IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 10, Issue 1, Ver. III (Jan - Feb. 2015), PP 61-72
www.iosrjournals.org

QOS of MPLS

Wesam Salah Dawood Khalil[1] Dr.Amin Babiker A/Nabi Mustafa[2]
Departmentof Communications, Faculty of Engineering, Al- Neelain University Khartoum, Sudan
Department of Communications,Faculty of Engineering, Al-Neelain University Dean of Faculty Khartoum, Sudan

Abstract: *Multiprotocol Label Switching (MPLS) is a standards-approved technology for speeding up network traffic flow and making it easier to manage. MPLS involves setting up a specific path for a given sequence of packets, identified by a label put in each packet, thus saving the time needed for a router to look up the address to the next node to forward the packet to.*
In this paper OPNET simulator is used to analyze MPLS network **.**
Keywords: *BGP, MPLS, VPN, PE , ATM , IP, QoS, LSP.*

I. Introduction

MPLS is an IETF initiative that integrates Layer 2 information about network links (e.g. bandwidth, latency, utilization) into Layer 3 (IP) within a particular autonomous system, or ISP, in order to simplify and improve IP packet exchange. MPLS gives network operators a great deal of flexibility to divert and route traffic around link failures, congestion, and bottlenecks.

MPLS is called multiprotocol because it works with the Internet Protocol (IP), Asynchronous Transport Mode (ATM), and frame relay network protocols. With reference to the standard model for a network (the Open Systems Interconnection, or OSI model), MPLS allows most packets to be forwarded at the Layer 2 (switching) level rather than at the Layer 3 (routing) level. In addition to moving traffic faster overall, MPLS makes it easy to manage a network for quality of service (QoS). For these reasons, the technique is expected to be readily adopted as networks begin to carry more and different mixtures of traffic.

From a quality of service QoS standpoint, ISPs will better be able to manage different kinds of data streams based on priority and service plan. For instance, those who subscribe to a premium service plan, or those who receive a lot of streaming media or high-bandwidth content can see minimal latency and packet loss. When packets enter a MPLS-based network, Label Edge Routers (LERs) give them a label (identifier). These labels not only contain information based on the routing table entry (i.e. destination, bandwidth, delay, and other metrics), but also refer to the IP header field (source IP address), Layer 4 socket number information, and differentiated service. Once this classification is complete and mapped, different packets are assigned to corresponding Labeled Switch Paths (LSPs), where Label Switch Routers (LSRs) place outgoing labels on the packets. With these LSPs, network operators can divert and route traffic based on data-stream type and Internet-access customer.

1.1 MPLS advantages

- MPLS enables a single converged network to support both new and legacy services, creating an efficient migration path to an IP-based infrastructure. MPLS operates over both legacy (DS3, SONET) and new infrastructure (10/100/1000/10G Ethernet) and networks (IP, ATM, Frame Relay, Ethernet, and TDM).
- MPLS enables traffic engineering. Explicit traffic routing and engineering help squeeze more data into available bandwidth.
- MPLS supports the delivery of services with Quality of Service (QoS) guarantees. Packets can be marked for high quality, enabling providers to maintain a specified low end-to-end latency for voice and video.
- MPLS reduces router processing requirements, since routers simply forward packets based on fixed labels.
- MPLS provides the appropriate level of security to make IP as secure as Frame Relay in the WAN, while reducing the need for encryption on public IP networks.
- MPLS VPNs scale better than customer-based VPNs since they are provider-network-based, reducing the configuration and management requirements for the customer.[1]

1.2 How does an MPLS enabled router distinguish between a labeled and unlabelled frame

protocol types were defined above Layer 2. These protocols modify Layer 2 protocol's protocol identifier. In case of Ethernet, Ethertype value is changed to 0x8847 or 0x8848. On a point to point link using PPP as layer 2 protocol, a new Network Control Protocol called MPLS Control Protocol (MPLSCP) was made. For MPLS packets, PPP protocol field value is changed to 0x8281. [2]

1.3MPLS Architecture
To understand the inner workings of MPLS its two major components have to be introduced:

Control plane: Takes care of the routing information exchange and the label exchange between adjacent devices.

Data plane: Takes care of forwarding either based on destination addresses or labels.
There is a large number of different routing protocols such as OSPF, IGRP,
EIGRP, IS-IS, RIP, BGP, etc. that can be used in the control plane.
The control plane also requires protocols to exchange labels, such as:

- Tag Distribution Protocol [TDP] (MPLS)
- Label Distribution Protocol [LDP] (MPLS)
- BGP (MPLS virtual private networks [VPNs])
- Resource-Reservation Protocol [RSVP] (MPLS Traffic Engineering [MPLSTE])
- CR-LDP (MPLS-TE)

The data plane however, is a simple label-based forwarding engine that is independent of the type of routing protocol or label exchange protocol. A Label Forwarding Information Base (LFIB) is used to forward packets based on labels.
The LFIB table is populated by the label exchange protocols used in the control plane.

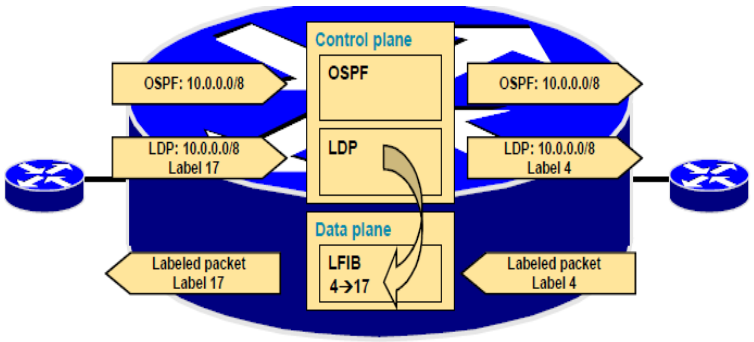

Fig (1) show MPLS architecture.

A simple MPLS implements destination-based forwarding that uses labels to make forwarding decisions.

A L3 routing protocol is still needed to propagate L3 routing information. A label exchange mechanism is simply an add-on to propagate labels that are used for L3 destinations.
This figure illustrates the two components of the control plane:
OSPF that receives IP network 10.0.0.0/8 from the left neighbor and forwards it to the right neighbor.

LDP that receives label 17 from the left neighbor to be used for packets with a destination address 10.x.x.x when forwarded to that neighbor. A local label 4 is generated and sent to upstream neighbors so these neighbors can label packets with the appropriate label. LDP inserts an entry into Data Plane's LFIB table where label 4 is mapped to label 17. The data plane then forwards all packets with label 4 through the appropriate interfaces and replaces the label with label 17.[3]

1.4 MPLS Modes of Operation: MPLS is designed for use on virtually any media and L2 encapsulation. Most L2 encapsulations are frame-based and MPLS simply inserts a 32-bit label between the L2 and L3 headers ("frame-mode" MPLS).
ATM is a special case where fixed-length cells are used and a label cannot be inserted on every cell. MPLS uses the virtual path identifier/ virtual channel identifier (VPI/VCI) fields in the ATM header as a label ("cell-mode" MPLS).[3]

1.5 MPLS routing: MPLS networks establish Label-Switched Paths (LSPs) for data crossing the network. An LSP is defined by a sequence of labels assigned to nodes on the packet's path from source to destination. LSPs direct packets in one of two ways: hop-by-hop routing or explicit routing.[4]

1.5.1 Hop-by-hop routing: In hop-by-hop routing, each MPLS router independently selects the next hop for a given Forwarding Equivalency Class (FEC). A FEC describes a group of packets of the same type; all packets assigned to a FEC receive the same routing treatment. FECs can be based on an IP address route or the service requirements for a packet, such as low latency.[4]

MPLS Header

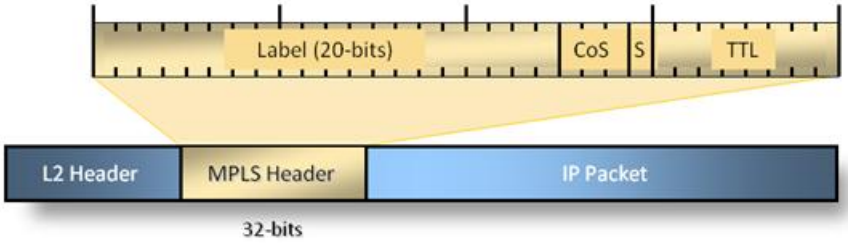

Fig (2) MPLS header.

MPLS starts with the concepts of MPLS header and some related information. Let us analyze what happens when a plain IP packet enters an MPLS enabled router. Before that, I would like to introduce some terms which are related to our discussion.

LSR: Label Switch Router is any router in the network which can process MPLS labels. Processing includes PUSH (add a new label to a frame), POP (remove a label from a frame), SWAP a label. An Edge LSR is a device which can process unlabelled packet, use Layer 3 lookup and assign a label.

FEC: Forwarding Equivalence Class is a set of packets which receive the same treatment in the forward direction. The treatment may be dependent on the destination IP address, source IP address, DSCP value etc.

LSP: Label Switched Path can be thought of as a virtual circuit from one end point (Edge LSR) to another end point (Edge LSR). A number of LSRs contribute to a full LSP. LSP is setup before the actual data flow.[4]

1.5.2 what happens when a plain IP packet enters an MPLS enabled router

The router (Edge LSR) would analyze the packet and assign an FEC to the packet. Secondly the packet is assigned a label based on the FEC. So how does this change incoming frame? Following picture depicts the transformation which a Layer 2 frame undergoes.[4]

1.6 MPLS Labels

Fig (3) MPLS labels.

It clearly shows that another label is inserted between Layer 3 datagram and Layer 3 Header. That is MPLS label. Sometimes, it is also called as Shim Header. Let us pay some more attention to MPLS label format. The total length of the MPLS header is 32 bits (4 bytes or octets).
Each label contains the following fields:

20-bit label: The actual label, which is a simple 20-bit number that has local significance and changes on every hop.

3-bit experimental field: Currently used to define a class of service such by reflecting the IP precedence of the encapsulated IP packet. Cisco routers
automatically assign the IP precedence value to this field.

Bottom-of-stack bit: MPLS allows multiple labels to be inserted. The
bottom-of-stack bit is used to determine if this is the last label in the packet.
This bit is set to "1" in the last label in the packet.

8-bit TTL field: It has the same purpose as the TTL field in the IP header. This field is decreased on every hop.[5]

1.6.1 MPLS Label Stack:

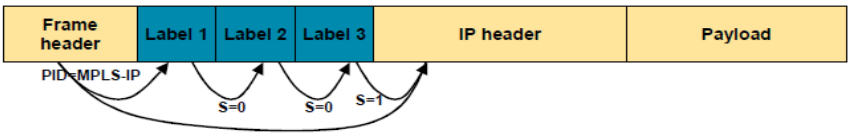

Fig (4) MPLS label stack

label does not contain any information about the L3 protocol being carried in a packet. A new protocol identifier is used for every MPLS enabled L3 protocol.
This list shows the ethertype values used to identify L3 protocols with most L2 encapsulations:

Unlabeled IP unicast: PID=0x0800 identifies that the frame payload is an IP packet.

Labeled IP unicast: PID=0x8847 identifies that the frame payload is a
unicast IP packet with at least one label preceding the IP header. The bottom of-bit indicates when the IP header actually starts.

Labeled IP multicast: PID=0x8848 identifies that the frame payload is a
multicast IP packet with at least one label preceding the IP header. The
bottom-of-bit indicates when the IP header actually starts.
A router that receives a frame where the PID indicates that it is a labeled packet uses only the top label in stack for forwarding decisions.
MPLS supports multiple labels in one packet. Simple MPLS uses just one label in each packet. The following applications may add additional
labels to packets:

- MPLS VPNs use multiprotocol BGP to propagate a second label that is used in addition to the one propagated by TDP or LDP.
- MPLS-TE uses RSVP to establish label-switched tunnels. RSVP also
- propagates labels that are used in addition to the one propagated by LDP or TDP.
- Any Transport over MPLS (AToM) uses a directed multihop LDP session between the edge routers to propagate a second label that is used in addition to the one propagated by the per link LDP- or TDP-sessions.
- A combination of the above mentioned mechanisms with some other features might result in three or more labels being inserted into one packet.[5]

1.6.2 LSR

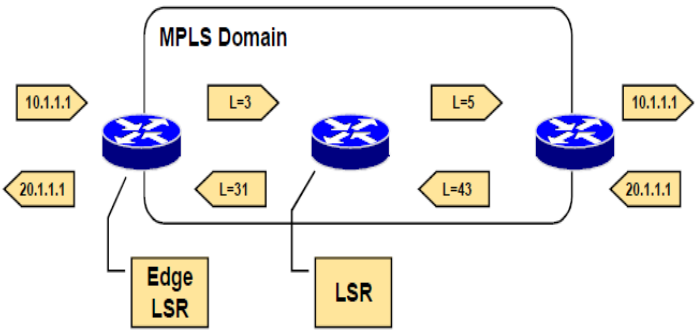

Fig (5) LSR & Edge LSR.

Before proceeding with a detailed description of MPLS, some of the terminology that is used in this course is presented:
LSR: A device that primarily forwards packets based on labels

Edge LSR: A device that primarily labels packets or removes labels LSRs and Edge LSRs are usually devices that are capable of doing both label switching and IP routing. Their names are based on their position in an MPLS domain. Routers that have all interfaces enabled for MPLS are called LSRs because they mostly forward labeled packets. Routers that have some interfaces that are not enabled for MPLS are usually at the edge of an MPLS domain (autonomous system). These routers also forward packets based on IP destination addresses and label them if the outgoing interface is enabled for MPLS.[7]

Architecture of LSRs
LSRs of all types must perform the following functions:

- Exchange L3 routing information (ATM LSRs must also exchange L3 routing information).
- Exchange labels.
- Forward packets or cells.

Frame-mode and cell-mode MPLS use a different data plane:
- Frame-mode MPLS forwards packets based on the 32-bit label.
- Cell-mode MPLS forwards packets based on labels encoded into the VPI/VCIfields in the ATM header.

The control plane performs the following functions:
- Exchange routing information regardless of the type of LSR.
- Exchange labels according to the type of MPLS (frame-mode or cell-mode).

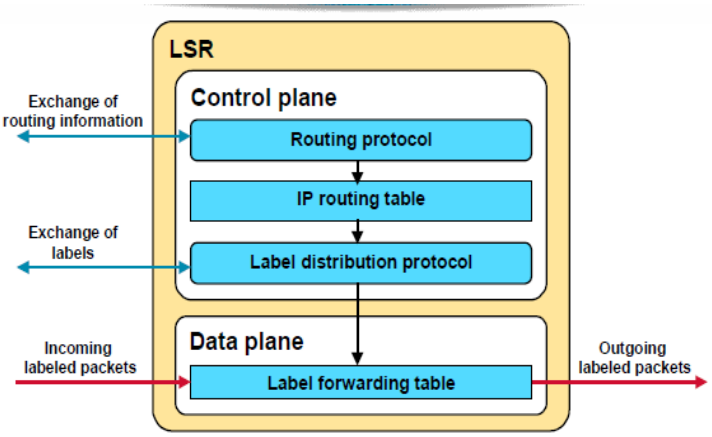

Fig (6) architecture of LSR.

The primary function of an LSR is to forward labeled packets. Therefore, every LSR needs a L3 routing protocol (OSPF, EIGRP, IS-IS, etc.) and a label exchange protocol (LDP, TDP, etc.).
The label exchange protocol populates the LFIB table in the data plane that is used to forward labeled packets.[7]

Architecture of Edge LSRs

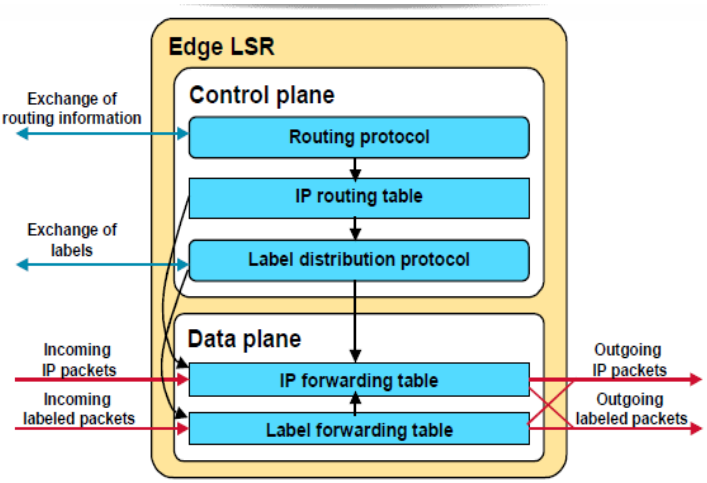

Fig (7) Architecture of Edge LSR.

Edge LSRs also forward IP packets based on their IP destination addresses and optionally label them if a label exists.
The following combinations are possible:
- A received IP packet is forwarded based on the IP destination address andsent as an IP packet.
- A received IP packet is forwarded based on the IP destination address andsent as a labeled packet.
- A received labeled packet is forwarded based on the label; the label is changed and the packet is sent.
- A received labeled packet is forwarded based on the label; the label is removed and the packet is sent out is an IP packet.
- The following scenarios are possible if the network is misconfigured:
- A received labeled packet is dropped if the label is not found in the LFIB table even if the IP destination exists in the FIB table.
- A received IP packet is dropped if the destination is not found in the FIB table even if there is a label-switched path (LSP) available for the destination.[7]

1.7 MPLS Forwarding

An IP packet going through an MPLS domain experiences the following:

- A label or a stack of labels is inserted (imposed) on an Edge LSR.
- The top label is swapped with a next-hop label or a stack of labels on an LSR.
- The top label is removed on the LSP endpoint (usually one hop before the egress Edge LSR or on the egress edge LSR itself) ATM LSRs only support the swapping of one label (normal ATM operation).[8]

MPLS Forwarding (Frame-Mode)

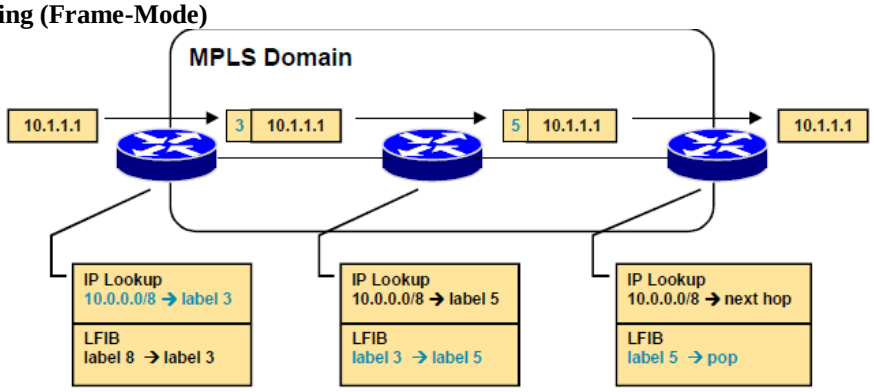

Fig (8) MPLS Forwarding (Frame-Mode).

This figure shows an MPLS network using frame-mode MPLS. All LSRs are capable of forwarding IP packets or labeled packets. The ingress edge LSR performs a routing lookup and assigns a label. The middle router simply swaps the label. The egress LSR removes the label (penultimate hop popping is covered later) and optionally performs a routing lookup.[8]

MPLS Forwarding (Cell-Mode)

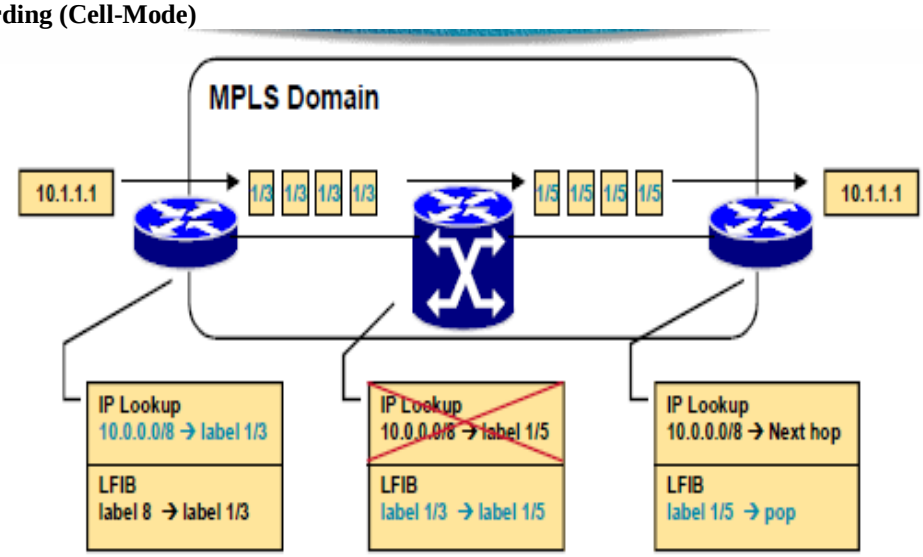

Fig (9) MPLS Forwarding (Cell-Mode).

Cell-mode MPLS is similar to frame-mode MPLS. The difference is that ATM LSRs (ATM switches) are not capable of forwarding IP packets:

The ingress ATM edge LSR (router) performs an IP routing table lookup and finds the outgoing interface and the label to use. It segments the IP packet into cells and assigns each cell's VPI/VCI field the label value.

The ATM LSR in the core (ATM switch) receives ATM cells and uses the VPI/VCI field to forward those cells. This is equivalent to ATM switching. The ATM LSR does not have any concept of packets or frames. It can only handle individual cells. Therefore it can never do any forwarding of IP packets.

On the egress ATM edge LSR (router), the cells are reassembled to form an AAL5 frame. The label values in each cell are lost during the reassembly. Also the label between the AAL5 header and the IP header is removed and the IP packet is forwarded.[8]

1.8 MPLS Applications

MPLS can be used in different applications:

- Unicast IP routing is the most common application for MPLS.
- Multicast IP routing is treated separately because of different forwarding Requirements.
- MPLS-TE is an add-on to MPLS that provides better and more intelligent link utilization.
- Differentiated QoS can also be provided with MPLS.
- MPLS VPNs are implemented using labels to allow overlapping address space between VPNs.
- AToM is allowing transport of L2 frames (or cells) across an MPLS cloud .

The data plane is the same regardless of the application. The control plane however needs appropriate mechanisms to exchange routing information and labels.

The term "Forwarding Equivalence Class" (FEC) is used to describe the packets that are using the same Labeled Switched Path (LSP) across the network.[7]

❖ **Unicast IP Routing**

Unicast IP routing setup usually requires two components:

- IP routing protocol (OSPF, EIGRP, IS-IS, etc).
- Label exchange protocol (TDP or LDP).

These two components are enough to create a full mesh of LSPs.
A label is assigned to every destination network found in the IP forwarding table.
Therefore, a FEC corresponds to an IP destination network.

❖ **Multicast IP Routing**

Multicast IP routing can also use MPLS. PIM version 2 with extensions for MPLS is used to propagate routing information and labels.
A FEC is equal to a destination multicast address.

❖ **MPLS-TE:**

Constraint-Based Routing manages traffic paths within an MPLS network, allowing traffic to be steered to desired paths. MPLS traffic engineering also enables resiliency and reliability to be built into carrier networks, increasing the availability and value of the network to their customers. Using MPLS traffic engineering, LSP connections can be optimized and preempted. When outages occur, traffic can be actively rerouted around failed links. An example of this is RSVP-TE Fast Reroute, which provides for sub-50ms switchovers between primary and back up LSPs or LSP bundles. Traffic engineering is deployed in MPLS networks via traffic engineering extensions to IGPs, such as OSPF and IS-IS. OSPF-TE and IS-IS-TE carry additional information —such as link bandwidth, link utilization, delay, priority, preemption, etc. — to allow the network to utilize paths that meet service requirements, resource availability, load balancing, and failure recovery objectives. RSVP-TE is widely used for MPLS signaling in networks that require traffic engineering. MPLS traffic engineering is typically deployed in the core of the MPLS network, while QoS is used at the edge. QoS at the edge ensures that high priority packets get preferential treatment, while traffic engineering avoids network congestion and appropriately utilizes available bandwidth resources. Together, QoS and traffic engineering enable organizations to move away from multiple, specialized networks for voice, video, and data to a single converged IP/MPLS network, dramatically reducing overhead and cost.

MPLS-TE has special requirements

- Every LSR must see the entire topology of the network (only OSPF and IS-IS hold the entire topology).
- Every LSR needs additional information about links in the network (available resources and constraints). OSPF and IS-IS have extensions to propagate this additional information.
- Every edge LSR must be able to create an LSP (Label Switched Path) on

demand. RSVP or Constraint-based Routing LDP (CR-LDP) is used to create an LSP and to propagate labels for MPLS-TE tunnels.

❖ **QoS:**

Differentiated QoS is achieved by using MPLS experimental bits or by creating separate LSPs for different classes. Extensions to TDP or LDP are used to create multiple LSPs for the same destination (one for each class). FEC corresponds to the combination of a destination network and the class of service.

❖ **VPN:**

MPLS VPNs use an additional label to determine the VPN and the corresponding VPN destination network. BGP with multiprotocol extensions is used to propagate VPN routing information and labels across the MPLS domain. TDP or LDP is still needed to link edge LSRs with a single LSP. FEC corresponds to a VPN destination network.

❖ **AToM:**

AToM provides forwarding of L2 frames (or cells) across an MPLS backbone.

Ethernet, Frame-Relay, High-Level Data Link Control/Point-to-Point Protocol (HDLC/PPP) frames or ATM cells are received by the ingress edge LSR. The L2 frames (or cells) are MPLS encapsulated and assigned a stack of two labels. The top most label will direct the frame to the egress edge LSR. The second label will indicate the outgoing interface on the egress edge LSR. A directed multihop LDP session between the ingress and egress edge LSRs is used to exchange the second label.

FEC correspond to an outgoing interface.

Interaction Between MPLS Applications

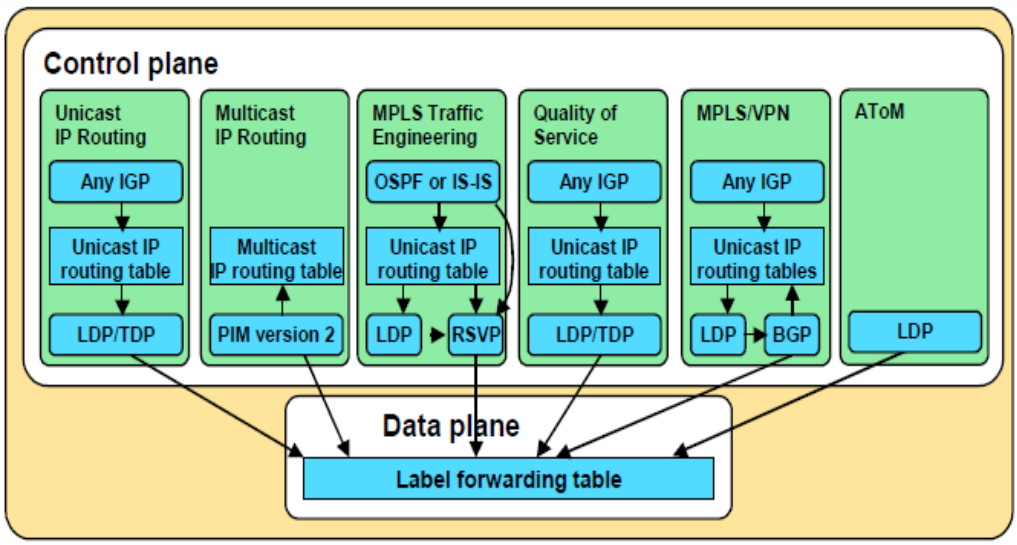

Fig (10) Interaction Between MPLS Applications.

This figure shows the complete architecture when all applications are used. Each application may use a different routing protocol and a different label exchange protocol, but all applications use one single label-forwarding engine.[9]

II. Methodology

In this paper OPNET simulator is used to analyze MPLS network . MPLS is a technology used for optimizing traffic forwarding through a network. Though MPLS can be applied in many different network environments, this discussion will focus primarily on MPLS in IP packet networks by far the most common application of MPLS today.

MPLS assigns labels to packets for transport across a network. The labels are contained in an MPLS header inserted into the data packet .

These short, fixed-length labels carry the information that tells each switching node (router) how to process and forward the packets, from source to destination. They have significance only on a local node-to- node connection. As each node forwards the packet, it swaps the current label for the appropriate label to route the packet to the next node.

This mechanism enables very-high-speed switching of the packets through the core MPLS network.

MPLS combines the best of both Layer 3 IP routing and Layer 2 switching. In fact, it is sometimes called a "Layer 2½" protocol. While routers require network-level intelligence to determine where to send traffic, switches only send data to the next hop, and so are inherently simpler, faster, and less costly. MPLS relies on traditional IP routing protocols to advertise and establish the network topology. MPLS is then overlaid on top of this topology. MPLS predetermines the path data takes across a network and encodes that information into a label that the network's routers understand. This is the connection-oriented approach previously discussed. Since route planning

occurs ahead of time and at the edge of the network (where the customer and service provider network meet), MPLS- labeled data requires less router horsepower to traverse the core of the service provider's network.[2]

2.1 The Network Simulation

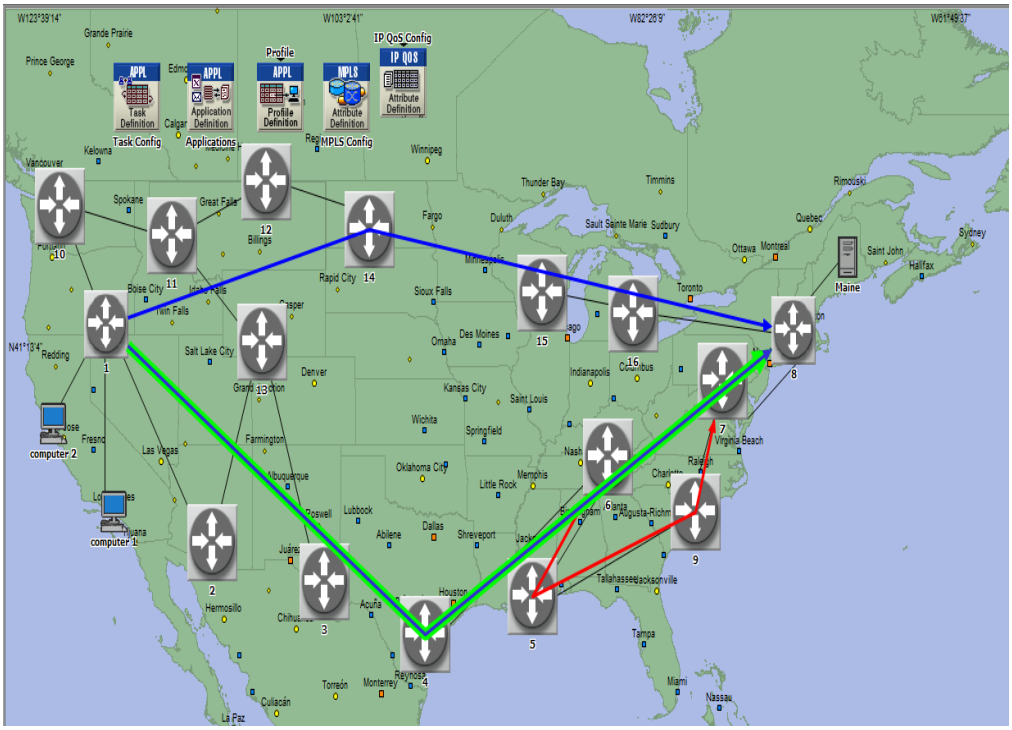

Fig (11) scenario of MPLS network by OPNET simulator.

This network has two workstations, one main server and 16 routers. R1 and R8 are the ingress and egress LSR respectively while R4 and R14 are transit LSR . There are two paths one is the primary ( ) and the second ( ) is the backup path and there is a bypass tunnel ( ). The workstations are connected to the R1 when any information is sent from any workstation to the main server R8, the information will pass from R1 to R8 through R4 on the primary path . If the primary path failed or there was any obstacle then the information takes the backup path which goes from R1 to R8 through R14. The bypass tunnel contains R6 , R5,R9 and R7 respectively. This scenario the use of RSVP-TE configure LSPs dynamically. And use the fact reroute to protect LSP locally by using bypass tunnel. And all routers are configured to use RSVP-TE for setting up LSPs.

III. Results And Disccusion

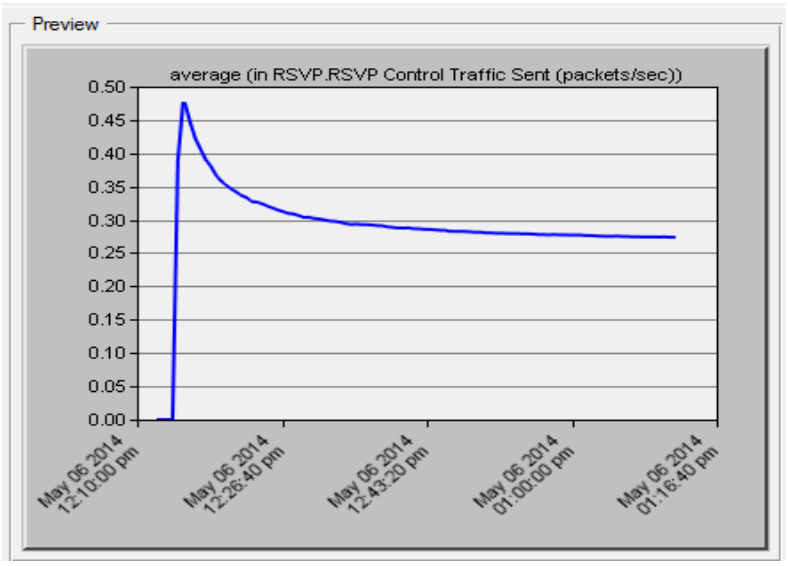

Fig (12) RSVP sent

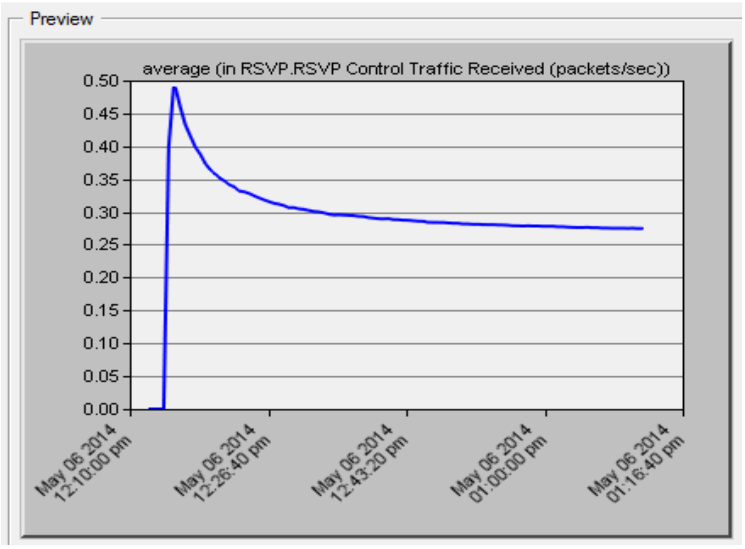

Fig (13) RSVP received

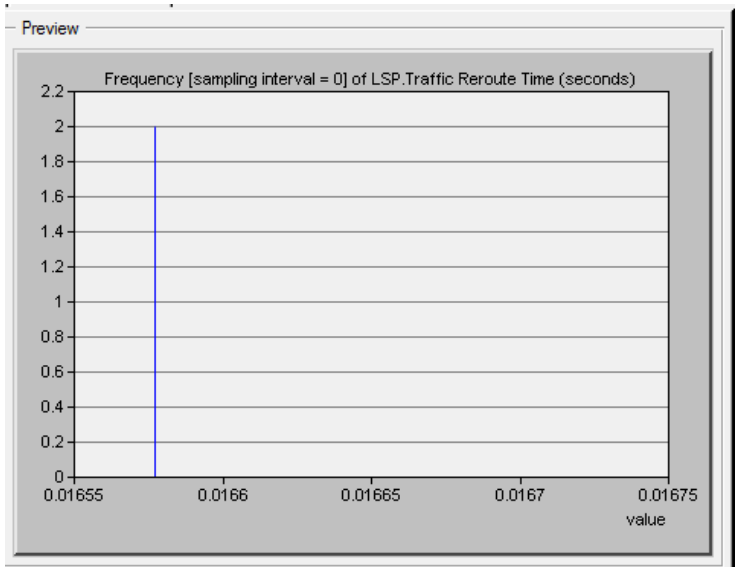

Fig (14) primary with bypass traffic reroute.

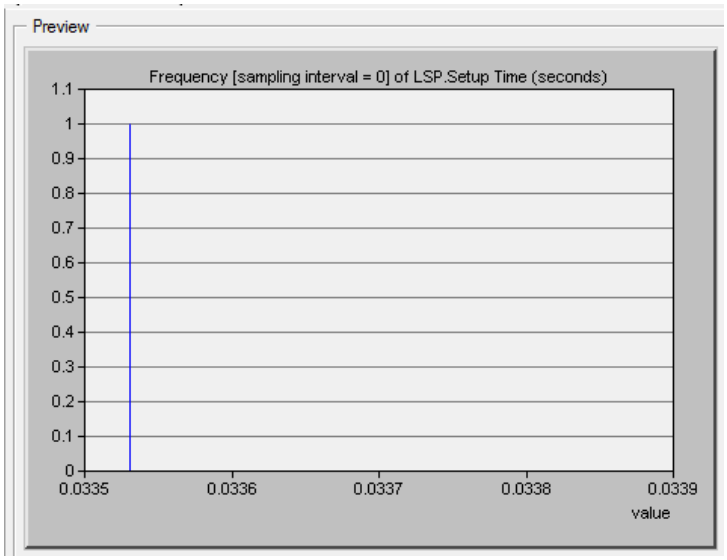

Fig (15) ingress backup LSP setup time.

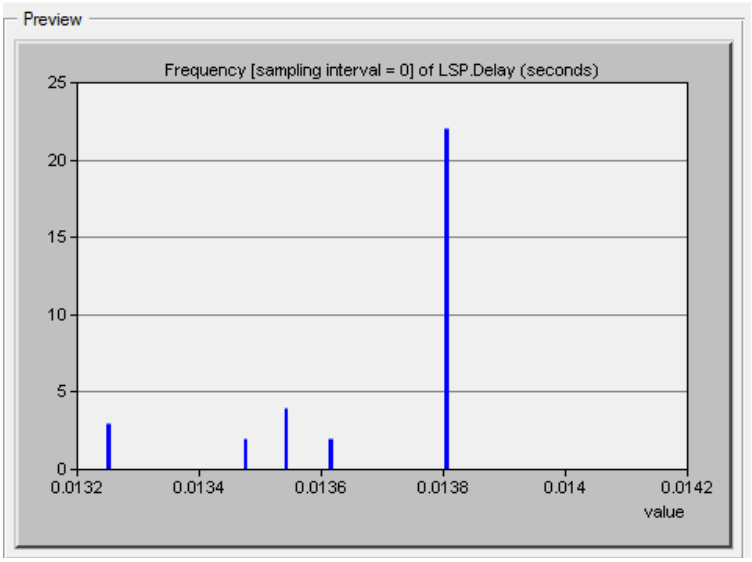

Fig (16) Ingress backup LSP delay.

1. Traffic reroute time has been shown for the primary LSPs:
   That is using fast reroute for protection with bypass tunnels. Traffic reroute time for LSP that use ingress initiated backup LSP .
2. Traffic in of the LSO in the network have also been shown.
   Results show that traffic is immediately bypassed using bypass tunnel for the LSP that uses fast reroute. Whereas, traffic is switched to backup LSP some time after failure or LSP that use ingress initiated backup LSP.

3.1 MPLS Challenges

1. MPLS is not a standalone technology — it is overlaid on Layer 2 technologies such as Ethernet or ATM, and must operate in conjunction with other control plane protocols, such as IP routing. The complexity of MPLS deployments is increased because of this interaction. In some cases, four or more protocols may be involved in a given network scenario, necessitating careful coordination and validation of the end-to-end system.
2. Ntegration of legacy services and deployment of new services, such as VPNs, requires tunneling, which in turn increases the setup requirements for a given circuit.
3. Though under development for a number of years, MPLS continues to evolve rapidly. The primary goals of the technology have shifted over time as technology has progressed.
4. A number of extensions to the MPLS protocols, as well as new functionality, are under development. New developments often obsolete older ones. This dynamic nature presents a moving target to those developing and deploying MPLS. Vendors must decide whether to implement a new feature with an eye on the industry's current direction.
5. Service providers gauge the viability of new developments by asking whether they solve a given problem better. On certain issues, the industry has split into multiple camps, further complicating the situation as organizations trade off the long term risk of obsolescence with the shorter term benefits of implementing a certain technology. Interoperability of MPLS equipment in heterogeneous networks remains an issue and will continue to be so for several years to come.
6. Though advances in silicon technology have vastly improved the raw performance of today's routers, the complexity of MPLS in real network applications presents performance and scalability issues. The challenge is typically not in the MPLS core network, where data is simply being label- switched, but at the network edge where MPLS must integrate with non-MPLS networks, and where services are initiated. As networks converge, traffic loads increase and networks must be able to deal with the overhead of handling real- time and prioritized traffic. The meshed connections required for VPN deployments can quickly challenge equipment scalability limitations, as well as provisioning and management requirements. Large service provider networks have the ultimate scalability challenge and must consider the limitations of their equipment as they look to maximize return on investment.
7. The challenges presented by MPLS ultimately necessitate thorough testing and validation of MPLS systems during development and prior to deployment. MPLS is by no means a plug-and-play proposition. Performing appropriate due diligence is the only way to ensure success when dealing with a broad-scope and rapidly evolving technology such as MPLS.[10]

IV. Conclusion

Multi-Protocol Label Switching (MPLS) is an evolving network technology that has been used to provide Traffic Engineering and high speed networking. There has been current demand on Internet Service Providers, which support MPLS technology, to provide Quality of Service (QoS) guarantees and security. Fault tolerance is an important QoS factor that needs to be considered to maintain network survivability. It is the property of a system that continues to operate the network properly in the event of failure of some of its parts. MPLS security has been mostly considered from the VPN point of view.

However, data confidentiality, integrity, and origin authentication in MPLS networks are still main security issues under discussion by many research groups**.**

References

[1]. C. Huang et al., "Building Reliable MPLS Networks using a path protection mechanism", IEEE Communication Magazine, vol. 40, no. 3, March 2002.

[2]. J.L. Marzo et al., "Adding QoS Protection in order to Enhance MPLS QoS Routing", IEEE International Conference on Communications, vol. 3, 2003, pp. 1973-1977.

[3]. Mina Amin, Kin-Hon Ho, George Pavlou, and Michael Howarth., '□ Improving Survivability through Traffic Engineering in MPLS Networks'', Centre for Communication Systems Research, University of Surrey, UK, vol. 4, no. 3, March 2010.

[4]. P. Marques, Constrained Route Distribution for Border Gateway Protocol/ MultiProtocol Label Switching (BGP/MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs), IETF RFC 4684, Nov. **2006**.

[5]. E. Rosen, A. Viswanathan, R. Callon, "Multiprotocol Label Switching Architecture", RFC-3031, January 2001.

[6]. P. Bhaniramka, W. Sun, R. Jain, "Quality of Service using Traffic Engineering over MPLS: An Analysis", September 2000.

[7]. Jian C, Chin L, "A restorable MPLS-based hose-model VPN network, " Computer Networks, vol. 5l, pp. 4836- 4848, 2007.

[8]. Awduche D.O., "MPLS and traffic engineering in IP networks," IEEE Communications Magazine, Volume: 37, Issue: 12, Dec. 1999, pp. 42-47.

[9]. Ayan B, "Generalized Multi-protocol label switching: An overview of signaling enhancements and recovery techniques," IEEE Communications Magazine, vol. 39, pp.144-151, 2001.

[10]. Myoungju Y, Jongmin L, Tai-Won U, "A new mechanism for seamless mobility based on MPLS LSP in BCN," IEICE Transactions on Communications, vol. 91, pp. 593-596, 2008.