layer 2 Ethernet header and layer 3 IP header. The 32 bit identifier is broken down to 20bits for the label, 3 experimental bits that define traffic class used for QoS, now called TC (traffic class), 1 bit that can comprise of multiple labels called the stack flag and 8 bits for route loop prevention called TTL. [7] Figure 2.1 below shows MPLS label contents as discussed above.

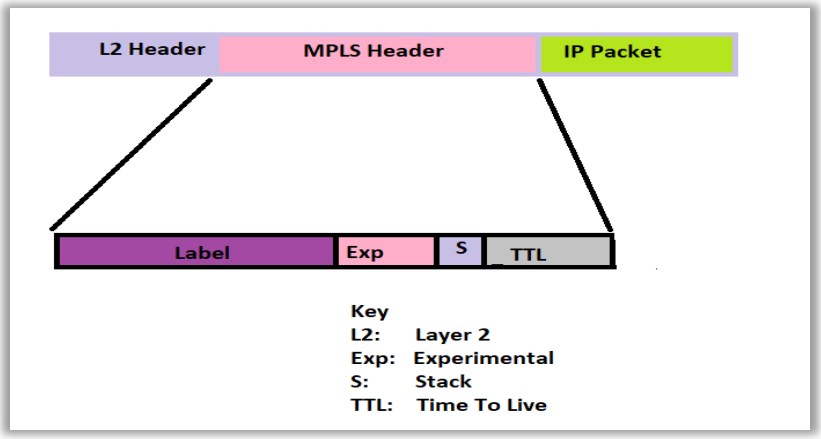

Figure 2.1: MPLS Header

Suffice to mention that MPLS operates at both Layer 2 and Layer 3 of the OSI model. Label information is exchanged in the control plane using dedicated label exchange protocols such as Resource Reservation Protocol (RSVP), Label Distribution Protocol (LDP) and Tunnel Destination Point (TDP). The control plane makes decisions regarding data processing, management, and routing. The control component creates and maintains label information to ensure consistent transfer between groups of labels. [8] The inserted labels specifies both the service attributes and routes. [9] Inserting the 4 byte MPLS label does not change the size of the IP packet, however, the size of the Ethernet Frame changes.

One of the notable features of MPLS is the ability to stack labels and thereby allowing a packet to carry multiple labels organized in a last-in, first-out (LIFO) stack. [10] MPLS packets can carry a set of labels in a stack. MPLS packets can undergo label operations such as ***push***, ***swap*** and **pop**. MPLS networks are composed of various types of routers with each playing a specific role in the routing and forwarding process. The two key types of routers in the MPLS network are Provider Router (P router) and Provider edge (PE) router. When MPLS router receives a packet, it performs one of these label operations:

1. **Push (impose)** – A new label is added to the IP packet before forwarding it on the Label Switched Path (LSP). This operation is performed by the Ingress router in the MPLS environment. Ingress is at the start of the LSP. The Provider Edge (PE) router configured at the boundary of the MPLS network runs both IP and MPLS protocols.

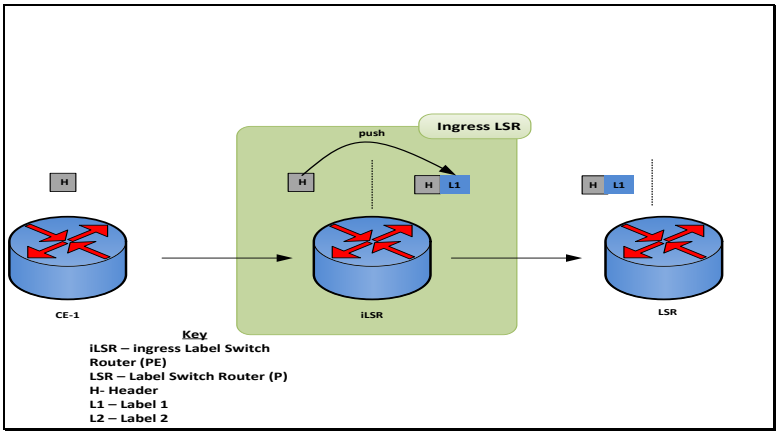

Figure 2.2: PE push operation

The PE router can act as Ingress or Egress router for the MPLS network. The PE that receives packets which are not labeled from the Customer Edge router acts as Ingress. It inserts a label at the front of the packet and forwards it on the data link. Figure 2.2 above shows how ingress router in the MPLS environment performs the push function as it receives packets from customer edge routers.

2. **Swap** – Labels are replaced with new ones for transiting traffic. The transit router carries out this function within the LSP

   The P router **swaps** old labels with new ones on a labeled packet before forwarding it out to the next node. The swap operation is performed on the top label in the label stack based on the LFIP information. This is part of the data plane which is responsible for the label and path associated information lookups. [8] This operation does not encrypt the data, however, the swapping of labels on the packets greatly improves security through isolation and unique identifiers. The P router is responsible for swapping top labels in the label stack of the packet and replacing them with new labels. [11] This is an intermediate label switch router (LSR) which is configured as a transit router in the MPLS core network. This node is crucial to understanding MPLS operation. The Provider (P) router only runs MPLS and is also known as Label Switch Router (LSR) and analyses the labeled packets and forwards them using the Label information Base (LIB) table. Typically, the P router connects to one or more Provider Edge (PE) routers and analyses and forwards labelled packets to the next hop. [7] The LSR forwards labelled packets on the created label switched paths (LSP). LSPs are set up at the Provider Edge (PE) router. When a packet moves through the MPLS network, each P router swaps the top labels as shown in Figure 2.3 below.

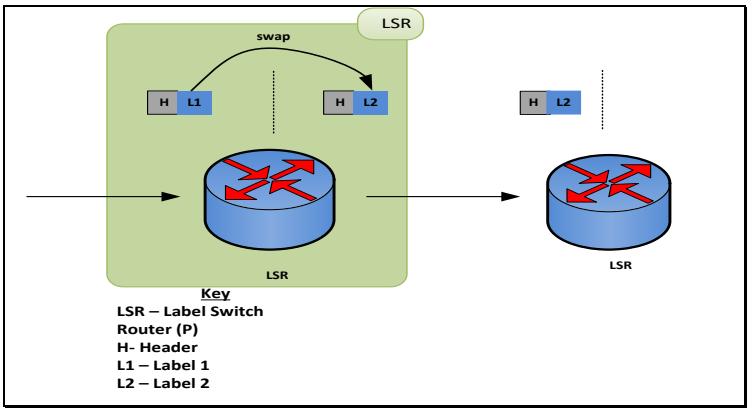

Figure 2.3: P router Label swap operation

3. **Pop (dispose)** – Strips off the label from packets leaving the MPLS environment to destination network. This function is performed by the Egress router. The router that strips off the labels from the packets are known as Egress Routers. In this case, the PE router removes the label from the packet and forwards it to the appropriate destination. Figure 2.4 below shows how the Egress Routers strips off the labels on the packet before forwarding to the receiving customer edge router. Once the label is removed, the packet is then routed to the IP network for the customer CE.

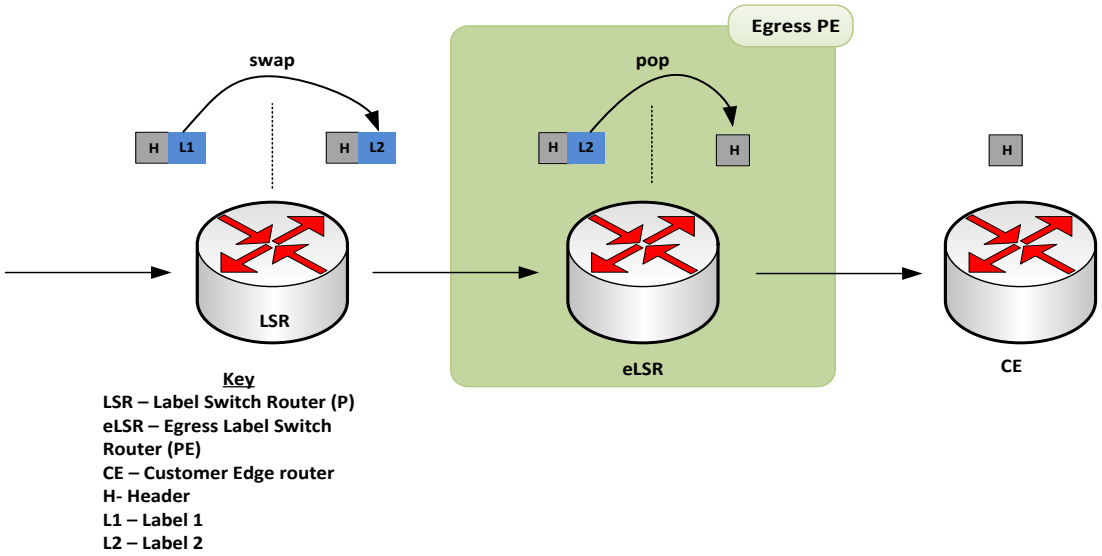

Figure 2.4: PE pop operation

MPLS is connection-oriented, supports multiple tags and Traffic Engineering (TE). The actual data transfer is performed in the data plane where packets are redirected

based on label lookups in the Forwarding Information Base (FIB) table. [8] MPLS-enabled routers utilize label information to route and forward traffic. The FIB table is generated and maintained through protocols such as Label Distribution Protocol (LDP) and Tag Distribution Protocol (TDP). When specified on the interface, these protocols are useful for peers using different protocols. LDP allows peers to establish label switched paths which map layer 3 routing information directly to layer 2 data link information. Figure 2.5 below shows the dedicated label switched path for a packet moving from CE1 through the MPLS environment to CE2 in another location.

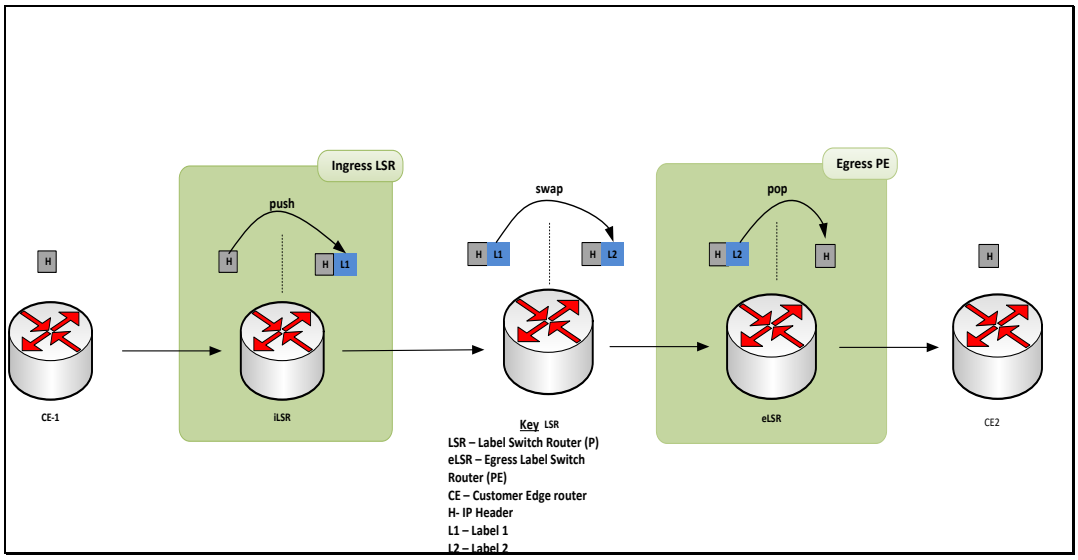

Figure 2.5: MPLS label switch path

2.2 IPsec Architecture

Internet Protocol Security (IPsec) is a set of protocols used to secure IP communications by providing authentication, integrity and confidentiality. IPsec consists of two main protocols which include Authentication Header (AH) and Encapsulating Security Payload (ESP). Additionally, IPsec employs other encryption standards such as DES (Data Encryption Standard), Triple DES, Diffie-Hellman, message digest, Secure Hash Algorithm (SHA-1), Rivest, Shamir and Adelman (RSA) signatures, Internet Key Exchange (IKE) and Certificate Authorities (CA). These encryption standards are supported by most vendor IOS such as Cisco Systems and Private Internet Exchange (PIX) firewall. [12] IPsec implementations come in two versions which include IPsec-v2 and IPsec-v3. Notable, IPsec-v2 is commonly used. [13]

IPsec ensures the confidentiality and authentication of application data exchanged between two end notes. It protects the data from replay (man-in-the-middle) attacks by verifying the integrity of sent packets and allowing the recipient to authenticate the source of the data. [14] It is worth noting that IPsec can secure more than one data flow. Data confidentiality is achieved through encryption of the payload before transmission and data integrity is provided by authenticating the packets at the receiving node. IPsec receivers can also detect and reject replayed packets. The sender and the recipient establish a secure IPsec session, negotiate requirements for the secure connection and calculate hash values of checksums to authenticate the exchange data. The following describes the operation between the sending peer and receiving peer that are configured with IPsec:

1. Sender verifies data against the security policy and initiates secure IPsec session with recipient.
2. Both the sender and recipient negotiate requirements for establishing secure connection such as authentication, encryption and security association (SA) parameters.
3. Exchange of information via IPsec tunnel between the two nodes.
4. Termination of IPsec session.

Figure 2.6 below shows the establishment of IPsec session between IPsec nodes as described above.

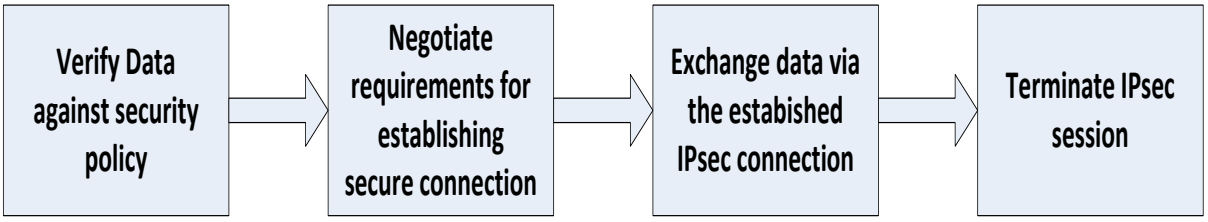

Figure 2.6: IPsec operation between nodes

Data integrity is provided through authentication of sent packets at the receiving node. The receiving node can also authenticate the origin or source of data received. Authentication is done through certificates and signatures. Each endpoint calculates the hash value or checksum of the data being exchanged. [15]Detection and rejection of replay packets is also done by the IPsec receiver.

When manually configured, IPsec can operate without the need to setup IKE. However, the basic configuration of encrypting data at the start node and decrypting at the end node using the same keys will make it easier for the eavesdropper to out the keys used. Additionally, changing the keys manually can be big challenge. This can cause misconfigured IPsec node and thereby introducing vulnerabilities to the secure connection. IKE plays an important role in the key exchange arena because it can be configured to allow automated and smooth key updates to be done between peers. Suffice to say that IKE is part of the suite of protocols in IPsec that offers additional benefits such as automatic negotiation and authentication, certification authority support and anti-replay services. [16]

Two versions of IKE can be found currently in implementations namely IKE1 and IKE2. IPsec uses IKE to negotiate Security Associations (SA) in two phases. During phase 1, authentication of IPsec peers and setting up a secure channel is done. This phase ensures that SAs are established either in Main mode or Aggressive mode. These modes both use Diffie-Hellman (DH) key exchange mechanism. The difference between these modes is that the Main mode provides identity protection while the Aggressive mode is used when identity protection is not required. [17] Once the phase 1 SA is established, IKE negotiates the IPsec SA parameters for other security protocols such as AH and ESP. The IPsec SAs that are generated and set between the peers are bi-directional, with one in each direction. Phase 2 also renegotiates IPsec SAs periodically to guarantee security. When IKE establishes a secure tunnel in phase 1, either party can initiate Quick mode exchanges to provide replay protection or/and renegotiate when the IPsec SAs lifetime expires. [18]

2.3 Related Work

Numerous research studies have been conducted on MPLS networks and IPsec operations. Ongoing advancements in these technologies provide opportunities for further research. Previous research works have attempted to investigate various aspects of MPLS networks including traffic engineering, performance analysis and security aspects. The studies also cover different aspects of IPsec such as security enhancements, key management and performance evaluation.

In a study conducted by Global Information Assurance Certification under the SANS institute, the paper highlights the benefits associated with implementing MPLS VPN technology. It shows why MPLS is an obvious choice when the goal is reduced complexity and reduced latency. However, it further shows why IPsec would be choice if the objective is data confidentiality. [4] While this study highlights capacity for MPLS to use network resources efficiently, setting up labeled switched paths (LSP) across one or more large networks can take significant amounts of time because LSPs have to be manually configured by the vendor using MPLS.

The study by Azhar Ali Mian and Sadar Usman discussed how rapid growth of the Internet has led to an increased demand for efficient management and performance of packet-switched network communications. While IP networks have been successful in supporting various applications, there are persistent challenges affecting the Quality of Service (QoS). These challenges necessitate the exploration of advanced technologies such as Multi-Protocol Label Switching (MPLS) to enhance network performance. [8] Prioritizing labels based on type of traffic or application can guarantee bandwidth for high priority labels for real time applications.

The study of Okhee Kim and Doug Montgomery took a deep dive into the behavior and performance characteristics of IPsec/IKE in Large-Scale VPNs. Their research highlighted used “detailed, packet level, simulation models to characterize the performance impact of security association (SA) policy, varying key management scenarios, cryptographic algorithms, management parameters and implementation options in IPsec/IKE suites. The results of this study showed that due to the increased performance overhead for a dynamic SA set-up, TCP based application experience increase in latency. [17] The gap of increased latency on the network affects the performance of applications and can result to degraded service. In a large-scale VPN using traditional IP routing, increased latency introduced by IPsec results in failures on real time applications.

Specifically in a study by Smith et al, the authors propose a novel approach to MPLS network security by incorporating IPsec functionality at the edge of the routers. This study explores the benefits of combining MPLS and IPsec by providing end-to-end security within MPLS networks. This study evaluates the performance and security aspects of the

proposed solution and compare it to traditional MPLS networks without IPsec. The results of this study demonstrate the effectiveness of the combined approach in providing enhanced security without compromising network performance. [19]

The study by C. K. Simatimbe and C. S. Lubobya concluded that even though IPsec over MPLS increases the size of the data packets and bandwidth usage, the acceptable operating levels of the network are maintained. Additionally, the use IPsec on an MPLS network significantly improves security of the data and the network. [20] This study does not exploit the performance impact of IPsec on MPLS enabled networks are connected to customer edge devices using the traditional IP routing techniques.

Another study by Johnson et al focuses on the scalability and performance analysis of MPLS networks with IPsec. The study analyses the impact of IPsec on MPLS network performance, particularly in large-scale deployments. The study investigated the overhead introduced by IPsec encryption and authentication processes and proposes optimization techniques to mitigate these overheads. The study provides valuable insights into the trade-offs between security and performance in MPLS networks with IPsec. [21]

The Analysis and Evaluation of MPLS Network Performance study by Rafamantanantsoa, F., Aubert, R. and Haja, R. used SCAPY to measure the response times by varying the size of the packets sent and validate the measurements with the MATLAB Simulink. The study compared the performance of Linus OS and FreeBSD on an MPLS enabled network. Based on Operating Systems of the computers passing traffic on an MPLS network, the study revealed that the transmission variations of labels is minimal because of the shortened MPLS stacking functions. This optimizes the speeds of execution and MPLS has proven to be effective in optimizing the use of network resources. [22]

In a study conducted by Shahid Ali and Bilal Zahid Rana on the behavior of routing protocols in an MPLS VPN enabled network, the researchers concluded that Open Shortest Path First (OSPF) performed better than Routing Information Protocol version two (RIPv2) in terms of queuing end to end delay and throughput. This study concluded that OSPF provides better performance results in the MPLS-BGP VPN architecture. Using VPN models on MPLS also provides minimum security for the data being transferred through the network. [23]

The study by Daniel Guermsey and others examined the security issues associated with the Label Distribution Protocol, which is the primary route construction protocol in MPLS networks. Their analysis identified ten attacks that exploit weaknesses in the LDP specification and six attacks that disrupt service and four that divert traffic from intended routes. [24] This study highlight the security flows inherent on MPLS networks thereby showing gaps for further research to protect data traversing across the public network.

Utkarsh Shah conducted the study on Performance Evaluation of MPLS in a Virtualized Service Provider Core (with/without Class of Service) in 2011 which highlighted that tradeoff exists when Quality of Service is introduced on congested primary and secondary MPLS enabled links. These tradeoffs include lower round trip times for application traffic while encountering packet drops on the network. On the other hand, disabling QoS leads to bandwidth contentions. However, MPLS provides efficient use of network resources through labeled switched paths. [25] In my opinion, the bandwidth contentions resulting from disabling QoS highlighted in this study can only significantly impact on application performance in networks with high real time traffic compared to non-real time traffic.

The study conducted by A. Z. Othman et al themed "The effect of QoS implementation in MPLS network" looked at implementations within the ISP. The paper looked at the high speed MPLS network implementation and the effects of QoS on the efficiency and speeds experienced by ISP users. The obtained results can be used by Network Administrators and ISPs in implementing the QoS and enhanced further with other type of queuing mechanism. [26] The implementation of QoS in the MPLS network allows for prioritizing of traffic streams for real time applications. For networks running Voice over Internet Protocol (VoIP) and Video, these applications perform better than non-real time applications because they are given priority during transmission.

In a study themed "Performance analysis of IPSec protocol: Encryption and authentication" by O. Elkeelany et al, presented the performance analysis of the algorithms DES, MD5 and SHA1. The study looked at processing power and input size for purposes of authentication and encryption. The results revealed that if the primary goal is authentication, MD5 algorithm is sufficient rather than using complicated configurations of SHA1. However, if the goal is encryption, authentication should be

combined with DES. IPsec provides secured tunneling for authenticated and encrypted data flows. [27] Even though the primary goal of authentication was achieved in this study, the method used is not secure enough for critical and sensitive data because highly skilled malicious actors can easily break the MD5 cryptographic authentication method.

Table 2.1 in Appendix B show the related works and the approaches used in their research.

The reviewed studies in this chapter highlight the performance of MPLS and IPsec in terms of efficiency, Quality of Service, Traffic Engineering and security for both real time and non-real time applications. This chapter has partially archived objective 1 in that it has explored and analyzed the MPLS and IPsec characteristics in terms of label switching, encapsulation and encryption. Additionally, it has examined the IPsec secure session setup between two end-nodes. The continuous studies being done on these protocols gives the industry more room for continued improvements on the protocols and standards. This study will explore the strengths of combining both technologies, to develop solutions that ensure secure and efficient communication in MPLS and IPsec enabled network environments.

CHAPTER THREE

METHODOLOGY

MPLS is an encapsulation mechanism most commonly implemented in Service Provider networks. In an enterprise environment, it can provide multi tenancy and segmentation. Ideally, the MPLS network architecture consists of the Provider (P), Provider Edge (PE) and Customer Edge (CE) routers. In order to conduct this research, the network is set up using the **peer-to-peer** VPN model in which the customer data is carried over the public network through the MPLS routers belonging to the ISP. In this setup, the Provider Edge (PE) routers participate in customer routing. One of the benefits for choosing to use the VPN model in this research is needed to provide the customer link only on the PE and CE routers. The downside to the VPN setup is that the customer will not have total control over its end to end routing as this responsibility is shared with the ISP. In this setup, Static routing is configured between the PE and the CE. It is worth noting that the MPLS cloud uses dynamic routing protocols for peering within the cloud. This protocol ensures that the routers in the MPLS cloud are able to form neighbor relationships and share router IP information.

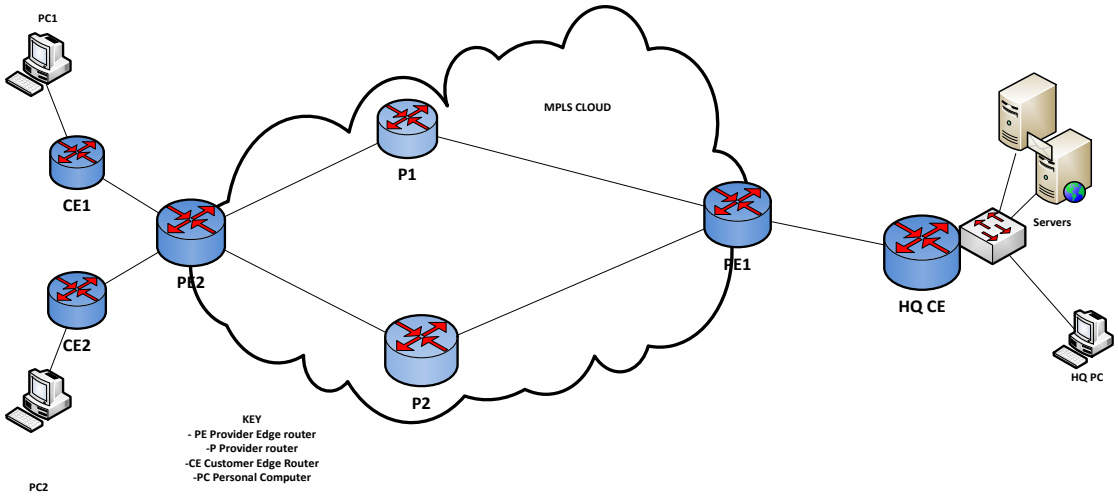

Figure 3.1: MPLS network setup

Figure 3.1 above shows the logical network setup and configuration for communication to CE1 and CE2. In this configuration, the CE routers are considered to be two branches offices of the enterprise wide area network (WAN) in different locations. The P and PE

routers are the routers considered to be in the MPLS trust zone while the CE is not in the MPLS trust zone and only runs the IP routing protocols. The MPLS cloud is the public network for the service provider. The CE routers are connected to the service provider MPLS network using fiber cables. However, the MPLS is enabled for forwarding data packets on the network.

Table 3.1 below shows the hardware, software and function each of these devices plays on the research network. The ISP environment (MPLS Cloud) uses HUAWEI equipment for MPLS while the Customer Edge network devices are Cisco proprietary. The end nodes are HP Server and computer used to monitor the network, generate network traffic and collect statistics and results for this research.

Table 3.1: Network Hardware

HARDWARE	**SOFTWARE**	**FUNCTION**	**PROTOCOL/ APPLICATION**
HUAWEI NE40E-X8	NE40E V800R010SPH172	Provider/Edge Routers (ISP Network)	MPLS and IP
CISCO 9300	IOS XE Software, Version 16.06.03	Customer Edge Router/ Switch	Internet Protocol
CISCO 1921	C1900 IOS Software	Customer Edge Router	Internet Protocol
CISCO 1841	1841 IOS Software	Customer Edge Router	Internet Protocol
	Windows Server 2019	File server	Wireshark and Security Onion
HP Intel CORE i5	Microsoft Windows 11	Desktop computer	FTP Server and Wireshark
HP Intel Pentium	Microsoft Windows 10	Desktop Computer	FTP Client

3.1 Experiments using Simulation Tools

Before deployment, the MPLS and IPsec network was simulated using Cisco Modelling Labs to test the connectivity and Internetworking Operating System (IOS) compatibility of the network devices. This section describes the steps taken to setup CML and Wireshark, the configuration of the MPLS enabled routers (P and PE), and the IPsec setup on the CE routers. The configurations shown in Appendix 3 are first deployed and tested on the CML sandbox before deployment on the live environment. It is worth noting that on the CML sandbox, all devices used on the network are cisco proprietary for both MPLS and IPsec. However, the deployment on the live environment was done on Huawei Enterprise ISP network (P and PE) for MPLS and Cisco Customer Edge equipment for IPsec deployment. Wireshark was installed on Windows machines for the live capture and storage of packets on the live network. Additionally, for mirroring of live packets on the network, a Linux Server appliance was installed with Security Onion to capture and store mirrored packets entering and leaving the head office edge device.

3.1.1 Cisco Modeling Labs (CML)

Cisco Modeling Labs (CML) will be used to simulate an on premise Enterprise network and configuration of network devices and protocols. This tool was used to design, test and troubleshoot the network infrastructure for cisco and non cisco networks. In order to design and test high reliable models in this research, a free version of CML was reserved to simulate on premise enterprise networks. From the website https://developer.cisco.com/site/sandbox/ , once signed up the CML portal was used to reserve the four hour access free for signed up users. The website guides the user on how to reserve and Devnet Sandbox. On the user dashboard, the user can access Learning Labs center, Code exchange and Events which provide updated insights to enhance the learning and research experience.

3.1.2 Cisco AnyConnect Client VPN Setup

The CML sandbox is used as a test environment for the research network. The Cisco AnyConnect Client VPN allows the user to access the Labs on CML. Figure 3.2 below shows the Cisco AnyConnect client VPN setup.

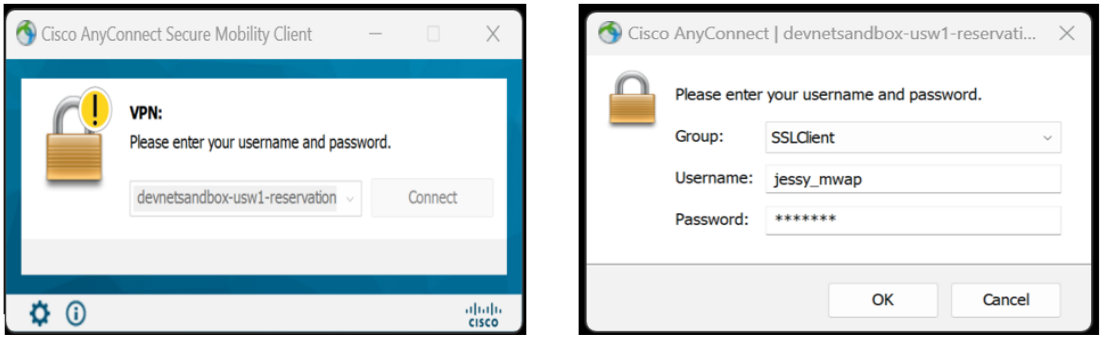

Figure 3.2: Cisco AnyConnect Client VPN setup

This research uses version 4.9.04043 of the VPN client. The user is prompted by the Cisco AnyConnect Client VPN to enter the username and password to authenticate and access their Labs on Cisco Devnet Sandbox. Once the login credentials are set up, the configurations in Appendix 3 are tested on the sandbox virtual environment before deployment on live environment.

3.2 Network Setup

3.2.1 Live Environment Setup of MPLS

The distance between CE1 and CE2 is nine kilometers. The distances between the PE routers and the P router is approximately ten kilometers (10Km) and the ISP uses fiber optic cables to interconnect to their core systems. CE1 and CE2 connects to PE2 using 10G fiber optic cables. The P, PE1 and PE2 are configured to run MPLS protocol. PE1, PE2, CORE CE, CE1 and CE2 are using static IP routing to peer with each other.

Table 3.2 below shows the IP scheme which is setup in this environment. For communication Between PE and CE, the IP addresses used are class A which subnet considering the number of devices in that subnet. The subnets that are connecting to the PE routers are using /29 subnets while the internal LAN for CE1 and CE2 are using /25 subnets.

Table 3.2: IP Scheme

Network Connection	Subnet	Source	Destination	Subnet Mask
PE1 to CORE CE HQ	10.200.200.8	10.200.200.11	10.200.200.9	255.255.255.248
PE1 to CE1	10.200.200.8	10.200.200.11	10.200.200.10	255.255.255.248
PE2 to CE2	10.200.200.0	10.200.200.2	10.200.200.1	255.255.255.252
CE1 to PC1	192.168.200.0	192.168.200.1	192.168.200.11	255.255.255.128
CE2 to PC2	192.168.200.128	192.168.200.129	192.168.200.142	255.255.255.128
Tunnel 10	172.16.220.0	172.16.220.1	172.16.220.2	255.255.255.252
Tunnel 20	172.16.220.4	172.16.220.5	172.16.220.6	255.255.255.252

3.2.2 Provider Edge (PE) router

The PE setup and configurations are done in the ISP environment. The standard configuration includes enabling the MPLS service, label tagging and routing on the routers in this environment. Figure 8 below shows the MPLS configuration on one of the PEs. The router Identity (ID) is 10.1.1.1 which is also used as the MPLS Label Switch router (LSR) ID. This IP address specifies the LSR ID for this device and is presented in decimal doted format. In the ISP network where MPLS is deployed, this ID is configured to identify the device during forwarding of labeled packets and is also used to advertise the device to other MPLS devices within the network. Since MPLS is deployed to increase the forwarding rates, packet headers are not analyzed on every hop but on the edges of the network. [28] By default, global Bidirectional Forwarding Detection (BFD) protocol is disabled on Huawei Ingress routers. This protocol is a hello mechanism used to detect network failures at specified intervals. When BFD MPLS is enabled, the Ingress router can dynamically create BFD sessions to monitor LDP LSPs. In this configuration, the MPLS BDF is set to passive to ensure that the Egress router does not automatically create BDF sessions until it receives a LSP request from the Ingress router. [29] In a large backbone network, the MPLS TE is enabled so that routers establish constraint-based routed label switched paths (CR-LSPs) that create virtual topology over the physical topology to map traffic and prevent congestion. This enable the MPLS router to guarantee

the bandwidth and QoS without the need to upgrade the hardware. [30] Figure 3.3 below shows the configuration of for an MPLS enabled router in the ISP environment. The router LSR 10.1.1.1 is configured with MPLS layer 2 and layer 3 VPN.

```
#
router id 10.1.1.1
#
bfd
 mpls-passive
#
mpls lsr-id 10.1.1.1
#
mpls
 label advertise non-null
 mpls te
 mpls rsvp-te
 mpls te cspf
 mpls bfd enable
 mpls bfd-trigger host
 mpls bfd min-tx-interval 50 min-rx-interval 50
#
mpls l2vpn
```

Figure 3.3: MPLS Configuration on PE

In this configuration, the relationship between the VPN instance and the interface is created. The VPN instance is configured with a route distinguisher which is used for forwarding within the MPLS cloud and used to identify the VPN the packet belongs to. The VPN instance RESEARCH-MENG will be used to forward and identify packets belonging to this instance. The ***vpn-target*** import and export configuration controls VPN learning within the MPLS network. [31]This configuration ensures that only routes in RESEARCH-MENG VPN are learned and added to the routing table for this instance. To achieve privacy of each customer on the MPLS network, the virtual routing forwarding (VRF) is used to separate the routing information for different customers. In this research, the Huawei router uses the vpn-instance to identify the VRF. Assigning labels to packets is critical to MPLS operation to ensure that data is accurately delivered to end user. The RESEARCH-MENG VPN instance is configured to use IP version 4 (IPv4) address family. The configuration on interface Gigabit Ethernet 0/3/0.603 enables the router to push the labels on the untagged packets when acting as Ingress and to pop the labels on the tagged packets when acting as the Egress. The interface IP address settings ensures that the PE is able to peer with the CE router and the ***statistics enable*** command enables

the monitoring of traffic behaviors on the interface. Figure 3.4 below show the configuration of the VPN instance RESEARCH-MENG in PE1.

```
#
ip vpn-instance RESEARCH-MENG
 ipv4-family
  route-distinguisher 65111:1
  apply-label per-instance
  vpn-target 65111:10 export-extcommunity
  vpn-target 65111:10 import-extcommunity
  vpn-target 65300:10 import-extcommunity
#
interface GigabitEthernet0/3/0.603
 vlan-type dot1q 603
 description LINK TO RESEARCH WAN CE1
 ip binding vpn-instance RESEARCH-MENG
 ip address 10.200.200.2 255.255.255.225
 statistic enable
```

Figure 3.4: Label tagging on PE

Routing configuration is vital to ensure that traffic flows between the PEs and CEs. Since PE routers run both MPLS and IP protocols, static routing is configured for peering from PE to CE and vice versa. As shown in Figure 3.5 below, the VPN instance RESEARCH-MENG is configured to import all static and direct routes specified in this VPN instance. Direct routes are learned through the link layer protocol and static routes are manually configured by the network administrator. All IP traffic meant for the RESEARCH_MENG network is routed by default to 10.200.200.1 which is CE1. This means that any routes not known by the PE router will be sent to the device 10.200.200.1 to find the destination for that route.

```
 ipv4-family vpn-instance RESEARCH-MENG
  import-route direct
  import-route static
#

ip route-static vpn-instance RESEARCH-MENG 0.0.0.0 0.0.0.0 10.200.200.1 description HEAD-OFFICE
ip route-static vpn-instance RESEARCH-MENG 192.168.200.0 255.255.255.128 10.200.200.1 description RESEARCH-MENG-LAN1


#
```

Figure 3.5: Static Routing Configuration on PE

3.2.3 Customer Edge (CE) routers

The configuration of the Customer Edge routers was done on the Cisco Systems 1800 and 1900 respectively. CE1 and CE2 use the ISP infrastructure to interconnect to each other.

A. ROUTER 1

CE1 used Cisco1921/K9 with three (3) Gigabit Ethernet Interfaces, 487424K/36864K bytes of memory. The Dynamic Random Access Memory (DRAM) is 64bits while the Non-Volatile Random Access Memory (NVRAM) is 255K Bytes. CE1 runs on the C1900 Software (C1900-UNIVERSALK9-M), Version 15.2(4) M5 release. The key features and benefits of the Cisco 1921 Integrated Services Router (ISR) include deployment of high-speed WAN environments with increased levels of service integration. Services such as security, data, mobility and wireless can be integrated with great efficiency and save costs. This router also offers modular architecture for services and interfaces for increased bandwidth and network resilience. [32] Figure 3.6 below shows the C1921 Cisco router version and features for CE1.

```
Cisco CISCO1921/K9 (revision 1.0) with 487424K/36864K bytes of memory.
Processor board ID FCZ180490SH
3 Gigabit Ethernet interfaces
1 terminal line
DRAM configuration is 64 bits wide with parity disabled.
255K bytes of non-volatile configuration memory.
245744K bytes of USB Flash usbflash0 (Read/Write)

License Info:

License UDI:

-------------------------------------------------
Device#    PID                 SN
-------------------------------------------------
*0         CISCO1921/K9        FCZ180490SH


Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology     Technology-package           Technology-package
               Current       Type           Next reboot
-----------------------------------------------------------------
ipbase         ipbasek9      Permanent      ipbasek9
security       None          None           None
data           None          None           None

Configuration register is 0x2102
```

Figure 3.6: CE1 router version

CE1 is set to 0*2102 configuration register. The configuration register is a 16bits value configured on Cisco routers to determine how the router boots, available boot options and setting the console speed. The router checks configuration register to determine its software and configuration files. Additionally, the configuration register is used for router

password recovery. [33] With the configuration register set to 0*2102, CE1 will follow the boot sequence shown in Figure 3.7 below.

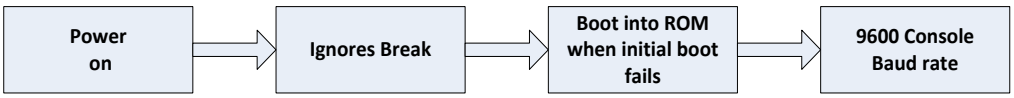

*Figure 3.7: 0*2102 Configuration register*

CE1 is configured with hostname RT-IPsec-TEST1 and the Dynamic Host Configuration Protocol (DHCP) pool named MPLS_IPsec_Site1. The DHCP pool excludes the IP addresses 192.168.200.1 to 192.168.200.10 from automatic leases. The LAN network range is 192.168.200.0 to 192.168.200.127. This subnet has 124 usable IP addresses. Typically, an IP address is 4 bytes long which is divided into five classes with each IP subnet class being split into subnets. Splitting IP network ranges into sizable subnets ensures broadcasts are contained in those subnets and improves efficiency and performance of the network. All IP addresses in one subnet share the same broadcast domain. [34] Since DHCP is automatic and reliable, it reduces the errors and conflicts associated with static configurations of IP information. Network management is centralized and this makes it easy to add portable devices and new clients to the network. IP address reuse is another advantage of configuring DHCP. [35] The DHCP pool lease is set to infinite to ensure that the DHCP lease does not expire for the end devices to maintain same IP address information for easy management. In a large network, the lease time should be configured to expire to avoid filling up the DHCP lease table with stale leases. The lease time is usually determined by the size of the pool, stability and turnover of devices on the network. Large and public serving networks are better optimized with short lease time while smaller networks can be set to a longer DHCP lease time. [36] The lease time is set to infinite.

The configured Domain Name System (DNS) server IP addresses are 192.168.0.10 and 172.16.120.249. These local servers provide domain name to IP address translations for devices on the network. DNS uses known domain names such as www.unza.zm and maps them to the IP address which is used by computer networks to locate a particular website machine. In order for users on CE1 network to connect to remote users, DNS quickly provides necessary information to resolve the name to IP address for the connection. [37]

In this configuration, CE1 uses the local DNS servers which are within the network. This ensures that local IP addresses are kept private within the enterprise network. Figure 3.8 below show the DHCP configurations for CE1.

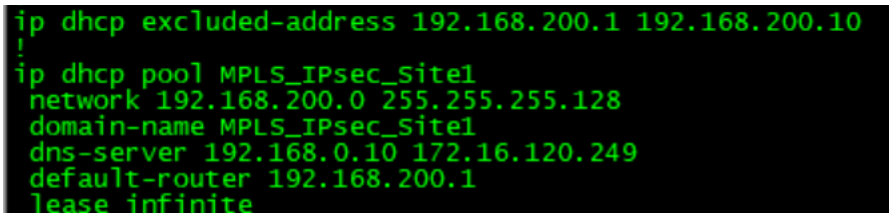

Figure 3.8: CE2 DHCP configuration

In order to prevent unauthorized access to the router information, a username and password in configured for administration of the device. These parameters are used to verify the identity of the user accessing the network devices. Configuration of username and password is a crucial line of defense in protecting sensitive network information. It also serves as an access control mechanism on device administration. In this experiment, type 6 and 7 cisco passwords are used for console, Virtual Teletype (VTY) and BGP routing protocol peering with ISP. Since 2006, Type 6 password has been supported on Cisco Internetwork Operating System (IOS) 12.3 (2) and possibly earlier. Type 6 password uses the 128 bit AES counter mode where the administrator defines a master key for the IOS to decrypt the password. The type 7 Cisco password uses the Vigenere cipher which is legacy and very poor way of storing passwords because it can be easily decrypted. [38] By default the type 7 password is used when the type is not defined by the administrator and there are limitations on the (IOS) for some router versions.

Both CE1 and CE2 are configured with Service password encryption which prevents unauthorized users from learning the password. When service password encryption is enabled, all configured passwords on the router are encoded. While this command hides the plain text password, anyone with access to the router can decode the password easily using tools on the internet. In this configuration all passwords are encrypted and would appear as shown in Figure 3.9 below.

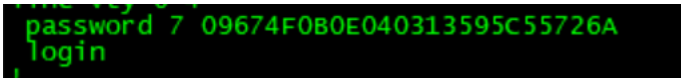

Figure 3.9: Type 7 Encrypted password

CE1 consists of three (3) Gigabit Ethernet interfaces. In computer networks, Gigabit Ethernet can provide up to 1000Mbps (Megabits per second). [39] The distance between PE1 and CE1 is less than 100meters and hence the unshielded twisted pair (UTP) category six (CAT6) cable is used to connect the two devices. UTP CAT6 offers better performance and throughput in Ethernet networks. [40]

Interface GigabitEthernet0/0 is connected to the ISP MPLS PE with IP address 10.200.200.1/30 and interface GigabitEthernet0/1 is connected to the CE1 LAN interface. The subnet mask which has only two usable IP addresses in the subnet. The IP address for GigabitEthernet0/1 is 192.168.200.1/25. The slash (/) notation indicated on the IP addresses is a compact way to present the subnet mask of the configured IP address. The slash notation is also known as Classless Inter-Domain Routing (CIDR) notation which identifies the number of bits on the network prefix. The traditional allocation of IP addresses was based on their class, however, the idea in CIDR is to allocate and route IP addresses based on their network prefix. The benefits of using CIDR are that IP addresses can be efficiently allocated based on the size of the network and avoid waste. CIDR allows routers to route traffic in a flexible way and reduce the size of the routing table which reduces the administrative overhead. [41] Figure 3.10 below show the Gigabit Ethernet interface IP settings and descriptions. The subnet masks for the interfaces is shown in decimal representation.

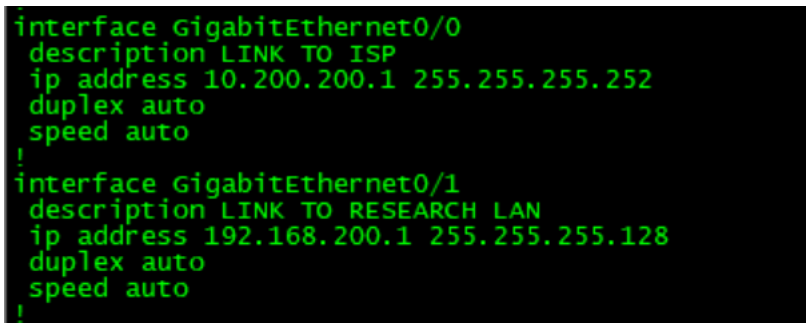

Figure 3.10: CE1 Interface Configurations

The process of path selection and routing network traffic between routers and other networks is called routing. Each router maintains a routing table which aids in finding the next hop for outgoing traffic. Additionally, dynamic routing supports other features such as security and priority. In a broad sense, routing is done across different kinds of networks. [42] In this research, routing is configured for the two Customer Edge routers to route traffic through the MPLS network. CE1 maintains static tables when routing traffic to PE1. The choice of static routing in this research is mainly based on the size of the network. The Research network is small and few static routes can easily be configured and maintained in the routing table. However, in large networks, static routing may prove to be problematic due to administration mistakes. Additionally, static routing in large networks means longer downtime on faulty statically configured routes because traffic will not be rerouted to other active links on the network. Figure 3.11 below show the static routing configuration on CE1. The Internet Protocol forwarding rules are defined to forward all packets whose IP addresses are not found on the LAN and in the routing table to the default route 10.200.200.2. When CE1 receives a packet and finds that its IP address is not on one of the local subnets, it forwards the packet to the device 10.200.200.2 for further routing. The subnets 10.200.200.8/29 and 192.168.200.128 are also forwarded to 10.200.200.2 because CE1 uses the MPLS network to route traffic to CE2.

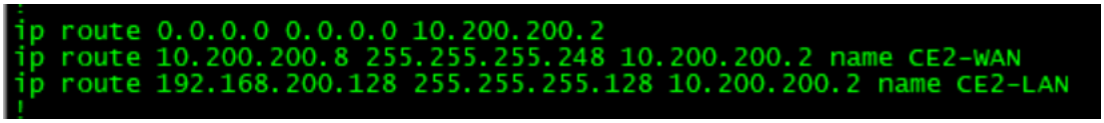

Figure 3.11: CE1 routing configuration

In an enterprise network, securing of data is very critical. One way of securing data is through implementation of an Access Control List (ACL) used to filter traffic and limit user access to information, systems and files on the network. Configuring an access control list enhances the network security through the defined permissions and access rights. [43] There are several types of ACLs. CE1 is configured with an extended ACL. An extended ACL provides granular level of control. Data packets can be filtered with more precision based on different factors such as source and destination ports, IP addresses and protocol types. [43] In Cisco systems, a single-entry deny entry blocks all traffic. Hence, it is advisable that one has one permit entry on the ACL in order to allow

traffic to authorized users to have access. This is due to the implicit deny that exist on Cisco routers by default. [44]

Figure 3.12 below shows the configured extended ACL on CE1. The extended ACL is called CE1-IPSEC and the IP entries 10.200.200.0/29, 192.168.200.0/25 and 192.168.200.128/29 are permitted subnets. All IP traffic is allowed to flow through the router. This ACL is applied on Gigabit Interface 0/0 which connects to the ISP.

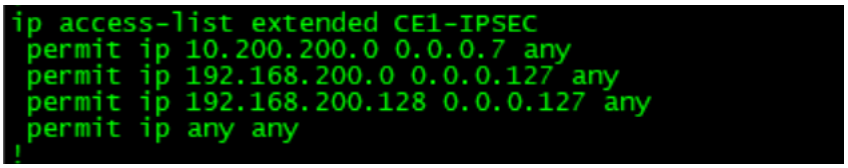

Figure 3.12: CE1 Access Control List

The console port on CE1 is located on the back plain of the router. This is the physical port used for local direct access for the administrator to manage the device. This port is used for initial and ongoing configurations, it is also used to access and manage the device when remote access fails. On CE1, the line console 0 port is configured with a type 7 password for login. This ensures that only an administrator with the password is allowed to access the router through the console port. CE1 has 0-15 Virtual teletype (VTY) lines that can be used for remote access to the router using telnet or Secure Shell (SSH). This means that 16 simultaneous virtual connections can be allowed either through telnet or SSH. The inbound connections to the router use type 7 password and login local. This means that all virtual connections will be authenticated using the password configured under VTY lines. Figure 3.13 below shows the console and VTY configurations for CE1.

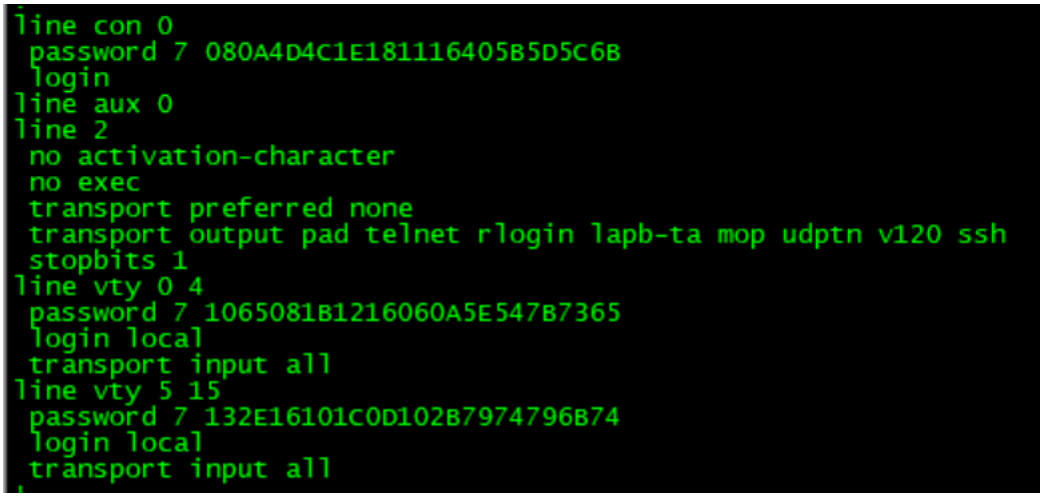

Figure 3.13: Console and VTY configuration for CE1

B. *ROUTER 2*

CE2 is configured on Cisco IOS Software, 1841 Software. The router runs on 191K bytes of NVRAM, with 233472K/28672K bytes of memory with two (2) Fast Ethernet ports. The router has 62720K bytes of Read/Write ATA CompactFlash as shown in Figure 3.14 below. The router consist of two Fast Ethernet interfaces, two serial ports and two terminal lines.

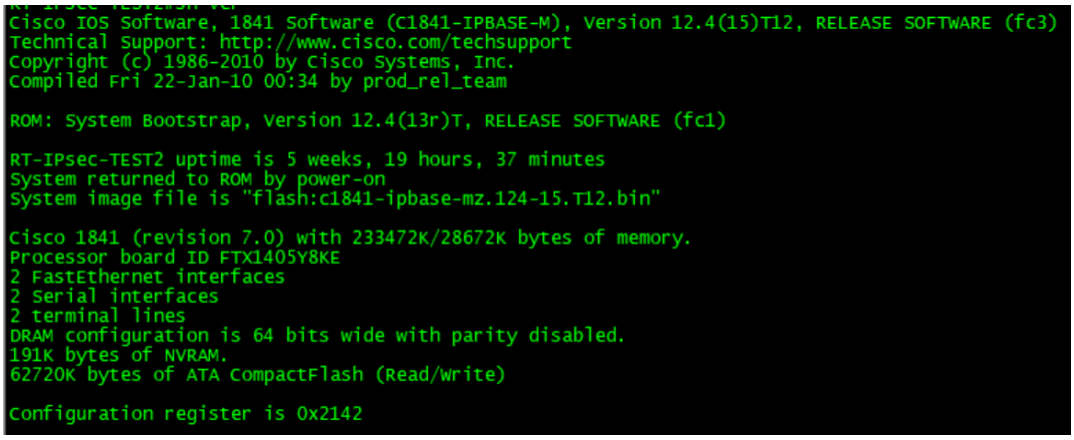

Figure 3.14: CE2 router version

The configuration register on CE2 is set to 0*2142. With the configuration register of 0*2142 on CE2, the router's boot process follows the sequence shown in Figure 3.15 below. Since the configuration register 0*2142 ignores all configurations in the Non-

Volatile Random Access Memory (NVRAM) it means that when a router is rebooted, all data not written to the Read-only memory (ROM). In this case all start-up configurations will be bypassed. [33]

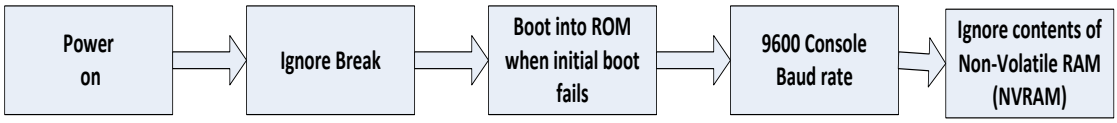

*Figure 3.15: Router Configuration Register of 0*2142 boot process*

The hostname for CE2 configured as RT-IPsec-TEST2, with the naming sequence as device type, Protocol and Site number. RT for router, IPsec being the protocol suite under research and TEST2 for test site number 2. The router is also configured with Dynamic Host Configuration Protocol (DHCP) to assign IP address, subnet mask and default gateway information to Local Area Network (LAN) hosts automatically. The DHCP pool is named MPLS_IPsec_Site2 and address range is 192.168.200.128 to 192.168.200.255. The DHCP pool excludes IP addresses 192.168.200.129 to 192.168.200.140 from being assigned to hosts automatically. These ten (10) IP addresses have been excluded to allow for devices such as switches, routers and servers to be assigned statically. The lease time is infinite and CE2 also uses the same DNS servers 192.168.0.10 and 172.16.120.249. Figure 3.16 below shows the DHCP pool configuration on CE2.

```
ip dhcp excluded-address 192.168.200.129 192.168.200.140
!
ip dhcp pool MPLS_IPsec_Site2
   network 192.168.200.128 255.255.255.128
   default-router 192.168.200.10
   domain-name MPLS_IPsec_Site2
   dns-server 192.168.0.10 172.16.120.249
   lease infinite
!
!
```

Figure 3.16: CE2 DHCP pool

The two Fast Ethernet interfaces on CE2 are 0/0 connected to PE2 through fiber cable and 0/1 connected to the CE2 LAN. The distance between CE2 and PE2 is two kilometers (1Km). Fast Ethernet can support LAN speeds of up to 100Mbps and is suitable for small networks such as home applications and small businesses. Fast Ethernet runs on both half duplex and full duplex modes. Fast Ethernet is cheaper than Gigabit Ethernet and can cover distances of up to seventy kilometers (70Km). However, in large Enterprise

networks, Fast Ethernet would create bottlenecks and cause high latency and packet losses due to the high demand for high speed and high traffic volumes. [45] Figure 3.17 below shows the Fast Ethernet configuration on CE2. Fast Ethernet 0/0 connects to PE 2 and is assigned IP address 10.200.200.10/29 which Fast Ethernet 0/1 which connects to CE2 LAN is assigned 192.168.200.129/25. The IP address subnet for PE2 to CE2 has eight IP addresses. This is to allow the intermediate device between PE2 and CE2 to be assigned the IP address within this IP range. The configured duplex is auto which allows the interface to determine the ideal duplex mode.

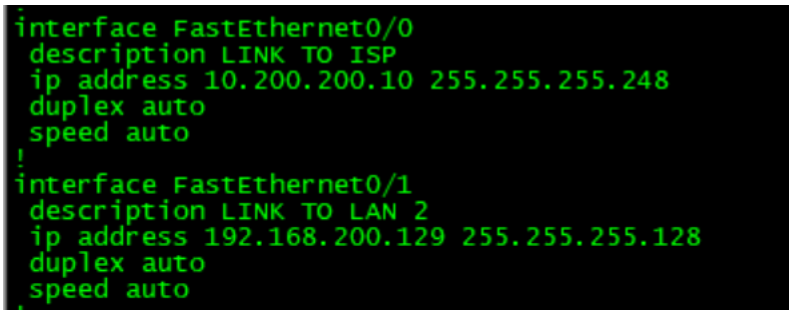

Figure 3.17: CE2 Interface Configurations

The default route for CE2 is 10.200.200.9 which is PE2. All traffic to from CE2 to CE1 is routed through PE1 as shown in the static routing configuration specified in Figure 3.18 below. In this configuration, the entry IP route 0.0.0.0 0.0.0.0 10.200.200.9 acts as the gateway of the last resort for all unknown IP routes for CE2. CE2 will also use this entry to route traffic for all unspecified. Since CE2 runs IP only, its uses these entries in the routing table to find the best route for forwarding traffic to the next hop on the network.

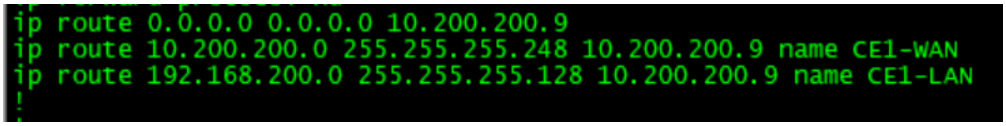

Figure 3.18: CE2 routing configuration

The extended ACL for CE2 is called CE2-IPSEC and has four entries as shown in Figure 3.19 below. The rules in the extended ACL permit access for the subnets 192.168.200.0/27, 192.168.200.128/25 and 10.200.200.8/29. All other IP traffic is

allowed to flow through the router by the entry ***permit ip any any*** on the ACL. The ACL is applied on the interface connecting to the ISP.

```
ip access-list extended CE2-IPSEC
 permit ip 192.168.200.0 0.0.0.127 any
 permit ip 10.200.200.8 0.0.0.7 any
 permit ip any any
 permit ip 192.168.200.128 0.0.0.127 any
!
```

Figure 3.19: CE2 Access Control List

Line console 0 is configured with a type 7 password to login and manage the device physically. CE2 allows for five remote sessions through telnet and SSH using VTY 0 to 4. In order to access the router through console or VTY terminal, the user is required to login with the configured password for these connections. If login is not enabled on the VTY terminal, it means the router cannot be managed remotely. The console and VTY configurations for CE2 are shown in Figure 3.20 below.

```
line con 0
 password 7 0724204E59080D0445425A5445
 login
line aux 0
line 0/0/0 0/0/1
line vty 0 4
 password 7 09674F0B0E040313595C55726A
 login
!
```

Figure 3.20: Console and VTY configuration on CE2

3.2.4 Port Mirroring and Packet Sniffing

In order to monitor the incoming and outgoing traffic at the HQ CE, Switched Port Analyzer (SPAN) session was configured. This feature is sometimes called port monitoring or port mirroring which allows for selected network traffic to be copied to the sniffer for monitoring and analysis. [46] As shown in Figure 3.21 below, the SPAN session 30 has been configured to capture traffic from VLAN 603 and floods all copies of packets to Gigabit Ethernet 0/0 where the Security Onion sniffer is connected. All packets received by the network analyzer are saved for further analysis.

```
monitor session 30 source vlan 603
monitor session 30 destination interface GigabitEthernet0/0
```

Figure 3.21: SPAN configuration

A. Security Onion

Security onion is a free open source threat hunting, enterprise security monitoring, and log management tool. It has been configured on the file server at HQ to monitor and analyze the mirrored packets. Security Onion is installed in a distributed deployment which includes manager node, sensor nodes, and search nodes. The sensor nodes run Elastic search components. Security Onion is used to perform deep packet inspection to hunt for vulnerabilities inherent on the deployed IPsec over MPLS network.

B. Wireshark

In addition to Security Onion, Wireshark, the packet capturing tool that has been used to sniff, analyze and dissect the raw data traversing the network. The traffic analyzer captures frames in the MPLS/IPsec enabled network, analyzes the data and provide statistics that enable the researcher to evaluate the security posture of the enterprise network using these technologies. Wireshark will analyze IPv4, MPLS and ESP parameter for the data packets and examine the ability of viewing raw data once packets are captured. In order to capture and store the packets for analysis, two folders named MPLS Capture and IPsec Capture been configured. Figure 3.22 below shows the IPv4 preference configuration for Wireshark. When the ***decode IPv4 TOS field as diffserv field*** is enabled in Wireshark, it means the IPv4 type of service will be decoded as a differentiated service.

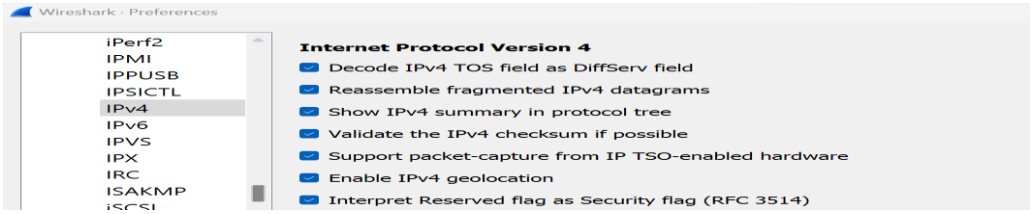

Figure 3.22: IPv4 Wireshark preferences enabled

By default, this preference is enabled in Wireshark and follows the RFC2474/RFC2475 standards for differentiated services providing different service levels for traffic streams on the network infrastructure. [47] The other IPv4 preferences enabled on this capture are reassemble fragmented IPv4 datagrams, show summary in protocol tree, validating the checksum for IPv4 and packet capture from Internet Protocol TCP Segmentation offload (TSO) enabled hardware is supported. In this capture, the originally reserved flag will be interpreted as a security flag. This follows the RFC 3514 which describes the security flag

in the IP header. [48] It is important to specify how this bit will be interpreted in this capture because in networks where packet filters, firewalls and intrusion detection systems are implemented, it is difficult to distinguish between unusual and malicious packets. MPLS header capture is also enabled on UDP port 6635. In this study, it is assumed that the lowest label is used to identify the flow of MPLS packets on the LSP. Figure 3.23 below shows that this feature is enabled during the capture of packets on the network.

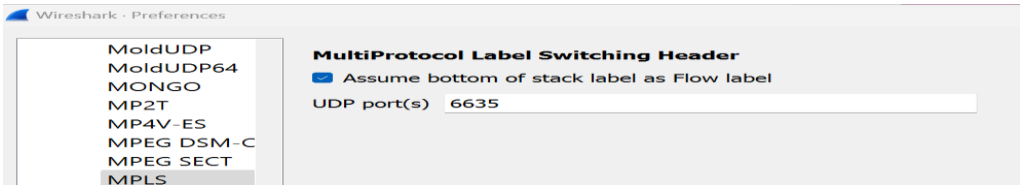

Figure 3.23: MPLS Wireshark preferences enabled

The Encapsulation Security Payload (ESP) preferences enabled on both the MPLS capture and IPsec capture are shown in Figure 3.24 below. The ESP security associations include checking the sequence numbers of the ESP frames, attempting detection or decoding NULL encrypted and encrypted ESP payloads. The NULL encrypted payload is payload whose plain text is not change. This means that NULL encrypted payload does not provide confidentiality for data, however, authentication and integrity of data is fully supported. Hence the decoded payload captured from a device passing IPsec traffic will show in plain text. The feature to detect or decode encrypted ESP payload will support authentication, integrity and confidentiality. The decoded payload will be encrypted. [49] Additionally, the Wireshark capture will attempt to check the ESP authentication.

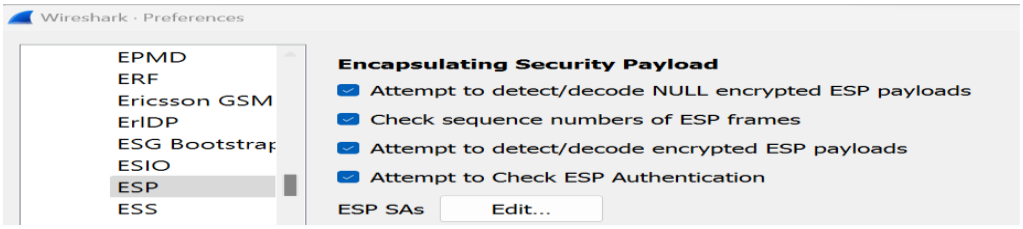

Figure 3.24: ESP preferences enabled on Wireshark

3.3 IPsec over MPLS

IPsec provides security during transmission of sensitive data over the service provider MPLS network. It acts as network layer protection by authenticating and protecting IP

packets between IPsec nodes. [14] In this study, IPsec-v2 and IKE-v1 is used during implementation. In the configuration for the cisco routers CE1 and CE2, IKE is synonymous with Internet Security Association and Key Management Protocol (ISAKMP). [50] The IPsec tunnels 10 and 20 are configured between HQ CE and the remote sites CE1 and CE2 as shown in figure 3.25 below.

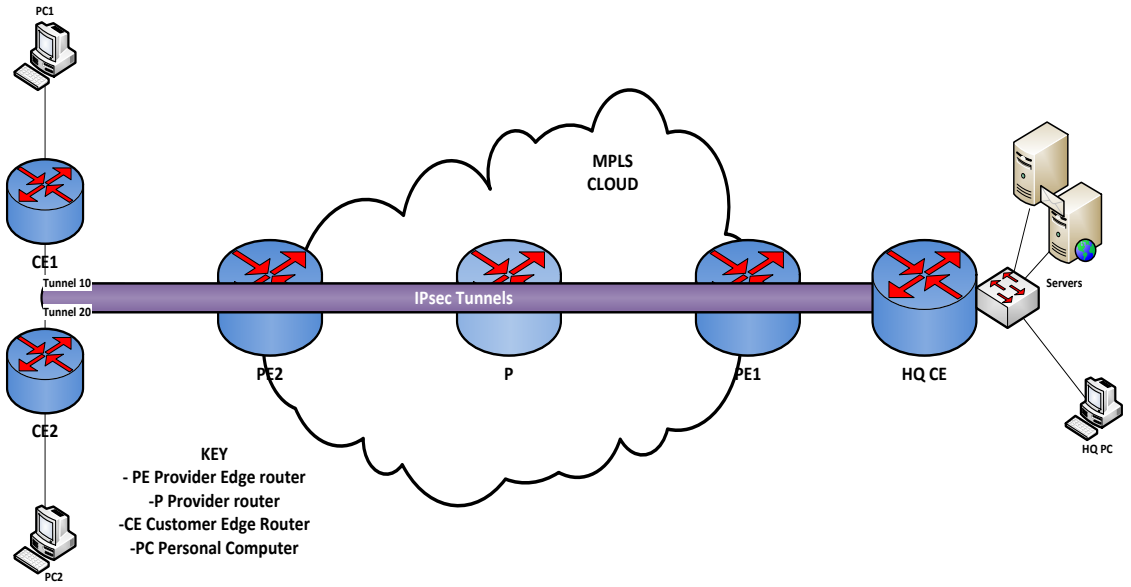

Figure 3.25: IPsec implementation

The configuration of the ISAKMP policy is required for both Remote Access IPsec VPN and Site-to-Site (L2L) which provides more secure negotiations between the tunnels between two points such as CE1 and CE2. ISAKMP is part of IKE and the standard and procedures for authenticating peers communicating, Security Associations (SA) creation and management and mitigating threats using IKEv1 are described in RFC 2407, 2408 and 2409 which have been obsoleted by RFC4306. This framework for key exchange and authentication is necessary in order to establish and maintain secure communication on the network. [51] [52] In this study, the IPsec configuration is policy based. The VPN tunnels created from HQ CE to CE1 and CE2 are specified in the configured policies 10 and 20. The policy numbers specify the order of priority in this configuration. The ISAKMP Policy 10 is configured to use the Advanced Encryption Standard (AES) encryption and the SHA hash. AES is a symmetric block cypher which converts blocks with key sizes of 128, 192 and 256. It is the most strong security protocol, since it can be

applied in both hardware and software [53]. In the policy 10 configuration the command ***encr aes*** shows that the encryption standard used is AES 128. However, in policy 20, the encryption standard used is AES 256. In both policies, the authentication method used is pre-share. This authentication argument specifies the IKE authentication to be used on ISAKMP policy 10 and 20. The policies are applied using group 2 which is a default group using the Diffie-Hellman group 2 (1024 bit). The crypto configuration of the ISAKMP policies 10 and 20 is shown in Figure 3.26 below.

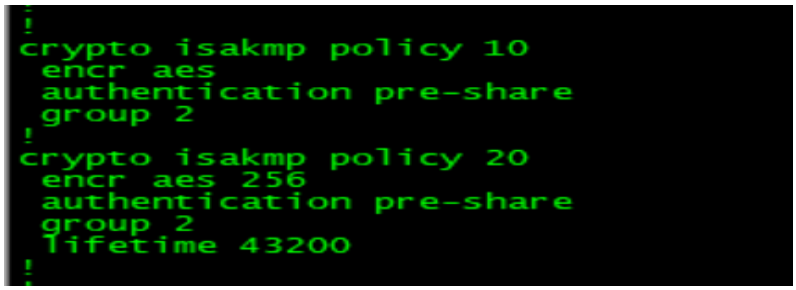

Figure 3.26: ISAKMP policies configuration

The IPsec mode configured is tunnel mode. In this mode, the entire IP packet is encapsulated and offers security for data between two different networks. The configuration also contains the IPsec transform sets, profile, the security association lifetime of 24 hours as well as the periodic ISAKMP keep-alive time. The transforms set specifies the combination of security algorithms and protocols which should match on both ends of the peers. The transform set is used during the IPsec SA negotiations by peers and to create an SA for protecting data flows. The SA lifetime and transform set are in relation to the IPsec tunnel. Figure 3.27 below shows the ISAKMP keys for CE1 with IP address 10.200.200.1 and CE2 with IP address 10.200.200.10, transform set, SA lifetime and IPsec profile.

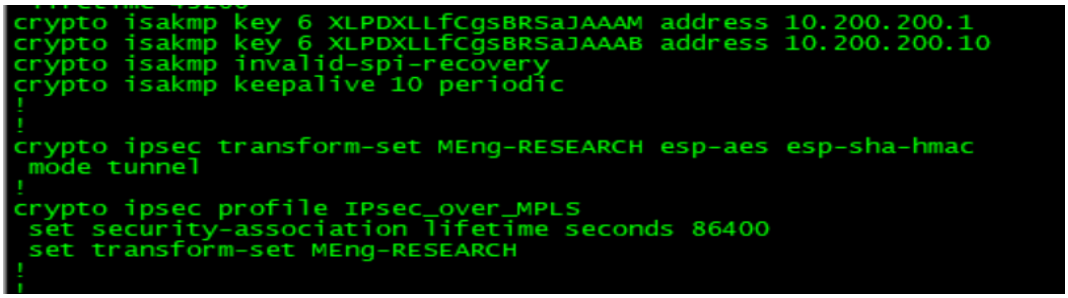

Figure 3.27: IPsec Profile, transform set and ISAKMP keys

Two tunnels have been configured. Tunnel 10 is configured between the intermediate CORE network switch with the IPv4 address 172.16.220.1 through the ISP MPLS network to CE1. The tunnel is configured with the Maximum transmission unit (MTU) of 1400. The MTU specifies the maximum limit of the packet length to be transmitted on tunnel 10. By default, most enterprise links support the MTU of 1500. However, when encapsulation takes place, the size of the packets is increased and this may result in fragmentation. Since not all networks handle fragmented packets this may result in loss of data. In order to avoid packets on the tunnel from being fragmented, the MTU is specified to 1400. The source of tunnel 10 is 10.200.200.9 and the destination is 10.200.200.200.1. Tunnel 20 is configured with the point to point IPv4 address 172.16.220.5. The source is 10.200.200.9 while the destination is 10.200.200.10 which is CE2. Figure 3.28 below shows the configuration for tunnel 10 and 20 on the intermediate router from CE1 to CE2.

```
interface Tunnel10
 description CE1-TUNNEL-VIA-ZAMTEL
 ip address 172.16.220.1 255.255.255.252
 ip mtu 1400
 tunnel source 10.200.200.9
 tunnel destination 10.200.200.1
!
interface Tunnel20
 description CE2-TUNNEL-VIA-ZAMTEL
 ip address 172.16.220.5 255.255.255.252
 ip mtu 1400
 tunnel source 10.200.200.9
 tunnel destination 10.200.200.10
!
```

Figure 3.28: Tunnel 10 and 20 configuration

The interface VLAN 603 has been configured with helper address 192.168.0.10 and 172.16.130.249 which are both DHCP and DNS servers in this research network. The extended ACL named IPsec_over_MPLS filters subnets and protocols on the network. The permitted subnets and protocols are permitted while those not defined are denied. The Access control list enabled on a Cisco device contains an implicit deny rule at the end. This means that all entries not listed on the ACL will be denied by default. Figure 3.29 below shows the interface vlan 603 which is the source of the tunnels and the Access Control List (ACL) implemented on the CORE CE.

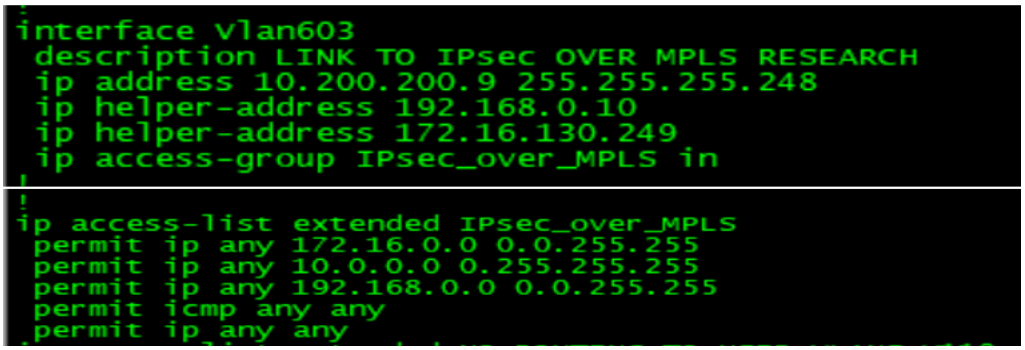

Figure 3.29: Access Control list applied on CORE CE

The IPsec peers exchange authenticated and encrypted messages using the parameter configured on the Customer Edge routers. Table 3.3 below summarizes the configurations of IPsec Tunnel 10 and 20 on the Core router to CE 1 and CE2.

Table 3.3: IPsec Configuration Table

Tunnel	**IP Address**	**Operation Mode**	**Tunnel Source**	**Tunnel Destination**	**Policy**	**Encryption Infor.**
10	172.16.220.1	Tunnel	10.200.200.9	10.200.200.1	10 and 20	AES 128
20	172.16.220.5	Tunnel	10.200.200.9	10.200.200.10	10 and 20	AES 256

This chapter has focused on the design and implementation aspect of the IPsec over MPLS network as stated in objective 1 of this study. During the design and deployment of the network in the live environment, several tools have been used. The use of simulation, configuration, troubleshooting and testing tools ensured that initial device configurations were completed and tested for functionality and compatibility. Additionally, the deployment of sniffing and mirroring tools in the network ensured that live data was being captured and stored in preparation for data analysis.

CHAPTER FOUR

DATA COLLECTION, ANALYSIS AND DISCUSSION

In this chapter, the packets from the MPLS and IPsec network are captured, stored and examined using Wireshark and Security Onion to determine the security posture of the network implemented with the technologies under review. Collection of packets was conducted for eighty three (83) days. The period for capturing the packets was long enough to study the traffic patterns and trends on the network for analysis.

4.1 Data Collection on MPLS Capture

These packets are captured on the interface between the PE and CE routers. The PE exit interface is the entry point for the Customer network environment and the appliance for capturing and mirroring packets is placed there. The choice to place the MPLS capture at this point of the network is two-fold. The ISP's MPLS environment is a trust network where devices from customers are not allowed to connect. Additionally, this point is the entry and exit point for the customer network. Capturing packets at this point of the network gives the overall picture of network activities for incoming and outgoing traffic. Using Wireshark conversation filter to analyze the captured packets, the discovered packet information includes time of capture, source and destination IP address, protocol type, packet length or size. Figure 4.1 below shows a Wireshark snippet for the captured packets before IPsec implementation.

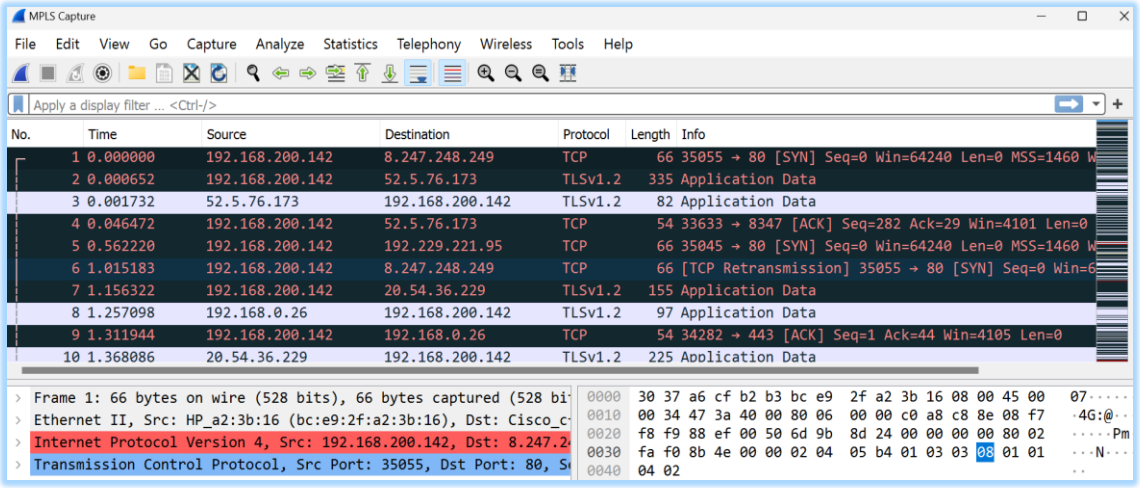

Figure 4.1: Wireshark MPLS capture sample

During the hunt on the MPLS capture, the total number of packets captured were 7,228,396. The total size of the captured file was three Mega Bytes 3MB) during the MPLS hunt. These included 7,100,772 total TCP packets, 117, 526 UDP packets, 6,984 TELNET traffic and 3,114 packets whose protocols could not be determined. These statistics give an in-depth overview of what services are being accessed on the network. While the traffic obtained on the edge routers transverses over the ISP MPLS network, no labels are obtained on both the MPLS capture and the IPsec capture. This shows that all labels are inserted and removed by the Provider Edge routers on the ISP network boundary before entering the Customer Edge device.

Table 4.1: Packet Capture Information before IPsec implementation

MPLS PACKET CAPTURE FOR		
COUNT	**TYPE**	**INFORMATION**
7, 228, 396	All Packets	
7, 100, 772	TCP Packets	IPs, Ports, MACs, services
117, 526	UDP Packets	IPs, Ports, MACs, services
6, 984	TELNET	Passwords, commands run on devices
626, 875	HTTP	Requests and Responses
54,752	HTTPS	Requests and Responses
534, 752	DNS	Query, response, service, type stats
33	LOOP	Network device information (source and destination), type, time and looping interface.
3, 114	Unknown	
48	Endpoints	Ethernet, IPv4, IPv6
0	Labels	No information captured

Table 4.1 above shows a summary of the packets captured on network traffic that transverse from HQ to CE1 and CE2. This summary also includes network traffic to and

from internet. Interestingly, thirty three packets where captured as routing loops between network devices.

4.2 Data Analysis on MPLS Capture

4.2.1 Packet Information

The TCP packets captured contains Synchronization flags, Acknowledgement messages, their length and actual data packets. The deep packet inspection on the MPLS Capture shows that the packets contains information about the source and destination IP addresses, source and destination port numbers, source and destination device type, sequence numbers, protocol types and the status of the conversation (either complete or incomplete). The type and length of the TCP and UDP payload can be determined from this analysis. Figure 4.2 below shows the traffic patterns on the network.

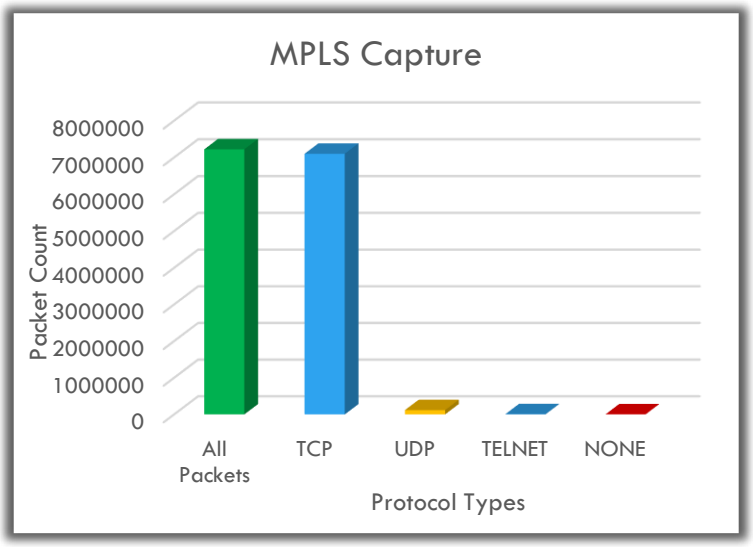

Figure 4.2: MPLS Capture Packet Information

It is worth noting that even though TELNET uses TCP port 23, analyzing the packet capture shows that TELNET traffic is not presented as part of the total TCP packet count. Other protocols such as HTTP, HTTPS, DNS and ARP are presented on either TCP and/or UDP packet count. Packet information also includes the endpoints on the network such IPv4 and IPv6 devices. Additionally, the Media Access Control (MAC) addresses can be seen in the analyzed packets. By observing the traffic patterns and the captured packets on the network, one can determine the transactions and utilization on network systems,

trace connections and machines accessing secure and unsecure sites, view transaction contents for suspected traffic streams and determine traffic that poses a threat on network security. These traffic streams might include machines working as botnets. This information helps the network administrator to identify traffic bursts and develop risk profiles, mitigation policies and guidelines for securing the enterprise network.

MPLS provides traffic separation for the packets as the move along the network. With the use of labels in MPLS environment, it is hard for an attacker to spoof labels. For example, since MPLS labels ***are only used*** in the ISP environment to separate traffic flows for several customers, the routing packets are protected from traditional IP attacks on the IP addresses. MPLS also protects the network from routing table poisoning attacks in which the actor uses the advertised IP address routes on the network to edit the routing table and inject unwanted IP address routes on the network routers. However, this does not extend to the CE network where the customer uses traditional IP routing. The MPLS capture gives the network administrator an overview of the transactions and traffic patterns on the network. The packet information captured on the customer's infrastructure exposes the network to security risks and vulnerabilities that actors can use to attack the CE network. This poses a risk of common traditional IP targeted attacks towards this network.

4.2.2 MPLS Security

Using the follow conversation stream feature, it can be seen that information for any default unsecure settings on devices and unsecure protocols is not secured as data passes through the MPLS network. Information such as credentials for network devices using TELNET are discovered in plain text. All transactions using unsecure protocols such as HTTP and TELNET are not encrypted.

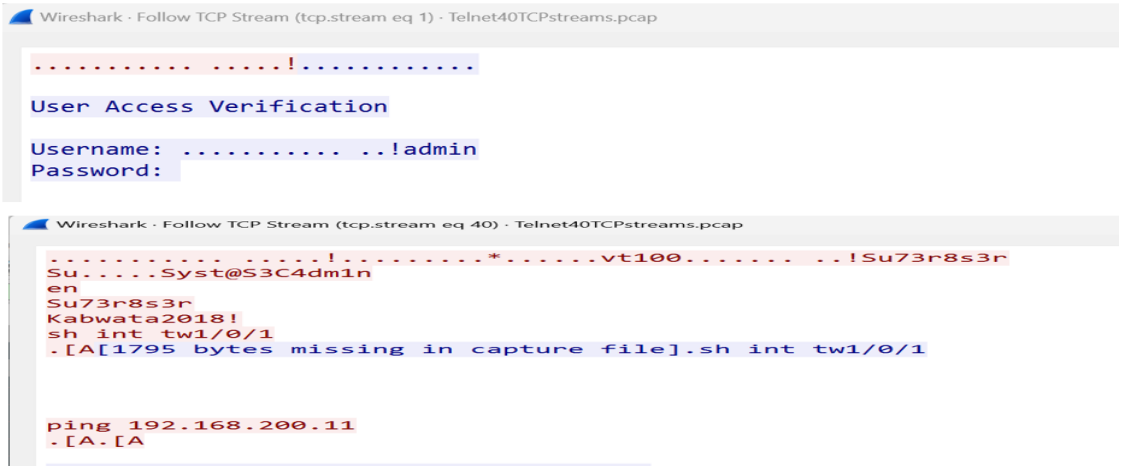

Figure 4.3: TCP streams for Telnet traffic

Figure 4.3 above shows a snippet of TCP streams for TELNET traffic. The snippet shows the analyzed packets with username and passwords in plain text. The TCP stream is the TELNET conversation between the CORE CE router 10.200.200.9 and CE1 10.200.200.1. MPLS does not hide information transmitted with unsecure protocols. In an event that a malicious actor is listening in on these TELNET streams, they can use the discovered credentials to log into network devices and change the configurations on them. This will result in Denial of Service (DoS) and disrupt availability of network resources to intended users. This may also result in more exploitation for user because once a malicious actor has access to network devices, they are able to scan active devices on the network and cause more harm to systems and resources on the network. While MPLS provides the separation of traffic streams, it does not provide confidentiality for the network resources. Additionally, in enterprise networks where legacy systems that use unsecure protocols such as HTTP and TELNET still exist, MPLS cannot provide adequate security to protect the data from being read by anyone listening in the conversation. The source and destination IP addresses in the CE network also exposes the network to IP spoofing attacks.

While encrypting passwords provides some level of security for network device credentials, the unencrypted configurations on the device such as user names and device settings will appear in plain text as long at unsecure protocols are used to transmit traffic over the MPLS network.

Figure 4.4 below shows the TELNET stream for CORE CE. The stream shows the network device configuration with usernames and passwords that are encrypted using SHA256. The snippet shows type 7 and type 8 passwords that have been encrypted. This shows that when password encryption is configured on the CE router, the device will hash the plain test password only.

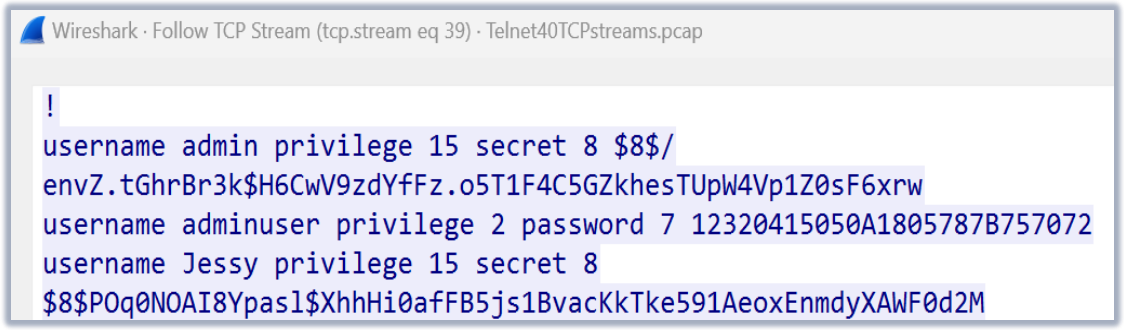

Figure 4.4: TELNET Stream with encrypted passwords

By nature, MPLS will not provide any hashing mechanism to the data sent in plain text. However, for TCP traffic accessing web service through secure protocol HTTPS, the payload is encrypted using TLSv1.2. This result indicates that MPLS will transmit packets that encrypted by the source protocol. The payload for Web traffic will be transmitted as TLS encrypted as it accesses web servers. This provides data privacy and security per connection for network traffic crossing the perimeter.

4.2.3 Applications Response Time

In order to measure the performance of interactive systems such as Email and Websites from the devices connected to CE1 and CE2 through the MPLS network, analyzing the round trip times for PC 192.168.200.142 to the internal E-mail server at the CORE CE at Head Office and an external Website are frequently used. For Email service, thirty (30) streams of incoming and outgoing email traffic was analyzed. It can be seen from Figure 4.5 below that the round trip time was consistently between 42ms and 56ms over a sample time of 25 minutes for each email stream from the mail server connected to HQ CE to the Personal Computer of the user at CE1. This shows that performance of MPLS links between CORE CE at Head Office and CE1 and CE2 for TCP traffic is optimal. MPLS

efficient use of network resources results in better performance for application TCP traffic such as email.

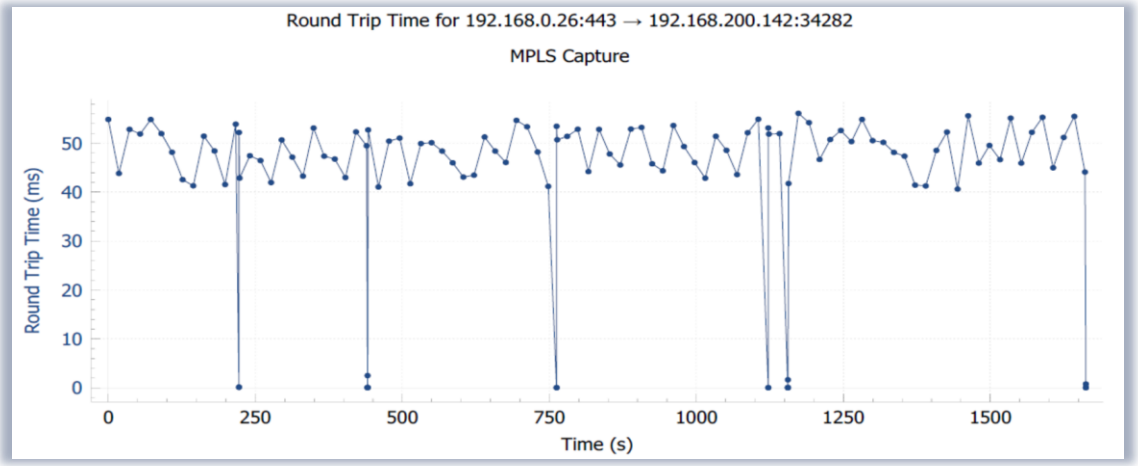

Figure 4.5: Email Response Time

Forty two (42) streams of internal HTTP and external HTTPS traffic was analyzed to assess the average response time. In order to access Websites on the internet, PC2 connects to CE2 which connects to ISP MPLS environment to access CORE CE. Since internet connectivity is through CORE CE at Head Office, all external web traffic takes that path from CE1 and CE2. Figure 4.6 below shows the round trip time for Web traffic from an external Website to the PC connected to CE2.

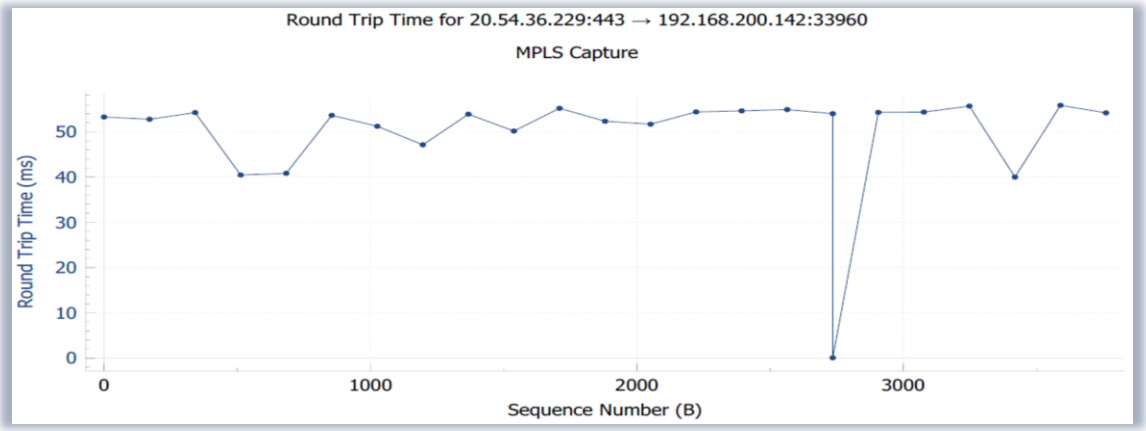

Figure 4.6: Response time from website to computer

This is the average depiction of the response time for all website traffic analyzed. The round trip time for external Web traffic is between 40ms and 52ms while the internal web traffic streams showed the average round trip times between 10ms and 22ms. These results show that MPLS is quiet efficient in the use of network resources both for internal and external web traffic. The response times are optimal for both scenarios.

4.3 Data Collection on IPsec Capture

The IPsec packets are captured at the Customer Edge (CE) routers. The capture indicated 7, 049, 860 packets was actual data, 798, 330 showed identity protection and 285, 770 in quick mode. Out of all the packets captured on IPsec, 268,920 packets had TCP errors. Table 4.2 below shows the summary of the IPsec capture. The IPsec capture also shows each packet is time stamped.

Table 4.2: IPSEC PACKET CAPTURE

IPSEC PACKET CAPTURE		
Packet Count	**Protocol Type**	**Information**
8, 133, 960	Total Packets	Identity protected, Quick Mode and encrypted packets
7, 049, 860	Data Packets	Packet count, Time, Source and Destination IP address, ESP payload
798, 330	Identity Protection	SA proposals, key exchange, authentication and identification of IPsec peers.
285, 770	Quick Mode	Transform set information
268, 920	Errors	TCP errors

4.4 Data Analysis of IPsec Capture

4.4.1 Data Security

The results in IPsec Capture shows a set of sis (6) packets with Security Associations at the beginning of each stream. Two of the six packets show SA proposals between peers. In this pair of packets, the initiator and responder negotiates for encryption algorithm, length of the key, hash algorithm, authentication method and duration. The next two packets shows the key exchange between the peers. In these packets, key exchange information such as key exchange data, the exchange type and the nonse data. The last two packets shows the identification and authentication of IPsec peers. The IPsec peers are 10.200.200.9 for the CORE CE, 10.200.200.1 CE1 and 10.200.200.10 for CE2. The CORE CE exchanges these sets of packets with either CE1 or CE before actual data is transmitted on the IPsec tunnel. Following the six SA packets are three packets showing quick mode. Analysis of these packets shows that the SA for tunnel 10 and tunnel 20 are fully protected. The packets also contain information set out in the transform set named MEng-RESEARCH configured on the CE routers. At this point the protected data can be tunneled through the IPsec link. All payload packet shows ESP encapsulated on the IPsec Capture. When data is ESP protected, it becomes much more secure than data transmitted without any encryption. IPsec provides nonrepudiation during SA parameter setup for peers. This improves security of data in that its source can be verified without any refusal of responsibility. The source data can be compared with the destination data and this reduces the chance of data being manipulates as it travels along the network path. Since MPLS environment is in the public domain, IPsec protects the data from being read by anyone who may be listening in. The basic security features inherent on MPLS cannot replace IPsec. The results analyzed in this paper show that while MPLS provides efficient use of network resources, it cannot provide the confidentiality and integrity required for sensitive data being transmitted by Enterprise customers through the public infrastructure. This is even more evident when the transmitted data is using unsecure protocols and applications. IPsec provides the security that MPLS cannot provide to the transmitted data. The results obtained also show that ESP provides encryption and authentication of data between peers. This is especially critical for IPsec peers that are connected through the public network.

4.4.2 Larger Packet Length

The results show that all analyzed IPsec packet lengths were larger than the packet lengths for MPLS capture by average 20 bytes. Regarding the packets larger than 1500, it is assumed that packets will be fragmented as they travel along the way. This in effect reduces the network performance as it increases the traffic overhead. With increased overhead, the reliability of data transmission reduces as error rate and latency on the IPsec links increases. Figure 4.7 below shows the minimum and maximum packet lengths for both MPLS and IPsec capture. The results indicate that IPsec capture had larger packets compared to MPLS capture. The MPLS capture shows that packet lengths were between 39bytes to 1,280 bytes for minimum values and 40bytes to 1,514bytes for the maximum values. On the other hand, IPsec capture results show that the minimum packet values were between 81bytes to 1,300bytes while the maximum values are between 99bytes to 1,540bytes.

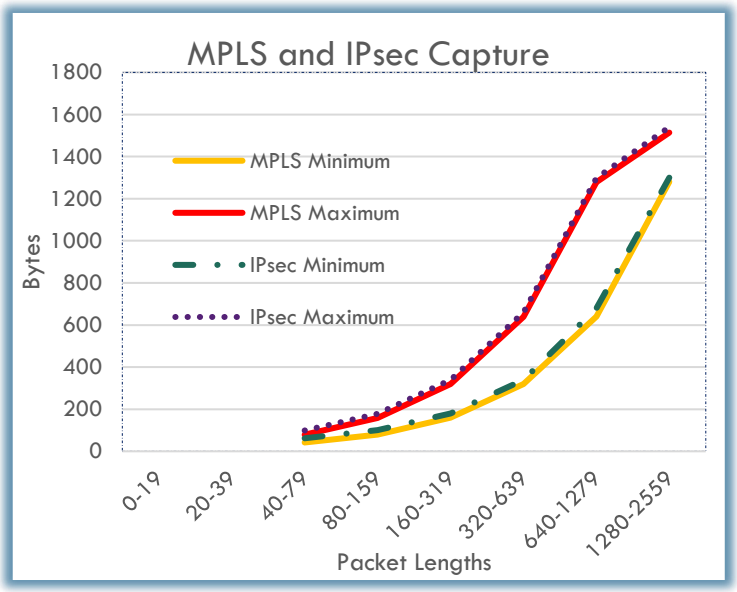

Figure 4.7: IPsec Packet Lengths

4.4.3 Error Rate

Due to the increase packet length on IPsec, it is reasonable to conclude that the additional overhead results in TCP errors. Typically, the allowed MTU for interfaces on the CE routers in this network is 1500. It is assumed that the 268, 920 TCP errors observed are as

a result of packets larger than the default 1500 bytes failing to pass on the actual router interfaces. Figure 4.8 below shows the total packet errors on IPsec network.

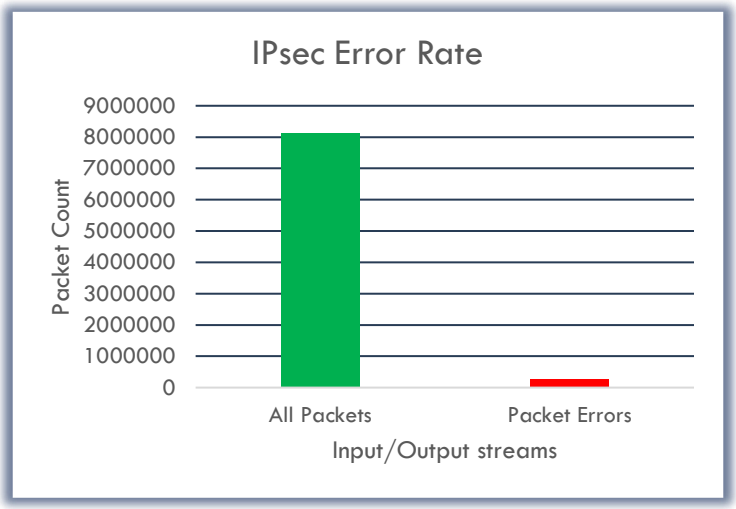

Figure 4.8: IPsec Error rate

While there was 43,845 errors found on the MPLS capture, the number of errors on the IPsec packets is significantly higher. By comparison there is percent error rate on 8, 133, 960 IPsec packets while 7, 228, 396 MPLS packets incur 0.6 percent error rate. The higher TCP error rate results in data loss on the IPsec links which can affect performance of larger Enterprise networks transmitting larger amounts of data.

The error rate due to additional payload prompted the researcher to limit the interface MTU to 1400 stop packets larger than1500 from being transmitted on the IPsec over MPLS links. This configuration automatically blocks all packets larger than 1400byts and avoids packet drops on the network. The performance impact of reducing the MTU from the default 1500 bytes to 1400 bytes on the interface creates a gap for further analysis in future research.

This chapter has assessed the security limitations of MPLS using the captured packets. It has also investigated the impact of implementing IPsec over MPLS. Of utmost concern is the lack of data security for MPLS network without IPsec implementation. The chapter has also shown the impact of IPsec on applications performance and security on enterprise

networks. The goal of securing data as it traverses the public network has been achieved through data encryption and authentication.

.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATION

When MPLS is combined with Internet Protocol Security (IPsec), both technologies can provide more security for enterprise WAN networks. The framework of related protocols that IPsec provides protects one or more data flows between network peers, thus data confidentiality and integrity can be achieved. Both MPLS and IPsec provide inherent security features that improve the security posture and are flexible to work with other IP solutions for large enterprises.

This study used observation and experiments for an IPsec over MPLS network through the service provider's public network. The tools SecureCRT, Putty, Cisco Modeling Labs (CML) and Microsoft Visio used for modelling, emulation, setup and configuration of network helped the researcher to deploy the network. Wireshark and Security Onion were used for packet sniffing, capturing and analysis of data packets. The research focused on MPLS and IPsec operations and architecture, their implementation over an enterprise network and performance in terms of efficiency and security when combined.

5.1 Conclusion

The study has looked at benefits of implementing IPsec over MPLS in order to provide data protection and leverage on MPLS features for the efficient use of network resources. MPLS and IPsec are better together. They are both transparent to the applications on the network. This means that MPLS and IPsec can be implemented on any network type without compatibility issues. The study has also looked at the MPLS architecture, configuration and deployment of IPsec over MPLS in an enterprise network. It has been established that using MPLS provides minimal security to data through the use of labels. This feature both separates traffic streams and provides efficient use of network resources as IP addresses are not used to route traffic in the MPLS environment. This lowers the latency and improves speeds on the network. Additionally, the use of VPN instances in MPLS provides security to the routing information for enterprise customers in that each customer has their own routing information separated from the other. This protects one's routing information from being learnt by another MPLS customer. The efficient use of network resources can be seen from the application response times on MPLS. For both

external and internal systems, the application response times are way below 100ms for the traffic streams analyzed. However, MPLS does not provide any encryption or authentication of peers and confidentiality of the data is not protected. PE routers transmit data as it is received without providing any form of encryption to protect the data from being read. When the PE router receives data in an insecure protocol or application, the packets are labelled in order to improve the speeds of transmission and provide flow control for the packets. When data is directed through labelled paths, this provides low latency low packet loss and low jitter that traditional IP networks. Additionally, the complex manual configurations of LSPs takes significant amounts of time to implement and can make it difficult for large enterprises to quickly scale up the network.

It is worth noting that implementing IPsec over MPLS improves the security of the network and data. IPsec is not a replacement of MPLS. Further, the authentication of peers and data provides the mechanism of identification and verifying the IPsec peers and validating the authenticity of the data send against the one received. The CE routers in the IPsec environment are able to identify and verify their peers. This stops unauthorized network devices from gaining access and guarantees safe transmission of data across the public network. IPsec also protects data from replay attacks. The use of nonse data and time stamps while transmitting IPsec packets protects the data from replay attacks by attackers. In a rapidly evolving technological landscape where data privacy and confidentiality are critical concerns, understanding the benefits of IPsec implementation can empower Zambian enterprises to make informed decisions about their network architecture. This knowledge can help enhance the cybersecurity posture, comply with regulatory requirements and ensure the privacy and integrity of business operations and customer data. Evaluating the benefits of implanting IPsec over MPLS in an enterprise network holds significance as it offers insights into the advantages that organizations can gain by adopting this network security protocol.

The study also observed that while IPsec provides data privacy and security per connection for network traffic crossing the perimeter, the packet size also increases. This is owing to the additional overhead of encryption of IP packets between the Customer Edge routers. With the additional overhead provided by IPsec encryption, performance of

real time applications can be impacted negatively. However, since MPLS provides the efficiency required to route traffic quickly using labels, the application performance with IPsec implemented may be within acceptable levels. This is critical to providing consistent user experience on the network.

5.2 Recommendation

As the demand and complexity of network connectivity increases, the need for integrating and securing several services continues to unfold. Data confidentiality and integrity have now become critical parts of design and implementation for most enterprises using MPLS enabled networks. Additionally, the potential risks associated with Wide Area Networks (WAN) such as Phishing scams, data breaches and increase in cyberattacks have increased the demand for security in data networks. In order to provide data confidentiality and integrity, some Enterprises have combined MPLS technology with different security mechanisms on network infrastructure. It is recommended that in addition to implementing IPsec over MPLS, multiple security strategies should be implemented on the enterprise network. These strategies includes blocking the use of unsecure protocols and only allow the use of secure protocols and applications such as HTTPS and SSH. Additionally, segmenting the network and restricting access to any device that has not been authenticated in large enterprise networks is recommended.

In this study IPsec over MPLS provides security for perimeter devices. This leaves internal systems vulnerable to attacks. It is recommended that dynamic security controls are implemented for internal systems and end devices. This includes continuous verification for users, continuous monitoring of traffic patterns on the network and threat detection. Such measures will reduce the attack surface and improve the security posture of an enterprise network.

5.3 Future research

The error rate on the IPsec capture provides evidence that as the packets become larger than the allowed interface MTU on the router, this causes errors and loss of data. While adjusting the MTU to 1400 avoids dropping packets on the configured internal devices, this does not extend to devices on external networks. Since the internal network administrator lacks control of managing the configurations on the external networks,

default MTU size may exist on the external devices. Therefore, the impact on MPLS and IPsec performance due to MTU adjustment need to be researched further. This provides a basis for future research.

Additionally, according to the Wireshark organization, Encrypted Payloads of IKEv2 packets can be decrypted using this tool if necessary information is provided. In order to decrypt IKEv1 or ESP packets, the Log Filename setting can be used in the ESAKMP and ESP protocols preference respectively. This means that IPsec packets can be vulnerable to an attacker who ease drops on them as they traverse the network. This feature provides an opportunity for future research on the security of packets encrypted using IKEv2. This can include the impact of certificate based authentication on the network performance.

The research has shown that implementing IPsec over MPLS improves the security of the data as it travels through the public network. However, there is need to implement adaptive security models to protect internal network traffic that uses unsecure protocols such as HTTP and TELNET for one reason or another. Future research can focus on evaluating the compatibility and complexity of implementing systems that find and respond to suspicious behavior within the network, while using IPsec over MPLS.

References

[1] The Internet Society, "RFC3031," January 2001. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc3031. [Accessed 25 April 2023].

[2] The Internet Society, "MPLS Label Stack Encoding," January 2001. [Online]. Available: https://www.rfc-editor.org/rfc/rfc3032.html#:~:text=RFC%203032%3A%20MPLS%20Label%20Stack%20Encoding. [Accessed December 2023].

[3] T. I. S. (2006), "RFC4364 -BGP/MPLS IP Virtual Private Networks (VPNs)," February 2006. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4364. [Accessed 20 April 2023].

[4] GIAC Security Essentials Certification (GSEC), "IPSec and MPLS, (Even Better Together)," SANS Institute, Rockville Pike, 2023.

[5] IETF, "IP Security Maintenance and Extensions (ipsecme)," 29 03 2023. [Online]. Available: https://datatracker.ietf.org/wg/ipsecme/about/. [Accessed 16 04 2023].

[6] Cisco Systems, "MPLS History and building blocks," Cisco Systems, 24 July 2020. [Online]. Available: https://learningnetwork.cisco.com/s/article/MPLS-History-and-building-blocks. [Accessed 27 April 2023].

[7] RF & Wireless Vendors and Resources, "Tutorial on MPLS network, MPLS label format," RF Wireless World, 2012. [Online]. Available: https://www.rfwireless-world.com/Tutorials/MPLS-tutorial.html. [Accessed 27 April 2023].

[8] A. A. Mian, S. U. Khalid, "Multi-Protocol Label Switching Traffic Engineering with QoS," Blekinge Institute of Technology, Sweden, 2010.

[9] R. Q. Shawl, R. Thaker, E. Jasvinder Singh, "A Review: Multi Protocol Label Switching (Mpls)," *Internationa Journal of Engineering Research and Applications,* vol. 4, no. 1, pp. 66-70, 2014.

[10] R. Fontaine , C. A. Razafindramonja and L. H. Rabetafika, "Analysis and Evaluation of MPLS Network Perfomance," Scientific Research Publishing, Fianarantsoa, Madagascar.

[11] L. D. Ghein, MPLS Fundamentals, 1897 ed., Indianapolis: Cisco Press, 2006.

[12] Cisco Press, "IPSec Overview Part One: General IPSec Standards," Cisco Systems, 22 February 2002. [Online]. Available: https://www.ciscopress.com/articles/article.asp?p=25470. [Accessed 31 December 2022].

[13] IETF, "IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap," February 2011. [Online]. Available: https://www.rfc-editor.org/rfc/rfc6071.html. [Accessed 17 June 2023].

[14] Cisco Systems, Inc, IPsec Configuration Guide, Cisco IOS XE 16 (Cisco ASR 920 Series), San Jose: Cisco Systems, 2020.

[15] M. Elezi and B. Raufi, "Conception of Virtual Private Networks using IPsec suite of protocols, comparative analysis of distributed database queries using different IPsec modes of encryption," in *World Conference on Technology, Innovation and Entrepreneurship*, Macedonia, 2015.

[16] A. Zola and A. S. Gillis, "Internet Key Exchange (IKE)," Tech Target, February 2022. [Online]. Available: https://www.techtarget.com/searchsecurity/definition/Internet-Key-Exchange#:~:text=This%20is%20required%20for%20the,keys%20during%20an%20IPsec%20session.. [Accessed 18 July 2023].

[17] O. Kim, D. Montgomery, "Behavioral and Performance Characteristics ofIPsec/IKE in Large-Scale VPN," National Institute of Standards and Technology, United States, 2003.

[18] Cisco Systems Press, "IPSec Overview Part Four: Internet Key Exchange (IKE)," *IPsec Overview,* 22 Feebruary 2002.

[19] S. e. al, "Enhancing MPLS Network Security with IPsec Functionality," *Journal of Network Security.*

[20] C. K. Simatimbe and C. S. Dr. Lubobya, "Performance Evaluation of an Internet Protocol Security (IPSec) Based Multiprotocol Label Switching (MPLS) Virtual Private Network," *Journal of Computer and Communications,* vol. 8, pp. 100-108, 2020.

[21] R. Johnson, Williams, G. Thompson, "Scalability and Performance Analysis of MPLS Networks with IPsec.," in *International Conference on Communications and Networking*.

[22] F. Rafamantanantsoa, R. Aubert, R. Haja, , "Analysis and Evaluation of MPLS Network Performance," *Communications and Networks,* vol. 13, no. 1, pp. 25-35, February 2021.

[23] S. Ali and B. Z. Rana, "OPNET Analysis of VoIP over MPLS VPN," Blekinge Institute of Technology, Sweden, 2011.

[24] D. Guernsey, A. Engel, J. Butts, S. Shenoi, "SECURITY ANALYSIS OF THE MPLS," in *International Conference on Critical Infrastructure Protection*, Washingtone DC, 2016.

[25] U. Shah, "Performance Evaluation of MPLS in a Virtualized Service Provider Core (with/without Class of Service)," Rochester Institute of Technology, 2017.

[26] A. Z. Othman, R. A. Rahman, M. M. Md Zan and M. I. Yusof, "The effect of QoS implementation in MPLS network," in *EEE Symposium on Wireless Technology and Applications (ISWTA)*, Bandung, Indonesia, 2012.

[27] O. Elkeelany, M. M. Matalgah, K.P. Sheikh and M. Thaker, "Performance analysis of IPSec protocol: Encryption and authentication," in *2002 IEEE International Conference on Communications.*, New York, 2002.

[28] H. Corporation, "What Is MPLS?," HUAWE Corporation, January 2023. [Online]. Available: https://support.huawei.com/enterprise/en/doc/EDOC1100118961. [Accessed 14 August 2023].

[29] H. Corporation, "NetEngine AR V300R019 CLI-based Configuration Guide - MPLS," HUAWEI Corporation, 2023. [Online]. Available: https://support.huawei.com/enterprise/en/doc/EDOC1100112353/d57213f1/configuring-dynamic-bfd-for-ldp-lsps. [Accessed 15 August 2023].

[30] H. Corporation, "Overview of MPLS TE," HUAWEI Corporation, 2023. [Online]. Available: https://support.huawei.com/enterprise/en/doc/EDOC1100116614/ed998132/overview-of-mpls-te. [Accessed 15 August 2023].

[31] H. Corporation, "CX320 Switch Module V100R001 Command Reference 11," HUAWEI Corporation, 2023. [Online]. Available: https://support.huawei.com/enterprise/en/doc/EDOC1000128405/dcc225a1/vpn-target. [Accessed 15 August 2023].

[32] Cisco Systems, "Cisco 1921 Series Integrated Services Routers Data Sheet," Cisco Systems, 22 August 2017. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/routers/1900-series-integrated-services-routers-isr/data_sheet_c78-598389.html. [Accessed 4 August 2023].

[33] Cisco Systems , "Configuration Register," Cisco Systems, February 2023. [Online]. Available: https://ipcisco.com/lesson/configuration-register/#:~:text=Config%20Register%200x2142,will%20be%20Configuration%20Register%200x2142.. [Accessed 1 August 2023].

[34] Network Academy, "Why do we need IP Subnetting?," Network Academy, 25 March 2023. [Online]. Available: https://www.networkacademy.io/ccna/ip-subnetting/why-do-we-need-ip-subnetting. [Accessed 4 August 2023].

[35] M. Yaibuates, R. Chaisricharoen, "Implementing of IP address Recovery for DHCP Service," *International Journal of Applied Engineering Research,* vol. 13, no. 5, pp. 2659-2662, 2018.

[36] R. Mens, "DHCP Lease Time – What is it and How does it work?," LAZYADMIN, 28 November 2019. [Online]. Available: https://lazyadmin.nl/home-network/dhcp-lease-time/. [Accessed 03 August 2023].

[37] A. Khormali, J. Park, "Domain name system security and privacy: A contemporary survey," *Journal of Information Security and Applications,* vol. 185, no. 107699, 11 February 2021.

[38] Cisco Systems, "Understanding the differences between the Cisco password \ secret Types," Cisco Systems, 26 October 2021. [Online]. Available: https://community.cisco.com/t5/networking-knowledge-base/understanding-the-differences-between-the-cisco-password-secret/ta-p/3163238#:~:text=Type%206%20Passwords-,Type%207,these%20will%20be%20depreciated%20soon.. [Accessed 2 August 2023].

[39] G. T. Point, "An assessment of Gigabit Ethernet technology and its applications at the NASA Glenn Research Center: a case study," *Journal of Engineering and Technology Management,* vol. 20, no. 3, pp. 245-272, September 2003.

[40] B. K. Soorty, S. S. Kolahi, Z. Qu and N. Chand, "Performance Comparison of Category 5e vs. Category 6 Cabling Systems for both IPv4 and IPv6 in Gigabit Ethernet," UNITEC Institute of Technology, New Zealand, 2010.

[41] G. f. Geeks, "Classless Inter Domain Routing (CIDR)," 19 July 2023. [Online]. Available: https://www.geeksforgeeks.org/classless-inter-domain-routing-cidr/. [Accessed 11 August 2023].

[42] Computer Science Department, University of Cape Town, "Routers and routing - Chapter 7. Network Infrastructure," Computer Science Department, University of Cape Town, June 2010. [Online]. Available: https://www.cs.uct.ac.za/mit_notes/web_programming/html/ch07s05.html. [Accessed 11 August 2023].

[43] Solarwinds, "What is an Access Control List?," July 2023. [Online]. Available: https://www.solarwinds.com/resources/it-glossary/access-control-list-acl. [Accessed 11 August 2023].

[44] Cisco Systems, "Configure and Filter IP Access Lists," 7 October 2022. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html#:~:text=There%20is%20an%20implied%20deny,102)%20have%20the%20same%20effect.. [Accessed 11 August 2023].

[45] R. H.-. C. Expert, "Fast Ethernet vs Gigabit Ethernet: Which Data Protocol is Right for You?," CDW Corporation (Nasdaq: CDW) , 9 Aust 2022. [Online]. Available: https://www.cdw.com/content/cdw/en/articles/networking/fast-ethernet-vs-gigabit-ethernet.html. [Accessed 12 August 2023].

[46] Cisco Systems, "Configure Catalyst Switched Port Analyzer (SPAN): Example," 11 July 2023. [Online]. Available: https://www.cisco.com/c/en/us/support/docs/switches/catalyst-6500-series-switches/10570-41.html. [Accessed 29 October 2023].

[47] Wireshark Organization, "Internet Protocol version 4 (IP)," 11 August 2020. [Online]. Available: https://wiki.wireshark.org/Internet_Protocol. [Accessed 25 August 2023].

[48] T. I. Society, Writer, *The Security Flag in the IPv4 Header.* [Performance]. 2003.

[49] IP on WIRE Technogy Landscape, "How to Decode Null Encryption in Wireshark," IP ON WIRE, 2022. [Online]. Available: https://iponwire.com/decode-null-encryption-in-wireshark/. [Accessed 19 September 2023].

[50] Cisco Systems Press, "IPSec Overview Part One: General IPSec Standards," Pearson Education, 22 February 2002. [Online]. Available: https://www.ciscopress.com/articles/article.asp?p=25470&seqNum=9. [Accessed 10 June 2023].

[51] The Internet Society, "Internet Security Association and Key Management Protocol (ISAKMP)," November 1998. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc2408. [Accessed 1 Spetember 2023].

[52] The Internet Society , "Internet Key Exchange (IKEv2) Protocol," December 2005. [Online]. Available: https://datatracker.ietf.org/doc/html/rfc4306. [Accessed 4 Spetember 2023].

[53] A. Loay , S. D. Yehya and M. Joud, "AES Encryption: Study & Evaluation," Rafik Hariri University , 2020.

[54] B. Madhulika, D. Gaurang and J. N. Pro Varshapriva , "Comparative Analysis of Mpls and Non -Mpls Network," *International Journal of Engineering Research and Applications (IJERA) ,* vol. 3, no. 4, pp. 71-76, 2013.

[55] Z. Zhipeng, S. Chandel, S. Jingyao, Yan Shilin, Yu Yunnan and Zang Jingji, "VPN: a Boon or Trap?," in *International Conference on Computing Methodologies and Communication*, Nanjing, China, 2018.

[56] Wireshark Organisation, "Customizing Wireshark," Wireshark, January 2023. [Online]. Available: https://www.wireshark.org/docs/wsug_html_chunked/ChIKEv2DecryptionSection.html. [Accessed 16 April 2023].

[57] O. Kim and D. Montgomery, "Behavioral and Performance Characteristics of IPsec/IKE in Large-Scale VPNs," 2003.

Appendices

Appendix A: Definitions

OSI: The conceptual model that was created by the International Organization for Standardization which enables diverse communication systems to communicate using standard protocols.

Traffic Engineering: The science of managing the flow of traffic flow on the network. It involves studying traffic patterns and developing strategies to improve security and efficiency of traffic flows by understanding flows, bottlenecks and develop solutions to reduce network congestion.

QoS: The use of technologies to control traffic and ensure the performance of critical applications such as real time application with limited network capacity. QoS enables organizations to adjust their overall network traffic by prioritizing specific high-performance applications.

Encapsulation: The process of adding headers and trailers around some data. This includes adding various functionalities and features to the data transmission such as the security and reliability of data transmission between two nodes in a network.

Fragmentation: In computer networks, this refers to the breaking up of a data packet into smaller pieces in order to fit it through a network with a smaller maximum transmission unit (MTU) than the initial packet size.

Nonse data: This is a randomly generated number used only once in cryptographic communication. It is typically used by an authentication protocol to ensure communication that is old cannot be reused in replay attacks.

Packet Length: The length of the entire Internet Protocol packet including the header and data measured in bytes.

Defense in depth: The use of multiple security strategies in the network to provide security and every level of network and application communication. Layers of defense may include Firewalls, Antivirus systems, intrusion detection and response systems that both protect and prevent attacks on the organization's network.

Policy map: Defines the series of functions to be applied to inbound and outbound traffic on the network.

Enterprise network: An enterprise network is the backbone network of the organization that requires advanced and efficient switching and routing devices to transfer business-critical data between servers, applications, desktops, and more. Enterprise networks enable users and systems to connect easily via different connectivity modes such as LAN or cloud.

Network Resources: These are hardware, software and data elements that are connected and configured on the Enterprise network.

Network Traffic types: There are three basic types of network traffic types namely video, voice and data. These are categorized in real time and non-real time traffic. Video and voice normally takes the form or real time traffic.

Transmission Control Protocol (TCP): TCP defines the rules for delivering data over a network. It is connection oriented and non-real time traffic includes but not limited to email and web browsing. It emphasizes reliability of data delivery over speed.

User Datagram Protocol (UDP): UDP is the protocol used to deliver time sensitive traffic over the network. It is a connectionless protocol that emphasizes speed over reliability. UDP is used to deliver real time applications such as gaming, video, voice and Domain Name System (DNS) lookups.

Appendix B- Related Works

TABLE 2.1: RELATED WORKS

Author	**Project Title**	**Summary of Work**	**Tools/ Protocols used**	**Research Gap**
Azhar Ali Mian[1] Sardar Usman Khalid[2]	Multi-Protocol Label Switching Traffic Engineering with QoS	Main aim of the thesis is to discuss Traffic Engineering in accordance with improving Quality of Service (QoS) and to show how MPLS is best suited for resolving existing QoS issues.	MPLS modes and Traffic Engineering.	Persistent challenges affecting the Quality of Service (QoS).
Madhulika Bhandure[1] Gaurang Deshmukh[2] Prof. Varshapriya J N[3]	Comparative Analysis of MPLS and Non-MPLS Network	"MPLS simplifies the network infrastructure by allowing the consolidation of multiple technologies and Applications such as voice, video and data. MPLS provides enhanced security, scalability and high Availability." [54]	GNS3 simulator	Consolidating multiple applications such as video, voice and data and technologies

Conrad K. Simatimbe[1] Smart Charles Lubobya[2]	Performance Evaluation of an Internet Protocol Security (IPsec) Based Multiprotocol Label Switching (MPLS) Virtual Private Network [20]	Evaluating the performance of non-real time and real time applications through and MPLS/IPsec enabled network.	MPLS, IPsec and OPNET Modeler	Real time applications performance on IPsec and MPLS network
GIAC Security Essentials Certification	IPsec and MPLS, (Even Better Together) [4]	The paper show that if the Objective is integrity and confidentiality, IPsec will be the obvious choice, but if the objective is strictly security, MPLS VPNs will meet the customer's needs without introducing	MPLS VPN and IPsec deployed on Cisco IOS devices.	Reducing the complexities of vendor interoperability by providing IPsec on the CE routers at the network's edge while providing a very scalable, manageable and

		Latency associated with IPsec. [4]		affordable IPsec service.
Okhee Kim[1], Doug Montgomery[2]	Behavioral and Performance Characteristics of IPsec/IKE in Large-Scale VPNs [17]	Highlighting the significant performance impact of subtle IPsec/IKE implementation and policy decisions on the overall performance and behavior of TCP based applications in large scale VPNs.	Asymmhost, asymmnet and fullsymm network configuration models	Examine dynamic behavior and relative performance characteristics of large scale VPN environments based upon IPsec and IKE version 1 (version 2 of IKE is currently under development by IETF).
Z. Sun, W. Meng, and L. Song (2007)	Performance Evaluation of IPsec over MPLS for Secure Virtual Private Networks	This study evaluates the performance of IPsec over MPLS in providing secure virtual private networks (VPNs) and compares it with traditional IPsec implementations.	MPLS VPN and IPsec	Focuses on various performance metrics such as throughput, latency, and CPU utilization.

Azeddien M. Sllame (2022)	Performance Evaluation of Multimedia over MPLS VPN and IPsec Networks	Multimedia streaming applications have very strict Transmission requirements.	OPNET Simulation tool, MPLS VPN, OSPF, H.323 and IPsec	Performance of multimedia applications
Shahid Ali[1] Bilal Zahid Rana[2] (2011)	OPNET Analysis of VoIP over MPLS VPN with IP QoS	The study examines the behavior of routing protocols on MPLS VPN when heavy Voice over Internet Protocol is used on the network. The results indicate that when OSPF is used, there's lower delay and has better throughput. However, RIPv2 is lower in performance compared to OSPF. [23]	OSPF RIPv2 OPNET	Analyzing the behavior of OSPF and RIPv2 based MPLSBGP VPN architectures by using intense VoIP traffic
F. Yang, W. Zhang, and Q.	"Performance Evaluation of	This study examines the performance of IPsec over MPLS using different	DES, 3DES and AES	The effects of an encryption algorithm on throughput,

Qi (2012):	IPsec over MPLS with Different Encryption Algorithms"	encryption algorithms, including DES, 3DES, and AES. The research compares the performance in terms of throughput, delay, and CPU utilization under various network conditions.		delay and CPU utilization of network resources
Utkarsh Shah (2017)	Performance Evaluation of MPLS in a Virtualized Service Provider Core (with/without Class of Service) [25]	It was observed through the results that having Quality of Service enabled drops more Packets, however gives the advantage of lower Round Trip Time for in-profile traffic. On the hand, having Quality of Service disabled, permits more traffic but leads to contention between the three traffic classes leading to higher Round-Trip Times. The true benefit of QoS is	Junos OS, VMware Fusion 7, OSPF, Wireshark, Filezilla and Microsoft applications	The main aim of this thesis is to evaluate the performance of voice, data and video traffic in a virtualized service provider core.

		seen in traffic congestion scenarios.		
A. Z. Othman et al (2012)	The effect of QoS implementation in MPLS network	This paper presents the implementation of Quality of Service (QoS) based on the Class Based QoS IP Precedence in MPLS network. ISP test lab has been used to implement QoS in MPLS network. Results obtained can be used by ISPs and Network Administrators in implementing the QoS and can be enhanced further with other type of queuing mechanism.	MPLS	Quality of Service in the Internet Service provider network
O. Elkeelany et al (2002)	Performance analysis of IPSec protocol: encryption and authentication [27]	The study presents performance analysis and comparisons between DES, MD5 and SHA1 terms of time complexity and space complexity, and the parameters considered are processing power	DES, MD5 and SHA1	Time complexity and space complexity of the three algorithms.

		and input size. The analysis results revealed that HMAC-MD5 can be sufficient for the authentication purposes rather than using the more complicated HMAC-SHA1 algorithm.		
Zhipeng, Zhang; Chandel, Sonali; Jingyao, Sun; Yan Shilin; Yu Yunnan; Zang Jingji;	VPN: a Boon or Trap?	The study looks at three types of the most common VPNs and shows a comparative study of their features in terms of performance, security and a few other aspects. The research offers a clear understanding of the users and will help them make decisions which VPN based configuration fits their needs and priority regarding security, speed, and cost. [55]	MPLS, IPsec and SSL	Determining which VPN technology works for user's needs and priorities.

A. M. Al-Emran and M. A. Latiff (2017)	"Performance Evaluation of IPsec over MPLS using Different Tunneling Protocols"	This study assesses the performance of IPsec over MPLS using different tunneling protocols, including Generic Routing Encapsulation (GRE) and Layer 2 Tunneling Protocol (L2TP). The research focuses on various performance metrics, such as throughput, delay, and packet.	GRE and L2TP	Performance of IPsec when using tunneling protocol
Rafamantanantsoa, F., Aubert, R.C. and Haja, R.L. (2021)	Analysis And Evaluation of MPLS Network Performance. Communications and Network, 13, 25-35.	The basic aim of this research is to get the best MPLS network performance towards linux and FreeBSD operating systems.	The study used SCAPY to measure the response times by varying the size of the packets sent and validate the measurements with the MATLAB Simulink.	Addressing complexity of network connectivity and the integration of several services.

	https://doi.org/10.4236/cn.2021.131003			
Daniel Guernsey[1] Aaron Engel[2] Jonathan Butts[3] Sujeet Shenoi[4]	Security analysis of the MPLS label distribution protocol [24]	This paper examines security issues associated with the Label Distribution Protocol (LDP), which is the primary route construction protocol in MPLS networks.	MPLS Label Distribution Protocol (LDP)	Their analysis has identified ten attacks that exploit weaknesses in the LDP specification: six attacks that disrupt service and four that divert traffic from intended routes.
Sahel Ahmad Alouneh	On Fault-tolerance and Security in MPLS networks	Provide fault tolerance and to enhance the security in MPLS networks	Modified (k,n) Threshold Sharing Scheme (TSS)	Addressing fault tolerance and security on MPLS
Mohammad Azmi Ridwan[1] Nurul Asyikin	Recent trends in MPLS networks: technologies,	This study provides a review of MPLS networks and their promising technologies, such as traffic engineering, protection and	MPLS-TE DiffServ MPLS-TP	Proposal to review protocols or designs for MPLS to ensure that it achieves the most efficient and

Mohamedzi[2] Wan Sih Halimatul Munirah Wan Ahmad[3] Fairuz Abdullah[4] Md.Zaini Jamaludin[5]	applications and challenges	restoration, differentiated services, and MPLS-transport profile (MPLS-TP) and its applications.		optimal performance.
Simatimbe, C.K.[1] and Lubobya, S.C[2]	Performance Evaluation of an Internet Protocol Security (IPSec) Based Multiprotocol Label	The study evaluates the performance of Internet Protocol Security (IPSec) Based Multiprotocol Label Switching (MPLS) virtual private network (VPN) in a small to medium sized organization.	OPNET Version 14.5 Simulation software	The MPLS networks ride on the public network backbone that is porous and highly Susceptible to attacks and so the need for reliable security mechanisms to

	Switching (MPLS) Virtual Private Network			be part of the plan for deployment.

Appendix C: MPLS and IPsec Initial Configurations on PEs and CEs

PE1 Configuration

```
sysname LUSAKA-LC1
#
dns resolve
dns server 165.56.45.2
dns server 165.56.45.3
#
router id 10.1.1.1
#
bfd
 mpls-passive
#
mpls lsr-id 10.1.1.1
#
mpls
 label advertise non-null
 mpls te
 mpls rsvp-te
 mpls te cspf
 mpls bfd enable
 mpls bfd-trigger host
 mpls bfd min-tx-interval 50 min-rx-interval 50
```

```
#
mpls l2vpn
#
vsi 931 static
 pwsignal ldp
 mtu 1600
#
mpls ldp
 #
 ipv4-family
#
mpls ldp remote-peer 10.5.5.5
 remote-ip 10.5.5.5
mpls ldp local-lsr-id LoopBack11
#
vlan 603
 description RESEARCH-MENG
#
ip vpn-instance RESEARCH-MENG
 ipv4-family
  route-distinguisher 65111:1
  apply-label per-instance
  vpn-target 65111:10 export-extcommunity
```

```
  vpn-target 65111:10 import-extcommunity
  vpn-target 65300:10 import-extcommunity
#
interface GigabitEthernet0/3/0.603
 vlan-type dot1q 603
 description LINK TO RESEARCH WAN CE1
 ip binding vpn-instance RESEARCH-MENG
 ip address 10.200.200.2 255.255.255.252
 statistic enable
#
bgp 37154
 group RR internal
 peer RR connect-interface LoopBack0
 peer RR bfd min-tx-interval 1000 min-rx-interval 1000
 peer RR bfd enable
 #
 ipv4-family vpn-instance RESEARCH-MENG
  import-route direct
  import-route static
#
ip route-static vpn-instance RESEARCH-MENG 0.0.0.0 0.0.0.0 10.200.200.9 description
HEAD-OFFICE
```

ip route-static vpn-instance RESEARCH-MENG 192.168.200.0 255.255.255.128 10.200.200.1 description RESEARCH-MENG-LAN1

PE2 Configuration

```
sysname LUSAKA-LC2
#
dns resolve
dns server 165.56.45.2
dns server 165.56.45.3
#
router id 10.5.5.5
#
bfd
 mpls-passive
#
mpls lsr-id 10.5.5.5
#
mpls
 label advertise non-null
 mpls te
 mpls rsvp-te
 mpls te cspf
 mpls bfd enable
```

```
 mpls bfd-trigger host
 mpls bfd min-tx-interval 50 min-rx-interval 50
#
mpls l2vpn
#
vsi 931 static
 pwsignal ldp
 mtu 1600
#
mpls ldp
 #
 ipv4-family
#
mpls ldp remote-peer 10.1.1.1
 remote-ip 10.1.1.1
mpls ldp local-lsr-id LoopBack1
#
vlan 603
 description RESEARCH-MENG
#
ip vpn-instance RESEARCH-MENG
 ipv4-family
  route-distinguisher 65111:1
```

```
 apply-label per-instance
 vpn-target 65111:10 export-extcommunity
 vpn-target 65111:10 import-extcommunity
 vpn-target 65300:10 import-extcommunity
#
interface GigabitEthernet0/6/0.603
 vlan-type dot1q 603
 description LINK TO RESEARCH WAN CE2
 ip binding vpn-instance RESEARCH-MENG
 ip address 10.200.200.11 255.255.255.248
 statistic enable
#
bgp 37154
 group RR internal
 peer RR connect-interface LoopBack0
 peer RR bfd min-tx-interval 1000 min-rx-interval 1000
 peer RR bfd enable

#

 ipv4-family vpn-instance RESEARCH-MENG
  import-route direct
  import-route static
```

#

ip route-static vpn-instance RESEARCH-MENG 0.0.0.0 0.0.0.0 10.200.200.9 description HEAD-OFFICE

ip route-static vpn-instance RESEARCH-MENG 10.200.200.8 255.255.255.128 10.200.200.10 description CE2

ip route-static vpn-instance RESEARCH-MENG 192.168.200.128 255.255.255.128 10.200.200.10 description RESEARCH-MENG-LAN2

#

CE1 Configuration

Current configuration : 2570 bytes

!

! Last configuration change at 14:10:32 UTC Wed Aug 9 2023 by admin

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname RT-IPsec-TEST1

!

boot-start-marker

boot-end-marker

!

enable secret 4 41My1ps88G72xo4jABUZJ.JVOv7sqhM.2awwF1n3/sY

```
!
no aaa new-model
!
ip cef
!
ip dhcp excluded-address 192.168.200.1 192.168.200.10
!
ip dhcp pool MPLS_IPsec_Site1
 network 192.168.200.0 255.255.255.128
 domain-name MPLS_IPsec_Site1
 dns-server 192.168.0.10 172.16.120.249
 default-router 192.168.200.1
 lease infinite
!
no ip domain lookup
ip domain name MPLS_IPsec_Site1
ip name-server 8.8.8.8
login delay 10
login on-failure log
login on-success log
no ipv6 cef
multilink bundle-name authenticated
!
```

```
license udi pid CISCO1921/K9 sn FCZ180490SH
!
username admin privilege 15 password 7 122A1C04062B3F57097F2025623B
!
ip ssh version 2
!
interface Loopback0
 ip address 4.4.4.4 255.255.255.255
!
interface Embedded-Service-Engine0/0
 no ip address
 shutdown
!
interface GigabitEthernet0/0
 description LINK TO ISP
 ip address 10.200.200.1 255.255.255.252
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 description LINK TO RESEARCH LAN
 ip address 192.168.200.1 255.255.255.128
 duplex auto
```

```
 speed auto
!
interface GigabitEthernet0/0/0
 no ip address
 duplex auto
 speed auto
!
no ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
ip route 0.0.0.0 0.0.0.0 10.200.200.2
ip route 10.200.200.8 255.255.255.248 10.200.200.2 name CE2-WAN
ip route 192.168.200.128 255.255.255.128 10.200.200.2 name CE2-LAN
!
ip access-list extended CE1-IPSEC
 permit ip 10.200.200.0 0.0.0.7 any
 permit ip 192.168.200.0 0.0.0.127 any
 permit ip 192.168.200.128 0.0.0.127 any
 permit ip any any
!
access-list 100 permit ip 192.168.200.0 0.0.0.127 any
```

```
access-list 100 permit ip 10.200.200.0 0.0.0.7 any
!
control-plane
!
line con 0
 password 7 080A4D4C1E181116405B5D5C6B
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0 4
 password 7 1065081B1216060A5E547B7365
 login local
 transport input all
line vty 5 15
 password 7 132E16101C0D102B7974796B74
 login local
 transport input all
!
```

```
scheduler allocate 20000 1000
!
end
```

CE2 Configuration

```
Current configuration : 1834 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname RT-IPsec-TEST2
!
boot-start-marker
boot-end-marker
!
no aaa new-model
ip cef
!
no ip dhcp use vrf connected
ip dhcp excluded-address 192.168.200.129 192.168.200.140
!
ip dhcp pool MPLS_IPsec_Site2
  network 192.168.200.128 255.255.255.128
  default-router 192.168.200.10
  domain-name MPLS_IPsec_Site2
  dns-server 192.168.0.10 172.16.120.249
  lease infinite
!
multilink bundle-name authenticated
!
archive
```

```
 log config
  hidekeys
!
interface FastEthernet0/0
 description LINK TO ISP
 ip address 10.200.200.10 255.255.255.248
 duplex auto
 speed auto
!
interface FastEthernet0/1
 description LINK TO LAN 2
 ip address 192.168.200.129 255.255.255.128
 duplex auto
 speed auto
!
interface Async0/0/0
 no ip address
 encapsulation slip
!
interface Async0/0/1
 no ip address
 encapsulation slip
!
router bgp 65530
 bgp log-neighbor-changes
 neighbor 10.200.200.11 remote-as 37154
 neighbor 10.200.200.11 password 6 !!!!!!!
 !
 address-family ipv4
```

```
 neighbor 10.200.200.11 activate
 no auto-summary
 no synchronization
 network 10.200.200.8
 network 192.168.200.128
exit-address-family
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 10.200.200.9
ip route 10.200.200.0 255.255.255.248 10.200.200.9 name CE1-WAN
ip route 192.168.200.0 255.255.255.128 10.200.200.9 name CE1-LAN
!
no ip http server
!
ip access-list extended CE2-IPSEC
 permit ip 192.168.200.0 0.0.0.127 any
 permit ip 10.200.200.8 0.0.0.7 any
 permit ip any any
 permit ip 192.168.200.128 0.0.0.127 any
!
!
!
control-plane
!
!
line con 0
 password 7 0724204E59080D0445425A5445
 login
line aux 0
```

line 0/0/0 0/0/1

line vty 0 4

password 7 09674F0B0E040313595C55726A

login

!

scheduler allocate 20000 1000

end

IPsec SETUP

CORE CE

crypto isakmp policy 10

encr aes

hash sha

authentication pre-share

group 2

#

crypto isakmp policy 20

encr aes 256

authentication pre-share

group 2

lifetime 43200

#

crypto isakmp key 6 XLPDXLLfCgsBRSaJAAAM address 192.168.200.1

crypto isakmp key 6 XLPDXLLfCgsBRSaJAAAB address 192.168.200.10

```
crypto isakmp invalid-spi-recovery
crypto isakmp keepalive 10 periodic
#
crypto ipsec transform-set MEng-RESEARCH esp-aes esp-md5-hmac
 mode transport
!
crypto ipsec profile IPsec_over_MPLS
 set security-association lifetime seconds 86400
 set transform-set MEng-RESEARCH
#
interface Tunnel10
 description CE1-TUNNEL-VIA-ZAMTEL
 ip address 172.16.200.1 255.255.255.252
 ip mtu 1400
 tunnel source 10.200.200.9
 tunnel destination 10.200.200.1
#
interface Tunnel10
 description CE2-TUNNEL-VIA-ZAMTEL
 ip address 172.16.200.5 255.255.255.252
 ip mtu 1400
 tunnel source 10.200.200.9
 tunnel destination 10.200.200.10
```

```
#
interface Vlan603
 description LINK TO IPsec OVER MPLS RESEARCH
 ip address 10.200.200.9 255.255.255.248
 ip helper-address 192.168.0.10
 ip helper-address 172.16.130.249
 ip access-group IPsec_over_MPLS in
!
ip access-list extended IPsec_over_MPLS
 permit ip any 172.16.0.0 0.0.255.255
 permit ip any 10.0.0.0 0.255.255.255
 permit ip any 192.168.0.0 0.0.255.255
 permit icmp any any
 permit ip any any
```

Appendix D: Ethical Clearance - DRGS

THE UNIVERSITY OF ZAMBIA

DIRECTORATE OF RESEARCH AND GRADUATE STUDIES

Great East Road Campus | P.O. Box 32379 | Lusaka 10101 | **Tel:** +260-290 258/291 777
Fax: (+260) 211 290 258/253 952 | **Email:** director.drgs@unza.zm | **Website:** www.unza.zm /directorates/drgs

APPROVAL OF STUDY

5th March, 2024

Ms. Jessy Chisenga Mwape
University of Zambia
School of Engineering
LUSAKA

Dear Ms. Mwape

RE: APPROVAL – REQUEST FOR RESEARCH ETHICAL REVIEW WAIVER (JESSY CHISENGA MWAPE - NASREC: 2024-JAN-007)

"PERFORMANCE EVALUTION OF INTERNET PROTOCOL SECURITY OVER MULTIPROTOCOL LABLE SWITICHING (MPLS)"

The University of Zambia Natural and Applied Sciences Research Ethics Committee IRB has approved the study noting that there are no ethical concerns.

On behalf of The University of Zambia Natural and Applied Sciences Research Ethics Committee IRB, we would like to wish you all the success as you carry out your study.

In future ensure that you submit an application for ethical approval early enough.

Yours faithfully,

Dr. E. M. Mwanaumo

CHAIRPERSON
THE UNIVERSITY OF ZAMBIA NATURAL AND APPLIED SCIENCES RESEARCH ETHICS COMMITTEE - IRB

cc: Director, Directorate of Research and Graduate Studies
Assistant Director (Research), Directorate of Research and Graduate Studies
Assistant Registrar (Research), Directorate of Research and Graduate Studies

Towards Improving Service and Excellence in High Education Beyond Fifty Years

Appendix E: Proof of Publication

Transactions on Engineering and Computing Sciences - Vol. 11,

No. 5 Publication Date: October 25, 2023. D

OI:10.14738/tecs.115.15645.

Mwape, J. C., & Lubobya, C. S.Transactions on Engineering and Computing Sciences (2023). Performance Evaluation of IPv4 and IPv6 on IPsec/MPLS Enabled Network: A Case of Zambia, 11(5). 88-100. .

Performance Evaluation of IPv4 and IPv6 on IPsec/MPLS Enabled Network: A Case of Zambia

Jessy Chisenga Mwape

Department of Electrical and Electronics, School of Engineering,
University of Zambia, Lusaka, Zambia

Charles Smart Lubobya

Department of Electrical and Electronics, School of Engineering,
University of Zambia, Lusaka, Zambia

ABSTRACT

This paper explores the performance of IPv4 versus that of IPv6 in an MPLS/IPsec enabled network for real time applications and non-real time applications. Major Internet Service Providers (ISP) in Zambia have implemented MPLS within their core networks in order to provide traffic engineering and Quality of Service and network efficiency, however, MPLS does not encrypt the data as it travels through the network. To mitigate this, customers using the public infrastructure to connect to their remote sites have implemented IPsec. This framework of related protocols protects one or more data flows between network peers; thus, data confidentiality and integrity can be achieved. When MPLS is combined with IPsec both technologies can provide more security for enterprise WAN networks. However, most service providers and ISPs in Zambia and their Enterprise customers have implemented these technologies using Internet Protocol version Four (IPv4). As the number of devices requiring connectivity to the internet and core systems increases exponentially, the limited address space for IPv4 has reached exhaustion. This has prompted the Zambia Information and Communications Technology Authority (ZICTA) which is the statutory body for regulating Information and Communications Technology (ICT) in Zambia to include the development and implementation plan for migration from IPv4 to IPv6 in their 2022

to 2024 strategy. Once implemented, this strategy hopes to increase access and usage of ICT and postal services and increase the internet penetration rate from 60 percent to 70 percent by 2025. Based on Google's statistics, the IPv6 adoption rates for Zambia is still at 0 percent. In order to analyze the penetration rates of IPv4 versus IPv6, a structured questionnaire has been administered on 30 ISP employees and 30 enterprise customer employees to access the use of IPv4 and IPv6 protocols in their MPLS/IPsec networks. The data simulation for Voice over Internet Protocol (VoIP), Video conferencing, and Email was done using Riverbed Modeler simulation software and observe the performance of IPv4 in comparison with IPv6 in terms of jitter, throughput and delay.

Keywords: *Multi-Protocol LS, Internet Protocol Security, Internet Protocol version 4 (IPv4) and version 6 (IPv6), Voice over IP, Video Conferencing, throughput, jitter and delay.*

Services for Science and Education – United Kingdom