DESIGNING OF MPLS AND ENSURING FAST CONVERGENCE AND SECURITY PERFORMANCE THROUGH VPN

N.Abinaiya[1], S.Rashmi[1], J.Jayageetha[2]

[1]PG Student/ Communication Systems, [2]Assistant Professor/ Department of ECE,
SNS College of Technology, Coimbatore, (India)

ABSTRACT

Need of global networking is increasing day by day and is a primary need. There has been a rapid growth of the routing protocols in the area of communication. A routing protocol is a protocol which is responsible to determine how routers communicate with each other and forward the packets through optimal path to travel from source node to destination node. The performance of each routing protocol is different from each other. In the context of routing protocol, protocol performance, each of them has different architecture, adaptability, route processing delays, convergence capabilities and many more. Among different routing protocols, Multi Protocol Label Switching (MPLS) has been considered for the IPv4 network. When we want to design a Wide Area Network (WAN), Open Shortest path First (OSPF) is a standard protocol which is being widely used. OSPF is classified as an Interior Gateway Protocol (IGP) which provides fast convergence in larger network. It can be ensure that the latency can be reduced and convergence speed can be made still faster when MPLS protocol is used. MPLS is an innovative approach in which forwarding decision is taken based on labels. It also provides a flexible and graceful VPN solution based on the use of LSP tunnels to encapsulate VPN data. Multi-protocol Layer Switching (MPLS) VPNs are best solution for medium and large enterprises that currently deploy site-to-site VPN services. MPLS provides sophisticated traffic engineering capabilities that, coupled with IP QoS, enable multiple classes of service so business critical applications are treated with higher priority than less important applications and "best effort" services. This project is based on simulation for performance analysis of OSPF protocol and MPLS protocol in IPv4 network by the parameters like Latency and Throughput. The simulation tool used is Graphic Network Simulator (GNS-3) and Wireshark

Keywords: Adaptability, Convergence, Ipv4, OSPF, VPN.

I.INTRODUCTION

MPLS is a scalable, protocol-independent transport. In an MPLS network, data packets are assigned labels. Packet-forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself. This allows one to create end-to-end circuits across any type of transport medium, using any protocol. The primary benefit is to eliminate dependence on a particular OSI model data link layer technology, such as Asynchronous Transfer Mode

(ATM), Frame Relay, Synchronous Optical Networking (SONET) or Ethernet, and eliminate the need for multiple layer-2 networks to satisfy different types of traffic. MPLS belongs to the family of packet-switched networks.

MPLS operates at a layer that is generally considered to lie between traditional definitions of layer 2 (data link layer) and layer 3 (network layer), and thus is often referred to as a "layer 2.5" protocol. It was designed to provide a unified data-carrying service for both circuit-based clients and packet-switching clients which provide a datagram service model. It can be used to carry many different kinds of traffic, including IP packets, as well as native ATM, SONET, and Ethernet frames.

A number of different technologies were previously deployed with essentially identical goals, such as Frame Relay and ATM. Frame Relay and ATM use it to move frames or cells throughout a network. The header of the ATM cell and the Frame Relay frame refer to the virtual circuit that the cell or frame resides on. The similarity between Frame Relay and ATM is that at each hop throughout the network, the “label” value in the header is changed. This is different from the forwarding of IP packets. MPLS technologies have evolved with the strengths and weaknesses of ATM in mind. Many network engineers agree that ATM should be replaced with a protocol that requires less overhead, while providing connection-oriented services for variable-length frames. MPLS is currently replacing some of these technologies in the marketplace. It is highly possible that MPLS will completely replace these technologies in the future, thus aligning these technologies with current and future technology needs.

At the same time, MPLS attempts to preserve the traffic engineering and out-of-band control that made Frame Relay and ATM attractive for deploying large-scale networks. While the traffic management benefits of migrating to MPLS are quite valuable (better reliability, increased performance), there is a significant loss of visibility and access into the MPLS cloud for IT departments.

II.EXISTING SYSTEM

2.1 Introduction

Implementation of high speed networks in internetworking environment very essentials in the present century, at present IPv4 networks provides communication in internet work environment. In IPv4 network, routing is being done at layer 3 network layer based destination network ID. The IPv4 network has disadvantage such as less security, less QoS and Latency. Also routing being done at Layer 3 has the following disadvantages:

- When the number of nodes increased, then the Routing database increases.
- When Routing database increased, processing delay gets increases
- Due to the Processing delay, Latency increases so that the Reliability of the network becomes decreases.

When the WAN has to be designed, at present OSPF is the standard protocol which is being used.

2.2 Overview of OSPF Protocol

OSPF is a link-state routing protocol based on open standards and is highly scalable. As such, OSPF can scale 1000s of nodes and therefore routing tables can get very big. To combat this, OSPF networks are divided into multiple areas. It can support up to FOUR equal cost paths and converges quickly. It uses partial updates with only the changes being flooded to the network. OSPF supports VLSM therefore OSPF is classless. It is good for very large networks i.e. those having a diameter of 15 hops or more. It makes good use of bandwidth; OSPF multicasts link-state updates – these are only sent when a topology change occurs.

OSPF selects routes based on cost (bandwidth). OSPF group's members into 'areas' and breaks the network into small clusters of routers. OSPF limits traffic regionally and can prevent changes in one area affecting another.

OSPF Protocol has the following Characteristics:

- Fast detection of changes in the topology and very fast reestablishment of routes without loops.
- Low overload, use updates that inform about changes on routes.
- Division of traffic by several equivalent routes.
- Routing according type of service.
- Use of multi-send in local area networks.
- Subnet and Super-net mask.
- Authentication

2.3 OSPF Packet

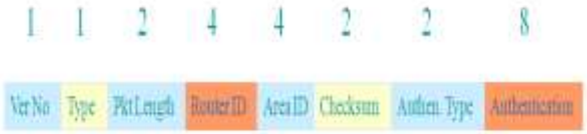

Fig.1: OSPF Packet

VERSION field: Describes which version of the OSPF protocol it is (1 or 2)

TYPE: Describes the type of packet. It includes Hello, Database description, LS request, LS update and LS acknowledgement

PACKET LENGTH: Packet length including header

ROUTER ID: IP of the generated router and IP of the interface over which the message has to be sent

AREA ID: Area to which the message belongs

AUTHENTICATION TYPE: No authentication, Simple password, Cryptographic authentication

III. PROPOSED SYSTEM

3.1 Introduction

IPv4 network with MPLS protocol is proposed to overcome all the limitation of IPv4 network. This network shares the information through VPN and it provides the corporate domains to access, transfer, receive, data (voice, video, or any form of data) with high efficiency, security, resource management. This VPN provided at layer one and two have efficiency's but lacked in providing uninterrupted transmission and reception of data their higher physical connectivity and reduced knowledge of high layered devices.

MPLS plays a Key role in NG Networks by delivering high efficient QoS (Quality of Service) and traffic engineering features.

It also proposed that MPLS employed with OSPFv2 protocol (for IPv4 addressing) provides standard Traffic engineering along with BGPv4 protocol provides inter AS high reliable connectivity in an secured L3VPN layered Network. This scheme can achieve reliable explicit routing which deploys maximally-disjoint pre-calculated alternate paths with improved secured packet transmission in networks supported even in heavy traffic environments.

3.2 MPLS Overview

Multi-Protocol Label Switching (MPLS) networks are the next-generation of networks designed to allow customers create end-to-end circuits across any type of transport medium using any available WAN technology. Until recent years, customers with the need to connect remote offices in locations across the country were restricted to the limited WAN options service providers offered, usually Frame Relay or T1/E1 dedicated links. The problem with these WAN technologies is that they are usually very expensive and complex to manage, but also not very flexible, making them a headache for both the end customer and service provider. Worst of all, as the distance between the customer's end points increased, so did the monthly bill. MPLS works by tagging the traffic entering the MPLS network. An identifier (label) is used to help distinguish the Label Switched Path (LSP) to be used to route the packet to its correct destination. Once the best LSP is identified by the router, the packet is forwarded to the next-hop router. A different label is used for every hop and the label is selected by the router (or switch) that is performing the forwarding operation.

3.3 Operation of MPLS

MPLS works by prefixing packets with an MPLS header, containing one or more labels. Fig.2 shows the label format of MPLS. This is called a label stack. Each label stack entry contains four fields:

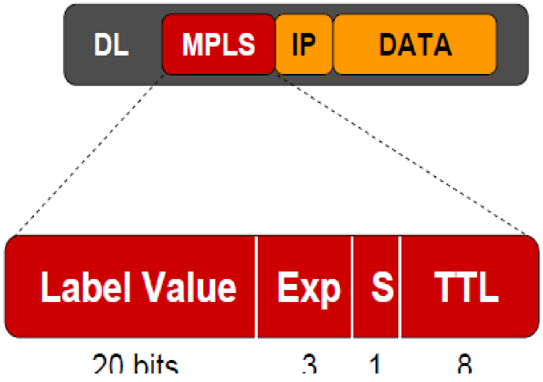

Fig.2: Generic MPLS Label Format

- A 20-bit label value. A label with the value of 1 represents the router alert label.
- A 3-bit *Traffic Class* field for QoS (quality of service) priority (experimental) and ECN (Explicit Congestion Notification).
- A 1-bit *bottom of stack* flag. If this is set, it signifies that the current label is the last in the stack.
- An 8-bit TTL (time to live) field.

3.4 MPLS Architecture

MPLS is a tunneling technology used in many service provider networks. MPLS works by prefixing packets with an MPLS header having one or more label known as label stack. With the contribution of MPLS-capable routers or switches in central gateway protocols such as Open Shortest Path First (OSPF) or Intermediate System to Intermediate System (IS-IS), the network automatically builds routing tables.

As shown in the fig.3, the MPLS network consists of the following components:

- **Customer Edge**

  It structures the customer message into IP Packets and sends to the entry node of MPLS domain. While receiving the IP Packets from the egress node of the MPLS domain, CE sends packets to Network layer of its own, after removing the IP address.

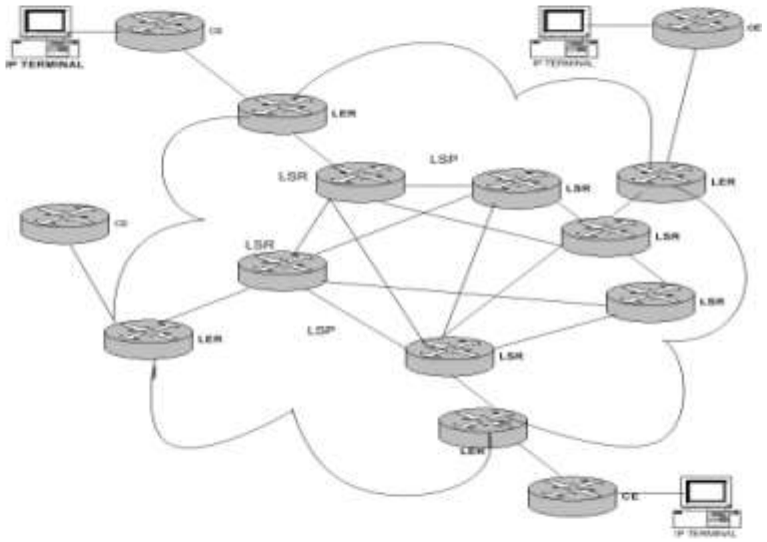

Fig. 3: Architecture of MPLS

- **Label Edge Router**

  Label Edge Routers are working as the gateways of MPLS Domain. Ingress LER, it receives the IP Packet from CE, assigns the appropriate Label. After wrapping label, it sends labeled packet towards the next hop through the Label Switched Path, which is assigned for the specific Forward Equivalence Class. Assigning the Label is known as Label Binding. LER also acts as the egress Router. It receives the labeled IP Packets from the previous transit router, pops up the label (removes the label) and routes the IP packets towards the destined CE. LER receives the multiplexed input from CE, and extends the switched output towards the transit routers.

- **Label Switching Router**

  Label Switched Routers are basically working as transit switches in MPLS cloud. It receives Labeled IP packets through the appropriate LSP.

  It analyses the Label bound over the packet, consults the forwarding information table (LIB) and routes the packet through the appropriately mapped out going LSP. When the LSR is routing the packets from incoming LSP to outgoing LSP, it strips out the Incoming Label and assigns a new label to same packet to ensure the security from the intruders. This process is known as Label Swapping or Label Changing. MPLS Network architecture is as shown in the diagram. Lines, shown between CE and LER carry the IP Packets bi-directionally.

- **Label distribution protocol (LDP)**

  It is one of the primary signaling protocols for distributing labels in MPLS network. It is a set of procedures and messages by which Label Switched routers (LSR) establish Label Switched Path (LSP) through a network by mapping network layer routing information directly to data link layer switched paths. By means of LDP LSR can collect , distribute and release label binding information to other LSRs in the MPLS network thus enabling hop-by-hop delivery of packets in the network along routed paths.

- **Label Switched Paths**

  Within an MPLS domain, a path is set up for a given packet to travel based on an FEC. The LSP is set up prior to data transmission. Lines, shown in the MPLS domain, are the Label Switched Paths that carry labeled IP Packets between the routers. There are two types of Label Switched Path. One is Static LSP and the other is Signaled LSP.

3.5 Services Provided By MPLS

- **MPLS VPN**

It is a tunneling technology, which gives the platform to create and implement MPLS based Virtual Private Networks (VPNs). It is developed to enhance the packet forwarding over the high performance backbone networks. MPLS forwards the IP packets to the distinct routers instead of the end devices on the basis of small labels . The MPLS application helps to create a tunnel or Label Switched Path (LSP). The small labels are sent over the path. The ingress (entry point of MPLS network) router over the MPLS network path appends this small label to the arriving packet. Over LSP, the hops swap the labels with the new ones to forward the packet. This process keeps on going until the packet arrives at the egress (exit point of MPLS network) router. The egress router strips-off the label and sends the packet towards its destination. The basic advantage of MPLS technology which we just noticed is that IP header analysis which on the other hand is necessary in traditional IP packet forwarding mechanism does not need here. The IP header is analyzed and a small label is appended to the packet at the entry point of the MPLS network. The ingress router may also analyze some extra information about the entering packet to assign it the best route which results in achieving the Quality of Service (QoS). When we talk about the traffic engineering as compared to traditional IP networks, it becomes so easier after choosing the explicit routes in MPLS network. So, this makes the MPLS technology more efficient.

The demand of securely sharing confidential data over public networks is growing day by day as the organizations are expanding their networks. The data sharing between offices, sub offices, and end users is an important requirement of large organizations and ensuring data confidentiality and integrity is a major concern. Keeping these requirements in view, the technology which is in use is VPN. The VPNs provides the platform to share data securely across the public network. The main users of VPNs are the service provider administrators, local enterprise network administrators and the end users.

The MPLS based VPNs offers verity of good services as compared to the traditional VPNs. They offer scalability, better flexibility, eases management. They are low cost, and support different QoS models MPLS VPNs use Border Gateway Protocol to distribute routes and MPLS technology to forward packets across the network. BGP/MPLS is point-to-point VPN, which uses the services of both BGP and MPLS. The introduction of MPLS technology into VPN network is made to achieve different services like, easy integration, simplification of virtual network, enhance network security, minimizes the complexity, cost reduction and the most important is QoS. The QoS is the major point of concern when services are required from service providers. Therefore, the MPLS VPN technology helps the service provider to achieve QoS over high performance backbone networks.

- **Traffic Engineering**

Traffic Engineering is the process of routing data traffic in order to balance the traffic load on various links, router and switches in the network. It has the ability to control specific routes across a network to reduce congestion and improves the cost of efficiency of carrying IP Traffic. MPLS is capable of full traffic engineering.

- **Quality Of Service Of Mpls**

QoS stand for Quality of Service is defined as the set of techniques to control bandwidth, delay, and jitter and packet loss in a network. QoS also provides techniques to supervise network traffic. It refers to a number of related features of telephony and computer networks that permits the transportation of traffic with the necessities. At the ingress to the MPLS network, Internet Protocol (IP) precedence information can be copied as Class of Service (CoS) bits or can be mapped to set the appropriate MPLS CoS value in the MPLS label. This is the distinction between IP QoS that is based on IP precedence field in the IP header and MPLS QoS that is based on the CoS bits in the MPLS label. MPLS CoS information is used to provide differentiated services. Hence MPLS CoS enables end-to-end IP QoS across the network.

IV. VPN

A virtual private network (VPN) is a technology for using the Internet or another intermediate network to connect computers to isolated remote computer networks that would otherwise be inaccessible. A VPN provides varying levels of security so that traffic sent through the VPN connection stays isolated from other computers on the intermediate network, either through the use of a dedicated connection from one "end" of the VPN to the other, or through encryption. VPNs can connect individual users to a remote network or connect multiple networks together.

There are two types of VPN,

1. Remote access VPN
2. Site-to-site VPN

In a site-to-site VPN, hosts do not have VPN client software; they send and receive normal TCP/IP traffic through a VPN gateway. The VPN gateway is responsible for encapsulating and encrypting outbound traffic, sending it through a VPN tunnel over the Internet, to a peer VPN gateway at the target site. Upon receipt, the peer VPN gateway strips the headers, decrypts the content, and relays the packet towards the target host inside its private network.

Nowadays, the network traffic growth rapidly, so the traditional networks like ATM, frame relay, Ethernet are not able to support this situation. So service provider discovers a new technology that solves this problem. The new IP forwarding that can handle this situation is Multi Protocol Label switching (MPLS). This technology can give higher ability such as scale, traffic engineering capability and provides Quality of Services (QOS).

4.1 MPLS VPN

MPLS popularity has increased exponentially in the last few years. One of the most compelling drivers for MPLS in service provider networks is its support for Virtual Private Networks (VPNs), in which the provider's customers can connect geographically diverse sites across the provider's network .First thing people confuse is the usage of the words MPLS and VPN. Both are separate terminologies. MPLS is the protocol that runs on top of your routing protocols. And VPN is all about creating a virtual network end to end across the internet. Traditionally VPN were based on IPsec (layer 3) or TLS (layer 2) which were slow and sluggish and merely less on features. MPLS had all these points into consideration as it evolved right inside Cisco labs, where it took birth. The MPLS VPN backbone and the customer sites exchange layer-3 customer routing information and packets are forwarded between multiple customer sites through the MPLS enabled backbone using the MPLS VPN services.

4.1.1 Components of MPLS VPN

As shown in the fig. 4, the MPLS VPN has the following five components:

- **Customer network**: It is under customer's administrative domain.
- **Provider network**: It is under Provider's admin control and responsible for providing routing between various customer's sites.
- **CE Routers**: Customer edge routers connecting the Provider MPLS network.
- **PE Routers**: Provider MPLS edge router connecting to single or multiple customer CE routers.
- **P Routers**: Provider MPLS backbone routers that interface with either other Provider backbone or PE routers.

MPLS based VPN accommodates for the overlapping IP address space between multiple customers by isolating each customer's traffic. The CE routers only get the traditional IP traffic and no labeled packets are forwarded to the CE routers. CE routers do not need any MPLS configuration for connecting to the Provider MPLS VPN network. PE Router is the first place where the MPLS VPN implementation starts, the PE router is responsible for isolating customer traffic if multiple customers are connected to the PE router. This is done in PE router by assigning an independent routing table to each customer, which is as good as assigning a dedicated router to each customer. The rest of the Provider network (P routers), the routing is done using the global routing table where P routers provide label switching between provider edge router and they are unaware of the VPN routes. The entire process is transparent to the customer as the CE routers are not aware of the presence of the P routers and Provider network's internal topology. In the Provider network the P routers are only responsible for the label switching and they do not carry VPN routes and do not participate in the MPLS VPN routing.

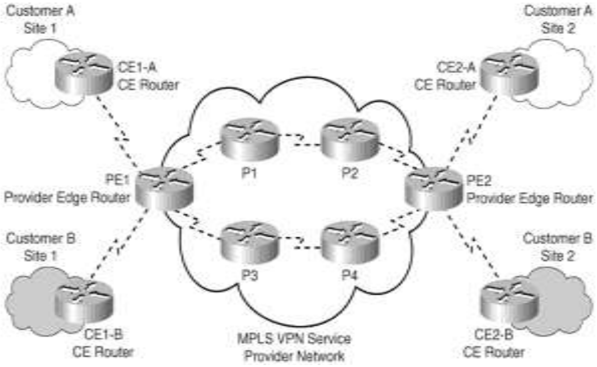

Fig.4: Architecture of MPLS VPN

V. RESULTS

5.1 Network Topology

The network topology is created with seven routers and eight clouds as shown in Fig.5. This is considered as a Wide Area Network and it is converged with OSPF and MPLS protocol and the comparisons are made between them. **Graphic Network Simulator** (GNS-3) and **Wireshark** are the simulation tools which are used to make the performance analysis.

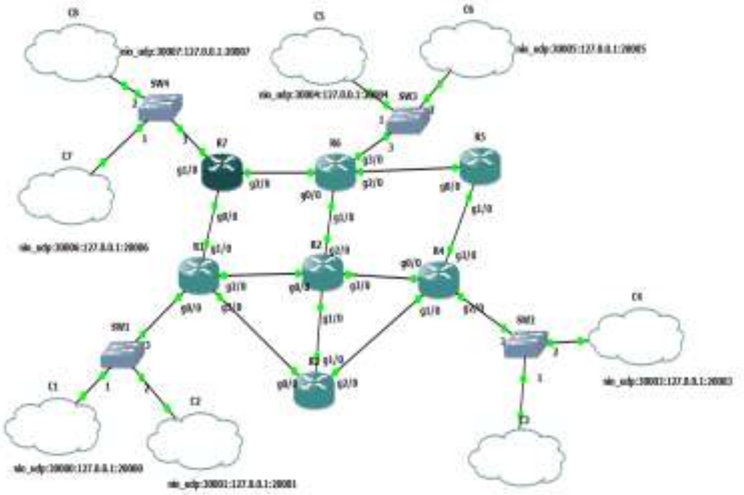

Fig.5: Network Topology

5.2Latency Analysis

In evaluating the performance of the convergence of OSPF and MPLS, the average transmission latency was measured first. Typically, the average transmission latency is the time taken for a packet to be transmitted across a network connection from sender to receiver.

TABLE.1: Latency Analysis of OSPF

PACKET SIZE (bits/sec)	400	600	800	1000	1200
LATENCY (ms)	135	150	155	158	160

TABLE.2: Latency Analysis of MPLS

PACKET SIZE (bits/sec)	400	600	800	1000	1200
LATENCY (ms)	105	120	125	129	132

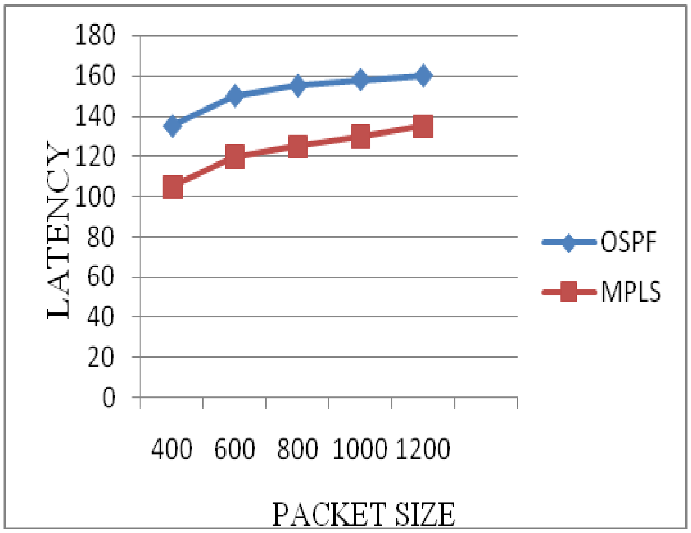

Fig.6: Comparison of Latency Analysis

As shown in the figure 6, The MPLS protocol reduces the latency when compared to OSPF protocol.

5.3 Analysis of Convergence Time

In evaluating the performance of the convergence time of OSPF and MPLS, the convergence time was measured. The time taken for the packet to take alternative path when any link gets failure is termed as convergence time. By the analysis of convergence time of OSPF and MPLS protocol it has been proved that the MPLS protocol has very less convergence time as compared to OSPF protocol.

VI.CONCLUSION

This project highlights the need for implementing MPLS technology to overcome some of the limitations involved in pure IP based forwarding. This paper also explains the concept of MPLS protocol in depth by providing the fundamentals of MPLS protocol and operation and working of MPLS network module. So, for this MPLS is an emerging technology and by no means a perfect solution to current IP network problems. It provides much better Traffic Engineering capability than the other networks. MPLS operates in coordination with IP Routing and its main objective is to provide the speed of switching to Layer 3. Introduction of labels provides an effective alternative and evades the need of large routing table lookups and results in fast routing. However, the telling factor of MPLS is its ability to manage and classify the traffic in order to provide better utilization of resources. Hence, this technology is used to effectively resolve integration and traffic engineering issues in carrier networks.

Also by the study of VPN, it can be conclude that MPLS VPN simplifies the network infrastructure by allowing the consolidation of multiple technologies and applications such as voice, video and data. MPLS provides sophisticated traffic engineering capabilities that, coupled with IP QoS, enable multiple classes of service so business critical applications are treated with higher priority than less important applications Via the above-mentioned theories analysis we can see, the MPLS VPN best among all other VPNs and it works best even in case of overlapping address spaces. The proposed system will provides enhanced security, scalability and high availability and will satisfy customer needs in better way.

REFERENCES

[1] Er.Jasvinder Sing, Rashed Quayoom Shawl, Rukhsana Thaker, “A Review: Multi Protocol Label Switching,” *International journal of Engineering Research and Applications*, ISSN: 2248-9642, Vol.4, Issue 1 (Version 2), January 2014, pp.66-70

[2] Abid Shah, Mureed Hussain,” *IP Bachbone Security: MPLS VPN Technology*,”International Journal of Fututre Generation Communication and Networking, Vol.6, No.5 (2013), pp.81-96

[3] Dinesh kumar and Gurpreet karur, “MPLS Technology on IP Backbone network,” *International journal of Computer Applications*, Vol.5-No.1, pp.13-16, Aug 2010

[4] Ramakrishnan, V.Wargo, John.s, *“MPLS network security: Gap Analysis,”*ICNS Conference, 2008 IEEE systems, pp.1-7,5-7, May 2008

[5] M.A.Breton, M.Bennani and M.E.Hachimi, *"EfficIent QoS implementation for MPLS VPN,"* International Conference of Advanced Information Networking and Applications, pp.259-263, March 2008.

[6] Botham.P, Liwen He, "*Pure MPLS Technology, Availability, Reliability and Security,"* third international conference, pp.253-259, 4-7, March 2008

[7] Fang.L, Bita.N, Miles.J, *"Interprovider IP-MPLS Services: requirements, implementations and Challenges,"*Communication Magazine, IEEE, Vol.43, no.6, pp.119-128, June 2005

[8] J.H.Lee, Y.H.Kang, *"The Implementation of the Premium Services for MPLS IP VPNs,*" Proceedings of the 7th International Conference on Advanced Communication Technology, pp. 1107-1110, 2005

[9] Daugherty.B, Metz.c, "*MPLS and IP, Part1: MPLS VPNs over IP Tunnels,"* IEEE International Computing, pp.68-72, May-June 2005

[10] L.D.Chou and M.Yuan Hong, "*Design and Implementation of Two Level VPN Service Provisioning Systems over MPLS Networks,"* Proceedings of the 7th IEEE International Symposium on Computer Networks (ISCN'06), (2006), pp.42-48

[11] Y.Nenghai, S.Qiong, G.Yanhui, C.Yuzhong, "A Novel Approach to Improve the Performance of MPLS-VPN," 8th Korea-Russia International Symposium on Science and Technology, KO-RUS,(2004), pp.35-39

[12] M.Ahmad Khan, "Quantiative Analysis of MPLS in VPNs," Proceedings of the IEEE Students Conference, ISCON'02,(2001), pp.56-65