DEVELOPMENT OF WEBSITES FOR SECURE DATA COMMUNICATION TRHOUGH A VIRTUAL PRIVATE NETWORK

Akbor Aziz Susom

POST GRADUATE DIPLOMA IN INFORMATION AND COMMUNICATION TECHNOLOGY

Institute of Information and Communication Technology (IICT)

BANGLADESH UNIVERSITY OF ENGINEERING AND TECHNOLOGY (BUET)

SEPTEMBER 2018

The project titled "DEVELOPMENT OF WEBSITES FOR SECURE DATA COMMUNICATION TRHOUGH A VIRTUAL PRIVATE NETWORK" submitted by Akbor Aziz Susom, Roll No: 1014311002, session: October 2014 has been accepted as satisfactory in partial fulfilment of the requirements for the degree of Post-Graduation Diploma in Information and communication technology on September 30, 2018.

Boards of Examiners:

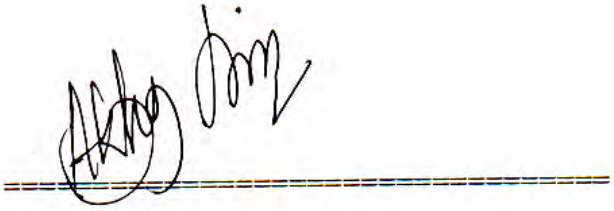
1. Dr. Md. Rubaiyat Hossain Mondal — Chairman (Supervisor)
   Associate Professor
   Institute of Information and Communication Technology (IICT),
   Bangladesh University of Engineering and Technology (BUET),
   Dhaka-1000, Bangladesh.

2. Dr. Md. Saiful Islam — Member
   Professor
   Institute of Information and Communication Technology (IICT),
   Bangladesh University of Engineering and Technology (BUET),
   Dhaka-1000, Bangladesh.

3. Dr. Md. Liakot Ali — Member
   Professor
   Institute of Information and Communication Technology (IICT),
   Bangladesh University of Engineering and Technology (BUET),
   Dhaka-1000, Bangladesh.

Candidate's declaration

It is hereby declared that this report or any part of it has not been submitted elsewhere for the award of any degree and diploma.



AKBOR AZIZ SUSOM

Table of Content

List of Figures

Abbreviations and Key Terms

VPN	Virtual private network
RIP	Routing Information Protocols
IGRP	Interior Gateway Protocol
OSPF	Open Shortest Path First
EIGRP	Enhanced interior gateway routing protocol
BGP	Border Gateway Protocol
EGP	Exterior Gateway Protocol
GNS3	Graphical Network Simulator-3
VLSM	Variable-Length Subnet Masking
IKE	Internet Key Exchange
ISAKMP	Internet security association and key management protocol
AES	Advanced Encryption Standard
SSL	Secure Socket Layer
TLS	Transport Layer security

Acknowledgement

Incipiently, I would like to express my profound gratitude and deep regards to my supervisor Dr. Md. Rubaiyat Hossain Mondal, Associate Professor of IICT, BUET for his guidance and invariable support throughout the project. I have successfully accomplished the goal of the project due to his tireless and patient monitoring during the time of my project. I am extremely grateful to him as he gives me the opportunities and exposure that I never would have had if he had not worked with me.

In addition, I take this opportunity to express my deepest appreciation to the staff of IICT in BUET who provided me the ideas and perception of the IT related activities and the issues of networking through the implementation. I am also so pleased to all the faculty members of IICT for their guidance and support for the successive completion of my graduation degree. Similarly, I would like to acknowledge with much appreciation the crucial role of the Internet Service Officer of Advanced Networking Lab at IICT, BUET.

Moreover, I would like to thank to all my friends, batch-mates for their companion and lifting me up in any type of situation for their inspirative presence with me. I would like to pay my homage to my parents whose encouragement and prayer are always with me and moving with me like a shadow of mine which will protect me in any emergency situation. The name without whom my thanksgiving is incomplete is the Almightily Allah, who allowed me to live in this beautiful world.

Abstract

The use of virtual private network (VPN) has been very popular in network security in order to combat cyber crimes and network vulnerabilities. A virtual private network is essentially a combination of tunneling, encryption, authentication and access control used to carry traffic over the public Internet. For the case of site-to-site VPN, users in different fixed locations can establish secure connections with each other over public networks and access resources from another location. In remote-access VPN, individual users connect to a computer network in a remote location as if they are inherently connected to that network. In developing countries, although many organizations already use VPNs, many private companies, some government institutions and banks are about to use VPNs. Therefore, implementation of VPN between two websites is focused on this project.

In this project, two websites have been developed on each of two servers. The two servers are configured using Apache HTTP Server, PHP and MySQL. Next, a site-to-site VPN is implemented between the two LANs using a pair of Huawei routers and personal computers. A remote access VPN is also implemented using Secure Socket Layer (SSL) and Transport Layer security (TLS).

Furthermore, this research evaluates the routing protocols namely RIPv2, OSPF and EIGRP along with its possible combinations that have been utilized in a hybrid network and VPN in a real time topology using GNS3 on the basis of some parameters- throughput, jitter, packet length and packet loss using Wireshark and Iperf. An intensive simulation process was conducted for each and combined protocols considering two different networks. Moreover, a meaningful comparison of the protocols based on the analysis of the simulation results is also shown in this report. It suggests the best option-either individual or combined routing protocols for different infrastructure of the networks.

The results indicate that EIGRP performs better showing the average highest throughput (28 packet/sec) while average lowest throughput (16 packet/sec) is obtained for combined RIP-OSPF protocol. For jitter, the overall best value is captured for combined RIP-OSPF-EIGRP and OSPF-EIGRP protocols. However, maximum packet size is attained using RIP and OSPF protocols. For better QoS, the lowest value of packet loss is calculated for EIGRP is 2.66 while RIP-OSPF-EIGRP shows the maximum value of packet loss (9.0).

CHAPTER- 1

Introduction

1.1 Introduction:

Connection of group of routers that are used to build different networking systems based on the requirements and affordability mainly follow two basic functions – select a path through networks and then transmit information packet across that selected path to reach the determined destination. In so doing, routing protocols and algorithms play most significant role to plot the routes through networks so that packet can transmit to the most efficient possible paths. First routing protocol shares information among immediate neighbors, and then throughout the network. This way, routers gain information of the topology of the network. Throughout this process, routing protocols follow some criteria based on throughput, delay, efficiency, simplicity, low overhead, reliability/stability, and flexibility. Therefore, performance and efficiency of a networking system is dependent on the routing protocols. As it varies protocol to protocol as well as performance changes in different networking systems. In this experiment, the purpose is to find throughput, jitter, Packet length and packet loss in three different networks with seven different combinations of protocols. Then to compare those results with each other from protocols to protocols, and system to system. However, during the evaluation of two different networks, two different websites have been established which have few options like uploading, downloading. After that, websites are accessed from different devices like computers or mobile phones that are connected in that particular LAN, while those computers are not connected through VPN , could not access the websites . Then it is focused to evaluate the routing protocols performance evaluation to test the performance of that particular networks.

The use of virtual private network (VPN) has been very popular in network security in order to combat cybercrimes and network vulnerabilities. A virtual private network is essentially a combination of tunneling, encryption, authentication and access control used to carry traffic over the public Internet. For the case of site-to-site VPN, users in different fixed locations can establish secure connections with each other over public networks and access resources from

another location. In remote-access VPN, individual users connect to a computer network in a remote location as if they are inherently connected to that network. The effectiveness of VPN becomes more challenging for mobile devices using wireless networks. Therefore, routing protocol selection is also important for VPN network.

As with most complex technologies and requirements for diversity, there's no one-size-fits-all solution when it comes to develop networking systems. The necessity and resources of each unique sector will correlate to a different set of networking systems and solutions. Therefore, development and changes in the development of the networking systems has been a vital need for fulfilling different demands and requirements. It is needed to carefully consider the situation and determine to change the network design for their situation to create an optimized networking solution for that situation. For that reason, in this research report we have analyzed with three different networks on the basis of experimented networks that uses 7 routers then we extended and retracted the system by corresponding 9 and 3 routers respectively to diversify the networking systems.

A network that has been well designed is characterized by consistency and performance of some parameters and protocols used in the networks. A consistently high level of performance is observed with the good combination of different networking protocols. As Routing protocols has significant influence on networking system also each routing protocols have both positive sides and negatives sides on different networking systems. So, we have selected three routing protocols-RIP, OSPF, EIGRP and the hybrid protocols consisting of these three individual ones. An important point to note that all through this study, RIPv2 is considered as RIP. The hybrid protocols considered are RIP-OSPF, RIP-EIGRP, OSPF-EIGRP and RIP-OSPF-EIGRP. It can be noted that the three individual protocols: RIP (version 2), OSPF and EIGRP are supported by VLSM, and these have built in algorithms of Bellman-Ford, Dijkstra and Dual, respectively. These protocols are used for evaluating not any single networking system rather focusing on different networking systems to find the effective and efficient match of routing protocols and algorithms for that specific system and also to suggest whether it satisfies the need of design or

redesign of different networking infrastructure based on some parameters like throughput, Jitter, Packet Length and Packet Loss.

This research is determined to do a comparative analysis of routing protocols alone and combined routing protocols performance in hybrid and VPN networks while websites have been tested to measure the performance and security level of Virtual Private Network. Finally, to suggest the best combination of routing protocols that will meet the requirements of the networking system as well as to show the best performance for the particular computer networks.

1. 2 Related Works

There are several papers [2,3,4,5,6,7] related to Virtual private Network and evaluation of networking protocols performance like dynamic routing protocols- RIP, OSPF and EIGRP and using these protocols to conduct the other scientific research. In paper [2] describes the selection method of authentication protocols for Virtual private Network. In paper [3] they analysis performance of Virtual private Lan service network using Kerberos-enabled protocols (alternative authentication protocols) to measure the throughput value with respect to Normal VPLS network using Wireshark software IO graph. However, some other parameters like Delay, time factor, transmission efficiency is also important to precisely measure the performance of an authentication protocols in VPLS network. In paper [4] shows the configuration of VPN network and performance evaluation for increasing the efficiency for low cost business profit for corporate companies to establish VPN network. Paper [5] evaluated the routing protocols while they also considered combined routing protocols performance in Ipv6 network using iperf software which measured the throughput, jitter and packet loss value in a same networks' platform. After all this result may change with the demand or design of different other computer networks. Besides, Paper [6] experimented the routing protocols for VOIP VPN over MPLS network and it suggests OSPF and BGP-MPLS VPN for better performance. In the paper [7], author examined the performance of Ipv4 and Ipv6 when routing protocols have been utilized in both Ipv4 and Ipv6 virtual networks using GNS3 simulator software. They compared end to end delay and latency result for Ipv4 and Ipv6 and commented Ipv6 is the better choice for these two parameters.

1.3 Objective with specific aims and possible outcome:

The main objective of this project is to ensure secure data communication using hardware-based VPN. This will be achieved by the following tasks:

1. To set up two websites on two different web servers placed in two different local area networks (LANs)

2. To implement site-to-site VPNs on the two LANs having the two websites and to implement a remote access VPN on the two LANs

3. To evaluate different routing protocols for VPNs.

1.4 Outline of this Report:

The rest of the report is organized as follows. Chapter 2 presents the methodology of the study, Chapter 3 describes the related work, and Chapter 4 presents the performance results obtained from computer simulations. Finally, Chapter 5 provides the concluding remarks and future research directions.

CHAPTER- 2

Methodology

The way of implantation of virtual private and hybrid network has been demonstrated in this chapter. The network for each network first established in packet tracer and the same way, it has been developed in GNS3 software for more accurate result. Virtual Private Network has also been developed with Huawei routers creating site to site VPN for the network. The design cited in system design has been followed for testing the network. Besides, simulation process conducted with Iperf, Wireshark and different other simulator for protocol analysis of Virtual Private Network.

2.1 System Design:

Hybrid and Virtual Private Network:

We consider Virtual private networking models and Hybrid network, for this experiment. The models have been developed on the basis of real time topology with combination of 9 routers. Two computers are also connected with the networks for the transmission of the packet to create traffic that is used for simulation purpose of the network. GNS3 software has been used to design the network that is as followed in figure 2.1 and figure 2.1.1 respectively. Both figures have been tested through ensp software for Huawei router and GNS-3 software for Cisco Router. Besides simulation software have been used for testing purpose to understand the performance of the network for combination of different routing protocols.

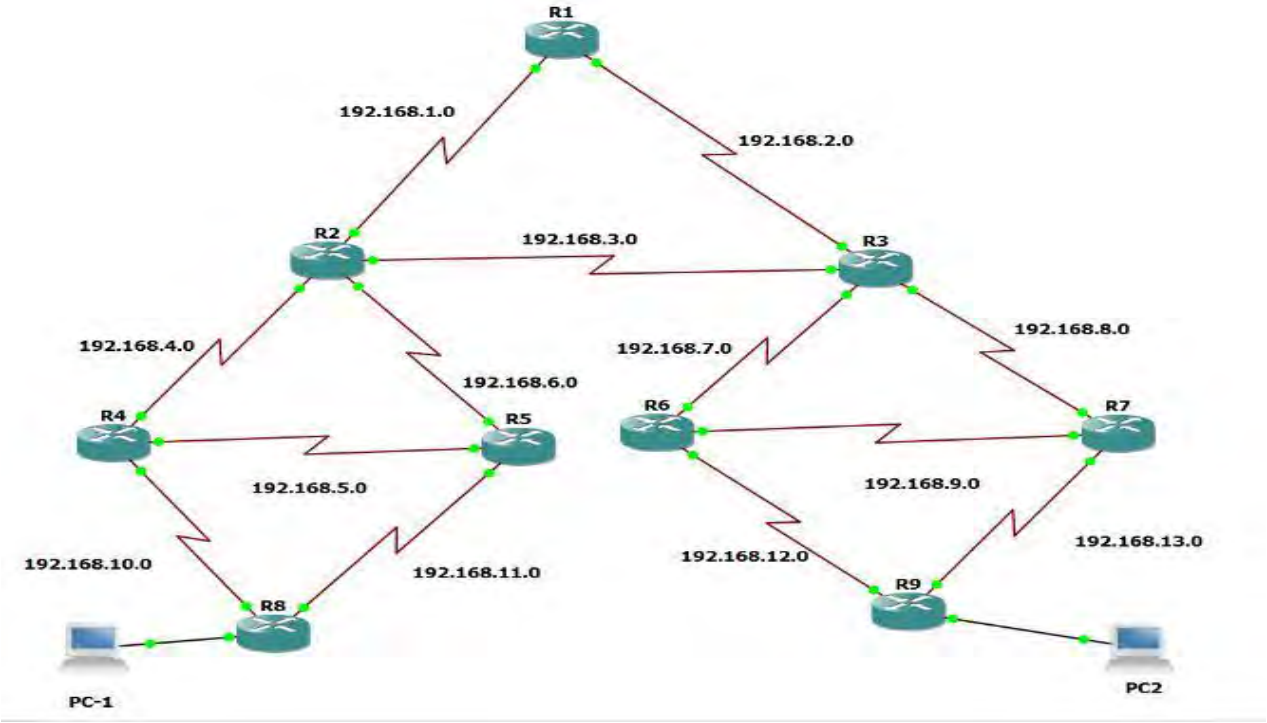


Figure 2.1: Model of a Hybrid network.

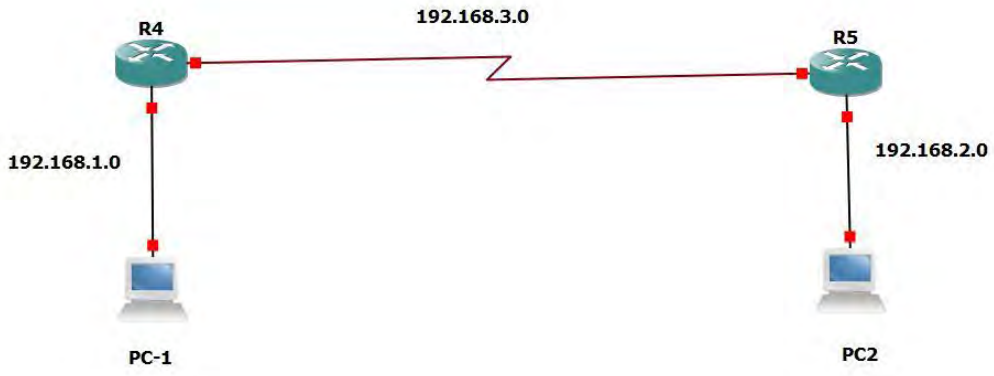


Figure 2.1.1: Model of a Virtual Private Network.

2.2 Procedures

With combination of routing protocols in VPN and hybrid networks, first to establish VPN and hybrid networks with specific router configuration that are all configured with real time topology. This research then executed to create traffic with transmission of information packet over a fixed time period to observe the real time figure and values of different performance measuring parameters of the networks and analyzing the captured traffic based on these parameters. This report first measured each protocols throughput and jitter value both in software and manually with raw data for every network using the same resources and conditions. Showing each protocols graph for both throughput and jitter value is demonstrated in section 4 (simulation results portion of thereport). Similarly packet length value and packet loss percentage are measured with the same conditions of the networks. Finally, to demonstrate the comparison graph for each routing protocols in VPN and hybrid networks provide the significant ideas of the protocols performance and efficiency. Depending on the comparison graph, decision has been made in the conclusion section to determine the best combination of routing protocols that can be implemented in a particular networking system.

Configuration of Virtual Private Network

- Part 1: Enable router access and controlling to computer
- Part 2: Configure required Parameters on R1
- Part 3: Configure required Parameters on R2
- Part 4: Verify the connection

Connection between router and computer for VPN

HyperTerminal tools, Putty software or secure CRT, included with Windows 10, has been used to communicate directly with your system's modem. Through HyperTerminal can reset the modem or issue configuration and diagnostic commands. These capabilities can help you determine whether or not the modem and computer are communicating correctly.

Starting HyperTerminal and setting up a new connection Before using HyperTerminal to troubleshoot the modem, a port connection is created to do so as follow these steps:

1. Click Start | Programs | Accessories | Communications | HyperTerminal.
2. Once HyperTerminal opens, it will automatically prompt you to create a new connection if none exist. If no connection(s) exists, you can click File | New Connection to create a new one.
3. Specify a name for the connection, choose an icon, and click OK.
4. In the Connect To dialog box, choose the COM port being used by your modem (usually COM1 or COM2) from the Connect Using drop-down list and click OK.
5. In the port property sheet that appears, choose a port speed (bits per second) that matches the device. (For a modem, choose its maximum speed.)
6. Then, choose communications parameters that match the device. For most devices, you can typically use 8 data bits, no parity (set to none), one stop bit, and hardware flow control. When you click OK, HyperTerminal will immediately open a connection to the port. You'll then be ready to troubleshoot.
7. HyperTerminal connection to test communications. You should receive an OK message if your settings are correct and the modem is working, as shown in Figure A.

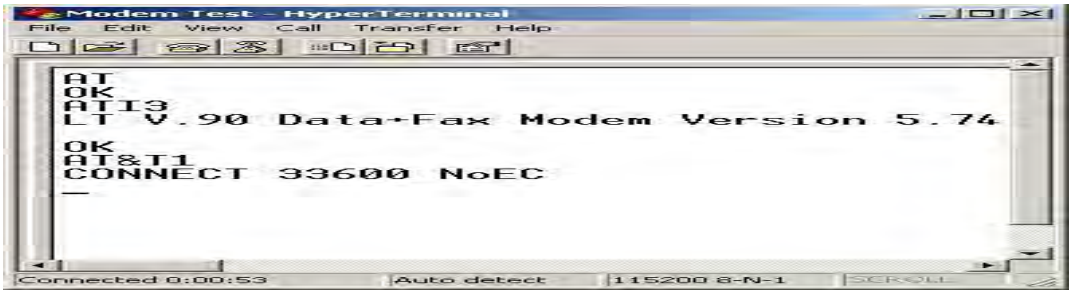


Figure 2.2: HyperTerminal preview

If you don't see the AT text appears when you type, choose File | Properties, click the Settings tab, and then click ASCII Setup. Select Echo Type Characters Locally and click OK twice.

Once you know the modem is at least communicating with the computer, you can use an AT command to perform further diagnostic testing or change configuration settings. Refer to your modem's manual for configuration and diagnostic commands.

Process description

Addressing Table

Device Default	Interface	IP Address	Subnet Mask	Gateway
R1 (model no)	G0/0/0	192.168.1.1	255.255.255.0	N/A
	G0/0/1	192.168.2.1	255.255.255.0	N/A
R2 ()	G0/0/0	192.168.3.1	255.255.255.0	N/A
	Ga0/0/1	192.168.2.2	255.255.255.0	N/A
PC 0	Fa0/0/1	192.168.1.10	255.255.255.0	192.168.1.1
PC 1	Fa0/0/1	192.168.3.10	255.255.255.0	192.168.3.1

Configuration coding on R 1

Step 1: IP address interfacing

<Huawei>system-view

[Huawei] interface GigabitEthernet 0/0/0 [Huawei-

GigabitEthernet0/0/0]ip address 192.168.1.1 255.255.255.0

[Huawei-GigabitEthernet0/0/0] undo shutdown

[Huawei-GigabitEthernet0/0/0] interface GigabitEthernet 0/0/1

[Huawei-GigabitEthernet0/0/1]ip address 192.168.2.1 255.255.255.0

[Huawei-GigabitEthernet0/0/1] undo shutdown

[Huawei-GigabitEthernet0/0/1] quit

<Huawei>

Configuration coding on R 2

<Huawei>system-view

[Huawei] interface GigabitEthernet 0/0/0 [Huawei-

GigabitEthernet0/0/0]ip address 192.168.3.1 255.255.255.0

[Huawei-GigabitEthernet0/0/0] undo shutdown

[Huawei-GigabitEthernet0/0/0] interface GigabitEthernet 0/0/1

[Huawei-GigabitEthernet0/0/1]ip address 192.168.2.2 255.255.255.0

[Huawei-GigabitEthernet0/0/1] undo shutdown [Huawei-

GigabitEthernet0/0/1] quit <Huawei>

Step 2: routing protocol implementation coding

On R1:

[Huawei] rip

[Huawei-rip-1] version 2

[Huawei-rip-1] network 192.168.1.0

[Huawei-rip-1] network 192.168.2.0

[Huawei-rip-1] quit

On R2:

[Huawei] rip

[Huawei-rip-1] version 2

[Huawei-rip-1] network 192.168.3.0

[Huawei-rip-1] network 192.168.2.0

[Huawei-rip-1] quit

Step 3: Verification of the connection

On R1: ping 192.168.2.2 (router gateway)

Ping 192.168.3.10 (distant PC)

On R2: ping 192.168.2.1 (router gateway)

Ping 192.168.1.10 (distant PC)

On PC 1: ping 192.168.3.10

On PC 2: ping 192.168.1.10

After successful configuration, one pc will be able to communicate with another pc without any packet loss and delay.

VPN set-up in Packet tracer and GNS-3 Software for testing:

Initially the network for Virtual private Network and hybrid network has been initiated in packet tracer and eNSP software both for Cisco and Huawei routers. The configuration for particular networks is quite similar with security, encryption, authentication and verification protocols both for packet tracer and eNSP softwires. After that, same configuration had been implemented in GNS-3 software for real time experiences of the VPN and hybrid network while it has also been tested with websites and protocol analysis.

The output result is followed in Figure 2.2.1 for isakmp in router one and router two is shown in Figure 2.2.2 respectively.

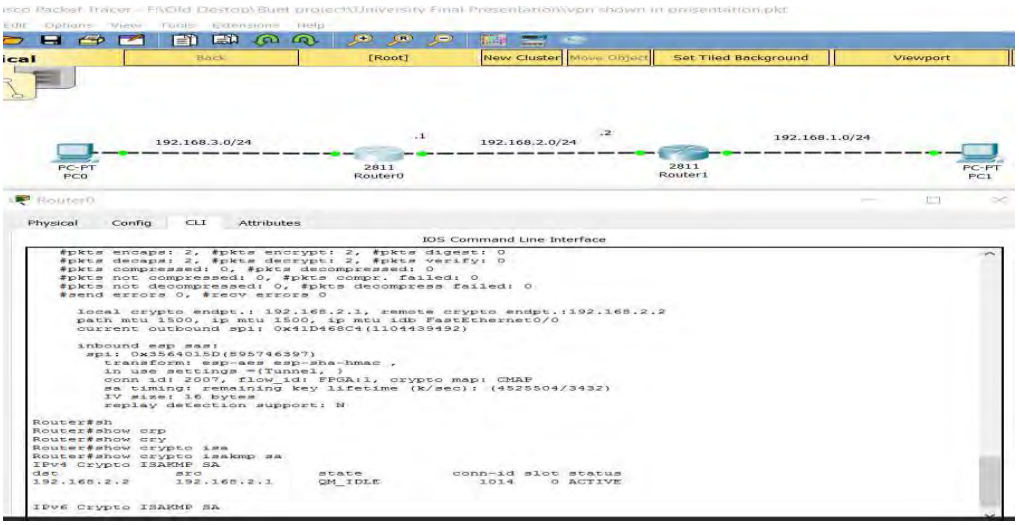


Figure 2.2.1: Output of VPN network for IPSEC

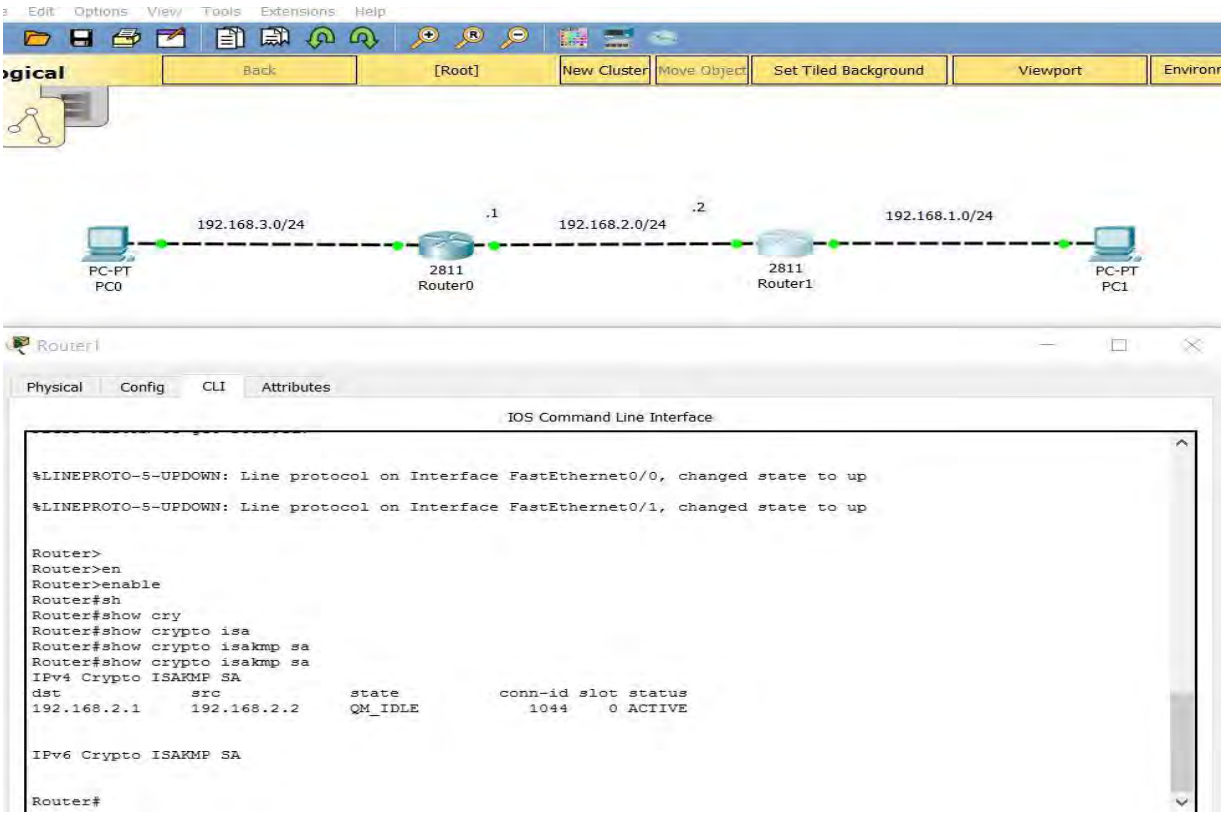


Figure 2.2.2: Output of VPN network for ISAKMP

The above output shows Isakmp protocol testing in Router one. And the output test for router two shows the result to understand the configuration of the router.

Practical implementation of Virtual Private network in Huawei Devices:

This project developed then in Huawei routers with connection of computers for establishing the Virtual private network. The aforementioned configuration followed to create site to site VPN network and security protocols was initiated according to the coding of the configurations.

Figure 2.2.3: Practical network scenario for VPN network

Verification of the establishment of VPN network

To verify the networking performance of virtual private network, we are to check it to give the command of the command windows or to send the packets to observe that

whether it's being encrypted or not. Depending on the packets sent to the destination from the source, we are to check, how many packets are encrypted, how many packets are digested also the result of decrypted message and verification will be shown.

To check the source and destination of the sending packets are to give the command: show crypto isakmp sa. To check the overall results of encrypted and decrypted message, we are to give the command like: show crypto IPSec sa .

The result will be like shown in Figure 2.2.4.

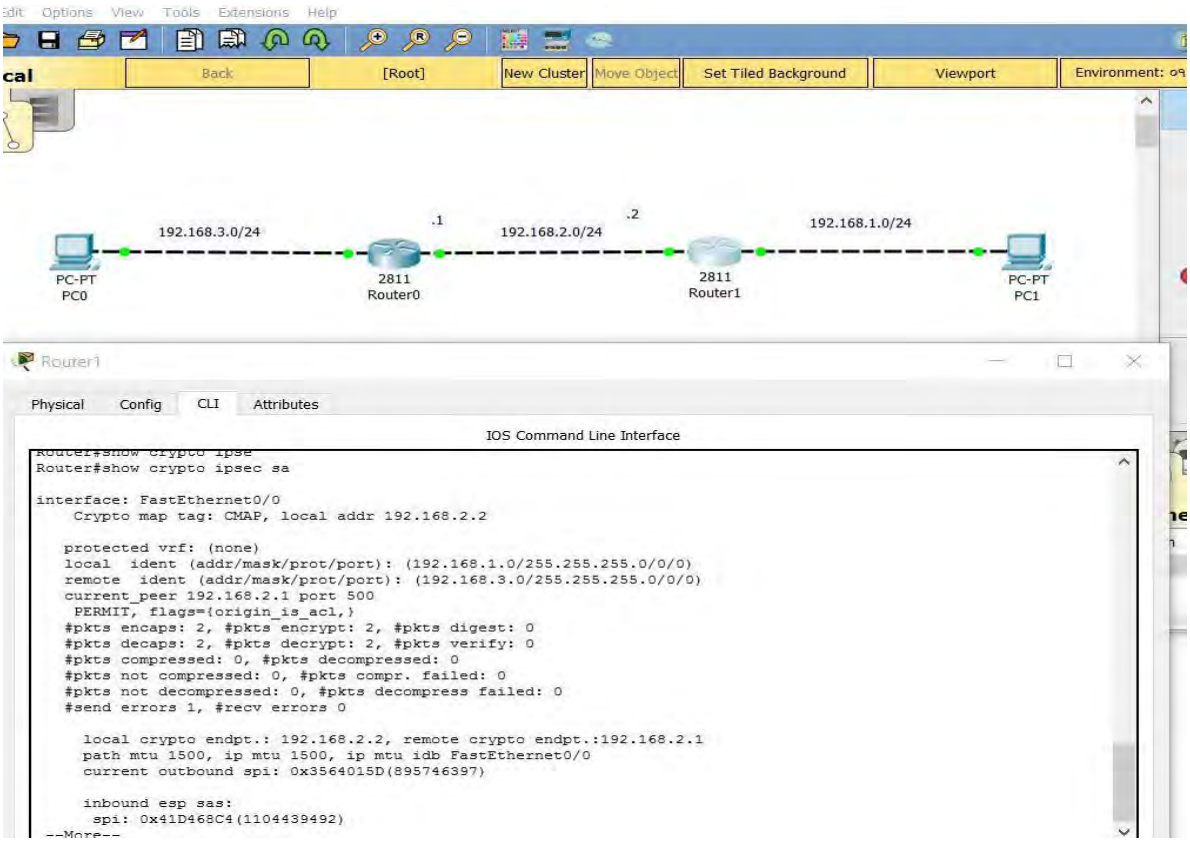


Figure 2.2.4: Verification of protocols for VPN

2.3 Establishment of Websites

At this time, all of the individual graphic elements are taken from the prototype and use them to establish the actual, functional website. Firstly, developed the home page. The shell is important as a template for the content of the website of the page, as it contains the main structure for the web site. After creating the shell, content of the site has been distributed throughout the site. This entire time, I continue to make a web site convenient for testing my experiment, it can be possible also to test the networking performance for that particular website.

On the technical front, an effective web site requires an understanding of front-end web development that is written in valid HTML / CSS code that complies the standards of the website, maximizing functionality and accessibility. Technical requirements for completing this report, Joomla 3.3 has been used requiring PHP version 5.3 or higher, MySQL, Nginx 1.0 or Microsoft IIS 7 as the webserver SQL Server, Postgre SQL database and Apache 2.0.

Information Architecture refers to what is meant with an information architecture and different types of methods can be applied in its design process. However, the content is based on sources from online. Here it is considered for information architecture is that a structural design of shared information environments and the combination of organization, labeling, search, and navigation systems for web sites. For shaping information of the products, art and science to support usability and findability of the websites. Maintaining principles of design and architecture, an emerging discipline and community of practice focused on the digital landscape. Generally, information architecture (IA) refers to information system's structural solution for structuring, organizing and categorizing content in precise, efficient and sustainable way. It focusses on some topics that has been ensured to develop this usability, user experience (UX), layout and user-interface design.

Write detail about VPN implementation. Provide figures of networks with VPN implementation. You may use the pictures of networks developed in Packet Tracer AND in GNS3, etc

2.4. Software and Simulation Tools

The Network has been established in Graphical Network Simulator 3 (GNS3) version 2.1.5 using VirtualBox version 5.2.12 that runs on the Windows 10 operating system. The Router 3725 Series with Cisco IOS operating system enabled that runs in GNS3, and Windows 10 operating system is running in VirtualBox as a PC. For simulation purpose, Wireshark software version 2.5.1 is used and version 3.1.3 Iperf applications running on the PC.

2.5. Prototype Modeling

Simulation will be performed in Virtual private Network (VPN) and Hybrid network with a combination of routing protocols in seven different scenarios following as RIP, OSPF, EIGRP, RIP-OSPF, RIP-EIGRP, OSPF-EIGRP, RIP-OSPF-EIGRP.

CHAPTER-3

Evaluation of Protocols

To configure the hybrid and Virtual private network used different cryptographic and routing protocols for implementing the connection. In fact, network performance is dependent on the functionalities of the protocols. Therefore, this chapter demonstrates the parameters are considered to measure the performance of the network those are described respectively.

3.1. Parameters to evaluate the protocols

I Throughput

Network throughput refers to the average data rate of successful communication of a network or message delivery over a specific networking link. It measures a comparable effectiveness and efficiency of an operation or a system. It defines how strong and consistent the connection is maintained during the session. It is calculated by a theory as

$$h\ \ h\ \ \ h\ \ \ \ ( ) = \sum \frac{(h\ \ h\ ())}{\sum\ \ h\ \ h\ ()}$$

In our experiment, we have measured throughput value for each system to find the throughput for that specific protocol or combined protocols to see the transmission of packet over that fixed period in a network.

II Jitter

Jitter refers to statistical variation of Packet Delay and it is cited in IETF RFC 3393 and 5481.It is calculated to find the delay for all the packets from a source to a destination.. Here, we have both calculated the jitter value in iperf software and taking the raw data from Wireshark that is calculated as follows:

Jitter rata -rata =

Measuring the total delay,

Total Variant Delay = (Ri -Si) (R i+1 -Sj+1)

Here, Ri = Received Time

Si = Sent Start time

III Packet Length

Packet size is a considerable issue for energy constrained and performance evaluation of a network. Because of larger size of packets, data bit corruption creating higher frequency of re-transmission may be caused. And bigger packet might have problem if it is above the size of MTU (Maximum Transmission Unit). Moreover, NIC (Network Interface Controller) and OS has memory size restriction. On the other hand, small size packets are more efficient but creating too short packet size might cause faults, like higher overhead and startup energy consumption for each packet can degrade the network performance. Besides, small size packets have issues with fragmentation and security problem. For this reason, Packet length for protocols and combination of the protocols in three different networks is measured to evaluate the particular networking system.

IV. Packet Loss

Packet loss refers to small bits of lost data over a transmission period to or from one networking equipment to another equipment. Some amount of packet loss, generally just a small percentage can be available in a connection of a network. However, Packet loss is closely associated with quality of service considerations as network performance is impacted by packet loss and retransmission. Because of saturation, bandwidth outage, misconfiguration, network may be defected to lose acknowledge when retransmission is needed although the packet was transmitted. Moreover, TCP congestion window size is effected for packet loss when it will not accept optimal throughput value for the network.

CHAPTER-4

Simulation Results

This experiment has been done to measure the throughput value in terms of Virtual private and hybrid networks and combination of the protocols for two types of networks. Here, x and y axis are considered as time and packet sent over that time period. The average and maximum throughput value is calculated as packet per second. For the simulation purpose, SMA period is set as 10 interval SMA and corresponding value for y axis is considered as 1000 interval SMA. Specific protocol is selected every time to find the throughput value for the graph.

Simulation Results

4.1 For Hybrid Network considering throughput

Scenario 1: Throughput is calculated for hybrid network and figure shown for RIP protocol in Figure 4.1.

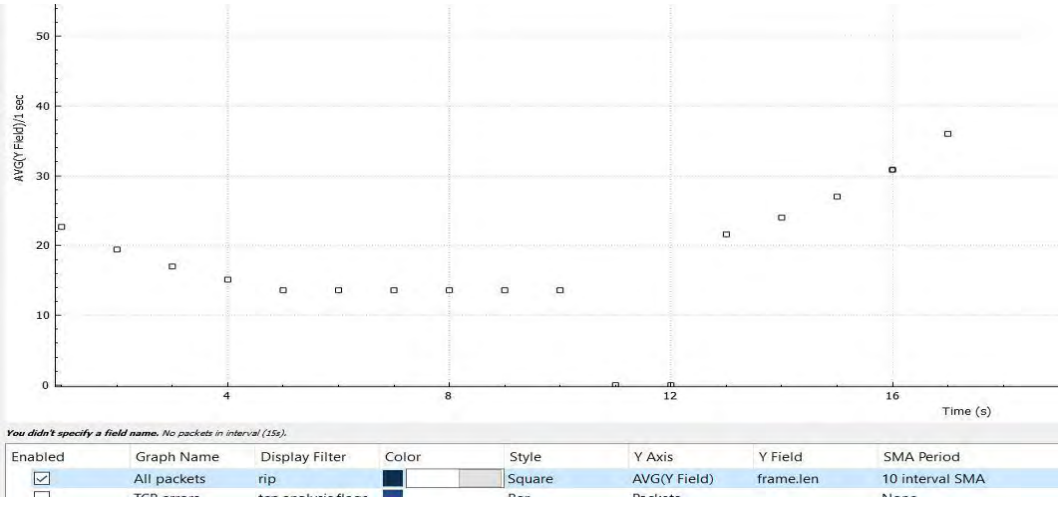


Figure 4.1 : Rip throughput

In this figure, the average throughput value for this network using rip protocol is 22 packet / sec which show maximum throughput is 35. The value of throughput initially got down up to 10 secs then went upward.

Scenario 2 : Throughput is calculated for hybrid network and figure shown for OSPF protocol in Figure 4.2.

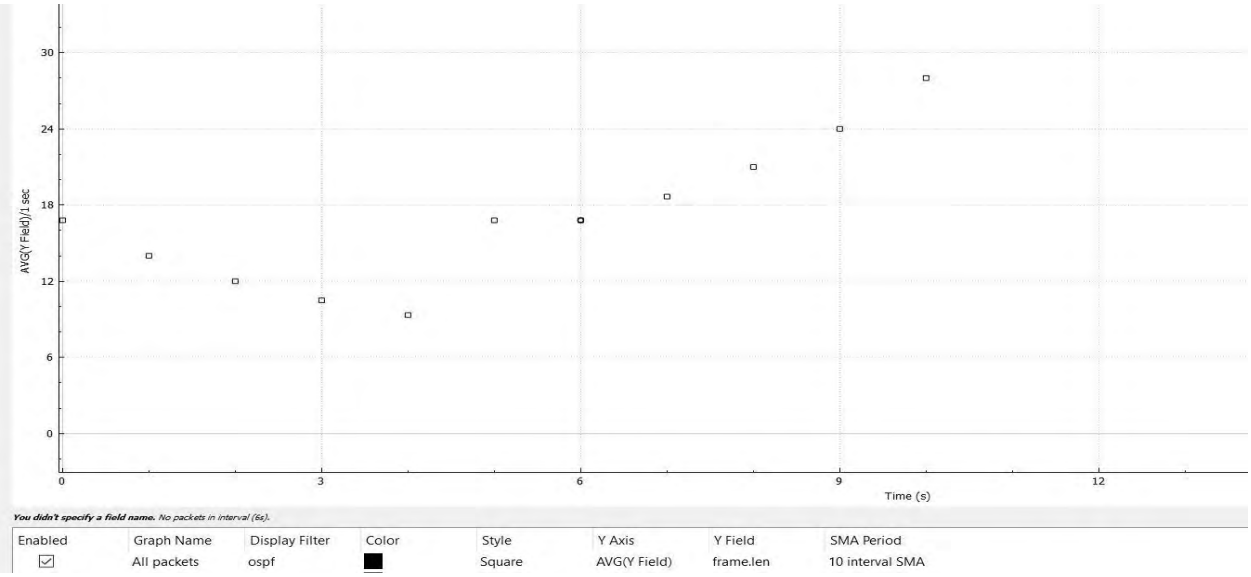


Figure 4.2: OSPF throughput

In this figure, we have found that the average throughput value for this network using ospf protocol is 18 packet / sec which show maximum throughput is 28. The value of throughput initially got down up to 5 secs then went upward.

Scenario 3: Throughput is calculated for hybrid network and figure shown for EIGRP protocol in Figure 4.3

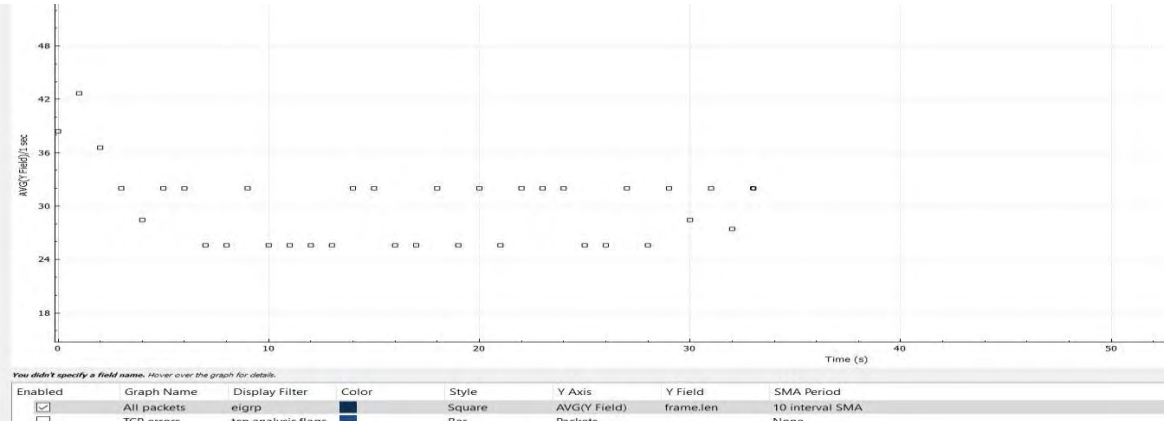


Figure 4.3: EIGRP throughput

In this figure, we have found that the average throughput value for this network using eigrp protocol is 27 packet / sec which show maximum throughput is 44. The value of throughput maintains a stable rate between 24 to 36 packets per second.

Scenario 4: Throughput is calculated for hybrid network and figure shown for RIP – OSPF in Figure 4.4.

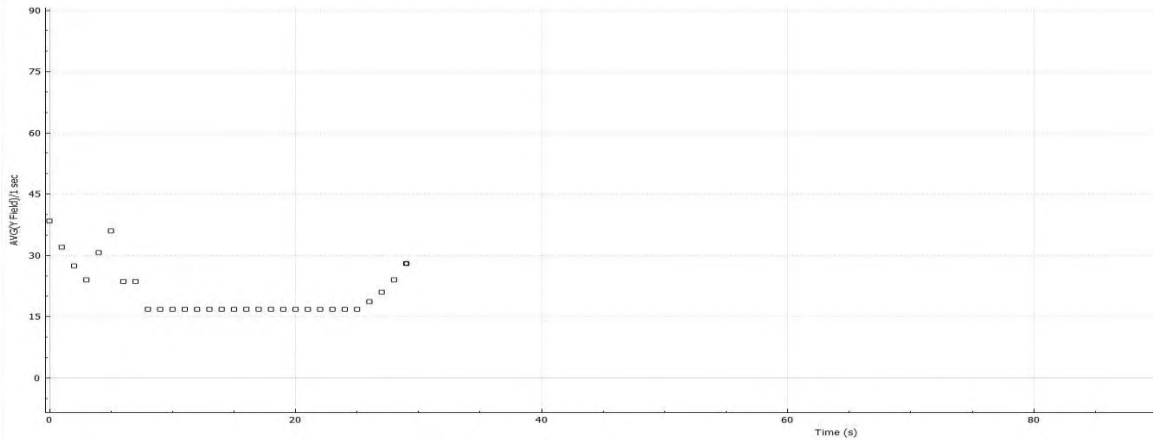


Figure 4.4: RIP-OSPF throughput

In this figure, the average throughput value for this network using rip-ospf protocol is 19 packet / sec which show maximum throughput is 34.

Scenario 5: Throughput is calculated for hybrid network and figure shown for RIP-EIGRP in Figure 4.5.

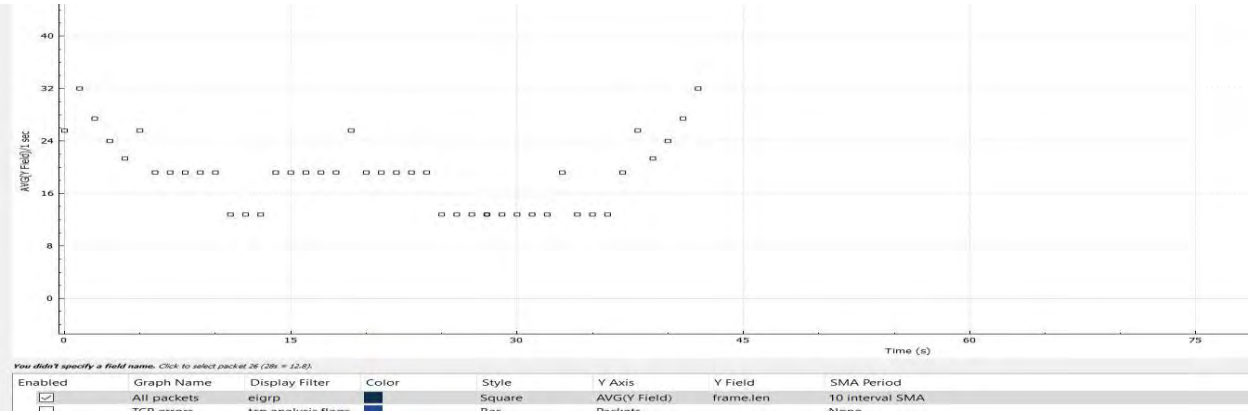


Figure 4.5: RIP-EIGRP throughput

In this figure, the average throughput value for this network using rip-eigrp protocol is 23 packet / sec which show maximum throughput is 32.

Scenario 6: Throughput is calculated for hybrid network and figure shown for OSPF-EIGRP in Figure 4.6.

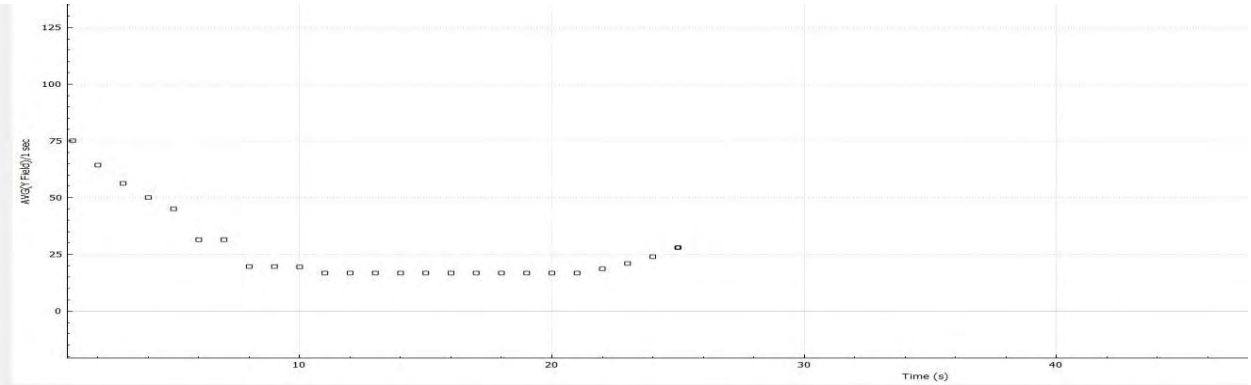


Figure 4.6: OSPF- EIGRP throughput

In this figure, the average throughput value for this network using ospf-eigrp protocol is 28 packet / sec which show maximum throughput is 75.

Scenario 7: Throughput is calculated for hybrid Network and figure shown for RIP-OSPF-EIGRP in Figure 4.7

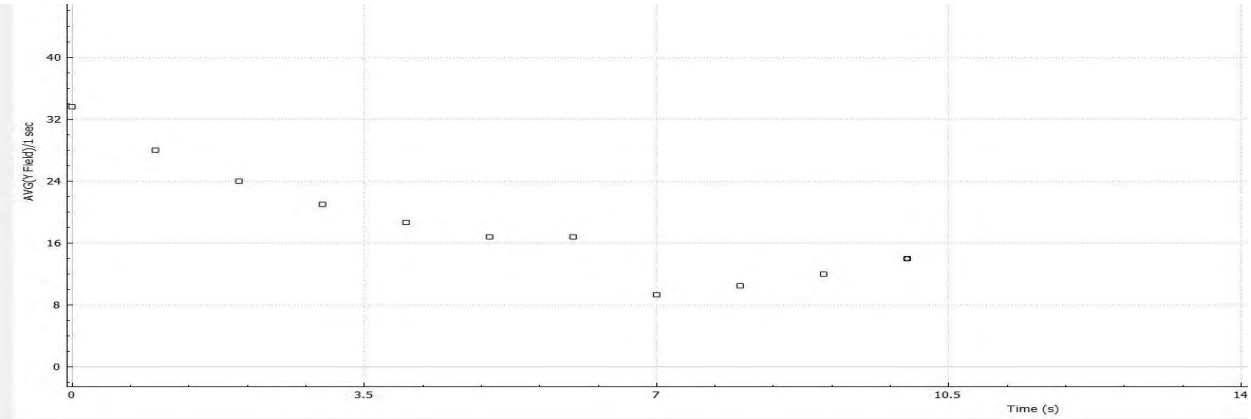


Figure 4.7: RIP-OSPF-EIGRP throughput

In this Figure, the average throughput value for this network using rip-ospf-eigrp protocol is 21 packet / sec which show maximum throughput is 34.

4.2 For Virtual Private Network:

Scenario 1: Throughput is calculated for Virtual private Network and figure shown for RIP Protocol shown in Figure 4.8.

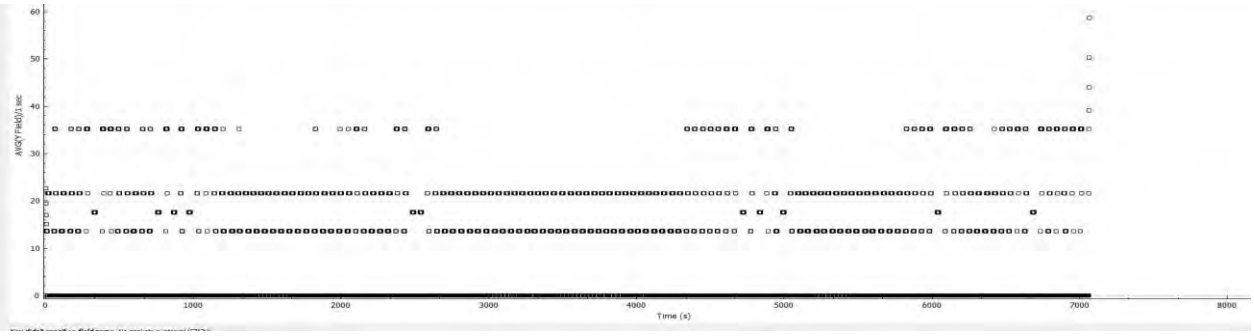


Figure 4.8 RIP throughput

In this figure, the average throughput value for this network using rip protocol is 22 packet / sec which show maximum throughput is 58.

Scenario 2: Throughput is calculated for Virtual private Network and figure shown for OSPF protocol in Figure 4.9.

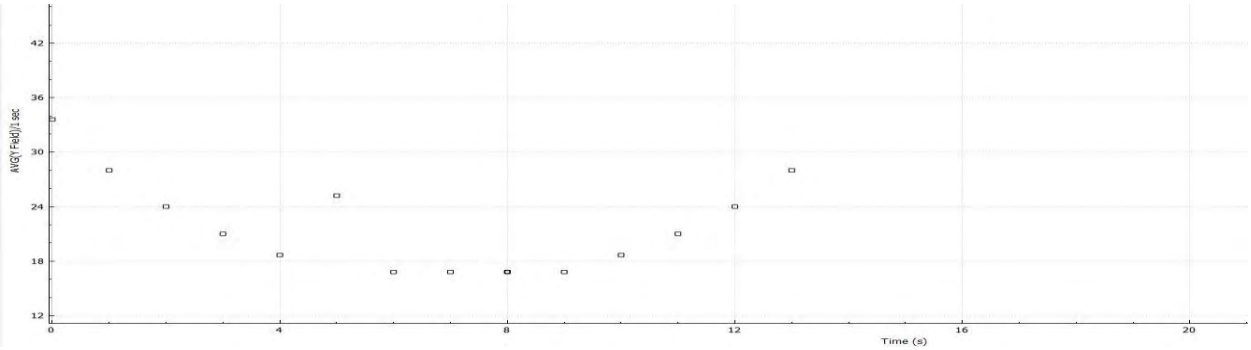


Figure 4.9: OSPF throughput

In this figure, the average throughput value for this network using ospf protocol is 20 packet / sec which show maximum throughput is 32.

Scenario 3: Throughput is calculated for Virtual private Network and figure shown for EIGRP in Figure 4.10.

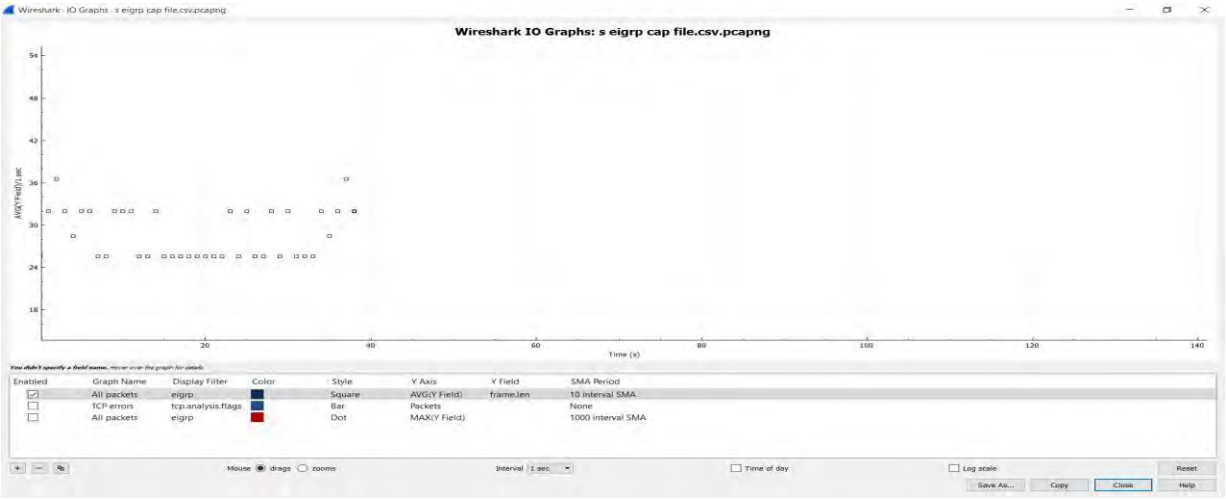


Figure 4.10: EIGRP throughput

In this figure, the average throughput value for this network using eigrp protocol is 14 packet / sec which show maximum throughput.

Scenario 4: Throughput is calculated for Virtual private Network and figure shown for RIP-OSPF in Figure 4.11.

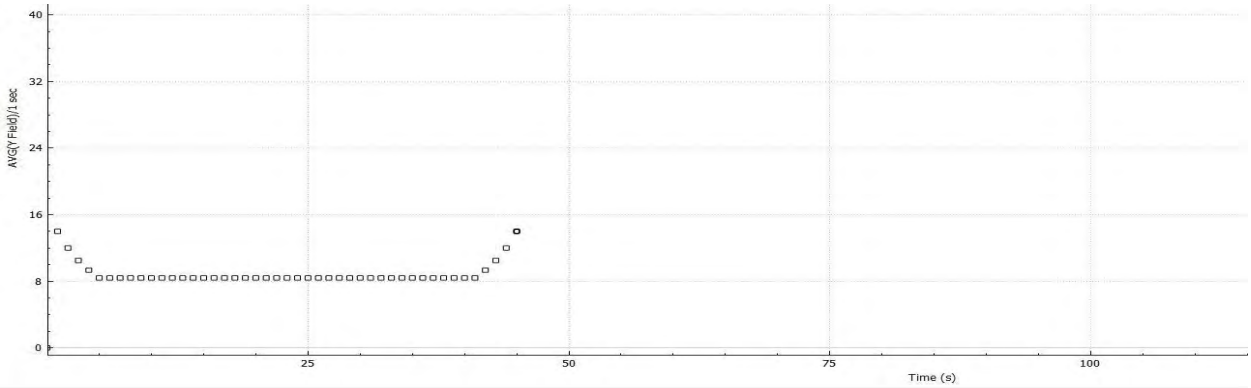


Figure 4.11: RIP-OSPF throughput

In this figure, the average throughput value for this network using rip-ospf protocol is 13 packet / sec which show maximum throughput is 15.

Scenario 5 : Throughput is calculated for Virtual private Network and figure shown for RIP-EIGRP in Figure 4.12

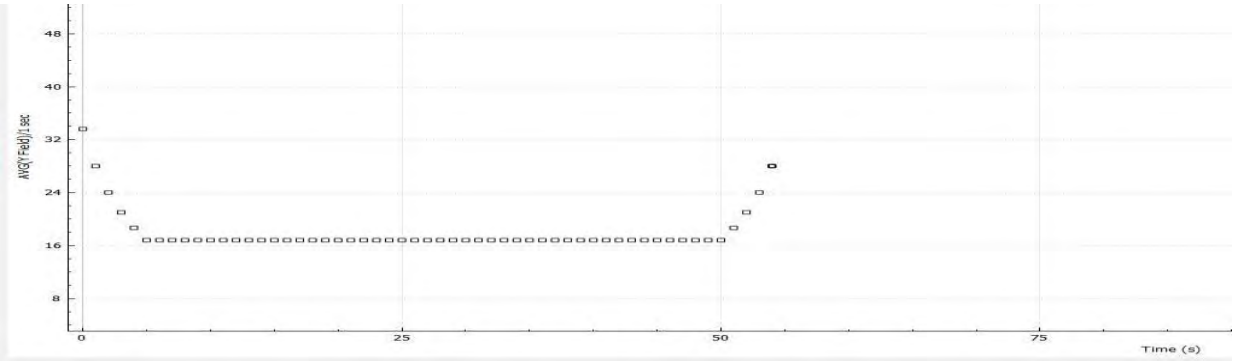


Figure 4.12: RIP-EIGRP throughput

In this figure, the average throughput value for this network using rip-eigrp protocol is 28 packet / sec which show maximum throughput is 28.

Scenario 6: Throughput is calculated for Virtual private Network and figure shown for OSPF-EIGRP.

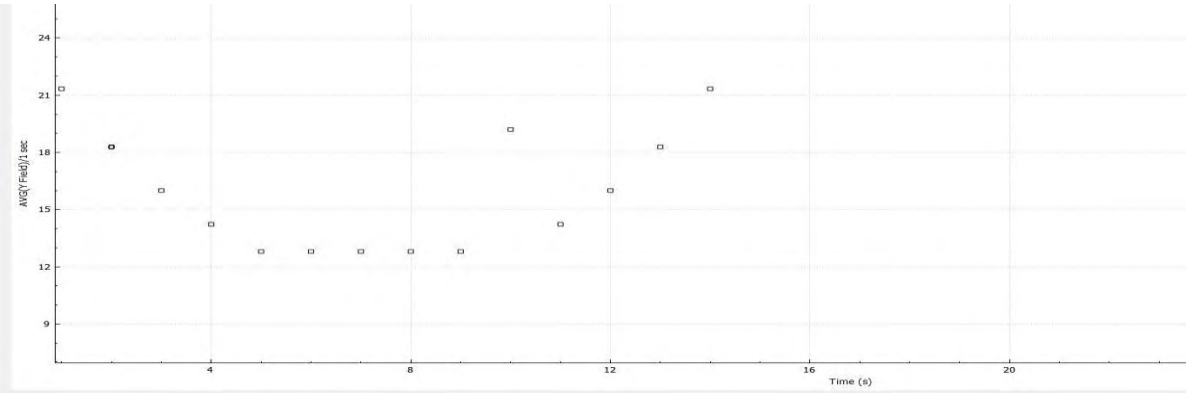


Figure 4.13: OSPF-EIGRP throughput

In this figure, the average throughput value for this network using ospf-eigrp protocol is 17 packet / sec which show maximum throughput is 22.

Scenario 7: Throughput is calculated for Virtual private Network and figure shown for RIP-OSPF-EIGRP in Figure 4.13.

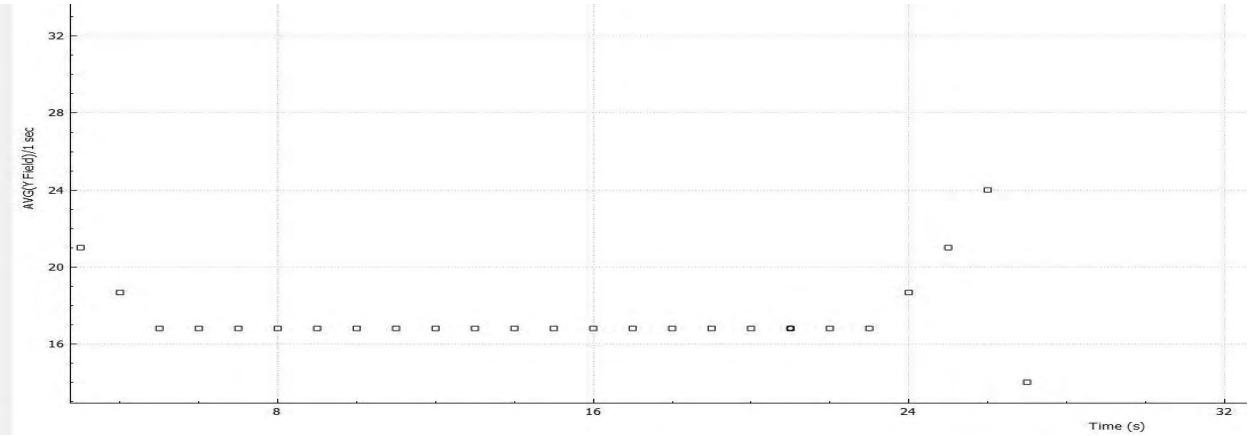


Figure 4.14: RIP-OSPF-EIGRP throughput

In this figure, the average throughput value for this network using rip-ospf-eigrp protocol is 18 packet / sec which show maximum throughput is 24.

4.2 Valuation of Protocols:

Result has been found based on the previous graph and finally creating this comparison graph for throughput both for virtual private network and hybrid network.

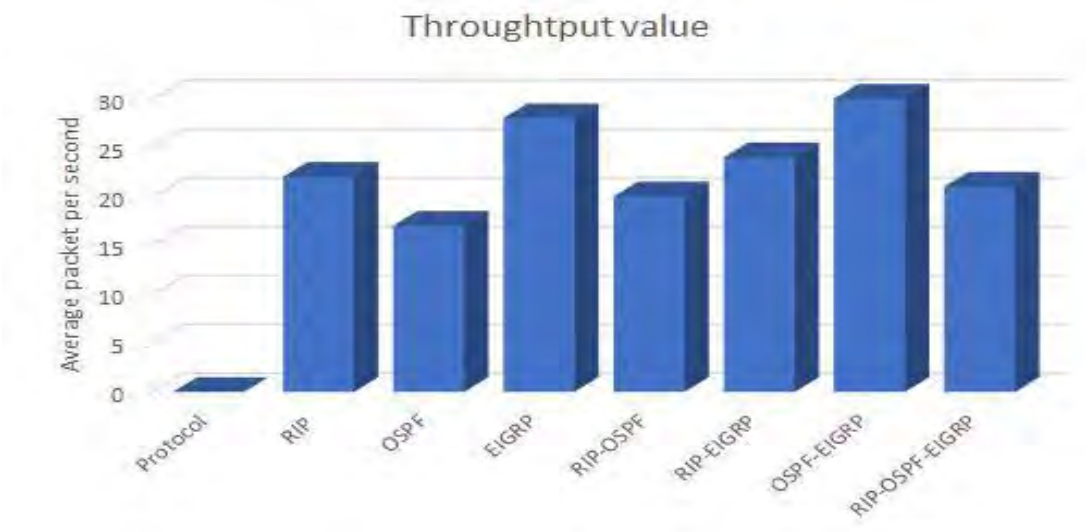


Figure 4.15: Comparison graph for Hybrid Network in seven scenarios for Throughput.

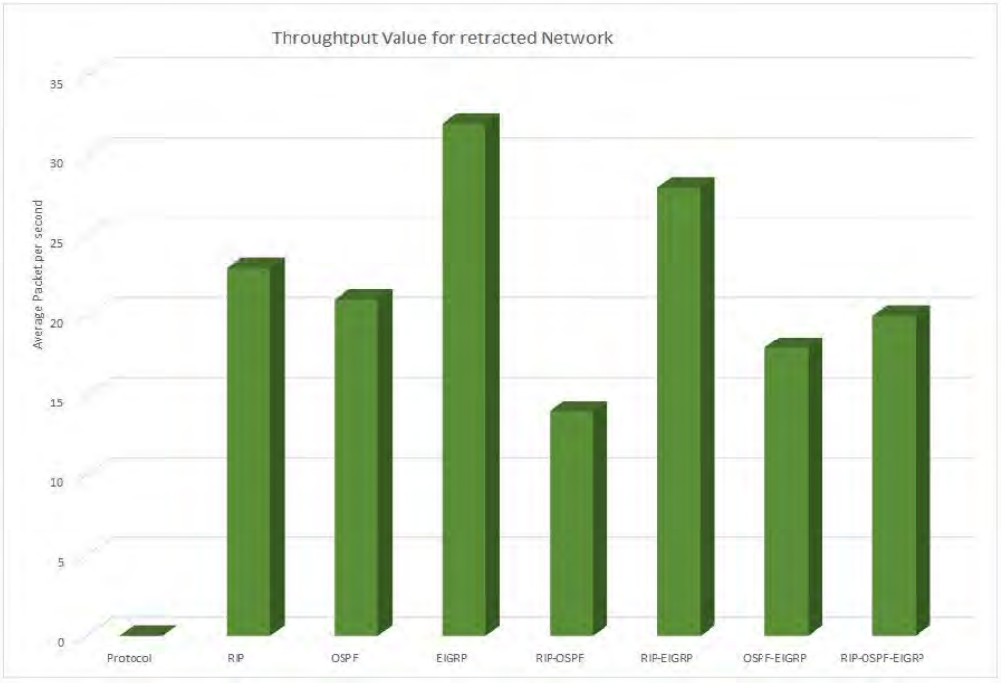


Figure 4.16: Comparison graph for Virtual private Network for throughput.

4.3 Results Analysis and decision:

Analyzing the above figures, combined OSPF-EIGRP protocol performs better for hybrid network with maintaining average throughput almost 30 packets per sec. Here alone EIGRP and combined RIP-EIGRP maintains average throughput 28 and 23 respectively. Poor performance is observed for OSPF and RIP-OSPF protocols that are below throughput value of 20. However, best performance is obtained for alone EIGRP (above 25 packets per second) which was actually proposed by researchers for big networking system. Lower performance is shown for combination of three protocols and RIP protocols that is below 13 packets per second. Similarly, EIGRP protocol achievement for Virtual private network is also the highest number of throughput value that is 32 packets per second while RIP-EIGRP and alone RIP protocols have shown considerable performance for this networking system. However, least throughput is attained for combined RIP-OSPF protocols.

Performance gain is obtained for RIP and EIGRP protocols for Virtual private Network compared to hybrid network that are 9.52% and 23.07% while performance penalty is observed for combined RIP-OSPF protocols (46.15%).

CHAPTER-5

Evaluation for Networks

Hybrid network protocol analysis based on jitter, packet length and packet loss will be cited in this chapter along with the comparison chart for Virtual private network and Hybrid network. IP networks for jitter is the variation in the latency on transmission of packet through the network that is measured to evaluate the networking performance of the networks. Besides, Packet loss and packet length comparison graph show a substantial idea about the networks.

jitter value is calculated maintaining seven different scenarios in Hybrid and VPN networks. It shows the deviation during the transmission of the packets as shown in x axis with respect to time in y axis for every particular networking system. Jitter value is calculated in both way by iperf application and manually to take the raw data from capture data in each networking module for specific protocols to find the actual figure and then to compare those to select the best one.

5.1 Evaluation for jitter

Hybrid Network considering jitter, packet loss, packet length

Scenario 8: jitter value is calculated and figure shown for RIP in Figure 5.1.

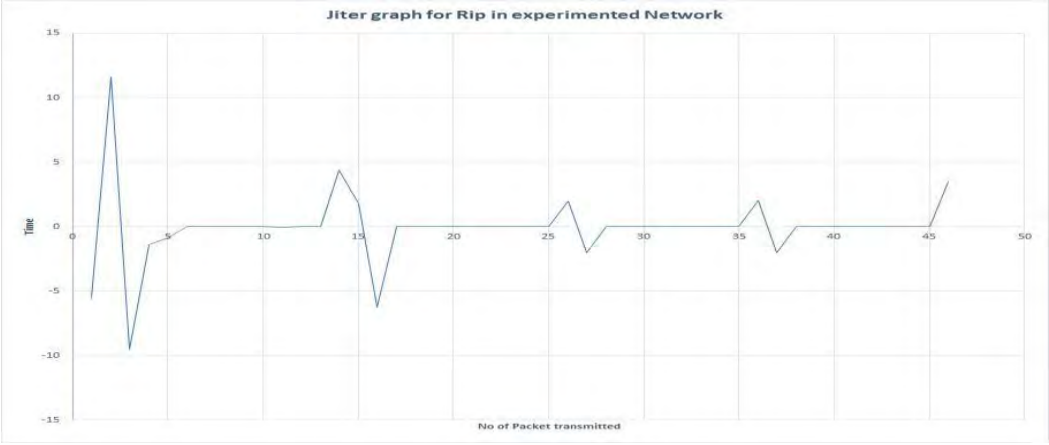


Figure 5.1: Jitter graph for RIP

Scenario 9: jitter value is calculated and figure shown for OSPF in Figure 5.2.

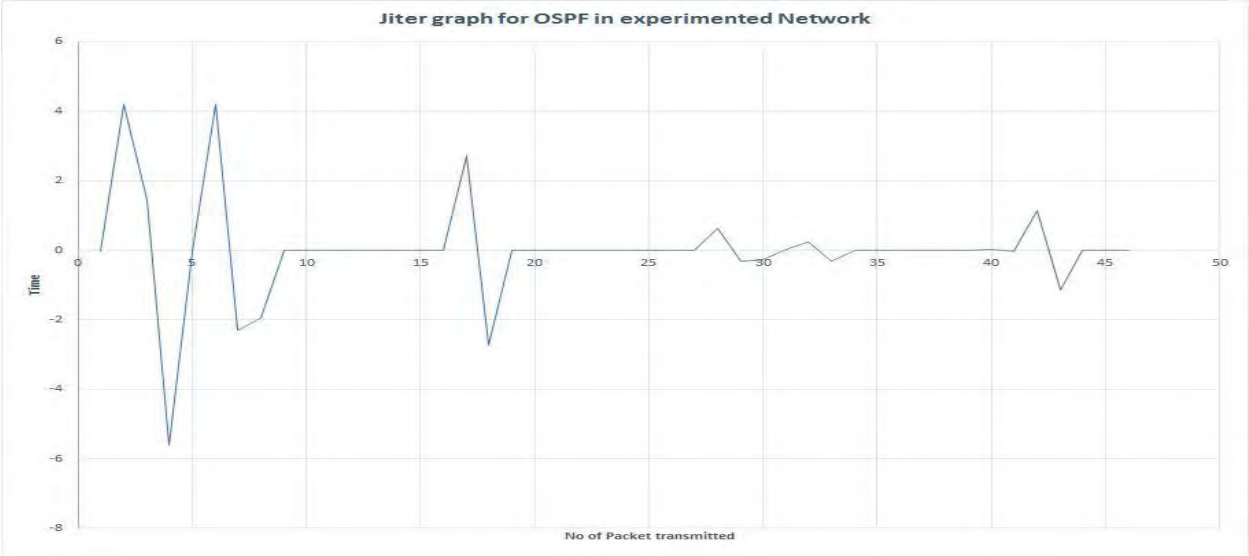


Figure 5.2: Jitter graph for OSPF

Scenario 10: jitter value is calculated and figure shown for EIGRP in figure 5.3.

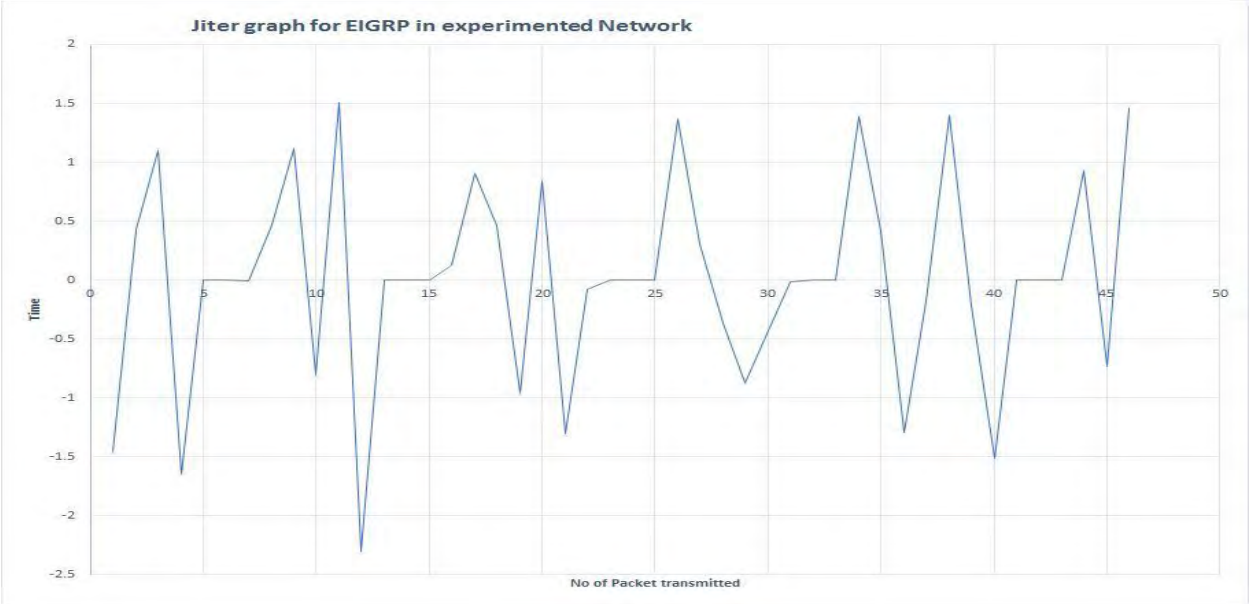


Figure 5.3: Jitter graph for EIGRP

Scenario 11: jitter value is calculated and figure shown for RIP- OSPF in Figure 5.4.

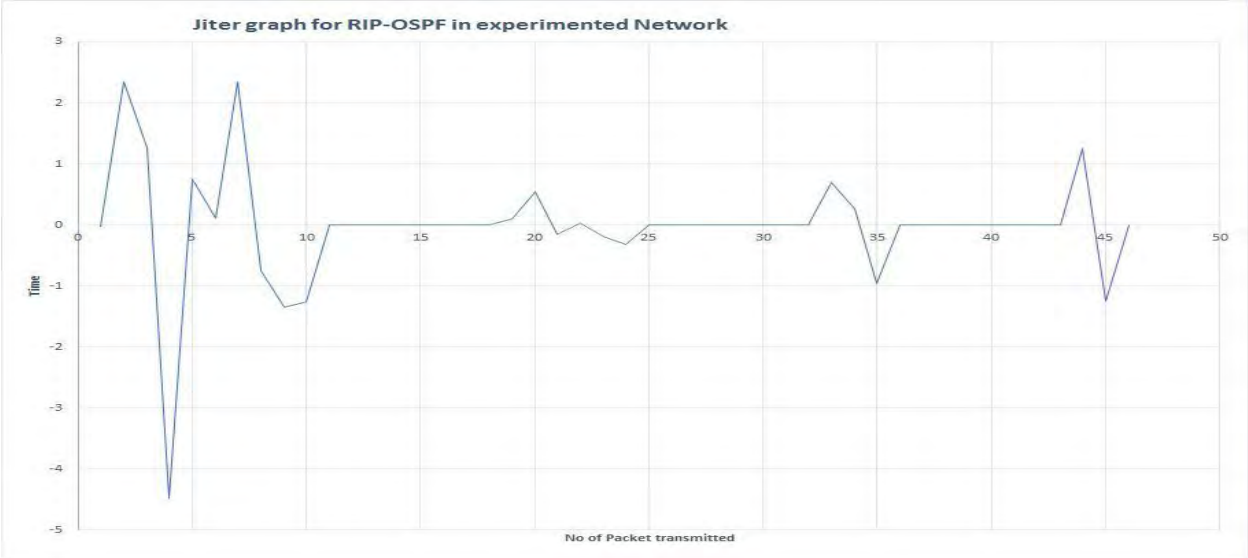


Figure 5.4: Jitter graph for RIP-OSPF.

Scenario 12: jitter value is calculated and figure shown for RIP-EIGRP in Figure 5.5.

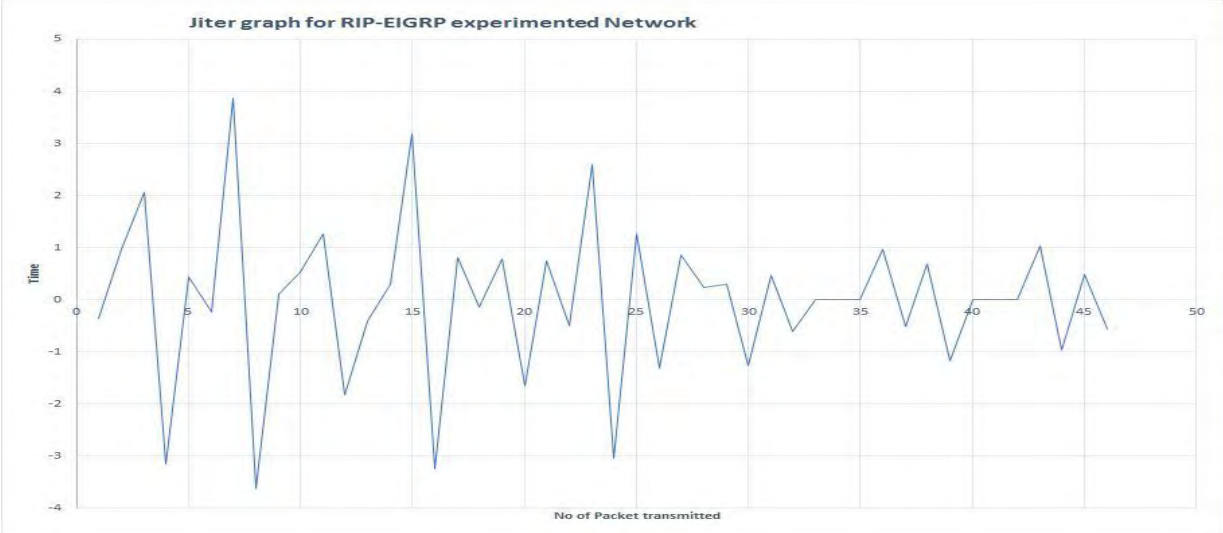


Figure 5.5: Jitter graph for RIP-EIGRP

Scenario 13: jitter value is calculated and figure shown for OSPF-EIGRP in Figure 5.6.

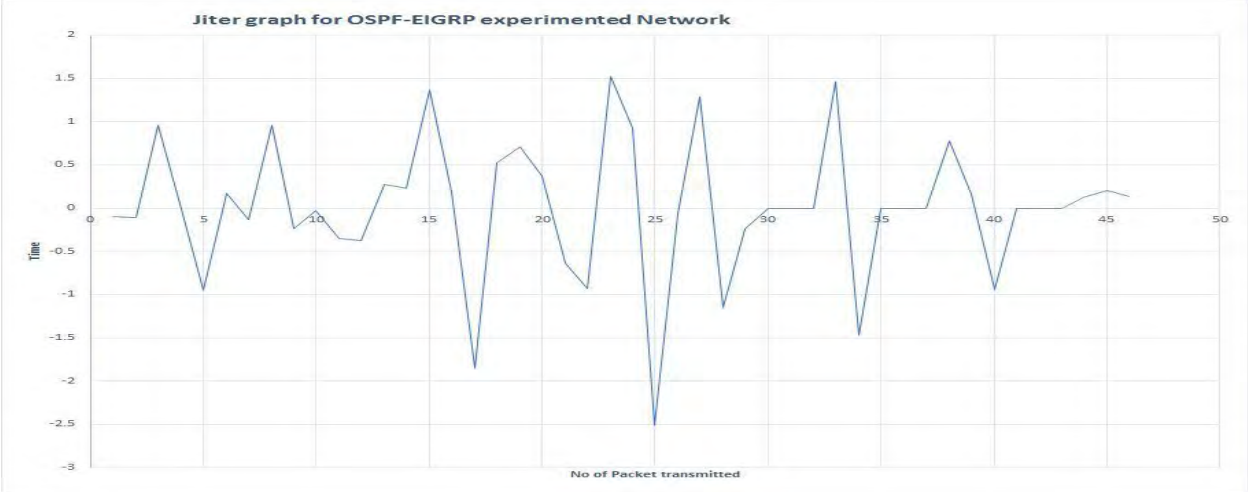


Figure 5.6: Jitter graph for OSPF-EIGRP

Scenario 14: jitter value is calculated and figure shown for RIP-OSPF-EIGRP in Figure 5.7.

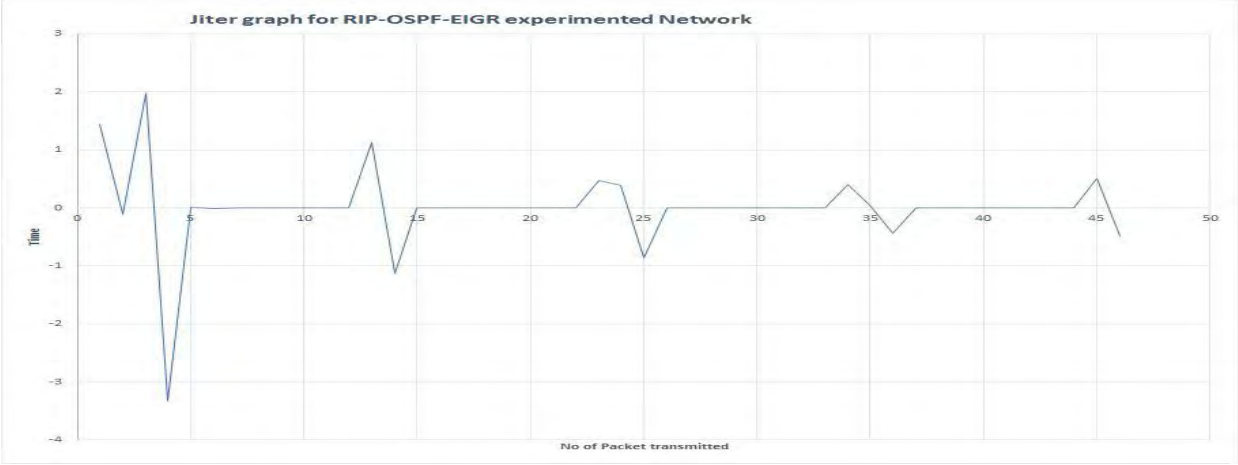


Figure 5.7: Jitter graph for RIP-OSPF-EIGRP

Scenario 15 : jitter value is calculated for Virtual Private Network and figure shown for RIP in Figure 5.8.

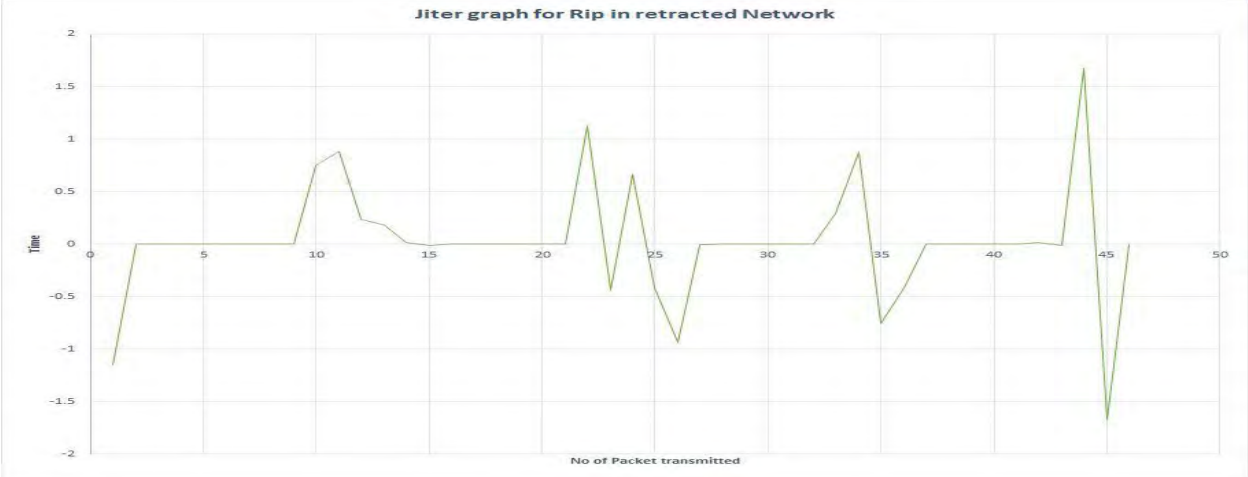


Figure 5.8: Jitter graph for RIP

Scenario 16 : jitter value is calculated for Virtual Private Network and figure shown for OSPF in Figure 5.9

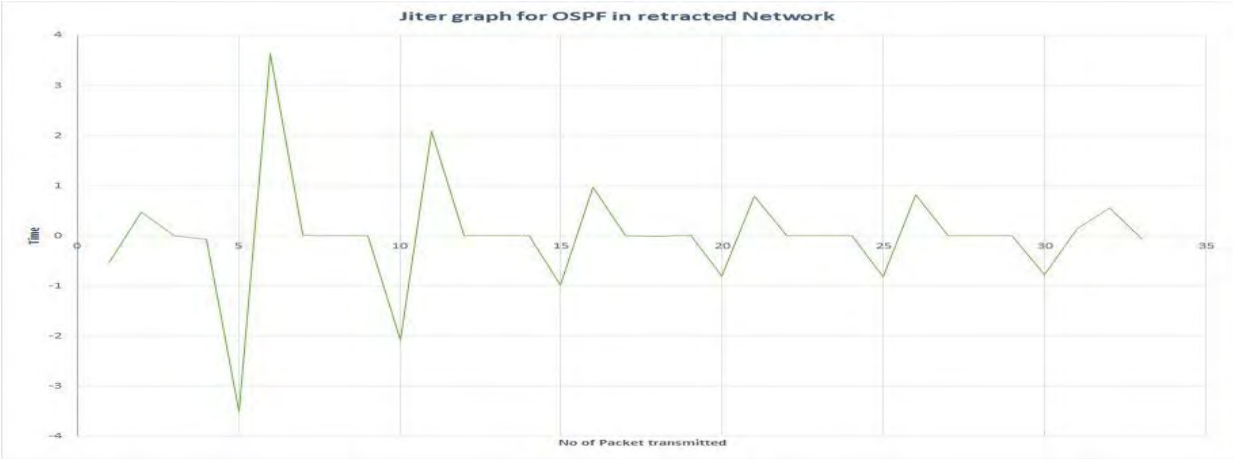


Figure 5.9: Jitter graph for OSPF

Scenario 17: jitter value is calculated for Virtual Private Network and figure shown for EIGRP in Figure 5.10.

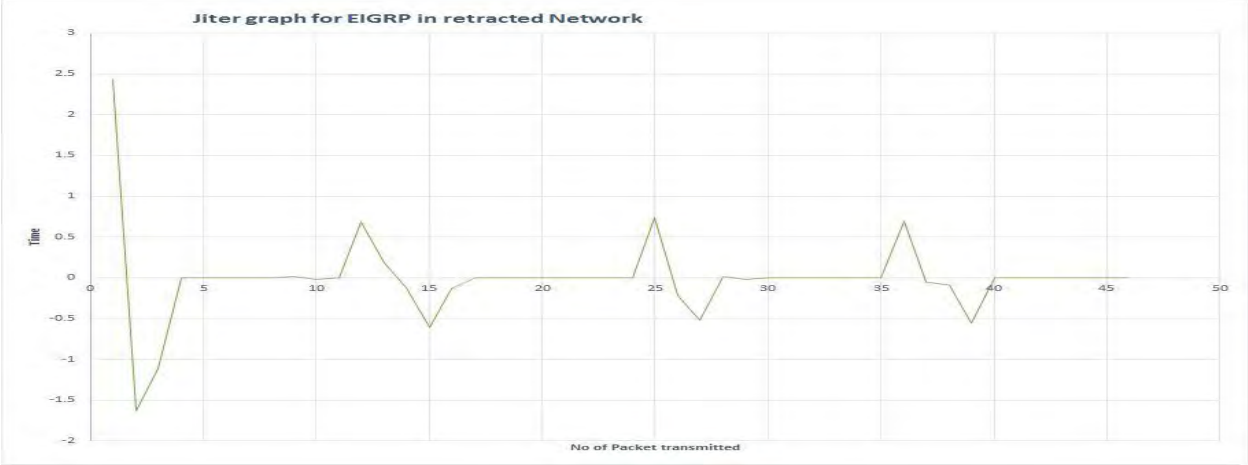


Figure 5.10: Jitter graph for EIGRP

Scenario 18: jitter value is calculated for Virtual Private Network and figure shown for RIP – OSPF in Figure 5.11.

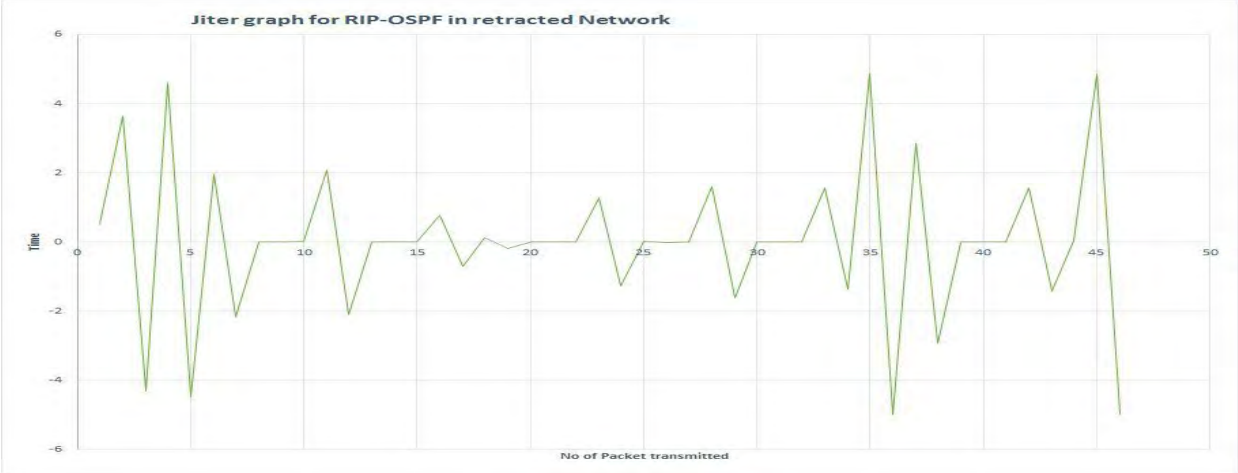


Figure 5.11: Jitter graph for RIP-OSPF

Scenario 19 : jitter value is calculated for Virtual Private Network and figure shown for RIP –EIGRP in Figure 5.12.

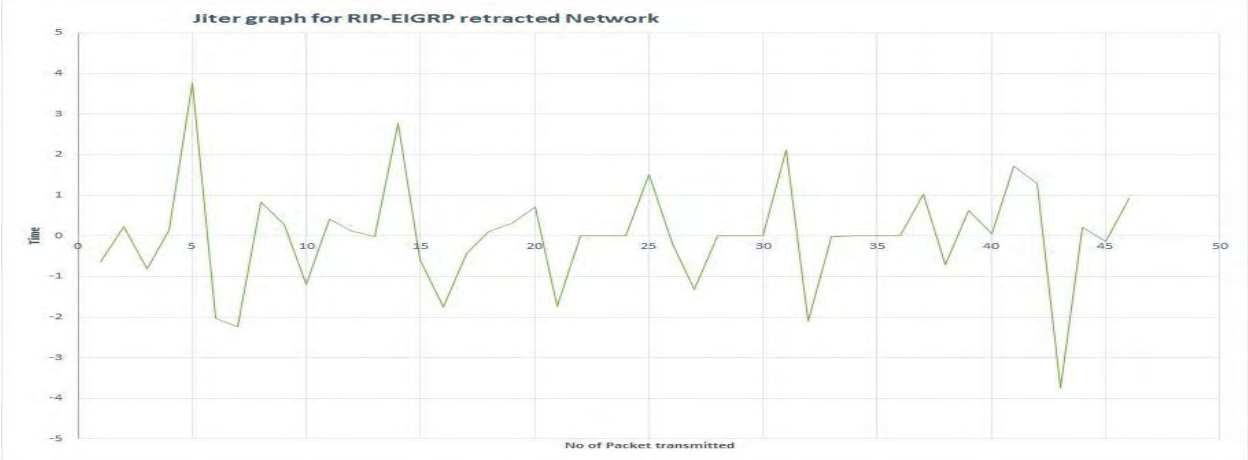


Figure 5.12: Jitter graph for RIP-EIGRP

Scenario 20: jitter value is calculated for Virtual Private Network and figure shown for OSPF-EIGRP in Figure 5.13.

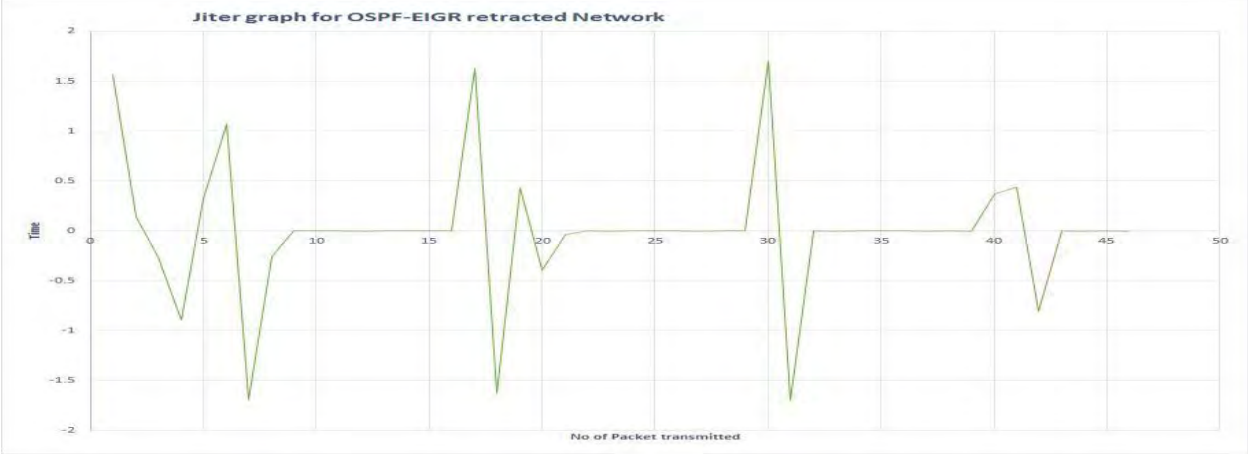


Figure 5.13: Jitter graph for OSPF-EIGRP

Scenario 21: jitter value is calculated for Virtual Private Network and figure shown for RIP - OSPF-EIGRP in Figure 5.14.

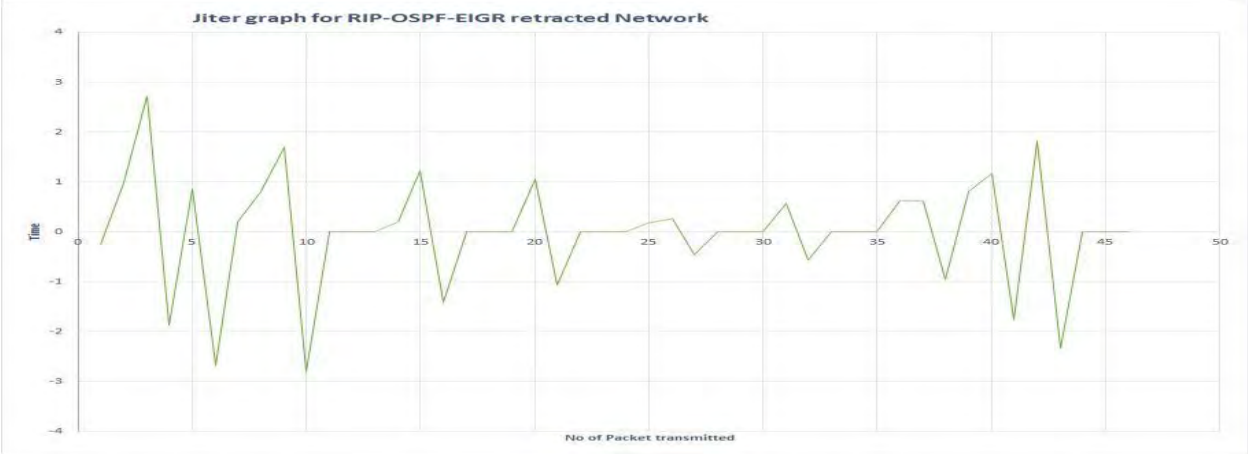


Figure 5.14: Jitter graph for RIP-OSPF-EIGRP

5.1.1 Jitter Valuation:

Result has been found based on the previous graph and finally creating this comparison graph for jitter value both for virtual private network and hybrid network in the figure 5.15 and 5.16 respectively

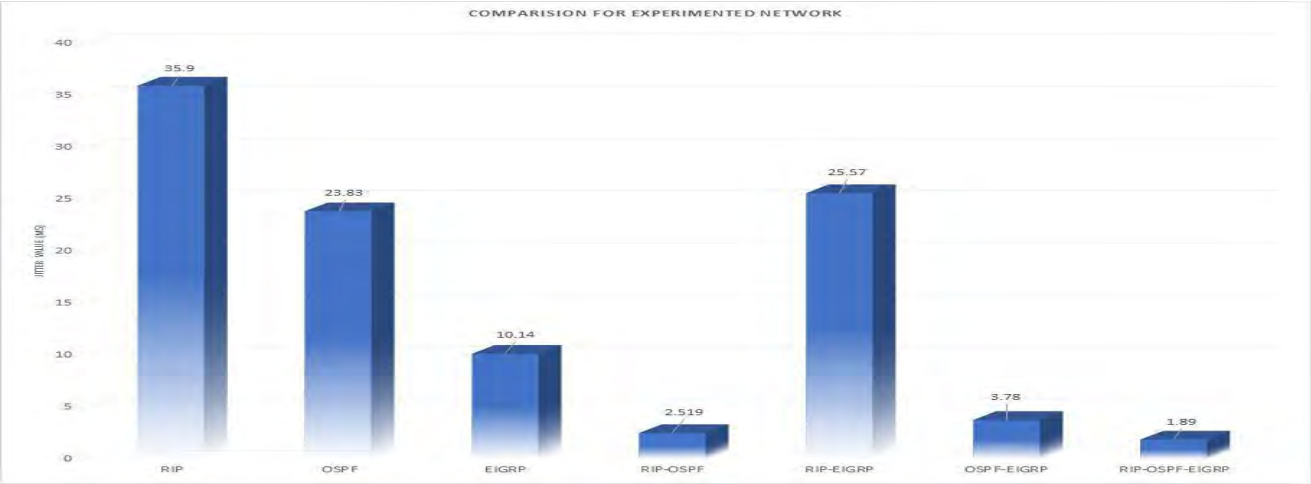


Figure 5.15: Comparison of Jitter Value for Hybrid Network

In the case of virtual private network , comparison of jitter value is shown in figure 5.16.

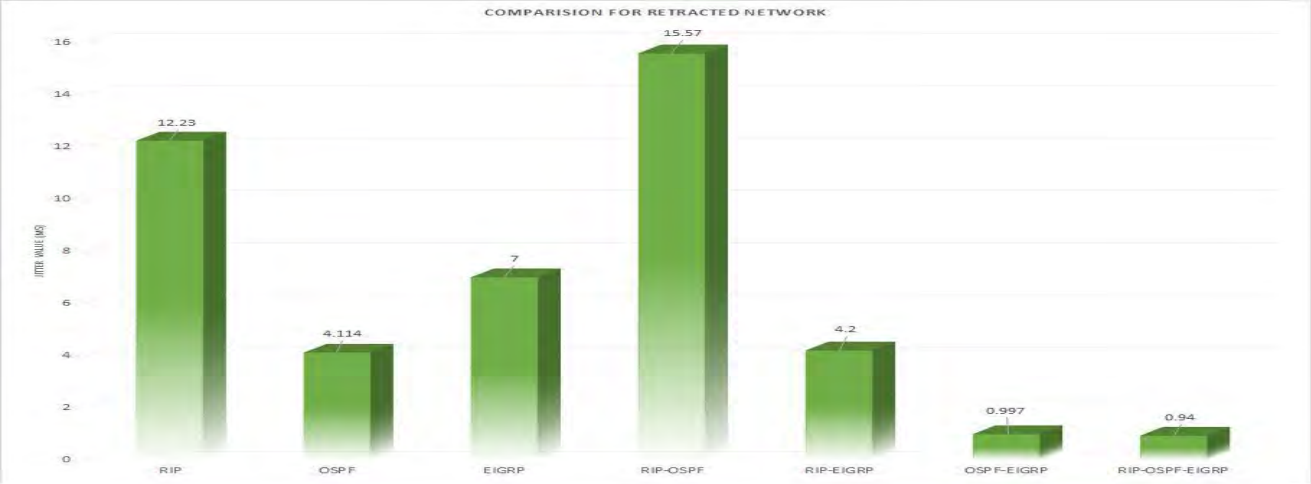


Figure 5.16: Comparison of Jitter Value for Virtual Private Network

5.1.2 Jitter Result analysis and decision

Minimum jitter value captured for the protocols is considered the best one for that particular networking system. Following the hybrid network, the lowest jitter value is got for combination of three protocols in a network "RIP-OSPF-EIGRP" that is 1.89ms. RIP-OSPF and OSPF-EIGRP also show the good result for jitter are 2.5 and 3.78 respectively. The very poor result observed for the protocol of RIP (35.9 ms). Similar result is also obtained for Virtual private network considering the flow graph performance of the protocols that RIP-OSPF -EIGRP combined networking protocols show the best performance for every networking design. However, for VPN network, performance increased for every combination and alone protocols comparing the jitter value. Considerable performance shown for RIP, OSPF, RIP-EIGRP that are gained by 65.93%, 81% and 83.57% respectively for VPN network. Only combine RIP-OSPF performance got down as jitter value increased from 2.51 to 15.57 in VPN network.

5.2.1 Evaluation for Packet Length:

Packet Length is measured considering ten different range of the size of the packet that is described through x axis and y – axis is cited as the number of packets in a particular range in percentage. The result is obtained first for each protocol and combined protocols then showing the comparison graph on the basis of the simulation results.

Packet Length Valuation is shown in the figure 5.17 for hybrid network.

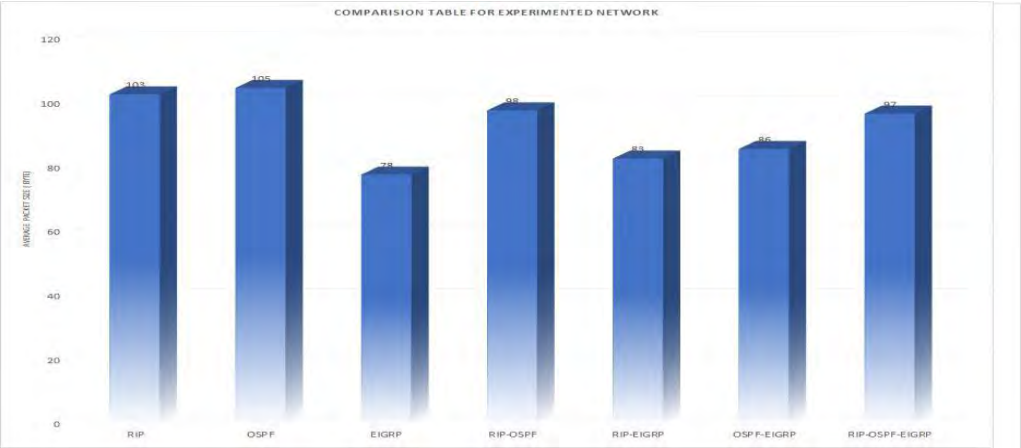


Figure 5.17: Packet Size comparison for Hybrid Network

Packet Length Valuation is shown in the Figure 5.18 for Virtual private network

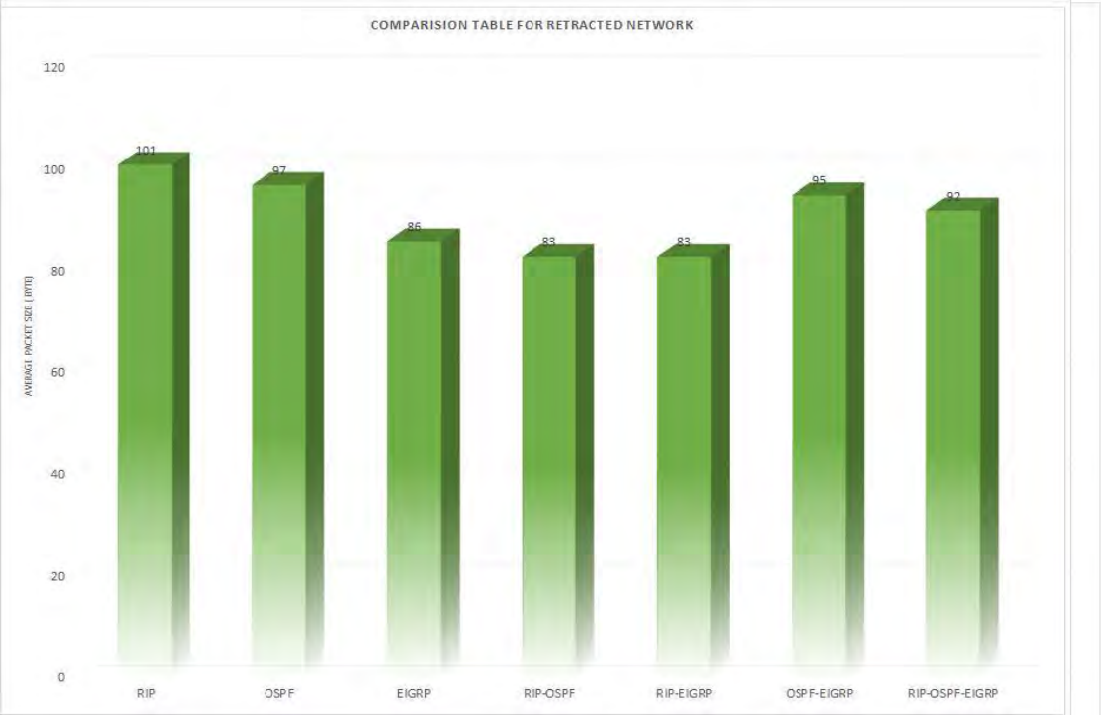


Figure 5.18: Packet Size comparison for Virtual Private Network.

5.2.2 Packet Length Result Analysis and Decision

There is no big difference found in packet size during the transmission of the packet in all there networking system. For Hybrid network, packet size ranges from 78 to 106 for protocols while highest average packet size got for OSPF is 106 and lowest size for EIGRP is 78.

On the contrary, average packet size for Virtual Private network ranges from 83 to 101 which shows minor difference in packet length for all protocols. Here, same average size packet is obtained for RIP-OSPF and RIP-EIGRP , is 83. The maximum packet size is seen for RIP is 101 that is somewhat similar to all other networking systems. Overall, RIP and OSPF protocols show bit more higher packet size for the network.

5.3.1 Evaluation of Packet loss

Result has been found based on the previous graph and finally creating this comparison graph for Packet loss value both for virtual private network and hybrid network.

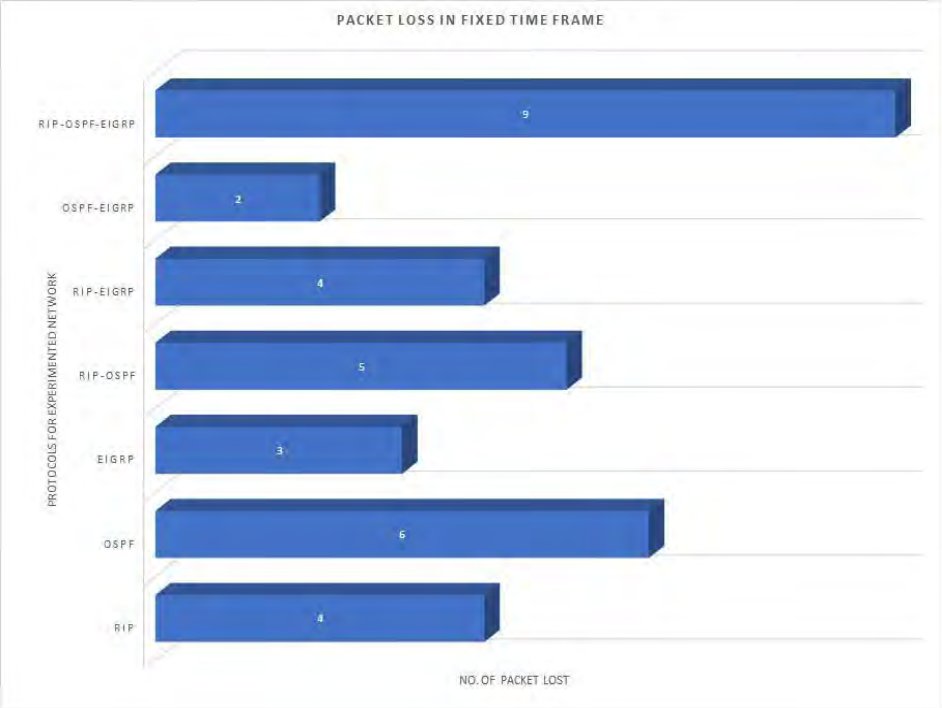


Figure 5.19: Packet loss in Hybrid Network.

Result has been found based on the previous graph and finally creating this comparison graph for Packet loss value both for virtual private network and it is shown in Figure 5.20.

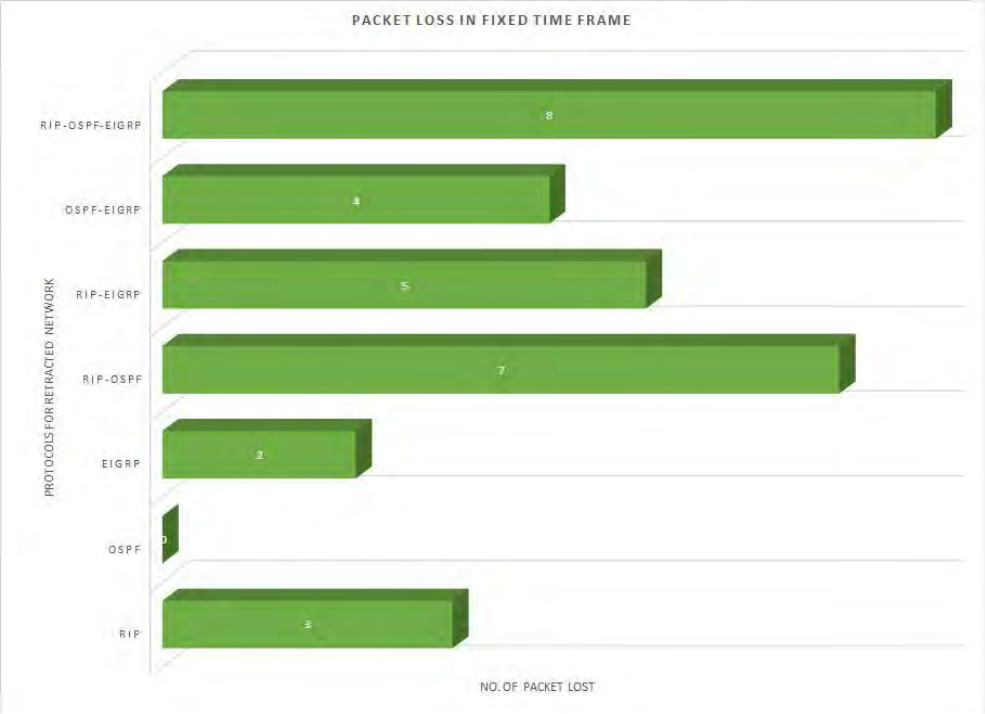


Figure 5.20: Packet loss in Virtual Private Network.

5.3.2 Packet Loss Result Analysis and Decision

Comparison graph for hybrid network indicated that the average percentage of the packet loss is lowest for OSPF-EIGRP as it shows packet loss value is 2 during the transmission steam of the packet. The second-best performance shown for this network is EIGRP having packet loss value 3 . However, poor performance is shown for RIP-OSPF-EIGRP and OSPF for this network that shows 6 and 9 packet loss value during the transmission of the packet.

In the case of Virtual Private network, excellent result shown by OSPF having zero packet loss while RIP-OSPF and RIP-OSPF-EIGRP depicts poor performance as usual in packet loss for all networking systems. Finding the reason for this result for these two protocols, raw data shows many numbers of retransmission request and drop packet that causes higher packet loss percentage for RIP-OSPF and RIP-OSPF-EIGRP.

Comparison table 1: Comparison of routing protocols

Protocols	Hybrid Network				Virtual Private Network				Average			
	Throughput	Jitter	Packet Length	Packet Loss	Throughput	Jitter	Packet Length	Packet Loss	Throughput	Jitter	Packet Length	Packet Loss
RIP	21	35.9	103	4	22	12.23	102	3	21.5	24.06	102.5	3.5
OSPF	24	23.8	105	6	32	4.11	102	0	28.00	13.97	103.5	3
EIGRP	26	10.14	78	3	28	7.0	102	2	27.00	8.57	90	2.5
RIP-OSPF	19	2.519	98	5	12	15.57	104	7	15.50	9.0445	101	6
RIP-EIGRP	22	25.57	83	4	27	4.2	99	5	24.50	14.885	91	4.5
OSPF-EIGRP	30	3.78	86	2	24	0.997	94	4	27.00	2.3885	90	3
RIP-OSPF-EIGRP	15	1.89	97	9	19	0.940	95	8	17.00	1.415	96	8.5

CHAPTER-6

Conclusion and Future Works

6.1 Conclusion

In this report, we designed and evaluated Routing protocols namely RIP, OSPF, EIGRP along with its all possible combinations for Virtual private Network and Hybrid network and applied it to measure throughput, jitter, packet length and packet loss to demonstrate its performance and utility. Initially, websites for two different networks have been developed configuring Apache HTTP Server while PHP will be used as scripting language and MySQL as database. Download and upload option have been initiated with a number of PDF files for each website to check the security measures of the networks. We demonstrated how the results obtained in one network design can change for the configuration of the same protocol in response to dynamically changing conditions of another network. On comparing the results of the simulation of different protocols and combined protocols, the overall best performance is shown for throughput value by combined OSPF-EIGRP and EIGRP protocols while OSPF protocol haves the highest throughput value for Virtual Private Network. Besides, EIGRP and RIP-EIGRP be chosen as the second-best selection for the VPN network. After that, the suggestion goes to combined protocols of either RIP-OSPF-EIGRP or OSPF-EIGRP in term of jitter value, that shows minimum packet delay in both VPN and hybrid networks. The average minimum jitter value for RIP-OSPF-EIGRP and OSPF-EIGRP are 1.415ms and 2.3885ms respectively while the poor performance having maximum jitter is examined for RIP-OSPF is average 15.57 ms for both networks. Moreover, mixed results are captured for packet length in different networks. In general, RIP, OSPF and RIP-OSPF shows the standard and largest packet size during the networks communication. Finally, for the best possible value for packet loss is obtained by EIGRP which average packet loss value is 2.5 in overall two different networks whereas OSPF-EIGRP is suggested for hybrid network and OSPF is for Virtul Private network which shows no packet loss during communication. The results backed by simulation evaluation and validation demonstrate that EIGRP and combined OSPF-EIGRP are best solution to choose routing

protocols for enhancing hybrid networking performance while OSPF can be best solution for Virtual Private Network.

6.2 Future works

There are several future research areas including (I) exploring other routing protocols and its combination with which we could further demonstrate the performance and utility of the network; (II) designing and implementing modern communication secured networks is inevitable for more scientific research in future to combat cybercrimes and network vulnerabilities where different types of cryptographic algorithms like encryption protocols, authentication and hashing protocols are utilized. Therefore, further research will be conducted also to evaluate the particular routing protocols performance in case of using different security protocols in the networks; (III) Our proposed protocols from this research report will be further examined and validated for different other security- enabled networking environments.

Reference

[1] Abdulkadhim, M., “Routing Protocols Convergence Activity and Protocols Related Traffic Simulation with Its Impact on the Network", in international Journal of Computer Science

(2015).http://ijcset.net/docs/Volumes/volume5issue3/ijcset2015050302.pdf

[2] Shrivastava, A., and Rizvi, M. A., "External authentication approach for virtual private network using LDAP," *2014 First International Conference on Networks & Soft Computing (ICNSC2014)*, Guntur, 2014, pp. 50-54

[3] C. Fancy, L. M. M. Thanveer,“An evaluation of alternative protocols-based Virtual Private LAN Service (VPLS),” in IoT and Application (ICIOT), International Conference, Nagapattinam, India, May. 2017, pp. 1-6 (2017). https://ieeexplore.ieee.org/document/8073621/

[4] Younglove, R., "Virtual private networks - how they work," in *Computing & Control Engineering Journal*, vol. 11, no. 6, pp. 260-262, Dec. 2000.

[5] S.U. Masruroh, F. Robby, and N. Hakiem, “Performance Evaluation of Routing Protocols RIPng, OSPFv3, and EIGRP in an IPv6 Network,” in International Conference on Informatics and Computing **(**ICIC**)**, Mataram, Indonesia Oct. 2016, pp. 111-116 (2016). https://ieeexplore.ieee.org/document/7905699/

[6] Rozita Yunos, Siti Arpah Ahmad, Noorhayati Mohamed Noor, “Analysis of routing Protocols of VOIP VPN over MPLS network” in IEEE conference on systems, process and controls (ICSPC) , Kuala Lampur , Malaysia, Dec, 2013.

[7] D. R. Al-Ani, A. R. Al-Ani, “The performance of IPv4 and IPv6 in terms of Routing Protocols using GNS 3 Simulator,” in 9th International Conference on Ambient Systems, Networks and Technologies, ANT-2018 and the 8th International Conference on Sustainable Energy Information Technology, SEIT 2018, May. 2018, pp. 1-6 (2018). https://dl.acm.org/citation.cfm?id=3223610

[8] Luo, Z., Yu, G., Qi, H., and Liu, Y., "Research of a VPN secure networking model," *Proceedings of 2013 2nd International Conference on Measurement, Information and Control*, Harbin, 2013, pp. 567-569.

[9] Akunuri, K., Arora, R., Guardiola, I. G.," A study of speed aware routing for mobile ad hoc networks*,"* in *International Journal of Interdisciplinary Telecommunications and Networking*, Vol 3,pp. 40-61, 2011

[10] Lowe, D. (2016*) Networking All in one*. Dummies Series., United States.

[11] Donald W. J., Bartlett, A. (2013) *Network Security, Firewalls, And Vpns*,. Jones & Bartlett Learning Information Systems & Assurance., United States.

[12] Tanenbaum, A. S. (2010) *Computer Network.* Amsterdam, Netherlands.

[13] Meeran, M., *Wireless Mesh Networks Impact on Voice over IP*, PhD Thesis, Institute of Informatics, Tallinn University, 2014.

[14] Solution for issues connecting wifi or wireless network. (Last accessed on 28 October, 2017) From https://h30434.www3.hp.com/t5/Notebook-Wireless-and-Networking/Solution-for- issues connecting-wifi-or-wireless-using-Ralink/td-p/2248179