International Journal of Computer Applications (0975 – 8887)
International Conference on Computer Technology (ICCT 2015)

Implementing QOS Policy in MPLS Network

Vishal H. Shukla
ME Student
DJSCOE
Vile Parle (west), Mumbai-56

Sanjay B. Deshmukh
Asst. Professor
DJSCOE
Vile Parle (west), Mumbai-56

ABSTRACT
Quality of Service (QoS) is defined as those methods which enables network managers to organize the combination of bandwidth, delay and packet loss in the network. The main motive of QoS is to offer different levels of services for different types/classification of traffic in the network. QoS capabilities allow service providers to prioritize service groups, assign bandwidth, and avoid jamming. In this paper few QoS strategies are executed in a MPLS based network and simulate variable parameters for performance analysis purposes.

Keywords
MPLS; QoS Policy; GNS3

1. INTRODUCTION
From a Service Providers (SP) approach, one of the main goals to allow QoS is it has multiple different levels of customers buying different levels of service. First step here is to make sure that as the traffic enters the network it must be followed with whatever agreed up service level agreement between the provider & the customer , so that is what mainly considered an admission control from the customer edge(CE).Now, typically this is where customer bought the service level agreements from service provider. In order to actually enforce this, mainly the SP is applying the classification scheme of CE. That involved SP to look at the DSCP/IP precedence to MPLS EXP mappings. The Internet Engineering Task Force (IETF) has defined two models for QoS implementation: Integrated Services (IntServ) and Differentiated Services (DiffServ). IntServ trails the signaled QoS model, where the end users indicate their QoS need to the network for reservation of bandwidth and device resources. DiffServ works on the conditioned QoS model, in which network elements are associated to examine various classes of traffic with varying QoS conditions. [1].Once the traffic is received from the customer the SP is concerned with the transiting the traffic through SP core. Now as the traffic goes from the edge and has admitted to the network, the network admin has to ensure that some sort of classification scheme need to be done that once got into the core, also could distinguish that from the non-real time flows of traffic and make sure that traffic is prioritized. The idea behind the integrated service model is that the actual in point of the network has to request specific type of service for an individual flow as compared to the differentiated Service model; where the guarantee is based on the actual configuration & classification of the network. [2] In common cases DiffServ Model is observed. The only thing falls in the IntServ QoS model is the RSVP which is used for MPLS-TE. The original design goal of RSVP & IntServ Model is that it is up to the Host to find the type of service required from the network like guaranteed bandwidth, low latency, etc. so it is up to the application to figure that out. This is assumed that the transit network would enforce the level of service the application is trying to store, but practically it is not really achievable to do that since the amount of control plane information that the network required to maintain gets quickly out of control. So the only way to overcome this is to implement MPLS traffic engineering. After categorization of traffic, different markings are used in SP network to actually enforce the QoS policies. [3] The DiffServ Model basically provides the attributes that will help in the data plane to tell the difference between different types of traffic. One of the difficult thing is actually implementing DiffServ Model in SP network is that as the traffic is transiting the core, the routers are no longer be able to classify based on the information in the layer 3 Header, since in the MPLS network the routers in the core are not making decisions based on IP header but make decisions based on MPLS label, that means the admin has to take this marking of layer 3 header to move down further to MPLS header and this is what the MPLS –EXP bits are used to achieve. Now when the MPLS label imposition at ingress PE & label disposition at egress PE router is done, the issue is that there must be some way to correlate what is previously in the layer 2 MPLS-EXP bits & how it should be correlated with the layer 3 DSCP /IP precedence and that has to be done with the order of operation of problem of QoS classifier on the router. The solution to this is locally significant value that could be used in order to pass the information from the egress to the ingress interface without having to actually remarking any traffic of the customer that is sending. Once the traffic is classified, traffic could be prioritized, planed for low-latency like weighted fair queue (WFQ), weighted round robin (WRQ) or congestion avoiding techniques like weighted random early detection (WRED). This is actually would be the QoS enforcement once the different types of traffic are found. [4]

2. IMPLEMENTED METHODOLOGY
This topology is implemented on Graphical Network Simulator 3 (GNS3), where the MPLS-VPN is implemented using 7200 series of routers presented in the service provider network & 3640 series of routers are presented in customer networks. [5]

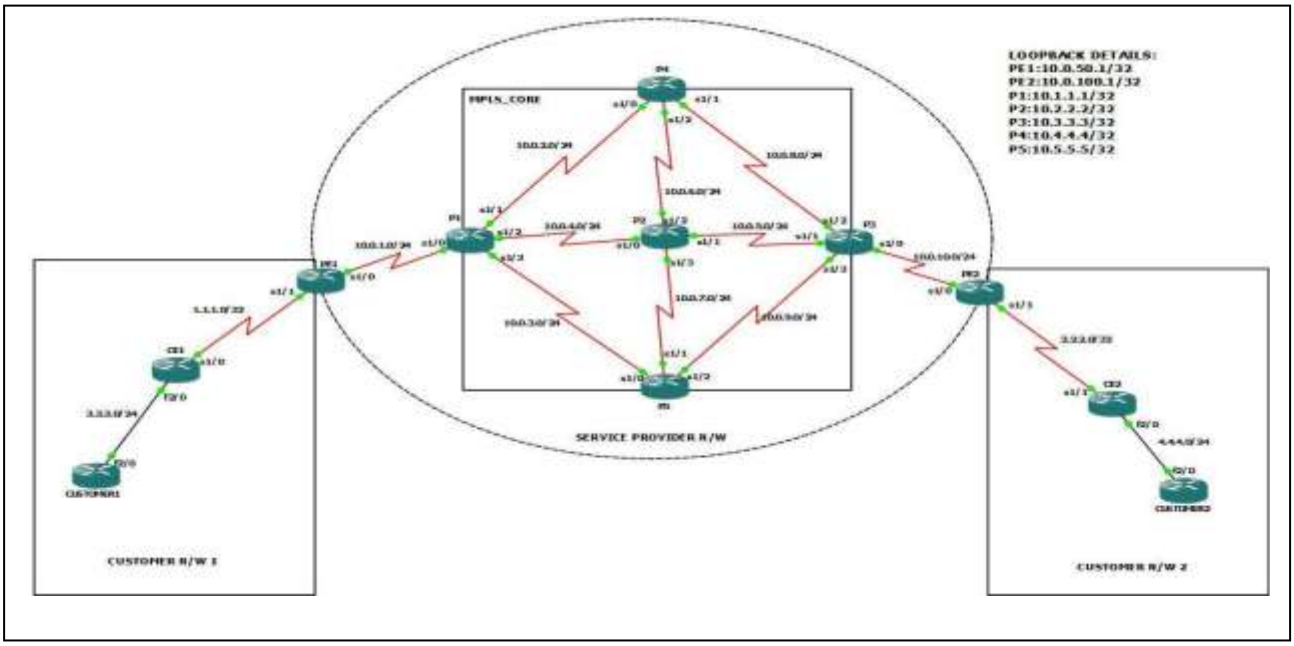


Fig 1: Network Topology.

In this implementation different QoS policies are configured, classified, marked & prioritized. So 2 routers are taken at Customer Edge (CE) i.e. customer1 & customer2 they aren't attached to provider network at all. On the ingress of both customer1 & customer2 routers from CE there is going to be a customer QoS policy ,which would look for some precedence value and run a counter on how many of those packets have received. At this point the Layer 3 MPLS-VPN is preconfigured [6] so on cusomer1 router respective routes are checked in the routing table. At this point the customer1 should reach customer2 to make sure basic connectivity through the configured SP network is formed. [7]Now on router (customer1 & customer2), basic QoS policy is configured that would simply match the traffic based on the precedence values. So for Modular QoS CLI (MQC) implementation there are 3 steps:

1. Classify traffic for the Class map.

2. Define the QoS policy with Policy map.

3. Apply service policy at the particular interface.

So here first class maps for all different precedence value are defined and then in policy map individual class maps have been called. This is used as a basic counter for what type of traffic is received from the other side of the network. After this QoS policy is applied. Here the focus is on matching the type of traffic so a MATCH policy is defined. Now in the policy map all the classes which are defined previously have been called, just to use them as a counter.At this time the service policy is applied on the ingress/entrance of the customer1 router i.e.; interface f2/0. So on this link, number of packets basically is observed for different classes.Now, same policy is configured on customer2 as well. In order to test this, traffic is generated. So on customer2 telnet traffic is generated. Thus on customer1 a bunch of hits is observed on precedence 6; since its telnet traffic by default.Now, when the MPLS core is observed, when a debug of MPLS packet is done, some of the control plane protocols like BGP keep-a-lives would have an EXP bit value 6 which depicts that by default when the router is doing IP to MPLS imposition condition, it is automatically copying the precedence value from layer 3 header to the EXP bits of MPLS layer 2 header.[8. Another way to observe this, is that to mark the traffic as it is leaving the CE router going out to PE router. So in addition to this match policy, mark policy is configured .i.e. changing the classification as traffic is leaving from CE to PE and this is done on both CE1 & CE2.Now to observe the difference between some of the different flows which can be done based on different types of applications like basic testing applications: ICMP ping, TELNET, TFTP, FTP. Now basic traffic flows are generated from customer1 & customer2 to observe when those different types of traffic are sent into the network how they are got differentiated when they reach the other end. [9]So 4 different types of flows are generated to figure out what are their markings when they get to the other end. Now as this traffic is leaving the network, so out bound on s1/0 a policy map MARK is configured. [10] In order to watch how many packets are marked initially show policy-map command is used.Now as the traffic is being received in from the customer some sort of service level agreement is applied. So here the traffic got categorized with respect to the priority.

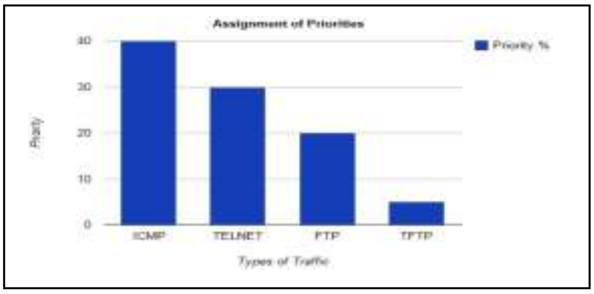
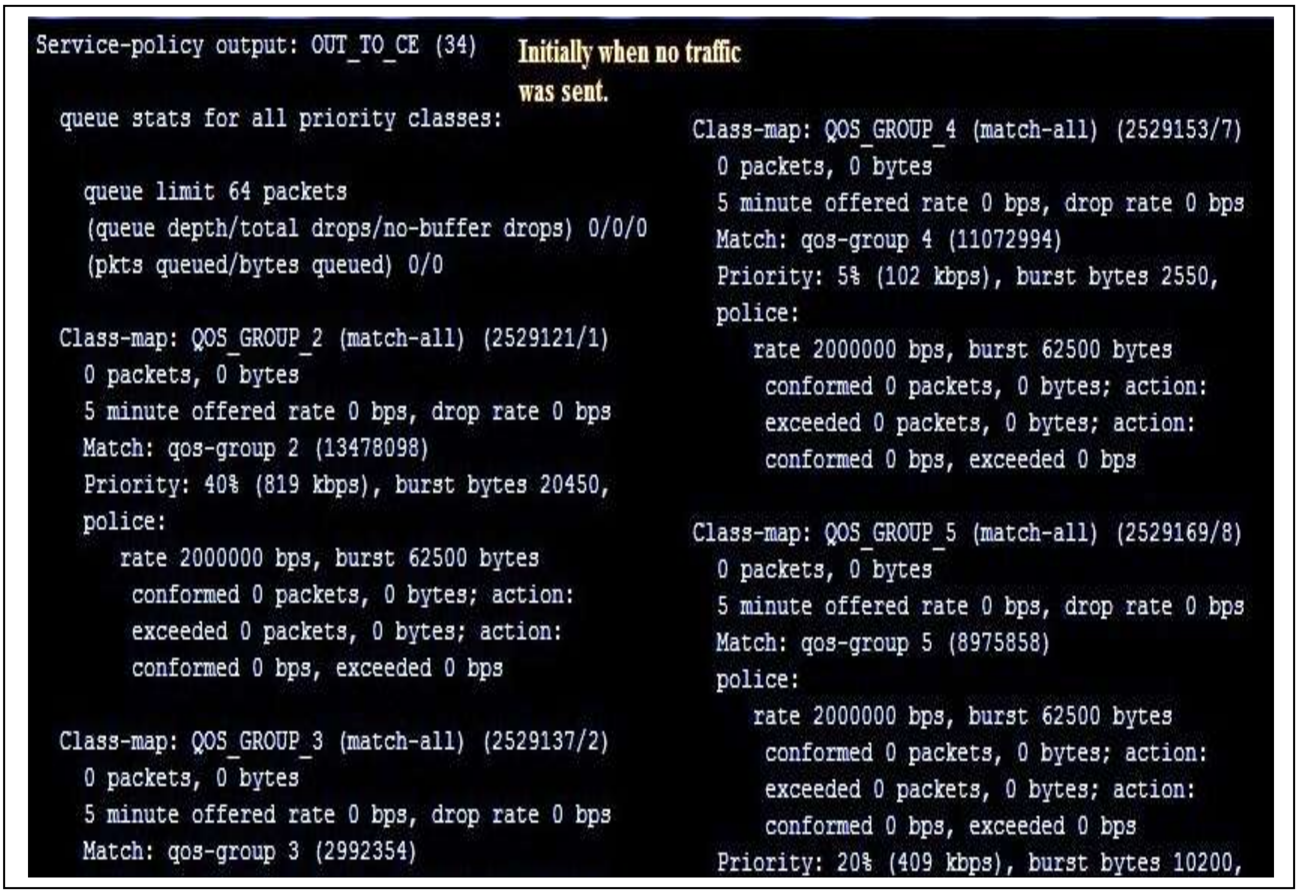


Fig 2: Assignment of priorities to different classes.

Thus the highest priority is assigned here i.e., to the ICMP and the least priority is assigned to the TFTP which results the ICMP traffic to travel faster than the TFTP in the network. Now from the router PE1 perspective here for ICMP, TELNET, TFTP & FTP traffic priority in terms of percentage of bandwidth available in the network is set as 40, 30, 5 and 20 respectively. Now, finding the trace of this traffic along the path as it exits & get towards PE2,i.e, from CE1 to CE2 so that this policy gets maintained end-to-end, the exact same policy is configured on the PE2 as well and the traffic is scheduled on the exit interface of PE2 towards CE. Here the issue is that the PE2 wants to extend their QoS policies on the last hop link and this is done by QoS groups. So in the PE2, if the traffic is experimental bit 2 then it would be set to QOS_GROUP_2 for ICMP and if the traffic is experimental bit 3 then it would be set to QOS_GROUP_3 for TELNET and so on for the rest of the types. Then the traffic is moved to the interface going to the customer, it will check the QoS group and if it’s there then assign it to the specific queue which is desired. After the proper configuration of the service policy on both the PE routers it has been observed the policy map which now consist of four QoS group. Initially when no traffic is sent between the customers the policy map on PE2 router shows zero counters for all the groups.




```
Service-policy output: OUT_TO_CE (34)

  queue stats for all priority classes:

    queue limit 64 packets
    (queue depth/total drops/no-buffer drops) 0/0/0
    (pkts queued/bytes queued) 0/0

  Class-map: QOS_GROUP_2 (match-all) (2529121/1)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: qos-group 2 (13478098)
    Priority: 40% (819 kbps), burst bytes 20450,
    police:
       rate 2000000 bps, burst 62500 bytes
        conformed 0 packets, 0 bytes; action:
        exceeded 0 packets, 0 bytes; action:
        conformed 0 bps, exceeded 0 bps

  Class-map: QOS_GROUP_3 (match-all) (2529137/2)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: qos-group 3 (2992354)

  Class-map: QOS_GROUP_4 (match-all) (2529153/7)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: qos-group 4 (11072994)
    Priority: 5% (102 kbps), burst bytes 2550,
    police:
       rate 2000000 bps, burst 62500 bytes
        conformed 0 packets, 0 bytes; action:
        exceeded 0 packets, 0 bytes; action:
        conformed 0 bps, exceeded 0 bps

  Class-map: QOS_GROUP_5 (match-all) (2529169/8)
    0 packets, 0 bytes
    5 minute offered rate 0 bps, drop rate 0 bps
    Match: qos-group 5 (8975858)
    police:
       rate 2000000 bps, burst 62500 bytes
        conformed 0 packets, 0 bytes; action:
        exceeded 0 packets, 0 bytes; action:
        conformed 0 bps, exceeded 0 bps
    Priority: 20% (409 kbps), burst bytes 10200,
```

Fig 3: Initial output of policy map on the output interface of router PE2.

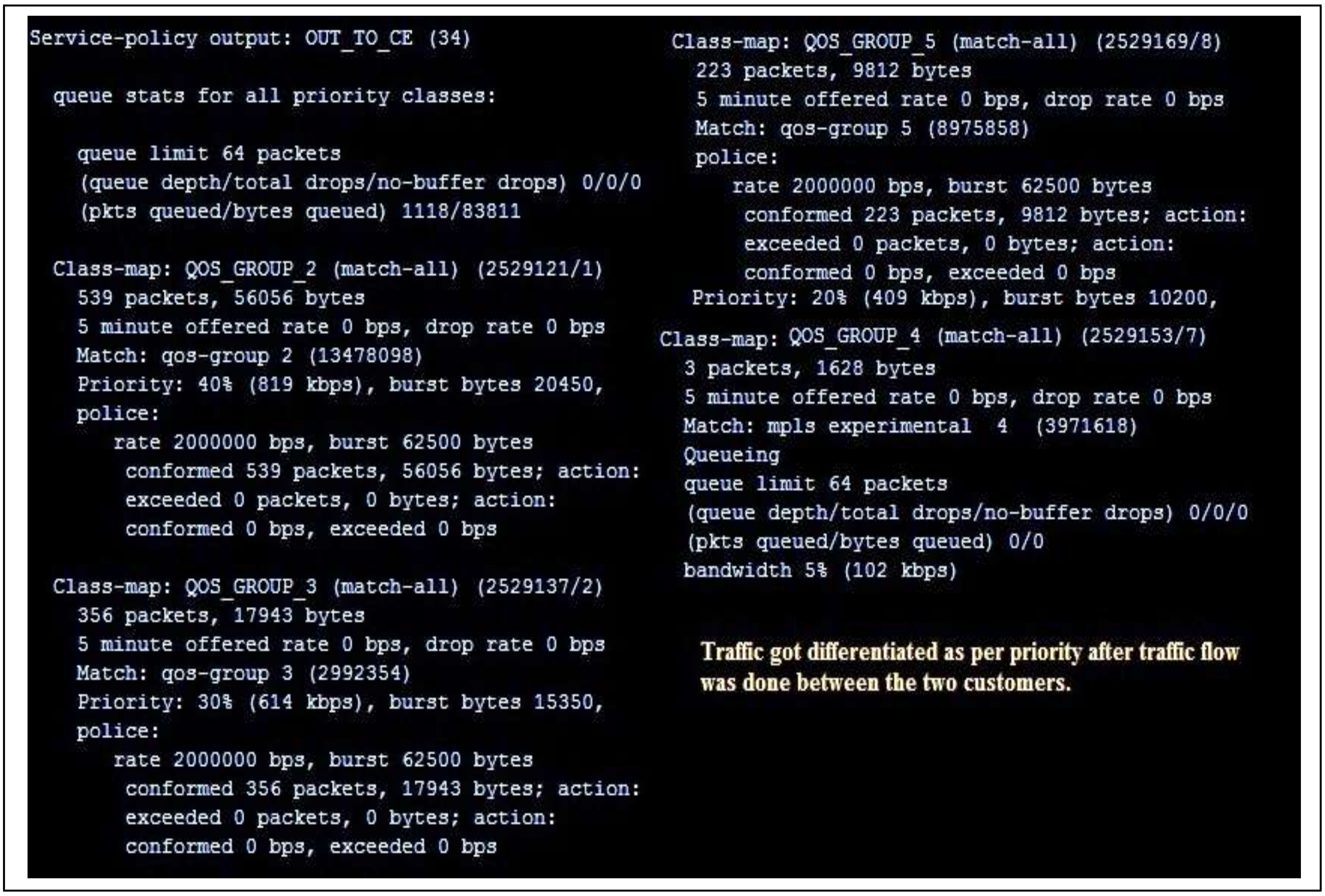


Fig 4: Final output of policy map on the output interface of router PE2.

So from the final output it's observed that when a lot of traffic has generated between the customers, the Service provider network has done its classification into ICMP, TELNET, FTP and TFTP and gave the proper hits on the QoS groups which have configured earlier. Also the traffic which has higher priority transmitted with faster rate.

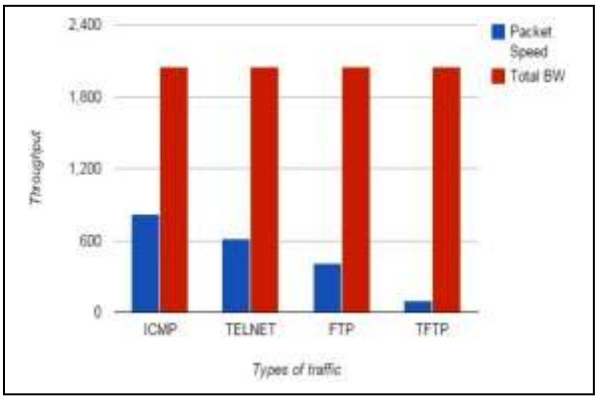


Fig 5: Packet speed throughout the network.

From the above graph it's observed that the ICMP traffic which is set to highest priority provides higher throughput than the TFTP traffic which is set to the least priority level.

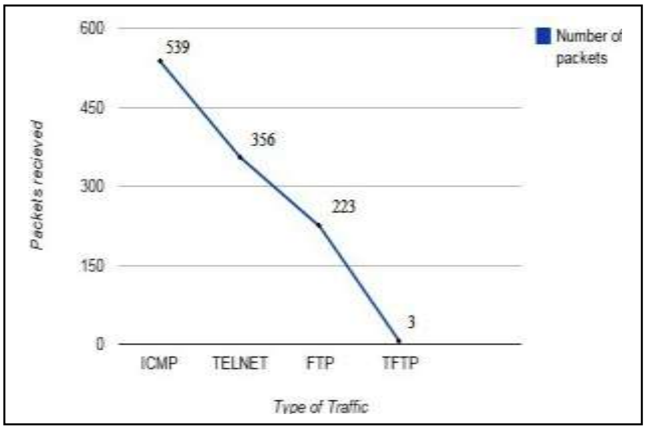


Fig 6: Packets received for different types of traffic.

Also from the above graph it's observed that ICMP packets have received more with lesser delay since the priority percent of bandwidth is highest of ICMP than to TFTP. This shows that if the demand is to make the applications which are least tolerable to delay and packet loss it can be prioritized to higher priority than to those applications which can afford small amount of delay. Also, it's monitored that the classification, marking & service polices have been working properly. It is also observed that the SP core by default isn't changing the customer's marking when IP to MPLS imposition & MPLS to IP disposition is performed so these routers in the MPLS core aren't changing anything in the IP header, which is on the design point of view, the majority of time it's mandatory that the SP really not want to be involved in finding the customer marking.

3. CONCLUSION

Hence by implementing the QoS policies in the MPLS VPN network it's capable to differentiate the traffic between two customers at remote site and as from a Service Provider point of view it is vital to categories traffic in order to provide proper services by assigning proper service level agreements. By this guaranteed Bandwidth with less congestion would be achieved. Future scope of this implementation is that the next generation networks require high QoS guarantees so the Multi- Service Core Network tries to achieve sufficient QoS provisioning by adopting an application-based MPLS network. This would optimize the network and would provide various services to multiple customers efficiently.

4. REFERENCES

[1] Vivek Alwayn, "Advanced MPLS Design & Implementation"- Cisco Press, 2002.

[2] Eric Osborne,Ajay Simha, "Traffic Engineering with MPLS technology" – Cisco Press, 2002.

[3] John Evans and Clarence Filsfils: "Deploying IP and MPLS QOS for Multiservice Networks: Theory and practice", Morgan Kaufmann Publishers is an imprint of Elsevier, USA, 2007.

[4] Santiago Alvarez, "Qos for IP/MPLS network"-Cisco Press, 2006.

[5] Wendellodom, Michael.J.Cavanaugh, "Cisco QoS Guide-2nd Edition"-Cisco Press,2005.

[6] Rosen E., Viswanathan A., & Callon R.: "Multiprotocol Label Switching Architecture", IETF RFC 3031, 2001.

[7] B.S. Davie, and Yakov Rekhler, "MPLS: Technology and Applications", Morgan kaufmam, 2000. ISBN 1-55860-6564.

[8] Mahesh Kr. Porwal, Anjulata Yadav and S.V.Charhate, Traffic Analysis of MPLS and Non MPLS Network including MPLS signaling Protocols and Traffic distribution in OSPF and MPLS, IEEE 2008.

[9] Thaeyoung Lee, "Multiprotocol label switching (MPLS) and differentiated services (DS) as quality of service (QoS) solutions"-ICACT, 2005.

[10] Brian McGahan, "Service Provider Advanced Technologies.version3"-INE, Inc, 2013.