

**PURDUE UNIVERSITY
GRADUATE SCHOOL
Thesis/Dissertation Acceptance**

This is to certify that the thesis/dissertation prepared

By AAMANI NEMTUR

Entitled

FAILURE RECOVERY TECHNIQUES OVER AN MPLS NETWORK USING OPNET

For the degree of Master of Science in Electrical and Computer Engineering

Is approved by the final examining committee:

Dr. Mohamed El-Sharkawy

Dr. Brian King

Dr. Maher Rizkalla

To the best of my knowledge and as understood by the student in the Thesis/Dissertation Agreement, Publication Delay, and Certification/Disclaimer (Graduate School Form 32), this thesis/dissertation adheres to the provisions of Purdue University's "Policy on Integrity in Research" and the use of copyrighted material.

Dr. Mohamed El-Sharkawy

Approved by Major Professor(s): _____

Approved by: Dr. Brian King

11/07/2014

Head of the Department Graduate Program

Date

FAILURE RECOVERY TECHNIQUES OVER AN MPLS NETWORK USING
OPNET

A Thesis
Submitted to the Faculty
of
Purdue University
by
Aamani Nemtur

In Partial Fulfillment of the
Requirements for the Degree
of
Master of Science in Electrical and Computer Engineering

December 2014
Purdue University
Indianapolis, Indiana

To My Family and Friends

TABLE OF CONTENTS

	Page
LIST OF FIGURES	vi
LIST OF TABLES	ix
ABSTRACT	x
1 INTRODUCTION	1
1.1 Motivation	2
1.2 Background	3
1.3 Thesis Outline	4
2 OVERVIEW OF MPLS NETWORKS	5
2.1 MPLS Operation	5
2.2 MPLS Architecture	6
2.3 MPLS Network Design	9
2.4 MPLS Functionality	10
2.5 Routing Protocols	13
3 TRAFFIC ENGINEERING IN MPLS NETWORKS	14
3.1 Working Of MPLS-TE	16
3.2 Constraint Based Routing	16
3.3 Prerequisites of the Signaling protocols to be used in MPLSTE	17
3.4 Signaling Protocols in MPLS-TE:	18
3.5 Resource Reservation Protocol	19
3.5.1 Different Ways of Reservation	20
3.5.2 RSVP-TE Messages:	21
3.6 Label Distribution Protocol	23
3.6.1 LDP Messaging Technique	24
3.6.2 LDP - PDU and other procedures:	25

	Page
3.6.3	Constraint Routing Label Distribution Protocol 26
3.6.4	CR- LDP Protocol Specifications 27
3.7	Differences Between RSVP and CR-LDP Signaling Protocols 27
3.8	Advantages and Disadvantages of Signaling Protocols 29
4	FAULT-TOLERANCE IN MPLS-TE NETWORKS 33
4.1	Fast Failure Detection 34
4.1.1	IGP Failure Detection 34
4.1.2	RSVP Hello Detection 35
4.1.3	Bi-Directional Forwarding Discovery 35
4.2	MPLS-TE Protection Mechanisms 36
4.2.1	Path Protection 36
4.3	Local Protection 38
4.3.1	Link Protection 41
4.3.2	Node Protection 44
4.4	LDP Fast Reroute 45
4.4.1	Node Protection 48
4.5	Source Routing Implementation Over MPLS Networks 48
4.5.1	Working Of Source Routing Over MPLS Networks 49
4.5.2	Source Routed LSP 51
5	NETWORK MODEL SIMULATION OF MPLS NETWORKS FOR FAIL- URE DETECTION AND RECOVERY USING OPNET MODELER 17.5 55
5.1	OPNET Model Configuration 56
5.1.1	OPNET Application Traffic Types: 61
5.2	OPNET Simulation Network 64
5.3	Various Scenarios Implemented in OPNET 65
5.3.1	MPLS Network Simulations without any Failed network com- ponents. 66
5.3.2	MPLS Network Simulations with 3 Failed Links. 69

	Page
5.3.3 MPLS Network Performance with 3 Link Failures and Restoration Techniques implemented on the Network with RSVP Signaling Enabled.	72
5.3.4 MPLS Network Performance With 1 Node Failure in the Network with RSVP Signaling Enabled in the network.	75
5.3.5 MPLS Network performance with 1 node Failure and Restoration Techniques Implemented on the Network with RSVP Signaling Enabled.	77
5.3.6 MPLS Network Performance with 3 Link Failures and Restoration Techniques Implemented on the Network with CR-LDP Signaling Enabled.	78
5.3.7 MPLS Network Performance with 1 node Failure and Restoration Techniques Implemented on the Network with CR-LDP Signaling Enabled.	81
5.3.8 MPLS Network Performance with 3 link Failures and Restoration Techniques Implemented on the Network with Source Routing.	82
5.3.9 Comparison of Traffic Received in all 3 scenarios	86
5.3.10 Comparison of Voice Packet Delay in all 3 scenarios.	86
5.3.11 Comparison of Voice Jitter in all 3 scenarios.	87
6 CONCLUSION	88
LIST OF REFERENCES	89

LIST OF FIGURES

Figure	Page
2.1 Data Packet Contents	5
2.2 MPLS Label Header	6
2.3 MPLS Operation	7
2.4 LSR and LER of MPLS Communication	9
2.5 Different Plane Operations in MPLS Communication	9
2.6 MPLS Control Plane and Data Plane	10
2.7 Control Plane of MPLS	11
2.8 MPLS Network Flow	12
3.1 Network Reservation in RSVP	20
3.2 Messages Flow in RSVP Signaling Protocol	22
3.3 Labels Flow in LDP	23
3.4 Messages Flow in LDP	24
3.5 LDP PDU Label Format	25
3.6 Network Flow in CR-LDP	27
3.7 Summary Explanation of Constraint TLVs	28
3.8 Flows in the LDP Network with Network Topology Changes	31
3.9 LDP over RSVP TE	32
4.1 Path Protection Technique	37
4.2 Secondary LSP in Path Protection	38
4.3 Network with Link Failure	39
4.4 Point of Local Repair and Merging Point in the Network	40
4.5 Label Swapping in the Network with Failed Link	41
4.6 FRR Link Protection for MPLS Network	42
4.7 Node Failure in MPLS Networks	43

Figure	Page
4.8 NHOP and NNHOP Tunnel in MPLS Networks	45
4.9 LDP Fast Re Route in MPLS Networks	47
4.10 LDP Fast Re-Route LFA in MPLS Networks	47
4.11 Failed Scenario in MPLS Networks	48
4.12 Source Routing Demo	49
4.13 Local Label in MPLS	50
4.14 Domain Wide Label in MPLS	50
4.15 Label Stack Mechanism in MPLS Networks	51
4.16 Alternate Path in Source Routing	52
4.17 RLFA in MPLS Networks	53
5.1 Application Configuration in OPNET	59
5.2 Profile Configuration in OPNET	60
5.3 Voice Application Traffic in OPNET	61
5.4 Video Application Traffic in OPNET	62
5.5 HTTP Application Traffic in OPNET	62
5.6 FTP Application Traffic in OPNET	63
5.7 Email Application Traffic in OPNET	63
5.8 Network in OPNET	64
5.9 Traffic Received (packets/sec) in MPLS Network Without any Failure.	66
5.10 Voice Jitter (sec) in MPLS Network without any Failure	67
5.11 Voice Packet Delay in MPLS Network Without any Failure	68
5.12 Traffic Received in MPLS Network with 3 Links Failure	69
5.13 Voice Packet Delay in MPLS Network with 3 Links Failure	70
5.14 Voice Jitter in MPLS Network with 3 Links Failure	71
5.15 Traffic Received in MPLS Network with 3 Links Failure/Recovery in RSVP Signaling	72
5.16 Voice Jitter in MPLS Network with 3 Links Failure/Recovery in RSVP Signaling	73

Figure	Page
5.17 Voice Packet End to End Delay in MPLS Network with 3 Links Failure/Recovery in RSVP Signaling	74
5.18 Node Failure in MPLS Networks with RSVP Signaling	75
5.19 Traffic Received in MPLS Network with 1 Node failure in RSVP Signaling	76
5.20 Traffic Received in MPLS Network with 1 Node Failure/Recovery in RSVP Signaling	77
5.21 Traffic Received in MPLS Network with 3 Links Failure/Detection in CR-LDP Signaling	78
5.22 Voice Packet Delay in MPLS Network with 3 Links Failure/Detection in CR-LDP Signaling	79
5.23 Voice Jitter in MPLS Network with 3 Links Failure/Detection in CR-LDP Signaling	80
5.24 Traffic Received in MPLS Network with 1 Node Failure Detection in CR-LDP Signaling	81
5.25 Traffic Received in MPLS Network with 3 Links Failure/Detection using LFA	82
5.26 Traffic Received in MPLS Network with 3 Links Failure/Detection using RLFA	83
5.27 Voice Packet Delay in MPLS Network with 3 Links Failure/Detection using Source Routing	84
5.28 Voice Jitter in MPLS Network in Source Routing	85
5.29 Comparison of Traffic Received in Various Scenarios in MPLS Network	86
5.30 Comparison of Voice Packet Delay in Various Scenarios in MPLS Network.	87
5.31 Comparison of Voice Jitter in Various Scenarios in MPLS Network. . .	87

LIST OF TABLES

Table	Page
5.1 List of Link Failures in MPLS Network	61

ABSTRACT

Nemtur, Aamani MSECE, Purdue University, December 2014. Failure Recovery Techniques over an MPLS Network using OPNET. Major Professor: Mohamed El-Sharkawy.

Multi-Protocol Label Switching (MPLS) is an emerging technology which is the initial step for the forthcoming generation of communication. It uses Labels in order to identify the packets unlike the conventional IP Routing Mechanism which uses the routing table at each router to route the packet. MPLS uses the techniques of FRR with the help of RSVP/CR-LDP to overcome the link and/or node failures in the network.

On the other hand there are certain limitations/drawbacks of using the above mechanisms for Failure Detection and Recovery which are multiple protocols such as RSVP/CR-LDP over OSPF/IS-IS and complex algorithms to generate backup paths since each router works individually in order to create a backup tunnel. So to overcome the listed limitations, this paper discusses a new technique for MPLS Networks which is Source Routing [1]. Source Routing is the technique in which the source plays the role of directing the packet to the destination and no other router plays the role of routing the packet in the network. Using the OPNET Modeler 17.5 tool for implementing source routing when there is a network failure is performed and the results are compared by implementing RSVP/CR-LDP over the same failed network.

The comparative results show that the network performance is best in the case of Source Routing implementation as compared to the RSVP and CR-LDP signaling over the MPLS Networks.

1. INTRODUCTION

The Internet is the complete set of all interconnected computer networks which uses a standard IP protocol for connectivity. With the applications such as phone and TV being used to communicate, Internet is in high demand. But with a growing number of users, providing real time service without any faults is still an existent problem. So in order to overcome this situation, a new technique is introduced, Multi-Protocol Label Switching (MPLS). Multi-Protocol Label Switching (MPLS) is a labeling mechanism where each packet is directed from one Network node to another Network node in the same autonomous system with the help of the extra label which is added to the packet which is to be routed [2].

With conventional IP routing, it is not possible to provide a technique for load balancing across unequal cost paths, because there is always a single best path towards a destination by taking into account the multiple path metrics. Each data packet from source to destination will select its own path by using the routing lookup table at each intermediate table. In the worst cases, the packets can get lost. Providing a path enough guarantee of no packet loss often requires idle bandwidth. The policy routing can affect the destination which is based on the mechanism used by the routers to transmit the packet. Policy routing once configured on the device allows it to make forwarding decisions based on the information other than the destination IP address, but still the nodes on the path need to look up each incoming packet's IP header information for the forwarding decision on the edge interface [2].

The failure occurring inside the IP network is a very common issue [3]. The failure can be for many reasons which can be software failure inside the routers control, forwarding plane or it can be a hardware failure which can lead to the network failure. The main issue is to handle these unexpected and unwanted failures. There should be some techniques which should ensure that the IP network is able to provide a specific

quality to the users on the different applications. A network failure in the IP network will degrade the service because of the fact that IP is only responsible for the routing related function and provides the unreliable transport for the data. So TCP is used in relation to the IP technology because TCP provides reliability over the transmission of the data. This reliability results in the increased resource utilization in terms of the processing of the end node for packet re-ordering and bandwidth consumption along the path when there is a packet retransmission. The system can also use UDP and this can be the optimal solution to avoid extra burden to handle the failures in the system [4].

1.1 Motivation

MPLS is well known for providing reliable, fast and efficient packet switching techniques over the network. It is mainly used because of the increase in demand by the customers for high quality of service regarding their application requirements. The service providers implement the MPLS in the network domain to utilize and manage the network resources in a very cost effective way. MPLS provides the functionality so that the intermediate routers do not process the network layer information. This information is attached to each packet which is traversing the MPLS network. The intermediate nodes will perform the forwarding decisions by using the MPLS label which is attached to the labelled packet. This label makes the routing on the hardware level by which it can act as the double edge sword lowering latency inherited by the packets across the domain.

The users always desire the best services through the providers network. MPLS takes this factor into consideration by reusing the IP quality of service architecture for the applications running over it. Many features have been added to the MPLS network architecture over time making it a fault tolerant architecture to depend on. The main focus in this work is to study and analyze the failure detection techniques and recovery mechanisms over the failed network.

1.2 Background

The IP protocol is itself the routing protocol which can carry the payload on the IP domains toward a specific destination. The destination prefix and the next hop should be known in advance on each node across the most used path to be taken by the traffic. The routing table is mainly populated with the help of IGP or it can be done with the help of EGP. When network metrics change, the control information is exchanged among the routers which are the intermediate nodes. Network states change generally as the result of any failure or any link state update. In this situation, nodes which are affected get connected and will update the information in the database table. This table is advertised to other nodes participating in building up the domain topology.

The topological information update require advertisements to be exchanged among the participating nodes. In DVRP like RIP and EIGRP, the information which is updated is exchanged between the connected nodes and they advertise only the known best paths which are reachable through them which results in the distributed route calculation. Link state like OSPF update the information exchanged with each and every LSRP capable router [5].

MPLS technology has a complete change in the IP routing mechanism. When MPLS is enabled, the network not only gets benefit by fast reroute on the failed resources but it also helps the system to efficiently use the resources using the MPLS-TE. MPLS FRR will enhance the domain capability in response to the failures in the system. MPLS deployment pushes the IP routing capabilities to the edge of the MPLS domain. The MPLS core network will not be aware of the IP routes and it doesnt perform the lookup on the IP layer information. This benefit will enable the core routers not to carry the global routing label, and the single MPLS domain will provide the overlay network architecture for the multiple application traffic to be carried over.

The MPLS header can contain more than one label. The label information will determine the path to be covered by the data packet. Each node in the MPLS

domain forwards the labeled packet but there is no independent decision on it. The thesis work is mainly concentrated on the abilities of the MPLS networks in providing certain services like FRR. It also explains the MPLS functionality over the IP network performance in terms of the better utilization of the network resources and guaranteed quality of service. This thesis finds the optimum solution for the failed networks [6].

1.3 Thesis Outline

In section 1, introduction, background and thesis scope is covered. Second section covers the entire MPLS Network functionality including with the architecture and various MPLS network components. Third section explains about the traffic engineering concept in MPLS Network and about the various signaling protocols which are used for failure detection and recovery. In Section 4 different scenarios which can arise when failure is occurred is explained. Fifth section has all the simulations which are taken using OPNET simulating tool. The sixth section concludes the thesis. It covers the basic Information about the MPLS Network, its architecture and the functionality.

2. OVERVIEW OF MPLS NETWORKS

Multi-Protocol Label Switching is an emerging technology for high performance packet forwarding and controlling in the data networks. The MPLS mechanism is considered to be a protocol independent mechanism as it works in the same way on different layer protocols like ATM, SONET, and Frame Relay etc [2]. MPLS is a Layer 2.5 Networking protocol. It is located between Layer 2 and Layer 3 of the Traditional OSI Model and it provides additional features for transport of the data packet in the network. The MPLS mechanism is considered to provide fast service because it uses short path labels instead of long network address as used in the conventional IP networks. Since there is no use of long IP address, there is no need of complex lookups in the routing table. MPLS is not a replacement for the conventional IP networks but it added some additional features for better performance. MPLS combines the advantage of IP Routing and simplicity of Label Switching [7].

2.1 MPLS Operation

Label is the reason for the discussion about the MPLS mechanism. Label is considered to be a short entity and it does not have any structure within it. MPLS is considered to be a layer 2.5 protocol because label is placed in between layer 2 and layer 3 networks. It uses layer 2 switching functionality without any layer 3 routing capability. So all the packet routing is done with the help of Labels.

Link-layer header	MPLS label	IP header	Data
-------------------	------------	-----------	------

Figure 2.1.: Data Packet Contents

MPLS Header: Each Data packet is prefixed with the MPLS header which can contain one or more labels and this stack of labels contains 4 fields.

1. A 20 bit label value.
2. bit traffic class for QOS purpose (EXP).
3. 1 bit stack flag (S).
4. 8 bit TTL field.

The 20 bit label value is used to find the Label Switched Path in the MPLS domain. The labels of packets are generally set by the Forward Equivalence Class (FEC). A three bit traffic class field is used for quality of service related purposes. Next is the Stack field which is 1 bit and it indicates the bottom of the stack. The last field is the 8 bit TTL field which is used to encode the TTL Value. The TTL value is decreased by 1 at the hop which avoids the packet to get into the routing loop.



Figure 2.2.: MPLS Label Header

2.2 MPLS Architecture

MPLS has a new technology which operates on labels. So the network components required by this mechanism should have the ability to route the label attached to the packet IP header. The MPLS domain is mainly divided into 2 parts.

1. MPLS Core.
2. MPLS Edge.

The MPLS core consists of a set of label Switch Routers and the MPLS Edge consists of Label Edge Routers with the LSPs connecting them.

Figure 1: MPLS Operation

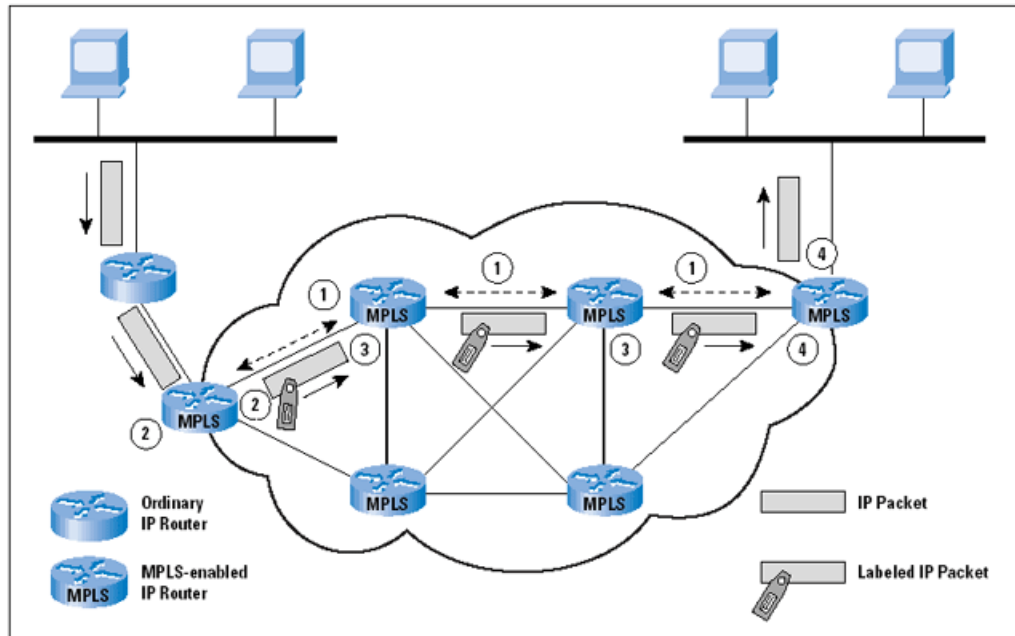


Figure 2.3.: MPLS Operation

The main terms used in the MPLS Architecture is discussed below:

Label Switch Router: This type of Router belongs to the MPLS Core. These routers are placed in the middle of the network. LSR is responsible to route the packet in the MPLS domain with the help of the label attached to it and then removes the old label from the header and it attaches a new label before it forwards the packet to another router. LSR uses the label as an index to determine the next hop on the LSP of the network. Label Switch Routers generally swaps the label which was attached to the packet header which will reach to the next LSR with a new label which is attached by the LSR in order to help the router to find the next hop in the MPLS Domain [2].

Label Edge Routers: In any network based on MPLS Technology, there should be two Edge Routers and they are the Ingress Router and the Egress Router. The Ingress router is placed at the entry edge of the MPLS domain of the network and the label is attached to the packet header. The label consists of the routing information of what is the next hop in the shortest path of the MPLS Domain. The Egress router removes the label from the packet at the exit of the MPLS Domain. After the Packet exits from this router, it enters the IP Domain [2].

Forward Equivalence Class: FEC is used to explain a set of packets with similar or identical characteristics which are routed in the same way. This means they may be bound to the same MPLS label. Each packet is assigned with FEC at the Ingress Router.

Label Switched Path: A Label switched path is generally formed by various signaling protocols like RSVP etc. It generally starts at the ingress router where the label is attached and the packet is forwarded based on the outer label. It reaches the router where the outer label is removed and it pushes to the next router with a new label attached to it. This process continues until it reaches the egress router where the label is completely removed from the packet. There exists multiple LSPs in the network. LSPs are unidirectional and enable label switching along the path. Since the forwarding of packets through an LSP is opaque to upper network layers, an LSP is also referred to as MPLS tunnel [8].

Label distribution Protocol: LDP is responsible for distributing the packets between LERs and LSRs in the MPLS Domain. Labels are communicated between the LSRs and LERs with the help of the Label distribution Protocol [8].

MPLS has traffic management and QOS mechanisms to manage flow of traffic. Some of the traffic management capabilities include traffic policing and congestion management [9].

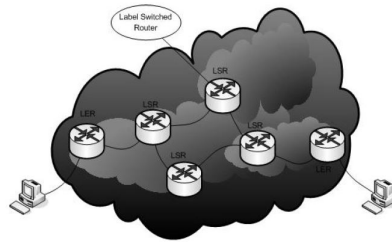


Figure 2.4.: LSR and LER of MPLS Communication

2.3 MPLS Network Design

LSR runs the MPLS Protocol to provide label binding to FEC, IP packet forwarding and also carries the IP forwarding technique.

MPLS architecture is mainly divided into two planes:

1. Data Plane: The Data plane contains all the information which is required to transfer the packet.
2. Control Plane: This plane consists of the transfer information and the routing information across the network. The routing information is mainly obtained through the network protocols like OSPF, EIGRP etc. Routing is mainly done by updating the label bindings exchanged between the routers [10].

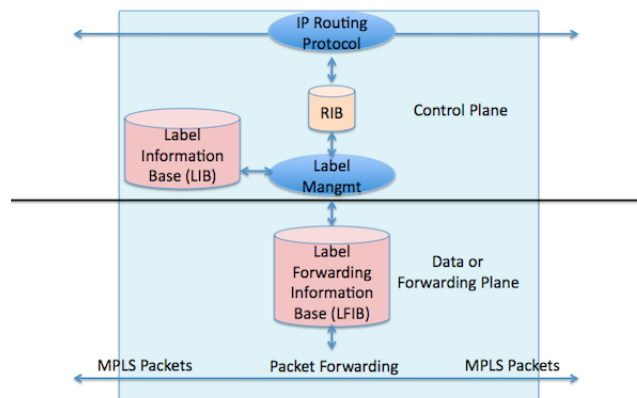


Figure 2.5.: Different Plane Operations in MPLS Communication

2.4 MPLS Functionality

The MPLS router mainly operates on two functional blocks:

1. The difference between data and control plane.
2. Label-Swap technique [9], [11].

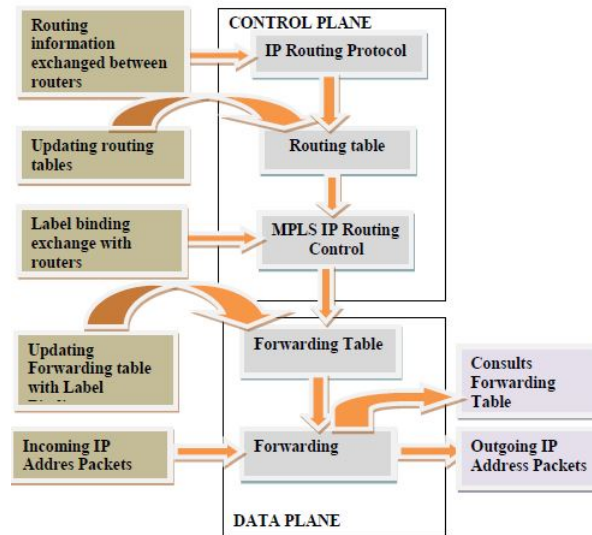


Figure 2.6.: MPLS Control Plane and Data Plane

The Control plane depends on the IP infrastructure by maintaining paths. In the MPLS Domain, the LSR maintains a forward information base which is used to update the forwarding table. Based on the data in the forwarding table, a decision is to be made on selecting the next hop in the network. The separation of the two planes has an added advantage of deploying one technique for multiple services and types of traffic [12].

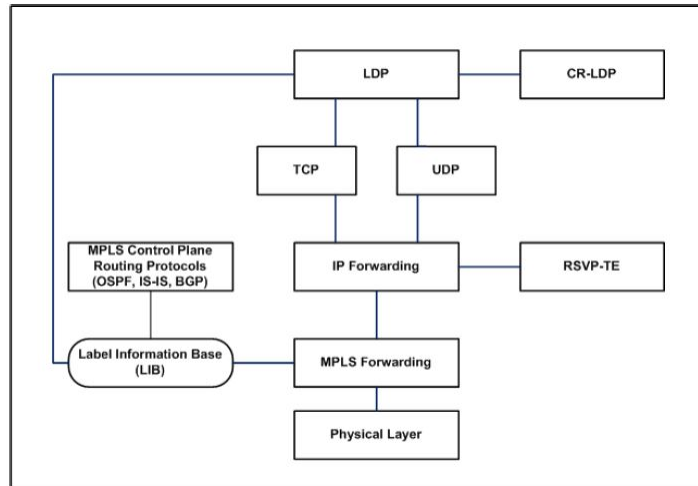


Figure 2.7.: Control Plane of MPLS

The Label Swap technique clearly explains how the packets are made to route in the MPLS. The entire technique is explained below:

1. When the data packet enters the MPLS domain, a fixed label is added by the ingress router at the start of the MPLS Domain.
2. The packets with the same FEC tend to forward in the same way across the MPLS Network.
3. The packets which follow the path with the help of labels reach the next hop in the network along the LSP.
4. All the network components in which LSR forwards the packet across the LSP based on the label value. At each LSR, the old label is swapped with the new label. This new label is the way to find out the next hop in the network.
5. Every hop of the MPLS Network always forwards the packet with the help of labels. It never looks for the long IP address. So this allows the routers to avoid going through the long and complex routing tables. This saves time and hence this technique is generally used for real time applications.

6. The technique of label swapping across the network between the LSRs is carried out until the packet reaches the egress router which is one of the label edge routers that is placed at the exit of the MPLS Domain. At the egress router, the label is completely removed. Clear understanding of the MPLS Functionality is explained in Figure 2.7 [11].

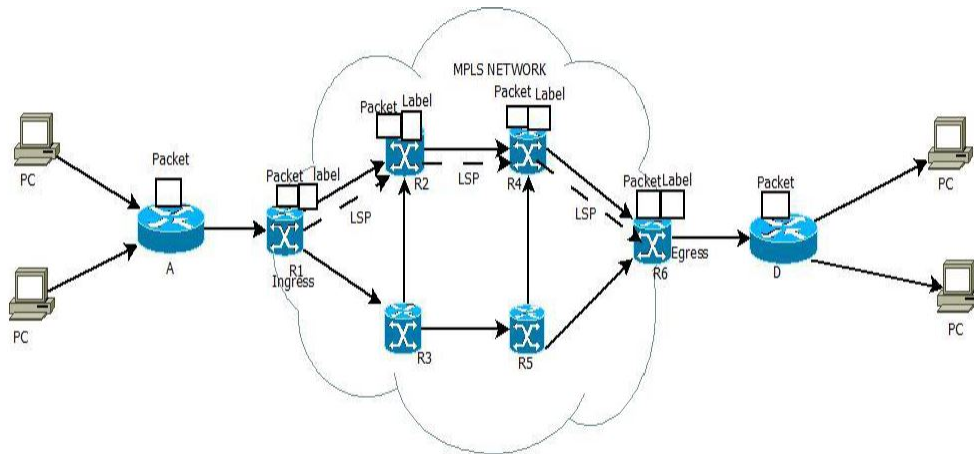


Figure 2.8.: MPLS Network Flow

MPLS uses certain Signaling protocols in order to set up the Label Switched Paths. All the packets are made to travel along the LSP.

In Figure 2.8, the label edge routers are R1 and R6 where R1 is the Ingress Router and R6 is the Egress Router. At R1, a label is added to the packet header which is the starting point of the MPLS Domain. With the help of the attached label, the packet finds out the correct LSP through which it is forwarded. The dotted line shows the packet's path from the Ingress Router (R1) to Label Switch Router (R2) [13].

When the packet reaches LSR (R2) the old label is removed and a new label is added which directs the packet to LSR (R4). The swapping of the labels is performed at LSR (R4) and the new label added to the packet is redirected to the Egress Router (R6).

At the Egress Router, the label is completely removed from the packet. After the packet gets processed at the router (R6) the packet no longer belongs to the MPLS Domain. It enters into the IP Network Domain.

2.5 Routing Protocols

MPLS uses certain protocols such as Open source shortest path (OSPF), Intermediate System-Intermediate System (IS-IS), and BGP Protocol to collect the topological information of the network. This topological information is then used by the routers such as LERs and LSRs to determine the routes across the MPLS network [14], [15].

These routing protocols are extended to implement the Traffic Engineering. These extended versions OSPF-TE and ISIS-TE have a traffic engineering database into which all the network topology is stored [16].

3. TRAFFIC ENGINEERING IN MPLS NETWORKS

Traffic Engineering is a technique which is used to control the traffic flow and maintain the network resources to optimize the performance of the network. Some of the important features of the traffic engineering are Resource Reservation, Fault Tolerance etc.

Important factors affecting the traffic Engineering are:

1. Path Selection.
2. Traffic Direction along the pre-computed path.
3. Traffic Management.
4. Topology Information distribution [17].

Path Selection: The path which is used to traverse the packet along the network needs to be computed with the help of several link parameters like delay, jitter, Bandwidth etc. The optimum path is selected among the various paths available across the network.

Traffic Direction along the pre-computed path: The path selected based on various constraints is mainly obtained through the forwarding table. The packets which need to travel should go along this path for better network performance.

Traffic Management: The traffic which is forwarded along the path should have some desired quality. The quality measurements can be based on certain network measurements such as voice packet delay, throughput, voice jitter etc.

Topology Information Distribution: It is very important for each and every node in the network to know about the entire network topology in order to route the packets in the correct way. The network topology information should be known by every network node and this is needed to create a network map at each node in the network.

Traffic Engineering is very efficient in the case of MPLS Networks because of the better quality of the service and efficient use of all the provided network resources. The main basis for the traffic engineering is the constraint based routing which considers network topology, Bandwidth etc. and uses certain IP routing mechanisms such as OSPF or IS-IS which accurately calculates the shortest path through which the data packet can pass through for establishing the network path to forward packets in MPLS networks.

Traffic Engineering is set to provide certain capabilities which are to be integrated to layer 3 so that it optimizes the IP traffic routing.

The main functionalities of Traffic engineering are:

1. It enhances the performance of conventional IGPs like OSPF, IS-IS to map the packets to a specific traffic flow.
2. It allows sending the traffic across the network with the help of MPLS Forwarding.
3. With the help of all the resources available across the network, it decides the best route for the traffic.
4. It deploys Constraint based Routing across the network for the flow of traffic to follow the shortest available path which should also obey the network constraints.
5. In MPLS TE the traffic has bandwidth requirements, certain priority and so on.

6. Another major functionality of the MPLS-TE is the efficiency in the case of any network failures such as node or link in the network. This node or link failures results in the change of entire network topology. This change of network topology should abide by the new set of the network constraints [18].

3.1 Working Of MPLS-TE

Since MPLS is the integration of both layer 2 and layer 3 technologies, so by making layer 2 features accessible to layer 3 MPLS can enable the traffic Engineering. MPLS traffic engineering establishes and also maintains the label switched path in the network backbone with the help of certain signaling protocols like RSVP and CR-LDP. The path which is along the LSP is mainly determined by the network resources and resource requirements. This path availability calculation for LSP in the network with the help of available network resources is the main concept behind constraint based routing [19]. The Interior Gateway Protocol (IGP) such as OSPF, IS-IS routes the packets onto this calculated path automatically. In a brief way one can say that any data packet which cross through the MPLS Backbone should travel on a single LSP which connects Ingress router and Egress router [15].

3.2 Constraint Based Routing

The different aspects of traffic engineering are the availability of resources and various other network characteristics on the links of the network. With the help of the resources a good and efficient path is chosen along the LSP paths. Link state Routing protocols involves in updating the network with any metric or topology change and these routing protocols are responsible to efficiently route the information related to the network resources availability with the help of which an appropriate path is chosen. These link state routing function will let other routers to know about attached networks and network resource information and other related information. This information is required in future to perform Constraint-based SPF.

Constraint Based routing is mainly the extension of the Shortest path first algorithms. It mainly calculates the path with the help of the network resources like the amount of bandwidth available for a link for an optimum end to end delay. In Constraint based routing the path is mainly selected on the basis of the procedure which involves, deleting the paths with less available bandwidth or the paths that does not satisfy the network constraints. The path which is provided by constraint based routing may be longer but it is lightly loaded and is better compared to the heavy loaded shortest path [20].

3.3 Prerequisites of the Signaling protocols to be used in MPLSTE

Below is the list of pre requisites which are required by the signaling protocols:

1. Scalability: It is very important for the signaling protocol to handle large number of the LSP's in the network which is large. So the signaling system should be scalable so that it can deliver the optimum performance even when the network is large.
2. Reliability: It is very important to deliver the data packet even when there is a failure in the network. So it is very important for the signaling protocol to be very reliable.
3. Re-Routing Capacity: To deliver any real time application data across the network it is very important to have back up plan to handle the network data in case of failure. So it is important to have a re-routing capacity for failure recovery and resilience in the network.
4. LSP Maintenance: It is very important for signaling protocol to provide LSP establishment and should have the capability to maintain it [7].

3.4 Signaling Protocols in MPLS-TE:

A Signaling protocol is the protocol which is used to identify the connectivity between two networking components [13]. Signaling protocols also provide some advanced features like LSP Explicit routing, resource reservation and looping prevention.

In MPLS Networks, there are two ways of establishing the LSP across the network. First, is the control driven LSP where the LSP is set up using the LDP protocol. This type of LSP is also called as hop-by-hop LSP. This type of control driven LSP involves the process of LSR in determining the next hop with the help of the forward table of IP after which each LSR sends the label request to the next hop for LSP establishment. This process is carried on until the whole LSP reaches the other edge router (egress router) in the MPLS network [21].

The other way of establishing the LSP across the network is explicit routed LSPs. This is also called Constraint based routed LSPs. This type of message passes through all the hops in the network along the specified route. At each hop on the route, a label request is sent to the next hop on the LSP. The major difference between the two approaches is that the packet in a control driven approach will always follow the path specified by the IP routing table whereas CR-LSRs are generally set by the network administrator or a management application on which the traffic is sent. These type of LSPs unlike the control driven LSPs are independent of the LSP computed by the IP routing mechanism. So it is always recommended to use CR-LSPs for traffic engineering in MPLS Networks [21].

Two Protocols which are used to set LSPs in MPLS are:

1. Resource reservation Protocol (RSVP).
2. Constraint based routed LDP (CR-LDP).

3.5 Resource Reservation Protocol

Resource Reservation Protocol is a Transport layer protocol. It consists of a set of communication rules which allows the paths on the network to be reserved for transmission of any high bandwidth message. It is generally considered to be a soft state protocol [22].

In the earlier switched networks, RSVP is mainly used by the host in order to place a request for QOS for a network data stream to transmit across the network. Routers in the network also use this RSVP to reserve the network resources and also to ensure the requirements for QOS on each path are met or not. The Routing protocol is decided on the paths on which the packets are routed and RSVP Signaling protocol ensures that the all the requirements for the QOS are successfully met for the paths selected.

RSVP for the traffic engineering in MPLS networks has an extended version known as RSVP-TE [23]. This extended version has many additional specifications which are mainly focused onto the differentiated services for MPLS traffic engineering networks. RSVP-TE is used to support both the resource reserved explicit routed LSPs and explicit routed LSPs which are not reserved. Since traffic engineering is also used to avoid loop formation in the network and to provide a re-routing mechanism in the network, RSVP-TE provides all the functions as stated.

Re-Routing mechanism should be done in a very efficient way so that traffic flow is not disturbed due to the rerouting process. The ideology behind RSVP-TE is to make before break. To achieve this idea, a new tunnel is forwarded well in advance before the old link is torn down.

RSVPTE will provide the sender with MTU which is available on the LSP extending from sender to receiver [23]. The ingress LER should always verify the MTU and also should ensure all the outgoing packets size should not be more than MTU. The information which is more than MTU is fragmented and then sent on the network.

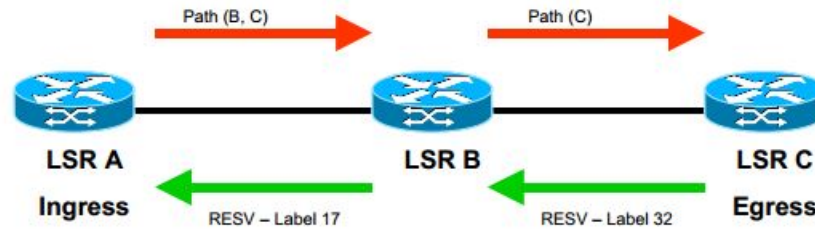


Figure 3.1.: Network Reservation in RSVP

3.5.1 Different Ways of Reservation

There are in total three ways of reservation. It is not the sender who decides on which reservation style to use in the network.

1. Fixed Filter (FF): This type of reservation has unique reservations among various explicit senders. Video applications and any other unicast applications generally use this style of reservation. In both video and unicast applications, flows require a different reservation for every sender. So this reservation always creates a separate reservation for each sender and this type of reservation cannot be shared with other senders which lead to the point to point LSP for every pair of sender and receiver [7].
2. Wild Card Filter: This type of reservation style consists of the shared reservations among all the wild card senders. Wild card senders are a way in which all senders are selected at once and then all participate in the session. An example of wild card applications can be an audio sample where the sender transmits the data stream. Generally only a few of the senders are sending the data at a time. This type of flow need not have any separate reservation for every sender. The result of this is a multi-point to point LSP.
3. Shared Explicit (SE): In this type of reservation, a receiver specifies to the sender that the particular sender needs to be included.

3.5.2 RSVP-TE Messages:

RSVP-TE mainly uses two types of messages. They are:

1. RESV Message.
2. Path Message.

RSVP Path Message: This message is first generated at the head router and then it is forwarded along the network. At every hop, this message always checks for the network resource availability and saves the information. This path message will work as the label request in the MPLS-TE domain. The path message is used by the LSR which needs to establish LSP to the receiver [24].

RESV Message: This is called the Reservation message. It is created at the tail end of the MPLS Domain. This message is the reply to the path message. Path message functions as the reservation request and RESV message functions as reservation confirmation. The receiver always replies with the RESV message to the sender from whom the receiver gets the path message [24].

RSVP-TE contains five new entities to RSVP. The objects with the messages are stated in the figure 3.2.

In the figure 3.2, a complete network flow with RSVP is provided. In this a sender sends a PATH message to the intermediate router. The Router then transmits the path message to the receiver block. When the receiver is available, it sends the acknowledgment signal in terms of RESV message. This message is passed through the intermediate routers and then it reaches the sender. As and when the sender gets the RESV message which indicates the resources are allocated in the network and the network is ready for communication, data is sent along the link on which the reservation is made in the earlier steps in the network.

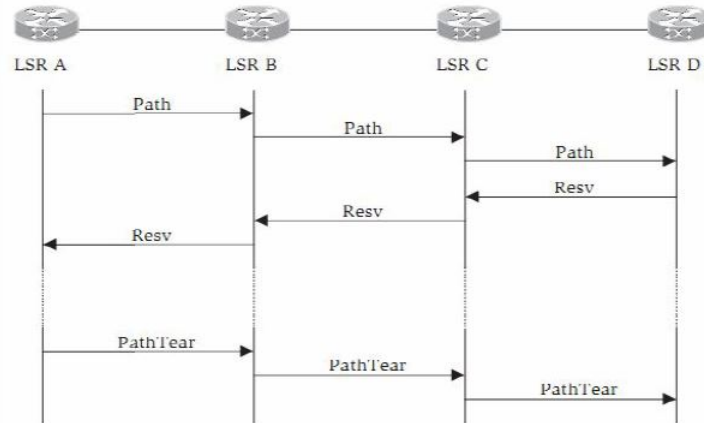


Figure 3.2.: Messages Flow in RSVP Signaling Protocol

When the transmission of data is completed, it is time for the termination of the communication. In order to carry out this functionality, an RESV tear message is sent from the receiver indicating that the communication process has reached an end. When the RESV tear signal reaches the sender the sender will now stop communication which means it stops sending data packets along the network [24].

One advantage of using RSVP-TE in a network is its independence over IGP. RSVP-TE will not follow the IGP Shortest path, and LSP is created along the multiple IGP as required. The flow of RSVP Messages are found in the figure 3.2. RSVP messages exchange between LSR-TE to setup a TE-LSP in the network and the network flow includes the following:

1. Path Message.
2. Resv Message.
3. PathTear Message.
4. PathErr Message (Generates if the LSP setup is failed).
5. ResvTear Message (It is generated by the Egress Edge).
6. ResvErr Message (It is generated when an LSP gets preempted).

The creation of LSP in RSVP-TE is started by the edge router (Ingress) in the above diagram it is LSR A by transmitting the Path Message. The destination address of the path message will be another edge router which is egress router in the figure 3.2. RSVP-TE is set to transmit the set of network nodes which are not part of the shortest path in the network. In order to include the participation of an intermediate LSR the path message has an option of Router Alert which is turned on. This Router alert option is used to alert the LSR that the packet needs to have a very close inspection and if needed make the necessary modifications to it.

3.6 Label Distribution Protocol

LDP includes a set of messages and methods which are mainly used by LSRs to create LSPs in MPLS networks. LSRs can do this by linking the network layer routing information to the layer 2 switched paths.

TCP is mainly used as the transport layer protocol for LDP sessions. For the setup of multiple LDP sessions, multiple TCP Sessions are created, one for each LDP Session [25].

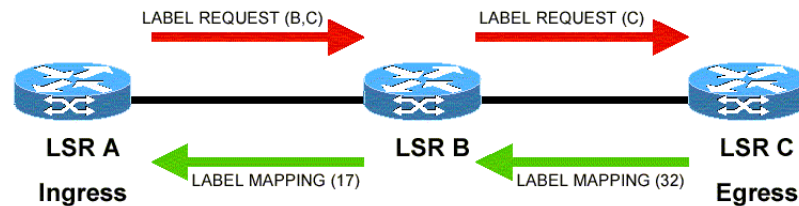


Figure 3.3.: Labels Flow in LDP

3.6.1 LDP Messaging Technique

For the information exchange LDP has four types of messages which are sent among other LSRs. Messages are:

Discovery messages: These are the Hello Messages which are used for multi casting to the adjacent neighbors with the help of UDP. These messages are used for the maintenance of LSR in the network.

Advertisement Messages: These type of messages are mainly used for creating, modifying the labels which are already existing for a particular FEC.

Session Messages: These are used to handle the sessions by creating, modifying and deleting them in between the two peer LSRs.

Notification Messages: This message is used to provide some advisory information and also to detect the error [26].

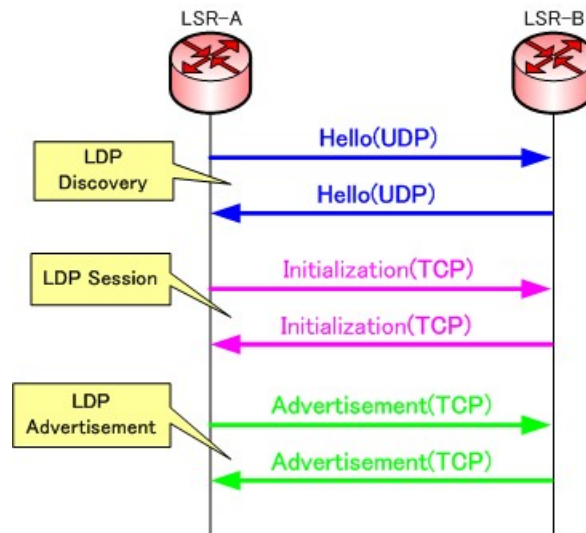


Figure 3.4.: Messages Flow in LDP

3.6.2 LDP - PDU and other procedures:

The PDU mainly consists of a header and one to many LDP messages. The figure 3.5 shows the LDP PDU.

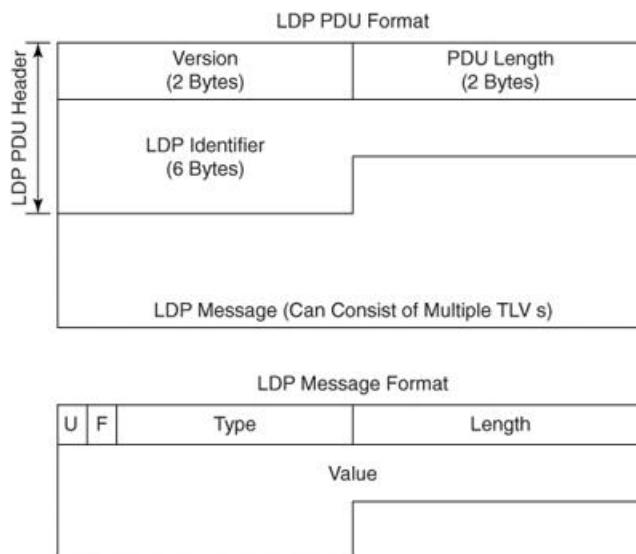


Figure 3.5.: LDP PDU Label Format

The various fields of LDP PDU are discussed below:

1. The various fields of LDP PDU are discussed below.
2. Version: It gives the LDP protocol version number.
3. PDU Length: It gives the information about the total length in octets by removing version field and PDU length.
4. LDP Identifier: It is used to uniquely identify the senders LSR label space.
5. U Bit: It is used to give information about unknown type length value (TLV).
6. F Bit: After U bit is set, F bit gives the information whether unknown TLV should be forwarded or not.
7. Type: it has the knowledge about the way to interpret the type value.

The main functions of LDP are:

1. Session Management.
2. Label distribution.
3. Error notification.
4. Advisory information.
5. Peer Discovery [26].

LDP can't provide the support for traffic engineering but it can set up the control driven label switch paths.

3.6.3 Constraint Routing Label Distribution Protocol

Certain extensions are added to the label distribution protocol so that it can support constraint based routed label switched paths (CR-LSP) and the resulting in the protocol which is known as CR-LDP (Constraint based routed LDP) can provide the features and benefits of traffic engineering. Some of the features of CR-LDP are given below:

1. QOS and traffic parameters.
2. Loop finding in loosely routed LSPs.
3. Managing individual LSPs.
4. Path re-optimizing and the followed changes in traffic patterns.
5. Ability to perform preemption of LSPs.
6. Notification of Failure and its recovery process [21].

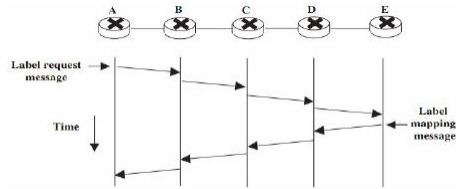


Figure 3.6.: Network Flow in CR-LDP

When the label message reaches the edge router (egress) along the shortest path, it then checks the resources which are available. If the message has the ability to accommodate a new LSP in the network it then assigns the label for that particular LSP and then sends the label mapping information. Each forwarding node then assigns the resources specified in label mapping information. In this way the CR-LDP is setup along the specified path.

3.6.4 CR- LDP Protocol Specifications

CR-LDP has the same data structure unit as its parent LDP. As it is the extended version of LDP it extends LDP by defining LSPID as a very important TLV for every PDU.

In LDP, TLV always encodes the message which has to be actually sent. The actual structure of the TLV mainly depends on the type of message. PDU can contain multiple number of nested TLVs. So every constraint is always encoded as a separate TLV. The table below will give the entire list of the constraint TLVs.

3.7 Differences Between RSVP and CR-LDP Signaling Protocols

The main differences between CR-LDP and RSVP are their reliability of the underlying transport layer protocol. The differences are also based on the way the resource reservations are performed. The resource reservations can be in forward direction or in backward direction.

Constraint TLV	Summarized Explanation
Explicit Route (ER -TLV)	It points to the path chosen by the LSP which is being set up
Explicit Route Hop (ER Hop)	It indicates whether the ER-Hop value is strict or loose.
Preemption TLV	It specifies LSP priority level (lease ,default or highest)
Traffic Parameters TLV	It specifies one traffic parameter value (which means PDR ,PBR , CDR ,CBS ,EBS)
LSPID TLV	It perfectly points every CR-LSP in the MPLS network
Resource Class TLV	It specifies what links are accepted for CR-LSP
Route Pinning TLV	It prevents the modification of the path which is then followed by the loosely routed LSP at the case of when better path is discovered.
CR-LSP FECTLV	It indicates the Forward Equivalence Class (FEC) that belongs to a specified CR-LSP

Figure 3.7.: Summary Explanation of Constraint TLVs

There are various factors which are similar in case of both RSVP and CR-LDP protocols and there are certain differences which are the points to discuss about the preference of choosing one signaling protocol [13].

Below are the factors listed which are the consideration of their similarities and the differences:

1. Transport: CR-LDP supports TCP layer protocol whereas RSVP functions on Conventional IP networks.
2. Security: Security of data is ensured in both the signaling protocols.
3. Multipoint to Point: Both Signaling protocols provide communication between multiple source to a single destination.
4. LSP State: LSP state is hard in case of CR-LDP and soft in the case of RSVP Signaling technique.
5. LSP Refresh: LSP needs to be refreshed periodically in the case of RSVP whereas it is not required in CR-LDP.
6. LSP Protection: Both signaling protocols provide LSP Protection.

7. Shared Reservations: Reservation of network resources are not shared in CR-LDP Signaling whereas they are shared in RSVP.
8. Traffic Control: A large extent of traffic control is done in forward direction in CR-LDP signaling but in the case of RSVP the traffic control is performed in the reverse direction.
9. Rerouting: Both CR-LDP and RSVP supports the rerouting mechanism in the case of network failure.
10. Policy Control: CR-LDP provides implicit policy control whereas RSVP provides explicit policy control.
11. Multi cast support: Both signaling protocols do not provide multi cast communication.
12. Resource class constraint: CR-LDP signaling always supports resource class constraint whereas RSVP does not support it.
13. Route Pinning: Route pinning is supported by both protocols but in the case of RSVP it is performed with the help of path recordings.
14. Layer 3 protocol indication: Layer 3 protocol is not indicated in CR-LDP Signaling but is well specified in RSVP.

3.8 Advantages and Disadvantages of Signaling Protocols

Below are the various advantages and disadvantages of Signaling protocols.

1. Transport: CR-LDP supports TCP layer protocol whereas RSVP functions on Conventional IP networks [13].
2. In the case of CR-LDP QOS is very relative but the RSVP Signaling has the ability to give guarantee for QOS.

3. CR-LDP is comparatively simple compared to RSVP [13].
4. In CR-LDP LSPs are formed for every network element which is present in the routing table. There is a redundancy in the excess presence of unusable LSPs in the network.
5. The disadvantage of CR-LDP is its limitation to provide QOS capability. EXP bits are used to incorporate the QOS with LDP. This relative QOS is basically related to priority and queue scheduling. It is highly impossible to provide a guarantee with the help of relative QOS but if enough resources are available then this situation can be handled very well [13].
6. RSVP-TE will create a particular LSP when all the parameters for that LSP are manually deployed. If all the parameters satisfy the information in traffic engineering base, RSVP-TE signaling is used to establish the network connection. The parameters will include destination and will also contain link attributes requirements, bandwidth requirements, explicit route requirements, fast re-route information and also backup information.
7. In the case of CR-LDP, QOS is very relative but the RSVP Signaling has the ability to give a guarantee for QOS.
8. One disadvantage is that each LSP in the network is manually configured. If the network is very huge with a large number of routers, and if there is a need to create an LSP between each router to every other router, then the number of LSPs which needs to get created in the network will grow exponentially with respect to the number of network routers. Manually configuring this many LSPs is a very tiresome task. Also if there is a case where one node is failed or removed from the network, then there is need to reconfigure all the LSPs in the network manually because if there is one change in any one network element, the entire network topology is changed [13].

9. When there is a change in the network topology, change which means addition of a node or any deletion or position change of the network node, then directly attached neighbors of the new node or the changed node will have both RSVP and LDP sessions. The RSVP LSPs are limited to only the next hop but LDP will perform the function of advertising the labels for this new node addresses or changed node address to all the remaining nodes in the network [13].

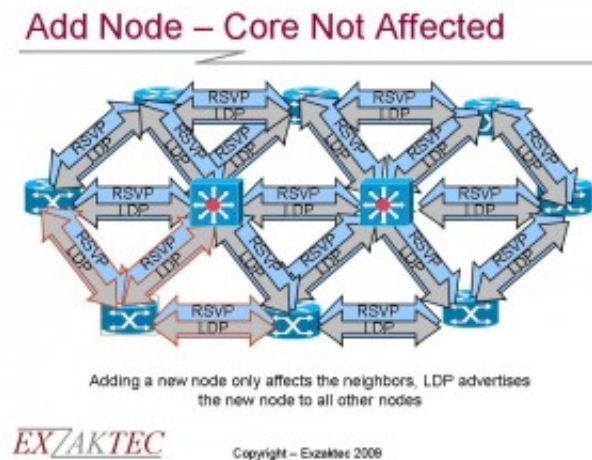


Figure 3.8.: Flows in the LDP Network with Network Topology Changes

There is no problem in implementing both signaling protocols on a network. For best effort traffic and for the users who want an inexpensive type of service providers use CR-LDP LSPs [24]. The same providers can also use RSVP-TE for those customers who are ready to pay extra for bandwidth guarantee and ultra-reliability.

In this case LDP does not perform over RSVP-TE but LDP signaled LSP runs through a tunnel formed with the help of RSVPTE. LDP over RSVP-TE is mainly related to the control plane in the network [13], [24].

The main idea is to use both protocols in order to setup LSPs in the implementation which is performed in a nested way. In this case LDP is mainly used at the edge of the network whereas RSVP-TE is used in the core of the network and RSVP-TE also acts as the link which connects two LDP elements [27]. The main advantage of

this method is the number of LSPs in the core is lowered and forwarding tables are always kept very small. Another main advantage is that of implementing FRR in the core which leads to avoiding the long convergence timings to keep optimum traffic flow.

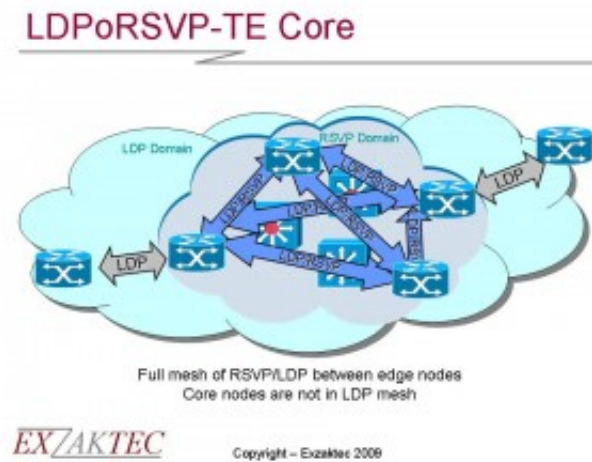


Figure 3.9.: LDP over RSVP TE

The main idea of this implementation is to build point-point TE tunnels to directly connected neighbors. These TE tunnels will go on a hop by hop basis and not an end to end basis. When LDP is performed on these TE tunnels, the sessions are created to the directly attached neighbor. Since all these sessions are passing through the tunnel, the LDP session is mainly aimed even when the neighbor is directly connected [27].

4. FAULT-TOLERANCE IN MPLS-TE NETWORKS

The real time applications require a guaranteed service operation not only at the time of normal condition but also at the failure condition. End system applications are not implemented for connection reliability over TCP. TCP can support the system to undergo retransmission and reordering of packets. Real time applications like television and telephone always use UDP as an underlying protocol for transportation [28]. UDP is considered to be a connectionless protocol and IP provides the best delivery techniques. IP cannot do anything if the network has network failure or any packet loss due to failure. It completely depends on the end system for the solution. It is also not feasible to construct a data flow which is lost along the path. The number of packets which are lost during the failure scenario or during any re-convergence period can have severe effects over the network service quality [28].

The first way to provide recovery in the network failure is to provide protection over layer 1. This type of protection has the restriction because the network is the set of different links which are connected to different devices and not all of them provide SONET connections. SONET APS (Automation Protection Switching) is one of the protection techniques for layer 1 protection. But this SONET APS is the hardware solution for the network failure problem. MPLS-TE faces this solution of failures in terms of Fast Reroute techniques which will help the network operators within the MPLS domain to provide strict QOS guaranteed for the system requirements [28]. Before implementing this MPLS-FRR function, TDM (Time division Multiplex) is used to carry the traffic with Service level Agreements.

The MPLS FRR mechanism is not limited to only a particular link type and it does not require any extra hardware. It also provides fast reroute in the case of node and link failures and the switch of the traffic is a very fast process. APS techniques provide 50ms fast convergence switchover on a backup path.

Even though there is a fast recovery process by switching the traffic over the backup path at point of failure, there is a need to detect the failure very quickly or else there is no importance for the fast failure recovery. The amount of traffic that is lost mainly depends on the point of how fast the failure is detected.

4.1 Fast Failure Detection

The capability of detecting the failure in a network is the foremost step in the failure recovery process [29] and the failure detection is done at the proximity of the physical layer in order to achieve high efficiency. There are some transmission media which indicate when there is a loss in connectivity and break in the transmission link; this detection is done very quickly and the time is equal or less than tens of milliseconds. But this type of hardware detection is not always available in case of network failure. So the failure detection is performed by the higher layer protocols. They are:

1. IGP Failure Detection.
2. RSVP Hello Detection.
3. Bidirectional Forwarding Detection (BFD).

4.1.1 IGP Failure Detection

The neighbors of IGP will always exchange the control messages known as Hello messages with each other so that it can maintain the connectivity in the network. When a hello messages arrival is stopped, it is assumed that there occurred a failure in the network. Hello and dead timers are descriptive entities in the IGP configuration table and they are used to provide the minimum bound for failure to get detected. This provides the reason for the low performance of Hello based detection because using IGP hello cannot provide fast detection times.

1. An IGP neighbor is able to miss more than one hello message by not taking into account the opposite end as dead. The time taken for failure detection is 3 sec for OSPF and the time taken by IS-IS is 1 second [30].
2. IGP hellos handling is very difficult and very expensive in terms of CPU cycles. Hello packets are processed by the CPU and they keep track of the dead timer for a specific neighbor to be considered dead. The Timer is reset when the hello packet is reset and processed by the central CPU.
3. IGP failure detection starts with the set of steps which are needed to be performed once a change in the network occurs [30].

4.1.2 RSVP Hello Detection

As RSVP is a soft state protocol which requires periodic refreshment. RSVP Hello Operation will enable the RSVP nodes to detect when the adjacent node is not reachable. This is known as node to node link failure detection [26]. RSVP hello settings are needed at two sides of the link. RSVP help based detection is considered sufficient for failure detection in local protection and its switchover time is much faster than conventional IP or MPLS-TE without any fast reroute. A very large number of Hello messages are transmitted between two adjacent LSRs resulting in very high utilization and heavy loading on the router resources. This Hello instance is created only one time when it is required and gets removed when it is of no use.

4.1.3 Bi-Directional Forwarding Discovery

BFD is a very lightweight protocol which was developed for fast failure detection by IETF. BFD detects the failure in both directions between two forwarding elements in a periodic manner at a constant rate [24]. This can function in echo mode, without causing the other end to participate in starting the BFD. BFD control packets are utilized to detect failures like the Hello protocol but in a very high rate. BFD indicates

the forwarding element just once as it can detect the fault to the forwarding element. BFD has the advantage of reducing the switch over time because the detection time of the failed network is in the range of tens of milliseconds [28]. This is a very high range of improvement for the detection time in the order of seconds. BFD can be deployed on an interface basis or the routing level.

4.2 MPLS-TE Protection Mechanisms

MPLS-TE LSP is greatly benefited by the use of BFD fast detecting mechanism. The next process for the fast failure recovery technique is the way to protect the traffic loss over a logical resource like LSP from a physical failure of the network element (Node or Link). MPLS-TE has the capability to provide a wide range of protection techniques to ensure the guaranteed quality of service in IP/MPLS networks. Each technique has its own benefits and drawbacks inside the MPLSTE domain.

4.2.1 Path Protection

The complete network protection in the terms of the end to end is mainly desired. A common technique for the path protection is to utilize the secondary path in addition to the primary path for the resilience purpose. MPLS Path protection provides the solution to these types of scenarios where the primary path is the LSP tunnel. With the help of path protection, a secondary LSP is then generated in addition to the primary LSP, that passes through the set of LSRs which are along another Shared Risk Link Group (SRLG) than the primary path SRLG. The secondary LSP needs to be signaled in advance of the time because initially it is in standby mode [31]. There is an equal ration of relation between the primary and the backup tunnel as they can have the same network characteristics.

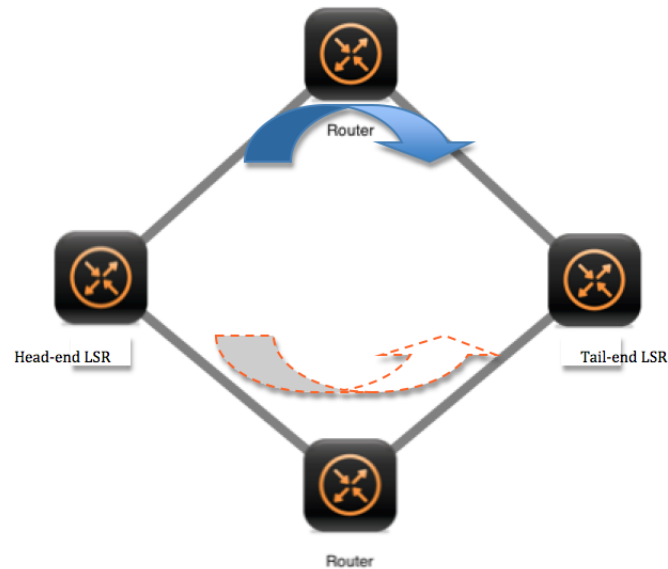


Figure 4.1.: Path Protection Technique

SRLG is the set of links which are affected by the single incident, so this group of resources is affected by the single failure situation. Once the fault is detected along the primary LSP, an RSVP Path Err message is started from the point of failure and then forwards towards the start end. When this error message arrives, the head node LSR shifts the packet data over the already set secondary path [21]. A path protection may result in providing unnecessary protection in the case of links along a path which are protected by other techniques (APS) [24].

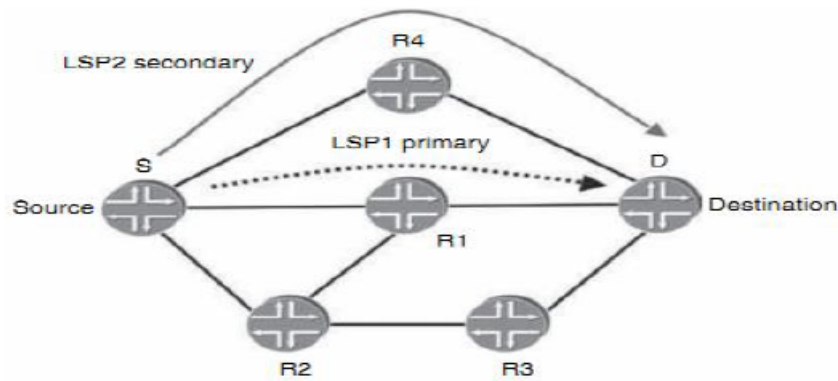


Figure 4.2.: Secondary LSP in Path Protection

Advanced path protection can be obtained by utilizing multiple backup paths [31] for a single LSP with the restriction that can only signal one backup path in advance. Path diversity can be taken into consideration for multiple backup paths. With the path protection it can be made sure about the exact path taken by the traffic if there occurs a failure [24].

4.3 Local Protection

In order to reduce the failure detection time at the head LSR during which the traffic is lost, protection should be applied at the proximity of point of failure [29]. Local protection tries to fix the issue which is inheriting by the path protection by providing the local protection by not involving the head LSR for rerouting the traffic. Local protection achieves the fast failure detection with the help of FRR mechanism. In FRR mechanism a detour is created around the failed network element. It also have the benefit that not only the traffic will flow locally on the repaired path but RSVP Signaling will also flow over it and the traffic engineering tunnel will be signaled for the time frame of FRR on the failed element. MPLS FRR is implemented locally, besides IGP convergence which is considered to be distributed operation and IGP operated nodes have to accept on the common topology before the traffic will start

flowing around the failed network element [28]. MPLS FRR is a locally operated repair method and the PLR(Point of Local Repair) has no complete view into the TED as head end, so it is convenient to choose one network element to protect. At PLR a backup tunnel is merged with the primary path just in advance of the failed resource at the merging point (MP). Compared to the technique used by the Path protection(end to end path protection), MPLS FRR has benefits of high speed of failure recovery and it also provides the deterministic delay of the order of 10s of milliseconds with BFD [28].

The two protection schemes which are available under the local protection are as follows [28]:

1. Link Protection.
2. Node Protection.

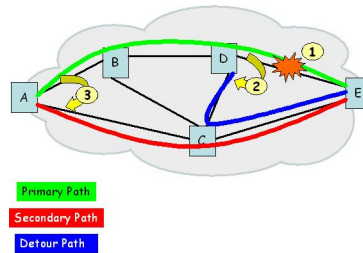


Figure 4.3.: Network with Link Failure

In the figure 4.3 the source is node A and the destination is node E. An initial primary path is created between node A and Node E via node B and node D. There is a complete end to end path protection which is provided by the secondary path via node C. The MPLS FRR technique provides the protection at the point of local repair by creating the backup tunnel at the link failure between D-E. The backup tunnel is formed between node D to node E via node C.

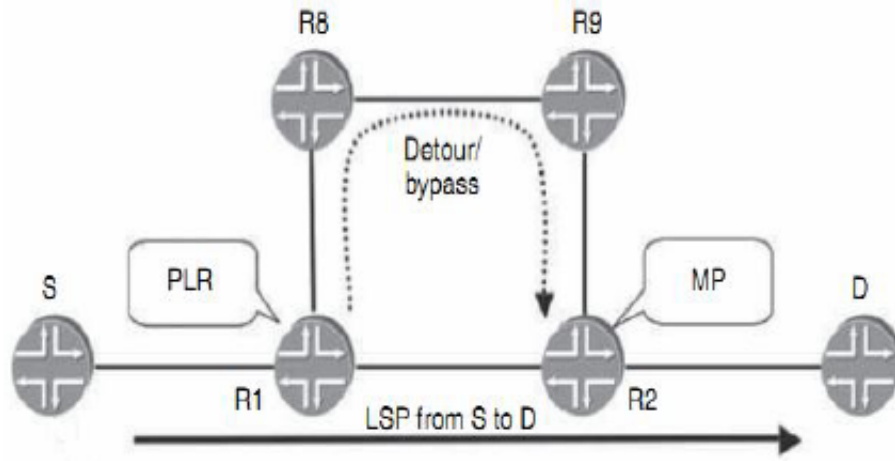


Figure 4.4.: Point of Local Repair and Merging Point in the Network

The number of LSPs which is protected by the protection tunnel can be 1:1 or N:1. These are termed as One to One backup or Facility backup [32].

One to One backup: When the failure occurs in the network, every FEC along the failed network element is backed up with the help of the tunnel for every FEC towards their particular destination.

Facility backup: The next hop which is followed by a failed node or the failed link is considered to be the merging point for the packet data which is traveling along the failed resource.

When the protection schemes are combined with some of the backup techniques, it results in the four different mechanisms for the MPLS FRR [33].

1. Link Protection with facility backup.
2. Link Protection with one to one backup.
3. Node Protection with facility backup.
4. Node Protection with one-to-one backup.

When an LSP requires the local protection, the head node sets the Local Protection desired flag in the RSVP Session Attribute object and Fast Reroute object for

the LSP. This type of local protection flag is considered by every LSP downstream. The downstream LSR which has the protection technique available with the help of the backup path replies to the head node with the Protection available flag [31].

4.3.1 Link Protection

The MPLS FRR technique which protects the link has a single TE link along the LSP which needs to be protected. All the traffic data which decided to pass over that link is protected by the bypass tunnel (considering the facility backup). The complete set of links which consists of all the TE LSP is backed up. LSP is unidirectional, so it can perform as a bypass tunnel. If there is a need for the two way communication then a backup tunnel is required at each side as the backup tunnel is unidirectional as stated above. The bypass tunnel which is used to provide the protection to the single link is known as the Next-Hop(NHOP) bypass tunnel [34]. This is named as the NHOP backup tunnel because the bypass tunnel is made to merge at the primary LSP at the next hop which is followed by the failed link. An NHOP tunnel can jump over many hops, but it is limited to merge at the next hop (MP) across the failed link. RSVP-TE signaling is used to create the backup tunnel and it also provides the label which is used over the NHOP tunnel [33], [34].

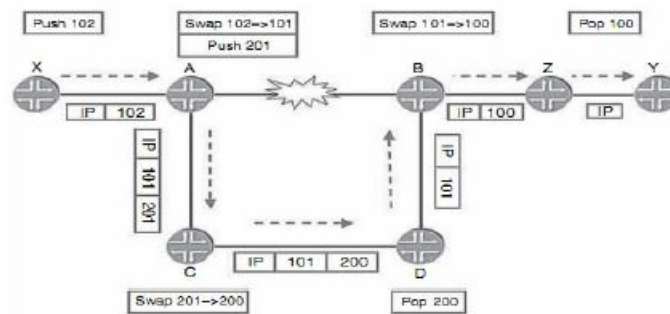


Figure 4.5.: Label Swapping in the Network with Failed Link

A single label is enhanced at PLR for the NHOP bypass tunnel (A-C-D-B), so this should be taken into consideration in advance by setting the MPLS MRU along all the links which are related to the NHOP tunnel. The major difference at LSR B is that the labeled packets will arrive from another interface, but it will not have any effect as long as per-platform label space is used [21]. LSR D will be the PHP router for this particular NHOP tunnel.

PLR will carry the traffic data along the NHOP tunnel for the time being. When the failure is first detected on the protected link, PLR then repairs the tunnel on a local basis and then it is made to propagate an RSVP PathErr message towards the head end reporting that the tunnel is locally repaired at a point along the downstream. When the RSVP Path message is received with the local repaired flag turned on in the session attribute object, the head router does not mark this tunnel down, but it keeps the forwarding traffic on it and it tries to calculate the best path to reroute the LSP traffic on the failed link [34]. The PLR controls the traffic and the signaling message (Path, Refresh message) along the failed link at the time in which the FRR is active. This is achieved by sending the control messages and traffic data over the NHOP bypass tunnel.

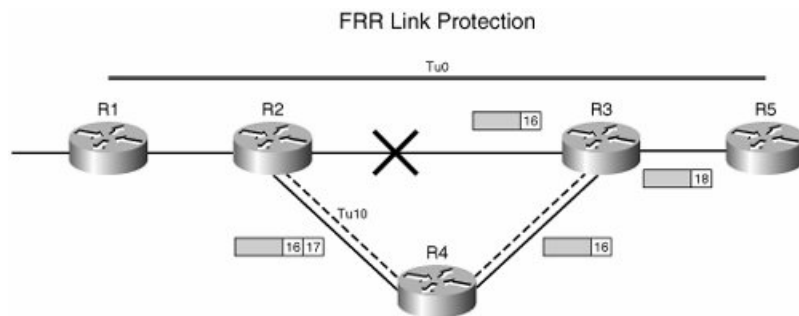


Figure 4.6.: FRR Link Protection for MPLS Network

IGP neighbors on both sides of the failed link will also update their link state when failure occurs. The IGP updates are sent to each and every router in the IGP and then they try to compute the path to reach the destination by not taking into account

the failed link. This IGP update does not have any effect on the tunnel head LSR, as it has gotten the RSVP Path Err message with the local repair flag set [30]. If the head end does not receive the RSVP Path Err message, it will then wait for the RSVP Path Err message and only mark the tunnel down when it receives the RSVP Path Err message without any local repair which is active from the downstream node. The advertisement of the IGP will reach the tail node LSR, but as the FRR link protection was desired on the protected LSP, the tail end will discard this update. The new sender is the PLR for the RSVP Path message; the tail end will know the path message that is coming from the new sender but it will belong to the same session and it will never create any RESV Tear message [28].

At a particular time the LSPs which are passing through the link will always reserve the bandwidth on the link. When failure occurs it is possible that not the complete bandwidth for the LSP is made available along the NHOP bypass tunnel so there are chances that the traffic might get lost [31]. Link protection mechanism will take advantage by terming it as the temporary repair, once the head end LSR establishes the new path, the data is switched onto the newly created LSP and resources which are reserved on the failed link are released using the Path Tear message [30].

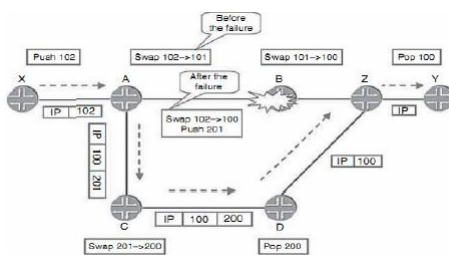


Figure 4.7.: Node Failure in MPLS Networks

4.3.2 Node Protection

MPLS FRR local protection provides the mechanism to provide the traffic data on the adjacent node. Node Protection will not only provide the node but also provides the link protection [35]. This is because the cause of the link failure is not known for sure most of the time. Failure can be because of the link itself or because of the next hop LSR which is down. PLR picks the node protection tunnel to forward the traffic data. This node protection tunnel is known as the Next-Next Hop(NNHOP) bypass tunnel.

The NNHOP tunnel avoids the protected node during the failure, but RSVP ERP still carries the IP address of the protected failed LSR even when the LSR is bypassed [35]. There are certain factors which are needed to be taken into consideration when using the NNHOP bypass tunnel. In the figure 4.7, it is visible that LSR A should know the details about the incoming label which is used by the main LSP at LSR Z and the IP address of LSR-Z.

The Address of the destination LSR is received from the RRO of the RSVP Path message or ERO of the RESV message. To obtain the label which is used by the incoming label at the tail end LSR which is LSR-Z, the RSVP Session Attribute object is extended with a Label Recording Desired flag [24]. When the session attribute object is received at the intermediate LSR, it then records the assigned label for the particular prefix in the RRO Label sub object. So when using the node protection, label recording is required and it should provide the label information at the particular node [35].

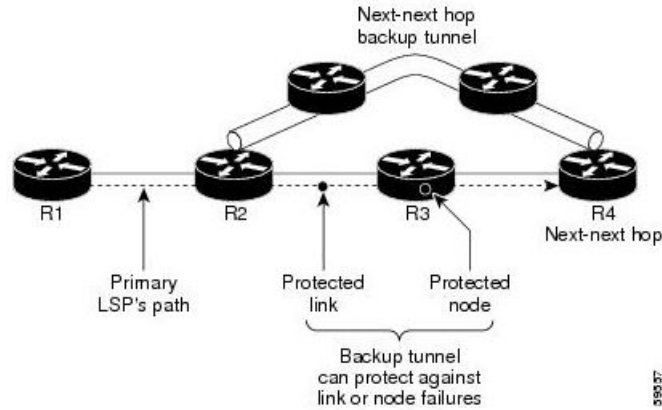


Figure 4.8.: NHOP and NNHOP Tunnel in MPLS Networks

In the figure 4.8 it is shown that the Next-Next Hop backup tunnel is created to provide the protection to both the node(R4) and also the link (R2-R3). Here in this case the head end LSR is node R2 and tail end LSR is node R4. The NNHOP Backup tunnel is between the node R2 and the node R4.

4.4 LDP Fast Reroute

The above mentioned local protection techniques are all based on the RSVP-TE signaling. But some important applications which are functioning over the LDP or in particular CR-LDP based MPLS-TE networks also require some resilience from the underlying architecture [33]. The main difference between CR-LDP signaled LSP and the RSVP-TE signaled LSP is mainly due to the fact that CR-LDP based CR-LSP will follow the IGP provided shortest path but RSVP is not influenced by any IGP-TE shortest path.

The tunnel based technique for LDP switchover provided can be one of the solutions once the traffic reaches the PLR and then this PLR will transmit the traffic on the RSVP-TE signaled bypass tunnel towards NHOP or on NNHOP [33]. An end to end LDP fast reroute LSP can be created by establishing NHOP or NNHOP RSVP-TE tunnel across each and every node on the IGP shortest path and use the

LSP Switching mechanism to unite the separated RSVP-TE tunnels to make the end to end protection path. LSP switching is used to establish inter domain RSVP-TE tunnels in which the domain is responsible for routing traffic through its own admin domain. The established TE LSP across IGP path is susceptible to change the shortest path created by IGP over time and it is not guarantee that the packet data which is following the LDP path will reach PLR and also pick up the RSVP-TE backup tunnel [36].

A common solution to the issue is the alternate path approach [31]. The Alternate path depends on maintaining the alternate path towards the destination and taking into consideration this path as failure is detected at PLR. IGP routing protocols for traffic engineering did not utilize the alternate path. IGP uses the concept of the ECMP and so there are chances of two or more paths of existence between source and destination, so this results in load balancing on multiple paths. A new technique called IP LFA (Loop Free Alternative) is initialized so that it can add a pre-sigaled backup next hop into the plane. LFA provides the 50ms IGP convergence time by not adding the additional burden on nodes [33].

Failure detection initially occurs in the forwarding plane, which signals the information to the control plane. When the failure occurs, the routing protocol will perform the series of steps [37]. Loop Free Alternative (LFA) enhances the IP network's ability to give the loop free rerouting by not involving the control plane after the failure. LFA provides the local repair and the alternate path is pre-installed which will be activated locally when the forwarding engine detects the link failure. The Local repair path should be active till the time the global repair completes its task and IGP-TE area converged upon the TED. The paper [38] defines the process of transmitting the traffic over the Less Equal Cost Multi Path (LECMP), used specifically for the connectivity restoration. As long as the LECMP cannot create the loop, it can be used as an alternate path. LECMP which does not create the forwarding loops is considered to be the LFA. The LFA node performs the computation in advance to determine the backup path [37].

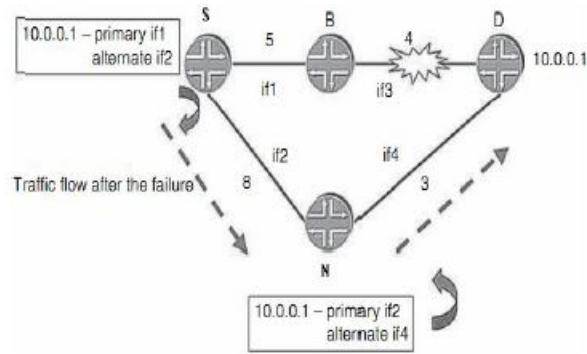


Figure 4.9.: LDP Fast Re Route in MPLS Networks

In the above criterion, the source S which requires the LFA. N is the neighboring LSR. D is the Destination node which needs to attend through LFA. If the above criterion is satisfied then N is considered to be the LFA for source S with respect to the destination D, computation can be performed by any traffic engineering enabled node because the LSR will share the common topology.

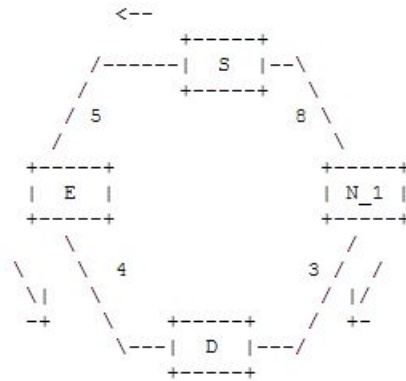


Figure 4.10.: LDP Fast Re-Route LFA in MPLS Networks

4.4.1 Node Protection

For an alternate next-hop N to protect against node failure of a primary neighbor E for destination D, N must be loop-free with respect to both E and D. In other words, N's path to D must not go through E. This is the case if Inequality 3 is true, where N is the neighbor providing a loop-free alternate [37]. If the path from source to destination contains a node which is failed which means if node E is failed, the neighbor N whose path to D crosses through the node E which is failed, then there is no chance of the connection from the source to destination [33], [37].

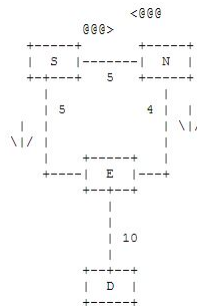


Figure 4.11.: Failed Scenario in MPLS Networks

4.5 Source Routing Implementation Over MPLS Networks

Source Routing gives the authority to the sender of the network to provide partially or fully the complete route of the packet data across the network, whereas in the case of non-source routing protocols, the intermediate routers of the network will determine the path which is based on the packet's destination address.

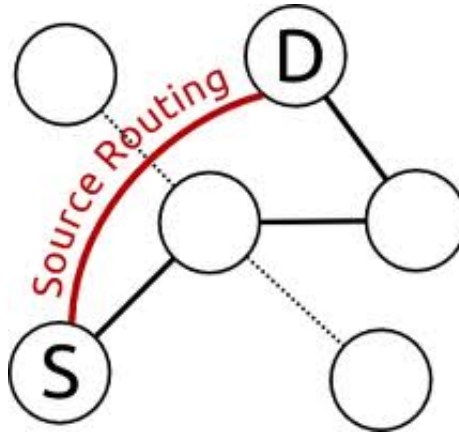


Figure 4.12.: Source Routing Demo

Here in the figure 4.12 above the source S determines the path to the destination node D by crossing the intermediate nodes in the network. The main advantages of source routing implementation are:

1. Troubleshooting across the network is made very easy as it is the source which decides the entire packet route and there is no role of the intermediate routers.
2. Improvement in the trace route.
3. It also enables a particular node to identify the possible routes in the network to the source.
4. It will not allow the source to manage the network directly by pumping the packets to travel over a particular path to prevent congestion on another path.

4.5.1 Working Of Source Routing Over MPLS Networks

In the MPLS network, the LDP Signaling protocol makes use of the labels which have the local significance, meaning an FEC can bind to different labels on various other links in a network. In this way every LSR can achieve the conflict free label allocation. But there are certain situations where a domain wide label binding to a particular FEC is preferred [1].

In this domain wide FEC, a label is made to bound to one FEC on all the links in the network if there exists a binding to that label. This type of label is known as a Domain Wide Label (DWL).

The difference in the way local labels and domain wide labels work is shown below:

There is a particular FEC d which corresponds to a loop back interface address D. In conventional FEC label mapping, FEC d can bind to different labels on different links.

```

label 30  label 20  label 10
FEC-d : A ----- B ----- C ----- D

```

Figure 4.13.: Local Label in MPLS

In the case of Domain Wide Label binding, FEC d is allowed to bind to a single label in the entire network by which the label gets global recognition which means the entire network.

```

label 10  label 10  label 10
FEC-d : A ----- B ----- C ----- D

```

Figure 4.14.: Domain Wide Label in MPLS

Domain Wide Label (DWL): A label is considered as the domain wide label if and only if the FECs which bind to that labels are same on all the links across the network.

Local Label: A label is considered as the local label if multiple FECs map to the same label on different links in the MPLS domain.

4.5.2 Source Routed LSP

Domain Wide label is the main concept which supports the source routing in the LDP enabled network with the help of the stack of labels.

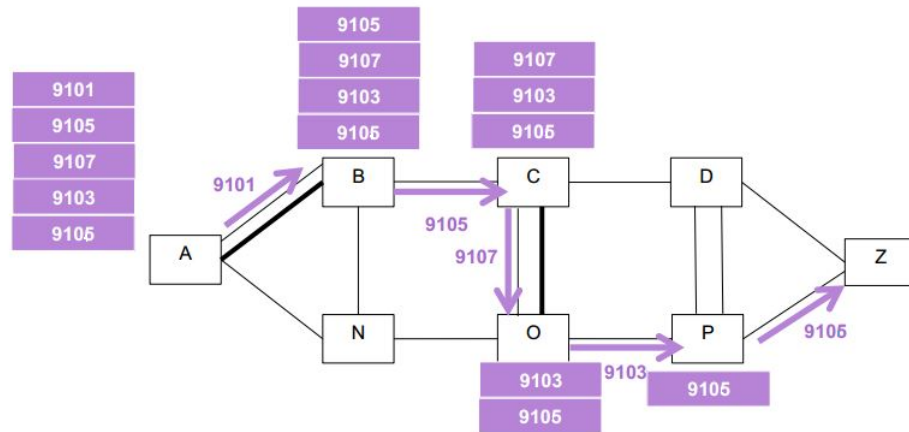


Figure 4.15.: Label Stack Mechanism in MPLS Networks

The Source contains the entire stack of labels through which the packet should be passed to reach the destination. Since the labels are constant (Domain wide label) throughout the network, this type of source routing is possible over MPLS Networks [27]. Label Stack is updated at the source based on the route the packet needs to travel and the path is initially computed at the source node. The other intermediate LSRs do not push other label as in the other signaling protocols but just pop the label of its own from the label stack and forwards the packet with the remaining stack of labels. Hence this process of transferring the label stack from one node to another by removing that particular node label from the stack continues till the traffic reaches the destination [1].

Protection Lists: It is the list of segments or links which are used for encoding the detour path from the protecting node S to the repair node R avoiding the link which is failed. Here the protecting node is the source node and the node which is failed in the network is known as the repair node.

Protection Techniques for Link Failure using LFA:

If a path to a destination D from a neighbor N of S does not contain S (N is a loop-free alternate of S for the failure of link S-F), then S can pre-install a repair forwarding message to detour the packet data to node N when the failure occurs between S-E. In the case of LFA applicability, the protection list is empty. A protecting router S needs to send the protected packet as is to its LFA neighbor N [37].

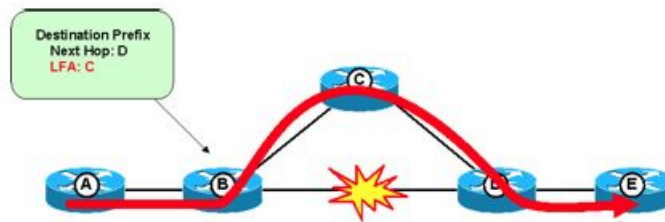


Figure 4.16.: Alternate Path in Source Routing

Here in the figure 4.16 there is a link failure between node S and D so there is a pre-installed detour path via C and the label stack at the source gets updated very quickly before it sends the label stack to its neighbor.

Protection Techniques for Link Failure using RLFA:

If there is no LFA neighbor which is not on the path of the failed link, then there occurs the problem of setting the detour path. In this case the Source will create a virtual LFA with the help of the tunnel to carry the packet data to a particular point in the network which is not a direct neighbor of S, and from where the packet will

be delivered to the destination without looping back to S. The Remote LFA proposal calls such a tunnel a repair tunnel. The tail-end of this tunnel (R) is called a "remote LFA" [37].

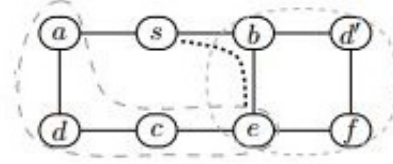


Figure 4.17.: RLFA in MPLS Networks

The difference between LFA and RLFA is there will be some cases where the neighboring node may not be present to form a backup path as mentioned in the concept of LFA. In the figure 4.17 source s needs to send data to node d. Suppose there is a link failure between s-a. So the alternate path to reach node d is through node b but because of the concept of ECMP, node b tends to send data to node d again through the path b-s-a-d. So there occurs loss of data and results in performance degradation. In this case, the importance of the virtual tunnel is realized where the virtual repair tunnel is created between node S to node E and from node E the data is flown to the destination D. In this case there is very little scope of loss of data in the network.

Advantages of Source Routed LSP:

1. Zero Signaling and maintenance overhead: The routing in the network is completely based on the source so there is no signaling which is required in order to establish the path and there is no need of any maintenance.
2. No Signaling Delay: Since all the LSPs are based on the source routing, these LSPs are made available immediately when the stack of labels at the source are determined. The make before break concept is followed in this technique.

3. The major benefit of DWL is its great advantage on the troubleshooting of the network. Since all FECs are using the DWL bind to the same label on all the links in the network, packets with that label can be related to the FEC very easily.
4. The other major advantage of DWL is its performance on the node protection [36]. Because in Node protection an LSR should know about the labels which are allocated by the NNHOP LSR for a particular FEC. Initially the protocols were made to propagate the label information, but when DWL is used in MPLS Networks the NNHOP label for FEC will always be the same as the label which is allocated on the local basis.

5. NETWORK MODEL SIMULATION OF MPLS NETWORKS FOR FAILURE DETECTION AND RECOVERY USING OPNET MODELER 17.5

The network which is used to study the failure techniques over MPLS Networks is described in this section. Further in this chapter it discusses about the proposed model which is under study and how to implement the model in the OPNET Modeler is mentioned. The version of OPNET used here is 17.5, latest version as of today. OPNET is short for Optimized Network Engineering Tool and it has major utilization in the research of computer networks [39]. OPNET provides the comprehensive development environment which supports the designing of the communication networks and the distributed systems. It supports in collecting behavior and performance of OPNET modeled network systems which can be analyzed later by performing discrete event simulations. OPNET Modeler developed various models in the wide range of systems which includes:

1. Internet work planning.
2. Resource sizing.
3. Standard LAN/WAN performance modeling.
4. Research and development of advance distributed network.

OPNET Modeler 17.5 is chosen as the simulation tool to design and implement the network which is under the study. When the complete model is available, built in simulations are executed to study the systems behavior and the performance. But, before executing the simulations, the user should consider the information which is obtained from the modeled environment.

In order to obtain the results, OPNET mainly works as the active network monitoring tool. The active network monitoring tools sends the additional traffic onto the network. Active monitoring is performed through the probes which do not affect the network properties in either way. Probes are mainly aimed to emulate the actual network traffic and are sent among the active network agents (devices). The agents measure the received streams and typically keep a statistical analysis of measured results, which can be studied periodically by the active monitoring device [40]. The active network monitoring is in contrast to passive network monitoring where each network device records statistics on the actual network traffic result passing through it as an indication of status at the particular network element. In Passive monitoring, it looks at each device in isolation and by looking at multiple devices an aggregated view of the status of the network is deduced.

5.1 OPNET Model Configuration

This chapter discusses the network model and the different network elements which are used in the network including about their placement and their functionality in the MPLS Network. To study the characteristics of the proposed network, the base network topology will be same. The configuration on the interacting nodes will vary. The network components which are used in this work are described below:

Ethernet 2 slip8 ler: LER means Label edge Router. It consists of two Ethernet ports and 8 serial interfaces for the WAN PPP connections. It simulates the main component of the MPLS Domain. Its functionality is mainly on the edge of the MPLS domain which is used to connect the MPLS domain to other non-MPLS/MPLS networks. The same LER router is used to simulate the IP or MPLS domain end node. It is the settings that decides the working in a particular configured environment. It also provides the IP layer functionalities as routing and runs the IP routing protocols [40].

Ethernet2 slip8 lsr: LSR is known as label switched router. It is the intermediate router in the MPLS Domain. It has 2 Ethernet ports and also has 8 serial interfaces for the WAN PPP connections. It is considered as the core of the MPLS domain. It is used specifically for the purpose of receiving the incoming labeled packet to swap the label and forward to the next hop on the LSP. Once the LSR is enabled for MPLS and starts working, it constructs the Forwarding information based on the advertised labels and also performs the label swapping functionalities [40].

PPP adv: Point to Point serial full duplex link at the specified rate in bps is used to simulate the link in between the routers. All the core links are duplex and are set to 5 Mbps data rate. The low bandwidth serial links are mainly used for the study of the application characteristics at the network core [40].

Ethernet wkstn adv: Ethernet workstation OPNET element is used for the simulation for the network users. It mainly consists of a single Ethernet connection at the given rate which is directed by the medium which is used to connect to an Ethernet switch. Advanced station is selected for the reason to implement RSVP in the simulated network. The destination preference is configured to reduce the service server resolution traffic and time. The module is used to simulate the single user in the network design using different applications.

Ethernet server adv: The Ethernet server which is provided in OPNET is mainly used to simulate the service server in the network. It mainly contains one Ethernet connection to the switch, facilitating that particular subnet [40].

Ethernet16 switch: This OPNET module simulates the Ethernet switch with a total of 16 Ethernet ports available, on other side of the LER. The edge devices, ethernet server adv and ethernet wkstn adv are always connected with this module by using different link types.

10BaseT: This link is used to connect ethernet wkstn adv to ethernet16 switch [40].

10Gbps Ethernet: This is a high speed full duplex link and it is used to connect the LER to the associated West switch on both the sides of the network. High speed link is mainly used so that the application can inherit no congestion on the interface outside the simulated network core [40].

1000BaseX: This connection link is mainly used to connect the East switch to the related LER.

MPLS E LSP Dynamic: When the network topology is built for MPLS, the LSPs are created automatically inside the network. But those LSPs follow the IP shortest path in between two nodes. To develop the explicit LSP along the network, OPNET is used to simulate the behavior of the dynamic LSP. If not configured with explicit nodes along the LSP path, the dynamic LSP gets adjusted with the changing network conditions and also with the guaranteed resources along the network. A dynamic LSP is signaled using RSVP or CR-LDP Signaling protocols, when the simulation has begun. CR-LDP Signaling protocol makes use of the dynamic routing protocols to compute the dynamic LSP towards a certain destination, as mentioned in its explicit path [40].

MPLS E LSP Static: Static LSP is not triggered at the time of the startup. Static LSP will allow more than one routing control but fewer resiliencies to node or link failure.

Besides the above mentioned OPNET network elements, there are certain OPNET control elements used to configure policies, network wide configurations and adjusting scenarios. The OPNET control objects used in this thesis work include:

Application Config: This element is used to describe how the application is going to be modeled on the designed network. This description is sent to OPNET with the help of this block.

An Application Config is used to instruct OPNET for multiple network applications. Application parameters are configured for various applications in this block.

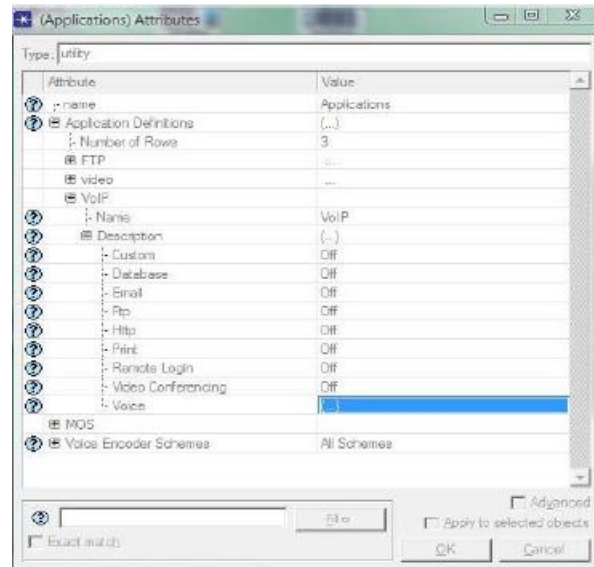


Figure 5.1.: Application Configuration in OPNET

Profile Config: Profile in OPNET describes the activity of an individual user or group of users in terms of the applications which are used over a period of time [40]. User profiles have different properties, so creating a certain profile with all the settings with a specific application is done here. The configured profiles are then assigned to the network users.

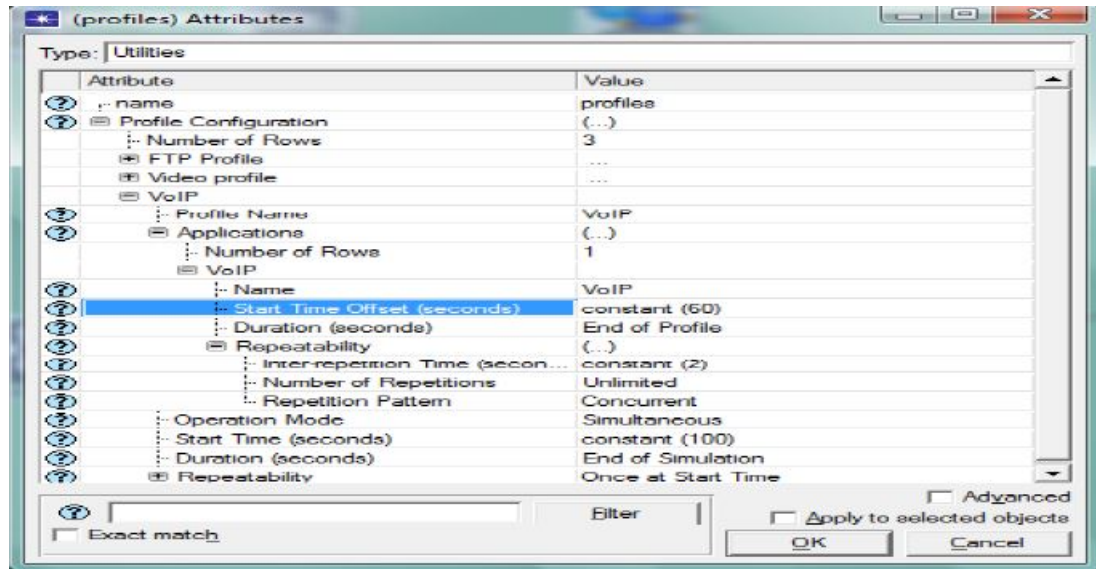


Figure 5.2.: Profile Configuration in OPNET

QoS Attribute Config: Different QoS conditions are to be implemented in the network which help in better understanding of the traffic characteristics which are configured. This block helps in implementing the network wide QoS at one place.

MPLS config object: The function of Configuring the MPLS FEC and Traffic Trunk is done in this network element. This configuration specification is mainly used at the Ingress Edge router to direct the traffic flows and assign to different LSPs for different application traffic.

Failure Recovery block: In order to analyze the simulated network model during/after failure, OPNET model has built in an element called Failure Recovery [40]. This covers link or node failure/recovery situations at specifically configured simulation time. The below table is the Failure recovery block where the links which failed are mentioned along with their time frames [40].

Table 5.1: List of Link Failures in MPLS Network

link Name	Status	Time
R1-R4	Fail	100
R1-R4	Recover	600
East-R4	Fail	100
East-R4	Recover	600
R1-R4	Fail	100
R1-R4	Recover	600

5.1.1 OPNET Application Traffic Types:

The current work uses five different types of application traffic. The difference between application traffic is mainly based on the TOS value as mentioned with each application flow which will help in the DiffServ domain. Voice Traffic: The voice traffic has the characteristics which are mentioned in the figure 5.3. Highest application TOS is given to voice traffic which is equal to Interactive Voice (6).



Figure 5.3.: Voice Application Traffic in OPNET

Video Traffic: The video traffic has the characteristics which are mentioned in the figure 5.4. It has given the TOS value which is equal to Interactive multimedia (5). The traffic generated by the video application per second is 1.2 Mbits/sec.

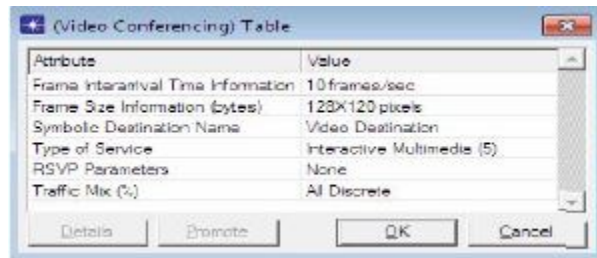


Figure 5.4.: Video Application Traffic in OPNET

HTTP Traffic: Hyper Text Transfer Protocol is used to simulate the web browsing in the network design. The characteristics of the HTTP are mentioned in the figure 5.5. The TOS value of the HTTP traffic is equal to the Standard (2).

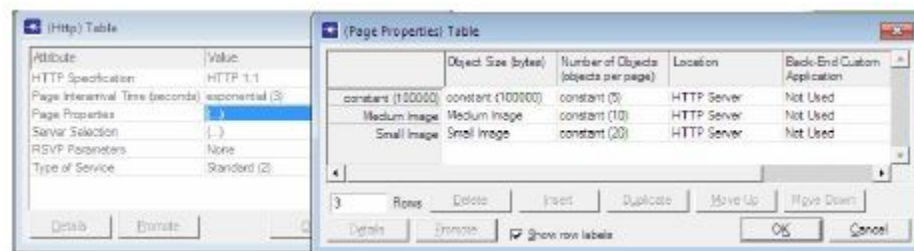


Figure 5.5.: HTTP Application Traffic in OPNET

FTP Traffic: FTP is used to generate the traffic flow from the FTP Server to the FTP client. FTP means File Transform Protocol. It will simulate the file which is downloaded based on the request from the client. The FTP characteristics are shown in the figure 5.6.

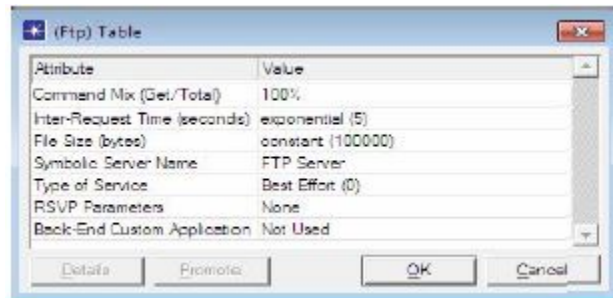


Figure 5.6.: FTP Application Traffic in OPNET

Email Traffic: The Email Traffic is used to check the behavior of the email service. The characteristics of Email are given in the figure 5.7. Emails are given the TOS which is equal to the Excellent Effort (3). Emails use the TCP for the transport. This traffic is used to understand the network attributes in terms of delay variation and packet loss. Both video and voice traffic use the UDP traffic mechanism. Voice and video constitutes the network major traffic share.



Figure 5.7.: Email Application Traffic in OPNET

5.2 OPNET Simulation Network

The Network design and the applications to run on the network is provided in the chapter. The network which is used in the thesis is provided below.

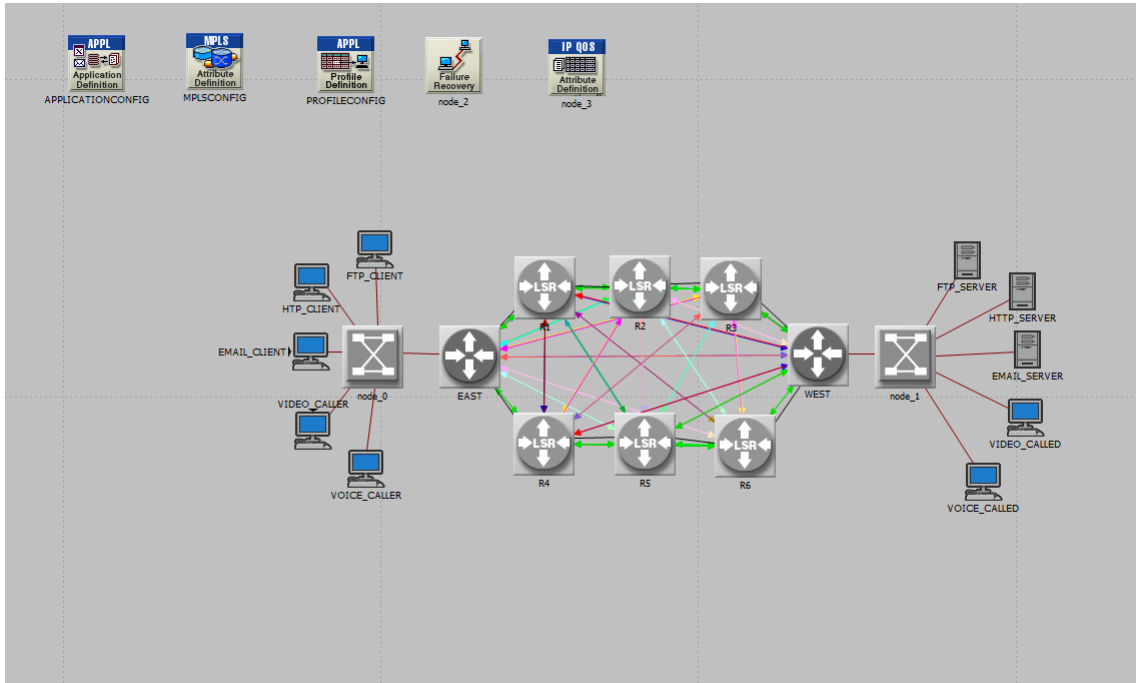


Figure 5.8.: Network in OPNET

The labeled edge routers are designated as East and West. All core nodes constitute towards the full mesh as they are connected to others and the network connectivity is 3.75 links per core node in average. Various network scenarios are implemented over the base. These network scenarios are based on the various failure scenarios implemented on the MPLS networks and the recovery techniques are implemented on the network. In order to test the network during the failure, mainly voice traffic is utilized.

5.3 Various Scenarios Implemented in OPNET

Before starting the simulations in the OPNET tool first it is very important to set the application attributes and Profile configuration for the network. Application attributes are used to set the parameters of the voice traffic which is used in the network for simulations and Profile configurations are also set.

In the network topology the baseline configuration is MPLS and OSPF is taken as the routing protocol for the core network. OSPF is preferred because it implements Link state routing algorithm with traffic engineering capabilities. OSPF will build the shortest path with the help of Dijkstra algorithm. It also uses the additive link bandwidth as cost to reach a remote destination. Link is configured on the ppp adv link models. Every link consists of 5 Mbps Bandwidth. When there exists a situation where multiple paths point to a single destination the dynamic routing protocols will automatically provide the Equal Cost Multi Path (ECMP) for the destination which is accessible with same cost. In the network all links from one end to another end are ECMP in both forward and reverse direction. The main functionality of ECMP is to use the concept of load balancing across the network domain and this is done by sending the traffic around the multiple network paths. So by this ECMP is responsible for the reduction in the network congestion.

5.3.1 MPLS Network Simulations without any Failed network components.

The network performance is mainly evaluated in terms of three network properties:

1. Average Traffic Received (Packets/sec): It is the number of packets which are received at the receiver end per second.
2. Voice Packet End to End Delay (sec): It is termed as the delay in reaching the packet from end to other end in the network.
3. Voice Jitter (sec): If there is any disturbance in the packet arrival time because of the disturbances in the network it is termed as Voice Jitter (Sec).

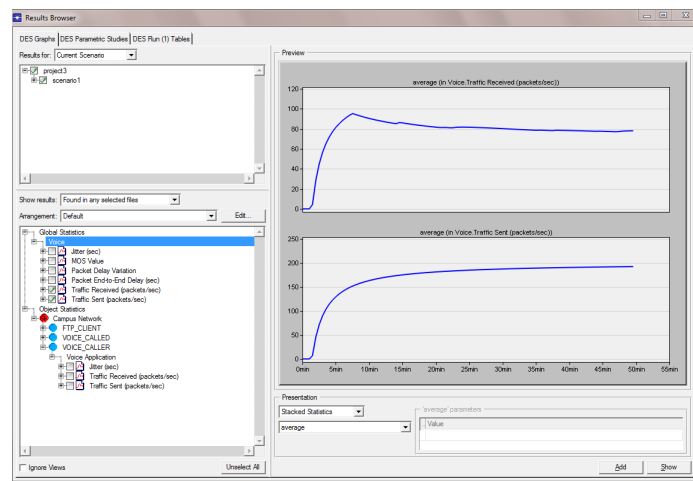


Figure 5.9.: Traffic Received (packets/sec) in MPLS Network Without any Failure.

The figure 5.9 gives the information regarding the voice traffic received in terms of packets per sec. The diagram shows the amount of traffic sent and also the amount of traffic received. This is the actual data which is expected when there occurs the failure and when the recovery techniques are applied on the network.

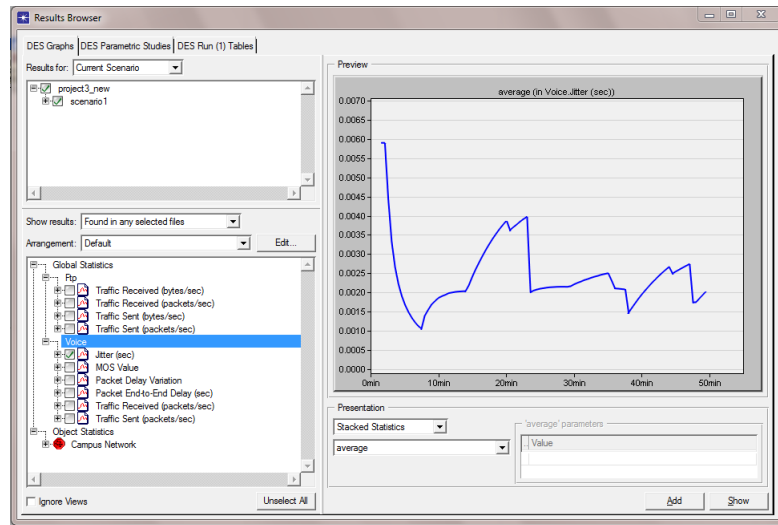


Figure 5.10.: Voice Jitter (sec) in MPLS Network without any Failure

The figure 5.10 gives the information regarding the voice Jitter in terms of seconds. The diagram shows the disturbance in the voice traffic in the MPLS Network. This is the actual data which is expected when there occurs the failure and when the recovery techniques are applied on the network.

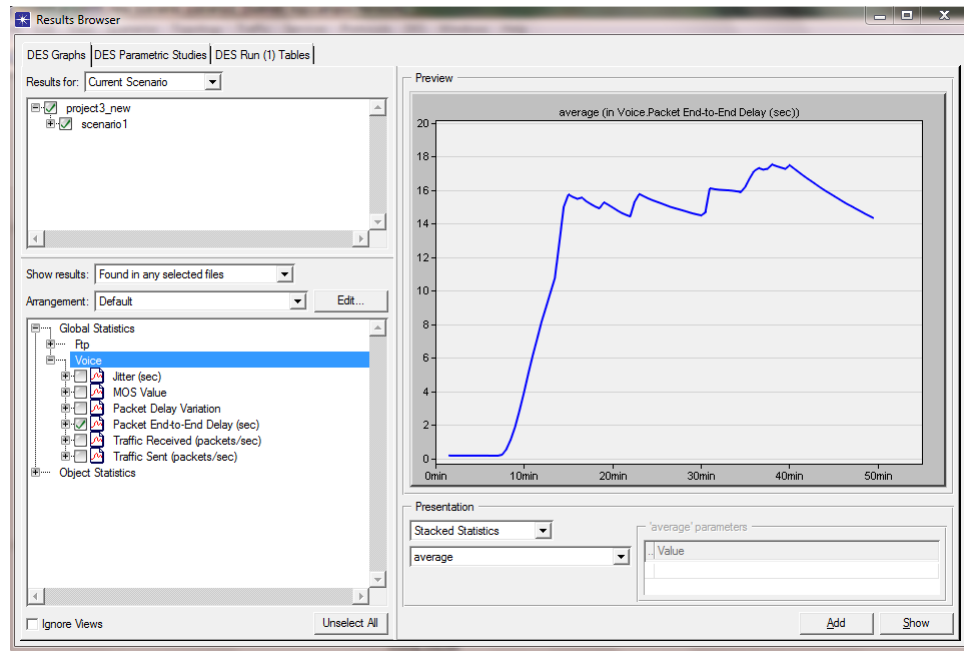


Figure 5.11.: Voice Packet Delay in MPLS Network Without any Failure

The figure 5.11 gives the information regarding the voice Packet End to End Delay in terms of seconds. The diagram shows the delay in the voice traffic to reach the receiver end from the source in the MPLS Network. This is the actual data which is expected when there occurs the failure and when the recovery techniques are applied on the network.

5.3.2 MPLS Network Simulations with 3 Failed Links.

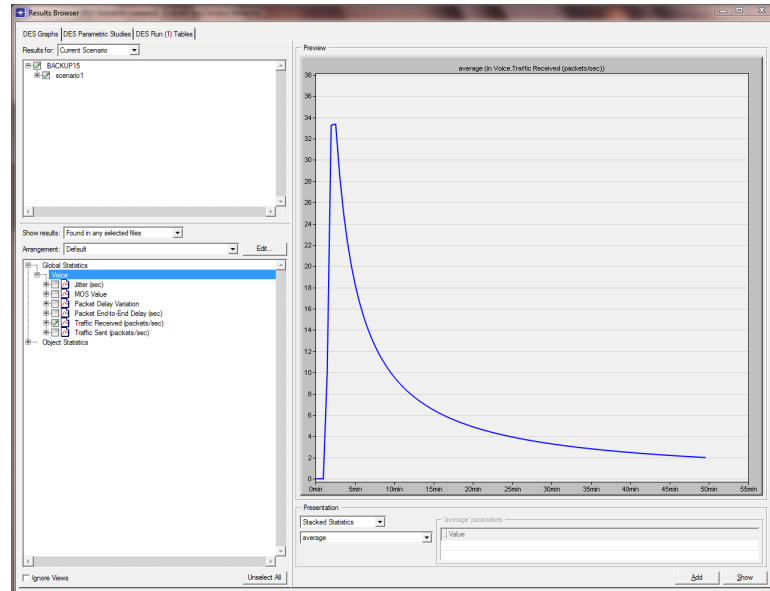


Figure 5.12.: Traffic Received in MPLS Network with 3 Links Failure

The figure 5.12 depicts the average number of packets which are received at the receiver end. It is clearly understood that there is a lot of traffic loss in the network because the link is affected and no repair techniques are implemented on the network. The traffic which is planned to carry the traffic is lost and it will result in the degradation of the network performance. The links which are failed in this case is between R2-R3, R4-45, R1-R4.

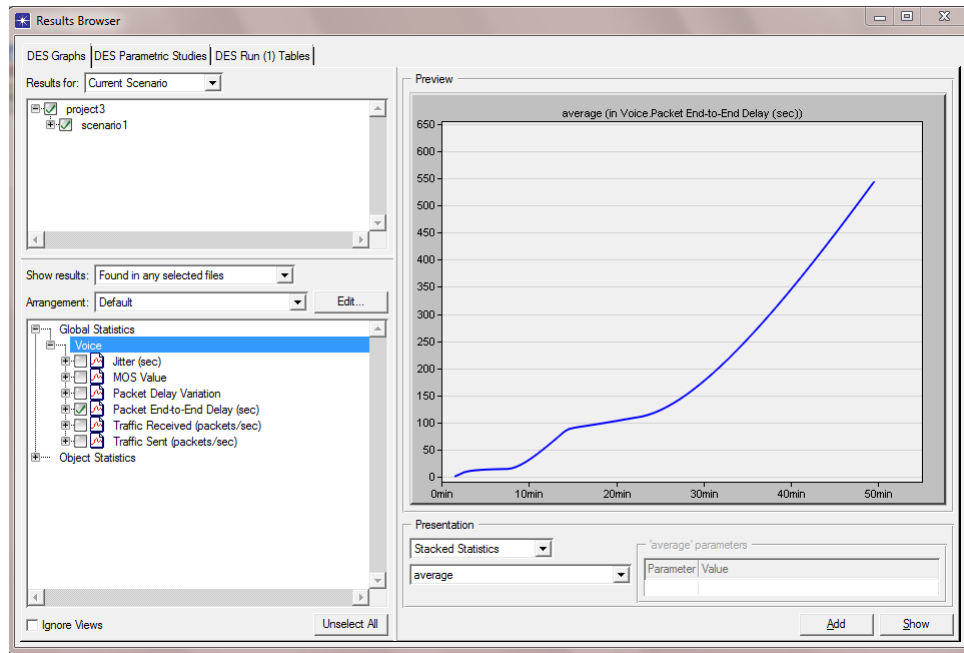


Figure 5.13.: Voice Packet Delay in MPLS Network with 3 Links Failure

The figure 5.13 shows the performance of the voice packet end to end delay when there occurs a link failure in the network. It is clearly visible that there is high increase in the voice packet delay in the network because of the failure in the network. The packet once lost during the link failure in the network takes a lot of time to reach the destination.

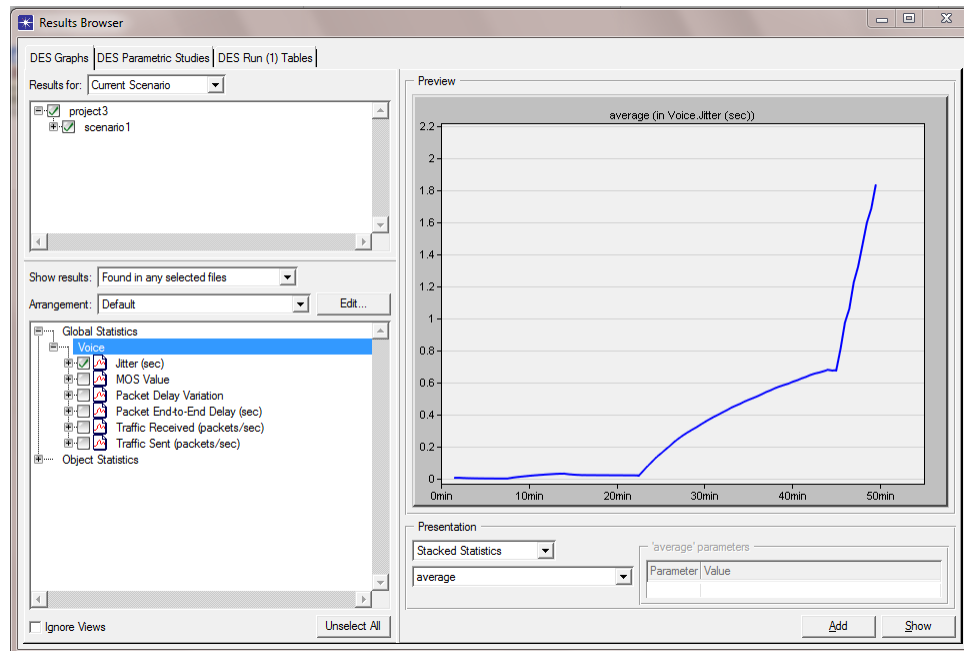


Figure 5.14.: Voice Jitter in MPLS Network with 3 Links Failure

The figure 5.14 shows the performance of the voice Jitter in the RSVP enabled with 3 failed links occurs in the network. It is shown that there is high increase in the voice jitter because there occurred a lot of congestion in the network due to failure in the network. When there occurs failure in the network packets once lost during the link failure in the network gets disturbed and takes a lot more time to reach the destination.

5.3.3 MPLS Network Performance with 3 Link Failures and Restoration Techniques implemented on the Network with RSVP Signaling Enabled.

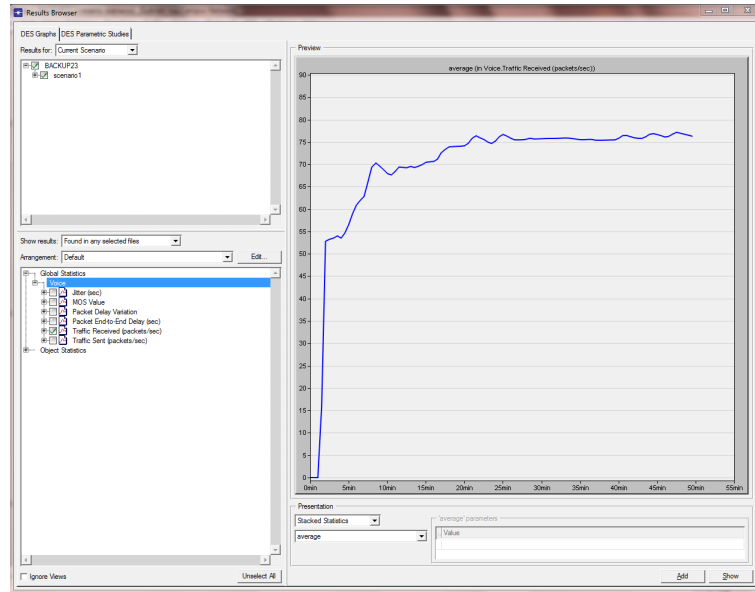


Figure 5.15.: Traffic Received in MPLS Network with 3 Links Failure/Recovery in RSVP Signaling

The figure 5.15 shows the average number of packets received at the receiver when 3 links are failed in the network. The performance of the network is enhanced as the number of packets has increased at all the times. When there are no restoration techniques implemented at an average only 36 packets are received per second. When the restoration techniques are applied on the network the average number of packets is increased on an average of 75 packets per second. This improvement is because of the backup tunnel which is established in the network at the point of failure.

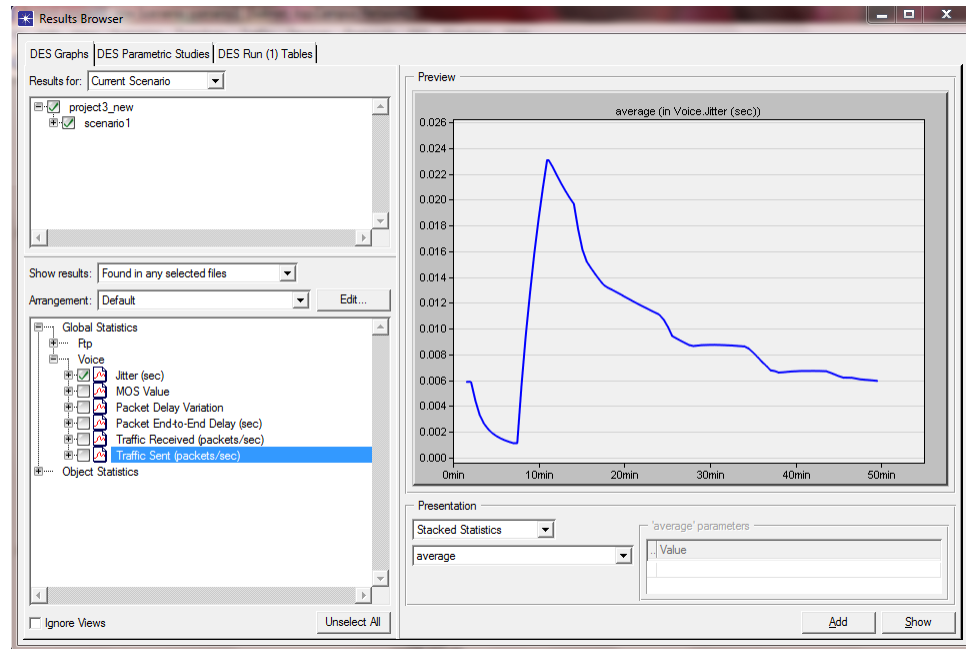


Figure 5.16.: Voice Jitter in MPLS Network with 3 Links Failure/Recovery in RSVP Signaling

The figure 5.16 shows the voice jitter at the receiver when 3 links are failed in the network. The performance of the network is enhanced as the Voice jitter is decreased drastically by 90 percent at all the times. When there are no restoration techniques implemented at an average 2 seconds of voice jitter is generated. When the restoration techniques are applied on the network the average of voice jitter is decreased to 0.024 seconds. This improvement is because of the backup tunnel which is established in the network at the point of failure.

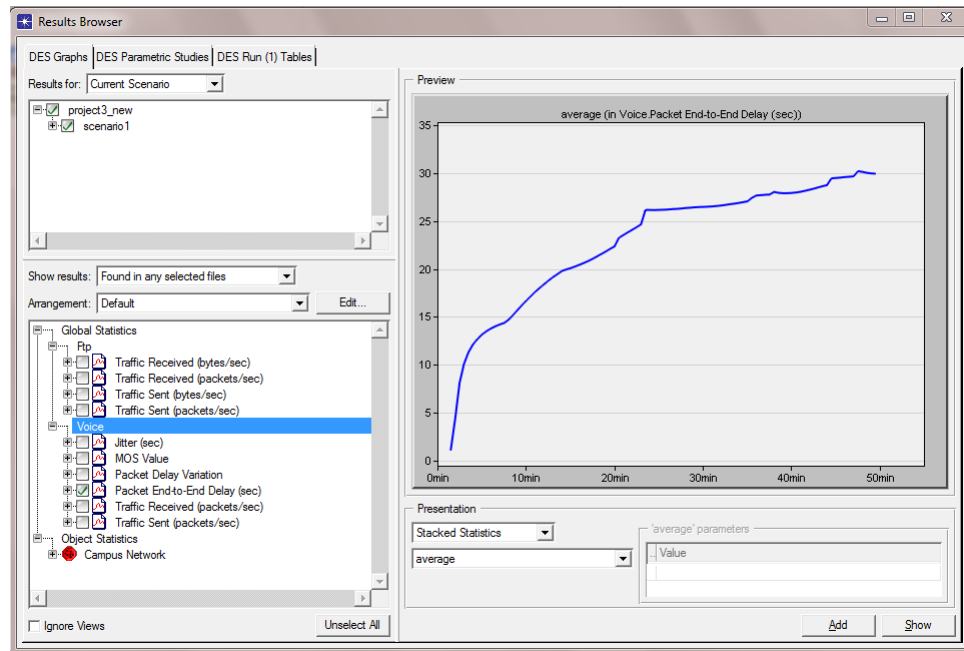
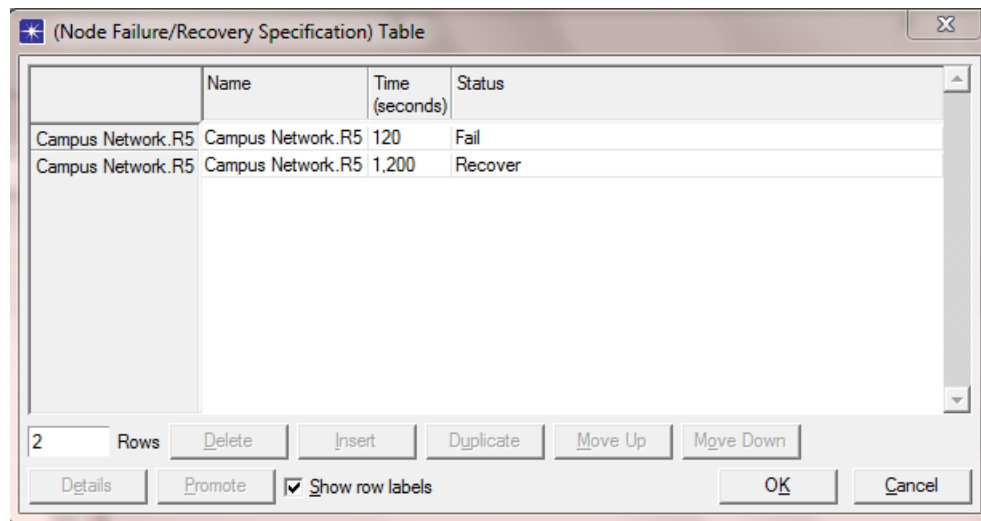


Figure 5.17.: Voice Packet End to End Delay in MPLS Network with 3 Links
Failure/Recovery in RSVP Signaling

The figure 5.17 is voice packet end to end delay which will vary as the scenarios in the network changes because of the failures and the variance in the convergence time on the alternate backup tunnels at the point of failure. As these times vary in the network the time the voice packet which is received at the receiver will vary accordingly. The performance of the network is enhanced as the voice packet end to end delay at all the times has lowered. When there are no restoration techniques implemented the end delay average value is around 250 seconds. When the restoration techniques are applied on the network the average end to end packet delay is decreased to 25 seconds. This improvement is because of the backup tunnel which is established in the network at the point of failure. As the switch over time is very less it has a great influence on the overall network performance.

5.3.4 MPLS Network Performance With 1 Node Failure in the Network with RSVP Signaling Enabled in the network.

The node is failed in the network with the help of the block Failure Recovery where it can be mentioned what particular node is to be failed and when it should be recovered back. The below diagram shows how to set the node fail and recovery in the network.



	Name	Time (seconds)	Status
Campus Network.R5	Campus Network.R5	120	Fail
Campus Network.R5	Campus Network.R5	1,200	Recover

Figure 5.18.: Node Failure in MPLS Networks with RSVP Signaling

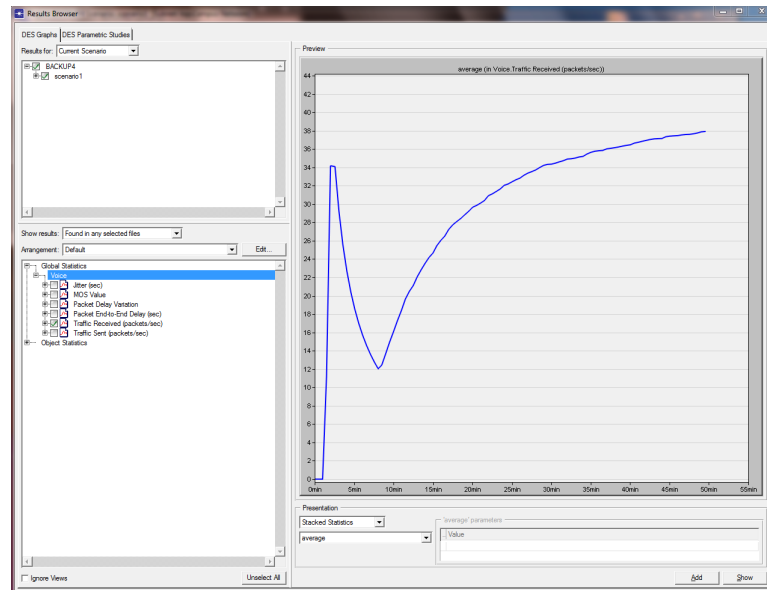


Figure 5.19.: Traffic Received in MPLS Network with 1 Node failure in RSVP Signaling

The figure 5.19 depicts the average number of packets which are received at the receiver end when a node R5 is failed and recovered in the time period of 2 to 10 minutes. It is clearly visible that there is a lot of traffic loss in the network because the link is affected and no repair techniques are implemented on the network. The traffic is decreased greatly till the node got recovered at the time of 10 minutes. The traffic which is planned to carry the traffic is lost in the time frame and this has resulted in the degradation of the network performance. The node which is failed in this case is R5.

5.3.5 MPLS Network performance with 1 node Failure and Restoration Techniques Implemented on the Network with RSVP Signaling Enabled.

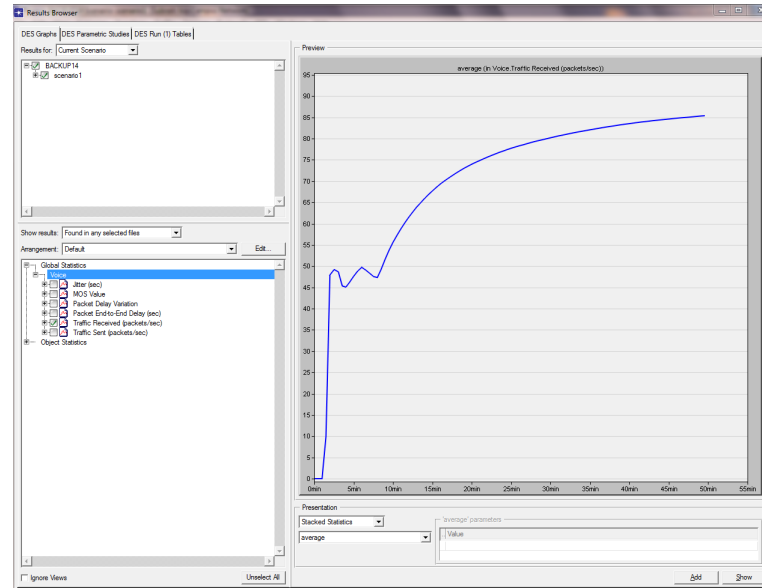


Figure 5.20.: Traffic Received in MPLS Network with 1 Node Failure/Recovery in RSVP Signaling

The figure 5.20 shows the average number of packets received at the receiver when a node is failed and recovered in the network. The performance of the network is enhanced as it is shown the number of packets received has increased at all the times in the graph. When there are no restoration techniques implemented at an average only 20 packets are received per second. When the restoration techniques which are backup tunnel implementation are applied on the network the average number of packets is increased on an average of 64 packets per second. This improvement is because of the backup tunnel which is established in the network at the point of failure and the traffic which is initially set to cross the node R5 uses NNHOP tunnel to bypass the traffic over the failed link for mentioned time frame.

5.3.6 MPLS Network Performance with 3 Link Failures and Restoration Techniques Implemented on the Network with CR-LDP Signaling Enabled.

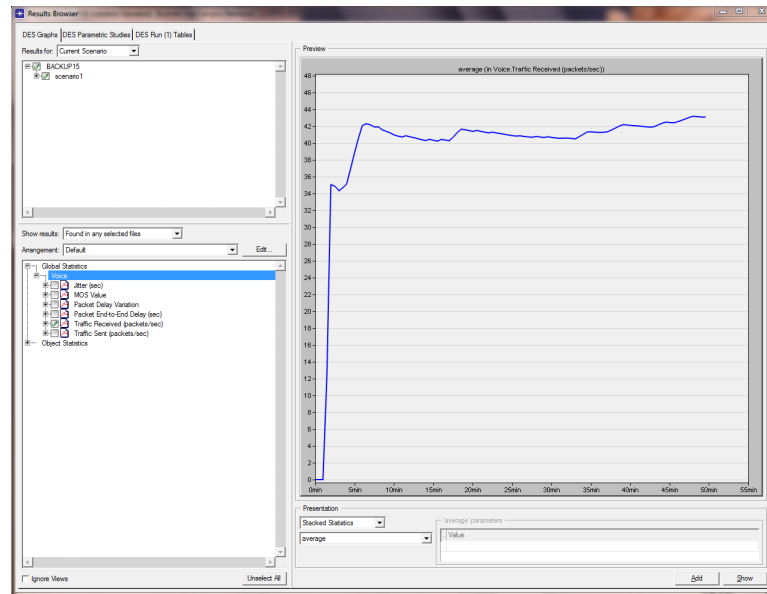


Figure 5.21.: Traffic Received in MPLS Network with 3 Links Failure/Detection in CR-LDP Signaling

The figure 5.21 shows the average number of packets received at the receiver when 3 links are failed in the MPLS network with CR-LDP Signaling enabled. The performance of the network is enhanced as the number of packets has increased at all the times. When there are no restoration techniques implemented at an average only 14 packets are received per second. But when the restoration techniques are implemented on the network such as the setting up of backup tunnel with the loop free criterion followed the average number of packets is increased on an average of 40 packets per second. This improvement is because of the backup tunnel which is established in the network at the point of failure.

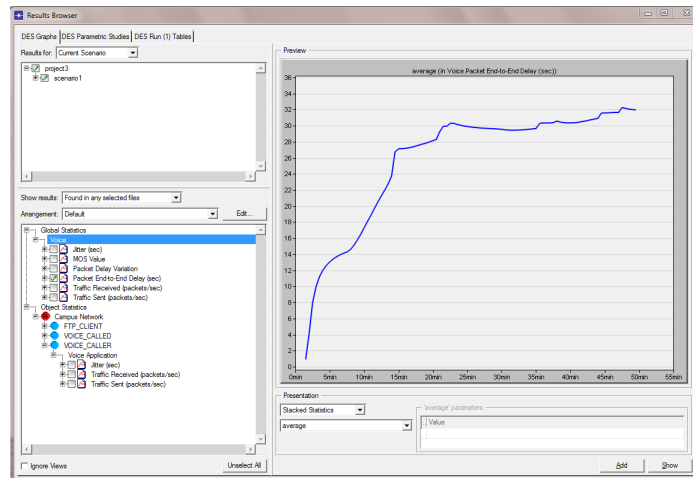


Figure 5.22.: Voice Packet Delay in MPLS Network with 3 Links Failure/Detection in CR-LDP Signaling

The figure 5.22 is voice packet end to end delay which will differ as the type of failures and the repair techniques that are applied on the network changes this will result in variance in the convergence time on the repair tunnels at the point of repair. As these times vary in the network the time the voice packet received will also vary accordingly. The performance of the network is enhanced as it is shown that the voice packet end to end delay at all the times has lowered. When there are no restoration techniques implemented the end delay average value is around 350 seconds. When the repair techniques are implemented on the network the average end to end packet delay is decreased to 25 seconds. This improvement is because of the backup tunnel which is established in the network at the point of failure. As the switch over time is very less the packet gets switched over to the tunnel and this has a great influence on the overall network performance.

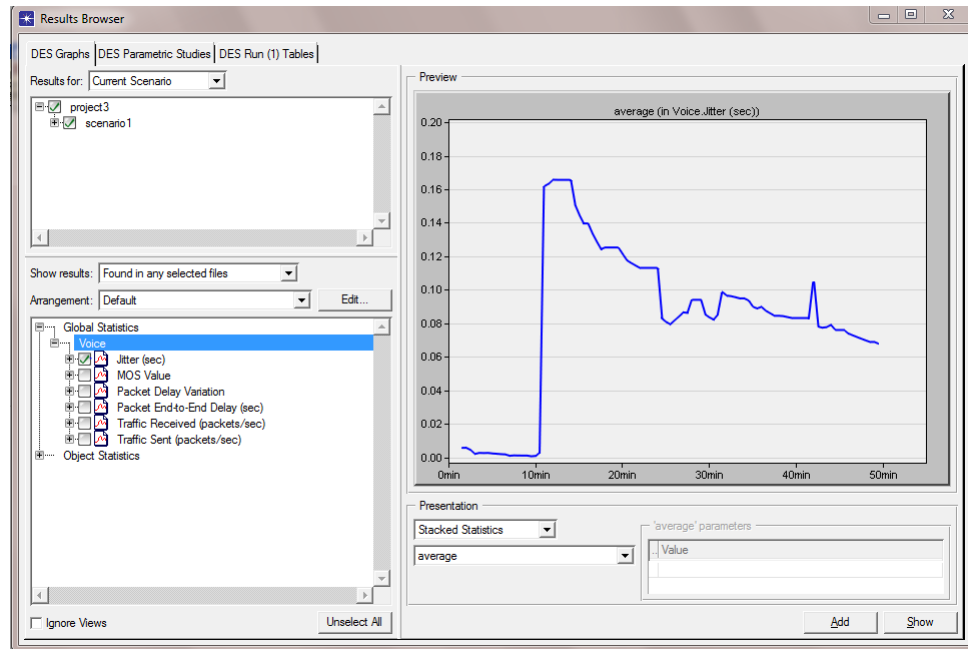


Figure 5.23.: Voice Jitter in MPLS Network with 3 Links Failure/Detection in CR-LDP Signaling

The figure 5.23 gives the results for the voice jitter at the receiver end when 3 links are failed in the MPLS network with CR-LDP Signaling enabled. The performance of the network is enhanced as the Voice jitter is decreased drastically by 40 percent at all the times. When there are no repair mechanisms which are implemented the average 0.45 seconds of voice jitter is generated. When the restoration techniques are applied on the network the average of voice jitter is decreased to 0.10 seconds. This improvement is because of the backup tunnel which is established in the network at the point of failure.

5.3.7 MPLS Network Performance with 1 node Failure and Restoration Techniques Implemented on the Network with CR-LDP Signaling Enabled.

The figure 5.24 shows the average number of packets received at the receiver when a node R5 is failed and recovered in the MPLS network with CR-LDP signaling. The performance of the network is enhanced as it is shown the number of packets received has increased at all the times in the graph. When there are no restoration techniques implemented at an average only 20 packets are received per second. When the restoration techniques which are backup tunnel implementation are applied on the network the average number of packets is increased on an average of 40 packets per second. This improvement is because of the backup tunnel which is established in the network at the point of failure and the traffic which is initially set to cross the node R5 uses NNHOP to bypass the traffic over the failed link for the time frame.

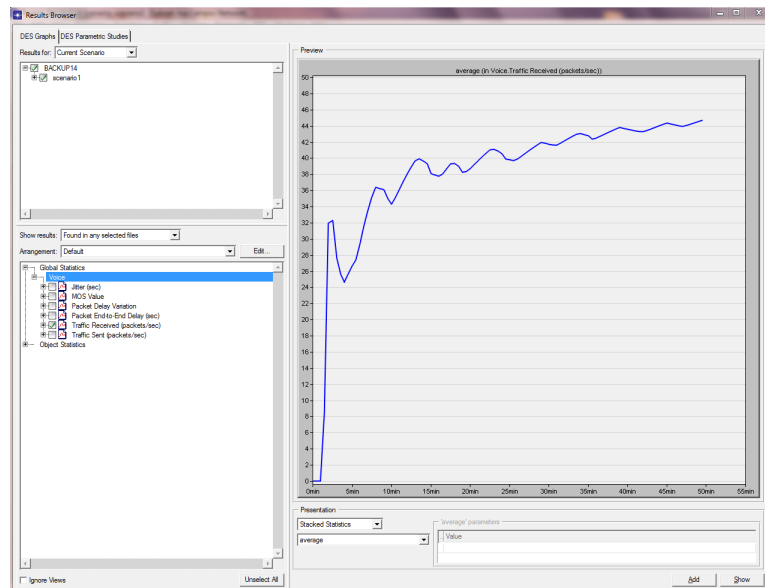


Figure 5.24.: Traffic Received in MPLS Network with 1 Node Failure Detection in CR-LDP Signaling

5.3.8 MPLS Network Performance with 3 link Failures and Restoration Techniques Implemented on the Network with Source Routing.

Loop Free Alternative (LFA):

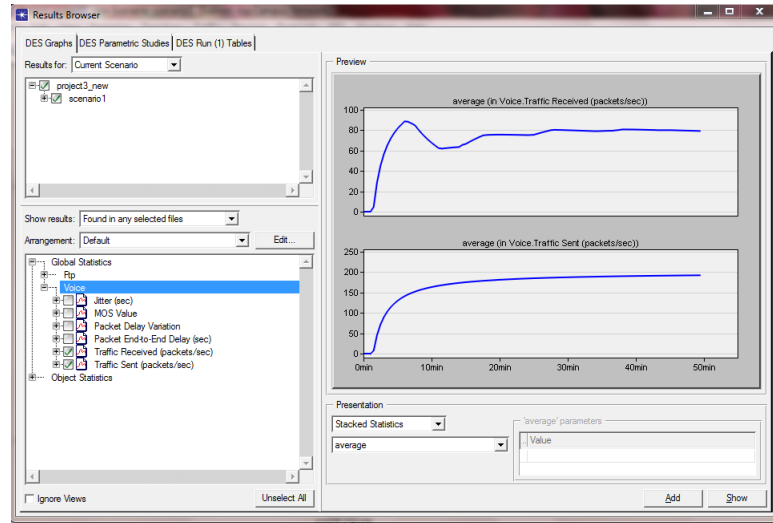


Figure 5.25.: Traffic Received in MPLS Network with 3 Links Failure/Detection using LFA

The figure 5.25 shows the performance of the MPLS Network when Source Routing is implemented. The mechanism is Loop Free Alternative. The neighbor for the source if available will be used to create an alternate path which is also satisfying the Loop free criterion. But in all the cases the adjacent node cannot be present for the alternate path which is used when the link failure occurs in the system. In source routing as the network topology changes with the LFA mechanism the labeled stack gets automatically updated at the source and accordingly the packets are forwarded. Since this system does not use any other extra signaling protocol it has the simpler network protocols and the complexity is minimized. The average number of packets received at the receiver is around 70 packets per second compared to 40 packets per second when there occurred failure in the network.

Remote Loop Free Alternative(RLFA):

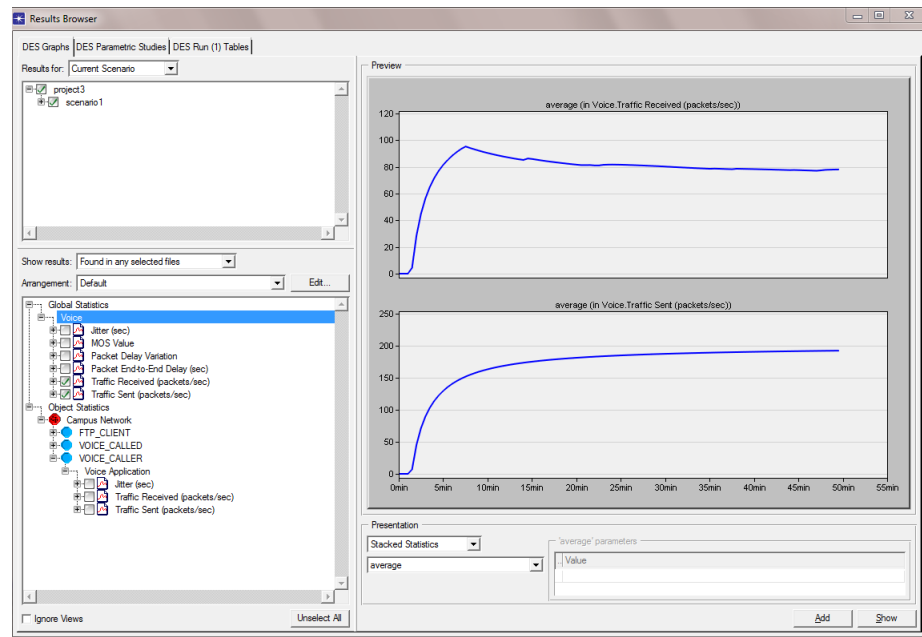


Figure 5.26.: Traffic Received in MPLS Network with 3 Links Failure/Detection using RLFA

The figure 5.26 shows the performance of the MPLS Network when Source Routing is implemented. The neighbor for the source if not available then tunneling concept is used where the tunnel connects source to that particular node from where routing can be possible. The average number of packets received at the receiver is around 96 packets per second compared to 40 packets per second when there occurred failure in the network. This improvement is because of the implementation of LFA on source routing enabled MPLS network.

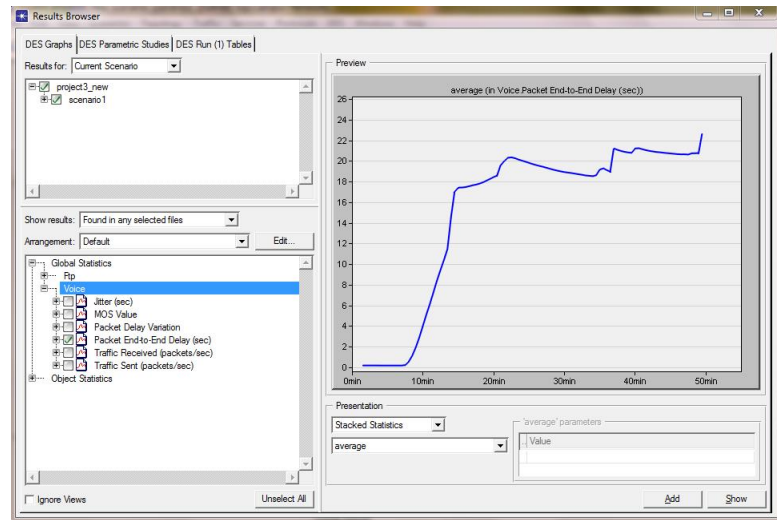


Figure 5.27.: Voice Packet Delay in MPLS Network with 3 Links Failure/Detection using Source Routing

The end to end voice packet delay has decreased to the extent of almost the best case simulate till now with the average timing delay of 12 seconds. The reason is because of the source routing. Source routing doesn't involve intermediate routers to take routing decisions. So the time waste at the routers other than source is omitted. So this has caused the improved performance on the entire network system.

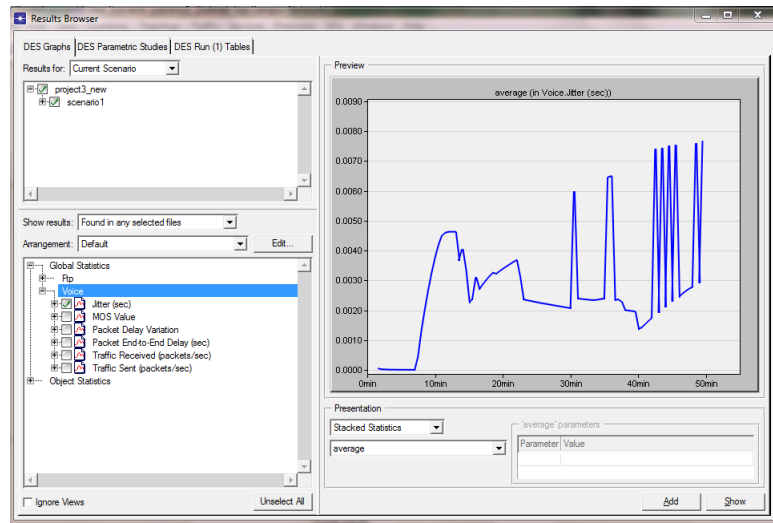


Figure 5.28.: Voice Jitter in MPLS Network in Source Routing

The average voice jitter in the figure 5.28 is around 0.045. This value is 90 percent less than the jitter produced during RSVP signaling. This is mainly because of the congestion avoidance in the network with the implementation of the Source routing which dynamically gets the network topology changes and gets its label stack updated near the source router. This is the whole reason for the improvement in the voice jitter values.

5.3.9 Comparison of Traffic Received in all 3 scenarios

The comparison chart shows that at any time RLFA Source Routing has the highest performance in terms of the traffic received. This is because in LFA its not always that the node connecting the failed link or node has the correct adjacent router to forward the traffic.

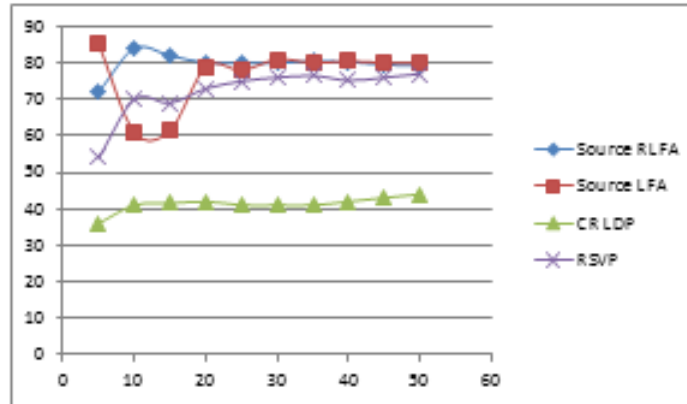


Figure 5.29.: Comparison of Traffic Received in Various Scenarios in MPLS Network

So its performance is less as compared to the LFA Source routing. The reason why RSVP and CR-LDP has the less performance is because of the convergence time which is high compared to the source routing. Since the convergence time is high there is more probability of the traffic loss in the network so the traffic received is less in these two cases.

5.3.10 Comparison of Voice Packet Delay in all 3 scenarios.

The voice packet end to end delay is least in source routing because of no role of the intermediate routers in the routing decisions and also it has no problem with the convergence time as it is very low compared to CR-LDP and RSVP.

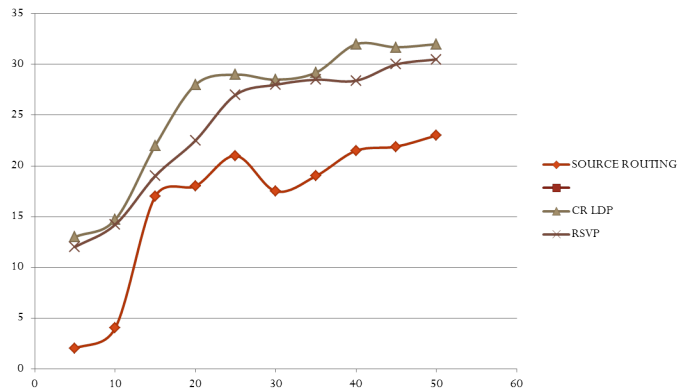


Figure 5.30.: Comparison of Voice Packet Delay in Various Scenarios in MPLS Network.

5.3.11 Comparison of Voice Jitter in all 3 scenarios.

The voice jitter is least in source routing because of no congestion and disturbance in the network and its topology. If there are any changes then the label stack gets updated and the routing follows it.

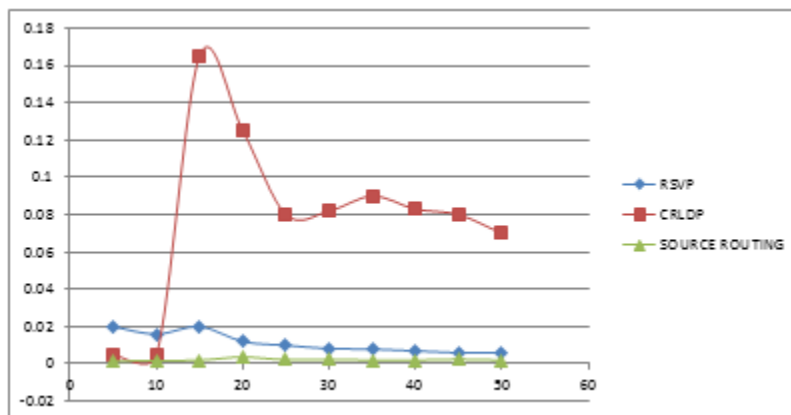


Figure 5.31.: Comparison of Voice Jitter in Various Scenarios in MPLS Network.

6. CONCLUSION

This thesis work presented the in-depth study of the MPLS Networks. The simulation work is mainly based on the fault failure scenarios in the MPLS Networks. Failure can be differentiated by the way they affect the network. The failures are hard failures and soft failures. Hard Failures are caused by the network breakdowns in the network and the soft failures are caused by certain network situations in the network such as network congestion. Hard failures will cause the network black out where as soft failures cause network brown out.

For a network to be resilient for the failures it should handle both Hard and soft failures. IP networks have the capacity to handle the frequently occurring soft failures by using differentiated services architecture. MPLS domain can handle both soft and network failures. The EXP bits in the MPLS header is used to provide the QOS in MPLS-TE. MPLS-TE is can handle the network brownouts. MPLS-TE converts the packet switching network to circuit technology. A circuit technology is more prone to to get into congestion and fail the network. Congestion in the network is resolved by weight balancing and the failure is recovered by MPLS FRR techniques. Link is protected by the NHOP tunnel and Node is protected by NNHOP tunnel. The tunneling concept is implemented in both RSVP and CR-LDP Signaling. But the disadvantage of the MPLS FRR is it can protect only the adjacent resource in the network. In order to bypass the disadvantage in the failed MPLS network source routing is implemented where the tunnel can protect any network resource as compared to the MPLS FRR techniques.

The entire thesis is implemented in OPNET Modeler 17.5 and the results have been validated by the simulated results for all the three techniques and the best way to protect the MPLS Network from failures is to implement the source routing over the MPLS Network.

LIST OF REFERENCES

LIST OF REFERENCES

- [1] Y. Tao, C. Shanzhi, L. Xin, and Q. Zhen, "Increasing ip network survivability in harsh scenarios with dynamic source routing," in *3rd IEEE/IFIP International Conference in Central Asia on Internet, ICI*, pp. 1–4, September 2007.
- [2] M. Bocci, "Introduction to multi-protocol label switching (mpls)," in *The 5th International Telecom Sync Forum, ITSF*, pp. 1–14, November 2007.
- [3] A. Malis, "Mpls-tp: Where are we?," in *Optical Fiber Communication Conference and Exposition (OFC/NFOEC) and the National Fiber Optic Engineers Conference*, pp. 1–3, March 2012.
- [4] Y. Xiao, H. Jiang, B. Liu, Y. Li, and X. Li, "A novel failure detection mechanism for fault-tolerant mpls network," in *Advanced Computer Theory and Engineering (ICACTE), 3rd International Conference*, vol. 1, pp. V1–168–V1–172, August 2010.
- [5] A. Ala, M. Essaaidi, and D. El Ouadghiri, "Fast convergence mechanisms and features deployment within operator backbone infrastructures," in *Microwave Symposium (MMS), Mediterranean*, pp. 1–5, November 2009.
- [6] L. D. Ghein, *MPLS Fundamentals*. Cisco Press, 2006.
- [7] I. Hussain, "Overview of mpls technology and traffic engineering applications," in *International Networking and Communication Conference, INCC*, June 2004.
- [8] K. Nguyen and B. Jaumard, "A distributed and scalable mpls architecture for next generation routers," in *International Conference on High Performance Switching and Routing*, pp. 63–68, May 2008.
- [9] M. Rahimi, H. Hashim, and R. Rahman, "Implementation of quality of service (qos) in multi protocol label switching (mpls) networks," in *5th International Colloquium on Signal Processing Its Applications, CSPA*, pp. 98–103, March 2009.
- [10] F. Le Faucheur, "Ietf multiprotocol label switching (mpls) architecture," in *1st IEEE International Conference ATM, ICATM*, pp. 6–15, June 1998.
- [11] M. Porwal, A. Yadav, and S. Charhate, "Traffic analysis of mpls and non mpls network including mpls signaling protocols and traffic distribution in ospf and mpls," in *First International Conference on Emerging Trends in Engineering and Technology, ICETET*, pp. 187–192, July 2008.
- [12] C. Metz, C. Barth, and C. Filsfils, "Beyond mpls ...less is more," *Internet Computing, IEEE*, vol. 11, pp. 72–76, September 2007.

- [13] D. Adami, C. Callegari, S. Giordano, F. Mustacchio, M. Pagano, and F. Vitucci, "Signalling protocols in diffserv-aware mpls networks: design and implementation of rsvp-te network simulator," in *Global Telecommunications Conference, GLOBECOM, IEEE*, vol. 2, pp. 792–796, December 2005.
- [14] K. Shuaib and F. Sallabi, "Extending ospf for large scale mpls networks," in *IEEE/Sarnoff Symposium on Advances in Wired and Wireless Communication*, pp. 13–16, April 2005.
- [15] A. Bongale, N. Nithin, and L. Jyothi, "Traffic prioritization in mpls enabled ospf network," in *World Congress on Information and Communication Technologies (WICT)*, pp. 132–137, October 2012.
- [16] M. Porwal, A. Yadav, and S. Charhate, "Traffic analysis of mpls and non mpls network including mpls signaling protocols and traffic distribution in ospf and mpls," in *First International Conference on Emerging Trends in Engineering and Technology, ICETET*, pp. 187–192, July 2008.
- [17] E. Oki, I. Inoue, and K. Shiimoto, "Path computation element (pce)-based traffic engineering in mpls and gmpls networks," in *Sarnoff Symposium, IEEE*, pp. 1–5, April 2007.
- [18] L. Zhenyu and Z. Zhongzao, "Bandwidth constrained qos routing scheme for mpls traffic engineering," *Journal of Systems Engineering and Electronics*, vol. 15, pp. 735–740, December 2004.
- [19] K. Abboud, A. Toguyeni, and A. Rahmani, "Performance and complexity evaluation of multi-path routing algorithms for mpls-te applied on large scales topologies," in *Second International Conference on Sensor Technologies and Applications, SENSORCOMM*, pp. 782–787, August 2008.
- [20] H. Hodzic and S. Zoric, "Traffic engineering with constraint based routing in mpls networks," in *50th International Symposium, ELMAR*, vol. 1, pp. 269–272, September 2008.
- [21] H. Hodzic and E. Secerbegovic, "Online constraint-based routing as support for mpls traffic engineering," in *International Symposium ELMAR, ELMAR*, pp. 127–130, September 2009.
- [22] C.-H. Yeh, H. Mouftah, and H. Hassanein, "Signaling and qos guarantees in mobile ad hoc networks," in *IEEE International Conference on Communications, ICC*, vol. 5, pp. 3284–3290 vol. 5, 2002.
- [23] R. Peterkin and D. Ionescu, "A hardware/software co-design for rsvp-te mpls," in *Canadian Conference on Electrical and Computer Engineering, CCECE*, pp. 1409–1412, May 2006.
- [24] M. Rahman, A. Kabir, K. Lutfullah, M. Hassan, and M. Amin, "Performance analysis and the study of the behavior of mpls protocols," in *International Conference on Computer and Communication Engineering, ICCCE*, pp. 226–229, May 2008.
- [25] S.-C. Kim and J.-M. Chung, "Analysis of mpls signaling protocols and traffic dissemination in ospf and mpls," in *First Asia International Conference on Modelling Simulation, AMS*, pp. 276–281, March 2007.

- [26] G. Ahn and W. Chun, "Design and implementation of mpls network simulator supporting ldp and cr-ldp," in *IEEE International Conference on Networks, (ICON)*, pp. 441–446, 2000.
- [27] P. Rasiah and J.-M. Chung, "Traffic engineering optimal routing for lsp setup in mpls," in *The 2002 45th Midwest Symposium on Circuits and Systems, MWS-CAS*, vol. 3, pp. III-272–III-275 vol.3, August 2002.
- [28] S. Alouneh, A. Agarwal, and A. En-Nouaary, "A novel approach for fault tolerance in mpls networks," in *Innovations in Information Technology*, pp. 1–5, November 2006.
- [29] M. Callejo-Rodrigitez, J. Enriquez-Gabeiras, W. Burakowski, A. Beben, J. Sliwinski, O. Dugeon, E. Mingozzi, G. Stea, M. Diaz, and L. Baresse, "Euqos: End-to-end qos over heterogeneous networks," in *First ITU-T Kaleidoscope Academic Conference Innovations in NGN: Future Network and Services, K-INGN*, pp. 177–184, May 2008.
- [30] L. Fang, A. Atlas, F. Chiussi, K. Kompella, and G. Swallow, "Ldp failure detection and recovery," *Communications Magazine, IEEE*, vol. 42, pp. 117–123, October 2004.
- [31] P.-K. Park, H.-S. Yoon, S. C. Kim, J. Park, and S. Yang, "Design of a dynamic path protection mechanism in mpls networks," in *The 6th International Conference on Advanced Communication Technology*, vol. 2, pp. 857–861, February 2004.
- [32] M. Sridharan, R. Srinivasan, and A. Somani, "On improving partial information routing with segmented path protection," in *International Conference on Parallel Processing Workshops, Proceedings*, pp. 193–198, 2002.
- [33] R. Martin and M. Menth, "Backup capacity requirements for mpls fast reroute," in *ITG Symposium on Photonic Networks*, pp. 1–8, April 2006.
- [34] R. Martin, M. Menth, and K. Canbolat, "Capacity requirements for the one-to-one backup option in mpls fast reroute," in *3rd International Conference on Broadband Communications, Networks and Systems, BROADNETS*, pp. 1–8, October 2006.
- [35] R. Bartos and M. Raman, "A heuristic approach to service restoration in mpls networks," in *IEEE International Conference on Communications, ICC*, vol. 1, pp. 117–121 vol.1, June 2001.
- [36] J.-M. Chung, "Analysis of mpls traffic engineering," in *Proceedings of the 43rd IEEE Midwest Symposium on Circuits and Systems*, vol. 2, pp. 550–553 vol.2, 2000.
- [37] L. Csikor and G. Retvari, "Ip fast reroute with remote loop-free alternates: The unit link cost case," in *4th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT)*, pp. 663–669, October 2012.
- [38] J. Kim and B. Ahn, "Next-hop selection algorithm over ecmp," in *Asia-Pacific Conference on Communications, APCC*, pp. 1–5, August 2006.

- [39] J. bo Xia, M. hui Li, and L. jun Wan, “Research on mpls vpn networking application based on opnet,” in *International Symposium on Information Science and Engineering, ISISE*, vol. 1, pp. 404–408, December 2008.
- [40] X. Chang, “Network simulations with opnet,” in *Proceedings of the 31st Conference on Winter Simulation: Simulation—a Bridge to the Future - Volume 1*, WSC '99, pp. 307–314, 1999.