IJCTA, 9(21), 2016, pp. 87-96

Analyzing for Performanc Factors in Cloud Computing

Shweta Singh* Arun Kumar Tripathi**

Abstract : A need to an on-demand services and maintenance-free architecture is encouraged in current's scenario. Cloud computing is one the emerging technology that is providing opportunities to number of users and even for numbers of enterprises. Since it need no or minimum costs involving maintenance and management of resources while communication is established, this feature lead to its greater success in an IT world. In such environment, a user is allowed to make access to required service and resources with a fact of 'any-time and any-quantity' basis. To accomplish the goals for increased performance, OPNET IT GURU EDUCATION VERSION 14.5 is being used. The performance metrics such as queuing delay, packet latency and throughput will be analyzed to check for increased or decreased utilization in the proposed scenarios.

Keywords : Cloud Computing, Fragmentation Threshold, PPP, Digital Signal, Internet Protocol, IP Routing Protocol, IPv4, IPv6, RIPng, OSPF, IS-IS, Queuing Delay, Packet Latency, Throughput.

1. INTRODUCTION

On taking into consideration for growing needs of each of enterprises and individual users, a technology known as Cloud Computing [1] has emerged. Cloud computing as a technology provides its users to make access to desirable resources which are made to share in a cloud-based network. A virtual on-demand computing facility is provided where multiple users can communicate and access applications with distant geographical locations.

A pool of resources is maintained and is made to be used whenever a user is connected to a cloud environment. The resources and applications are shared to the necessary one at any-time and any quantity basis. This virtual-cloud environment provides enterprises to perform a speed-up access and adjust numbers of resources in meeting their fluctuating needs more rapidly. This feature of pooling resources and services on an on-demand basis lead to a gradual increase in usage for cloud computing, and also it doesn't need to be maintained and managed or implemented with large costs involving such complex architectures.

Following features of cloud computing encouraged its growth in an IT world, some can be as: scalability, availability, cheaper cost for services, high performance, and accessibility of resources, etc. including an automatic failure recovery service.

Since, cloud computing is an on-demand technology and so it follows strictly the architecture of Service-Oriented Architecture (SOA) [2]; and is evolved by reliability problems and Quality-of-Service (QoS) [3]. Cloud computing is an aspect of SOA that helps user to come out or break though these problems and provide solution in an integrated manner. SOA provides a standard manner to cloud computing to make an access to services on cloud easily and globally.

Cloud computing has other characteristics too in fields such as: Device independence, location independence, agility, cost reduction, maintenance, performance, scalability, elasticity, productivity, security, reliability. Five essential terminologies of cloud computing can be as following:

* KIET Group of Institutions, Ghaziabad, India shweta.vidudi272@gmail.com

** KIET Group of Institutions, Ghaziabad, India mailtoaruntripathi@gmail.com

1.1. On-demand self-service

This service is accomplished on an automatic basis that needs no human intervention to make access through network storage.

1.2. Resource pooling-

A pool of all the shared resources is maintained so that dynamically needs for multiple users can be fulfilled.

1.3. Broad network access-

The capability of network is distributed over different platforms consisting of mobile phones, laptops, etc.

1.4. Rapid elasticity

Capabilities can be anytime increased and decreased as per the user's demand. Demands are appreciated at any time at any quantity basis.

1.5. Measured service-

This facilitates a service under which a list of resources and their availability is automatically managed and optimized for both the consumer and provider of service.

Wireless Local Area Network (WLAN) [4] is one of the network types which strictly follow concepts of a distributed system. A cloud network is in some sense a distributed network onto which resources are being shared; services are being accessed involving distant geographical locations for each to store and access.

The architecture for WLAN can include the following three:

1.6. Stations

Mainly two devices are involved in WLAN communication i.e. Access Point (AP) [4] and clients.

1.7. Basic service Set

Basic Service Set (BSS) [4] include the list of stations that are intended to communicate with the appropriate AP in any network segment.

1.8. Extended Service Set-

Extended Service Set (ESS) is used for further distribution of particular network segment.

1.9. Distributed System-

Distributed Systems (DS) is used to extend the network coverage for AP in ESS while roaming.

Furthermore, the paper is sectioned under following headings: II. Digital Signal, Internet Protocols (IP) [5], Routing Internet Protocol (RIP) [6] and its types. III. Simulation process i.e. defining scenarios to analyze; two scenarios are made: Simple Internet Protocol version-6 (IPv6) [5] and IPv6 with Fragmentation Threshold [4]. IV. Analysis report for two proposed scenarios i.e. discussing about the performance of network in each of the scenario. V. Conclusion and References about text and idea.

2. USEFUL WORK

Cloud computing is usually a technique that relies on a distributed environment. By distribution of environment, we meant that there would be different network segment; there would be one centralised autonomous network segment which will be responsible to maintain all the applications for number of its users, and also to facilitate a reliable access to the shared resources. Distribution of each of the resources and applications is relevant today because this technology establishes a convenient manner to perform networking or related purposes. Through cloud computing this accessibility to work within a distributed environment has reached to its way to success. Each

of the network segments is made to attach via a peer-to-peer linking mechanism. This link is generally used to establish communication in between each network segment by following a protocol set i.e. Point-to-Point Protocol (PPP) [7].

PPP is a protocol that belongs to data link (layer 2) in an OSI model. PPP protocol is mainly used to connect two devices and make them eligible enough so that they can communicate. PPP provides with three aspects that describes higher levels of reliability, such as transmission encryption, connection authentication and compression techniques. The two basic types of carrier systems can be:

2.1. Digital Signal 1

DS-1 is also known as T1 line. DS1 is just a bit pattern on a physical T1 link. It follows a serial bit rate of 1.544 Mbps.

2.2. Digital Signal 3

DS-3 is an extended version of DS-1 carrier, it is commonly known as T-3 carrier. DS-3 in a simpler way is combination of several DS-1 carrier lines, providing with a greater data rate *i.e.* 44.736 Mbps and consisting of at-most 28 T1 channels.

To establish a communication or rather a valid and efficient communication between one or more connected devices, it is necessary to assign some sort of address formats and to specifically define an appropriate destination and source devices in a network. IP is the principle format to specifically address any number of devices and in any network as an individual device of an individual network. IP sets boundaries to any network, defining a geographical boundary to each network so that data packets can clearly be justified on their address basis. Mainly every data packet consists of three sections i.e. source address, destination address and information or message section. These three sections are encapsulated in a packet that can follow any addressing format. The two formats for IP can be:

2.3. IPv4

Internet Protocol version-4 (IPv4) [5] is a fourth version of IPs. IPv4 supports connectionless environment to operate and relies on a packet-switched network type. One of the drawbacks of this protocol is that it doesn't guarantee for successful or duplicate delivery of data packets. These factors lead to an exhaustion to 32-bit IPv4, and was replaced by a newer version of data packet addressing format i.e. IPv6 format.

2.4. IPv6

IPv6 is a sixth version for IPs. It is an extended version for IPv4 encapsulating scheme. It supports 128-bit address format rather than just 32-bit address format. With the emergence of IPv6 version, numbers of user were facilitated with greater flexibility and larger space requirements were also fulfilled. Along with these factors device mobility, configurations to design and security are also implemented.

IPv6 also facilitates a combination of set of regulations or protocol set, so that an efficient communication is achieved every-time. RIP is one of the routing protocols encouraged in generally an IPv6 environment. RIP employs a distance vector routing analysis for every-while a data packet is to be sent. RIP works by taking in consideration of limited number of hops between any two pairs of devices; an entry is maintained for every route discovery through preference choices developed in routing tables. Routing tables are maintained and managed every-time an update is done in a route while any route failure has occurred. RIP is based on mechanism followed by User Datagram Protocol as transport protocol.

Besides usage of RIP, several other versions are also encouraged to ensure highest levels of routing and efficient working environment. These can be as follows:

2.5. RIPng

It is one of the versions of RIP protocol. Additional authentication is provided by this protocol to an IPv6 environment.

2.6. OSPF

Open Shortest Path First (OSPF) [6] or interior routing protocol usually operates for an autonomous network. It is most widely used protocol by numbers of enterprise networks supporting IPv6 protocol. A topological structure helps in developing defining link availability and its reliability.

2.7. IS-IS

Intermediate System-Intermediate System (IS-IS) [8] protocol relies on maintaining our best possible ways to route each encapsulated data packet to its destined device. This is done by moving into a network where devices are linked via physical aspects by using a packet-switched transfer mechanism.

3. SIMULATION

This section is the basis for making an appropriate comparison between one or more different configurations for different scenarios. The simulation is conducted on the basis of proposed scenarios for each of them supporting IPv6 environment so that appropriate working mechanism can be attained.

The simulation environment for both the two scenarios differ by their set configurations, including one with simple protocols set and other with included additional functionality that efficiently uses bandwidth.

Both the environments consist of an IP Cloud that further connects several autonomous segments of a network with each other and allows them to make access to provided applications, shared resources. Every autonomous segment has 16 wireless stations that are connected through two routers are made to move in a network with fixed trajectories for each station i.e. each station is made as Mobile Node. Each router is enabled with the BSS and acts as Home agent to every Mobile Node. Each group of 8 stations is only communicating to the associated BSS. The routes are made to connect to outer network via firewall, followed by two routers for each inner and outer network. Two Cisco 4000 routers [9] are being used to filter and to assure reliability in communication. Cisco 4000 routers are used here as they are the most powerful routers till date. They provide higher levels of performance. Largely, these routers have been encouraged by business enterprises because they save money for them by accomplishing all its work done in just few minutes. Also, they can automate their configuration, management and monitoring methods for the network. DS-3 links are being used to connect each of the Cisco 4000 routers to the other networks through an IP Cloud.

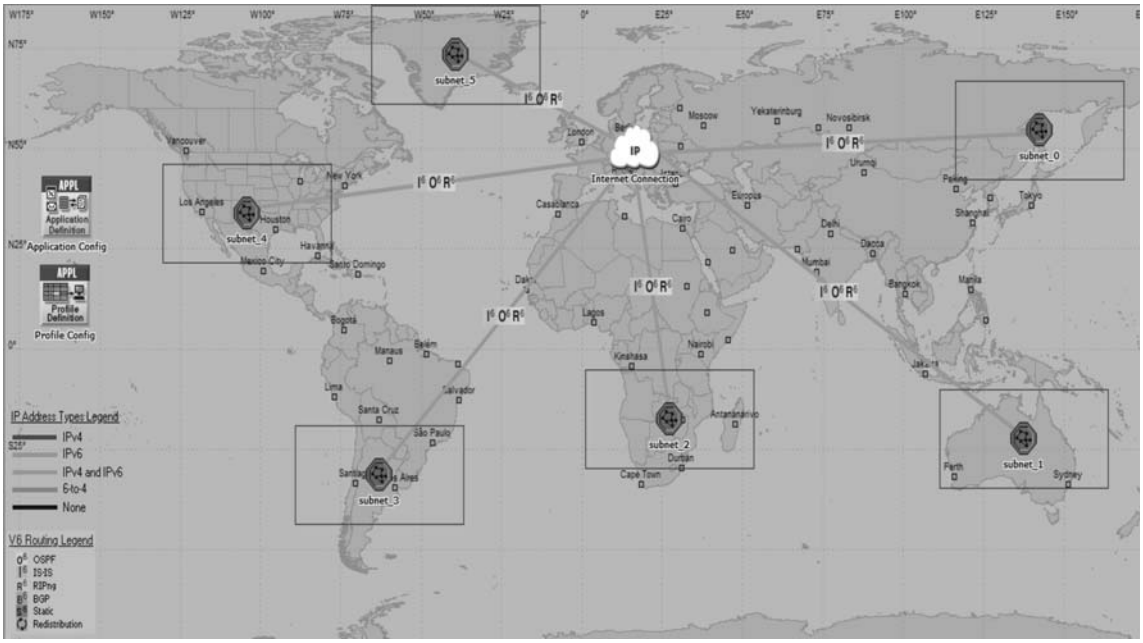

Fig. 1. Internet Connection following cloud-based network

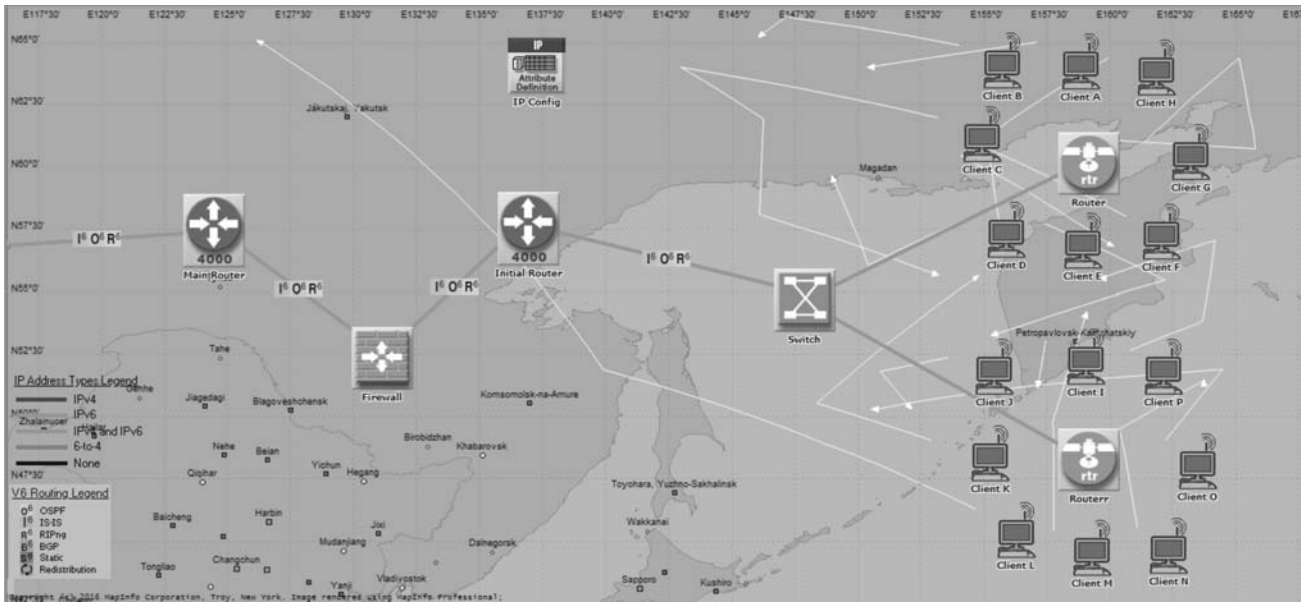

Fig. 2. An Autonomous Network Segment

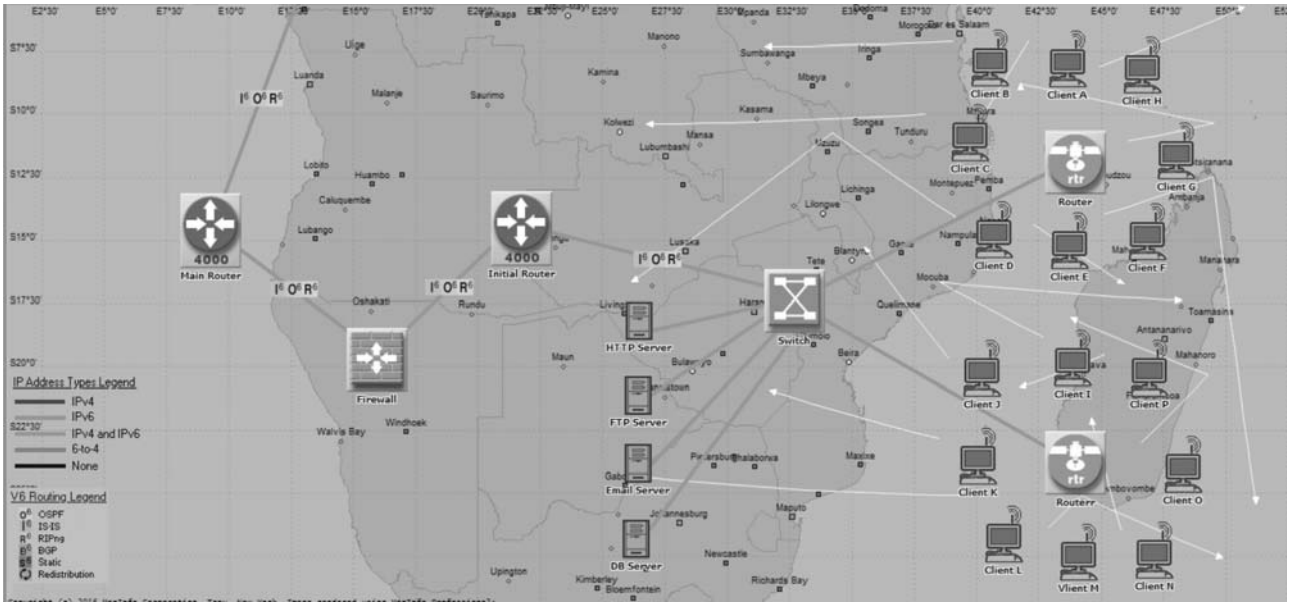

Fig 3. Autonomous Network defining Applications

Two scenarios are made that explains the best possible ways to justify an architecture needed to compute in a cloud computing technology. The two scenarios can possibly be:

3.1. Simple IPv6 with stations in Mobility

In this scenario, IPv6 architecture is implemented. All the devices are communicating in IPv6 environment and are strictly following IPv6 addressing formats. Three protocols are also implemented for each and every station i.e. RIPng, OSPF, and IS-IS so that performance level is improved. Along with this, all stations are made moveable such that they are allowed to roam while communication in a cloud network.

3.2. IPv6 with fragmentation threshold with stations in Mobility

This scenario is an extended version to the first scenario. Along with three listed protocols set and mobility in nodes, one more functionality is introduced here, *i.e*. fragmentation threshold. In fragmentation threshold property, the bandwidth [4] is being divided into fixed length units which are then utilized by all the available devices in that network.

Figure 1, 2, 3 represents the divisions of simulation environment *i.e.* architecture to a parent network, a simple autonomous segment and with application servers.

4. ANALYSING THE SIMULATION

This section is representing analysis for the proposed scenarios in simulation environment. Performance of both the proposed scenarios is measured on certain parametric basis, these would be: queuing delay, packet latency and throughput. These factors are analyzed to measure possible performance statistics for communications held in between the inter-connected devices in each of the network segment. The analysis will be showing metrics for Internet connect and Firewall devices in two subnets (Subnet 2 and Subnet 5).These two subnets are only chosen for analysis because one of the subnets is made as server subnet and other one is a normal one. The analysis would be as follows:

4.1. Queuing Delay

Queuing Delay [10] is defined as an amount of time spent by a data packet in a queue to reach to its assigned destination device. The amount of time before time out has occurred to reach a packet to its destination covers queuing delay. Fig. 4, 5 represents the queuing delay in an IP Cloud and firewall device in both the scenarios.

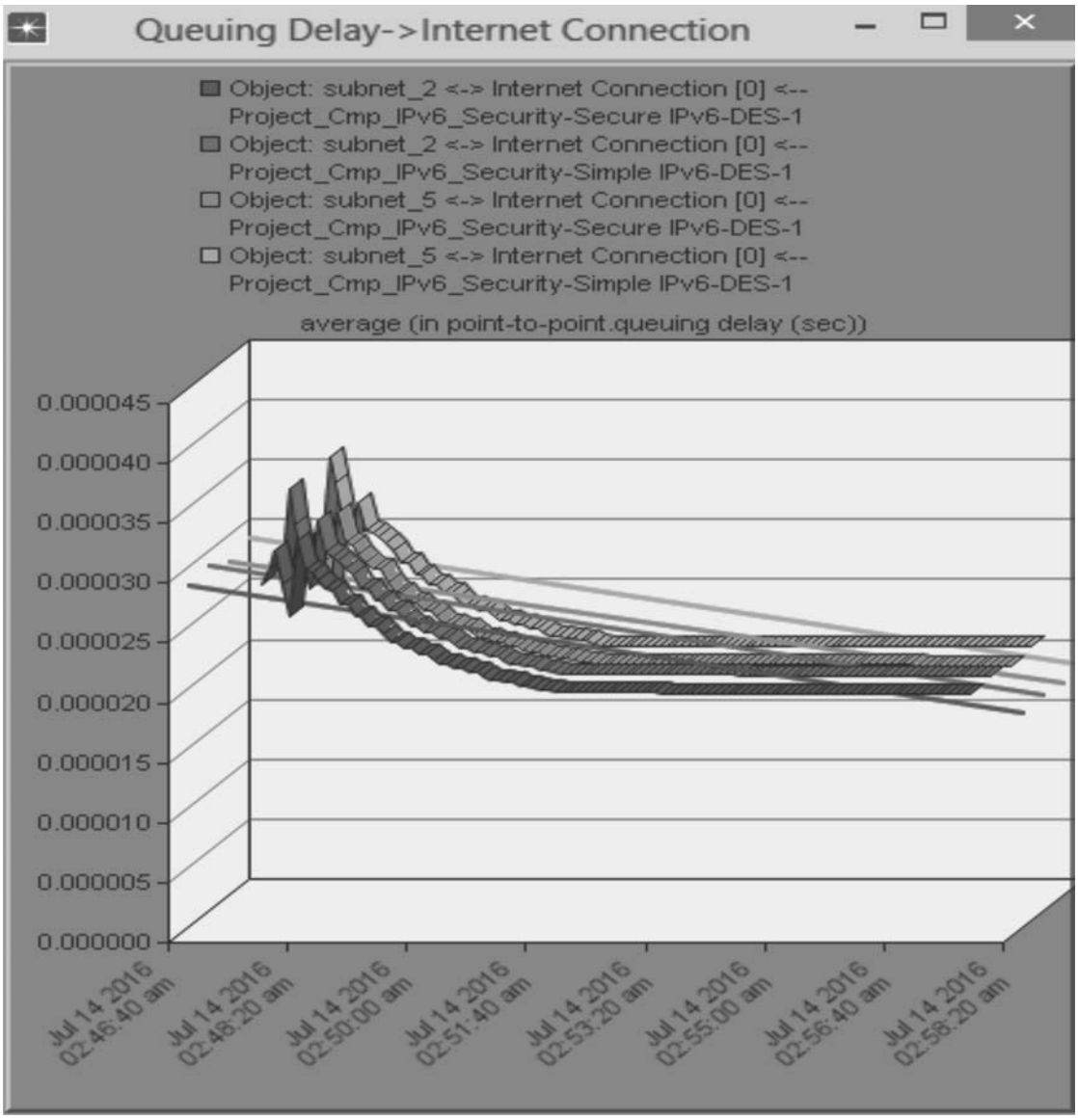

Fig 4. Internet Connection (Subnet 2 and Subnet 5): Queuing Delay

Fig. 4 is depicting a queuing delay in an Internet Connection for two subnets. From above generated graph a conclusion can be achieved that there is slightly any difference between the performances of two scenarios. But then too it can be analysed that an IPv6 environment with fragmentation for bandwidth performs much better and is encountered with reduced queuing delay.

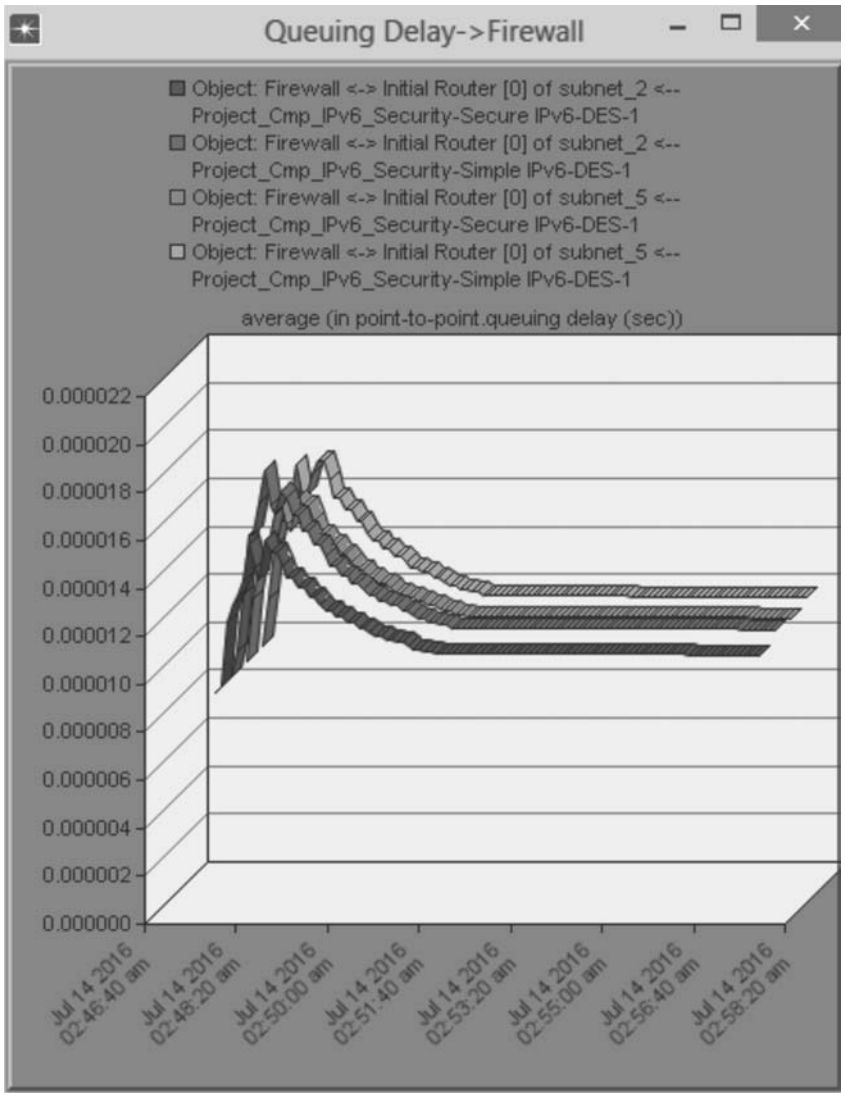

Fig. 5. Firewall (Subnet 2 and Subnet 5): Queuing Delay.

Fig. 5 depicts queuing delay for firewall in both the subnets following different configurations. It has been analysed from graph that both scenarios acted same at the beginning, but as soon as numbers of data packet are increased with respect to time the delay has reduced when fragmentation strategy has established. The fragmentation allows several devices to communicate in a more reliable manner then with the normal manner to transmission.

4.2. Packet Latency

Packet latency [11] is the amount of time spent by the data packet to reach from its source to destination device, but other than the normal delay (queuing delay). The extra time spent by the data packet to reach to its destination for accessing is termed as packet latency. Fig. 6 represents packet latency for Internet Connection in both the scenarios.

Fig. 6 represents packet latency in an Internet Connection. In graph, it can be easily classified as there are positive results for IPv6 environment with fragmentation threshold. This property of fragmentation doesn't allow multiple users to broadcast data packets while other devices are communicating. One big advantage of this is that an efficient and flexible platform is achieved and hence latency in accessing every data packet is reduced.

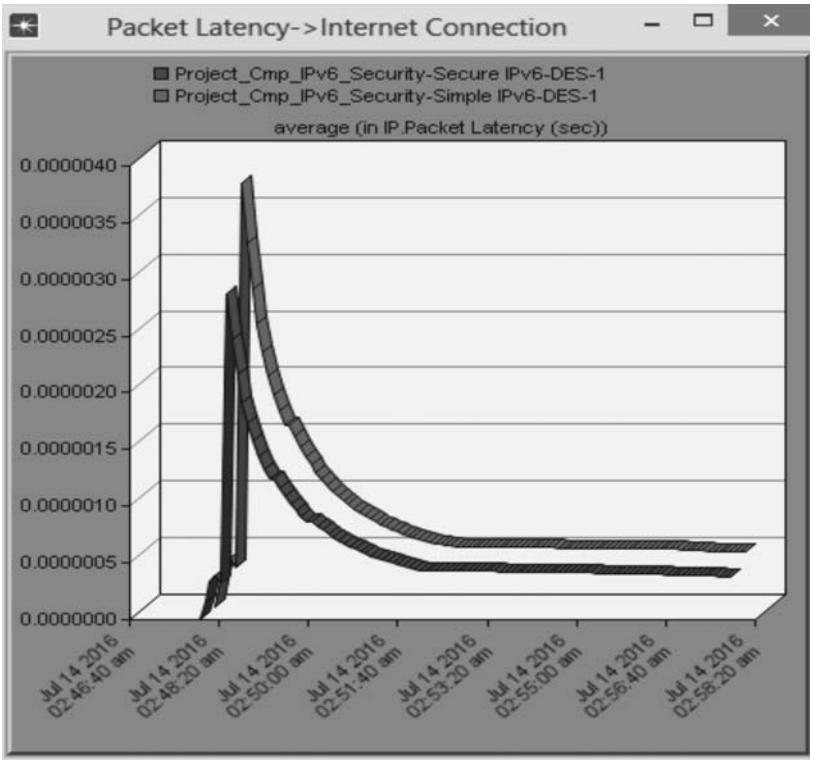

Fig. 6. Internet Connection: Packet Latency

4.3. Throughput

Throughput [12] is defined as rate of performance for any proposed network. For every successful communication of delivery of data packet a throughput is gained. The factor throughput is directly proportional to the utilization factor, the higher the throughput rate is; the higher will be the utilization of network. Fig. 7, 8 represents throughput for Internet Connection and Firewall in both the scenarios.

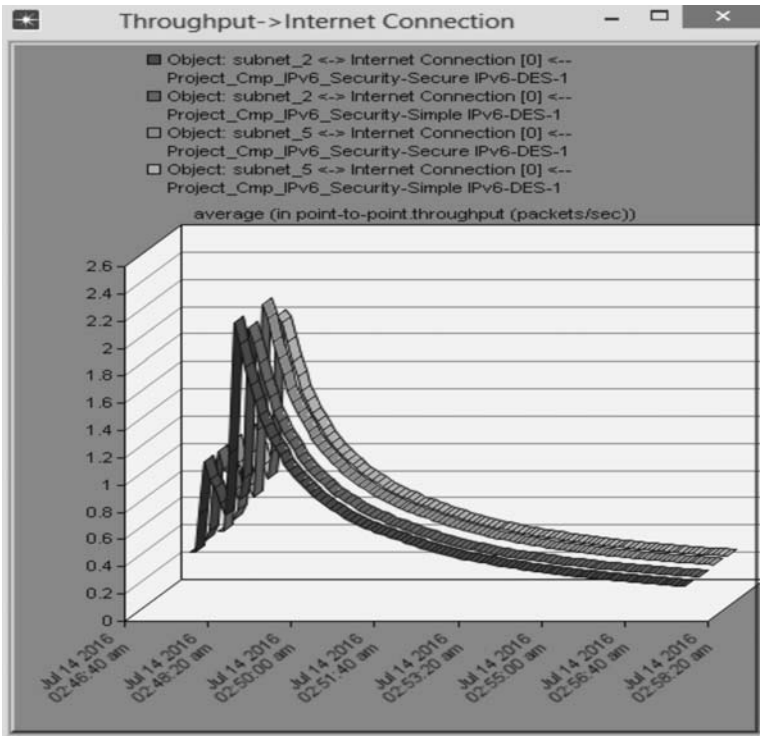

Fig. 7. Internet Connection (Subnet 2 and Subnet 5): Throughput

Fig. 8 represents throughput factor in Internet Connection for two named subnets. It can be clearly justified by the graph so generated that when device configuration is completely changed to IPv6 addressing scheme, an increased throughput is achieved. One more reason for this can include the fragmentation property that is set to bandwidth, hence saving space for others to communicate in mean time.

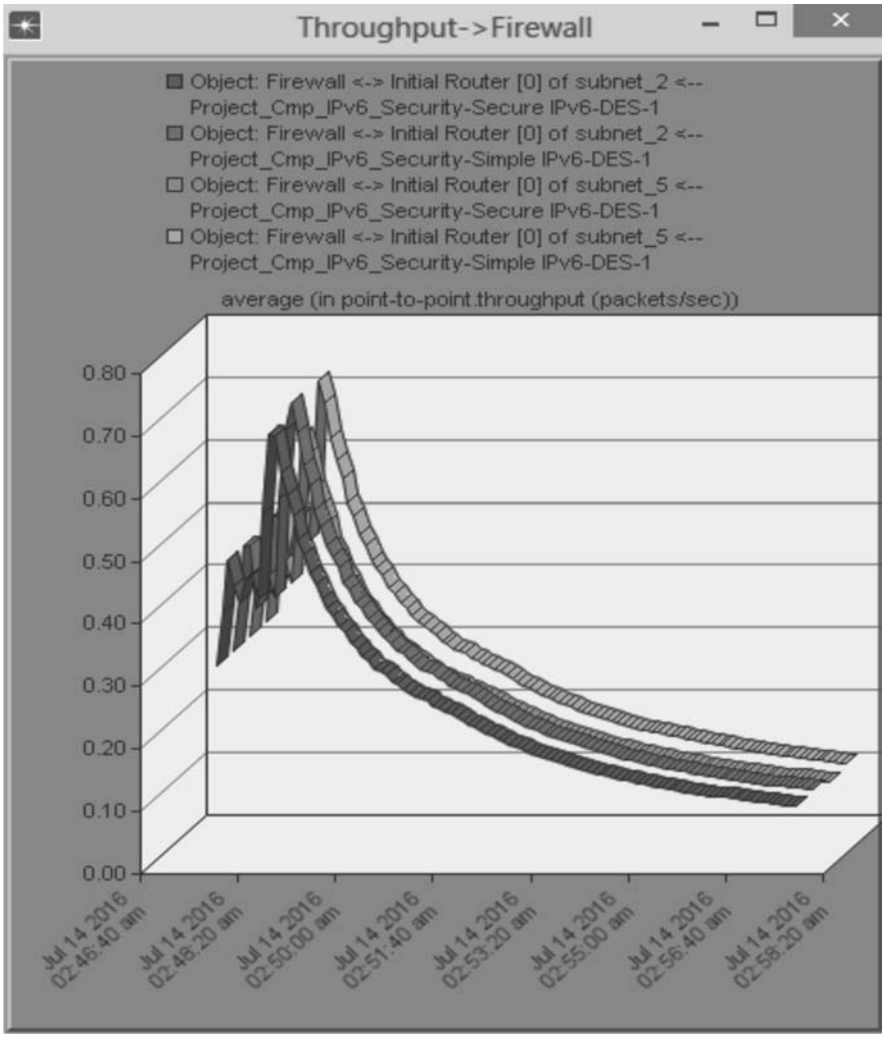

Fig. 8. Firewall (Subnet 2 and Subnet 5): Throughput

Fig. 8 represents throughput factor in firewall for two subnets. It can be depicted from above generated graph that initially both the scenarios acted as equal, but as number of packets are increased along with time, the performance for simple IPv6 has gradually increased, and this is because it is not implemented with only RIP and need to perform any additional fragmentation process for bandwidth, hence saves its time in sending and receiving data packets.

5. CONCLUSION

The overall purpose for simulation and analysis is based to measure performance of IPv6 protocol under different configurations consisting different scenarios. The above simulation shows performance of mobile stations following an IPv6 addressing format. It is analysed that when RIP, OSPF and IS-IS protocols are engaged with an IPv6 environment, a more higher levels for utilization, increased throughput and reduced throughput is attained. But when fragmentation threshold is also introduced with the existing configuration, not too explicit, but a difference in performance it attained. It can be clearly seen by so generated graph that when bandwidth is being fragmented and is used in a more efficient manner, there is a gradual increase in throughput for engaged devices while communication. Another reason behind increased utilization is availability of bandwidth in the mean-time so that delay is reduced and data packets are communicated in desired time duration.

6. REFERENCES

1. Rajkumar Buyya: "Introduction to the IEEE Transactions on Cloud Computing", Ieee Transactions On Cloud Computing, Vol. 1, NO. 1, ISSN NO: 2168-7161, Jan-June 2013, pp: 1-19

2. I. Jerstad , S. Dustdar, D. V. Thanh: "A service oriented architecture framework for collaborative services", 14th IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprise (WETICE'05), ISBN No.: 1524-4547, June 2015, pp: 121-125.

3. R.K.Nadesh , D.Sumathy, M. B. BenjulaAnbu Malar, "Performance Analysis Of MANET (WLAN) Using Different Routing Protocols In Multi Service Environments-An Quantitative Study", Int. J. Advanced Networking and Applications Volume: 03, Issue: 02, Pages:1076-1079 (2011).

4. Shweta Singh and Arun Kr. Tripathi: "Analysis of Delay and Load Factors in Wired and Wireless Environment", Second International Conference on Recent Trends in Science, Technology, Management & Social Development (RTSTMSD-15), IJSTM, ISSN NO: 2250-0596, Dec-2015, PP. 1-8.

5. Eun-Young Park, Jae-Hwoon Lee, Byoung-Gu Choe: "An IPv4-to-IPv6 dual stack transition mechanism supporting transparent connections between IPv6 hosts and IPv4 hosts in integrated IPv6/IPv4 network", communications, 2004 IEEE International Conference on (volume:2), ISBN No.: 0-7803-8533-0, June 2004, pp. 1024-1027.

6. Ioan Fiþigãu, Gavril Toderean, "Network performance evaluation for RIP, OSPF and EIGRP routing protocols", 2013 International Conference on Electronics, Computers and Artificial Intelligence (ECAI), ISBN No.: 9778-1-4673-4935-2, June 2013, pp: 1-4.

7. M. W. Youssef, Hazem El-Gendy: "Securing Authentication of TCP/IP Layer Two By Modifying Challenge-Handshake Authentication Protocol", Advanced Computing: An International Journal (ACIJ), Vol.3, No.2, ISSN No.: 2012-3202.

8. Jagmeet Kaur, Er. Prabhdeep Singh: "COMPARATIVE STUDY OF OSPFV3, ISIS AND OSPFV3_IS-IS PROTOCOLS USING OPNET", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 8, ISSN No.: 2278 – 1323, Aug 2014, PP: 2656-2662.

9. http://www.cisco.com/c/dam/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/whitepaper_c11-732909.pdf.

10. Jahwan Koo, Seongjin Ahn, Jinwook Chung: "A COMPARATIVE STUDY OF QUEUE, DELAY, AND LOSS CHARACTERISTICS OF AQM SCHEMES IN QOS-ENABLED NETWORKS", Computing and Informatics, Vol. 22, 2003, PP: 317–335.

11. G.M.Tamilselvan, A.Shanmugam: "EFFECT OF INTER PACKET DELAY IN PERFORMANCE ANALYSIS OF COEXISTENCE HETEROGENEOUS WIRELESS PACKET NETWORKS", International Journal of Network Security & Its Applications (IJNSA), Vol 1, No 2, July 2009, ISSN No.: 1004-0596, PP: 40-49.

12. Shweta Singh, Naresh Chandra, and Arun Kr. Tripathi, "Performance analysis for Channel Utilization in Wireless LAN", International Journal of Computer Applications (IJCA), Vol. 122(20), ISSN No. : 0975 – 8887, July 2015, PP. 40-44.