International Journal of Computing and Network Technology
ISSN 2210-1519
Int. J. Com. Net. Teach. 2, No. 3 (Sept. 2014)

# Performance Analysis of Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) over MPLS

**Firdous Ahmad Khan, Falak Reyaz Wani, Mohammad Ahsan Chishti**

*Computer Science and Engineering, National Institute of Technology Srinagar, Kashmir, India*

*Received: 5 Apr. 2014, Revised: 13 Aug. 2014, Accepted: 20 Aug. 2014, Published: Sept. 2014*

**Abstract:** Exhaustion of the address space of current version of Internet Protocol (IPv4) actuated the development of next-generation Internet Protocol version 6 (IPv6). Even though the deployment of IPv6 has not progressed as per the predictions given by the technologists, primarily the reason being lack of awareness about IPv6 as well as the technical immaturity of people about the same as compared to IPv4. Now for IPv4 and IPv6 to coexist, various IPv6 transition mechanisms have been developed, in addition to that Multiprotocol Label Switching (MPLS) is a switching technology that regulates data traffic and packet forwarding in a complex network to make data forwarding decisions. The various applications of MPLS are VPN'S (Virtual Private Network), TE (Traffic Engineering), QoS (Quality of Service), AToM (any transport over MPLS). Nowadays keeping in view the explosive growth of Internet Traffic, primarily the cause being high definition audio/video, and multicast routing protocols are run over unicast routing protocols to provide efficient routing of such applications. This unicasting and multicasting has been proven to be efficient with minimum delay than the traditional IPv4 and IPv6 networks. In this paper, we compare the MPLS enabled networks with the traditional networks (IPv4/IPv6) for unicast and multicast traffic, and also the routing protocol comparison is shown by employing different routing protocols like RIP, OSPF, IGRP and EIGRP over the MPLS network. Simulation environment was created to evaluate the comparative performance of network traffic behavior. The results of the simulation conclude that MPLS enabled networks perform better than the traditional networks with lesser Jitter, lesser delay and better throughput.

**Keywords:** Unicast, Multicast, IRP, MPLS, IPv4, IPv6

## 1. INTRODUCTION

The advancements in the hardware technology over the last few years had positive impact on the rapid growth of Internet. The Internet as it started of as an experiment has grown to the worldwide chain of connected networks. Today large number of users subscribe to online multimedia services such as audio/video streaming, Video conferencing and messenger services such as Skype, Whatsapp, Google Hangouts and Facebook are replacing traditional phones for long distance calls across urban areas in many countries. In the present era, Information exchange can be mainly classified as unicast (one-to-one), broadcast (one-to-all) and multicast (one-to-many). In unicast transmission (Figure 1), individual packets are sent to all the desired recipients on a network which differs from broadcast wherein packets are sent to all the recipients on a network. However the multicast server sends out just one packet and the router then generates multiple packets to reach each of the receivers having same multicast group address. A typical example of multicasting is Facebook messenger where multiple hosts subscribe to the service and the server communicates only with those hosts that have subscribed to it. The most important advantage of multicasting is the bandwidth conservation as the network resources are used efficiently.Also, multicasting ensures timely reception of the data by the receivers [1]. A more recent variation of multicast is any cast wherein one to nearest association phenomenon is employed. There may be multiple recipients of an any cast message, but the sender sends the message only to the node that is logically or topologically the closest to it as shown in Figure 1.Multi-Protocol Label Switching was originally introduced in 1970s by several Internet engineers with the initial purpose of getting rid of the drawbacks in packet switching mechanism, in which every packet's header should be read and analyzed before sending it out for the right destination [2]. Also its core technology can be extended to multiple network protocols, such as IPv6, Internet Packet Exchange (IPX), and Connectionless Network Protocol (CLNP).

After almost 20 years MPLS was received and confirmed by the IETF in 1990[3]. MPLS technology is actually performed between the L2 and 3 networks,

*E-mail: firukhan.98@gmail.com, falakreyaz@gmail.com, ahsan@nitsri.net*

which makes it to be called the L2.5 technology. It uses short labels (20 bits) rather than longer IP addresses (32 bits in IPv4 and 128 bits in IPv6). There are 4 segments in an MPLS header: Label [4], EXP, S and TTL [5]. Label is a fixed length, four-byte identifier that identifies a Forwarding Equivalence Class (FEC); EXP is often preserved for special usage, such as in QoS operation. S is the indicator for bottom label; and TTL is short for Time to Live, shows how far the header could travel along the route. The central idea of MPLS is to attach a short fixed length label to packets at the ingress router which is basically the starting edge router of the MPLS domain.

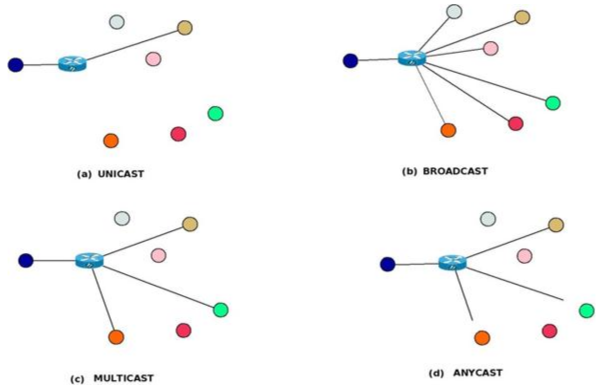
(a) UNICAST (b) BROADCAST (c) MULTICAST (d) ANYCAST

**Figure 1. Unicast, Broadcast, Multicast, and Any cast**

Packet forwarding then depends on the tagged label, not on longest address match, as in traditional IP forwarding. A router placed on the edge of the MPLS domain, named Label Edge Router (LER) that is associated to a label on the basis of Forwarding Equivalence Class (FEC). In the MPLS network, internal routers that perform swapping and label-based packet forwarding are called Label Switching Routers (LSRs). The label switching technique is not new. Frame Relay and ATM (Asynchronous Transfer Mode) use it to move frames or cells throughout a network. The similarity between Frame Relay and ATM is that at each hop throughout the network, the “label” value in the header is changed. The fact that the MPLS labels are used to forward the packets and no longer the destination IP address has led to the popularity of MPLS [6]. The benefits such as the better integration of IP over ATM and the popular MPLS virtual private network (VPN) application make MPLS a hot field of research. Figure 2 illustrates a backbone network composed of IP core routers surrounded by Provider Edge (PE) routers that are, in turn, connected to the global Internet and/or private VPNs [7].

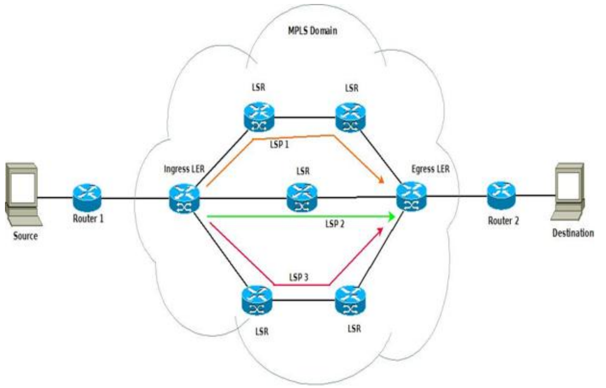

**Figure 2. MPLS Network**

Forwarding Equivalence Class (FEC) is a concept defined such that the packets that belong to a class based on any combination of source address, destination address, source port, destination port, protocol type and VPN are forwarded with the same treatment across the MPLS domain. Label switching router (LSR) is a fundamental component on an MPLS network. All routers in the MPLS domain capable of label switching are called as Label Switching Routers. Label Switching Path (LSP) functions much like a virtual circuit in ATM or frame relay. It is a unidirectional path from the ingress edge router of the MPLS domain to the egress edge router. The Label Distribution Protocol (LDP) classifies FECs, distributes labels, and establishes and maintains LSPs. It is used by MPLS for control. An LDP functions in the same manner as signaling protocols do on traditional networks.

In this paper we compared jitter, delay and throughput for traditional networks with and without MPLS. Four scenarios were created in each case for IPv4, IPv6, MPLS IPv4 and MPLS IPv6. Also the delay that results by changing various routing protocols RIP, OSPF, IGRP, EIGRP has been shown as well.

## 2. LITERATURE SURVEY

The internet since its inception used IPv4 [8] protocol, which provides 2^32 [4.3 billion addresses] distinct addresses. The exponential growth in demand for IP addresses (unique numbers to ensure the identification and location of network equipment) made the Internet address exhaust faster than it was expected, to the level that the first prediction of the end of the Internet was published in 1994[9]. Emergency measures were immediately sought and applied individually or jointly to look for alternative workarounds and fix-ups. These measures included the exceptional allocation of "Class B", address blocks, the reuse of “Class C” blocks [10], then the abolition of classes in the allocation and routing mechanisms of IP prefixes (CIDR, Classless Internet Domain Routing). Later additions included the "development" of a private address space [11], the use of “proxies” or Network Address Translators (NAT). Parallel with this in 1993 the Internet Engineering Task Force (IETF) started the research work for the succession to IPv4.Today we see every person has on an average 2-3 connected devices having unique IP addresses and as the World gets smarter the number is ever increasing much faster owing to the pace of technological advancements. We have roughly some 14 Billion connected devices, that means the IPv4 address space has already exhausted and it is expected that the number of these connected devices is going to go up to more than 50 Billion by 2020[12]. It is very important that we enable IPv6 [13] capabilities on all existing networks as it provides 2^128 addresses (340 trillion trillion trillion unique IPv6 addresses) and in addition to this IPv6 provides more efficient routing, more efficient packet processing, directed data flows, simplified network configuration, support for new services, and improved security [14] but IPv6 adoption has not proceeded as quickly as its designers expected. This is partially due to the perception of the technical immaturity of IPv6 as compared to IPv4. Service providers are highly risk-adverse and are not receptive to new changes so instantly. Additionally, there is a lack of IPv6 awareness and the technical incompatibilities to convert all the network devices to understand IPv6 instantly is another issue that must be met. These factors lead us to look for alternatives that support co-existence of IPv4 and IPv6 addressing schemes in networks.

The basic factor for the development of MPLS was the motivation to simplify wide-area, high performance IP backbone networks. The only viable and reliable solution in the mid 90’s was to use ATM. The addressing schemes used by IP and ATM were mainly orthogonal that led to logical separation of overlays of IP routers which worked over the ATM backbone and ATM just provided wide area connectivity. An IP/ATM network consisted of logical IP subnets (LISs) that were connected by routers [15]. Inter-LIS traffic was routed even when a direct ATM path existed from source to destination. Moreover IP routers were significantly slower than ATM switches and wherever minimization of IP/ATM router hops was possible, it was done by placing all their routers in one LIS [16]. Multiprotocol label switching (MPLS) is the result of convergence of connection-oriented forwarding techniques and the Internet routing protocols [17]. MPLS integrated the high-performance cell switching capabilities of asynchronous transfer mode (ATM) switch hardware with a network using existing IP routing protocols [18]. With advancements in technology packet-based MPLS also emerged to simplify the mechanics of packet processing within core routers, substituting full or partial header classification and longest-prefix match lookups with simple index label lookups.

MPLS solves the IP/ATM scaling problem by making every interior ATM switch an IGRP peer with its neighbors (other directly attached ATM switches or the directly attached IP Routers originally surrounding the single LIS). ATM switches become IGRP peers by having their ATM control plane replaced with an IP control plane running an instance of the network’s IGRP. With the addition of the Label Distribution Protocol (LDP) [19], each ATM switch becomes a core (or interior) LSR, while each participating IP router becomes an edge LSR (or label edge router, LER). Core LSRs provide transit service in the middle of the network, and edge LSRs provide the interface between external networks and the internal ATM switched paths. The demand on the IGRP drops dramatically, since each node now has only as many peers as directly ATM-attached neighbors.

IP multicasting has been around for over two decades now. This section highlights some of the related work that has been conducted in the area of this research. Research in the multicast domain started in the early 80s. Steve Deering invented multicasting and in 1989 RFC 1112 [20] was formulated and the initial works were on IGMP and DVMRP. DVMRP being a distance vector routing protocol had the same shortcomings as those faced by unicast distance vector protocols such as Routing Information Protocol (RIP), where the hop count limited the protocols to be used only in smaller networks. Owing to this shortcoming link state routing protocols soon gained popularity as they could be deployed in larger networks. Open Shortest Path First (OSPF) had its own extension to support multicast called Multicast Open Shortest Path First (MOSPF – RFC 1584) [21]. This protocol failed and is not supported by lead vendors like Cisco [22].

## 3. SIMULATION SCENARIO

OPNET [26] was used to create the topology as shown in figure for both traditional and MPLS networks. The simulation has been developed to emphasize the impact of MPLS over the traditional network. Ppp_adv workstations were used in both the simulations for Unicast & Multicast. The source workstation was configured for Voice & Video Conferencing only. The simulations in two phases, first with background traffic (50Mbps between routers & 10 Mbps in the links connecting workstations & routers) & second one without background traffic was done.

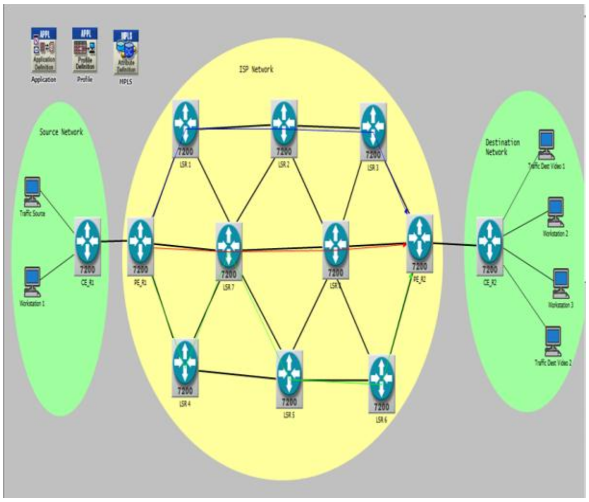

**Figure 3. Simulation Network Scenario**

The following devices and links are used in setting up the desired network:

- IP workstations having model name as ppp_wkstn_adv in the object palette.
- IP routers having model name as CS_7206 in the object palette.
- Links connecting the routers having model name as ppp_OC3.
- Links connecting routers with workstations having model name as ppp_DS3.
- Application configuration, profile configuration and MPLS configuration.

We divided the entire project into 4 scenarios and in each case simulation was done with and without background traffic.

- ➢ Scenario 1. IPv4
- ➢ Scenario 2. IPv6
- ➢ Scenario 3. MPLS IPv4
- ➢ Scenario 4. MPLS IPv6

We carried out simulations in three Phases, altering the configurations only while keeping the scenarios same for all the phases. Unicasting, Multicasting and besides that we changed the Routing Protocols (RIP, OSPF, IGRP, EIGRP). We used dual stack IPv4/IPv6 in both the cases with and without MPLS as well as with the background traffic ones in multicasting topology. As seen from figure 2 we have a single source node and two receiver nodes. The source sends out two separate packets for the two receivers in unicasting case and only one packet in Multicasting case. The packet sent out in multicasting cases is duplicated accordingly as per the number of receivers that are a part of multicasting group by the Rendezvous Point (RP). The group to RP mapping in our network was configured as Static and PE_R2 router was configured as the RP point. The network was successfully run for 1 hour simulation while the elapsed simulation time was 4.40 minutes on an average.

## 4. RESULT ANALYSIS

The network was simulated for multicasting & unicasting traffic, and in both the cases firstly pure traffic was allowed and in second case background traffic was added to the network to check the effect of it on Jitter, throughput and delay. Further all these were done for both IPv4 and IPv6 and lastly the routing protocols (OSPF, RIP, IGRP, and EIGRP) were changed to study there effect on the delay in network. The simulation results are explained below:

**Legend:** For the study of graphs following convention should be followed:

**Table 1. Convention used in graphs**

| | | | |
|---|---|---|---|
| ***Red Line*** | ***IPv6 (EIGRP)*** | ***Blue Line*** | ***IPv4 (OSPF)*** |
| **Green Line** | **MPLS IPv4** (IGRP) | Turquoise Line | **MPLS IPv6** (RIP) |

### 4.1 PACKET DELAY VARIATIONS (JITTER) IN UNICASTING:

During the transmission of packets form source to destination, if the transmission time of different packets from a source to a destination is varying, conceivable glitches in real time traffic were observed. The variation of transmission time from one end to other end is called jitter. Jitter is also the variation in end to end delay or the variation in packet arrival time is also called jitter. Analysis of the graph Figure 4 (without any background traffic) and Figure 5 (with background traffic) shows that there is lot of variations in the jitter in the beginning of the simulation, attributed to the start and setting up of various protocols and different messages for initialization and creation of ARP tables, routing information etc. This is the transient phase of the network. Also it can be seen that in Figure 4 there is a good difference between the jitter between MPLS IPv6 and pure IPv4 network while in Figure 5 the jitter of pure IPv4 is nearly same as that of MPLS IPv6.

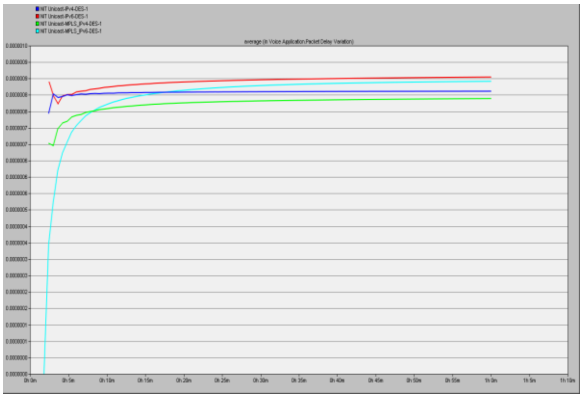

**Figure 4. Packet Delay Variations**

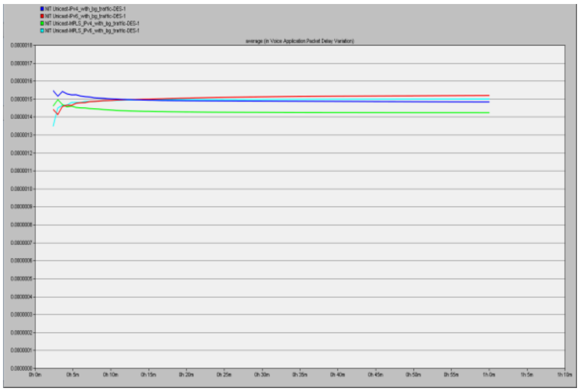

**Figure 5. Packet Delay Variations (with background traffic)**

However in both the cases as the network traffic gets stabilized, we observe that the jitter for MPLS enabled networks in comparison to the non MPLS networks is less since traditional IP networks follow connectionless flow while MPLS is connection oriented switching technology which clearly indicates that enabling MPLS lowers the jitter of pure IPv6 networks, hence are promising for future real time traffic.

## 4.2 Point to Point Queuing delay in Unicastig and Multicasting

Queuing delay is an important design and performance characteristic of a computer network or telecommunications network. The delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another. It is typically measured in multiples or fractions of seconds. Delay may differ slightly, depending on the location of the specific pair of communicating nodes. Queues may be caused by delays at the originating switch, intermediate switches, or the call receiver servicing switch. Queuing delays increase as the congestion in the network increases and as a result of it the queue buffer often overflows which result in lost packets. Thus software for reliable connections must check for losses and do resends. If a resend is needed, the overall delay is at least doubled; the no ther round-trip time is added for a resend request and response. For higher speed reliable data transfer protocols the impact can be even greater. Queuing delays are usually small and can be around 30ms for a cross country network. In the simulation it was observed that the minimum queing delay was for IPv4 in case of pure unicast traffic shown in Figure 6 while as for pure multicast traffic shown in Figure 7 MPLS IPv4 proved promising with minimum queuing delay compared to other 3 scenarios.

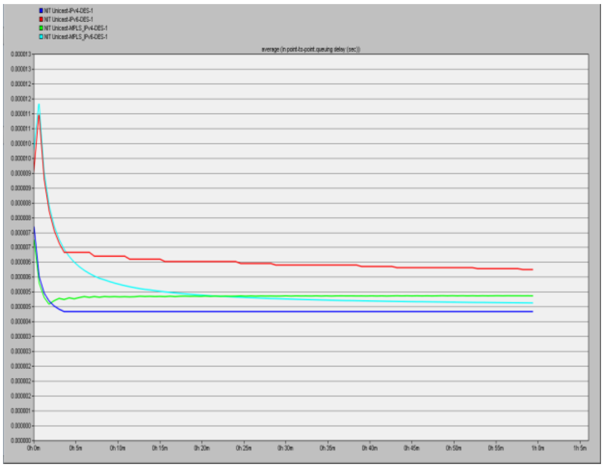

**Figure 6. Delay Unicasting**

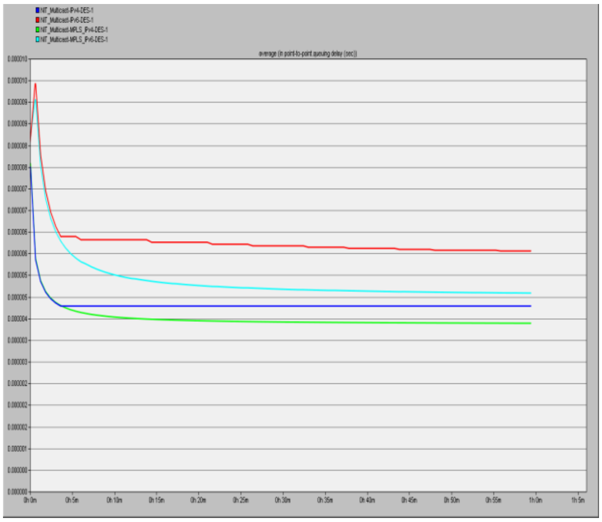

**Figure 7. Delay Multicasting**

However when background traffic was added to the network it can be seen that for both unicast traffic Figure 8 and multicast traffic Figure 9 MPLS enabled networks were having less queuing delay as compared to traditional networks. This can be explained by the fact that in MPLS only the label is checked and the underlying IP header is not used or forwarding and routing desions. IPv6 MPL Shasmore queing delay than IPv4 because of the fact that the packet header is larger in IPv6 than in IPv4, the addition of the MPLS header increases the packet size even more. The maximum queing delay in all the cases was for IPv6.

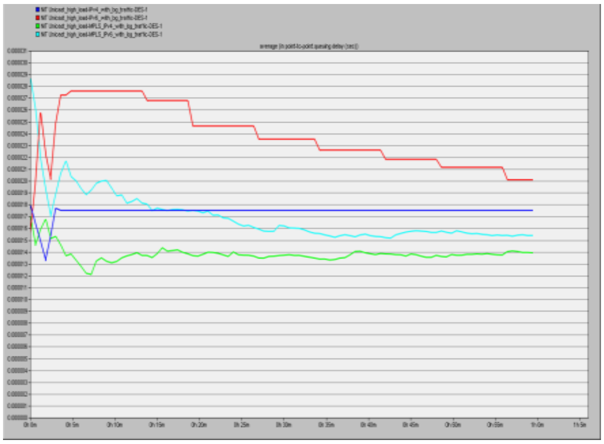

**Figure 8. Delay Unicasting (with background traffic)**

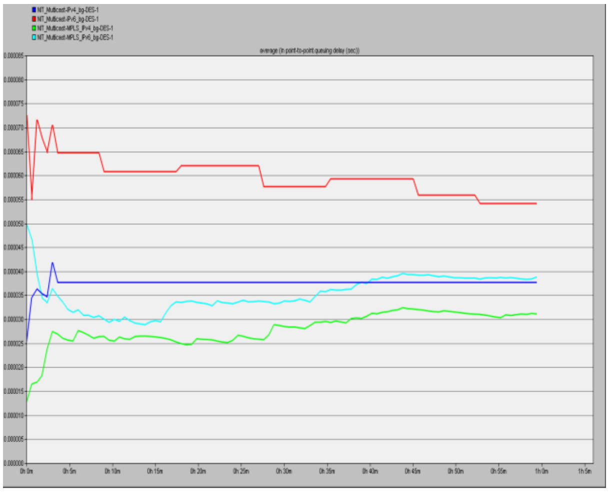

**Figure 9. Delay Multicasting with background traffic**

### 4.3 POINT TO POINT THROUGHPUT IN UNICASTING & MULTICASTING:

Throughput is the number of packets successfully delivered per unit time. Available bandwidth, signal to noise ratio as well as hardware limitations have considerable effect on the throughput of a network.

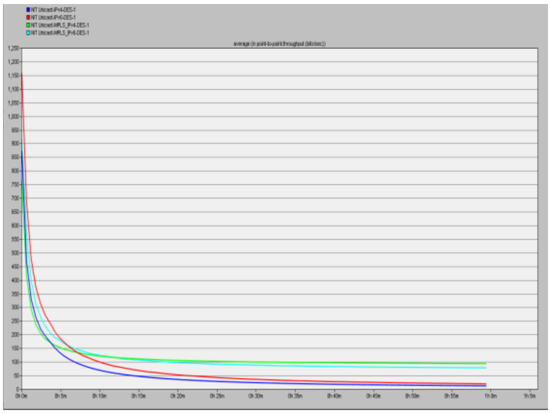

**Figure 10. Throughput Unicasting**

For the network shown in Figure 3, the effect of throughput will be understood and measured from the arrival of first bit of data at the receiver. The dominating factor in the calculation of throughput is often taken as the time window of packets and as far as latency is concerned its effect on throughput depends on the fact whether it is taken into account or not for the network. In this simulation the throughput was calculated for IPv4, IPv6, MPLS IPv4 and MPLS IPv6 for both unicasting and multicasting traffic. Figure 10 shows the throughput for unicasting traffic and Figure 11 shows the throughput for multicasting traffic. As it can be seen that in both the cases the throughput for MPLS enabled networks is high than the traditional IP networks. Also the transient throughput is high because of the fact that in initial messages which are transmitted, to set up the network protocols and various tables e.g., the ARP table.

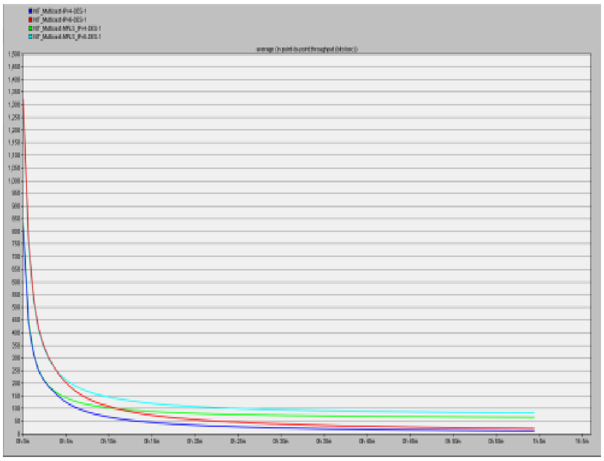

**Figure 11. Throughput Multicasting**

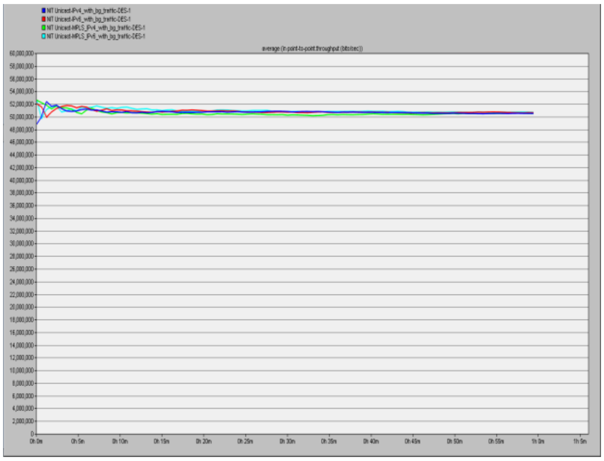

**Figure 12. Throughput Unicasting (with background traffic)**

Also as far as MPLS enabled networks are concerned there is no limit on the size of the packet that can be transmitted under MPLS label thus MPLS IPv6 is having the maximum throughput among all the 4 scenarios discussed in 3.0.

When the background traffic was added to the network the difference in the results shown in Figure 12 and Figure 13 for unicasting and multicasting traffic respectively, were not significantly different, thus the idea that most of the people have regarding the throughput for an IPv6 network being larger owing to its larger address space is not correct. However still as the graph Figure 10 and Figure 11 show, the throughput is larger for MPLS enabled networks though the difference in not significantly noticeable in the ones having background traffic enabled.

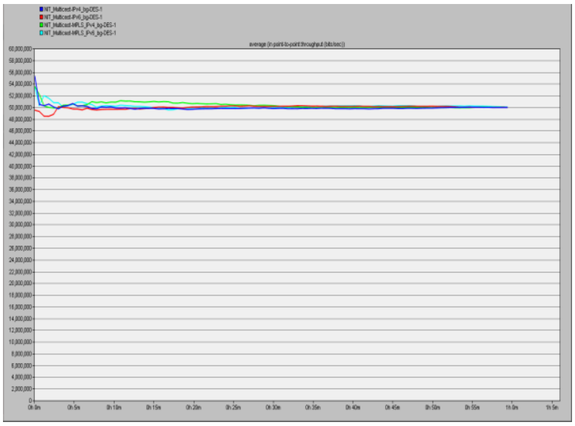

**Figure 1. Throughput Multicasting (with background Traffic)**

### 4.4 POINT TO POINT QUEUING DELAY IN UNICASTING & MULTICASTING (WITH DIFFERENT IRP'S):

A routing protocol is used for exchanging routing information between gateways (routers commonly) within an Autonomous system (AS). This information can be used to route network level protocols like IP. It can be divided into two categories distance vector, example Routing Information Protocol (RIP) and link state protocol, example Open Shortest Path First (OSPF). In OSPF the routers send information about the state of the links to the entire network that they are a part of. In this way each router understands the entire network topology. They run an algorithm every time a network change is announced to recalculate the best routes through the network. This makes link state routing protocols much more processor intensive, but they only send triggered updates and not periodic. RIP being a distance vector protocol operates differently; it periodically sends information about their known routes to their connected neighbors. Distance vector protocols have slow convergence and have chances for loops, they compare their routing tables against the information they receive from their neighbors - if it matches, they are good, if not they update their tables to reflect the changes. Interior gateway routing protocol (IGRP) is also distance vector routing protocols, it is proprietary of cisco and was developed to overcome the limitations of RIP. Enhanced Interior gateway routing protocol (EIGRP) is an advanced distance vector routing protocol developed by Cisco as a proprietary protocol but in 2013 Cisco converted it into an Open standard [27]. The main reason for the replacement of IGRP was that there was no support for Classless IPv4address.In a way EIGRP borrows the best attributes of both distance vector and link state designs as it doesn't not send periodic updates about route messages; instead it sends updates only when changes occur.

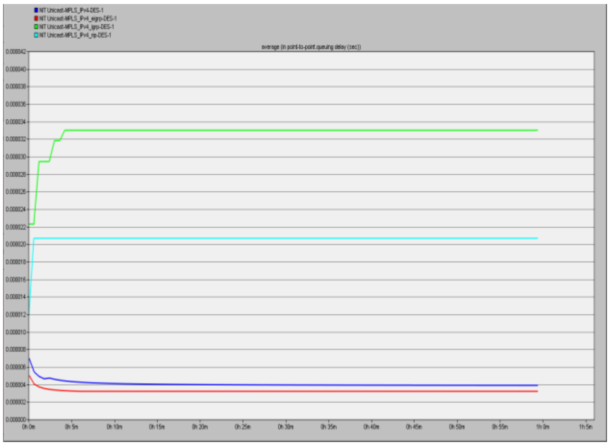

**Figure 2. Delay Unicasting**

EIGRP also form neighbor relations with its directly connected peers and only updates them - not the entire network, (like the distance vector protocols). Contrastingly exterior protocols are used to exchange routing information between autonomous systems and rely on Interior routing protocolsIRP) to resolveroutes within an AS.In Figure 14 and Figure 15 the comparison is shown between RIP, IGRP, OSPF and EIGRPfor unicast and multicast traffic over IPv4.

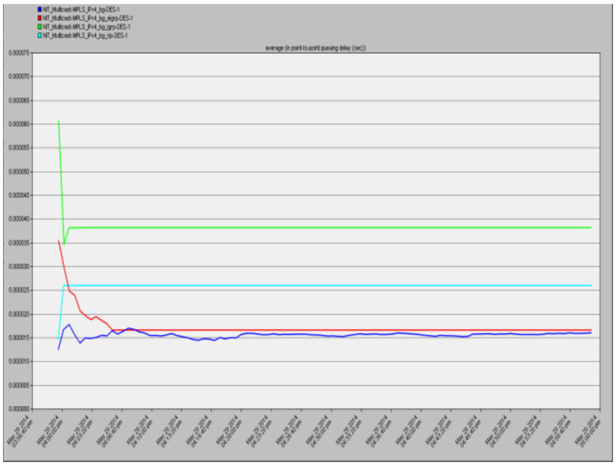

**Figure 3. Delay Multicasting**

It is observed that in both unicasting and multicasting traffic the queing delay of OSPF is the least followed by EIGRP and IGRP while maximum delay is for RIP. The results in this graph can be explained by the fact that in both OSPF and EIGRP as stated above the best routes through the network are calculated only when a network change is observed. While in RIP irrespective of network change full updates are transmitted every 30 seconds which adds to the delay in the network.

## 5. CONCLUSION AND FUTURE WORK

Using MPLS methodology, all the backbone nodes have to support MPLS protocols such as Label Distribution Protocol (LDP). Decisions are made in the ingress node which replace IP addresses with labels, however once packets enter the MPLS network they are processed quickly because only the MPLS labels are used. The IPv6 flow label feature takes the advantage of the MPLS label and uses the IPv6 flow label field to process packets thus minimizing lookup (long match up method) time in routers. In the case of special Quality of service (QoS) requirements use of the class of service field provides more choices than the type of service field in IPv4. In this paper the comparison between the traditional IPv4 & IPv6 networks was shown with the MPLS enabled networks & it was seen that MPLS networks perform better than the traditional networks. Thus we conclude with the following points:

1. Multicasting consumes much less tag labels and processing time, which are quite the resource in MPLS network. This is achieved by referencing the concept of hierarchical data transportation in IPv6 multicasting network.
2. Multicasting in IPv6 could upgrade the safety of the whole system by adding IPsec encapsulation on data packets before attaching tag labels. Since IPv6 possess inherit support for security the whole network security will get enhanced.

Multicasting in MPLS VPN services, which is the new Virtual Private Network (VPN) technology, could also be easily deployed in IPv6 network but with higher safety. Also as a next step, other traffic like File Transfer Protocol (FTP), Database etc., can be introduced into the network, to study the performance in a closer to real-world setup by adding additional background traffic as well. Further complexity can be introduced into the network, by adding more multicast groups and receivers being members of more than one multicast group. This would help in determining and understanding what latency/jitter the router introduces when it has to process more multicast traffic and multicast routing decisions. Also some further research based on MPLS by expanding it into MPLS VPN'S and QoS, Traffic Engineering (TE) scenarios in both IPv4/IPv6 dual stack networks & IPv6 networks.

## REFERENCES

[1] S.E. Deering, Multicast routing in internetworks and extended LANs. Stanford, CA: ACM, 1988, pp. 55-64J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[2] M. Laubach and J. Halpern,Classical IP and ARP over ATM, RFC 2225,Apr. 1998; http://www.rfc-editor.org/rfc/rfc2225.txt

[3] E. Rosen, A. Viswanathan and R. Callon,Multiprotocol Label Switching Architecture, RFC 3031, January 2001.

[4] Uyless Black, MPLS and Label Switching Networks, Prentice Hall PTR, Upper Saddle River, NJ, 2000

[5] Esther Lam, Christine Polewarczyk, and Steve Taylor (2007, April 17) [Online]. Available: http://searchnetworking.techtarget.com/definition/time-tolive

[6] Luc De Ghein, MPLS Fundamentals, Cisco Press, 2006

[7] Jong-Moon Chung, "Analysis of MPLS traffic engineering," Circuits and Systems, 2000. Proceedings of the 43rd IEEE Midwest Symposium on, vol.2, no., pp.550, 553 vol.2, 2000 doi: 10.1109/MWSCAS.2000.952816

[8] Jon Postel, Information Sciences Institute: Internet Protocol, RFC 791, September 1981; http://www.rfc-editor.org/rfc/rfc791.txt

[9] Michael Fry (2011, April 4) [Online]. Available: http://theconversation.com/the-end-of-the-internet-ipv4-versus-ipv6-145

[10] J. Mogul and J. Postel, Internet Standard Subnetting Procedure, RFC 950, August 1985; http://www.rfc-editor.org/rfc/rfc950.txt

[11] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, and E. Lear, Address Allocation of Private Internets, RFC 1918, February 1996; http://www.rfc-editor.org/rfc/rfc1918.txt

[12] Dave Evans, The Internet of Things, Cisco Internet Business Solutions Group (IBSG), April 2011

[13] S. Deering, R. Hinden, Internet Protocol, Version 6 (IPv6) Specification, RFC 2460, December 1998; http://www.rfc-editor.org/rfc/rfc2460.txt

[14] Network Computing (2011, August 6) [Online]. Available: http://www.networkcomputing.com/netw-orking/sixbenefits-of-ipv6/d/d-id/1232791?

[15] M. Laubach and J. Halpern, Classical IP and ARP over ATM, RFC 2225, Apr. 1998; http://www.rfc-editor.org/rfc/rfc2225.txt

[16] Grenville Armitage, Bell Labs Research, MPLS: The Magic behind the Myths, January 2000.

[17] E. Rosen, A. Viswanathan, and R. Callon, "A Proposed Architecture for MPLS," draftietf-MPLS-arch-06.txt, Aug. 1999 (approved by IESG for RFC status Sept. 1999).

[18] B. Davie, P. Doolan and Y. Rekhter, Switching in IP Networks — IP Switching, Tag Switching, and Related Technologies, Morgan Kaufmann, 1998.

[19] L. Andersson et al., "LDP Specification," Internet draft (work in progress) draft-ietfMPLS-ldp-06.txt, Oct. 1999.

[20] S. Deering, Host extensions for IP multicasting, RFC 1112, August 1989; http://www.ietf.org/rfc/rfc1112.txt

[21] J. Moy, Multicast extensions to OSPF, RFC 1548, March 1994; http://www.rfc-editor.org/rfc/rfc1584.txt

[22] Kevin Dooley, Ian Brown, Cisco IOS Cookbook, O'Reilly Media, Inc., 2006

[23] S.E. Deering, Multicast routing in internetworks and extended LANs. Stanford, CA: ACM, 1988, pp. 55-64

[24] Kazuaki Tsuchiya, "An IPv6/IPv4 Multicast Translator based on IGMP/MLD Proxying (MTP)", presented at 52nd IETF MAGMA Meeting, Salt Lake City, Utah, and December2001. http://www.ietf.org/proceedings/52/slides/magma-4.pdf

[25] R. Hinden and S. Deering, IP Version 6 Addressing Architecture, RFC 4291, Network Working Group, February 2006; http://www.rfc-editor.org/rfc/rfc4291.txt

[26] Enhanced Interior Gateway Routing Protocol (EIGRP), Cisco Public Documentation, (2013 March) [Online].Available; http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/enhanced-interior-gateway-routing-protocol-eigrp/qa_C67-726299.html

**Firdous Ahmad Khan**

Firdous Ahmad Khan has done his B Tech in Computer Science and Engineering from National Institute of Technology Srinagar. His fields of interest are Linux, Networking, and Open Source.

**Falak Reyaz Wani**

Falak Reyaz Wani has done his B Tech in Computer Science and Engineering from National Institute of Technology Srinagar. His fields of interest are Unix, Networking, Security, andComputer Architecture.

**Mohammad Ahsan Chishti**

Mohammad Ahsan Chishti has done his B.E. and M.S. in Computer and Information Engineering from International Islamic University Malaysia with specialization in Computer Networking. Presently he is Assistant Professor and Head of the Department of Computer Science & Engineering, National Institute of Technology Srinagar. He has around 50 publications to his credit and 5 patents. He is Principal Investigator of Department of Science & Technology, Government of Jammu and Kashmir sponsored research project on IPv6. He has been guiding M.Tech and B. Tech research projects and his research area includes Computer Networks, Next Generation Networks, MPLS and Technology Roadmapping.