

FOUNDATIONAL RESEARCH OF INTERARRIVAL  
PACKET JITTER FOR HOMOGENOUS CBR  
TRAFFIC IN MPLS NETWORKS

By

LIJY JOSE KALLIDUKIL

Bachelor of Engineering

Bharathiar University

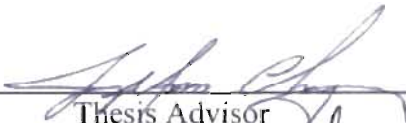
Coimbatore, India

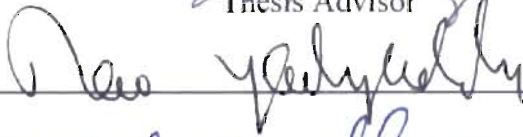
1991

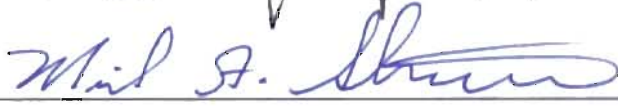
Submitted to the Faculty of the  
Graduate College of the  
Oklahoma State University  
in partial fulfillment of  
the requirements for  
the Degree of  
MASTER OF SCIENCE  
December, 2001


FOUNDATIONAL RESEARCH OF INTERARRIVAL  
PACKET JITTER FOR HOMOGENOUS CBR  
TRAFFIC IN MPLS NETWORKS

Thesis Approved:

  
\_\_\_\_\_  
Thesis Advisor

  
\_\_\_\_\_  
Neil Yeddyby

  
\_\_\_\_\_  
Mil A. Kumar

  
\_\_\_\_\_  
Dean of the Graduate College

## PREFACE

A great deal of interest revolves around the possibility of using Internet Protocol based networks to provide multiple classes of service to various types of traffic such as voice, data and video[3]. A key protocol that is expected to make possible this capability is Multiprotocol Label Switching (MPLS).

Multiprotocol Label Switching (MPLS) is a technique that brings most of the qualities and attributes of switched networks to Internet Protocol (IP) networks. MPLS is a flexible solution that addresses the problems faced by the IP networks of today - speed, scalability, Quality of Service (QoS) management and traffic engineering. MPLS can exist over existing asynchronous transfer mode (ATM) and frame-relay networks[3]. It is an well-designed solution to meet the bandwidth-management and service requirements of next generation IP based backbone networks.

In this thesis we examine the jitter performance of differentiated services in MPLS networks. In order to derive the effects of interarrival packet jitter in MPLS networks applying differentiated services, the derivation of the Jitter probability becomes the essential building block. In this thesis we define how to derive this jitter probability.

## ACKNOWLEDGMENTS

I wish to express my deep and sincere thanks and gratitude to my advisor Dr. Jong-Moon Chung for his supervision, support, critical suggestions, and inspiration without whom this thesis would not have been possible. . My appreciation and thanks are also due to my committee members, Dr. R. K. Yarlagadda and Dr. Michael A. Soderstrand for their support, assistance, encouragement and guidance throughout my Master's program here at the Oklahoma State University.

I would like to thank the Advanced Communication Systems Engineering Laboratories (ACSEL) at the Oklahoma State University for supporting resources. I would like to thank my group members for their contribution. I would also like to thank other members of the ACSEL laboratories for their recommendations and support and my friends who made my thesis work an enjoyable and pleasant one.

Finally, I would like to thank my husband Jojo John for his support and encouragement.

## TABLE OF CONTENTS

Chapter	Page
I. INTRODUCTION.....	1
1.1 A brief overview of MPLS.....	1
1.2 A brief overview of Signaling Mechanisms.....	2
1.2.1 RSVP Signaling.....	2
1.2.2 CR-LDP Signaling.....	2
1.3 Motivation for Research.....	3
1.4 Thesis Outline.....	3
II.LITERATURE REVIEW.....	5
2.1 MPLS.....	5
2.2 Components of MPLS.....	5
2.2.1 Label Switched Routers and Label Edged Routers.....	6
2.2.2 Forward Equivalence Class.....	7
2.2.3 Labels and label bindings.....	7
2.2.4 Label creation.....	9
2.2.5 Label distribution.....	9
2.2.6 Label Switched Paths.....	10
2.2.7 Label spaces.....	11
2.2.8 Label merging.....	11
2.2.9 Label retention.....	12
2.2.10 Label control.....	12
2.2.11 Signaling Mechanisms.....	13
2.2.12 Label Distribution Protocol.....	13
2.2.13 Traffic Engineering.....	14
2.3 MPLS operation.....	15
2.3.1 MPLS actions.....	15
2.3.2 Tunneling in MPLS.....	18
2.4 Applications of MPLS.....	19
III. LITERATURE REVIEW.....	21
3.1 RSVP.....	21
3.2 Extensions to RSVP for LSP Tunnels.....	22
3.3 LSP Tunnels.....	23
3.3.1 Traffic Engineered Tunnels.....	23
3.4 LSP Tunnel related message Format.....	24

Chapter	Page
3.4.1 Path Message –E-RSVP.....	24
3.4.2 Resv Message –E-RSVP.....	25
3.5 Operation of LSP Tunnels.....	26
3.5.1 Rerouting traffic Engineered Tunnels.....	28
3.6 LSP Tunnel related object .....	29
3.6.1 Label Object .....	29
3.6.2 Label request object .....	29
3.6.2.1 Label request without label range .....	29
3.6.2.2 Label request with ATM label range .....	30
3.6.2.3 Label request with Frame relay label range .....	31
3.7 Explicit Route Object.....	32
3.8 Record Route Object.....	33
3.9 Session Object.....	33
3.9.1 LSP_Tunnel_IPv4 session object.....	33
3.9.2 LSP_Tunnel_IPv6 session object.....	34
3.10 Sender Template Object.....	34
3.10.1 LSP_Tunnel_IPv4 sender template object.....	34
3.10.2 LSP_Tunnel_IPv6 sender template object.....	35
3.11 Filter Specification object.....	35
3.11.1LSP_Tunnel_IPv4 filter specification object.....	35
3.12 Hello Extension.....	35
 IV. LITERATURE REVIEW.....	 37
4.1 Constraint-Based LSP setup using LDP.....	37
4.1.1 Strict and Loose explicit routes.....	37
4.1.2 Traffic Characteristics.....	38
4.1.3 Pre-emption.....	38
4.1.4 Route Pinning.....	39
4.2 Label Request Message.....	39
4.3 Label Mapping Message.....	40
4.4 Notification Message.....	41
4.5 Release , Withdraw and Abort Message.....	42
4.6 Protocol Specification.....	42
4.6.1 Explicit Route TLV (ER-TLV).....	42
4.6.2 Explicit Route hop TLV (ER-hopTLV).....	43
4.6.3 Traffic Parameters TLV.....	44
4.6.3.1 Frequency.....	47
4.6.3.2 Peak Rate.....	47
4.6.3.3 Committed Rate.....	47
4.6.3.4 Excess Burst Size.....	48
4.6.3.5 Peak rate token bucket.....	48
4.6.3.6 Committed data rate token bucket.....	48

Chapter	Page
4.6.3.7 Weight.....	49
4.6.4 Procedures.....	49
4.6.4.1 Label Request Message.....	49
4.6.4.2 Label Mapping Message.....	50
4.6.4.3 Notification Message.....	51
4.7 Preemption TLV.....	51
4.8 LSPID TLV.....	52
4.9 Resource Class TL.....	52
 V.INTERARRIVAL PACKET JITTER IN MPLS NETWORKS.....	 54
5.1 System Model.....	55
5.2 Performance Analysis.....	57
5.3 Proof & Explanations.....	58
 VI.OBSERVATIONS AND RESULTS .....	 62
 VII CONCLUSION AND RESULTS .....	 66
 REFERENCES.....	 68

## LIST OF TABLES

Table	Page
3-1 LSP Tunnel related message format.....	24
3-2 Format of PATH message E-RSVP.....	24
3-3 Format of RESV message E-RSVP.....	25
2-4 Format of Label object.....	29
3-4 Format of label request object without label range.....	30
3-5 Format of label request with ATM label.....	30
3-6 Format of label request with Frame relay.....	31
3-7 Format of Explicit route object.....	32
3-8 Format of LSP_Tunnel_Ipv4 session object.....	33
3-9 Format of LSP_Tunnel_Ipv4 sender template object.....	34
4-1 Encoding for CR-LDP Label request message.....	40
4-2 Encoding for CR-LDP Label Mapping Message.....	41
4-3 Encoding for CR-LDP Notification Message.....	42
4-4 Explicit Route TLV.....	43
4-5 Explicit Route hop TLV.....	43
4-6 Traffic Parameter TLV.....	44
4-7 Flag Fields of Traffic Parameter TLV.....	45
4-8 Resource Class TLV.....	53
4-9 The Distribution of Centered jitter for homogenous CBR traffic .....	65



## LIST OF FIGURES

Figure	Page
2-1 MPLS Generic Label Format.....	6
2-2 Signaling Mechanism.....	13
2-3 LSP Creation and Packet Forwarding through a MPLS Domain.....	16
2-4 Tunneling in MPLS.....	18
3-1 Path Message and RESV message across a MPLS network.....	26
5-1 The Queuing Model.....	55
5-2 Time Slot assignment diagram .....	58
5-3 Discrete Triangular density shown for $K=5$ .....	60
6-1 Jitter Variance for various values of $T$ and $N$ .....	62
6-2 Jitter Variance for fully utilized system.....	63
6-3 Jitter Histogram for $T=32$ and various values of $N$ .....	64

# CHAPTER I

## INTRODUCTION

### 1.1 A Brief Overview of MPLS

As recent history tells us , bandwidth doubles and sometimes quadruples every nine to twelve months[1]. Within the next three to five years ,ultra-high bandwidth networks will be provided and matching data transferring topologies as well as improved system reliability will become a necessity[1]. MPLS has been emerging as the protocol of the future because of its multiprotocol architecture. MPLS utilizes a simple label switching mechanism where it's versatility in application exists. Through utilizing classification, queue and scheduling (CQS) traffic Engineering topologies MPLS is capable of providing controllable quality of service (QoS) features. MPLS provides a solution to scalability and enables significant flexibility in routing. The connection oriented architecture and QoS reliability features easily enable high quality end-to-end service features that are necessary in applications such as virtual private networks (VPN).[4]

MPLS is designed to meet all the mandatory characteristics of large scale carrier class networks. It is evolutionary in the sense that it uses existing layer 3 routing protocol as well as all the widely available layer 2 transport mechanism and protocols , such as ATM , frame relay, leased lines/PPP and Ethernet . MPLS solves the problem of how to integrate the best attributes of traditional layer 2 and layer 3 technologies[3].

## **1.2 A Brief Overview of Signaling Mechanism**

### **1.2.1 RSVP Signaling**

RSVP is a soft state protocol which uses PATH AND RESV commands to establish a LSP. In RSVP, based on the destination IP address and protocol ID, packets are transferred based on raw IP datagram routing[1][3]. The ingress LSR uses a PATH message to inform every router along the selected LSP to acknowledge that this is a desired LSP to be established[1][3]. Following this, the receiving LSR will use the RESV message with traffic and QoS parameters traversing upstream to reserve the resources on each node along the desired LSP[1][3]. The node along the LSP will install the reservation for the related state by creating an entry on the label forwarding table. At every node along the path , the PATH and RESV messages are used periodically to referesh the path and reservation states[1][3].

Extensions to RSVP( E-RSVP) have been made and proposed to support ER-LSP as well as provide additional features to RSVP. E-RSVP has been proposed to support both strict and loose explicit routed LSPs (ER-LSP). For the loose segment in the ER-LSP , the hop-by-hop routing can be employed to determine where to send the PATH message[1][3].

### **1.2.1 CR-LDP Signaling**

CR-LDP standards attempt to enable the LSP protocol to work over an explicit route, transporting various traffic parameters for resource reservation as well as options for CR-LSP robustness features[1][3]. Both LDP and CR-LDP are hard state protocols,

where signaling messages are transmitted once without any refreshing –information requirements. The transport mechanism for peer discovery is UDP, while TCP is used for session, advertisement, notification, and LDP messages. To setup an explicit route, a LABEL REQUEST message containing a list of nodes along the constraint-based route to be traversed is sent. The signaling message will be sent to the destination following the selected path and if the the requested path is able to satisfy the requirements , labels are allocated and distributed by means of LABEL MAPPING message starting with the destination and propagating in the reverse direction back to the source.CR-LDP is capable of establishing both strict and loose path setups with setup and holding priority , path preemption, and path re-optimization[1].

### **1.3 Motivation For the Research**

A vast amount of research exists regarding estimating packet delivery delay, but there seems to be a paucity of information in the literature regarding packet jitter[3]. For many of the proposed high quality internet service such as interactive voice , or video streaming , control of jitter can be just as important as control of network delivery delay.

This thesis will seek to identify the inter-arrival packet jitter for homogenous CBR traffic in MPLS networks for differentiated services. A solid understanding will be gained on the probability of jitter within MPLS networks for differentiated services of constant bit rate traffic.

### **1.3 Thesis Outline**

In this thesis , Chapter 2 provides a literature review on MPLS . Chapter 3 provides a literature review on RSVP and Extensions to RSVP. Chapter 4 provides a literature review on CR-LDP. Chapter 5 discusses about jitter and how the analysis can be done in a MPLS network for homogeneous CBR data traffic. Chapter 6 gives the observation and results for the analysis done. Chapter 7 provides the conclusion of the research and suggestion for future work.

## **CHAPTER II**

### **LITERATURE REVIEW**

#### **2.1 Multiprotocol label switching**

Multiprotocol label switching (MPLS) is a versatile solution to address the problems faced by present-day networks—speed, scalability, quality-of-service (QoS) management, and traffic engineering[5][8]. MPLS has emerged as an elegant solution to meet the bandwidth-management and service requirements for next-generation Internet protocol (IP)–based backbone networks. MPLS addresses issues related to scalability and routing (based on QoS and service quality metrics) and can exist over existing asynchronous transfer mode (ATM) and frame-relay networks[4].

#### **2.2 Components Of MPLS**

MPLS is an Internet Engineering Task Force (IETF)–specified framework that provides for the efficient designation, routing, forwarding, and switching of traffic flows through the network.

MPLS performs the following functions[8]:

- specifies mechanisms to manage traffic flows of various granularities, such as flows between different hardware, machines, or even flows between different applications
- remains independent of the Layer-2 and Layer-3 protocols

- provides a means to map IP addresses to simple, fixed-length labels used by different packet-forwarding and packet-switching technologies
- interfaces to existing routing protocols such as resource reservation protocol (RSVP) and open shortest path first (OSPF)
- supports the IP, ATM, and frame-relay Layer-2 protocols

In MPLS, data transmission occurs on label-switched paths (LSPs). LSPs are a sequence of labels at each and every node along the path from the source to the destination. LSPs are established either prior to data transmission (control-driven) or upon detection of a certain flow of data (data-driven). The labels, which are underlying protocol-specific identifiers, are distributed using label distribution protocol (LDP) or RSVP or piggybacked on routing protocols like border gateway protocol (BGP) and OSPF. Each data packet encapsulates and carries the labels during their journey from source to destination. High-speed switching of data is possible because the fixed-length labels are inserted at the very beginning of the packet or cell and can be used by hardware to switch packets quickly between links[5][8].

### **2.2.1 Label Switched routers and Label Edge Routers [5][8]**

The devices that participate in the MPLS protocol mechanisms can be classified into label edge routers (LERs) and label switching routers (LSRs). An LSR is a high-speed router device in the core of an MPLS network that participates in the establishment of LSPs using the appropriate label signaling protocol and high-speed switching of the data traffic based on the established paths.

An LER is a device that operates at the edge of the access network and MPLS network. LERs support multiple ports connected to dissimilar networks (such as frame relay, ATM, and Ethernet) and forwards this traffic on to the MPLS network after establishing LSPs, using the label signaling protocol at the ingress and distributing the traffic back to the access networks at the egress. The LER plays a very important role in the assignment and removal of labels, as traffic enters or exits an MPLS network.

### **2.2.2 Forward Equivalence Class [5][8]**

The forward equivalence class (FEC) is a representation of a group of packets that share the same requirements for their transport. All packets in such a group are provided the same treatment en route to the destination. As opposed to conventional IP forwarding, in MPLS, the assignment of a particular packet to a particular FEC is done just once, as the packet enters the network. FECs are based on service requirements for a given set of packets or simply for an address prefix. Each LSR builds a table to specify how a packet must be forwarded. This table, called a label information base (LIB), is comprised of FEC-to-label bindings.

### **2.2.3 Labels and Label Bindings [5][8]**

A label, in its simplest form, identifies the path a packet should traverse. A label is carried or encapsulated in a Layer-2 header along with the packet. The receiving router examines the packet for its label content to determine the next hop. Once a packet has been labeled, the rest of the journey of the packet through the backbone is based on label switching. The label values are of local significance only, meaning that they pertain only to hops between LSRs.



Once a packet has been classified as a new or existing FEC, a label is assigned to the packet. The label values are derived from the underlying data link layer. For data link layers (such as frame relay or ATM), Layer-2 identifiers, such as data link connection identifiers (DLCIs) in the case of frame-relay networks or virtual path identifiers (VPIs)/virtual channel identifiers (VCIs) in case of ATM networks, can be used directly as labels. The packets are then forwarded based on their label value.

Labels are bound to an FEC as a result of some event or policy that indicates a need for such binding. These events can be either data-driven bindings or control-driven bindings. The latter is preferable because of its advanced scaling properties that can be used in MPLS.

Label assignment decisions may be based on forwarding criteria such as the following[5]:

- destination unicast routing
- traffic engineering
- multicast
- virtual private network (VPN)
- QoS

The generic label format is illustrated in Figure 2-1.

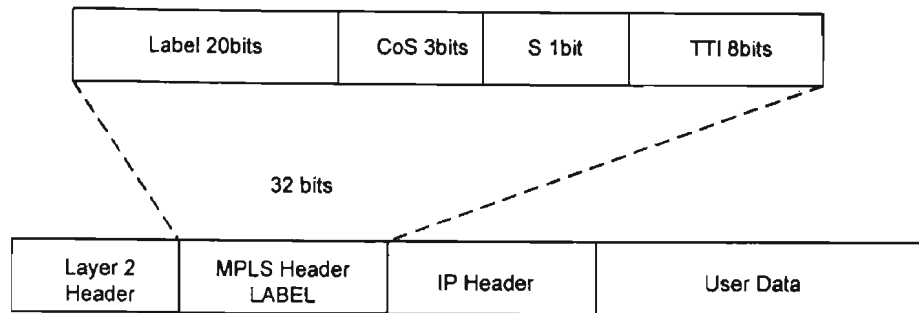


Figure 2-1. MPLS Generic Label Format

### 2.2.4 Label Creation

There are several methods used in label creation[8]:

- **topology-based method**—uses normal processing of routing protocols (such as OSPF and BGP)
- **request-based method**—uses processing of request-based control traffic (such as RSVP)
- **traffic-based method**—uses the reception of a packet to trigger the assignment and distribution of a label

The topology- and request-based methods are examples of control-driven label bindings, while the traffic-based method is an example of data-driven bindings.

### 2.2.5 Label Distribution [5][8]

MPLS architecture does not mandate a single method of signaling for label distribution. Existing routing protocols, such as the border gateway protocol (BGP), have been enhanced to piggyback the label information within the contents of the protocol.

The RSVP has also been extended to support piggybacked exchange of labels. The Internet Engineering Task Force (IETF) has also defined a new protocol known as the label distribution protocol (LDP) for explicit signaling and management of the label space. Extensions to the base LDP protocol have also been defined to support explicit routing based on QoS and CoS requirements. These extensions are captured in the constraint-based routing (CR)-LDP protocol definition.

A summary of the various schemes for label exchange is as follows:

- **LDP**—maps unicast IP destinations into labels
- **RSVP, CR-LDP**—used for traffic engineering and resource reservation
- **protocol-independent multicast (PIM)**—used for multicast states label mapping
- **BGP**—external labels (VPN)

#### 2.2.6 Label-Switched Paths (LSPs) [5][8]

Within an MPLS domain, a path is set up for a given packet to travel based on an FEC. The LSP is set up prior to data transmission. MPLS provides the following two options to set up an LSP.

- **hop-by-hop routing**—Each LSR independently selects the next hop for a given FEC. This methodology is similar to that currently used in IP networks. The LSR uses any available routing protocols, such as OSPF, ATM private network-to-network interface (PNNI), etc.

- **explicit routing**—Explicit routing is similar to source routing. The ingress LSR (i.e., the LSR where the data flow to the network first starts) specifies the list of nodes through which the ER–LSP traverses. The path specified could be nonoptimal, as well. Along the path, the resources may be reserved to ensure QoS to the data traffic. This eases traffic engineering throughout the network, and differentiated services can be provided using flows based on policies or network management methods.

The LSP setup for an FEC is unidirectional in nature. The return traffic must take another LSP.

### 2.2.7 Label Spaces [5][8]

The labels used by an LSR for FEC–label bindings are categorized as follows[5][8]:

- **per platform**—The label values are unique across the whole LSR. The labels are allocated from a common pool. No two labels distributed on different interfaces have the same value.
- **per interface**—The label ranges are associated with interfaces. Multiple label pools are defined for interfaces, and the labels provided on those interfaces are allocated from the separate pools. The label values provided on different interfaces could be the same.

### 2.2.8 Label Merging [5][8]

The incoming streams of traffic from different interfaces can be merged together and switched using a common label if they are traversing the network towards the same final destination. This is known as stream merging or aggregation of flows.

If the underlying transport network is an ATM network, LSRs could employ virtual path (VP) or virtual channel (VC) merging. In this scenario, cell interleaving problems, which arise when multiple streams of traffic are merged in the ATM network, need to be avoided.

### 2.2.9 Label Retention [5][8]

MPLS defines the treatment for label bindings received from LSRs that are not the next hop for a given FEC. Two modes are defined[5][8].

- **conservative**—In this mode, the bindings between a label and an FEC received from LSRs that are not the next hop for a given FEC are discarded. This mode requires an LSR to maintain fewer labels. This is the recommended mode for ATM-LSRs.
- **liberal**—In this mode, the bindings between a label and an FEC received from LSRs that are not the next hop for a given FEC are retained. This mode allows for quicker adaptation to topology changes and allows for the switching of traffic to other LSPs in case of changes.

### 2.2.10 Label Control [5][8]

MPLS defines modes for distribution of labels to neighboring LSRs.

- **independent**—In this mode, an LSR recognizes a particular FEC and makes the decision to bind a label to the FEC independently to distribute the binding to its peers. The new FECs are recognized whenever new routes become visible to the router.

- **ordered**—In this mode, an LSR binds a label to a particular FEC if and only if it is the egress router or it has received a label binding for the FEC from its next hop LSR. This mode is recommended for ATM-LSRs.

### 2.2.11 Signaling Mechanisms [5][8]

- **label request**—Using this mechanism, an LSR requests a label from its downstream neighbor so that it can bind to a specific FEC. This mechanism can be employed down the chain of LSRs up until the egress LER (i.e., the point at which the packet exits the MPLS domain).
- **label mapping**—In response to a label request, a downstream LSR will send a label to the upstream initiator using the label mapping mechanism.

The above concepts for label request and label mapping are explained in Figure 2-2.

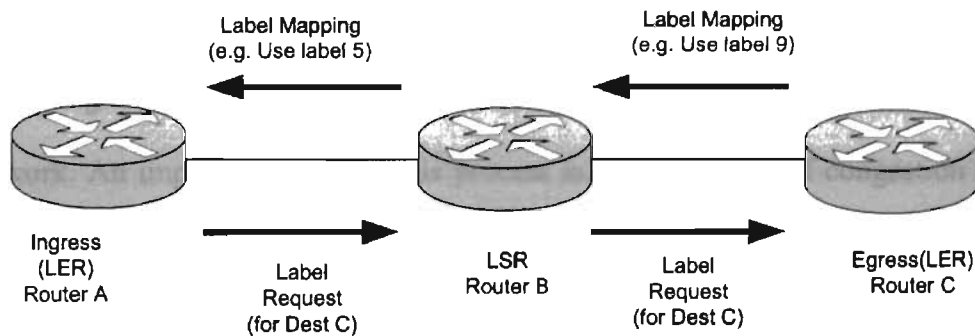


Figure 2-2. Signaling Mechanisms

### 2.2.12 Label Distribution Protocol (LDP) [5][8]

The LDP is a new protocol for the distribution of label binding information to LSRs in an MPLS network. It is used to map FECs to labels, which, in turn, create LSPs. LDP

sessions are established between LDP peers in the MPLS network (not necessarily adjacent). The peers exchange the following types of LDP messages[5][8]:

- **discovery messages**—announce and maintain the presence of an LSR in a network
- **session messages**—establish, maintain, and terminate sessions between LDP peers
- **advertisement messages**—create, change, and delete label mappings for FECs
- **notification messages**—provide advisory information and signal error information

### 2.2.13 Traffic Engineering [5][8]

Traffic engineering is a process that enhances overall network utilization by attempting to create a uniform or differentiated distribution of traffic throughout the network. An important result of this process is the avoidance of congestion on any one path. It is important to note that traffic engineering does not necessarily select the shortest path between two devices. It is possible that, for two packet data flows, the packets may traverse completely different paths even though their originating node and the final destination node are the same. This way, the less-exposed or less-used network segments can be used and differentiated services can be provided.

In MPLS, traffic engineering is inherently provided using explicitly routed paths. The LSPs are created independently, specifying different paths that are based on user-

defined policies. However, this may require extensive operator intervention. RSVP and CR-LDP are two possible approaches to supply dynamic traffic engineering and QoS in MPLS.

### **2.3 MPLS Operation [5][8]**

The following steps must be taken for a data packet to travel through an MPLS domain.

- label creation and distribution
- table creation at each router
- label-switched path creation
- label insertion/table lookup
- packet forwarding

The source sends its data to the destination. In an MPLS domain, not all of the source traffic is necessarily transported through the same path. Depending on the traffic characteristics, different LSPs could be created for packets with different CoS requirements.

#### **2.3.1 MPLS Actions [5][8]**

1. **Label Creation and Distribution:** The routers make decision to bind a label to a specific FEC before the flow of any traffic begins and they build their tables. Downstream routers in LDP initiate the distribution of labels and label/FEC binding. The traffic-related characteristics and MPLS capabilities are negotiated using LDP. LDP uses TCP as a reliable and ordered transport protocol.



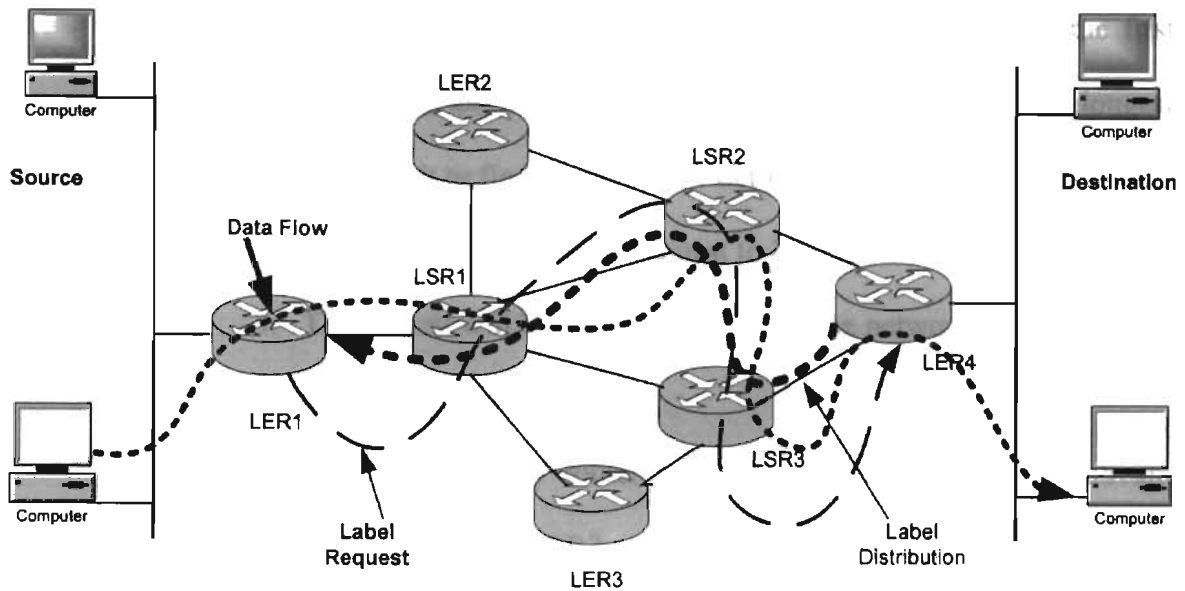


Figure 2-3 LSP Creation and Packet Forwarding through a MPLS Domain

2. Table creation: When an LSR receives label bindings, it creates label information base (LIB). The contents of this table specify the mapping between a label and an FEC.
3. Label switched path creation: The mid thick lines in figure 4-2 show the creation of LSPs. The LSPs are created in a direction reverse to the creation of entries in the LIBs.
4. Label insertion/table lookup: The first router (LER1 in figure 4-2) uses the LIB table to find the next hop and request a label for a specific FEC. Subsequent routers just use the label to find the next hop. Once the packet reaches the egress LSR (LER4), the label is removed and the packet is supplied to the destination.
5. Packet Forwarding: The path of a packet is examined with reference to figure2. The path is from the ingress LSR, LER1, to the egress LSR, LER4.

1. LER1 may not have any labels for this packet, as it is the first occurrence of this request. In an IP network, it will find the longest address match to find the next hop. Let LSR1 be the next hop.
2. LER1 will initiate a label request to LSR1.
3. The request will be propagated through the network as indicated by the least thick lines.
4. Each intermediary router receives a label from its downstream router starting from LER2 and going upstream until LER1. The mid thick lines using any signaling protocol like, for example, LDP indicate the LSP setup.
5. LER1 inserts the label and forwards the packet to LSR1.
6. Each subsequent LSR examines the label in the received packet and replaces it with the outgoing label and forwards it.
7. When the packet reaches LER4, it removes the label as the packet is departing from an MPLS domain and delivers it to the destination.
8. The thickest lines indicate the actual data path.

### **2.3.2 Tunneling in MPLS [5][8]**

A unique feature of MPLS is that it can control the entire path of a packet without explicitly specifying the intermediate routers. It does this by creating tunnels through the intermediary routers that can span multiple segments. This concept is used in provisioning MPLS-based VPNs.

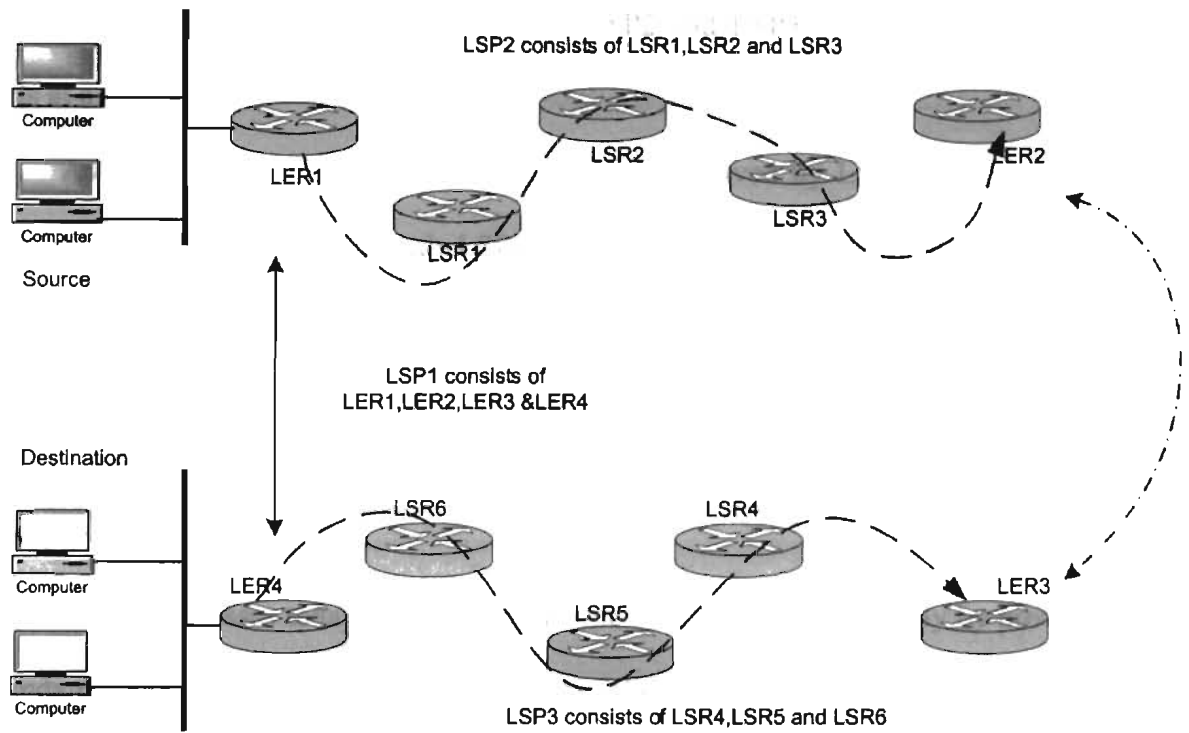


Figure 2-4. Tunneling in MPLS

Consider the figure above. LERs (LER1, LER2, LER3 and LER4) use BGP and create an LSP between them, which is LSP1 as shown in figure1- 4. These LERs use LDP to receive and store labels from the egress LER (LER4) all the way to the ingress router (LER1).

Nevertheless, for LER1 to send its data to LER2, it must go through 3 LERs. Therefore, a separate LSP (LSP2 in figure 4-3) is created between LER1 and LER2 and this spans LSR1, LSR2 and LSR3. This represents a tunnel between the two LSRs. The labels used in this path are different from the labels that the LERs created for LSP1. This is also true for LER3 and LER4 and for LSRs in between them. LSP3 is created for this particular segment. Label stack is used when transporting the packet through two network

segments. As a packet travels through LSP1, LSP2 and LSP3 it carries two complete labels at a time.

As the packet exists the first network and is received by LER3, it removes the label for LSP2 and replaces it with LSP3 label, also swapping LSP1 label within the packet with the next hop label. LER4 removes both labels before it sends the packet to the destination.

## **2.4 MPLS Applications [5][8]**

MPLS addresses today's network backbone requirements effectively by providing a standards-based solution that accomplishes the following[3][5][8]:

1. Improves packet-forwarding performance in the network
  - MPLS enhances and simplifies packet forwarding through routers using Layer-2 switching paradigms.
  - MPLS is simple, which allows for easy implementation.
  - MPLS increases network performance because it enables routing by switching at wireline speeds.
2. Supports QoS and CoS for service differentiation
  - MPLS uses traffic-engineered path setup and helps achieve service-level guarantees.
  - MPLS incorporates provisions for constraint-based and explicit path setup.
3. Supports network scalability
4. Integrates IP and ATM in the network

- MPLS provides a bridge between access IP and core ATM.
- MPLS can reuse existing router/ATM switch hardware, effectively joining the two disparate networks.

#### 5. MPLS interoperable networks

- It achieves synergy between IP and ATM networks.
- It facilitates IP-over-synchronous optical network (SONET) integration in optical switching.
- It helps build scalable VPNs with traffic-engineering capability.

## CHAPTER III

### LITERATURE REVIEW

#### 3.1 RSVP

The RSVP protocol is used by a host to request specific qualities of service from the network for particular application data streams or flows[3]. RSVP is also used by routers to deliver quality-of-service (QoS) requests to all nodes along the path(s) of the flows and to establish and maintain state to provide the requested service. RSVP requests will generally result in resources being reserved in each node along the data path.

RSVP requests resources for simplex flows, i.e., it requests resources in only one direction. Therefore, RSVP treats a sender as logically distinct from a receiver, although the same application process may act as both a sender and a receiver at the same time. RSVP operates on top of IPv4 or IPv6, occupying the place of a transport protocol in the protocol stack. However, RSVP does not transport application data but is rather an Internet control protocol, like ICMP, IGMP, or routing protocols[3].

RSVP is not itself a routing protocol; RSVP is designed to operate with current and future unicast and multicast routing protocols. An RSVP process consults the local routing database(s) to obtain routes. In the multicast case, for example, a host sends IGMP messages to join a multicast group and then sends RSVP messages to reserve resources along the delivery path(s) of that group. Routing protocols determine where packets get forwarded; RSVP is only concerned with the QoS of those packets that are forwarded in accordance with routing[3].

In order to efficiently accommodate large groups, dynamic group membership, and heterogeneous receiver requirements, RSVP makes receivers responsible for requesting a specific QoS . A QoS request from a receiver host application is passed to the local RSVP process. The RSVP protocol then carries the request to all the nodes (routers and hosts) along the reverse data path(s) to the data source(s), but only as far as the router where the receiver's data path joins the multicast distribution tree. As a result, RSVP's reservation overhead is in general logarithmic rather than linear in the number of receivers.

### **3.2 Extensions to RSVP for LSP Tunnels**

Extensions to RSVP has been proposed for establishing label switched paths (LSPs) in Multi-protocol Label Switching (MPLS) networks.

Extended RSVP protocol supports [6]

- Implementation of explicitly routed LSP
- Smooth rerouting of LSPs
- Preemption
- Loop detection

Labels are associated with RSVP flows for Hosts and routers that support both RSVP and Multi-Protocol Label Switching. Once a label switched path (LSP) is established, the traffic through the path is defined by the label applied at the ingress node of the LSP.

Extended RSVP signaling protocol uses downstream-on-demand label distribution. An ingress node requests to bind labels to a specific LSP tunnel in the RSVP Path

message. LABEL\_REQUEST object in the RSVP Path message is used for this purpose. Labels are allocated downstream and distributed (propagated upstream) by means of the RSVP Resv message. The LABEL object in the RSVP Resv message is used for this purpose[6].

Extended RSVP signaling protocol model also supports explicit routing capability. EXPLICIT\_ROUTE object in the RSVP Path messages is used to accomplish this. The EXPLICIT\_ROUTE object encapsulates a set of hops which constitutes the explicitly routed path. The EXPLICIT\_ROUTE object defines the paths taken by label-switched RSVP-MPLS flows, there by making it independent of conventional IP routing.

### **3.3 LSP Tunnels**

Once a label is assigned to a set of packets, the label defines the "flow" through the LSP. Such an LSP is called a "LSP tunnel" because the traffic through it is opaque to intermediate nodes along the label switched path.

LSP tunnels allows network performance optimization. LSP tunnels can be automatically or manually routed away from network failures, congestion, and bottlenecks.

LSP\_TUNNEL\_IPv4 and LSP\_TUNNEL\_IPv6 have been defined to support the LSP tunnel feature.

#### **3.3.1 Traffic Engineered Tunnels**

Sets of LSP tunnels are called traffic-engineered tunnels (TE tunnels). This can be useful during reroute operations or to spread a traffic trunk over multiple paths[6].



Tunnel ID which is part of the SESSION object, SENDER\_TEMPLATE and FILTER\_SPEC objects have been defined to support traffic engineered tunnel features.

### 3.4 LSP Tunnel Related Message Formats

Object Name	Applicable RSVP Message
LABEL_REQUEST	Path
LABEL	Resv
EXPLICIT_ROUTE	Path
RECORD_ROUTE	Path, Resv
SESSION_ATTRIBUTE	Path

Table 3-1: LSP Tunnel related message formats

#### 3.4.1 Path Message – E-RSVP

The format of the Path message is as follows:

RSVP HEADER
INTEGRITY
SESSION
RSVP_HOP
TIME_VALUE
EXPLICIT_ROUTE (Optional)
LABEL_REQUEST
SESSION_ATTRIBUTE (Optional)
POLICY_DATA (Optional)

SENDER DESCRIPTOR
-------------------

Table 3-2: Format of the PATH message E-RSVP

The sender descriptor has objects like Sender \_Template, Sender –Tspec, Adspec (optional) and Record Route (optional). All these objects give information about the sender.

### 3.4.2 Resv Message – E-RSVP

The format of the Resv message is as follows:

RSVP HEADER
INTEGRITY (Optional)
SESSION
RSVP_HOP
TIME _VALUE
RESV_CONFIRM (Optional)
SCOPE (Optional)
POLICY _DATA (Optional)
STYLE
FLOW DESCRIPTOR LIST

Table 3-3 : Format for RESV message –E-RSVP

The flow descriptor list has objects like Flowspec, Filter spec ,Label and Record Route (optional).

### 3.5 Operation Of Lsp Tunnels

Features supported by extended RSVP related to the operation of LSP tunnels include:

- the ability to establish LSP tunnels with or without QoS requirements
- the ability to dynamically reroute an established LSP tunnel
- the ability to observe the actual route traversed by an established LSP tunnel
- the ability to identify and diagnose LSP tunnels
- the ability to preempt an established LSP tunnel
- the ability to perform downstream-on-demand label allocation, distribution, and binding.

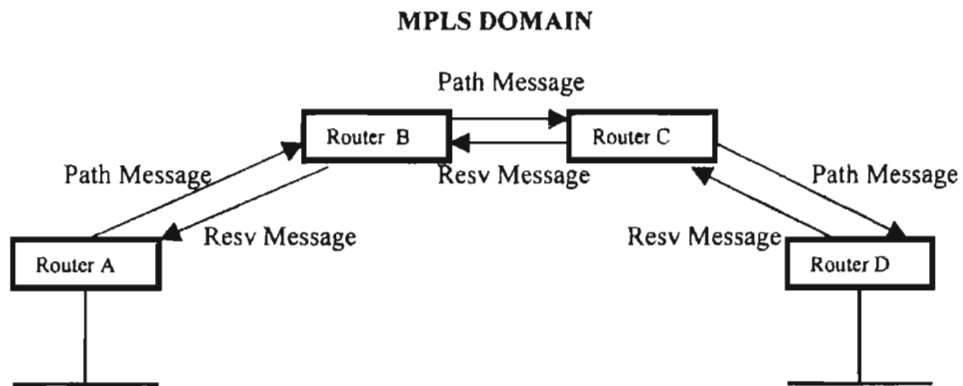


Figure 3-1: Path Message and Resv Message across a MPLS network

To create an LSP tunnel, the first MPLS node on the path that is, the sender node (Router A) with respect to the path creates an RSVP Path message with a session type of LSP\_TUNNEL\_IPv4 or LSP\_TUNNEL\_IPv6 and inserts a LABEL\_REQUEST object into the Path message. The LABEL\_REQUEST object indicates that a label binding for

this path is requested . If a node is incapable of providing a label binding, it sends a PathErr message.

The sender node (Router A) adds an EXPLICIT\_ROUTE object to the RSVP Path message. The EXPLICIT\_ROUTE object specifies the route as a sequence of abstract nodes. If the sender node discovers a better route after a session has been successfully established , the sender can dynamically reroute the session by simply changing the EXPLICIT\_ROUTE object.

The RECORD\_ROUTE object in the Path message, gives the sender node information about the actual route that the LSP tunnel traverses. The sender node can also use this object to request notification from the network concerning changes to the routing path.

The SESSION\_ATTRIBUTE object can be added to Path messages to aid in session identification and diagnostics .Control information, such as setup and hold priorities, resource affinities and local-protection, are also included in this object.

The destination node of a label-switched path responds to a LABEL\_REQUEST by including a LABEL object in its response RSVP Resv message. The LABEL object is inserted in the filter spec list immediately following the filter spec to which it pertains.

The Resv message (from Router D to Router A) is sent back upstream towards the sender in reverse order. When the Resv message propagates upstream to the sender node, a label-switched path is successfully established.

### **3.5.1 Rerouting Traffic Engineered Tunnels**

One of the requirements for Traffic Engineering is the capability to reroute an established TE tunnel. Smooth rerouting requires establishing a new LSP tunnel and transferring traffic from the old LSP tunnel onto it before tearing down the old LSP tunnel. This concept is called "**make-before-break.**" In order to support make-before-break, it is necessary that on links that are common to the old and new LSPs, resources used by the old LSP tunnel should not be released before traffic is transitioned to the new LSP tunnel, and reservations should not be counted twice because this might cause Admission Control to reject the new LSP tunnel[6].

To achieve a reroute, the ingress node picks a new LSP ID and forms a new SENDER\_TEMPLATE. The ingress node then creates a new EXPLICIT\_ROUTE Object (ERO) to define the new path. Thereafter the node sends a new Path Message using the original SESSION object and the new SENDER\_TEMPLATE and ERO. It continues to use the old LSP and refresh the old Path message. On links that are not held in common, the new Path message is treated as a new LSP tunnel setup. On links held in common, the shared SESSION object and Shared Explicit Style (SE) style allow the LSP to be established sharing resources with the old LSP. Once the ingress node receives a Resv message for the new LSP, it can change traffic to it and tear down the old LSP[6].

### 3.6 LSP Tunnel Related Objects

#### 3.6.1 Label Object

Labels may be carried in Resv messages. A label is associated with each sender for the Fixed filter (FF) and Shared Explicit (SE) styles. The label for a sender MUST immediately follow the FILTER\_SPEC in the Resv message.

The LABEL object has the following format[6] :

LABEL class = 16, C\_Type = 1

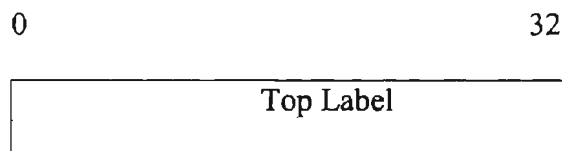


Table 3-3 : Format of a label object

The contents of a LABEL is a single label, encoded in 4 octets. Each generic MPLS label is an unsigned integer in the range 0 through 1048575

#### 3.6.2 LABEL REQUEST OBJECT

The Label Request Class is 19. There are three possible C\_Types[6] .

Type 1 is a Label Request without label range.

Type 2 is a label request with an ATM label range.

Type 3 is a label request with a Frame Relay label range.

The LABEL\_REQUEST object formats are shown below.

##### 3.6.2.1 Label Request without Label Range [6]

Class = 19, C\_Type = 1

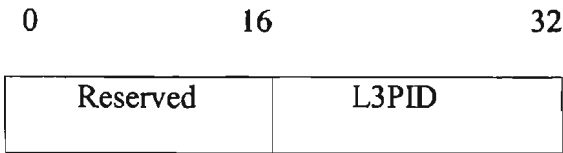


Table 3-4 : Format of label request without label range

**Reserved:** This field is reserved. On transmission it **MUST** be set to zero and **MUST** be ignored on receipt.

**L3PID:** An identifier of the layer 3 protocol using this path.

### 3.6.2.2 Label Request with ATM Label Range [6]

Class = 19, C\_Type = 2

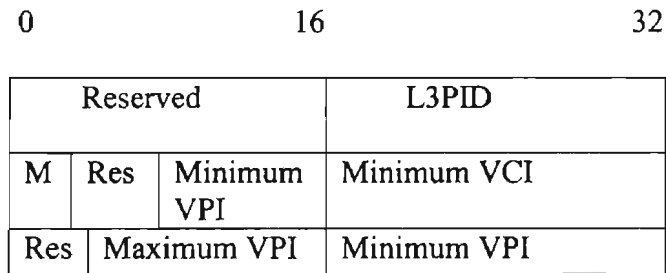


Table 3-5 : Format of label request with ATM label range

**Reserved (Res):** This field is reserved. It **MUST** be set to zero on transmission and **MUST** be ignored on receipt.

**L3PID:** An identifier of the layer 3 protocol using this path.

**M :** Setting this bit to one indicates that the node is capable of merging in the data plane.

Minimum VPI (12 bits) : This 12 bit field specifies the lower bound of a block of Virtual Path Identifiers

Minimum VCI (16 bits) : This 16 bit field specifies the lower bound of a block of Virtual Connection Identifiers

Maximum VPI (12 bits) : This 12 bit field specifies the upper bound of a block of Virtual Path Identifiers

Maximum VCI (16 bits) : This 16 bit field specifies the upper bound of a block of Virtual Connection Identifiers

### 3.6.2.3 Label Request with Frame Relay Label Range [6]

Class = 19, C\_Type = 3

0	16	32
Reserved		L3PID
Reserved	DLI	Minimum DLCI
Reserved		Maximum DLCI

Table 3-6: Format of label request with frame relay label range.



Reserved : This field is reserved. It MUST be set to zero on transmission and ignored on receipt.

L3PID: An identifier of the layer 3 protocol using this path.

DLI : DLCI Length Indicator. The number of bits in the DLCI.

The following values are supported:

Len	DLCI bits
0	10
2	23

Minimum DLCI : This 23-bit field specifies the lower bound of a block of Data Link Connection Identifiers (DLCIs)

Maximum DLCI : This 23-bit field specifies the upper bound of a block of Data Link Connection Identifiers (DLCIs)

### 3.7 Explicit Route Object [6]

Explicit routes are specified by the EXPLICIT\_ROUTE object (ERO). The Explicit Route Class is 20. The EXPLICIT\_ROUTE object has the following format:

Class = 20, C\_Type = 1

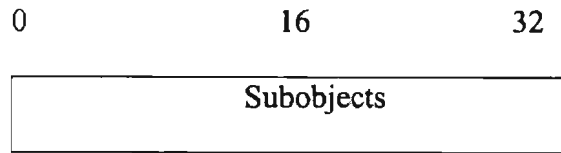


Table 3-7 : Format of Explicit route object

Subobjects : Subobjects are a series of variable-length data items.

The explicit route is encoded as a series of subobjects contained in an EXPLICIT\_ROUTE object. Each subobject identifies a group of nodes in the explicit route. An explicit route is thus a specification of groups of nodes to be traversed.

### 3.8 Record Route Object [6]

Routes can be recorded via the RECORD\_ROUTE object (RRO).

The Record Route Class is 21.

The RECORD\_ROUTE object has the following format:

Class = 21, C\_Type = 1

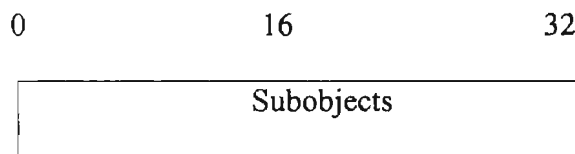


Table 3-8: Format of Record route object

Subobjects : The contents of a RECORD\_ROUTE object are a series of variable-length data items called subobjects.

### 3.9 Session Object

#### 3.9.1 LSP\_TUNNEL\_IPv4 Session Object [6]

Class = SESSION, LSP\_TUNNEL\_IPv4 C-Type = 7

0	16	32
IPV4 tunnel endpoint address		
Must be Zero	Tunnel ID	
Extended Tunnel ID		

Table 3-9: Format of LSP\_Tunnel\_IPv4 Session Object

IPv4 tunnel end point address : IPv4 address of the egress node for the tunnel.

Tunnel ID : A 16-bit identifier used in the SESSION that remains constant over the life of the tunnel.

Extended Tunnel ID : A 32-bit identifier used in the SESSION that remains constant over the life of the tunnel

#### 3.9.2 LSP\_TUNNEL\_IPv6 Session Object [6]

Class = SESSION, LSP\_TUNNEL\_IPv6 C\_Type = 8

Same as LSP\_TUNNEL\_IPV4 except for 16 byte identifier

### 3.10 Sender Template Object

#### 3.10.1 LSP\_TUNNEL\_IPv4 Sender Template Object [6]

Class = SENDER\_TEMPLATE, LSP\_TUNNEL\_IPv4 C-Type = 7

0	16	32
IPv4 tunnel sender address		
Must be Zero	LSP ID	

Table 3-10 : Format of LSP\_Tunnel\_IPv4 sender template object

IPv4 tunnel sender address : IPv4 address for a sender node

LSP ID : A 16-bit identifier used in the SENDER\_TEMPLATE and the

FILTER\_SPEC that can be changed to allow a sender to share resources with itself.

### 3.10.2 LSP\_TUNNEL\_IPv6 Sender Template Object

Class = SENDER\_TEMPLATE, LSP\_TUNNEL\_IPv6 C\_Type = 8 [6]

Same as for LSP\_TUNNEL\_Ipv4

## 3.11 Filter Specification Object

### 3.11.1 LSP\_TUNNEL\_IPv4 Filter Specification Object

Class = FILTER SPECIFICATION, LSP\_TUNNEL\_IPv4 C-Type = 7 [6]

The format of the LSP\_TUNNEL\_IPv4 FILTER\_SPEC object is identical to the LSP\_TUNNEL\_IPv4 SENDER\_TEMPLATE object.

### 3.11.2 LSP\_TUNNEL\_IPv6 Filter Specification Object[6]

Class = FILTER SPECIFICATION, LSP\_TUNNEL\_IPv6 C\_Type = 8

The format of the LSP\_TUNNEL\_IPv6 FILTER\_SPEC object is identical to the LSP\_TUNNEL\_IPv6 SENDER\_TEMPLATE object.

### **3.12 HELLO EXTENSION**

Hello Extension provides node to node failure detection. It enables RSVP nodes to detect when a neighboring node is not reachable [6].

The Hello extension is composed of a Hello message, a HELLO REQUEST object and a HELLO ACK object. Hello processing between two neighbors supports independent selection of, typically configured, failure detection intervals. Each neighbor can separately issue HELLO REQUEST objects. Each request is answered by an acknowledgment. Hello Messages also contain enough information so that one neighbor can suppress issuing hello requests and still perform neighbor failure detection.

Neighbor failure detection is accomplished by collecting and storing a neighbor's "instance" value. If a change in value is seen or if the neighbor is not properly reporting the locally advertised value, then the neighbor is presumed to have reset.

## **CHAPTER IV**

### **LITERATURE REVIEW**

#### **4.1 Constraint-Based LSP Setup using LDP**

Constraint-based routing is a mechanism that supports the TrafficEngineering requirements . Explicit Routing is a subset of the more general constraint-based routing where the constraint is the explicit route (ER). Like any other LSP a CR-LSP is a path through an MPLS network[1][3]. The difference is that while other paths are setup solely based on information in routing tables or from a management system, the constraint-based route is calculated at one point at the edge of network based on criteria, including but not limited to routing information. The intention is that this functionality shall give desired special characteristics to the LSP in order to better support the traffic sent over the LSP. The reason for setting up CR-LSPs might be that one wants to assign certain bandwidth or other Service Class characteristics to the LSP, or that one wants to make sure that alternative routes use physically separate paths through the network[1][3].

##### **4.1.1 Strict and Loose Explicit Routes**

An explicit route is represented in a Label Request Message as a list of nodes or groups of nodes along the constraint-based route. When the CR-LSP is established, all or a subset of the nodes in a group may be traversed by the LSP. The capability to specify, in addition to specified nodes, groups of nodes, of which a subset will be traversed by the CR-LSP, allows the system a significant amount of local flexibility in fulfilling a request for a constraint-based route. This allows the generator of the constraint-based route to have some degree of imperfect information about the details of the path[7].

The constraint-based route is encoded as a series of ER-Hops contained in a constraint-based route TLV. Each ER-Hop may identify a group of nodes in the constraint-based route. A constraint-based route is then a path including all of the identified groups of nodes in the order in which they appear in the TLV.

#### **4.1.2 Traffic Characteristics**

The traffic characteristics of a path are described in the Traffic Parameters TLV in terms of a peak rate, committed rate, and service granularity. The peak and committed rates describe the bandwidth constraints of a path while the service granularity can be used to specify a constraint on the delay variation that the CR-LDP MPLS domain may introduce to a path traffic [7].

#### **4.1.3 Pre-emption**

CR-LDP signals the resources required by a path on each hop of the route. If a route with sufficient resources can not be found, existing paths may be rerouted to reallocate resources to the new path. This is the process of path pre-emption. Setup and holding priorities are used to rank existing paths (holding priority) and the new path (setup priority) to determine if the new path can pre-empt an existing path. The allocation of setup and holding priority values to paths is an aspect of network policy [9].

#### 4.1.4 Route Pinning

Route pinning is applicable to segments of an LSP that are loosely routed - i.e. those segments which are specified with a next hop with the "L" bit set or where the next hop is an abstract node. A CR-LSP may be setup using route pinning if it is undesirable to change the path used by an LSP even when a better next hop becomes available at some LSR along the loosely routed portion of the LSP [9].

#### 4.2 Label Request Message

An LSR sends the Label Request Message to an LDP peer to request a binding (mapping) for a FEC with the following modifications[9]:

- The Label Request Message MUST include a single FEC-TLV element.  
The CR-LSP FEC TLV element SHOULD be used. However, the other FEC-TLVs defined in [1] MAY be used instead for certain applications.
- The Optional Parameters TLV includes the definition of any of the Constraint-based TLVs .
- The Procedures to handle the Label Request Message are augmented by the procedures for processing of the CR-TLVs

The encoding for the CR-LDP Label Request Message is as follows:



0	32	
0	Label Request (0x0401)	Message Length
Message ID		
FEC TLV		
LSPID TLV (CR-LDP, mandatory)		
ER-TLV (CR-LDP, optional)		
Traffic TLV (CR-LDP, optional)		
Pinning TLV (CR-LDP, optional)		
Resource Class TLV (CR-LDP, optional)		
Pre-emption TLV (CR-LDP, optional)		

Table 4-1: Encoding for CR-LDP Label Request Message

### 4.3 Label Mapping Message

A Mapping message is transmitted by a downstream LSR to an upstream LSR under one of the following conditions [7]:

1. The LSR is the egress end of the CR-LSP and an upstream mapping has been requested.
2. The LSR received a mapping from its downstream next hop LSR for an CR-LSP for which an upstream request is still pending.

The encoding for the CR-LDP Label Mapping Message is as follows:

0	32	
0	Label Request (0x0400)	Message Length
Message ID		
FEC TLV		
Label TLV		
Label Request Message ID TLV		
LSPID TLV (CR-LDP,Optional)		
Traffic TLV (CR-LDP,Optional)		

Table 4-2: Encoding for CR-LDP Label Mapping Message

#### 4.4 Notification Message

An LSR sends a Notification message to inform an LDP peer of a significant event. A notification message signals a fatal error or provides advisory information such as the outcome of processing an LDP message or the state of the LDP session[7].

Establishment of an CR-LSP may fail for a variety of reasons. All such failures are considered advisory conditions and they are signaled by the Notification Message.

Notification Messages carry Status TLVs to specify events being signaled. The Notification Message MAY carry the LSPID TLV of the corresponding CR-LSP. Notification Messages MUST be forwarded toward the LSR originating the Label Request at each hop.

The encoding of the notification message is as follows[7]:

0	32	
0	Notification (0x0001)	Message Length
Message ID		
Status TLV		
Optional Parameters		

Table 4-3: Encoding for CR-LDP Notification Message

#### 4.5 Release , Withdraw, and Abort Messages [7]

These messages may also carry the LSPID TLV. LSPID is a unique tunnel identifier within an MPLS network. An upstream LSR may send a Label Abort Request message to abort an outstanding label request message for FEC sent to downstream LSR. An LSR sends a Label Release message to an LDP peer to signal the peer that the LSR no longer needs specific FEC-label mappings previously requested of and/or advertised by the peer. An LSR sends a Label Withdraw message to an LDP peer to signal the peer that the peer may not continue to use specific FEC-label mappings the LSR had previously advertised. This breaks the mapping between the FECs and the labels.

#### 4.6 Protocol Specification

The Label Request Message in the LDP protocol **MUST** carry the LSPID TLV and **MAY** carry one or more of the optional Constraint-based Routing TLVs (CR-TLVs) defined below.

##### 4.6.1 Explicit Route TLV (ER-TLV) [7]

The ER-TLV is an object that specifies the path to be taken by the LSP being established. It is composed of one or more Explicit Route

0	0	Type = 0x0800	Length	32
ER-Hop TLV 1				
ER-Hop TLV 2				
.....				
ER-Hopt TLV n				

Table 4-4: Explicit Route TLV

Type : A fourteen-bit field carrying the value of the ER-TLV Type = 0x0800.

Length : Specifies the length of the value field in bytes.

ER-Hop TLVs : One or more ER-Hop TLVs defined in Section 4.2.

#### 4.6.2 Explicit Route Hop TLV (ER-Hop TLV) [7]

The contents of an ER-TLV are a series of variable length ER-Hop TLVs.

A node receiving a label request message including an ER-Hop type that is not supported MUST not progress the label request message to the downstream LSR and MUST send back a "No Route" Notification Message.

Each ER-Hop TLV has the form:

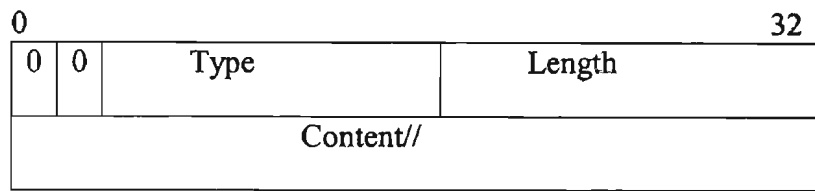


Table 4-5: Explicit Route Hop TLV

ER-Hop Type : A fourteen-bit field carrying the type of the ER-Hop contents.

Length : Specifies the length of the value field in bytes.

L bit :The L bit in the ER-Hop is a one-bit attribute. If the L bit is set, then the value of the attribute is "loose". Otherwise, the value of the attribute is "strict. Loose and strict nodes are always interpreted relative to their prior abstract nodes. The path between a strict node and its prior node MUST include only network nodes from the strict node and its prior abstract node.The path between a loose node and its prior node MAY include other network nodes, which are not part of the strict node or its prior abstract node.

Contents :A variable length field containing a node or abstract node which is one of the consecutive nodes that make up the explicitly routed LSP.

#### 4.6.3 Traffic Parameters TLV [7]

A Traffic Parameters TLV, is used to signal the Traffic Parameter values.

0	0	Type = 0x0810	Length =24		
Flags		Frequency	Reserved		Weight
Peak Data Rate (PDR)					
Peak Burst Size (PBS)					
Committed Data Rate (CDR)					
Committed Burst Size (CBS)					
Excess Burst size (EBS)					

Table 4-6: Traffic parameters TLV

**Type :** A fourteen-bit field carrying the value of the Traffic Parameters TLV Type = 0x0810.

**Length :** Specifies the length of the value field in bytes = 24.

**Flags :** The Flags field is shown below:

Res	F6	F5	F4	F3	F2	F1
-----	----	----	----	----	----	----

Table 4-7: Flag Fields of Traffic parameters TLV

**Res -** These bits are reserved.

Zero on transmission.

Ignored on receipt.

- F1 - Corresponds to the PDR.
- F2 - Corresponds to the PBS.
- F3 - Corresponds to the CDR.
- F4 - Corresponds to the CBS.
- F5 - Corresponds to the EBS.
- F6 - Corresponds to the Weight.

Each flag  $F_i$  is a Negotiable Flag corresponding to a Traffic Parameter. The Negotiable Flag value zero denotes NotNegotiable and value one denotes Negotiable.

Frequency : The Frequency field is coded as an 8 bit unsigned integer with the following code points defined:

0- Unspecified

1- Frequent

2- Very Frequent

3-255 - Reserved

Reserved - Zero on transmission. Ignored on receipt.

Weight : An 8 bit unsigned integer indicating the weight of the CR-LSP. Valid weight values are from 1 to 255. The value 0 means that weight is not applicable for the CR-LSP.

Traffic Parameters : Each Traffic Parameter is encoded as a 32-bit IEEE single- precision floating-point number.

#### **4.6.3.1 Frequency [7]**

The Frequency specifies at what granularity the CDR allocated to the CR-LSP is made available. The value Very Frequent means that the available rate should average at least the CDR when measured over any time interval equal to or longer than the shortest packet time at the CDR. The value Frequent means that the available rate should average at least the CDR when measured over any time interval equal to or longer than a small number of shortest packet times at the CDR. The value Unspecified means that the CDR MAY be provided at any granularity.

#### **4.6.3.2 Peak Rate [7]**

The Peak Rate defines the maximum rate at which traffic SHOULD be sent to the CR-LSP. The Peak Rate is useful for the purpose of resource allocation. If resource allocation within the MPLS domain depends on the Peak Rate value then it should be enforced at the ingress to the MPLS domain. The Peak Rate is defined in terms of the two Traffic Parameters PDR and PBS.

#### **4.6.3.3 Committed Rate [7]**

The Committed Rate defines the rate that the MPLS domain commits to be available to the CR-LSP. The Committed Rate is defined in terms of the two Traffic Parameters CDR and CBS.



#### 4.6.3.4 Excess Burst Size [7]

The Excess Burst Size may be used at the edge of an MPLS domain for the purpose of traffic conditioning. The EBS MAY be used to measure the extent by which the traffic sent on a CR-LSP exceeds the committed rate. The possible traffic conditioning actions, such as passing, marking or dropping, are specific to the MPLS domain.

#### 4.6.3.5 Peak Rate Token Bucket [7]

The Peak Rate of a CR-LSP is specified in terms of a token bucket P with token rate PDR and maximum token bucket size PBS.

The token bucket P is initially (at time 0) full, i.e., the token count  $T_p(0) = PBS$ . Thereafter, the token count  $T_p$ , if less than PBS, is incremented by one PDR times per second. When a packet of size B bytes arrives at time t, the following happens:

- If  $T_p(t) - B \geq 0$ , the packet is not in excess of the peak rate and  $T_p$  is decremented by B down to the minimum value of 0, else
- the packet is in excess of the peak rate and  $T_p$  is not decremented.

#### 4.6.3.6 Committed Data Rate Token Bucket [7]

The committed rate of a CR-LSP is specified in terms of a token bucket C with rate CDR. The extent by which the offered rate exceeds the committed rate MAY be

measured in terms of another token bucket E, which also operates at rate CDR. The maximum size of the token bucket C is CBS and the maximum size of the token bucket E is EBS.

Thereafter, the token counts Tc and Te are updated CDR times per second as follows:

- If Tc is less than CBS, Tc is incremented by one, else
- if Te is less than EBS, Te is incremented by one, else
- neither Tc nor Te is incremented.

#### **4.6.3.7 Weight [7]**

The weight determines the CR-LSP's relative share of the possible excess bandwidth above its committed rate. The definition of "relative share" is MPLS domain specific.

### **4.6.4 Procedures**

#### **4.6.4.1 Label Request Message [7]**

If an LSR receives an incorrectly encoded Traffic Parameters TLV in which the value of PDR is less than the value of CDR then it MUST send a Notification Message including the Status code "Traffic Parameters Unavailable" to the upstream LSR from which it received the erroneous message.

If a Traffic Parameter is indicated as Negotiable in the Label Request Message by the corresponding Negotiable Flag then an LSR MAY replace the Traffic Parameter value with a smaller value.

If the Weight is indicated as Negotiable in the Label Request Message by the corresponding Negotiable Flag then an LSR may replace the Weight value with a lower value (down to 0). If, after possible Traffic Parameter negotiation, an LSR can support the CR-LSP Traffic Parameters then the LSR MUST reserve the corresponding resources for the CR-LSP. If, after possible Traffic Parameter negotiation, an LSR cannot support the CR-LSP Traffic Parameters then the LSR MUST send a Notification Message that contains the "Resource Unavailable" status code.

#### **4.6.4.2 Label Mapping Message [7]**

If an LSR receives an incorrectly encoded Traffic Parameters TLV in which the value of PDR is less than the value of CDR then it MUST send a Label Release message containing the Status code "Traffic Parameters Unavailable" to the LSR from which it received the erroneous message. In addition, the LSP should send a Notification Message upstream with the status code "Label Request Aborted".

If the negotiation flag was set in the label request message, the egress LSR MUST include the (possibly negotiated) Traffic Parameters and Weight in the Label Mapping message.

The Traffic Parameters and the Weight in a Label Mapping message MUST be forwarded unchanged. An LSR SHOULD adjust the resources that it reserved for a CR-

LSP when it receives a Label Mapping Message if the Traffic Parameters differ from those in the corresponding Label Request Message.

#### **4.6.4.3 Notification Message [7]**

If an LSR receives a Notification Message for a CR-LSP, it SHOULD release any resources that it possibly had reserved for the CR-LSP. In addition, on receiving a Notification Message from a Downstream LSR that is associated with a Label Request from an upstream LSR, the local LSR MUST propagate the Notification message .

#### **4.7 Preemption TLV [7]**

The default value of the setup and holding priorities should be in the middle of the range so that this feature can be turned on gradually in an operational network by increasing or decreasing the priority starting at the middle of the range.

Since the Preemption TLV is an optional TLV, LSPs that are setup without an explicitly signaled preemption TLV SHOULD be treated as LSPs with the default setup and holding priorities (e.g., 4). When an established LSP is preempted, the LSR that initiates the preemption sends a Withdraw Message upstream and a Release Message downstream.

When an LSP in the process of being established (outstanding Label Request without getting a Label Mapping back) is preempted, the LSR that initiates the preemption, sends a Notification Message upstream and an Abort Message downstream.

#### **4.8 LSPID TLV [7]**

LSPID is a unique identifier of a CR-LSP within an MPLS network. The LSPID is composed of the ingress LSR Router ID (or any of its own Ipv4 addresses) and a Locally unique CR-LSP ID to that LSR.

The LSPID is useful in network management, in CR-LSP repair, and in using an already established CR-LSP as a hop in an ER-TLV. An "action indicator flag" is carried in the LSPID TLV. This "action indicator flag" indicates explicitly the action that should be taken if the LSP already exists on the LSR receiving the message.

After a CR-LSP is set up, its bandwidth reservation may need to be changed by the network operator, due to the new requirements for the traffic carried on that CR-LSP. The "action indicator flag" is used indicate the need to modify the bandwidth and possibly other parameters of an established CR-LSP without service interruption. This feature has application in dynamic network resources management where traffic of different priorities and service classes is involved.

#### **4.9 Resource Class TLV [7]**

The Resource Class as defined is used to specify which links are acceptable by this CR-LSP.

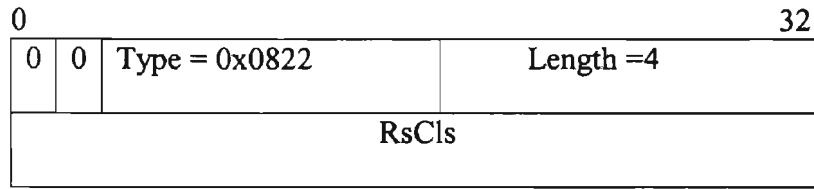


Table 4-8: Resource Class TLV

Type : A fourteen-bit field carrying the value of the ResCls-TLV Type = 0x0822.

Length : Specifies the length of the value field in bytes = 4.

RsCls : The Resource Class bit mask indicating which of the 32 "administrative groups" or "colors" of links the CR-LSP can traverse.

## CHAPTER V

### INTERARRIVAL PACKET JITTER IN MPLS NETWORKS

The success of MPLS networks will be dependent upon its ability to provide the required QoS to the classes of traffic supported by the network. An important class of traffic to be supported by the MPLS networks are those for which a timing relation should be maintained between the source and the destination.

Constant Bit rate (CBR) traffic sources, e.g. CBR audio and video sources will be supported by MPLS networks and it is expected to be a major portion of the traffic in the networks. An important performance measure for CBR traffic, is the jitter which is defined as the alteration of the periodic nature of the cell arrival process at multiplexing (queuing) stages of the network.

In this thesis, we consider **homogeneous CBR traffic/ MPLS / Time Division Multiple Access (TDMA)**. It is assumed that the all individual traffic streams are periodic and the analysis is provided for the jitter incurred to individual periodic streams going through an LSR in the MPLS network . We only consider the **top priority traffic** in our analysis. The CBR traffic will only compete with other CBR traffic in the network. If multiple packets arrive from different streams in the same time slot , they enter the buffer randomly. For mathematical tractability we always assume that the buffer is fully utilized, i.e., the queue utilization is 100 percent.

## 5.1 SYSTEM MODEL

We assume in the MPLS environment, time is slotted and takes non-negative integer value  $t = \{0,1,2,\dots\}$ . The time interval  $[t-1,t)$  is referred to as time slot  $t$ . We assume that the sources produce fixed length MPLS packets independently of each other. In the case of VBR packets as in voice the packets are formatted into CBR platform, i.e., the packets are either truncated or padded to fit in to the CBR format .

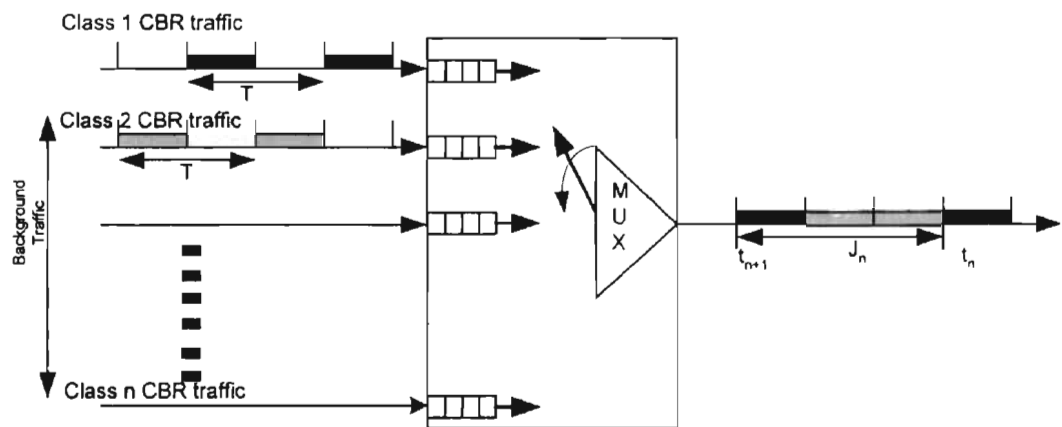


Figure :5-1 The Queuing Model

The packets are stored in a loss-free buffer. It is assumed that the departure from the cell buffer takes place at the beginning of slots, and the arrivals during a slot. We define

$q_t$  = queue length ( in number of packets) at the end of the  $t^{\text{th}}$  slot



$A_t$  = number of arrivals from all sources in the  $t^{th}$  slot

So that we have the following evolution equation[9]

$$q_{t+1} = \max(q_t - 1, 0) + A_t \quad (1)$$

The tagged stream refers to the traffic stream of interest and it is assumed to be periodic when entering the first node in the network. The background traffic refers to the traffic, which competes for MPLS time slots in a node.

In what follows, we describe the arrival process of individual streams. The individual traffic source of interest CBR (tagged stream) is assumed to be periodic with period  $T$  and cells arrive in slots[9]

$$t_n = (n-1)T + 1, n \geq 1, \text{ so that the } n\text{th tagged cell arrives in slot } t_n \quad (2)$$

Other periodical streams i.e., background traffic in this case is also considered to be periodic. A stream  $i$  is fully described by the doublet  $\{I_i, T_i\}$  where  $I_i$  denotes the offset random variable denoting the slot number of the first cell arriving from source  $I$ , and  $T_i$  denotes the source period[9]. It is assumed that  $I_i$  is an integer-valued random variable uniformly distributed in  $[1, T_i]$ . The offset random variable of all sources are assumed to be mutually independent[9].

The packet transmission is assumed to be First Come First Serve (FCFS) and one packet per slot is transmitted as long as the buffer is not empty. The packet arriving in the

same time slot enter the buffer randomly[9]. Let  $Q(t_n)$  denote the number of packets seen in the buffer by the  $n^{\text{th}}$  tagged packet arriving at time  $t_n$  [9] We note that in the event of multiple arrivals at time  $t_n$ ,  $Q(t_n)$  includes those cells entering the buffer ahead of the tagged cell[9].

We define the random variable  $J_n$  as the inter-departures of  $n^{\text{th}}$  and  $(n+1)^{\text{st}}$  cells. We have [9]

$$J_n = Q(t_{n+1}) - Q(t_n) + T \quad (3)$$

And the centered jitter process

$$\tilde{J}_n = J_n - T \quad (4)$$

## 5.2 PERFORMANCE ANALYSIS

The analysis of jitter performance of differentiated services in MPLS networks relies on the case study of assignment methods of the tagged packet of interest in comparison to the background traffic packets. In order to derive the effects of interarrival packet jitter in MPLS networks applying differentiated services, the derivations of the jitter probability (i.e.,  $P\{\tilde{J}_n = j\}$ ) becomes the essential building block. In this section, we derive the jitter probability of one tagged stream among multiplexed with homogenous CBR data streams, and provide explanations to its characteristics.

**Proposition 1:** Assuming the initial queue length is zero ( $q_0 = 0$ ),  $t \geq T$ , and  $q_t$  is periodic with period  $T$  and for  $n > 1$ , the probability of  $\tilde{J}_n = j$  is given as

$$P\{\tilde{J}_n = j\} = \sum_{k=|j|}^N B_k\left(\frac{1}{T}, N\right) f_k(j), \quad \text{for } |j| \leq N. \quad (5)$$

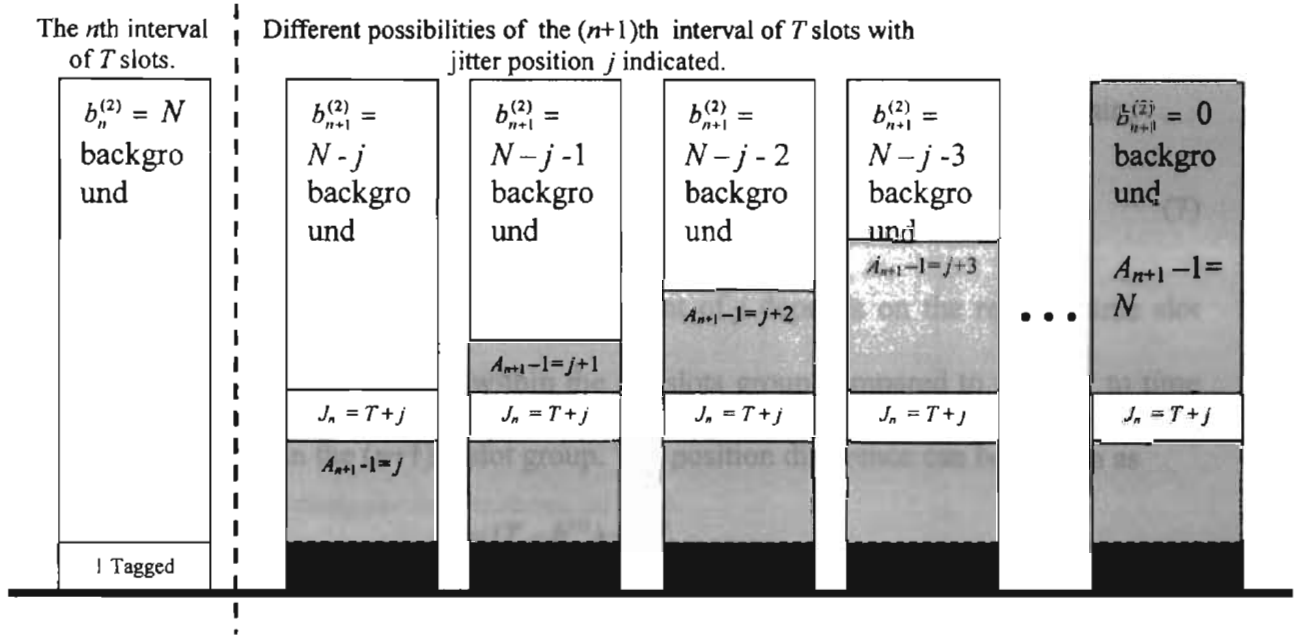


Figure:5-2 Time slot assignment diagram of the tagged frame in the  $n$ th and  $(n+1)$ th time slot group.

### 5.3 PROOF & EXPLANATIONS

The probability of jitter based on the homogeneous CBR traffic case can be derived from the conditional probability rule of

$$P\{\tilde{J}_n = j\} = \sum_{k=|j|}^N P\{\tilde{J}_n = j \mid A_{n+1} - 1 = k\} \cdot P\{A_{n+1} - 1 = k\}. \quad (6)$$

The  $P\{A_{n+1} - 1 = k\}$  term is based on the consideration that the probability of each time slot assignment becomes different based on the number of frames that arrive within a given time slot group. We subtract 1 from the total number of frames that arrive in time slot group  $(n+1)$  (i.e.,  $A_{n+1}$ ) due to the fact that the tagged frame is a fixed arrival into

jitter position  $\tilde{J}_n = j$ . The binomial distribution  $B_k(N, p)$  can be used to provide this probability computation, where the total number of cells that can arrive is upper limited by  $N+1$ , for the case of full utilization. The density  $B_k(N, p)$  provides the probability of  $A_n - 1 = k$  frames arriving among the  $N+1$  frames time slots available, given that the tagged frame is considered a fixed arrival into jitter position  $\tilde{J}_n = j$ . Thus we obtain,

$$P\{A_{n+1} - 1 = k\} = \binom{N}{K} p^k (1-p)^{N-k}. \quad (7)$$

The probability of having a jitter amount of  $j$  depends on the relative time slot assignment of the tagged stream within the  $n$ th slots group compared to the new to time slot position taken in the  $(n+1)$ th slot group. The position difference can be written as

$$\begin{aligned} J_n &= (T - b_n^{(1)}) + b_{n+1}^{(1)} \\ &= 1 + b_n^{(2)} + b_{n+1}^{(1)}, \end{aligned} \quad (8)$$

where the centralized jitter sequence can be written as  $\tilde{J}_n = (b_{n+1}^{(1)} - b_n^{(1)})$  which can be either positive or negative. Here we apply the triangle distribution, which is given by

$$f_k(j) = \begin{cases} \frac{1}{k+1} - \frac{|j|}{(k+1)^2}, & \text{for } |j| \leq k, \\ 0, & \text{otherwise} \end{cases}. \quad (9)$$

The triangle distribution is a symmetric distribution which represents the probability that the time slot position of two sequential arriving frames from a CBR source will be offset by a jitter amount of  $+j$  or  $-j$ . As can be observed from the triangular density (in Fig.5-3), for the probability of arriving in the same slot of the next slot group has the highest probability, and that the probability of position assignment becomes smaller on a linear scale as the time slots are farther away from the center time slot position. Based on this, we can derive

$$P\{\tilde{J}_n = j | A_{n+1} - 1 = k\} = f_k(j), \quad (6)$$

which is the probability of jitter  $j$  given  $k$  background CBR frame arrivals.

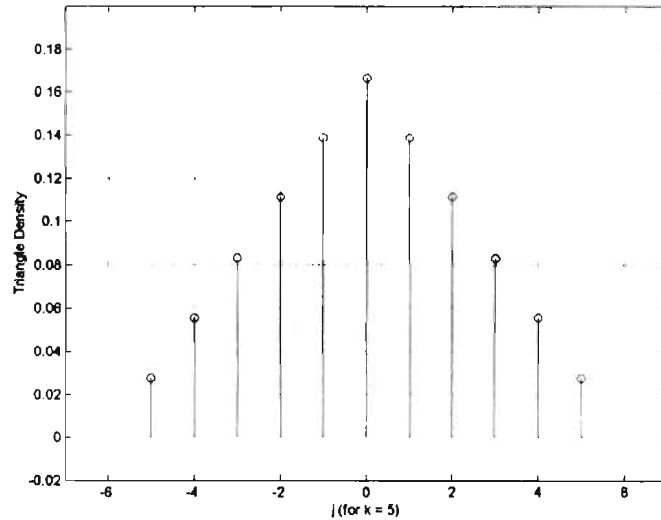


Figure 5- 3. Discrete triangular density shown for  $k = 5$ .

For the example in Fig. 5-2, the tagged frame for the  $n$ th slots group will be fixed to the 1<sup>st</sup> time slot position of  $[(n-1)T] \leq t \leq [(n-1)T+(1/T)]$ . For the  $(n+1)$ th slot group the position of the tagged frame is ordered into position  $j+1$ , which creates a jitter value of  $J_n = (T + j)$ , or equivalently,  $\tilde{J}_n = j$ . The assignment of the tagged frame into the 1<sup>st</sup> slot of the  $n$ th slot group can be easily generalized based on the fact that the derivations stay valid for a positive or negative  $\tilde{J}_n = j$  value (which is noted by the absolute value sign on the  $j$  value), and the jitter value is only dependent to the two sequential time slot assignments of the subsequent time slot groups.

Based on (6), (7), and (10), we can conclude that (5) is a valid expression for the jitter probability under the given assumptions. Thus we obtain the jitter Probability as ,

$$\begin{aligned}
P\{\tilde{J}_n = j\} &= \sum_{k=|j|}^N P\{\tilde{J}_n = j \mid A_{n+1} - 1 = k\} \cdot P\{A_{n+1} - 1 = k\} \\
&= \sum_{k=|j|}^N B_k\left(\frac{1}{T}, N\right) f_k(j), \quad \text{for } |j| \leq N.
\end{aligned} \tag{11}$$

Thus the probability of jitter can be defined as the product of the binomial distribution and triangular distribution summed from  $k$  to  $N$ , the number of background traffic streams. It is considered that  $k$  equals to the absolute value of jitter  $j$ , in order to indicate the symmetric feature of the triangular distribution.

By estimating the probability of jitter within MPLS networks for homogeneous CBR data traffic the receiver buffer size can be estimated so that we can reconstruct the data streams into its original pattern before it is delivered to its final destination.

## CHAPTER VI

### OBSERVATIONS AND RESULTS.

In my thesis I have only done the analysis for the top priority class of traffic with in MPLS networks for homogenous CBR data traffic. The following graphs are plotted and the observations made were as follows.

#### Observation 1:

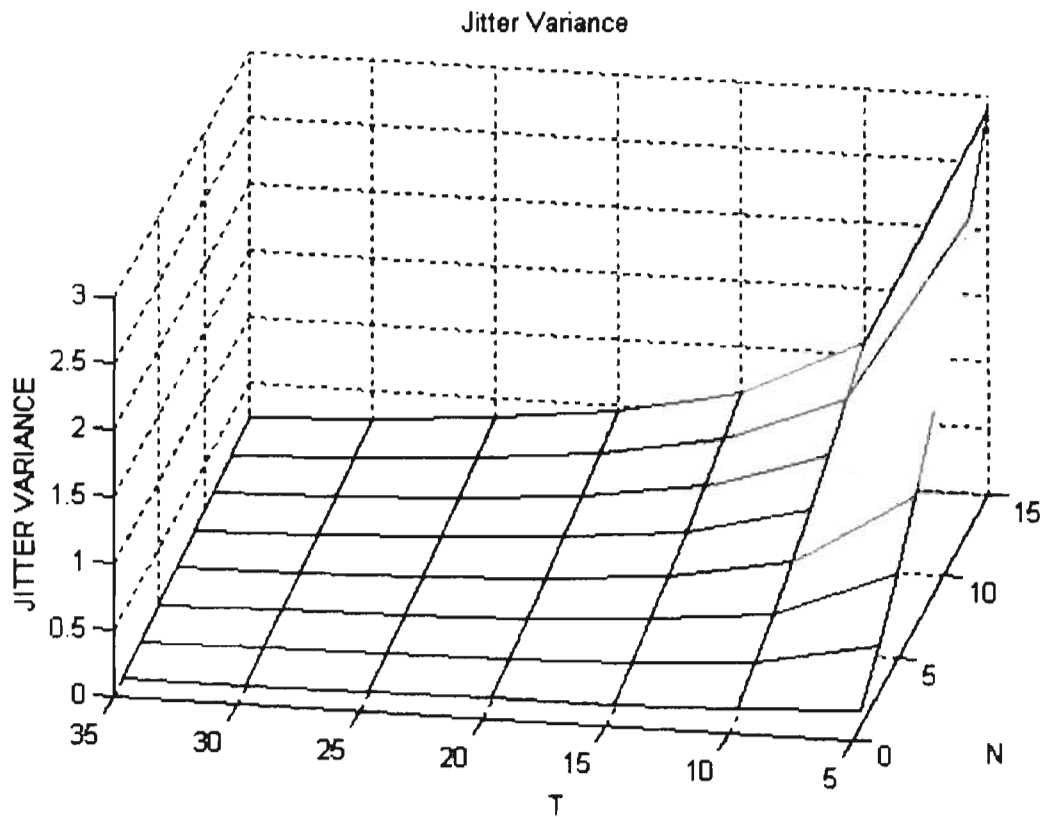
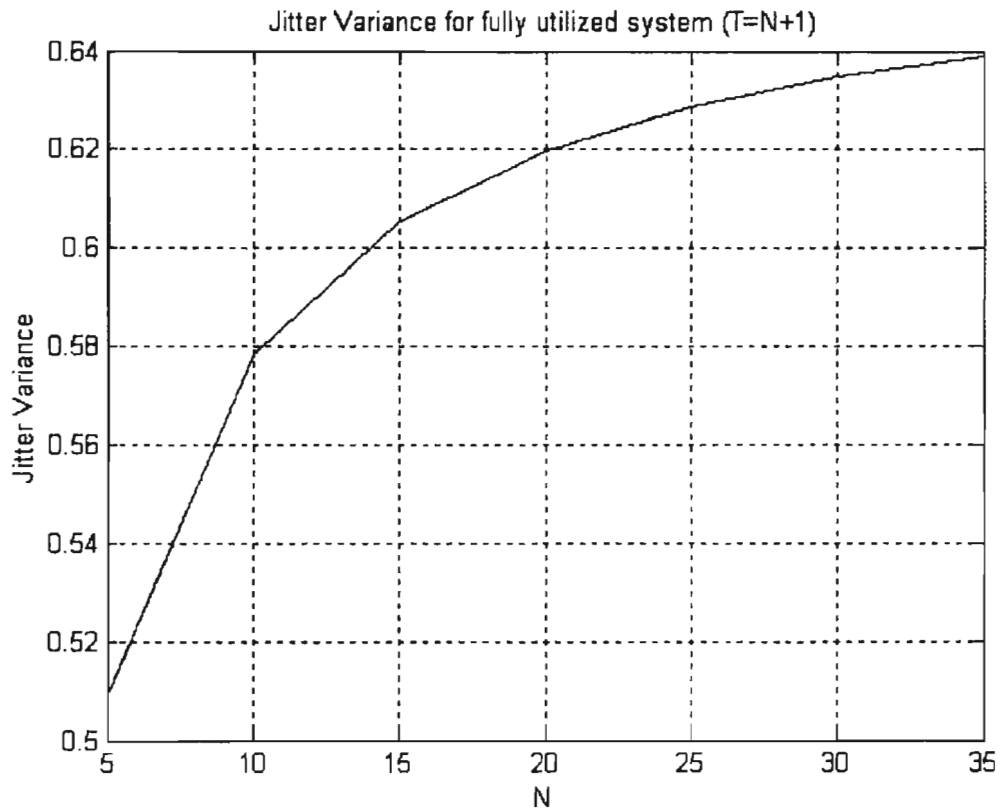


Figure 6-1 : Jitter Variance for various values of T and N.

In fig 6-1, Jitter variance for  $T = 5, 10, 15, 20, 25, 32$  and  $N = 1, 3, 6, 9, 15$  has be plotted. From the graph two things can be observed.

- As the number of background streams  $N$  increases the jitter variance increases.
- As  $T$ , the period of time slot increases the jitter variance decreases.

**Observation 2:**

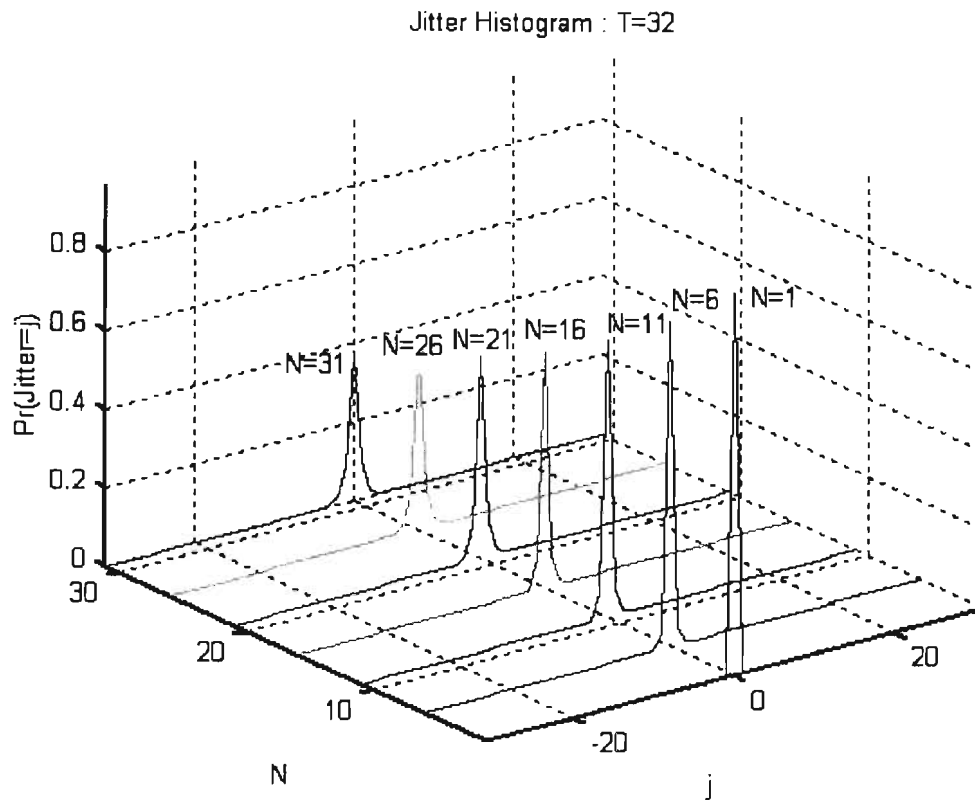


**Figure 6-2 Jitter Variance for a fully utilized system.**

In figure 6-2, we plot the jitter variance for various values of  $N$  the background traffic stream for a fully utilized system. A fully utilized system is one for which the time period  $T = N+1$ . It can be observed that as  $N$  increases the jitter variance also increases.



**Observation 3:**



**Fig 6-3 Jitter Histogram for T=32 and various values of N**

In figure 6-3, Jitter histogram for T=32, and values of N =1,6,11,16,21,26,31 are plotted. The axis representation are as follows on the Z axis the probability of centered jitter  $P\{\tilde{J}_n = j\}$  is plotted, on x axis different values of  $j$  are plotted and on y axis values of N are plotted. From the graph the following is observed

- For each value of N the probability of zero (centered) jitter is maximum for a utilization and any probability of non-zero jitter is minimum for the same utilization.

- It is also been observed that for a fixed value of T as N increases \, the system utilization also increases, but the probability of jitter decreases.

$j$	$P\{\tilde{J}_n = j\}$						
	N=1 $\rho = 0.0625$	N=6 $\rho = 0.2187$	N=11 $\rho = 0.375$	N=16 $\rho = 0.5312$	N=21 $\rho = 0.6875$	N=26 $\rho = 0.843$	N=31 $\rho = 1$
0	9.69e-01	8.27e-01	7.05e-01	6.02e-01	5.13e-01	4.38e-01	3.74e-01
$\pm 1$	7.81e-03	4.00e-02	6.26e-02	7.76e-02	8.69e-02	9.18e-02	9.34e-02
$\pm 2$	0	1.43e-03	4.48e-03	8.35e-03	1.25e-02	1.65e-02	2.01e-02
$\pm 3$	0	3.47e-05	2.44e-04	7.07e-04	1.43e-03	2.39e-03	3.52e-03
$\pm 4$	0	5.37e-07	1.01e-05	4.74e-05	1.33e-04	2.84e-04	5.09e-04
$\pm 5$	0	4.81e-09	3.16e-07	2.55e-06	1.01e-05	2.80e-05	6.16e-05
$\pm 6$	0	1.90e-11	7.49e-09	1.11e-07	6.41e-07	2.32e-06	6.33e-06
$\pm 7$	0	0	1.32e-10	3.91e-09	3.39e-08	1.64e-07	5.58e-07
$\pm 8$	0	0	1.68e-12	1.12e-10	1.51e-09	9.91e-09	4.27e-08
$\pm 9$	0	0	1.47e-14	2.60e-12	5.71e-11	5.18e-10	2.85e-09
$\pm 10$	0	0	7.82e-17	4.86e-14	1.83e-12	2.35e-11	1.67e-10
$\pm 11$	0	0	1.93e-19	7.18e-16	4.95e-14	9.25e-13	8.65e-12
$\pm 12$	0	0	0	8.23e-18	1.13e-15	3.18e-14	3.96e-13
$\pm 13$	0	0	0	7.04e-20	2.18e-17	9.52e-16	1.61e-14
$\pm 14$	0	0	0	4.24e-22	3.51e-19	2.48e-17	5.82e-16
$\pm 15$	0	0	0	1.60e-24	4.64e-21	5.63e-19	1.87e-17
$\pm 16$	0	0	0	2.86e-27	4.97e-23	1.11e-20	5.34e-19
$\pm 17$	0	0	0	0	4.21e-25	1.87e-22	1.36e-20
$\pm 18$	0	0	0	0	2.71e-27	2.71e-24	3.05e-22
$\pm 19$	0	0	0	0	1.24e-29	3.32e-26	6.08e-24
$\pm 20$	0	0	0	0	3.64e-32	3.40e-28	1.07e-25
$\pm 21$	0	0	0	0	5.09e-35	2.86e-30	1.64e-27
$\pm 22$	0	0	0	0	0	1.92e-32	2.21e-29
$\pm 23$	0	0	0	0	0	9.88e-35	2.56e-31
$\pm 24$	0	0	0	0	0	3.67e-37	2.53e-33
$\pm 25$	0	0	0	0	0	8.76e-40	2.12e-35
$\pm 26$	0	0	0	0	0	1.01e-42	1.46e-37
$\pm 27$	0	0	0	0	0	0	8.12e-40
$\pm 28$	0	0	0	0	0	0	3.49e-42
$\pm 29$	0	0	0	0	0	0	1.09e-44
$\pm 30$	0	0	0	0	0	0	2.19e-47
$\pm 31$	0	0	0	0	0	0	2.14e-50
Total Probability	1	1	1	1	1	1	1

Table 6-1 The distribution of centered jitter for homogenous CBR traffic

From table 6-1 it can be observed that the system utilization  $\rho = 1$ , i.e. the maximum for the case of  $N=31$ , for  $T=32$ . It can also be observed that the system utilization increases as the number of  $N$  increases. The system utilization can be defined as  $\rho = \frac{N+1}{T}$  [9]. It is observed from the table that, the probability of zero (centered) jitter is minimum when  $N=31$  and  $\rho = 1$  and the probability of non zero jitter is maximum at this utilization for the time period of  $T=32$ . It is observed that as  $N$  increases the probability of zero jitter decreases and the probability of non zero jitter increases.

## CHAPTER V

### CONCLUSION & FUTURE WORK

Jitter is an important QoS parameter for real time services , such as voice traffic and video. A sequence of negative jitter (clustering) can result in downstream node congestion and consecutive packet loss; a sequence of positive jitter (dispersion) can result in consecutive packet experiencing excessive delays. Both these events results in the worsening in the quality of service for real time traffic.

This thesis is a foundational research done for the interarrival packet jitter in MPLS networks. The jitter probability which is an essential building block within the MPLS network has been investigated and derived. Here we have taken into account only constant bit rate packets and we have derived the jitter probability of one tagged stream multiplexed with homogeneous CBR data streams.

In chapter II , a literature review has been provided for MPLS. In chapter III and IV the literature review for the signaling protocols namely E-RSVP and CR-LDP used for the implementation of label switching in the MPLS network has been provided. In chapter V we discuss the jitter probability with in the MPLS networks and in chapter VI the observation and results are discussed.

The future work for jitter with in MPLS network include , the variance of jitter within MPLS networks for CBR traffic ,the probability of jitter and variance of jitter

within MPLS networks for both CBR and VBR traffic and the End-to-end jitter analysis in the network for periodic flows. As my thesis is the first of its kind to analyze the jitter within MPLS networks a lot of challenging work is expected in the near future.

## REFERENCES

- [1] J.-M. Chung, (*Invited Paper*) "Analysis of MPLS Traffic Engineering," *Proceedings of the IEEE Midwest Symposium on Circuits and Systems 2000 conference (IEEE MWSCAS'00)*, East Lansing, Michigan, USA, Aug. 8-11, 2000.
- [2] J.-M. Chung, (*Invited Paper*) "Wireless Multiprotocol Label Switching," *Proceedings of the 35<sup>th</sup> Asilomar Conference on Signals, Systems and Computers 2001*, Pacific Grove, California, USA, Nov. 4-7, 2001.
- [3] J.-M. Chung, "Report-3: Performance Enhancement and Service Improvement Recommendations for Multiprotocol Label Switching and Multicasting Applications," Technical Project Report, Williams Communications, June 29, 2001.
- [4] J.-M. Chung, E. Marroun, H. Sandhu, and S-C. Kim, "VoIP over MPLS Networking Requirements," *Proceedings of the IEEE International Conference on Networking 2001 (IEEE ICN'01)*, Colmar, France, July 9-13, 2001.
- [5] "Multiprotocol Label Switching Architecture," *RFC 3031*.
- [6] Der-Hwa Gna, Tony Li, Geogrg Swallow, Lou Berger, Vijay Srinivasan, Daniel Awduche "RSVP-TE: Extension to RSVP for LSP Tunnels," *IETF Draft*.
- [7] Bilel Jamoussi, "Constraint-Based LSP Setup using LDP," *IETF Draft*.
- [8] <http://www.iec.org/online/tutorials/mpls>.
- [9] A.Privalov, K.Sohraby, "Per-Stream Jitter Analysis in CBR ATM Multiplexors," *IEEE/ACM Transactions on Networking*, vol.5, No.1, pp.141-149, April 1998.
- [10] C.Bisdikan, W.Matragi, and K.Sohraby, "A Framework for Jitter Analysis in Cell Based Multiplexors," *Performance Evaluation*, vol.22, pages 122-133, 1995.
- [11] W.Matragi, and K.Sohraby, "Jitter Calculus in ATM networks: multiple node case," *IEEE/ACM Transactions on Networking*, vol.22, pp.122-133, Feb 1997.
- [12] J.Roberts, and F.Guillemin, "Jitter in ATM networks and its impact on peak rate enforcement," *Performance Evaluation*, vol.16, pp.35-48, 1992.
- [13] C.Bisdikan, W.Matragi, and K.Sohraby, "Jitter Calculus in ATM Networks : single node case," In Proc. IEEE INFOCOM, Toronto, Ontario, Canada, June 1994.

VITA <sup>~</sup>

Lijy Jose Kallidukil

Candidate for the Degree of

Master of Science

Thesis: FOUNDATIONAL RESEARCH OF INTERARRIVAL  
PACKET JITTER FOR HOMOGENOUS CBR  
TRAFFIC IN MPLS NETWORKS

Major Field: Electrical Engineering

Biographical:

Education: Received a Bachelor of Engineering degree in Electronics and Communication Engineering from the Bharathiar University, India in May 1991. Completed the requirements for the Master of Science degree with a major in Electrical Engineering at the Oklahoma State University in December 2001.

Experience: Employed as a Research Assistant by the ACSEL Laboratories at the School of Electrical and Computer Engineering, Oklahoma State University, Aug. 2000 to present.

Professional Membership: Student member of the honorary Institute of Electrical and Electronics Engineers, Inc. (IEEE) for the academic years 2000 and 2001.