DEVELOPMENT OF AN IMPROVED APPLICATION SPECIFIC TUNELLING PROTOCOL SELECTION SCHEME FOR SITE TO SITE VIRTUAL PRIVATE NETWORKS

BY

ALICE OCHANYA LAWRENCE

DEPARTMENT OF COMPUTER ENGINEERING

FACULTY OF ENGINEERING

AHMADU BELLO UNIVERSITY ZARIA

NIGERIA

MARCH, 2019

DEVELOPMENT OF AN IMPROVED APPLICATION SPECIFIC TUNNELLING PROTOCOL SELECTION SCHEME FOR SITE TO SITE VIRTUAL PRIVATE NETWORKS

BY

Alice Ochanya LAWRENCE, PGD (ABU), 2016

P16EGCP8011

A DISSERTATION SUBMITTED TO THE SCHOOL OF POSTGRADUATE STUDIES, AHMADU BELLO UNIVERSITY, ZARIA
IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTER OF SCIENCE (M.Sc) DEGREE IN COMPUTER ENGINEERING

DEPARTMENT OF COMPUTER ENGINEERING
FACULTY OF ENGINEERING
AHMADU BELLO UNIVERSITY, ZARIA
NIGERIA

MARCH, 2019

DECLARATION

I declare that this dissertation titled**:** "**Development of an improved Application Specific Tunnelling Protocol Selection Scheme for Site to Site Virtual Private Networks**" was carried out by me in the Department of Computer Engineering, Ahmadu Bello University, Zaria. The information derived from the literature has been duly acknowledged in the text and a list of references provided. No part of this dissertation was previously presented for another degree or diploma at this or any other institution.

Alice Ochanya LAWRENCE _____ _____

(Student) Signature Date

CERTIFICATION

This dissertation title: "DEVELOPMENT OF AN IMPROVED APPLICATION SPECIFIC TUNNELLING PROTOCOL SELECTION SCHEME FOR SITE TO SITE VIRTUAL PRIVATE NETWORKS" by Alice Ochanya LAWRENCE meets the regulations governing the award of a Master of Science degree (MSc) in Computer Engineering of the Ahmadu Bello University, and is approved for its contribution to knowledge and literary presentation.

Dr. E. A. Adedokun	_____	_____
(Chairman, Supervisory Committee)	(Signature)	Date
Prof. M. B. Mu'azu	_____	_____
(Member, Supervisory Committee)	(Signature)	Date
Prof. M. B. Mu'azu	_____	_____
(Head of Department)	(Signature)	Date
Prof. S. Z. Abubakar	_____	_____
(Dean, School of Postgraduate Studies)	(Signature)	Date

DEDICATION

This dissertation is dedicated to the Almighty God, the Holy Spirit my inspiration, my supervisors and my beloved family.

ACKNOWLEDGEMENT

My immediate and heartfelt gratitude goes to the Almighty God for all He has been to me. I could only imagine what life would have been for me without Him. Lord, I am forever grateful

Next in line of gratitude is my supervisory team, Dr E. A. Adedokun and Prof. M. B. Mu'azu. Words alone are not enough to express my appreciation to them for guiding me through this path from inception to completion. Dr Adedokun's insistence that I take on this research path is worthy of note. Quoting him "Alice, your research is your take home from MSc, go and do it, should you have any difficulty along the way, come back". Never had anyone constructively made me embark on a task I initially loathed like he did. Those lines changed my orientation about the whole research thing and I went straight to the drawing board. True to his words, he had never refused to assist each time I encountered grey areas in the work. What of the numerous calls to know how it was going? OMG! this was too humbling for me to suck in. Sir, may the heavens reward you handsomely because you have not only redefined my perception about the whole MSc research program, but also charted a career path for me which I hitherto have not set. What can I say of Prof. M. B. Mu'azu? His good works speak for him and the records are there for those who care to know more to digest. I am thankful sir for the painstaking effort you took to guide me through this program, it shall remain forever indelible in my heart.

Names are too numerous to mention but worthy of note are the entire lecturers of the Department of Computer Engineering, Ahmadu Bello University, Zaria: Dr. Y A Shaaban, Dr. T. H. Sikiru, Dr. I. J. Umoh, Dr. M. B. Abdulrazaq, Dr. I. A. Bello, Dr Bashir O. Sadiq, Dr. Salawudeen T. A, Mrs Z. M. Abubakar, Dr. (Mrs) B. Yahaya, Mr I Yusuf and these notable persons Engr. Bashir Sani, Unit Head, NIS and Mr Kabiru Abdulazeez. I shall remain thankful for your contributions and encouragement.

Mr Douglas Johnny of the Cisco Academy, Ahmadu Bello University main campus and my colleague, Engr. Ibrahim Ladan, whose office became my second workstation, I remain thankful. I could be charged for oversight should I forget to mention the immense contribution of the Computer Control research group; your input has been indispensable. To all P16, P15 and P17 Computer/Control students, I say thanks a whole lot for your contributions. To my friends Aromsd, Pindar, Roseadah, Raji, Lizzy Nyam, Meena my roommate, thank you all for adding value to my life, I value our friendship.

For those whose names I could not mention, I cannot forget you, the records are there, a proof that we met and you added value to my life remotely and closely.

Finally, I say a "BIG thank you" to my lovely family. In my next life, I would love to be a part of you still. You are the reason I am here today. Lots of love to all of you, you make me proud of you always. Thanks for loving me this much, do not think I deserve it.

Alice Ochanya LAWRENCE

MARCH, 2019

ABSTRACT

This dissertation presents the development of an improved application specific tunnelling protocol selection scheme (iASTPSS) for site-to-site virtual private network (VPN). The aim is to develop an improved tunnelling protocol selection scheme for site to site VPN that is application specific, requiring security, bandwidth, and time sensitivity as a service for applications. ASTPSS has been developed for security, bandwidth, and time sensitive applications, but in the Internet protocol security (IPsec) tunnel which is responsible for providing security as a service to applications, the security algorithms used such as triple data encryption standard (3DES) and message digest 5 (MD5) are vulnerable to a couple of attacks that exposed the network to such attacks. Therefore, iASTPSS was developed to address these attacks through configurations on the tunnel, security algorithms with longer block size and key length namely advanced encryption standard 256 (AES256) and secure hash algorithm 256 (SHA256) that were optimised against these attacks. All software, graphical network simulator3 (GNS3), windows7 operating system (OS), virtual personal computers (VPCs) and Cisco Internetworking operating system (iOS) necessary for the emulation were setup in a virtual network environment running on Ubuntu 14.04 long term space (LTS) as host. Considering security, bandwidth, and time sensitivity as application requirements in a site-to-site VPN testbed, two layer-3 tunnelling protocols that met these requirements, IPsec and generic routing encapsulation (GRE) were deployed on the network developed in GNS3. Network performance was measured using throughput, latency, and round-trip time (RTT) as metrics. In the first stage of development in the IPsec tunnel, using these metrics, a trade-off of network performance for security occurred in iASTPSS in comparison to ASTPSS due to the computational overhead involved in the encryption process of iASTPSS. A second instance of iASTPSS was yet developed for the IPsec tunnel by using open shortest path first (OSPF) routing protocol to improve route convergence time and scale up the network. The effect of using OSPF was seen in the improvement of the network performance in throughput by 1.62% with a corresponding reduction in latency and RTT by 12.58% and 9.25% respectively compared to the first instance of iASTPSS that was configured with RIPv2. Consequently, this made the second instance of iASTPSS also suitable for both bandwidth and time sensitive applications besides security. In the GRE tunnel, iASTPSS outperformed ASTPSS with an improvement in throughput by 10.90%, with a 17.08%, and 66.29% reduction in latency, and RTT respectively.

TABLE OF CONTENTS

TITLE PAGE ……i
DECLARATION..... ii
CERTIFICATION..... iii
DEDICATION..... iv
ACKNOWLEDGEMENT v
ABSTRACT..... vii
TABLE OF CONTENTS viii
LIST OF FIGURES xi
LIST OF TABLES xiii
LIST OF APPENDICES xiv
LIST OF ABBREVIATIONS..... xiv

CHAPTER ONE:**INTRODUCTION**

1.1 Background of Research 1
1.2 Significance of Research..... 3
1.3 Statement of Problem 4
1.4 Aim and Objectives 5
1.5 Scope of Research..... 5

CHAPTER TWO:**LITERATURE REVIEW**

2.1 Introduction..... 7
2.2 Review of Fundamental Concepts 7
2..2.1 Internet protocol addressing..... 7
2.2.1.1 Classes of IP address..... 8
2.2.1.2 Private IP addresses..... 8
2.2.2 Network and networking 9
2.2.2.1 VPN vulnerabilities..... 10
2.2.2.2 Types of VPN 13
2.2.1.3 VPN tunnelling protocols classification 14
2.2.3 Overview of layer 3 tunnelling protocols 15
2.2.4 Access control lists 20
2.2.4.1 Types of access lists..... 21
2.2.5 Routers and routing protocols..... 22

2.2.5.1 Routing protocols 23
2.2.6 Network security 25
2.2.6.1 Data encryption standard 27
2.2.6.2 3DES 28
2.2.6.3 Advanced encryption standard 29
2.2.6.4 Hashing algorithms 30
2.2.7 Network performance metrics 32
2.2.8 Graphical network simulator 33
2.3 Review of Similar Works 34

CHAPTER THREE:MATERIALS AND METHODS

3.1 Introduction 43
3.2 Materials 43
3.2.1 Hardware platform 43
3.2.2 VM workstation pro v12.0.1.3 43
3.2.3 GNS3 software 44
3.2.4 GNS3 VM 44
3.2.5 Windows7 OS 44
3.3 Methods 44
3.3.1 Network topology design and development 46
3.3.2 ASTPS implementation 46
3.3.3 iASTPSS implementation 47
3.3.4 Experimental procedure for ASTPS and iASTPSS 50
3.3.5 Performance validation 52
3.3.5.1 Throughput parameters and conversion 53

CHAPTER FOUR:RESULTS AND DISCUSSIONS

4.1 Introduction 54
4.2 Experimental Outcome 54
4.3 Result Analysis 58
4.4 Performance Comparison and Analysis 62
4.4.1 Result comparison and analysis from the IPsec tunnel 62
4.4.1.1iASTPSS_case1 and ASTPS comparison in terms of throughput from the IPsec Tunnel 62
4.3.1.2 iASTPSS_case1 and ASTPS comparison in terms of latency from the IPsec Tunnel 63
*4.4.1.3 iASTPSS_case1 and ASTPS comparison in terms of RTT from the IPsec tunnel*64
4.4.2 iASTPSS_case1 and iASTPSS_case2 results comparison and analysis 65

4.4.2.1 iASTPSS_case2 and iASTPSS_case1 comparison using throughput 65
4.4.2.2 iASTPSS_case2 and iASTPSS_case1 comparison using latency..... 66
4.4.2.3 Comparison of iASTPSS_case2 and iASTPSS_case1 using RTT 66
4.4.3 Results comparison and analysis from the GRE tunnel..... 67
4.4.3.2 iASTPSS and ASTPS comparison and analysis in terms of latency 68
4.4.3.3 iASTPSS and ASTPS comparison and analysis in terms of RTT..... 69
4.5 Performance Percentage Improvement of iASTPSS over ASTPS..... 70
CHAPTER FIVE:**CONCLUSION AND RECOMMENDATION**
5.1 Summary..... 72
5.2 Conclusion..... 72
5.3 Significant Contributions..... 73
5.4 Recommendations for Further Work..... 73
REFERENCES 74

LIST OF FIGURES

Fig 1.1: Tunnelling Process 2

Fig 2.1: GRE Tunnel Structure 16

Fig 2.2: Generic Routing Encapsulation 17

Fig 2.3: GRE packet forwarding 17

Fig 2.4: Authentication Header 19

Fig 2.5: Encapsulation Security Payload Header and Trailer 19

Fig 2.6: Tunnel mode packet header 20

Fig 2.7: Transport mode packet header 20

Fig 2.8: Overview of Block Cipher Cryptographic Algorithms 26

Fig 3.1: Network Topology 46

Fig 3.2: Snippet of start-up configuration page 51

Fig 4.1: Snippet of captured packets from an IPSec tunnel from the ASTPS network 54

Fig 4.2: Snippet of captured packets from a GRE tunnel of the iASTPSS network 55

Fig 4.3: Snippet of the Wireshark capture from an IPsec tunnel 56

Fig 4.4: Snippet of IPsec tunnel output 57

Fig 4.5: Snippet of the output of a GRE tunnel 58

Fig 4.6: Graph of Throughput against Packet Size for iASTPSS_case1 and ASTPS in the IPsec Tunnel 63

Fig 4.7: Graph of Latency against Packet Size for iASTPSS_case1 and ASTPS through the IPsec Tunnel 63

Fig 4.8: Graphical Output of RTT against Packet Size for iASTPSS_case1 and ASTPS 64

Fig 4.9: Graph of throughput against packet size for iASTPSS_case2 and iASTPSS_case1 65

Fig 4.10: Graph of Latency against Packet Size for iASTPSS_case2 and ASTPSS_case1 66

Fig 4.11: Graph of RTT against Packet Size for iASTPSS_case2 and iASTPSS_case1 67

Fig 4.12: Graphical presentation of RTT against packet size for iASTPSS and ASTPS from the GRE tunnel 68

Fig 4.13: Graph of Latency against Packet Size for iASTPSS and ASTPS in GRE Tunnel 69

Fig 4.14: Graph of RTT against Packet Size for iASTPSS and ASTPS from the GRE Tunnel 70

LIST OF TABLES

Table 2.1 Private IP addresses classification 8

Table 2.2 Feature comparison between DV and LS routing protocol 24

Table 3.1 ASTPS network emulation parameter list 47

Table 3.2 iASTPSS Network Parameter list 50

Table 3.3 Throughput parameter conversion 53

Table 4.1 Results of ASTPS for varying packet sizes for throughput, latency and RTT 59

Table 4.2 Results of iASTPSS_case1 for varying packet sizes showing the throughput latency and RTT from the IPSec tunnel 60

Table 4.3 Results of iASTPSS_case2 for varying packet sizes for throughput, latency and RTT from the IPsec tunnel 60

Table 4.4: Results of ASTPS for throughput, latency and RTT from the GRE tunnel 61

Table 4.5 Results of iASTPSS for throughput, latency and RTT from the GRE tunnel 61

Table 4.6: Percentage Performance Improvement of ASTPS and iASTPSS_case1 70

Table 4.7: Percentage Improvement of iATPSS over ASTPS in the GRE Tunnel 71

Table 4.8: Percentage Improvement of iATPSS_case2 over iASTPSS_case1 in the IPsec Tunnel 71

LIST OF APPENDICES

APPENDIX A: Installation of VMware Workstation Pro 12 78
APPENDIX B: Installing GNS3 on the HP Laptop 79
APPENDIX C: Installing GNS3 VM 80
APPENDIX D: Installing Windows 7 OS 81
APPENDIX E: ASTPS IPsec codes 82
APPENDIX F: ASTPS GRE codes 89
APPENDIX G: iASTPSS IPsec codes varying only security algorithms 95
APPENDIX H: iASTPSS IPsec codes varying security algorithms and routing protocol 102
APPENDIX I: iASTPSS GRE codes 109
APPENDIX J: Experimental procedure for ASTPS and iASTPSS 115
APPENDIX K: Throughput Comparison of iASTPSS_case1 and ASTPS 116
APPENDIX L: Latency Comparison of iASTPSS_case1 and ASTPS 116
APPENDIX M: RTT Comparison for iASTPSS_case1 and ASTPS 117
APPENDIX N: Throughput Comparison of iASTPSS_case2 and iASTPSS_case1 117
APPENDIX O: Comparison of iASTPSS_case1 and iASTPSS_case2 using Latency 118
APPENDIX P: Comparison of iASTPSS_case2 and iASTPSS_case1 using RTT 118
APPENDIX Q: Throughput Comparison for iASTPSS and ASTPS from the GRE Tunnel 119
APPENDIX R: GRE Tunnel Latency Values for iASTPSS and ASTPS 119
APPENDIX S: GRE Tunnel RTT Values for iASTPSS and ASTPS 120

LIST OF ABBREVIATIONS

Acronyms	**Definitions**
AES	Advanced Encryption Standard
AH	Authentication Header

ANSI	American national standard institute
AS	Autonomous System
ATM	Asynchronous Transfer Mode
AU	Active User
BGP	Border Gateway Protocol
CAN	Campus Area Network
CLI	Command Line Interface
DES	Data Encryption Standard
DH	Diffie Helman
DOS	Denial of Service
DV	Distance Vector
EAL	Extended Access List
EGP	Exterior Gateway Protocol
EIGRP	Exterior Internal Gateway Routing Protocol
ESP	Encapsulation Security Payload
FDDI	Fibre Distributed Data Interface
FIPS	Federal Information Processing Standards
GF	Galois Field
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
HDLC	High-Level Data Link Control
HTTPS	Hypertext Transfer Protocol Security
IANA	Internet Assigned Numbers Authority
IBM	International Business Machine
ICMP	Internet Control Message Protocol
IETF	Internet engineering task force
IGP	Interior Gateway Protocol
IGRP	Interior Gateway Routing Protocol
IKE	Internet Key Exchange
IOS	Internetworking Operating System
IP	Internet Protocol
IPSec	Internet Protocol Security
ISAKMP	Internet Security Association Key Management Protocol
ISDN	Integrated Services Digital Network

LAPB	Link Access Procedure Balanced
LS	Link State
LTS	Long Term Space
MAN	Metropolitan Area Network
MD5	Message Digest5
MIM	Man in the Middle
MPLS	Multi-Protocol Label Switch
MTU	Maximum Transfer Unit
NAT	Network Address Translation
NIC	Network Interface Card
NIST	National Institute of Standards Technology
OVA	Open Virtualization Application
OSPF	Open Shortest Path First
QEMU	Quick Emulator
QOS	Quality of Service
RFC	Request for Comment
RIP	Routing Information Protocol
RTT	Round Trip Time
SA	Security Association
SAL	Standard Access List
SHA	Secure Hash Algorithm
SLA	Service Level Agreement
SSL	Secure Socket Layer
TLS	Transport Layer Security
UDP	User Datagram Protocol
VLSM	Variable Length Subnet Mask
VPC	Virtual Personal Computer
VPN	Virtual Private Network
VPDN	Virtual Private Dial-in Network
VIRL	Virtual Internet Routing

CHAPTER ONE

INTRODUCTION

1.1 Background of Research

Virtual private networks (VPN) is a private but virtual network created in a public network. It allows the creation of private networks in a public network such as the Internet enabling privacy and tunnelling of Internet protocol (IP) and non IP networks (Shrivastava & Rizvi, 2014). The Internet is not secured to guarantee safety of data transmitted across it from source to destination for participating networks. This is because no layer provides security by default for transmitted packets, except with the intervention of an Internet service provider (ISP) through the provision of dedicated or leased lines. Obtaining security through the use of these lines comes at a throat-cutting price to organizations. VPN offers this security at a minimal cost through the use of VPN tunnelling protocols. Tunnelling, as seen in Fig: 1.1 relates to the process of wrapping data payload with the header information of a protocol, passing it through a tunnel across the network from source to destination. It involves data encapsulation, data transfer, and data de-encapsulation. VPNs are used daily to give remote users and branch offices secured connectivity over the Internet through to the corporate headquarters instead of using leased or permanent lines. Security services offered by VPN are confidentiality, authenticity, and data integrity to ensure transmitted data protection against interception by unauthorised persons (Ismoyo & Wardhani, 2016).

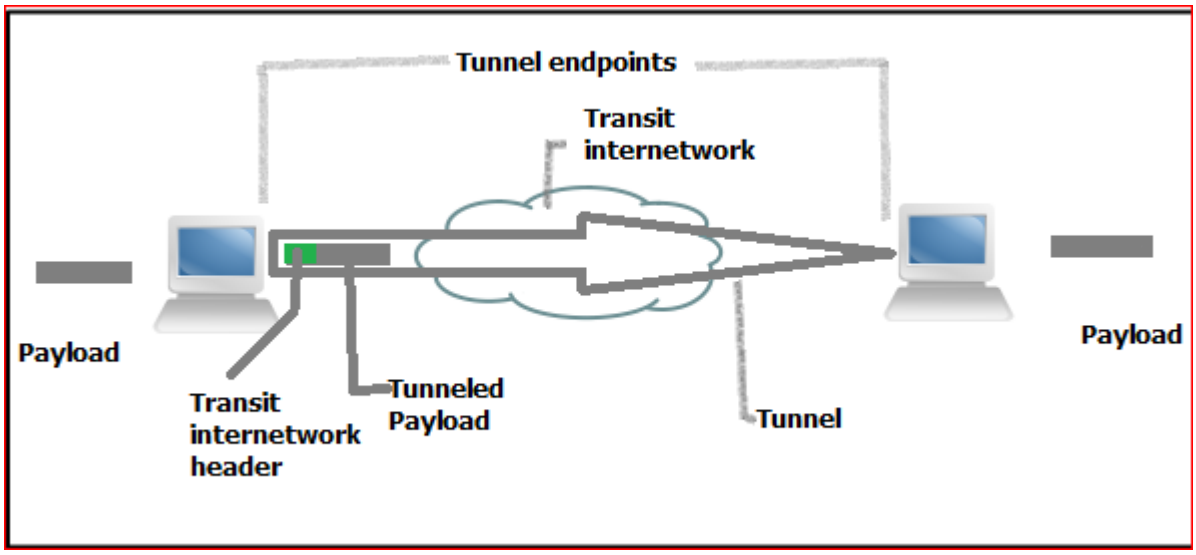


Fig 1.1: Tunnelling Process (Degefa, 2015)

The process as seen in Fig: 1.1 shows a data payload that is encapsulated at the source end and passed through the tunnel to the destination end, where the data payload is de-encapsulated to retrieve the payload. The payload at the source end is wrapped with an extra header which is the protocol information of the tunnelling protocol used (Degefa, 2015).

The virtual concept in VPN is due to the fact that the physical infrastructure of the network is transparent to the VPN user, though, not owned by the VPN user. It is also private due to the privacy (advanced encryption and authentication) of the traffic that flows through the VPN, and finally it is a network that has no physical network infrastructure, it exists as part of an existing network (Elezi & Raufi, 2015).

Overtime, VPN tunnelling protocols are deployed based on the technology involved and the area of deployment. Some tunnelling protocols are an alternative to others such as transport layer security (TLS) and secure socket layer (SSL), while, some are used in

conjunction with one another. Examples of protocols used in conjunction with one another are layer two tunnelling protocol over Internet protocol security (L2TP/IPsec) or point to point tunnelling protocol over Internet protocol security (PPTP/IPsec). Based on this, tunnelling protocols such as IPSec, generic routing encapsulation (GRE), multi-protocol label switch (MPLS) are mostly used for site to site VPN. PPTP, L2TP/IPsec, SSL on the other hand are used for remote access VPN (Lammle, 2013).

Most recently, there is a paradigm shift in the deployment of tunnelling protocols according to technology involved or areas of deployment as research has begun advocating for the deployment of VPN technologies based on organizational needs or application requirements (Jahan *et al.*, 2017). This advocacy is timely as deploying VPN technology based on application requirements or organizational needs would not only reduce network overhead in terms of management cost but it would also improve network performance in terms of latency and throughput. (Jahan *et al.*, 2017).

1.2 Significance of Research

VPN provides a cost effective, secure and scalable platform for connecting branch offices to the head office or a remote user to the enterprise network through the Internet compared to leased or dedicated lines issued by ISPs. This is because VPN leverages on the existing physical network infrastructure to achieve security and scalability at a minimal cost with high security. The major reason for deploying VPN on a network, aside cost saving, is the security.

However, the deployment of VPN on a network is achieved through some tunnelling technologies which should be done in compliance with organizational needs or application requirements (Jahan *et al.*, 2017). Beyond this, it is also necessary to ensure

that a trade-off is maintained between performance, security and the chosen protocol. This could be achieved by using protocols that complement the operation of each other since a weakness in a protocol could be a strength in another. Previous researches on VPN tunnelling protocols were based on the following (Jahan *et al.*, 2017):

a) areas of deployment (either site to site or remote access) and

b) VPN classification (secured or trusted, Layer 2 and Layer 3)

Meanwhile, not much attention has been paid to the deployment of these technologies based on specific application requirements or organizational needs. Taking cognisance of the fact that security is the main thrust of VPN, this research took a step further on application specific tunnelling protocol selection scheme (ASTPSS) by Jahan *et al*., (2017) by strengthening the security algorithm with the aim of further strengthening the tunnel against possible forms of unauthorised access on the network. This is to meet the security as a service need of applications. In the final analysis, an improved ASTPSS (iASTPSS) for site to site VPN that provides security, bandwidth, and time sensitivity as requirements for applications with appreciable throughput, latency and RTT values on the IPsec and GRE tunnels was developed.

1.3 Statement of Problem

VPN is deployed in networks basically for the benefits it renders such as security, scalability and cost saving. In fact, security is the major goal of VPN deployment in networks. Security vulnerabilities are the major problems associated with VPN. These vulnerabilities arose mostly from the encryption and hashing algorithms used in the VPN. Encryption and hashing algorithms with shorter key lengths and block sizes are known to be vulnerable to certain forms of attacks. In addition, it reduces attack complexity. Using security algorithms with longer key length and block sizes mitigates these vulnerabilities

with an increase attack complexity. Also, earlier practice of VPN deployment based on the technology involved or area of deployment instead of deployment according to application needs introduces vulnerabilities in the network especially where the deployed tunnelling protocols are not compatible in operation. As a result, research is now advocating VPN deployment based on application requirements (Jahan *et al.*, 2017). Deploying a VPN technology without reference to organizational needs or applications requirements would, beside creating extra vulnerability in the network, also increase network overhead in terms of management cost. As a result, it is expedient to deploy VPN technologies based on application requirements and draw a line between application requirements and technology to be deployed while placing high premium on security.

1.4 Aim and Objectives

The aim of this research is to develop an improved application specific tunnelling protocol selection scheme for site-to-site VPN

The objectives are:

a) To emulate the network environment on a virtual machine necessary for the implementation of application specific tunnelling protocol selection scheme (ASTPSS) by Jahan *et al*., (2017)
b) To develop an improved ASTPSS based on a) called iASTPSS
c) To perform a comparison of iASTPSS and ASTPSS using throughput, latency and round trip time (RTT) as metrics.

1.5 Scope of Research

The scope of the research are as follows:

a) It is limited to ASTPSS for site to site VPN that requires security, bandwidth and time sensitivity as application requirements using IPsec and GRE with the network topology set up in a virtual environment in GNS3.
b) Network performance is measured using throughput, latency, and RTT as metrics.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This section presents the review of fundamental concepts relevant to this work and previous works relevant to the research. These aid the understanding of some important principles, tools, and approaches used in those researches before this one. Such understanding contributed significantly to the selection of the right tools to achieve better results.

2.2 Review of Fundamental Concepts

This section reviews concepts that are fundamental to the research such as IP addressing, network types, VPN classification, access control list, network security and network simulators. These gave a better insight into the research thus helping to validate each claim made.

2..2.1 Internet protocol addressing

An IP address is a numeric identifier assigned to each machine on an IP network. It showed the specific location of a device on the network. An IP address is a logical address, not a physical address which is used for locating hosts on a network (Lammle, 2004). IP addressing is created to allow a host on one network to communicate with a host on another network irrespective of the LAN the hosts are participating in. An IP address has 32-bits divided into four octets (four sets of eight binary digits). An IP address is either public or private. The only difference between the two addresses being that, while the public IP addresses are routable through the Internet, the private IP addresses are not routable through the Internet except with the use of network address translation (NAT).

The private IP address scheme was developed to cater to the fast depletion of the public IP addresses (Lammle, 2004).

2.2.1.1 Classes of IP address

Five classes of IP addresses (A-E) exists. Classes A-C are assigned to governments, companies, schools and public entities, class D for multicast and E for experimentation. The IP address classes and ranges are set by the Internet assigned numbers authority (IANA) (Lammle, 2004). A consideration of the private IP addressing scheme was made as it relates to this research. Table 2.1 presented a summary of private addressing scheme classifications as was set by the IANA.

2.2.1.2. Private IP addresses

Private addresses are for internal use in organizations. These addresses are used on a private network, but they are not routable through the Internet except when a network address translator (NAT) is used. Request for comment (RFC) 1918 defined these addresses and respective range for classes A, B, and C. This is designed for the sole aim of creating a degree of desired security and also conveniently saves valuable IP address space. By using private IP addresses, ISPs, corporations, and home users only need a relatively small group of public IP addresses to connect their networks to the Internet.

Table 2.1: Private IP Address Classification (Lammle, 2004)

SN	Address class	Reserved address space
1	**Class A**	10.0.0.0 through 10.255.255.255
2	**Class B**	172.16.0.0 through 172.31.255.255
3	**Class C**	192.168.0.0 through 192.168.255.255

If these private address ranges are used for an internal network, they are not routable on the Internet. This is fine for most organizations because they have one or more gateway

devices (such as routers, firewalls, or proxy servers) that provide connectivity to the Internet. These gateway devices have network interface connections to both the internal network and the Internet and route packets between them (thereby providing Internet connectivity to internal clients). The company simply obtains one or more official IP addresses if it chooses to provide services (like an organizational website) to people using the Internet.

2.2.2 Network and networking

A network is defined as the configuration of two or more networking devices such as computers, routers, and switches over a communication medium for the purpose of sharing information (Donahue, 2007). Networking is simply the art of manipulating these communication devices to perform the task of reception or/and transmission of information in the form of voice or data from source to destination.

There are many types of networks: wide area networks (WANs), local area networks (LANs), VPNs, metropolitan area networks (MANs), campus area networks (CANs). A discussion of the first three was made as they are within the scope of this work. The fundamental differences among them are distance or area of coverage, transmission speed, media and error rate (Lammle, 2011).

A WAN links two or more distant LAN using routers and ISP. Examples are frame relay, asynchronous transfer mode (ATM), integrated services digital network (ISDN), link access procedure balanced (LAPB), high-level data-link control (HDLC) and point-to-point protocol (PPP) - these are all WAN protocols with several connection types such as leased lines, circuit switching and packet switching (Lammle, 2011). A LAN is a network linking two or more computers located within the same geographical location such as an office building. They are typically high-speed, low-error rate networks within an office.

Examples are Ethernet, fibre distributed data interface (FDDI), token ring, etc. (Lammle, 2011). VPN is a private (secure) network in a public (insecure) network infrastructure. It is simply a private network that is integrated into a public network (Shrivastava & Rizvi, 2014). VPN provides a platform for the transmission of secure and private information over unsecure network such as the Internet and/or over shared infrastructure. The concept, virtual in VPN implies that the network bandwidth and the capacity of the physical infrastructure are transparent to the VPN user and this is made possible through tunnelling techniques employed at the upper layers. By transparency, it implies the physical network infrastructure such as the network's bandwidth and the capacity are available to VPN user. The insecure network in most cases, if not all, is owned by an ISP (Elezi & Raufi, 2015). VPN has the following benefits: security, scalability (expandability and flexibility in case of new users), manageability, and cost saving in comparison to dedicated and leased lines (Lu & Dong, 2011).

As part of its security capability, VPN provides privacy of transmitted packets through encryption to prevent possible forms of unauthorised access; authentication, that is, verification that packet came from valid user; provision of data integrity through hashing to ensure data integrity while on transit and anti-replay protection such that packets are not captured and retransmitted by unauthorised users. However, there are certain vulnerabilities associated with the VPN (and this is the point of interest for this research). The following section highlights some of the known vulnerabilities in VPN.

2.2.2.1 VPN vulnerabilities

Although, security is the main benefit of VPN, yet, the basic vulnerabilities of VPN are security based and they range from VPN hijacking, man in the middle (MIM) attack, denial of service (DoS) attack to brute force attack. This is made possible through the use of encryption algorithms with short key lengths and block sizes, weak authentication of

valid users, viruses and malwares, interoperability issues that arise out of non-compatibility of tunnelling technologies deployed with each other, vulnerabilities on the client machine through exposure of logging details when a user on a VPN network accesses the Internet exposing the private network where an attacker could have access if security algorithms used on such VPN network are weak (Gokulakrishnan & Bai, 2014). Besides, a client's system could also be compromised through espionage**.** These vulnerabilities are discussed in the following lines:

a) **VPN hijacking:** It is a targeted attack that uses heartbled to hijack active VPN sessions. This is a common attack in remote access VPN, where active user (AU) session tokens are stolen and used to bypass the organization's multifactor authentication and VPN client software used to validate the authenticity of systems connected to the network resources. It leverages on vulnerability in the user's system to hijack the network. The attacker exploits the security vulnerability in the protocol used by tuning the client's VPN concentrator to remotely access active sessions. This attack is common in SSL VPN. The attacker repeatedly send malformed heartbled request to the hypertext transfer protocol security (HTTPS) web server running on the VPN device which was compiled with a vulnerable version of OpenSSL running in the client's SSL VPN concentrator to remotely access active session tokens for currently authenticated users (Mimoso, 2014) .

b) Denial of service (DoS) attack: In a DoS attack, an attacker attempts to prevent legitimate users from accessing information or services on a network. DoS lowers anonymity as messages need to get retransmitted and delivered, thus presenting more opportunities for attack. The attack can be protocol or infrastructure based. Infrastructure based attacks are again of two types, which are bandwidth attack

and resource depletion attack. Traditional DoS attacks are flooding based attacks which fill the network with the unwanted messages or packets. The attacks directed at network infrastructure can have a serious impact on the overall operation of the Internet and hence the VPN (Monika, 2013).

c) **Man-in-the middle (MIM) attack** in VPN is an attack on the IPSec protocol parameters such as the encryption and the Diffie-Helman (DH) key. The DH key exchange, for instance, allows the exchange of a secret key over a public channel, thereby gaining privacy no matter the type of listener on this DH key exchange. The DH key exchange guarantees privacy, that is, there is no third party involved in the conversation. However, this public channel used for the DH key exchange could be manipulated. This is because, DH does not address how to authenticate the other party, to ensure the conversation is not with a MIM and hence it is a vulnerability (Wouters & Bantoft, 2006). Encryption algorithms like triple data encryption standard (3DES) can be broken using MIM attack (Vennela *et al.*, 2018). In summary, MIM attack is a form of eavesdropping where the attacker inserts himself in the middle of a conversation, masquerading as a wireless access point, router, proxy server, and so on.

d) **Brute force attack** is a password or key search attack on the encryption and hash keys on the IPSec protocol. In VPN, ciphers with shorter key lengths like data encryption standard (DES), 3DES, message digest 5 (MD5) can be broken using this attack (Dev,2013; Barker *et al.,* 2017). A brute-force attack involves trying every possible key until an intelligible translation of the cipher-text into plaintext is obtained. On the average, half of all possible keys must be tried to achieve success (Stallings, 2017). Overcoming this attack is made possible using ciphers with longer key length and block size (García, 2015).

There are several types of VPN as discussed in section 2.2.1.2.

2.2.2.2 Types of VPN

There are two basic types of VPN namely site to site and remote access VPN.

a) **Site to site VPN** otherwise known as branch office to head office VPN occurs between two branches of an organization and allows both to communicate securely over encrypted channels in a public network infrastructure such as the Internet (Elezi & Raufi, 2015)**.** It provides network services to more hosts on a network and the connections are permanent. It is a network to network type of connection. In other words, it is a LAN to LAN network.

b) **Remote access (client-server VPN)** is created between a remote user (home user or the salesman on the field) and the corporate office. This enables the remote user to have access to the enterprise' network while away from the head or corporate office. It is established from a client machine to an enterprise' network, created and destroyed on demand and is created per time, that is, for the time the user requires the connections (Lakbabi *et al.*, 2012). It is also called virtual private dial-in network (VPDN), a dial-in type of network that connects a remote user to the LAN connection. A company with multiple sales persons at the field who needs access to files and other information on the organization's network server over secure, private and encrypted channels using a third-party service provider network employs such remote access VPN (Krithikaa *et al.*, 2016).

The choice of either of these is dependent on the need to be met and this in turn determine the choice of tunnelling protocol to be considered for deployment.

2.2.1.3 VPN tunnelling protocols classification

VPN tunnelling protocols can be classified according to their areas of operation in the open system interconnect (OSI) or transport control protocol/Internet protocol (TCP/IP) model giving birth to the following (Elezi & Raufi, 2015):

a) Layers 2 tunnelling protocols: layer 2 forwarding (L2F), PPTP, L2TP

b) Layer 3 tunnelling protocols: GRE, IPSec, MPLS, L2TPv3

c) Layer 4 tunnelling protocols: SSL, TLS

Implementation of any of these protocols should be based on organizational need or application requirement. These needs could range from security, scalability to management cost but in all cases, a trade-off must be maintained between a desired need and performance while placing a high premium on security. Note that, the implementation does not in any way change the physical infrastructure of the backbone network, that is, the public network infrastructure in which the VPN is created since it is virtual, rather it achieves these needs at a least cost compared to dedicated or leased lines (Lu & Dong, 2011).

Beside implementing protocols based on organizational needs or application requirements, it is also advisable to implement at the layers considered vulnerable because of their proximity to the physical layer. By implication, implementing VPN tunnelling protocols at the data link and Internet layers is a better practice than implementing them at layers above these two layers because it provides security for layers above data link and Internet layers **(**Haidar & Houseni, 2016**).** Considering layer 3 tunnelling protocols as a layer of interest, section 2.2.2 would be of great help to understanding these protocols and the principle behind their operation.

2.2.3 Overview of layer 3 tunnelling protocols

Layer 3 tunnelling protocols are GRE, IPSec, MPLS and L2TPv3. MPLS is used for large networks especially when scalability is a pre-requisite on a network but the deployment is complex (Jahan *et al.*, 2017). L2TPv3 is an upgraded version of L2TP (Elezi & Raufi, 2015)

a) **GRE:** request for comment (RFC) 2784 described GRE as a communication protocol that establishes a direct point to point connection between network gateways. Using a public network like the Internet, it allows two end devices or network peers to directly share data in an efficient and simple way. It can encapsulate multicast stream of data for Internet transmissions and it has the advantage of connecting non-contiguous subnets, less resource consumption, supports broadcast, unicast, and multicast messages, and can encapsulate any layer 3 protocol and non IP protocols (Bensalah *et al.*, 2017). Its major drawback is security because, unlike IPSec, it lacks the security properties of encryption and authentication (Jahan *et al.*, 2017).

GRE is used when IP and non-IP traffic such as Novell IPX or Appletalk that are not routable over an IP network needs to be transported over a public IP network. This is done by creating a virtual point to point link between such networks over the public IP network as shown in Fig: 2.1. GRE has these basic features, a protocol field that allows the passage of any layer 3 protocol, it is stateless having no flow control, offers no security, and in some cases adds an extra overhead of 24 bytes for tunnelled packets. It also supports a header for each of the following (Lammle, 2013):

i) Passenger or encapsulation protocols like Internet protocol version4 (IPV4) and Internet protocol version6 (IPV6). It allows IPv6 packets to be routed over IPv4 network or links such similar networks over an infrastructure that uses different IP addressing

ii) Transport delivery protocol that is IP based

iii) GRE encapsulation protocol

iv) Encrypt multicast traffic such that multicast packets are encapsulated within the GRE tunnel and then routed over a VPN tunnel and eventually by IPsec if need be (Bensalah *et al.*, 2017)

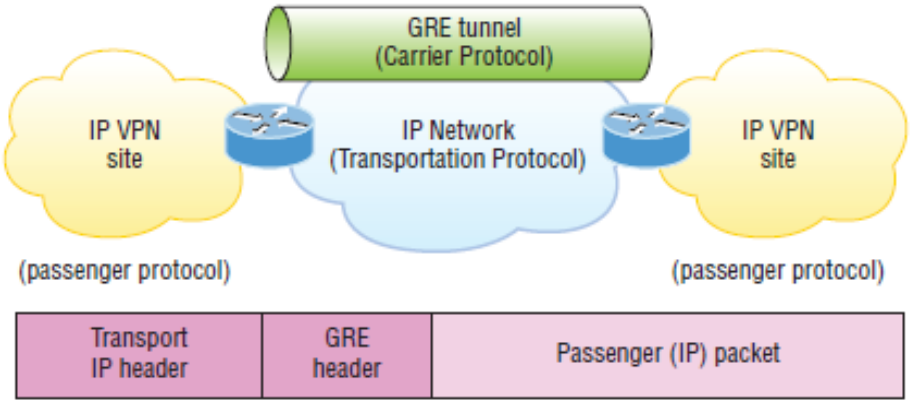


Fig. 2.1: GRE Tunnel Structure (Lammle, 2013)

Fig. 2.1 shows a GRE tunnel structure that consists of three main parts, the passenger protocol carrying the IP header, the transportation protocol which is the network and the carrier protocol which is the GRE tunnel. In Summary, the GRE structure consists of transport IP header, GRE header, and the passenger IP packet.

For instance, when encapsulating protocol A over protocol B, as shown in Fig 2.2 and Fig 2.3, it takes a packet in format A and assumes it to be the payload packet. It firstly encapsulates this in a GRE packet and then encapsulates the GRE packet in protocol B which is the delivery protocol. Request for comment (RFC) 2890 extends the GRE header to allow multiplexing several packet flows within a GRE tunnel with in-order delivery packets enabling GRE to encapsulate point-to-point protocol (PPP) (Alshalan *et al.*, 2016).

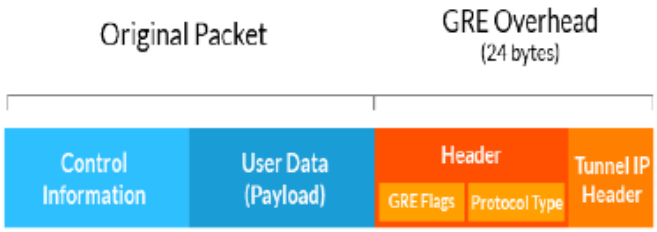


Fig. 2.2: Generic Routing Encapsulation (Bensalah *et al.*, 2017)

Fig. 2.2 shows the encapsulation of a GRE protocol. It is made up of two component parts, the original packet (which is made up of the control information and the payload, that is, the user data) and the GRE overhead which is 24 bytes. It consists of a header (the GRE flags and protocol type) and the tunnel IP header.

While Fig. 2.2 shows the GRE encapsulation, Fig. 2.3 shows how packet forwarding is done in a GRE tunnel. This happens between the ingress and the egress interface of the tunnel. Using a router as interface between these two, the original IP payload (ingress) going in through the tunnel source is routed through the router to the egress interface where the payload is encapsulated with a GRE header as shown in Fig.2.3. This saves time and network resources.

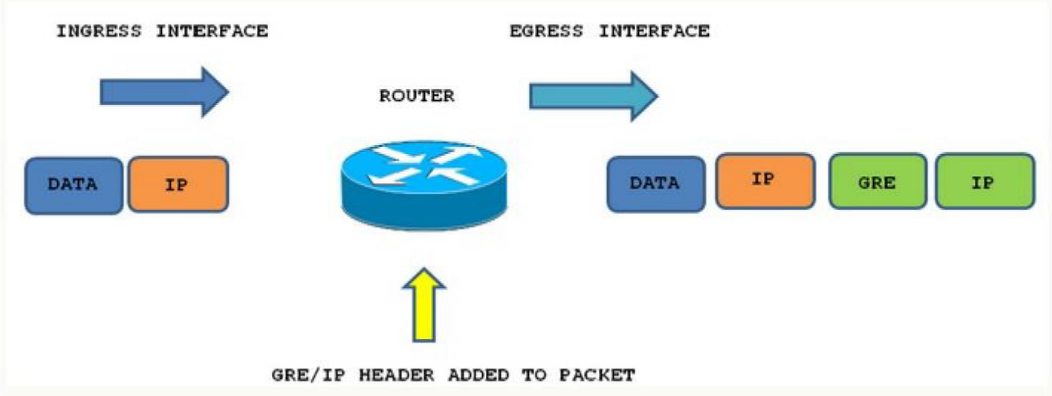


Fig 2.3: GRE Packet Forwarding (Bensalah *et al.*, 2017)

b) **IPSec** is a protocol suite developed by the Internet engineering task force (IETF) and defined by a series of RFCs: 1825, 1826 and 1827 respectively. These RFCs

defined the overall structure of the IPSec protocol. It is referred to as a protocol suite because aside the core protocols of encapsulation security payload (ESP) and authentication header (AH), it provides services such as security associations (SA), Internet key exchange (IKE) otherwise known as Internet security association key management protocol (ISAKMP).

ESP provides data integrity, confidentiality and authentication while AH provides only data integrity and authentication without confidentiality making ESP a better choice for optimized security over AH but, the two cannot be used simultaneously on the same network. IPSec operates at the network layer of the OSI stack or the Internet layer of the TCP/IP model. It has the following features: anti-replay protection through the assignment of sequence numbers to packets, provision of access control, data origin authentication, network-level peer authentication, confidentiality, limited traffic flow since it supports only unicast traffic and, connectionless integrity (Narayan *et al.,* 2015)**.** It is also interoperable with other protocols because it allows the optional usage of its components such that one could choose from a list of options depending on organizational requirements or application needs (Elezi & Raufi, 2015).

i) **AH**: Fig. 2.4 shows the structure of AH. As earlier said, AH only provides data integrity and authentication without confidentiality. Unlike ESP that does not authenticate the preceding IP header before the ESP header, AH authenticates the entire datagram as shown in Fig. 2.4 (Alshalan *et al.*, 2016). AH also provides anti-replay like ESP through the use of sequence numbers.

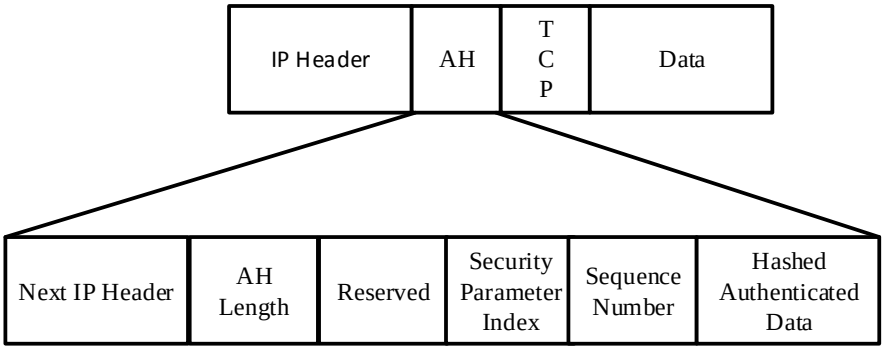


Fig 2.4: Authentication Header (Alshalan *et al.*, 2016)

ii) The ESP header is presented in Fig 2.5. ESP does not authenticate the IP header before the ESP header. It only acts on the data that need protection between the ESP head and the trailer. ESP provides data confidentiality unlike AH and anti-replay properties (Alshalan *et al.*, 2016). ESP allows the implementation of either encryption or authentication only option (Narayan *et al.*, 2015).

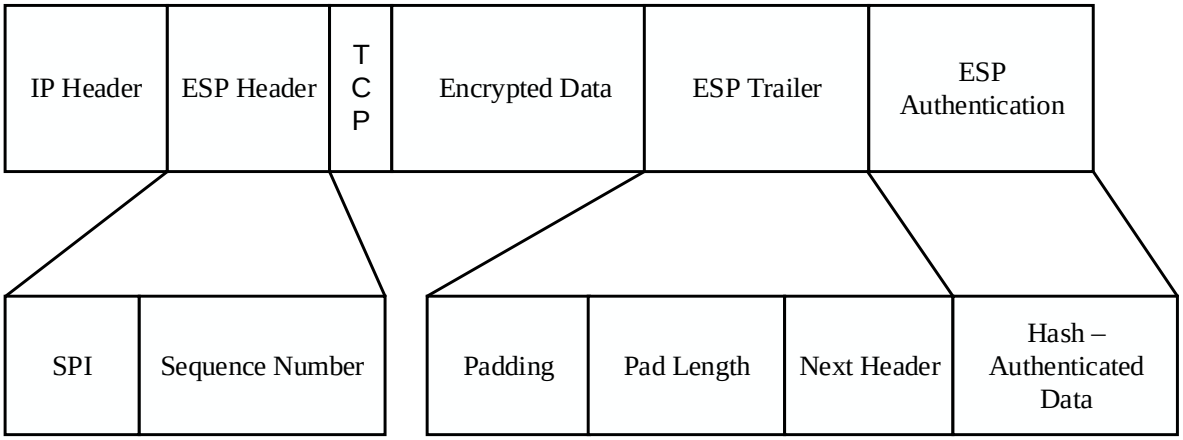


Fig. 2.5: ESP Header and Trailer (Alshalan *et al.*, 2016)

IPSec operates in two modes, tunnel and transport modes. In tunnel mode, as seen in Fig 2.6, the entire IP packet, that is, the header and the payload are encrypted and then encapsulated within a new IP header, thus creating a new IP packet header. This is implemented between network to network and it is the default mode in which IPSec operates (Bensalah *et al.*, 2017). Fig 2.6 shows the tunnel mode packet header. Here, the

entire network layer IP payload is encapsulated with either authentication header or encapsulation security payload before a new IP header is created (Jahan *et al.*, 2017)

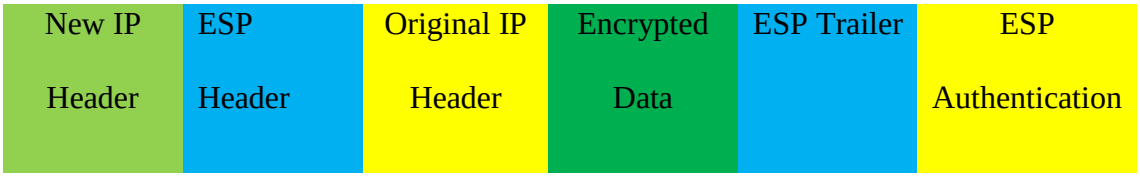


Fig 2.6: Tunnel Mode Packet Header (Bensalah *et al.*, 2017)

Fig 2.7 shows the transport mode packet header. In this mode, only the payload is encapsulated, preserving the IP packet header to allow for seamless routing operation. This mode is implemented between two end devices, that is, between two hosts. (Bensalah *et al.*, 2017). The transport mode operates at the transport layer, it encapsulates the transport layer payload, protecting only the original payload but does not provide any protection for the IP header (Jahan *et al.*, 2017)

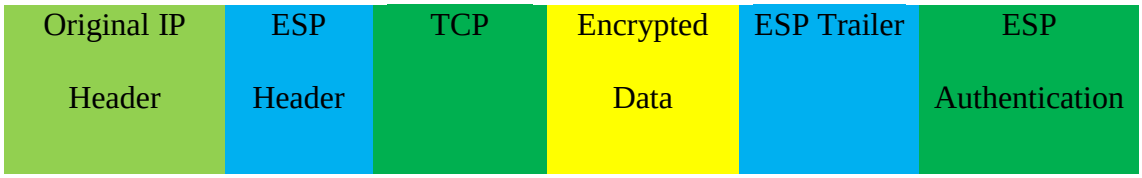


Fig 2.7: Transport Mode Packet Format (Bensalah *et al.*, 2017)

c) **Internet key exchange** (IKE) otherwise known as ISAKMP is a protocol that defines the security parameters, the negotiation keys and the management of IPSec communication. It negotiates IPSec connection settings and validates end points (Alshalan *et al.*, 2016).

2.2.4 Access control lists

An access list is a form of security implemented on a network. It is used to filter out unwanted packets when security policies are implemented. Access list helps to regulate the flow of packets through the network by use of rules, like in programming, where a set of if-else statements are used. It is an ordered list, an error in a preceding stage affects all other stages and the implementation must follow a particular order. An access list is a

series of rules that instruct the router on how to select or match a route or packet (Boney, 2005). It is used for controlling traffic that flows through an interface. Each rule in a standard access list contains three important parts: a number that identifies the list when it is referred to in other parts of the router's configuration, a deny or permit statement, and an address that identifies the packets (Boney, 2005)

There are three important rules that a packet follows when it is being compared with an access list. These guide the operation of access control lists (Boney, 2005).

a) The packet is always compared with each line of the access list in sequential order and always starts with the first line of the access list, move on to line 2, then line 3, and so on.
b) The packet is compared with lines of the access list until a match is made. Once it matches the condition on a line of the access list, the packet is acted upon and no further comparisons take place.
c) There is an implicit "deny" at the end of each access list. This means that if a packet does not match the condition on any of the lines in the access list, the packet is discarded.

2.2.4.1 Types of access lists

There are basically two types of access lists, standard and extended access control lists. While standard access list works at layer 3 of the OSI or TCP/IP model, extended access list works at both layers 3 and 4 of the OSI or TCP/IP model, that is, the network and transport layers respectively (Boney, 2005).

a) **Standard access list (SAL):** It uses only the source IP address in an IP packet as the condition test. All decisions are made based on the source IP address. This means that standard access lists basically permit or deny an entire suite of protocols. They do not distinguish between any of the many types of IP traffic

such as web, telnet, user datagram protocol (UDP), and so on. The number range for standard access list is 1-99 or in the expanded range of 1300–1999.

An example of the syntax is as follows:

<access-list> number <1-99 > action <deny/permit> source <source ip>

b) **Extended access list (EAL):** It can evaluate many of the other fields in the layer 3 and layer 4 headers of an IP packet. They can evaluate source and destination IP addresses, the protocol field in the network layer header, and the port number at the transport layer header. This gives extended access lists the ability to make much more detailed decisions when controlling traffic.

An example of the EAL syntax is:

Access-list <number 100-199> <permit/deny> <protocol> <source><source mask> <operator source port> <destination> <destination mask> <operator destination port> <optional -args> as an example consider: access-list 101 permit icmp 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255.

This rule is simply asking the router to permit Internet control message protocol (ICMP) packets from the source IP on 192.168.20.0/24 through the destination IP of 192.168.10.0/24. The number range for extended access-list is 100-199, and the expanded form is from 2000–2699 (Lammle, 2013). The network in this research would employ the use of the extended access list for packet filtering, network access and application restriction on tunnels.

2.2.5 Routers and routing protocols

Routers are network devices that operate at the network layer or Internet layer of the OSI or TCP/IP model. They are used for connecting two or more networks, routing data packets from source to destination, and fragmentation of packets when maximum transfer unit (MTU) is exceeded. They serve three primary purposes. First, they route network

traffic based on predetermined rules or routing information in routing tables. Second, they segment frames for transmission between LANs. For example, they can frame 10-Mbps Ethernet LAN frames for transmission on a 16-Mbps token ring LAN or a frame relay connection WAN. Third, routers provide the ability to deny or block unauthorized traffic. This can be accomplished through filtering commands that limit certain protocols (that is, http, ftp) or by employing access lists that control the IP addresses that are allowed through (Canavan, 2001).

2.2.5.1 Routing protocols

Routing protocols are functionally classified into two, interior gateway protocol (IGP) and exterior gateway protocol (EGP) (Boney, 2005).

a) IGPs are used on routers within the same autonomous systems (AS), administrative domain or the same intranet. AS is a collection of routers under the control of one organization, for example, one corporation's network. Within this organization, the routers share routing information only among themselves (Boney, 2005). Examples of IGP are routing information protocol (RIP), interior gateway routing protocol (IGRP), enhanced interior gateway routing protocol (EIGRP) and open shortest path first (OSPF). These are configured and designed to handle routing on a small scale unlike EGP which handles much complex networks.

   IGPs are further classified into two classes based on the way they handle routing decisions and the kind of information they share. These are distance-vector (DV) and link-state (LS) routing protocols.

   i) Distance vector (DV) protocols provides two pieces of information for every route, a distance (metric) and a vector. This information is distributed as part

of a network map to all other routes. The “distance” is some measurement of the route's quality based on parameters such as bandwidth, delay, or the number of intervening routers and is not related to the actual physical distance between routers. The “vector” is the IP address of the router to which the packet must be delivered and is called the next hop. The “metric” is simply the number of hops (that is, number of routers) between the current router and the destination. Examples of DV routing protocols are RIP, RIPv2, EIGRP, and IGRP (Boney, 2005).

ii) Link state (LS) protocols build photographs of the network topology on each router. This topology of the surrounding network is then distributed to all other routers and allow all the routers to build a snapshot of the entire network. This allows each router to compute the best path to any destination at any time. OSPF is an example of LS routing protocol (Boney, 2005).

Table 2.2 presents a feature summary of DV and LS routing protocols.

Table 2.2: Features Comparison between DV and LS Routing Protocols (Boney, 2005):

SN	Features	RIP	RIPv2	IGRP	EIGRP	OSPF
1	**VLSM Support**	No	Yes	No	Yes	Yes
2	**Convergence**	Slow	Slow	Medium	Fast	Fast
3	**Configuration**	Easy	Easy	Medium	Medium	Hard
4	**Bandwidth Use**	High	High	High	Low	Low
5	**Scalability**	Poor	Poor	Good	Good	Good
6	**Interoperability**	Yes	Yes	No	No	Yes

b) EGPs are used to route traffic between routers in different AS, for example, between ISPs or between a single corporate network and two or more ISPs. It could also be used on a single large network that is so widely distributed that it cannot be managed as a single unit. For example, a corporate network that spans several continents. Border gateway protocol (BGP) is an example of EGP. EGPs

handle more routing information and perform better route summarization at the same time, thus making them more complex than IGP (Boney, 2005).

2.2.6 Network security

In plain terms, network security means securing a network through encryption and authentication to prevent unauthorised access. By popular demand, every network is expected to be secured against any possible form of unauthorised access both on the network's hardware and software resources. Several approaches are available in achieving security on a network. A combination of security algorithms with varying key lengths could be deployed based on the level of security desired. Cryptographic algorithms are classified as symmetric and asymmetric ciphers. Symmetric ciphers use the same key for encryption and decryption and this key must be shared between communicating peers before the commencement of communication. Common examples of these are data encryption standard (DES), triple DES (3DES) advanced encryption standard (AES), blowfish fish (BF), twofish, RC4, RC6, CAST. Asymmetric encryption uses one key for encryption called the public key and another for decryption called the private key. The key need not get shared before the commencement of communication. Some examples of this are RSA, digital signatures and Diffie-Helman. Asymmetric encryptions are much slower than symmetric encryption because they use more computational powers (Shanta, 2012; Yassein *et al.*, 2017).

The security focus in this work is on symmetric encryption since asymmetric encryption does not scale well with IPsec tunnelling protocol. It leads to increase overhead in respect of the key negotiation time as it involves the use of different keys for encryption and decryption (Shanta, 2012). For this reason, only symmetric encryption is so far used in IPSec.

In symmetric encryption, the key length matters, as shorter key lengths reduce attack complexity for an attacker. Thus, the strength of the encryption depends on the key length and not on the algorithm used. Ciphers with key lengths less than 128 bits such as DES, RC2, RC6, 3DES (assumed to have a key length of 112 bits yet the block size is 64 bits) are considered weak for a network needing security as a service. But, AES, having a 128-bits block size uses various key combinations of 128, 192 and 256 bit keys with 10, 12, and 14 rounds of iterations, respectively to deliver the cipher text or receive the plain text and is considered strong over the other (Singh & Kinger, 2013). A summary of a cryptographic scheme is presented in Fig 2.8. It presents a simple classification of cryptographic algorithms, narrowing it down to block ciphers which are the focus of this work.

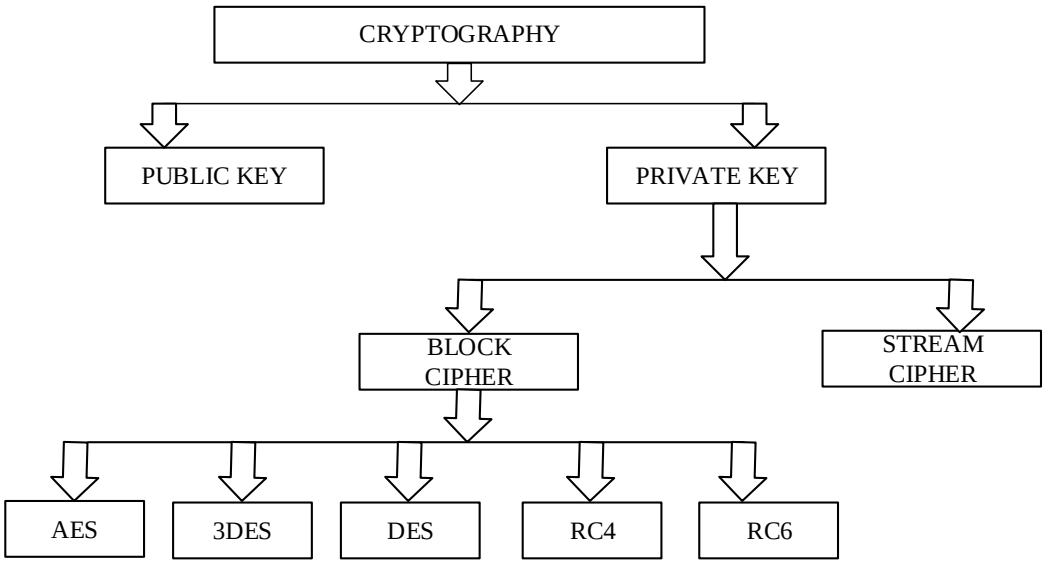


Fig. 2.8: Overview of Block Cipher Cryptographic Algorithms

Only DES, 3DES, and AES are discussed as they fall within the scope of this work.

2.2.6.1 Data encryption standard

Data encryption standard (DES) is a block cipher of 64-bits block size, 56-bits key size encryption algorithm defined and endorsed officially by the US government in 1977 as a standard. The American national standards institute (ANSI) also adopted it as US national standard. It uses a 16-round Fiestal ladder with a 64-bits block size to encrypt 64-bit plaintext as input to output a 64-bits key cipher text. These keys consist of 56-distinct key bits that determines the cryptographic transform precisely and an 8-parity bits for error detection. This 8-bits have no effect whatsoever on the encryption and decryption processes. There are six main operations that could be either permutation or substitution, that are used in the key expansion and the cipher. Both permutations and substitutions are performed in one round of DES algorithm. The decryption is similar to the encryption process just that the keys are applied in the reverse order.

The strength of an encryption is directly proportional to a power of the key length and block size. This algorithm is considered weak due to its short key length of 56-bits and 64-bits block size making several key search attacks against it possible. As a result, it has been recommended that its usage be discontinued (Shanta, 2012). DES requires about 2^56 steps to break by brute force attack. Using a single core processor of 2GHz carrying one test per cycle, it takes at most two years to crack but with the increasing computational powers of systems, this would take a few hours to break. In 1999, distributed .net and the electronic frontier foundation (EFF) jointly and openly broke a DES key in 22hrs, 15mins by brute force attack (Wahid *et al.*, 2018)**.** The computational powers of computers these days have gone higher than it was in 1999 and would take less than that now to break

2.2.6.2 3DES

3DES is a clever way of reusing DES. It is believed to be practically more secure than DES but insecure in theory. It was developed to replace DES without a new algorithm or crypto system. It simply encrypts the original DES three times. It uses three options in the key selection namely:

i) Using 3-mutually independent keys such that K1≠K2≠K3

ii) Use 2-mutually independent keys such that K1≠K2 and K3=K1 and lastly,

iii) Use 3-mutually dependent keys such that K1=K2=K3 (Wahid *et al.*, 2018**;** Yassein *et al.*, 2017).

3DES takes a 64-bit data block, which is the same as that of DES, encrypt, decrypt and encrypt it using 56bits key lengths as the 8-bits are ignored just as in the case of DES. In summary, DES is encrypted with key 1 (K1), decrypted with key 2 (K2) and encrypted again with key 3 (K3) (Singh & Supriya, 2013). Although separate keys were used to encrypt, decrypt, and encrypt the DES algorithm to secure it, the key strength does not yield 168bits (56*3 ≠ 168 but 112 bits). The decryption follows the reverse, encrypt with K3, decrypt with K2, and finally encrypt with K1.

However, even with the improvement on DES through 3DES, the encryption is vulnerable to some form of attacks such as brute force, sweet32 birthday, MIM and other related keys attacks. The security of 3DES, for instance, is affected by the number of blocks processed with one key bundle. 3DES processes data using 2^32 (2^64/2) data block within one data bundle and this exposes the cipher text to collision due to the large size of the data. Standard practice is, to avoid collision, one key must not be used to encrypt more than 2^20 in 64-bits data block. The failure of 3DES to adopt this practice enables an attacker to take advantage of the collisions to carry out attacks on the key.

Using the birthday attack, for instance, researchers discovered that in using 3DES to encrypt data across a HTTPS connection, an attacker executing a sweet32 birthday attack could retrieve the plaintext in the form of cookies by capturing about 785GB data between the server and client if the connection is alive for up to two days and with that have access to the content without authorization. The trade-offs in using 3DES to secure a network are too obvious to be ignored. As a result of these vulnerabilities, 3DES' usage for providing security as a service has been recommended by NIST, IBM, IETF to be discontinued in VPN, Kerberos and others and has thus been advised to be replaced with AES (Barker *et al*., 2017; Kaduk & Short, 2018; Vennela *et al*., 2018). 3DES works better in hardware than in software implementations (Patil *et al.*, 2016).

2.2.6.3 Advanced encryption standard

AES was adopted in 2001 as a federal information processing standards (FIPS) for use in the US federal administration. AES is an iterative, 128-bits block size algorithm that performs encryption and decryption using fixed key sizes of 128, 192, and 256 bits key lengths of 10, 12, and 14 rounds respectively. Each iteration is referred to as a round and the round number is varied depending on the data and key length (García, 2015). The incoming data is stored in a matrix form called the state matrix, all operation are performed over this matrix. Byte substitution, shift row, mix column, and add round key transformations are the major activities performed in one round. For instance, in byte substitution, the matrix state is replaced with a substitution table element that is calculated with a non-linear transform in the Galois field (GF).

In shift row, rows of the matrix are shifted to the right cyclically, mix column transform acts independently on every column of the matrix, add round key operation uses a bitwise

EX-OR on the matrix. All these occur in one round making AES a very secure encryption algorithm over other block ciphers. Advanced encryption standard (AES) is currently the most used algorithm for securing a network as it is harder to break than DES and 3DES. Aside using variable key lengths, it has a higher degree of randomness in output information which helps in increasing the complexity of a successful attack on its keys. The complexity of breaking a cipher key increases exponentially with the key size (Patil et al., 2016; Sivakumar et al., 2018).

According to Sachin and Kumar (2010)**,** using brute force attack on DES, 3DES and AES with 64-bits key length in each case, it took 60789.12s, 98294.54s, and 554277.87s to break DES, 3DES and AES of same key lengths respectively. It would require a lot of years for computers to attain the computational power required to achieve a brute force attack in an acceptable time for a network secured with AES as seen from the results and as confirmed by García (2015). According to Wahid *et al.* (2018), it is therefore right to say that if confidentiality and integrity are a major requirements on a network as in this research AES is the answer. Aside having a block size of 128-bits and variable key lengths offering a better security than most symmetric algorithms, it has been recommended by NIST, IETF, and IBM to replace DES and 3DES (Shanta, 2012; Barker *et al*., 2017; Kaduk & Short, 2018; Vennela *et al*., 2018).

Presently, no security flaws have been identified with the use of AES and it is good for both hardware and software implementations (Patil *et al.*, 2016).

2.2.6.4 Hashing algorithms

Hash algorithms are used alongside encryption algorithms on networks that require maximal security such as in IPsec configuration. Hash functions are used to map data of arbitrary length to a data of fixed length called the digest. They are used majorly for

message integrity preservation, that is, to establish that the intended message has not been tampered with, for password verification and digital finger printing amongst others. There are basically two types of hash algorithms, message digest (MD) and secure hash algorithm (SHA) (Dev, 2013). These are discussed as follows:

a) **MD** is a cryptographic hash function that contains a string of digits created by a one-way hashing formula designed to protect data integrity. The most recently used of the MD family tree is the MD5 which was created to replace MD4 in 1991 after MD4 was broken. MD5 is a 128-bit hash value of 512-bit block size cryptographic hash function. It was soon found vulnerable to collision resistance attack as Wang *et al.* (2004) performed the first successful collision attack on MD5. In 2013, Xie *et al.* (2013) performed the same collision resistance in about 2^18 seconds. MD5 aside the collision attack is also found to be vulnerable to birthday and brute force attacks (Dev, 2013). Collision simply means having two different messages hashing to the same digest. MD5's use in cryptographic hash function has since been discouraged due to its inability to resist collision attacks. The presence of this collision enabled Sotirov *et al.* (2008) to develop a rogue CA certificate that enabled them to impersonate any website that uses HTTPS. Similarly, the flame malware also leveraged on this vulnerability to fake a Microsoft digital signature to enable its installation as a legal code. A recommended replacement for it are SHA-2 and SHA-3 (Shuai *et al.*, 2014)**.**

b) **SHA**: The SHA series also began with SHA-0 to SHA-3. SHA-0 and SHA-1 like MD5 have been found vulnerable to collision attack as well (Stevens *et al.*, 2017). SHA-2 and SHA-3 are the two hash algorithms currently in use. There is currently no successful attack against SHA-2 since it was published in 2001 although efforts are underway by hackers to achieve this through the pre-image resistance attack,

which has not yet been proven to able to attack the hash function. SHA-3, published in 2015, is not known to be vulnerable to any attack yet (Eichlseder *et al.*, 2014). Google announced on February 23, 2017 that SHA-1 be replaced with SHA2 or SHA-3 as a result of SHA-1's vulnerability to collision attacks. Same with Microsoft, Apple, and Mozilla who also proposed the stoppage of SHA-1 by 2017 on their browsers. SHA-2 has 64 to 80 rounds of iterations with digest size of 224, 256, 384, and 512 bits respectively. (Gupta & Kumar, 2014) www.security.googleblog.com. The complexity of finding a collision with SHA-2 is about 10^ (76) steps and this is practically impossible (Soliman *et al.*, 2017).

2.2.7 Network performance metrics

Network performance metrics are quantifiable measures by which the performance of a network could be evaluated. Briefly discussed hereunder are network performance metrics that are directly employed in this work.

a) **Throughput:** This is the rate of successful packet delivery per seconds over a communication medium. It is measured in bits per seconds (b/s)

It is calculated as:

$$Tr = \frac{\mathrm{Ws}}{\mathrm{L}} \tag{2.1}$$

where Tr is throughput measured in b/s

Ws is window size measured in bits and

L is latency measured in milliseconds (ms)

A conversion to seconds of the variable, latency, which is measured in milliseconds (ms) was done to obtain the unit of throughput is measured in b/s.

b) **Latency** is the time that elapsed in packet delivery as it traverses from source to destination over a communication medium. It is measured in milliseconds (ms). (Lammle, 2013).

c) **Round trip time (RTT):** is the time taken for the packet to traverse from the source to destination and back to the source measured in milliseconds (ms) (Jahan *et al.*, 2017).

2.2.8 Graphical network simulator

Building labs with physical hardware or time rental on a rack for the purpose of simulatinga network are not pocket-friendly and inconvenient most times necessitating the use of simulation software which are not only convenient but also inexpensive. They allow the virtualization of a network, obtaining the same output like as if the physical hardware was used, thus saving overhead on time and finances. A range of network simulation software abound and the choice of any is based on desired performance, compatibility, availability, flexibility, and scalability of the software. Software simulators such as Routersim and Boson Netsim are not as good as they are thought to be because they are not only limited in applications, but they, also, merely simulate the commands of cisco IOS rather than emulate them and they are not open source software as well. Cisco virtual Internet routing lab (VIRL) is another network simulation software but it is not an open source software as it requires an annual fee, has limited number of objects to use in the lab, and uses only simulated cisco OS. Cisco education is another platform that offers a pocket friendly virtualised rental rack but it is cisco proprietary that allows one to practice on only specific preconfigured network configurations (Neumann, 2015). Others are network simulator2 (NS2), an open source network simulator but with limited graphical user interface (GUI), hard to use, and does not scale well. Same with its upgraded version NS3, though it has a better GUI than NS2 (Kabir *et al.*, 2014).

GNS3 on the other hand was designed to overcome all the limitations of these network simulators. It has the characteristics of scalability, compatibility, emulates hardware, and

possess the ability to allow resource sharing across multiple computers. Not only does it allow one to create a virtualized network lab with a variety of networking devices, it also uses a backend hypervisor application to emulate the hardware that runs cisco IOS (Neumann, 2015).

GNS3 is a graphical network simulator that allows the emulation of complex networks. Just like Vmware and Vbox that are used in emulating various operating systems in a virtual environment thus allowing one to run operating systems such as Windows 7, Windows XP Professional or Ubuntu Linux in a virtual environment on a computer, GNS3 allows the same type of emulation using Cisco Internetwork operating systems (IOS). It allows a Cisco IOS to run in a virtual environment on a computer. It is a graphical front end to a product called Dynagen. Dynamips is the core program that allows IOS emulation. Dynagen runs on top of Dynamips to create a more user friendly, text-based environment. A user may create network topologies using simple Windows in-type files with Dynagen running on top of Dynamips. All the configuration commands and output are from a real IOS, and theoretically, any protocols or features that an IOS version supports are available to use in a network designs. In addition to Cisco IOS, GNS3 can integrate quick emulator (QEMU) and VMware, VirtualBox virtual machines running operating systems such as Linux, BSD, or Windows (Singh *et al.,* 2016)

2.3 Review of Similar Works

Several researches by different authors on VPN have been conducted but research based on tunnelling protocol selection based on application requirements is still at infancy (Jahan *et al.*, 2017). A review of related literatures is hereby presented.

Akinola and Zhang (2012) carried out a technical report on the performance of IPSec and GRE VPN tunnelling protocols in the light of their security versus performance

properties using Jperf software to measure the network performance and wireshark to analyse the bandwidth and jitter in a lab setting. Both TCP and UDP traffics were sent in both instances of GRE and IPSEc tunnels and the results from these were analysed using wireshark. Bandwidth and jitter were the network performance metrics used in both network cases. Although the report concluded IPSec had a better security over GRE, it did not relate this report in the context of either site to site or remote access VPN neither were these protocols chosen based on application requirements. The routing protocol used, EIGRP is Cisco proprietary and is not inter-operable with other vendors.

Dhall *et al.* (2012) wrote on the implementation of the IPSec protocol dwelling so much on the benefits, architecture, roadmap of the protocol, giving a general overview of the protocol and the implementation of the protocol suite in host, that was the device where the packet was originating and in routers. They went further to identify the various types of host and router implementation rounding it up with the working principle of the protocol. An algorithm was proposed for secure data communication in ad-hoc network combining both AH and ESP. The proposed algorithm was just an attempt to secure data communication as stated by the authors in their conclusion and not meant for implementation in the context of any VPN technology or application. Besides, the simulated result should have compared to practical output rather than a theoretical one since the implementation was not emulated. This work was too open-ended as one would need to further establish claims using an emulator or lab environment.

Lakbabi *et al.* (2012) compared two VPN tunnelling protocols, SSL and IPSec with respect to their security and management capabilities, baring the security and flexibility that both protocols offer to enable network security managers chose between either protocol. The work highlighted the features of each in terms of their respective properties

relating to security and implementation flexibility. Much as this was commendable, it went without saying still that SSL, a transport layer security could not offer a better security and QoS over IPSec as proposed by the authors.

Mao *et al.* (2012) analysed and presented two VPN tunnelling protocols in terms of their application scope, complexity, security with the strengths, and weakness of each. The work stated that SSL VPN could be used for such applications as email, filesharing and web applications while IPSec could be used for all application types. It established the security of IPSec over SSL, though with a higher installation complexity over SSL. In terms of network expansion when newer clients were added to the network, SSL scaled faster than IPSec but in site to site implementations IPSec was a better choice than SSL, thus establishing the choice of IPSec VPN as a better choice over SSL VPN for site to site VPN applications.

Fcmi and Hadi (2013) highlighted the impact of using security protocols on dedicated networks and Virtual Private Networks using OPNET 14.0. L2TP, PPTP and IPSec VPN tunnelling protocols were used as testbed protocol samples for these measurements. Five sites spread across different geographical location but connected to the head office was the research space. FTP, email, video, database, HTTP and voice were applications to be considered in the two network scenarios and the performance of these would be measured in terms of traffic sent and received, the response time in secs, e-mail and file transfer upload and download response time, jitter and Mean Opinion Score (MOS). ATM leased line was used in the dedicated private network while in the VPN setting, nine workstations connected through ethernet protocols, five 16-ports switches, five site routers and one ethernet server were used. Based on graphical results presented for both networks, it was

left to the reader's discretion to make a choice of protocol and network. However, even though this research was conducted in the context of 5-sites to site networks, the security algorithms used in the IPSec protocol suite is weak and vulnerable and could expose data to unauthorized access. 3DES, MD5 and AH are weak and susceptible to bruteforce and collision attacks respectively (Barker *et al.*, 2017; Stallings, 2017). Besides, the AH protocol used only provides data authentication and integrity without any form of confidentiality. (Bensalah *et al.*, 2017)

Chawla. *et al.* (2014) presented a study on IPSec and SSL VPN as tunnelling protocols that could be used in connecting remote users. The architecture of each protocol, merits and demerits and cases for real time applications was presented. Using a feature comparison table for both protocols, a highlight of each protocol's features was made. It concluded by recommending SSL VPN for site to site VPN applications for the mere fact that it does not require a VPN client installation. This recommendation is flawed as SSL VPN is browser dependent that supports only web based applications that requires the installation of a java or ActiveX based agent in the remote asset to mitigate this challenge which is an added overhead in terms of installation cost. Besides, SSL unlike IPSec provides access to only specific applications on a networks and that is a limitation as all packets must get protected at the network layer where IPSec operates before it moves to the transport layer where SSL works (Chawla *et al.*, 2014; Haidar & Houseni, 2016).

Gokulakrishnan and Bai (2014) the authors presented an overview of VPN security, dwelling on the usage of VPN for the provision of security in networks as well as threats and vulnerabilities in VPN and how to mitigate such. Specific VPN protocols, IPSec, L2TP and PPTP were then discussed in the light of their individual features and

functionalities. This presentation is rather too generic than specific as it is conducted with no bearing to an application testbed or requirements.

Shrivastava and Rizvi (2014) presented an analysis of two physical layer protocols, L2TP and PPTP, one network layer protocol, IPSec and SSL, a transport layer protocol in the light of their principles of operation, feature comparison, strengths and weaknesses and presented it as a guide to users when the need arises to make a protocol choice. While this is commendable, it is not fair to recommend SSL for site to site application seeing it cannot be used for all application types (Chawla. *et al.*, 2014) except if they had specified what applications in site to site VPN this recommendation was made for plus SSL is browser dependent (Jahan *et al.*, 2017) and need additional installations to offset this effect which is an additional overhead in terms of cost (Chawla. *et al.*, 2014). In addition, the IP address of the network needs be protected at the network/IP layer using IPSec before packets gets to the transport layer where SSL operates (Chawla. *et al.*, 2014).

Asadi Eskandar *et al.* (2015) performed an analysis VOIP over GRE tunnel. The authors simulated the performance of VOIP traffic over GRE tunnel using OPNET modeler 17.5. Quality of Service (QoS) parameters as choice of voice signalling protocol and voice codec were used. These parameters were examined in both heterogeneous and homogeneous network environments. The configuration was based on H.323 and session initiation protocol, (SIP). For voice codecs, G.711 and G.723 were configured and tested. Although the call quality was poor in terms of end to end delay, call set up time, and a decrease in MOS, this was said to be due to the heterogeneity of the network and the lack of QoS parameters in the backbone network and not as a result of the tunnel thus establishing that GRE was not responsible for the poor QoS performance seen.

Elezi and Raufi (2015) gave an overview of the Internetworking concept that involved the Internet and transport layer of the TCP/IP reference model using methodological issues based on experimental research through the provision of comparative analysis of outcomes from the use of IPSec protocol suite in a site to site VPN. The aim was to present conclusions that are more exact against simulated results. By using .NET C# program interface, SQL 2012 database, three database record samples were queried over an IPSec VPN implementation applying different encryption and authentication modes per time and evaluating the outcome. They concluded that using varying encryption algorithm is more impactful than using varying authentication algorithm. However, running IPSec in aggressive mode as done in the experiment exposes the data to unauthorised access as the hash is sent before the encryption in this mode (Singh *et al.*, 2012). Also, AH does not provide any sort of data confidentiality like ESP, the authentication algorithm, MD5 is vulnerable to collision as it has been proven to hash to the same message digest.

Padhiar and Verma (2015) compared the performance of four VPN tunnelling protocols namely IPSec, PPTP, SSL and L2TP on different operating systems (OS): Win2003, WinVista and Linux Fedora. Iperf was used as the network generator on a network setup with TCP/IP. The performance metric used was throughput but in no particular testbed. The throughput value of each protocol using a combination of several security algorithm was taken and the results were matched against themselves with respect to the OS used. The results showed that PPTP has the highest throughput in Win2003 OS and SSL the lowest, SSL gave a better throughput than IPSec in Linux OS leading to a conclusion that the network performance of a VPN tunnel is dependent on the OS, the security algorithms

used and the selected protocol. While these does not represent throughput values for all WinOS using these technologies, the security algorithm combination used in IPSec, 3DES and MD5 are vulnerable and could expose data to unauthorised access. A testbed such as either of site to site or remote access should have been used as an environment where these systems' performance could be tested.

Haidar and Houseni (2016) carried out an analysis of the impact of security on quality of service (QoS) using a layer2 (L2TP) and a layer3 (IPSEC) tunnelling protocols using OPNET simulator software. These layers are considered the weakest among the other layers in the OSI model due to their closeness to the physical layer thus employing protection at these layers will safeguard layers 4,5 and 6. QoS performance measures used are jitter, loss ratio and delay. Differentiated service (DiffServe) QoS type that works on provisioned QoS model where network elements are set up to address multiple types of traffic with varying QoS requirements was used. Results showed that for response time, IPSec performed better than L2TP however, 3DES and MD5 security parameters used in IPSec are vulnerable to bruetforce attack and collision.

Alharbi *et al.* (2017) carried out a performance evaluation of VOIP in different network environments; simulation, emulation and laboratory experiments using GNS3, Netmeeting conferencing software, Omnipeek for packet sniffing, FTP server and client over VPN multipoint network. IPSec protocol suite was used as the VPN technology. The emulation setup used GNS3 running VMware workstation running on Linux OS based on Ubuntu 14.04. The simulation environment used GNS3 and VPCs. The routing protocol used was not specified, only mention was made of RIP, OSPF and BGP. The performance metrics for all network environment are jitter, delay, packet loss and MOS.

Results showed that simulation results sharply contrasts with lab and emulation whose results followed each other closely for all performance metrics. Though security algorithm used in IPsec and the routing protocol used were not mentioned specifically, the work is s proof that laboratory experiments and emulations reflect the true nature of a network than does a simulation.

Bensalah *et al.* (2017) carried out an analysis of the performance of voice traffic over IP to evaluate the scalability of layer 3 tunnelling protocols using GNS3. The background traffic was generated using voice traffic, IP Service Level Agreement (SLA) for traffic generation on 96 different scenarios. Layer 3 VPN tunnelling protocols considered were IP, GRE, IPSEC, GRE over IPSEC, DMVPN and DMVPN IPSEC. Evaluation parameters used were jitter, latency, packet loss, MOS. The evaluation revealed that IPSEC performed best in terms of loss packet, scaled better than the others. Although this analysis was not carried out with respect to any application area, yet, it established that good QoS could be achieved in terms of security and scalability with IPSEC.

Deshmukh and Iyer (2017) used Cisco packet tracer to simulate, analyse and verify VPN tunnel for a remote site. The security algorithms combination used (AES and SHA) are considered strong enough to protect against any form of attack to prevent unauthorized access to data on the network but the authors were not specific which AES and SHA type was used. The network's performance was not tested against any metrics, rather only assumptions were made that the configuration would reduce delay, jitter and drop. Simulation besides, does not give a true reflection of a network performance (Alharbi *et al.*, 2017).

Jahan *et al.* (2017) based on organizational application requirements analysed different VPN tunnelling protocols to measure their performance in terms of throughput, latency, RTT in both site-to-site and remote access VPN using GNS3 software, Cisco IOS 3745, Cisco 8-port ethernet switch, Win7 OS, VPCs for the network emulation. Based on the analyses which was carried out for both site to site and remote access VPN respectively, the authors inferred that for delay and bandwidth sensitive applications like Internet telephony, video conferencing, audio/video streaming in site to site VPN, GRE tunnelling protocol is most suitable since they exhibited high throughput and low latency properties whereas IPSec is suitable for security sensitive applications. However, for remote access VPN, L2TP/IPSec is preferred for all applications especially for bandwidth, security and time sensitive applications. The limitation with this work is that the tunnel is not adequately secured against some possible forms of attack as the security algorithms used (3DES and MD5), are vulnerable and can be broken by a brute force or MIM attack (Barker *et al.*, 2017; Dev, 2013).

From the similar works reviewed, it could be concluded that a few researchers have explored a couple of methods at deploying VPN tunnels. However, deploying these according to specific application requirements such that VPN networks could be specifically identified by the type of service they provide has attracted even less attention. This work will attempt to improve on ASTPS 2017 with the main aim of improving on the security of the network using stronger encryption algorithms while retaining appreciable throughput, latency and RTT properties of the network. This is to meet application demands that require security as a service.

CHAPTER THREE

MATERIALS AND METHODS

3.1 Introduction

This chapter captures the detailed description of the materials, and methods employed for the successful development of the application specific tunnelling protocol selection scheme (ASTPSS) and the improved ASTPSS (iASTPSS) both emulated in a virtualized environment on graphical network simulator, GNS3. The steps of the methodology are outlined in the following subsections

3.2 Materials

All materials used for the successful completion of this research work are discussed in the following sections. They include all hardware and software used for the implementation and realization of the set objectives.

3.2.1 Hardware platform

The research was emulated on a HP Laptop, (Intel ® Core(™) i5-7200 CPU @2.70GHz, 64 –bits Operating System, x64-based processor, 1-TB HDD, 8GB RAM

3.2.2 VM workstation pro v12.0.1.3

Virtualization has proven to be as effective as real life scenarios in the determination of the behaviour of networks. This is due to the ease of implementation and ability to provide real-life results as at when live network devices or equipment are used. For this research, VMware workstation Pro v12.0.1.3 was chosen as the virtualization platform for the installation of GNS3, where the VPN network topology was emulated. Based on the network needs such as compatibility with other VMs and OS, execution speed, extended features, integration with GNS3, and support for embedded virtualization, VMware was chosen and installed on HP laptop, (Intel ® Core(™) i5-7200 CPU @2.70GHz, 64 –bits

Operating System, x64-based processor, 1-TB HDD, 8GB RAM. Installation steps and procedures for VMware is found in Appendix A.

3.2.3 GNS3 software

GNS3 software, version is 2.0.3 was the backbone network simulator used and it was installed on the HP laptop used for this work. The installation process is found in Appendix B.

3.2.4 GNS3 VM

The GNS3 Virtual Machine (VM) open virtualization application (OVA) version for VMware was installed on the VMware. This is to enable the installed GNS3 on the hardware platform run in a virtual environment where the emulation is to be implemented. The installed version, however, must be compatible with the version installed on the physical device. The installation steps are shown in Appendix C.

3.2.5 Windows7 OS

Windows7 Operating System (OS) is installed on the VMware before importing to the network topology in GNS3 VM. The installed version is Windows7 Professional SP1, intel ® core ™ i5-7200, 2.71GHz, 2GB RAM, 64-bit Operating System. This serves as a network server for the developed network topology. The installation steps are shown in Appendix D.

3.3 Methods

The steps of the methodology used in achieving the set objectives are as follows:

a) Emulation of the network environment on a virtual machine necessary for the implementation of ASTPSS by Jahan et al., (2017) adopting the following steps:
    i) Install GNS3 software
    ii) Install VMware

iii) Install GNS3 VM on VMware

iv) Install Windows7 OS on VMware

v) Interconnect GNS3 VM to GNS3 software

vi) Develop and configure the network topology with RIPv2 as routing protocol

vii) Configure the VPN tunnel using IPsec and GRE tunnelling protocols based on security, bandwidth and time sensitivity as application needs

viii) Use 3DES for encryption and MD5 for hashing on the IPsec tunnel

ix) Upon successful configuration, send traffic to the network using the "ping" command varying the packet sizes to determine the throughput, latency and RTT of the network

b) Development of an iASTPSS using the under listed steps:

i) Repeat steps a) i) – vi)

ii) Develop first instance of iASTPSS by developing and configuring network policies (access control) to define interesting traffic pattern

iii) Configure IPsec and GRE tunnelling protocols on separate network address classes to distinguish the networks

iv) Use advanced encryption standard (AES 256) for encryption and secure hash algorithm (SHA256) for hashing in the IPsec phase I and phase II

v) Repeat step a) ix)

vi) Develop a second instance of iASTPSS

vii) Repeat step a) vi) but with OSPF as routing protocol

viii) Repeat steps b) iii) – v)

c) Compare iASTPSS and ASTPSS using throughput, latency and RTT in both IPsec and GRE tunnels respectively.

3.3.1 Network topology design and development

The network topology for the implementation of ASTPSS and iASTPSS was designed and developed in GNS3 as shown in Fig 3.1

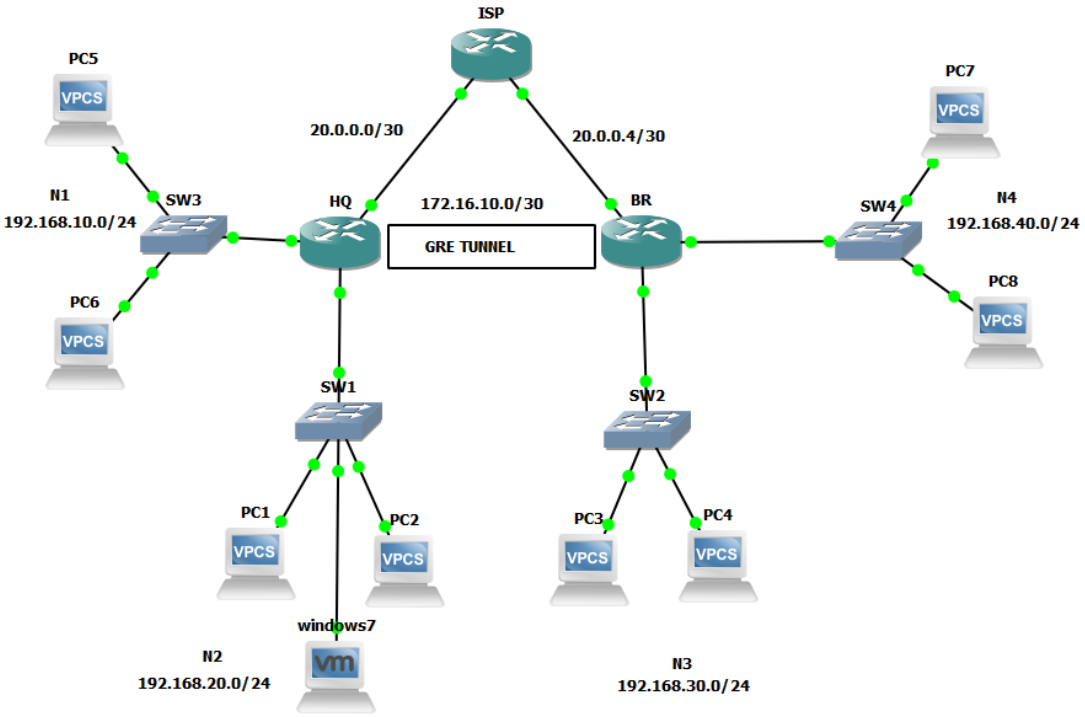


Fig 3.1: Network Topology

3.3.2 ASTPS implementation

Based on security, bandwidth, and time sensitivity requirements of applications, two tunnelling protocols, IPSec and GRE was deployed on the network topology of Fig 3.1. The IPsec tunnel was configured between networks 192.168.20.0/24 and 192.168.30.0/24 on N2 and N3 as tunnel source and destination respectively while the GRE tunnel was configured on network 172.16.10.0/30. In IPsec phase 1 and 2, security algorithms such as 3DES for encryption, MD5 for hashing and pre-share for authentication, crypto map, transform set, and access control lists for defining traffic pattern of interest was configured. After a successful configuration of both phases one and two, a ping request

was sent from one tunnel end to the other to obtain the ICMP messages. From these ICMP messages returned from the ping statistics of the tunnel, the throughput, latency and RTT of the network was analysed. IPsec tunnel was configured for security sensitive applications due to the encryption and authentication properties of the tunnel. GRE, a point to point protocol lacking in any security properties but fast to ensure good throughput and low latency was configured at the two ends of the tunnel on the 172.16.10.0/30 network. This served the bandwidth and time sensitivity needs of applications. Other parameters that was used for the implementation of this network are as shown in Table 3.1. The codes for this network implementation are found in Appendix E.

Table 3.1: ASTPS Network Emulation Parameter List Jahan *et al.* (2017)

S/N	Parameter	Value
1	Simulation software	GNS3 2.0.3
2	Router	Cisco Router C3745
3	Switch	Cisco 8-port Ethernet switch
4	Operating system	Windows 7
5	Routing protocol	RIP v2
6	Computers	VPCs
7	Virtual machine workstation	Ubuntu 14.04 LTS
8	Encryption algorithm	3DES
9	Hashing algorithm	MD5

3.3.3 iASTPSS implementation

The implementation of iASTPSS was done progressively until a desired performance in terms of network throughput, latency, and RTT that met the security, bandwidth, and time sensitivity needs of applications were achieved for the IPsec and GRE tunnels. The first stage was improving on the security of the existing system which was considered vulnerable in the IPsec tunnel. Based on security, bandwidth and time sensitivity requirements of applications as in ASTPSS, IPsec and GRE that met these demands, see

section 2.2.2, are deployed on the network of Fig 3.1. The tunnels were configured consecutively. Beginning with the IPsec tunnel, this was deployed on the N2 and N3 networks on 192.168.20.0/24 and 192.168.30.0/24 respectively. The IPsec configuration was done in two phases. Phase one dealt with the IKE SA negotiations. These include the encryption mode, the hash mode, the authentication mode, the key lifetime and Diffie-Helman (DH) group. The encryption mode was set to AES256, the hash was set to SHA256, the authentication was set to preshare, the lifetime of the key was set to 86400 and the DH group was set to group 14. All these were done in phase one to enable the formation of a SA between the communicating peers on the participating routers, HQ and BR on the two sites. Once this phase was successfully configured between the two sites, the second phase was immediately initiated. This involved the establishment of the tunnel using the negotiated SA parameters in phase one. The first thing was to set the transform set, the implementation protocol which is ESP configured in tunnel mode, the perfect forward security (PFS). The network policies to allow the passage of security sensitive applications through the IPsec tunnel using EAL was defined and, a crypto map was then created and applied on the outgoing interface of the of the participating routers, HQ and BR. ISAKMP turns "ON' as soon as this was applied, to mean that, the tunnel has been established and ready for communication between the two sites on networks N2 and N3. A ping from one end of the tunnel to the other with varying packet sizes was then used to determine the network performance with respect to throughput, latency, and RTT. Although, a better security was obtained in this case than in ASTPSS due to the security algorithms used, AES 256 and SHA 256, yet, the network performance was poor in comparison to ASTPSS due to the computational overhead as a result of these security algorithms used. In summary, network performance was traded for security in this case. This necessitated a second stage in the development of iASTPSS leading to the renaming

of this first stage of implementation as iASTPSS_case1 and the second stage as iASTPSS_case2. iASTPSS_case2 was developed by changing the routing protocol to enable faster convergence of routes and scale up the network's performance. The OSPF routing protocol was configured on the network of Fig: 3.1 while AES 256 and SHA 256 security algorithms were retained in the IPsec tunnel. After a successful configuration, the performance of iASTPSS_case1 and iASTPSS_case2 were again compared and analysed using throughput, latency, and RTT as metrics.

Consecutively, the GRE tunnel was configured on the 172.16.10.0/30 network. The configurations were performed at the two tunnel ends of the HQ and BR routers with a default route through to the 192.168.20.0/24 and 192.168.30.0/24 networks on N2 and N3 as end stations. Then, using EAL, the traffic pattern was defined for applications that require bandwidth and time sensitivity as a requirement. OSPF routing protocol was configured on the network topology of Fig: 3.1 for packet routing in the network. RIPv2 routing protocol used in the base work produced no new change in network performance when deployed. The ICMP message was then obtained using the ping statistics from the tunnel to analyse the throughput, latency, and RTT behaviour of the network. The results were compared with that of ASTPSS and extensively discussed in Chapter Four.

This scheme did not present an analysis of application requirements based on tunnel outputs, rather tunnels were configured on the network based on pre-determined application requirements. Parameters employed on the network topology used for this implementation are listed in Table 3.2. All codes for this implementation are found in Appendix F

Table 3.2: iASTPSS Network Parameter List

S/N	Parameter	Value
1	Simulation software	GNS3 2.03
2	Router	Cisco router C7200
3	Switch	Cisco 8-port Ethernet switch
4	Operating system	Windows 7
5	Routing protocol	RIPv2
6	Routing protocol	OSPF
7	Computers	VPCs
8	VMWare	Ubuntu 14.04 LTS
9	Encryption algorithm	AES 256
10	Hashing algorithm	SHA 256

3.3.4 Experimental procedure for ASTPS and iASTPSS

Upon completion of the configuration of the network topology as shown in Fig 3.1, the start button on the GNS3's GUI was clicked. This turned "ON" all VMs used on the network topology design in GNS3 automatically. The next stage was to click on a particular router to enter the console. The router was first enabled using the # command in the CLI to enter the privilege executive mode. The next stage was to enter the global configuration mode. This was done by entering the *configure terminal* command in the CLI in order to configure the router with the requisite configurations such as the hostname, gateway and host IP addresses to networks and routers, interface IDs, routing protocols, DHCP and the tunnel deployment. The tunnels were only deployed between the HQ and BR routers as the ISP router was unaware of the existence of the VPN between the two routers. The initial start-up page of the console was shown in Fig 3.2.

The routers were configured consecutively, that is, one after the other. The IPsec configuration was done in two phases. Phase one dealt with the Internet key exchange

(IKE) negotiation which included the selection of the security association (SA) parameters – encryption, hash, authentication and DH group setting and the key lifetime.

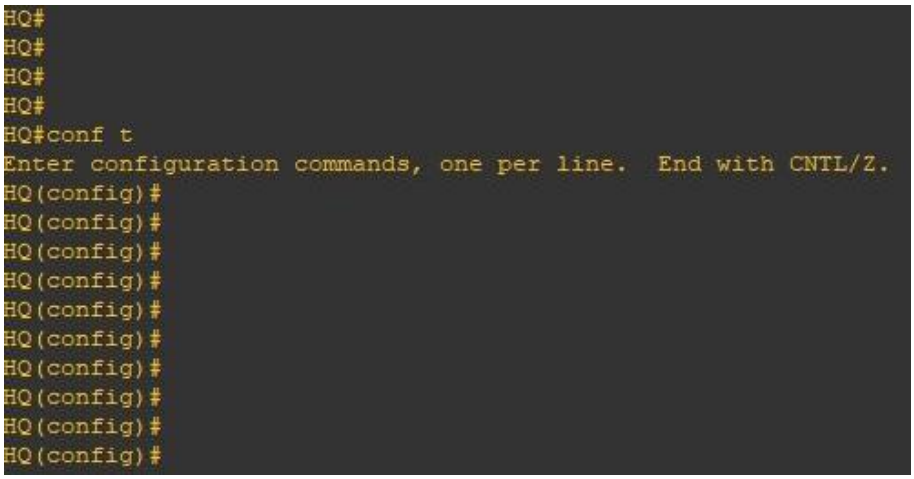


Fig 3.2: Snippet of Start-up Configuration Page

Phase two was concerned with the establishment of the tunnel that had been setup in phase one. This included setting up the transform set, the ESP in tunnel mode, that is, the mode the tunnel should operate. An extended access control list was created to define traffic flow of interest. A crypto map was then created and applied to the outgoing interface of the participating routers. Once the process was successfully completed, ISAKMP turned "ON". This could be seen in Fig. 3.3 as it revealed that the IPSec tunnel between the HQ and BR routers was successful. A ping from one end of the tunnel to the other further determined the success of the connection. The ping request either timed out if the configuration was not rightly done or returned with the ping statistics from the tunnel if it was rightly done. Going further, on a separate network other than that on which the IPsec was established, but between the participating routers within the VPN, that is, HQ and BR, a GRE tunnel was configured. This was set up as a point to point connection between the two ends of the tunnel. Once configurations were successful for both tunnels, it was saved either in the privilege executive mode or in the global configuration mode using the *write* or *do write* commands in the CLI, respectively. Ping requests were then

sent through the tunnels to generate the ICMP statistics to determine the throughput, latency, RTT of the networks. These results were elaborately discussed in Chapter Four. This experimental procedure was adopted for the implementation of both ASTPSS and iASTPSS but with the definition of network policies using access control in iASTPSS to make the networks application defined. The systematic procedures are clearly outlined in Appendix G

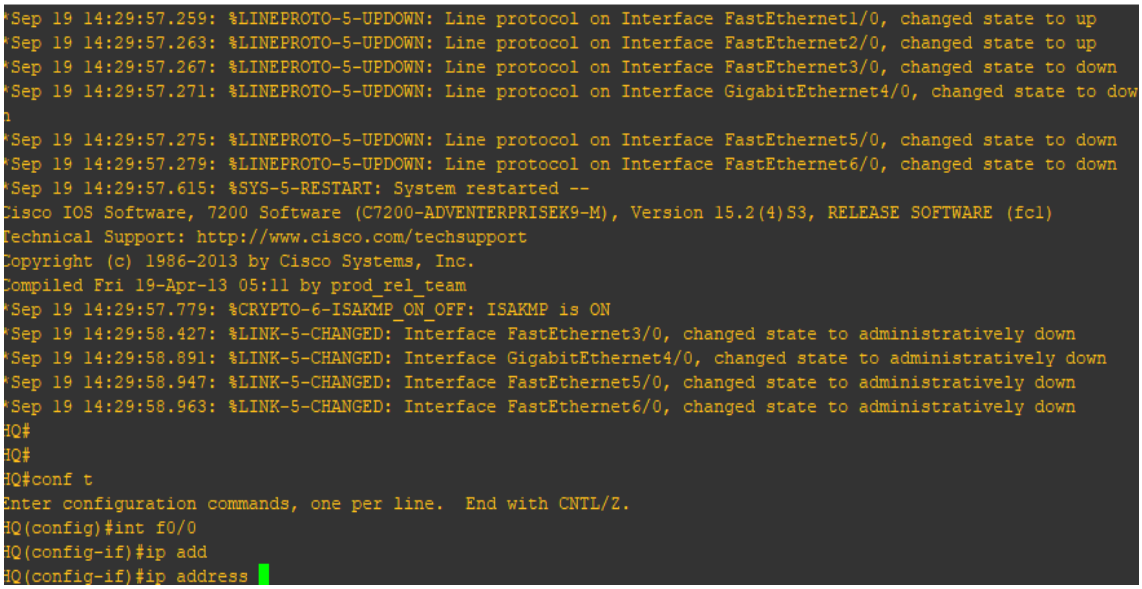


Fig 3.3: Snippet of a successful configuration from the IPsec tunnel

3.3.5 Performance validation

Performance metrics used for the validation of iASTPSS against ASTPSS were throughput, latency, and RTT. The percentage improvement of iASTPSS_case1 over ASTPS was measured using:

$$\%\ \text{Improvement} = \frac{\text{iATPSS_case1} - \text{ASTPS}}{\text{iASTPSS_case1}}\ \text{x}100\% \qquad (3.1)$$

Similarly, the percentage improvement of iASTPSS_case2 over iASTPSS_case1 was measured using:

$$\%\ \text{Improvement} = \frac{\text{iATPSS_case2} - \text{iASTPSS_case1}}{\text{iASTPSS_case2}}\ \text{x}100\% \qquad (3.2)$$

The results from Equation (3.2) was presented as the improved ASTPSS.

The throughput calculation was measured using equation (2.1)

3.3.5.1 Throughput parameters and conversion

The unit of throughput is bps. Packet sizes are in bytes and these need be converted to bits (b). Similarly, the network latency is in milliseconds (ms), this needs be converted to seconds (s) as well to achieve the unit of measurement for throughput. Table 3.3 presents a conversion table used in this work.

Table 3.3: Throughput Parameter Conversion

S/N	**Parameter**	**Unit of measurement**	**Equivalent in corresponding units**
1	Window size	Bytes	1-byte = 8-bits
2	Latency	Milliseconds (ms)	1-ms = 1 x 10^{-3}s

CHAPTER FOUR

RESULTS AND DISCUSSIONS

4.1 Introduction

In this chapter, the results of the outcome of research on iASTPSS and ASTPSS were discussed using the defined performance metrics.

4.2 Experimental Outcome

The ping statistics of the ICMP message showed the tunnel behaviour as the packets traverse the network from the source to destination for both protocols. This statistic was made possible when packets were injected into the network using the ping command. Fig 4.1 presented a snippet of a captured ICMP message for a 32bytes and 64bytes packet through an IPsec tunnel of the ASTPSS network. This was repeated for varying packet sizes and the results were obtained and analysed accordingly.

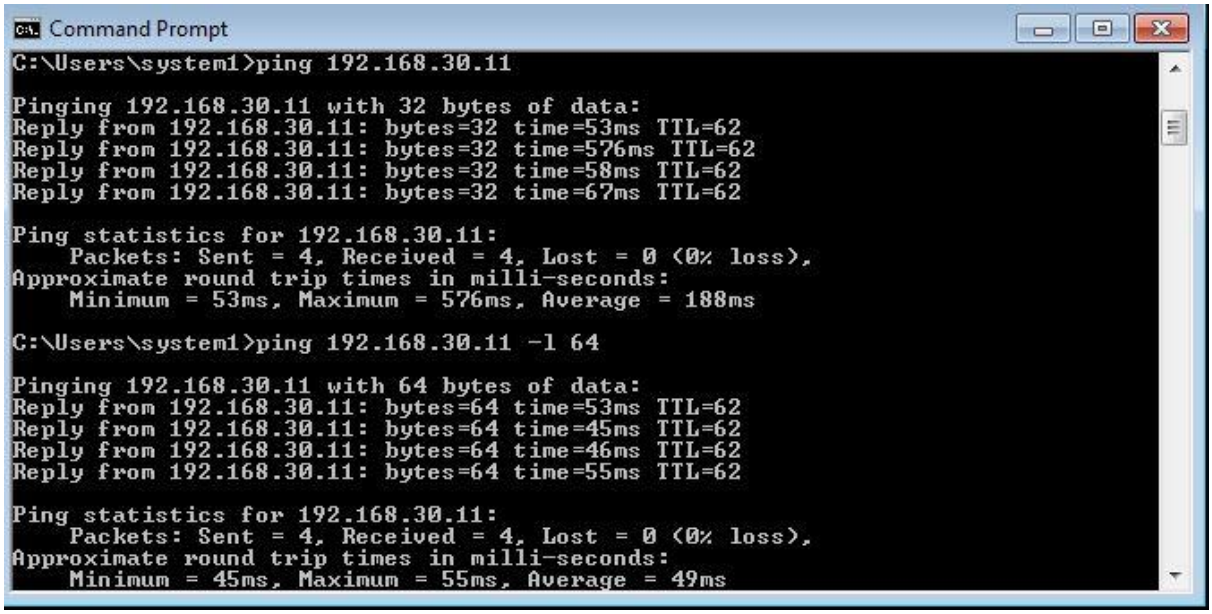


Fig 4.1: Snippet of Captured Packets from an IPSec Tunnel of the ASTPSS Network

Fig: 4.1 was shown to reflect how the results were captured for both ASTPSS and iASTPSS networks. A comprehensive result for all packet sizes considered for the IPsec

tunnel for ASTPSS and iASTPSS case1 and case2 are presented in Tables 4.1 to 4.3 respectively.

Likewise, Fig. 4.2 showed the ping statistics from a GRE tunnel of iASTPSS network. Fig: 4.2 was shown to reflect how the results were obtained for the iASTPSS and ASTPSS networks. A comprehensive result of all packets considered in iASTPSS and ASTPSS for the GRE tunnel are presented in Tables 4.4 and 4.5 respectively.

A more detailed Wireshark capture was presented in Fig 4.3.

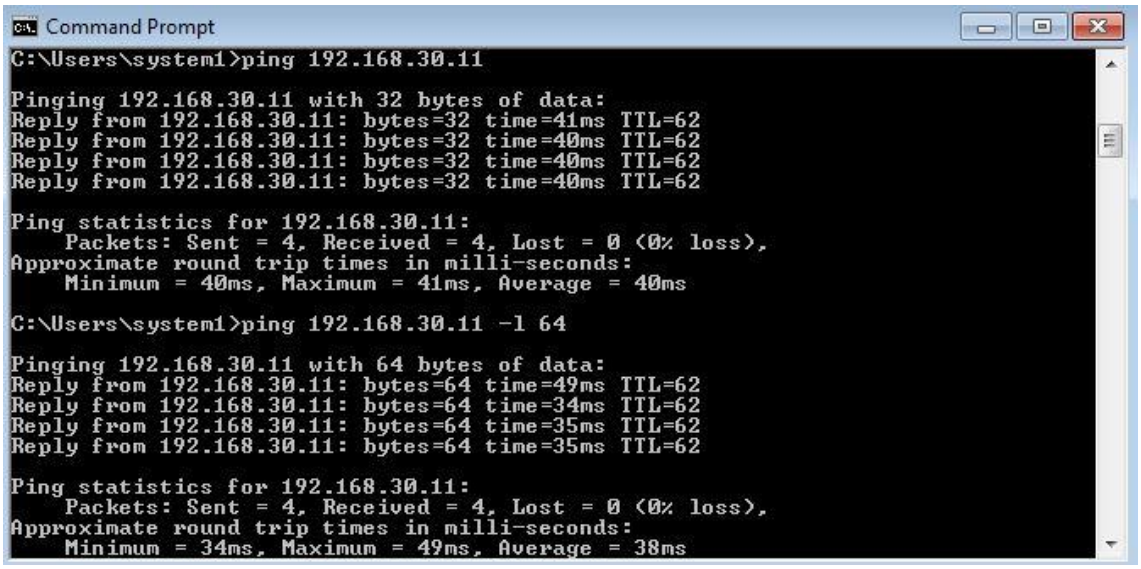


Fig 4.2: Snippet of Captured Packets from a GRE Tunnel of the iASTPSS Network

Fig 4.3 presented a more detailed capture from the IPsec tunnel displaying the packet source and destination, the protocol type, packet length, the sequence number and the time to live (TTL) for each packet as it went through the tunnel. ICMP messages represented response from the tunnel.

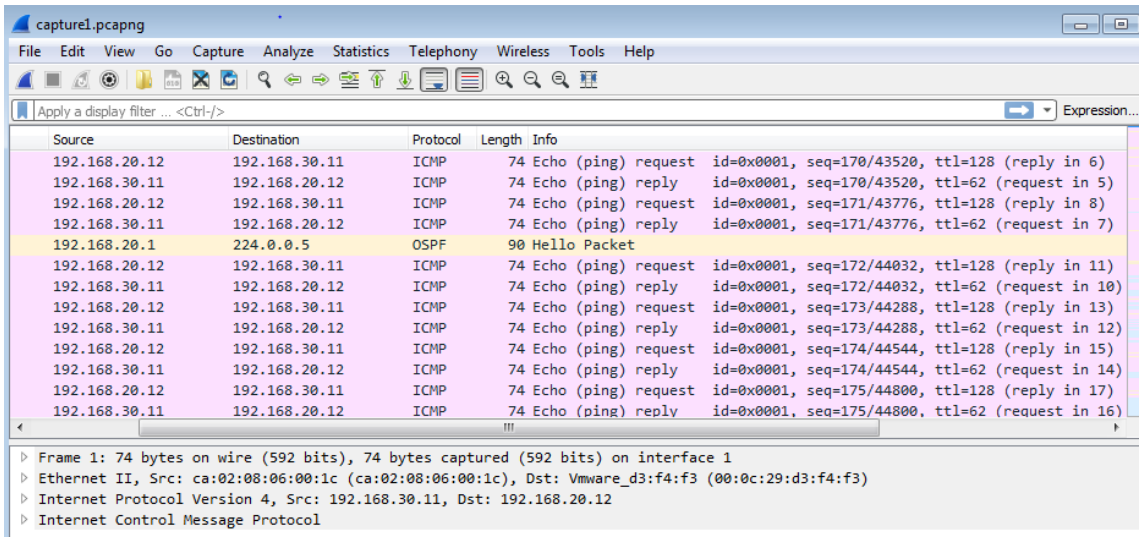


Fig: 4.3: Snippet of the Wireshark Capture from the IPSec Tunnel of ASTPSS

As packets traverse through the IPsec tunnel from source to the destination, they went through the process of encapsulation, encryption, and digest at the source and decapsulation, decryption, and verify at the destination as seen in Fig. 4.4. This process is the same for both ASTPSS and iASTPSS. Fig: 4.4 presented the tunnel performance and response as packets were injected into the network through the IPsec tunnel of ASTPSS.

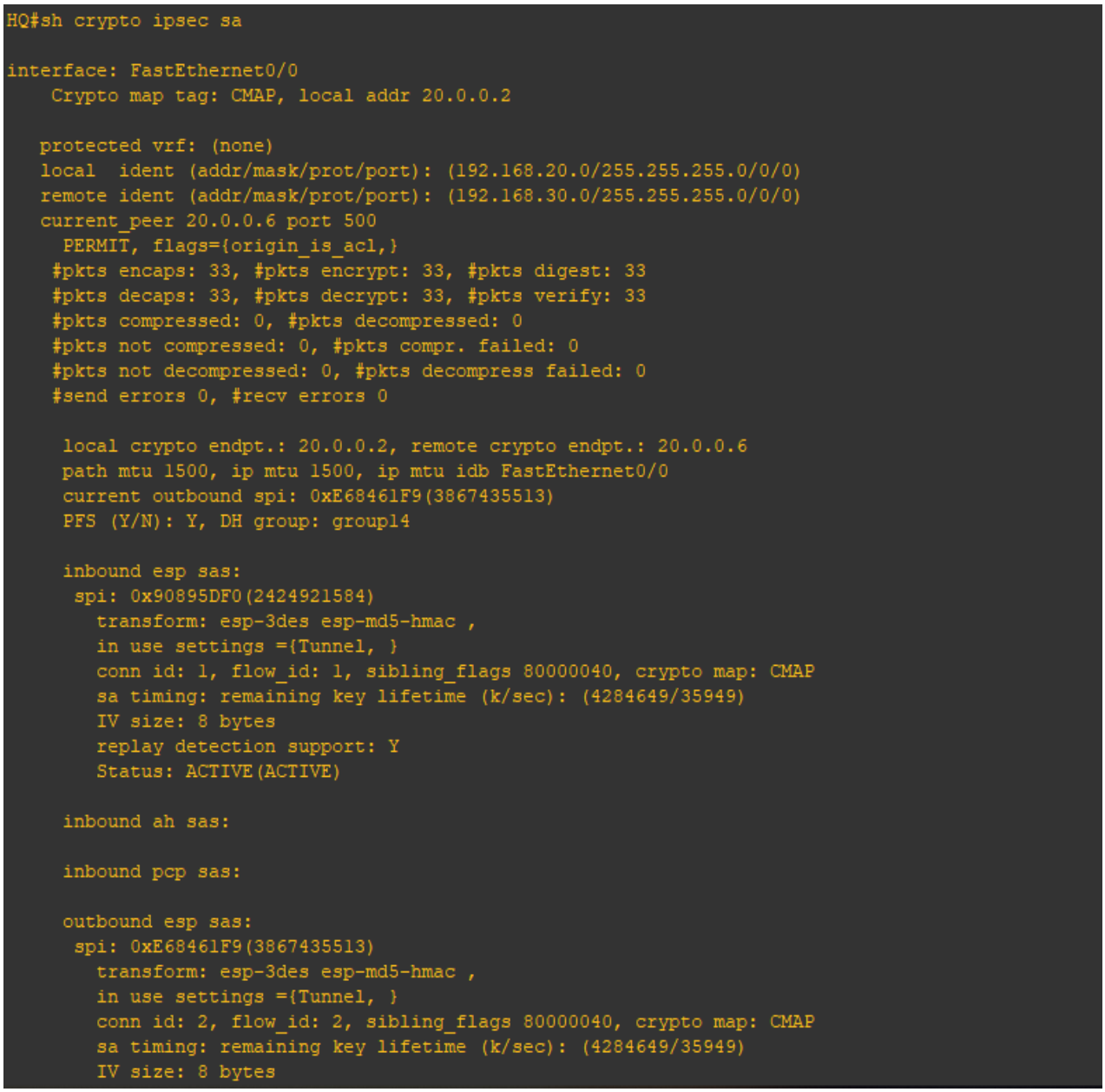


Fig 4.4: Snippet of IPsec Tunnel Output of ASTPSS

Similarly, Fig. 4.5 showed the tunnel behaviour as for a GRE tunnel as packets were injected into the iASTPSS network through the tunnel. This packet behaviour through the tunnel is the same in both cases, iASTPSS and ASTPSS.

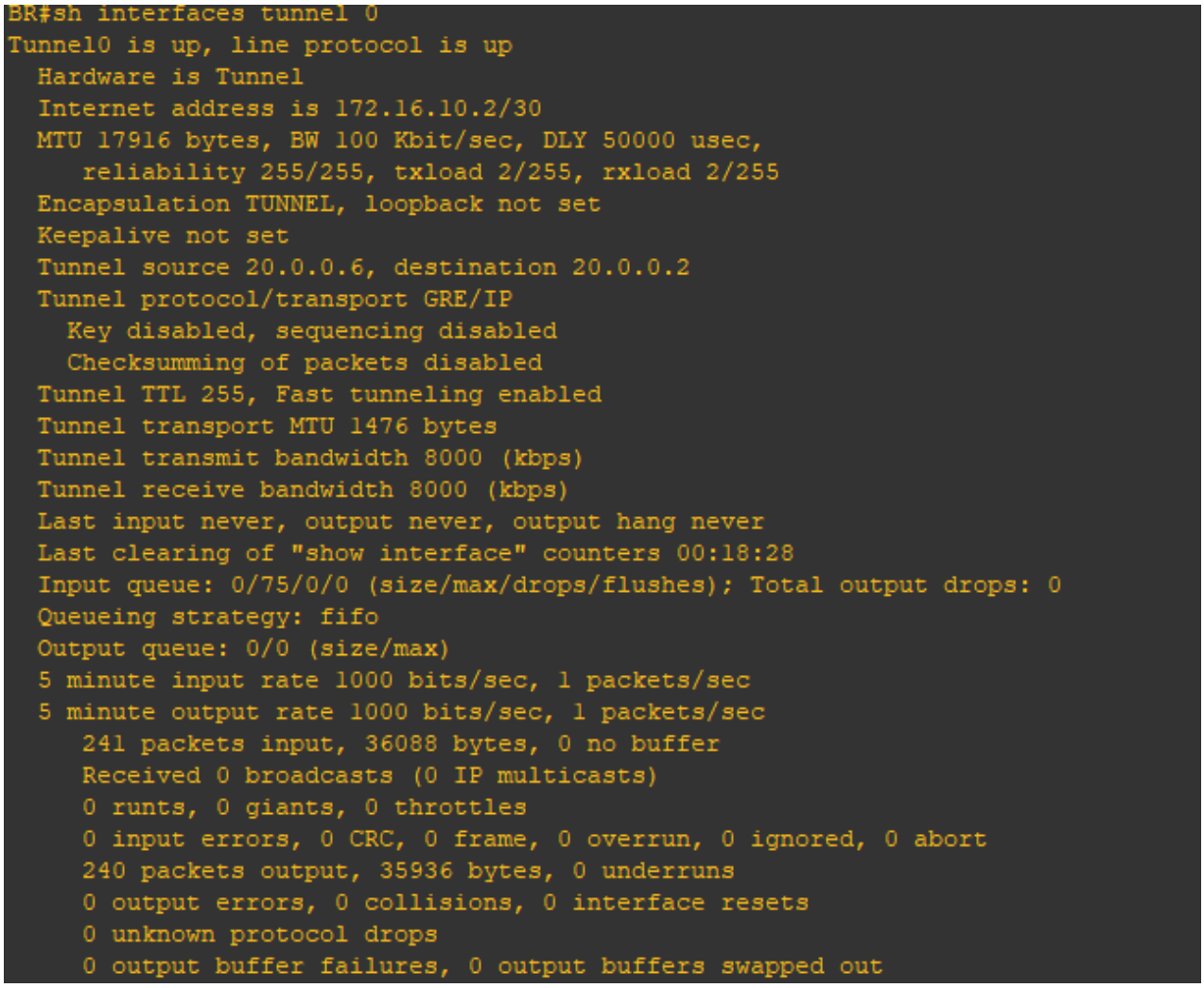


Fig 4.5: Snippet of the Output of a GRE Tunnel of iASTPSS network

The figure showed the number of packets inputted, packet size and the buffer size with the corresponding packets outputted, packet size and the underruns after encapsulation and decapsulation of packet from the tunnel.

4.3 Result Analysis

Varying packet sizes were injected into ASTPSS and iASTPSS_case1 to analyse tunnel network performance in terms of throughput, latency and RTT as packets traverse from source to destination through the tunnels. These were derived from the ICMP messages from the ping statistics. The values were captured for each network scenario and presented in Tables 4.1 to 4.5.

Table 4.1 presented the throughput, latency, and RTT values from the IPsec tunnel of ASTPSS.

Table 4.1: Throughput, Latency and RTT Values from the IPsec Tunnel of ASTPS

S/N	Packet Size (bytes)	Throughput (Kb/s)	Latency (ms)	RTT (ms)
1	32	4.830	53	150
2	64	11.387	45	49
3	128	27.676	37	66
4	256	45.511	45	55
5	512	113.778	36	39
6	1024	163.840	50	58
7	1100	187.234	47	51
8	1200	213.333	45	800
9	1300	288.889	36	53
10	1400	169.697	66	69

Similarly, Table 4.2 presents the throughput, latency, and RTT values from the IPsec tunnel of iASTPSS_case1. These values for both network were then compared and analysed. From the analysis, Table 4.1 representing the network performance values of ASTPSS presented appreciable throughput, latency, and RTT values over iASTPSS_case1 whose network performance values in terms of throughput, latency, and RTT values are presented in Table 4.2. The simple reason for ASTPSS outperforming iASTPSS_case1 is due to the computational overhead in encryption from the iASTPSS_case1.

Table 4.2: Throughput, Latency and RTT Results from the IPsec Tunnel of iASTPSS_case1

S/N	Packet Size (bytes)	Throughput (Kb/s)	Latency (ms)	RTT (ms)
1	32	6.095	42	52
2	64	9.309	55	58
3	128	23.814	43	48
4	256	37.236	55	59
5	512	65.016	63	64
6	1024	151.704	54	58
7	1100	157.143	56	59
8	1200	282.353	34	858
9	1300	315.152	33	49
10	1400	169.697	66	112

Based on the outcome of the analysis from Tables 4.1 and 4.2, it was necessary to further change some parameters so as to improve the network performance. To improve the network performance in iASTPSS_case1, OSPF routing protocol known to have a faster route convergence over RIPv2 was configured. The results generated from this network was presented in Table 4.3his was because, by default, ASTPSS should have a better network performance than iASTPSS_case1 due to the longer key size used for encryption in iASTPSS_case1 that increased the computational overhead and slowed down network performance. This led to the generation of Table 4.3 from iASTPSS_case2.

Table 4.3: Throughput, Latency and RTT Results from the IPsec Tunnel of iASTPSS_case2

S/N	Packet Size (bytes)	Throughput (Kb/s)	Latency (ms)	RTT (ms)
1	32	7.111	36	46
2	64	10.240	50	56
3	128	31.030	33	50
4	256	41.796	49	54
5	512	81.920	50	58
6	1024	210.051	39	51
7	1100	187.234	47	803
8	1200	188.235	51	71

9	1300	231.111	45	51
10	1400	248.889	45	57

Finally, Tables 4.4 and 4.5 showed the GRE tunnel output for ASTPS and iASTPSS, in terms of the throughput, latency, and RTT respectively.

Table 4.4: Throughput, Latency, and RTT Results from the GRE Tunnel of ASTPSS

S/N	Packet Size (bytes)	Throughput (Kb/s)	Latency (ms)	RTT (ms)
1	32	5.565	46	46
2	64	9.309	55	58
3	128	22.261	46	803
4	256	41.796	49	61
5	512	67.148	61	63
6	1024	174.298	47	51
7	1100	258.824	34	44
8	1200	228.571	42	54
9	1300	196.226	53	57
10	1400	280.000	40	800

Table 4.4 showed the results for throughput, latency, and RTT values for the GRE tunnel using RIPv2 as routing protocol. Fig 4.5 showed the results of throughput, latency and RTT values from the GRE tunnel for iASTPSS using OSPF as routing protocol. No change occurred when RIPv2, the routing protocol used in ASTPSS was used. This necessitated a change in the routing protocol to OSPF.

Table 4.5: Throughput, Latency and RTT Results from the GRE Tunnel of iASTPSS

S/N	Packet Size (bytes)	Throughput (Kb/s)	Latency (ms)	RTT (ms)
1	32	6.400	40	40
2	64	15.059	34	38
3	128	17.067	60	62
4	256	60.235	34	40
5	512	107.789	38	69
6	1024	186.182	44	52
7	1100	244.444	36	38
8	1200	234.146	41	795
9	1300	315.152	33	37

10	1400	254.545	44	54

4.4 Performance Comparison and Analysis

iASTPSS performance was compared with ASTPSS in terms of throughput, latency, and RTT in all configuration scenarios. A comparison of the network security was as established in section 2.2.6.

4.4.1 Result comparison and analysis from the IPsec tunnel

The throughput, latency, and RTT values from the IPsec tunnel for both iASTPSS_case1 and ASTPSS were compared and analysed in this section.

4.4.1.1 iASTPSS_case1 and ASTPS comparison in terms of throughput from the IPsec Tunnel

iASTPSS_case1 and ASTPSS were both analysed in terms of throughput for varying packet sizes from the IPsec tunnel. The result showed an improvement in throughput of ASTPSS over iASTPSS_case1. The graphical output was shown in Fig 4.6 and the tabular result was shown in Appendix K. Traffic behaviour through the tunnel for varying packet sizes showed that at initial packet injection, throughput values from the tunnel for both networks were basically constant but as the packet size increases, iASTPSS_case1 showed a fluctuating decline in throughput while ASTPSS maintained a rise. By popular demand, it was expected that with the encryption algorithms used in iASTPSS_case1, a lower throughput value should be expected as was the case here.

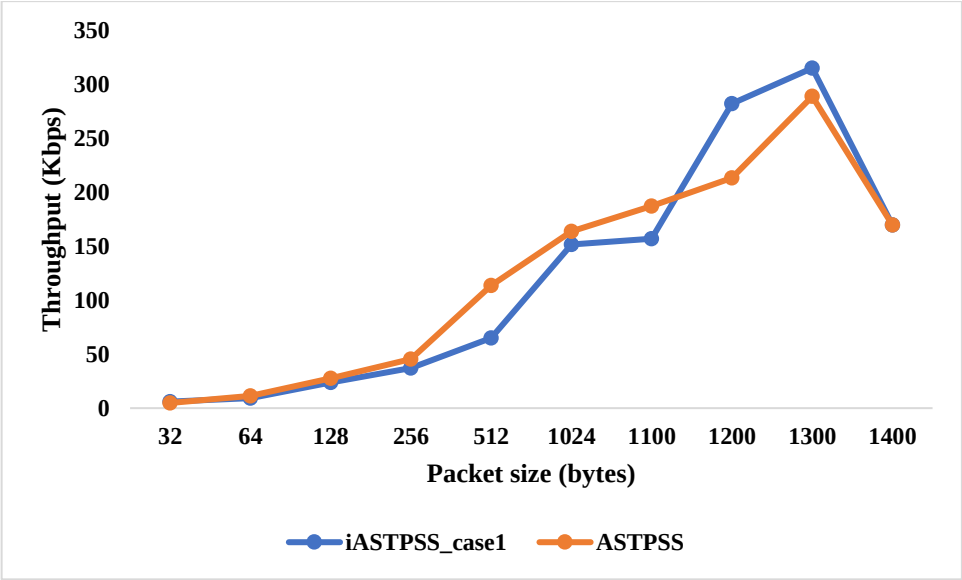


Fig 4.6: Graph of Throughput against Packet Size for iASTPSS_case1 and ASTPSS in the IPsec Tunnel

4.3.1.2 iASTPSS_case1 and ASTPS comparison in terms of latency from the IPsec Tunnel

Similarly, the network latency values from the IPsec tunnel for the two networks were compared and analysed. Fig 4.7 presents a graphical presentation of these results and the tabular results was shown in Appendix L.

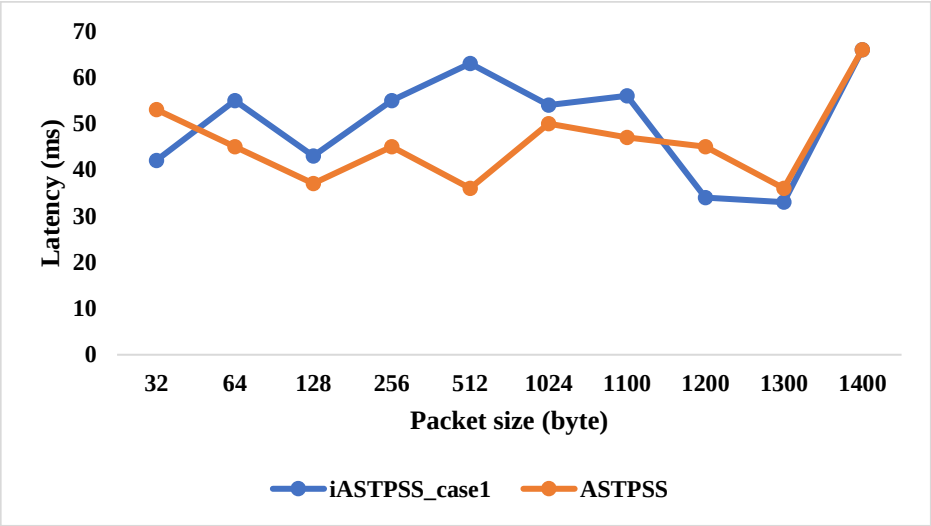


Fig 4.7: Graph of Latency against Packet Size for iASTPSS_case1 and ASTPSS through the IPsec Tunnel

iASTPSS_case1 as shown from the graph had a higher latency than ASTPSS though, these values equalled at the end of packet injection. This was as a result of the computational overhead in iASTPSS_case1 as they were both configured with the same protocol for packet routing.

4.4.1.3 iASTPSS_case1 and ASTPS comparison in terms of RTT from the IPsec tunnel

Finally, RTT which is the time it takes for a packet to travel through the network from the source to the destination and back to the source were also captured and analysed. Fig 4.8 presents these in a graphical and the tabular results was shown in Appendix M.

.

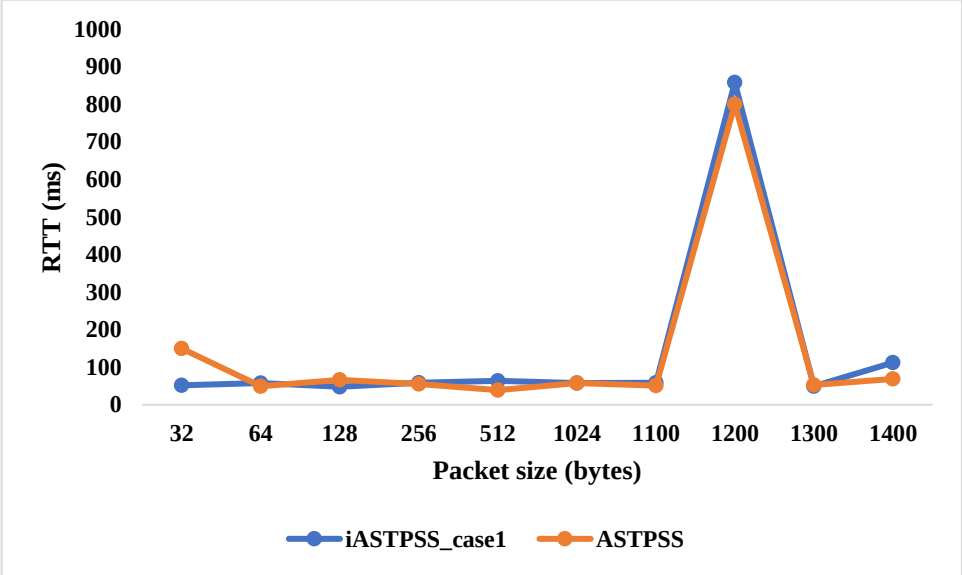


Fig 4.8: Graphical Output of RTT against Packet Size for iASTPSS_case1 and ASTPSS

It can be deduced from the graph that iASTPSS_case1 has a higher RTT than ASTPSS.

From the foregoing results therefore, it could be concluded that, although, ASTPSS outperformed iASTPSS_case1 in all network performance metrics considered, but, it was not something to rejoice over as it came at the cost of security which iASTPSS_case1

provided thus making iASTPSS_case1 a better choice for meeting security as a service need for applications than ASTPSS in spite of the better network performance.

4.4.2 iASTPSS_case1 and iASTPSS_case2 results comparison and analysis

The results from iASTPSS_case1 and iASTPSS_case2 were presented in Tables 4.2 and 4.3 respectively. In the following sections, the network performance of these schemes were discussed with respect to throughput, latency, and RTT.

4.4.2.1 iASTPSS_case2 and iASTPSS_case1 comparison using throughput

Fig 4.9 presents the throughput values and graphical presentation for the two network scenarios. iASTPSS_case2 represents values from the network using OSPF as routing protocol while iASTPSS_case1 represents a network using RIPv2 as routing protocol. The tabular result was shown in Appendix N.

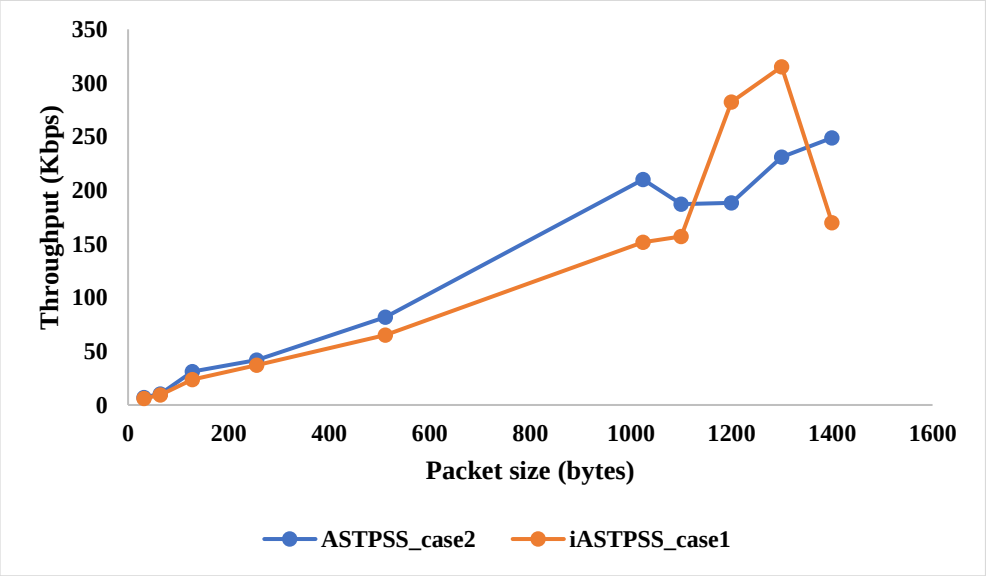


Fig 4.9: Graph of throughput against packet size for iASTPSS_case2 and iASTPSS_case1 from the IPsec Tunnel

From the graph, iASTPSS_case2 has a steady and better throughput than iASTPSS_case1 from the beginning of packet injection until the end.

4.4.2.2 iASTPSS_case2 and iASTPSS_case1 comparison using latency

The latency of both networks were also compared and analysed as shown in Fig. 4.10. As expected, iASTPSS_case2 produced a lower latency than iASTPSS_case1 from the beginning to the end of packet injection in spite of the same encryption type on both networks. The tabular result was shown in Appendix O.

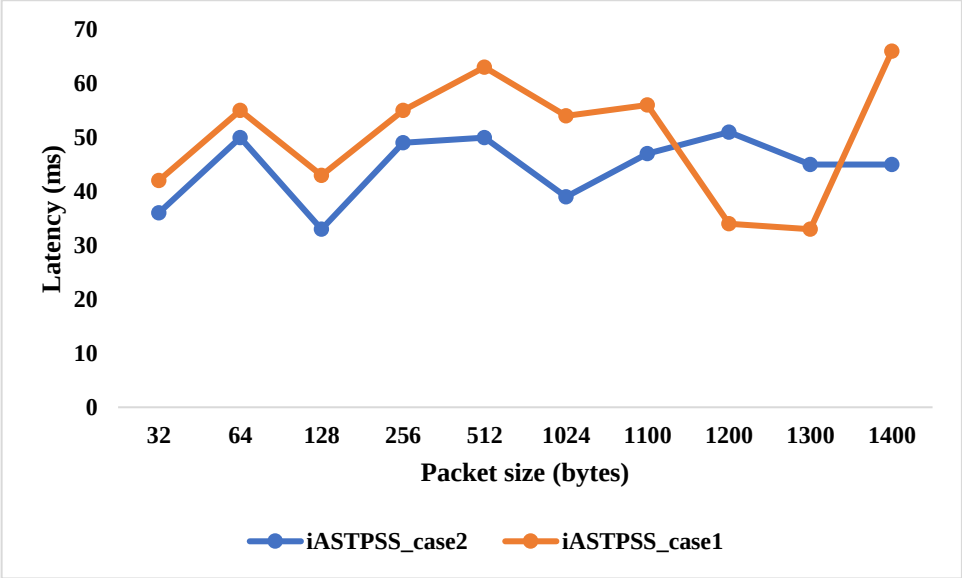


Fig 4.10 Graph of Latency against Packet Size for iASTPSS_case2 and iASTPSS_case1 from the IPsec Tunnel

4.4.2.3 Comparison of iASTPSS_case2 and iASTPSS_case1 using RTT

Finally, the RTT was also compared and analysed for both networks as presented in Fig. 4.11. The tabular result was shown in Appendix P.

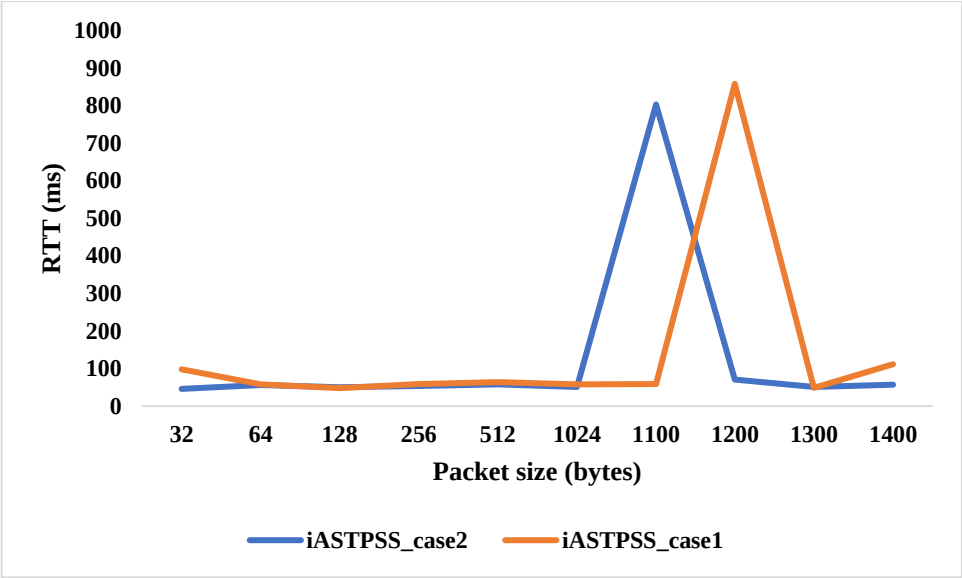


Fig 4.11: Graph of RTT against Packet Size for iASTPSS_case2 and iASTPSS_case1 from the IPsec Tunnel

Form the results presented, it could be stated that iASTPSS_case1 had a higher RTT than iASTPSS_case2. Conclusively, it could be said that for all metrics considered, iASTPSS_case2 outperformed iASTPSS_case1. iASTPSS_case2 does not only guarantee better security but it also had a better network performance over iASTPSS_case1.

4.4.3 Results comparison and analysis from the GRE tunnel

Just like section 4.3.1, the throughput, latency, and RTT values from the GRE tunnel for both iASTPSS and ASTPSS were compared and analysed in this section. In addition, the analysis was done based on networks configured with RIPv2 and OSPF routing protocols. This was because no change in values occurred when RIPv2, the routing protocol in the base work was configured on the new scheme.

4.4.3.1 iASTPSS and ASTPS comparison and analysis in terms of throughput

The GRE tunnel was configured on a separate network thus having its throughput values distinct from that on the IPsec tunnel. Fig. 4.12 presented the throughput values from the GRE tunnels of iASTPSS and ASTPSS. The tabular result was shown in Appendix Q

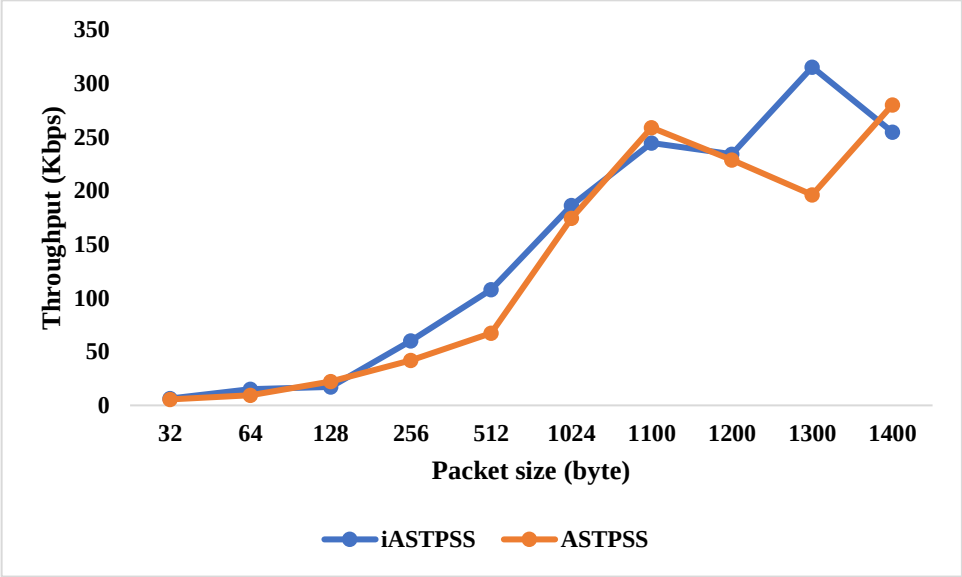


Fig 4.12: Graph of Throughput against Packet Size for iASTPSS and ASTPSS from the GRE Tunnel

From the graph, it can be inferred that iASTPSS has a better throughput than ASTPSS as the throughput values of the iASTPSS network gave a steady rise until the last byte when it experienced a descent but this was not abysmal.

4.4.3.2 iASTPSS and ASTPS comparison and analysis in terms of latency

The latency values from both networks were compared and analysed as shown in Fig. 4.13. iASTPSS showed to have a lower latency than ASTPSS. The latency of a network impacts greatly on the network throughput and hence the bandwidth. Although, iASTPSS had a higher latency than ASTPSS at initial packet injection, this nosedived as packet size increased and iASTPSS maintained a lower latency even as packet approaches MTU. One reason ASTPSS produced a lower latency value than iASTPSS at initial packet injection was due to the fact that, RIP, using hop count runs faster than OSPF on a network with

few hop counts as was in this case. However, as packet size increased, OSPF outperformed RIP irrespective of the number of routers as it was in this case. The tabular result was shown in Appendix R

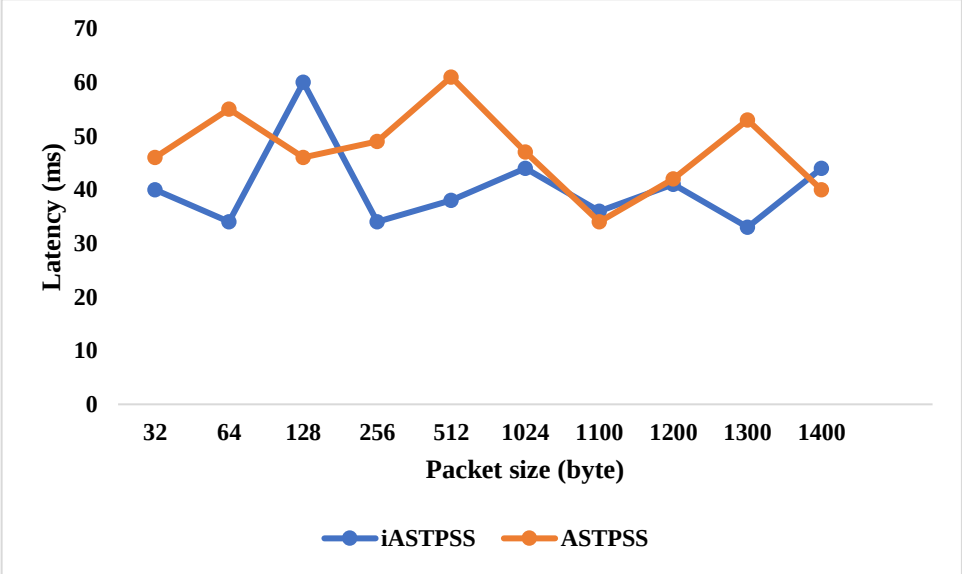


Fig 4.13: Graph of Latency against Packet Size for iASTPSS and ASTPSS in GRE Tunnel

4.4.3.3 iASTPSS and ASTPS comparison and analysis in terms of RTT

Lastly, for the GRE tunnel, the RTT for both networks were analysed and this was presented in Fig. 4.14. ASTPSS had a higher RTT than iASTPSS. It can be inferred from the foregoing that for bandwidth and time sensitive applications such as VOIP, video conferencing, iASTPSS is a better option over ASTPSS. The tabular result was shown in Appendix S

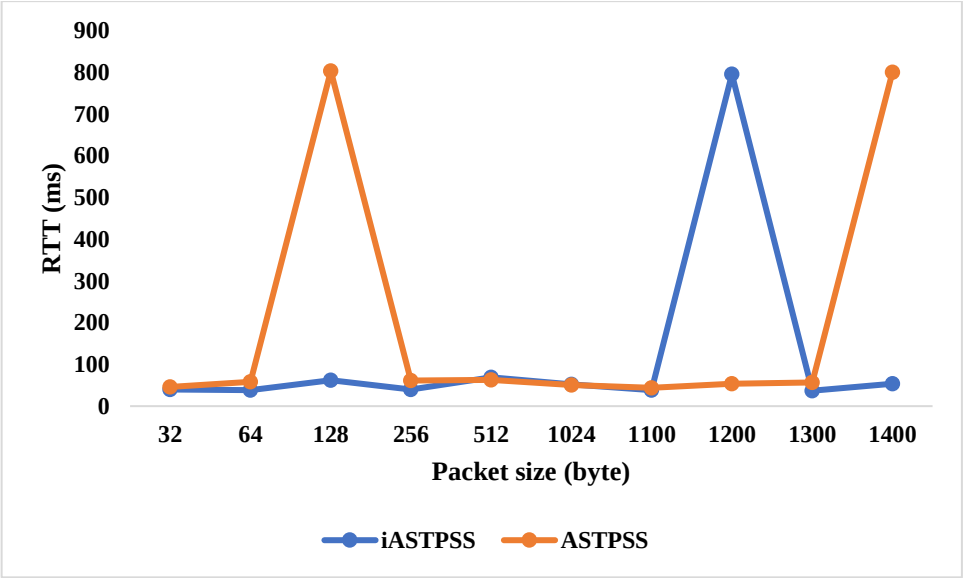


Fig 4.14: Graph of RTT against Packet Size for iASTPSS and ASTPSS from the GRE Tunnel

4.5 Performance Percentage Improvement of iASTPSS over ASTPS

The performance measurement of the improvement of iASTPSS_case1 over ASTPSS was measured using Equation (3.1). This was achieved by taking the average of each performance metrics considered in both network scenarios for both tunnels. Tables 4.6 and 4.7 present these results. Equation (3.2) was used to measure the performance of iASTPSS_case2 and iASTPSS_case1 as shown in Table 4.8.

Table 4.6: Percentage Performance Improvement of ASTPS and iASTPSS_case1

Performance Metrics	**iASTPSS_case1**	**ASTPS**	**% Improvement**
Average Throughput	121.751	122.618	-0.712%
Average Latency	50.1	46.0	8.184%
Average RTT	141.7	139.0	1.905%

It could be seen from Table 4.6 that the throughput of ASTPSS improved over iASTPSS_case1 by 0.712%, a reduction in latency and RTT by 8.184% and 1.905%

respectively. This trade off of performance for security in iASTPSS was due to the encryption and hashing algorithms used in iASTPSS_case1.

Table 4.7: Percentage Improvement of iATPSS over ASTPS in the GRE Tunnel

Performance Metrics	**iASTPSS**	**ASTPS**	**% Improvement**
Average Throughput	144.102	128.4	10.896%
Average Latency	40.4	47.3	-17.079%
Average RTT	122.5	203.7	- 66.286%

It could be seen from Table 4.7 that the throughput of iASTPSS from the GRE tunnel improved over ASTPS by 10.896%, with a corresponding reduction in latency and RTT values of 17.079% and 66.286% respectively.

Table 4.8: Percentage Improvement of iATPSS_case2 over iASTPSS_case1 in the IPsec Tunnel

Performance Metrics	**iASTPSS_case2**	**iASTPSS_case1**	**% Improvement**
Average Throughput	123.762	121.752	1.62%
Average Latency	44.5	50.1	- 12.58%
Average RTT	129.7	141.7	- 9.25%

In the final analysis, iASTPSS_case2 from the IPsec tunnel had an improved network performance and security. An improvement of 1.62% in throughput over iASTPSS_case1 with a corresponding reduction of 12.58% in latency, and 9.25% in RTT was achieved. Therefore, iASTPSS_case2 offered a better platform for applications that required not just security, but also bandwidth and time sensitivity as a service over iASTPSS_case1.

CHAPTER FIVE

CONCLUSION AND RECOMMENDATION

5.1 Summary

Over the years, works done on VPN tunnelling protocols deployment were centred on the technology involved, areas of deployment with little attention to deployment based on organizational application requirements. However, it is necessary to consider deploying VPN tunnelling protocols based on the latter than the former. The main benefit of deploying VPN on a network aside cost saving and scalability is security. This security must in no wise be compromised for any reason and at whatever cost. Also, the choice of the tunnelling protocol to be deployed must align with application requirements so as not to create extra vulnerability in the network or increase network overhead.

5.2 Conclusion

This research developed iASTPSS for site to site VPN requiring security, bandwidth and time sensitivity as a service to applications.

The emulated ASTPSS set up in GNS3 was configured for security, bandwidth and time sensitivity as applications requirements using IPsec and GRE as tunnelling protocols. In the IPsec tunnel configured with 3DES and MD5 and using RIPv2 as routing protocol, ASTPSS outperformed iASTPSS in throughput, latency, and RTT due to the computational overhead in encryption from iASTPSS but underperformed iASTPSS in the GRE tunnel.

The developed iASTPSS in GNS3 was configured for security, bandwidth and time sensitivity as applications requirement using IPsec and GRE tunnelling protocols. The developed scheme in the IPsec tunnel configured with AES256 and SHA256, first, with RIPv2 as routing protocol, and then, with OSPF as routing protocol, had a better security

over the existing scheme with improved network performance. A 1.62% improvement in throughput with a corresponding reduction in latency, and RTT values of 12.58%, and 9.25% respectively was achieved in the final analysis. Similarly, in the GRE tunnel, iASTPSS outperformed ASTPSS with a 10.90% improvement in throughput and a corresponding reduction in latency and RTT values by 17.08%, and 66.29% respectively.

5.3 Significant Contributions

The significant contributions of this work to knowledge include the following

a) Development of an improved application specific tunnelling protocol selection scheme for site to site VPN with a better throughput, latency and RTT over existing systems that meets the security, bandwidth and time sensitivity requirements of applications for an application specific VPN.
b) The developed iASTPSS in the IPsec tunnel achieved a performance improvement of 1.62% in throughput with a corresponding reduction in latency and RTT values by 12.58%, and 9.25% respectively.
c) Also, the developed iASTPSS in the GRE tunnel achieved a performance improvement of 10.90% in throughput, 17.08% and 66.29% reduction in latency and RTT respectively.

5.4 Recommendations for Further Work

The under-listed are recommendations for further work

a) Implement on live network environment to exceed MTU for both tunnels and consider tunnel behaviour at higher packet injection when MTU is exceeded
b) Considering security, scalability and bandwidth as application requirements on four sites, deploy IPsec and MPLS tunnelling protocols to meet these requirements.

REFERENCES

Akamai Kaduk, B., & Short, M. (2018). Deprecate Triple-DES (3DES) and RC4 in Kerberos (pp. Pp 1-10): Internet Engineering Task Force (IETF)

Akinola, A. P., & Zhang, C. (2012). *Tunnel comparison between Generic Routing Encapsulation (GRE) and IP Security (IPSec).* (Project), Halmstad University, Hogskolan Halmstad.

Alharbi, A., Bahnasse, A., & Talea, M. (2017). A Comparison of VoIP Performance Evaluation on different environments Over VPN Multipoint Network. *International Journal of Computer Science and Network Security (IJCSNS), 17*(4), 123.

Alshalan, A., Pisharody, S., & Huang, D. (2016). A survey of mobile VPN technologies. *IEEE Communications Surveys & Tutorials, 18*(2), 1177-1196.

Asadi Eskandar, A., R. Syed, M., & Zarei.M, B. (2015). Performance Analysis of VOIP over GRE Tunnel. *International Journal of Computer Network and Information Security, 7*(12), 1-9. doi: 10.5815/ijcnis.2015.12.01

Barker, E., Feldman, L., & Witte, G. (2017). Information Technology Laboratory Guidance on Triple Data Encryption Algorithm Block Ciphers. *National Institute of Standards and Technology, 2*(800-67), 4.

Bensalah, F., El Kamoun, N., & Bahnasse, A. (2017). Analytical Performance and Evaluation of the Scalability of Layer 3 Tunneling Protocols: Case of Voice Traffic Over IP. *International Journal of Computer Science and Network Security (IJCSNS), 17*(4), 361.

Boney, J. (2005). *Cisco IOS in a nutshell: a desktop quick reference for IOS on IP networks*: " O'Reilly Media, Inc.".

Canavan, J. E. (2001). *Fundamentals of network security*: Artech House.

Chawla., B. K., Gupta., O. P., & Sawhney, B. K. (2014). A Review on IPSec and SSL VPN. *International Journal of Scientific and Engineering Research, 5*(11), 21-24.

Degefa, R. T. (2015). VPN Scenarios, Configuration and Analysis.

Deshmukh, D., & Iyer, B. (2017). *Design of IPSec virtual private network for remote access.* Paper presented at the International Conference on Computing, Communication and Automation (ICCCA), 2017

Dev, J. A. (2013). *Usage of botnets for high speed md5 hash cracking.* Paper presented at the Third International Conference on Innovative Computing Technology (INTECH), 2013

Dhall, H., Dhall, D., Batra, S., & Rani, P. (2012). *Implementation of IPSec protocol.* Paper presented at the Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on Advanced Computing & Communication Technologies.

Donahue, G. (2007). *Network warrior*: " O'Reilly Media, Inc.".

Eichlseder, M., Mendel, F., & Schläffer, M. (2014). *Branching heuristics in differential collision search with applications to SHA-512.* Paper presented at the International Workshop on Fast Software Encryption.

Elezi, M., & Raufi, B. (2015). Conception of Virtual Private Networks using IPsec suite of protocols, comparative analysis of distributed database queries using different IPsec modes of encryption. *Procedia-Social and Behavioral Sciences, 195*, 1938-1948.

Fcmi, S. N. H., & Hadi, A. H. A. (2013). The Impact Of Using Security Protocols In Dedicated Private Network And Virtual Private Network. *International Journal of Scientific & Technology Research, 2*(11), 170-175.

García, D. F. (2015). *Performance Evaluation of Advanced Encryption Standard Algorithm.* Paper presented at the 2015 Second International Conference on Mathematics and Computers in Sciences and in Industry (MCSI), .

Gokulakrishnan, J., & Bai, D. V. T. (2014). A SURVEY REPORT ON VPN SECURITY & ITS TECHNOLOGIES. *Indian Journal of Computer Scienceand Engineering (IJCSE), 5*(4).

Gupta, P., & Kumar, S. (2014). A Comparative Analysis of SHA and MD5 Algorithm. *Indian Journal of Computer Science and Information Technologies (IJCSIT), Vol.5(3),* 4.

Haidar, A. H., & Houseni, M. (2016). The Difference Impact on QoS Parameters between the IPSEC and L2TP. *International Journal of Innovative Research in Advanced Engineering (IJIRAE), 3*(11), 31-42.

Ismoyo, D. D., & Wardhani, R. W. (2016). *Block cipher and stream cipher algorithm performance comparison in a personal VPN gateway.* Paper presented at the Technology of Information and Communication (ISemantic), International Seminar on Application for Technology of Information and Communication.

Jahan, S., Rahman, M. S., & Saha, S. (2017). *Application specific tunneling protocol selection for Virtual Private Networks.* Paper presented at the International Conference on Networking, Systems and Security (NSysS), 2017.

Kabir, M. H., Islam, S., Hossain, M. J., & Hossain, S. (2014). Detail Comparison of Network Simulators. *International Journal of Scientific & Engineering Research, Vol 5*(Issue 10), 203-218. doi: October - 2014

Krithikaa, M., Priyadharsini, M., & Subha, C. (2016). Virtual Private Network - A Survey. *International Journal of Trend in Research and Development, 3*(1), 78-81.

Lakbabi, A., Orhanou, G., & El Hajji, S. (2012). *VPN IPSEC & SSL technology Security and management point of view.* Paper presented at the Next Generation Networks and Services (NGNS), 2012.

Lammle, T. (2004). *CCNA: Cisco Certified Network Associate Study Guide* (pp. 652).

Lammle, T. (2011). *CCNA Cisco Certified Network Associate Deluxe Study Guide*: John Wiley & Sons.

Lammle, T. (2013). *CCNA Routing and Switching Study Guide: Exams 100-101, 200-101, and 200-120*: John Wiley & Sons.

Lu, J., & Dong, C. (2011). *Study on the application of VPN technology based on IPSec in the modern universities.* Paper presented at the IEEE 2nd International Conference on Software Engineering and Service Science (ICSESS), 2011

Mao, H., Zhu, L., & Qin, H. (2012). *A comparative research on SSL VPN and IPSec VPN.* Paper presented at the 8th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), 2012.

Mimoso, M. (2014). Targeted Attack Uses Heartbleed to Hijack VPN Sessions. Retrieved from https://threatpost.com/targeted-attack-uses-heartbleed-to-hijack-vpn-sessions/105567/

Monika, S. K. (2013). Mitigating DoS Attack in VPN. *Internatioonal Journal of Computer Trends and Technology (IJCTT), Vol-4*(5-Month), 1192-1195.

Narayan, S., Williams, C. J., Hart, D. K., & Qualtrough, M. W. (2015). *Network performance comparison of VPN protocols on wired and wireless networks.* Paper presented at the International Conference on Computer Communication and Informatics (ICCCI), 2015

Neumann, J. C. (2015). *The Book of GNS3: Build Virtual Network Labs Using Cisco, Juniper, and More*: No Starch Press.

Padhiar, S., & Verma, P. (2015). A Survey on Performance Evaluation of VPN on Various Operating System. *International Journal of Engineering Development and Research (IJEDR), 3*(4), 516-519.

Patil, P., Narayankar, P., Narayan, D., & Meena, S. M. (2016). A comprehensive evaluation of cryptographic algorithms: DES, 3DES, AES, RSA and Blowfish. *Procedia Computer Science, 78*, 617-624.

Sachin, M., & Kumar, D. (2010). Implementation and Analysis of AES, DES and Triple DES on GSM Network. *IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.1*, 6.

Shanta, J. V. (2012). Evaluating the performance of Symmetric Key Algorithms: AES (Advanced Encryption Standard) and DES (Data Encryption Standard). *published in IJCEM International Journal of Computational Engineering & Management, 15*(4), 43-49.

Shrivastava, A., & Rizvi, M. (2014). Analysis and Comparison of major mechanisms implementing Virtual Private Networks. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), 3*(7), 2374-2381.

Shuai, S., Guowei, D., Tao, G., Tianchang, Y., & Chenjie, S. (2014). *Modelling analysis and auto-detection of cryptographic misuse in android applications.* Paper presented at the 2014 IEEE 12th International Conference on Dependable, Autonomic and Secure Computing (DASC), .

Singh, A. K., Samaddar, S. G., & Misra, A. K. (2012). *Enhancing VPN security through security policy management.* Paper presented at the Recent Advances in Information Technology (RAIT), 2012 1st International Conference on.

Singh, M. K., Argawal, H., & Saini, P. (2016). Performance Comparison of GNS3 and VYATTA Routers Using Nmap. *MIT International Journal of Computer Science and Information Technology, 6*(2), 63-71.

Sivakumar, R., Balakumar, B., & Pandeeswaran, V. A. (2018). A Study of Encryption Algorithms (DES, 3DES and AES) for Information Security.

Soliman, J. N., Mageed, T. A., & El-Hennawy, H. M. (2017). *Digital Signature and Authentication Mechanisms Using New Customized Hash Function for Cognitive Radio Networks.* Paper presented at the 12th International Conference on Computer Engineering and Systems (ICCES), 2017

Sotirov, A., Stevens, M., Appelbaum, J., Lenstra, A. K., Molnar, D., Osvik, D. A., & de Weger, B. (2008). *MD5 considered harmful today, creating a rogue CA certificate.* Paper presented at the 25th Annual Chaos Communication Congress.

Stallings, W. (2017). *Cryptography and Network Security* T. J. (Dunkelberger) (Ed.) *Principles and Practice* (pp. 1-767).

Stevens, M., Bursztein, E., Karpman, P., Albertini, A., & Markov, Y. (2017). *The first collision for full SHA-1.* Paper presented at the Annual International Cryptology Conference.

Vennela, G. S., Varun, N. V., Neelima, N., Priya, L. S., & Yeswanth, J. (2018). *Performance Analysis of Cryptographic Algorithms for Cloud Security.* Paper presented at the Proceedings of the 2nd International Conference on Inventive Communication and Computational Technology (ICICCT 2018).

Wahid, M. N. A., Ali, A., Esparham, B., & Marwan, M. (2018). A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention. *J o u r n a l o f C omputer Science Applications and Information Technology*.

Wang, X., Feng, D., Lai, X., & Yu, H. (2004). Collisions for Hash Functions MD4, MD5, HAVAL-128 and RIPEMD. *IACR Cryptology ePrint Archive, 2004*, 199.

Wouters, P., & Bantoft, K. (2006). *Building and Integrating Virtual Private Networks with Openswan: Learn from the Developers of Openswan how to Building Industry-standard, Military-grade VPNs and Connect Them with Windows, Mac OS X, and Other VPN Vendors*: Packt Publishing Ltd.

Xie, T., Liu, F., & Feng, D. (2013). Fast Collision Attack on MD5. *IACR Cryptology ePrint Archive, 2013*, 170.

APPENDIX A

Installation of VMware Workstation Pro 12

Installation steps

i) Download VMware workstation from VMware site, double click on the downloaded file to run
ii) Click ‘agree’ to the License Agreement and click next to continue
iii) Choose an installation path, either of desktop or document and click next
iv) Chose create a desktop shortcut and click next
v) Click install to commence installation process
vi) Either insert the License key or chose to use a trial version for 30-days
vii) Register the product using your email address
viii) Click finish to close the installer

Installation of Ubuntu 14.04 LTS

Installation steps

i) Download the Ubuntu 14.04 LTS OVA for VMware
ii) Store in a preferred location
iii) Start VMware workstation Pro 12
iv) Click on the new Virtual Machine and launch it
v) Navigate to the VM OVA storage location and click open
vi) Set the name or use default
vii) Go to edit, preferences and set the select appropriate memory, network adapter
viii) The VMware turns on automatically whenever the GNS3 software is turned ON

APPENDIX B

Installing GNS3 on the HP Laptop

Installation steps:

i) Download GNS3 for Windows from gns3 website
ii) Download gns3-all-in-one package
iii) Create a gns3 user account
iv) Click on the download to run
v) Agree to the License Agreement
vi) Create a Desktop shortcut
vii) Run in default state or select more features and click next
viii) Choose location to install and click install
ix) This runs for some times, pausing in between to ask permission to either install or not install some features. It continues based on user's response
x) When installation is complete, the click to finish installation message would be displayed, click and finish the installation
xi) Start GNS3

APPENDIX C

Installing GNS3 VM

Installation steps

i) Download GNS3 VM OVA for VMware compatible with the version installed on the HP Laptop
ii) Extract the OVA from the zipped folder
iii) Go to VMware workstation and click open a virtual machine
iv) Go to the file location where the downloaded VM OVA is located
v) Click open to enable installation on the VMware workstation
vi) Leave the name as default
vii) Import file
viii) Upon completion, this would appear in the workstation's library
ix) Go to GNS3 software on HP laptop and import the installed GNS3 VM into it

APPENDIX D

Installing Windows 7 OS

Installation steps

i) Download a Windows7 OVA for VM
ii) Extract the OVA from the zipped folder
iii) Go to VMware workstation and click open a virtual machine
iv) Go to the file location where the downloaded VM OVA is located
v) Click open to enable installation on the VMware workstation
vi) Leave the name as default
vii) Import file
viii) Upon completion, this would appear in the workstation's library
ix) Go to GNS3 software on HP laptop and import the installed Windows7 VM into it

APPENDIX E

ASTPS IPsec codes

a) ISP router codes

```
hostname ISP
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
no ip domain lookup
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
 description LINK-TO-HQ
 ip address 20.0.0.1 255.255.255.252
 duplex full
!
interface FastEthernet1/0
 description LINK-TO-BR
 ip address 20.0.0.5 255.255.255.252
 duplex full
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex full
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex full
```

```
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
router rip
 version 2
 network 20.0.0.0
 no auto-summary
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
End
```

b) HQ router codes

```
hostname HQ
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp excluded-address 192.168.20.1 192.168.20.10
!
ip dhcp pool N1
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 192.168.10.1
!
```

```
ip dhcp pool N2
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 192.168.20.1
!
no ip domain lookup
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
ip tcp synwait-time 5
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 14
 lifetime 36000
crypto isakmp key alice address 20.0.0.6
!
crypto ipsec transform-set TS esp-3des esp-md5-hmac
 mode tunnel
!
crypto map CMAP 10 ipsec-isakmp
 set peer 20.0.0.6
 set security-association lifetime seconds 36000
 set transform-set TS
 set pfs group14
 match address 100
!
interface FastEthernet0/0
 description LINK-TO-ISP
 ip address 20.0.0.2 255.255.255.252
 ip access-group 100 out
 duplex full
 crypto map CMAP
!
interface FastEthernet1/0
 description LINK-T0-SW2
 ip address 192.168.20.1 255.255.255.0
 duplex full
!
interface FastEthernet2/0
 description LINK-TO-SW1
 ip address 192.168.10.1 255.255.255.0
 duplex full
!
interface FastEthernet3/0
```

```
 no ip address
 shutdown
 duplex full
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
router rip
 version 2
 network 20.0.0.0
 network 192.168.10.0
 network 192.168.20.0
 no auto-summary
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
!
access-list 100 permit ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255 eq smtp
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
```

c) BR router codes

```
hostname BR
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip dhcp excluded-address 192.168.30.1 192.168.30.10
ip dhcp excluded-address 192.168.40.1 192.168.40.10
!
ip dhcp pool N3
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 192.168.30.1
!
ip dhcp pool N4
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.1
 dns-server 192.168.40.1
!
no ip domain lookup
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
ip tcp synwait-time 5
!
interface Tunnel0
 ip address 172.16.10.2 255.255.255.252
 ip access-group 100 out
 ip mtu 1400
 ip tcp adjust-mss 1360
 tunnel source 20.0.0.6
 tunnel destination 20.0.0.2
!
interface FastEthernet0/0
 description LINK-TO-ISP
 ip address 20.0.0.6 255.255.255.252
 duplex full
!
interface FastEthernet1/0
 description LINK-TO-SW3
 ip address 192.168.30.1 255.255.255.0
 duplex full
!
interface FastEthernet2/0
```

```
 description LINK-TO-SW4
 ip address 192.168.40.1 255.255.255.0
 duplex full
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex full
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
router rip
 version 2
 network 20.0.0.0
 network 192.168.30.0
 network 192.168.40.0
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 192.168.20.0 255.255.255.0 172.16.10.1
!
access-list 100 permit udp 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
!
 control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
```

```
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
```

APPENDIX F
ASTPS GRE codes

a) ISP router codes

```
hostname ISP
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
 description LINK-TO-HQ
 ip address 20.0.0.1 255.255.255.252
 duplex full
!
interface FastEthernet1/0
 description LINK-TO-BR
 ip address 20.0.0.5 255.255.255.252
 duplex full
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex full
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet6/0
```

```
 no ip address
 shutdown
 duplex full
!
router rip
 version 2
 network 20.0.0.0
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
end
```

b) HQ router codes

```
hostname HQ
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp excluded-address 192.168.20.1 192.168.20.10
!
ip dhcp pool N1
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 192.168.10.1
!
ip dhcp pool N2
```

```
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 192.168.20.1
!
no ip domain lookup
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
ip tcp synwait-time 5
!
interface Tunnel0
 ip address 172.16.10.1 255.255.255.252
 ip access-group 100 out
 ip mtu 1400
 ip tcp adjust-mss 1360
 tunnel source 20.0.0.2
 tunnel destination 20.0.0.6
!
interface FastEthernet0/0
 description LINK-TO-ISP
 ip address 20.0.0.2 255.255.255.252
 duplex full
!
interface FastEthernet1/0
 description LINK-TO-SW2
 ip address 192.168.20.1 255.255.255.0
 duplex full
!
interface FastEthernet2/0
 description LINK-TO-SW1
 ip address 192.168.10.1 255.255.255.0
 duplex full
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex full
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex full
```

```
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
router ospf 101
 network 20.0.0.0 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route 192.168.30.0 255.255.255.0 172.16.10.2
!
access-list 100 permit udp 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
End
```

c) BR router codes

```
hostname BR
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip dhcp excluded-address 192.168.30.1 192.168.30.10
ip dhcp excluded-address 192.168.40.1 192.168.40.10
!
ip dhcp pool N3
```

```
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 192.168.30.1
!
ip dhcp pool N4
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.1
 dns-server 192.168.40.1
!
no ip domain lookup
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
ip tcp synwait-time 5
!
interface Tunnel0
 ip address 172.16.10.2 255.255.255.252
 ip access-group 100 out
 ip mtu 1400
 ip tcp adjust-mss 1360
 tunnel source 20.0.0.6
 tunnel destination 20.0.0.2
!
interface FastEthernet0/0
 description LINK-TO-ISP
 ip address 20.0.0.6 255.255.255.252
 duplex full
!
interface FastEthernet1/0
 description LINK-TO-SW3
 ip address 192.168.30.1 255.255.255.0
 duplex full
!
interface FastEthernet2/0
 description LINK-TO-SW4
 ip address 192.168.40.1 255.255.255.0
 duplex full
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex full
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
```

```
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
router ospf 101
 network 20.0.0.4 0.0.0.3 area 0
 network 192.168.30.0 0.0.0.255 area 0
 network 192.168.40.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 192.168.20.0 255.255.255.0 172.16.10.1
!
access-list 100 permit udp 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
```

APPENDIX G
iASTPSS IPsec codes varying only security algorithms

a) ISP router codes

```
hostname ISP
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
no ip domain lookup
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
ip tcp synwait-time 5
!
!
interface FastEthernet0/0
 description LINK-TO-R2
 ip address 20.0.0.1 255.255.255.252
 duplex full
!
interface FastEthernet1/0
 description LINK-TO-R3
 ip address 20.0.0.5 255.255.255.252
 duplex full
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex full
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
!
interface FastEthernet5/0
 no ip address
 shutdown
```

```
 duplex full
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
router rip
 version 2
 network 20.0.0.0
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
```

b) HR router codes

```
hostname HQ
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip dhcp excluded-address 192.168.10.1 192.168.10.10
```

```
ip dhcp excluded-address 192.168.30.1 192.168.30.10
!
ip dhcp pool N1
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 192.168.10.1
!
ip dhcp pool N3
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 192.168.30.1
!
no ip domain lookup
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
ip tcp synwait-time 5
!
crypto isakmp policy 10
 encr aes 256
 hash sha256
 authentication pre-share
 group 14
crypto isakmp key alice address 20.0.0.6
!
crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
 mode tunnel
!
crypto map CMAP 10 ipsec-isakmp
 set peer 20.0.0.6
 set security-association lifetime seconds 86400
 set transform-set TS
 set pfs group14
 match address 101
!
interface FastEthernet0/0
 description LINK-TO-R1
 ip address 20.0.0.2 255.255.255.252
 ip access-group 101 out
 duplex full
 crypto map CMAP
!
interface FastEthernet1/0
 description LINK-TO-SW1
 ip address 192.168.10.1 255.255.255.0
 duplex full
!
```

```
interface FastEthernet2/0
 description LINK-TO-SW3
 ip address 192.168.30.1 255.255.255.0
 duplex full
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex full
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
router rip
 version 2
 network 20.0.0.0
 network 192.168.10.0
 network 192.168.30.0
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255 eq smtp
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
```

```
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
```

c) BR router codes

```
hostname BR
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip dhcp excluded-address 192.168.20.1 192.168.20.10
ip dhcp excluded-address 192.168.40.1 192.168.40.10
!
ip dhcp pool N2
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 192.168.20.1
!
ip dhcp pool N4
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.1
 dns-server 192.168.40.1
!
no ip domain lookup
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
ip tcp synwait-time 5
!
crypto isakmp policy 10
 encr aes 256
 hash sha256
 authentication pre-share
 group 14
crypto isakmp key alice address 20.0.0.2
!
crypto ipsec transform-set TS esp-aes 256 esp-sha256-hmac
```

```
 mode tunnel
!
crypto map CMAP 10 ipsec-isakmp
 set peer 20.0.0.2
 set security-association lifetime seconds 86400
 set transform-set TS
 set pfs group14
 match address 101
!
interface FastEthernet0/0
 description LINK-TO-R1
 ip address 20.0.0.6 255.255.255.252
 ip access-group 101 out
 duplex full
 crypto map CMAP
!
interface FastEthernet1/0
 description LINK-TO-SW2
 ip address 192.168.20.1 255.255.255.0
 duplex full
!
interface FastEthernet2/0
 description LINK-TO-SW4
 ip address 192.168.40.1 255.255.255.0
 duplex full
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex full
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
router rip
 version 2
 network 20.0.0.0
 network 192.168.20.0
```

```
 network 192.168.40.0
 no auto-summary
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255 eq smtp
!
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
```

APPENDIX H
iASTPSS IPsec codes varying the security algorithms and routing protocol

a) ISP router codes

```
hostname ISP
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
no ip domain lookup
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
ip tcp synwait-time 5
!
!
interface FastEthernet0/0
 description LINK-TO-S1
 ip address 20.0.0.1 255.255.255.252
 duplex full
!
interface FastEthernet1/0
 description LINK-TO-S2
 ip address 20.0.0.5 255.255.255.252
 duplex full
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex full
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
!
interface FastEthernet5/0
 no ip address
```

```
 shutdown
 duplex full
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
router ospf 101
 network 20.0.0.0 0.0.0.3 area 0
 network 20.0.0.4 0.0.0.3 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
```

b) HQ router codes

```
hostname HQ
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip dhcp excluded-address 192.168.30.1 192.168.30.10
ip dhcp excluded-address 192.168.20.1 192.168.20.10
!
```

```
ip dhcp pool N1
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 192.168.30.0
!
ip dhcp pool N2
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 192.168.20.0
no ip domain lookup
!
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
!
ip tcp synwait-time 5
!
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 14
crypto isakmp key alice address 20.0.0.6
!
!
crypto ipsec transform-set TS esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto map CMAP 10 ipsec-isakmp
 set peer 20.0.0.6
 set security-association lifetime seconds 86400
 set transform-set TS
 set pfs group14
 match address 101
!
interface FastEthernet0/0
 description LINK-TO-ISP
 ip address 20.0.0.2 255.255.255.252
 ip access-group 101 out
 duplex full
 crypto map CMAP
!
interface FastEthernet1/0
 description LINK-TO-SW1
 ip address 192.168.20.1 255.255.255.0
 duplex full
!
```

```
interface FastEthernet2/0
 description LINK-TO-SW3
 ip address 192.168.30.1 255.255.255.0
 duplex full
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex full
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
router ospf 101
 network 20.0.0.0 0.0.0.3 area 0
 network 192.168.20.0 0.0.0.255 area 0
 network 192.168.30.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
access-list 101 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255 eq smtp
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
```

```
 stopbits 1
line vty 0 4
 login
!
!
end
```

c) BR router codes

```
hostname BR
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp excluded-address 192.168.40.1 192.168.40.10
!
ip dhcp pool N3
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 192.168.10.0
!
ip dhcp pool N4
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.1
 dns-server 192.168.40.0
!
no ip domain lookup
ip cef
no ipv6 cef
!
!
multilink bundle-name authenticated
!
ip tcp synwait-time 5
!
!
crypto isakmp policy 10
 encr aes 256
 authentication pre-share
 group 14
crypto isakmp key alice address 20.0.0.2
!
!
crypto ipsec transform-set TS esp-aes 256 esp-sha-hmac
 mode tunnel
!
crypto map CMAP 10 ipsec-isakmp
```

```
 set peer 20.0.0.2
 set security-association lifetime seconds 86400
 set transform-set TS
 set pfs group14
 match address 101
!
interface FastEthernet0/0
 description LINK-TO-ISP
 ip address 20.0.0.6 255.255.255.252
 ip access-group 101 out
 duplex full
 crypto map CMAP
!
interface FastEthernet1/0
 description LINK-TO-SW2
 ip address 192.168.10.1 255.255.255.0
 duplex full
!
interface FastEthernet2/0
 description LINK-TO-SW4
 ip address 192.168.40.1 255.255.255.0
 duplex full
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex full
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
router ospf 101
 network 20.0.0.4 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.40.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
```

```
!
no ip http server
no ip http secure-server
!
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255 eq smtp
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
```

APPENDIX I
iASTPSS GRE Codes

a) ISP router codes

```
hostname ISP
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
ip tcp synwait-time 5
!
interface FastEthernet0/0
 description LINK-TO-HQ
 ip address 20.0.0.1 255.255.255.252
 duplex full
!
interface FastEthernet1/0
 description LINK-TO-BR
 ip address 20.0.0.5 255.255.255.252
 duplex full
!
interface FastEthernet2/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex full
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex full
!
```

```
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
router ospf 101
 network 20.0.0.0 0.0.0.3 area 0
 network 20.0.0.4 0.0.0.3 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
!
control-plane
!
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
```

b) HQ router codes

```
hostname HQ
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip dhcp excluded-address 192.168.10.1 192.168.10.10
ip dhcp excluded-address 192.168.20.1 192.168.20.10
!
ip dhcp pool N1
 network 192.168.10.0 255.255.255.0
 default-router 192.168.10.1
 dns-server 192.168.10.1
```

```
!
ip dhcp pool N2
 network 192.168.20.0 255.255.255.0
 default-router 192.168.20.1
 dns-server 192.168.20.1
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
ip tcp synwait-time 5
!
interface Tunnel0
 ip address 172.16.10.1 255.255.255.252
 ip access-group 100 out
 ip mtu 1400
 ip tcp adjust-mss 1360
 tunnel source 20.0.0.2
 tunnel destination 20.0.0.6
!
interface FastEthernet0/0
 description LINK-TO-ISP
 ip address 20.0.0.2 255.255.255.252
 duplex full
!
interface FastEthernet1/0
 description LINK-TO-SW2
 ip address 192.168.20.1 255.255.255.0
 duplex full
!
interface FastEthernet2/0
 description LINK-TO-SW1
 ip address 192.168.10.1 255.255.255.0
 duplex full
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex full
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
!
interface FastEthernet5/0
 no ip address
 shutdown
```

```
 duplex full
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
router ospf 101
 network 20.0.0.0 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.20.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
!
no ip http server
no ip http secure-server
ip route 192.168.30.0 255.255.255.0 172.16.10.2
!
access-list 100 permit udp 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
end
```

c) BR router codes

```
hostname BR
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
!
ip dhcp excluded-address 192.168.30.1 192.168.30.10
ip dhcp excluded-address 192.168.40.1 192.168.40.10
!
```

```
ip dhcp pool N3
 network 192.168.30.0 255.255.255.0
 default-router 192.168.30.1
 dns-server 192.168.30.1
!
ip dhcp pool N4
 network 192.168.40.0 255.255.255.0
 default-router 192.168.40.1
 dns-server 192.168.40.1
!
no ip domain lookup
ip cef
no ipv6 cef
!
multilink bundle-name authenticated
!
ip tcp synwait-time 5
!
interface Tunnel0
 ip address 172.16.10.2 255.255.255.252
 ip access-group 100 out
 ip mtu 1400
 ip tcp adjust-mss 1360
 tunnel source 20.0.0.6
 tunnel destination 20.0.0.2
!
interface FastEthernet0/0
 description LINK-TO-ISP
 ip address 20.0.0.6 255.255.255.252
 duplex full
!
interface FastEthernet1/0
 description LINK-TO-SW3
 ip address 192.168.30.1 255.255.255.0
 duplex full
!
interface FastEthernet2/0
 description LINK-TO-SW4
 ip address 192.168.40.1 255.255.255.0
 duplex full
!
interface FastEthernet3/0
 no ip address
 shutdown
 duplex full
!
interface GigabitEthernet4/0
 no ip address
 shutdown
 negotiation auto
```

```
!
interface FastEthernet5/0
 no ip address
 shutdown
 duplex full
!
interface FastEthernet6/0
 no ip address
 shutdown
 duplex full
!
router ospf 101
 network 20.0.0.4 0.0.0.3 area 0
 network 192.168.30.0 0.0.0.255 area 0
 network 192.168.40.0 0.0.0.255 area 0
!
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route 192.168.20.0 255.255.255.0 172.16.10.1
!
access-list 100 permit udp 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
!
control-plane
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
```

APPENDIX J
Experimental procedure for ASTPS and iASTPSS

The following steps led to the successful implementation of ASTPS

i) Design the desired network topology
ii) Configure basic device settings such as cabling, host names, interface IDs,
iii) Configure RIP v2 routing protocol on all 3-routers for ASTPS
iv) Configure RIP and OSPF routing protocol on all routers for iASTPSS for both iASTPSS stage 1 and stage 2 respectively
v) Configure PC host IP settings using dynamic host configuration protocol (DHCP) on HQ and BR routers
vi) Configure and encrypt passwords on all routers
vii) Save basic configs for all routers using the *write* command in the CLI
viii) Based on i) – vi), verify connectivity between the networks of interest using the ping request
ix) Configure the GRE tunnel on network 172.16.10.0/30 between the outgoing interface of HQ and BR routers respectively
x) Configure IPsec tunnel on networks N2 and N3
xi) In ISAKMP phase 1 and 2, use 3des, md5 for encryption and hash for ASTPS
xii) In ISAKMP phase 1 and 2, use AES256, SHA256 for encryption and hash for iASTPSS in both stages 1 and 2
xiii) Configure the transform set and set the key lifetime in seconds
xiv) Create and apply extended access control list to the outgoing interface on the HQ and BR routers respectively
xv) Create and apply a crypto map on the outgoing interface of the HQ and BR routers
xvi) If it is properly configured, upon application of the crypto map, ISAKMP turns ON
xvii) Verify the tunnels
xviii) If the ping returns an ICMP message successfully, the tunnels are up else diagnose.
xix) Using throughput, latency and RTT, analyse the two networks and validate iASTPSS against ASTPS
xx) Display results

.

Appendix K

Throughput Comparison of iASTPSS_case1 and ASTPS

S/N	Packet Size (Bytes)	Throughput (Kb/s)	
		iASTPSS_case1	ASTPS
1	32	6.095	4.830
2	64	9.309	11.387
3	128	23.814	27.676
4	256	37.236	45.511
5	512	65.016	113.778
6	1024	151.704	163.840
7	1100	157.143	187.234
8	1200	282.353	213.333
9	1300	315.152	288.889
10	1400	169.697	169.697

Appendix L

Latency Comparison of iASTPSS_case1 and ASTPS

S/N	Packet Size (Bytes)	Latency (ms)	
		iASTPSS_case1	**ASTPS**
1	32	42	53
2	64	55	45
3	128	43	37
4	256	55	45
5	512	63	36
6	1024	54	50
7	1100	56	47
8	1200	34	45
9	1300	33	36
10	1400	66	66

Appendix M

RTT Comparison for iASTPSS_case1 and ASTPS

S/N	Packet Size (Bytes)	RTT (ms)	
		iASTPSS_case1	ASTPS
1	32	52	150
2	64	58	49
3	128	48	66
4	256	59	55
5	512	64	39
6	1024	58	58
7	1100	59	51
8	1200	858	800
9	1300	49	53
10	1400	112	69

Appendix N

Throughput Comparison of iASTPSS_case2 and iASTPSS_case1

S/N	Packet Size (Bytes)	Throughput (Kb/s)	
		iASTPSS_case2	iASTPSS_case1
1	32	7.111	6.095
2	64	10.240	9.309
3	128	31.030	23.814
4	256	41.796	37.236
5	512	81.920	65.016
6	1024	210.051	151.704
7	1100	187.234	157.143
8	1200	188.235	282.353
9	1300	231.111	315.152
10	1400	248.889	169.697

Appendix O

Comparison of iASTPSS_case1 and iASTPSS_case2 using Latency

S/N	Packet Size (Bytes)	Latency (ms)	
		iASTPSS_case2	iASTPSS_case1
1	32	36	42
2	64	50	55
3	128	33	43
4	256	49	55
5	512	50	63
6	1024	39	54
7	1100	47	56
8	1200	51	34
9	1300	45	33
10	1400	45	66

Appendix P

Comparison of iASTPSS_case2 and iASTPSS_case1 using RTT

S/N	Packet Size (Bytes)	RTT (ms)	
		iASTPSS_case2	iASTPSS (i)
1	32	46	52
2	64	56	58
3	128	50	48
4	256	54	59
5	512	58	64
6	1024	51	58
7	1100	803	59
8	1200	71	858
9	1300	51	49
10	1400	57	112

Appendix Q

Throughput Comparison for iASTPSS and ASTPS from the GRE Tunnel

S/N	Packet Size (Bytes)	Throughput (Kb/s)	
		iASTPSS	ASTPS
1	32	6.400	5.565
2	64	15.059	9.309
3	128	17.067	22.261
4	256	60.235	41.796
5	512	107.789	67.148
6	1024	186.182	174.298
7	1100	244.444	258.824
8	1200	234.146	228.571
9	1300	315.152	196.226
10	1400	254.545	280.000

Appendix R

GRE Tunnel Latency Values for iASTPSS and ASTPS

S/N	Packet Size (Bytes)	Latency (ms)	
		iASTPSS	**ASTPS**
1	32	40	46
2	64	34	55
3	128	60	46
4	256	34	49
5	512	38	61
6	1024	44	47
7	1100	36	34
8	1200	41	42
9	1300	33	53
10	1400	44	40

Appendix S

GRE Tunnel RTT Values for iASTPSS and ASTPS

S/N	Packet Size (Bytes)	RTT (ms)	
		iASTPSS	ASTPS
1	32	40	46
2	64	38	58
3	128	62	803
4	256	40	61
5	512	69	63
6	1024	52	51
7	1100	38	44
8	1200	795	54
9	1300	37	57
10	1400	54	800