Analysis of Generic Routing Encapsulation (GRE) over IP Security (IPSec) VPN Tunneling in IPv6 Network

Md. Raihan Uddin[1(✉)], Nawshad Ahmad Evan[1], Md Raiyan Alam[2], and Md. Taslim Arefin[1]

[1] Daffodil International University, Dhaka, Bangladesh
arefin@diu.edu.bd
[2] Texas A&M University - Kingsville, Kingsville, Texas, USA
md_raiyan.alam@student.tamuk.edu

Abstract. The virtual private network has become an essential technique used for providing a secure remote connection to exchange information over the Internet Protocol network. As the Internet Protocol version 4 and version 6 have different features and structures, the existing virtual private networks are modified to run in the new environment. This paper 'Simulation of Generic Routing Encapsulation (GRE) over IPsec VPN Tunneling on IPv6 Network' is simulated by using a GNS3 network simulator. Here, the solution provided for GRE over IPSec VPN between two remote offices equipped with IPv4 network where the WAN is connected with IPv6 network. In general, IPv6 does not support any kinds of IPSec VPN but the need for this VPN is high for encrypted data. So, this paper will demonstrate an examined method of using the GRE over IPSec VPN through the IPv6 network.

Keywords: GRE · IPv6 · IPSec VPN tunneling · IPv4

1 Introduction

IPV6 is ready to use for 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 not backward compatible. It lacks backward compatibility with the existing internet protocol, which is IPv4. The IPv6 network deployment is not done more in the network world. We need new transition tools until all network devices are compatible with the coexistence of IPv4 and IPv6.

A virtual private network is a technology for creating reachability between different private networks by establishing an end to end connectivity. And there are various tunneling protocols like Point to point tunneling protocol, Internet

N. Kumar et al. (Eds.): UBICNET 2021, LNICST 383, pp. 3–15, 2021.
https://doi.org/10.1007/978-3-030-79276-3_1

protocol security, Layer 2 tunneling protocol, Generic routing encapsulation, Secure socket layer to provide security for VPN tunnel. These protocols are working fine on the current IPV4 networks. But as mentioned earlier, the network world is moving forward rapidly from IPv4 to IPv6, where IPV6 promises better security and more advanced tunneling techniques have to be developed [2]. IPsec (Internet Protocol Security) is a protocol that provides a virtual private network service between sites. IPsec had designed to support a secure TCP/IP connectivity over the IP network by maintaining flexibility and scalability. IPsec is generally used for the service of cryptographic security. Due to maintaining data security through the VPN, the demand for IPsec is increasing [3]. IPsec proves the importance with various security features aiming at a secured data transmission between end devices. IPsec provides confidentiality of VPN traffic by encrypting it. It has also an encapsulation method that is known as Hashing algorithms. IPsec provides authentication services by using Digital certificates or Pre-shared keys. It protects against Reply attacks using a sequence number that built in the IPsec packets. By using these sequence numbers, IPsec can identify the packets which it already sent. IPsec can provide network security by encapsulating and encrypting traffic that passes through VPN from source to destination [4].

The backward compatibility issues of IPv6, this paper will analyze two of the existing VPN tunneling protocols, IPsec and GRE. The aim of this task to develop a standard and secure tunneling technique. That envisioned is a scenario where the remote end devices compatible with the existing Internet Protocol. Which can be connected with the internet and that incorporates IPV6 using GNS3 simulator. The following section on related works where we will discuss about the related publications and similar works on this topic.

As far as we know, no one has published any work about the implementation in Ipv6 network. Therefore, the research in this paper is kind of an innovative work.

2 Related Works

The transition from IPv4 to IPv6 is an active area of research. In [5] 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 [6]. 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 was compared in different environments [7]. They have compared IPv4 or IPv6 with multiple transition mechanisms in terms of various parameters containing UDP and TCP traffic throughput, delay of the packets, jitter in the system, DNS, and VoIP with and without VPN.

The task in [8] proposes a new ISP Independent Architecture (IIA) for interconnectivity in a hybrid network running with IPv4 and IPv6 networks. More flexibility issues of the users to deploy their required transition solutions are provided for their promised ISP. 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 [9] and [10] 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 security in the path or peering, bad TCP connection, error in DNS resolution are taken into consideration in [9] causing issues like delay and disconnection. In contrast, the following section of our proposed system will represent the GRE over IPSec-VPN Tunneling over IPv6 using GNS3 where the mentioned paper has been shown the simulation of GRE over IPSec in IPv6.

3 Methodology

GRE over IPSec tunneling is a most used concept where this paper proposed in Fig. 1; a new method for the most advanced IPSec tunneling on the IPv6 network system. The way the procedure is elaborately explained below.

1. We will take two routers as source and destination and both will be CISCO routers.
2. Both source and destination will be connected via cloud or service provider and both routers loopback is reachable via the cloud.
3. GRE (Generic Routing Encapsulation) tunnel is based on the IPv6 loopback of the routers but we will use the IPv4 tunnel address as the peering address of the tunnel.
4. Then we will do IPv4 routing over IPv6 using the GRE tunnel and created another IPv4 loopback for both routers. Also the reachable IPv4 loopbacks by routing through the tunnel.
5. After that, we will configure GRE over IPSEC using that IPv4 loopback of our source and destination router.
6. We will set up our workstations (PC/Server) that will be configured by IPv4 address and check by ping and found that we can reach our destination successfully.
7. We will measure in Solar Winds that for ICMP traffic we are getting a bandwidth graph.
8. By Wire Shark we will check the packets are sending from source to destination are encrypted by ESP protocol. After finishing all measurements, we will be able to find our LANs are communicating and the IPv4 data get encrypted by GRE over IPSec which were passed through the service providers IPv6 network.

IPv4 and IPv6 are playing a big rule in the transition to create a platform where both ipv4 and IPv6 can co-exist. 3 basic transition mechanisms are mentioned below.

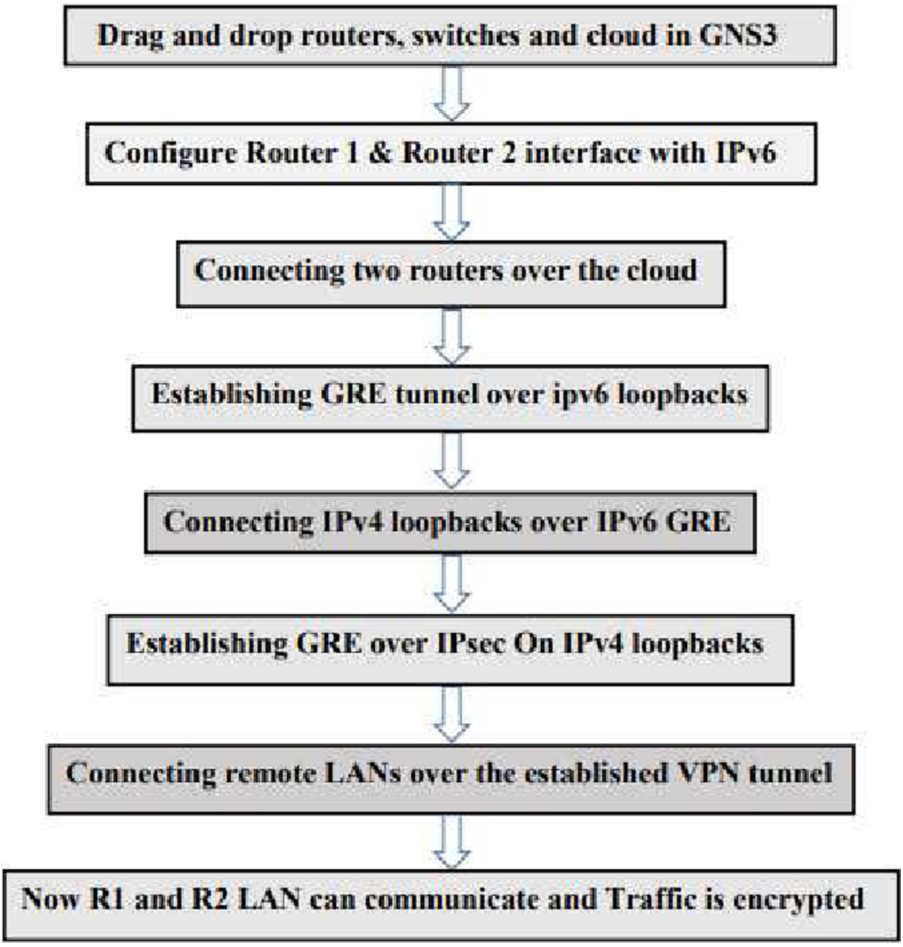

Fig. 1. Proposed working block diagram.

1. Dual Stack
2. Tunneling
3. Translation Techniques

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 [11]. This mechanism is put into 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. In Fig. 2, The Domain Name Server plays an important role to translate from Internet Protocol addresses to the domain name. For the dual-stack scenario, the IPv4 traffic communicates with the version 4 DNS server, and IPv6 communicates with the version 6 DNS server. To operate this mechanism, the

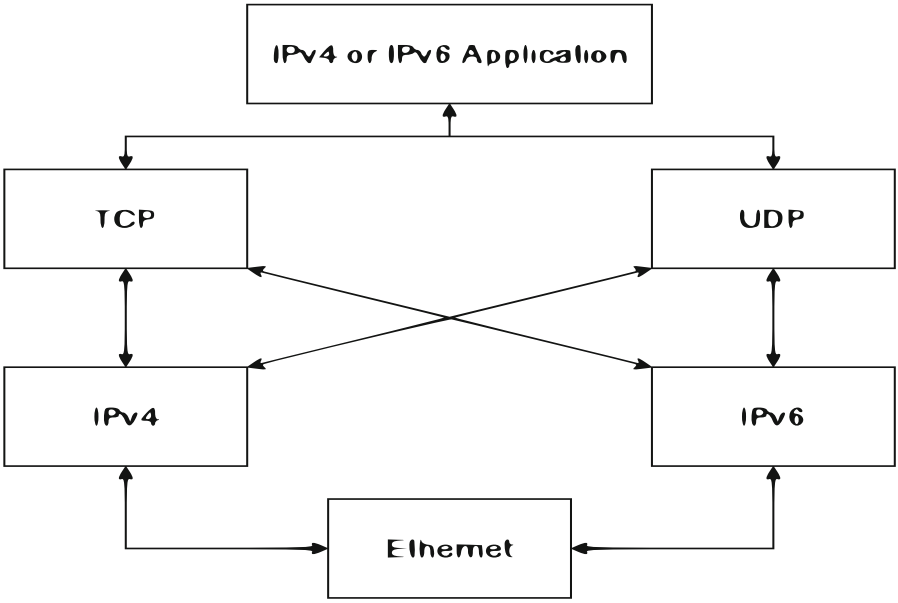

Fig. 2. Dual stack mechanism.

routers must be enabled in both IPv4 and IPv6 routing [12].
All recent IoT devices and operating systems, are now supported by both IPv4 and IPv6.

2. ***Tunneling.*** Tunneling is a technique to create a point to point network connectivity from one network to another remote network for transferring data. For conveying IPvN packets through the IPvM network we configured a tunnel by measuring IPvN (Host1) as source and IPvN (Host2) as the destination. In Fig. 3, When the packets from IPvN travels via the 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

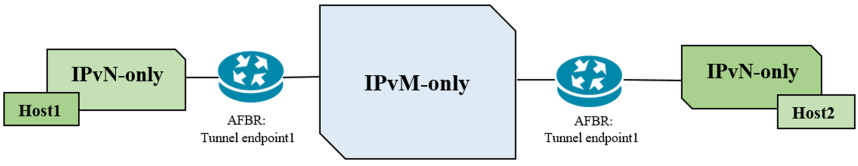

Fig. 3. Tunneling mechanism.

over IPv4 [12]. Five popular tunneling techniques are - Manual Tunnels, 6to4 tunnels, 6RD, GRE, and ISATAP [5].

- **6in4 Tunnel or Manual Tunnel** – The 6in4 tunneling mechanism provides a tunneling technique that will be configured manually [13]. Like other tunneling techniques, it will also be encapsulated but the tunnel needs to be configured manually for each connection. Scalability is absent here. This is suitable for individual connectivity for home or SME but in an enterprise network, it will be tough to maintain a lot of tunnel for different sources and destinations.
- **6to4 Tunnel** – 6to4 tunneling protocol provides scalability for IPv6 tunneling through IPv4 network [14] Like 6in4 this tunnel does not require manual configuration of the tunnel for each source. Only if the destination is different the tunnel will be different here. The encapsulation process will be the same as others that the IPv6 traffic will forward including the IPv4 header.
- **6rd or 6RD** – The 6rd is very efficient for the production network. When the customer end has a DSL connection with IPv4 the 6rd provides a translation process from IPv4 to IPv6. Here the service provider router needs to be capable of 6rd process and the customer router needs to be capable of IPv6 configuration. By this mechanism, the IPv4 addresses will convert into the hexadecimal format and set up a new IPv6 address. Then it travels via a tunnel which is configured in the service providers' router [15].
- **ISATAP** – ISATAP or Intra Site Automatic Tunneling Address Protocol. It forwards IPv6 packets over the IPv4 network using dual stack technology. ISATAP circuit set up a header for the IPv6 packet and passes the traffic via circuit or end to end tunnel [16].
- **GRE Tunnel** – The GRE Tunnel maintains its ideal technique to process tunneling mechanism and transfer traffic over the tunnel. GRE provides a point to point tunnel which includes 4 bytes GRE header before the original IP packet and by encapsulating the packet transfer to its destination. This is one of the most used VPN for routing IPv4 over IPv6 network and vice versa [17].

3. ***Translation Techniques.*** Direct communication between IPv4 and IPv6 is achieved by the IPv4-IPv6 translation technique. In Fig. 4, The basic principle of translation is shown in the figure below. The idea is to convert the semantics between Here er can measure IPvM as IPv4 and IPvN as IPv6. Generally, translation happens when an IPv4 device wants to communicate with an IPv6 destination. For IPv6 translation, the IPv4 is converted to a hexadecimal state and set up in IPv6 format maintaining the 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 the 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 the translation by exchanging information with each other. For this one translator server will

be added before IPv6 and IPv4 DNS server [18].

Some of the very popular translation technique are discussed below:

- **NAT-PT** IPv4 and IPv6 bidirectional communication happened via translation and NAT-PT translator has the exact feature for this. This also works in protocol level and translates Internet Protocol, Domain Name Server, and Internet Control Message Protocol [19].
- **NAT64 and DNS64** Network Address Translation 64 DNS64 [20] is a popular translation technique for IPv4 and IPv6. It enables IPv6 hosts to communicate with IPv4 servers or workstations and IPv4 to IPv6. The received IPv4 packets are converted by the NAT64 translator by converting IPv4 hexadecimal bits in IPv6 Hextet for developing a new IPv6 address to communicate with IPv6 servers. IPv6 DNS also has a NAT64 DNS server that allows communication with both IPv4 DNS and IPv6 DNS.
- **464 XLAT** For both stateful and stateless translation 464XLET is used in the enterprise network. For translating IPv4 to IPv6 this technique has the advance feature and scalability more than NAT64 and DNS64 due to its fast deployment. The major thing is that to run this no new protocol is needed in the enterprise network [21].

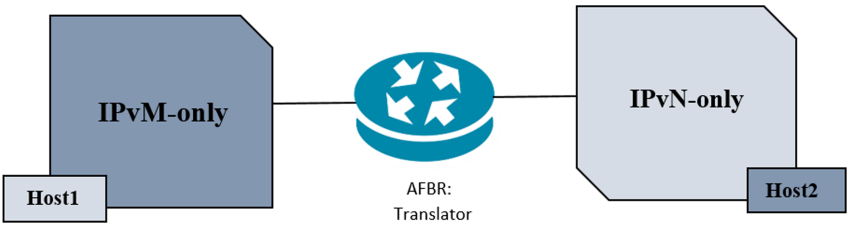

Fig. 4. Translator mechanism.

4 Implementation

This paper has considered a scenario where two remote branches, one located at Dhanmondi and another located at Ashulia having network equipment compatible with IPv4, are connected via the internet of the IPv6 network shown in Fig. 5. The network simulation is done using the GNS3 version: 2.2.5 consisting of routers with the Cisco 7200 VXR series and switches with Catalyst 2600 series. Now at the 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.

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 a GRE tunnel over IPv6 loopbacks of 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 communicating and transferring data. The data is getting encrypted by IPSec parameters and for GRE parameter we can set any static route over the tunnel. The IPv6 has a drawback that it does not support the IPSec tunnel for that reason we make a hybrid solution for that. We did IPv4 communication over the IPv6 service provider network and used GRE over IPSec VPN to encrypt our data and easy routing process for communication of IPv4 workstations at the source and destination premises. All measurement parameters and their results are given here.

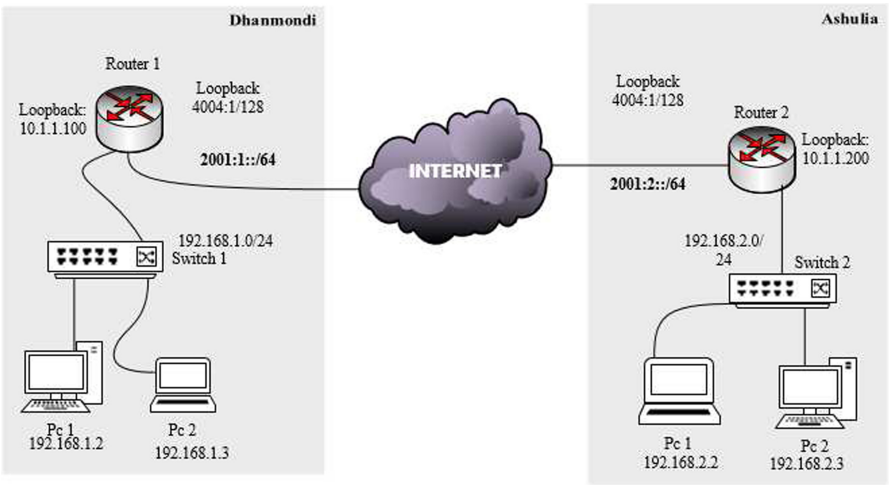

Fig. 5. Implemented network topology.

4.1 Graphical Networking 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 collected and run the different operating systems in a virtual environment and can get the test of real infrastructure. This program allows different systems and devices to communicate with each other and a user can create topology according to his planning. Cisco devices can be deployed as Dynamaps in GNS and by using command lines we can operate it. Dynamics 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.

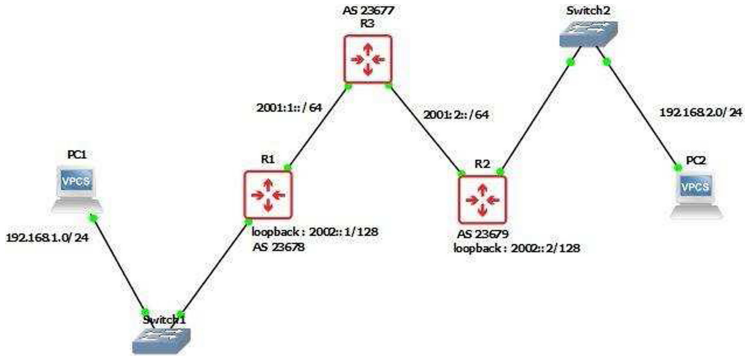

Fig. 6. Network topology in GNS3 simulator.

4.1.1 WireShark

Wireshark is an important tool that is used for analyzing packets. By using Wireshark, we can capture the network packets and analyze the detailed 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.

4.1.2 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 command. 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.

4.1.3 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 analyze in real time.

4.2 Design and Analysis in GNS3

In Fig. 6, We designed a model in the 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 the virtual environment. The diagram is displayed here.

5 Results and Analysis

5.1 Response Time

Response time is the travel time of packets from one source to destination in a computer network. In Fig. 7 We will calculate the response time from the Packet Internet Gopher (PING) report. The lowest response time is 35.795 ms and the highest is 47.795 ms. So, the average for five response time is 40.372 ms. 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 in Table 1.

5.2 Throughput

The highest production or extreme production rate is measured as throughput at which we can produce something. In Ethernet technology or computer networks, we can measure throughput with different parameters. Successful transmission of any packet depends on both physical and logical connectivity. In Fig. 8, Generally, we calculate the data transfer via an interface in bps, Kbps, Mbps, and Gbps. Here we found a throughput in Kbps after transferring ICMP traffic from source for router-1 (source router) out interface.

```
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>
```

Fig. 7. Ping report.

Table 1. Responses of the packet sequences

Packet type	Sq.	Source (host)	Dest. (host)	Response time (ms)	Avg. response time (ms)
ICMP	1	192.168.1.2	192.168.2.2	36.789	40.372
	2			38.298	
	3			35.795	
	4			43.254	
	5			47.725	

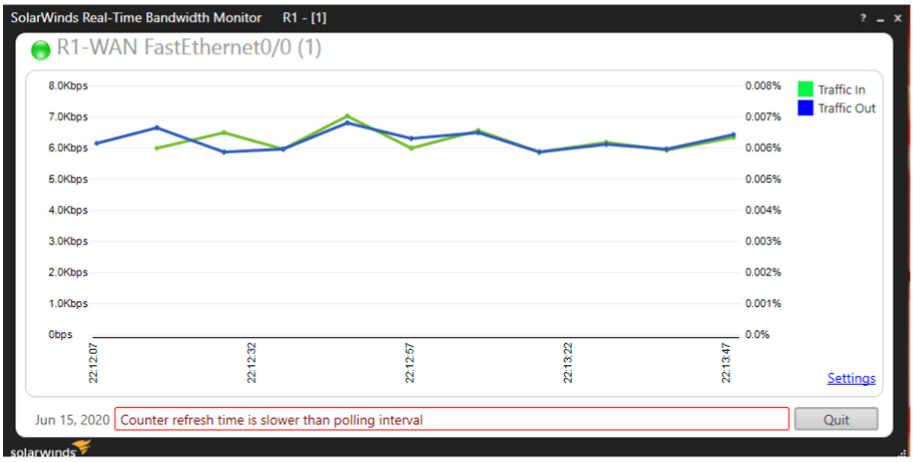

Fig. 8. Throughput analysis.

5.3 Packet Analysing

We can analyze our network traffic by Wireshark and can analyze packets that we are sending. As we are using IPSec, the ESP protocol will encrypt our traffic and it will be completely unable to analyze data from encrypted packets showed in Fig. 9. Hereafter, the crypto session established we analyze the encrypted packets via Wire Shark.

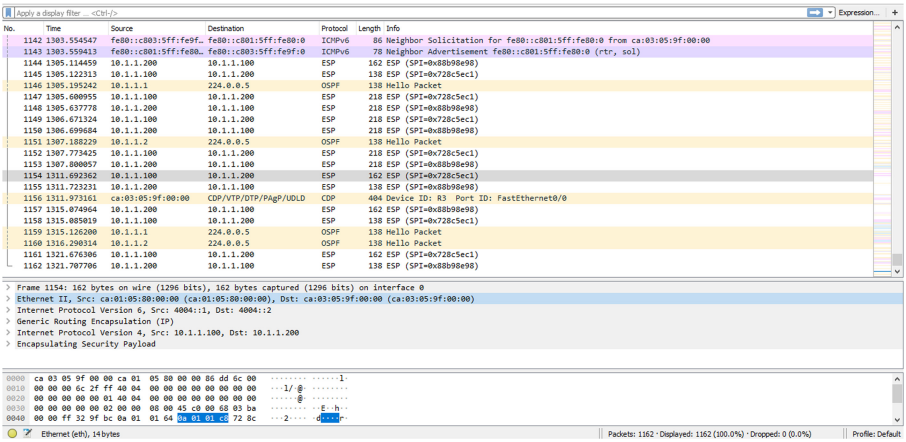

Fig. 9. Packet analyzing.

6 Conclusions

This paper aims to connect to remote offices that were using IPv4 compatible equipment and their WAN network is an IPv6 network. To combine the IPSec VPN tunneling technology and IPv6 we simulated GRE over IPSec as a VPN tunnel using GNS3. This is a prominent solution to the fact that most of the network equipment is still IPv4 compatible while the world is rapidly moving towards the deployment of IPv6 worldwide. The translation between IPv4 and IPv6 is very important as we can not ignore the IPv4 when we had to move forward with IPv6. Again IPv6 does not support the most popular VPN for encryption. This paper demonstrates a clear solution for encrypted data transfer of IPv4 over a new generation Internet Protocol.

References

1. Ahmad, N.M., Yaacob, A.H.: IPSec over heterogeneous IPv4 and IPv6 networks: issues and implementation. Int. J. Comput. Netw. Commun. **4**(5), 57 (2012)
2. Venkateswaran, R.: Virtual private networks. IEEE Potentials **20**(1), 11–15 (2001)
3. Tjahjono, D., Shaikh, R., Ren, W.: U.S. Patent and Trademark Office. U.S. Patent No. 8,893,262. Washington, DC (2014)
4. Yildirim, T., Radcliffe, P.J.: VoIP traffic classification in IPSec tunnels. In: 2010 International Conference on Electronics and Information Engineering, vol. 1, pp. V1–151. IEEE, August 2010
5. Singalar, S., Banakar, R.M.: Performance analysis of IPv4 to IPv6 transition mechanisms. In: 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), pp. 1–6. IEEE, August 2018
6. Kim, P.S.: Analysis and comparison of tunneling based IPv6 transition mechanisms. Int. J. Appl. Eng. Res. **12**(6), 894–897 (2017)

7. Narayan, S., Ishrar, S., Kumar, A., Gupta, R., Khan, Z.: 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, July 2016
8. Saraj, T., Yousaf, M., Akbar, S., Qayyum, A., Tufail, M.: ISP independent architecture (IIA) for IPv6 packet traversing and inter-connectivity over hybrid (IPv4/IPv6) internet. Procedia Comput. Sci. **32**, 973–978 (2014)
9. Hirorai, R., Yoshifuji, H.: Problems on IPv4-IPv6 network transition. In: International Symposium on Applications and the Internet Workshops (SAINTW 2006), pp. 5-pp. IEEE, January 2006
10. Ahmed, A.S., Hassan, R., Othman, N.E.: Security threats for IPv6 transition strategies: a review. In: 2014 4th International Conference on Engineering Technology and Technopreneuship (ICE2T), pp. 83–88. IEEE, August 2014
11. Haider, A., Houseini, M.: The difference impact on QoS parameters between the IPSec and L2TP. Int. J. Innovative Adv. Eng. (IJIRAE) **11**(3), 31–42 (2016)
12. Wu, P., Cui, Y., Wu, J., Liu, J., Metz, C.: Transition from IPv4 to IPv6: a state-of-the-art survey. IEEE Commun. Surv. Tutorials **15**(3), 1407–1424 (2012)
13. Babatunde, O., Al-Debagy, O.: A comparative review of internet protocol version 4 (IPv4) and internet protocol version 6 (IPv6). arXiv preprint arXiv:1407.2717 (2014)
14. Huijun, D.U.: Application of 6to4 tunnel technique based on dual stack. J. Guangdong Polytechnic Normal Univ. **12** (2007)
15. Yoon, S.J., Park, J.T., Choi, D.I., Kahng, H.K.: Performance comparison of 6to4, 6RD, and ISATAP tunnelling methods on real test beds. Int. J. Internet Distrib. Comput. Syst. **2**(2) (2012)
16. Guo, L.L., Guo, Y.M., Wang, Y., Dong, N.: Implementation of IPv6 network based on combination of 6to4 and ISATAP tunnel techniques. Radio Commun. Technol. **3** (2006)
17. Sansa-Otim, J.S., Mile, A.: IPv4 to IPv6 transition strategies for enterprise networks in developing countries. In: Jonas, K., Rai, I.A., Tchuente, M. (eds.) AFRICOMM 2012. LNICST, vol. 119, pp. 94–104. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-41178-6_10
18. Gilligan, R.E., Nordmark, E.: Basic transition mechanisms for IPv6 hosts and routers. In: IETF RFC (2005)
19. Aravind, S., Padmavathi, G.: 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, May 2015
20. Raicu, I., Zeadally, S.: Evaluating IPv4 to IPv6 transition mechanisms. In: 10th International Conference on Telecommunications, ICT 2003, vol. 2, pp. 1091–1098. IEEE, February 2003
21. Al-Azzawi, A., Lencse, G.: Towards the identification of the possible security issues of the 464XLAT IPv6 transition technology. In: 2020 43rd International Conference on Telecommunications and Signal Processing (TSP), pp. 439–444. IEEE, July 2020