**TELKOMNIKA**, Vol.17, No.3, June 2019, pp.1185~1192
ISSN: 1693-6930, accredited First Grade by Kemenristekdikti, Decree No: 21/E/KPT/2018
**DOI:** 10.12928/TELKOMNIKA.v17i3.12231


# Performance analysis of tunnel broker through open virtual private network

**Rendy Munadi*[1], Danu Dwi Sanjoyo[2], Doan Perdana[3], Fidar Adjie[4]**
[1,2,3]School of Electical Engineering, Telkom University, Terusan Buah Batu, Bandung, Indonesia
[4]BCN Labs, Telkom Corporate, Indonesia, Sukarasa, Sukasari, Bandung, Indonesia
*Corresponding author, e-mail: rendymunadi@telkomuniversity.ac.id[1], danudwj@telkomuniversity.ac.id[2], doanperdana@telkomuniversity.ac.id[3], 720416@telkom.co.id[4]

***Abstract***

*Tunnel Broker uses automatic configuration tunneling mechanism for IPv6 clients connected to IPv4 internet. Connectivity between clients and service providers in IPv6 is urgently needed. Open VPN as a provider implemented configures it by a VPN network, so IPv6 and IPv4 public IP clients can easily connect to the server. In this research focused on the performance of tunnel broker mechanism by utilizing open VPN as access to the network. IPv6 tunnel broker is developed by installing Open VPN and providing IPv6 IPs. Implementation of public IP usage in observing the performance of tunnel broker development is done in BCN Telkom Laboratory Network. The measurement results show that TCP and UDP throughput of IPv6 is slightly higher than IPv4. The research using OpenVPN as a server Tunnel Broker for client access to the server is still rarely done, especially in the field of the network based on Internet Protocol.*

***Keywords***: *IPV6, open VPN, performance, tunnel broker*



## 1. Introduction

Ipv6, as a new standard, needs to be able to be interconnected with Ipv4 that had been commonly used. IPv6 has different header format than Ipv4 [1]. As IPv6 is basically not compatible with IPv4, a mechanism is needed for IPv6 to be interconnected with IPv4. One basic mechanism for connecting IPv4 to IPv6 is by Tunnelling [2]. A tunnelling system is a system that connects IPv4 and IPv6 networks by using a tunnel broker. A tunnel broker IPv6 is a tunnel that is automatically activated by a tunnel broker to an IPv6/IPv4 dual stack host isolated from an IPv6 network, so that IPv6 clients can connect over an existing IPv4 network. The architecture of an IPv6 tunnel broker can be seen in Figure 1.

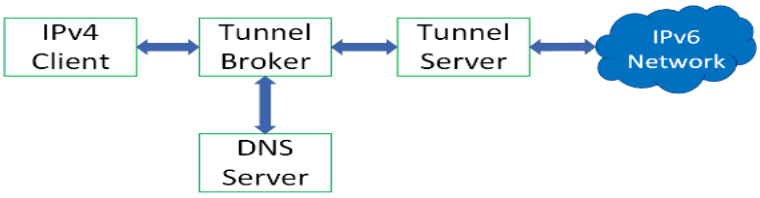


Figure 1. Tunnel broker architecture

From Figure 1, tunnel broker is a client tunnel connection space to conduct registration and tunnel activation by using an IPv4 network. Meanwhile, a tunnel server is a dual stack (IPv6 and IPv4) router that is connected to both IPv4 and IPv6 internet networks. There are several tunnelling mechanisms. The first one is 6over4. 6over4 is a tunnel technique for the IPv6 nodes that are in a collection of IPv4 networks to communicate with each other through the creation of virtual links made with IPv4 multicast [3].

The second technique is 6to4. 6to4 is a tunnel technique that can connect IPv6 domains separated by an IPv4 network. 6to4 is known as an automatic tunnel because the IPv4 network

*Received June 20, 2018; Revised January 31, 2019; Accepted February 25, 2019*

acts as a connector between IPv6 networks. Where IPv4 infrastructure is used to transfer IPv6 packets. Therefore, the IPv4's is a part of the IPv6 address during the packet delivery process [4-6]. The last one is Tunnel Broker. Tunnel broker development required dual stack (Ipv4/IPv6) router, web server, tunnel automatic configuration and DNS server. The use of a tunnel broker is said to be ready if the client is already registered and give authentication and providing configuration information after tunnel already activated [4, 6].

The tunnelling mechanism is done by encapsulating IPv6 packets with an IPv4 header to provide both flexibility and efficiency in IPv6 datagram. After this process that packet is directly sent to an IPv4 network. The encapsulation process is done by the sender router to a client who would de-encapsulate the packet [7–9]. From Figure 2, during the tunnelling mechanism, packet data that were sent by a host will increase in size due to packet encapsulation. When sending large packets, a larger sending time will also be needed. IPv6 Tunnel Broker system is developed by installing Open VPN first, then the Open VPN server will provide Clients IPv6 Ips. Figure 3 shows Open VPN as a provider of IPv6 (IPv6 broker), then the network configuration will use the VPN network configuration [10]. After a client is connected with VPN Sever, then tunneling will occur between the client and the VPN Server. So later known by the server service (eg: web server) when browsing is IP public of VPN Server.

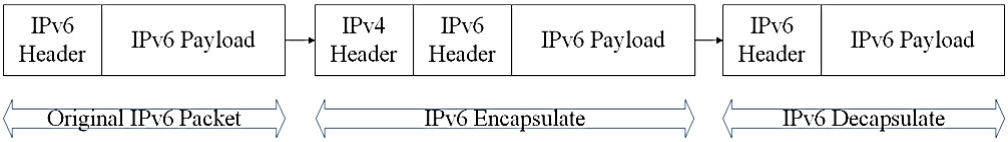


Figure 2. Tunnelling transmission mechanism encapsulation process

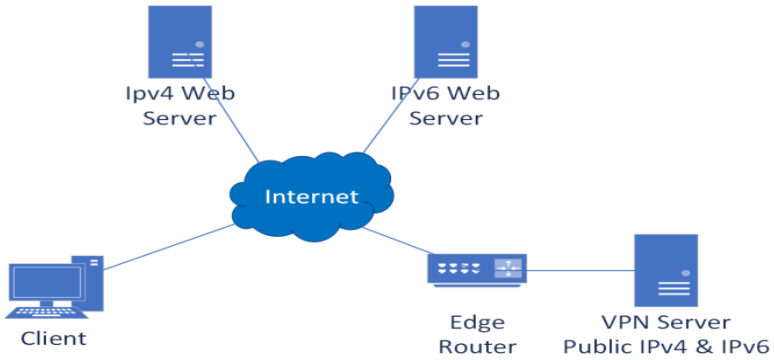


Figure 3. OpenVPN configuration

The opposite, if the client will connect to VPN server, the IPv4 public required for running applications Open VPN. For illustration: as a Tunnel Broker, the VPN server will provide IPv4 (10.8.0.0/24 and IPv6 network/112*). Some of the references and tutorials, says that Open VPN could not allocate smaller segment. If seen from any given IPv4 (/24) then the number of clients that can be served by a VPN server ($2^8$-2) maximum user. Therefore /112 for IPv6 already very enough. In other words, that IPv6 client is used to browse to the service provider IPv6 based. Thus, IPv6 client will not equal the IPv6 servers.

In recent years, the growing number of clients IPv6 very rapidly while generally in existing network still IPv4 network, this is giving problem for IPv6 clients. It's means that IPv6 client cannot communicate with clients who are in the existing IPv4 network. In RFC 7059 is given an overview of various ways to tunnel IPv6 packets over IPv4 networks [11]. In this research to state of the necessary of tunnel systems solutions client to a server that is using the mechanism of a tunnel broker. The system of tunnel brokers utilizing the existence of dual stack router IPv6/IPv4 and open VPN as a server, then two different IP protocol client can easier connect to each other. As the study of implementation in building the tunnel broker system selected BCN Telkom Laboratory in Indonesia with consideration meet the completeness of the

hardware and software in building the system of tunnel brokers.This paper is organized as follows. In section 2, we provide the Literature Survey. In Section 3, we provide the Topology and experiment setup. In section 4, we provide results of measuring and analysis. We evaluate the performance metrics of network topology. Finally, we conclude the paper in section 5.

## 2. Related Works

Ali Albkerat and BijuIssac [4]: In this paper, authors analyzed the IPv6 transition technologies. In their work for performance analysis, authors propose some networks for design and simulation by using Opnet Modeler on different translation schemes. The tunnel broker is defined as an automatic configuration service and it contains different parts and works as a tunnel monitor. From the simulation results, authors conclude that the network's performance depend on configuration schemes. The throughput of simulation results shows that IPv6 has higher throughput than the IPv4, Dual Stack, 6to4 and manual tunnel.

Adarsh Misra et al. [7]: In this paper authors to states that for tunnel configuration does not require direct management, it's called automatic tunnelling. The header of IPv4 address can be inserted to IPv6 packet, so the IPv6 packets can over the IPv4 network. For forwarding packet if IPv6 sites anywhere in IPv4 internet, so the configure of tunnels not always needed. The results from design and test performance states dual stack protocol IPv6 network for all metrics parameter has better performance if compared to other techniques. Nazrulazhar Bahaman et al. [12]: In this paper the authors present about the evaluation of network performance tunnel mechanism. The results show that the performance of tunneling mechanisms on TCP data transmission for IPv6 is lower than IPv4 protocol, but for the transmission of UDP data on tunnel mechanisms the results obtained are almost similar to the use of both protocols. In other words, UDP data transmission with tunnel mechanism does not affect actual network performance. They concluded that during the transition period, tunnel mechanisms are well suited for further investigation and experiments for actual network performance.

Md. Asif Hossain et al. [13]: The study about analysis performance of three mechanisms between IPv4 and IPv6 networks by using packet tracer simulation software. This result show that tunnelling gives the high throughput rate than other transition mechanism and also packets loss very lowest than other. From the above survey literature is generally the tunneling mechanism performance analysis at the limit of simulation by using software that match the configuration made, and other review of IPv4 and IPv6 for Research Test Bed [14]. There is no use of Open VPN as a server supporting the network configuration and has not reached the implementation stage in the public network that there are two different protocols (IPv6/IPv4).

## 3. Topology and Experiment Setup

### 3.1. Network Topology

The topology used during the process of this Open VPN Tunnel Broker research project is showed at Figure 4. The topology is modified from [15, 16]. In our topology, the relay router (Router MX960) is connected to a server that runs as Tunnelbroker and OpenVPN Server. The server used VMWare ESXi v5.0 as a virtualization media and the VM tunnel broker that has been ported to the VMWare was connected to two networks that is in BCN Telkom Risti Laboratory, which were public IPv4 address aaa.bbb.ccc.162/28 and Public Network IPv6 2001:xxxx:yyyy:zzzz::2/64. The setting on the OpenVPN server is set so that the OpenVPN interface generates IPv6 for tunnel broker clients on the 2001:xxxx:yyyy:zzzz:80::0/112 subnet. This IPv6 subnet will be the one accepted by the client and be used to communicate through IPv6.

### 3.2. Experiment Setup

The specification of the server used is as follows:

- Operating System: Ubuntu Server 14.04
- RAM Capacity: 1 GB
- Number of Virtual Processor: 1 Core
- Storage Capacity: 30 GB
- Network Interface: eth1 (for IPv4 and IPv6)

the server had the IP set to Static IP:

IPv4→ aaa.bbb.ccc.162/28 (eth1)
IPv6→2001:xxxx:yyyy:zzzz::2/64 (eth1)
Next, the subnet allocated for OpenVPN client tunnel broker is as follow:
IPv4 → 10.8.0.0/24
IPv6→2001:xxxx:yyyy: zzzz:80::0/112
where the stated IP will be at interface tun0 which will appear on the client's device when OpenVPN Tunnel Broker registration is successful.

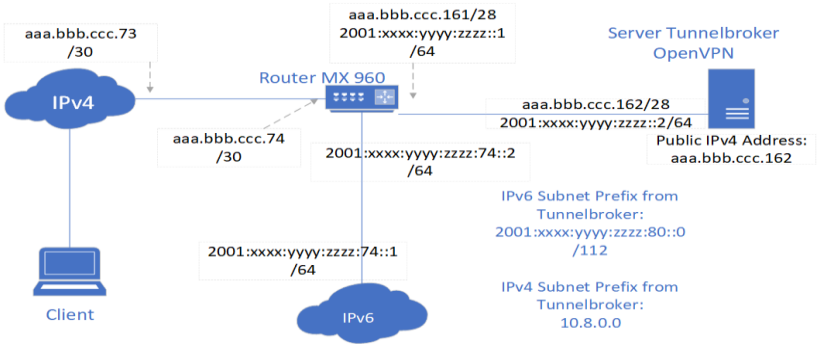


Figure 4. Experiment network topology

### 3.2.1. Switching on NAT and NDP Proxy

The first step in installing OpenVPN Tunnel Broker server is to activate NAT for IPv4 and NDP Proxy for IPv6 [17]. First, allow the kernel server to forward traffic from the client's device to the internet.

```
nano /etc/sysctl.conf
```

then, through IP table, several rules were added, including to activate NAT and to allow the eth1 interface to forward traffic from client's device to the internet.

### 3.2.2. Install OpenVPN on Server

First, update the ubuntu server packages

```
apt-get update
```

then, install the packages OpenVPN.

```
apt-get install openvpneasy-rsa
```

### 3.2.3. Generate Server Certificate and Key

After OpenVPN had been successfully installed in the server, the next step was to generate certificate and key for the client and OpenVPN server. This ties with the security needed in tunnel broker connection between client and server.
Server Configuration. During the server configuration, the following points are expected:

- Full IPv6 Connectivity over IPv4
- IPv4 TCP Connection on port 443
- Clients can communicate with each other using IPv4 and IPv6
- IP address is the Static IP clients are accepted
- Internet access on a client through a tunnel broker using the script client-connect.

### 3.2.4. Server Activation

Once the OpenVPN tunnel broker had been successfully installed, the server is activated with the following command:

```
serviceopenvpn restart
```

afterwards we can check whether the server has been activated by using the following command:

```
serviceopenvpn status
```

### 3.2.5. Client Configuration

The final process is to is configure each client. First is by creating a certificate and key by following the same steps to create a certificate and key for the server. Then, download the file generated certificate and key file to the device (client device).

```
/etc/openvpn/easy-rsa/keys/ca.crt
/etc/openvpn/easy-rsa/keys/iphone-nicolas.crt
/etc/openvpn/easy-rsa/keys/iphone-nicolas.key
```

Then, create a.ovpn file as a configuration file for the client that will be used in the client's OpenVPN application. Change the server IP VPN on the script with our own server IP (which in this case is aaa.bbb.ccc.162. On the asus-android device, we input the IPv4 10.8.0.102 dan IPv6 2001:xxxx:yyyy:zzzz:80::1004. We do this by inputing the following command:

```
nano /etc/openvpn/ccd/asus-android
```

Finally, download or move the asus-android.ovpn file to the client's device (smart phone, laptop, PC) by using the client's OpenVPN application to access the tunnel broker and to allow IPv6 to communicate by using IPv6 on top of IPv4 network. Testing: To make sure that the IPv6 is working properly, conduct a PING test from the client's device to the tunnel broker server IP VPN (2001:xxxx:yyyy:zzzz:80::1).

## 4. Results of Measuring and Analysis

The next main objectives of this research are measuring and analysis of performance metrics as TCP and UDP throughput, UDP Jitter and UDP Packet loss. The Performance matrics as a part of Quality of Service (QoS) is designed to ensure that end users get reliable performance from applications or services provided by a network [18].

### 4.1. TCP Delivery

The TCP delivery vs round trip latency measurement is intended to find out how big the TCP traffic that can be received by the client, so that it can indicate the level of stability of the BCN Telkom Laboratory, namely is public Ipv4 address aaa.bbb.ccc.162/28 and public Ipv6 address 2001:xxxx:yyyy:zzzz::1/64. Measurements are performed on clients in different Ipv4 and Ipv6 networks which arecaptured in every 10 seconds to 100 seconds. Figure 5 shows the result of TCP delivery vs round trip latency measurement with tool iperf software.

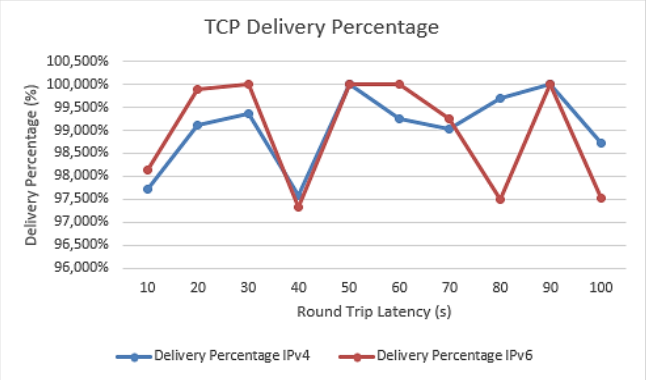


Figure 5. TCP delivery vs round trip latency

The delivery percentage of Ipv6, in frame time from initial up to 70 seconds in generally bigger than delivery percentage of Ipv4 and it's can reach maximum values around 100%. While in the next period will decrease until reach the minimum values is 97.5%. This shows that the stability of TCP traffic in the application client to access the OpenVPN tunnel broker is very high, and at the beginning and in the next few moments is at a minimum value. From delivery percentage of Ipv4 or for Ipv6 is still quite high and said the stability of the access client to tunnel broker is still good. In tunneling method, found that TCP performance is degraded due to the header and payload of the Ipv6 packet [19].

### 4.2. TCP Throughput

The TCP throughput vs round trip latency measurement is mainly focused for to know how much TCP traffic bandwidth can be received by client or host terminal. In other words, what's the network can guarantee bandwidth for client requirement. Measurements are performed on clients in different IPv4 and Ipv6 networks and are performed every 10 seconds to 100 seconds. Figure 6 shows the result of TCP throughput vs round trip latency measurement with tool iperf software. The TCP Throughput on client Ipv6 up to 40 seconds in generally larger than Ipv4 client and can achieves almost 7 MBps. Where as in the next period will decrease until it reaches a minimum value around 2.5 MBps. This indicates that connection by OpenVPN client Ipv6 will be better than the Ipv4 client. After that on the next few moments opposite, the Ipv4 client get bandwidth is higher, so the period will be repeated. The TCP throughput that can be received by client in VPN access through the tunnel broker, both for Ipv4 or Ipv6 is still very high and enough to get the multimedia application in the network. In the internet community, the user's need for network access will increase, so with the speed of the user in the Megabit order the problem to the speed will be low data and the instability of the connection will not happen [9], [19–21].

### 4.3. UDP Throughput

The UDP throughput vs bandwidth measurement is intended to find out how big the client get rate service by networks that are already using the mechanism of tunnel brokers as openVPN access. The measurements taken from clients that inside the IPv4 network and the Ipv6 network, with increasing bandwidth from 2 MBps up to maximum 10 MBps. In this experiment the UDP throughput is measured by using tool Iperf software. Theoretically, the throughput represents the upper bound for each Ipv4 and Ipv6 [22]. The UDP throughput measurements for Ethernet is depicted in Figure 7, where the UDP throughput of Ipv4 always same with the UDP throughput of Ipv6 for all bandwidth rates and increasing with the increase of bandwidth rate. Its mean that, tunnel broker as tunneling techniques with add an Ipv4 header to the Ipv6 packets to travel the Ipv4 network, can causes throughput received by client will increase if the link bandwidth increasing. The UDP transmission data with throughput measurements via tunnel broker does not affect the metrics performance of Ipv4 and Ipv6 protocols. In other words, it can be concluded that the tunnel broker mechanism in BCN Telkom Laboratory working well to service different clients.

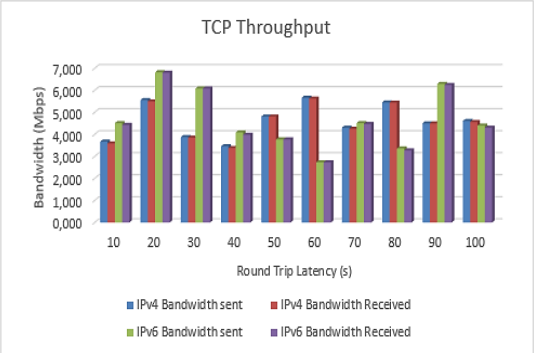


Figure 6. TCP throughput vs round trip latency

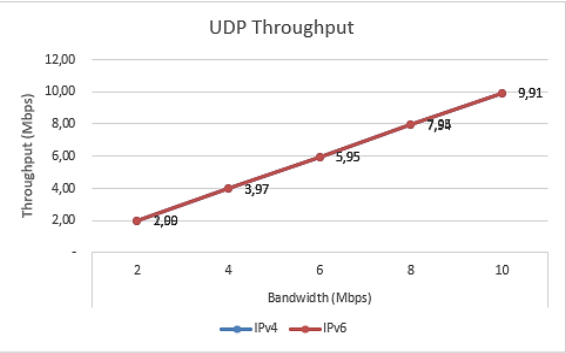


Figure 7. UDP throughput vs bandwidth

### 4.4. UDP Jitter

The UDP jitter vs bandwidth measurement is intended to find out how sensitive to changes network link bandwidth provided. The measurements taken from clients that inside the IPv4 network and the Ipv6 network, with increasing bandwidth from 2 MBps up to maximum 10 MBps. Figure 8 shows the result of UDP jitter vs bandwidth measurement with using tool iperf software. The UDP jitter for Ipv6 on all rate bandwidth has a value greater than Ipv4, although having the same pattern that if the bandwidth rising so the value of the UDP jitter will increasingly significant. The bigger value of Ipv6 UDP jitter caused due to the increase of the size of the Ipv6 packet due to addition of Ipv4 packet header. The value of UDP jitter from both the protocol can also illustrate the magnitude of the perceived delay in access VPN client through a tunnel broker. From the graph it can be concluded that to get jitter values that are not too high, then it needs a link bandwidth must be provided around the maximum bandwidth that is 10 MBps. The UDP jitter value besides depends on bandwidth link, it also depends on packet size, jitter will increases with increasing packet size [23].

### 4.5. UDP Packet loss

We concentrate on packet loss as one of the main QoS parameters, which means that different classes of service will be differentiated from each other based on packet loss. Packet loss is defined as the ratio of the total number of packets lost to the total number of packets that arrive [20]. The next measurement is towards in UDP packet loss vs bandwidth. It's intended to find out how much loss probability in the network if changes link bandwidth is occurred. The measurements taken from clients that inside the IPv4 network and the Ipv6 network, with increasing bandwidth from 2 MBps up to maximum 10 MBps.

From Figure 9 shows the UDP packet loss for Ipv6 was initially low far below 5%, after increasing bandwidth then increased also the values of packet loss. Compare to [24], the 6-to-4 loss rate of voice and video conferencing are less than 5%. This condition also occurs on Ipv4, although not as big as that experienced by Ipv6. The value of the Ipv6 UDP packet loss larger due to some security issues that will be solved by Ipsec (IP security). The value of UDP packet loss is resulted from client VPN access through the tunnel broker can describes how big a success the system can guarantee services on the customers. To get the values of UDP packet loss of less than 5%, to recommended that the network is working on link bandwidth not exceeding 6 MBps. In general, testing network performance whether based on TCP or UDP will depend on the size of the IP datagram itself [25].

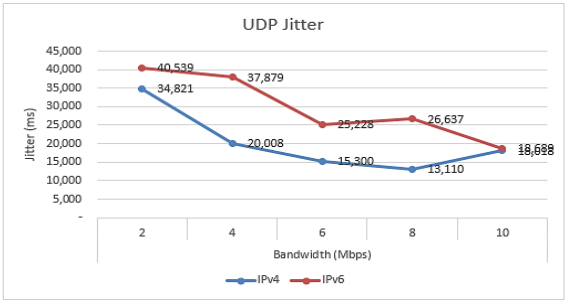


Figure 8. UDP jitter vs bandwidth

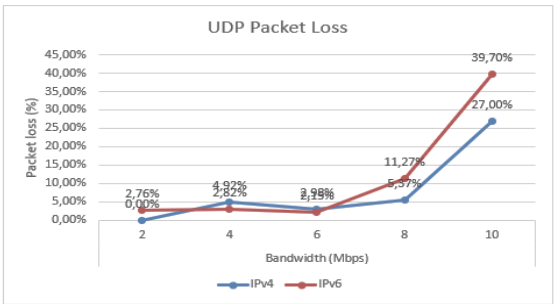


Figure 9. UDP packet loss vs bandwidth

## 5. Conclusion

In this research focused on the performance of tunnel broker mechanism by utilizing open VPN as access to the network. Open VPN as a provider that implements that the network configures itself as a VPN network, so IPv6 and IPv4 public IP clients can easily connect to the VPN server. From the result of topology design and experiment conducted at BCN Telkom Laboratory shows that TCP traffic stability perceived by IPv4 client and IPv6 in accessing tunnel broker through open VPN is still very good that is at achievement of TCP delivery percentage minimum 97.5% and in range throughput 2.5-7MBps. Similarly, to UDP throughput, both clients can obtain a 2s-10 MBps throughput range, this indicates that the client can access the services or multimedia applications is very well. To keep the value of packet loss and jitter low its means

below 5%, then what need to be done by tunnel mechanism that is tunnel broker based on Open VPN is link bandwidth between client-server or otherwise can not exceed 6 MBps, if this can not be fulfilled then network performance will decrease.

## References


[1] [R Hinden. Internet protocol, version 6 (IPv6) specification. RFC 8200, 2017.
[2] N Ravi, M Saravanan, M Periyasamy. Implementation of IPv6/IPv4 Dual-Stack Transition Mechanicm. *IJIRCCE*. 2014: 2(11): 6326-6332.
[3] IoanRaicu, S Zeadally. *Impact of IPv6 on End-user Applications*. In: Proceedings of the 10th International Conference on Telecommunications. 2003: 973–80.
[4] Ali Albkerat, Biju Issac. Analysis of IPv6 transition technologies. *Int J Comput Networks Commun*. 2014; 6(5): 19-38.
[5] Adira Quintero, Francisco Sans, EG. Performance Evaluation of IPv4/IPv6 Transition Mechanisms. *Int J Comput Networks Inf Secur*, 2016; 2: 1-14.
[6] D Shalini Punithavathani. IPv4/IPv6 Transition Mechanisms. *Eur J Sci Res*. 2009; 34(1): 110–24.
[7] Adarsh M, Hasha C. Performance Analysis of IPv6 Dual-Protocol Stack and Tunnel Transition. *Int J Sci Eng Technol Res*. 2016; 5(5): 1494-1499.
[8] C V Ravi Kumar, Kakumanilakshmi Venkatesh MVS, KPB. Performance Analysis of IPv4 to IPv6 Transition Methods. *Indian J Sci Technol*. 2016; 9(20): 1-8.
[9] Chen J, Chang Y, Lin C. *Performance investigation of IPv4/IPv6 transition Mechanisms*. In: Proceedings of the 6th International Conference on Advanced Communication Technology. 2004: 545–54.
[10] Fatimah Abdulnabi Salman. Implementation of IPsec-VPN Tunneling using GNS3. *Indonesian Journal of Electrical Engineering and Computing Science*. 2017; 7(3): 855-860.
[11] S Steffann, I Van Beijnum, R Van Rein, A Comparation of IPv6-over-IPv4 Tunnel Mechanism, RFC 7059, ISSN 2070-1721, 2013.
[12] Nazrulazhar Bahaman AS. Network Performance Evaluation of Tunnelling Mechanism. *J Appl Sci*. 2012; 12(5): 459–65.
[13] Md Asif Hossaina, DurjoyPodderb, SarwarJahanc MH. Performance Analysis of Three Transition Mechanisms between IPv6 Network and IPv4 Network: Dual Stack, Tunnelling and Translation. *Int J Comput*. 2016; 20(1): 217–28.
[14] Mohd.KhairiSailan, Rosilah Hassan AP. *A Comparative Review of IPv4 and IPv6 for Research Test Bed*. In: 2009 International Conference on Electrical Engineering and Informatics. Selangor, Malaysia; 2009.
[15] Ta Te Lu, Cheng Yen Wu, Wen Yen Lin, Hsin Pei Chen, and Kuang Po Hseueh. Comparison of IPv4-over-IPv6 (4over6) and Dual Stack Technologies in Dynamic Configuration for IPv4/IPv6 Address. *Springer International Publishing AG*. 2017.
[16] M Fawad, S I Ullah, H Noureen, AW Khan, Z Khitab, S Khan, A Salam, MA Khan. Performance ANalysis of VoIP over IPv4, IPv6 and 6-to-4 Tunneling Networks. IJCSIS, 2016; 14(6): 368-372.
[17] Bali P. A Detail Comprehensive Review on IPv4-to-IPv6 Transition and Co-Existence Strategies. *Int J Adv Res Comput Eng Technol*. 2015; 4(4): 1429-1432.
[18] ITU-T. Transmission System And Media, Digital System And Networks, Quality of Services and Performance. ITU-T Recommendation G.1010, 2001.
[19] Aris Cahyadi Risdianto, R Rumani. I*Pv6 Tunnel Broker Implementation and Analysis for IPv6 and IPv4 Interconnection*, The 6th International Conference on Telecommunication Systems, Services, and Applications 2011.
[20] Mufadhol, GuruhAryotejo A. Netscan and Networx for Management Bandwidth and Traffic with Simple Routing. *TELKOMNIKA Telecommunication, Computing, Electronics and Control*. 2017; 15(1): 464–70.
[21] Omar Najah, KamaruzzamanSeman K. Packet Loss Rate Differentiation in slotted Optical Packet Switching OCDM/WDM. *TELKOMNIKA Telecommunication, Computing, Electronics and Control*. 2017; 15(3): 1061–71.
[22] Galkwad PP. Routing Mechanism for the Improvement of Network Throughput. *Int J Adv Res Comput Sci Softw Eng*. 2014; 4(5): 423–6.
[23] S Narayan; S Tauch. *IPv4-v6 configured tunnel and 6to4 transition mechanisms network performance evaluation on Linux operating systems*. International Conference on Signal Processing System (ICSPS), Auckland, New Zealand. 2010.
[24] KE Khadiri, O Labouidya, N Elkamoun, R Hilal. Performance Evaluation of IPv4/IPv6 Transition Mechanisms for Real-Time Application using OPNET Modeler. *IJACSA*, 2018; 9(4): 387-392.
[25] Se-Joon Yoon, Jong-Tak Park, Dae-In Choi and Hyun K. Kahng. Performance Comparison of 6to4, 6RD, and ISATAP Tunnelling Methods on Real Testbeds. *(IJIDCS) International Journal on Internet and Distributed Computing Systems*. 2012; 2(2): 149-156.