

Performance Analysis of Network Applications on IPv6 Cloud Connected Virtual Machine

Zeeshan Ashraf

The University of Lahore Gujrat Campus, Gujrat, Pakistan
E-mail: zeeshan.ashraf@cs.uol.edu.pk

Adnan Sohail

IQRA University Islamabad Campus, Islamabad, Pakistan
E-mail: adnan.sohail@iqraisb.edu.pk

Muhammad Yousaf

Riphah International University Islamabad Campus, Islamabad, Pakistan
E-mail: muhammad.yousaf@riphah.edu.pk

Received: 05 October 2019; Accepted: 16 October 2019; Published: 08 December 2019

Abstract—The rapid growth of the Internet and a number of changes in the technology landscape have resulted to move traditional IPv4 networks to virtualized IPv6 networks. Reliable and fast delivery of network services with minimum hardware and lower cost are the main challenges for network operators in the modern technological era. Network operators are moving towards the virtual IPv6 networks. As IP protocol does not guarantee packet delivery, therefore, for reliable delivery of services like FTP, HTTP, and SMTP, the IP protocol is associated with TCP on the transport layer while audio/video live streaming, and real-time applications use UDP. QoS of video streaming and real-time applications are depended upon better network resources management and planning while QoE is dependent on network performance. Different sizes of the packet affect overall QoS. Optimum services can be achieved through the proper selection of routing protocol in the network. In this study, the performance of the IPv6 virtual machine connected to the large scale virtual IPv6 network through the cloud is measured and compared on the basis of the packet sizes of TCP and UDP. GNS3 network emulator and VMware have been used for testing and analyzing the performance of the IPv6 virtual network in terms of several parameters such as convergence, RTT, throughput, jitter, and packet loss. Results indicate that the EIGRPv6 routing protocol with the collaboration of BGPv4 delivers better performance through virtual network services over the cloud network.

Index Terms—BGPv4, Cloud Infrastructure, EIGRPv6, OSPFv3, NSV, VRF.

I. INTRODUCTION

With the fast development of the IoT, the Internet is growing towards IPv6 in all over the world quickly since

last few years [1]. IP version 6 is said to be a next-generation IP protocol. It offers larger IP addresses, small header size, efficient routing, and better QoS (Quality of Services) [2]. According to Google updated survey report [3], IPv6 adoption is completed more than 25 % throughout the world. Home users are using easily different types of services like real-time applications, online gaming, audio/video streaming, web browsing, and emails by directly connected with the Internet through smartphones which are supported by 4G & 5G technologies respectively. Cloud computing is a new emerging paradigm which is based on virtualization and has been developed into the backbone of the modern economy [4]. It is the on-demand delivery of services such as database, storage, applications, and other IT resources over the Internet without direct active management by the user with pay-as-you-go [5]. Cloud computing provides major benefits such as scalability, resilience, flexibility, efficiency, and the outsourcing of non-core activities [6]. Real-time applications, online gaming, and audio/video streaming are based on high network traffic and demand minor delays [1].

Traditional IP network architecture is designed for end-to-end packet delivery service by using IP protocol. IP is a connectionless protocol and does not provide a guarantee of packet delivery service. Indeed, IP protocol tries best efforts to deliver a packet through different routes over the network [7]. Some application protocols such as FTP, SMTP, and HTTP have required a guarantee of packet delivery. To provide a guarantee of packet delivery services, the IP protocol is associated with TCP protocol on the transport layer. TCP is a connection-oriented and reliable protocol. It provides a guarantee of packet delivery by receiving acknowledge of every packet [8]. If the packet dropped by virtue of any reason then it re-transmits dropped the packet and waits for an acknowledgment. However, the audio/video traffic is delivered through UDP on the transport layer and does

not afford a huge delay.

An IP packet is traversed from one router to the next based on the independent forwarding decision of every individual router [9]. The destination IP address is stored in the IP header. The router gets the destination address from the IP header, looks up in the routing table. If the address found in the routing table then the packet is forwarded to next hop otherwise, the router discards the packet. Each router runs a routing protocol to compute optimal paths, complete routing tables in large size and complex networks [10]. The larger size of the routing table increases the lookup delay. Routing protocols are upgraded in the IPv6 network. RIPng, OSPFv3, and EIGRPv6 are upgraded versions of interior gateway routing protocols while BGPv4 is an enhanced version of an exterior gateway routing protocol in IPv6. IPv6 routing protocols are different from each other in terms of performance, metrics, and configuration style. Optimum services can be achieved through the proper selection of routing protocol in the network. OSPFv3 is more scalable because of the hierarchical nature [11]. The overall performance of the network may cut down due to the larger size of the IPv6 addresses, end-to-end delay, jitter, and packet loss. The guarantee of service to any kind of traffic with maximum throughput and minimum transmission delays is called QoS. To provide better QoS, the packets are classified into different categories and sizes [12]. The packet size is a very important factor for the performance of the devices. Packet loss ratio and throughput depend upon the size of the packets [13]. The packet prioritization technique is adopted to increase the throughput of the particular application for QoS. Moreover, Quality of Experience (QoE) is the reaction given by users based upon services provided by a system. User feedback is reliant on how much the user is satisfied in terms of usability, accessibility, and integrity of the QoS.

Virtualized network architecture is also an adoptive model in Next Generation Network (NGN). Network operators are shifting physical networks towards cloud and virtual networks. The virtual network enables the decoupling of dedicated hardware and provides the services on software-based virtual machines. It provides a lot of benefits over traditional physical networks in order to reduce equipment cost, to reduce the energy consumption of hardware, flexibility, easy management, and openness of platforms [14]. The virtualization techniques are successfully implemented in networking for the last several years in the form of VLAN, VPN, VRF, and VMware infrastructure [15]. Virtual Route Forward (VRF) is a technique that creates multiple virtual independent routing tables within a single network entity. In a single network component, multiple VRF resources create isolation between virtual networks. Several other virtual network models such as Software Defined Network (SDN), Network Function Virtualization (NFV), Network Services Virtualization (NSV), and Hypervisor are available to provide services on software-based instead of physical dedicated hardware.

In this study, the focus is on comparing the

performance of different sizes of TCP/UDP packets sent/received by a virtual machine connected with a large scale IPv6 virtual network through cloud. The virtual IPv6 network consists of different levels of service providers. The service providers run different IPv6 routing protocols for packets delivery. EIGRPv6 and OSPFv3 with BGPv4 are analyzed on the basis of the packet sizes of TCP/UDP in terms of several parameters like convergence, throughput, delay, jitter, and packet loss over the cloud network. The objectives of this research are very clear related to minimize the involvement of physical equipment, move networks towards openness, and provide better performance to customers with minor costs. To achieve goals, we arranged a cloud-based virtual IPv6 network with the help of a GNS3 emulator and VMware. We deployed network services virtualization and hypervisor. Rest of the paper is structured as follows: Section II presents related works and compares this research with existing studies, Section III describes cloud computing, Section IV highlights the IPv6 routing protocols and differences. In Section V, we display the experimental results and finally, Section VI concludes the paper.

II. RELATED WORKS

In [16], the authors evaluated the performance of IPv4 and IPv6 routing protocols by designing a conceptual network model in the GNS3 emulator in terms of latency and end-to-end delay on the basis of different packet sizes. After getting the results, the researchers observed the performance of IPv6 routing protocols is better than the performance of IPv4 routing protocols in all parameters. However, the packet size affects the travel time which requires to reach its destination. In [17, 18, 19], the authors measured the performance of video streaming through IPv6 routing protocols on the basis of several parameters such as packet loss, throughput, end-to-end delay, and jitter. The researchers investigated the performance of RIPng, OSPFv3, and EIGRPv6 by designing the network topology in the OPNET simulator. The results showed that RIPng performed better in most of the above-mentioned parameters. In [20, 21], the authors examined the performance of real-time applications, database, video, voice, and web through IPv6 routing protocols with the help of the OPNET simulator. The researchers measured the performance of RIPng, EIGRPv6, and OSPFv3 based on a number of criteria including network convergence duration, response time, DB query response time, IPv6 packet drop, video packet delay variation, and video packet end-to-end delay.

In [22, 23], researchers compared the performance of OSPFv3 and EIGRPv6 on the basis of optimization technique, converge times and resources such as CPU utilization, memory utilization, and tunnel overhead used by routers in a small IPv6 enterprise network and hybrid IPv4-IPv6 network respectively with the help of simulators. In [24], the authors highlighted the impact of routing protocols and compared the performance in the

dual-stack, manual tunnel, and 6to4 tunnel. The researchers measured the performance of real-time applications of video conferencing on the basis of delay, delay variation, and packet loss by using the OPNET simulator. The results showed that the performance of the dual-stack technique is better than tunneling techniques along with the IS-IS routing protocol. In [25], the authors compared the performance of RIPng, OSPFv3, and EIGRPv6 with IPv6 external routing protocol BGPv4 by using GNS3 emulator through several parameters such as throughput, jitter, packet loss, and network convergence. The results indicated that the convergence of OSPFv3 was fast and the combination of OSPFv3 with BGPv4 has the highest throughput, lowest packet loss, and smallest jitter value.

The work presented in this paper differs from the above-cited works in several ways. In the above-cited works, the researchers compared the performance of RIPng, IS-IS, OSPFv3, and EIGRPv6 while in this research work, the focus is only on OSPFv3 and EIGRPv6 through network services virtualization along with external IPv6 routing protocol (BGPv4) over the cloud. Because OSPFv3 and EIGRPv6 are mostly used as interior IPv6 routing protocols in large networks. In addition, a virtual client is connected with a server located in another autonomous system through the cloud and sends/receives a variety of traffic in different sizes.

III. CLOUD COMPUTING

Cloud computing has been recognized as the de facto computing standard for hosting and delivering services over the Internet. Cloud computing is being quickly implemented by service providers and end-users because of many benefits over traditional computing models such as cost-saving, scheduling, energy efficiency, scalability, unlimited storage, anytime anywhere access, and high fault tolerance capability [26]. Cloud computing is divided into three main service models.

- Software as a Service (SaaS)
- Platform as a Service (PaaS)
- Infrastructure as a Service (IaaS)

A. Software as a Service (SaaS)

SaaS is a software distribution model. It allows users to access applications using a thin client in the form of a web browser, hosted in cloud data centers over the Internet [4]. Occasionally, it is referred to as on-demand software. In this model, a third-party provider hosts the application and makes them available to customers. It allowed organizations to avoid earning license fees and IT infrastructure maintenance. It has become a delivery model for many business and scientific applications such as messaging software, databases, and Management Information System [6]. It is based on a multitenant architecture in which a single application with single hardware resources, network, and operating system is used for multi-tenant. Some SaaS models do not support multi-tenancy while some use a virtualization mechanism.

B. Platform as a Service (PaaS)

PaaS provides a simple platform and environment for customers or developers to build, run, and manage applications and services over the Internet without the complexity of maintaining the infrastructure typically associated with launching an application. PaaS services are hosted in the cloud and accessed by users simply via a web browser. PaaS is categorized into public, private, and hybrid [6]. A public PaaS is derived from SaaS. It is situated between SaaS and IaaS in cloud computing. A private PaaS can typically be downloaded and the hybrid is the mixture of both. PaaS is custom-made for users require more control over IT recourses and the difficulties of traffic routing systems.

C. Infrastructure as a Service (IaaS)

IaaS provides virtualized computing resources in cloud computing over the Internet. It combines SaaS along with PaaS. It is not only the foundation for SaaS and PaaS but has also been the pillar of cloud computing. A hypervisor, such as VMware or Hyper-V runs the virtual machines as guests [4]. Typically IaaS involves the use of a cloud orchestration technology. Currently, IaaS providers mostly rely on either static or dynamic VM provisioning policies.

The next generation clouds should also be ready to emerge traditional or non-traditional architectures trends such as neuromorphic, quantum computing, adiabatic, nano computing, containerization, SDN, and Fog/Edge computing.

IV. IPV6 ROUTING PROTOCOLS

Routing is also a challenging task for network professionals when the network size is large, complex, heterogeneous, and scalable. Without a proper scalable routing system, a network does not provide better performance. Scalable routing protocol determines the best path from source to destination quickly and efficiently if multiple paths exist in the large and complex network [27]. Routing protocols are introduced to overcome convergence and scaling issues. A kind variety of routing protocols is available for IPv6 networks. IPv6 protocols are different from each other in terms of configuration, metrics, path calculation method, and convergence [23].

A. EIGRPv6

Enhanced Interior Gateway Routing Protocol version 6 (EIGRPv6) is a hybrid and interior gateway IPv6 routing protocol. It was designed by "CISCO Systems" as a proprietary protocol and available only on CISCO devices. Later on, its proprietary status was converted to an open standard for the multi-vendor environment since 2016 [28]. Now, any vendor can be implemented EIGRP freely.

Routing information is exchanged between the two devices when both devices are running the same protocol. During convergence, EIGRP shares information with

other devices and tries to make adjacency. When the adjacency is completed then EIGRP exchanges complete routing table [23]. After this, only topological changes are sent. It uses a specific algorithm Diffusing Update Algorithm (DUAL) to achieve fast loop-free convergence with little overhead. Usually, bandwidth and delay are used as metrics to measure the best route. By default, administrative distance is 90 which helps to prefer when multiple routing protocols are configured. It works in an Autonomous System (AS). The 32-bit IP address is used for router-id. It is configured either by name or an AS number. It supports MD5 and SHA-2 authentications [10]. It supports route summarization and route redistribution. It supports un-equal load balancing. It supports VRF-Lite when configured by name.

B. OSPFv3

Open Shortest Path First version 3 (OSPFv3) is a pure link state and interior gateway IPv6 routing protocol. It was proposed by IETF as an open standard protocol [11]. Due to the open standard, it was widely used in the industry. It also works in AS.

OSPF uses the “Dijkstra” algorithm to calculate the best routes. It uses cost as a metric. It works in the hierarchy and divides the network into different areas for better management. By default, area 0 is a backbone area if there are multiple areas exist in the network. Virtual links are used to connect multiple areas with the backbone area. During convergence, OSPF shares area ID along with other information. In OSPF, two devices could be neighbors when the area will be the same. OSPF sends a complete routing table for the first time then only changes are sent. Its administrative distance is 110. It also supports a 32-bit IP address as a router-id [29]. It supports route summarization and route redistribution. In OSPFv3, the authentication fields have been removed from the OSPFv3 packet header. It relies on the IP authentication header. It supports equal load balancing.

C. BGPv4

Border Gateway Protocol version 4 (BGPv4) is an exterior gateway IPv6 routing protocol. It was proposed by IETF as a patch vector and inter-AS routing protocol [30]. It is different from the distance vector and link-state routing protocols. The routing decision is based on paths, network policies, or set of rules configured by a network administrator. In the routing table of the BGP, every entry contains the destination network address, the next router, and the path to reach the destination.

BGP may be used for routing either i-BGP or e-BGP. Within AS, it configures as i-BGP. Its administrative distance for internal is 200 and 20 for external. BGP neighbors among devices are called peers. In BGP, peers are established by manual configuration. BGP is a unique routing protocol in a sense, it uses TCP with port 179 as a transport protocol. It supports MD5 and SHA-1 for peer authentications [23]. It supports route summarization and route redistribution. It also supports multi-homing. Its convergence is slow as compared to other IPv6 routing protocols.

V. EXPERIMENTS AND RESULTS

The Graphical Network Simulation (GNS3 v2.1.16) and VMware are adopted for experiments on a laptop. GNS is an emulator and provides support to load actual IOS of the devices. The results are received through GNS seem very close to the results obtained by real routers. The topology of this paper is described in Fig. 1.

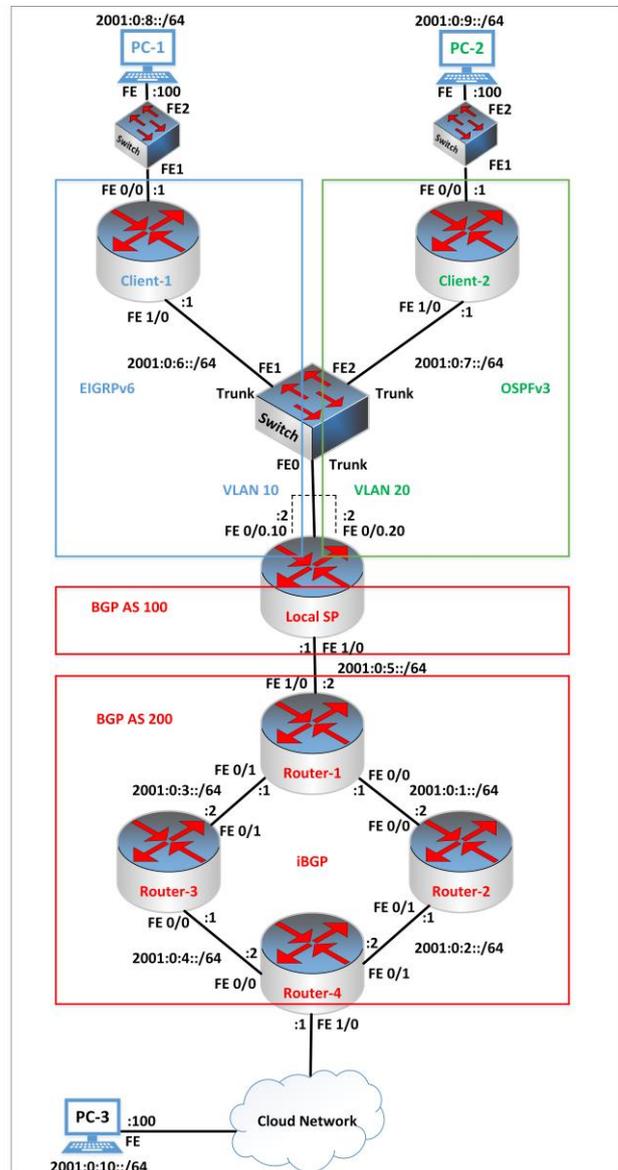


Fig.1. Experimental Setup

In this arrangement, a local service provider wants to provide services to its multiple clients with minimum resources. Therefore, two clients are directly connected through trunk links with a switch. Similarly, more clients may also connect easily. A single physical trunk link is established between the local service provider’s router and switch with encapsulation of “dot1q”. In this situation, it is not feasible to configure multiple IP addresses on a single link. The physical link is divided into multiple sub-interfaces which are called virtual links.

The IP addresses are assigned per virtual link. Fast Ethernet or Gigabit Ethernet links are used for better performance. VRF can be configured when multiple routing tables are needed. VRF isolates routes among different clients. The routes in VRFs are exported or imported among VRFs. The concept of import/export routes in VRF is also called route leaking [15]. The client-1 runs the EIGRPv6 routing protocol while client-2 runs OSPFv3. Both clients send/receive traffic simultaneously through a physical shared link without traffic overlapping. The local service provider is further connected with a regional service provider through BGP.

The regional service provider consists of several routers directly connected to each other by a mesh topology. The regional service provider runs e-BGPv4 among different AS while runs i-BGPv4 within AS. The regional service provider is connected with other service providers through cloud computing. A virtual machine host-3 is connected with a regional service provider through a private cloud with the help of VMware and tries to access services provided by either client-1 or client-2.

The description of the devices used in experiments is shown in Table 1.

Table 1. Devices with Description

| S# | Device | Description |
|----|----------|--|
| 1 | Laptop | Core i3 HP Pavilion g Series, 6 GB RAM 64-bit Microsoft Windows 10 Operating System |
| 2 | Router | GNS3 based CISCO 7200 series, IOS v. 15.2(4)S3, c7200-adventerprisek9-mz.152-4.S3 Total = 5 |
| 3 | Router | GNS3 based CISCO 3700 Series, IOS v. 12.4(15)T10, C3725-adventerprisek9-mz.124-15.T10 Total = 2 (Client-1 and Client-2) |
| 4 | Switch | GNS3 based fastEthernet Switch with Trunk Ports Total = 3 |
| 5 | PC1, PC2 | 64-bit Windows 10 |
| 6 | PC3 | VMware Virtual Machine with 64-bit Windows 8.1 |

Data is captured through the “Jperf v2.0.2” tool and network’s commands during experiments. The Jperf is a client/server GUI based network performance measurement and traffic generated tool with IPv6 supported. All experiments are performed repeatedly (5 times) during different times of the different days then we took the mean of the results. The experimental setup and time duration remain the same for all protocols.

A. Convergence

Convergence is the time in which devices share routing information with neighbors and try to complete the routing table. It is measured as to how fast a router becomes ready for user traffic. In this research study, three IPv6 routing protocols are run. The average convergence and re-convergence time in seconds of the IPv6 routing protocols are shown in Fig. 2.

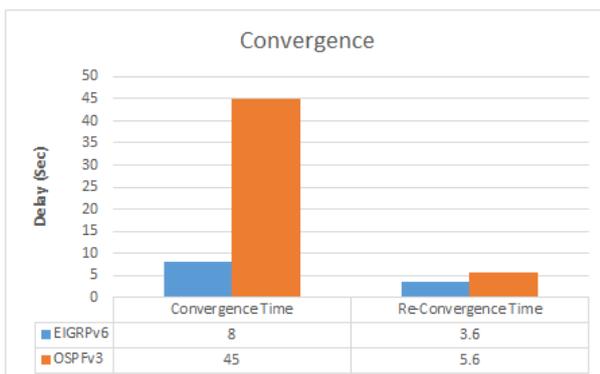


Fig.2. Convergence & Re-Convergence

Results show that the convergence & re-convergence of EIGRPv6 is much better than OSPFv3 because EIGRPv6 learns the topology information more rapidly. It means the router with EIGRPv6 becomes ready for user traffic quickly as compared with OSPFv3. The OSPFv3 relies on a more complex algorithm as compared to EIGRPv6 and requires more time to converge [31, 32]. The OSPFv3 works in the hierarchical model in which first of all it selects Designated Router (DR) through the election process on Ethernet.

B. Round Trip Time

The Round Trip Time (RTT) is the total time required for a packet to travel from source to destination and its acknowledgment back to the source. It is calculated through the “PING” command. The RTT results make sure the connectivity between source and destination and show how much the network is congested. It is based on queuing delay in routers and processing in the end system. More delay and heavy congestion will cause the packet drop [13].

Fig. 3 shows the average RTT from the source node PC-3 to destination nodes PC-1 and PC-2 respectively over the cloud network on the basis of different packet sizes. By default packet size is 32-bytes in Windows while 56-bytes in Linux. When the packet size is increased then the RTT is also increased. The graph shows the variation in the results. For discrete value, it is needed to calculate the Standard Deviation (SD) and Coefficient of Variation (CV) as in (1) and (2) respectively for such kind of variations in the graphs.

$$S = \sqrt{\frac{\sum_{i=1}^n (x_i - \bar{x})^2}{n-1}} \tag{1}$$

$$CV = \frac{S}{\bar{X}} \times 100 \tag{2}$$

Where S is represented as a standard deviation and \bar{X} symbolized the mean.

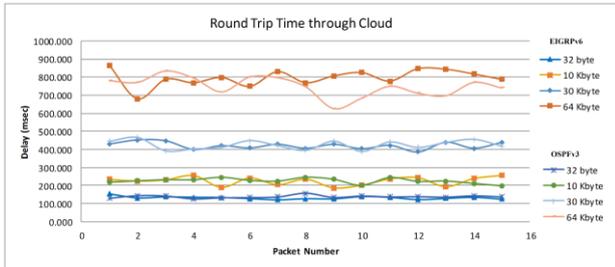


Fig.3. Average RTT of Packets

Table 2 describes the mean, SD, and CV of the delays between EIGRPv6 and OSPFv3 over the cloud network on the basis of packet sizes.

The results show that the RTT with OSPFv3 is lower with the small sizes of the packet while the RTT with EIGRPv6 is lower with the large sizes of the packet. It means, OSPFv3 consumed extra time in queuing delay with larger packet size.

Table 2. RTT of Packets

| S# | Packet Size | Protocol | Mean (ms) | S. Deviation (ms) | CV (ms) |
|----|-------------|----------|-----------|-------------------|---------|
| 1 | 32 byte | EIGRPv6 | 131.87 | 8.19 | 6.21 |
| | | OSPFv3 | 137.85 | 7.44 | 5.40 |
| 2 | 10 Kbyte | EIGRPv6 | 225.01 | 23.39 | 10.40 |
| | | OSPFv3 | 226.11 | 14.63 | 6.47 |
| 3 | 30 Kbyte | EIGRPv6 | 421.60 | 19.33 | 4.58 |
| | | OSPFv3 | 425.47 | 25.06 | 5.89 |
| 4 | 64 Kbyte | EIGRPv6 | 797.25 | 46.06 | 5.78 |
| | | OSPFv3 | 748.33 | 54.02 | 7.22 |

C. Jitter

Voice or video data require speed over the network. Jitter refers to the variation in latency of packets carrying voice or video data through UDP protocol over a communication channel. The UDP protocol does not re-transmit lost data. If jitter is increased over the network then, the packet may be lost.

Fig. 4 shows the average calculated jitter with a fixed 64 Kbytes buffer size of UDP among different packet sizes over the cloud network from source PC-3 to destination PC-1 and PC-2 respectively.

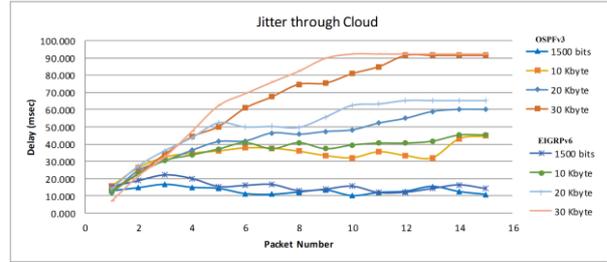


Fig.4. Average Jitter of Packets

Results show that when the size of the packet is increased then jitter also increased in both EIGRPv6 and OSPFv3. The comparison of jitter between OSPFv3 and EIGRPv6 on the basis of packet sizes is described in Table 3. Variation in latency can increase due to improper queuing, network congestion, and configuration errors.

The results show that the jitter with OSPFv3 is lower with the small size of the packets while the jitter with EIGRPv6 is lower with the large size of the packets. The performance of EIGRPv6 is better than OSPFv3 in large packet sizes with a minor difference.

Table 3. Jitter of Packets

| S# | Packet Size | Protocol | Mean (ms) | S. Deviation (ms) | CV (ms) |
|----|-------------|----------|-----------|-------------------|---------|
| 1 | 1500 bits | EIGRPv6 | 15.69 | 2.86 | 18.23 |
| | | OSPFv3 | 12.96 | 1.91 | 14.70 |
| 2 | 10 Kbyte | EIGRPv6 | 36.35 | 8.81 | 24.24 |
| | | OSPFv3 | 34.04 | 6.78 | 19.92 |
| 3 | 20 Kbyte | EIGRPv6 | 51.07 | 15.41 | 30.18 |
| | | OSPFv3 | 44.02 | 13.79 | 31.33 |
| 4 | 30 Kbyte | EIGRPv6 | 69.44 | 29.09 | 41.89 |
| | | OSPFv3 | 65.03 | 27.33 | 42.02 |

D. Throughput

Throughput is the rate of successful packet delivery over a communication channel through TCP protocol. Usually, it measures in bits per second (bit/s or bps).

The average throughput of various sizes of the packets is measured with a fixed 64 Kbytes TCP windows size over the cloud is shown in Fig. 5.

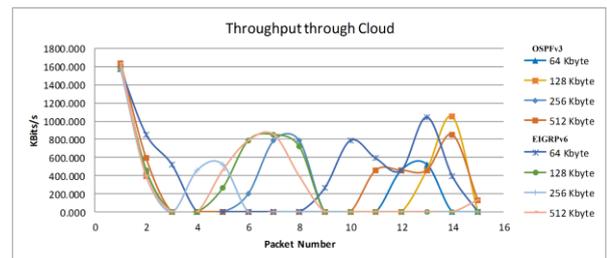


Fig.5. Average Throughput of Packets

The comparison of throughput between OSPFv3 and EIGRPv6 on the basis of packet size is described in Table 4.

Table 4. Throughput of Packets

| S# | Packet Size | Protocol | Mean (Kbits/s) | S. Deviation (Kbits/s) | CV (Kbits/s) |
|----|-------------|----------|----------------|------------------------|--------------|
| 1 | 64 Kbyte | EIGRPv6 | 432.20 | 475.28 | 109.97 |
| | | OSPFv3 | 201.00 | 427.97 | 212.92 |
| 2 | 128 Kbyte | EIGRPv6 | 310.20 | 476.13 | 153.49 |
| | | OSPFv3 | 231.60 | 473.23 | 204.33 |
| 3 | 256 Kbyte | EIGRPv6 | 196.60 | 425.46 | 216.41 |
| | | OSPFv3 | 253.40 | 462.62 | 182.56 |
| 4 | 512 Kbyte | EIGRPv6 | 310.13 | 472.13 | 152.24 |
| | | OSPFv3 | 305.87 | 463.14 | 151.42 |

The results show that the performance of OSPFv3 is better than EIGRPv6 with the small size of the packets due to low congestion in the link while the throughput with EIGRPv6 is higher than the OSPFv3 in large size of the packets. For a fixed buffer size, when the packets increased, the throughput of TCP flows decreased then it fluctuated in a specific range.

E. Packet Loss

Packet loss occurs when one or more packets fail to reach the destination through traveling across a network. Packet loss occurs due to errors in data transmission, buffer overflow, or network congestion. Packet loss is measured as a percentage of packets lost with respect to packets sent. In this research study, various sizes of the packet of ICMPv6 are sent through the "PING" command from source PC-3 to the destination PC-1 and PC-2 respectively to check packet loss in EIGRPv6 and OSPFv3. The TCP provides reliable services. TCP notices packet loss and performs retransmission of the lost packet. Its connection-oriented and reliable services help to avoid congestion over the network. However, UDP does not perceive packet loss. Table 5 describes the average packet loss of the numerous sizes of the packet.

Table 5. Packet Loss

| S# | Packet Size | Protocol | Packet Sent | Packet Dropped | Packet Loss (%) |
|----|-------------|----------|-------------|----------------|-----------------|
| 1 | 32 byte | EIGRPv6 | 75 | 0 | 0 |
| | | OSPFv3 | 75 | 0 | 0 |
| 2 | 10 Kbyte | EIGRPv6 | 75 | 0 | 0 |
| | | OSPFv3 | 75 | 0 | 0 |
| 3 | 30 Kbyte | EIGRPv6 | 75 | 1 | 1 |
| | | OSPFv3 | 75 | 1 | 1 |
| 4 | 64 Kbyte | EIGRPv6 | 75 | 11 | 14 |
| | | OSPFv3 | 75 | 14 | 18 |

The results show that packet loss did not occur in smaller packet sizes. When the size of the packet increased up to 64 Kbyte then packets dropped in both EIGRPv6 and OSPFv3 due to congestion. The results indicated that the performance of EIGRPv6 is much better than OSPFv3. In live audio/video streaming and

online game applications, packet loss affects QoE [33].

VI. CONCLUSIONS

This study focused on comparison and analysis of the performance of IPv6 virtual machines connected to the network through the private cloud on the basis of different sizes of the packet of TCP and UDP. The network consisted of regional-level service providers and local service providers. The regional level service providers provided services to local service providers through BGP. The local service provider configured different IPv6 routing protocols. In this study, client-1, and client-2 connected with the local service provider through virtual links and run EIGRPv6 and OSPFv3 respectively. IPv6 routes are shared among different IPv6 routing protocols. The different sizes of the packet of TCP and UDP sent through a virtual machine connected with the network through a private cloud and then measured the performance in EIGRPv6 and OSPFv3 with the collaboration of BGPv4 respectively. The performance of traffic measured through several parameters such as convergence speed, RTT, jitter, throughput, and packet loss on the basis of different packet sizes. Results displayed that a larger size of the packet affected the quality of services. Experimental results indicated that the overall performance of the virtual machine with EIGRPv6 routing is better than OSPFv3 over the cloud network. In the future, the focus will be on to optimize the performance of an upgraded version of Linux kernel with the larger size of the packets in the virtualized IPv6 datacenter through NFV.

REFERENCES

- [1] Y. Luo, X. Zhou, T. Dreiholz, and H. Kuang, "A Real-Time Video Streaming System over IPv6+ MPTCP Technology," in Workshops of the International Conference on Advanced Information Networking and Applications, 2019: Springer, pp. 1007-1019.
- [2] S. Deering and R. Hinden, "Internet protocol, version 6 (IPv6) specification," 2070-1721, 2017.
- [3] Google IPv6 Adoption Statistics, <https://www.google.com/intl/en/ipv6/statistics.html>
- [4] R. Buyya et al., "A manifesto for future generation cloud computing: research directions for the next decade," ACM computing surveys (CSUR), vol. 51, no. 5, p. 105, 2018.
- [5] A. Taherkordi, F. Zahid, Y. Verginadis, and G. Horn, "Future cloud systems design: challenges and research directions," IEEE Access, vol. 6, pp. 74120-74150, 2018.
- [6] B. B. Rad, T. Diaby, and M. E. Rana, "Cloud computing adoption: a short review of issues and challenges," in Proceedings of the 2017 International Conference on E-commerce, E-Business and E-Government, 2017: ACM, pp. 51-55.
- [7] R. Bush and D. Meyer, "RFC 3439: Some internet architectural guidelines and philosophy," ed: December 2003.
- [8] Y.-C. Lai, A. Ali, M. S. Hossain, and Y.-D. Lin, "Performance modeling and analysis of TCP and UDP flows over software-defined networks," Journal of Network and Computer Applications, vol. 130, pp. 76-88, 2019.

- [9] Z. Ashraf and M. Yousaf, "Optimized Convergence of OSPFv3 in Large Scale Hybrid IPv4-IPv6 Network," in 2018 14th International Conference on Emerging Technologies (ICET), 2018: IEEE, pp. 1-6.
- [10] Z. Ashraf, IPv6 Routing: A practitioner approach. Germany: LAP-LAMBERT, 2013.
- [11] R. Coltun, D. Ferguson, J. Moy, and A. Lindem, "OSPF for IPv6," 2070-1721, 2008.
- [12] J. Korhonen, H. Tschofenig, M. Arumathurai, M. Jones, and A. Lior, "Traffic classification and quality of service (QoS) attributes for diameter," 2070-1721, 2010.
- [13] B. Zhang, Y. Li, and Y. Liang, "Impact of Packet Size on Performance of TCP traffic with Small Router buffers," in MATEC Web of Conferences, 2017, vol. 128: EDP Sciences, p. 02023.
- [14] L. Atzori et al., "SDN&NFV contribution to IoT objects virtualization," Computer Networks, vol. 149, pp. 200-212, 2019.
- [15] "Virtual Route Forwarding Design Guide", https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cueme/vrf/design/guide/vrfDesignGuide.html
- [16] D. R. Al-Ani and A. R. Al-Ani, "The performance of IPv4 and IPv6 in terms of Routing Protocols using GNS 3 Simulator," Procedia computer science, vol. 130, no. C, pp. 1051-1056, 2018.
- [17] M. M. H. Sabbir, M. T. Islam, S. Z. Rashid, A. Gafur, and M. H. Kabir, "An Approach to Performance and Qualitative Analysis of Routing Protocols on IPv6," in 2019 International Conference on Electrical, Computer and Communication Engineering (ECCE), 2019: IEEE, pp. 1-6.
- [18] R. F. Al Farizky, "Routing protocol RIPng, OSPFv3, and EIGRP on IPv6 for video streaming services," in 2017 5th International Conference on Cyber and IT Service Management (CITSM), 2017: IEEE, pp. 1-6.
- [19] F. L. Lugayizi, N. Gasela, and E. B. Michael, "Performance evaluation of OSPF and EIGRP routing Protocols for video streaming over next-generation networks," Advances in Computer Science: an International Journal, vol. 4, no. 5, pp. 29-35, 2015.
- [20] S. S. Samaan, "Performance evaluation of RIPng, EIGRPv6, and OSPFv3 for real-time applications," Journal of Engineering, vol. 24, no. 1, pp. 111-122, 2018.
- [21] K. El Khadiri, O. Labouidya, N. Elkamoun, and R. Hilal, "Comparative Study Between Dynamic IPv6 Routing Protocols of Distance Vectors and Link States," in 2018 6th International Conference on Wireless Networks and Mobile Communications (WINCOM), 2018: IEEE, pp. 1-6.
- [22] R. Whitfield and S. Y. Zhu, "A comparison of OSPFv3 and EIGRPv6 in a small IPv6 enterprise network," International Journal of Advanced Computer Science and Applications (IJACSA), 2015.
- [23] Z. Ashraf and M. Yousaf, "Optimized Routing Information Exchange in Hybrid IPv4-IPv6 Network using OSPFv3 & EIGRPv6," International Journal of Advanced Computer Science And Applications, vol. 8, no. 4, pp. 220-229, 2017.
- [24] K. El Khadiri, O. Labouidya, N. El Kamoun, and R. Hilal, "Study of the Impact of Routing on the Performance of IPv4/IPv6 Transition Mechanisms," in International Conference on Advanced Information Technology, Services and Systems, 2018: Springer, pp. 43-51.
- [25] S. U. Masuroh, A. Fiade, and M. F. Iman, "Performance evaluation of routing protocol RIPv2, OSPF, EIGRP with BGP," in 2017 International Conference on Innovative and Creative Information Technology (ICITech), 2017: IEEE, pp. 1-7.
- [26] G. P. Xavier and B. Kantarci, "A survey on the communication and network enablers for cloud-based services: state of the art, challenges, and opportunities," Annals of Telecommunications, vol. 73, no. 3-4, pp. 169-192, 2018.
- [27] J. J. Yu, "Scalable routing design principles," 2000.
- [28] D. Savage, J. Ng, S. Moore, D. Slice, P. Paluch, and R. White, "Cisco's Enhanced Interior Gateway Routing Protocol (EIGRP)," 2070-1721, 2016.
- [29] R. Sharma and N. Yadav, "Implementation of Open Shortest Path First Version 3 (OSPFv3) with Encryption and Authentication in IPv6 Network," in International Conference on Computer Networks and Communication Technologies, 2019: Springer, pp. 767-776.
- [30] Y. Rekhter, "RFC 4271: A border gateway protocol 4 (BGP-4)," <http://www.ietf.org/rfc/rfc4271.txt>, 2006.
- [31] H. Saini and A. K. Garg, "Performance Analysis of OSPF Routing Protocol Under Single and Multiple Link Failure," in International Conference on Recent Developments in Science, Engineering and Technology, 2017: Springer, pp. 450-458.
- [32] R. Petija, M. Michalko, F. Jakab, and P. Fecil'ak, "Convergence of Routing Protocols in Real and Simulated Environments," in 2018 16th International Conference on Emerging eLearning Technologies and Applications (ICETA), 2018: IEEE, pp. 425-430.
- [33] J. Wang and Y. bin Hou, "Packet loss rate mapped to the quality of experience," Multimedia Tools and Applications, vol. 77, no. 1, pp. 387-422, 2018.

Authors' Profiles



Zeeshan Ashraf is a Ph.D. scholar in IQRA University Islamabad Campus, Islamabad, Pakistan.

He has done MSCS with a specialization in computer networks from UMT, Lahore, Pakistan. He has more than 10 years of experience in the IT field. He is CISCO CCNP (R&S) certified. He is the author of several books. His research articles have been published in well-reputed International Journals and Conferences. Currently, he is serving as a permanent faculty member of the Computer Science and IT department at The University of Lahore Gujrat Campus, Gujrat, Pakistan. His main research interests include next-generation virtualize Internet architecture, IPv6 routing, performance modeling, optimization techniques, and security.



Adnan Sohail has received a Ph.D. degree in Electrical Engineering and Information Technology from the Institute of Telecommunications, Vienna University of Technology, Vienna, Austria. He has completed his Masters in Computer Science, Bahria University Islamabad, Pakistan.

During Ph.D. studies, his research focus was on performance modeling and evaluation of network access nodes. Currently, he is serving as an Assistant Professor in the Computing and Technology department of IQRA University Islamabad Campus, Islamabad, Pakistan. He also served as an Assistant Professor in CUI and IIUI Pakistan. His main research interests are performance modeling and analysis of communication networks, optimization techniques, quality of

service of communication networks.



Muhammad Yousaf is an associate professor and head of the Department of Cybersecurity and Data Science, Riphah Institute of Systems Engineering, Riphah International University, Islamabad, Pakistan.

He completed his MS Computer Engineering and Ph.D. Computer Engineering from CASE, University of Engineering and Technology, Taxila, Pakistan in 2006 and 2013 respectively. His research interests include Cryptography, Network Security, Cybersecurity, Network Forensics, Traffic Analysis, Secure Infrastructure Design, and Security Management.

How to cite this paper: Zeeshan Ashraf, Adnan Sohail, Muhammad Yousaf, "Performance Analysis of Network Applications on IPv6 Cloud Connected Virtual Machine", International Journal of Computer Network and Information Security(IJCNIS), Vol.11, No.12, pp.1-9, 2019. DOI: 10.5815/ijcnis.2019.12.01