International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-5, March 2020

Implementation and Analysis of IP Tunnel in Virtual Private Networks

Kavita Rani, Avinash Jethi

Abstract*: In Virtual Private Network tunneling is designed to examine the performance of Private network for transferring the data. It implements and analysis the IP tunnel in Virtual Private Network (VPN). Tunneling is a method that is used to transfer the data or packet of one protocol using different network communication mediums of another protocol. This research is emphasized to examine the performance of Private network using tunneling for the transfer of data. Basically tunneling is used to send a packet, data or traffic of one protocol using an intermediate structure of another protocol. It is called as the process of encapsulation, transmission, over different types of secured networks as encapsulation and security is one of the procedure within this network provides security .This paper gives overview of a Virtual Private Network with IP Tunnel. Virtual private Network generates a secure encryption and decryption of data with the help of IP tunneling at end points. Basically VPN routes through the internet from a private network to transferring the data from one end (source) to other end (destination). With the help of tunneling and VPN user can check the working of different parameters under various applications.

Index Terms: IPV4, IPV6, VPN, IP Tunneling.

I. INTRODUCTION

There are two main functions of tunneling, it encapsulates the data packet to reach its other end point and decapsulation the packet when it delivers to its destination point. With the help of tunneling VPN creates a secure connection with the help of IP tunnel, which is called VPN tunnel. With this whole the traffic on internet passes through the VPN tunnel. With the use of IP tunnel in Virtual Private Network connection becomes more secure and powerful for sending any personal data over a network. Tunneling is a term which provides security and integrity at both ends (source and destination) using virtual private network.

II.IPV4

IPV4 (Internet Protocol Version 4) is 32 bit long address. The Internet Protocol divides the data stream into datagram's and these are routed independent of each other. The format used by the IP datagram's that carries the data messages in the network is called IP Packet Format. An IP datagram consists of a header part and a text part. There are two parts of header, first is variable length part and other is complete IP packet format.

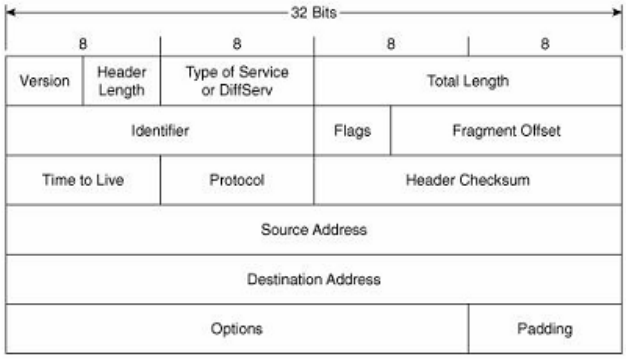

Fig. 1. IPV4 header format

III. IPV6

IPV6 address is having 128 bit long. IPV6 gives more address space than 32 bit long address space used by IPV4. To resolve the large traffic problems, it uses flow label field in place of Type of Services fields of IPV4. Benefit of this field is that the user can request for the type of service system provides during data sending and receiving request. The IPV6 is used to perform different functions to encrypt and decrypt the data. This provides extra security to data, packet and frame. In IPV6, Internet Protocol was developed to provide other features of security to the growth of the Internet.

This technique is used to increase the speed of the routing configuration process because routers do not check many options. IPV6 is basically provides extension to the protocol. The Encryption and security points in IPV6 provide privacy from unauthorized users and security of the packet.

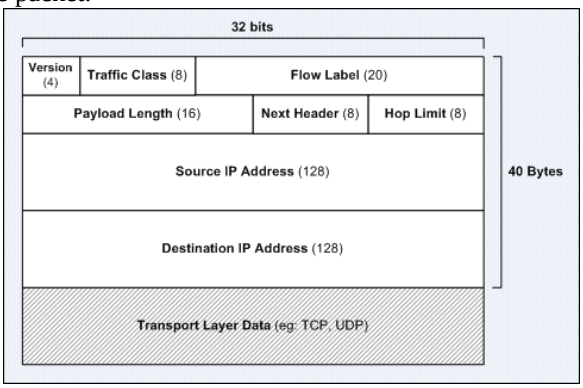

Fig. 2.IPV6 header format

IV. RELATED WORKS

In [1] they evaluated and tested the working of Manual Tunneling and MIPv6 to MIPv4 Tunneling types by defining and evaluated many performance parameters (End to End delay,

Revised Manuscript Received on March 30, 2020.

* Correspondence Author
Kavita Rani, Studying her Masters in the field of Computer Science and Engineering from BGIET, Sangrur.
Avinash Jethi, Assistant Professor in BGIET, Sangrur (Punjab).

Throughput and Response Time) of various internet applications of protocol like FTP, HTTP, Database and Email. MIPv6 is an extension of IPv6, which is not compatible with IPv4. As per the results author has evaluated that the manual tunneling is better than 6 to 4 tunneling in two applications like HTTP and Email, in all performance parameters then in Database application, in case of FTP two parameters were having the equal and same performance. According to the authors, Manual Tunneling is not used for large networks. In this paper they compared MIPV6 over IPV4. MIPV6 and IPV6 are having same working is, therefore it is not compatible with IPV4.

In [2] they had prepared and showed the results simulation for the following three performance parameters, these are jitter, latency and throughput of IP (Internet Protocol) and MPLS (Multiprotocol Label Switching Protocol) under given conditions (first using data and second using voice). Voice Over Internet Protocol is a type of technology which provides reliable communication tool for the transmission of data and voice. It uses IP (Internet Protocol) to send the voice over packets through the IP network. Author concluded in this paper that MPLS having better performance in both the conditions (data and voice).

In [6] the performance of three learning techniques SVM (Support Vector Machine), NB (Native Byes) and J48 (also called Decision Tree) were evaluated. These Three learning techniques are used for detecting the DNS (Domain Name System) tunneling. Therefore SVM has the best classifier by achieving the highest measure performance. SVM is one of the classified methods that perform the working based upon dividing the data space using multiple class labels. DNS a type of cyber attack is the most important issue that has raised in the era of information Technology. DNS (Domain Name System) has a important role related to Web activities such as browsing and emailing. Author evaluated that the SVM (Support Vector Machine) has the better performance as compare to NB (Native Bayes) and J48.

V. IP TUNNELING

A tunnel (a path, which is used to send the data, packet and frame from source to destination) is created and the data, packets and frames are routed between the tunnel end points through the communication medium. Tunneling is a type of protocol called communication Protocol that allows for the movement of data from one network to another network. It allows private network communication to be sent across a public network.

There are two types of tunnels called configured and automatic. Configured tunnels are predefined by administrators in advance during communication, whereas automatic tunnel does not require its pre configuration. Tunneling provides a method to use IPV4 routing mechanism to handle IPV6 traffic. In tunneling every packet including address information of its source and destination IP networks.

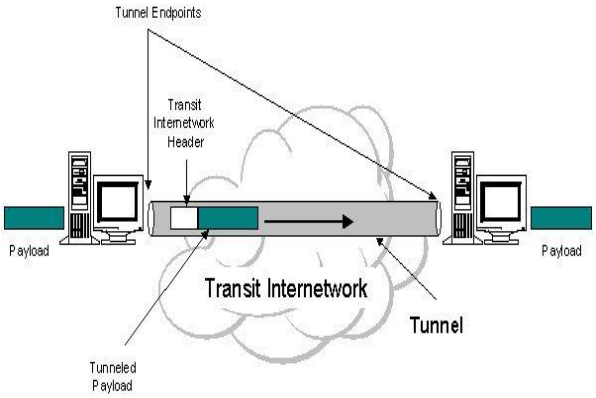

Fig. 3. IP Tunneling

VI. VIRTUAL PRIVATE NETWORK

A Virtual Private Network is a type of network that creates a secure network over a network which is less safe as the internet. It transfers the data and makes a private communication across a public network and allows the users to send and receive the data through unsecure network or public network. A VPN is created by maintaining the virtual one end to other end (from source to destination) connection with the use of dedicated circuits or with the use of tunneling protocols over the pre maintained networks. From the user side, resources which are available can be run or accessed through the remote side .

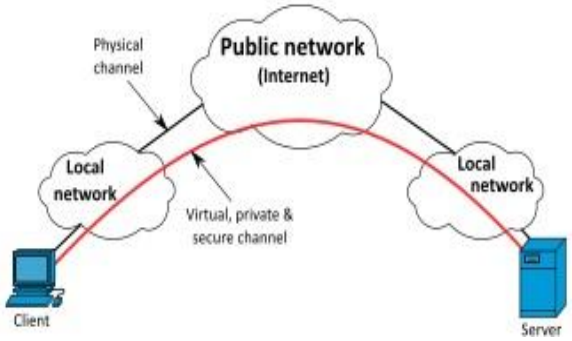

Fig. 4. Virtual Private Network

VII. RESULTS

A Virtual Private Network is in OPNET 14.0 has been developed for analysis of IP Tunneling. The effect of Configured tunnels on performance of developed network for Traffic Sent/ Received, End to End Delay, Queuing Delay, Throughput, Delay Variation with and without tunnel.

A. Flow of work

The Flow of work is shown by the following diagram

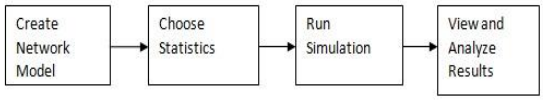

Fig. 5.Flow Diagram of Present Work

To build a network model the workflow centres on the Project Editor.

This is used to create network models, collect statistics directly from each network, execute a simulation and view results.

B.Simulation Results of Network Using IP Tunnelling

Opnet 14.0 Software is used to obtained the simulation results of network using IP Tunneling using different parameters like Traffic sent/received, End to end delay, Queuing Delay, Throughput, Delay Variation in HQ Gateway and Enterprise Gateway.

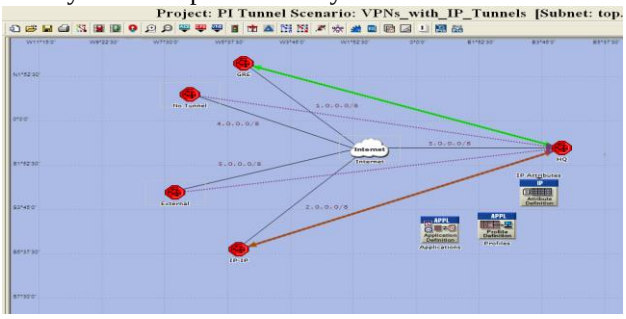

Fig. 6. Scenario developed to implement Network using IP Tunneling.

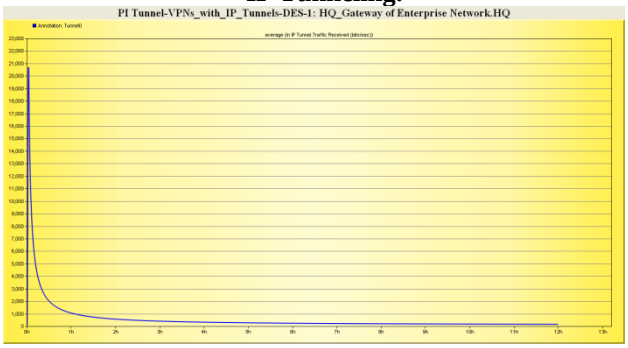

Fig. 7. Show the results obtained for Traffic Received in bits per Second HQ Gateway

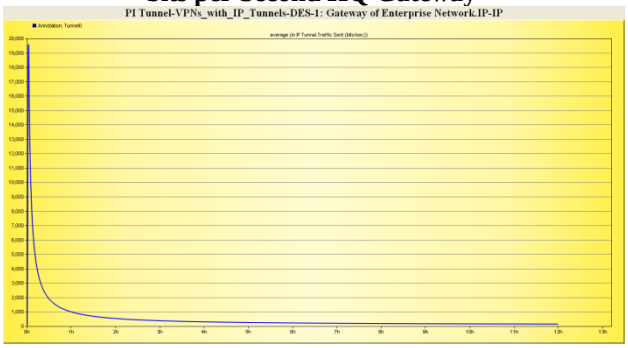

Fig. 8. Show the results obtained for Traffic Sent in bits per Second Enterprise Gateway.

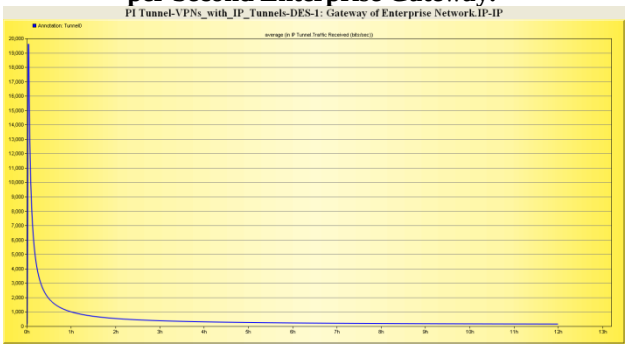

Fig. 9. Show the results obtained for Traffic Received in bits per Second Enterprise Gateway.

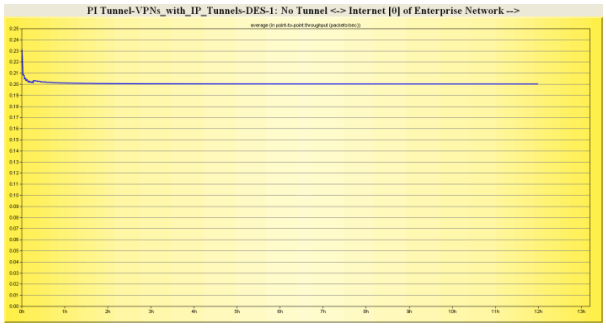

Fig. 10. Show the results obtained for throughput of network in bits per Second without Tunnel.

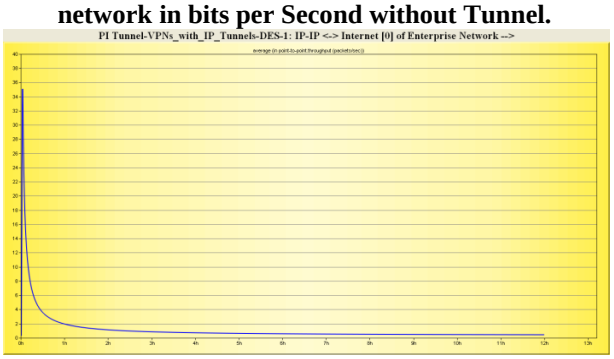

Fig. 11. Show the results obtained for throughput of network in bits per Second with Tunnel.

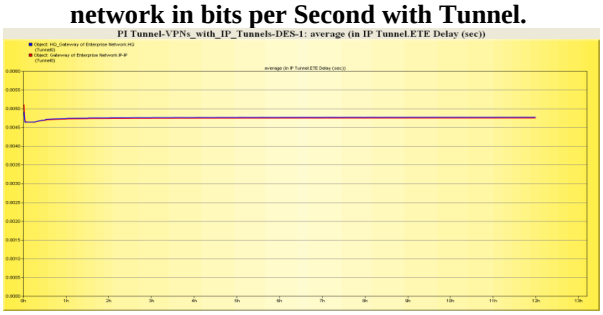

Fig. 12. Show the results obtained for End to end Delay in Second at HQ Gateway and Enterprise Gateway.

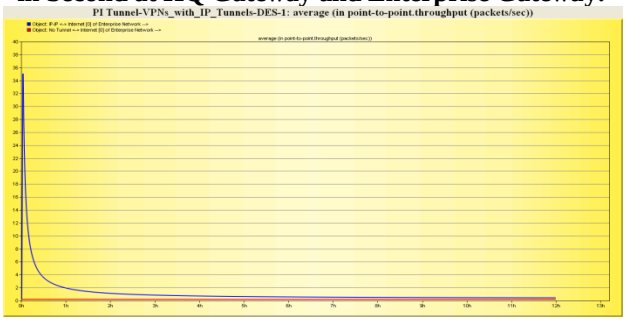

Fig. 13. Show the results obtained for throughput in packets per Second with and without Tunnel.

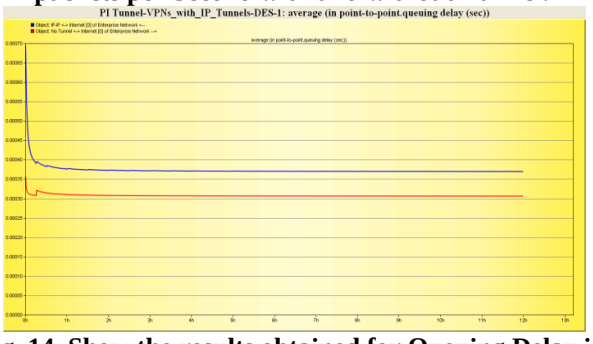

Fig. 14. Show the results obtained for Queuing Delay in network with and without Tunnel.

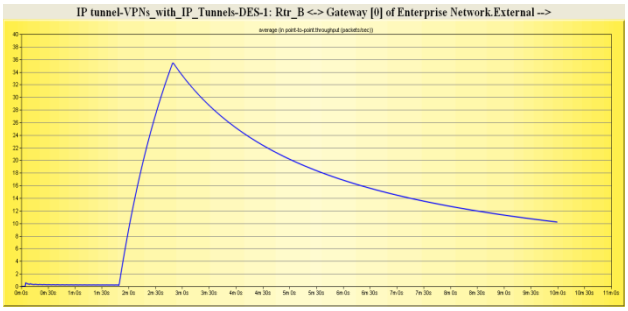

Fig. 15. Show the results obtained for Average throughput in network using Tunnel.

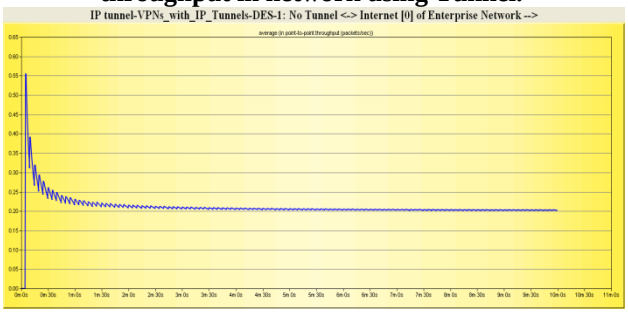

Fig. 16. Show the results obtained for Average throughput in network without Tunnel.

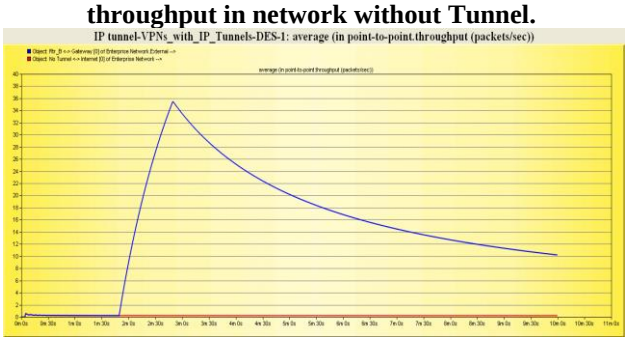

Fig. 17. Show comparison of the results obtained for Average throughput in network.

C. Summary in form of tables

Simulation for the developed scenario is run for ten hours. Results presented in various graphs Table shows the values of different parameters used for analysis of Virtual private network. It shows the value observation in form of different parameters and units.

Table No.1 Show the parameters observed for the Virtual Private Network

PARAMETER	VALUE	UNITS
Traffic Received	20500	bits per second
Traffic Sent	15,000	bits per second
Traffic Sent	19500	bits per second
Throughput	0.2	packets per second
Throughput	25	packets per second
End to End Delay	0.47	seconds

This table describes the different parameters like traffic received, traffic sent, throughput and end to end delay and shows the value with its units.

Table No .2 Show the comparison parameters for the designed network with and without Tunnels

Parameters	With Tunnels	Without Tunnels	Units
Point to Point Queuing delay	0.0007	0.00033	seconds
Point to Point Throughput	0.35	0.22	packets per second

This table describes parameters like point to point queuing delay and point to point throughput results with tunnels and without tunnels and describes the units as well in the form of bits per second. It increases overall throughput as well

VIII. CONCLUSION

In this Paper we have made assessment and analysis the working of IPv4 and IPv6. Major drawback of IPV4 and IPV6 is that they both are not compatible with each other, therefore we will develop a Private Network with IP tunnel. The major concern of this research is to analyze and implement the IP tunnelling in a Virtual Private Network. Tunnelling will be used for transfer the payload of one protocol using a internetwork medium. This research is used to examine the performance of private network using tunnelling for the transfer of data. Tunnelling enables routing the IPv6 packet routing easily over IPv4 map. The IPv6 packet is used to carry the frame or data load over the IPv4 packet.

Hence finally this research brings out a suggestion on reducing the ratio across the local traffic in the IPV6 environment. Everyone has to be educated completely about deploying Ipv6 and it has to be converted slowly by using Dual stack initially and then later, proper tunnelling and transition techniques has to be adopted appropriately to achieve an efficient transition from IPV4 to IPV6. Later the concept of header compression can also be considered while the packet is moving within a LAN and also while using VPN across the LAN.

REFERENCES

1. Ahmed Ali Kwizera, Cemal Kocak, “Performance Evaluation of Tunnelling Mechanism in MIPV6 over IPV4, “July 2017.
2. D.Badrinarayanan, T.Dinesh, **R**.Ganapathy, A.Jagadeeshwaran, “Performance Analysis of VoIP in MPLS core network using Virtual Routing Instances (VRF),”In International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE), ISSN: 0976-1353, Volume 24 Issue 5.
3. Avinash Jethi and Ms. Ambica, “Improved Greedy Routing Protocol for VANET,” International Journal of Advanced Trends in Computer Applications (IJATCA), Volume-2, No.7, December-2015.
4. C.V Ravi Kumar, Kakumanilakhshmi Venkatesh, Marry Vinay Sagar, “Performance Anaylsis of IPV4 to IPV6 Transition methods,” Indian Journal of Science and technology, Volume-9, May-2016.
5. Rameshar T. Murade, Pavan M. Ingale, Rahul U. Kale, Sarfaraz S. Sayyad,” Comparative analysis of IP, ATM and MPLS with their QoS” International Journal of Innovation Technology and Exploring Engineering (IJITEE) ISSN: 2278, Volume-2, Issue-5, April 2013.
6. Mahmoud Sammour, Burairah Hussain, Mohd Fairuz Iskandar Othman, “Comparative Analysis for Detecting DNS Tunnelling Using Machine Learning Techniques” In International Journal of Applied Engineering Research ISSN 0973-4562 Volume 12, 2017.
7. Avinash Jethi, Harpreet Kaur, “Efficient Routing Protocol in Mobile Ad-hoc Networks,” International Journal of Advanced and Management Studies (IJACMS) Computronics Volume-1, Issue-6, November-2016.

8. Srinidhi K.S, Smt.R.Anitha, A.V Shrikanthan, "Tunnel based IPV6 transition with Automatic bandwidth Management,"International Journal of Computer Science and Mobile Computing, IJCSMC, Volume-3, Issue-6, June-2014.
9. Henry Chukwuemeka Paul, "A study on IPV4 and IPV6", International Journal of Information System and Engineering, Volume-4, November-2016.
10. Avinash Jethi, Ms. Seema, "Clustor based Security Architecture in Wireless Adhoc Networks-An Overview," Volume-2, No. 8, August 2011.

AUTHORS PROFILE

Ms. Kavita Rani has completed her Graduation in the field of Information Technology from BBSBEC, Fatehgarh Sahib (Punjab).Currently she is studying her Masters in the field of Computer Science and Engineering from BGIET, Sangrur. Her research interests are Ad-hoc networks, Wireless Adhoc Networks.

Er. Avinash Jethi working as Assistant Professor in BGIET, Sangrur (Punjab) has completed his Mtech (CSE) from Punjabi University, Patiala and now pursuing Phd. His active research includes WSN, Ad-hoc networks and Big Data.