QOS and TE in MPLS Networks

[1]Gurtej Singh, [2]Dr.Madan Lal
[1]Student, [2]Assistant Professor
[1]Dept. of Computer Science and Engineering,
[1]Punjabi University, Patiala, India

Abstract - MPLS is the core of any service provider in the world. Almost all the ISPs uses MPLS as its backbone technology to take data from one provider edge to other provider edge. Benefits that MPLS brings for the ISPs are making other competitive technologies of MPLS fade way in a short time and made MPLS so popular. Some of the benefits which makes it a clear winner is that it makes the core of ISP totally BGP free and the ability to create Layer 2 and Layer 3 VPNs. Internet is rising at a very rapid pace and millions of internet enabled devices are connected with the internet every day,With the advent of IOT and cloud, it is getting more fast and contains different challenges to the ISP engineers. QoS and Traffic engineering are some of the challenges that ISP faces with new traffic types like Voice, Video, Cloud, IoT etc. This paper explains the importance of MPLS in ISP network and describes how MPLS plays an important role in taking the traffic from source to destination on the internet when traffic moves within ISP. Different QOS models are compared and a new policy is proposed which can be used in large scale ISPs to have much better traffic management than before. This paper explains a method with which different types of traffics can be transmitted from ingress provider edge to egress provider edge in best possible manner.

Keywords- MPLS, LDP, QOS, DSCP, TRAFFIC ENGINEERING, MPLS EXP, MPLS QOS MODELS, GNS3

I. INTRODUCTION

Multiprotocol Label switching is a method used to forwards packets on the basis of Labels. Labels are attached to packets when they enter Service Provider Edge Routers(SPER) and all the packets are forwarded inside Service Provider Core on the basis of labels.When packets try to exit from Service Provider edge towards the customer, then labels get disposed off from the packet and the customer gets only pure IP packets. Labels are distributed among the routers with the help of Label distribution protocols(LDP) Resource Reservation Protocols - RSVP and Multiprotocol Border Gateway protocol or MP-BGP. By default when we configure MPLS, LDP is used as the Label Distribution Protocol and is the most used Label Distribution Protocol in the world. When we use LDP, then labels can only be assigned to non-BGP routes present in Routing Table, and for BGP, we can use MP-BGP.

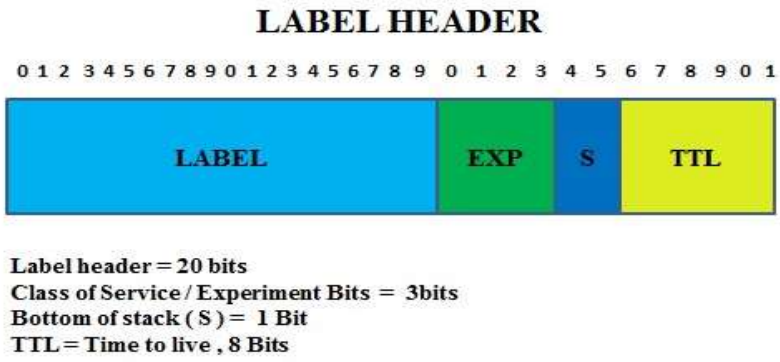

Fig. 1.1 Label Header

II. MPLS ADVANTAGES

MPLS offers various benefits to Service Providers and Clients over other service providers.

- **No BGP in Core Networks :**
  This is a very big advantage that MPLS provides as Service Provider need not to run BGP in the Core routers and BGP is used only at Service Provider Edge routers which are also known as Provider Edge devices. One major reason of not using BGP in the core is that packets are forwarded on the basis of labels and not on the basis of destination IP routing table.
- **Optimal Traffic Flow :**
  MPLS provides smooth data flow within Service Provider Networks. In traditional WAN networks, data had to traverse twice from Service Provider Networks to reach the destination which results in wastage of bandwidth and consumes much more time than MPLS.

- **Use of one Unified Network Infrastructure :**
  Same infrastructure is used to transport both Layer 2 and Layer 3 packets based on labels. This means that we can send any sort of traffic like IP, Ethernet, PPP, POS etc over the same infrastructure. VoIP, Video and data traffic can be sent without need to have any change in infrastructure.

- **Traffic Engineering :**
  This is one of the advantage in which MPLS clearly beats its counterparts like Frame Relay or ATM Switching or Dynamic Multipoint Virtual Private Networks. With traffic engineering, network resources can be utilized in much more efficient manner than if traffic engineering is not deployed. It helps in Fast Rerouting of traffic or make links usable which are not exactly the best paths to reach the destination, therefore we can use traffic engineering for unequal cost load balancing also. but the biggest advantage that MPLS provides is its ability to create Virtual Private Networks(VPNs). It can create both Layer 2 and Layer 3 VPNs.

III. MPLS VPN Types

As mentioned before, MPLS can create both Layer 2 and Layer 3 VPNs. It means MPLS can create both Peer to Peer and Overlay VPNs.VPNs are connecting different private networks over the public infrastructure. Below are the various types of VPNs that Service Providers offer with MPLS :

- **MPLS Layer 3 VPN :** MPLS L3 Virtual Private Network creates a peer to peer connectivity between CE Router and Service Provider Edge Router. Client shares its routing table information with Service Provider Edge router. Label is attached when IP based traffic from CE enters the Service Provider Edge router, and all the forwarding from one Provider Edge to other end Provider Edge router connected with other CE router is done on the basis of Label Switching technique, when other end Provider edge router receives the traffic that it needs to send to CE Router, it then removes the label and sends only IP based traffic.

- **MPLS Layer 2 VPN**
  With MPLS Layer 2 VPN, MPLS offers an overlay VPN in which routing information of Customer is not shared with PE device and routing is shared directly between CE devices ISP's MPLS network just act as a Layer 2 Switch. MPLS offers various types of Layer 2 VPNs :
  - **Virtual Private Wire Service (VPWS) / Any transport over MPLS (AToM)**
  - **Virtual Private LAN Service (VPLS)**
  - **Ethernet VPN (EVPN)**

IV. QOS AND TRAFFIC ENGINEERING IN MPLS BASED NETWORKS

Quality of Service or QoS is a technology used to prioritize one type of traffic over another. QoS is mainly needed when we have limited bandwidth and we need to send different traffic types like Voice, Video and Data with some specific type needed to be prioritized. For example, VoIP traffic is benign means it is needed to be constant and extra delay can disconnect the VoIP connection or if we have any video conferencing in place, then the sync of voice and video is disconnected. Therefore in those types of networks, Quality of Service is implemented to have Voice or Video traffic flow optimally. MPLS run inside Service Provider Networks and Service providers deals with customers having all types of traffic like Voice, Video and Data, therefore QoS is needed to be implemented there to have benign traffic flow in case of Voice and Video type of traffic. Traffic Engineering is used in MPLS networks for re-routing and to use under utilized links for unequal load balancing between the multiple links.

V. MPLS TRAFFIC ENGINEERING

MPLS Traffic Engineering is used to utilize network resources and all the paths in a more efficient manner than with MPLS without traffic engineering. Protocol that we can use with MPLS traffic engineering is RSVP-TE. We can reserve explicit paths also which are not the best paths to reach destination according to Interior Gateway Routing Protocols like OSPF(Open Shortest Path First) or IS-IS(Intermediate-System to Intermediate-System) . The best thing about traffic engineering is that underutilized links can also be used, therefore load can be balanced in a much better manner. Fast Rerouting is another traffic engineering feature that helps in fast failover in case of primary Label Switch Path failure from one PE to other PE.In MPLS, Traffic engineering is solely based on Experimental bits and bandwidth can be reserved by using RSVP TE mechanisms.

VI. RESULTS AND DISCUSSIONS

Performance of different traffic types over MPLS with Plain Traffic with no QoS and with QoS applied on it. By default when traffic enters into Service Provider Core Network from Customer, MPLS labels are attached to the IP packets and all the forwarding is done on the basis of the experimental bits. Below is the topology used for MPLS QOS and TE :-

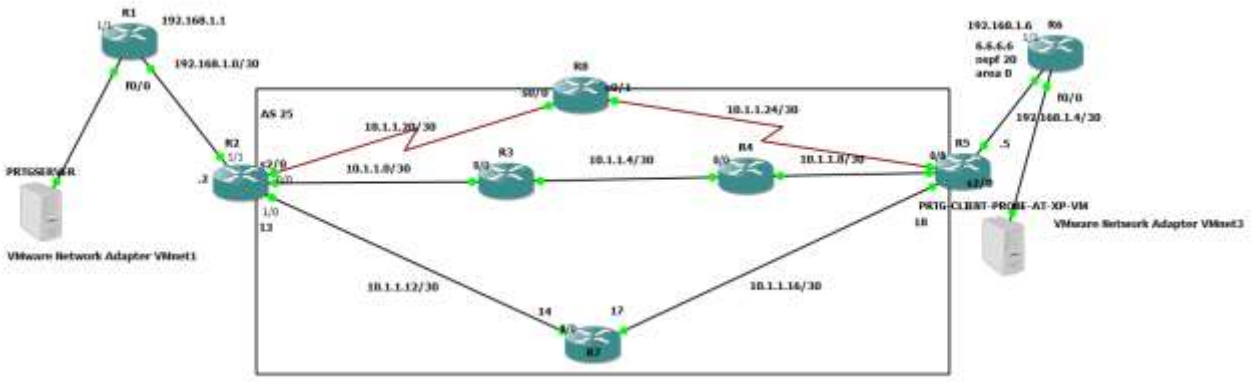

Figure 3.1 - MPLS Topology used for testing.

Above is the MPLS topology used for QoS testing in MPLS networks. R1 and R6 are used CE routers and ICICI is the client of the Vodafone. R1 is ICICI office in France, while R6 is a ICICI office in Holland. Vodafone, which is one of the largest Internet Service Providers in the world connected different ICICI sites using Layer 3 MPLS VPN. R2 is the Provider edge router in Vodafone France while R5 is the Provider Edge router in Vodafone Holland. Both the Ingress and Egress PE are connected using redundant links over Provider routers. Customer ICICI France when sends some packets at ICICI Holland, uses which link depends on the OSPF's Dijkstra's Algorithm by default.

Below is the capture that was taken between the PE1 and PE2 router, it shows that different types of traffic like UDP, TCP, ICMP all are going from ingress PE to egress PE through the same link :-

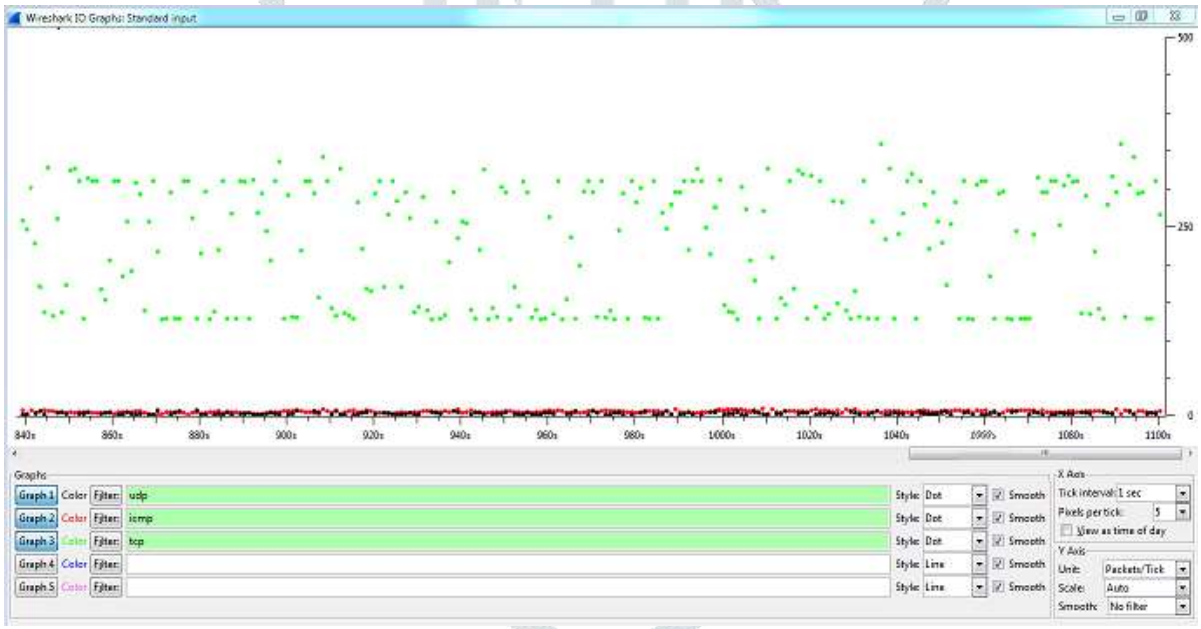

Figure 3.2 - TCP Burst, UDP and ICMP traffic on same input queue.

Now that service providers always have multiple links from one PE to other PE, other links can be used to balance different types of traffic. It will also help in reduction of packet drops and lesser delay in case of Voice and Data traffic on same LSP. It used Ostinato traffic generator software to generate traffic bursts. Following figure shows how data starts to drop when traffic burst from TCP is started :-

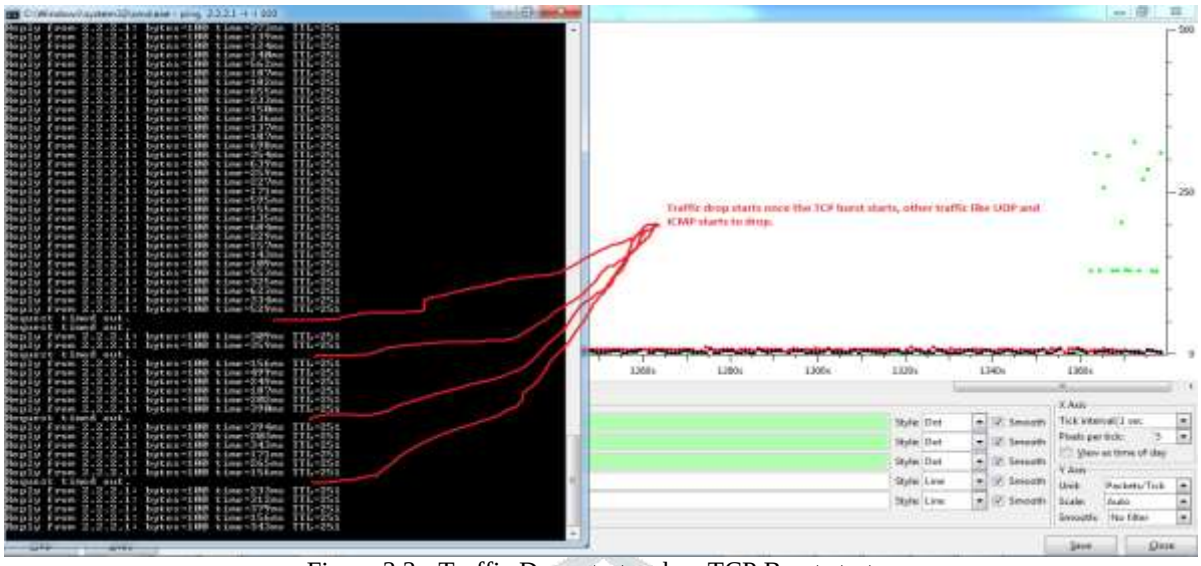

Figure 3.3 - Traffic Drop starts when TCP Burst starts.

The above problem can be reduced to large part if the following algorithm is used :

Step 1 - Check the different links between ingress and egress Provider Edge devices.
Step 2 - Assign MPLS Experimental bits to different types of traffic entering MPLS and prioritize them according to the traffic types bandwidth requirement.
Step 3 - Create traffic engineering tunnels between MPLS PEs and provide different explicit paths to packets with different Experimental bits.
Step 4 - If there is single path, then prioritize real time traffic over other traffic type.
Step 5 - Decision on best ingress PE - egress PE link is taken by Dijkstra's Algorithm as service providers runs only link state routing protocols as the Interior Gateway routing protocol in the core.
Step 6 - In case of primary link failure, traffic can turn to the dynamic best path or we can also assign some other explicit path too, which can reduce the workload of Step 5.
In the above proposed algorithm, different traffic types are sent via different links and Voice and Video traffic is on a total different link which provides smooth flow for UDP traffic and any sort of TCP burst will not create any problem whatsoever. All the traffic is divided on the basis of experimental bits and traffic type with experimental bit 5 is on different link, traffic type with experimental bit 4 is on different, while we have explicitly defined the best paths for different types of traffic, a back dynamic path is also defined in order of primary link failure between ingress and egress Provider edge device. Following are the results occured during the implementation of above steps and they are also comparison with the Uniform Model :-

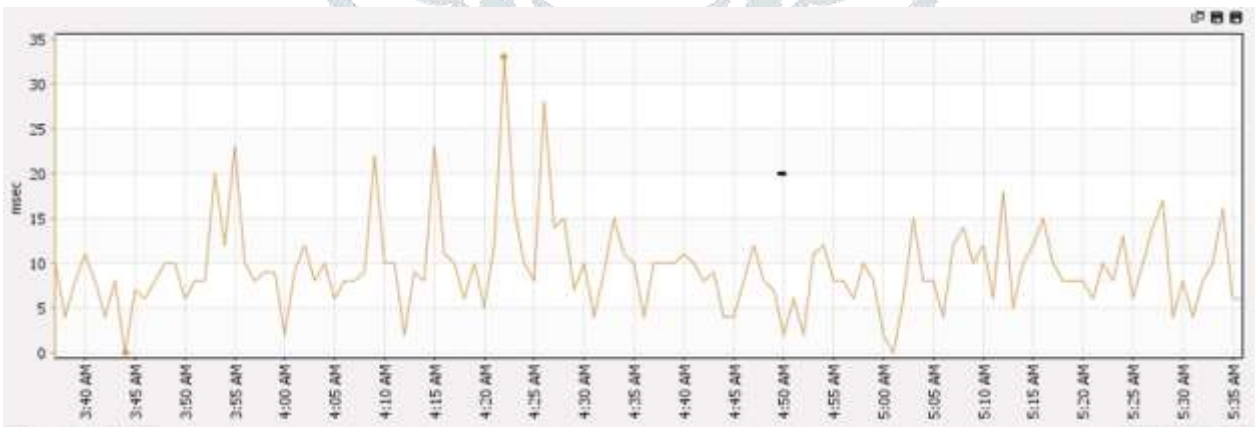

Figure 3.4 - Maximum Jitter during Voice traffic with proposed algorithm

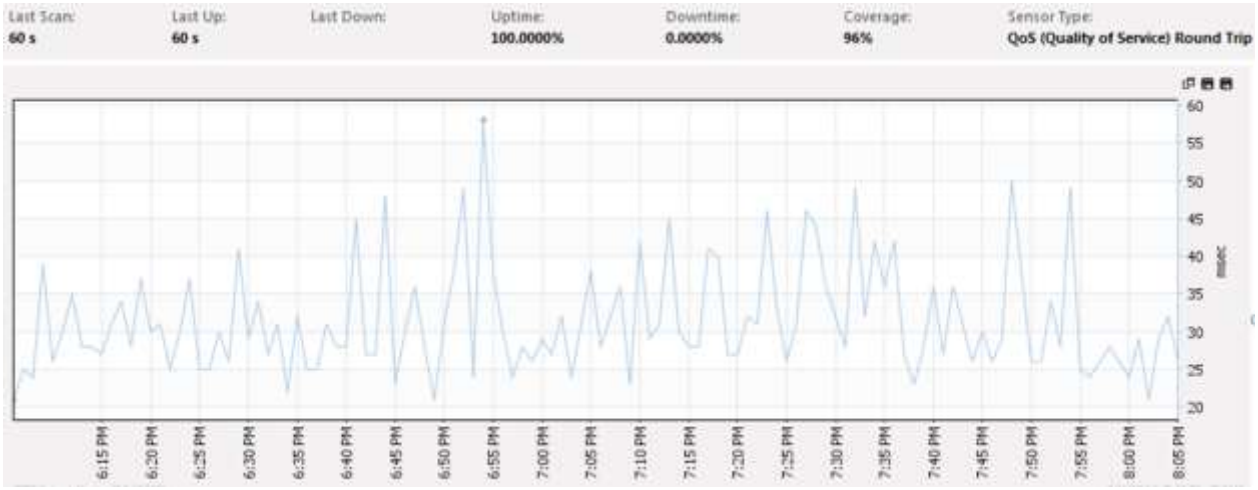

Figure 3.5 - Max Jitter with Uniform Model

Above graph taken in PRTG QoS sensor shows the maximum jitter in the voice traffic using Uniform Model and proposed algorithm. It clearly shows that our proposed algorithm provides better results.
Following graph shows the average jitter between the two end points :-

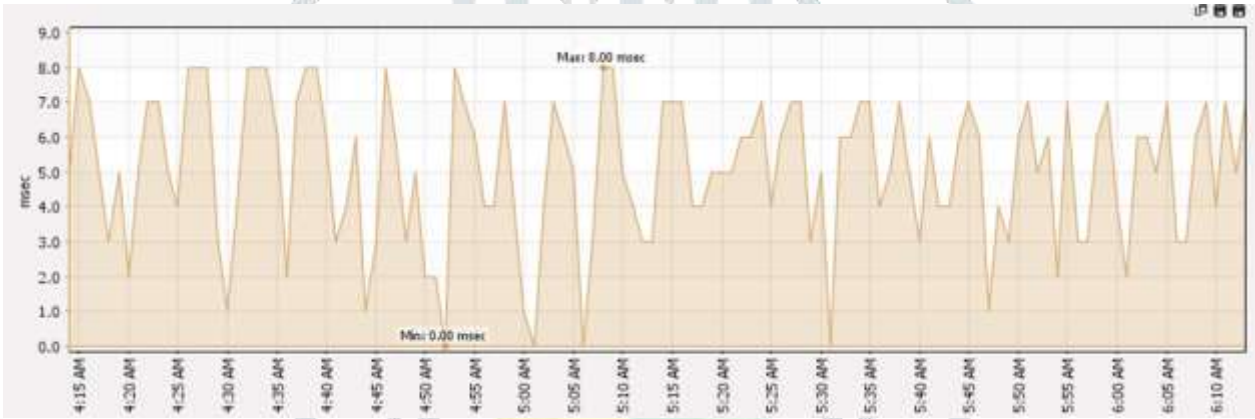

Figure 3.6 - Average jitter between the two voice endpoints using proposed algorithm.

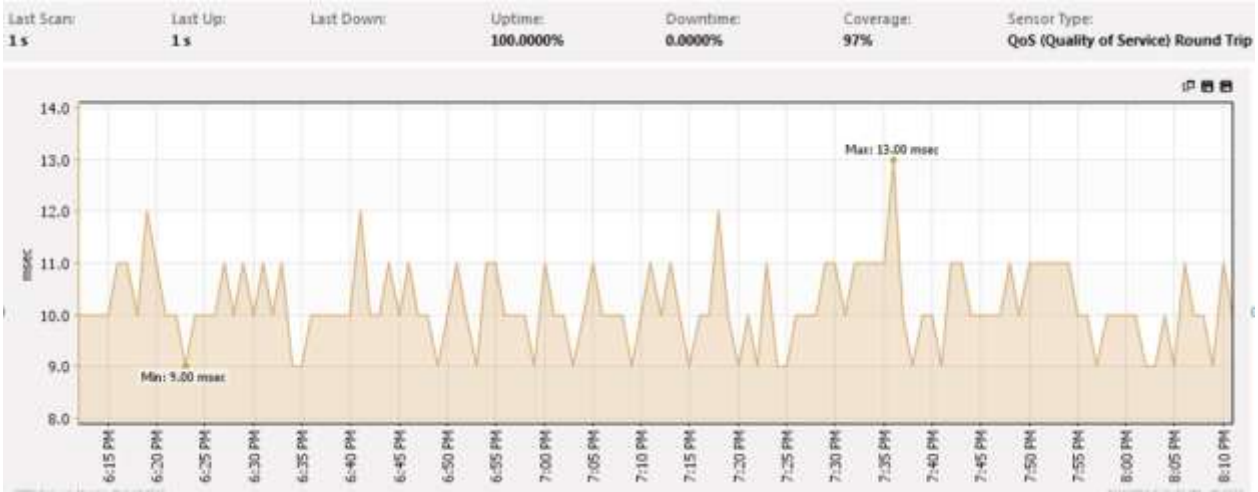

Figure 3.7 - Average Jitter using Uniform Model.

In Figure 3.6 and figure 3.7 graphs clearly shows that our proposed algorithm is better when compared with uniform model in terms of average jitter. Above graph shows that there is an average of 7-8 msec between the voice packets captured using our proposed algorithm while around 13 msec average jitter was experienced with Uniform model. This graph shows the average jitter between the Voice packets between the two CEs connected through MPLS VPN. Below is the single graph showing minimum, maximum and average jitter between the two CE devices connected via MPLS Virtual Private Network.

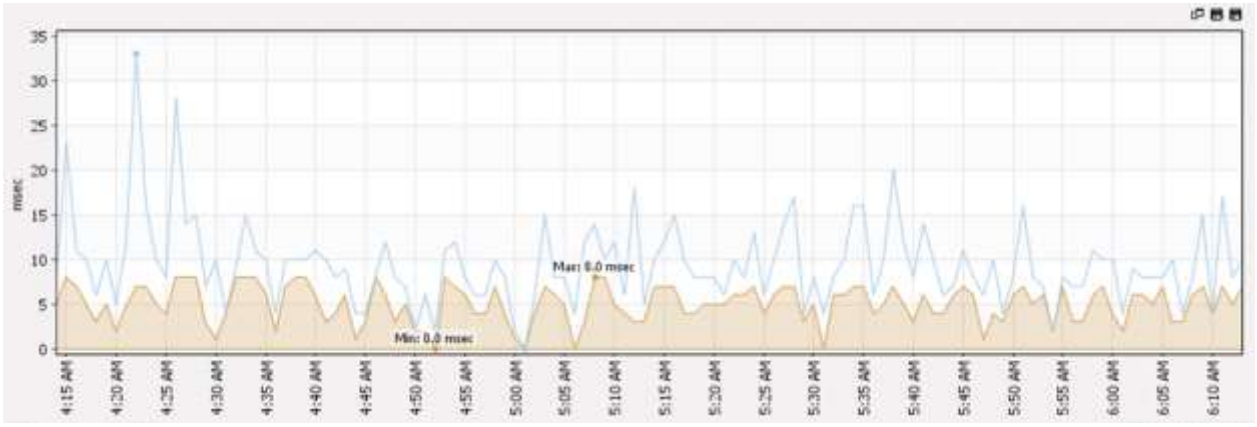

Figure 3.8 - Minimum, Maximum and Average Jitter between the two CE devices using proposed algorithm.

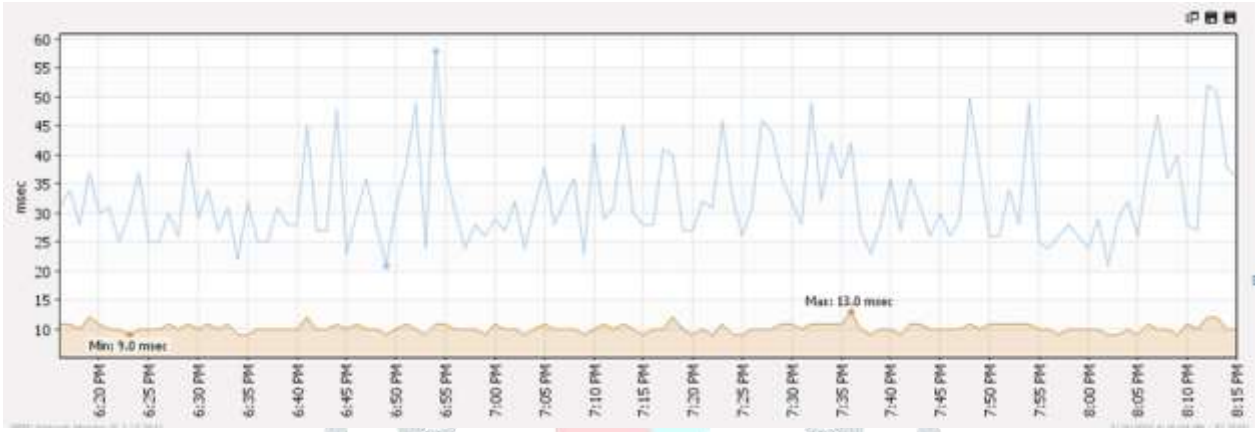

Figure 3.9 - Minimum, Maximum and Average Jitter between the two CE devices using uniform model.

Above are the jitter based graphs between the two CEs. As specified before also, jitter is the variation in the packet delay, but this term is used differently by various people. Jitter actually has two meanings according to IETF RFC 3393, the first meaning is variation of a signal which is with respect to a clock signal, and here the arrival time of signal is expected to coincide with the arrival of the clock signal. This is used to measure the quality if a circuit emulation. Second meaning is related to variation in metric like delay with reference to some metric like minimum delay.

Another parameter that very much influence the Quality of Service and delivery of data is packet delay variation. It is just like jitter when we look at its definition, but it is different. Packet delay variation or PDV is the difference between end to end one way delay between some packets in a flow. Below is the graph captured using QoS sensor in PRTG shows the minimum packet delay variation between the two CEs traffic :-

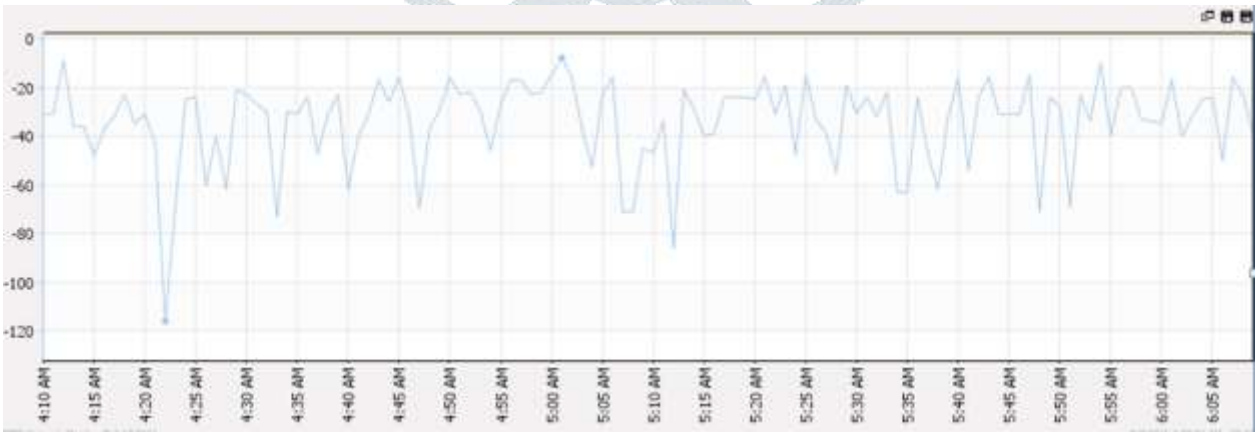

Figure 3.10 - Minimum PDV between two CEs using our proposed algorithm.

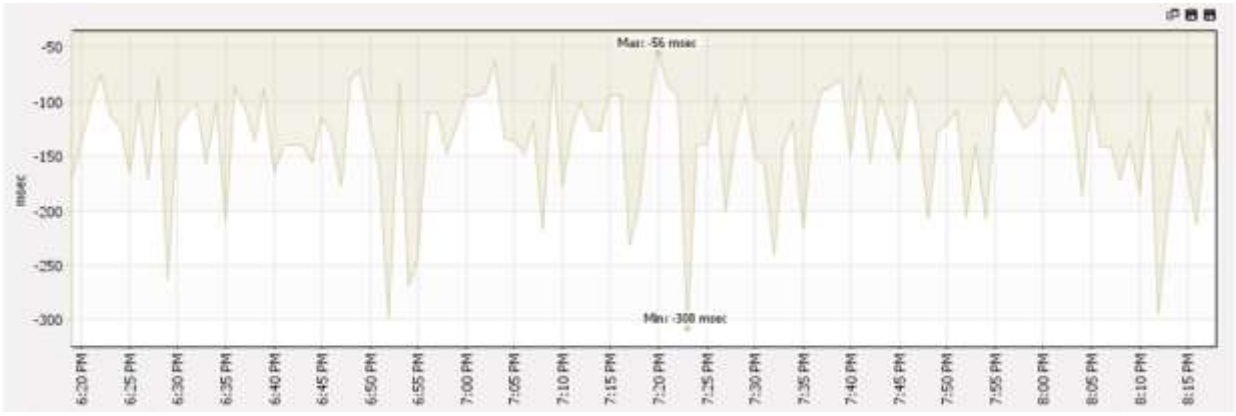

Figure 3.11 - Minimum PDV between two CEs using our uniform model.

Above minimum PDV graphs shows that our proposed algorithm provides better values than the uniform model.
For real time applications like voice, Packet delay variation is very important and VoIP environments have QoS enabled networks for a high quality channel. The problems related with PDV can be reduced by using a proper sized buffer at the receiver end. Instantaneous packet delay variation or IPDV is the variation between successive packets which is sometimes referred as delay. If packets are sent every 20ms and the second packet is received after 30 ms of first packet, then the IPDV is -10ms, it is known as dispersion and if the second packet is received after the first packet then the IPDV is +10ms which is known as clumping. End to end experience of each packet is calculated as :-

$$di = dtrans + dprop + dqueuei .$$

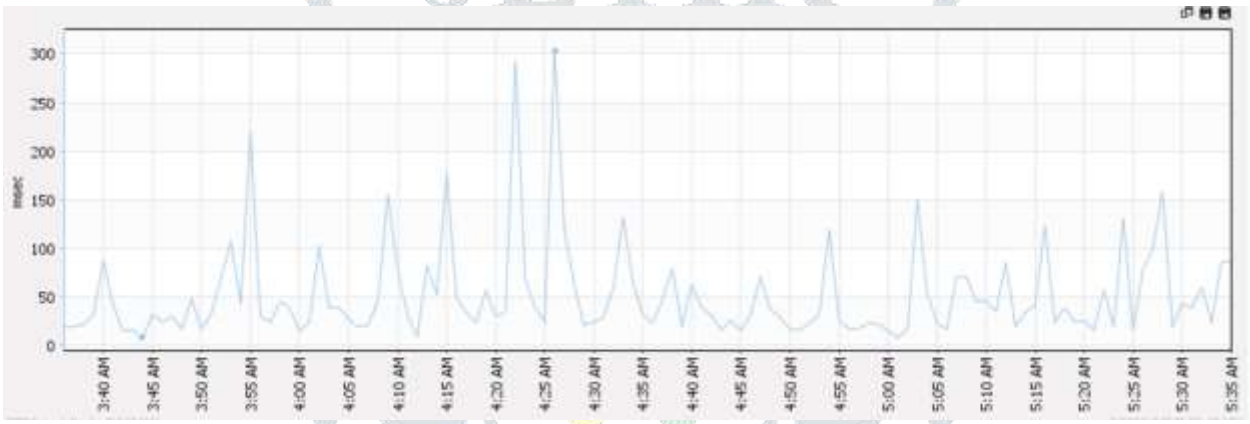

Figure 3.12 - Maximum Packet delay variation using our proposed algorithm

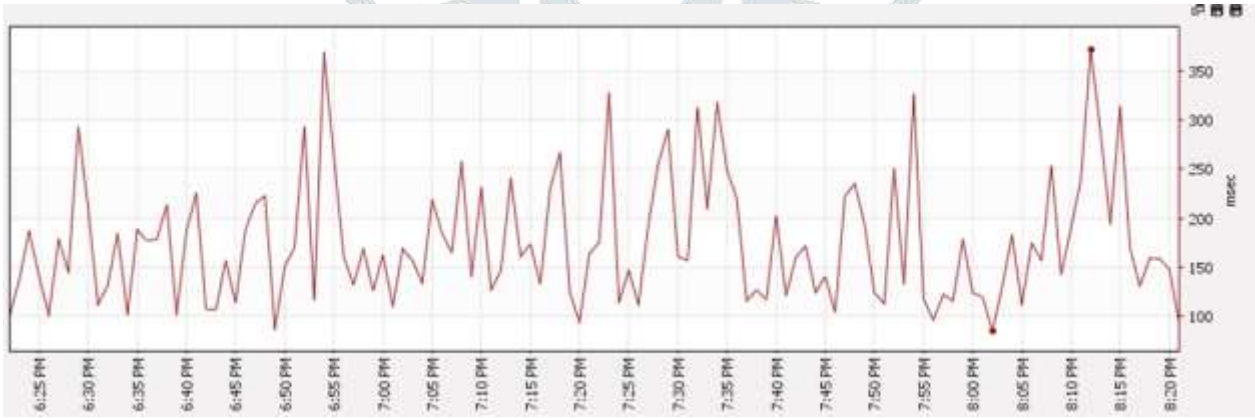

Figure 3.13 - Maximum Packet delay variation using Uniform Model

Above graph shows the comparisons of maximum PDVs.It shows that our proposed algorithm is slightly better than the Uniform model.
Graph shows that maximum PDV is around 305 msec whereas average PDVs is around 72 msec using our proposed algorithm and maximum PDV is around 365 msec whereas average PDVs is around 185 msec with Uniform Model.
Mean Opinion Score (MOS) is used in telephony networks to get the human user's view of the quality of the network. It is a subjective measurement where listeners should sit in a quiet room and score the quality of the call as they perceived it. MOS is expressed as a single number that ranges from 1 to 5, where 1 is the lowest quality of audio and 5 is the highest audio quality measurement. Below are the MOS scores and their impairment :-

MOS	QUALIY	IMPAIRMENT
5	Excellent	Imperceptible
4	Good	Perceptible but not annoying
3	Fair	Slightly Annoying
2	Poor	Annoying
1	Bad	Very annoying

Table 3.1 - MOS mean score and their impairments.

Below is the graph captured in PRTG that shows MOS for the call quality :-

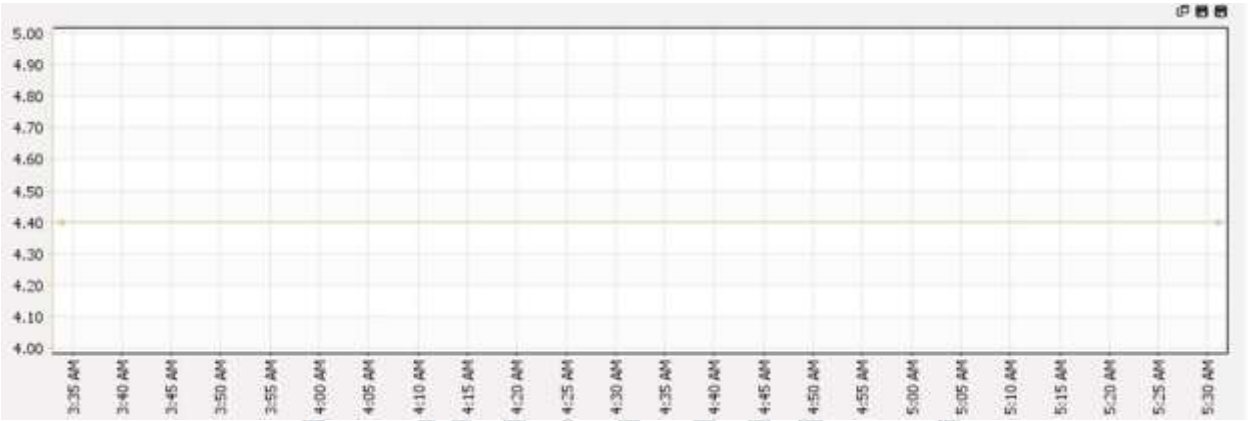

Figure 3.14 - MOS for the call quality between two CE voip devices using our proposed algorithm.

MOS score of 4.4 compared that the call quality is good and hence it shows that the algorithm scores great.
So when we compare our work with the other work done previously, major emphasis was on queuing delay and packet loss and the work was performed on data traffic mainly. Also the work was performed on Opnet, which does not run real Networking operating system. We have taken Data and Voice Traffic and have worked on parameters which are more likely to have impact on the voip traffic like Packet Delay Variation(PDV), Jitter, Round Trip and One-way delay, Packet Loss, MOS and Convergence on network links in case of any link goes down in MPLS backbone. A table showing the parameter comparison of previous researches and what we did is shown below:

Parameters we used	Uniform Model	Proposed Model
Packet Delay Variation	185 msec	72 msec
Jitter	13 msec	8 msec
Packet Loss	Depends on IGP	Low
Convergence	Depends on IGP	100 msec
Mean Opinion Score(MOS)	4.0	4.4
Applicable for VoIP	No	Yes

Table 1 – Comparison Table between MPLS Uniform Model and Proposed Model

Below is a bar graph that compares the average jitter and PDV between proposed and uniform model and clearly shows that the proposed model works better for VOIP traffic:

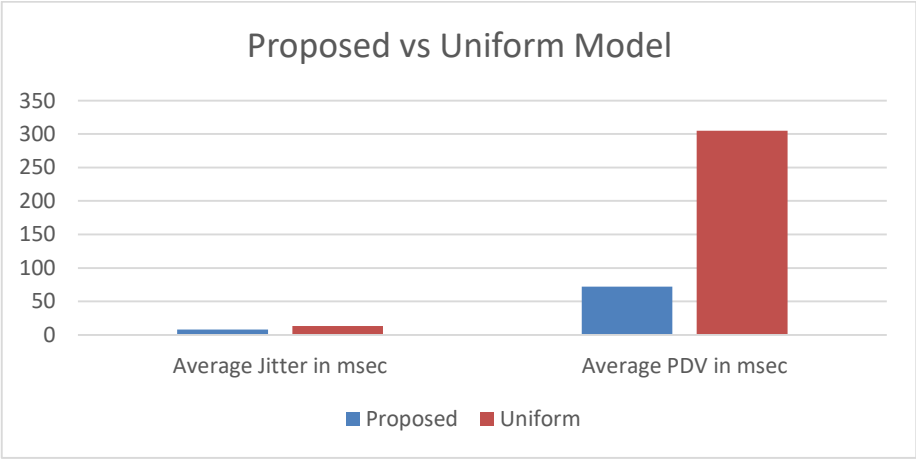

Figure 3.15 – Average Jitter and PDV comparison between Uniform and Proposed Model

VII. CONCLUSION

MPLS is an ISP technology which is mainly used in the Service Provider backbone networks. Major role of MPLS is to create VPNs for the clients in both Layer 3 and Layer 2 fashion. Apart from that MPLS is also used to create BGP free core networks. Service Providers provide core infrastructure and therefore they need to have lot of Traffic engineering and Quality of Service in their network to have as minimal delay and jitter as possible to eliminate the packet loss. Creating different tunnels for different types of traffic using experimental bits can create make delay much lower and provides better quality real time application performance than with simple MPLS or with other algorithms, It provides a better jitter and packet variation delays than normal and other MPLS QOS techniques. Mean Opinion Score of 4.4 shows that that the voice quality is very good. MPLS is and will be the primary technology used by the service providers because of its benefits that it provides, therefore MPLS has to have quality of service and MPLS traffic engineering enabled to make billions of bytes to data flow properly through the service provider with minimal packet loss or minimal delay.

.

REFERENCES

[1] Petac Eugen(2017), "A MPLS Simulation for Use in Design Networking for Multi Site Businesses", "Ovidius" University Annals, Economic Sciences Series Volume XVII, Issue 1 /2017.

[2] Raman, Silki Baghla, Dr. Himanshu Monga(2016), "Method & Implementation of data flow to improve QoS in Mpls Network", Applied Engineering Letters 1 (2016) 105-110.

[3] HESAM HOSEINZADEH (2015) ,"Path Selection Analysis in MPLS Network Based on QoS" under Science Journal (CSJ), Vol. 36, No: 6 Special Issue (2015) ISSN: 1300-1949.

[4] Jyoti Aggarwal and Akansha Dhall (2015),"Simulation Based Comparative Analysis of Voice over Internet Protocol over MPLS and Traditional IP Network" under International Journal of Science, Engineering and Technology Research (IJSETR), Volume 4, Issue 6 (June 2015) ISSN: 2278 – 7798.

[5] Umar Bashir Sofi , Er. Rupinder Kaur Gurm (May 2015), "Comparative Analysis of MPLS Layer 3vpn and MPLS Layer 2 VPN" of RIMT Institute of Engineering and Technology under (IJCST) – Volume 3 Issue 3, ISSN: 2347-8578.

[6] Isaac and Aldrin (2014)" Requirements for Ethernet VPN (EVPN)".

[7] Ezeh. G.N, Onyeakusi C.E, Adimonyemma T.M and Diala U.H. (2014) ,"Comparative Performance Evaluation of Multimedia Traffic over Multiprotocol Label Switching using VPN and traditional IP networks" under IJETR – ISSN(E):2347-5900 ISSN(P): 2347-6079

[8] Sajassi, Ali, et al.(2011) "BGP MPLS Based Ethernet VPN" .

[9] Darukhanawalla, Nash, et al.(2009)," Interconnecting data centers using VPLS". Cisco Press.

[10] Kompella, Kireeti, and Yakov Rekhter(2007),"Virtual private LAN service (VPLS) using BGP for auto-discovery and signalling".

[11] Lasserre, Marc, and Vach Kompella(2007)," Virtual private LAN service (VPLS) using label distribution protocol (LDP) signalling". RFC 4762.

[12] Press, Cisco.(2007) "MPLS fundamentals." Page 438 .

[13] Press, Cisco.(2007) "MPLS fundamentals".

[14] Andersson, Loa, and E. Rosen (2006) ,"Framework for layer 2 virtual private networks (L2VPNs)". RFC 4664.

[15] Martini, Luca. (2006)," Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)".

[16] Martini and Luca (2006) "Encapsulation methods for transport of Ethernet over MPLS networks." RFC4448.

[17] Luo, Wei, et al.(2004)," Layer 2 VPN architectures." Pearson Education,.

[18] Rosen, Eric, Arun Viswanathan, and Ross Callon (2001),"Multiprotocol label switching architecture".

[19] Armitage and Grenville. (2000) "MPLS: the magic behind the myths [multiprotocol label switching]." Communications Magazine, IEEE 38.1 (2000): 124-131.

[20] Zhang, Lixia, et al.(1997) "Resource Reservation protocol (RSVP)--version 1 functional specification." Resource

[21] Cisco," ASR 9000 Series L2VPN and Ethernet Services Configuration Guide",http://www.cisco.com/c/dam/en/us/td/i/300001400000/360001370000/361000362000/361074.eps/_jcr_content/renditions/361074.jpg".

[22] "Ciscopress MPLS and Next Generation Networks,"Foundations for NGN and EnterpriseVirtualization",http://ptgmedia.pearsoncmg.com/images/chap3_9781587201202/elementLinks/md100302.gif" ISBN-10:1-58720-120-8