

Comparative Evaluation of MPLS and non-MPLS Network

By

M. Abdullah Al Mamun

ID: 101-19-1214

Sadia Ahmed

ID: 101-19-1211

Md. Khadimul Islam

ID: 101-19-1192

This Thesis Report is Presented in Partial Fulfillment of the Requirements of the Degree of
Bachelor of Science in Electronics and Telecommunication Engineering

Supervised by

Dr. A.K.M. Fazlul Haque,

Head Of Department

Department Of ETE

Daffodil International University



DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

January, 2014

APPROVAL

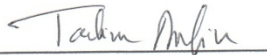
This thesis titled “**Comparative Evaluation of MPLS Network and Conventional IP Network**” submitted By M. Abdullah Al Mamun, Sadia Ahmed, Md. Khadimul Islam to the Department of Electronics and Telecommunication Engineering (ETE), Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Electronics and Telecommunication Engineering and approved as to its style and contents.

BOARD OF EXAMINERS



Dr. A.K.M. Fazlul Haque
Associate Professor and Head
Department of ETE
Faculty of Science & Information Technology
Daffodil International University

Chairman



Mr. Md. Taslim Arefin
Assistant Professor
Department of ETE
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Mrs. Shahina Haque
Assistant Professor
Department of ETE
Faculty of Science & Information Technology
Daffodil International University

Internal Examiner



Dr. Subrata Kumar Aditya
Professor and Chairman
Department of Applied Physics,
Electronics and Communication Engineering, University of Dhaka

External Examiner

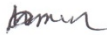
DECLARATION

We hereby declare that, this thesis has been done by us under the supervision of **Dr. A.K.M. Fazlul Haque**, Associate Professor & Head, Department Of Electronics and Telecommunication Engineering, Daffodil International University, Dhaka. The presentation has been held January, 2014

Supervised By:



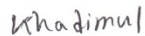
Dr. A.K.M. Fazlul Haque,
Associate Professor and Head
Department Of ETE
Daffodil International University



M. Abdullah Al Mamun
ID: 101-19-1214
Department Of ETE
Daffodil International University



Sadia Ahmed
ID: 101-19-1211
Department Of ETE
Daffodil International University



Md. Khadimul Islam
ID: 101-19-1192
Department Of ETE
Daffodil International University

Acknowledgement

At first we express our heartiest gratefulness to the most gracious, most merciful Almighty ALLAH for his greatness for blessing me with health and mind.

We express our boundless honor and respect to Our thesis supervisor **Dr. A.K.M Fazlul Haque** Associate Professor and Head, at Department of Electronics and Telecommunication Engineering Daffodil International University (DIU), for providing us this opportunity to complete our thesis with complete support and guidance during entire period.

We would like to express our heartiest gratitude to **Dr. Golam Mowla Choudhury**, Professor of Electronics and Telecommunication, Daffodil International University, **Dr. Subrata Kumar Aditya**, Professor, Department of Applied Physics, Electronics and Communication Engineering, University of Dhaka and all of our respectful teachers of ETE Department.

And at last we cannot but express our acknowledgement with due respect to the constant support and patience of our family members for completing this thesis report

Abstract

Multiprotocol Label Switching (MPLS) is a new means to enhance the speed, scalability and service provisioning capabilities for optimization of transmission resources. Traffic Engineering (TE) is the key feature of MPLS which is effectively used for managing the networks for efficient utilization of network resources. MPLS technology provides lower network delay, efficient forwarding mechanism, scalability and predictable performance of the services which makes it more suitable for implementing real-time applications such as Voice and video. In this report, comparative performance of MPLS network over conventional Internet Protocol (IP) network has been analyzed. NS-2 is used to simulate the both networks and the comparison and analysis is made based on the parameters such as Packet jitter, Packet delay, Packet drop. The simulation results are analyzed and it shows that MPLS network provides better performance than conventional IP network in implementing real-time applications such as Voice and video.

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

TABLE OF CONTENTS

Chapter 1	INTRODUCTION	
1.1	Motivation.....	1
1.2	Outcomes.....	1
1.3	Thesis Outline.....	1
Chapter 2	TECHNICAL BACKGROUND	
2.1	Data Transmission Types	2
2.2	Network Management.....	2
Chapter 3	MPLS Overview	
3.1	MPLS Benefits	4
3.1.1	Single Network Structure.....	4
3.1.2	IP over MPLS	4
3.1.3	ISP protocol Dependency.....	5
3.1.4	MPLS VPN Model.....	5
3.1.5	Traffic Engineering.....	5
3.2	MPLS Architecture.....	5
3.2.1	Ingress/Egress Label Switching Router.....	6
3.2.2	Intermediate Label Switching Router.....	6
3.2.3	Label Switching Paths.....	6
3.2.4	MPLS Label.....	7
3.2.5	Forwards Equivalency Class.....	8
3.2.6	LSR Operational Model.....	9
3.3	MPLS Label Packet Forwarding.....	9
3.4	Traffic Engineering in MPLS.....	11
3.5	MPLS TE Operations.....	12
3.5.1	Link Information Distribution.....	12
3.5.2	Computing Paths.....	12
3.5.3	TE LSPs Signalling.....	12
3.6	MPLS Operational Modes.....	13
Chapter 4	IP NETWORKS	
4.1	IP Standard Architecture	15
4.2	Internet Protocol.....	17
4.2.1	Datagram Fragmentation/Defragmentation.....	17
4.2.2	IP Header	18
4.3	Intranet work Routing Communication.....	19
4.4	Routing Information Protocol	20
4.5	Exterior Gateway Protocol	22
4.6	Border Gateway Protocol.....	22

Chapter 5	ROUTING PROTOCOLS AND MECHANISM	
5.1	MPLS Protocols	24
5.2	MPLS Routing Protocols	24
5.3	MPLS Signalling Protocols	24
5.4	Label Distribution Protocol.....	25
5.4.1	Version	26
5.4.2	PDU Length.....	26
5.4.3	LDP Identifier.....	26
5.4.4	LDP Messages.....	26
5.5	LDP Messages Exchange Mechanism.....	29
5.5.1	Discovery Message.....	29
5.5.2	Session Message	29
5.5.3	Advertisement Message.....	29
5.5.4	Notification Message	29
5.6	Resource Reservation Protocol.....	30
5.7	Transmission Control Protocol.....	31
5.8	User Datagram Protocol.....	32
Chapter 6	MPLS TRAFFIC ENGINEERING AND VPN	
6.1	MPLS Traffic Engineering.....	33
6.2	Traffic Engineering Basic.....	33
6.3	MPLS Traffic Engineering Overview.....	34
6.4	RSVP with Traffic Engineering Extension	34
6.4.1	RSVP Path Message	34
6.4.2	RSVP Reservation Message	35
6.4.3	RSVP Error Message	35
6.4.4	RSVP Tear Message	36
6.5	MPLS VPN Networks.....	36
6.6	Definition of VPN.....	37
Chapter 7	SIMULATION	
7.1	Simulation Tools.....	38
7.2	NS-2 Simulation.....	39
7.2.1	MPLS Simulation Model.....	39
7.2.2	Conventional IP simulation model	41
Chapter 8	RESULTS AND ANALYSIS	
8.1	Packet Drop Scenario.....	42
8.1.1	Packet Drop Behavior O MPLS Network.....	42
8.1.2	Packet Drop Behavior Of NON-MPLS Network.....	43
8.2	Packet Jitter.....	45
8.3	Packet Delay.....	46
8.4	Packet Loss Calculation.....	48

Chapter 9 CONCLUSION

Conclusion.....	49
Appendix.....	50
References.....	55

LIST OF FIGURES

Figure 3.1	LSP through an MPLS network.....	6-7
Figure 3.2	Label.....	8
Figure 3.3	TE label switching path.....	11
Figure 4.1	Generalized Internet / ISP Architecture.....	16
Figure 4.2	IP Datagram.....	18
Figure 4.3	IP Header.....	19
Figure 4.4	RIP Header.....	20
Figure 4.5	EGP Packet Header.....	22
Figure 4.6	BGP Message Header.....	23
Figure 5.1	LDP Packet Format.....	26
Figure 5.2	LDP Message Format.....	27
Figure 5.3	LDP Message Format.....	28
Figure 5.4	LDP Overview Network Diagram.....	30
Figure 5.5	RSVP Operation.....	31
Figure 6.1	Networks with IP Forwarding.....	33
Figure 6.2	RSVP Path Message.....	35
Figure 6.3	RSVP Error Message.....	55-36
Figure 7.1	MPLS network arrangement for simulation.....	39
Figure 7.2	Label Switched Path.....	40
Figure 7.3	Conventional IP network arrangement for simulation.....	41
Figure 8.1	Packet drop at 0.678 sec.....	42
Figure 8.2	Packet drop at 1.65 sec.....	43
Figure 8.3	Packet drop at 0.936sec.....	43
Figure 8.4	Packet drop at 1.27 sec.....	44
Figure 8.5	Packet drop at 2.87 sec.....	44
Figure 8.6	Packet jitter for MPLS network.....	45
Figure 8.7	Packet jitter for non-MPLS network.....	46
Figure 8.8	Packet delay for MPLS network.....	47
Figure 8.9	Packet delay for non-MPLS network.....	47

Chapter 1

Introduction

1.1 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^[1-2].

1.2 Outcomes

The thesis mainly compares 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 us to develop solid theoretical background for simulation projects in MPLS.

1.3 Thesis Outline

Introduction is chapter1 that provides motivation and expected outcomes. Chapter 2 gives 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 describes simulation using NS-2. 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

2.1 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.

2.2 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 notification.

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 a technology that forward packets as a way of communication by using labels to make forwarding decisions. Process switching is obsolete and so not in use today .MPLS forward packets by using label lookup because it is extremely fast and efficient. As the packet enters the MPLS domain layer-3 analysis is performed and a particular label is assigned to each incoming packet based on the layer 3 destination address. A MPLS network consists of a number of nodes called Label Switched Router (LSRs), others nodes that connects with IP routers or ATM switches are called Label Edge Router (LERs). Those router within MPLS domain that connects with the outside world, thorough which a packet enters the network are called ingress routes and the one through which the packets leaves the MPLS domain is called egress route. The idea is to attach a label to a packet at the ingress router within the MPLS domain and later can be used to make forwarding decisions instead of looking up for the destination address at each point because the label define the fast and effective label switch path (LSP) to direct the traffic all the way to the destination

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 ^[3].

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 Dependency

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^[3-4].

3.2.1 Ingress/Egress Label Switch Router (LSR)

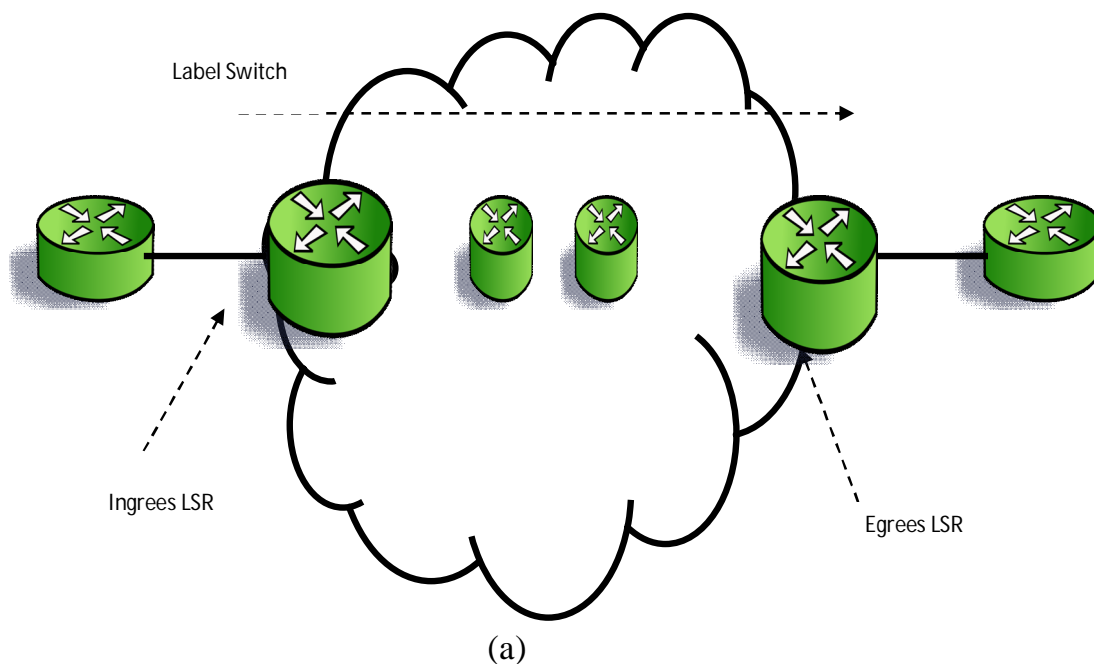
LSRs deployed at perimeter of MPLS network which provides an interface to inside MPLS domain and to outside the IP network. The role of ingress/egress LSR is to insert and remove labels when deployed as an ingress and egress. An ingress LER inserts label on the data packet called as imposing LSR and 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.



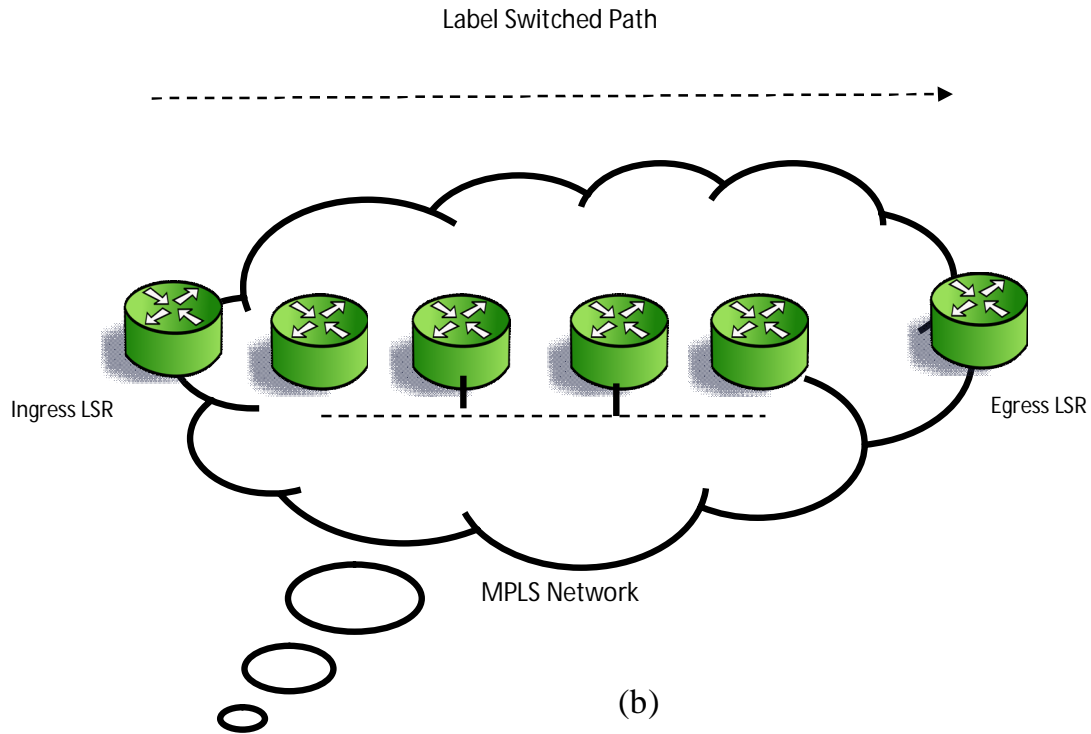


Figure 3.1: LSP through an MPLS network

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.

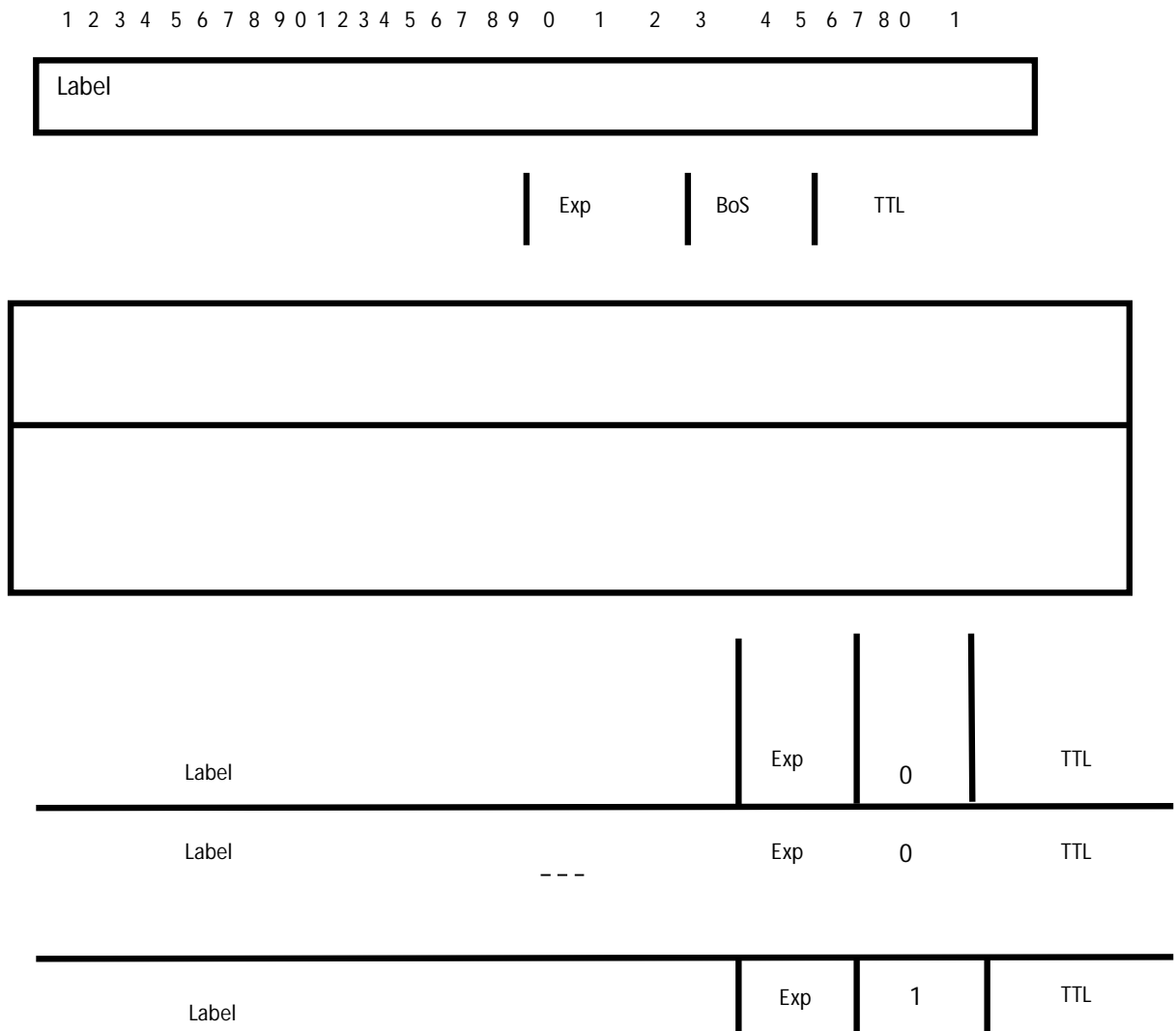


Figure 3.2: Label

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 .

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^[4].

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 nearby 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 down streaming 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.

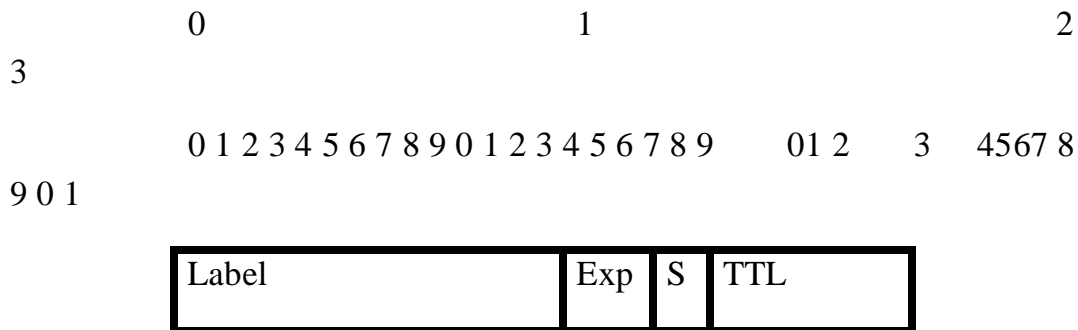
3.3 MPLS Label Packet Forwarding

A label is a short fixed length entity (header) created by label edge router to forward packets. Label Edge Routers and Label Switch Routers then use these label to make

forwarding decision. Labels contain values that indicate where and how to forward frame with specific value by looking into label forwarding information base (LFIB)^[5].

Label format of MPLS

TABLE 1: MPLS LABEL FORMAT



MPLS label contains following information:

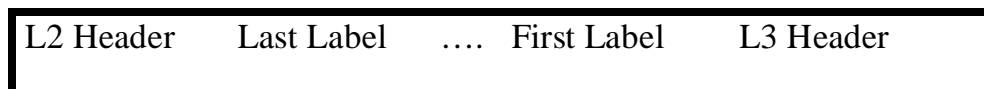
20 bit contain label

3 bit contain exp

1 bit contain in S and

8 bit contain in TTL

TABLE 2: MPLS LABELS BETWEEN LAYER-2 AND LAYER-3 HEADERS



The shim header may contain more than one label. Labels act as path identifiers, at each router the contents of the labels are examined and the next hop is determined. The fixed length 20 bit space in the label is set aside for the address space having a local significance only. Labels are chosen locally and are advertised by a router to its neighbours using a Label Distribution Protocols and are swapped away of each incoming packet before being forwarded to the next routers. MPLS is a datagram oriented technology though it uses IP routing protocols. In MPLS label the EXP is a 3 bit field set aside for experimental use. S bit is a 1 bit field that indicates the bottom and

is set for the stacking of labels and finally TTL is an 8 bit field which determines the time and number of hops a packet has to traverse before it can die.

Each label has a local significance and short identifier with fixed length, which is used to identify a particular FEC. When they reach at MPLS network at the ingress node, packets are divided into different FECs, on which different labels are encapsulated. Later forwarding of the packet is based on these labels.

3.4 Traffic Engineering In MPLS

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^[4]. 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.

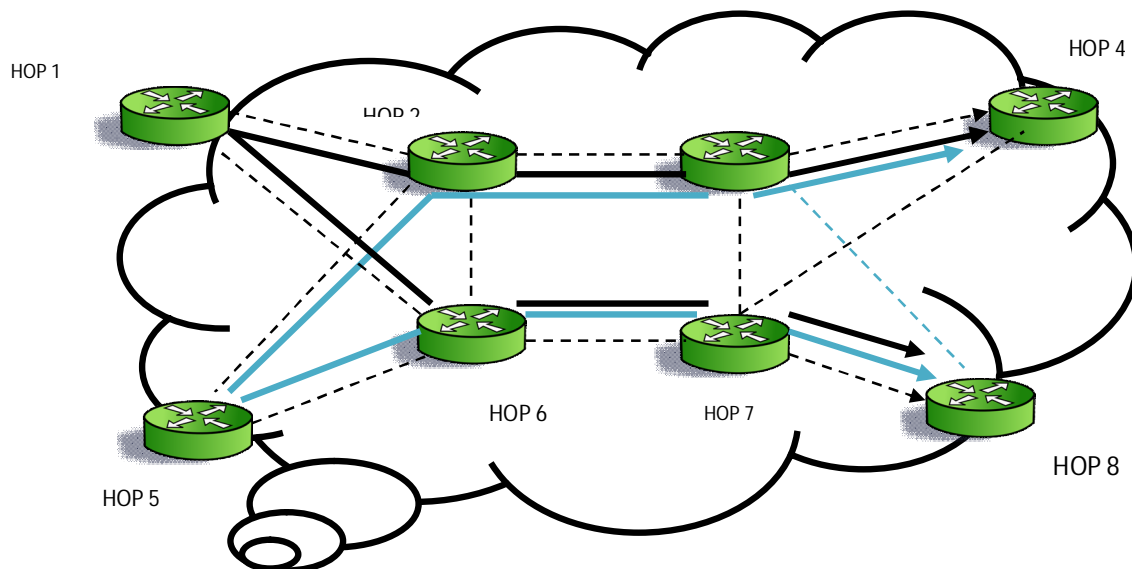


Figure 3.3: TE label switching path

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.

3.5 MPLS TE Operation

There are four main operations performed in MPLS TE.

3.5.1 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.

3.5.2 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.

3.5.3 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 signaling.

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.

3.6 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

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 entertainment 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^[6]. 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^[7].

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 channel i.e. fiber 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 connects 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^[8].

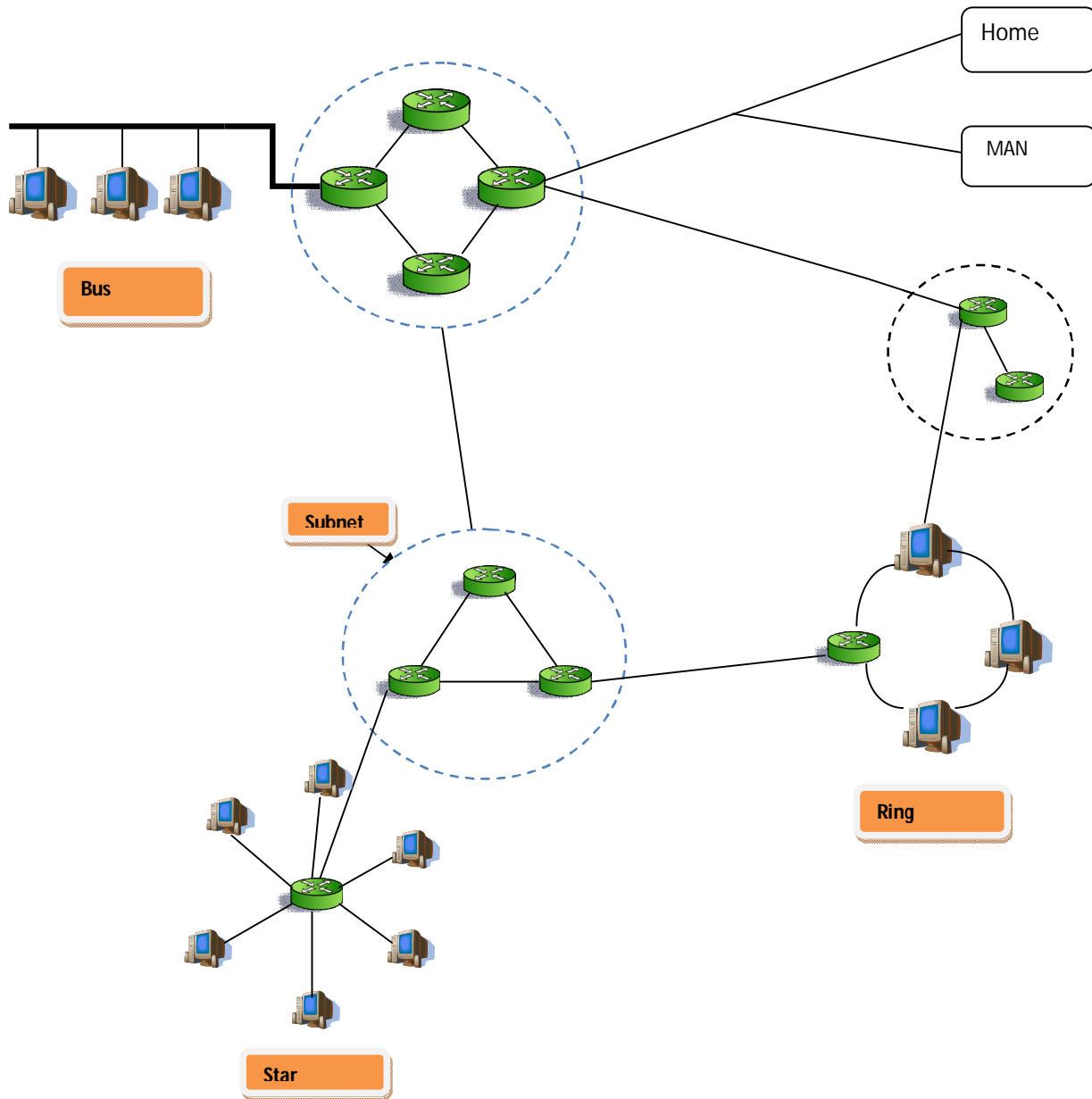


Figure 4.1: Generalized Internet / ISP Architecture

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^[9-10].

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^[11], 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^[8].

4.2.1 Datagram 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.

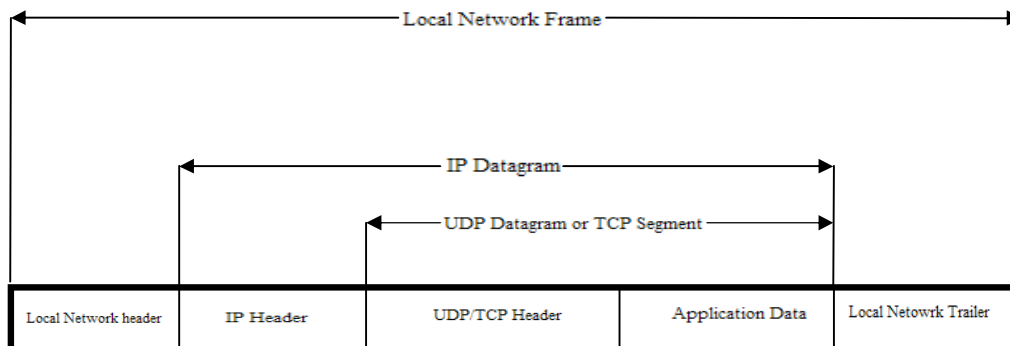


Figure 4.2: IP Datagram

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^[11].

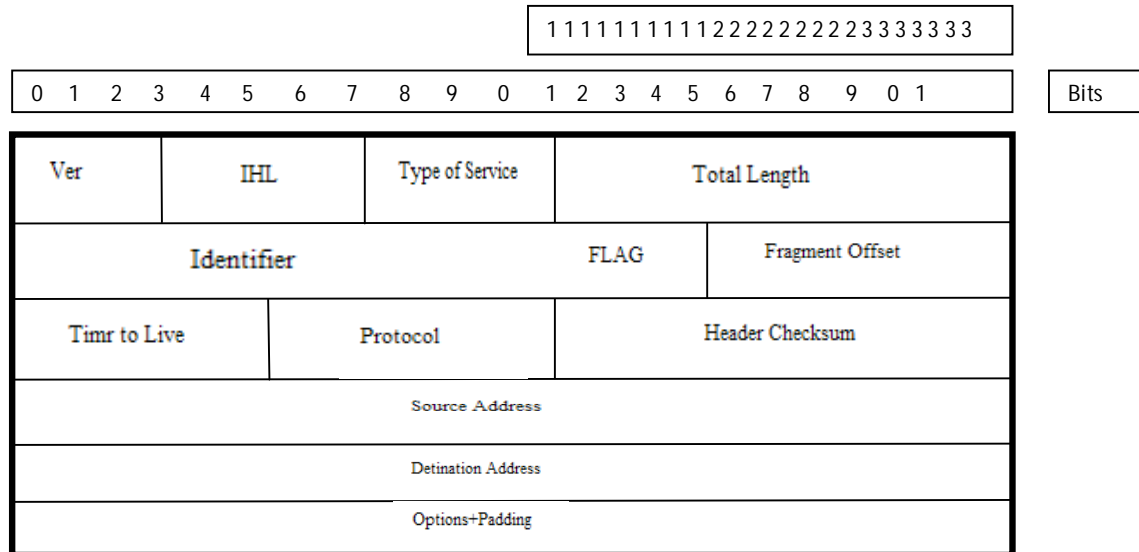


Figure 4.3: IP Header

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^[6].

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 be based on shortest path or list cost between the end points. Link state algorithms make decisions based on links which connect the nodes in the network. Distance vector algorithms measure the smallest distance between source and destination to transmit datagram. Routers implement link 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 that decides routes through link state algorithms.

4.4 Routing Information Protocol

RIP is used for integrated way communication, it uses distance vector algorithms in which routers exchange information through its routing table periodically. The path from 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 in networks because it 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 cost next router address and a flag value. RIP packets exchange routing information by transmitting message from 522 UDP port^[12].

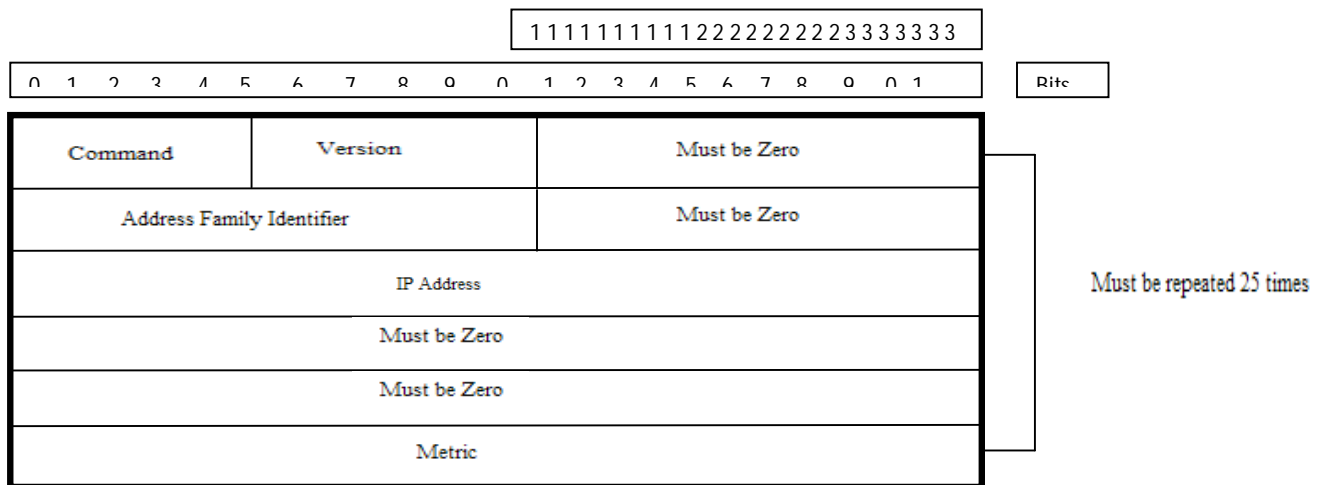


Figure 4.4: RIP Header

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

1	It request for information in the routing table
2	Receive reply from the routing table
3	Trace on
4	Trace off
5	Sun micro system has reserve this value
9	To update the request
10	To update response
11	To update acknowledge

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 ^[12] provides additional security to RIP messages and is almost identical 2 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 cast 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 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^[2] 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^[13].

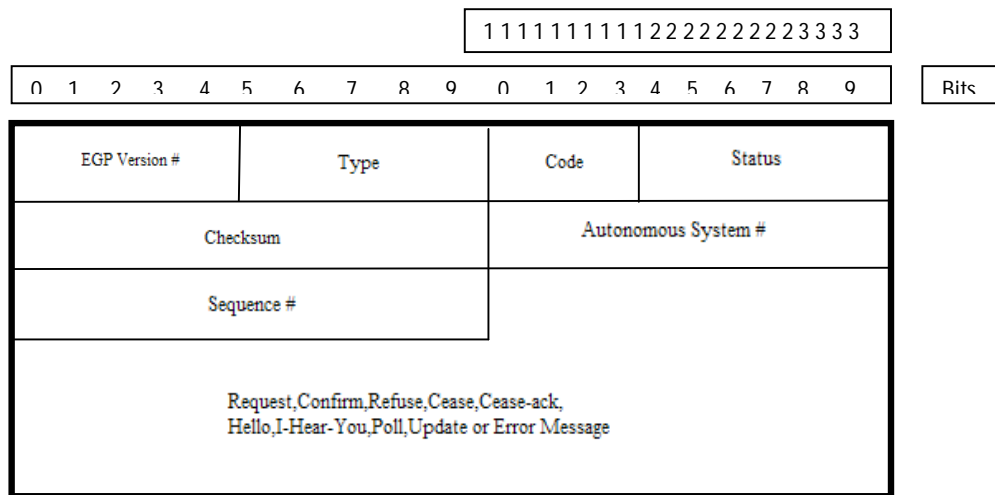


Figure 4.5: EGP Packet Header

4.6 Border Gateway Protocol

In^[14] 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 provide support in route aggregation and classless inter domain routing. If two systems i.e. routers runs BGP and connect two different AS the links are termed as an external links while if the connects in same AS there are called as interlinks. TCP is

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 have constant 152 bit message header, which contain four message type i.e. update open keep-alive and notification messages only keep-alive message provide automatic message request while the other messages also include more information.

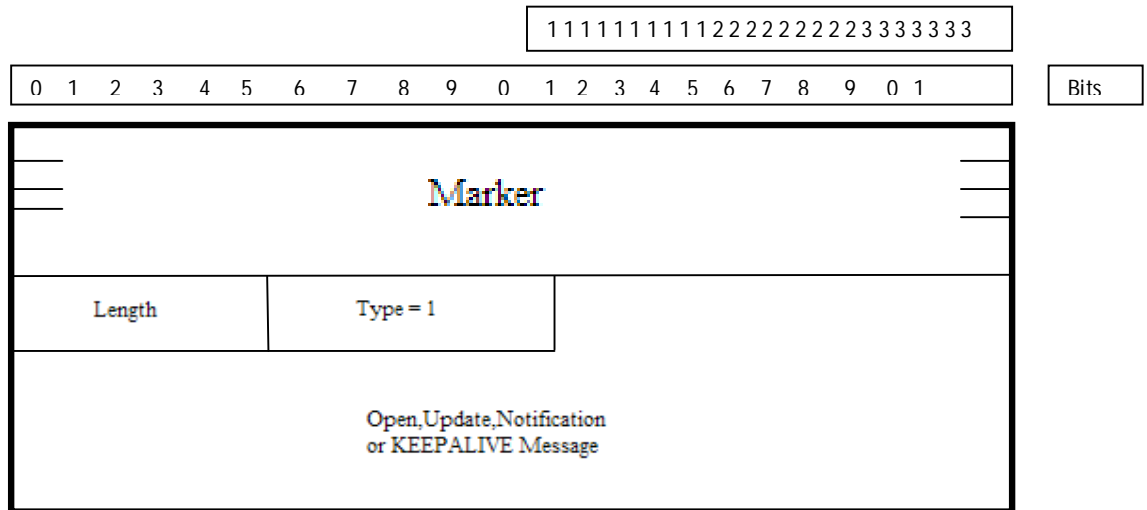


Figure 4.6: BGP Message Header

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 Signaling 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^[15].

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 works 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^[15].

2 bytes	2 bytes
Version	PDU Length
LDP Identifier(6 bytes)	
LDP Messages	

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

U	Message type	Message length
Message ID		
Parameters		

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

U	F	Type	Length
Value			
TLV format			

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^[16]. These four types of messages which are given below:

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

- It creates label mapping.
- It change label mapping.
- It delete label mapping.

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.

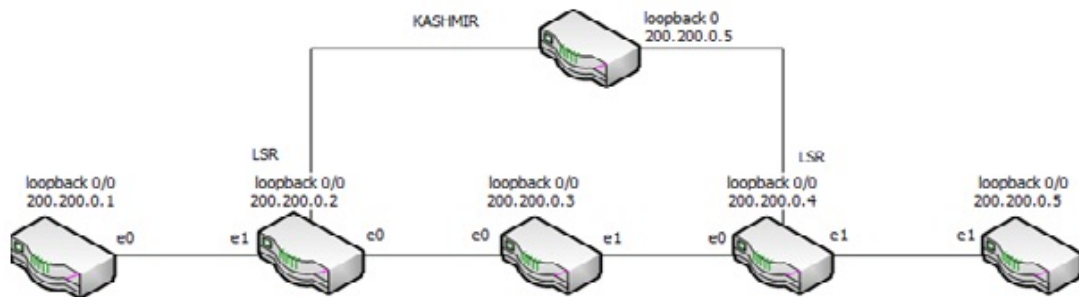


Figure 5.4 LDP Overview Network Diagram

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^[16] 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, jitter and through put performance parameters cause lowering 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 important 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.

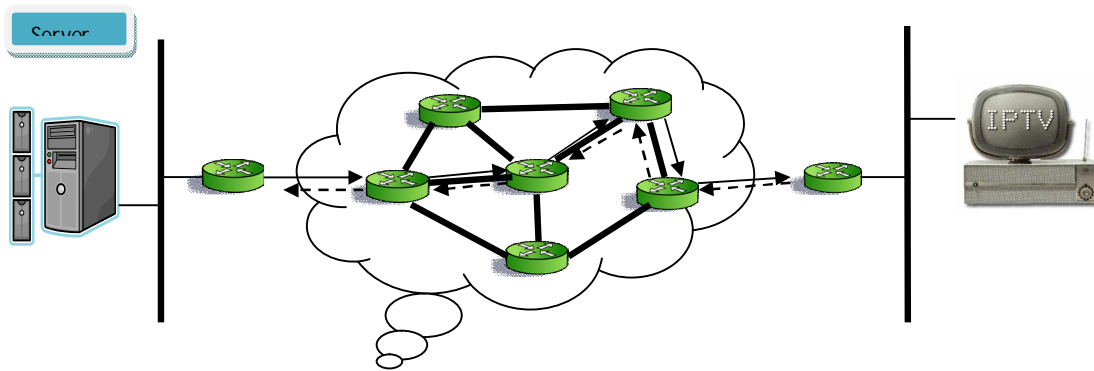


Figure 5.5 RSVP Operation

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^[17].

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^[17].

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

MPLS Traffic Engineering and VPN

6.1 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^[18-19].

6.2 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.

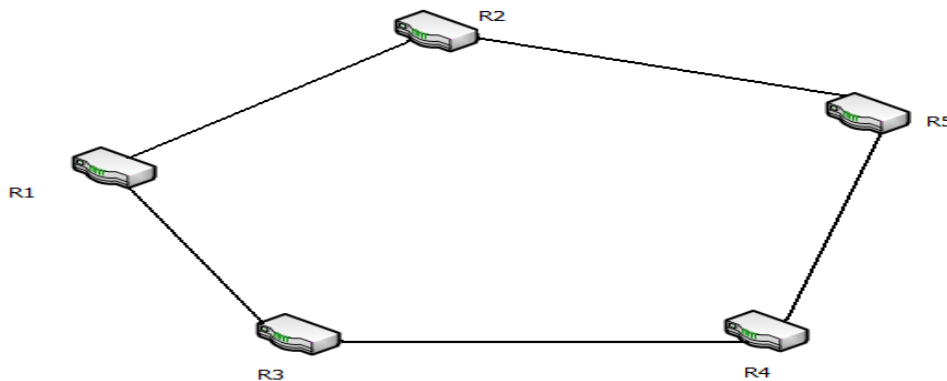


Figure 6.1 Networks with IP Forwarding

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.

6.3 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 hope 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 ^[20].

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.

6.4 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

6.4.1 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.

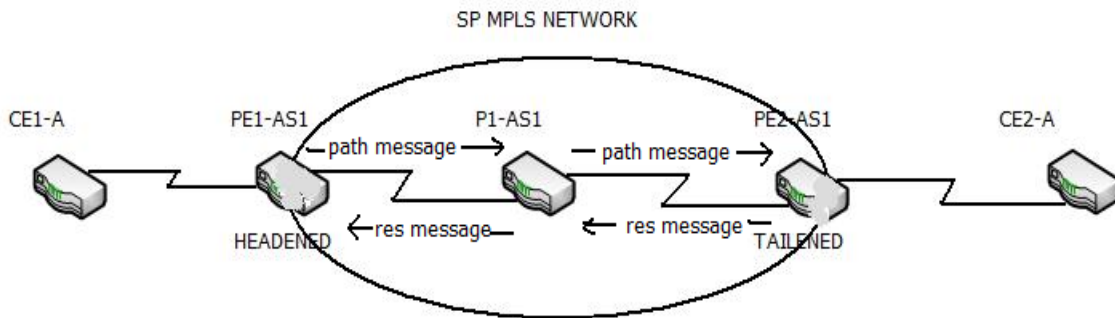


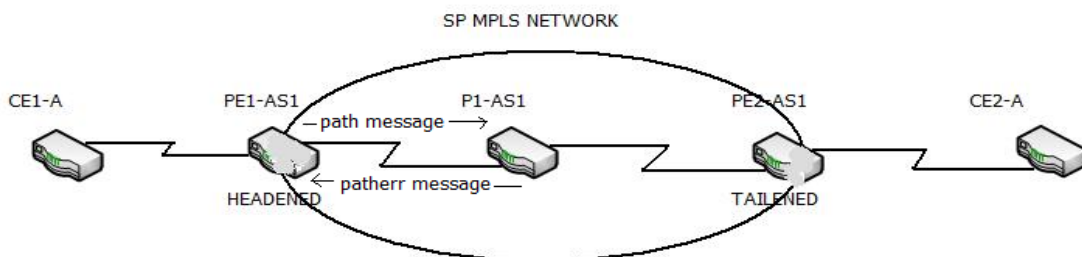
Figure 6.2 RSVP Path Message

6.4.2 RSVP Reservation message

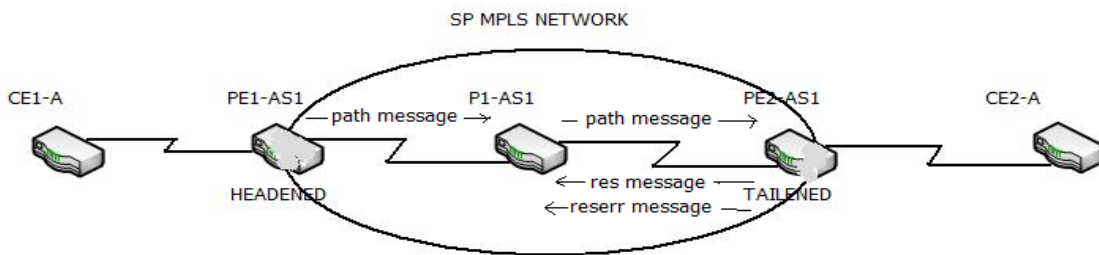
After the analysis of the Headened router it will apply the resource reservation on the required path and then use it in an effective manner. In the above figure when headened router send message to the inside router then it will send it to the next router and when it found that the resource is free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

6.4.3 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.



(a)



(b)

Figure 6.3 RSVP Error Message

6.4.4 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 headed router reserves any resources then it will send back message that is called tear message.

6.5 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^[21].

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

6.6 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.

Chapter 7

Simulation and Result

7.1 Simulation Tools

Simulation is the process of testing a designed model on a platform which imitates the real environment. It provides the opportunity to create, modify and study the behavior of proposed design so that one can predict its strengths and weakness before implementing the model in real environment. Some of the popular simulators used to simulate the data networks are

- OMNet++
- OPNET Modeler
- NS2

OMNet++

OMNet++ is the discrete event environment programmed in C++. This is used to simulate computer networks. OMNet++ usage is not straightforward, in order to start building of simulation topologies it requires in learning of number of tutorials, demos and walking through large web based documentation. Although it provides MPLS, LDP and RSVP-TE modules, it provides poor documentation for those modules^[22].

OPNET Modeler

OPNET provides several modules for the simulation comprising a vast universe of the protocols and network elements . It has gained popularity in academia as it is offered for free of cost to institutions and it is also obtained as a student version. The user doesn't need to OPNET simulation of voice over MPLS with considering Traffic Engineering have any programming knowledge in order to use OPNET; the user can directly concentrate in building and analyzing model from simulation. The main feature of OPNET is that it provides various real-life network configuration capabilities that make the simulation environment close to reality. The advantages of OPNET compared to other simulators include GUI interface, comprehensive library of network protocols and models, graphical interface to view the results, availability of documentation for the user to develop the network models etc.

NS-2

NS-2 is the simulator targeted at network research. The user interfaces with the simulator by using object-oriented script language OTcl on the UNIX systems (although it is possible to install NS-2 in windows). In order to build the simulation

topologies on NS-2 one has to know OTcl language. Moreover in NS-2 MPLS and RSVP-TE modules are not available as standard libraries these modules are implemented from third party. The documentation is not available for all modules and it is required by the user to read the source code in order to learn how to interface with it, generation of results and are not automatic^[22]. In our thesis we have used NS-2 for our network modeling and analysis.

7.2 NS-2 Simulation

To analyze the performance of MPLS and conventional IP network we have designed two scenario using NS-2.

- Scenario 1 consists of simulation of MPLS network
- Scenario 2 consists of simulation of IP network
-

7.2.1 MPLS Simulation Model

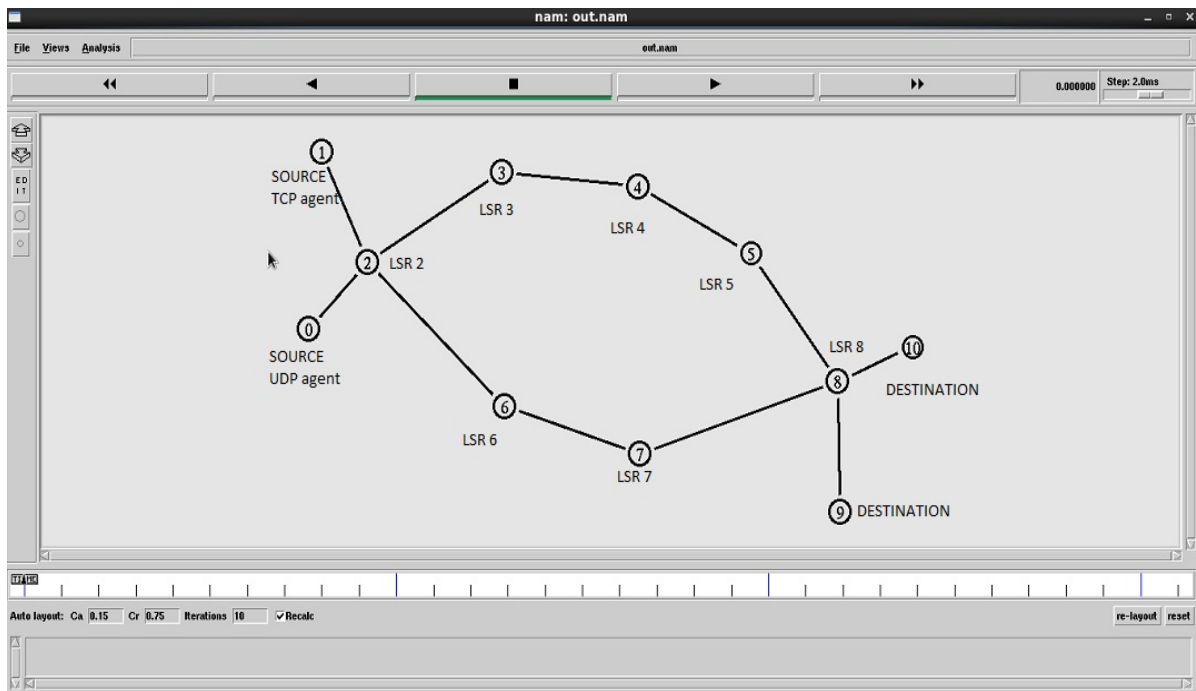


Fig7.1: MPLS network arrangement for simulation

The fig1 shows the arrangement of MPLS network. Here node 0 and node 1 are traffic source. The above network arrangement consists

- seven label switched router (LSR)
- one TCP agent as source (node 1)
- one UDP agent as source (node 0)

- ✚ one TCP agent destination (node 10)
- ✚ one UDP agent destination (node 9)

Source node 0 has been configured with CBR traffic using UDP connection. Node 1 has been configured with FTP traffic using TCP agent. FTP traffic are configured for heavy load on this network. Node 2, node 3, node 4, node 5, node 6, node 7, node 8 are MPLS node. These nodes are configured as Label Switched Router (LSR).

A MPLS router that performs routing based only on the label is called a label switch router (LSR) or transit router. This is a type of router located in the middle of a MPLS network. It is responsible for switching the labels used to route packets. When an LSR receives a packet, it uses the label included in the packet header as an index to determine the next hop on the Label Switched Path (LSP) and a corresponding label for the packet from a lookup table. The old label is then removed from the header and replaced with the new label before the packet is routed forward.

In this model we used 1Mb and 0.5 Mb duplex-link between nodes. The connections between node 0 & node 2 and node 1 & node 2 are 1Mb duplex-link. The connections between node 2 & node 6 and node 7 & node 8 are 1Mb SFQ type duplex-link. The connection between node 6 & node 7 is 0.5 Mb duplex-link. Node 8 is connected to node 9 & node 10 using 1Mb drop tail type duplex-link. node 2, node 3, node 4, node 5 & node 8 are connected using 0.5 Mb duplex-link.

The path or connection which are made by using label switched router is known as label switched path (LSP). The following figure shows the label switched path.

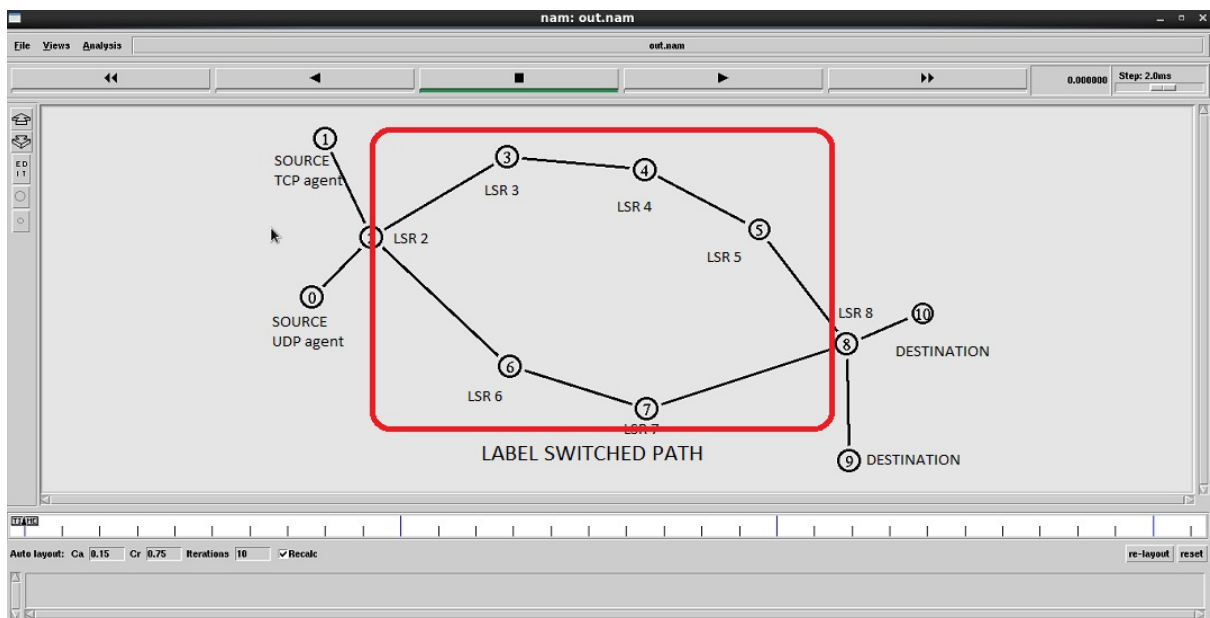


Fig 7.2: Label Switched Path

The next chapter will show how the MPLS network labeled the heavy load of a network and reduce the packet drop.

7.2.2 Conventional IP simulation model

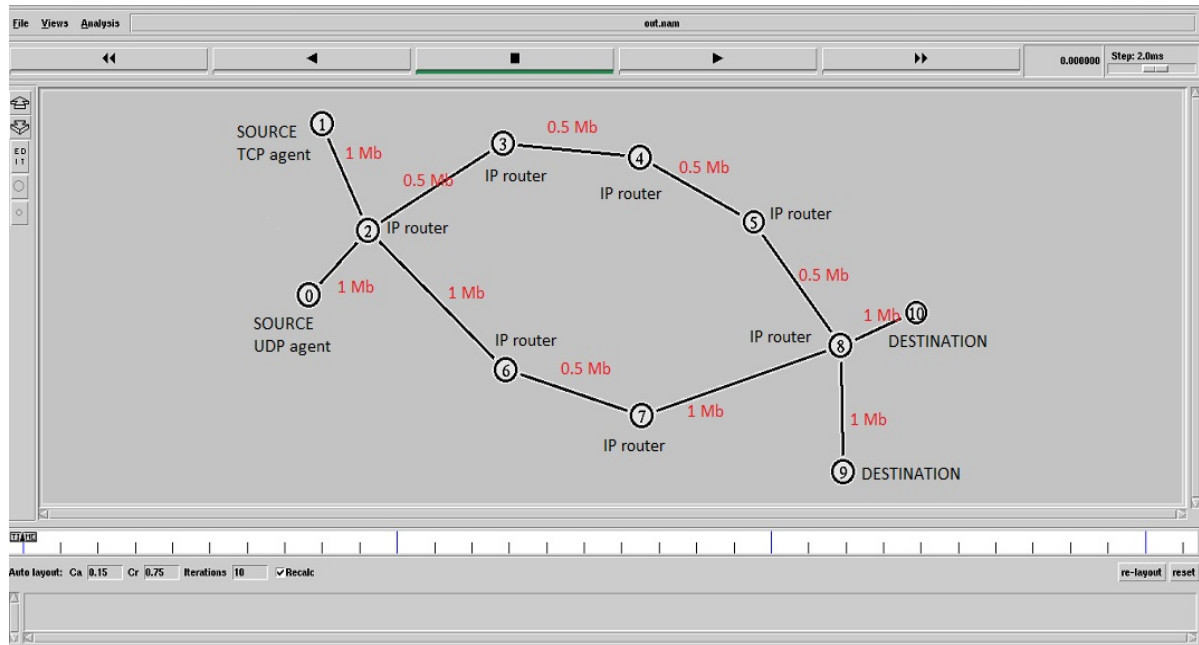


Fig 7.3: conventional IP network arrangement for simulation

The fig 3 shows the network arrangements for conventional IP network. Here we have used the same source and destination as used in the MPLS network. Sources are configured using tcp and udp agent as configured in MPLS network. In MPLS network we used the LSR's between source and destination to configure a label switched path. But in conventional IP network we have used normal IP routers to show the behavior of IP network. Node 2, node 3, node 4, node 5, node 6, node 7 & node 8 are normal IP routers or normal ns node.

The connections between all the nodes are configured as we configured in the MPLS network. There is no difference in connection links between MPLS and IP network.

Chapter 8

Analysis

8.1 Packet Drop Scenario

Packet drop scenario has been shown below for both MPLS and non-MPLS network.

8.1.1 Packet Drop Behavior Of MPLS Network

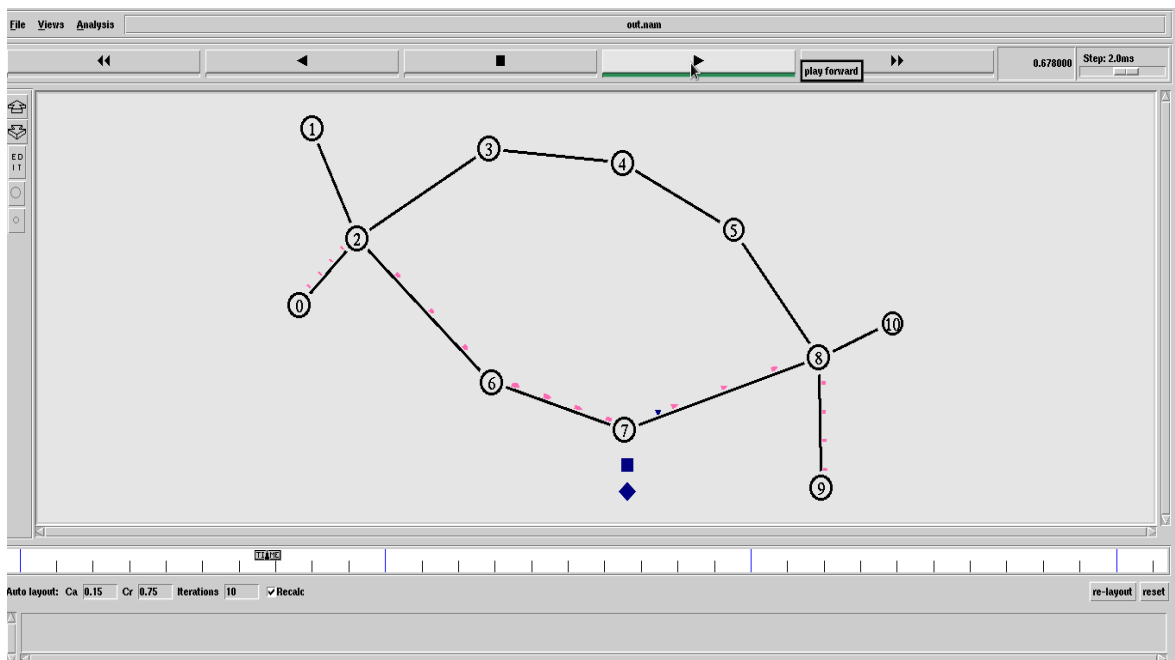


Fig 8.1: packet drop at 0.678 sec

Here hot pink color indicates the CBR traffics from UDP agent and navy-blue color indicates FTP traffics from TCP agent. From fig 1 we can easily see that at 0.678 sec there is some FTP traffic drop happened. At LSR7 some packets are dropped.

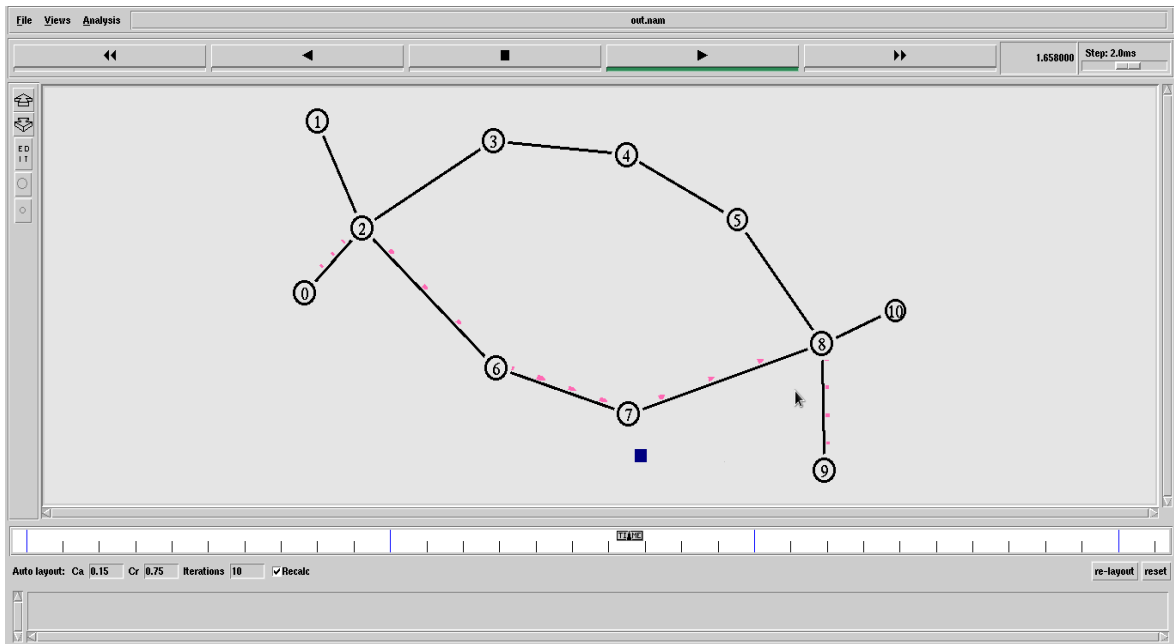


Fig 8.2: packet drop at 1.65 sec

The fig 2 shows the packet drop at 1.65 sec at LSR7. During the whole simulation time (3.2 sec) we have seen few packet drops only at LSR7. Only traffics which are generated from UDP agent are dropped.

8.1.2 Packet Drop Behavior Of Non-MPLS Network

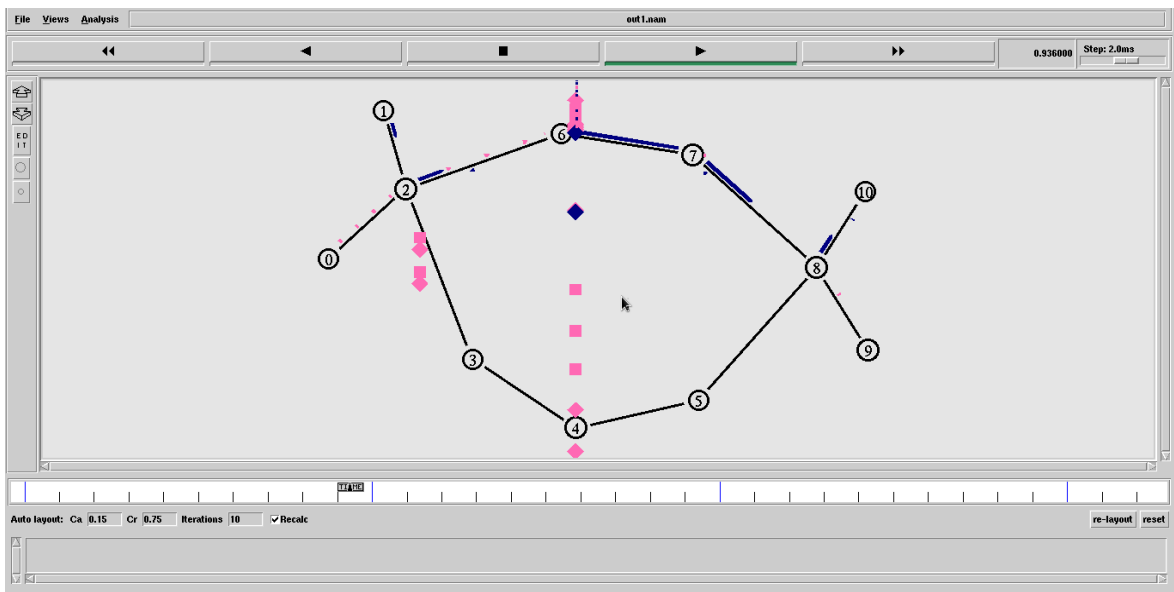


Fig 8.3: packet drop at 0.936sec

From fig 3 we can see the packet drop behavior of conventional IP network or non-MPLS network. Here heavy packet drop has been happened. We can see that packet drops are occurred at node 2 and node 3. In MPLS network only FTP traffics are dropped at minimal amount but in non-mpls network we can see that both CBR and FTP traffics are dropped with huge amount.

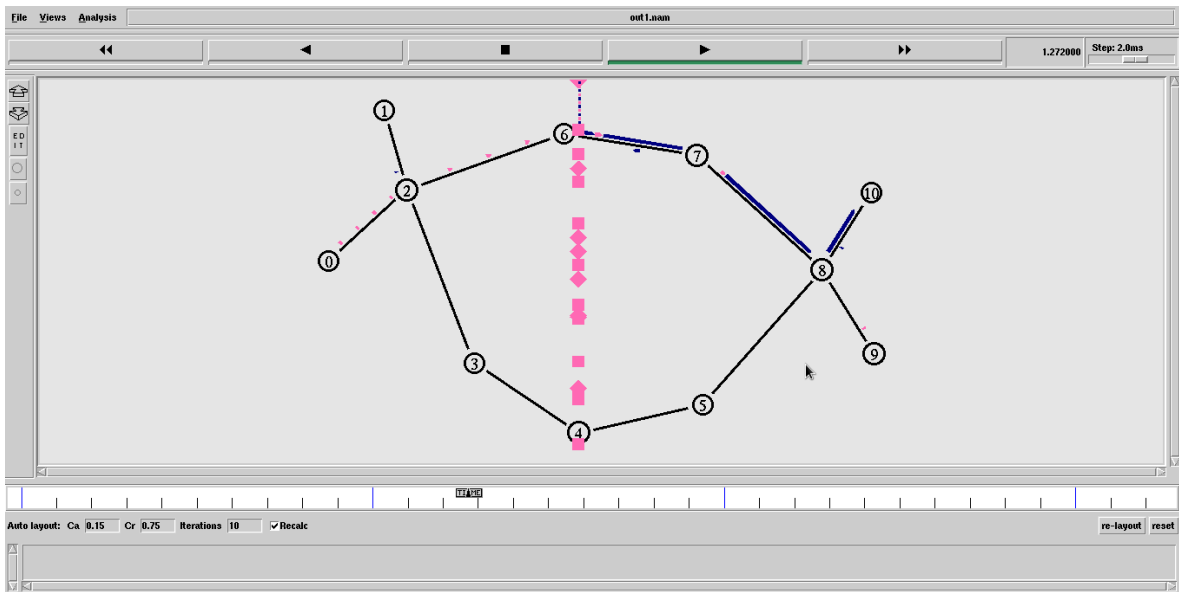


Fig 8.4: packet drop at 1.27 sec

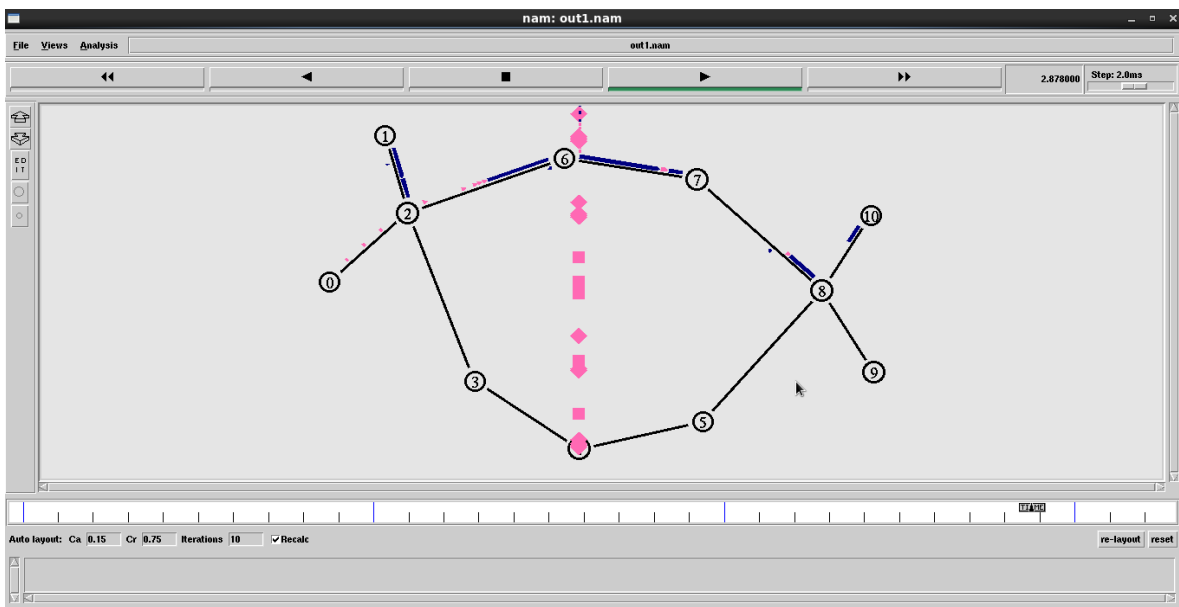


Fig 8.5: packet drop at 2.87 sec

Fig 4 & fig 5 shows the heavy packet drop at 1.27 sec and 2.87 sec respectively. During the whole simulation time (3.2 sec) we have got heavy packet drop simultaneously. From these above figures we can simply say that MPLS network gives much better performance than the conventional IP network.

8.2 Packet Jitter

Jitter is the fluctuation of end-to-end delay from one packet to the next packet of connection flow. Packet jitter can be calculated by

$$\text{Jitter, } J = |D_{j+1} - D_j|$$

Where D_{j+1} is the delay of $i_{th} + 1$ packet and D_j is the delay of i_{th} packet. The following figures (Fig 6 & Fig 7) shows the comparison of packet jitter for MPLS and non-MPLS network. Here we have done all the calculation using NS-2 visual trace analyser.

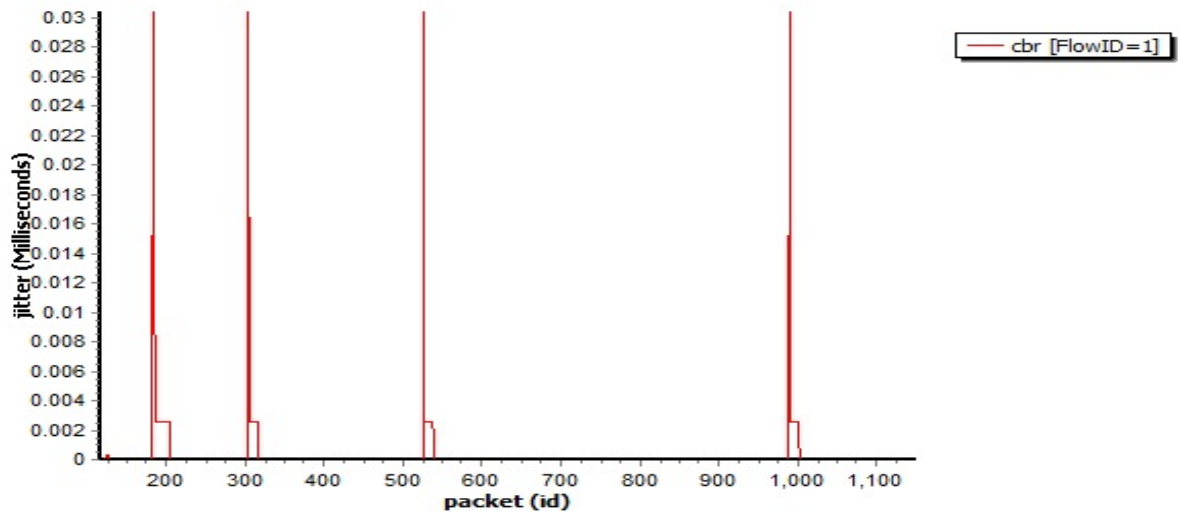


Fig 8.6: packet jitter for MPLS network

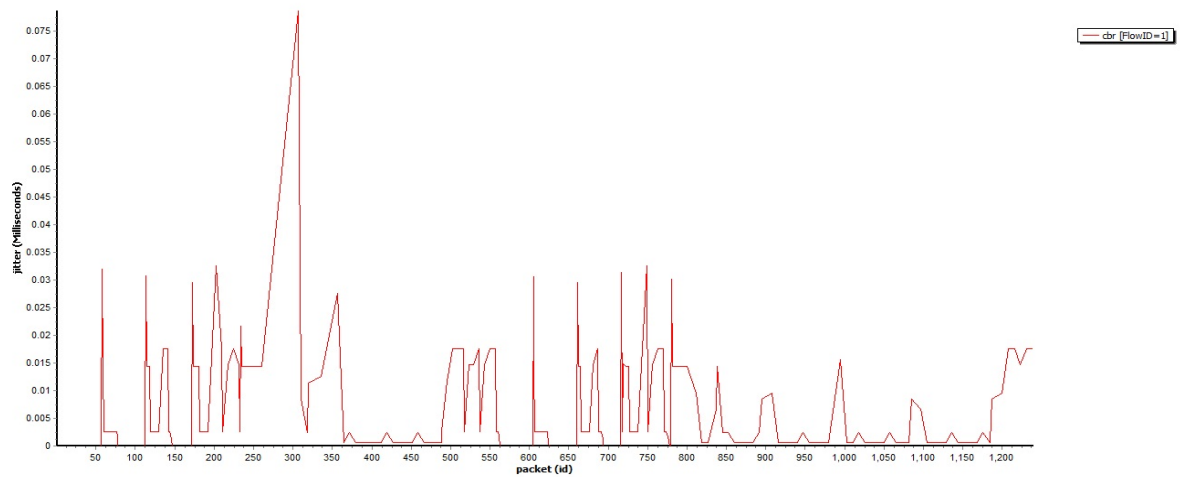


Fig 8.7: packet jitter for non-MPLS network

8.3 Packet Delay

Packet delay refers to the time taken for a packet to be transmitted across a network from source to destination. Packet delay or end-to-end delay can be calculated by

End-to-end delay, $D = T_d - T_s$

Where T_d is the packet receives time at the destination and T_s is the packet sends time at source node.

When a packet is transferred from sender to receiver, the packet takes some time to reach destination which is known packet delay. If we see video on youtube then we can see buffering which happened for packet delay i.e. the packet takes much time to reach the destination. A network can be defined as good if the packet delay is minimum. To provide good service engineers have to reduce packet delay of a network. The following figures show the packet delay for MPLS & non-MPLS network both. From fig8 we can see that delay for MPLS network is approximately 0.01 sec where for non-MPLS network approximately 0.32 sec. as minimum delay is desired for a good network we can say performance of MPLS network is better than conventional IP network.

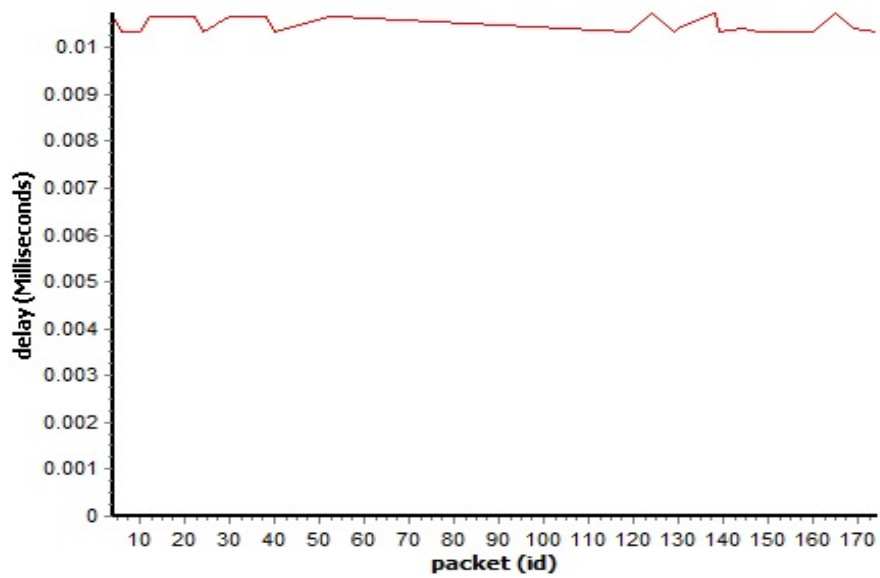


Fig 8.8: packet delay for MPLS network

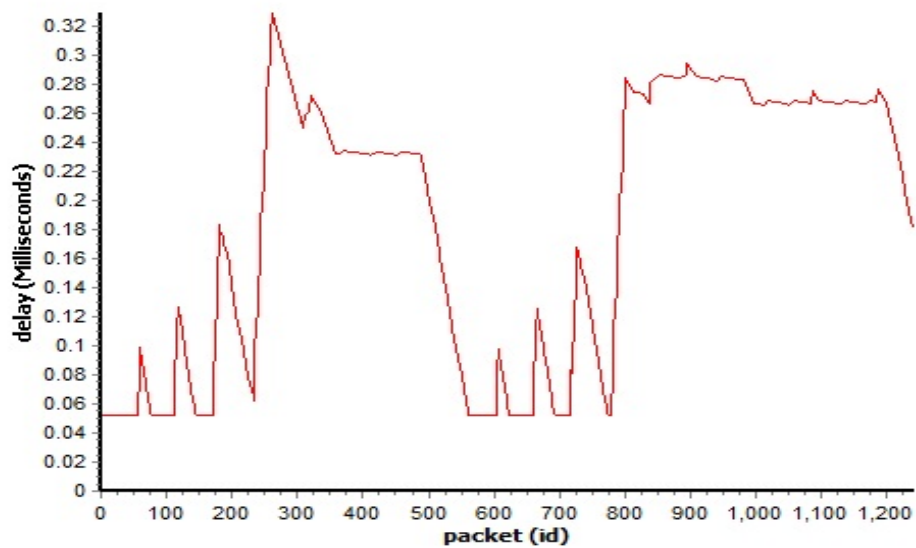


Fig 8.9: packet delay for non-MPLS network

8.4 Packet Loss Calculation

Packet loss is where network traffic fails to reach its destination in a timely manner. Most commonly packets get dropped before the destination can be reached. Packet loss can be calculated by

$$\text{Packet dropped/loss, } P_d = P_s - P_a$$

Where P_s is the amount of packet sent and P_a is the amount of packet received. The following tables show the comparison of packet drop / loss behavior for both MPLS network and non-MPLS network. Here we have done all the calculation using NS-2 visual trace analyzer.

Categories	Non-MPLS network	MPLS network
Total generated packets	1253	1137
Total received packets	717	1132
Total lost packets	536	5

Table 1: comparison of packet lost behavior

Chapter9

Conclusion

In conclusion, conventional IP network and MPLS network has been considered for evaluating the performance. The performance analysis for MPLS and IP networks is designed, tested and implemented by NS-2. The parameters like jitter, packet delay, and packet send and received, packet loss have been measured for extracting the features. Based on the simulation results it can be concluded that MPLS provides best solution compared to conventional IP networks.

Appendix

TCL scripts for MPLS network:

```

set ns [new Simulator]

set tracefile [open out.tr w]
$ns trace-all $tracefile

set nf [open out.nam w]
$ns namtrace-all $nf

proc finish {} {
global ns tracefile nf
$ns flush-trace
close $nf
close $tracefile
exec nam out.nam &
exit 0
}
set n0 [$ns node]
set n1 [$ns node]
$ns node-config -MPLS ON
set LSR(2) [$ns node]
set LSR(3) [$ns node]
set LSR(4) [$ns node]
set LSR(5) [$ns node]
set LSR(6) [$ns node]
set LSR(7) [$ns node]
set LSR(8) [$ns node]
$ns node-config -MPLS OFF
set n9 [$ns node]
set n10 [$ns node]
$ns duplex-link $n0 $LSR(2) 1Mb 10ms DropTail
$ns duplex-link $n1 $LSR(2) 1Mb 10ms DropTail
$ns duplex-link $LSR(2) $LSR(3) 0.5Mb 10ms DropTail
$ns duplex-link $LSR(3) $LSR(4) 0.5Mb 10ms DropTail
$ns duplex-link $LSR(4) $LSR(5) 0.5Mb 10ms DropTail
$ns duplex-link $LSR(5) $LSR(8) 0.5Mb 10ms DropTail
$ns duplex-link $LSR(2) $LSR(6) 1Mb 10ms SFQ
$ns duplex-link $LSR(6) $LSR(7) 0.5Mb 10ms SFQ
$ns duplex-link $LSR(7) $LSR(8) 1Mb 10ms SFQ
$ns duplex-link $LSR(8) $n9 1Mb 10ms DropTail
$ns duplex-link $LSR(8) $n10 1Mb 10ms DropTail
$ns duplex-link-op $n0 $LSR(2) queuePos 0.5
$ns duplex-link-op $n1 $LSR(2) queuePos 0.5
$ns duplex-link-op $LSR(2) $LSR(3) queuePos 0.5
$ns duplex-link-op $LSR(3) $LSR(4) queuePos 0.5
$ns duplex-link-op $LSR(4) $LSR(5) queuePos 0.5
$ns duplex-link-op $LSR(2) $LSR(6) queuePos 0.5
$ns duplex-link-op $LSR(6) $LSR(7) queuePos 0.5
$ns duplex-link-op $LSR(5) $LSR(8) queuePos 0.5
$ns duplex-link-op $LSR(7) $LSR(8) queuePos 0.5
$ns duplex-link-op $LSR(8) $n9 queuePos 0.5
$ns duplex-link-op $LSR(8) $n10 queuePos 0.5
for {set i 2} {$i<9} { incr i} {

```

```

    for {set j [expr $i+1]} {$j<9} {incr j} {
        set a LSR($i)
        set b LSR($j)
        eval $ns LDP-peer $$a $$b
    }
    set m [eval $$a get-module "MPLS"]
    $m enable-reroute "new"
}
}$ns configure-ldp-on-all-mpls-nodes
$ns ldp-request-color blue
$ns ldp-mapping-color red
$ns ldp-withdraw-color magenta
$ns ldp-release-color orange
$ns ldp-notification-color yellow
$ns color 1 Hotpink
$ns color 2 Navyblue
[$LSR(2) get-module "MPLS"] enable-control-driven
[$LSR(3) get-module "MPLS"] enable-control-driven
[$LSR(4) get-module "MPLS"] enable-control-driven
[$LSR(5) get-module "MPLS"] enable-control-driven
[$LSR(6) get-module "MPLS"] enable-control-driven
[$LSR(7) get-module "MPLS"] enable-control-driven
[$LSR(8) get-module "MPLS"] enable-control-driven
[$LSR(2) get-module "MPLS"] enable-data-driven
[$LSR(3) get-module "MPLS"] enable-data-driven
[$LSR(4) get-module "MPLS"] enable-data-driven
[$LSR(5) get-module "MPLS"] enable-data-driven
[$LSR(6) get-module "MPLS"] enable-data-driven
[$LSR(7) get-module "MPLS"] enable-data-driven
[$LSR(8) get-module "MPLS"] enable-data-driven
#[$LSR(2) get-module "MPLS"] enable-on-demand
#[$LSR(3) get-module "MPLS"] enable-on-demand
#[$LSR(4) get-module "MPLS"] enable-on-demand
#[$LSR(5) get-module "MPLS"] enable-on-demand
#[$LSR(6) get-module "MPLS"] enable-on-demand
#[$LSR(7) get-module "MPLS"] enable-on-demand
#[$LSR(8) get-module "MPLS"] enable-on-demand
#[$LSR(2) get-module "MPLS"] enable-ordered-control
#[$LSR(3) get-module "MPLS"] enable-ordered-control
#[$LSR(4) get-module "MPLS"] enable-ordered-control
#[$LSR(5) get-module "MPLS"] enable-ordered-control
#[$LSR(6) get-module "MPLS"] enable-ordered-control
#[$LSR(7) get-module "MPLS"] enable-ordered-control
#[$LSR(8) get-module "MPLS"] enable-ordered-control
}$ns enable-control-driven
#classifier/Addr/MPLS set control_driven_1
}$ns classifier/Addr/MPLS enable-data-driven
}$ns classifier/Addr/MPLS enable-on-demand
}$ns classifier/Addr/MPLS enable-ordered-control
}$ns enable-data-driven
}$ns enable-on-demand
}$ns enable-ordered-control
$ns rtproto DV
set udp0 [new Agent/UDP]
set null [new Agent/Null]
$ns attach-agent $n0 $udp0
$ns attach-agent $n9 $null

```

```

$ns connect $udp0 $null
$udp0 set class_ 1
set Src0 [new Application/Traffic/CBR]
$Src0 set packetSize_ 48
$Src0 set interval_ 0.003
$Src0 attach-agent $udp0
set tcp [new Agent/TCP]
$tcp set packetSize_ 1000
set tcpsink [new Agent/TCPSink]
$ns attach-agent $n1 $tcp
$ns attach-agent $n10 $tcpsink
$ns connect $tcp $tcpsink
$tcp set class_ 2
set Src1 [new Application/FTP]
$Src1 attach-agent $tcp
#set tfile [new Tracefile]
#$tfile filename pOct89_2000_TL.bin
#set Src1 [new Application/Traffic/Trace]
#$Src1 attach-tracefile $tfile
#$Src1 attach-agent $tcp
$ns at 0.05 "$Src0 start"
$ns at 0.1 "$Src1 start"
#$ns at 1.6 "$LSR(8) ldp-trigger-by-withdraw 9 -1"
#$ns at 1.8 "$LSR(2) make-explicit-route 8 2_3_4_5_8 3000 -1"
#$ns at 2.0 "$LSR(2) flow-erlsp-install 9 -1 3000"
#$ns at 2.8 "$LSR(2) ldp-trigger-by-release 9 3000"
$ns at 3.0 "$Src1 stop"
$ns at 3.0 "$Src0 stop"
$ns at 3.2 "finish"
$ns run

```

TCL scripts for non-MPLS network:

```

set ns [new Simulator]
set tracefile [open out1.tr w]
$ns trace-all $tracefile
set nf [open out1.nam w]
$ns namtrace-all $nf
proc finish {} {
  global ns tracefile nf
  $ns flush-trace
  close $nf
  close $tracefile
  exec nam out1.nam &
  exit 0
}
set n0 [$ns node]
set n1 [$ns node]
#$ns node-config -MPLS ON
set n2 [$ns node]
set n3 [$ns node]
set n4 [$ns node]
set n5 [$ns node]
set n6 [$ns node]

```

```

set n7 [$ns node]
set n8 [$ns node]
#$ns node-config -MPLS OFF
set n9 [$ns node]
set n10 [$ns node]
$ns duplex-link $n0 $n2 1Mb 10ms DropTail
$ns duplex-link $n1 $n2 1Mb 10ms DropTail
$ns duplex-link $n2 $n3 0.5Mb 10ms DropTail
$ns duplex-link $n3 $n4 0.5Mb 10ms DropTail
$ns duplex-link $n4 $n5 0.5Mb 10ms DropTail
$ns duplex-link $n5 $n8 0.5Mb 10ms DropTail
$ns duplex-link $n2 $n6 1Mb 10ms SFQ
$ns duplex-link $n6 $n7 0.5Mb 10ms SFQ
$ns duplex-link $n7 $n8 1Mb 10ms SFQ
$ns duplex-link $n8 $n9 1Mb 10ms DropTail
$ns duplex-link $n8 $n10 1Mb 10ms DropTail
$ns duplex-link-op $n0 $n2 queuePos 0.5
$ns duplex-link-op $n1 $n2 queuePos 0.5
$ns duplex-link-op $n2 $n3 queuePos 0.5
$ns duplex-link-op $n3 $n4 queuePos 0.5
$ns duplex-link-op $n4 $n5 queuePos 0.5
$ns duplex-link-op $n2 $n6 queuePos 0.5
$ns duplex-link-op $n6 $n7 queuePos 0.5
$ns duplex-link-op $n5 $n8 queuePos 0.5
$ns duplex-link-op $n7 $n8 queuePos 0.5
$ns duplex-link-op $n8 $n9 queuePos 0.5
$ns duplex-link-op $n8 $n10 queuePos 0.5
#for {set i 2} {$i<9} { incr i} {
    #for {set j [expr $i+1]} {$j<9} {incr j} {
        #set a LSR($i)
        #set b LSR($j)
        #eval $ns LDP-peer $$a $$b
    }
}
#$ns configure-ldp-on-all-mpls-nodes
#$ns ldp-request-color blue
#$ns ldp-mapping-color red
#$ns ldp-withdraw-color magenta
#$ns ldp-release-color orange
#$ns ldp-notification-color yellow
$ns color 1 Hotpink
$ns color 2 Navyblue
#$ns enable-control-driven
#$ns enable-data-driven
#$ns enable-on-demand
#$ns enable-ordered-control
#$ns rtproto DV
set udp0 [new Agent/UDP]
set null [new Agent/Null]
$ns attach-agent $n0 $udp0
$ns attach-agent $n9 $null
$ns connect $udp0 $null
$udp0 set class_ 1
set Src0 [new Application/Traffic/CBR]
$Src0 set packetSize_ 48
$Src0 set interval_ 0.003
$Src0 attach-agent $udp0

```

```
set tcp [new Agent/TCP]
$tcp set packetSize_ 1000
set tcpsink [new Agent/TCPSink]
$ns attach-agent $n1 $tcp
$ns attach-agent $n10 $tcpsink
$ns connect $tcp $tcpsink
$tcp set class_ 2
set Src1 [new Application/FTP]
$Src1 attach-agent $tcp
#set tfile [new Tracefile]
#$tfile filename pOct89_2000_TL.bin
#set Src1 [new Application/Traffic/Trace]
#$Src1 attach-tracefile $tfile
#$Src1 attach-agent $tcp
$ns at 0.05 "$Src0 start"
$ns at 0.1 "$Src1 start"
#$ns at 1.6 "$LSR(8) ldp-trigger-by-withdraw 9 -1"
#$ns at 1.8 "$LSR(2) make-explicit-route 8 2_3_4_5_8 3000 -1"
#$ns at 2.0 "$LSR(2) flow-erlsp-install 9 -1 3000"
#$ns at 2.8 "$LSR(2) ldp-trigger-by-release 9 3000"
$ns at 3.0 "$Src1 stop"
$ns at 3.0 "$Src0 stop"
$ns at 3.2 "finish"
$ns run
```

References

- [1] J. Reagan, "CCIP: MPLS Study Guide", 2002.
- [2] S. Alvarez, "QoS for IP/MPLS network", June 2006
- [3] D. Minoli, "Voice Over MPLS: Planning and Designing Networks", 2002
- [4] J. Guichard and I. Pepelnjak, "MPLS and VPN Architecture", October 2000
- [5] M.A. Miller, "Internet Technology Handbook", Optimizing the IP Net, 2004-
- [6] Adrain Farrel, The internet and its Protocols: A comparative Approach
- [7] K. Rao, Z. S. Bojkovic, and D. A. Milovanovic, "Multimedia Communication: Application, Middleware, Networking", 2006
- [8] S. Halabi, D. McPherson, "Internet routing architectures", 2nd edition, August 2000
- [9] P. Ferguson and G. Huston, "Quality Of Service: Delivering QoS on internet and Corporate networks", 1998.
- [10] M. Guizani, "wireless communication system and networks", 2004.
- [11] R. Perlman, "Interconnections: Bridges, Routers, Switches and Internetworking Protocols", 2nd edition 2003.
- [12] Request for Comments 2453, "Routing Information Protocol", Version 2, Network Working Group. [Online] Available: [HTTP://www.faqs.org/rfcs/rfc1058.html](http://www.faqs.org/rfcs/rfc1058.html)
- [13] Request for Comments 904, "Exterior Gateway Protocol Formal Specification", Network Working Group. [Online] Available: <http://www.faqs.org/rfcs/rfc904.html>
- [14] Request for Comments 1771, "A Border Gateway Protocol", Network Working Group. [Online] Available: <http://www.faqs.org/rfcs/rfc1771.html>
- [15] Request for Comments 3036, "LDP Specification", Network Working Group. [Online] Available: <http://www.faqs.org/rfcs/rfc3036.html>
- [16] Request for Comments 3037, "LDP Applicability", Network Working Group. [Online] Available: <http://www.faqs.org/rfcs/rfc3037.html>
- [17] A. S. Tanenbaum, "Computer Network", 4th edition, March 2003.
- [18] A. Rahman, A. Haque, K.A.M Lutfullah, M. Zahedul Hassan, M.R. Amin, "Performance Analysis and the Study of the behaviour of MPLS Protocol"
- [19] J. Barakovic, H. Bajric, A. Husic "QoS design issues and traffic engineering in next generation IP/MPLS network", June 2007.
- [20] http://www.cisco.com/en/US/tech/tk436/tk428/technologies_configuration_examples/e09186a00800a6c11.shtml
- [21] <http://www.iec.org/online/tutorials/vpn/index.asp>

[22] KeerthiPramukh Jannu, Radhakrishna Deekonda “OPNET simulation of voice over MPLS With

Considering Traffic Engineering ” School of Engineering, Blekinge Institute of Technology , Thesis no: MSE 2010-5311 , June 2010