

**Analysis of Generic Routing Encapsulation (GRE) over IP Security
(IPSec) VPN Tunneling in IPV6**

By

Johan Ferdous

ID:162-19-1893

Md. Mafiul Islam

ID: 162-19-1895

&

Sajib Chandra sutradhar

ID:161-19-1865

This Report Presented in Partial Fulfillment of the Requirements for the Degree of
Bachelor of Science in Electronics and Telecommunication Engineering
(BSc in ETE)

Supervised By

Md. Taslim Arefin

Associate Professor & Head

Department of Information and Communication Engineering

Daffodil International University



Department of Electronics & Telecommunication Engineering

Daffodil International University

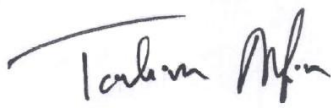
Dhaka, Bangladesh

September,2020

APPROVAL

The Thesis titled “**Simulation of GRE over IPSec-VPN Tunneling Using GNS3 Over IPv6**” submitted by Johan Ferdous Id: 162-19-1893, Md. Mafiul Islam ID: 162-19-1895 & Sajib Chandra sutradhar ID:161-19-1865 to the Department of Electronics and Telecommunication Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirement for the degree of Bachelor of Science in Electronics and Telecommunication Engineering and approved as to its style and contents. The presentation was held on September 02, 2020.

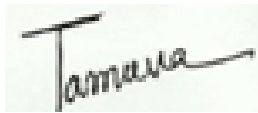
BOARD OF EXAMINERS



Md. Taslim Arefin
Associate Professor & Head
Department of ETE
Daffodil International University



Prof. Dr. A.K.M Fazlul Haque
Professor
Department of ETE
Daffodil International University



Ms. Tasnuva Ali
Assistant Professor
Department of ETE
Daffodil International University

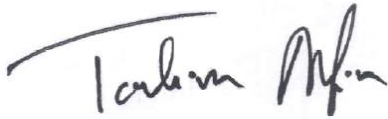


Dr. Saeed Mahmud Ullah
Associate Professor
Department of EEE
Dhaka University

DECLARATION

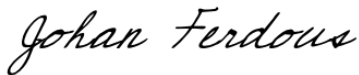
I hereby declare that this thesis Report has been done by us under the supervision of **Md. Taslim Arefin, Associate Professor & Head, Department of Information and Communication Engineering, Daffodil International University**. I also declare that neither this report nor any part of it has been submitted elsewhere for award of any degree or diploma.

Supervised By



Md. Taslim Arefin
Associate Professor & Head
Department of ETE
Daffodil International University

Submitted By



Johan Ferdous
ID:162-19-1893
Department of ETE
Daffodil International University



Md. Mafiul Islam
ID:162-19-1895
Department of ETE
Daffodil International University



Sajib Chandra sutradhar
ID:161-19-1865
Department of ETE
Daffodil International University

ACKNOWLEDGEMENT

First and foremost, praises and thanks to the God, the Almighty, for His showers of blessings throughout our research work to complete the research successfully.

We would like to express our deep and sincere gratitude to our research supervisor, **Md. Taslim Arefin**, Associate Professor & Head Department of Information and Communication Engineering for giving me the opportunity to do research and providing invaluable guidance throughout this research. His dynamism, vision, sincerity and motivation have deeply inspired me. He has taught us the methodology to carry out the research and to present the research works as clearly as possible. It was a great privilege and honor to work and study under his guidance. I would also like to thank him for his friendship, empathy, and great sense of humor.

We are extremely grateful to two of our alumni from our department **Md. Raihan Uddin** and **Nawshad Ahmed Evan** for their technical and lab support. Without their courage and gratefulness, it was quite impossible for to complete this paper.

We owe to our parents for their love, prayers, caring and sacrifices for educating and preparing me for my future.

I am extending my thanks to our classmates for their support during my research work. I also thank all the teacher and staff of Department of Information and Communication Engineering their kindness.

Johan Ferdous
Md. Mafiul Islam
&
Sajib Chandra Sutradhar

DEDICATION

**THIS THESIS IS DEDICATED
TO
THE FRONTLINE WARRIORS
WHO ARE LEADING THE BATTLE AGAINST
COVID-19**

ABSTRACT

Over the past years, Virtual private networks (VPN) is an essential technique for providing remotely secure connections to exchange information while IPv6 is the future of internet. It is superior to the currently reigning version of the internet protocol, Ipv4. But due to the backward compatibility problem of IPv6, is not deployed nationwide yet. In This Project Analysis of GRE over IPSec-VPN Tunneling Over IPv6 is done using GNS3 network simulator connecting two remote offices with IPv4 compatible devices over a IPv6 internet providing a VPN tunneling protocol solution for establishing a private secure network. Which facilitates the IPv6 deployment ensuring co-existence of Internet protocols until IPv6 compatible devices replaces entire old IPv4 combatable devices. The testing and verification analyzing of data packets have been done using the PING tool. Solar winds are used to measure the throughput and Wireshark ensures the encryption of data packets during data exchange between different sites belonging to the same institution. The performance in terms of response time, throughput and packet encryption of the proposed method is analyzed. The result shows the average response time of 40.372 ms, a throughput in Kbps after transferring ICMP traffic from source for router and finally after crypto session a analysing of the encrypted packet.

Table of Content

Content	Page No.
APPROVAL	ii
DECLARATION	iii
ACKNOWLEDGEMENT	iv
DEDICATION	v
ABSTRACT	vi
CHAPTER 1: INTRODUCTION	1-3
1.1 OBJECTIVES	2
CHAPTER 2: RELATED WORK	4
CHAPTER 3 VIRTUAL PRIVATE NETWORK	5-8
3.1 Tunneling Techniques	5
3.1.1 Configured tunneling	5
3.1.2 Automatic tunneling	5
3.2 Tunneling Protocols	5
3.2.1 Point to Point Tunneling protocol	5
3.2.2 Layer 2 Tunneling Protocol	6
3.2.2 Layer 2 Tunneling Protocol	6
3.2.3 Secure Socket Layer	6

3.2.4 IPSec	6
3.2.5 Generic Routing Encapsulation	7
3.2.6 GRE OVER IPSec	8
3.3 IPv4 Limitation	8
Chapter 4 INTERNET PROTOCL VERSION 6	9-11
4.1 Background Story	9
4.1.1 IPv6 timeline: A history of the Internet Protocol	9
4.2 Why is IPv6 Needed Now?	10
4.3 IPv6 Benefits	10
4.4 Ipv6 Deployment	10
CHAPTER 5 IPv6 TRANSITION MECHANISM	13-17
5.1 Dual stack	13
5.2 Tunneling	14
5.3 Translation	16
CHAPTER 6: METHODOLOGY	18-20
6.1 System Configuration	19
CHAPTER 7 SIMULATION & ANALYSIS	21-25
7.1 Simulation	21
7.2 Simulator	21
7.2.1 Graphical Network Simulator (GNS3)	21
7.2.2 Wireshark	21
7.2.3 Solar Putty	22
7.2.4 Solar Winds	22
7.3 Design and Analysis in GNS3	22

7.4 Resulting Parameter	23
7.4.1 Response Time	23
7.4.2 Throughput	24
7.4.3 Packet Analysis	25
Chapter 8: Conclusion	26
8.1 Future work	26
REFERENCES	27-29

List of Figures

Chapter 1	
Figure 1.1: Proposed Topology	2
Chapter 3	
Figure 3.1: GRE encapsulation	7
Figure 3.2: GRE Packet forwarding	7
Figure 3.3: GRE over IPSec Packet format	8
Chapter 4	
Figure 4.1: Figure 1 User adoption of IPv6 since late 2011.	11
Figure 4.2: User adoption of IPv6 (2017 to mid-2018)	11
Figure 4.3: IPv6 users per economy.	12
Figure 4.3: IPv6 users per economy.	12
Chapter 5	
Figure 5.1: Dual stack Mechanism	13
Figure 5.2: Tunneling Mechanism	14
Figure 5.4: Translator Mechanism	17
Chapter 6	
Figure 6.1: Network Topology	18
Figure 6.2: Step by Step work flowchart	19
Chapter 7	
Figure 7.1: Network topology in GNS3 simulator	23
Figure 7.2: Ping Report	24
Figure 7.2 Throughput analysis	25
Figure 7.3: Packet analyzing	25

List of Tables

Chapter 3

Table 3.1 Encapsulation of both ESP and AH protocols on tunnel and transport mode:	6
---	----------

Chapter 5

Table 5.1 A brief advantage or disadvantage	15
---	-----------

Chapter 7

Table 6.2 Responses of the packet sequences	24
---	-----------

CHAPTER 1

INTRODUCTION

IPv6 is ready to use future technology that rapidly increases its deployment in the network sector. Features like Auto configuration, a simplified header, Faster routing, Reduced network complexity, and many more that make it an easy pick for network administrators to choose ipv6 over ipv4. [1]

But the biggest drawback of ipv6 is it's not backward compatible. It lacks backward compatibility with the existing internet protocol, which is IPv4. The reason more IPv6 deployment isn't being done in the network world will need new transition tools until all network devices are compatible with the coexistence of IPv4 and IPv6. [2]

A virtual private network (VPN) is a technology for communicating different private networks or end to end connectivity. And there are various tunneling protocols such as Point to Point Tunneling Protocol (PPTP), Layer 2 Tunneling Protocol (L2TP), Internet Protocol Security (IPSec), Secure Socket Layer (SSL), Generic Routing Encapsulation (GRE) to provide security for VPN tunnel. These protocols are working fine on the current IPV4 networks. But as mentioned earlier the network world moving rapidly from IPV4 to IPV6 and IPV6 promises better security so more advanced tunneling has to be developed. [3]

IPSec (Internet Protocol Security) is a protocol or technique that provides security for the network layer. The Internet Engineering Task force form this protocol, so that it can be deployed to create a secure TCP/IP work environment over the Internet considering having various advantages like flexibility, scalability, and interoperability. It initially supports security among hosts rather than users, what the other security protocols do not support. Today IPSec is highlighted as one of the prominent security infrastructures for the future generation of the internet. It also has suitable features to implement VPN (Virtual Private Network) with great efficiency and it is expected that the application fields of IPSec will to grow quickly. [27] IPSec proves its importance with its various security features aiming at a secured data transmission between end devices. IPSec provides Data Confidentiality to Data by Encrypting it during its

journey. Data integrity is maintained by using Hashing algorithms in IPSec. While Digital Certificates or Pre-Shared keys gives Authentication services. A sequence of numbers built into the IPSec packets defends Replay Attacks. By using this sequence numbers. [28]

The generic routing encapsulation (GRE) is a VPN tunneling protocol, which we can establish a direct point-to-point connection between gateways. The GRE has a unique is ability to allow two peers to share data that they could not share on the public network directly. GRE tunnels can also support multicast data streams over Internet transmission. [11]

Keeping it in mind the backward compatibility issue of IPv6 This project analyzes two of the existing VPN tunneling protocols- IPSec and GRE to develop a more secure tunneling protocol envisioned in a scenario where the remote end devices compatible with the existing protocol(IPv4) are connected via the internet that incorporates IPV6 using GNS3 simulator.

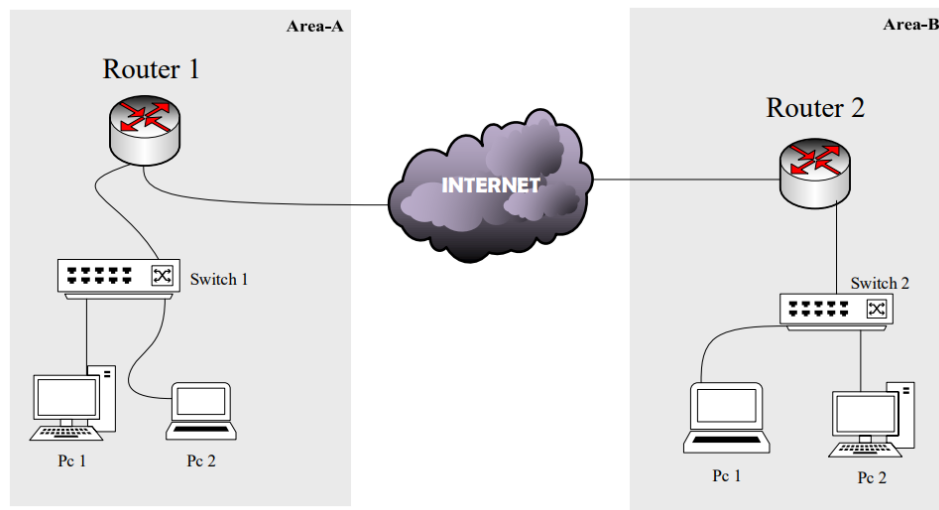


Figure 1.1: Sampled Topology

1.1 OBJECTIVES

- The main goal of this project is to create a VPN tunneling protocol for a scenario where both IPv4 and IPv6 can co-exist while establishing a secure data communication network between two remote campuses of a university.
- We are going to equip the 2 most used tunneling protocols.
 1. GRE (Generic routing encapsulation)
 2. IPSec (Internet Protocol Security)to achieve a high-security level for the VPN tunnel.
- Graphical Network simulator 3 is used to describe our work plan.
- To analyze the performance of our proposed method, the parameters considered are
 1. Response Time
 2. Packet Encryption
 3. Throughput
- The testing and verification analysis of data packets are done using the PING tool. Solar winds are used to measure the throughput and Wireshark to ensure the encryption of data packets during data exchange between different sites belong to the same institution.

CHAPTER 2

RELATED WORK

The transition from IPv4 to IPv6 is an active area of research. In [1] Various transition Techniques like dual-stack, tunneling, and translation are compared based on quality parameters such as Average round trip time(RTT), bandwidth, and throughput.

Various IPv6 Transition methods based on tunneling had an analytical discussion and later they were Compared in [2]. A variety of parameters such as deployment time, CPE change, IPv4 continuity, access network, address mapping, end-to-end transparency, scalability was put into consideration in this paper.

4to6 and 6to4 are two widely used transition Mechanisms over Point to Point and IPsec VPN. Their performance is compared in [7]. They have compared IPv4/IPv6 vs multiple transition mechanisms in terms of various parameters including UDP and TCP traffic throughput, delay of the packets, jitter in the system, DNS, and VoIP with and without VPN.

The work in [4] proposes a new ISP Independent Architecture (IIA) for interconnectivity in a hybrid network including IPv4 and IPv6 networks. More flexibility to the users to deploy their required transition solutions are provided by their proposed ISP independent solution. In their proposed model a network administrator can create multiple combinations of transition mechanisms for different destinations to manage security and load balancing.

Both in [5] and [6] the problems related to the transition between IPv4 and IPv6 are discussed. Problems like Interception by RA/DHCP server, Interception by Firewall. Unstable functions in the DNS zone record. poor coordinated tunnel network, lack of path/peering, Bad TCP reaction, misbehaving DNS resolution are taken into consideration in [5] causing issues like delay and disconnection. In contrast, our proposed system will represent the GRE over IPsec-VPN Tunneling over IPv6 using GNS3 where the mentioned paper is proposed the simulation of GRE over IPsec in IPv4.

CHAPTER 3

VIRTUAL PRIVATE NETWORK

A Virtual Private Network (VPN) is a brilliant technique for connecting remote destinations over the internet. VPN provides minimal cost, proficient utilization of bandwidth, versatile and flexible functionality, secure and private connections. VPN creates a virtual private line between two network sites through which encrypted data passes through. [3]

3.1 Tunneling Techniques

In VPN, transmitting encapsulated data over the public shared network uses tunneling mechanism. In order to fulfill various administrative requirement, there are two types of tunneling techniques are available: configured (static) and automatic (dynamic).

3.1.1 Configured tunneling

It is normally utilized when sites or hosts interchange data regularly. Whenever a little number sites needs connection, in which case network managers understand manual configuration at the both tunnel ends in not too difficult and time consuming process, they prefer this kind tunneling.

3.1.2 Automatic tunneling

An IPv4 address for each host in this tunneling scheme. In this kind of tunneling technique A node is empowered to set up a tunnel without configuration. [8]

3.2 Tunneling Protocols

In order to provide security to the VPN tunnel various protocols are used. The protocols ensure encrypted data transmission between two endpoints. They are discussed below:

3.2.1 Point to Point Tunneling Protocol (PPTP)

The data link layer is the operation area of this VPN protocol. From the point-to-point protocol. it has been expanded using the same authentication mechanisms as point to point protocol (PPP) [9]

3.2.2 Layer 2 Tunneling Protocol (L2TP)

Features of both PPTP and layer two forwarding is combined in this protocol. The network traffic is discarded by mechanism of flow control to keep both address congestion and overhead to lowest amount possible. [10]

3.2.3 Secure Socket Layer (SSL)

Internet traffic over an encrypted tunnel receives encryption and authentication with this VPN protocol. Because of working in the session layer various application such as email and web services. [9]

3.2.4 IPSec

Internet Engineering Task Force (IETF) created IPSec (Internet Protocol Security) as an end-to-end mechanism to ensure data security in IP communications. IPSec operates in two mode

- a. **Transport mode:** IP packets are secured between two end devices in transport mode. Only the payload is concerned by the processing and the IP packet header is preserved to allow the routing to operate seamlessly.
- b. **Tunnel mode:** In this mode of IPSec IP packet exchanges are secure from network to network. An entirely new IP packet header is created and the whole IP packet (header + payload) is encapsulated. [11]

Table 3.1 describes encapsulation of both ESP and AH protocols on tunnel and transport mode:

Protocol	Transport Mode	Tunnel Mode
AH	IP AH data	IP AH IP data
ESP	IP ESP data ESP-T	IP ESP IP data ESP-T
AH+ESP	IP AH ESP data ESP-T	IP AH ESP IP data ESP-T

3.2.5 Generic Routing Encapsulation

The generic routing encapsulation (GRE) is a VPN tunneling protocol, which we can establish a direct point-to-point connection between gateways. A feature that make GRE unique is its ability to allows two peers to share data that they could not share on the public network directly. GRE tunnels can also support multicast data streams over Internet transmission. [11]

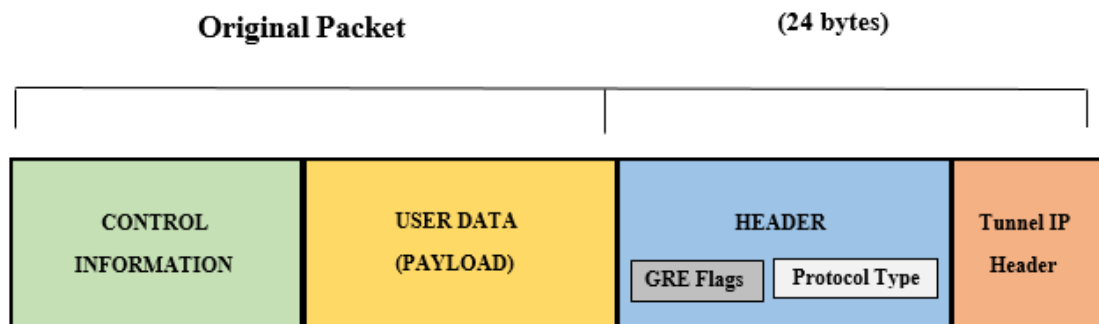


Figure 3.1: GRE encapsulation

In a tunnel, between the two endpoint a GRE data can travel directly. Even when the packet traverses other routers and while using this protocol there is no interaction with its payload.

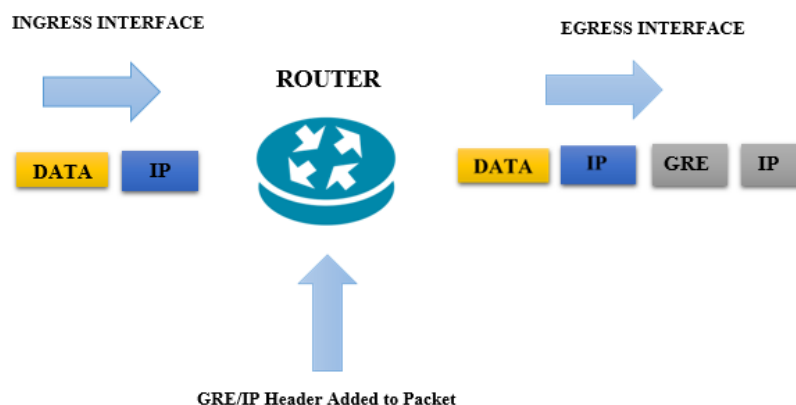


Figure 3.2: GRE Packet forwarding

3.2.6 GRE OVER IPSec

Both IPSec and GRE has its own limitation. IN case of IPSec that is it can only be used for unicast traffic while weak security of GRE makes in vulnerable to different attack from the figure 3.3 we can have the showcase of the fact that, by how adding GRE headers this solves the unicast problem of IPSec while the security features of IPSec strength the security level provided by the combined protocol. [12]

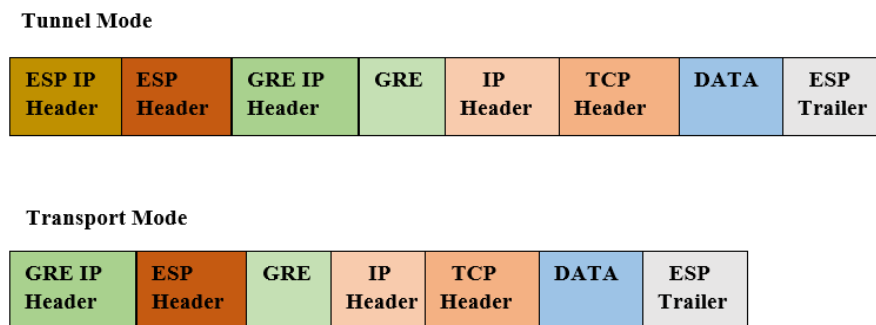


Figure 3.3: GRE over IPSec Packet format

3.3 IPv4 Limitation

When The Internet Protocol Version 4 (IPv4) published in 1981. Its developer could not have imagined that the user of IP address will increase that much in such a sort time which proved IPv4 needed to be changed. Beside this problem IPv4 cannot avoid some other flaws those listed below.

1. **Address Space insufficiency**
2. **Low Security**
3. **Network Congestion**
4. **Packet Loss**
5. **Lack of Data Priority [13]**

Chapter 4

INTERNET PROTOCL VERSION 6

Internet Protocol (IP) acknowledge that how computers communicate over a network. Internet Protocol version 6 (IPv6) is the latest edition of the Internet Protocol (IP) terminology. It is the alternative for Internet protocol for IPv4. Some of the flaws of IPv4 are fixed with IPv6. The process of addresses configuration and their handling by Internet hosts are now made much simpler by this new internet protocol. [14]

4.1 Background Story

Suffering from different issues with IPv4 The Internet Engineering Task Force (IETF) started their work on a new protocol from 1994, that was intended to take the place of currently using IPv4. [15] In order to tackle the headlining problem of IPv4 address exhaustion IPv6 was developed by them. in December 1998. Later, IPv6 became a Draft Standard for the IETF, and they also ratified it as an Internet Standard on 14 July 2017.

4.1.1 A brief recap of the major events in the development of the new protocol

1998: Basic protocol was published.

2003: Basic socket API and DHCPv6 was published.

2004: Mobile version IPv6 was published.

2004: Flow label specifications for the new protocol were added

2006: Address architecture of IPv6 was stable and had little revision

2006: Node requirements for setting up IPv6 published

2008: Google gets into the IPv6 regime. And the whole procedure recieved a boost.

2010: The IPv6 Forum recognizes the first IPv6 education and certification program from Learning@Cisco's professional networking portfolio.

2011: World IPv6 Day was organized by The Internet Society (ISOC)

4.2 Why is IPv6 Needed Now?

The first and foremost reason for migrating from IPv4 to IPv6 is to tackle the need of rapidly growing internet user's society. With the 32-bit address format, IPv4 can handle 4.3 billion unique IP addresses while 128-bit address format of IPv6, this new protocol can support up to 340,282,366,920,938,463,463,374,607,431,768,211,456 unique IP addresses. This huge number of addresses is large enough to configure a unique address on every ports, every device in the Internet and even after we will still have a lot of addresses at unused situation. [14]

4.3 IPv6 Benefits

Some of IPv6 benefits rather than the advantage of a wider address space are pointed out down:

1. **Scalability**
2. **Security**
3. **Real-time applications**
4. **Plug-and-play**
5. **Mobility**
6. **Optimized protocol**
7. **Better Addressing and routing**
8. **Extensibility**
9. **Merging [14]**

4.4 Ipv6 Deployment

It has been almost seven years since World IPv6 Launch day on 6 June 2011. The **Asia Pacific Network Information Centre (APNIC)** which is the regional Internet address registry (RIR) for the Asia-Pacific region conducts a survey that shows the increase in the rate of deployment IPv6 years in between 2011 to 2018. Figure 3.1 and 3.2 shows the User adoption of IPv6 since late 2011 to 2017. [16]

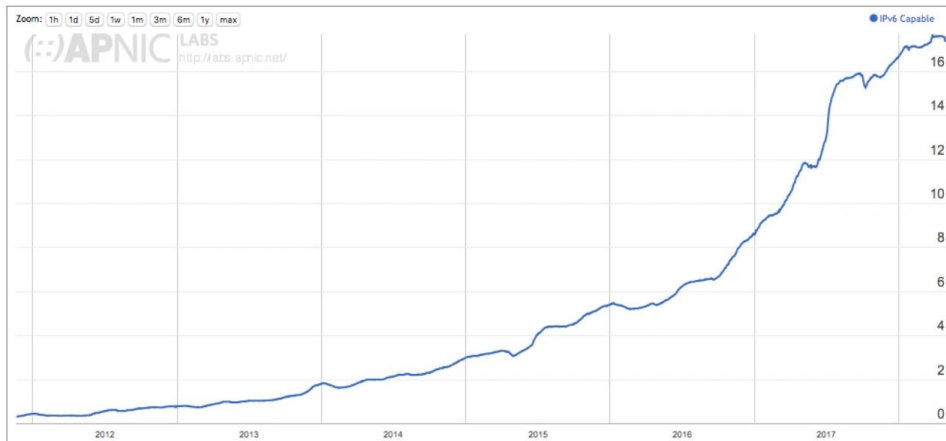


Figure 4.1: User adoption of IPv6 since late 2011.

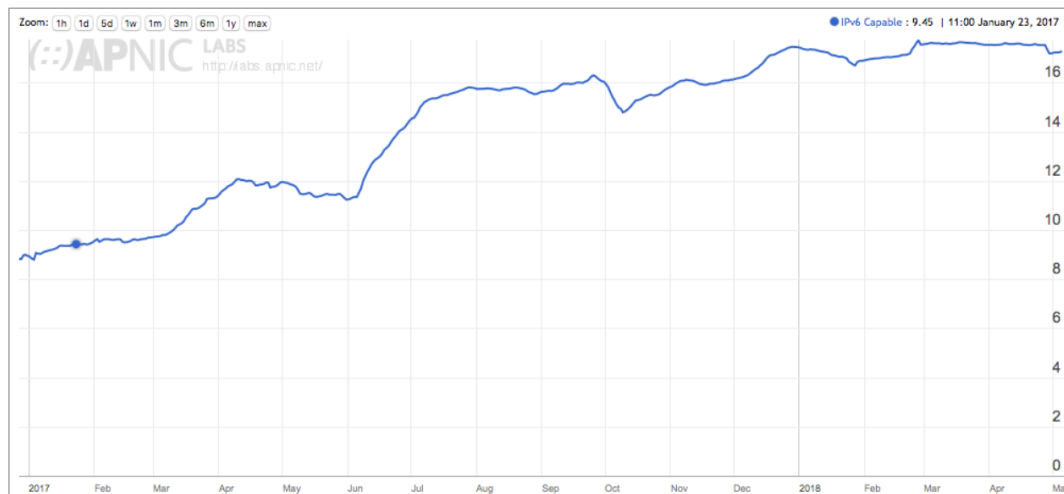


Figure 4.2: User adoption of IPv6 (2017 to mid-2018)

From the graphs and the data, it is obvious that the rate of ipv6 deployment is increasing rapidly over the years. And it is not a very difficult thing to assume that with the advanced services provided by IPv6, its deployment rate will increase faster in the upcoming years.

Now Figure 4.3: shows IPv6 users per economy. This also indicates how rapidly the people belonging to top economical countries are upgrading to IPv6

Country	IPv6 Users	% of Total World Count	% of National Users
India	242M	44%	52%
USA	117M	21%	40%
Germany	30M	6%	42%
Brazil	30M	6%	21%
Japan	28M	5%	24%
UK	17M	3%	27%
France	12M	2%	21%
Canada	7M	1%	20%
Belgium	6M	1%	58%
Malaysia	5M	1%	22%

Figure 4.3: IPv6 users per economy.

We can also have a look at the percentage of users who are using IPv6 of the world's top 20 ISPs. Figure 4.4 shows the popular ISP are migrating rapidly to IPv6.

Rank	AS	AS Name	CC	Users (est)	V6 Users (est)	V6%
1	AS55836	Reliance Jio	IN	257,116,163	236,669,761	92%
2	AS7922	Comcast Cable	US	48,845,229	35,701,856	73%
3	AS7018	ATT Services	US	27,190,530	21,621,772	80%
4	AS38266	Vodafone Essar Ltd.	IN	42,711,918	17,068,044	40%
5	AS22394	Verizon Wireless	US	18,499,350	15,788,328	85%
6	AS45271	Idea Cellular	IN	38,817,216	15,470,268	40%
7	AS21928	T-Mobile USA	US	15,402,964	14,513,144	94%
8	AS3320	Deutsche Telekom ISP	DE	23,392,392	14,118,853	60%
9	AS5607	BSKYB Broadband	GB	13,714,642	12,821,973	93%
10	AS2516	KDDI	JP	22,146,612	11,725,651	53%
11	AS28573	CLARO	BR	24,184,316	11,048,081	46%
12	AS17676	Softbank BB	JP	25,292,851	8,259,099	33%
13	AS3215	Orange	FR	16,990,645	7,976,416	47%
14	AS20057	ATT Mobility	US	14,455,761	7,967,862	55%

Figure 4.4: IPv6 users per ISP

CHAPTER 5

IPv6 TRANSITION MECHANISM

Since IPv4 and IPv6 are not interoperable and hence different transition mechanisms play the key role to create an environment where both ipv4 and IPv6 can co-exist. The three basic transition mechanisms – dual stack, tunneling and translation techniques.

5.1 Dual stack

Dual stack technology runs both IPv4 and IPv6 dual internet protocol in a single environment and it provides compatibility in communication for both routers and hosts. [10] This mechanism is put into an action when the router interfaces are cable to process both IPv4 and IPv6 traffic. The interfaces are usually preferred to configure both IPv6 and IPv4 alongside. The Domain Name Server plays an important role to translate from Internet Protocol addresses to domain name. For dual stack scenario the IPv4 traffic communicate with version 4 DNS server and IPv6 communicate with version 6 DNS server. To operate this mechanism, the routers must be enabled both IPv4 and IPv6 routing [18].

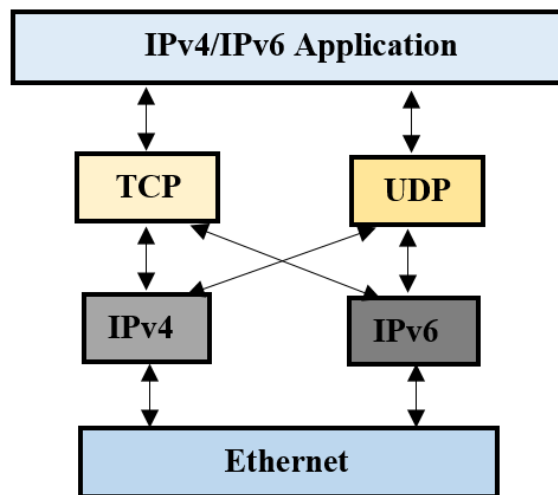


Figure 5.1: Dual stack Mechanism.

All recent IoT devices and operating systems, are now supported by both IPv4 and IPv6.

5.2 Tunneling

Tunneling is a technique to create end to end network connectivity from one network to another remote network for transferring data.

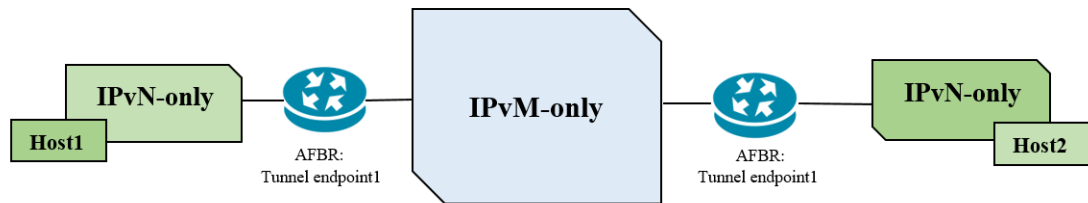


Figure 5.2: Tunneling Mechanism

For conveying IPvN packets through the IPvM network we configured a tunnel by measuring IPvN (Host1) as source and IPvN (Host2) as destination. When the packets from IPvN travels via tunnel it gets encapsulated by the tunnel header. Then the IPvN traffic is forwarded through the IPvM network. When the egress endpoint of the tunnel receives the encapsulated IPvN packet, it opens the encapsulated packet, extracts the original IPvN packet and forwards it to the destination Host2 network. The tunnel header is set up before the original IP header. Generic Routing Encapsulation is the best tunneling technique that allows routing of IPv4 over IPv6 or IPv6 over IPv4. [18]

Some of the most widely deployed tunneling techniques are point out down;

- a. **6in4 Tunnel or Manual Tunnel** [13].
- b. **6to4 Tunnel** [14] [1]
- c. **6rd or 6RD** [1] [18]
- d. **ISATAP** [20]
- e. **GRE Tunnel** [21]

Table 5.1 shows a brief advantage and disadvantages of different tunneling protocols

Table 5.1 A brief advantage or disadvantage

Tunneling Mechanism	Advantages	Limitations	Deployment Applications
6 in 4	Stable and secure links for regular communication.	Management overhead.	Site-to-site tunneling mechanism. Used for stable and secure connections
6to4	It's a site-to-multisite mechanism.	Security threats and vulnerabilities. Supports only BGP and static routing.	Site-to-multisite tunneling.
6rd	Statelessness and simplicity.	Vulnerable to spoofing attack	For Ipv6 connection over IPv4

ISATAP	Low maintenance,	Monitoring of traffic is difficult; Works only over the intranet;	Designed for Intrasite use Additional CPU load for encapsulation/decapsulation
GRE	Can be used with routing protocols	Firewall challenges	For Site-to-site tunneling only

5.3 Translation

Direct communication between IPv4 and IPv6 is achieved by IPv4-IPv6 translation technique. The basic principle of translation is shown in figure below. The idea is to convert the semantics between IPv6 and IPv4. Here IPvM is considered as IPv4 and IPvN as IPv6. Generally, translation happens when IPv4 device wants to communicate with IPv6 destination. Usually, translation happens on the IPvM-IPvN border, so the translator would be an AFBR (Address Family Border Router). For IPv6 translation the IPv4 is converted to a hexadecimal state and set up in IPv6 format maintaining last 64 bits and first 32 bits. The response will return to IPvM like vice versa. Again if the IPv6 device wants to communicate with IPv4 device an additional

IPv4 header will add to encapsulate the IPv6 packet. The NAT router will operate this process of translation.

The domain name service will also do translation by exchanging information with each other. For this one translator server will be added before IPv6 and IPv4 DNS server. [18]

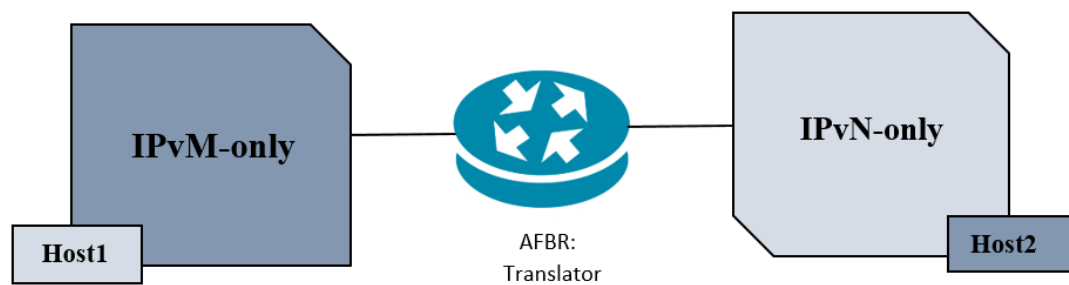


Figure 5.4: Translator Mechanism

Some of the very popular translation technique pointed below:

- a) **NAT - PT** [17].
- b) **NAT64 and DNS64** [18] [19]
- c) **464XLAT** [1]
- d) **BIS and BIA** [25] [26]

CHAPTER 6

METHODOLOGY

In this project we have considered a scenario where two remote branches one located at Dhanmondi another located at Ashulia having network equipment compatible with IPv4 are connected via the internet of IPv6.

The network simulation is done using GNS3 version:2.2.5 consisting of routers with Cisco 7200 VXR series type and switches with Catalyst 2600 series type.

Now at dhanmondi office we are considering two loopback addresses of router 1. where loopback address 10.1.1.100 is configured using IPv4 and loopback address 4004:1/128 is configured using IPv6.

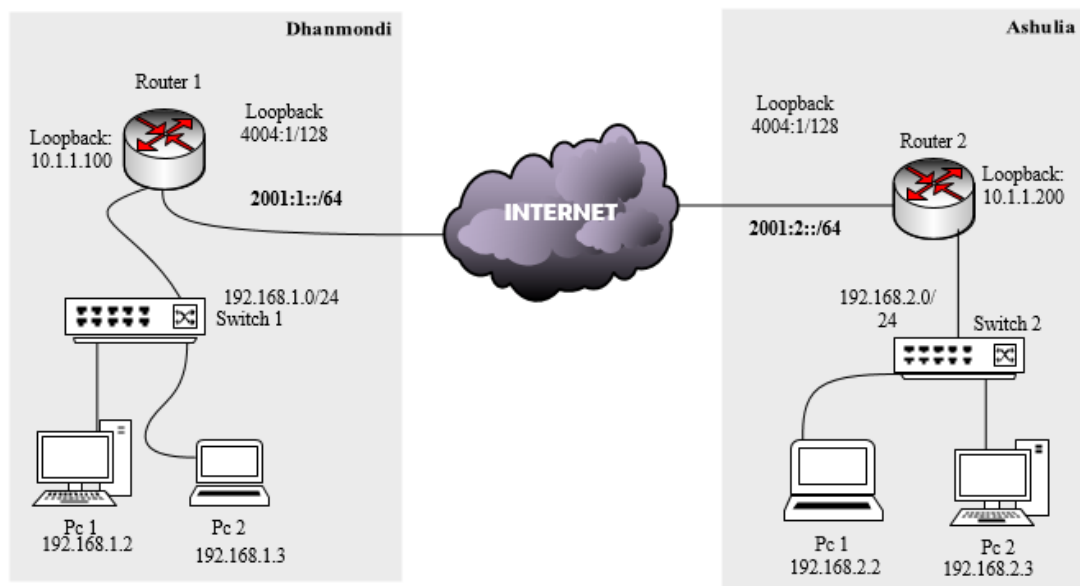


Figure 6.1: Network Topology

At the Ashulia office we have also considered two loopback addresses for router 2. Loopback address 10.1.1.200 is configured using IPv4 while the other loopback address 4004.1/128 is configured using IPv6.

After connecting the routers over the cloud we have established GRE tunnel over IPv6 loopbacks of the both routers. Then we have connected IPv4 loopbacks over IPv6 GRE tunnel establishing GRE over IPsec on IPv4 loopbacks. Thus two remote LANs are connected over the established VPN tunnel. Now router 1 LAN and router 2 LAN are connected and traffic encryption is obtained.

A step by step work flow chart of the methodology is given below

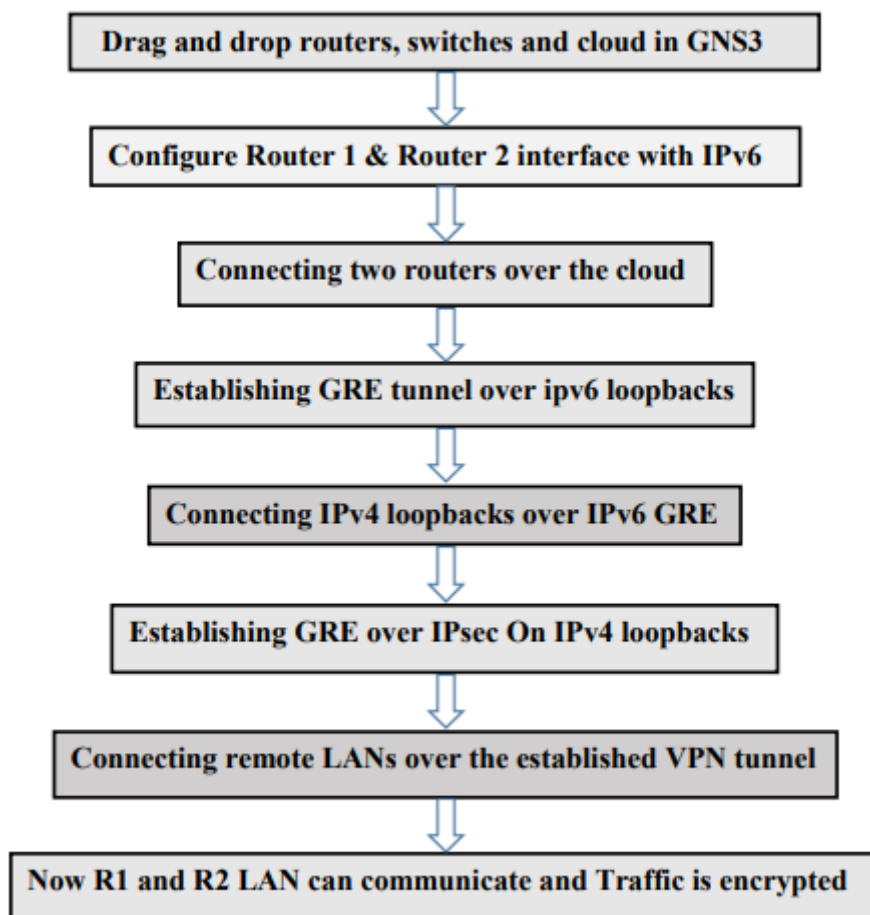


Figure 6.2: Step by Step work flowchart

6.1 SYSTEM CONFIGURATION

A detailed configuration of the system is provided below for better understanding of the platform environment where the simulations are performed.

OS Name:	Microsoft windows 10 pro
Version:	10.0.1863 Build 18363
Os Manufacturer:	Microsoft Corporation
System Manufacturer:	MSI
System Model:	MS-7A15
System type:	x64 based PC
System SKU:	Default string
Processor:	Inter® core™ i5-6500 CPU @ 3.20 GHz, 3192 , 4 core(s),4 Logical processor
BIOS Version/Date:	American Megatrends Inc. 1.70,21/04/2017
SMBIOS Version:	3.0
Embedded Controller:	Version: 255.255
BIOS Mode:	Legacy
Baseboard Manufacturer:	MSI
Baseboard Product:	H110M PRO-VD PLUS (MS-7A15)
Baseboard Version:	1.0
Platform Role:	Desktop
Secure Boot State:	Unsupported
Boot Device:	\Device\HarddiskVolume1
Hardware Abstraction Layer:	Version = 10.0.1832.752
Installed Physical Memory:	12.0 GB

CHAPTER 7

SIMULATION & ANALYSIS

7.1 Simulation

Simulation demonstrates the system and process of creating a structure of an existing or proposed model in order to identify and understand their working process. The estimated value and result can be predicted of the model by using and analysing simulation data and results.

7.2 Simulator

This project is simulated in GNS3. The Process and simulator tools implemented are discussed below.

- 1) We took Dhanmondi as router source and we set up a router there. Ashulia is our destination and we also set up a router there too. For both locations we choose CISCO as router.
- 2) Both source and destination are connected via cloud or service provider and both routers loopback is reachable via cloud.
- 3) We did GRE (Generic Routing Encapsulation) tunnel based on IPv6 loopback of the routers but we used IPv4 tunnel address as peering address of the tunnel.
- 4) Then we did IPv4 routing over IPv6 using GRE tunnel and created another IPv4 loopback for both routers. We also made reachable IPv4 loopbacks by routing through the tunnel.
- 5) After that we configure GRE over IPSEC using those IPv4 loopback of our source and destination router.
- 6) We set up our workstations (PC/Server) that is configured by IPv4 address and check by ping and found that we can reach our destination successfully.

- 7) We measured in Solar Winds that for ICMP traffic we are getting a bandwidth graph.
- 8) By Wire Shark we checked the packets are sending from source to destination are encrypted by ESP protocol.
- 9) After finishing all measurement we found that we can run GRE over IPSEC on IPv6 network to encrypt our traffic as well as IPv4 communication.

7.2.1 Graphical Network Simulator (GNS3)

Network equipment can be easily installed and available in Graphical Network Simulator or GNS which also allows critical network emulation. When it is installed with VMware or Virtual Box we can collect and run different operating systems in a virtual environment and can get the test of real infrastructure. This program allows different systems and devices to communicate each other and a user can create topology according to his own planning. Cisco devices can be deployed as Dynamips in GNS and by using command lines we can operate it. Dynamips are the program of CISCO IOS which is designed for running in a virtual environment. GNS3 provides a graphical environment to run different networks and systems.

7.2.3 Wireshark

Wireshark is an important tool which is used for analysing packets. By using Wireshark, we can capture the network packets and analyse the detail information contained in the packets. This is also used for deep troubleshooting. We can measure source information, destination information, protocol, packet type and other necessary information graphically.

7.2.3 Solar Putty

Solar putty provides us the command line interface with which we can operate the devices. To configure any device, we may need a console and an emulator terminal to generate commands. Solar Putty provides us an open source terminal emulator and console for the serial port as well as we can use different services from that like SSH, Telnet, SCP, and socket connection.

7.2.4 Solar Winds

We can measure the network bandwidth and network performance by Solar Winds. In this project we captured the network bandwidth by sending ICMP traffic from source to destination. Solar Winds is the tool for monitoring traffic bandwidth and analyse in real time.

7.3 Design and Analysis in GNS3

We designed a model in GNS3 network simulator and implemented a real model for our planned network topology. We used both IPv4 and IPv6, Cisco routers, Cisco Switches and PC as end devices in virtual environment. The diagram is displayed here

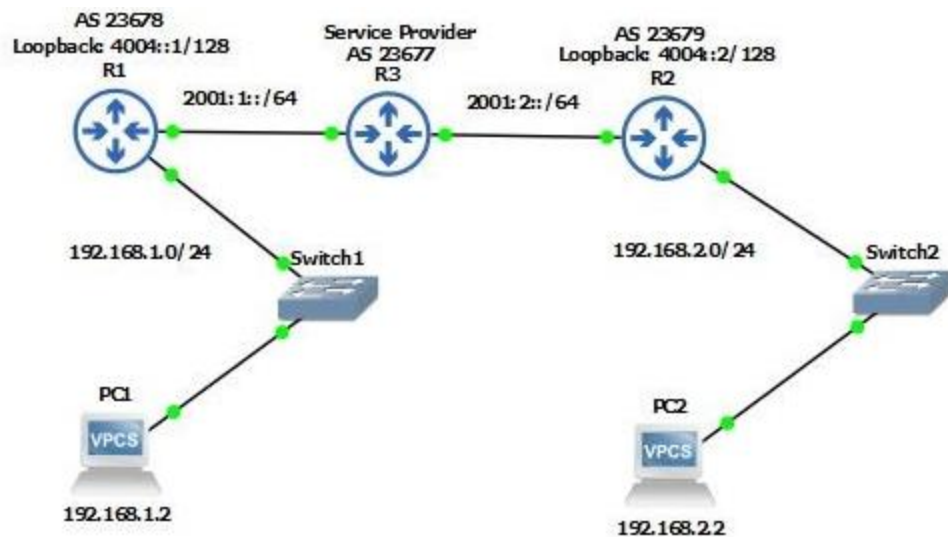


Figure 7.1: Network topology in GNS3 simulator

7.4 Resulting Parameter

7.4.1 Response Time

Response time is the travel time of packets from one source to destination in computer network. We will calculate the response time from the Packet Internet Gopher (PING) report. The lowest response time is 35.795ms and the highest is 47.795ms. So, the average for five response time is 40.372ms. Here the type of packet which travels from source to destination is ICMP (Internet Control Message Protocol). We measured, calculated and collected the data by sending ICMP traffic.

```

PC1> ping 192.168.2.2
84 bytes from 192.168.2.2 icmp_seq=1 ttl=62 time=36.789 ms
84 bytes from 192.168.2.2 icmp_seq=2 ttl=62 time=38.298 ms
84 bytes from 192.168.2.2 icmp_seq=3 ttl=62 time=35.795 ms
84 bytes from 192.168.2.2 icmp_seq=4 ttl=62 time=43.254 ms
84 bytes from 192.168.2.2 icmp_seq=5 ttl=62 time=47.725 ms

PC1> show ip

NAME       : PC1[1]
IP/MASK    : 192.168.1.2/24
GATEWAY    : 192.168.1.1
DNS        :
MAC        : 00:50:79:66:68:00
LPORT     : 20024
RHOST:PORT : 127.0.0.1:20025
MTU       : 1500

PC1> █

```

Figure 7.3: Ping Report

Table 7.2 Responses of the packet sequences

Packet Type	Sequence	Source (host)	Destination (host)	Response Time	Avg. Response Time
ICMP	1	192.168.1.2	192.168.2.2	36.789 ms	40.372 ms
	2			38.298 ms	
	3			35.795 ms	
	4			43.254 ms	
	5			47.725 ms	

7.4.2 Throughput

The highest production or extreme production rate is measured as throughput at which we can produce something. In Ethernet technology or in computer network we can measure throughput with different parameters. A successful transmission of any packet depends on both physical and logical connectivity. Generally, we calculate the data transfer via an interface in bytes per second (bps), kilobytes per second (Kbps), megabytes per second (Mbps) and gigabytes per second (Gbps). Here we found a throughput in Kbps after transferring ICMP traffic from source for router-1 (source router) out interface.

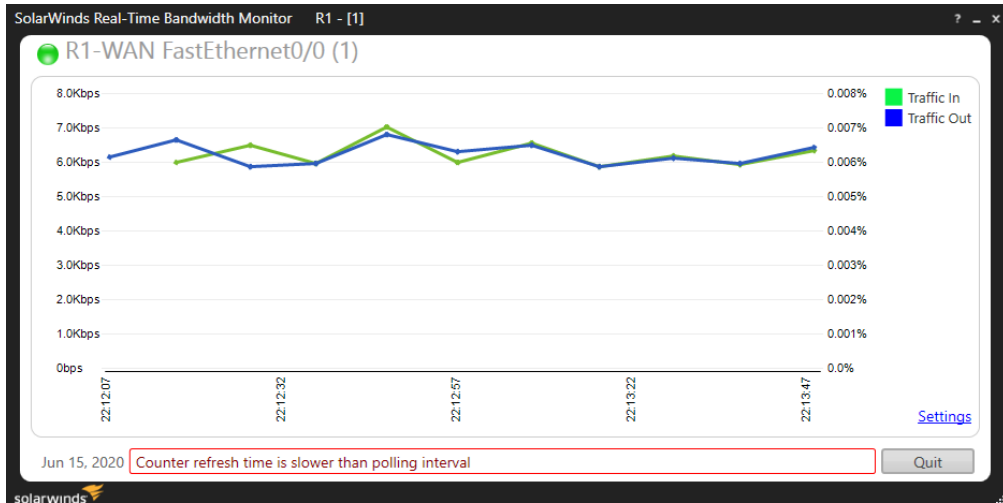


Figure 7.3: Throughput analysis.

7.4.4 Packet Analysing:

We have analyzed our network traffic by Wireshark and can analyse packets that we are sending. As we are using IPsec, the ESP protocol will encrypt our traffic and it will be complete unable to analyse data from encrypted packets. Here after crypto session established we analyse the encrypted packets via Wire Shark.

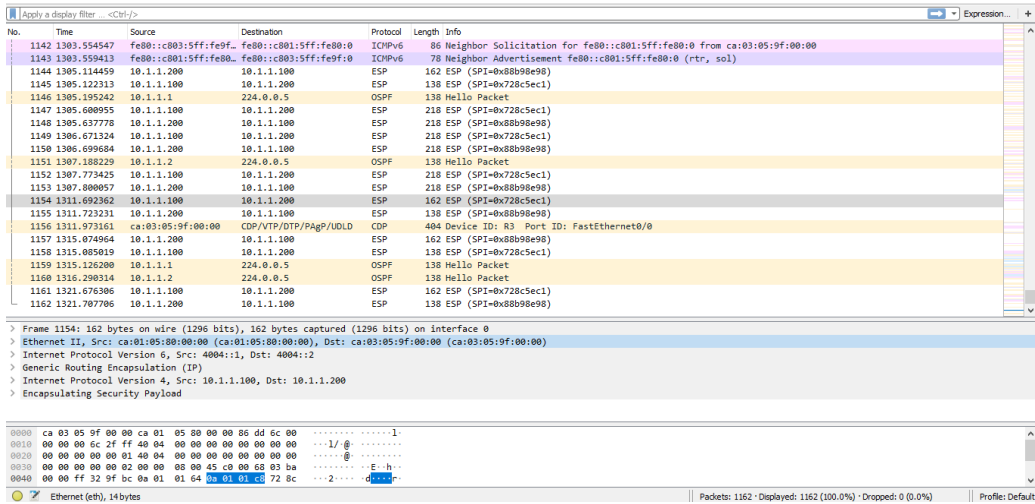


Figure 7.4: Packet analyzing

CHAPTER 8

CONCLUSION

This paper aims to connect to remote offices using IPv4 compatible equipment via IPv6 internet. In order to combine the VPN tunneling technology and IPv6 we simulated GRE over IPSec in a VPN tunnel using GNS3. This is prominent solution to the fact that most of the network equipment are still IPv4 compatible while the world is rapidly moving towards the deployment of IPv6 worldwide. The ping test shows the successful implementation. Response time and delays are also extracted from the ping report. Throughput and packet analysis is done by solar winds and wire shark respectively.

8.1 Future Work

In Future, we will attempt to implement this simulation, physically between the city and permanent campus of Daffodil International University and optimize the real time results using the same parameters. Then we will compare the theoretical values obtain from this paper and the real time values. This will lead us to find out the deviation from the simulated value to real time implemented values. And this will open further scopes to extend this research.

REFERENCES

1. Singalar, S., & Banakar, R. M. (2018, August). Performance analysis of IPv4 to IPv6 transition mechanisms. In *2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA)* (pp. 1-6). IEEE.
2. Kim, P. S. (2017). Analysis and comparison of tunneling based IPv6 transition mechanisms. *International Journal of Applied Engineering Research*, *12*(6), 894-897.
3. Salman, F. A. (2017). Implementation of IPSec-VPN tunneling using GNS3. *Indonesian Journal of Electrical Engineering and Computer Science*, *7*(3), 855-860.
4. Saraj, T., Yousaf, M., Akbar, S., Qayyum, A., & Tufail, M. (2014). Isp independent architecture (iia) for ipv6 packet traversing and inter-connectivity over hybrid (ipv4/ipv6) internet. *Procedia Computer Science*, *32*, 973-978.
5. Hirorai, R., & Yoshifuji, H. (2006, January). Problems on IPv4-IPv6 network transition. In *International Symposium on Applications and the Internet Workshops (SAINTW'06)* (pp. 5-pp). IEEE.
6. Ahmed, A. S., Hassan, R., & Othman, N. E. (2014, August). Security threats for IPv6 transition strategies: A review. In *2014 4th International Conference on Engineering Technology and Technopreneuship (ICE2T)* (pp. 83-88). IEEE.
7. Narayan, S., Ishrar, S., Kumar, A., Gupta, R., & Khan, Z. (2016, July). Performance analysis of 4to6 and 6to4 transition mechanisms over point to point and IPSec VPN protocols. In *2016 Thirteenth International Conference on Wireless and Optical Communications Networks (WOCN)* (pp. 1-7). IEEE.
8. Ahmed, A., Mustafa, A., & Ibrahim, G. (2015). Performance Evaluation of IPv4 vs. IPv6 and Tunnelling Techniques Using Optimized Network Engineering Tools. *IOSR Journal of Computer Engineering*, *17*(1).
9. Padhiar, S., Verma, P. (2015). A Survey on Performance Evaluation of VPN on various Operating System. *International Journal of Engineering Development and Research (IJEDR)*, *3*(4), 516-519.
10. Haider, A., & Houseini, M. (2016). The Difference Impact on QoS Parameters between the IPSec and L2TP. *International journal of Innovative n Advanced Engineering (IJIRAE)*, *11*(3), 31-42.
11. Bensalah, F., El Kamoun, N., & Bahnasse, A. (2017). Analytical performance and evaluation of the scalability of layer 3 tunneling protocols: case of voice traffic over IP. *IJCNS International Journal of Computer Science and Network Security*, *17*(4), 361-369.
12. Sushma, A., & Sanguankotchakorn, T. (2018, December). Implementation of IPSec VPN with SIP Softphones using GNS3. In *Proceedings of the 2018 VII International Conference on Network, Communication and Computing* (pp. 152-156).

13. Babatunde, O., & Al-Debagy, O. (2014). A comparative review of internet protocol version 4 (ipv4) and internet protocol version 6 (ipv6). *arXiv preprint arXiv:1407.2717*.
14. *Routing and Bridging Guide vA5(1.0), Cisco ACE Application Control Engine - Overview of IPv6 [Cisco ACE Application Control Engine Module]*. (2018, February 18). Cisco.
https://www.cisco.com/c/en/us/td/docs/interfaces_modules/services_modules/ace/vA5_1_0/configuration/rtg_brdg/guide/rtbrgdgd/ipv6.html
15. *IPv6 History and related RFCs*. (n.d.). <https://www.omnisecc.com>. Retrieved August 28, 2020, from <https://www.omnisecc.com/tcpip/ipv6/ipv6-history-and-related-rfcs.php>
16. Huston, G. (2018, May 21). *Skip to the article What drives IPv6 deployment?* <https://www.apnic.net/>. https://blog.apnic.net/2018/05/21/what-drives-ipv6-deployment/?fbclid=IwAR1FhKsi9_zsn9iI6ne8Plc3Dh2E3jXVvKlLmgS4tBTjmqgpSXEC6NZQN9U
17. Aravind, S., & Padmavathi, G. (2015, May). Migration to Ipv6 from IPV4 by dual stack and tunneling techniques. In *2015 International Conference on Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM)* (pp. 107-111). IEEE.
18. Wu, P., Cui, Y., Wu, J., Liu, J., & Metz, C. (2012). Transition from IPv4 to IPv6: A state-of-the-art survey. *IEEE Communications Surveys & Tutorials*, 15(3), 1407-1424.
19. Raicu, I., & Zeadally, S. (2003, February). Evaluating IPv4 to IPv6 transition mechanisms. In *10th International Conference on Telecommunications, 2003. ICT 2003*. (Vol. 2, pp. 1091-1098). IEEE.
20. Bly, J., & O'Brien, G. (2013, May 14). *How ISATAP Works And How It Can Help You Migrate To IPv6*. <https://teamarin.net/>. <https://teamarin.net/2013/05/14/how-isatap-works-and-how-it-can-help-you-migrate-to-ipv6-2/>
21. Sansa-Otim, J. S., & Mile, A. (2012, November). IPv4 to IPv6 Transition Strategies for Enterprise Networks in Developing Countries. In *International Conference on e-Infrastructure and e-Services for Developing Countries* (pp. 94-104). Springer, Berlin, Heidelberg.
22. Tsirtsis, G., Srisuresh, P. (2000). *Network Address Translation - Protocol Translation (NAT-PT)*. RFC 2766. Retrieved from <https://tools.ietf.org/html/rfc2766>
23. Bagnulo, M., Matthews, P., Beijnum, I.van. (2011). *Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers*. RFC 6146. Retrieved from <https://tools.ietf.org/html/rfc6146>
24. Bagnulo, M., Sullivan, A., Matthews, P., Beijnum I.van. (2011). *DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers*. RFC 6147. Retrieved from <https://tools.ietf.org/html/rfc6147>

25. Tsuchiya, K., Higuchi, H., Atarashi, Y. (2000). *Dual Stack Hosts using the "Bump-In-the-Stack" Technique (BIS)*. RFC 2767. Retrieved From <https://tools.ietf.org/html/rfc2767>
26. Lee, S., Shin, M-K., Kim, Y-Z., Nordmark, E., Durand, A. *Dual Stack Hosts Using "Bump-in-the-API" (BIA)*. (2002). RFC 3338. Retrieved from <https://tools.ietf.org/html/rfc3338>
27. Tjahjono, D., Shaikh, R., & Ren, W. (2014). U.S. Patent No. 8,893,262. Washington, DC: U.S. Patent and Trademark Office.
28. Yildirim, T., & Radcliffe, P. J. (2010, August). VoIP traffic classification in IPSec tunnels. In 2010 International Conference on Electronics and Information Engineering (Vol. 1, pp. V1-151). IEEE.