QoS in MPLS and IP Networks

Master of Electrical Engineering with emphasis in Telecommunication

9th November, 2009

University Supervisor/ Examiner:
Alexandru Popescu
alexandru.popescu@bth.se
Department of Telecommunication

University Examiners:
Professor Adrian Popescu
adrian.popescu@bth.se
Department of Telecommunication

Internet : www.bth.se/tek
Phone : +46 457 38 50 00
Fax : +46 457 279 14
Abstract

The thesis report provides broader information about IP and MPLS technologies and routing protocols. Internet architecture and problems in an IP networks are illustrated when different internet protocols are used. Small focus is provides on the demand oriented real time applications and data traffic for QoS parameters in IP and MPLS networks. Evaluation of QoS guarantee parameters such as delay, jitter and throughput are described with state of art study results mainly for real time applications in IP and MPLS networks. Finally MPLS TE implementation and working is described and proposed to achieve better network performance.

Keywords: IP network, MPLS network, TE, QoS.
Acknowledgement

I am very thankful to:

- ALL Mighty ALLAH for his greatness for blessing me with health and mind.
- My family and friends for helping me during my degree studies and in hard times.
- My Telecommunication thesis supervisor Mr. Alexandru Popescu at Department of Telecommunication Systems, Blekinge Tekniska Högskola (BTH), Sweden for providing me this opportunity to complete master degree thesis with complete support and guidance during entire period.
- Mikeal Åsman and Lena Magnusson for complete assistance in study throughout my master degree.
# TABLE OF CONTENTS

## Chapter 1  INTRODUCTION
1.1 Infrastructure ................................................................. 9  
1.2 Networking .......................................................................... 10  
1.3 Emerging Technologies .................................................... 10  
1.4 Arpanet ................................................................................ 10  
1.5 Application Services ......................................................... 11  
1.6 Internet Applications ....................................................... 11  
1.7 Problem Definition ........................................................... 11  
1.8 Motivation ............................................................................ 12  
1.9 Outcomes ............................................................................. 12  
1.10 Thesis Outline ................................................................. 12

## Chapter 2  TECHNICAL BACKGROUND
2.1 Communication model .................................................... 14  
2.2 ISP Network ........................................................................ 15  
2.3 Data Transmission Types .................................................. 16  
2.4 Enterprise Networks ....................................................... 16  
2.5 Network Management ..................................................... 17

## Chapter 3  MPLS Overview
3.1 MPLS Benefits ................................................................. 19  
3.1.1 Single Network Structure ............................................. 19  
3.1.2 IP over MPLS .............................................................. 19  
3.1.3 ISP protocol Dependency ............................................. 20  
3.1.4 MPLS VPN Model ....................................................... 20  
3.1.5 Traffic Engineering ....................................................... 20  
3.2 MPLS Architecture .......................................................... 20  
3.2.1 Ingress/Egress Label Switching Router ......................... 21  
3.2.2 Intermediate Label Switching Router ......................... 21  
3.2.3 Label Switching Paths ............................................... 21  
3.2.4 MPLS Label .............................................................. 22  
3.2.5 Forwards Equivalency Class ....................................... 23  
3.2.6 LSR Operational Model ............................................. 23  
3.3 MPLS Label Packet Forwarding ....................................... 24  
3.4 Cisco Express Forwarding ............................................... 26  
3.4.1 Process Switching ...................................................... 26  
3.4.2 Fast Switching .......................................................... 27  
3.5 Traffic Engineering in MPLS ............................................. 28  
3.6 MPLS TE Operations ...................................................... 29  
3.6.1 Link Information Distribution ................................... 29  
3.6.2 Computing Paths ....................................................... 29
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.5.1</td>
<td>Integrated Service Model for IP</td>
<td>60</td>
</tr>
<tr>
<td>6.5.2</td>
<td>Differentiated Service Model for IP</td>
<td>61</td>
</tr>
<tr>
<td>6.6</td>
<td>QoS in MPLS Networks</td>
<td>63</td>
</tr>
</tbody>
</table>

### Chapter 7 MPLS TRAFFIC ENGINEERING AND VPN

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.1</td>
<td>MPLS Traffic Engineering</td>
<td>70</td>
</tr>
<tr>
<td>7.2</td>
<td>Traffic Engineering Basic</td>
<td>70</td>
</tr>
<tr>
<td>7.3</td>
<td>MPLS Traffic Engineering Overview</td>
<td>71</td>
</tr>
<tr>
<td>7.4</td>
<td>RSVP with Traffic Engineering Extension</td>
<td>71</td>
</tr>
<tr>
<td>7.4.1</td>
<td>RSVP Path Message</td>
<td>71</td>
</tr>
<tr>
<td>7.4.2</td>
<td>RSVP Reservation Message</td>
<td>72</td>
</tr>
<tr>
<td>7.4.3</td>
<td>RSVP Error Message</td>
<td>72</td>
</tr>
<tr>
<td>7.4.4</td>
<td>RSVP Tear Message</td>
<td>73</td>
</tr>
<tr>
<td>7.5</td>
<td>MPLS VPN Networks</td>
<td>73</td>
</tr>
<tr>
<td>7.6</td>
<td>Definition of VPN</td>
<td>73</td>
</tr>
<tr>
<td>7.7</td>
<td>Advantages of MPLS VPN over Other Technologies</td>
<td>74</td>
</tr>
<tr>
<td>7.8</td>
<td>Kinds of MPLS Based VPN</td>
<td>75</td>
</tr>
<tr>
<td>7.9</td>
<td>Security Connection in MPLS Under the Circumstances of VPN</td>
<td>76</td>
</tr>
<tr>
<td>7.9.1</td>
<td>Virtual Routing Forwarding</td>
<td>77</td>
</tr>
<tr>
<td>7.9.2</td>
<td>Routing Distinguisher</td>
<td>77</td>
</tr>
<tr>
<td>7.9.3</td>
<td>Route Targets</td>
<td>78</td>
</tr>
</tbody>
</table>

### Chapter 8 COMPARISON AND ANALYSIS OF IP/ MPLS NETWORKS

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.1</td>
<td>Functionality</td>
<td>80</td>
</tr>
<tr>
<td>8.2</td>
<td>Multimedia Application</td>
<td>80</td>
</tr>
<tr>
<td>8.3</td>
<td>QoS in IP/MPLS</td>
<td>82</td>
</tr>
<tr>
<td>8.4</td>
<td>Performance Parameters</td>
<td>84</td>
</tr>
<tr>
<td>8.5</td>
<td>Traffic Engineering</td>
<td>84</td>
</tr>
<tr>
<td>8.6</td>
<td>Security Issues</td>
<td>84</td>
</tr>
<tr>
<td>8.7</td>
<td>GMPLS</td>
<td>85</td>
</tr>
</tbody>
</table>

### Chapter 9 CONCLUSION AND FUTURE WORK

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1</td>
<td>Conclusion</td>
<td>87</td>
</tr>
<tr>
<td>9.2</td>
<td>Future Work</td>
<td>88</td>
</tr>
</tbody>
</table>

REFERENCE | 89
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ARP</td>
<td>Automatic Repeat Request</td>
</tr>
<tr>
<td>ATM</td>
<td>Asynchronous Transfer Mode</td>
</tr>
<tr>
<td>BGP</td>
<td>Boarder gate Way Protocol</td>
</tr>
<tr>
<td>BoS</td>
<td>Bottom of Stack</td>
</tr>
<tr>
<td>CBR</td>
<td>Constant Bit Rate</td>
</tr>
<tr>
<td>CEF</td>
<td>Cisco Express Forwarding</td>
</tr>
<tr>
<td>CRC</td>
<td>Cyclic redundancy Check</td>
</tr>
<tr>
<td>DV</td>
<td>Distance Vector</td>
</tr>
<tr>
<td>DBMS</td>
<td>Data Base Management System</td>
</tr>
<tr>
<td>EGP</td>
<td>Exterior gateway Protocol</td>
</tr>
<tr>
<td>EIGRP</td>
<td>Enhanced Interior gateway Routing Protocol</td>
</tr>
<tr>
<td>FEC</td>
<td>Forward Error Correction</td>
</tr>
<tr>
<td>FTP</td>
<td>File Transfer protocol</td>
</tr>
<tr>
<td>GWT</td>
<td>Google wireless Transponder</td>
</tr>
<tr>
<td>ISP</td>
<td>Internet Service provider</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>IOS</td>
<td>Internet Operating System</td>
</tr>
<tr>
<td>IGP</td>
<td>Interior gateway Protocol</td>
</tr>
<tr>
<td>ISIS</td>
<td>Intermediate system to intermediate system</td>
</tr>
<tr>
<td>IPTV</td>
<td>Internet protocol television</td>
</tr>
<tr>
<td>IPV4</td>
<td>Internet protocol version4</td>
</tr>
<tr>
<td>ITU</td>
<td>International Telecommunication Unit</td>
</tr>
<tr>
<td>IHL</td>
<td>Internet Header Length</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>IBM</td>
<td>International Business Machines</td>
</tr>
<tr>
<td>ISDN</td>
<td>Integrated service Digital Network</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>LDP</td>
<td>Label Distribution Protocol</td>
</tr>
<tr>
<td>LSR</td>
<td>Label Switch Router</td>
</tr>
<tr>
<td>LSP</td>
<td>Label Switch Path</td>
</tr>
<tr>
<td>LFIB</td>
<td>Label Forwarding Information Base</td>
</tr>
<tr>
<td>MPLS</td>
<td>Multiprotocol Label Switching</td>
</tr>
<tr>
<td>Acronym</td>
<td>Definition</td>
</tr>
<tr>
<td>---------</td>
<td>------------</td>
</tr>
<tr>
<td>MAN</td>
<td>Metropolitan Area Network</td>
</tr>
<tr>
<td>MTU</td>
<td>Maximum Transmission Unit</td>
</tr>
<tr>
<td>MAC</td>
<td>Medium Access Control</td>
</tr>
<tr>
<td>MIB</td>
<td>Management Information Base</td>
</tr>
<tr>
<td>NMS</td>
<td>Network Monitoring System</td>
</tr>
<tr>
<td>NAT</td>
<td>Network Address Translation</td>
</tr>
<tr>
<td>NOC</td>
<td>Network Operation Centre</td>
</tr>
<tr>
<td>OSI</td>
<td>Open System Interconnection</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Path First</td>
</tr>
<tr>
<td>OAM</td>
<td>Object Access Method</td>
</tr>
<tr>
<td>PDU</td>
<td>Packet Distribution Unit</td>
</tr>
<tr>
<td>PVC</td>
<td>Permanent virtual circuit</td>
</tr>
<tr>
<td>PHB</td>
<td>Per Hop Behaviour</td>
</tr>
<tr>
<td>POP</td>
<td>Point of Presence</td>
</tr>
<tr>
<td>PSTN</td>
<td>Public Switch Telephone Network</td>
</tr>
<tr>
<td>PPP</td>
<td>Point to Point Protocol</td>
</tr>
<tr>
<td>PDU</td>
<td>Packet Distribution Unit</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>RSVP</td>
<td>Resource Reservation Control Protocol</td>
</tr>
<tr>
<td>RIP</td>
<td>Routing Information Protocol</td>
</tr>
<tr>
<td>SMS</td>
<td>Short Message Service</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management protocol</td>
</tr>
<tr>
<td>SLA</td>
<td>Service Level Agreement</td>
</tr>
<tr>
<td>TE</td>
<td>Traffic Engineering</td>
</tr>
<tr>
<td>TCP</td>
<td>Transmission Control protocol</td>
</tr>
<tr>
<td>TTL</td>
<td>Time to Live</td>
</tr>
<tr>
<td>LIB</td>
<td>Label Information Base</td>
</tr>
<tr>
<td>TDM</td>
<td>Time Division Multiplexing</td>
</tr>
<tr>
<td>TDP</td>
<td>Tag Distribution Protocol</td>
</tr>
<tr>
<td>TOS</td>
<td>Type of Service</td>
</tr>
<tr>
<td>VLAN</td>
<td>Virtual Local Area Network</td>
</tr>
<tr>
<td>VOIP</td>
<td>Voice Over Internet Protocol</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Network</td>
</tr>
</tbody>
</table>
Chapter 1

Introduction
Internet is an immense network and surrounds many network technologies, the existence of the Linux OS adheres esteems pioneer technology generation in the beginning. Linux technology was complex, but better and faster than the other competitors at the time. Linux innovation ideas embark the software development industry and the focus software’s consists and required for financial and economic transactions. This development phases lead the technology orientations to focus on transmission connectivity of the systems terms as data communication in a large scale so the meaning of the transactions and the lift boundless withdraws and the uniqueness of the network should form.

Linux built the internet though innovations of economic theories, since the many developers, businesses, corporations, governments, etc require it to deploy the Linux systems and make them operate able. Considering economy as a global internet and software enable and driven technology comprised of human cognitive speculations, we analyze the concepts for acceptance and credibility for learning the features and utilities in an internet development. Clearly, internet invent innovation lies ahead of any invention that causes to ultimate development but instead internet develop through innovative research consequences for better utilization of systems and incorporating technology standards.

Looking at the internet we see and unclear picture of data communication networks where the sources are attached at either side or destinations on the other side while the communication channel between them forms an internet itself. Focusing on the communication channel except complexities present at either sides of source and destinations, application and protocol involved in data communication, we extremely encircle the communication channel that comprises of network or internet i.e. bridges and routers, but mainly routers in this thesis. The creation of World Wide Web (www) was existed through Ted Nelson’s [1] ideas of 37 years of struggle with Tim Berner Lee as a first WWW programmer with the possibility of NeXT computers having the support of http and internet applications.

Existence of internet at the beginning was moreover illusionary concepts of use but current internet infrastructure and technology emergence make it possible to connect billions of users thousands of miles away with variety of impossible contents, multiple groups having discussions, businesses connecting through virtual connections, with multiple applications running at the nodes and transmitting different types of data. An idea of digital packet switched network for the message delivery between telegraph was studied in 1850s. At that time telegraph, telex and telephony were key developing technologies that make internet possible through characteristics. There are certain paradigms to consider knowing the reality behind internet.

1.1 INFRASTRUCTURE

In U.S telegraph networks started in early 1850s and quickly encompassing majority of the big cities while deploying first electronic and messaging communication systems [2]. With an increase in the connections, intermediate telegraph offices become dense and main offices formed into switching centers. Messages from the either side arrived at a wire or pneumatic tube where they were sorted and forwarded based on some tube system. Around 450 telegraphs were deployed in London that was connected through
68 tubes, so the main office in New York was running that tube system. Soon the problem of increased traffic followed the concentration to find telegraphy bottlenecks. An enormous effort was made by skilled operators having expertise in morse code, Charles Wheatstone who developed ABC telegraph and provided solution at that time. It was a solution that opened many questions and problems arising afterwards and then the solutions leading towards innovative internet.

1.2 NETWORKING

The term is based on telegraphy and until 19th century, some sort of communication infrastructure was developed through Graham Bell’s invention [2]. However, it was small distance communication system with low data capacity connections. In case of increase in the distance, fading was observed. Maxwell’s equations helped to design systems that were capable of transmitting electronic signals i.e. speech with higher distances. Through the improvement of communication medium i.e. twisted pair and coaxial cables, it became possible to achieve higher data rates and possibly television broadcasting was made possible.

1.3 EMERGING TECHNOLOGIES

In 19th century telephone became internationally available which caused telegraphy and telex services to reduce, as a result businesses required to adopt new technology to save the businesses and operators. Teletype captured the world of newspapers while Telex acted as a news service and their integration and improvements in the production provided promising results for commercial news operators. Since high accuracy and availability was required for telegraph lines to become highly acceptable so any quality constraints caused due to rain and high traffic increases the probability of errors. With the innovative hit and trial mechanism certain loopholes were eradicated but the development was very slow and telegraphs businesses wanted a change for quality, accuracy, availability and acceptability of communication medium that was even harder for Morse operators to provide. However research process and business innovation causes rapid changes in the system improvements and a company called Morkrum established facilities to provide and fulfill commercial telegrams.

Looking closely at telephone, telegraphy, fax, telex and computer networks as a communication medium are not identical. Every technology has different mode of operation and communication mechanism. Telephony mainly provides an infrastructure for communication mechanism between businesses or an individual while telex provided financial transactions in global organizations. Internet is considered as a research network, the history of data communication and networks without having cognitive reasons for computer applications.

1.4 ARPANET

The idea was proposed to Lawrence Robert and soon work was started to develop an interface message processor to connect interface machines by forming a simple network which was successfully implemented by ARPANET. Connectivity was made between four nodes and an extension was provided by Robert up till 15 nodes and so one with possible implementations and deployments at research and military sites. Network
Analysis Corporation was formed for planning the network and its operations to keep the network running. Future extensions lead the network at current stage.

1.5 APPLICATION SERVICES

Dynamic growth in internet causes the mind to reflect the ideas meant possible with involvement of internet technology while businesses are envisioning a radical change in the society and to compete in the world through technology orientation, so they develop some goals and objectives. The businesses should have computation capabilities, text editing possibilities, services to provide solutions to the problems, keeping records, establishing communication with business partners, reliable financial transactions, sale and purchase options, obtaining remote access to the information, etc. These application services were very early to point since the existing of new technologies required decades to fulfill the gap and develop them for market acceptability [3].

1.6 INTERNET APPLICATIONS

These are basically rich internet applications i.e. client server and web application running on the network nodes under standard web browsers. It includes frameworks, plug-ins, sandboxes and virtual machines sometimes dependent on Adobe Flash, Java, GWT etc features to run these applications. These applications are installed and running on rich clients or web client connected to the internet, sometimes these clients require VPN, CITRIX Hosting for server security [3]. YouTube, online gaming and other application servers on the telecommunication network are good examples.

Internet traffic depends of the internet applications i.e. real time applications require quality of service guarantee and thus generate more traffic. The core network consist of fiber optic medium that connects the seven continents and have much higher bandwidth to manage higher data rates connecting the ISPs. Moreover, ISPs connecting home businesses and corporate networks offer less bandwidth that causes increased congestion and network load at their networks.

1.7 PROBLEM DEFINITION

Internet lies through a network of interconnected nodes that transmit data through switching mechanism. Internet core routers connect and forms an internet through some communication mechanism i.e. protocols. Although OSI reference model and TCP/IP had been successful in early stages of implementation for reliable and efficient data transmission but with the development of heavy applications at the network nodes the bandwidth requirement is increased or the QoS is demand oriented [4-5]. It is however probable for the traditional internet protocols to transmit higher quality data at a higher rate as compared to normal text data packets. Real time applications demand for higher bandwidth and QoS guarantees and to be able to keep the businesses running, researcher are struggling to figure the solution to categorize and implement the routing protocols that separate the class of services at the core network.

MPLS is one solution to the existing problem; it not only takes different paths to avoid congestion, but uses label switched technology to efficiently deliver the packets through MPLS network. The thesis will focus on different type of applications that require QoS
1.8 MOTIVATION

MPLS is a new technology for design and implementation of reliable, secure, efficient and standard QoS services and application classes. This technology will have lasting solutions for traffic engineering, VPN tunneling, multicasting etc. The technology itself is the necessity of the current ISP stack holders. There will be more possible research in the development and advancement in its routing protocols and security features. MPLS will work efficiently in telecom industry since Nokia, Siemens, Ericsson; Apple etc are developing real time applications for mobile nodes in the horizons for internet connectivity had already been implemented through third generation telecommunication. IPTV is a real time application that requires extremely high quality of service and depends on the network traffic for efficient and reliable video packet data transfer over the internet. Since demand for the QoS applications increases so it ultimately affects internet and its solutions posed by MPLS network for bandwidth utilization through traffic engineering and optimization [4-5].

1.9 OUTCOMES

The thesis main contribution will comprise of state of the art study to compare IP networks with MPLS networks in terms of different routing protocols. The study will provide better understanding and learning concepts for the beginners, information regarding MPLS importance, uses and deployment for the businesses. This study will help me to develop solid theoretical background for industrial projects in MPLS.

1.10 THESIS OUTLINE

Introduction is chapter1 that provides detail description about internet development as an innovation process, problem definition, motivation and expected outcomes. Chapter 2 give technical background information about the communication network and technologies. Chapter 3 describe an overview of MPLS technology, MPLS architecture and its components, MPLS working, applications, MPLS label, components, LSPs and relevant material along with traffic engineering, VPN and QoS services. Chapter 4 discuss an overview of IP network, architecture description, internet protocols, QoS parameters, problems in IP network and required solutions. Chapter 5 explains fundamental IP and MPLS routing protocols and routing mechanisms. Chapter 6 discuss QoS issues in MPLS, class of services, service level agreement and the need for QoS. Chapter 7 describe MPLS Traffic Engineering concepts and VPN implementation. Chapter 8 is based on an analytical study for comparing of IP and MPLS networks. Finally chapter 9 provides conclusions and future work based upon comparison study.
Chapter 2

Technical Background
In this chapter we will discuss data communication, protocols, IP network infrastructure, application types, MPLS advantages and traffic engineering concepts.

2.1 Communication Model
In digital communication world packets are transmitted from source to destination, the channel called as transmission system is present in the central between source and destination. Source generates and transmits data packets towards destination through destination IP address, the transmission system consist of no. of hops from source to destination [1].

![Communication Model Diagram]

Above figure is a simplified communication model consisting of source transmission system and destination. Transmission system could be WAN, MAN, or LAN network of interconnected devices.

A protocol is required to perform communication between these devices and end nodes. These end nodes may contain FTP applications, DBMS, any web browser, financial software or specialized game applications requiring and internet connect activity to establish Client-Server access mechanism through protocols. In general communication comprises of three layer model is applied [6] i.e. Network Access layer, Transport layer, Application layer which surrounds applications, computers and network involved in
communication system. OSI is seven layers standard model for data communication but mainly TCP/IP five layers model is implemented in an internet.

Packet Switching Technology was emerged due to bottlenecks in the circuit switching technology to carry voice data for telecommunication networks. Since circuit switching networks must have dedicated connection for voice data and the availability of resources was limited as well as resource utilization was low, packet switching technology was developed to overcome problems associated with voice data packets. Also circuit switching only offers constant data rate while packet switching performs data transmission in small packets. In case of larger packets inter connected device performs fragmentation and defragmentation at either transmission nodes. Packet switching technology reduces propagation delay, transmission time, node delay, and thus increasing transmission performance over circuit switching technology.

Protocols are principally required to performs manipulation on incoming data packet from the source the and forward it to desired destination. This involves routing operation for required key protocol characterises to be considered for implementation. The routing function/algorithm must contain simplicity, efficiency, accuracy, stability, robustness, optimality and other routing functionality.

2.2 ISP Network

Internet service provider connects homes, enterprise business, and other ISPs and consists of multiple point of presence (POP) depending upon on ISPs size. POP topology consist core routers which are high speed traffic trunks connected through fibre optic transmission medium and connects other ISPs. Border routers lie on the edge of ISPs network connecting other ISPs while service routers like web hosting application servers are present are within ISPs networks that connect difference application server. ISP provide four types of connections [7].

a) Low speed connection with low band width, huge no of users, an often with less revenue generation capabilities i.e. Dialup PSTN and ISDN.

b) Medium speed connection also low band width, acceptable no of users, and 56/64K lines.

c) High speed connection like E1++ data rate are implemented for medium band width requirements and decrease no of users.

d) Broad band connection are cable wireless are xDSL connection with higher band width requirements facilitate large no of users.

Network operation centre (NOC) Module performs backups, network monitoring and analysis, log management and security management. NOC modules implement interior
gate way protocol i.e. ISIS, EIGRP and OSPF to provide point to point links. An exterior gateway protocol i.e. BGP or EGP is implemented to establish customer prefix and manage internet routes.

2.3 DATA TRANSMISSION TYPES

Internet implements packet switching technology where all the packets are provided with IP addresses. The MTU size is 1500 bytes that carries all types of application data i.e. data; voice and video which is also termed as triple play technology. Certain problem in IP network are describe in later chapter however IP packet carrying data performance is efficient as compare to voice and video data. UDP and TCP protocols are mainly used for different data types while TCP provides connection oriented data transmission instead of UDP connectionless data transmission. Routing protocols running on different hops in an internet infrastructure performs destination address traversing by allowing shortest path towards IP destination address. Mainly it reduces performance if congestion happens at shortest path while TCP tries to make slow start to keep the link active, and due to some unutilized paths. MPLS make use of label technology to limit these problems.

IP traffic can also manage voice and video data until less user traffic exists but as soon as the traffic increases through user request the packets travelling the same IP destination path become lost or slow due to OSPF congestion. So the quality of service guarantee voice and video data is no more accomplished. There is no standard way to provide QoS to voice and video data packets in IP packet transmission. MPLS describes separate quality of services classes at LSR to priorities data packet passing through its network.

Mainly three types of application data is used on computer nodes as well as in data traffic. Email, www, spreadsheets are all examples of data traffic type. Current multimedia services running at computer application need to have reliable real time traffic flows between source and destination to be able to avoid delay and packet loss.

2.4 ENTERPRISE NETWORK

Enterprise networks are similar to ISP except it provides connectivity to financial organisation, government sector, multinational organisation and health care organisation etc. WAN is an example of large enterprise network connecting branch offices at different location of the world. These networks comprise of legacy equipment which are difficult to manage spread around large geographical area. Enterprise network offer telecommunication and data transmission services to their clients i.e. print, email
accounts, data storing and sharing capabilities, share application access, intranet, internet, extranet, ecommerce, voice and video dialling and connectivity through IP technology, VLAN and VPNs, recovery management system and many more. The network is utilized for better business transaction, saving cost through VOIP solutions and reducing telecom traffic carriers. Enterprise networks are capable of supporting different devices and services which increase access flexibility. Internet facilitates enterprise information among company employees for posting different announcement to all the employees. Main issues in enterprise networks are unavailability of resources when devices become offline, capacity requirements, and traffic performance decrease. Thus we require network operations to be working and the business process to continue without any errors and problems.

2.5 NETWORK MANAGEMENT

Networks management requires managing enterprise, ISPs and MPLS networks through network management applications. Although intelligent switch, routers and other network devices are deployed on the network but still proper configuration is required and a system is suppose to be develop to dissolve any device failures. NMS have complete overview of the network manage record and audit files, help network, help traffic engineering, modelling, planning, backup configuration, quality of service provisioning etc effectively. SNMP V3 is currently used to configure devices on the network, extract information regarding fault, configuration, accounting, performance and security (FCAPS). The goal of NMS mainly concerns about any fault, event or alarms notificiation.

In MPLS network management addresses Management Information Base (MIB) and its elements to make MPLS network operation [8]. MPLS LSR MIB and MPLS TE MIB are two MIBs describe by IETF standard. They aim to obtain management of low level MPLS objects i.e. table segment interfaces and cross connect, high level MPLS objects i.e. resource blocks, EROs and traffic tunnels and creation of LSPs. LSR MIB include MPLS interface configuration, in/out segment, label stack, traffic, performance parameter and cross connects. TE MIB object consist of TE tunnel resources/ path/ and performance counters.
Chapter 3

MPLS Overview and Architecture
MPLS is evolved through ATM and frame relay VAN networks; MPLS uses labels to advertise between different routers by means of label mapping through label switching mechanism. Previously frame relay uses frames while ATM uses cells to map labels, to label switching techniques, frames cannot be of fix length while the cells consists of fix length with 5 bytes of header and 48 bytes of payload. ATM and frame relay are identical in a way when label traversing each hop in the network causes the label to change the header value. This differentiate from the traditional IP network when IP packets are forwarded through router it does not change the value at the header of the IP packet i.e. destination IP address. MPLS also adds the label at the ingress Label Edge Router (LER) of the MPLS network, changes the label value at each LER within MPLS network until it reaches the egress LER, where completely removes the MPLS label and the data packet is forwarded towards destination IP address [5].

The reason for implementing IP technology in early stage was such that label switching technology was slower and routers forward the IP packets toward the destination IP address by looking at the IP header and finding exact match in the routing table. This IP table lookup was easy in start but with unicast and multicast IP addresses the IP table lookup was complex and require more time then before. CPU capabilities for computing IP lookup table becomes limited and the bandwidth links were around 40 Gbps, which causes the link to be unused due to low processing speed or complex computations.

Network infrastructure for data communication is divided in to Control plane and Data plane. Control plane comprises of routing protocols, table, Signalling protocols etc. While Data plane forward packets between router and switches. Application specific ICs are built to perform data plane forwarding packets that enable IP packets as well as Label packets at identical data rate. In order to utilize the unused links or avoid congestion in the network can be done through implementing MPLS technology.

3.1 MPLS BENEFITS

This section will depict possible benefits as compare to IP, ATM and frame relay technologies.

3.1.1 SINGLE NETWORK STRUCTURE

MPLS network adhere ingress LER to describe labels for incoming packets toward egress LER through predefine criteria in network infrastructure. The reason for IP emergence and dominance is because of current IP support technologies development. Integrating MPLS with IP we can exhibit better transport for the packet delivery. Layer 3 IP backbone can implement MPLS similar to ATM and frame relay at layer 2. MPLS provide support for Point to Point Protocol (PPP), IPV4 and IPV6, Ethernet and similar layer 2 technology. Any transport over MPLS (AToM) mechanism allows routers to switch layer 2 traffic without interfering about MPLS payload while using label switching mechanism describe by MPLS [9].

3.1.2 IP OVER MPLS

Previously IP was deployed as layer 3 networking protocol due to its simplicity. ATM is layer 2 protocol which offers end to end protocol connectivity but had limitations in ISP
WAN protocols. RFC 1483 implements IP over ATM to achieve multiprotocol encapsulation over ATM adaptation layer 5. This implementation requires IP mapping and ATM end point to be configured manually. Another solution was an implementation of layer 2 Ethernet LAN emulation at the Edge Router connecting the network but this solution had limitation in reliability and network scalability at ISP side. The only possible solution was to make ATM switches intelligent enough to route label switching technology with label distribution protocol and also to run IP routing Protocol which was made possible through MPLS technology.

3.1.3 ISP PROTOCOL DEPENDANCY

In an ISP IP network, the forwarded traffic performs the destination IP address lookup in the router to send the data to desire destination. If destination is external to ISP network, which means an external IP prefix exists in the routing table of every ISP network router. Border Gateway Protocol (BGP) is responsible for both external internet and customer prefixes so every router of an ISP network must depend upon BGP protocol. While MPLS perform packet forwarding through label lookup only associated with egress router. Thus the label contains information regarding the packet for every intermediate router in the network instead of core router present at ISP network. Only MPLS edge router need to run BGP to perform destination IP address lookup to forward the packet in an ISP, IP network.

3.1.4 MPLS VPN MODEL

Virtual private network interconnects customer sites through common ISP network infrastructure. ISPs are able to deploy either overly VPN model or peer to peer VPN model. In an overlay model ISP provides point to point virtual circuits links between customer routers at desire location. ISP is unaware of customer routes due to direct peering routing between customer routers. The overlay model can be implemented through IP network or frame relay switches at either locations implementing tunnelling mechanism. In case of peer to peer model ISP routers participates in customer routing at layer 3.

3.1.5 TRAFFIC ENGINEERING (TE)

It is a mechanism of achieving optimal use of traffic resources and links which are left unutilized due to network and protocol limitations. Internet technology and protocols had proven to be worst in performance, congestion, bandwidth and link utilization, QoS guarantee and path selection. MPLS implements TE to control traffic flows between congested nodes, allows path selection for unutilized paths or shortest path first, low cost path mechanisms applied in IP routing. More detail about traffic engineering is discussed in later sections.

3.2 MPLS ARCHITECTURE

MPLS architecture consists of MPLS routers connected through mesh topology. MPLS infrastructure network consists of following routers [9-10].
3.2.1 INGRESS/EGRESS LABEL SWITCH ROUTER (LSR)

LSRs deployed at perimeter of MPLS network which provides an interface to inside MPLS domain and to outside the IP network. The role of ingress/egress LSR is to insert and remove labels when deployed as an ingress and egress. An ingress LER inserts label on the data packet called as imposing LSR and forward it towards egress LSR after passing through number of hops where egress LSR removes the label called as disposing LSR and forward it towards data link. These two routers are also known as Provider Edge Routers.

3.2.2 INTERMEDIATE LABEL SWITCHING ROUTER

LSR are devices present in MPLS domain to perform swapping, push and pop operations of incoming and outgoing packets towards ingress/egress LSRs. They receive an incoming label packets swap, push and pop labels perform packet switching and forward it towards correct data link. The packet forwarding mechanism based on information present at each label.

3.2.3 LABEL SWITCHING PATH (LSP)

It’s a sequence LSR path from ingress LSR followed by number of selectable intermediate paths towards egress LSR. The figure depicts unidirectional LSP from ingress LSR followed by three intermediate LSR towards egress LSR. If the packet has already been labelled by ingress LSR then this case is called as nested LSP.
3.2.4 MPLS LABELS

An MPLS label consists of 32 bits depicted in figure. The first label value consists of 120 bits followed by 3 experimental (exp) bits to control quality of services (QoS). Bottom of stack (BoS) identifies the number in the stack label, if it’s 0 which mean bottom label stack otherwise if it’s 1 stack contain number of labels above the packets so the stack can have one or more labels. First label in the stack is called top label while the last label is term as bottom label which is shown in figure 3.2. Time to Live (TTL) consists of 8 bits with the same functionality present in IP header. It avoids routing loops by decreasing TTL value after traversing each successful hop. If TTL value in label becomes 0, packet is discarded.
3.2.5 FORWARD EQUIVALENCY CLASS (FEC)

This term is used in MPLS to allow same group of packets to follow along same path and should be treated identically during packets forwarding. All the packets which belong to same class have same level however in some cases they have different labels if EXP have different value that will consider different forwarding mechanism due to different FEC. Ingress LSR decides packet forwarding based on FEC because it classify labels in the initial stage [10].

Layer 3 packets following towards destination IP address contain prefix, it might be certain group of multicast packets or packets based on precedence or forwarding treatment, and also layer 3 IP address maintaining same BGP prefix and same next BGP hop are some examples of Forwarding equivalency class.

3.2.6 LSR OPERATIONAL MODES

There are three different modes of LSR during label distribution mechanism to other LSR.

a) Label Distribution Mode

Its consists of downstream on demand label distribution mode in which every LSR make request to the coming hop in a downstream LSR through LSP for binding FEC. Single FEC binding is received by LSR through down streaming LSR is upcoming hop describe in IP table. The other distribution mode is downstream label distribution mode binds FEC distribution to nearly LSR, where every LSR received binding information through neighbouring LSR. Downstream on demand label distribution mode offer single binding while unsolicited downstream gives multiple FEC bindings.
b) Label Retention Mode

Liberal and conservative label retention modes are present. In case of liberal label retention Label Information Base (LIB) maintains remote binding information through downstream or through upcoming hop. The label binding is utilized in Label forwarding information base (LFIB) but no other labels are kept which are not used for forwarding packets. The cause for storing remote binding in LFIB is subject to topological change and implementation of dynamic routing due to downlink of router. Conservative label retention mode configure on an LSR does not contain all remote bindings except an associated upcoming hop in its LIB. However LLR will help in rapid routing topological change while CLR utilizes memory efficiently.

c) LSP Control Mode

In LSP control mode independent and ordered FEC bindings are performed. FEC local binding is established independently by the LSR without involving other LSR and creating a specific FEC local binding according to FEC classes. Ordered LSP binds FEC unless recognition is obtained through egress LSR or label binding from an upcoming hop.

3.3 MPLS LABEL PACKET FORWARDING

In MPLS network label packet forwarding has different phenomena then traditional IP packet forwarding. We describe packet forwarding mechanism in a step by step procedure [11].

a) Three main operations are performed in labels i.e. Push, Pop and Swap. Figure 3.3 illustrates an example of push pop and swap. LSR determines according to the LFIP information when label packet is received at LSR either top label should be swap, pop and push. In label swap operation label 20 is replaced by label 35 when it pass through LSR. During Pop operation stack label 12 is removed from the stack after passing through LSR. While in push operation label 9 is inserted on the top of stack.

```
<table>
<thead>
<tr>
<th>Label</th>
<th>Label</th>
<th>Label</th>
<th>Label</th>
</tr>
</thead>
<tbody>
<tr>
<td>20</td>
<td>35</td>
<td>5</td>
<td>7</td>
</tr>
<tr>
<td>IP</td>
<td>IP</td>
<td>IP</td>
<td>IP</td>
</tr>
<tr>
<td>12</td>
<td>POP</td>
<td>8</td>
<td>9</td>
</tr>
<tr>
<td>IP</td>
<td></td>
<td>IP</td>
<td></td>
</tr>
</tbody>
</table>
```

24
b) IP lookup is performed when IP packet is received at router while label lookup is performing at the router through LFIB with particular Cisco Express Forwarding (CEF) class. So router identifies an IP over label packet through protocol information at layer 2 header. If CEF or LFIB forward the packet so it can be unlabeled or labelled depending upon CEF-IP lookup or LFIB-label lookup. Both cases are shown in Figure 3.4. In first case CEF performs IP lookup for an incoming IP packet at LSR that leads to two possible outcomes i.e. IP-IP packet or IP-label packet respectively. In second case a label packet is received by the router so LFB performs label lookup and forward the packet either label-IP or label-label respectively.

Figure 3.4: CEF Lookup and LFIB Lookup

![Diagram of CEF and LFIB lookup](image)

c) Load balancing for desired label packets is performed by Cisco IOS, these packets may have same or different outgoing labels. Same label exist if the link is between the link and routers belonging to label platform space but they are different in case multiple upcoming LSR are present since upcoming LSR
independently provide labels. However IP over MPLS network offer packet labelling procedure for MPLS domain and whenever packet leaves MPLS network it becomes unlabelled.

d) There are 0 to 15 labels reserved which LSR doesn’t use in normal cases to forward packet where label 0 stands for explicit null label and label three for implicit null label. Implicit null label is assigned by egress LSR if label is not assigned for FEC to accomplish pop label operation. Alert label is defined by label 1 while OAM alert label is used through label 14 that provides network management operation and maintenance.

e) Beside reserved labels, unreserved label are used to forward normal packets and it consists of 20 bits, with the range of 16-10000 labels. They are significantly enough for normal labelling packet but if IGP prefixes are to be labelled we can change the range to make them sufficient.

f) Time to live (TTL) changes its values based on the label operation i.e. swap, pop and push at each arriving LSR. In order to perform swap label operation incoming packet label TTL become equal to current label – 1, for push label operation the incoming packet label TTL becomes also label – 1 and copied at swap label. In case of pop operation the incoming packet label TTL copies label – 1 to expose label.

g) When LSR receives the packet with TTL equal to 1, it automatically drop that packet and generate ICMP message for time expiry.

h) Maximum Transmission unit (MTU) is present in IP packet which indicates possible IP packet size sent through data link layer. Similarly MTU in MPLS is used for label packets and are bigger in size then IP packet since 4 bytes are used for every label in addition to the packet. MTU default value is 1500 bytes while MPLS MTU uses 1508 bytes including labels which are possible to sent over data link without any fragmentation processes.

3.4 CISCO EXPRESS FORWARDING

It is packet forwarding and switching mechanism specifically design for MPLS networks. Basic functionality of the router is to forward packets towards the destination through traversing addresses in IP table lookup and making decisions regarding next hop i.e. switch or router. Every router has specific protocol to perform packet forwarding mechanism and the information is stored in forward table. There are three basic ways in which routers forward the packets.

3.4.1 PROCESS SWITCHING

It is a slow process which involves routers to switch packets where Cisco IOS performs packet application in CPU memory to perform destination IP lookup in IP tables. After receiving result from IP lookup table packets are switch towards specific interface after housekeeping for IP headers, TTL and CRC are recalculated during housekeeping. Every IP packet forwarding information is present in the packets itself which routers CPU processes.
3.4.2 FAST SWITCHING

It is a switching mechanism based on demand forwarding. Process switching is performed during the recipient of first packet to the destination while CPU built and maintain the cache non as IP fast switching route cache to allow identical packets following the same destination. Although the cache is temporary and depends on the time entries in that cache or add and deleted causing CPU member free. Cache keep the entry records until packets are switch towards same destination, however these entries become unneeded and are deleted when no packets following the same distinction are switch. Problem pertaining fast switching occurs during prefix change related to routing table so cache entry become invalid and the packet switching process entry needs to be built again for route cache.

Due to demand building fast switching cache problems arise, the solution to avoid this switching cache resulted in CEF switching. Now switching tables are not constructed through demand rather they are built in advance such that every prefix has an entry in routing tables and CEF switching table.CEF is necessary for MPLS networks because router contains LFIB entries regarding the labels and IP packets which enter MPLS domain are switch through CEF tables. Despite of IP packet or label packets at LSR and IP table lookup are CEF table lookup the resultant packet forwarding could be either and IP packet are a label packet. CEF consist of two main data structures.

a) Forward Information Base
b) Adjacency Table

FIB itself is CEF table which handles lawyer 3 forwarding and is identical to IP routing table, even prefix entries are identical.FIB also contain information about IP prefix, upcoming hop and connected interfaces .It also contain information for distance and matrix calculation based on specific protocol. While Adjacency Table manages neighbouring devices through MAC layer 2 rewriting. In multi access enjoinment dynamic device discovery mechanism is used by the routers through ARP that MAC address to IP address.

IP packets are label through CEF table at ingress PE router while these IP packets obtain more than one labels travelling through MPLS networks.LSR are capable of inserting more labels only through LFIB functionality but cannot use CEF table to assign labels. LDP, RSVP or BGP are also capable of assigning labels through recursion.

CEF load Balancing or Sharing is of significant importance for dynamic multi direction links for forwarding IP are label packets and depends on maximum available path for prefix. Per- packet load balancing offers balancing all the packets with round robin technique. Per destination load balancing is default CEF scheme and performs hashing functionality for source and destination address.
Traffic engineering has to minimise network congestions by modifying routing patterns and exhibits traffic mapping streams with network resources that explicitly cause reduction in congestion and also it provides better quality service with latency packet loss and jitter [10]. MPLS TE is implemented by extending IP protocol for forwarding packets to decrease any failure caused in the network and increases efficient service delivery. MPLS TE defines routing capabilities in its network by TE label switch path.
In figure 3.6, there are multiple nodes from source hop 1 and hop 5 to destination hop 4 and 8. The traffic from hop 1 and 5 forwarded to hop 4 explicitly routed from hop 2 and 3 while traffic from hop 1 and 5 forward towards hop 8 explicitly routed from hop 6 and 7. Hop 2, 3, 6 and 7 are LSRs offering LSP A, LSP B, LSP C and LSP D.

- **LSP-A: (Hop1 - Hop2 - Hop3 - Hop4)**
  Hop 1 and hop 4 are ingress LSR and egress LSR while hop 2 and 3 are an intermediate LSRs.

- **LSP-B: (Hop5 - Hop2 - Hop3 - Hop4)**
  Hop 5 and hop 4 are ingress LSR and egress LSR while hop 2 and 3 are an intermediate LSRs.

- **LSP-C: (Hop1 – Hop6 – Hop7 – Hop8)**
  Hop 1 and hop 8 are ingress LSR and egress LSR while hop 6 and 7 are an intermediate LSRs.

- **LSP-D: (Hop5 – Hop6 – Hop7 – Hop8)**
  Hop 5 and hop 8 are ingress LSR and egress LSR while hop 6 and 7 are an intermediate LSRs.

However IGP in IP networks will only compute smallest path or cost towards source to destination i.e. hop 1 to hop 4, hop1 to hop 8, hop 5 to hop 4 and hop 5 to hop 8. IGP uses single metric to compute routing information which may be acceptable for very simple network but internet is complex networks of hops so MPLS TE will provide better routing capabilities through constrain based routing mechanism. MPLS TE routing mechanism follow certain constraints on LSRs for computing path towards ending LSRs to forward packets through TE LSP.

### 3.6 MPLS TE OPERATIONS

There are four main operations performed in MPLS TE.

#### 3.6.1 LINK INFORMATION DISTRIBUTION

It extends IP link state with distributed topology information since LSR implementing constraint base routing should know current extending link list and its attributes for implementing those constraints in path selection. OSPF and IS-IS are two link base protocols that offers capabilities for distributing attributes where LSR develop TE database apart from normal topological database based on these capabilities. MPLS TE also increments bandwidth availability attribute with 8 priority levels are describe for TE LSPs, TE metric attribute is used for optimizing paths identical to link metric in IGP, and administrative group attributes enforces inclusive an exclusive rules.

#### 3.6.2 COMPUTING PATHS

TE LSP develops a TE topological database to perform CBR along with shortest path first algorithm. Both work in integration to implement CSPF algorithm to determine
shortest path and optimal path approximation but are unable to guarantee optimal traffic mapping stream for network resources.

3.6.3 TE LSPs SIGNALING

MPLS TE signals LSP through RSVP by introducing following objects.

a) LABEL_REQUEST
   It is used to bind label at every hop.

b) LABEL
   It is used for Resv message distribution.

c) EXPLICIT_ROUTE
   It define explicit hop list for signalling.

d) RECORD_ROUTE
   This object gather label and hop information during signalling path.

e) SESSION_ATTRIBUTE
   It defines LSP attribute requirement such as protection, priority etc.

3.7 BASIC MPLS DEVICE AND INTERFACES

MPLS devices maybe IP routers, ATM switches or multiservice switches. However multiservice switch is best selection among the devices because it offers service connectivity with IP, MPLS, frame relay, Ethernet, X.25, and TDM. MPLS interface configuration include IP routing, IGP routing protocol along with TE i.e. ISIS-TE and OSPF-TE however IGP routing protocol implementation is not necessary while static routes are used, EGP protocol implementation in case of autonomous system, and LDP or RSVP signalling protocols.

3.8 MPLS OPERATIONAL MODES

There are two MPLS operational modes

a) Frame Mode
   In this operational mode packets are labelled and exchanged in frames at layer 2 to work through unicast IP destination routing. In MPLS data plane, three tasks are performed.

   • Ingress router perform FEC classification over received IP packet and stack the label corresponding with FEC while in destination based unicast IP routing FEC refers to subnet destination and layer 3 lookup is in the forward table is performed for packet classification.

   • Intermediate LSR then perform lookup in label forwarding table for inbound label and outbound label of incoming packet with respect to similar FEC i.e. IP subnet.
- The label packet received for similar FEC at egress router removes the label through layer 3 lookup which produces an IP packet.

Label binding in frame mode is implemented through IP subnet and MPLS labels for unicast destination based routing with the help of Tag distribution protocol (TDP) and label distribution protocols (LDP).

b) **Cell Mode**

In MPLS cell mode ATM LSRs forward cells instead of packets, similarly ingress router perform forwarding table lookup assign label to a packet. Each packet is segmented to form different cells while every cell VPI/VCI will get a label value. These cells are forwarded through intermediate LSRs based on the LFIB information. ATM LSR manages cells individually and cells with VPN/VCI label values are sent towards upcoming hop. At the edge of MPLS domain, egress router performs re-segmentation to form a frame.
Chapter 4

IP Networks
Rapid growth in the network technology emerge computer systems to communicate through protocols. Computers systems become connected through physical and logical transmission media to share information among the networks. Before single computer centre existed and the concept was completely change with organization needs to interconnect multiple computers for processing and storing data share information and running Clint server application on the systems, which is resulted in the formation computers networks. In a computer world the connection is establish between two autonomous systems for exchanging information connected through some transmission medium i.e. fibre, copper, microwaves, and satellites etc. Computer network consist of actual machine with similar /different operation systems running some programs and performs some operation through interconnection [12].

Computers networks are required for business application i.e. sharing same resources, storing data and databases, accessing printer and scanning devices, running client server applications; for home application i.e. e-commerce, person to person, multimedia and interactive entitlement which constitute of newspaper, history, information, hobbies, health, support, research, sms, chat rooms, video on demand, movies and television programs, product sale/ purchase, etc; for mobile users i.e. pads and note book connective to be able to access internet services during motilities, etc.

In an internet, computer networks consist of number of interconnected devices i.e. router, switches, servers, end nodes and they need common protocol mechanism to performs communication.OSI defines seven layers for the communication mechanism whereas   internets implements TCP/IP protocols to establish communication path and performs data transmission. Point to point and broadcast link transmission mechanism are used [13]. In broadcast network all the machine share single channel for communication while point to point network maintain individual connectivity between the devices. Short messages i.e. IP packets are sent from source to destination entertain by single/multiple routers and switches. IP packet contain destination address of the packets but in case of broadcast network all the packets are deliver to all the nodes connected to the network through using broadcasting code in the address field, multicasting occurs when IP packet are sent to a subset of nodes. In point to point networks unicasting is performed since they is single sender node and single recipient node [14].

4.1 IP STANDARD ARCHITECTURE

Traditional centralized IP network consist of large centralized processor connected with two terminals at either sides or computing resources. Internet contains an infrastructure of core routers connected through Tetra byte fibre optic transmission medium. The core routers provide link to ISPs or enterprise network through T3 line of Giga byte transmission such that ISPs connect common business, homes and other ISPs with local area network, or metropolitan area network.LAN consist of small number of networks
nodes connected through ether net and consist of bus, ring, star, mesh etc topologies.

Bus and token ring topologies form a broadcast network. MEN encircle cities through simple bus topology connected either through Ethernet or wireless access; cable TV is an example of MAN network. WAN covers larger geographic area i.e. countries, or continents. Larger ISPs are often consist of WAN networks and involves communication subnet to carry transmission lines and performs switches for end nodes running application programs at the user premises. Transmission lines consist of high speed cannel i.e. fibre optic, copper, radio links, whereas switching is performed through specialized computers which connect these lines across countries/continents. Since there are different types of networks which connect nodes and other networks, in order to perform transmission between nodes of different types of networks gateways are required to connect them and performs hardware software translation, this mechanism is called internet or network [12].
In Connection oriented communication architectures model network offers service through establishing connection before data transmission. PSTN is common example when receiver receives the calls it replies and end to end connection is establish through switching offices. Data follows in a sequential manner along in the path between source and destination. In data network TCP provide connection oriented services with quality and reliable of data transmission. Connection less architecture operates similar to post system in which source and destination addresses are present. Network devices use information attached to the packet and independently route the packet towards destination address. Connectionless transmissions depend on best efforts data transmission and do not provide guarantee QoS. So packet may deliver un-sequentially with delay variations, and may also be lost during transmission [15-16].

4.2 Internet Protocol

IP was developed to transmit internet data gram from source to destination by passing through interconnected system and network devices. Data gram is a bulk of data transmitting through connectionless network its transmission is analogous. An IP data gram of email message consist of data gram length and addition of information header implemented by TCP or TCP header forward the packet to the routers along with 802.3 frame header [17], router take off the frame header and forward data gram, check for destination IP address and forward the data gram towards the destination IP address. In case of virtual circuit connection a connection oriented mechanism, first the destination address is concerned and desired path is establish performed data transmission. After a change of information the path is realised by realising the network resources. Since IP is connectionless protocol while TCP is connection oriented protocol, by integrating two protocols we can converge between reliability and unreliability of data transmission [12].

4.2.1 Data gram Fragmentation/Defragmentation

IP deal with fragmentation and defragmentation during data gram transmission by IP address to ensure that data gram reached the correct destination address; this is how IP provide address consistency. IP data gram fragmentation and defragmentation is mandatory in some cases when data gram frame sizes are different with respect to LAN or WAN.
4.2.2 IP Header

IP header have 20 octets for control information, IP version is defined with Version (4 bits), IP header is 32 bits words measure through internet header length (IHL), IHL also measured offset, 8 bits of types of service defines required data gram QoS. Real time application like voice and video QoS is required to set a priority for voice datagram samples and therefore assure packet delivery and reliability. In one types of service fields is describe for voice and video application, total length field (16 bits) calculate IP datagram in octets up to 65,535. Fragmentation offset consist of 8 bits if data packet are different in sizes LAN and WAN fragmentation is performed on large IP datagram called fragments to fit in the communication traffic capacity and are reassemble at the destination node. 16 bit identification field is use to reassemble the datagram from the fragments, this field contain 3 flags values; if bit 0 is set 0 which mean “reserve”, if bit 1 set to 0 it mean “may fragment” and if set to 1 which means “don’t fragment”, similarly if bit 2 is set to 0 it mean “last fragment” and if set to 1 means “more fragment”. The 13 bit fragment offset links the fragment to a complete message. Time to live 8bits measures the time of datagram within the internet while if TTL is equal to 0 then datagram is destroyed is measured in second or per hops. The maximum TTL for datagram is 225 second while 64 is a default value used in many systems. Trace route and ping commands are used for diagnosing TTL. 8 bits protocol fields identifies higher layer protocols i.e. UDP TCP and ICMP. 16 bits header checksum performs integrate check on the receiving data pack. 32 bits source address identifies 32 bits source address of the network node while 32 bit destination address locate the IP destination of the network node. 32 bits option and padding fields is of variable length and contains datagram information as well as stream identifier, source routing, time stamp and security information [17].
4.3 Intranet work Routing Communication

IP datagram consist of 32 bits address per source and destination identification but in the communication channel internet work of datagram may perform and the intermediate devices i.e. routers manipulate information to identify destination address in their routing tables to forwards datagram to correct circuits, however due to change in network topology circuits might fail due to congestion.

Router perform some function on incoming packets by correcting destination address efficiently through routing table information and forwarding table and makes optimize paths available for each packets. Forwarding table can be built manually or can perform packet forwarding mechanism dynamically based on adjacent routers and network topology constants. Static routes are easy to construct but difficult to maintain because for same sources and destinations with packet flow with specify path which reduce efficiency bandwidth and resource utilization, can cause congestion and link/node failures due to continuous constant transmission between static routes, and some portion of the network resources still be unutilized. Static routes are not the correct solution for better quality of service, resource utilization and reliable transmission of data packet as compared to dynamic routing [13].

Dynamic routing is implemented to better to accept changes in network by running different protocols and algorithms to use metrics for finding shortest distance from source to destination. The metric parameters can based on shortest path or list cast between the end points. Link state algorithms makes decision based on links which connects the nodes in the network. Distance vector algorithms measures smallest
distance between source and destination to transmit datagram. Routers implements links state algorithms and distance vector algorithms in intranet work communication. IGPs use these algorithms while routing information protocol (RIP) implements DV algorithms. OSPF is also an IGP decide routes through like state algorithms.

4.4 Routing Information Protocol

RIP is used for integrate way communication, he uses distance vector algorithms in which routers exchange information through its routing table periodically. The path form source to destination is determined as a best path which contains less number of hops. The protocol implementation is such that many LAN OS itself implements RIP so it gives interoperability problems along with allowing only 50 hops path length which is less a number, Routing loops are present internetworks because its requires more time to get a updated routing information. All the devices running RIP must have RIP driven routing table contain destination IP address a matrix per calculating cast next router address and a flag value. RIP packets exchange routing information by transmitting message from 522 UDP port [18].

The packet format of RIP in which first 8 bits (Command).Command field takes following values:

![RIP Header](image-url)
<table>
<thead>
<tr>
<th></th>
<th>It request for information in the routing table</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>Receive reply from the routing table</td>
</tr>
<tr>
<td>3</td>
<td>Trace on</td>
</tr>
<tr>
<td>4</td>
<td>Trace off</td>
</tr>
<tr>
<td>5</td>
<td>Sun micro system has reserve this value</td>
</tr>
<tr>
<td>9</td>
<td>To update the request</td>
</tr>
<tr>
<td>10</td>
<td>To update response</td>
</tr>
<tr>
<td>11</td>
<td>To update acknowledge</td>
</tr>
</tbody>
</table>

Next 8 bits contain “Version”, which is version number of RIP. Next 16 bits must be 0 then 16 bits identifier; again next 16 bits must be 0. The RIP packets have routing information entries i.e. destination IP address and metric. Metric entry obtains normal values from 1 to 15 but if the entry becomes 16 then destination address become unreachable. RIP facilities 25 entries per routing information along with datagram. RIP V2 [18] provides additional security to RIP messages and is almost identical to original format 2 only the “version” field contains V2 while command, IP address, metric, field, address family identifier are similar. There is a route tag field to preserve route information i.e. internetwork or intra net. A subnet mask field consist of 24 bits and provide an association with routing entries, a next hop field also consist of 32 bits and provide IP address next hop in the routing entry.

RIP is implemented in WAN circuits for specific traffic demands and helps to establish connection by periodically transmit routing information however the cost met increase since fixed bandwidth and point to point link connectivity this provided as well as routing updates are transmitted periodically which ultimately effect user data. RIP modification is addressed in triggered RIP for receiving routing updates through some special request, or an update routing data base entry, or the change of destination state request initiated by circuit manager or when the device is switch on. RIP triggered updates are received through defining three new packet i.e. update request, response and acknowledge.

### 4.5 OSPF Protocol

It uses link state algorithms and have multiple advantage as compare to RIP protocol i.e. hierarchical topology configuration, dynamism in adopting internet changes, scalabilities option for large networks, based on minimum cast out with balance traffic loading, authentication for routing table information change, an ability to use different
subnet mask. Each datagram consists of type of service and IP address field in OSPF protocol to calculate and optimize path for each TOS [19].

### 4.5.1 Distance Vector verses Link state algorithms

We will compare some key aspects of both algorithms used for OSPF and RIP routing protocols.

<table>
<thead>
<tr>
<th>Distance Vector Algorithm</th>
<th>Link State Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Packets are routed through measuring the routers hops and the distance between source and destination.</td>
<td>- Link algorithms perform routes discovery through type of service instead of number of hops</td>
</tr>
<tr>
<td>- RIP implementing DVA can offer up to sixteen hops which seem as a huge disadvantage for network scalability.</td>
<td>- Network manager has flexibility to describe least cost path between two end nodes and delay, reliability, cost etc.</td>
</tr>
<tr>
<td>- DVA deployed in a network has flat topology and network is divided into small manageable domains.</td>
<td>- Link state has hierarchical topology for routers to internetwork routing information distributed networks which helps in reducing routing processing time and also bandwidth requirements and usage.</td>
</tr>
<tr>
<td>- The numbers of hops are measured without having an effect of communication link parameters i.e. Cost or speed of the link.</td>
<td>- Autonomous systems are running LSA to distribute their routing information to common setup protocols. Since as is split into different areas each of them having routers and host forming an invisible topology. Also as use different topology information for the databases.</td>
</tr>
<tr>
<td>- Router running rip broadcast routing table periodically, after every 30 second.</td>
<td>- Routers provide connection base upon different areas e.g. internal routers operate within their own area and built connection with other routers as well as maintain important information regarding that area. Router at border only connects with multiple areas and may run routing algorithms separately.</td>
</tr>
<tr>
<td>- Rip packet can have maximum half 25 route entry information so if routes have more than 25 routes then for every 25 routes single rip packet are required.</td>
<td></td>
</tr>
</tbody>
</table>
4.5.2 OSPF Packet

OSPF hello protocol message are transmitted to neighbouring routers for synchronizing databases and manipulate routes through routing table as well as transmitting link state advertisement in a domain. OSPF contain five packets within IP datagram to perform above operation. There are five main types of OSPF packets having a size of 24 octet header.

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Hello</td>
<td>Inform, maintain, and find neighbours</td>
</tr>
<tr>
<td>2</td>
<td>Database description</td>
<td>Its gets information about the contents of database</td>
</tr>
<tr>
<td>3</td>
<td>Link state request</td>
<td>To download the database</td>
</tr>
<tr>
<td>4</td>
<td>Update</td>
<td>To update the database</td>
</tr>
<tr>
<td>5</td>
<td>Link state acknowledgment</td>
<td>To receive acknowledgment after flooding</td>
</tr>
</tbody>
</table>

Header contain 32 bits of router ID, 32 bits of area ID, 16 bit Checksum, autype 16bit and authentication field of 64 bits for validating packet through three authentication types i.e. 0 for null authentication, 1 for simple password and 2 for cryptography implementation. In order to have null value in authentication type does not ensure any authentication procedure between the 2 routers exchanging there routing information.

A 64 bit authentication field contains simple authentication procedure by using 64 bit password on the router/network i.e. every device on network should have the same implementation configured. In case of cryptography, all the routers/network have configuration for shared secrete keys and the datagram is protected through digest message.

```
1111111111122222222333
```

![OSPF Packet Header Diagram](attachment:image)
4.6 Exterior Gateway Protocol

Autonomous systems are group of router belonging to a single domain which implements exterior gateway protocol for routing and communication with other domains. The main task of EGP is to convey messages for reachable/unreachable networks domain; IP runs EGP and assigned number 8. Acquisition request/conform messages are send between neighbouring network domain i.e. routers to exchange information regarding reach-ability and un reach-ability. IHY message are sent between neighbouring and update messages for reach-ability and un reach-ability are received. In [5] routing information messages exchange between AS has following procedure.

The request message is sent to inform the neighbours with variable parameters polling, a confirm message is obtained or refuse messages is obtained describing the neighbour acquisition acceptance or refuse. The cease and cease-Ack messages are sending to de-acquisitioning neighbour. Hello and IHU assured the neighbouring AS reach-ability while poll, update and error messages result in net reach-ability request/ update and an error [20].

Figure 4.5: EGP Packet Header
4.7 Border Gateway Protocol

In [21] BGP version 4 is described as it works as an inner AS protocol. BGP runs on TCP for connection-oriented transmission and higher reliability. It works through TCP port 179 and also provides support in route aggregation and classless interdomain routing. If two systems, i.e., routers, run BGP and connect two different AS the links are termed as external links while if the connects in same AS there are called as interlinks. TCP is used to establish connectivity between two routers in same or different AS to provide reliable exchange of routing tables and their updates stored in routing information base (RIB). BGP has a constant 152-bit message header, which contains four message types i.e. update, open, keep-alive, and notification messages. Only keep-alive messages provide automatic message request while the other messages also include more information.

![Figure 4.4: BGP Message Header](image)
Chapter 5

Routing Protocols and Mechanism
5.1 MPLS Protocols

Multi-protocol Label Switching (MPLS) defines a mechanism for sending packet data network routers. It was originally developed as soon as the packet is sent with the traditional routing IP, although improvements in hardware routers to reduce the value of the speed forwarding package. However, the flexibility of MPLS means that he is still the default in today's networks to ensure quality of service (QoS), VPN services and next-generation optical signals.

The traditional IP networks which are connectionless upon receiving the packet the next hop is determine by the router using the destination IP address which is present on the packet. The networks routers contain information about the topology of the network. These protocols OSPF, IS-IS, BGP, RIP are used by the IP router so the information or the data is synchronize with the network. The data flow of the MPLS is connection oriented and along the pre configured path the packets are forwarded. These pre configured paths are called as LSP’s.

5.2 MPLS routing protocol

The network topology information is distributed through the network by then use of the routing protocol so by this way the LSP can be calculated. OSPF or IS-IS, the interior gateway protocols are normally used, however only the network topology information is distributed in these protocols.

5.3 MPLS signalling protocol

Along the route the signalling protocol informs the switches which of the labels and the links are to be used for each LSP’s. Depends on the networks requirements the two main signalling protocols are used. Where the traffic engineering is required the RSVP-TE is used. When the traffic engineering is not required then the LDP is used as it requires less management.

5.4 Label Distribution Protocol (LDP)

The LDP is the fundamental protocol under the circumstances of the MPLS (Multiple Protocol Label Switching) environment, and it’s the responsibility of the label switching router (LSR) that whatever the traffic passing through it just swap the label and then forward the traffic. This all means that in any kind of traffic under the circumstances of the MPLS environment label distributed over the passing traffic. To achieve label distribution mechanism there is method that is called `piggyback’. Piggyback means that riding on the back, so it means that we can use the existing routing protocols and over them we can use the mechanism of piggyback [22].

In we want to use the Interior Routing Protocols (IGPs) like EIGRP (Enhanced Interior Gateway Routing Protocol), OSPF (Open Shortest Path First), IS-IS (Intermediate System-to-Intermediate System) and RIP (Routing Information Protocol) then what we have to do in order to use the label mechanism we have to change the IGP for the required protocol, because all these protocols are used as a routing protocol in today’s network environment.
There is also another solution for the label distribution mechanism that is we will develop a new protocol that works independent of the routing protocol. It works as a standard on the Internet traffic and there will be no dependency on the routing capabilities, which is the reason LDP (Label Distribution Protocol) is developed. LDP (Label Distributing Protocol) carries labels over the MPLS network. There is only one exception in the LDP protocol that is it doesn’t work under the circumstances of the Exterior Routing Protocol (ERP). There is one protocol which works under exterior routing mechanism that is called BGP (Border Gateway Protocol). Why there is an exception in LDP for the BGP? There are mainly two reasons that are more important which is given below:

1. BGP is more efficient and it is also a multiprotocol and it carries labels with little effort.
2. BGP is the exterior routing protocol which carries information between the two different autonomous systems and it is a trusted protocol which works among different companies.

In LDP protocol the main functional device is the LSR (Label Switching Routers) whenever the traffic comes under the circumstances of the LSR then LSR must agree upon the labels so that the traffic passes through it. LDP protocol uses a mechanism for the procedures and messages among the LSRs because whenever traffic pass through the LSR towards the other LSR then one LSR tells to the other LSR that what amendments it made and what you have to do in order to establish a binding of the labels among the switched path [22].

<table>
<thead>
<tr>
<th>2 bytes</th>
<th>2 bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>PDU Length</td>
</tr>
<tr>
<td>LDP Identifier(6 bytes)</td>
<td></td>
</tr>
<tr>
<td>LDP Messages</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 5.1 LDP Packet Format**

The above figure shows the packet format of Label Distribution Protocol (LDP). There is short description of the packet format which is given below:

**5.4.1 Version**

It is the version number of the LDP means which version is used now days because sometime due to the limitation of the packet headers there is an enhanced version will be used in order to cover the drawbacks that’s why version field is there in order to define the version number. Now a day’s version number 1 is used for the LDP.
5.4.2 PDU Length

It defines the total length of the LDP packet except the version field and the PDU length field. PDU stands for Packet Distribution Unit. The function of the PDU Length field is simple that it defines total size of the LDP packet because when traffic labeling mechanism is used then its size differentiates according to the given traffic.

5.4.3 LDP identifier

The LDP identifier is used for the identification of the packet under the circumstances of the LSRs. There are 6 bytes which are used for the LDP Identifier field the first four bytes are used for the encoding of the IP address of the LSR and the last two bytes are used to define the space for the labeling of the LSR. The main function of the LDP Identifier is that it is the identification of the packet when the packets are passing through the LSRs.

5.4.4 LDP Messages

LDP Messages define the messages and there is also a format for the LDP messages that which type of message it is that’s why there is another message format is used for the LDP Messages which is given below:

LDP Message Format

<table>
<thead>
<tr>
<th>U</th>
<th>Message type</th>
<th>Message Iength</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Message ID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Parameters</td>
<td></td>
</tr>
</tbody>
</table>

Figure 5.2 LDP Message Format

The above figure shows the LDP Message format of Label Distribution Protocol (LDP). There is short description of the LDP Message format which is given below:

- **U**

  The U bit is used for the unknown message sometime the messages are unknown then the U field is used to describe these kinds of messages.

- **Message type**

  There are different types of messages are used in the traffic that’s why in order to describe which message is this we use a field that is Message type which
simply tells about the message type. There are following message types are used in the message type field which are given below:

- Notification
- Hello
- Initialization
- Keep Alive
- Address
- Address Withdraw
- Label Request
- Label Withdraw
- Label Release
- Unknown Message name

These all message types have some specific function in order to identify the function of the message.

- **Message length**

  The message length field is used in order to describe the total length of the message. The size of the message length field is in bytes and there are some optional and mandatory fields which we have to use in the message length.

- **Message ID**

  The message id is used in order to describe the ID of the message. The size of the message length is 32 bit and these four bytes are used in order to describe the Message ID.

- **Parameters**

  As we know that some message have optional parameters and some message have mandatory parameters that’s why in order to handle such kind of scenario we have a parameter field. This parameter field contains TLVs. This parameter field contains both mandatory and optional parameters regarding the messages. There is also a TLV format which has some field parameters which are given below.

**TLV Packet Format**

<table>
<thead>
<tr>
<th>U</th>
<th>F</th>
<th>Type</th>
<th>Length</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Value</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>TLV format</td>
<td></td>
</tr>
</tbody>
</table>

*Figure 5.3 LDP Message Format*
The above figure shows the TLV Packet format of Label Distribution Protocol (LDP). There is short description of the TLV Packet format which is given below:

- **U**
  
  The U bit is used for the unknown message sometime the messages are unknown then the U field is used to describe these kinds of messages.

- **F**
  
  It is used in order to forward the unknown bit of the message that is only function it will do.

- **Type**
  
  It is used in order to handle the value field and it also specify the message type specifically.

- **Length**
  
  The size of the length field is in bytes and it is used in order to specify the size of the type field.

- **Value**
  
  The size of the value field is in bytes and the main function of the value field is to encodes the type field and then accordingly to perform an operation.

### 5.5 LDP Message Exchange Mechanism

There are four different types of messages which are used in order to exchange the information [23]. These four types of messages which are given below:

1. Discovery Messages.
2. Session Messages.
3. Advertisement Messages.

#### 5.5.1 Discovery Messages

The main task of the discovery message is that it made the presence of a LSR in the network and also discovers the LSRs. There may be more than one LSR in the network.

#### 5.5.2 Session Messages

There are three main tasks session message will perform and it is given below:

- It establishes session between the LDP peers.
- It maintains session between the LDP.
- It terminate the sessions between the peers.

#### 5.5.3 Advertisement Messages

There are three main tasks which advertisement message will perform.
5.5.4 Notification Messages

There are two main tasks which notification message will perform that is given below:

- It will provide the advisory information.
- It will provide the signal error information.

5.6 Resource Reservation Protocol

Due to increase number of application development and a need for times specific data transmission in the network to guarantee QoS RSVP has defined in [23] to meet the QoS requirements and offer reliable transmission of voice and video data. RSVP requires providing specific level of service guarantee in the network when voice and video application are running on end nodes i.e. clients or servers. It is mandatory that every router in the transmission path must implement and support RSVP because it’s difficult define same vendor products installed on the network having same set of protocol running on routers i.e. RSVP work effectively otherwise delay, getter and through put performance parameters cause lowing and down the transmission rate for real time application and ultimately decrease QoS services. Unlike OSPF and RIP which offers forwarding mechanism for datagram without QoS, RSVP forward datagram’s along with QoS by reserving resources along the data transmission path in
advance with the help of receiver information. RSVP support unicast as well as multicast application, the messages are in capsulated in UDP and are sending through IP datagram. It has two import ants’ types of messages define under:

- RESV message is sent to the source by the destination.
- Path messages is sent by the source to destination and contains desired path obtained through routing protocols, the message also contain information about the path at every hop in transmission network.

PRVP message has three headers i.e. 64 bits common header, 32 bits object header and object constant header have variable size. 4 bits version field consist of desired version of the protocol, 4 bits are flags reserve for future needs, 8 bits are for message type describe as;

- Message type 1 is called as “Path” that identifies the path between source and destination
- Message type 2 is called as “Resv” that identifies the reservation request along the path included routers and the destination.
- Message type 3 is called as “Path-Err” that identifies path errors and receiver reply obtains through path message.
- Message type 4 is called as “ResvErr” that identifies errors in Resv message processing and are sent to the receiver to down
- Message type 5 is called as “Path Tear” that identifies infects problems initiated through sender or time out towards the all receiver.
- Message type 6 is called as “Resv Tear” that identifies problems specified by receiver or the timeout is occurred and define up streaming senders.
- Message type 7 is called as “Resv Conf” that identifies the acknowledgment of Resv message such that resource reservation has been confirmed.

In Figure 5.5 RSVP operation is describe between numbers of hops.
There are six routers in the core network and two adjusting routers connecting sender and receiver on either side. If IPTV application is running on the server and receiver request for the information service, RSVP will send number of message packets to obtain the resource reservation before starting the transmission. If there resources are at hop are not available hop 3 will receive reserve error message initiate the problems in the resource reservation by hop 3 towards hop 2, hop 1, and IPTV server which is sender of the application service.

RSVP message contain 16 bits forever control with RSVP checksum, 8 bits for TTL operation, 16 bits for RSVP message length. There exist an additional 32 bits object header which includes 16 bits for length field identifier the object length, 8 bits class number identifier class of an object and 9 bits type field to include type of IP class address, normally C class. Finally “object constant” field contains complete message of variable length.

5.7 TCP (Transmission Control Protocol):

TCP provides us with reliable, connection oriented transport where as TCP used transport layer protocol which enables the users to run multiple software applications using single IP address. First of all it establishes a virtual connection then it can pass data bidirectional, for transmission sliding window method is adapted so that when it detects unacknowledged transmission it automatically retransmits it where as additional functionality allows the data flow between devices to be managed and in some cases to be addressed [6].

5.8 UDP (User Datagram Protocol):

It’s a simple protocol that provides transport layer addressing like TCP .The major role of a UDP is to act as a wrapper and provide a way to the protocol of accessing the internet but we must always remember that the transmission will be unreliable and data can be lost in case of UDP [6].

In analogy terms you can say that TCP is a whole tracking or navigation system it provides the user with lot of comfort and ease it virtual guarantees that your data will be successfully sent and received and in any problem the data can be retransmitted again, where as in contrast to TCP UDP priority is speed only whether u get the data or not.

Let us now consider some applications of TCP and UDP protocols. First are TCP applications in it more applications require reliability and other services provided by TCP it does not matter if s there is small amount of loss in the performance to the overhead for example most of the machines which transfer files between different machines requires TCP because loss of any part of the information will result in the total loss hence no use. Some of examples are WWW (World Wide Web), FTP (File Transport Protocol).

Now it UDP offers only speed and no reliable data transfer so why do we need it then in reality the use of UDP is more the TCP and there are two reasons first the application does not care about data loss like streaming and multimedia videos where as single loss of byte of data won’t even matter and the other reason is that when application itself
chooses UDP in case to fill the lack of functionality in UDP like application which send very small amount of data for example

Often used under circumstances if the request is sent and reply is no received the client will later on sent the request again this in respect will provide some reliability without the overhead of the TCP connection.
Chapter 6

QoS in IP/MPLS Networks
Quality of service (QoS) is the capability of providing improved services to a specific network traffic using different technologies like ATM, SONET, and MPLS etc. The main purpose of QoS is to prioritize a specific traffic over another i.e. to take into consideration Jitter, Latency, Packet Loss, and Burst of Jitter and Loss and minimize all these factors for that flow specifically. It should also be considered that prioritizing one traffic flow must not make another fail.

QoS of any service is acceptable when it fulfil SLA and leads to proper customer satisfaction. To guarantee the full throughput, specific level of assurance is required over the traffic load to reduce losses, jitters and delays. QoS consideration reflects in Class of Service (COS) refers to traffic classification and Type of Service (TOS) is octet service used in IPv4 packet header. QOS has several factors which involves like shaping, policing, scheduling, and classification when it comes to the condition of network. There are three basic parts in implementing QoS are

1. Identification and marking techniques for end to end networks elements
2. QoS within a single network element
3. Management, accounting and policing functions to control end to end traffic across a network.[26]

There are basically four internet services models

1. Best-effort Service Model
2. Integrated Service Model
3. Differentiated Service Model
4. Hybrid Model
6.1 Best-effort Service Model

Best effort service model give no guarantee while delivering the traffic, i.e. it is never known to the sender that either data is delivered or not. Best Effort service model provide performance oriented service of the network also nodes used are comparatively cheaper than others. As the resources are not allocated so traffic must have to go over the network under traffic load without having the information regarding the packet status whether it’s lost, corrupted or delivered. It can be concluded by the various analysis of performance evaluation that best effort service is not best suited for the application which needs specific level of quality of service.

6.2 Integrated Services Model

The integrated service model is used together with resource reservation protocol (RSVP) at every hop to allow per flow based service state based QoS guarantees [28]. The problem with this model is that it suffers from scalability issues. This model is very complex and if it used for services like providing telephony to subscribers it might result in having wrong billing information.

![Integrated services model](image)

The three main components of integrated service model are

6.2.1 Classes of Service

It is divided into three classes

a. **Guaranteed**

It provides the details about the maximum jitter and delay that can occur and also a specific level of bandwidth that is allocated for a certain flow. Guaranteed class is mostly used for those applications that need real time data flow.
b. **Controlled Load**  
It doesn’t provide any guarantees of service but provides a constant level to the traffic flow.

c. **Best Effort**  
As it’s clear from the name that it doesn’t provide any assurance about the flow, just does its best for the traffic to reach the specified node. It is mostly used for text based applications.

### 6.2.2 Control Mechanisms

The traffic is divided into flows based on traffic classes. All the flows are merged together within the same class [27].

If there are more than one type of flows in the same router than that number of output queues are used for each line, one for every class.

a. **Token bucket filter**  
It enforces queues and bandwidth in such a way that the maximum limit specified for delay, jitter and bandwidth are met.

b. **Random Early Detection**  
It helps in reducing the dropping of packets when the routers’ buffers are full.

c. **Weighted Fair Queuing**  
A queuing management schemes schedules the order in which the queued packets are transmitted.

d. **Resource Reservation Protocol**  
For each traffic flow it reserves the resources like bandwidth and buffer.

### 6.3 Differentiated Services Model

Differentiated Services Model manages the resources of each cloud. In it the packets are coloured so that the forwarding behaviour is indicated. Differentiated Service Model doesn’t focus on individual flow but on the aggregate flow. It provides QoS guarantees [31] for aggregated flow only. It can be used together with Multiprotocol Label Switching (MPLS) and Traffic Engineering (TE). The problem with differentiated services is that it’s very poor for end to end QoS guarantees.

In differentiated services the traffic is treated on per class basis not on per flow basis and in each service class the individual flows are aggregated together. In differentiated services network the DS field replaces the TOS field in the header.
There are varieties of reasons which are in favour of QoS one such application is of voice because as we know that IP connectivity is not reliable when we discuss in terms of delivery of data as it has some delay which make it’s not a good medium for the applications [28].

As we know for voice we must have QoS with a dedicated circuit so that there are no drop outs or delay. So the question arises to why use QoS it may have many reasons but let us consider one reason right now to explain it for example the technological reason, some of the points included can be explained. In real time applications it’s very difficult to tackle problems like jitter, delay and packet loss QoS proves useful to us in such situation. QoS can be useful in varying different service requirements such as voice, video and data their demand can be change with respect of QoS. Now days a major problem is of bandwidth QoS comes in that time it helps us in over subscription of available bandwidth for multiple applications. QoS also helps in the overall congestion and SLAs (service level agreements) in case of priority traffic in networks. It also helps us also in not only oversubscription of bandwidth but also in optimization of available bandwidth.

These were some points including the importance of QoS in technological field now let us discuss some other issues. We always know that during management of network we always seek it to be suitable and able to manage load then the certain thought in our mind come why QoS is needed. The answer is very simple QoS is always better option when you have sustainable and manageable network because the behaviour will be better and quality of service will be also an observable point.

Still there are also some reason to apply QoS either our network is a well behave network which can be explained. However a good network engineer but we know the fact that needs and load grows with the passage of time so he might be unable to cope with the situation. In this situation we have to put in front of us the original and the new requirements by doing this we will see the violation of initial bandwidth consumption between the original and new network. As we know that now a day’s spam emails and email viruses which are growing very fast now a day’s wasting the useful bandwidth these mails are counted as part of the bandwidth so we have to manage the additional bandwidth for this we need to check these flows also so QoS comes there. For internet
service providers by applying QoS different qualities of services can be provided at different rates hence increasing the earnings one thing must be remember that these services depend on the QoS provided to each group. At the same time service priority must also be kept in mind different users can be priority can be activated and deactivate according to the situation. We must always remember that without any QoS policies each packet is given equal amount access to the resources if we can not differentiate between voice and data packet we cannot give voice priority.

Now if any company wants to utilize its resources to the peak it must be able to recognize the critical network traffic so that it would be able to allocate appropriate resources to that traffic streams and this is for sure if voice is present in the network then it will be given more priority over all data stream otherwise we will get bad voice quality and hence will get complaints. For example if a voice and FTP(File Transport Protocol) Packet arrive at same time at router then without QoS the voice packet will have to wait until the FTP packet processing hasn’t completed.

6.4 Benefits of QoS

Now we will discuss some benefit of using QoS in network and its benefits to the providers which are as follows. Major benefit of QoS in network is in form of network capacity with new applications and services. Another benefit of QoS is the management area where it helps us in congestion and avoidance mechanism. It helps us in the increase in revenue where shared structures like MLPS are acting as major backbone. It helps in controlling of multimedia with impact on the network. QoS can be use for true convergence such as IP telephony.

6.5 QoS in IP Networks

Internet years tend IP to utilize TCP for delivery of data traffic in shortest time but with an increase in application development the mode of data and traffic increases, however TCP/IP was not merely capable of heavy traffic close and thus bandwidth variations/
limitations, latency and jitter and possible data losses were experienced problem required solutions for guaranteed data traffic flows. Application like voice and video were not supported by traditional best effort service model and IETF described QoS for IP in integrated service model and differentiated service model architecture.

6.5.1 Integrated Service Model for IP

To support QoS in IP, IETF described specification for the integrated service support to IntServ working group to work closely with working groups IntServ over specification link layer (ISSLL) and RSVP. ISSLL described IntServ implementation over Ethernet, ATM and many other “link layer” protocols. RSVP signalling was described for IntServ group as a signalling protocol for IP QoS.

IETS selection ofr the support of real time applications were non-feasible solution since they suggested to develop a “fair queuing algorithm” which will data and real time applications, however jitter and delay are still unsolved. Another idea was to use separate network for each set of separate application services or to increase the bandwidth and provide extra bandwidth but it’s actually also unreal and impossible as bandwidth is also a service entity and hold some cost. If priority application mechanism is design it will also fails because how we can prevent and increase in new developments and traffic flows which will ultimately results in degradation process of all the traffic flows. Also every real time application has different delay and rate limits when there is no admission control criterion.

To cater with these challenges, IntServ architecture for IP is defined with “Flow”, “traffic specifications”, “service request specifications”, and “flow specifications” parameters. Flow consists of single or multiple identified data packet streams associated with a node attached in a network with same QoS request. Traffic specification is a flow of traffic patterns over time. Service request specification is the desire for QoS characterization while flow specifications combine request specification and traffic specification.

Admission control manages finite number of resources through RSVP implementations. All the nodes connected to IntServ will reject and avoid any requests which can cause degradation in existing resource reservations. Every network user has rights to reserve resources based on resource rights. IntServ facilitate individual applications to select QoS resources and request while network load is controlled through qualitative methods to describe service qualities.

Flow is a basic unit for any application service characterized in packet streams with same QoS requirements in a unidirectional way. One to one or one to many destinations are specified since only one source is capable of reserving specialized QoS for an application traffic and forward data stream in a single or multiple flows. IntServ constitute of per flow state due to flow granularity in concatenation with RSVP and admission control.
In an IntServ model a common framework is maintained when receiver request the service/resource form the network by providing TSpec and RSpec. Upon acceptance of the resources/service requests, a network node (source) guarantees service according to TSpec flow description. TSpec utilizes four parameters i.e. token bucket rate and size, peak rate, minimum policed unit, and maximum packet size. IntServ contain Guarantee Service (GS) and Controlled Load Service (CLS) for QoS in IP as they are also included in Best Effort model without any changes. GS provide and describe flow for delay and guarantee bandwidth allocation [46] while CLS provides network transparency reliance in packet delivery even at congestion state to ensure that the applications that network maximize data delivery percentage towards final destination along with application assumptions to obtain a minimum delay for packets [47].

6.5.2 DiffServ Service Model for IP

In [48-49], DiffServ has incorporated number of architectural entities. DiffServ provides a domain, consisting of same DiffServ network implementation; a Region, consists of many domain; an Egress/ Interior and Ingress node; a DiffServ field; a DiffServ code point (DSCP); a Behaviour Aggregate (BH); Order Aggregate; BA classifier; a multi field classifier; Per Hope Behaviour (PHB) and Per Hope Behaviour Group; PHB scheduling class; Traffic Profiles; marking; metering; policing; shaping; SLA, and traffic conditioning specification and traffic conditioning.

Architecture is based on CO traffic along with non identical service requirements. Traffic headers consist of special marks to identify traffic classes to provide resources through service policies. Service is unidirectional without any QoS flow states, when mode is switching over time, fewer packets are marked in terms of numbers in micro flows which are inheritance of small classes caused through grouping an aggregate traffic while DiffServ provide scalability and granularity tradeoffs [48].
Differentiated service code point parameter is included in the latest version of the IPv4 and IPv6 which set the six most significant bits in the TOS of IPv4 header and traffic class in IPv6 header (octet) to serve each packet based on the DSCP while many packet groups consists of same DSCP. PHB define values and definition of services consists of DiffServ, code point pool and class sector code points fields in TOS for delay, reliability and throughput.

<table>
<thead>
<tr>
<th>0</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>DiffServ Field</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Code point pool</th>
<th>DiffServ Code point</th>
</tr>
</thead>
<tbody>
<tr>
<td>XXXXX0</td>
<td>Standard</td>
</tr>
<tr>
<td>XXXX11</td>
<td>Local use or</td>
</tr>
<tr>
<td></td>
<td>experimental</td>
</tr>
<tr>
<td>XXXX01</td>
<td>Future use</td>
</tr>
</tbody>
</table>

- 011000 Class sector 7
- 110000 Class sector 6
- 101000 Class sector 5
- 100000 Class sector 4
- 011000 Class sector 3
- 010000 Class sector 2
- 001000 Class sector 1
- 000000 Class sector 0

**Figure 6.6: DiffServ field, Code point and Class sector code point**

In the DiffServ, nodes are electric devices i.e. routers performing as an ingress boundary node, interior node and egress boundary node roles forming a domain having/sharing an identical DiffServ implementation where as nodes with in a domain perform same policing and service definition. A administrative unit controls a domain describe in nearby/neighbouring domains forming DiffServ region for providing DiffServ policy and traffic classification. In case of individual domain implementation, non identical policies, service level definitions and marking packets based on certain criteria, a peering mechanism is used to manage traffic during traversing different domains.

Nodes at boundary level i.e. egress and ingress provides an interface with outside of other domains to insure traffic marking and classification with an aggregates traffic flow amount. Interior nodes and boundary nodes both classify trafficking policy conditioning by implementing service policing at local nodes with a domain(s) through distribution of difference service level for every BA or PHB. Traffic conditioning and classification makes traffic identification during differentiated service by ensuring service level contracts, an aggregate terms defined by an architecture with SLA, by implementing ALA through boundary nodes by means of packet metering, marking, shipping, classification and policing according to service contracts.

62
Either BA or MF classifier is implemented by boundary nodes at an incoming packet width DSCP and packet header/information. BA support and implement DSCP while MF support implements packet header/information classification in traffic conditions either one or more operations are performed i.e. policing marking, metering or shaping since traffic classification input depends on classes. However SLA limit the boundary node value which result in node decision about dropping, buffering or marking traffic. These traffic classifications are performed at different instances at boundary nodes. Single or multiple PHB apply forwarding behaviour to BA for qualitative explanation of jitter, loss or latency during DiffServ node traversal. PHB mapping is performed through its DSCP with flexibility of arbitrary mapping configurations.

6.5.2 QoS in MPLS Networks

We know that service providers are attracting attention of no of MPLS based services but alone MPLS cannot just give us end to end quality of service. The complete QoS [29] has four parts which are traffic classification, traffic prioritization, bandwidth management and traffic monitoring. Any implementation that exceeds these four parameters cannot be considered to providing optimal performance. So we can deduce that all vendors cannot provide these parts so multiple vendors are needed to provide for solving this solution.

So we start first with traffic classification we need to classify application traffic so that it can be treated different relating on how important is it. Traffic is identified by marking the application end points or at intermediate device such as routers at same time marking some priority thus by identifying this priority the packet should receive as it traverses the network.

End points like video conferencing bridges can successfully mark the traffic but some time network managers try to avoid endpoint classification is cases where the user may be able to change the personal priority for e.g. for online e-gaming. Similarly routers can also identify traffic on known servers but old routers cannot difference between traffic on higher level of protocols they are unable to differentiate between multiple http applications but new routers have solved this problem.

Now when traffic is classified we must ensure that high priority traffic receive more importance then low priority traffic. Managing traffic priority is very important MPLS also provides different priority levels these levels are known as gold, silver and bronze each have different SLA (Service level agreement) having different goals for latency, packet loss and jitter. Here we must know that three classes can easily support the performance of real time traffic and less data traffic, among this voice has the highest priority the video and at last data, similarly QoS appliances can also help appliances like from Expand.

Another factor is of the bandwidth management because of this an application can perform well or better accordingly to the bandwidth allocated to it. The bandwidth management has two important factors one is network aspect and the other is application aspect, now in network aspect such bandwidth must be offered that lower priority that they can pass even in case of higher priority when it’s using its maximum bandwidth the traffic in other classes can also pass. Now in terms of application aspect
we always must be careful of application performance in limited bandwidth we must not only keep the specific application bandwidth in mind but also must manage applications so we can provide them with bandwidth constraints [30].

Bandwidth can always be managed at the application source and the router. At the source the number of users can be limited by denying calls which exceed the allocated bandwidth by using VOIP call managers and gate keepers. Similarly license mananger can also be used to control the bandwidth issue also bandwidth can be managed by switch routers by enabling them to set COS queue to forward traffic only up to maximum data rate. Then again we can QoS applications can solve these problems by differentiating within MPLS service classes, traffic within a class or a subclass can be shaped with predefined bandwidth limit to enforce this the appliance must already allocate bandwidth to others site or try to negotiate with the appliances at each site for additional bandwidth per class or subclass. Here we must always keep this in mind that traffic shaping can always help us to squeeze traffic in the available bandwidth, this proves to be useful where the bandwidth is limited. we must always keep in mind that QoS will work efficient in the available bandwidth if the application limit exceed the available bandwidth then it would cause the applications to suffer. Now a day as we know that IP networks are continuously changing due to upgradation which leads us to this conclusion that we should always be able to control the traffic at the same time MPLS meshes also enables any-to-any traffic that makes some traffic invisible in such way that it’s unable to centralize some monitoring networking devices. It’s important to monitor the traffic or it will affect the optimization of our network and this thing also is applicable to MPLS networks.

In general frame relay networks like Permanent virtual circuit (PVC) act as dedicated lines so its ease the job for us where as MPLS mesh architecture offer us more flexibility but the trade off is that it make the traffic control more complex and it also requires some extra tools.

We must be aware of the fact that Some of MPLS service include access to the portal that show bandwidth but this information is so limited that it is unknown to service classes that the providers offers. We can grasp some of the concept by reading the following table.

<table>
<thead>
<tr>
<th>Traffic Classification</th>
<th>Traffic Prioritization</th>
<th>Bandwidth management</th>
<th>Traffic Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router</td>
<td>Limited to 3 layers</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>MPLS service provider</td>
<td>No</td>
<td>Yes only 3 to 5 classes</td>
<td>No</td>
</tr>
<tr>
<td>Monitoring appliances</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>QoS Traffic and shaping appliances</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes through traffic shaping</td>
</tr>
</tbody>
</table>
Each of the functions in Table (QOS over MPLS Solutions) is required to insure a complete the QoS solution across the network. Routers and MPLS service providers each offer part of the solution, but its incomplete instead, each needs to be filled with additional monitoring which make the requirements fulfilled.

Now in order to explain different techniques of implementing QoS in MPLS we must know about few terms first we must know about two different mapping methods one is L-LSP (Label-only-inferred-PSC LSP) PSC is defined per LSP in such a way that the queue behaviour is specified by a certain value for flexible DiffServ parameter can be applied per LSP .similarly E-LSP(EXP-inferred-PSC LSP) in this case queue behaviour is defined by MPLS exp bit, in MPLS QoS are supported up to eight domains.

Now the techniques of QoS for MPLS are E-LSP (use the EXP bits)this is used by Cisco for frame based MPLS and also reuses the IP code where as L-LSP(Cos implicit in the label)here one Cisco approach for cell based MPLS and it supports up to four labels of each destination one each for a Cos.

Now in case of Cell-mode MPLS QoS the MPLS over QoS options includes Legacy ATM in which PVC (Permanent virtual circuit) act as a serial link which uses the frame base system such as single PVC mode.

Similarly ATM SLR has two options one single LSP and other Multi VC mode in which along with LSR it will create four LSP per destination. Lower order will contain two bits of EXP bits which will determine CoS where as higher order will determine ATM CLP bit. In an IntServ, MBLS support is not described since RSVP label distribution for MPLS is not supported, and capability or out of the reach of IntServ requirement contributing efforts to MPLS network for IntServ reservation. However, MPLS provides full support for DiffServ through small changes in architecture.

DiffServ PHB and traffic conditioning describe our remain unchanged for MPLS DiffServ and implemented through LSR, since it performs queuing, marking, policy, metering and shipping etc [50]. MPLS DiffServ is capable of caring not only IP traffic but also ATM and frame relay traffic types for the support of Qos with scalability of the network and services. MPLS DiffServ uses PHBs to handle QoS requirements for traffic types with possible extension in network design through increasing LSPs to offer/transport variety of data spectrum. E-LSP (EXP INFARED class LSP) only capable of single transporting and each of them use different encoding mechanisms for marking DiffServ as well as Shim Header [51] implement level stacking for encoding. Shim Header have EXP (3 bits) field to carry 8 service classes for all LSRs, however, E-LSP small number of classes are carried out along with multiple ranking example AF1 with two or more rankings but the EXP values are not specified for current DiffServ PHB i.e. AF, EF, CSN and also not the structure of 3 bits. E-LSPs are defined for admission control by LSRs.

In figure 6.7, there exist two E-LSPs i.e. one only carry EF traffic while second carry AF1 and AF2 traffic. However, E-LSP can carry all the three traffic points. Node C serves EF and AF1& AF2 regardless of any E-LSP but node A can or can’t split the whole traffic through micro flows. MPLS DiffServ support for defining E-LSP by mapping values in EXP & PHB through LSR associated at input levels to perform EXP
to PHB in regard to output labels while signalling mechanism is performed at initial LSP setup and is optional. LDP protocol extension for DiffServ TLV requires parameters i.e. type, length, value, label mapping, label release and notification to ensure signalling as an E-LSP and establish EXP to PHB mapping criteria. RSV also defines DiffServ object for messaging paths. Frame relay LSRs, ATM LSRs, LCATM LSRs and GMPLS LSRs does not offer support for EXP to PHB mapping i.e. E-LSP as they don’t support shim header NMPLS for forwarding packets.

MPLS DiffServ support for defining L-LSPs to transport singal traffic loss by LSR, it is determine through label that which class is associated with the packet and evaluate PHB and EXP combination fields. PHB are map with each class by table below. For signalling L-LSPs use different format which specify is as L-LSPS with identification of transporting classes to reserve bandwidth.

<table>
<thead>
<tr>
<th>Class</th>
<th>EXP (Decimal)</th>
<th>EXP (Binary)</th>
<th>PHB</th>
</tr>
</thead>
<tbody>
<tr>
<td>EF</td>
<td>0</td>
<td>000</td>
<td>EF</td>
</tr>
<tr>
<td>AF4</td>
<td>3</td>
<td>011</td>
<td>AF43</td>
</tr>
<tr>
<td>AF4</td>
<td>2</td>
<td>010</td>
<td>AF42</td>
</tr>
<tr>
<td>AF4</td>
<td>1</td>
<td>001</td>
<td>AF41</td>
</tr>
<tr>
<td>AF3</td>
<td>3</td>
<td>011</td>
<td>AF33</td>
</tr>
<tr>
<td>Class</td>
<td>EXP (Decimal)</td>
<td>EXP (Binary)</td>
<td>PHB</td>
</tr>
<tr>
<td>-------</td>
<td>---------------</td>
<td>--------------</td>
<td>-----</td>
</tr>
<tr>
<td>AF3</td>
<td>1</td>
<td>010</td>
<td>AF32</td>
</tr>
<tr>
<td>AF3</td>
<td>3</td>
<td>001</td>
<td>AF31</td>
</tr>
<tr>
<td>AF2</td>
<td>2</td>
<td>011</td>
<td>AF23</td>
</tr>
<tr>
<td>AF2</td>
<td>1</td>
<td>010</td>
<td>AF22</td>
</tr>
<tr>
<td>AF2</td>
<td>3</td>
<td>001</td>
<td>AF21</td>
</tr>
<tr>
<td>AF1</td>
<td>2</td>
<td>011</td>
<td>AF13</td>
</tr>
<tr>
<td>AF1</td>
<td>1</td>
<td>010</td>
<td>AF12</td>
</tr>
<tr>
<td>AF1</td>
<td>1</td>
<td>001</td>
<td>AF11</td>
</tr>
<tr>
<td>CS7</td>
<td>0</td>
<td>000</td>
<td>CS7</td>
</tr>
<tr>
<td>CS6</td>
<td>0</td>
<td>000</td>
<td>CS6</td>
</tr>
<tr>
<td>CS5</td>
<td>0</td>
<td>000</td>
<td>CS5</td>
</tr>
<tr>
<td>CS4</td>
<td>0</td>
<td>000</td>
<td>CS4</td>
</tr>
<tr>
<td>CS3</td>
<td>0</td>
<td>000</td>
<td>CS3</td>
</tr>
<tr>
<td>CS2</td>
<td>0</td>
<td>000</td>
<td>CS2</td>
</tr>
<tr>
<td>CS1</td>
<td>0</td>
<td>000</td>
<td>CS1</td>
</tr>
<tr>
<td>Default</td>
<td>0</td>
<td>000</td>
<td>Default</td>
</tr>
</tbody>
</table>

In figure 6.8 three different L-LSPs are supported each for EF, AF1 and AF2 traffics. MPLS network DiffServ support for E-LSPs and L-LSPs can also be supported by integrating these LSPs architectures. Simply two L-LSPs traffic flow between E to D and to E-LSPs traffic flows between A to D and can support three types of classes by network i.e. EF, AF1 and AF2 where C node in the network can transports all type of the network and both LSP types.
There are three interactions tunnelling modelling for marking between DiffServ and layer encapsulation support by MPLS LSPs.

1. Pipe Model
2. Short Pipe Model
3. Uniform Model

Viewing MPLS applications we get four concepts for MPLS development and implementation. The concepts benefit MPLS through traffic engineering, defining CoS and QoS, network scalability and IPVPN support.

Traffic engineering benefit QoS through efficiently controlled, rapid redistribution according to network topology change in resource utilization. In an IP network ATM performs TE while ATM has different networks with IP router doesn't know for possible decisions and results in two planes causing scalability limitations. MPLS and IP offer single control plane for physical topology and much simplicity. MPLambdaS is an emerging MPLS-TE to facilitate optical networks similar to GMPLS. IN CoS and QoS explicit part is described based on FEC to guarantee bandwidth, delay and burst size along with QoS DiffServ model support for EF and AF1 – AF12.

Innovative benefit of MPLS is unified network to support all service classes including real time applications i.e. voice and video as well IP and ATM platform. MPLS multiple domain not only has scalability issues but also reduce table sizing at transit router area of border routers. The future of QoS is MPLS definitely lead the exciting new generation networks since internet is the a cluster of meshed networks including enterprise and business networks to rule the application provisioning capabilites and end user demands. Business give more revenue to develop fast , efficient, robust required network and services to the integration of many technology solutions and tune them to offer best quality results.
Chapter 7

MPLS Traffic Engineering and VPN
7.1 MPLS Traffic Engineering

MPLS traffic engineering is the most popular implementation in the ISPs. Due to increase of the traffic load and we know also that there is so many different kinds of traffic on the Internet and due to this way there is a great load on the link of the required network due to this way packets loss problem comes and delays in the communication comes and also so many problems due to the traffic load. In order to resolve all these problems we use a mechanism that is called Traffic Engineering [32-33].

7.2 Traffic Engineering Basics

The most basic function of the traffic engineering is that in order to steering traffic in order to use the effective way bandwidth so that there will be no packet loss among the transmission of data.

If we discuss Traffic Engineering with respect to the IP then we know that in a network we will declare static paths among the source and destination network so that we can solve congestion on the network links and save our bandwidth and use it in an effective way.

Let’s suppose if all the links has the same cost and we want that we want to transfer that data from the R1 to the R5 then what we have to do there are two solutions one is from the R1, R2 and R5 and the other one is that from the R1, R3, R4 and R5. We know that the cost among the links between each other is the same so if the R1 want to communicate with the R5 then there are two ways one is expensive and the other one is not expensive in case of cost so that’s why we will set a static route in the network in order to use the effective bandwidth of the links.
7.3 MPLS Traffic Engineering Overview

In case of MPLS Traffic Engineering mechanism there is a comparatively different mechanism with respect to the IP traffic engineering. In IP traffic engineering when static routing defined among the two different networks or the same network then at each HOP means at each router when packet passes through then it will check the packet and then forward it to the next hop and same operation perform at the next hop and suppose if there are more than hundred routers or hops between the network then same function is performed by the router or hop which time consuming and creating delay among the traffic [34].

In case of MPLS Traffic Engineering mechanism there is another way to control the traffic and in order to reduce the time and also save the processing of the hop or the router. Suppose if traffic passing from point A to the point B with large number of routers, so what mechanism is used if we implement MPLS Traffic Engineering technique. When first packet comes under the circumstances of the first hop then it checks and forward to the other hop and on the next hop it doesn’t check because MPLS label tells that it is same traffic which is coming from the same source so due to this way there is time saving and also use the best effort among the traffic handling.

7.4 RSVP with Traffic Engineering Extensions

Resource Reservation Protocol (RSVP) by its name we knows that it reserve the resource for the network. The main task of the RSVP is that it reserves the bandwidth between the source and destination along the defined path. In order to get the information in the network there is a router in the network which will send the message packets in the network in order to get the details regarding the bandwidth. There are four main messages which are used by the RSVP protocol and these are given below:

1. RSVP PATH message
2. RSVP RESERVATION message
3. RSVP error message
4. RSVP tear message

7.4.1 RSVP PATH message

In this message the headened router is responsible for the reserve path. The main function of the headened router is that it sends the messages to the other routers and find out the path information and send it to the headened router. After that headened router will decide that which path is free from source to the destination?
7.4.2 RSVP RESERVATION message

After the analysis of the Headened router it will apply the resource reservation on the required path and then use it in an effective manner. In the above figure when headened router send message to the inside router then it will send it to the next router and when it found that the resource is free then it will generate the reservation message and finally it will come back to the headened router.

7.4.3 RSVP error message

In this mechanism when headened router send path message to the inside router there are basically two conditions first one is the suppose the inside router don’t have any resources then it will send back the message that I don’t have any resource right now with the identification of the PATHERR message. At the start there is no handling of the resource. On the other hand if there is a resource is available then it will send message to the other side most probably the destination and suppose at destination side there is no resource are available then it send an error message then it will wait for some time according to the limitation when it gets any resource then it will be successful otherwise it generate an error.
7.4.4 RSVP tear message
In case of RSVP tear message it will generate two types of tear messages one is for the clear of the resources and the other one is for the clear of the path. When headened router reserves any resources then it will send back message that is called tear message.

7.5 Multiple Protocol Label Switching Virtual Private Network
MPLS Virtual Private Network is the most popular and widespread implementation of the MPLS technology. It is the most popular and used network topology now a days and growing very well. It denies the previous implementations and gives a new solution in the WAN technology. Before that world is familiar with the frame relay and ATM services and in frame relay it works with the X.25 protocol which is very old protocol but reliable [35].

Now a day’s its almost not in use mostly frame relay works with the DXX technology and we know that ATM is new technology services but with the invention of the MPLS these all are not in use most part of the world. MPLS VPN is the best network solution for the WAN connection among the circumstances.

MPLS VPN provides the scalability especially in large networks it works outstandingly because it divide the networks into sub parts and make it simple to deal with and also provide security in the way of VPN technology. There are also different models used in the VPN technology due to this way it will enhanced the features of the MPLS. The models of VPN are given below:

- Peer-to-Peer VPN Model
- Overlay VPN Model
- Optimal Traffic Flow Model

7.6 Definition of VPN
VPN creates a private network over the normal circumstances or we can say an infrastructure. Most probably each company has one VPN network and if there is a
large company then there will be more than one VPN network in the network and these
VPNs mostly connected to each other or through the ISPs. There are some
requirements’ for the establishment of the VPN networks that VPN require the Internet
connectivity. In case of the MPLS VPN case it provide internet by default. In MPLS
VPN network and there backbone network is used in which MPLS is used at the back
end over it we use the VPN service through this way MPLS VPN network established.

7.7 Advantages of MPLS VPN over the other Technologies
There are some advantages of MPLS VPN network over the other technologies which
are given below:

1. It provides the services at the different layers like at layer 2 by the use of VPN
and also at layer 3 same by VPN and it also provide the services at layer 4 by the
use of MPLS also dial up VPNs.

2. It provide simplicity even any non experienced person can work on that network
and it is simple to use and even if anybody don’t have IP Routing knowledge.

3. With the help of MPLS VPN network anybody can deploy large networks
flexibly and it provides scalability.

4. It provides the security and reliable services to the customer and easy to handle
even in the large networks.

5. It is capable of providing customer requirements like security and QOS (Quality
of Service).

Configuration of the MPLS and VPN networks
There are four types of router configuration in the MPLS VPN network which are simple and easy to implement.

1. **P**  
   It is called the Provider Core Router and it is placed at the core network.

2. **PE**  
   It stands for the Provider Edge Router and it is mostly placed near the site location like the customer side.

3. **C**  
   It stands for the customer router and it is placed at the customer side.

4. **CE**  
   It stands for the Customer Router and it is placed at the customer side of the network like PE router at the provider side of the network.

In order to define the basic scenario of the network then we know that there are four parts in MPLS VPN network that’s there are two main basic parts in the network, one is at the customer side and other one is the provider side. In case of provider core router it simply works at the core network and in case of customer router it is also inside the customer network and away from the edge from the network and it is in the boundaries of the VPN network and where as in case of PE and CE is concerned it is placed to each other at their side opposite to each other and transfer LDPs information among to each other.

### 7.8 Kinds of MPLS-based VPN

There are three different kinds of MPLS-based VPN networks which are given below:

1. Layer 3 VPNs.
2. Layer 2 VPNs.

There are also three different situations where VPN can be secure solution for communication

1. Intranet-Based VPNs
2. Extranet-Based VPNs
3. Remote-Access VPNs

In case of Intranet-Based VPNs are concerned it is basically called Transport mode. Basically it is applied in the LAN environment where encryption on the packet above then layer 4 level because if it apply layer 3 and layer 2 level encryption then it's difficult for the switch to understand the packet.

In case of Extranet-Based VPNs are concerned it is basically called Tunnel Mode. Basically it is applied encryption on packet above then layer 3. We also hide our private
IP so nobody knows our inside IP address and we will not encrypt our LIVE IP so that they will also flow smoothly through the LAN environment. In case of Tunnel Mode is concerned the packet is changed and it looks like in such a way:

<table>
<thead>
<tr>
<th>DATA</th>
<th>IP</th>
<th>ESP</th>
<th>IP</th>
<th>MAC</th>
</tr>
</thead>
</table>

Figure 7.5 IP Header in Tunnel Mode

As we know that in Tunnel Mode the encryption applied above the layer 3 header. As we know that there are two IPs are mentioned in the header field one is after the ESP field and other is before the ESP field. The IP which is before the ESP field is not encrypted because when packet flows from the LAN (Local Area Network) it will not be encrypted because if it is encrypted then it is not understandable for the switch. OK fine we will accept that it is true for the problem then the question comes that what is the difference between the IP which is before ESP field and the IP which is after the ESP field?

The answer is that the IP which is before the ESP field is LIVE IP and the IP which is after the ESP field is the DEAD IP, so no one i.e. attacker will not come to know what network is working inside the organization or institution. The other IP which is LIVE IP will work for the routing mechanism.

In case of Remote-Access VPNs are concerned we have to install the software at the client side then it will easily connect with desired VPN network remotely. It also uses a mechanism that will helps to connect with the VPN network that mechanism is called NAT Transparency [37].

7.9 Security Concern in MPLS under the circumstances of the VPN

Security Association can be defined as "it is establishment secured connection between the two networks so that secure communication going on". Security Association may include the following things like cryptographic keys, digital certificates.

Security Association is a simple means one way communication which allows secure channels between the two end points so that the communication make secure. The fundamental use of the security association comes when two entities communicate with each other over more than one channel means they not depend upon the one channel it’s up to the requirement for example mobile subscriber and base station. Suppose a mobile subscriber subscribes more than one service on its mobile then each service has different service primitives like encryption, initialization vector. To make all this easy to handle all this security information is grouped logically. This logical group itself is a Security Association [38-39].

Security Association is identified with three parameters which are given below.

- Security Parameter Index (SPI)
- IP destination Address
- Security Protocol Identifier
There are some basic building blocks of MPLS VPN model which we must understand. There are following building blocks which are given below:
- Virtual Routing Forwarding (VRF)
- Route Distinguisher (RD)
- Route Targets (RT)
- Route Propagation through MP-BGP

### 7.9.1 Virtual Routing Forwarding (VRF)

A Virtual Routing Forwarding is the instance of the VPN forwarding table. Basically it is the combination of the following instances which are given below:
- VPN Routing table
- VRF Cisco Express Forwarding table
- PE router has IP routing table

### 7.9.2 Route Distinguisher (RD)

When VPN prefixes passing through MPLS VPN network through the multiprotocol BGP then in case of ISP is concerned it should be unique in case of IPV4 IP addressing, if there is a overlapping IP is used at the customer side then problem comes so in order to solve the problem we use a mechanism that is called RD. The main task of the RD is
that it generates a unique IPV4 IP in the ISPs and there will be no any overlapping IP problems come.

### 7.9.3 Route Targets (RT)

In case of RT mechanism there is some restriction among the different MPLS VPN network that one VPN communication with the other or which one is not be in order to solve this kind of problematic scenarios RT came in to being in order to solve the issue regarding process among the VPNs network.
Chapter 8

Comparison and Analysis of IP/MPLS Networks
This section will address IP/MPLS functionalities, applications, QoS, performance parameters, TE, protocol implementations, security issues and some simulation analysis form the relevant state of art study. The comparative study will describe prons and cons in the both technologies and the reasons to implement the desired features, functionality and mode of operations to cater with requirements.

8.1 Functionality

IP technology uses TCP/IP protocol stack to deliver data packet in the form of IP data grams of fixed size. IP datagram contain values of IP designation address to successfully deliver the packets. Main functionality of the IP technology is that it perform communication through IP layer by routing packets between routers and networks, implement but doesn’t guarantee QoS, offer multicasting transmission for network performance, complements IPSec security for data integrity, privacy, security and confidentially. It’s also possible to run IP over other transmission technologies such as ATM, Frame relay etc. it’s simple to implement and understandable while difficult to manage at the network level.

MPLS technology works and relies on IP technology since all the nodes connected to the ISP or enterprise networks have specific MAC and IP address called as source and destination addresses, unique to each node for data transmission. Labels are formed at the ingress LSR and removed at Egress which offers efficient data transmission between routes and switches attach in the MPLS domain. Traffic flows through LSP and becomes connection oriented [38]. LSPs are formed by configuring signalling protocols i.e. LDP or RSVP along with FECs based on IP addressing such that for identical FEC packet contain same label [38].

8.2 Multimedia Applications

MPLS and Non MPLS comparison for multimedia application traffic is provided in [32] that implements NS2 simulation tool with identical network topology. IP network with duplex communication, drop tail queuing and first come first serve parameters are deployed on the nodes with real time and best effort traffic. Best effort utilises background traffic while to obtain QoS real time parameters are configured. TCP UDP and CBR Protocols are used with variable packet sizes to transmit data across network. MPLS implements similar topology but offers labels instead of shortest path links through CR-LDP to offer explicit route in real time traffic.

Network performance for multimedia applications is observed through packet loss and packet received by TCP and UDP Protocols. An increase in number of TCP and UDP packets are obtained from MPLS TE simulation, throughput and network utilization has also increased as compare to non TE IP network.

In the figure 8.1 below, depicted the symmetric network topology for simulation without and with MPLS network implementations. On the left side of the figure, router 0 and router 1 are source router while router 6 and router 7 are destination routers, in figure 1 a), data flows between the networks through router 2-3-5 and reaches the destinations while router 4 is left under utilized due to traditional IP network protocols implementations. In figure 8.1 b), data flows from source to destination through
utilizing all the resourcing and thus router 4 serves for the data transmission between route 1 and router 7.

![Diagram of network flows with and without MPLS](image)

**Figure 8.1: Representation of a) Traditional and b) MPLS based TE flows [32]**

Simulations are performed in NS2 and results are displayed to measure and compare the performance of both networks. G.711 codec is used with CBR, UDP protocol for VOIP services with 226 media streaming are obtained. Voice packet size depends on the layer2 header, plus IP, UDP, RTP header and voice payload. UDP packet size consists of UDP header, RTP header and voice payload while drop tail queue mechanism is considered.

<table>
<thead>
<tr>
<th>Transmission Type</th>
<th>Traditional in bits</th>
<th>MPLS in bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>CBR PKT send</td>
<td>4567280</td>
<td>5389310</td>
</tr>
<tr>
<td>CBR PKT received</td>
<td>3876930</td>
<td>5105790</td>
</tr>
</tbody>
</table>

**Table 8.1: Throughput Comparison of Traditional and MPLS networks**

In figure 8.2 a), we see that the bytes receive at sources in 4.5 sec are less than in figure 8.2 b), which means implementing MPLS TE concepts will improve the performance of the network and resources as well as QoS but having high throughput of data stream. Also the number of nodes has strong effect on the throughput since with 6 nodes, more
data is transmitted in IP networks whereas small difference is seen in the graphs figure 8.2 b) when the number of nodes are increased.

![Graph 1](image1.png)  
Figure 8.2 a) IP Network Throughput [32]

![Graph 2](image2.png)  
Figure 8.2 a) MPLS Network Throughput [32]

If the relationship in the difference at network throughputs is high, so in reality every real time multimedia application is challenging the network resources to cater enough data bits that can sustain the QoS guarantee otherwise it will high influence single application, user, and network or as a whole on transmission, congestion, application, in terms of delay, jitter, load, packet loss, etc.

### 8.3 QoS in IP/MPLS

In IP network it is hard to control quality of services, ITU develop IP packet performance metrics which includes packet transfer delay, mean packet transfer delay,
delay variations, packet error ratio and packet loss ratio. End to end delay is observed between two reference points, to measure buffer overflow/underflow in real time application streaming for TCP protocol, the smaller delay variations causes negligible results, however depending upon the nature of application high delay variations cause errors in the receive packets or packet loss. Destination node is unable to recover these errors due to TCP protocol transmission delays. Packet loss ratio directly affects QoS of real time applications so application responds with three types. If the application is lost due to packet loss ratio crosses threshold level i.e. fragile type. Application tolerate type actually obtained less value in case of high packet loss while in performance application type intensive packet loss result in low performance. Some parameter like spurious IP packet rate, peak cell rate, sustainable cell rate, maximum burst size and maximum cell rate are also calculated for traffic performance. In [40] IPMM is IETF working group for defining internet performance metrics. There are two types of performance metrics in internet protocol.

a) Analytical Metric
A metrics specified and develop by A-Frame implementing metric concepts of propagation time of link, link bandwidth, and route and hop count.

b) Empirical Metric
It involves information about internet components, means to measure the parameters and extend it.

In order to use voice data for telecommunication services, Grade of Service (GoS) is measured through increase in traffic volume at network that requires more capacity to handle the traffic otherwise congestion can occur. The limitation posed on the service provider or telecommunication system and ISP exhibits QoS through measuring loss and delay in the GoS. Network traffic is divided across different classes through CoS for each packet to keep QoS measurement because sometimes different packets belonging to different CoS observes packet drop capability variations. In an IP packet type of service, precedence or priority consists of three bits and can obtain up to eight levels along with differentiated services.

Differentiated services contain information about application independence service, policing, QoS interoperability traffic flow and state of core network devices which is important to reserve resources during traffic flow at core network devices. DS forward the packets in per hop behaviour (PHB) through DS end points in DS domain. PHB assured forwarding group has four traffic classes and three drop precedence while DS nodes do not perform packet reordering for similar class. Every class get allocated bandwidth and buffering capacity for example any service class ‘A’ can get where bronze, silver and gold classes. PHB expedite forwarding group offers low latency, loss, jitter with end to end service and assured bandwidth delivery services.

MPLS is protocol independent architecture which does not provide specification to manage QoS but LSPs make it possible to deliver QoS through MPLS DiffServ integration. There are small changes in DiffServ and MPLS architecture, MPLS doesn’t facilitate PHB and traffic conditioning, however LSR router implement mechanisms for traffic management [33]. MPLS provide transparent mechanism to offer DiffServ as in traditional IP networks by identifying PHB.
8.4 Performance Parameters

In an IP network the performance of IP data packet is measured through number of parameters involved in the communication channel but mainly delay, throughput, network traffic utilization are interested parameters obtained during simulation. End to end delay from application layer of the source node to destination node, throughput in terms of routing or data packets, and network node i.e. switch or routers, transmission links and channels utilization. In [37] network topology is constructed and developed for IP ATM and MPLS technologies with FTP, voice and video traffic transmitting towards the clients. Different parameter values for models are selected based on traffic types. Delay, throughput, utilization, FTP response time and normalise delivered traffic is calculated during simulation. In simulation results IP offer fewer throughputs (Kbps) with constant number of loads (Kbps) as compare to MPLS. End to end delay for MPLS is more than the delay offered in IP networks while utilization of IP network.

8.5 Traffic Engineering

MPLS use TE mechanism to avoid network congestion and improve performance through mapping traffic streams. IP network require IGP tuning for traffic engineering in order to optimise the link and avoid congestion. MPLS TE adheres explicit routing capabilities through path computation LSP signalling, distribution of link information and desire traffic selection. MPLS DiffServ TE establishes control in per class TE and bandwidth and link bandwidth to reduce congestion. In an IP networks an ISP may implement inter domain TE by running IGP that are OSPF or IS-IS for optimise path and link selection, it causes protocol stability such that path remains constant until reconfiguring routing parameters or changing network topology, low protocol overhead such that no load and link state information is required, and increase performance constraints which means the constraint incorporated by ISPs are opted difficulty or new selection of constraints are defined. Link weights for routing configuration helps to have a compatibility of traditional routing, similar semantic representation as routers are configured through weights for every link, and fix weight or route recovery mechanism or computed automatically if topology is change.

8.6 Security Issues

IETF develop IPSec protocols [38-39] to provide application level security which enterprise network can implement on IP level to secure internet communication. It is done through building VPN network for branch offices, remote login and server access over internet, integrating extranet and internet connectivity and securing web/electronic commerce. IPSec provide encryption and authentication at IP level, such that all the applications distributed on different clients and servers use it [42]. IPSec offers strong security and is implemented in routers or firewalls. IPSec provides security association (SA) [9] across applications. IPSec operates either in transport mode or tunnel mode depending upon the implementation configuration [38]. Network Address Translation (NAT) [37] is also implemented at ISP network to secure incoming IP traffic. In MPLS, VPN include two models overlay and peer to peer at the ISP network. MPLS and VPN architecture implementation enable strong security among devices connected to the network.
8.7 GMPLS

Generalized MPLS [43] offer incorporating single control plane for the support of many switching technologies including packet, time, wavelength, and space by separating control plane form signalling plane and have high market for the new networks. GMPLS support for TE, CoS and QoS concepts, OSPF, ISIS, LDP and RSVP-TE protocols implementations. To enable optical network support it exhibits wave division multiplexing (WDM) along with QoS through defining (ER) explicit routes. A photonic multilayer called multilayer Hikari created by NTT Corporation can do switching between wavelength and IP layer, GMPLS incorporate SONET, ATM and Ethernet while TCP/IP lower layers aggregate GMPLS, ;PLS and MPLambdaS.

Presently, QoS in IP/MPLS are performing quite well but as the domain changes, the PHB and EXP fields containing QoS parameters are excluded and another domain synthesis the incoming packets according to the next/adjacent domain. Mesh topology of the internet infrastructure causes the end points to connect through different domain, but shortcoming of the data is trade off between the domain exchanges and QoS required are unspecified for any service delivery. GMPLS networks signalling/routing ensure traffic QoS between end to end devices in TDM, cell and packet, fibre and wavelength; which are presently deployed infrastructures. CBR routing imply (O)LSPs state schemes for network, OSPF-TE complements status information guarantee for LSA, RSVP-TE for connection and resource reservations as well as CR-LDP implementations causing TE in heterogeneous networks through multilayer phenomena. Along with MPLS scalability option, GMPLS also provides scalability since it implements DiffServ through traffic classification and QoS functioning due to DiffServ Code point (DSCP) field in the header marks the packets for class identification. Expedited forwarding, assured forwarding and defaults PHB defined by DiffServ assure low delay/ loss/jitter and bandwidth requirements.

In [44], IP and dense wavelength division multiplexing (DWDM) is describe by integrating them, through GMPLS and MTE for metro networks. To obtain IP/MPLS and wave length switching, GMPLS node is capable to act as (O)LSP and LSP. To establish QoS at optical layer; BER, delay and jitter are uniquely identified along with monitoring, security and protection mechanisms as well as QoS manager a details description is provided in [44]. During QoS scheme implementation probability of blocking is higher for sensitive data traffic, although EF requests by setting threshold level to maximum can control quality of the transmission is its set according to the SLA of an operator.

In [45], GMPLS networks nodes simulation is conducted to traffic QoS guarantee through measuring probability of expected recovery failure and time/ signal loss graphs plots and then they are investigated in terms of LSP length backup and network performance. Traffic recovery for the QoS metric is derived through BCS algorithm, which provides solution for QoS multiple classes guarantee as well as LSP backup resource sharing.
Chapter 9

Conclusions and Future Work
9.1 Conclusions:

The thesis aim was to conduct theoretical study of an IP and MPLS network technologies and observe the problem associated within IP networks. Mainly study had been done in the communication medium of both technologies as well as the architecture, entities, routing protocols, QoS and others aspects are also discussed.

The complete internet is the connectivity of small and large scale enterprise networks and ISPs that implements IP network architecture while the core internet infrastructure consists of interconnection of devices running multiple protocols to transmit data packets from one end to another end which is not very simple and easy to maintain due to link failure, routing, congestion, application running at end nodes, interconnectivity between devices, QoS, security risk, capacity and bandwidth limitation, vendor specific devices and applications etc.

We have tried to demonstrate the need for new technology emergence and its implementation over IP network to increase throughput i.e. transmission rate, decrease delay and jitter for better QoS delivery. IP become standard technology due to number of devices and end nodes involved in the transmission had been supplied with unique address on the internet i.e. IP address, however this technology perform transmission through IP packet datagram transmission across transmission medium because each source and destination contain and IP address i.e. server or nodes whose identification is only possible through IP packet datagram. There is no standard competing technology as IP technology because it offers both connection oriented and connectionless data transmission through TCP/IP protocol. With an ever increase in the number of real time application development and usages across the network through broadcasting, multicasting, and unicasting, it was necessary to perform the transmission with QoS guarantee and reliability.

IP technology is however not capable handling high data rate stream of voice and video data as compared to simple datagram. To increase data transmission rate at the core network either increase the bandwidth or implementing new protocol is required. However increasing bandwidth through physical mean is unnecessary because in an internet data transmission traffic follow through certain routing procedure to deduce routes from source to destination in connection oriented or connectionless transmission mechanism. The routes deduce through IP routing protocol follow the shortest path routes or least cost routes which leads to the circumstances of network congestion, underutilized network resources/links and proper load balancing procedures at the network level.

To overcome the problems associated in IP network, MPLS networks are introduced because they use label switching technology at the IP core routers to make routing mechanism efficient, configure data packet with small labels at the start and the end of the MPLS domain and to deliver QoS guarantee transmission almost any voice and video application. MPLS uses forwarded equivalency class parameters differentiate incoming traffic classes and label then according to different priority based on MPLS traffic engineering implementation. MPLS also offers various routing protocols to define routes at each MPLS domain and outside MPLS domain and performs connectivity operation through BGP and EGP. A part from QoS guarantee for real time
applications, traffic engineering provide better utilization of network resources if some devices/link are underutilized and limits/avoid congestion. MPLS also offers VPN implementation and interconnected with other network to provide secure and reliable communication.

To obtain QoS and cope with current network infrastructure we provide the following observations.

- Since MPLS/IP network delay and packet loss can be decreased through implementing efficient algorithms or optimizing existing algorithms for protocols without decreasing security.
- Use of multiple process/parallel processing capabilities should be deployed at core network routers.
- Slow processing routers and switches should be replaced with fast ones since processing speed of the router/switch has direct impact on data transmission rate as it runs algorithms and perform switching, signalling, database lookup, marking, labelling etc.
- To obtain/request for any QoS oriented services e.g. IP TV, the server is connected to the high speed transmission line but it is also important to measure delay, jitter and packet loss at access network side because most of the problems exist due to signal loss, inter symbol interference etc.
- The device connected to the access network can also participate negatively if there are multiple applications running on the user device so the incoming QoS of IP TV stream will require processing for the device (lower to upper layer) and ultimately result an unacceptable QoS.

Although everything works with IP but MPLS makes it possible to bind IP with label by quoting through ingress LSR and removing it at egress LSR the implementation of the MPLS should continue but IETF also provide specification to support IntServ model. Besides IP, MPLS DiffServ have 3 bit type of service field to offer 8 types of services at present with further splitting possibilities as well as EXP to PHB mapping and using E-LSP & L-LSPS to facilitate QoS transmission mechanisms.

9.2 Future Work:

During the last few years MPLS is the most prominent and most of the service providers going to replace their frame relay and ATM services with the MPLS technology. There are also so many implementation of the MPLS technology especially Cisco which will provide us the features of QOS and enhanced out network.

MPLS technology now lies at the backbone of the network, now days a lot new research is going on the QOS, VPN, and voice collaboration with the MPLS features in order to use its features. MPLS service works with the CoS (Class of Service) and is useful for the VOIP applications such as the video conferencing, ERP, CRM etc. It is also true that MPLS Technology is the future of the communication for businesses.

There are also some future aspects with respect to the MPLS on which service provider’s poses serious attention like new sensors in the MPLS traffic, raising cost and complexities and multiple management touch points.
References


[43] Analysis of GMPLS Architecture, Topologies, and Algorithms


