



**ANALYSIS AND IMPLEMENTATION OF REMOTE ACCESS COMPUTER
COMMUNICATION**

MOUATH SALIM

AUGUST 2015

**ANALYSIS AND IMPLEMENTATION OF REMOTE ACCESS COMPUTER
COMMUNICATION**

**A THESIS SUBMITTED TO
THE GRADUATE SCHOOL OF NATURAL AND APPLIED
SCIENCES OF
ÇANKAYA UNIVERSITY**

**BY
MOUATH SALIM**

**IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE
DEGREE OF
MASTER OF SCIENCE
IN
THE DEPARTMENT OF
ELECTRONIC AND COMMUNICATION ENGINEERING**

AUGUST 2015

Title of the Thesis: Analysis and Implementation of Remote Access Computer Communication.

Submitted by **Mouath Salim**

Approval of the Graduate School of Natural and Applied Sciences, Çankaya University.



Prof. Dr. Taner ALTUNOK

Director

I certify that this thesis satisfies all the requirements as a thesis for the degree of Master of Science.



Prof. Dr. Halil T. EYYUBOĞLU

Head of Department

This is to certify that we have read this thesis and that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.



Assist. Prof. Dr. Barbaros PREVEZE
Supervisor

Examination Date: 12.08.2015

Examining Committee Members

Assist. Prof. Dr. Barbaros PREVEZE

(Çankaya Univ.)



Asst. Prof. Dr. Göker ŞENER

(Çankaya Univ.)



Assoc. Prof. Dr. Fahd JARAD

(UTAA)



STATEMENT OF NON-PLAGIARISM PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name: MOUATH ABDALRAHMAN

Signature

: 

Date

:12.08.2015

ABSTRACT

ANALYSIS AND IMPLEMENTATION OF REMOTE ACCESS COMPUTER COMMUNICATION

ABDALRAHMAN, Mouath

M.Sc. Department of Electronic And Communication Engineering

Supervisor: Assist. Prof. Dr. Barbaros PREVEZE

August 2015, 56 pages

In this thesis three different kinds of Remote Access Virtual Private Network protocols (PPTP,SSL, and L2TP/IPsec) has been established virtually using VMware and GNS3 tools. In addition, various measure tests has been applied to test the performance of each protocol under similar conditions. Moreover, the test results studied carefully to make a comparison and to figure out the conclusion and advices for future works.

Keywords: VPN, PPTP, L2TP/IPsec, SSL.

ÖZ

ANALİZ VE UZAKTAN ERİŞİM BİLGİSAYAR İLETİŞİM UYGULAMA

ABDALRAHMAN, Mouath

Yüksek Lisans, Elektronik ve Haberleşme Mühendisliği Anabilim Dalı

Tez Yöneticisi: Y. Doç Dr. Barbaros PREVEZE

Ağustos 2015, 56 sayfa

Bu tezde uzaktan erişimli Sanal Özel ağ protokollerinin (PPTP,SSL, ve 2TP/IPsec) üç farklı tipi VMware ve GNS3 araçlarının kullanımı ile sanal olarak kurulmuştur. Buna ek olarak tüm protokollere benzer koşullar altında yapılan ölçüm testleri ile performansları test edilmiştir. Ayrıca, elde edilen bu sonuçlar, bir sonuca varılarak kıyaslama yapılabilmesi ve gelecek çalışmalara öneriler getirebilmesi için dikkatle çalışılmıştır.

Anahtar Kelimeler: VPN, PPTP, L2TP/IPsec, SSL.

ACKNOWLEDGEMENTS

First of all, I am thanking God for guiding me and helping me in all my life. Then I would like to express my sincere gratitude to assist. Prof. Dr. Barbaros PREVEZE for his supervision, special guidance, suggestions, and encouragement through the development of this thesis. A special thanks for my parents, words cannot express how grateful I am to my mother, and my father who tired a lot to make me what I am today. It is a pleasure to express my special thanks to my beloved wife for her valuable support and sacrifices, in addition to my sisters, and my friends who supported me and helped me to complete this work.

TABLE OF CONTENTS

STATEMENT OF NON PLAGIARISM.....	Ii
ABSTRACT.....	Iv
ÖZ.....	V
ACKNOWLEDGEMENTS.....	Vi
TABLE OF CONTENTS.....	Vii
LIST OF FIGURES.....	X
LIST OF TABLES.....	Xii
LIST OF ABBREVIATIONS.....	Xiii

CHAPTERS:

1. INTRODUCTION.....	1
1.1. Background.....	1
1.2. Study Motivation	2
1.3. Problem Statement.....	2
1.4. Aim And Objectives.....	3
1.5. Thesis Overview.....	3
2. WHAT IS VPN?.....	5
2.1. Overview.....	5
2.2. Common VPN Scenarios.....	6
2.2.1. Site-To-Site Connection.....	6
2.2.2. Client-To-Site VPN.....	7
2.2.3. Extranet VPN Scenario.....	8
2.3. VPN Security Policy.....	9
2.4. Tunneling Concept.....	10
2.5. Tunnel Types.....	11
2.5.1. Voluntary Tunnels.....	11

2.5.2.	Compulsory Tunnels.....	12
3.	PROTOCOLS OF VIRTUAL PRIVATE NETWORK.....	13
3.1.	VPN Protocols.....	13
3.1.1.	PPTP (Point-to-Point Tunneling Protocol).....	13
3.1.2.	L2TP (Layer 2 Tunneling Protocol)	14
3.1.3.	Ipssec(IP security protocols).....	15
3.1.4.	SSL/TLS (Secure Socket Layer/Transport Layer Security).....	16
4.	VPN PARAMETER AND TESTING TOOLS.....	17
4.1.	VPN Characteristics.....	17
4.1.1.	Round Trip Time (RTT).....	17
4.1.2.	Throughput.....	17
4.1.3.	Bandwidth.....	18
4.1.4.	Jitter.....	18
4.1.5.	Packet loss.....	18
4.2.	Tools used in test.....	19
4.2.1.	JPerf and Iperf.....	19
4.2.2.	Netperf.....	20
4.2.3.	Ping	21
4.2.4.	Wireshark.....	22
5.	NETWORK ESTABLISHMENT.....	24
5.1.	GNS3.....	24
5.1.1.	Overview.....	24
5.1.2.	Supported GNS3 Features.....	25
5.2.	VMware.....	25
5.2.1.	Virtualization technology.....	26
5.2.2.	VMware Virtualization.....	26
5.3.	VPN Establishment.....	27
5.3.1.	Overview.....	27
5.3.2.	Cisco ASA (Adaptive Security Appliance).....	27

5.3.3.	Initializing Work Environment.....	28
5.4.	Establishing PPTP VPN network using virtual lab.....	30
5.5.	Establishing SSL VPN network using virtual lab.....	34
5.6.	Establishing L2TP/IPsec VPN network using virtual lab.....	36
6.	RESULTS.....	39
6.1.	Overview.....	39
6.2.	Test Result	39
6.2.1.	Jperf and Iperf Bandwidth Results.....	39
6.2.2.	Ping RTT Results.....	44
7.	DISCUSSION.....	46
7.1.	Bandwidth and throughput comparison between SSL, PPTP, L2TP/ipsec.	46
7.1.1.	UDP Throughput.....	48
7.2.	RTT comparison between SSL, PPTP, L2TP.....	50
8.	CONCLUSION AND FUTURE WORK.....	54
8.1.	Overview.....	54
8.2.	Security In Vpn.....	54
8.3.	Future Work.....	55
	REFERENCES.....	R1
	APPENDICES.....	A1
A.	CURRICULUM VITAE.....	A1

LIST OF FIGURES

FIGURES

Figure 1	Site To Site VPN	7
Figure 2	Remote access VPN	7
Figure 3	Extranet VPN	9
Figure 4	VPN Tunneling.....	10
Figure 5	The structure of PPTP packets.....	13
Figure 6	L2TP packet encapsulation.....	14
Figure 7	IPsec Diagram	16
Figure 8	SSL Diagram	16
Figure 9	Executed the IPerf by using the JPerf	19
Figure 10	Sample of screen Netperf	21
Figure 11	A sample of pinging results.....	22
Figure 12	Wireshark analysis sample	23
Figure 13	Main screen for GNS3 program.....	25
Figure 14	Main screen for VMware program.....	26
Figure 15	ASA device	27
Figure 16	Cisco ASDM	28
Figure 17	Virtual Networks	29
Figure 18	Main network diagram	30
Figure 19	PPTP VPN network diagram.....	31
Figure 20	Users accounts and Network Policy.....	32
Figure 21	DHCP server and Windows Firewall.....	32
Figure 22	Client Side Connection 1.....	33
Figure 23	Client Side Connection 2.....	33
Figure 24	ASA configuration for SSL 1.....	34

FIGURES

Figure 25	ASA configuration for SSL 2.....	35
Figure 26	SSL client side.....	35
Figure 27	L2TP/IPsec VPN network diagram.....	36
Figure 28	Routing and remote access configurations.....	37
Figure 29	DHCP server and Windows Firewall	37
Figure 30	Client side connection configurations 1.....	38
Figure 31	Client side connection configurations 2	38
Figure 32	Measuring the bandwidth of SSL using the Jperf	40
Figure 33	Bandwidth of SSL in (Kbits/ sec)	40
Figure 34	Sample of data result from IPerf for SSL protocol	41
Figure 35	Bandwidth of PPTP in (Kbits / sec).....	41
Figure 36	Sample of data result from Iperf for PPTP protocol	42
Figure 37	Measuring the bandwidth of L2TP/IPsec using the Jperf.....	43
Figure 38	The Bandwidth of L2TP/ IPsec in (kbits / sec).....	43
Figure 39	Sample of data result from Iperf for L2TP/IPsec protocol....	44
Figure 40	Ping and RTT in SSL protocol	44
Figure 41	Ping RTT for the PPTP protocol	45
Figure 42	Ping RTT for the L2TP/IPsec	45
Figure 43	Sample of data result from SSL protocol	47
Figure 44	Sample of data result from Iperf for PPTP protocol	47
Figure 45	Measuring the bandwidth of L2TP/IPsec using the Jperf.....	48
Figure 46	Throughputs comparison between SSL, PPTP, L2TP/IPsec....	50
Figure 47	Ping and RTT in SSL protocol.....	51
Figure 48	Ping and RTT in PPTP protocol.....	51
Figure 49	Ping and RTT in L2TP protocol.....	52
Figure 50	RTT comparison between SSL, PPTP, L2TP.....	53

LIST OF TABLES

TABLES

Table 1	VMware Configuration	28
Table 2	Cisco ASA Configuration	29
Table 3	Cisco Router Configuration	29
Table 4	SSL Throughput Values	49
Table 5	PPTP Throughput Values	49
Table 6	L2TP Throughput Values	49
Table 7	Comparison Between Min, Max, Avg Values of RTT	52

LIST OF ABBREVIATIONS

ASA	Adaptive Security Appliance
ATM	Asynchronous Transfer Mode
ASDM	Adaptive Security Device Manager
DES	Data encrypting Standards
DHCP	Dynamics Host Configuration Protocol
DLSW	Data Link Switching
FEP	Front End Processor
GRE	Generic Routing Encapsulation
GUI	Graphical User Interface
IPSEC	Internet Protocol Security
L2TP	Layer 2 Tunneling Protocol
LAC	Internetwork Packet Exchange
MD5	Message Digest 5 Algorithm
NAS	Network Access Server
NSA	National Security Agency
PPTP	Point To Point Tunneling Protocol
RTT	Round-Trip Time
SSL	Secure Socket Layer
TLS	Transport Layer Security
UDP	User Datagram Protocol
VPDN	Virtual Private Dial-up Network
VPN	Virtual Private Network

CHAPTER 1

INTRODUCTION

1.1 Background

The VPN stands for "Virtual Private Network", the term network is defined as a group of devices which are able to communicate in order to transmit and receive data successfully among themselves, the term private is clear but in our context it means that the communications among the devices is secret so the data privacy and security must be considered an essential issue in VPN, although VPN it is a private network but it extends among public network just like the internet, VPN offers the data transmission among the public or shared networks. But it is offered for users as a direct connection to a private network with all the advantages and functionality, policies of management and the security of the private network [1].

Another definition for the VPN presented by (Stanaway and Kumar, 2001) referred that the VPNs are generated by using several protocols which offered for creating the VPN tunnels among the public network, these protocols contain procedures for the authentication, encryption, compressing and in other respects saving the data packet, while the packet is transferred among the public network which are not encrypted the addresses such as the "Internet protocol" IP addresses which are responsible for specifying each packet, which transferred among the network destination and source address. There is a safety gateway responsible of receiving the VPN packets, authenticating the process and communication of the payload with applying the standards of a specific VPN protocol which have been employed [2].

The technique which used in the infrastructure of internet network to conveying the data from a network over other network is defined by the tunneling technique. The payload or data which is conveyed over the network can be frames of different protocol. The protocol of tunneling responsible for encapsulate the frames and

adding a further header, the further header supplies the routing data, this data permit the payload to overpass the in-between internetwork, in other word these frames are routed among the tunnel endpoints through internetwork, and when the encapsulated frames reach the predefined destination, the frame will be un-encapsulated and arrive to the latest destination, the tunneling technologies contains the DLSW "Data Link Switching (SNA over IP)", "IPX for Novell Netware over IP", GRE "Generic Routing Encapsulation (rfc 1701/2)", "Mobile IP – For mobile users", IPsec "Internet Protocol Security " etc...[3].

"Remote-access VPNs" permit safe access to resources of corporation by instituting an "encrypted tunnel" among the internet. Indeed the VPNs is considered logical solution for remote-access, due to several reasons, such as supplying safe communication with "access rights" that is designed for the users, promoting the productivity by expansion the network and application of the corporate, reducing the cost, and increasing the flexibility [4].

1.2 Study Motivation

The motivation of this study comes from the motivation of the different companies to implement the VPN remote access network, because it supplies a secure communications and it is cost effective. A lot of networking technologies are not alive for a long time, the VPNs are emerged with all the features that related to it, so this study comes from the widely used and implemented of the VPN networks around the world between organizations. Indeed the VPN is also characterized by many features which force the organizations to deploy it, such as the flexibility which enables the organizations to start with low bandwidth then increase the bandwidth with the demand grows.

1.3 Problem Statement

With the growing popularity of Internet, the businesses are changed to become the means of expansion their own networks. In the initial stage, the intranets has emerged and can be protected by the passwords and it has designed to be available

for just the employees of company, but now a lot of companies are generating their own VPN "virtual private network" to meet the requirements of distant offices and remote employees. This research discusses and analyses the implementation of remote access of computer communication, and analysis the protocols of VPN "virtual private network" which involves the SSL "secure socket layer", PPTP "Point-to-Point Tunneling Protocol" and a Hybrid protocol which is a combined protocol between IPsec and LTP, then making a comparison between them under predefined criteria to help the researchers and companies in implementing the remote access VPN.

1.4 AIM and Objectives

The Aim of this study is to discuss and analyze various protocols of VPN "virtual private network" then it Intends to make a comparison between them. In addition, to discuss and analyze the implementation of remote access VPN for computer communication including the characteristic and specifications of the VPN network that will be established.

1.5 Thesis Overview

The thesis will be organized as the following:

The first chapter of this research introduces a background about the research, main objectives in addition to show an overview of the whole thesis, while the second chapter will introduce some of the recent studies which discuss, analyze and implement the remote access computer communication. The third chapter will introduce the concepts and types of tunnels in addition to introducing an overview of the VPN protocols including PPTP, L2TP/IPSec, and SSL/TLS. Whereas, Chapter four will introduce a detailed overview of the VPN characteristics including the RTT (Round trip time), Throughput, Bandwidth, Jitter, Packet loss in addition to an overview of the tools which will be used in this study that involved Iperf, Netperf, Ping, Wireshark. Chapter five will present the network establishment, and how the three famous protocols PPTP, SSL and L2TP/IPSec are implemented in virtual

environment and how the virtual lab will be built using the GNS3 networks simulator. Chapter six will present the results of testing the protocols, and the bandwidth test result which obtained from the Jperf and Iperf tools and the RTT, and packet loss which obtained by the Pinging tools. Chapter seven will illustrate a detailed discussion of the obtained results,required diagrams and graphs are engaged in this part too. Finally, chapter eight will show the conclusion of the whole work that has been introduced and achieved during the research, in addition to some future plans related with the research topic.

CHAPTER 2

WHAT IS VPN?

2.1 Overview

A VPN- preservation of for Virtual Private Network-, represents the private extension of a company that uses public network as internet. A secure connection is created by VPN in a private tunnel. A VPN connects in a secure way in corporate networks to offices and remote users. VPN aim is to increase the security levels to data exchange. Even when a company is using leased line, by use of this private extension, their data is protected.

Virtual: the network is not dependent on the physical infrastructure underlying: their sole function to the existing organization is adding extra logical layer. This implies that, in most cases the user doesn't have to own the underlying network. because of the nature of physical network being public and shared among many users, to achieve its objective, techniques of protocol tunneling are used.

Private: because of the follow of data and the privacy of date over VPN, it is termed as private. VPM traffic uses public network to flow and be shared, there are therefore methods aimed at providing security. The security is obtained by:

- Integrity: there is no modification of the message when it is being transported;
- Confidentiality: the message is sent and is accessed by only the user.
- Non-repudiation: when the user sends information, they cannot deny that they have sent the information and the intended receiver cannot deny that they have not received it.
- Authentication: there cannot be modification of message by another user and is sent from the right user.

Network: VPN represents the company's network extension even if virtual. This means that it is usable for the purposes of the company's intranet [1][5].

2.2 Scenarios of Common VPN

VPN can be used in many different contexts, the following being three common scenarios:

1. Site-to-Site VPN
2. Client-to-Site (Remote access VPN)
3. Extranet VPN

2.2.1 The Site-to-Site VPN

The use of Site-to-site VPN connection is linking the branch offices with the headquarters of the company. This interconnects in a safe way trusted intranets within an organization. Company intranet is protected by the site-to-site connection from external intruders and ensure that the data of the company is secure when flowing against a public network. This makes the connections cheaper, globally accessible and safer to use.

The common way that VPN connection is implemented between offices connections is purchasing access of internet from ISP (acronym of Internet Service Provider). VPN servers and the firewalls are placed at each intranets boundary in order to offer protection to the traffic of the company from intruders. Therefore, the servers and the clients are not required to support the technologies of VPN because the data authentication, encryption and VPN capabilities have VPN servers. Using the approach, the confident information is covered from the internet users who are intrusted, and to do this a firewall is availed to deny access to the unauthorized attackers.

The offices of the company are able to have safe communication with each other locally or far away. The use of VPN technology allows each branch to extend their existing intranet, where enterprise-wide corporate network is built As in the figure 1.

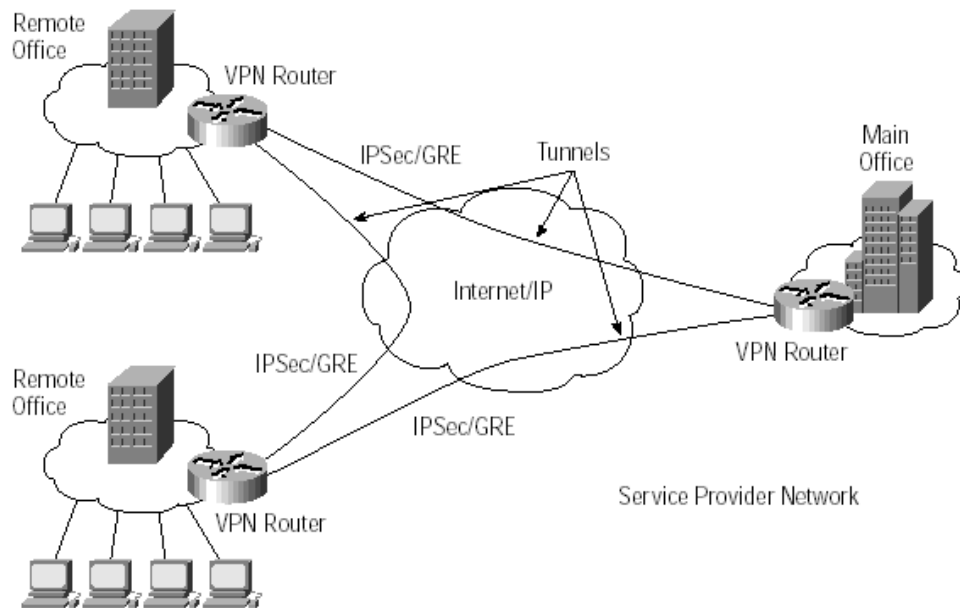


Figure 1 Site-to-site VPN

2.2.2 Client-to-Site VPN (Remote access VPN)

This allows a remote user on the road or home to communicate back securely to the corporate intranet. For instance, if an employee at home is in need of a file, they can get it from the server. With the access of internet, communication among employees becomes easy by use of the company's intranet server as well as having access to the files they require As in the figure 2 below:

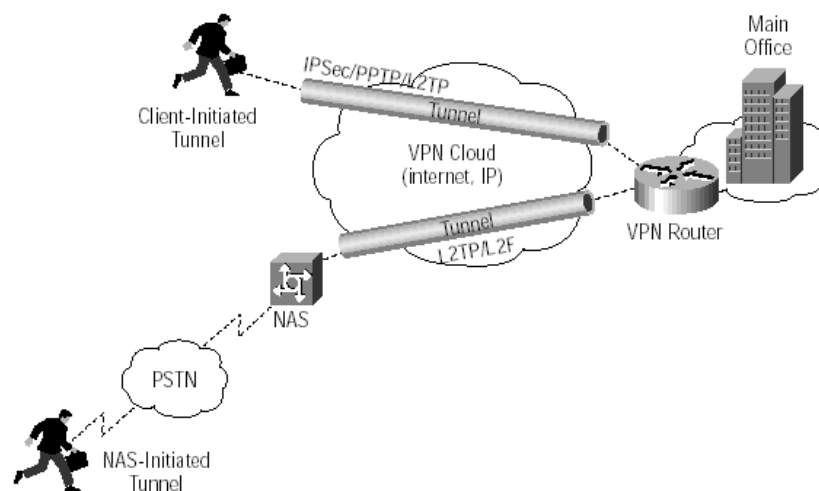


Figure 2 Remote access VPN

To realize the access tunneling protocol remotely, remote access VPN is very useful, apart from this use it enables the VPN firewall and VPN remote client. As a matter of fact, it is possible to use both solutions and this provides best solutions. Internet is used by the client either through dial-up or connection via broadband to ISP and this establish encrypted tunnel and authenticated tunnel between the firewall and himself using intranet boundary, When authentication is applied between the firewall and remote client, the internet is automatically protected from unauthorized IP packets and the traffic flowing between the firewall and remote host hence one can prevent intruders from sniffing the information being exchanged [6].

2.2.3 Scenario of Extranet VPN

It is the desire of companies to allow their businesses access resources on corporate intranet. It is however hard for such businesses to control the partner networks for the business, therefore, there is need to build a secure gateway with the capacity to provide required information. Use of VPN allows the company provide the secure and safe necessary information.

It is possible to build between client in the server and the business partner's intranet in the company intranet. The client has the ability to authenticate themselves to the server or the firewall or even both and a tunnel is established to ensure that all data from the client is encrypted, to the server through internet. The difference that exists between the site-to-site outline and the extranet VPN is fact that the intranet of the business partners is not trusted network hence there is need for additional security levels in the business [7].

Extranet VPN

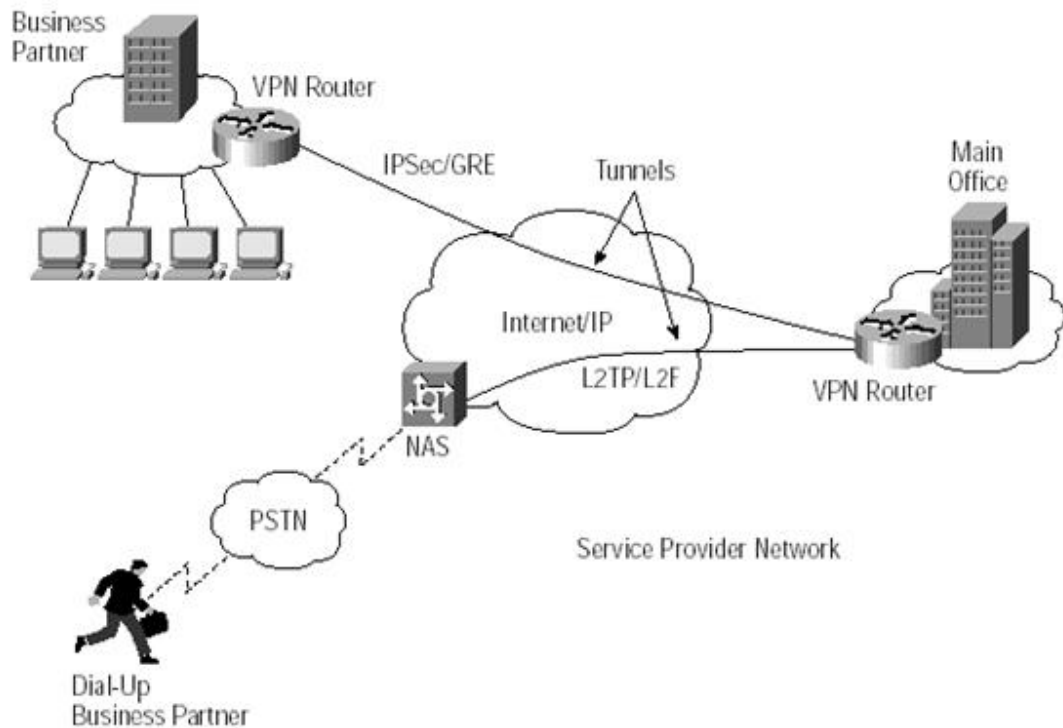


Figure 3 Extranet VPN

2.3 VPN Security Policy

Security policy for VPN explains the protection kind for particular traffic profile, on the other hand, network protection policy that is simple specifies the type of traffic that should be denied permission to the flow. This is therefore referred to as the network security policy subset, reason being it is granular and also dependent on former when allowing traffic between destinations before protection. Flow through the VPN should be done by traffic and then be protected from non-secure channels preventing them from the flow.

The Security policy for APN describes typically the profile for the traffic that is being protected, for instance, ports and protocols, destination and source, and requirements for security of self-protection, this includes encryption, authentication as wells as key lengths, transforms and lifetimes. The policies of VPN can be defined per the device; however, they need to be implemented in a directory that is centralized for better usage and stability.

There is need for the devices to mach in policies for similar traffic profile before allowance of traffic to flow between them. It is important to note that there is possibility of one traffic being more restrictive and grainy than the other so song as there is agreement between both parties in similar protection suites at a point in time [8].

2.4 Tunneling Concept

Tunneling is the transfer of data between two same or different networks using an intermediate network. this transfer of data includes one kind of data packet to another protocol's packet. At first there is the encapsulation, and then encryption of packets is done so the there is unread-ability of data to anyone monitoring that network As in the figure 4 below:

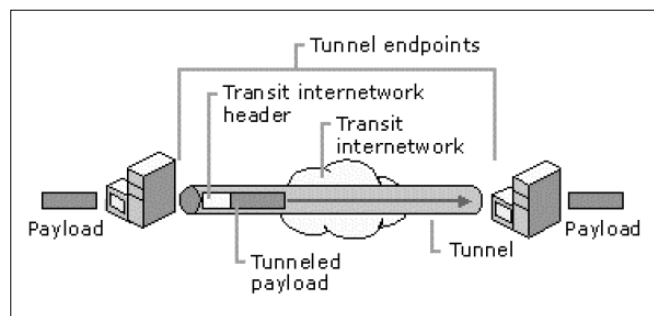


Figure 4 VPN Tunneling

These packets move using Internet, which serves as case of an intermediate network up to the time they reach desired destination. After arrival of the packets, they are decrypted and taken back to their original format. The encapsulating packets protocol is comprehended by network and by the two points that the packet enters and exit of the network.

To place the packet using protocol that is not in use used the Internet inside an IP packet and sending it securely, tunnel is important and does this over the Internet. One can use non-routable, private, IP addresses inside a packet using routable IP address, an assigned public to tunnel through the Internet your private network [9].

2.5 Tunnel Types

There are different kinds of tunnels:

- Voluntary: client or user computer issues VPN request to create and configure a voluntary tunnel. In such instance the computer of the user acts as a client end point and is a tunnel endpoint.
- Compulsory: capable dial-up VPN access the server, creates, and configures obligatory tunnels. By this tunnel, the computer user at this point is not an endpoint tunnel. For this reason, the dial-up server between the tunnel server and user's computer (another device) acts as the tunnel client.

2.5.1 Voluntary Tunnels

availability of voluntary tunnels is done with use of work station or tunneling of routine server client software where creation of virtual connection is done to the tunnel server. to achieve the objectives, there is need for suitable tunneling protocol installed to the client computer. With the occurrence of this the connections of IP are required for voluntary tunnel. There is need for establishment of a dial up connections by the client so that it facilitate internetwork and set up of tunnel. The dial up user must have an ISP and have also internet connections over the internet before a tunnel can be created, for a computer that is attached to LAN, for instance for a user on a corporate LAN, connections have already been done for the client on the internet and this provides routine for summarized payloads to the LAN tunnel server that has been chosen. With this, the client is able to obtain or so has a hidden or private subnet on the LAN. There is a delusion, which VPN connections need a dial-up. What only needed is an IP connectivity among the VPN server and VPN client. Certain users utilize dial-up connections to Internet in order to generate IP transport. What is done is beginning step of generating a tunnel which is not part of the tunnel protocol.

2.5.2 Compulsory tunnels

There have been an implemented ability that has enabled the creation of the dial up access on behalf of the users. This results to the client being provided with the collect tunnel through some known features such as the Front End Processor (FEP) in PPTP, L2TP Access Concentrator (LAC) in L2TP. In order to make this happen the FEB has to have their own installed protocols that should be followed after connecting to the internet. In the Internet case, a dial-up call is installed in the client computer for tunneling-enabled NAS at the ISP. The resultant FEPs generate tunnels over the Internet to a combined tunnel server with the private network corporation. This in turn offer consolidation calls from various places into single Internet connection at the corporate network. The new pattern is indicated as required tunneling and makes the user to apply it to enable an automatic connection and sending of information and therefore, the computer of user generate a single PPP connection where the dialing to the NAS by the user generate a tunnel and rout the while traffic through it. There is big difference in the way separate tunnel and FEP configuration for the dial up clients in that a separate tunnel uses a voluntary client at a time while FEP is constructed to the tunnel server in a multiple dial-up clients. When the end user disconnects the tunnel, it is then end. Because the Internet aids the generation of VPNs from anyplace, networks require high security to avoid unwanted access to private networks and offer protection for private data. The paper entails the capability of having a strong authentication and encryption of EAP and IPSec [9][10].

CHAPTER 3

PROTOCOLS of VIRUAL PRIVATE NETWORK

3.1 VPN Protocols

We have different types of protocols used to create VPNs over Internet, most famous protocols and Frequently used are :

- Layer-2 tunneling protocol (L2TP).
- Point-to-point tunneling protocol (PPTP).
- Secure socket layer(SSL).
- IP security protocol (IPSec).

3.1.1 PPTP (Point-to-Point Tunneling Protocol)

A layer 2 protocols with ability to encapsulate PPP frames in datagram IP can be referred as PPTP. TCP connections are used by PPTP for maintenance of the tunnel and version of generic routing encapsulation modification to help in PPP frame encapsulation for tunneled data. The encapsulated PPP frames payloads can be compressed and encrypted or just encrypted.

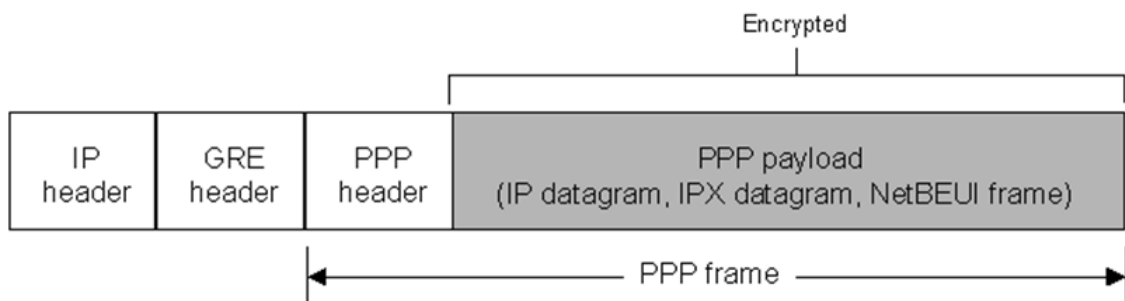


Figure 5 The Structure of PPTP Packets

The PPTP has capacity to support 128-bit and 40-bit encryption and uses any PPP supported authentication scheme. PPTP is a tunneling protocol that is used to provide remote users multi-protocol and encrypted access to a communal network over Internet. Network layer protocols, like NetBEUI and IPX, are summarized by the PPTP protocol for convey over the Internet.

Since it depends on PPP, PPTP is based on the authentication mechanisms within it, namely CHAP and (PAP)password authentication protocol. Again, PPTP can use PPP for data encryption, however Microsoft has come up with a stronger method of encryption called Microsoft point-to-point encryption (MPPE) for using with PPTP. The main advantage of the PPTP is tht it is designed and given the capability to auto run in the open systems interconnections even if the client support for the PPTP is simple. The link layer runs at layer 3 contrary to the IPsec, PPTP support transmits protocols rather than IP in its tunnels thus supporting dat transmission or communication. Each user has one tunnel that is supported by the PPTP[11][12].

3.1.2 L2TP (Layer 2 Tunneling Protocol)

From the membership of the three forums i.e. Cisco, PPTP and Internet Engineering Task Force (IETF)comes the L2Tp.this supports the IPsec by combining both L2F and PPTP. At a single time the L2TP can support several tunnels with each tunel having a user and be utilized as a tunneling protocol for site-to-site VPNs as well as remote-access VPNs. L2TP uses encryption methods of the IPsec's. L2TP includes mechanisms that authenticates PPP namely CHAP and PAP since it uses PPP.then supporting PPP's L2TPuses the extended authentication protocol used by other authentication system, for example RADIUS [13].

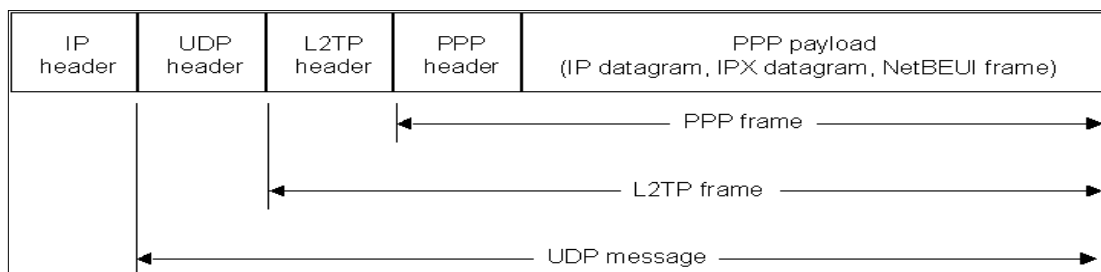


Figure 6 L2TP packet encapsulation

3.1.3 IPSec (IP Security Protocols)

IPSec (Internet Protocol Security) is an internet protocol which become a standard for VPNs. It addresses data that is very confidential information, tunneling, authentication and key management. This IPSec can work in both sites-to-site and remote-access VPNs.

Generally, IPSec encapsulates packet through wrapping other packet around the IPSec. Finally, it encrypts the entire packet. Secured network is formed across the network otherwise, unsecured network is formed. This works well for site-to-site VPNs. IPSec can allow the sender of the packet that is to encrypt all the IP addresses separately or authenticate or both operations are been applied.

Applications of packet authentication separation as well as encryption brings about two methods utilized by models of IPSec like in transport mode, the part of IP packet only known as transport layer is encrypted, the tunnel model is the entire packet of IP authenticated or encrypted. When the IPSec mode can be used in various cases the IPSec tunnel mode offers a more defense modes against traffics and attackers monitoring and this occurs in the internet. Cryptographic technologies that are standardized are used to build the IPSec to provide data integrity, confidentiality and authentication. IPSec use:

- Diffie-Hellman key exchanges in order to assist in delivery of secret key between peers on the public internet.
- Cryptography of the public key for signing exchanges of Diffie-Hellman to assurance security of the two parties from attacks.
- DES (Data encrypting Standards) and algorithms that are bulky for data encryption.
- The HMAC, SHA, MD5 keyed hash algorithms to authenticate packets
- Public key validation digital certificates that are two way to handle the management and key exchange within the architecture of IPSec; IKE automated key and manual key management.

Since IPSec is developed to only handle the packets of PPTP, IP and L2TP they are more suitable for multiprotocol non-IP use environment such as IPX, NetBEUI and apple talk [14].

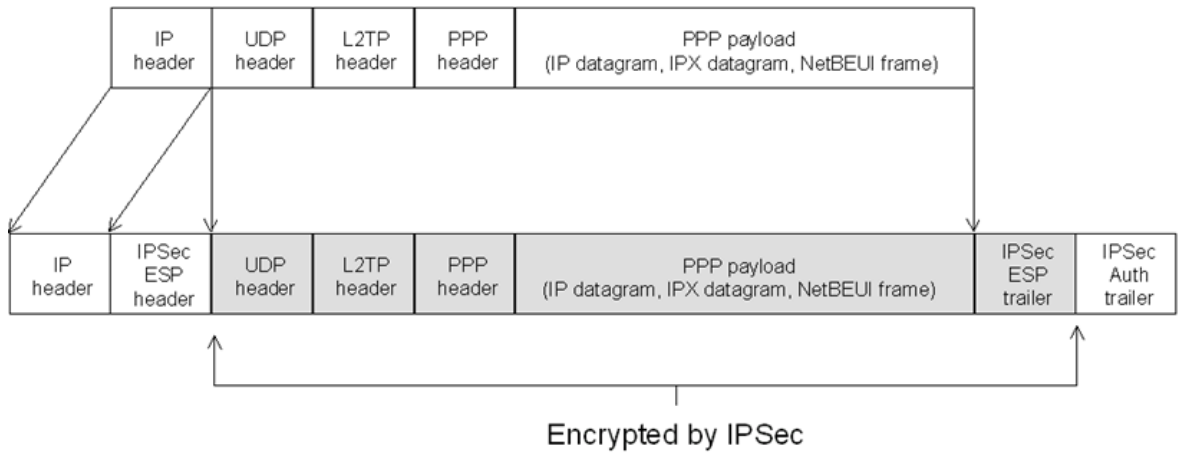


Figure 7 IPsec Diagram

3.1.4 SSL/TLS (Secure Socket Layer/Transport Layer Security)

The TCP port are usually used by some transport layers such as SSL / TLS and can be defined by the IETF in cases where there are no pure versions that are beyond 3.1. there are two main versions that are standardised and that look alike with TLS and TLS1.0 and they have similar features such as being confidential, integrity and that contain some digital signatures in them. An agreement between the communicating parties has been arrived about the features and functions to apply through SSL and TLS. Through a certified authority such as SSL through the use of VPN gateways users can identify themselves to the website and know whether they are really talking to the right person or not. This is due to the fact that some SSL-VPN uses some digitalized certificates that cannot be trusted by the commonly used web browsers and as a result the user has to their own trusted certificates [14].

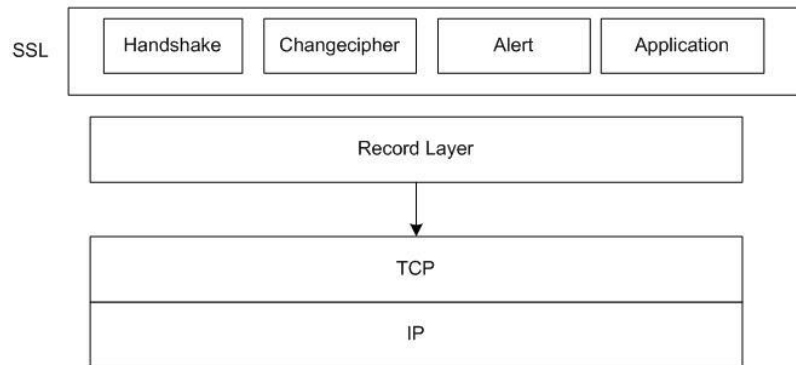


Figure 8 SSL Diagram

CHAPTER 4

VPN PARAMETER AND TESTING TOOLS

4.1 VPN Characteristics

4.1.1 Round Trip Time (RTT)

The time taken to respond to a signal and the overall time taken by a signal to before it is sent is what is referred to as RTT. In this content we use the data packet as the signal and the ping time as the RTT in which the user can use the ping commands to arrive at the RTT.

4.1.2 Throughput

The rate at which the a message uses to before it is delivered is referred to as the throughput and in most cases it uses the physical, logical or even network nodes to be successfully delivered. The most used measurement for throughput is data packets per time and per seconds. Since R: average throughput, MSS: packet size, RTT: round-trip time, P: packet loss. Total data packets that are delivered through a terminal are referred to as the system throughput. In addition the through the use of the queuing theory it is easy to analyse the throughput bandwidth. Throughput is a digital bandwidth consumption, the queuing theory can be applied to for analysis, where the load (in packets per time unit) is then indicated as the arrival rate and the throughput (in packets per time unit) as the departure rate. The average throughput (R) is evaluated as following:

$$R = \frac{MSS}{RTT} \cdot \frac{1}{1.2/p^{0.5}} \dots\dots\dots(1)$$

4.1.3 Bandwidth

The bandwidth defined by the link capacity. In our goals, is presenting the highest rate of transmission for the link. For example if the highest rates which transmit packets over a link is 10 Mbps, so the bandwidth which required is 10 Mbps, and the bandwidth unit is (bit/sec) [15].

4.1.4 Jitter

When a reference source is done the result is the deviation from the real periodicity of a presumed periodic signal. Successive bits and frequency are the commonly used characteristics to observe Jitter. In most cases the electromagnetic interference and crosstalk with carriers of other signals may have an effect on the communication links since it works as the most significant factor. The most physical appearance is the frittering of the monitor and processors failure. Furthermore they can cause poor network transmission. The affected application determines the amount to be tolerated [16].

4.1.5 Packet loss

When the rate of sending the internet content exceeds the receiving rate the possible effect is the network congestion which is also known as the packet loss and therefore the result is dropping the packets. Packet loss results from a different number of factors, which can dishonest or lose packets in transit:

- Hardware network failure
- Drivers network failure

Hoc routing and dynamic source routing can as well be another cause for packet dropping of normal routes. In addition, network dissuasion by thee management can as well cause drop routing. Another way of measuring the packet loss data is the frame loss rate that calculates the percentage of possible frames that could be forwarded but has failed. Since the resources available were not enough [17].

4.2 Tools used in test

4.2.1 Iperf and Jperf

The measuring of Performance, and testing used to measure the validate of the network, Jperf and Iperf is can be used for these purposes, by using Iperf between Iperf server and Iperf client, and the graphing results can be obtained the Jperf, the Iperf can be executed from the command line, or it can be launched by using Java frontend which also called JPef, Jperf it is more easy to make intricate parameters of command line, in addition to the ability to saving these results and as graphs in real-time. The following figure 9 presented a sample of how we executed the Iperf by using the Jperf [18].

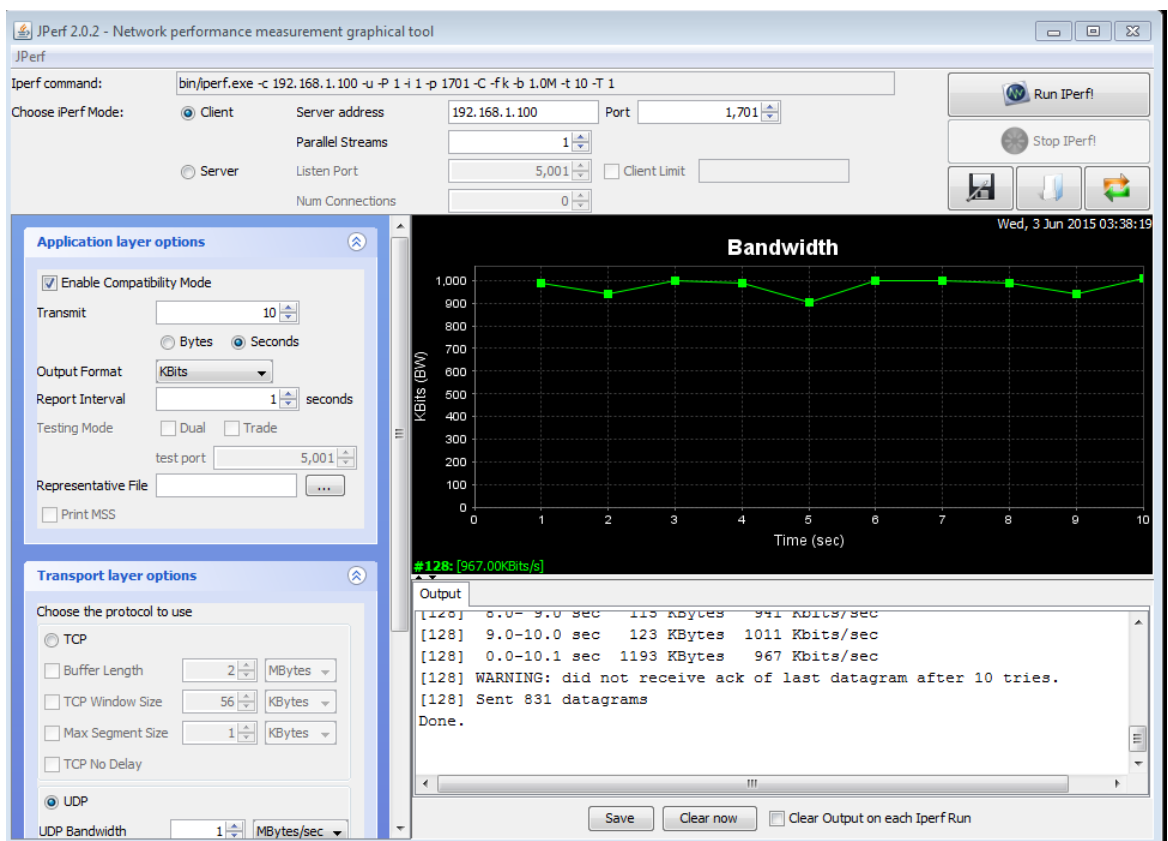


Figure 9 Executing the IPerf using the Jperf

4.2.2 Netperf

Network performance can be measured using various aspects such as they Netperf. Land can use either TCP or UDP and the Berkeley Sockets interface as transfer modes. During writing that are both conditional and unconditional tests that included.

- Link-level unidirectional transfer and request/response using the DLPI interface.
- TCP and UDP unidirectional transfer and request/response over IPv4 and IPv6 using the Sockets interface.
- SCTP unidirectional transfer and request/response over IPv4 and IPv6 using the sockets interface.
- TCP and UDP unidirectional transfer and request/response over IPv4 using the XTI interface.
- Unix domain sockets

In some cases the Netperf might not work perfectly with the above listings and therefore there are some other platforms that they can be applied on.

- Windows
- UNIX
- Linux
- Others

The major contributing editor of Netperf Rick Jones has been formally marinating amend supporting the platform. In addition there are other communities that needs to be appreciated due to their network but their usability does not support the performance of Hewlett-Packard. The main advantage of Netperf networks is that it gives the user a chance to make changes and enhancements that can fit their requirements so long as the user remains within the Netperf copyright. If there is any problem with the modifications the user may send the information to Netperf for inclusions and version update.

According to Jones the Netperf licence moves and looks like an open licence although the licence has not been certified for being an open. It is the Contributing license. The Netperf4 gives the users an opportunity to make contributions to the networking benchmark and that has its terms and conditions under the GPLv2.

Through the Netperf talk that offers an opportunity to share the user's interest in regard to the performance of the network. However it offers a room for subscribing in order to give the users a chance for sending and receiving mails [19].

```

C:\test\netperf>netclient.exe -H 10.1.1.1 -l 60
TCP STREAM TEST to 10.1.1.1
Recv  Send  Send
Socket Socket Message Elapsed
Size  Size  Size  Time
bytes bytes bytes secs.
8192  8192  8192  60.00
Throughput
10^6bits/sec
0.30

C:\test\netperf>netclient.exe -H 10.1.1.1 -l 60 -- -n 65536 -M 65536 -s 65536 -S
65536
TCP STREAM TEST to 10.1.1.1
Recv  Send  Send
Socket Socket Message Elapsed
Size  Size  Size  Time
bytes bytes bytes secs.
65536 65536 65536 60.00
Throughput
10^6bits/sec
1292.75

C:\test\netperf>netclient.exe -H 10.1.1.1 -l 60 -- -n 9000 -M 9000 -s 9000 -S 90
00
TCP STREAM TEST to 10.1.1.1
Recv  Send  Send
Socket Socket Message Elapsed
Size  Size  Size  Time
bytes bytes bytes secs.
9000  9000  9000  60.00
Throughput
10^6bits/sec
564.65

C:\test\netperf>

```

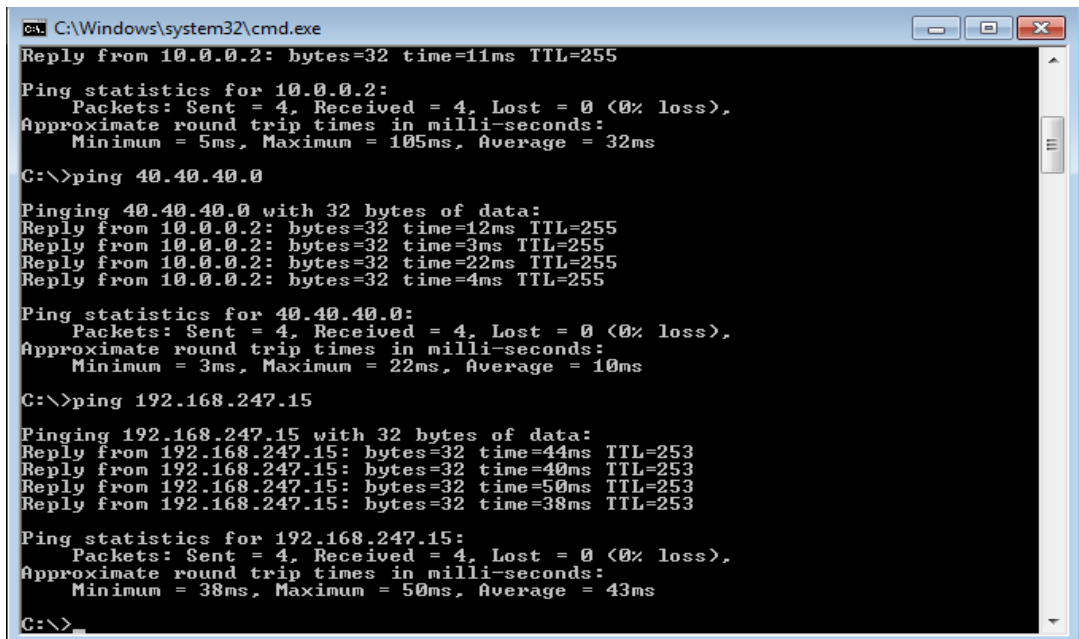
Figure 10 Sample of screen Netperf

4.2.3 Ping

There is a an administrative tool that is usually used by computers to test the reach ability of the IP networks as well as the round trip time used by messages between the host place to the destination. This device is called the Ping and is delivered from an active sonar that usually descends a pulse and then listens to the echo produced. In the internet case the ping sends the Internet Control Message Protocol that is referred to as the echo request to the host computer and waits for a response. During this process Ping measures the time taken to transfer and still records to check whether there has been any packet loss in the process. All the results are then put into printing and a summary of minimum, maximum as well as the round-trip time. The standard deviation might as well be included to be able to calculate the mean.

There are some utilities that can be used to execute and implement the commands and be able to switch it to the right mode some of the inclusive are:

- The time stamping.
- The packet size of the probe.
- The automatic repeated operation for sending a specified count of probes [20].



```
C:\Windows\system32\cmd.exe
Reply from 10.0.0.2: bytes=32 time=11ms TTL=255
Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 5ms, Maximum = 105ms, Average = 32ms
C:\>ping 40.40.40.0
Pinging 40.40.40.0 with 32 bytes of data:
Reply from 10.0.0.2: bytes=32 time=12ms TTL=255
Reply from 10.0.0.2: bytes=32 time=3ms TTL=255
Reply from 10.0.0.2: bytes=32 time=22ms TTL=255
Reply from 10.0.0.2: bytes=32 time=4ms TTL=255
Ping statistics for 40.40.40.0:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 22ms, Average = 10ms
C:\>ping 192.168.247.15
Pinging 192.168.247.15 with 32 bytes of data:
Reply from 192.168.247.15: bytes=32 time=44ms TTL=253
Reply from 192.168.247.15: bytes=32 time=40ms TTL=253
Reply from 192.168.247.15: bytes=32 time=50ms TTL=253
Reply from 192.168.247.15: bytes=32 time=38ms TTL=253
Ping statistics for 192.168.247.15:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 38ms, Maximum = 50ms, Average = 43ms
C:\>
```

Figure 11 A sample of pinging results

4.2.4 Wireshark

In order to have a proper troubleshooting, an analysis, software development as well as the required education, Wireshark can be used. The wireshark is cross-platform, which utilize the GTK+ widget toolkit in present releases and Qt in the growth version to design its user interface and utilizing PCAP to capture packets. This makes it possible for the application to run in various operating systems such as the Linux, BSD, Solaris as well as Microsoft windows. In addition there are some other versions of GUI that are useable by the general public through the General Public licence.

The main difference between the wire shark and the TCP Dump is due to the availability of graphical front-end, and certain incorporated sorting and filtering options. In addition the wireshark gives the user an allowance to add the network interface controller due to their promising modes, that support promiscuous that mode to show the whole traffic visible on the interface, not just traffic addressed to certain interface address and broadcast/multicast traffic. The wireshark therefore has the responsibility of distributing the packets after they are received and then sends them to the running machine i.e. a computer using the TZSP protocol [21].

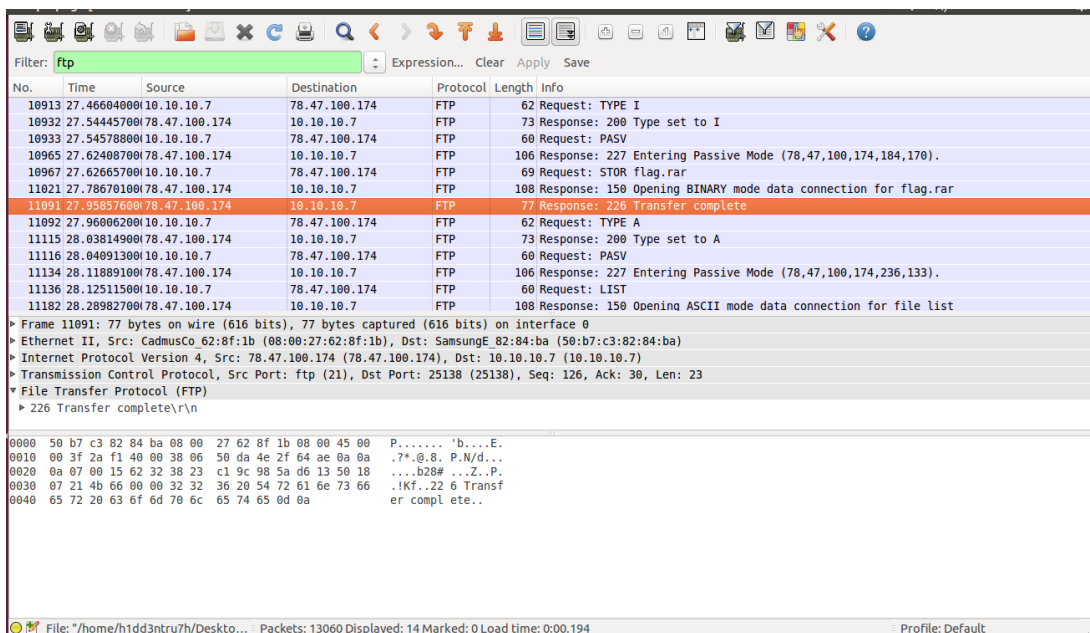


Figure 12 Wireshark analysis sample

CHAPTER 5

NETWORK ESTABLISHMENT

5.1 GNS3

5.1.1 Overview

This program is used in simulation in case of the lack of laboratory used for this purpose and to shorten the time and effort. The program contains features that make it the personal computer laboratory and complete control program is very easy through good GUI enjoyed by the program. The GNS3 network simulator is a free open-source software that can be downloaded and used by users. It works using real Cisco IOS images that are emulated using a program called Dynamips and it is like the GUI part of the overall product. This program does the real job of emulating the routers using real IOS images. With the GUI it is possible to use an interface that allows to build complex labs consisting of a variety of supported Cisco routers.

Dynagen is referred to be the front-end to the whole operation because it communicates with Dynamips using a Hypervisor to make the configuration process simpler. So, using the GUI provided by GNS3 it is possible to have an easy and powerful simulator As in the figure 13 below:

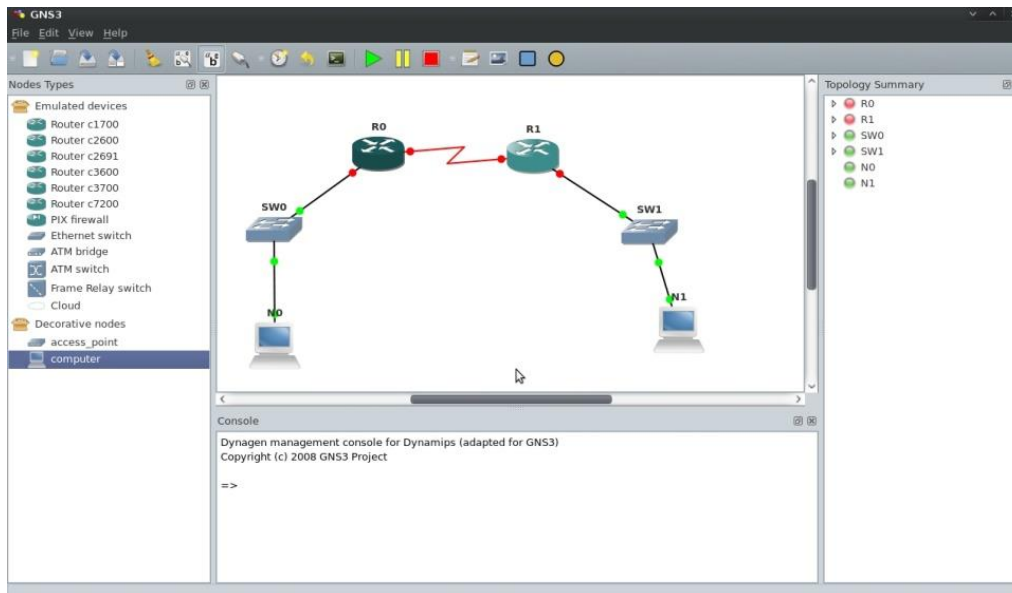


Figure 13 Main screen for GNS3 program

5.1.2 Supported GNS3 Features

The GNS3 has the following features provided by the simulator:

- Design of high quality and complex network topologies.
- Emulation of many Cisco router platforms and PIX firewalls.
- Simulation of simple Ethernet, ATM and Frame Relay switches.
- Connection of the simulated network to the real world.
- Packet capture using Wireshark [22].

5.2 VMware

This program is used to add a virtual computers for the purpose of simulation work, in this work different computers with different operating systems are needed. Thus, VMware was the best choice for simulation.

5.2.1 Virtualization technology

Virtualization technology increases the efficiency in the data center using a x86 servers to run multiple operating systems and applications. Workloads get deployed faster, performance and availability increases and operations become automated. It is simpler to manage and less costly to own and operate As shown in Figure 14.

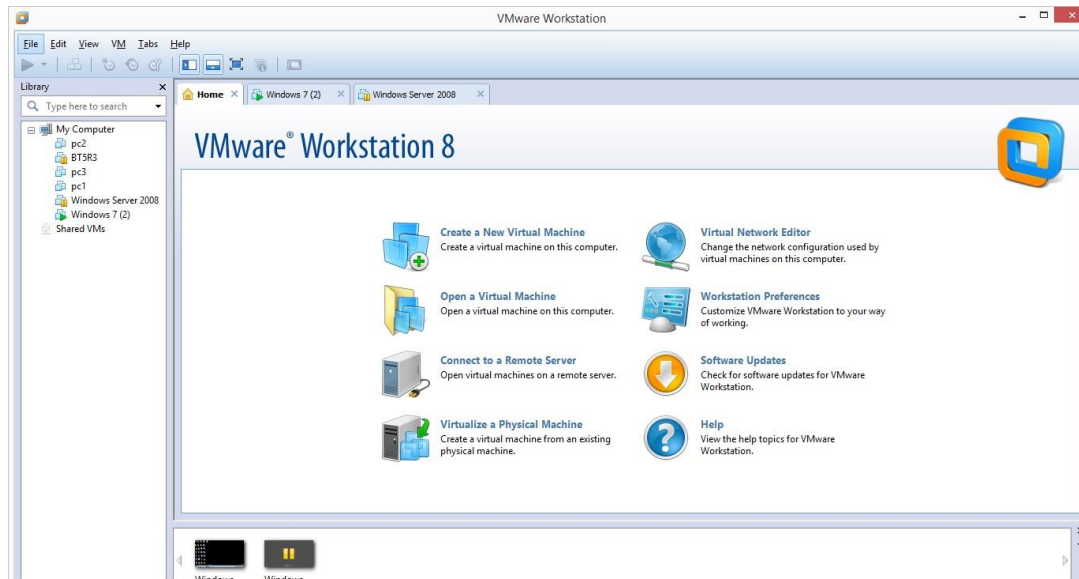


Figure 14 Main screen for VMware program

5.2.2 VMware Virtualization

VMware virtualization solutions are built on VMware vSphere with operations management, leading virtualization and cloud management platform. It is important because:

- It reduces capital and operational costs by increasing energy efficiency and using less hardware with server consolidation.
- It enhances business continuity and disaster recovery capabilities for your virtualized infrastructure.

- It virtualizes business critical applications and databases (Oracle Database, Microsoft SQL Server, SAP HANA, SAP Sybase, SAP Business Suite, Microsoft Exchange, SharePoint, SAP) for the highest SLAs and top performance [23].

5.3 VPN Establishment

5.3.1 Overview

This thesis aims to test the three famous protocols PPTP, SSL and L2TP/IPsec in a virtual environment, the virtual lab here build using networks emulator GNS3, because it has more realistic result and better work environment than simulation and this tool is widely used by CCIE studier. In addition, GNS3 has been used with VMware to simulate the entire network virtually.

5.3.2 Cisco ASA (Adaptive Security Appliance)

It is a hardware solution from Cisco, it is a firewall with more capabilities such as Route, IDS/IP, and VPN gateway, ASA supports PPTP, SSL and L2TP/IPsec for Site To Site and Remote Access VPN, it provides an easy way to establish, manager and control VPN networks using GUI ASDM scripts which can be uploaded to the ASA from FTP server and then install using consol. Figure 15 shows the ASA device and figure 16 shows Cisco ASDM.

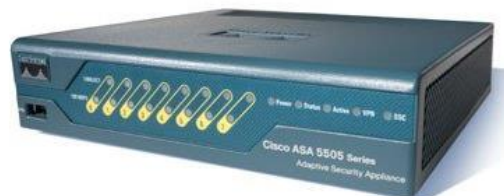


Figure 15 ASA device

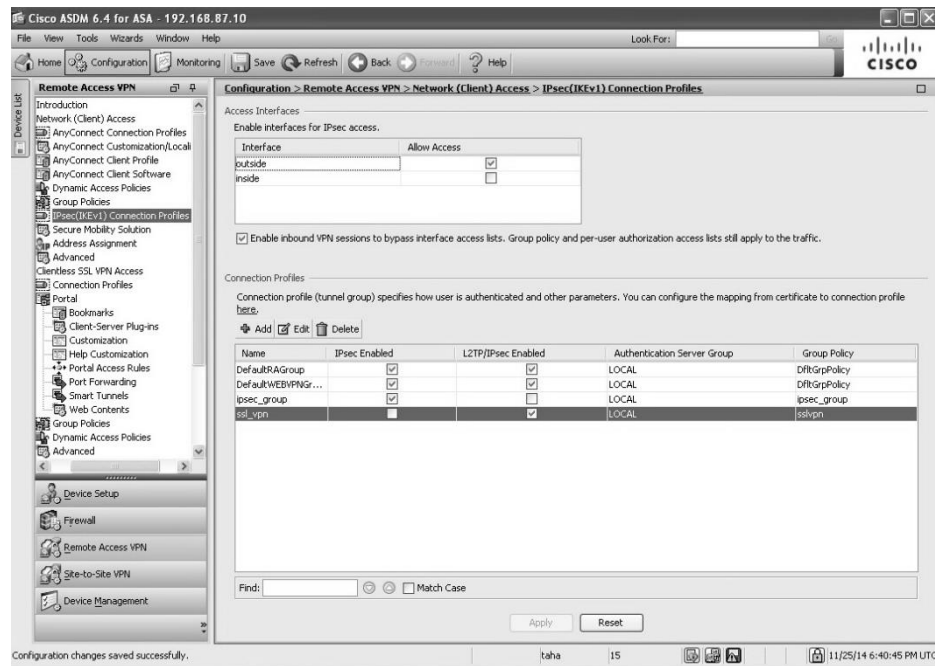


Figure 16 Cisco ASDM

5.3.3 Initializing Work Environment

In the beginning GNS3 and VMware were installed and later new virtual network adapters has been established with VMware that will represent the different networks in a virtual environment. In this thesis networks initialized As shown in the table below:

Name of network	IP	Name of LAN
Network 1	192.168.87.0/24	Vmnet1
Network 2	192.168.247.0/24	Vmnet2
Network 3	10.0.0.0 /24	Vmnet3

Table 1 VMware Configuration

The following figure shows that clearly:

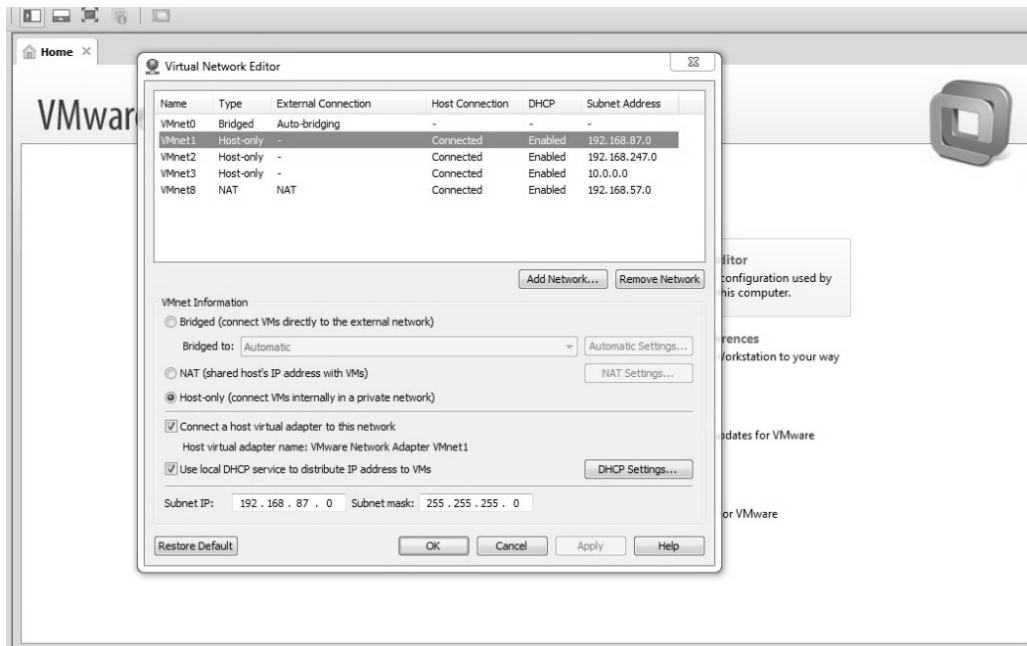


Figure 17 Virtual Networks

In addition, Cisco ASA 5520 and Cisco 2700 routers had been initialized with real images in GNS3 and prepared to work typically. For example, Cisco ASA programmed and got its own inside and outside Networks as follows:

Network	Name	Privilege	IP address
Inside network	Inside	100	192.168.87.10/24
Outside Network	Outside	0	192.168.247.15/24

Table 2 Cisco ASA Configuration

While two Cisco routers used to simulate the internet as simple as possible and got the following configuration:

Router	F1/0	F1/1	Routing Protocol
R1	192.168.247.10/24	40.40.40.1/24	Dynamic RIP
R2	40.40.40.2/24	10.0.0.2/24	Dynamic RIP

Table 3 Cisco Router Configuration

The following figure shows the main network diagram and routers IP addresses with connections:

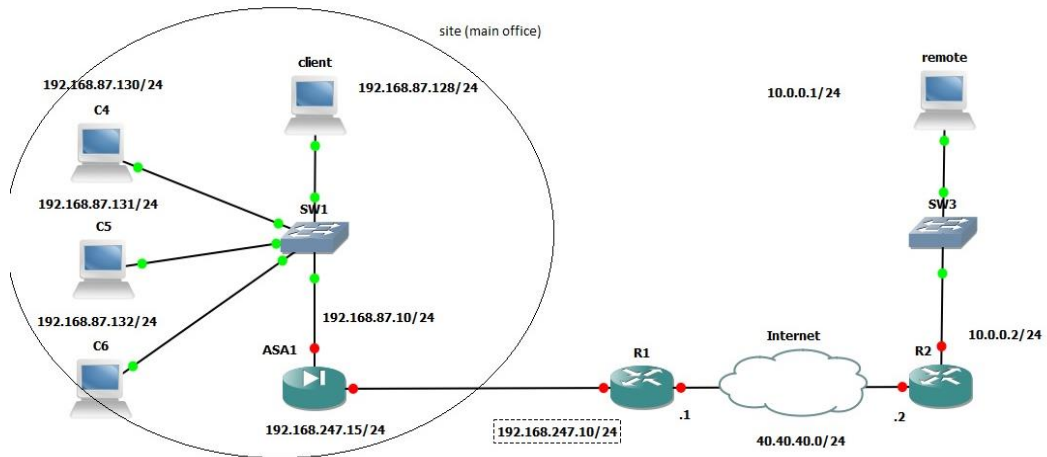


Figure 18 Main Network Diagram

Here Cisco ASA used as VPN hardware gateway and a router to establish a SSL VPN network, while Windows 2008 server virtual PC used instead for the PPTP VPN establishment.

5.4 Establishing PPTP VPN network using virtual lab

This section explains the procedures of establishing PPTP VPN based on Windows 2008 server as software VPN gateway in a virtual environment using GNS3 a network emulator and VMware as a virtual machine crating tool. Pay attention that host PC has windows 8 environment and 4GB of RAM, the following figure shows the main diagram of the network.

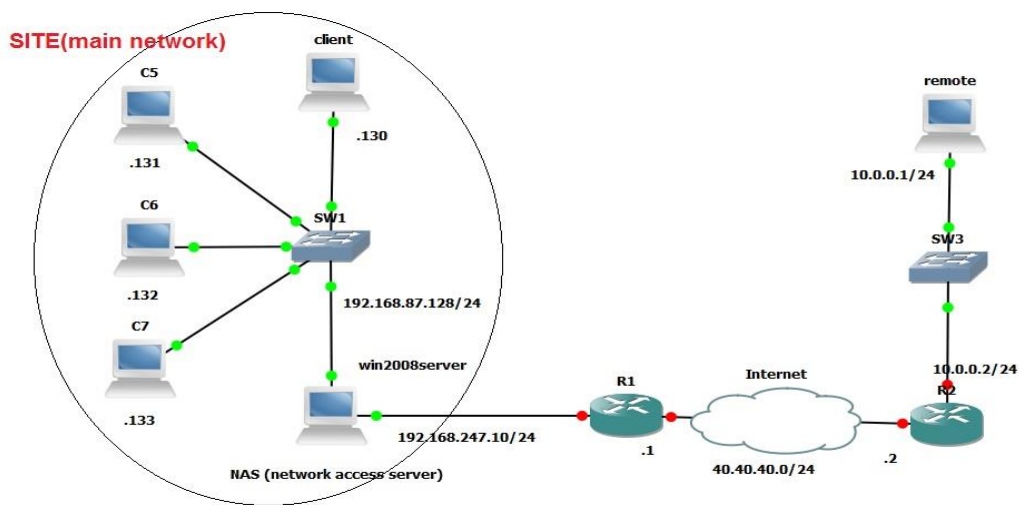


Figure 19 PPTP VPN network diagram

The procedures of establishing the network from the main network side are as follows:

- Creating users account with user name and password for each and enabling remote access.
- Configuring routing and remote access to accept connection from outside.
- Configuring new network policy to give access permissions for users from outside.
- Configuring a DHCP server to give suitable IP addresses after connecting.
- Configuring the windows firewall to allow VPN request.

The following figures show some of these configurations:

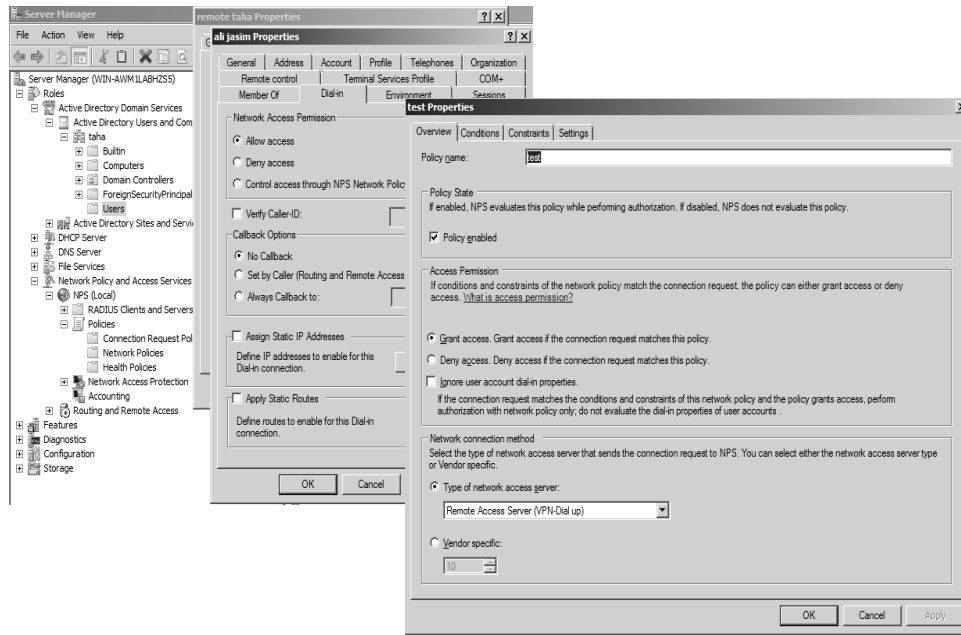


Figure 20 Users accounts and Network Policy

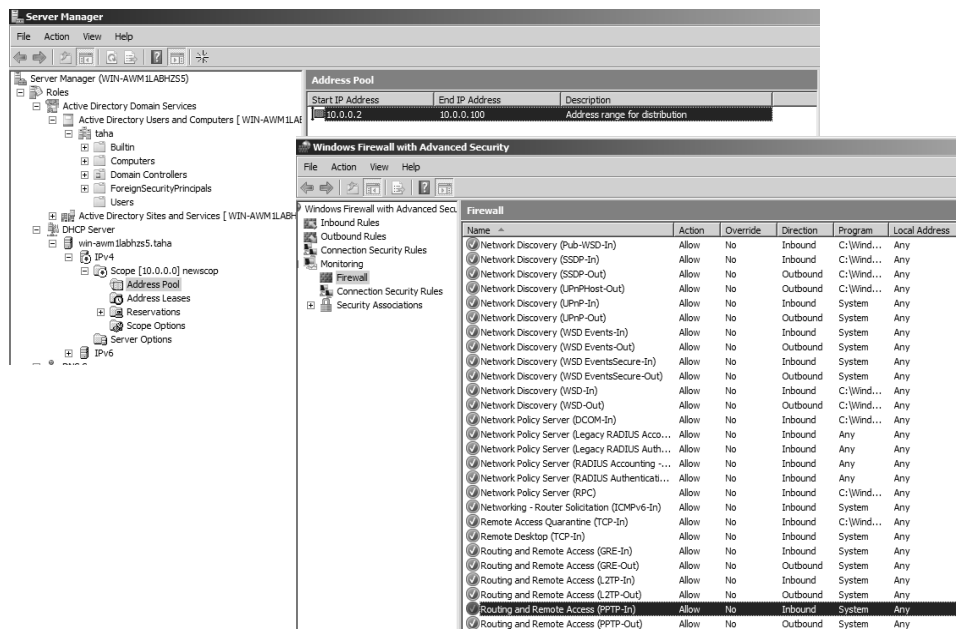


Figure 21 DHCP server and Windows Firewall

At Remote client side a simple configuration has been done by creating new connections and choosing VPN and dialup connection, then give a connection name and the server gateway IP address and that is all, when the user wants to connect he just has to enter the username and the password, the following figures 22 and 23 shows simple explanation:

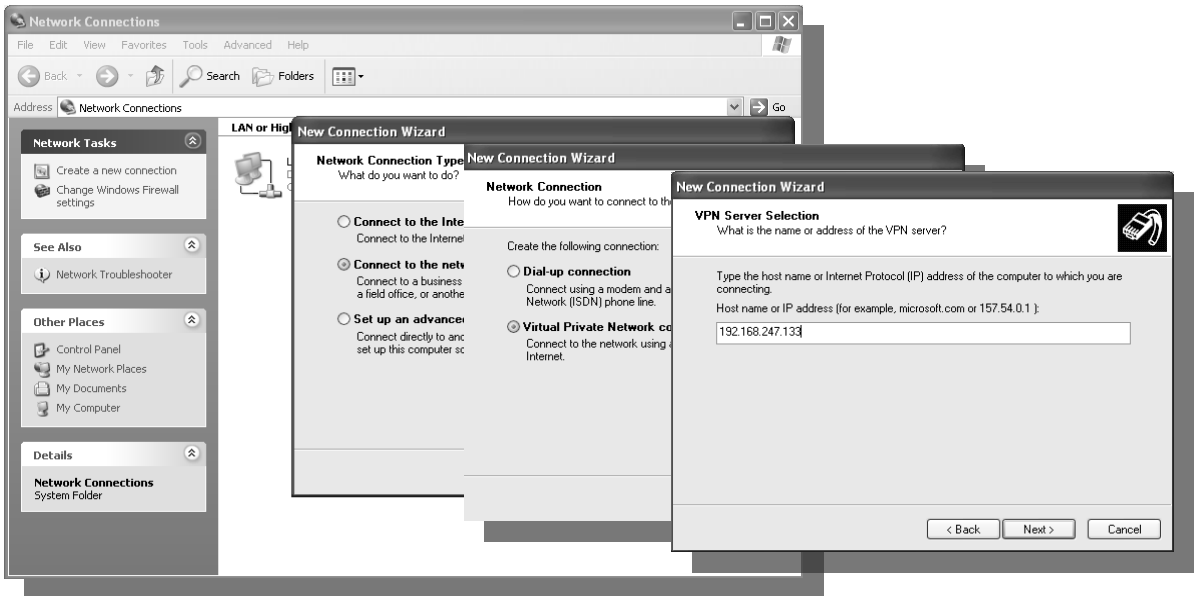


Figure 22 Client Side Connection 1,

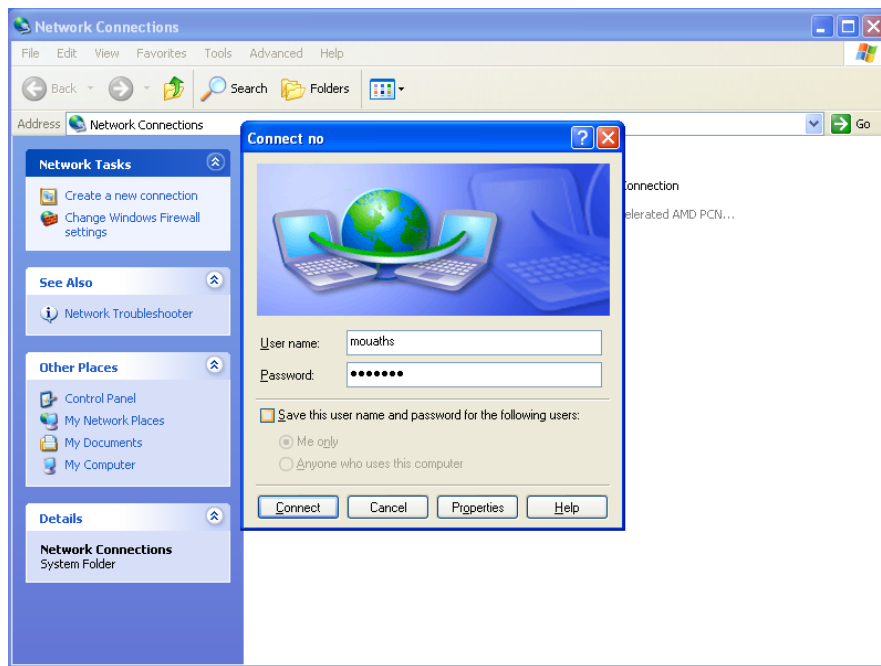


Figure 23 Client Side Connection 2

5.5 Establishing SSL VPN network using virtual lab

This section explains the procedures of establishing SSL VPN based on Cisco ASA as a hardware VPN gateway in a virtual environment using GNS3 as network emulator and VMware as a virtual machine virtualizing tool. Pay attention that host PC has windows 8 environment and 4GB of RAM as mentioned before, ASA image is for ASA 5520 device, figure 18 showed the main diagram of this network.

The procedures of establishing the network from Cisco ASA side using ASDM GUI are as follows:

- Specifying the Authentication method, ASA provides two methods, one using AAA server and the second is by the local user database where new user accounts can be creates, here the second method used.
- Specifying the SSL connection interface, here outside had been chosen, and giving a connection profile name.
- Defining the group policy for user accounts, or creating new group policy.
- Defining device certificate if certificates used for authentication, here PSK (pre shared key) used.

The following figure 24 and 25 shows some of four configurations:

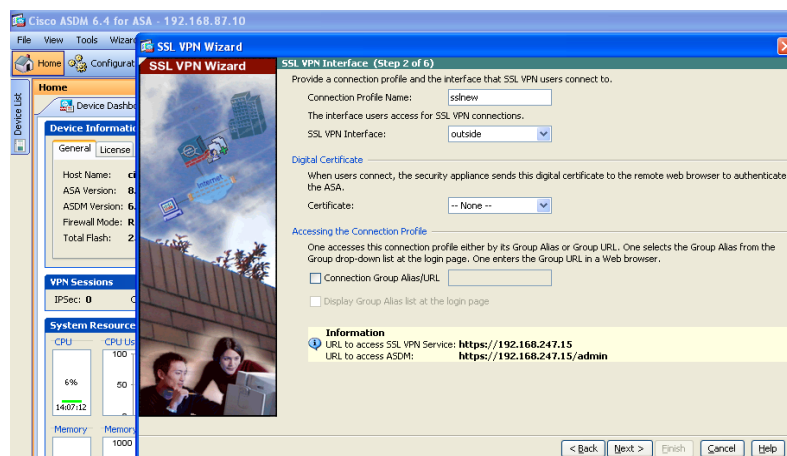


Figure 24 ASA configuration for SSL 1

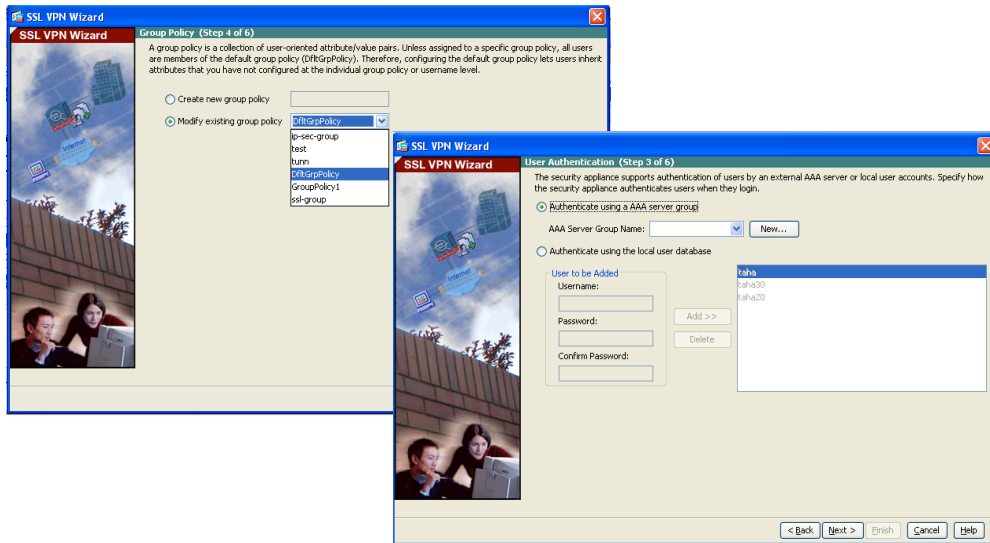


Figure 25 ASA configuration for SSL 2

At the Remote client side a special tools downloaded from ASA called (Cisco any connect client) has used to create a tunnel between client and server and apply the security parameters.



Figure 26 SSL client side

5.6 Establishing L2TP/IPsec VPN network using virtual lab

This section explains the procedures of establishing L2TP/IPsec VPN network based on Windows 2008 server as software VPN gateway in a virtual environment using GNS3 a network emulator and VMware as a virtual machine crating tool. Pay attention that the host PC has windows 8 environment and 4GB of RAM, the following figure shows the main diagram of the network.

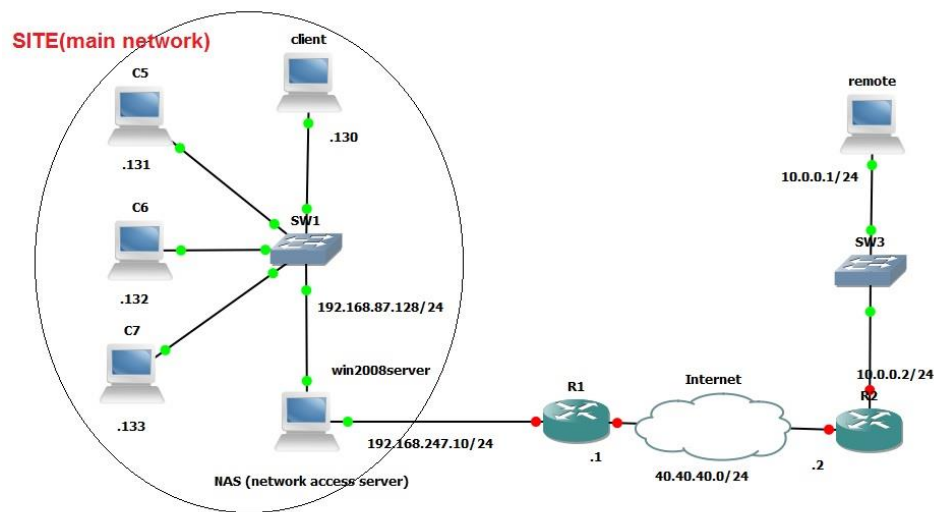


Figure 27 L2TP/IPsec VPN network diagram

The procedures of establishing the network from the main network side are as follows:

- Creating users account with user name and password for each and enabling remote access.
- Configuring routing and remote access to accept connection from outside.
- Configuring new network policy to give access permissions for users from outside.
- Configuring a DHCP server to give suitable IP addresses after connecting.
- Configuring the windows firewall to allow VPN request.

The following figures 28 and 29 shown some of these configurations:

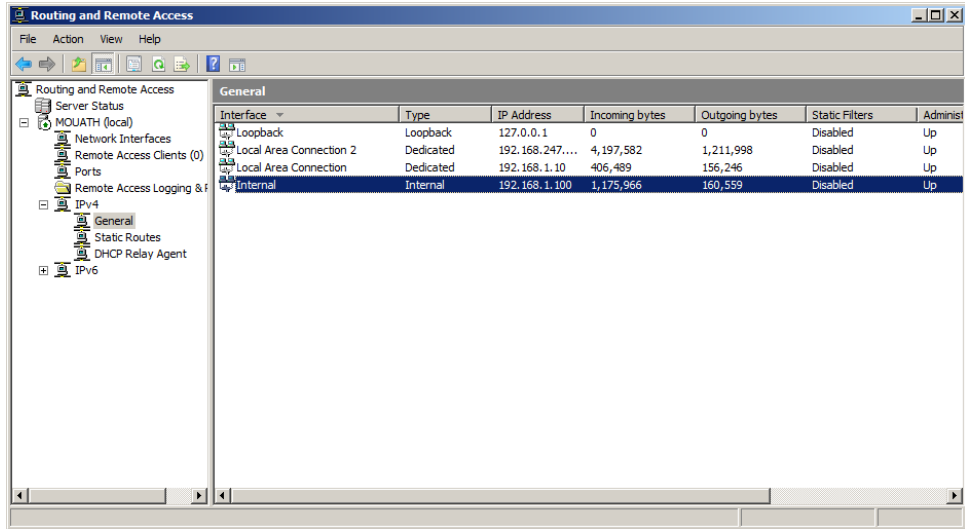


Figure 28 Routing and remote access configurations

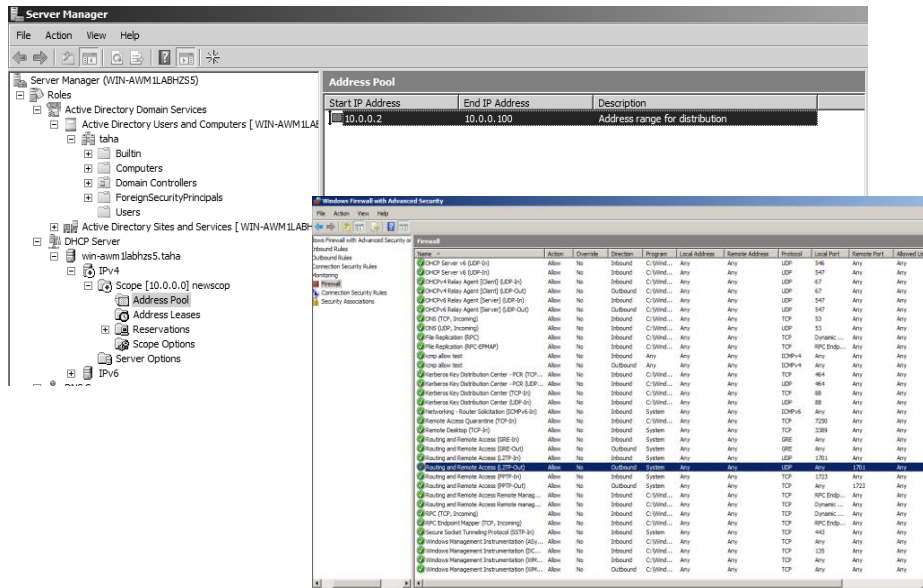


Figure 29 DHCP server and Windows Firewall

At Remote client side a simple configuration has been done by creating new connections and choosing VPN and dialup connection, then give a connection name and the server gateway IP address in addition to the preshare key, and that is all. When the user wants to connect he just has to enter the username and the password, the following figure shows simple explanation:

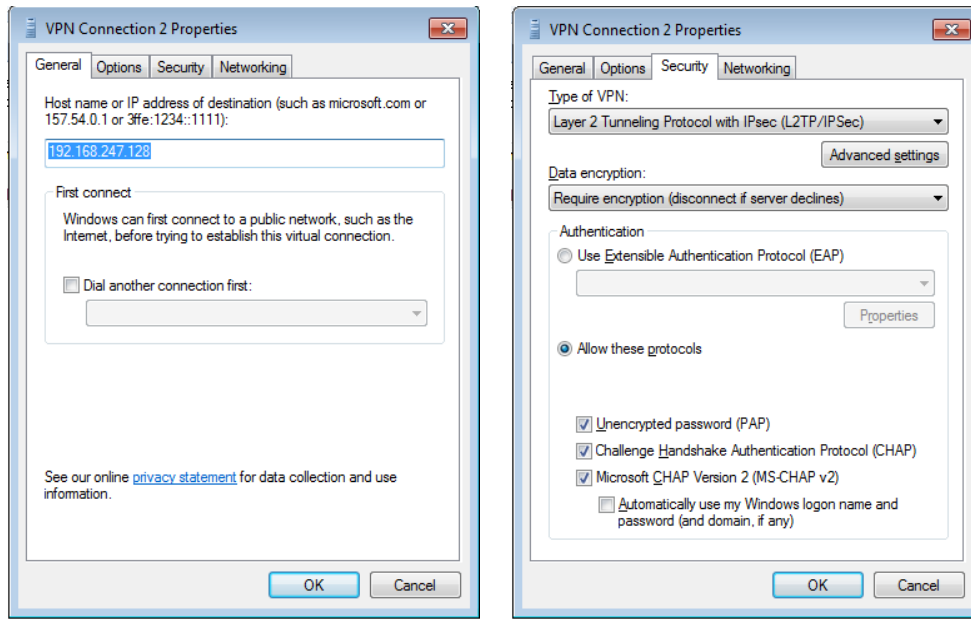


Figure 30 Client side connection configurations 1

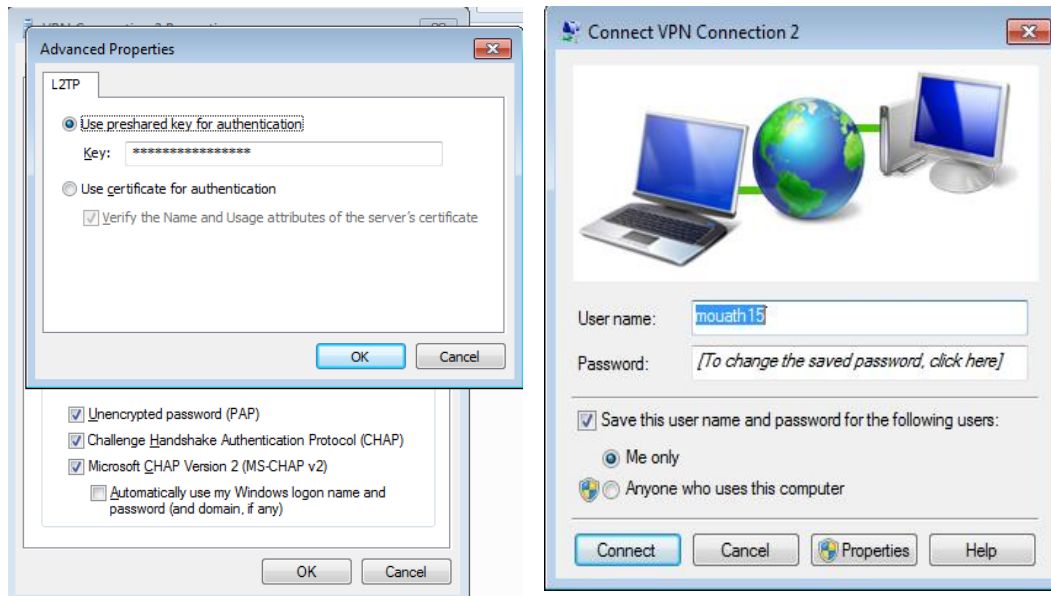


Figure 31 Client side connection configurations 2

CHAPTER 6

RESULTS

6.1 Overview

This chapter will introduce a detailed discussion of the obtained results for the protocols involving the SSL, L2TP/IPSec, and the PPTP, the obtained results are engaged with the required diagrams and graphs.

6.2 Test Result

6.2.1 Jperf and Iperf Bandwidth Results

Bandwidth Results for SSL:

By using the Jperf and Iperf we obtained the real-time graph for the bandwidth of the SSL protocol in interval of 10 second, first we execute the Iperf from the Jperf and then we saved the data of output results and finally the JPerf presented the data result in graph as shown in the figures (32, 33, 34) below:

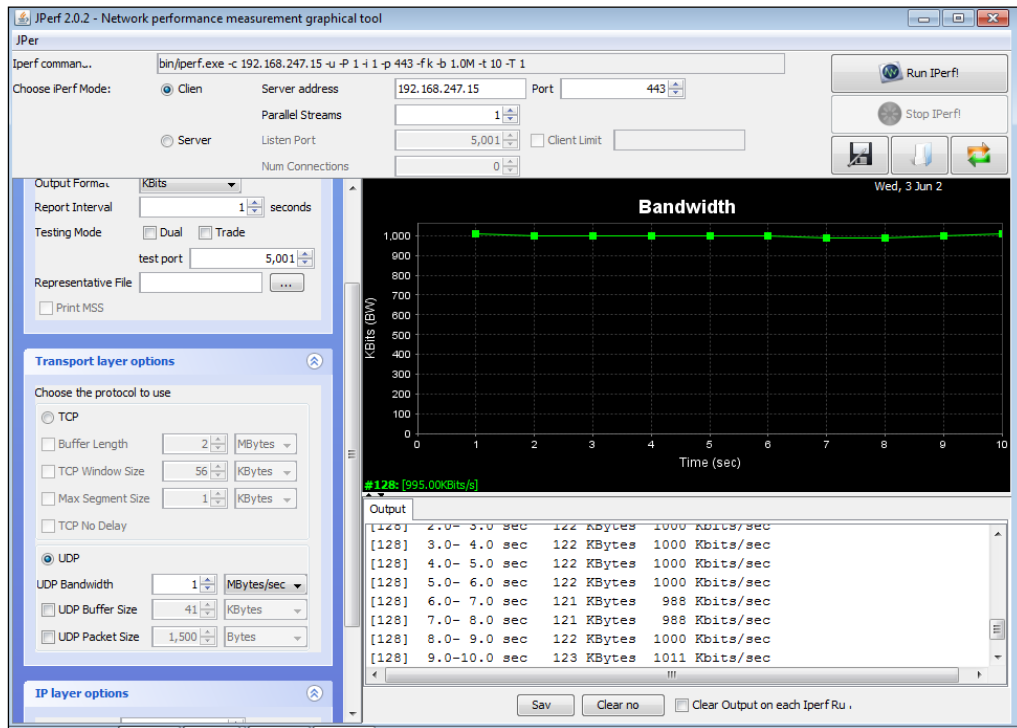


Figure 32 Measuring the bandwidth of SSL using the Jperf

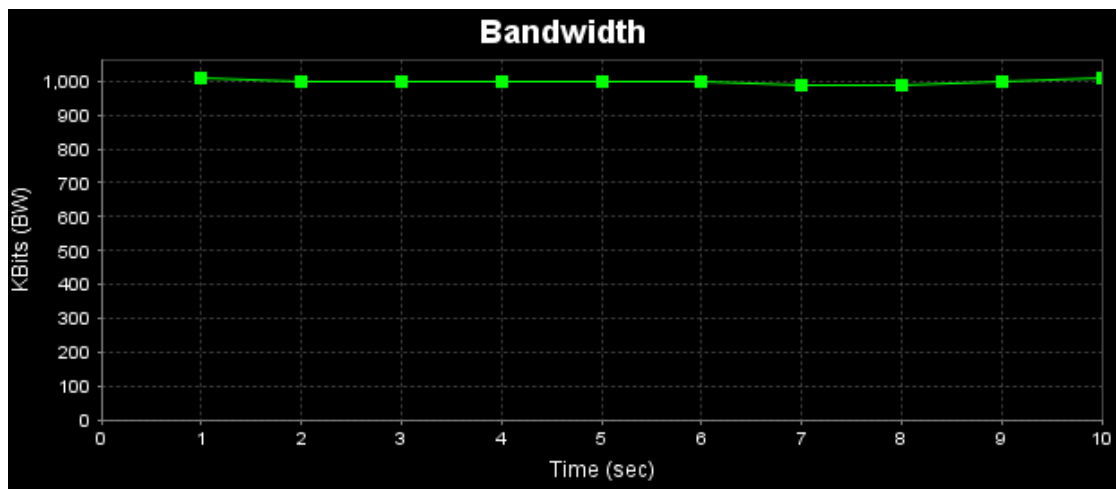


Figure 33 The bandwidth of SSL in (Kbits/ sec)

```
bin/iperf.exe -c 192.168.87.1 -P 1 -i 1 -p 443 -C -f k -t 10 -T 1
```

Client connecting to 192.168.87.1, TCP port 443
TCP window size: 8.00 KByte (default)

```
[128] local 192.168.87.20 port 49295 connected with 192.168.87.1 port 443
[ ID] Interval      Transfer    Bandwidth
[128] 0.0- 1.0 sec  8.00 KBytes 65.5 Kbits/sec
[128] 1.0- 2.0 sec  8.00 KBytes 65.5 Kbits/sec
[128] 2.0- 3.0 sec  8.00 KBytes 65.5 Kbits/sec
[128] 3.0- 4.0 sec 16.0 KBytes 131 Kbits/sec
[128] 4.0- 5.0 sec  8.00 KBytes 65.5 Kbits/sec
[128] 5.0- 6.0 sec  8.00 KBytes 65.5 Kbits/sec
[128] 6.0- 7.0 sec 24.0 KBytes 197 Kbits/sec
[128] 7.0- 8.0 sec 16.0 KBytes 131 Kbits/sec
[128] 8.0- 9.0 sec 16.0 KBytes 131 Kbits/sec
[128] 9.0-10.0 sec  8.00 KBytes 65.5 Kbits/sec
Done.
```

Figure 34 Sample of data result from IPerf for SSL protocol

Bandwidth Results for PPTP:

By using the Jperf and Iperf we obtained the real-time graph for the bandwidth of the PPTP protocol in interval of 10 second. First we execute the Iperf from the Jperf and then we saved the data of output results and finally the JPerf presented the data result in a graph, it is shown in figure 35.

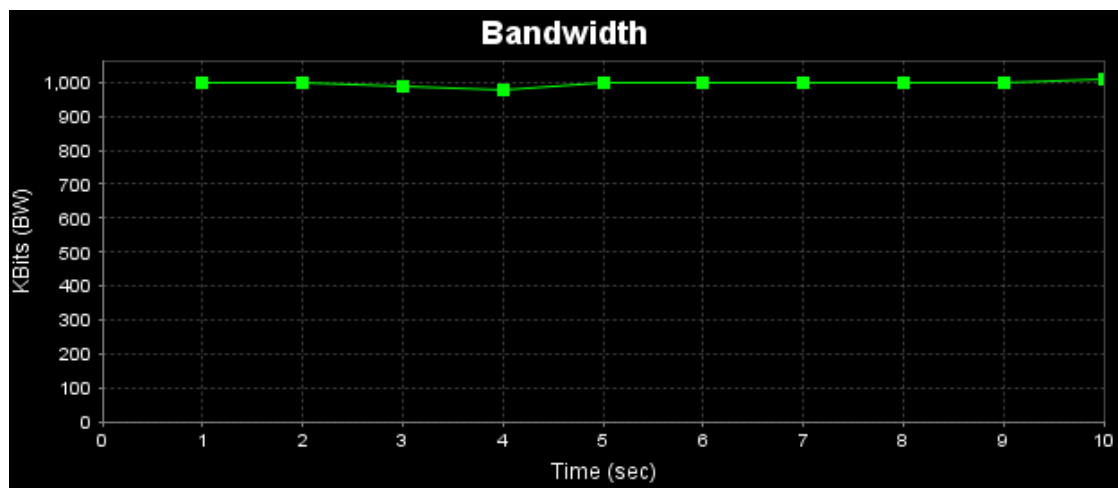


Figure 35 The bandwidth of PPTP in (Kbits / sec)

```

bin/iperf.exe -c 192.168.247.128 -u -P 1 -i 1 -p 1723 -f k -b 1.0M -t 10 -T 1 -S 0x04
-----
Client connecting to 192.168.247.128, UDP port 1723
Sending 1470 byte datagrams
UDP buffer size: 8.00 KByte (default)
-----
[128] local 10.0.0.129 port 62119 connected with 192.168.247.128 port 1723
[ ID] Interval      Transfer    Bandwidth
[128] 0.0- 1.0 sec  122 KBytes  1000 Kbits/sec
[128] 1.0- 2.0 sec  122 KBytes  1000 Kbits/sec
[128] 2.0- 3.0 sec  121 KBytes  988 Kbits/sec
[128] 3.0- 4.0 sec  119 KBytes  976 Kbits/sec
[128] 4.0- 5.0 sec  122 KBytes  1000 Kbits/sec
[128] 5.0- 6.0 sec  122 KBytes  1000 Kbits/sec
[128] 6.0- 7.0 sec  122 KBytes  1000 Kbits/sec
[128] 7.0- 8.0 sec  122 KBytes  1000 Kbits/sec
[128] 8.0- 9.0 sec  122 KBytes  1000 Kbits/sec
[128] 9.0-10.0 sec  123 KBytes  1011 Kbits/sec
[128] 0.0-10.1 sec  1219 KBytes  992 Kbits/sec
[128] WARNING: did not receive ack of last datagram after 10 tries.
[128] Sent 849 datagrams
Done.

```

Figure 36 Sample of data result from IPerf for PPTP protocol

Bandwidth Results for the L2TP/IPsec hypird:

By using the Jperf and Iperf we obtained the real-time graph for the bandwidth of the L2TP protocol in interval of 10 second. First we execute the Iperf from the Jperf and then we saved the data of output results and finally the JPerf presented the data result in graph.

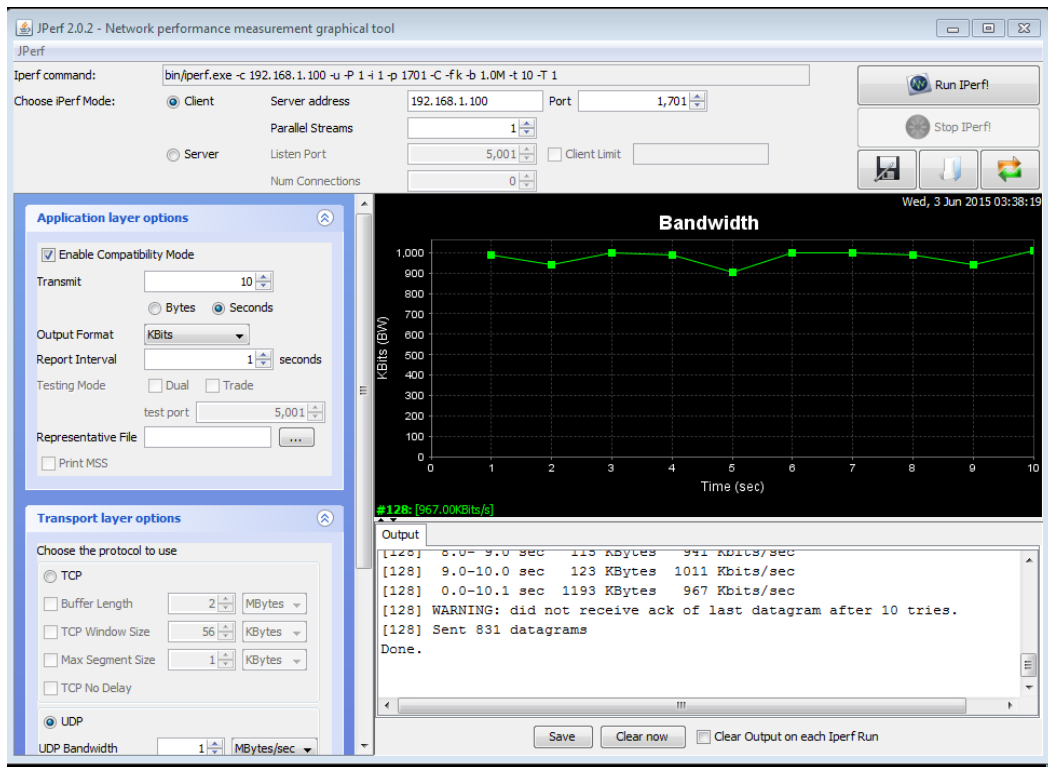


Figure 37 Measuring the bandwidth of L2TP/IPsec using the Jperf

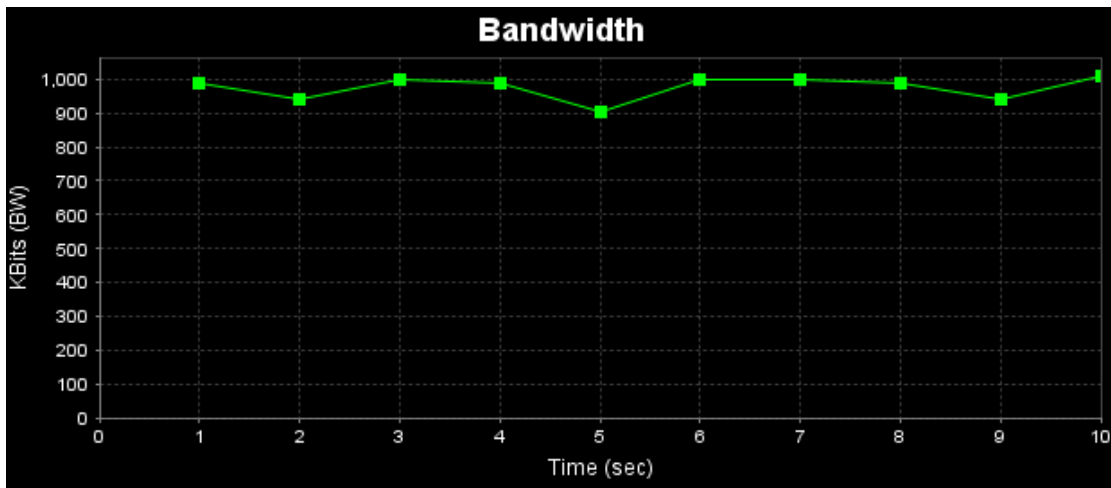


Figure 38 The bandwidth of L2TP/IPsec in (KBits / sec)

	Done.
-C -f k -b 1.0M -t 10 -T 1	bin/iperf.exe -c 192.168.1.100 -u -P 1 -i 1 -p 1701

	Client connecting to 192.168.1.100, UDP port 1701 Sending 1470 byte datagrams UDP buffer size: 8.00 KByte (default)

192.168.1.100 port 1701	[128] local 192.168.1.108 port 60647 connected with [ID] Interval Transfer Bandwidth
	[128] 0.0- 1.0 sec 121 KBytes 988 Kbits/sec
	[128] 1.0- 2.0 sec 115 KBytes 941 Kbits/sec
	[128] 2.0- 3.0 sec 122 KBytes 1000 Kbits/sec
	[128] 3.0- 4.0 sec 121 KBytes 988 Kbits/sec
	[128] 4.0- 5.0 sec 111 KBytes 906 Kbits/sec
	[128] 5.0- 6.0 sec 122 KBytes 1000 Kbits/sec
	[128] 6.0- 7.0 sec 122 KBytes 1000 Kbits/sec
	[128] 7.0- 8.0 sec 121 KBytes 988 Kbits/sec
	[128] 8.0- 9.0 sec 115 KBytes 941 Kbits/sec
	[128] 9.0-10.0 sec 123 KBytes 1011 Kbits/sec
	[128] 0.0-10.1 sec 1193 KBytes 967 Kbits/sec
after 10 tries.	[128] WARNING: did not receive ack of last datagram [128] Sent 831 datagrams
	Done.

Figure 39 Sample of data result from Iperf for L2TP/IPsec protocol

6.2.2 Ping RTT Results

Ping Results for SSL:

```

C:\Windows\system32\cmd.exe
Reply from 192.168.1.100: bytes=32 time=39ms TTL=128
Reply from 192.168.1.100: bytes=32 time=39ms TTL=128
Reply from 192.168.1.100: bytes=32 time=40ms TTL=128
Reply from 192.168.1.100: bytes=32 time=41ms TTL=128
Reply from 192.168.1.100: bytes=32 time=41ms TTL=128
Reply from 192.168.1.100: bytes=32 time=53ms TTL=128
Reply from 192.168.1.100: bytes=32 time=42ms TTL=128
Reply from 192.168.1.100: bytes=32 time=38ms TTL=128
Reply from 192.168.1.100: bytes=32 time=38ms TTL=128
Reply from 192.168.1.100: bytes=32 time=45ms TTL=128
Reply from 192.168.1.100: bytes=32 time=43ms TTL=128
Reply from 192.168.1.100: bytes=32 time=36ms TTL=128
Reply from 192.168.1.100: bytes=32 time=37ms TTL=128
Reply from 192.168.1.100: bytes=32 time=39ms TTL=128
Reply from 192.168.1.100: bytes=32 time=41ms TTL=128
Reply from 192.168.1.100: bytes=32 time=43ms TTL=128
Reply from 192.168.1.100: bytes=32 time=36ms TTL=128
Reply from 192.168.1.100: bytes=32 time=38ms TTL=128
Reply from 192.168.1.100: bytes=32 time=40ms TTL=128
Reply from 192.168.1.100: bytes=32 time=42ms TTL=128

Ping statistics for 192.168.1.100:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 33ms, Maximum = 69ms, Average = 39ms

C:\>

```

Figure 40 Ping and RTT in SSL protocol

Ping Results for PPTP as shown in the figure 41:

```
Reply from 192.168.87.1: bytes=32 time=37ms TTL=128
Reply from 192.168.87.1: bytes=32 time=31ms TTL=128
Reply from 192.168.87.1: bytes=32 time=329ms TTL=128
Reply from 192.168.87.1: bytes=32 time=35ms TTL=128
Reply from 192.168.87.1: bytes=32 time=37ms TTL=128
Reply from 192.168.87.1: bytes=32 time=40ms TTL=128
Reply from 192.168.87.1: bytes=32 time=42ms TTL=128
Reply from 192.168.87.1: bytes=32 time=34ms TTL=128
Reply from 192.168.87.1: bytes=32 time=36ms TTL=128
Reply from 192.168.87.1: bytes=32 time=39ms TTL=128
Reply from 192.168.87.1: bytes=32 time=40ms TTL=128
Reply from 192.168.87.1: bytes=32 time=32ms TTL=128
Reply from 192.168.87.1: bytes=32 time=40ms TTL=128
Reply from 192.168.87.1: bytes=32 time=31ms TTL=128
Reply from 192.168.87.1: bytes=32 time=37ms TTL=128
Reply from 192.168.87.1: bytes=32 time=39ms TTL=128
Reply from 192.168.87.1: bytes=32 time=41ms TTL=128
Reply from 192.168.87.1: bytes=32 time=44ms TTL=128
Reply from 192.168.87.1: bytes=32 time=35ms TTL=128
Reply from 192.168.87.1: bytes=32 time=37ms TTL=128

Ping statistics for 192.168.87.1:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 31ms, Maximum = 329ms, Average = 44ms

C:\>_
```

Figure 41 Ping RTT for PPTP protocol

Ping Results for the L2TP/ IPsec As shown in the figure 42:

```
Reply from 192.168.1.100: bytes=32 time=39ms TTL=128
Reply from 192.168.1.100: bytes=32 time=39ms TTL=128
Reply from 192.168.1.100: bytes=32 time=40ms TTL=128
Reply from 192.168.1.100: bytes=32 time=41ms TTL=128
Reply from 192.168.1.100: bytes=32 time=41ms TTL=128
Reply from 192.168.1.100: bytes=32 time=53ms TTL=128
Reply from 192.168.1.100: bytes=32 time=42ms TTL=128
Reply from 192.168.1.100: bytes=32 time=38ms TTL=128
Reply from 192.168.1.100: bytes=32 time=38ms TTL=128
Reply from 192.168.1.100: bytes=32 time=45ms TTL=128
Reply from 192.168.1.100: bytes=32 time=43ms TTL=128
Reply from 192.168.1.100: bytes=32 time=36ms TTL=128
Reply from 192.168.1.100: bytes=32 time=37ms TTL=128
Reply from 192.168.1.100: bytes=32 time=39ms TTL=128
Reply from 192.168.1.100: bytes=32 time=41ms TTL=128
Reply from 192.168.1.100: bytes=32 time=43ms TTL=128
Reply from 192.168.1.100: bytes=32 time=36ms TTL=128
Reply from 192.168.1.100: bytes=32 time=38ms TTL=128
Reply from 192.168.1.100: bytes=32 time=40ms TTL=128
Reply from 192.168.1.100: bytes=32 time=42ms TTL=128

Ping statistics for 192.168.1.100:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 33ms, Maximum = 69ms, Average = 39ms

C:\>_
```

Figure 42 Ping RTT for the L2TP / IPsec hypird

CHAPTER 7

DISCUSSION

In this chapter we will analyze the obtained measurements and results.

7.1 Bandwidth and throughput comparison among SSL, PPTP, L2TP/IPsec

Bandwidth tests have been performed by using the Jperf program. In those tests the JAVA GUI-based version of Jperf application has been used. Jperf calculates the bandwidth based on the size of transmitted data. The single measurement cycle is based on two end hosts where one of them is the server and the other acts as a client machine. The server listens for incoming connections and the client sends data. It has to be decided which port will be used for data measurement. The client must use the same port number as the server. In each single case, a single measurement lasts for 10s, where each single measurement value is taken every second. In the first test SSL protocol was investigated and the resulted graph was shown in Figure 44, the result bandwidth value is above 900 kbit/s, in reality the average link bandwidth was 999 kbit/s.

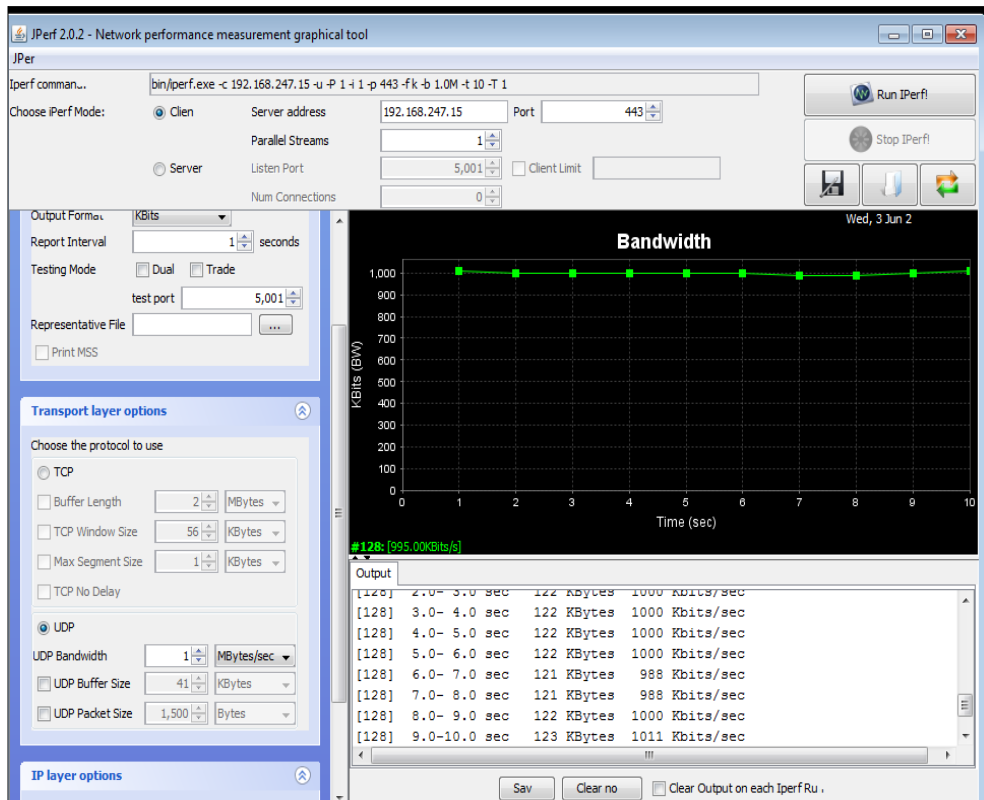


Figure 43 Sample of data result from SSL protocol

The similar test was performed for PPTP protocol, where average bandwidth was 996 kbit/s as shown in figure 43, and the obtained bandwidth result for L2TP protocol was 957 kbit/s as shown in figure 44.

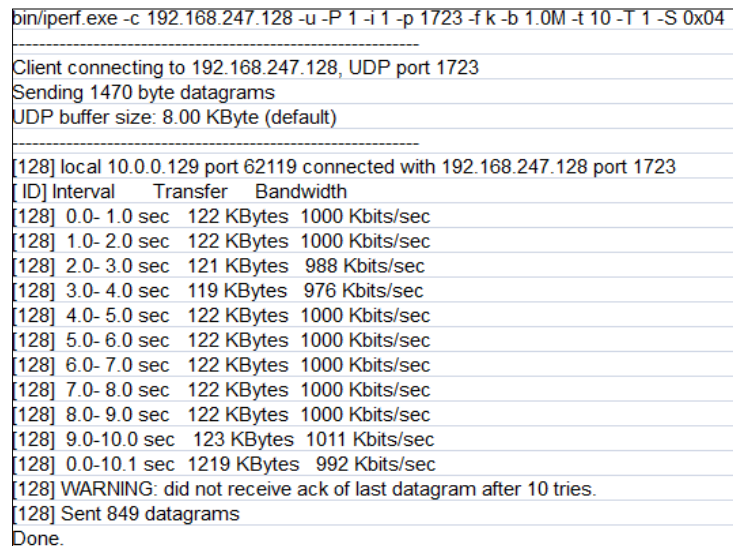


Figure 44 Sample of data result from IPerf for PPTP protocol

```

bin/iperf.exe -c 192.168.1.100 -P 1 -i 1 -p 1701 -C
Done.

bin/iperf.exe -c 192.168.1.100 -u -P 1 -i 1 -p 1701
-----
Client connecting to 192.168.1.100, UDP port 1701
Sending 1470 byte datagrams
UDP buffer size: 8.00 KByte (default)
-----
[128] local 192.168.1.108 port 60647 connected with
[ ID] Interval      Transfer    Bandwidth
[128] 0.0- 1.0 sec   121 KBytes  988 Kbits/sec
[128] 1.0- 2.0 sec   115 KBytes  941 Kbits/sec
[128] 2.0- 3.0 sec   122 KBytes 1000 Kbits/sec
[128] 3.0- 4.0 sec   121 KBytes  988 Kbits/sec
[128] 4.0- 5.0 sec   111 KBytes  906 Kbits/sec
[128] 5.0- 6.0 sec   122 KBytes 1000 Kbits/sec
[128] 6.0- 7.0 sec   122 KBytes 1000 Kbits/sec
[128] 7.0- 8.0 sec   121 KBytes  988 Kbits/sec
[128] 8.0- 9.0 sec   115 KBytes  941 Kbits/sec
[128] 9.0-10.0 sec   123 KBytes 1011 Kbits/sec
[128] 0.0-10.1 sec   1193 KBytes  967 Kbits/sec
[128] WARNING: did not receive ack of last datagram
[128] Sent 831 datagrams
Done.

```

Figure 45 Measuring the bandwidth of L2tp/IPsec using the Jperf

As mentioned earlier, the Jperf application works by measuring amounts of transferred data. VPN tunnels support data compression which is the lower values of bandwidth was in L2TP protocol and highest bandwidth result was in SSL protocol.

7.1.1 UDP Throughput

UDP throughput is measured according to UDP window size, time of test, and the number of flows (parallel streams). These experiments were repeated number of times to find the average UDP throughput.

The results of these experiments are based on figure 42, figure 43, and figure 44 and the following tables are brief of throughput results in each protocol. Table 4 includesthroughput values to the SSL protocol, Table 5 for PPTP protocol and the last one for L2TP protocol.

Interval time	Throughput
3	122
4	122
5	122
6	121
7	121
8	122
9	123

Table 4 SSL Throughput Values

Interval time	Throughput
3	119
4	122
5	122
6	122
7	122
8	122
9	123

Table 5 PPTP Throughput Values

Interval time	Throughput
3	121
4	111
5	122
6	122
7	121
8	115
9	123

Table 6 L2TP Throughput Values

The following figure shown a comparison among the PPTP, SSL, and L2TP/IPsec protocols from the Throughputs point of views

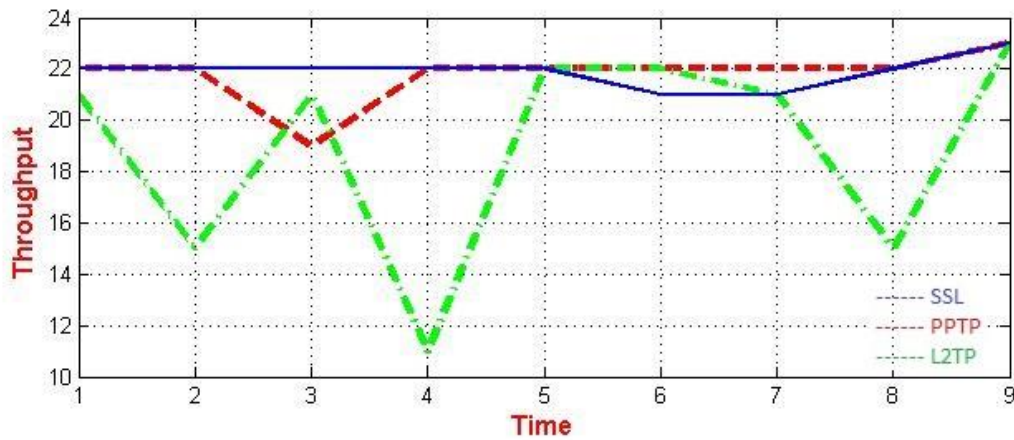


Figure 46 Throughputs comparison between SSL, PPTP, L2TP/IPsec

The results of these tables and this graph represent the final throughput results. These indicate clearly that the PPTP on windows server has produced the best UDP throughput value, the SSL on ASA has produced meduiam value for UDP throughput, the L2TP/IPSec has produced the lowest UDP throughput values.

7.2 RTT comparison between SSL, PPTP , L2TP

We can measure the RTT round-trip time by using Pinging, most times are measured in milliseconds, in addition to measure the packet loss, the following figure presents RTT measurement for each protocol. Figure 47 shows the ping result using SSL protocol, and figure 48 shows test ping for PPTP protocol and figure 49 presents the L2TP protocol.


```
C:\Windows\system32\cmd.exe
Reply from 192.168.1.100: bytes=32 time=39ms TTL=128
Reply from 192.168.1.100: bytes=32 time=39ms TTL=128
Reply from 192.168.1.100: bytes=32 time=40ms TTL=128
Reply from 192.168.1.100: bytes=32 time=41ms TTL=128
Reply from 192.168.1.100: bytes=32 time=41ms TTL=128
Reply from 192.168.1.100: bytes=32 time=53ms TTL=128
Reply from 192.168.1.100: bytes=32 time=42ms TTL=128
Reply from 192.168.1.100: bytes=32 time=38ms TTL=128
Reply from 192.168.1.100: bytes=32 time=38ms TTL=128
Reply from 192.168.1.100: bytes=32 time=45ms TTL=128
Reply from 192.168.1.100: bytes=32 time=43ms TTL=128
Reply from 192.168.1.100: bytes=32 time=36ms TTL=128
Reply from 192.168.1.100: bytes=32 time=37ms TTL=128
Reply from 192.168.1.100: bytes=32 time=39ms TTL=128
Reply from 192.168.1.100: bytes=32 time=41ms TTL=128
Reply from 192.168.1.100: bytes=32 time=43ms TTL=128
Reply from 192.168.1.100: bytes=32 time=36ms TTL=128
Reply from 192.168.1.100: bytes=32 time=38ms TTL=128
Reply from 192.168.1.100: bytes=32 time=38ms TTL=128
Reply from 192.168.1.100: bytes=32 time=40ms TTL=128
Reply from 192.168.1.100: bytes=32 time=42ms TTL=128

Ping statistics for 192.168.1.100:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 33ms, Maximum = 69ms, Average = 39ms

C:\>
```

Figure 47 Ping and RTT in SSL protocol

```
C:\Windows\system32\cmd.exe
Reply from 192.168.87.1: bytes=32 time=34ms TTL=128
Reply from 192.168.87.1: bytes=32 time=38ms TTL=128
Reply from 192.168.87.1: bytes=32 time=42ms TTL=128
Reply from 192.168.87.1: bytes=32 time=34ms TTL=128
Reply from 192.168.87.1: bytes=32 time=39ms TTL=128
Reply from 192.168.87.1: bytes=32 time=41ms TTL=128
Reply from 192.168.87.1: bytes=32 time=50ms TTL=128
Reply from 192.168.87.1: bytes=32 time=37ms TTL=128
Reply from 192.168.87.1: bytes=32 time=38ms TTL=128
Reply from 192.168.87.1: bytes=32 time=36ms TTL=128
Reply from 192.168.87.1: bytes=32 time=160ms TTL=128
Reply from 192.168.87.1: bytes=32 time=43ms TTL=128
Reply from 192.168.87.1: bytes=32 time=42ms TTL=128
Reply from 192.168.87.1: bytes=32 time=33ms TTL=128
Reply from 192.168.87.1: bytes=32 time=179ms TTL=128
Reply from 192.168.87.1: bytes=32 time=41ms TTL=128
Reply from 192.168.87.1: bytes=32 time=33ms TTL=128
Reply from 192.168.87.1: bytes=32 time=37ms TTL=128
Reply from 192.168.87.1: bytes=32 time=32ms TTL=128
Reply from 192.168.87.1: bytes=32 time=37ms TTL=128
Reply from 192.168.87.1: bytes=32 time=40ms TTL=128
Reply from 192.168.87.1: bytes=32 time=102ms TTL=128
Reply from 192.168.87.1: bytes=32 time=34ms TTL=128
Reply from 192.168.87.1: bytes=32 time=36ms TTL=128
Reply from 192.168.87.1: bytes=32 time=39ms TTL=128
Reply from 192.168.87.1: bytes=32 time=41ms TTL=128
Reply from 192.168.87.1: bytes=32 time=33ms TTL=128
Reply from 192.168.87.1: bytes=32 time=39ms TTL=128
Reply from 192.168.87.1: bytes=32 time=31ms TTL=128
Reply from 192.168.87.1: bytes=32 time=329ms TTL=128
Reply from 192.168.87.1: bytes=32 time=35ms TTL=128
Reply from 192.168.87.1: bytes=32 time=37ms TTL=128
Reply from 192.168.87.1: bytes=32 time=40ms TTL=128
Reply from 192.168.87.1: bytes=32 time=42ms TTL=128
Reply from 192.168.87.1: bytes=32 time=34ms TTL=128
Reply from 192.168.87.1: bytes=32 time=36ms TTL=128
Reply from 192.168.87.1: bytes=32 time=39ms TTL=128
Reply from 192.168.87.1: bytes=32 time=40ms TTL=128
Reply from 192.168.87.1: bytes=32 time=32ms TTL=128
Reply from 192.168.87.1: bytes=32 time=40ms TTL=128
Reply from 192.168.87.1: bytes=32 time=31ms TTL=128
Reply from 192.168.87.1: bytes=32 time=37ms TTL=128
Reply from 192.168.87.1: bytes=32 time=39ms TTL=128
Reply from 192.168.87.1: bytes=32 time=41ms TTL=128
Reply from 192.168.87.1: bytes=32 time=44ms TTL=128
Reply from 192.168.87.1: bytes=32 time=35ms TTL=128
Reply from 192.168.87.1: bytes=32 time=37ms TTL=128

Ping statistics for 192.168.87.1:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 31ms, Maximum = 329ms, Average = 44ms

C:\>
```

Figure 48 Ping and RTT in PPTP protocol

```

C:\Windows\system32\cmd.exe
Reply from 192.168.1.100: bytes=32 time=39ms TTL=128
Reply from 192.168.1.100: bytes=32 time=39ms TTL=128
Reply from 192.168.1.100: bytes=32 time=40ms TTL=128
Reply from 192.168.1.100: bytes=32 time=41ms TTL=128
Reply from 192.168.1.100: bytes=32 time=41ms TTL=128
Reply from 192.168.1.100: bytes=32 time=53ms TTL=128
Reply from 192.168.1.100: bytes=32 time=42ms TTL=128
Reply from 192.168.1.100: bytes=32 time=38ms TTL=128
Reply from 192.168.1.100: bytes=32 time=38ms TTL=128
Reply from 192.168.1.100: bytes=32 time=45ms TTL=128
Reply from 192.168.1.100: bytes=32 time=43ms TTL=128
Reply from 192.168.1.100: bytes=32 time=36ms TTL=128
Reply from 192.168.1.100: bytes=32 time=37ms TTL=128
Reply from 192.168.1.100: bytes=32 time=39ms TTL=128
Reply from 192.168.1.100: bytes=32 time=41ms TTL=128
Reply from 192.168.1.100: bytes=32 time=43ms TTL=128
Reply from 192.168.1.100: bytes=32 time=36ms TTL=128
Reply from 192.168.1.100: bytes=32 time=38ms TTL=128
Reply from 192.168.1.100: bytes=32 time=40ms TTL=128
Reply from 192.168.1.100: bytes=32 time=42ms TTL=128

Ping statistics for 192.168.1.100:
    Packets: Sent = 100, Received = 100, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 33ms, Maximum = 69ms, Average = 39ms

C:\>

```

Figure 49 Ping and RTT in L2TP protocol

The following table shows a comparison between the three protocols based on RTT min, max, and average values.

RTT (ms)	Min	Max	Average
SSL	33	69	39
PPTP	31	329	44
L2TP	33	69	39

Table 7 Comparison between Min, Max, and Avg Values of RTT

The table shows that the VPN tunneling using PPTP protocol requires maximum time to send and receive a packet, its maximum value reaches 329 ms within an average of 44ms.

The results of these experiments are presented in figures: 47, 48, 49; These figures indicate clearly that the SSL on ASA has produced the best RTT values, The L2TP/IPSec on windows server has produced the Same as SSL RTT values, the PPTP on windows server has produced the least values. Note : No enough test to cpu utilization and packet loss. Figure 50 shows that graphically:

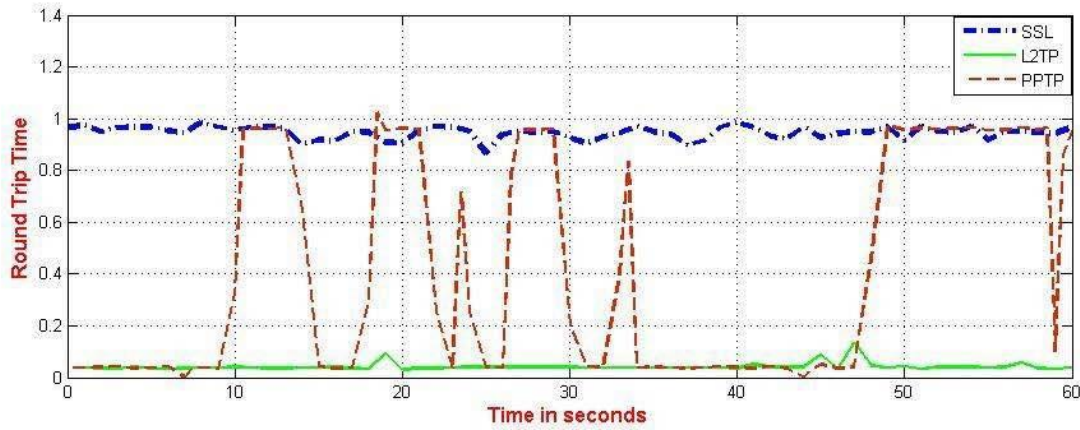


Figure 50 RTT Comparison between SSL, PPTP , L2TP

CHAPTER 8

CONCLUSION AND FUTURE WORK

8.1 Overview

This project has presented an experimental performance evaluation for the remote access VPNs, namely PPTP, L2TP/IPSec, and SSL on both windows server and cisco ASA. The following conclusions are obtained from investigating the output results described above:

- Due to the smallest overhead packets that have been introduced by PPTP, PPTP , windows server has produced the best performance values for UDP-based user applications.
- In order to have strong security, L2TP/IPSec combines L2TP's tunnel with IPSec's secure channel which increases the overhead packets. So, L2TP/IPSec on both windows server and ASA have produced a good performance values for UDP-based user applications.
- Because SSL was written as a user space daemon rather than a kernel module, SSL on both windows server and ASA have produced a low performance values in high traffic environments for the UDP-based user applications.
- The SSL needs to be manipulated to improve its performance with UDP-based user applications.

8.2 Security in VPN

SSL considered as a very secure protocol; many VPN companies are working to strengthen their VPN implementation . It would be great if providers also started to move away NIST standards, but for that we shall wait and see.

- PPTP is very insecure and should be avoided as much as possible . But it is easy to setup, and cross platform compatibility are attractive, L2TP/IPsec has the same advantages and is much more secure.
- L2TP/IPsec is a good VPN solution for non-critical use, although it has been severely weakened by the NSA. But it's good for a quick VPN setup without the need to install extra software it remains useful, particularly for mobile devices where SSL support remains somewhat patchy .
- Obviously, The SSL is the best all round VPN solution, despite needing third party software on all platforms. It is reliable, fast, and- themost important point-; secure; (even compared tothe NSA), although it usually needs a bit more setting up than the other protocols.

So basically, when security is more essential than performance;, you should choose SSL (or possibly IKEv2 if the option is available, especially for mobile devices). But if it is needed to have a quick solution,(such as for protecting your phone from casual criminals when connecting to public WiFi hotspot) then L2TP/IPsec will probably be the suitable choice,, given that the availability of SSL apps for mobile devices (especially Android) is growingly increasing.

PPTP is common and easy to set up. PPTP clients are built into many platforms, including Windows;That's the only advantage, and it's not worth it. It's time to move on.

Summary:

For the throughput, PPTP protocol has better values than the SSL, hence SSI is medium between the PPTP and the L2TP/IPsec,, where the L2TP/IPsec has the lowest performance. In terms of RTT it is clear that the SSL protocol has the highest values, L2TP/IPsec also has similar values. While PPTP protocol has the lowest values.

PPTP is old and vulnerable, although integrated into common operating systems and easy to set up. Stay away.

8.3 Future Work

The future of supporting VPN server is still exploring more possibilities of VPN implementation on stations. In fact, VPN can bring many benefits like establishing secure connection over Internet, and providing easy accessibility to internet. . And we believe that it much more applications will be provided relying on this technology..

For SSL -which is a good VPN solution that runs in user space-; many operations are needed to switch between kernel space and user space to process packets. Additional studies must encountered to study the influence of using SSL in Kernel Mode of Linux. Kernel Mode in Linux is an implementation enables user space applications to run in kernel space. The advantage of this appears when the overhead of context switching can be prevented. According to the author of SSL, James Yonan, this will not enhance the performance, but it might be extracted on 1 Gbps connections. A trade-off between stability and performance must be made, but more researches must be made in order to have better comparisons and optimization for the parameters of both security and performance.

REFERENCES

1. **Ferguson, P. Huston, G. 1998.** What is a VPN?.
2. **Stanaway, J. Kumar V. 2001.** Method and Apparatus for Order Independent Processing of Virtual Private Network Protocols. U.s. Patent Application .pp. 1-5.
3. **Moye, F. 2015.** Understanding Virtual Private Networks (VPN), SANS Institute. Pp. 4-5.
4. **Cisco Public Information.2013.Remote-Access VPNs:** Business Productivity, Deployment, and Security Considerations.
5. **Phifer, L. 2011.** Measure Wireless Network Performance using Testing Tool Iperf SearchNetworking.com
6. **Martin Hack and EVP, (2011)** “*Remote Access Challenges, Top 7 Remote Access Myths*”, NCP Engineering, NCP Secure Communications.
7. **Charlie Scott, Paul Wolfe, and Mike Erwin (1999),** “*Virtual Private Networks*”.
8. **Special Administrative Region, (2008),** “*VPN Security* ”, **Hong Kong Government.**
9. **CISCO , (2005),** “*IP Tunneling and VPNs*”.

10. **Syngress.com, (2005)**, “*Advance VPN Concepts and Tunnel Monitoring* ”, Chapter 5.
11. **Microsoft, (2014)**, “*Point To Point Tunneling Protocol (PPTP) Profile* ”, Microsoft.
12. **Hawke Robinson, (2002)**, “*Microsoft PPTP VPN Vulnerabilities Exploits in Action* ”, SANS Institute.
13. **Martin W. Murhammer, Orcun Atakan, Zikrun Badri, Beomjun Cho Hyun Jeong Lee and Alexander Schmid, (1999)**, “*A Comprehensive Guide to Virtual Private Networks*”, International Technical Support Organization, IBM.
14. **James S. Tiller, (2001)**, “*Security of Virtual Private Networks* ”,.
15. **Rajesh and Sajesh, Openvpn Installation and Configuration, 2006**, URL: www.esnips.com/_t_/Openvpn , Accessed on February 2008.
16. **Net Gear Inc., (2005)**, “*Virtual Private Network Basics*”, Chapter 2.
17. **Mijlud M. Alsbabayee, (2005)**, “*Theoretical and Practical Virtual Private Networks*”.
18. **Roy Hills, (2005)**, “*Common VPN Security Flows* ”, NTA monitoring Ltd.
19. **Equinox AG and Equinox USA, (2005)**, “*VPN Configuration Guide* ”.
20. **Bruce Sehneier and Mudge, (2005)**, “*Cryptanalysis of Microsoft Point To Point Tunneling Protocol (PPTP)* ”.

21. **Neon Surge, (2005)**,“*Understanding PPTP and VPN's*”, Rhino9 Publications.
22. **Chris Wilson, (2005)**, “*GNS3 Simulation Guide* ”, Packt Publishing.
23. **VMware, (2006)**, “VMware Server Administration Guide”.

APPENDICES A

CURRICULUM VITAE

PERSONAL INFORMATION

Surname, Name: Abdalrahman, Mouath

Date and Place of Birth: 13 march 1981,iraq

Marital Status: married

Phone: +90 538 065 71 96

Email: mouaths1981@gmail.com



EDUCATION

Degree	Institution	Year of Graduation
M.Sc.	Çankaya Univ., Electronic and Communication Engineering	2015
B.Sc.	Technical College of Mosul	2005
High School	Alghrbea for Boys Secondary	2001

WORK EXPERIENCE

Year	Place	Enrollment
2006- Present	Iraqi Ministry of Electricity Computer Department Official Electronic	Specialist
2004-2005	A special office for computer maintenance	Trainer
2002-2003	IALD Co.	Trainer

FOREIN LANGUAGES

Native Arabic, Advanced English.

PUBLICATIONS

1. Mouath Salim Abdalrahman., “Comparison between Embedding On Edges in Spatial and Frequency Domains”, The Second International Conference on Education Technologies and Computers (ICETC2015) IEEE.

PROJECTS

1. A database project designed by Maker file, The Ministry of Electricity / Electricity distribution Nineveh office, Iraq/Mosul 2010.
2. Project drawing the borders of the province of Nineveh by GIS program, urban planning office, Iraq/Mosul 2011.

HONOURS AND AWARDS

1. Arab Engineers Union 2010 / Egypt
2. Iraqi engineers Association 2012/ Mosul

HOBBIES

Reading, Writing, Billiards, Travel, Networking.