ISSN 2047-3338

Implementation of Traffic Engineering and Addressing QoS in MPLS VPN Based IP Backbone

Mushtaq Ahmed[1] and Abdul Basit[2]

[1,2]Department of Computer Science and Engineering, University of Engineering and Technology, Lahore, Pakistan

***Abstract*– With increasing popularity and ever emerging business needs there was an immense focus to improve the Internet world and to provide guarantee for service delivery. Simplest example for this case is VoIP where two subscribers make a voice call through MPLS based backbone. The end subscribers should have similar quality as that of POTS. Subscribers will expect a real time conversation with limited or no jitter. A guaranteed bandwidth must be provided to VoIP users as they don't care about core network which logically should be transparent to end users. Another feature of MPLS called Quality of Services (QoS) addressed these issues effectively by ensuring real time conversation and guaranteed bandwidth. VPN is a tunnel through Internet to connect two different local area networks in a strict security and data encryption techniques. MPLS VPN use peer to peer VPN which merges the salient feature of Overlay VPN model and peer to peer VPN. In this paper we have enlighten MPLS introduction, MPLS VPN, Traffic Engineering and MPLS QoS in MPLS IP backbone. We have provided connectivity to different customers in MPLS backbone by implementing MPLS VPN and Provide Quality of Service to these customers locally in this backbone area. Also apply Traffic Engineering in MPLS backbone to optimize the backbone resources. On top of MPLS TE and MPLS QoS, we have also discussed MPLS QoS which guarantees less or no jitter and fixed bandwidth. Mainly we have used GNS3 for implementation and simulation.**

***Index Terms*– Traffic Engineering, MPLS, Implementation and Simulation**

I. INTRODUCTION

ROBUSTNESS of routing protocol and Scalability in addressing mechanism is main drivers of popularity of current internet world. Route Aggregation, Generalized multilevel hierarchical address (CIDR), Routing Protocols and Route Selection based on shortest path and considered to be main constituent of internet scalability. There are many performance bottlenecks in today's internet in terms of IP address lookup, Traffic engineering and best effort delivery. So what service provider came up with is to use ATM as a backbone solution. ATM uses short fixed length packets called cells where we use VC based switching in core network which have QoS parameters associated with them. ATM also provides Traffic engineering as it takes into account to distribute traffic on all links in a way that none of links is underutilized and none of link is over utilized which is the major concern of all service providers. VC is selected between source and destination; it takes into account bandwidth available in each link, buffer capacity in each link and congestion condition on each link. An ATM over IP network in its simplest form is shown in Fig. 1.

As ATM network makes a VC from source to destination to start communication, so it was limited to backbone network and was not extended to end customers. Otherwise this will enormously increase the number of states and load in the core network as each VC for each connection will have to be saved in core network which ends up with highly loaded core network. That is why service providers used IP over ATM to get the best of both worlds that is QoS is achieved by ATM in core network and Robustness and Scalability is achieved by IP network at the edges. ATM was also taunted as high speed network to be extended up to end customer as initial ATM had a speed of 155 Mbps leading to 622 Mbps, but Ethernet also evolved from 100Mbps to 1Gbps then up to 10Gbps. So ATM was not extended to end customer and was limited up to core network. So we were using an Overlay model (IP over ATM) of different kinds and each had some drawbacks associated with it.

A) Classical IP Over ATM

There is a considerable segmentation and re-assembly overhead. You have IP packets of different lengths, but when they need to be forwarded into an ATM world, and then you have to convert them into 53 bytes fixed length packets in the ingress of ATM world. Then on the egress of ATM world,

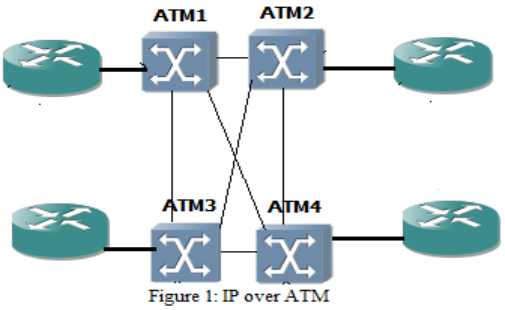

Figure 1: IP over ATM

when packet goes out of ATM world into IP world, packet needs to be re-assembled. This is a significant overhead that is *coming* in terms of 'Segmentation and Re-assembly'.

B) Next Hop Resolution Protocol (NHRP)

The major disadvantage of NHRP is the overhead in terms of identifying the hosts if they are in same cloud or if they are in different cloud. Second disadvantage is still same, that is 'Segmentation and Re-assembly' [3].

An Overlay model has many drawbacks as listed below.

1) In an overlay model to make communication between 'N' routers in IP network, we need to make a mesh of the order 'NxN'. In other words in ATM cloud, to make communication between 'N' routers in IP network we will have to have 'NxN' virtual circuits.

2) All the routers in IP world within same IP over ATM network are adjacent to each other. Each router maintains its neighborhood table and keeps record of all of its routers in same network. Now if there is a small topology update in the network then this update will be sent to all routers in same network. Keeping into mind N^2 mesh within IP over ATM network, there will be N^4 topology update messages for single topology update in network.

3) Huge computation is required with the increasing number of routers in IP over ATM network, consequently overall scalability is decreased.

4) We have two separate protocols running in same network which increases management complexity. We are running IP protocol on the edges and ATm protocol in core of the network. We need to manage both IP routing and VCs.

5) As ATM network within core is capable to provide QoS parameters, yet it is not possible to transfer QoS functionality from ATM world to outside IP world. In other words QoS available at link layer can't be extended to IP layer as IP is not supporting any QoS guarantee. So QoS quality of ATM network is also not there by using Overlay paradigm.

These all drawbacks motivated service provider to look for some alternative technique in core network and they came up with MPLS and achieved major goals like Network layer stability, High speed scalable switching and traffic engineering capabilities. Some salient features of MPLS are listed below.

1) LER (Label Edge Router) is located at the ingress of the network and LSR (Labeled switched Router) is located in core of the network. LER are bit more complex as they will classify incoming packets in their corresponding classes and also assign label paradigm. LSR are much simpler as they will be just swapping labels for each incoming packets and will be forwarding to next hop. MPLS is its simplest form is shown in Fig. 2.

2) A path is established between end points that want to communicate. This is just similar to establishment of VC between end points in ATM world.

3) Forwarding equivalence classes (FEC) are used in the ingress of the network. There are multiple FECs in ingress of the network based of the Traffic engineering and Quality of service parameters. Each FEC may be associated with an application layer flow, so classify the packets into flows and setup a path for each FEC or application flow. Each of FECs will be associated with label in ingress of the network.

4) In ingress of the network, the forwarding is based on labels instead of IP addresses. Labels may or may not be swapped with a New Label from hop to hop within the core network.

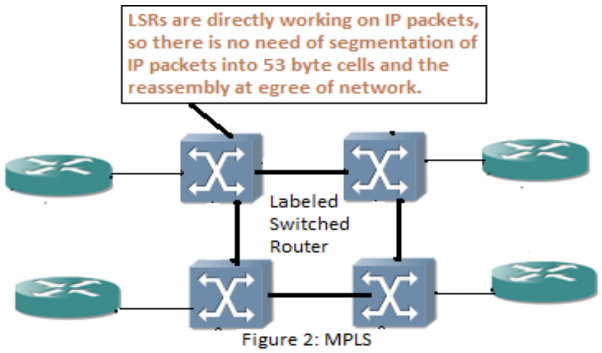

Figure 2: MPLS

MPLS is an IETF technique in which forwarding in core network is done based on 16 bit or 20 bit labels instead of 32 bit IP packets as in previous technologies like IP over ATM. MPLS classifies packets into classes called Forward equivalence classes and routes them over the backbone through a specific route. MPLS also ensures QoS parameters like bandwidth and voice quality. MPLS is called layer 2.5 protocols as it is encapsulated between layer 2 and layer 3 as shown in Fig. 3.

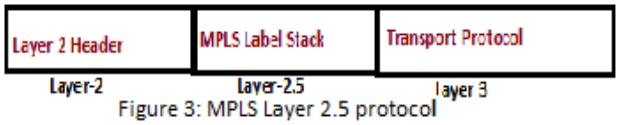

Figure 3: MPLS Layer 2.5 protocol

MPLS is mainly composed of Data Plane and Control Plane [4] and there are two modes of operation for MPLS called Cell mode MPLS and Frame mode MPLS [5]. There are various components of an MPLS network like Labeled Edge Router (LER), Labeled Switched Router (LSR), labeled distribution protocol (LDP) and forwarding equivalence class (FEC) that facilitate an MPLS based backbone to forward packets from source to destination from an optimal path (Traffic Engineering) with guaranteed delivery and assured bandwidth (Quality of Service) and hence making two end communicating users to feel like as if they are on same local area network (Virtual Private Network). There are various types of packets in MPLS based network like reserved labels, unreserved labels and unknown labels.

C) MPLS Services

As we have seen there are various benefits of MPLS that it delivers to service providers in their backbone network in terms of Virtual Private Network (VPN), Traffic Engineering (TE) and Quality of Service (QoS). We will explain these salient features of MPLS one by one to clarify how MPLS is existing in today's competitive era and why SP prefer MPLS

as backbone technology instead of its ancestor like ATM or Frame Relay.

D) MPLS Virtual Private Network (VPN)

Traditionally, VPN in provider network can be implemented in two ways:

1) Overlay Model

These are P2P links (leased line) where two end routers communicate with each other through service provider network. End routers don't participate in service providers internal routers, in other words service provider routers are transparent to end routers. Such P2P services can be either layer-1 like SONET, E1, E3 etc.; or layer-2 like Frame Relay, ATM or even it can be Layer-3. In overlay VPN models two protocols are running at the same time, one in service provider network and second one in customer network. For example IP over ATM is a famous example. IP is running in customer network and ATM is running in provider network that is why such networks are called Overlay models.

Service providers provide the customer with leased lines called Virtual Circuits (VCs) as shown in Fig. 4. Service provider network is invisible to a customer having three offices in different geographical locations. Customers having different offices at different locations feel like if all offices are on same Local Area Network (LAN) called Virtual Private Network (VPN).

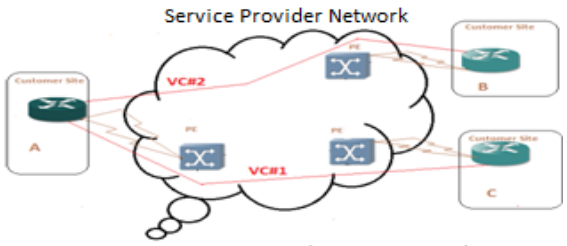

Figure 4: MPLS Virtual Private Network

Service provider network is transparent from customer perspective, customer sites will look like connected to each other like a LAN (virtual) as shown in Fig. 5:

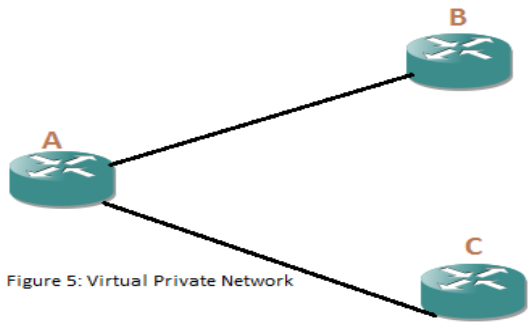

Figure 5: Virtual Private Network

There are certain drawbacks of Overlay VPN model

- It is useful when we have less central sites and more remote sites. VC will be established only for central sites. So it is more useful for non-redundant configuration and becomes more complex with increased number of mesh circuits.
- In order to establish VC, we need to know site by site profiles for all customer sites which may or may not be available at the time of implementation.

2) Peer to peer VPN Model

Peer to Peer VPN model is shown in Fig. 6:

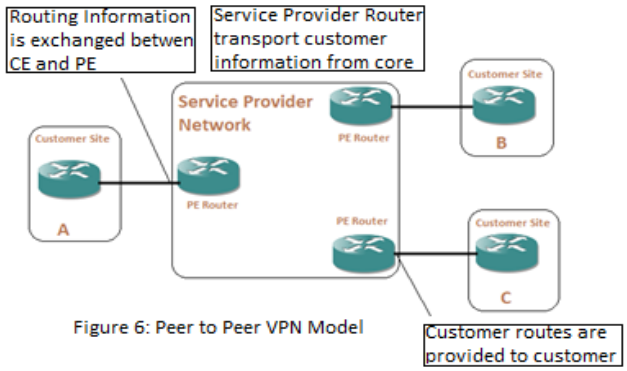

Figure 6: Peer to Peer VPN Model

This model was introduced to overcome the drawbacks of Overlay model. Here PE device is a router that directly communicates with customer router and routing information is exchanged and transported through service provider network to customer router in other site in Fig. 6. There are certain advantages of Peer to Peer VPN like customer router and PE router are directly working on Layer-3 and start exchanging routing information with each other, so there is no limitation in terms of mesh of VCs anymore. The QoS parameters like committed information rate, committed access rate are much simpler with this approach.

E) MPLS Traffic Engineering

Routing protocol determines the shortest path to transfer packets between source and destination, based on minimum number of hops. Congestion on the link or bandwidth of the link or available bandwidth of link is not taken into account. In this case some of the routes in SP network will remain underutilized and others will remain over utilized that can be controlled by applying some specific rules. For example, we can implement in the routing protocol to follow the route based on congestion that will lead to some other complications like routes flapping or oscillation which is also not desired in service provider networks. So the major objective is traffic should always be evenly distributed among all paths in service provider network [1].

MPLS provides solution to such kind of issues by enabling tunnels between routers to transport information from source to destination. These tunnels are established based on available BW on specific link, as we are looking at available BW on link before enabling tunnel so there is no chance of overload on that specific link as shown in Fig. 9:

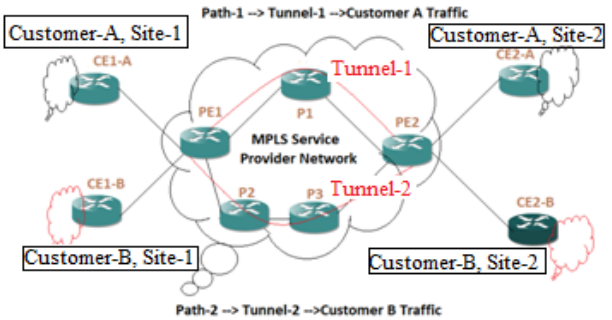

Figure 9: MPLS Traffic Engineering Tunneling

MPLS classifies the traffic of customers based on BW requirement and available path having required BW. TE tunnels have following set of properties.

- TE Tunnel has start point (ingress of MPLS network) and end point (egress of MPLS network). It also takes into account the Bandwidth requirement of customer and Class of Service (CoS) for data.
- Each tunnel follows a specific path within the network called LSP (Label switch path) which is defined by Label switching protocol (LDP). Tunnels can reroute data to any path in SP network unless otherwise defined strictly. In case of primary route failure of a tunnel, it takes secondary route, an important property of MPLE TE.
- Labels are applied to forward packets from CE to egress PE them to ingress PE through set of P routers within MPLS network. IS-IS or OSPF is used to carry information like available BW on link within tunnel. It enables tunnel to select correct route which is not congested. RSVP (Resource Reservation Protocol) is used for signaling within MPLE TE environment.
- MPLS TE is basically Constraint Based Routing (CBR) which makes sure the availability of multiple paths between source and destination. It is implemented at ingress PE router with IGP (OSPF or IS-IS).

Constraint Base Routing (CBR) results is an ordered list of IPs to identify next hop in tunnel. CBR calculation is done by ingress PE router in MPLS domain; none of P router participates in CBR calculation. Basically PE router transfers CBR calculation to all routers within tunnel while it sends RSVP signaling to check resource availability. Resources are reserved by RSVP and TE on each Labeled switched router (LSR) in tunnel path, LSP (labeled switched path). Objects and messages in RSVP signaling to support TE in MPLS based backbone are given in Table 1:

Ingress PE router sends PATH message in TE Tunnel (LSP). PATH message from ingress PE router is received by 'P' router in MPLS domain where explicit_Route is checked based on L-bit value. If destination router is not directly connected, then PATH message is routed to next hop via Record-Route Object. Finally RSVP PATH message is received by Egress PE Router of MPLS network which generates 'RESERVATION' message. This is stage where label assignment is started and Reservation message is sent in upward direction. A POP label is assigned at egress PE

Message	Object	Functionality
PATH	Label_Request	PATH message is sent by ingress PE router and collects label routing for TE tunnel (LSP) from all core routers involves (P routers).
PATH	Explicit_Route	This message is also sent by ingress PE router. It defines a specific path for a tunnel.
RESERVATION	Label	This message is generated by egress PE router and allocates Labels to TE path (LSP) and sends it backwards to ingress PE router.
PATH, RESERVATION	Record_Route	It can be generated by ingress PE (in case of PATH message) or it can e generated by egress PE (in case of RESERVATION message). The idea is to notify the originating node (ingress PE or egress PE) about the original LSP
PATH	Session_Attribute	Defines session attributes for TE LSP.

Table 1: RSVP Objects and Messages

router and sent backward (uplink) direction and Route_Record object is re-initiated at this stage. This RESERVATION label then propagates to 'P' router and label assignment and next hop in Record-Route object are appended and sent to next hop [7]. Next hop in my case is Ingres PE router. When RESERVATION message reaches ingress PE router, then Record-Route carries LSP tunnel for TE and labels (it also carries BW requirement and other QoS parameters) assigned that need to be swapped at each hop within tunnel.

CBR is basically an extension of CSPF (constrained shortest path first) and CSPF is an extension of SPF (Shortest path First). Main idea is to route the traffic from source to destination through the shortest path from network (SPF) but with some constraints like bandwidth availability, link metric (CSPF). MPLS TE widely uses the extension of CSPF called CBR. CBR in context of MPS is also known as CR-LDP [1].

CBR selects the shortest path within backbone network but, the only requirement is the resource availability and resource requirements which are evaluated based on set of rules and constraints. Let us consider we have to select a path from PE1 to PE2 as shown in Fig. 10 and we need 20 Mbps on that specific LSP. In this case the only best option is PE1→P2→P3→PE2 as it guarantees 20 Mbps throughout the path while rest of two paths can't.

Internet world provides host to destination communication based on best effort and there is no QoS guarantee. With increasing popularity and ever emerging business needs there was an immense focus to improve QoS and to provide guarantee for service delivery. IETF came up with multiple solutions like RSVP, DiffServ, MPLS for improving the scalability of internet world [2], [3]. CBR selects path in backbone network that is subject to certain constraints [2] in

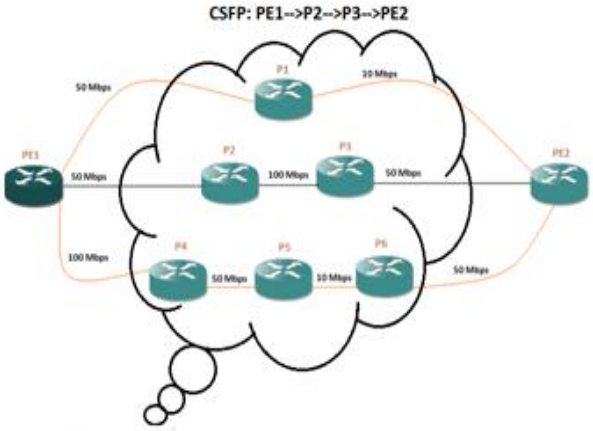

Figure 10: MPLS Constrained Based Routing (CBR) and Shortest Path First (SPF)

terms of Bandwidth and certain QoS parameters. CR-LSP not only considers network topology to calculate LSP but also considers some other constraints that can result in longer less loaded LSP compared to shorter congested LSP. This feature is basically the main requirement of every ISP so that all of their routes in backbone network are properly and well utilized so that none of routes of underutilized and none is over utilized. From provider interest, an administrator is configuring the LSPs by keeping into mind the individual constraint of LSP itself and then constraints at network level. CR-LDP being capable of distributing traffic evenly in provider network is highly appreciated in MPLS TE.

F) MPLS Quality of Service

Internet world provides host to destination communication based on best effort delivery. With increasing popularity and ever emerging business needs there was an immense focus to improve internet world and to provide guarantee for service delivery and some other parameter like guaranteed bandwidth and minimum or no jitter. There are a series of applications that require real time communication without delay or minimum delay that is not considerable; such applications include Voice over IP (VoIP), session initiation protocol trunk (SIP-T), Ethernet Virtual Private network (E-VPN), Internet Protocol Virtual Private network (IP-VPN) and some other applications like secure finance transaction or online money transfer. Such applications require real time communication with minimum or no delay and fixed BW.

QoS is a mechanism to prioritize set of traffic over another set of traffic [4] QoS is a network feature (not device parameter) that enables Service provider to control set of attributes like Jitter (especially for VoIP), bandwidth (Queues allocation), and packet loss which have immense importance for end users for real time conversation and application sharing. Service provider should have QoS implemented in their network to fulfill grooming business requirements and to meet ever changing demands of end customers with thrilling groom in IT world. Service providers use queues in their network to differentiate different kind of traffic, important or real time information is given high priority to rest of information. There are eight queues (0→7) in provider network, 0 having highest priority and 7 having least priority.

MPLS QoS is more scalable compared to IP QoS because it aggregates flows at PE router and forwards aggregated routes from core in the form of Forward Equivalence class. The only difference of IP QoS and MPLS QoS is that, PREC/DSCP bits are not visible to MPLS LSR as they are working on Labels not IPs. The solution was to map PREC/DSCP bits into EXP field of MPLS Label. So the idea is to map 6 PREC/DSCP bits into 3 Exp bits of MPLS label to make it visible by Labeled Switched Router, this mapping is shown in below Table 2

Forwarding	DSCP Values	EXP Values
EF → Extended Forwarding	101110	101
AF1 → Assured Forwarding	001010	001
	001100	
	001110	
AF2 → Assured Forwarding	010010	010
	010100	
	010110	
AF3 → Assured Forwarding	011010	011
	011100	
	011110	
AF4 → Assured Forwarding	100101	100
	100100	
	100110	
BE --> Best Effort	000000	000

Table 2: Mapping 6 DSCP into 3 EXP Bits of MPLS Label .

II. METHODOLOGY

We used GNS 3 for simulation of MPLS based VPN, Traffic engineering and Quality of Service for two different customers as shown in Fig. 13.

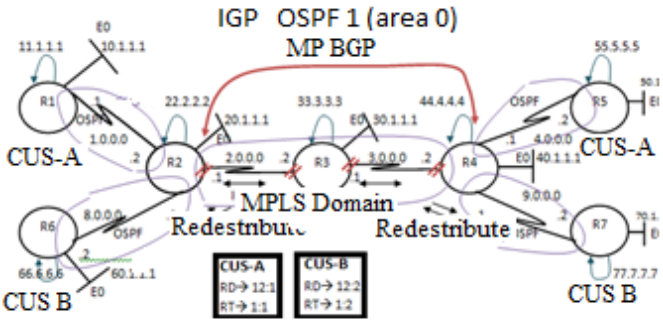

Figure 13: MPLS VPN, TE, QoS Implementation

There are 8 major steps that contribute to achieve overall tasks (VPN, TE, QoS):

i. Client OSPF
ii. Service Provider – OSPF + MPLS
iii. VRF - A & B
iv. Assign Interface to VRF
v. Run OSPF for VRF
vi. MP-BGP
vii. Redistribution
viii. Import

III. RESULTS

When we compare the graphs obtained by conventional SP network with MPLS based SP network, a clear improvement in performance can be observed. Data rate of a conventional IP network and MPLS based network are as shown in Fig. 14 and Fig. 15.

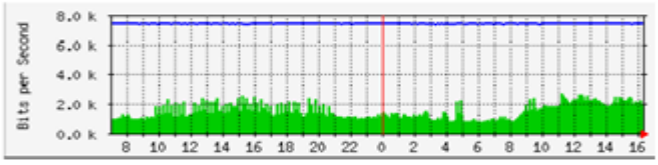

Figure 14: Data rate using conventional IP based network

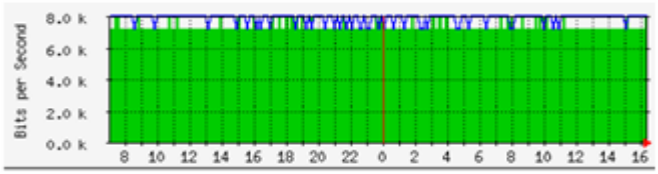

Figure 15: Data Rate using IP MPLS TE

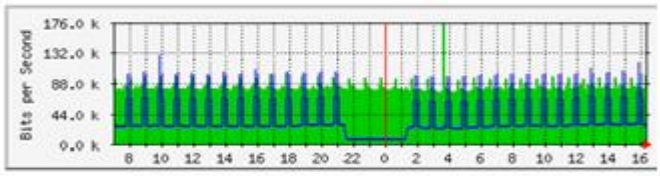

Figure 16: Jitter Rate using conventional IP Based network

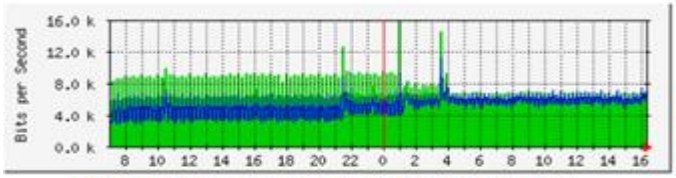

Figure 17: Jitter Rate using IP MPLS Network

We observed similar improvement for jitter using conventional IP network and MPLS based network as shown in Fig. 16 and Fig. 17.

IV. CONCLUSION

MPLS is an optimal choice by service providers in their backbone network to forward packets from source to destination from an optimal path (Traffic Engineering) with guaranteed delivery, assured bandwidth and minimum or no jitter (Quality of Service) and hence making two end communicating users to feel like as if they are on same local area network (Virtual Private Network).

REFERENCES

[1]. B. John Oommen, Sudip Misra, Ole-Christoffer Granmo, "Routing Bandwidth-Guaranteed Paths in MPLS Traffic Engineering: A Multiple Race Track Learning Approach," IEEE Transactions on Computers, vol. 56, no. 7, pp. 959-976, July 2007, doi:10.1109/TC.2007.1045

[2]. Cisco IOS MPLS Configuration Guide, by Cisco Systems 2nd Edition.

[3]. Traffic engineering 3rd Edition, by Adrian Farrel

[4]. Advanced MPLS Design and Implementation, by Vivek Alwayn.

[5]. http://www.cs.cornell.edu/courses/cs619/2004fa/documents/mpls.te.pdf

[6]. MPLS study guide, by James Reagan.

[7]. http://www.cisco.com

[8]. Generalized MPLS and their application version 2, by Neil Jerram.

[9]. How to implement quality of service across MPLS version 1, by Ben Wright.