REAL-TIME BANDWIDTH ENCAPSULATION FOR IP/MPLS PROTECTION SWITCHING

Mampi Nakutoma Lubasi

This thesis is submitted in partial fulfilment of the requirements for the degree of

Master of Science in Electrical Engineering

in the Faculty of Engineering and the Built Environment

September 2011

As the candidate's supervisor, I have approved this dissertation for submission.

Name: Dr. Alexandru Murgu

Signed: _____ Date: _____

DECLARATION

I know the meaning of plagiarism and declare that all the work in the document, save for that which is properly acknowledged is my own. Where collaboration with other people has taken place, or material generated by other researchers is included, the parties and/or materials are indicated in the acknowledgements or are explicitly stated with references as appropriate.

This work is being submitted in partial fulfilment of the requirements for the Master of Science degree in Electrical Engineering at the University of Cape Town. It has not been submitted to any other university for any other degree or examination.

I hereby grant the university of Cape Town free licence to reproduce for the purpose of research either the whole or any portion of the contents in any manner whatsoever of the above dissertation.

Name: Mampi Nakutoma Lubasi

Sign: _____ Date:_____

DEDICATION

To my late mother Inonge Sibutu Lubasi

ACKNOWLEDGEMENTS

I would like to thank my supervisor Dr. Alexandru Murgu for the guidance and great support during my research work.

I thank my colleagues in the research group for their support during my research work.

To my brother and sister, Ronald and Thumelo Mambwe, thank you for your selflessness and sacrifice. Words are not enough to express how grateful I am for all you have done for me. May God richly bless you.

I thank my family for their love and support during my Master's programme. Many thanks go to my brother Imasiku Lubasi for his financial support, my late uncle Clifford Sifuniso Sibutu and my aunt Inonge Nyumbu for being great parents.

I thank all my friends for being a blessing during my Master's programme at UCT.

Above all, I give glory and honour to my Lord and saviour Jesus Christ, for he has been my sustainer, my provider, my strength, my faithful friend and my all.

ABSTRACT

IP/MPLS communication networks are experiencing an increase in real-time multimedia applications like voice over IP (VOIP) and video. Real-time multimedia applications have stringent quality of service (QoS) requirements with regard to delay, loss, bandwidth and availability. These applications must therefore be provided with prompt recovery from network failure. MPLS fast reroute provides recovery of about 50ms which makes it attractive for the recovery of voice traffic. Voice traffic must be recovered within 50ms so that call quality is not compromised.

Bandwidth reservation and bandwidth allocation are needed to guarantee the protection of voice traffic during network failure. Since voice has a time constraint of 50ms within which traffic must be recovered, real-time bandwidth allocation is required. A bandwidth allocation scheme that prioritises voice traffic will ensure that voice is guaranteed bandwidth during network failure. A mechanism is also required to provide bandwidth to voice traffic when the reserved bandwidth is insufficient to accommodate voice traffic. This mechanism must be able to utilise the working bandwidth or bandwidth reserved for lower priority applications and allocate it to the voice traffic when a network failure occurs.

This research therefore proposes a real-time bandwidth encapsulation mechanism to guarantee Quality of Protection (QoP) to voice traffic during single link and node failures. The mechanism uses label switched path (LSP) preemption and the Russian dolls bandwidth constraint model to guarantee bandwidth to voice. LSP preemption is used to free up bandwidth for protection and the Russian dolls model is used for bandwidth allocation. The metrics used to evaluate the performance of the proposed mechanism are LSP reroute time and packet loss.

Simulations conducted in Optimised Network Engineering Tool (OPNET) modeler showed that this solution achieved faster LSP reroute time and minimal packet loss to voice.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

BGP	Border Gateway Protocol
CR-LDP	Constraint Based Routing Label Distribution Protocol
CSPF	Constrained Shortest Path First
DS-TE	Diffserv-Aware MPLS Traffic Engineering
FEC	Forward Equivalence Class
FIS	Fault Indication Signal
FRS	Fault Restoration Signal
ISIS	Intermediate System-to Intermediate System
LDP	Label Distribution Protocol
LER	Label Edge Router
LFIB	Label Forwarding Information Base
LSR	Label Switching Router
MAM	Maximum Allocation Model
MAR	Maximum Allocation with Reservation
MP	Merge Point
MPLS	Multiprotocol Label Protocol
NHOP	Next-Hop
NNHOP	Next-Next Hop
OSPF	Open Shortest Path First
QOP	Quality of Protection

QOS	Quality of Service
RSVP	Resource Reservation Protocol
RSVP-TE	Resource Reservation Protocol Traffic Extension
VoIP	Voice over IP

1. INTRODUCTION

1.1 BACKGROUND

The continued advancements in technology have enabled communication networks to provide a plethora of network applications and services. These include real-time multimedia applications like voice over IP (VoIP) and video. These applications require high quality of service (QoS) and availability. However, communication networks experience a variety of failures. The failures can be classified as unplanned and planned outages. Planned outages are those that occur during a scheduled maintenance operation while unplanned outages are unpredicted or unexpected. For a scheduled maintenance, the service provider informs the customer in advance and preventive measures are taken to ensure that the outage causes minimal disruption to the services. Since unplanned failures are unpredictable, mechanisms must be in place to accommodate network services in case of failure. Failures are caused by a number of factors such as cable cuts, power failures, human errors, software bugs, hardware failures and natural disasters in the form of earthquakes, fires and floods. Failures cause a degradation in the quality of service (QoS) provided by the network. They can also cause a disruption in communication services and critical operations of an organisation thus leading to revenue losses. Service level agreements (SLAs) between the service provider and customer are therefore important as they state the system availability and the QoS that the network is expected to provide. SLAs are usually defined in terms of latency, jitter, bandwidth guarantees, down time and resilience in terms of failure.

According to a study that was conducted on failures in an IP backbone [1], 80% of failures that occur are unplanned while 20% occur during a period of scheduled maintenance. Of the unplanned failures, 70% affect a single link at a time while the remaining 30% are multiple failures involving a shared router or link. Network resilience or survivability must therefore be an inherent attribute of communication networks. Service protection guarantees that the network will provide an acceptable level of service during failure conditions. The network must be resilient enough to ensure that there will be minimal disruption to the affected services. To guarantee service protection, a communication network should have mechanisms to quickly detect and localize network failures and divert services onto alternative paths. Therefore single

points of failure should be avoided in the network. Enough resources are also required to accommodate network services during failure conditions. These resources include storage, processing, memory and bandwidth. The network resource that this research focuses on is bandwidth.

Multimedia applications have stringent QoS requirements with regard to delay, bandwidth and availability. Prompt recovery from network failure is therefore critical for these applications. Multi Protocol Label Switching (MPLS) recovery provides faster restoration compared to IP rerouting which is too slow for real-time applications.

1.2 MEASURES OF NETWORK RESILIENCE

Network resilience measures include restorability, reliability and availability [2]. Restorability is the fraction of working paths that are capable of being restored by backup routes in the network. Reliability is the probability of a network element operating fully without a failure occurring within a time period. The availability of a network is the probability that the network can deliver the specified QoS at a particular point in time. Network or system availability, A is defined as:

$$A = 1 - MTTR / MTBF ,$$

where MTTR is the mean time to repair and MTBF is the mean time between failures.

- **Mean Time Between Failures (MTBF)**

  The Mean Time between Failures is the average time between consecutive failures.

- **Mean Time To Repair (MTTR)**

  The Mean Time to Repair is the average time to repair a failed network element.

Therefore network unavailability *U*, is defined as:

$$U = 1 - A$$

1.3 OVERVIEW OF IP/MPLS NETWORKS

Multiprotocol Label Switching (MPLS) [3] was developed by the Internet Engineering Task Force (IETF). It is referred to as a layer 2.5 technology because it combines layer 3 IP routing and layer 2 switching. MPLS supports IP, Asynchronous Transfer Mode (ATM) and frame relay protocols hence the name multiprotocol. An MPLS network or domain consists of label edge routers (LERs) at the edge and label switching routers (LSRs) at the core as depicted in Figure 1.1. When an IP packet enters the MPLS network, the ingress node classifies and encapsulates the packet in an MPLS label. The packet is forwarded from one LSR to another based on labels along a label switched path (LSP). The label is removed at the egress node and the packet is delivered to its destination. A label is a short fixed length identifier which is used to identify a forward equivalence class (FEC). A group of packets forwarded the same way or given the same treatment are said to belong to the same FEC. These can be packets with the same destination address or packets belonging to a particular application. Figure 1.2 gives an illustration of the operation of MPLS.

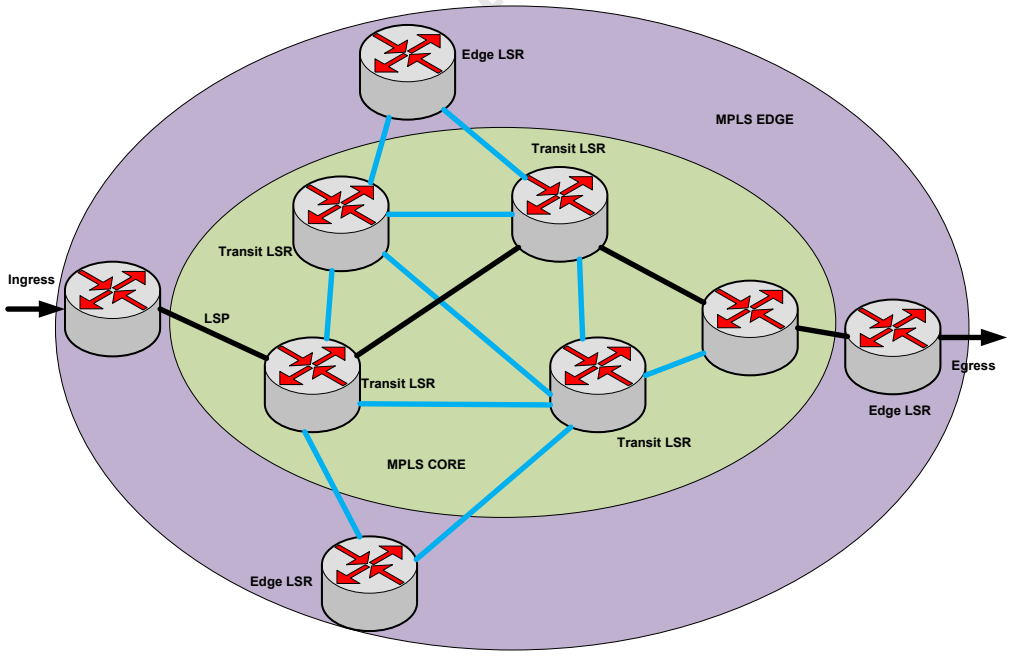

Figure 1.1: MPLS Domain [4]

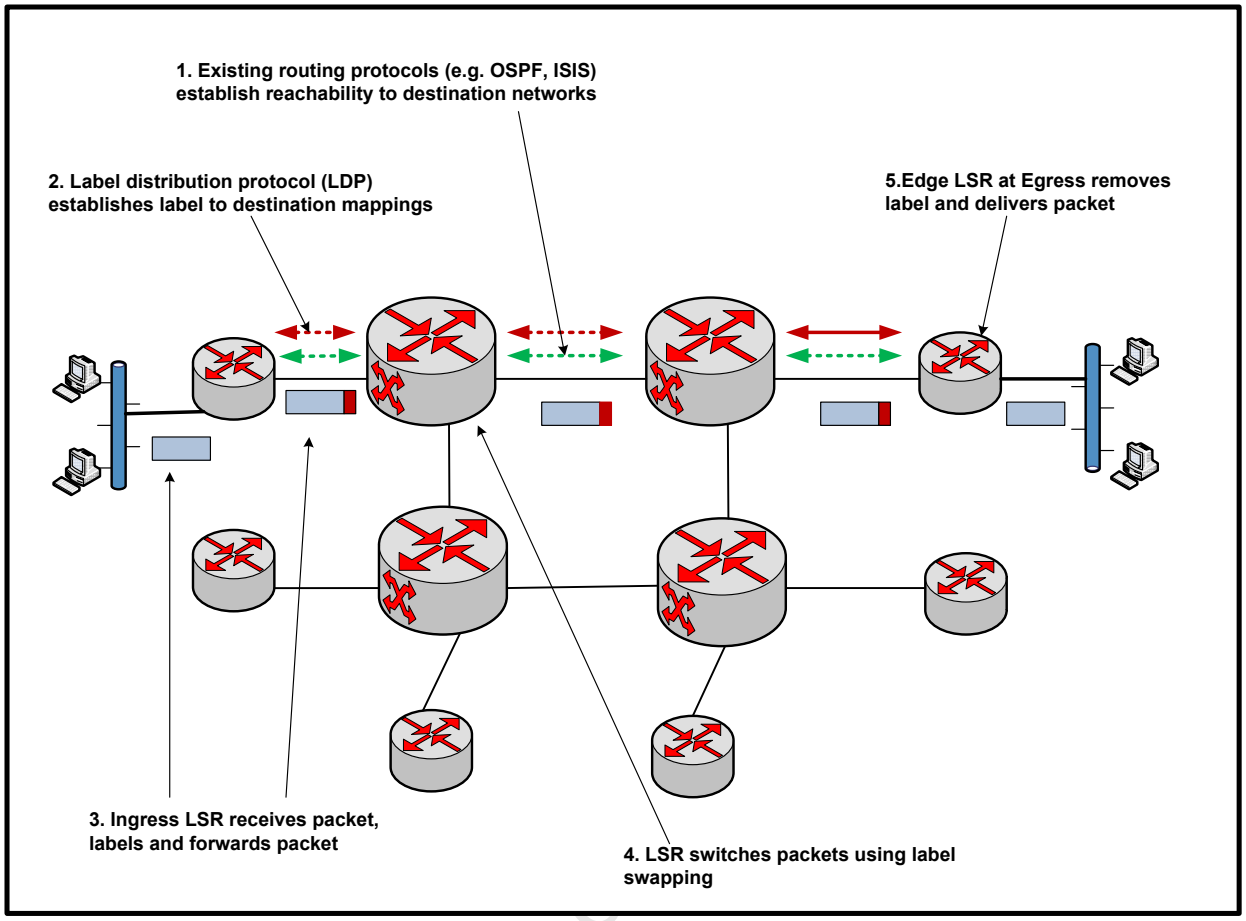

Figure 1.2: MPLS Operation [5]

MPLS is based on two building blocks which are the separation of the control and forwarding or data planes and the label swapping forwarding algorithm [6]. The control plane is responsible for the exchange of routing information and label distribution among LSRs. Routing information exchange is done through the standard routing protocols like Open Shortest Path First (OSPF), Intermediate System-to-Intermediate System (ISIS) and Border Gateway Protocol (BGP). Label distribution protocols that are used are Constraint-based Routing Label Distribution Protocol (CR-LDP), Resource Reservation protocol (RSVP) and Resource Reservation Protocol Traffic Extension (RSVP-TE). These are used to maintain the forwarding table known as the Label Forwarding Information Base (LFIB)

The forwarding or data plane is responsible for the transfer of data across the network. The forwarding algorithm is based on two sources of information and these are the forwarding table

maintained by the LSR and the label carried in a packet. The forwarding table contains entries of an incoming label which may also contain subentries of the outgoing label, outgoing interface and the next hop address. The forwarding plane allows a label to be carried in a packet. This can be supported over link layer technologies by carrying the label in a shim header and the network layer header. The MPLS shim header is depicted in Figure 1.3 and the fields it contains are discussed below [7]:

- A 20 bit header. This is used as an index in the forwarding table and is used for MPLS forwarding.
- Three Experimental (EXP) bits. These are used to specify the class of service of a packet.
- One Bottom of Stack bit (S-bit). This is set on the MPLS packet header at the bottom of the stack.
- Eight Time-to-Live (TTL) bits. These are decremented at each hop as the label encapsulated packet is forwarded within the MPLS packet.

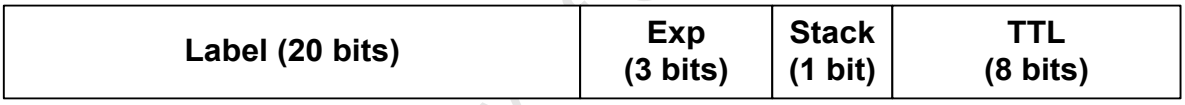

Figure 1.3: MPLS Shim Header [8]

The forwarding algorithm is based on label swapping. Figure 1.4 gives an illustration of how label swapping works. Host A sends IP packets to LSR P using its default route. LSR P which is the ingress node classifies the IP packets according to their destination address, assigns the packets to the appropriate LSP and labels them. Packets destined for host B are assigned to LSP 1 and labeled 20. Packets destined for host C are assigned to LSP 2 and labeled 25. The packets are then sent towards LSR Q. LSR Q checks its LFIB to determine the incoming interface and outgoing interface for the packets. The LFIB contains a mapping for (incoming interface, incoming label) to (outgoing interface, outgoing label). Table 1 shows the LFIB at LSR Q. Label swapping is done, that is, label 20 is swapped with label 32 and forwarded through the specified outgoing interface to LSR R. Label 25 is swapped with label 72 and forwarded through the

specified outgoing interface towards LSR S. LSRs R and S are egress routers. The labels are removed at these LSRs and the packets are delivered to hosts B and C respectively.

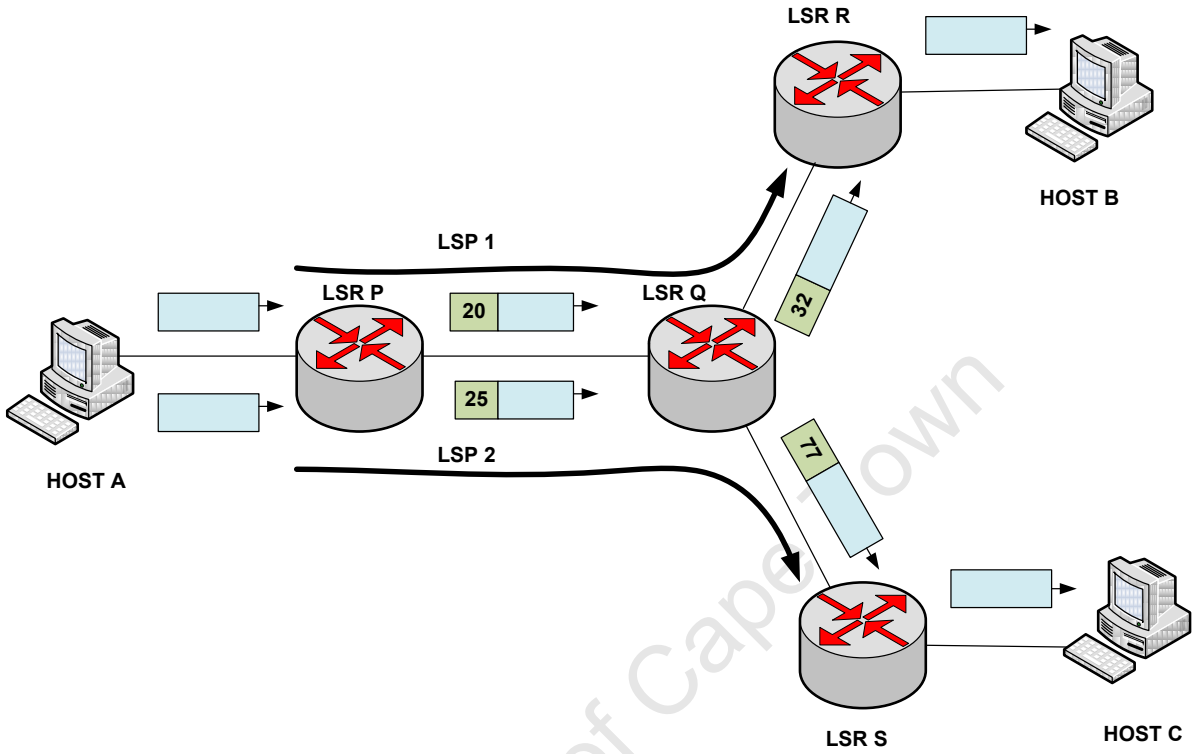

Figure 1.4: Label Swapping [8]

Table 1.1: LFIB at LSR Q

Incoming Interface	Incoming Label	Outgoing Interface	Outgoing Label
From LSR P	20	To LSR R	32
From LSR P	25	To LSR S	77

1.3.1 Advantages of MPLS

MPLS provides several benefits to IP networks. Some of these benefits include:

a) Traffic Engineering

Traffic engineering is the directing of traffic along paths where network resources are available. This is done to improve resource utilisation. Traffic engineering prevents areas of a network from being congested while other areas are underutilized. The path that is taken by traffic is thus controlled to ensure that slow links and those with insufficient bandwidth are avoided. Traffic engineering also enables high priority traffic to be provided with resources when there is contention for network resources.

b) QoS Guarantees

MPLS provides QoS guarantees to delay sensitive traffic like voice and video. MPLS works with Differentiated Services (Diffserv) to provide QoS guarantees to this sensitive traffic. Diffserv uses a differentiated services code point (DSCP) to classify and prioritise traffic. This helps to ensure that higher priority traffic experiences less delay and has bandwidth guarantees in the network.

c) Fast Recovery

MPLS fast reroute provides fast recovery from link and node failures of approximately 50ms thus making it attractive for the protection of real-time applications like VOIP [9]. The backup paths in MPLS fast reroute are pre-computed and signaled before a failure occurs. Traffic is redirected as close to the failure point as possible thus achieving fast restoration.

1.4 PROBLEM DEFINITION

IP/MPLS communication networks support a variety of applications that have different QoS and recovery requirements. Real-time applications like voice demand that they be recovered in 50ms while other applications may not have stringent recovery requirements. Voice traffic is sensitive to loss and delay. Therefore it does not tolerate QoS degradation for long without this being noticed. In order to avoid this QoS degradation, fast recovery with QoS guarantees must be provided to voice traffic. Real-time applications also have high bandwidth consumption therefore efficient bandwidth management is necessary to ensure efficient resource utilisation in providing service protection.

Bandwidth reservation and allocation are necessary to guarantee protection of voice applications. However when there is insufficient bandwidth to allocate to the voice traffic, protection cannot be provided. Therefore there must be a mechanism to provide bandwidth to voice traffic even when there is insufficient bandwidth. Some bandwidth allocation schemes that have been implemented or proposed waste bandwidth while others require high processing capability. Due to the real-time nature of voice traffic a bandwidth allocation scheme that allows for efficient bandwidth utilisation without a lot of processing involved is required.

Customers require that service protection parameters such as recovery time and availability be adhered to as specified in the service level agreement (SLA). Service providers must therefore ensure that they guarantee quality of protection (QoP). QoP is concerned with how effective a failure handling mechanism is. Parameters used to measure QoP include the recovery time or protection switching time and the protection bandwidth amount [10]. The goal of QoP is to provide fast restoration with efficient bandwidth utilisation. Hence efficient provisioning and allocation of resources for protection is vital.

1.5 RESEARCH OBJECTIVES

The objectives of the research are therefore to:

- Investigate MPLS Quality of Protection for single link and node failures.
- Investigate bandwidth allocation to guarantee real-time protection of voice traffic and efficient bandwidth utilisation.
- Investigate the effect of preemption on bandwidth allocation and bandwidth usage.
- Propose a bandwidth management scheme that will guarantee real-time protection of multimedia traffic from single link and node failures.

1.6 METHODOLOGY

This study focuses on the integration of bandwidth allocation with service protection in an MPLS network. Optimised network engineering tool (OPNET) modeler V14.0 was used to simulate an MPLS network. The performance metrics used for evaluation were LSP reroute time, packet loss and end-to-end delay.

1.7 SCOPE AND LIMITATIONS OF RESEARCH

This research focuses on real-time bandwidth allocation for voice traffic during single link and node failures for MPLS local protection. The protection scheme that has been considered in the study is facility backup or many-to-one. The research did not consider how much bandwidth must be reserved to provide a certain degree of protection but assumes that bandwidth to be reserved has already been determined.

1.8 RESEARCH CONTRIBUTION

The contribution of this research is a bandwidth management solution for the real-time protection of voice traffic. The proposed solution incorporates LSP preemption to guarantee bandwidth to voice traffic after a network failure and the Russian dolls model for bandwidth allocation. Simulation results show that this solution guarantees minimum packet loss to voice traffic.

1.9 THESIS OUTLINE

The rest of the thesis is organised as follows:

Chapter 2 discusses MPLS based recovery. Global protection and fast reroute are presented and how they are achieved. The chapter also briefly looks at some hybrid mechanisms that have been proposed.

Chapter 3 discusses bandwidth management in an MPLS network. Resource reservation protocol (RSVP) and its role in MPLS is presented. Diffserv-aware MPLS traffic engineering (DS-TE) bandwidth constraint models with particular emphasis on the Russian Dolls Model (RDM) are discussed. The chapter also presents a literature review on current trends in MPLS recovery.

Chapter 4 presents the proposed real-time bandwidth encapsulation mechanism to guarantee Quality of Protection (QoP) to voice traffic during single link and node failures. The system model used to test the solution and the simulations done in OPNET are also presented.

Chapter 5 presents and discusses the results of the simulations done.

Chapter 6 concludes the thesis and presents recommendations for future work.

2. MPLS RECOVERY MECHANISMS

2.1 INTRODUCTION

Chapter 1 gave an introduction to the thesis and set the context for the research. This chapter presents a background on MPLS based recovery. The chapter begins by discussing the MPLS recovery cycle and proceeds to discuss MPLS based recovery mechanisms. Global protection and local protection are discussed and how these are achieved. The criteria used for performance evaluation of a recovery mechanism are presented and the chapter concludes by discussing hybrid MPLS recovery mechanisms.

2.2 MPLS RECOVERY CYCLE

Before delving into the discussion of MPLS recovery mechanisms, the MPLS recovery cycle will be discussed. The MPLS recovery cycle gives the stages that a recovery mechanism transitions from the occurrence of a failure to the restoration of traffic onto Label Switched Paths (LSPs). Figure 2.1 gives an illustration of the MPLS recovery cycle.

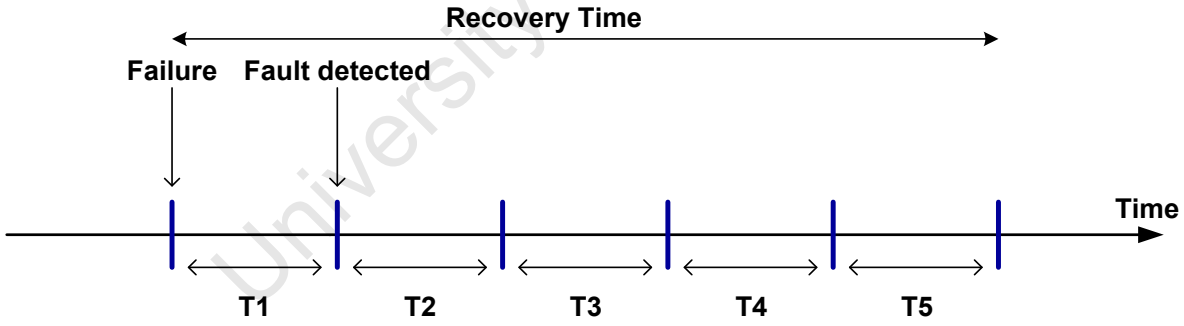

Figure 2.1: MPLS Recovery Cycle [11]

T1 = Fault Detection Time

T2 = Fault Hold-off Time

T3 = Fault Notification Time

T4 = Recovery Operation Time

T5 = Traffic Recovery Time

As illustrated in Figure 2.1, the phases of the MPLS recovery cycle are discussed in the next section:

- **Fault Detection Time**

  This is the time between the occurrence of a network failure and the moment when a fault is detected by MPLS recovery mechanisms.

- **Fault Hold-off Time**

  This is the waiting time between detection of a failure and taking MPLS based recovery action to allow for lower layer protection to take effect.

- **Fault Notification Time**

  This is the time for the fault indication signal (FIS) to be received by the node in charge of traffic recovery. FIS is the signal of a failure to the node in charge of the traffic recovery. This could be the node immediately upstream to the failure point known as the Point of local repair (PLR) or the head-end LSR.

- **Traffic Operation Time**

  This is the time between the first and last recovery cycle.

- **Traffic Recovery Time**

  This is the time between the last recovery action and the time traffic is completely recovered.

2.3 TYPES OF MPLS RECOVERY

Recovery mechanisms in MPLS [11] can be classified into protection switching and restoration. In protection switching, the backup path is preplanned and fully signaled before a failure occurs. In restoration, a backup path may be preplanned or dynamically allocated, however additional signaling will be required to establish the backup path when a failure occurs. Protection switching has the advantage of fast recovery times. Restoration is more flexible in terms of the failure scenarios that it can recover from. Therefore to achieve fast recovery of protection traffic, protection switching is preferred.

Protection switching mechanisms are classified as global protection and local protection [8, 12]. These mechanisms are discussed in the section that follows:

2.3.1 Global Protection

Global protection is also known as path protection. In global protection, when a link or node failure occurs, the FIS is sent to the ingress node for the triggering of the recovery process. This leads to a longer recovery time which may not be ideal for the protection of real-time applications. The entire path from source to destination is bypassed when a failure occurs along the working path. As shown in Figure 2.2, when a failure occurs on the link B→C, the entire path A→B→C→D→E is avoided. Traffic will be redirected onto the path A→G→F→E. There are several variants of path protection and these are discussed next:

(i) 1+1 Protection

In 1+1 protection, there is one dedicated backup path to protect the working path. Resources on the backup path are dedicated to the protection of the working path and may not be used for anything else. 1+1 protection has short recovery times, however it is expensive to implement due to high bandwidth usage.

(ii) 1:1 Protection

In 1:1 protection, there is one backup path to protect the working path. Low priority traffic may be carried on the backup path. When a failure occurs, the low priority traffic is pre-empted or dropped from the recovery path to accommodate the high priority traffic to be protected.

1:1 protection can be extended to 1:N protection and M:N protection. 1:N protection has 1 working path protected by N backup paths. M:N protection has M working paths protected by N backup paths.

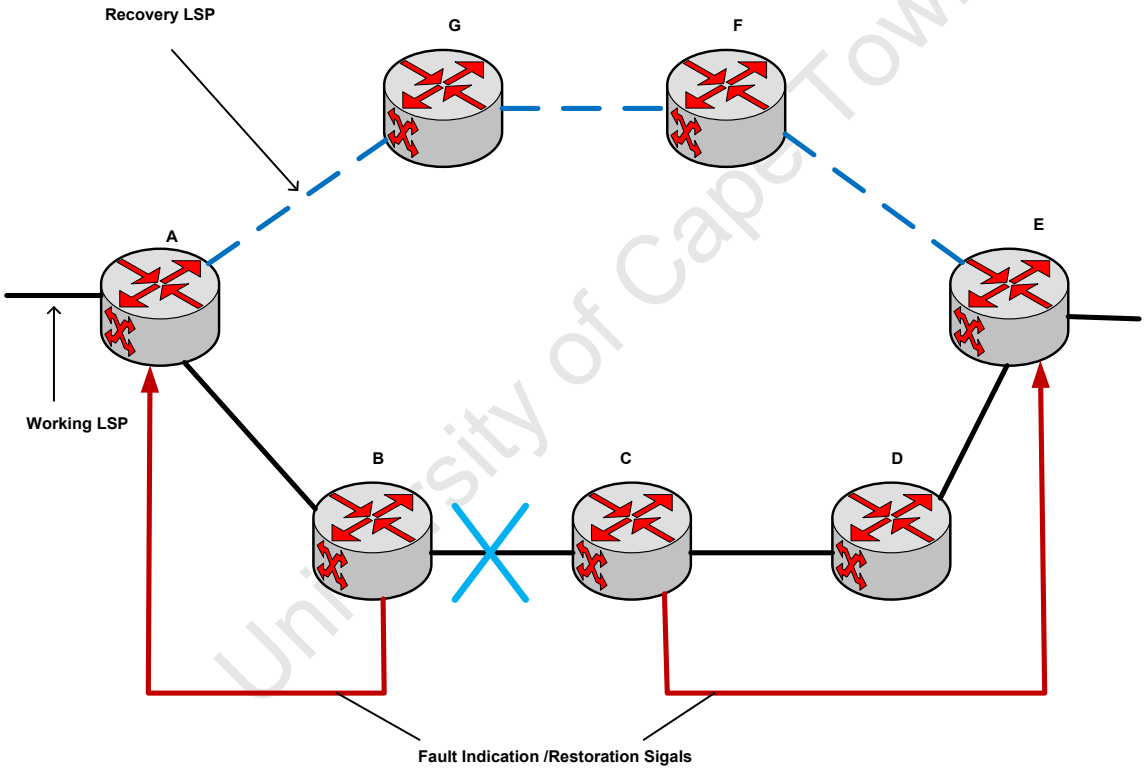

Figure 2.2: Global Protection [8]

2.3.2 Local Protection

The term Fast reroute is used to refer to local protection. Local protection can be either link protection or node protection. When a node or link failure occurs, the LSP is rerouted by the node that is immediately upstream to the failed network element. This node is called the point of local repair (PLR). The head-end of the backup path is the upstream router and the tail-end is the downstream router. In local protection, only the failed network elements are bypassed, therefore, recovery is done as close to the failure point as possible. When a backup LSP terminates at the PLR's next hop neighbor, the backup LSP is known as a next-hop (NHOP) backup tunnel. If the backup LSP terminates at the neighbor of the PLR's neighour it is known as a next-next-hop (NNHOP) backup tunnel. The node where the backup tunnel terminates is known as the merge point (MP). This is where the backup tunnel rejoins the path of the protected LSP. To ensure fast reroute the backup path must be pre-computed and pre-signaled before a failure occurs and the forwarding state must be in place at the PLR, MP and transit nodes. This will allow traffic to be forwarded onto the backup path by the PLR node and back onto the main path at the MP. There are two methods used for local protection and these are one-to-one backup and facility backup.

Local protection achieves short recovery times hence is ideal for the protection of real-time multimedia traffic which is sensitive to loss and delay.

i. One-to-One Backup

In One-to-One backup, a backup tunnel is established for each protected LSP. The backup tunnel is known as a detour. To protect an LSP that traverses N nodes, there could be as many as (N-1) detours. As shown in Figure 2.3, if there is a failure on the link B→C or if node C fails, traffic on the LSP A→B→C→D→E will be redirected onto the backup tunnel B→F→G→D. Traffic on the LSP H→B→C→D→J will be redirected onto the backup tunnel B→I→D.

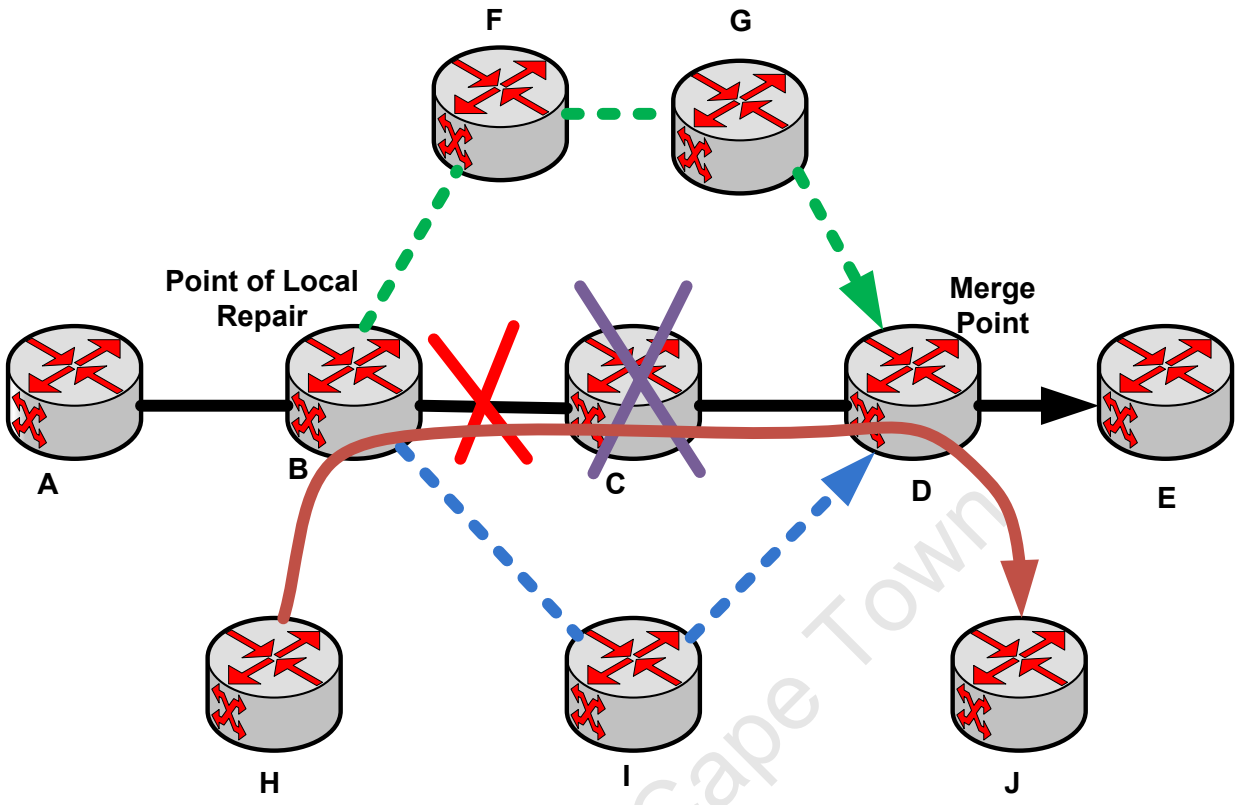

Figure 2.3: One-to-One Backup

In one-to-one backup the label the traffic arrives with at the merge point is different from the label the traffic would have arrived with on the protected LSP. Figure 2.4 shows the protected LSP A→B→C→D→E and the backup tunnel B→F→G→C set up to protect the link B→C. The forwarding state at each node is also shown.

Figure 2.5 shows an IP packet with the label 50 pushed onto it at node A. When a failure occurs on link BC, the label 50 is swapped with the backup tunnel label 100 and the IP packet is forwarded onto the backup tunnel B→F→G→C with label 100. At node F on the backup tunnel, label 100 is swapped with label 200. At node G, label 200 is swapped with label 300 and the traffic is forwarded back onto the protected LSP at the merge point. The traffic therefore arrives back onto the protected LSP at the merge point with a different label, that is, the label of the backup tunnel. Label 300 is then swapped with label 70, label 70 is popped from the IP packet and the packet is delivered to its destination. Therefore, the merge point must maintain the forwarding state that maps the backup tunnel label with the label of the protected LSP. New

forwarding state must be installed at the PLR and the MP. One to one backup increases the state overhead since a separate backup path has to be in place for each protected LSP.

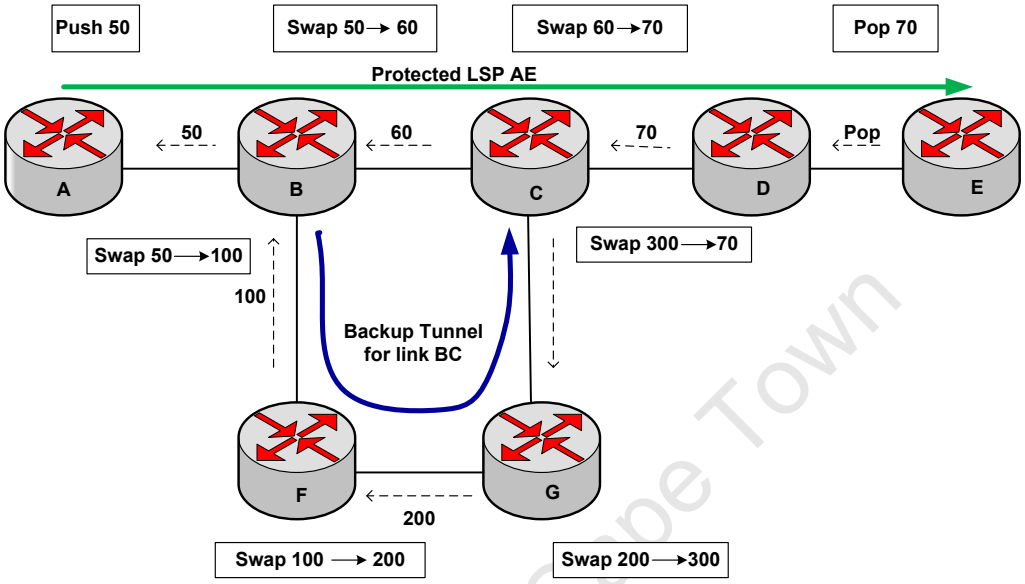

Figure 2.4: One-to-One Backup Setup [7]

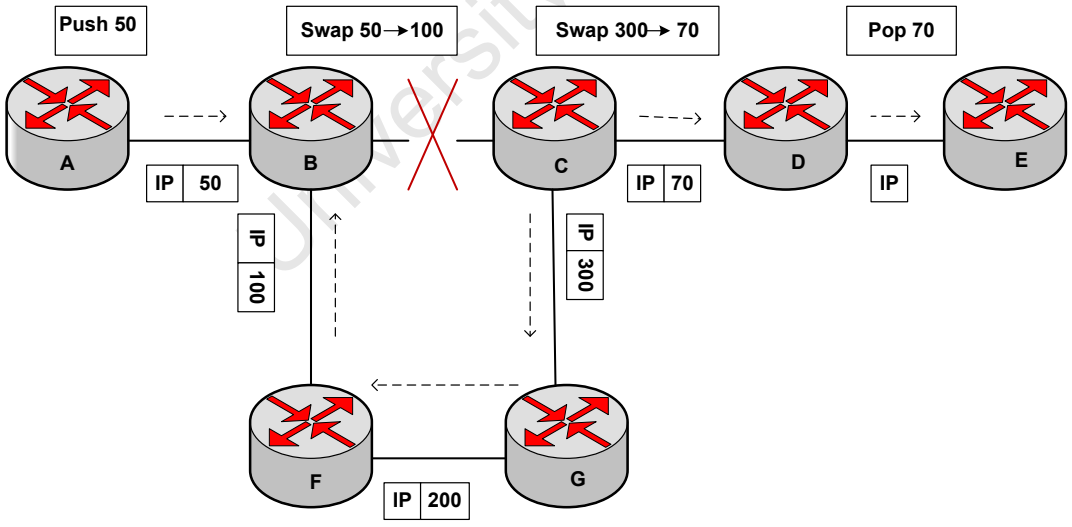

Figure 2.5: One-to-One backup Traffic Forwarding [7]

ii. Facility Backup

Facility backup is also known as many-to-one. In Facility backup, a backup tunnel can protect a set of LSPs. The backup tunnel established is known as bypass. Similarly, there can be (N -1) bypass tunnels to protect an LSP that traverses N nodes. When an NHOP backup tunnel is used this is referred to as link protection and when an NNHOP backup tunnel is used, this is referred to as node protection. As shown in Figure 2.6, one NNHOP bypass tunnel is configured on node B to protect the LSPs A→B→C→D→E and H→B→C→D→I from a failure of node C and the link B→C.

In facility backup, the label the traffic arrives with on the backup path is the same label it would arrive with on the main or protection path. This is accomplished by label stacking and penultimate hop-popping. Label stacking is achieved by pushing the label of the backup tunnel on top of the label of the protection LSP at the PLR node. Penultimate hop-popping is achieved when the backup tunnel label is removed one hop before the MP node. This allows traffic to flow back onto the main path with the original label it had before being redirected onto the backup tunnel

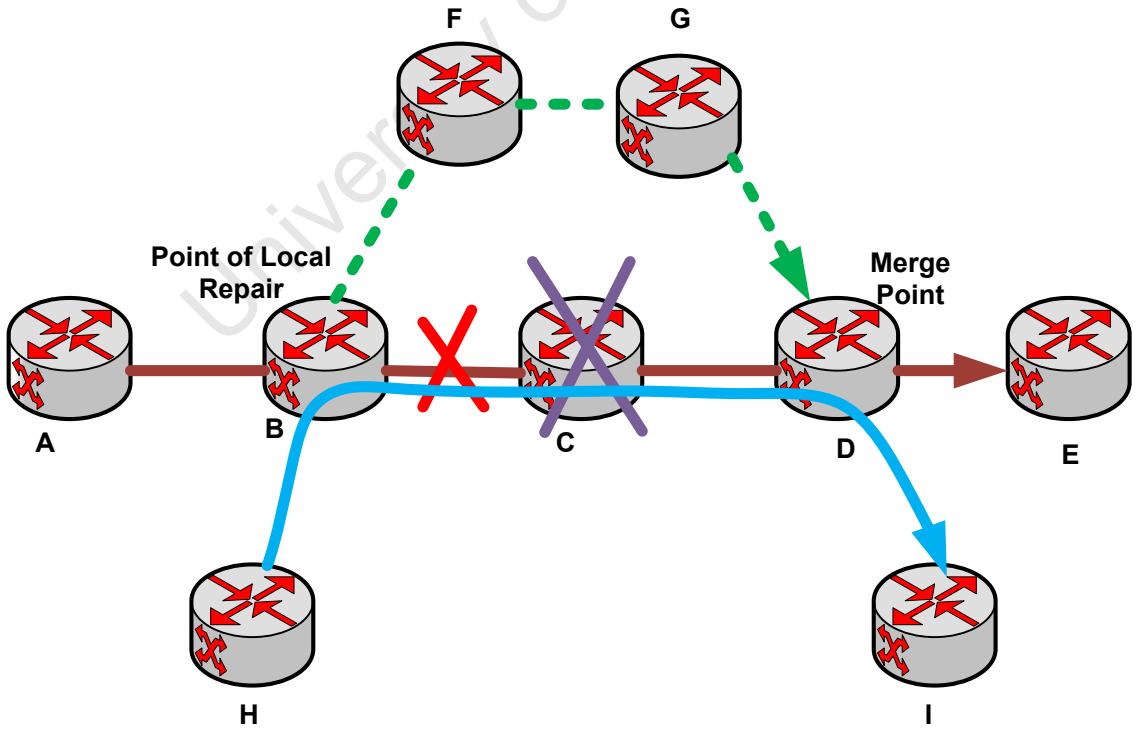

Figure 2.6: Facility Backup

Figure 2.7 shows the LSP A→B→C→D→E which is protected by the backup tunnel B→F→G→C if the link B→C fails. The forwarding state at each hop along the path is shown. Figure 2.8 shows an IP packet with the label 50 pushed onto it at router A. When link B→C fails, label 50 is swapped with label 60 and the backup tunnel label 100 is pushed on top of the protected LSP label. When the packet gets to router F, label 200 is swapped with label 100. At node G, which is one hop before the MP, the label 200 is popped from the IP packet. At node C, which is the merge point, the label 60 is swapped with label 70 and traffic flows back onto the main or protected LSP with the original label it would have had before the failure.

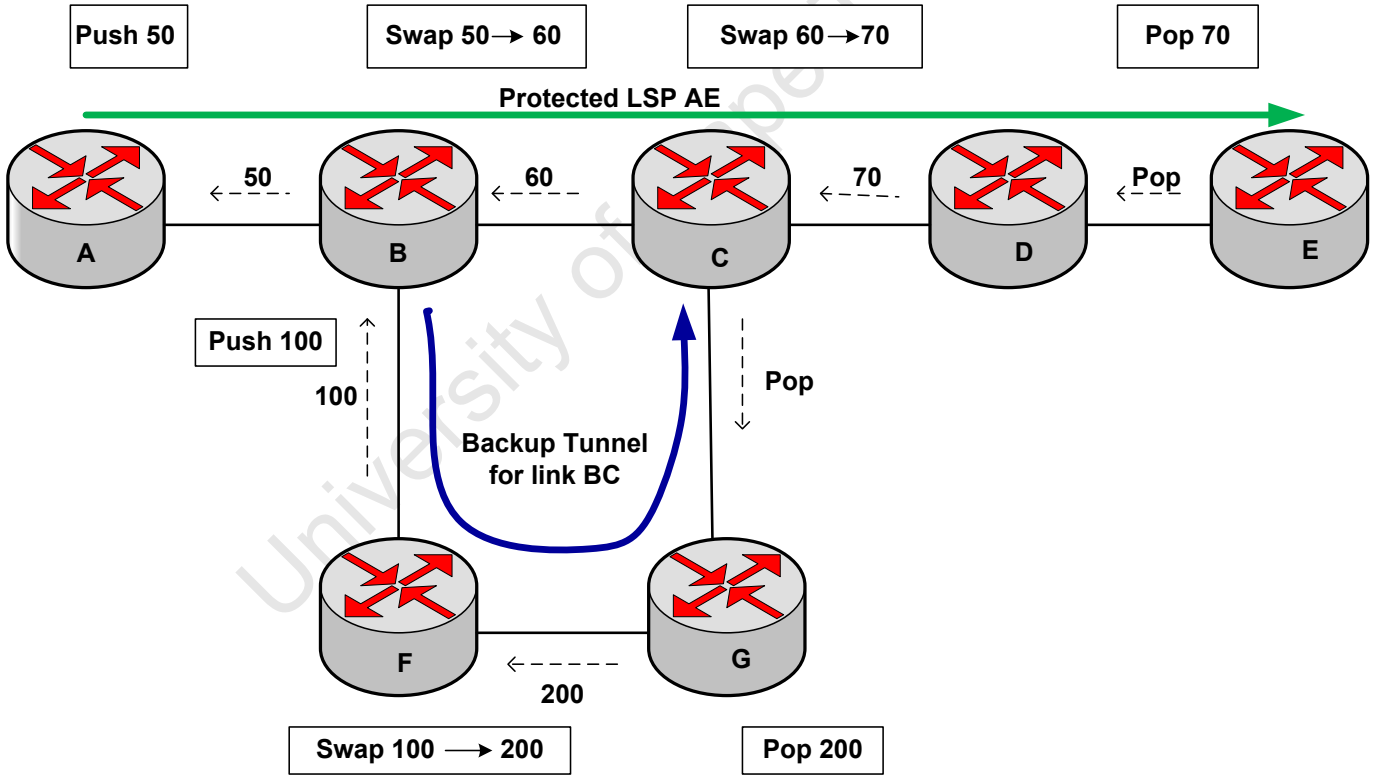

Figure 2.7: Backup Tunnel Setup for Facility Backup [7]

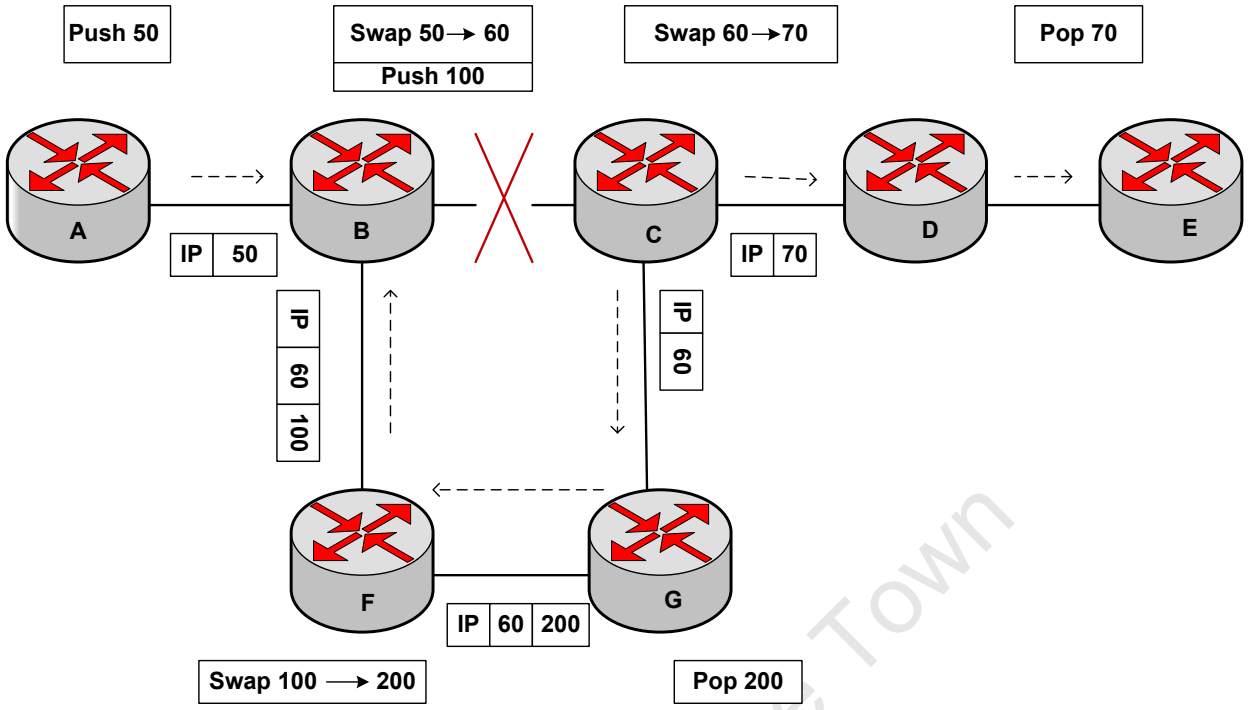

Figure 2.8: Facility Backup Traffic Forwarding [7]

For node protection, the backup tunnel used is a next-next hop (NNHOP). Figure 2.9 shows the LSP A→B→C→D→E which is protected by the NNHOP backup tunnel B→F→G→D when the node C fails. Node B will therefore require the following information to set up the backup tunnel:

- Node D's address which is the merge point. This address is used as a loose hop to the merge point. This address can be the router ID or the interface address.
- The label of the main LSP at node D. Since traffic on the backup path must arrive at the merge point with the same label as that of the main LSP, node B must swap the incoming label, 50 with label 70 which is the expected label at node D instead of label 60 which is used for normal forwarding on the main path.

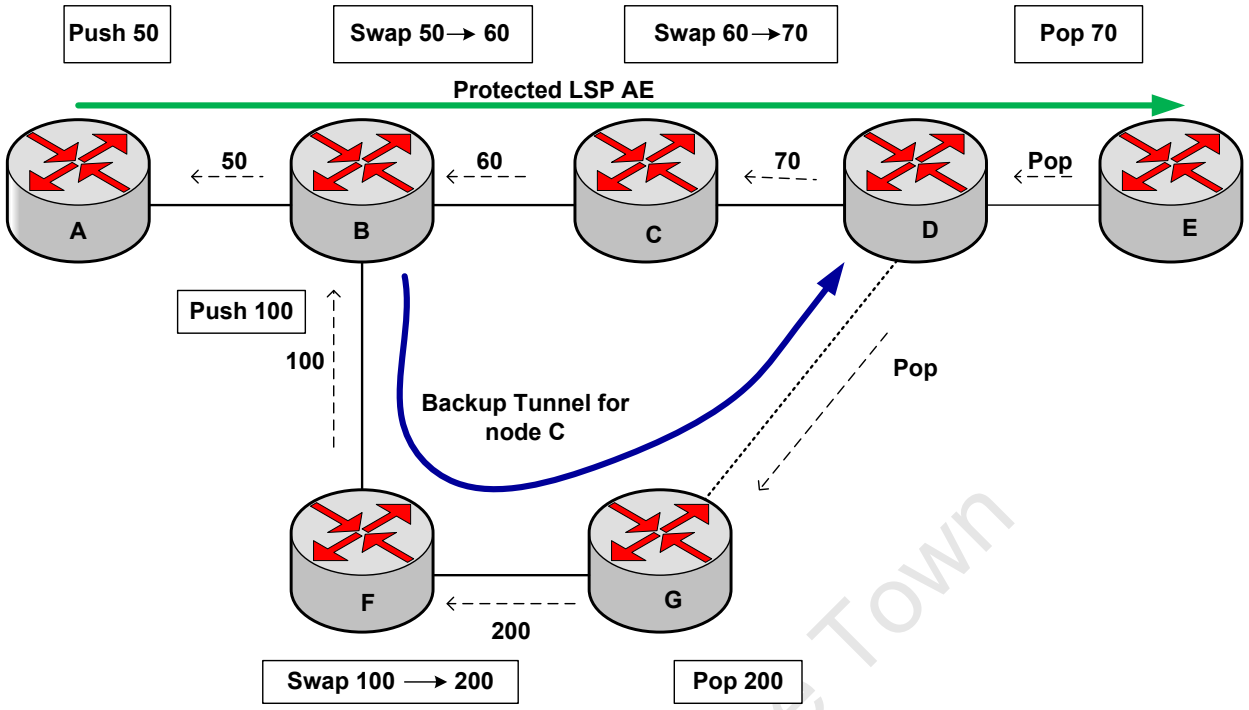

Figure 2.9: Node Protection Setup [7]

Figure 2.10 shows an IP packet with the label 50 pushed onto it at node A. At node B, traffic is already labeled with the label expected by node D before the backup tunnel label is pushed onto it. After the failure of node C, label 50 is swapped with label 70 which is the label expected at node D. The backup tunnel label 100 is pushed onto the IP packet and the packet is forwarded onto the backup tunnel. At node F, the label 100 is swapped with label 200. At node G, the label 200 is popped out and the packet is forwarded with label 70. At the merge point, the label 70 is popped out and the packet is forwarded to its destination.

Node protection protects against both link and node failures. Label recording is also necessary for the PLR to know the label expected at the MP.

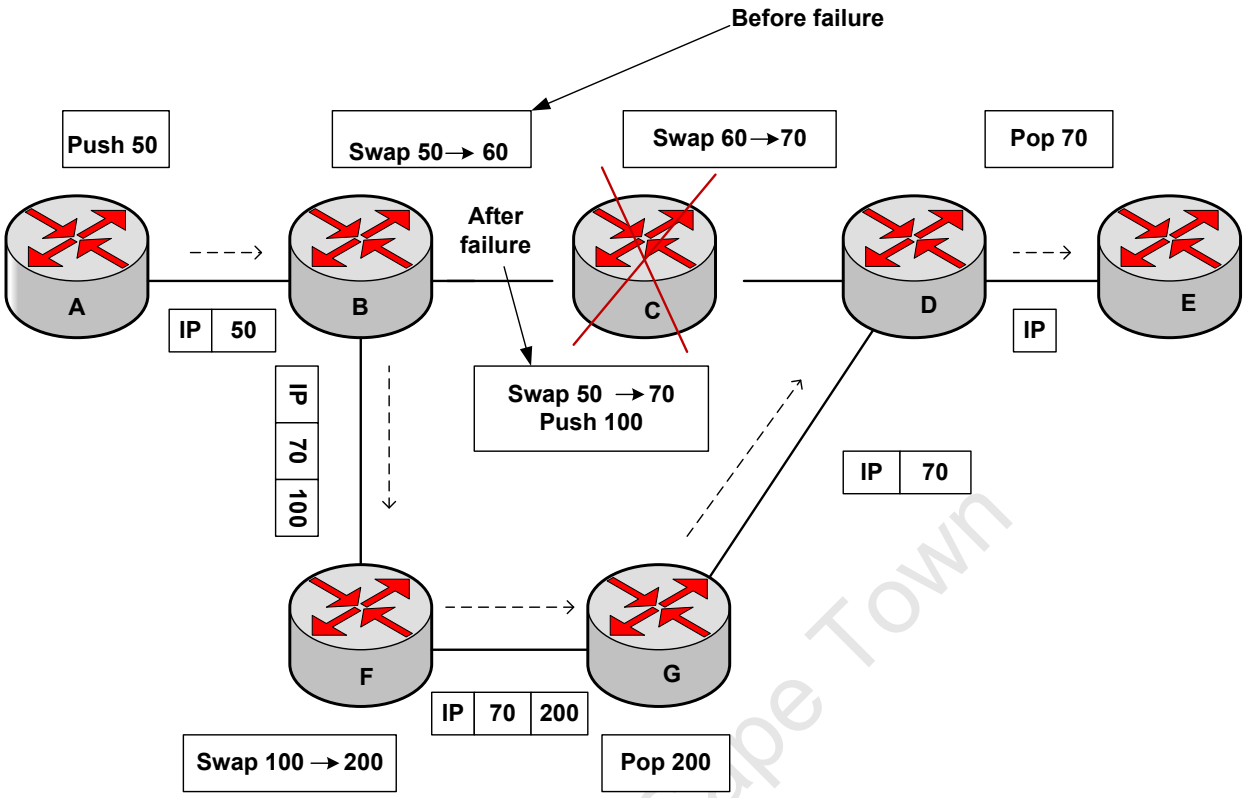

Figure 2.10: Node Protection Traffic Engineering [7]

The one-to-one backup option has more overhead than the facility backup. This is due to the fact that one-to-one backup requires more backup paths than facility backup thus increasing the overhead. In [13] the configuration overhead in terms of backup paths for facility backup and one-to-one backup was evaluated. The results showed that facility backup had less configuration overhead than one-to-one backup.

2.4 PATH CALCULATION AND SETUP

Paths are calculated offline using an offline tool or online using Constrained Shortest Path First (CSPF). CSPF is based on constraint based routing and calculates the shortest path that meets a set of constraints. These constraints include bandwidth, number of hops and link colouring. Link colouring is used to include or exclude a set of links from a path.

After the path has been calculated or computed, the path is set up or signaled using a signaling protocol like resource reservation protocol RSVP. There are three options for path set up and these are discussed in the section that follows [11]:

- **Pre-established**
  A pre-established recovery path is setup before a failure occurs.

- **On-demand**
  An on-demand recovery path is established after a failure occurs.

- **Pre-qualified**
  A pre-qualified recovery path is set up for other purposes but is designated as a recovery path when it is deemed suitable to be a recovery path after a failure occurs.

2.5 PERFORMANCE EVALUATION FOR RECOVERY MECHANISM

There are a number of criteria used to evaluate the performance of a recovery mechanism. Some of the criteria used are discussed in this section [11, 13]:

- **Recovery Time**
  The recovery time is the time between the occurrence of a failure and the time that a recovery or backup path is installed and traffic starts to flows through it. Higher recovery times lead to higher packet losses thus adversely affecting critical services. Smaller recovery times are desirable especially for real time applications like voice that require recovery times of about 50ms.

- **Backup capacity**

  Different recovery mechanisms have different bandwidth requirements. The backup capacity requirements may depend on factors such as the algorithm used for the recovery mechanism. One of the goals of a recovery mechanism is to allow for efficient capacity utilisation.

- **Quality of Protection (QoP)**

  The quality of protection is the effectiveness of the failure handling. An important parameter that is used to measure the quality of protection is the protection switching time. A small protection switching time and efficient bandwidth utilisation are important features of a recovery or protection scheme.

- **State overhead**

  Having more recovery paths increases the state required to store information in the network nodes. A recovery scheme must aim to reduce the state overhead.

- **Reordering**

  After traffic has been switched to a backup path, packet reordering may occur at the destination.

- **Additive latency**
-

  In some cases a backup path may be longer than the main path thus increasing the additive latency. Longer backup paths may also require more backup capacity.

- **Signaling requirements**
-

  Some recovery mechanisms may require more signaling than others. Having a high number of signaling messages leads to high resource usage thereby reducing available resources in the network.

- **Notion of recovery class**

  Some recovery mechanisms provide differentiated recovery. Different traffic classes may have different recovery requirements. For instance, voice requires recovery times of about 50ms while other traffic types may not have stringent requirements in terms of recovery time.

2.6 HYBRID MECHANISMS

MPLS recovery mechanisms that seek to benefit from the merits of protection switching (proactive) and restoration (reactive) have been proposed. In, [14] a hybrid algorithm that combines Gonfa, a protection switching algorithm and Otel, a restoration algorithm was proposed. Simulations were carried out in Network Simulator Version 2 (NS2) and the parameters used for performance evaluation were recovery time, packet loss, packet re-ordering and ability to recover from multiple faults. The results from their analysis showed that the hybrid mechanism performed better than protection switching and restoration mechanisms.

Ali et al [15] proposed a hybrid mechanism that combines protection switching where backup paths are pre-planned and on-line backup path calculation. This mechanism allows for more efficient resource utilisation due to an up-to-date network state. Computation of LSPs is done by a master node working in collaboration with a path computation element. Simulations were conducted in NS2 and the metrics used for performance evaluation were packet loss and packet re-ordering. The results of this approach showed that there was a reduction in the recovery time and efficient resource utilisation.

Another hybrid approach is segment repair. Segment repair is a hybrid of global repair and local repair. In segment repair, the working path is viewed as adjacent segments each having one backup path. In [16] an adaptive segment repair scheme aimed at improving failure recovery was proposed. QoS parameters that were used to evaluate the performance of the scheme included resource utilisation, packet loss, recovery time and failure probability. Simulations were conducted in NS2 with MPLS Network Simulator (MNS v2.0) and the results showed that there was a strong relation between packet loss and recovery time. The proposed scheme achieved fast restoration and increased network resource utilisation.

2.7 CHAPTER SUMMARY

This chapter presented background information on MPLS recovery mechanisms. Restoration and protection switching are the two types of recovery in MPLS. In restoration the backup paths are dynamically allocated. In protection switching the paths are preplanned. Protection switching achieves faster recovery than restoration.

Protection mechanisms are classified as global protection and local protection. Global protection is also known as path protection and local protection is also known as fast reroute. Global protection avoids the entire path when a failure occurs on the path. Fast reroute bypasses the failed network elements only thus achieving faster restoration. Fast restoration is therefore ideal for protection of real-time applications like voice. One-to-one backup and facility backup also known as many-to-one are the two types of local protection. Local protection is also known as fast reroute. One-to-one backup has a protection LSP for all LSPs that need protection while many-to-one backup only has one LSP protecting all LSPs that need protection.

To establish LSPs and reserve bandwidth in MPLS a signaling protocol like RSVP is required. The next chapter will therefore discuss RSVP and its role in bandwidth management in MPLS. The next chapter will also present a literature review on the current trends in MPLS recovery.

3. BANDWIDTH MANAGEMENT AND LITERATURE REVIEW

3.1 INTRODUCTION

In chapter 1, it was emphasized that in order to guarantee service protection, mechanisms must be in place to quickly detect a fault and redirect traffic onto alternative paths. It was also emphasised that bandwidth must also be available to accommodate traffic during failure conditions. Chapter 2 discussed how traffic is redirected onto backup paths when a link or node failure occurs through MPLS recovery mechanisms. This chapter discusses bandwidth management for service protection. Bandwidth is a valuable resource in a communication network and must therefore be managed well to achieve efficient bandwidth utilisation.

This chapter begins by discussing bandwidth protection and the need for bandwidth reservation. The chapter then proceeds to discuss Resource Reservation protocol (RSVP) and its role in LSP setup and bandwidth reservation. Bandwidth Constraints models for bandwidth allocation with particular emphasis on the Russian Dolls Model (RDM) are discussed. Finally, a literature review on the current approaches to MPLS recovery is presented. The aims of this chapter are therefore to:

- Explain the need for bandwidth protection in service protection.
- Explain the role of RSVP in bandwidth management.
- Validate the suitability of the Russian Dolls Model for bandwidth allocation.
- Describe the current methods used in MPLS recovery and the factors that are considered.

3.2 BANDWIDTH PROTECTION

Bandwidth protection guarantees that the backup path is able to provide equivalent bandwidth as that of the protected LSP. This implies that traffic on the backup path will not suffer QoS degradation. Therefore, there is need to reserve bandwidth to accommodate traffic during failure conditions.

Bandwidth reservation prevents unstable behaviour by ensuring that there is sufficient backup capacity. Backup capacity can be dedicated or shared.

Dedicated backup capacity allows for a one-to-one relationship between capacity for the working path and the backup resources. This is illustrated in Figure 3.1. The LSP A→B→C is protected by the backup path A→D→E→F→C if node B fails. The LSP G→H→I is protected by the backup LSP G→D→E→F→I if node H fails. The backup LSPs A→D→E→F→C and G→D→E→F→I do not share common resources despite both paths passing through D→E→F.

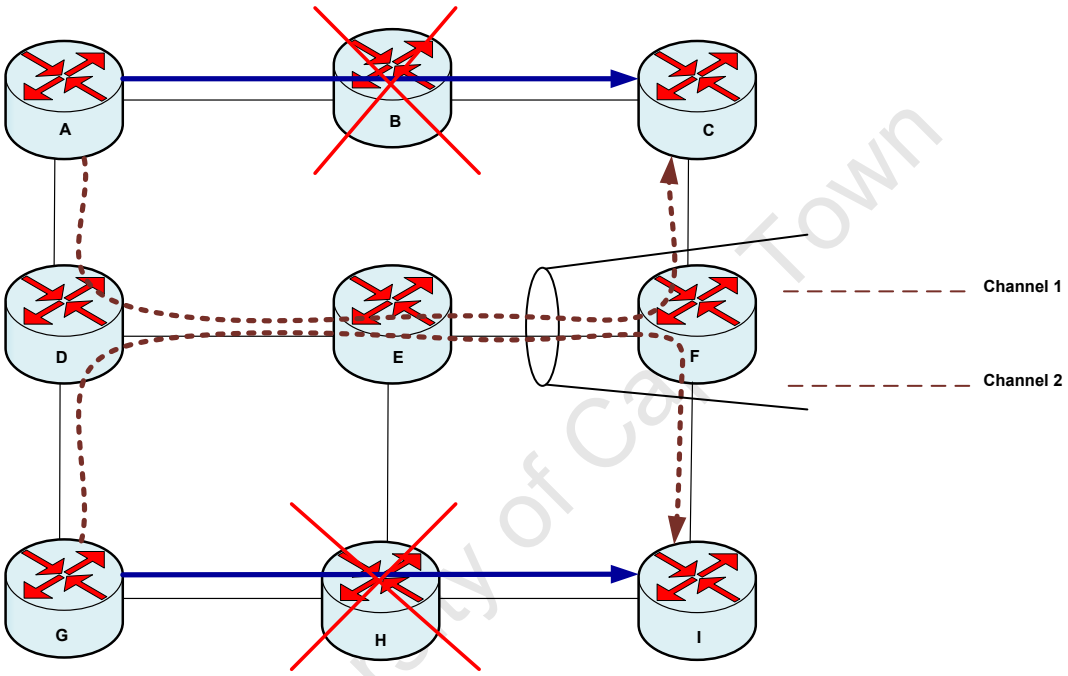

Figure 3.1: Dedicated Backup Capacity [12]

Shared capacity allows several working paths to use a single backup resource. There is a one-to-many relationship between the backup resource and the working paths. This works under the assumption that there will be only one single failure at a time and there will not be simultaneous or multiple failures. If resources were reserved for each backup path in the network the network would be overloaded and the resources would be quickly used up. Backup paths can share resources along common paths thus allowing efficient resource utilisation. Figure 3.2 shows the backup paths A→D→E→F→C and G→D→E→F→I sharing one common channel.

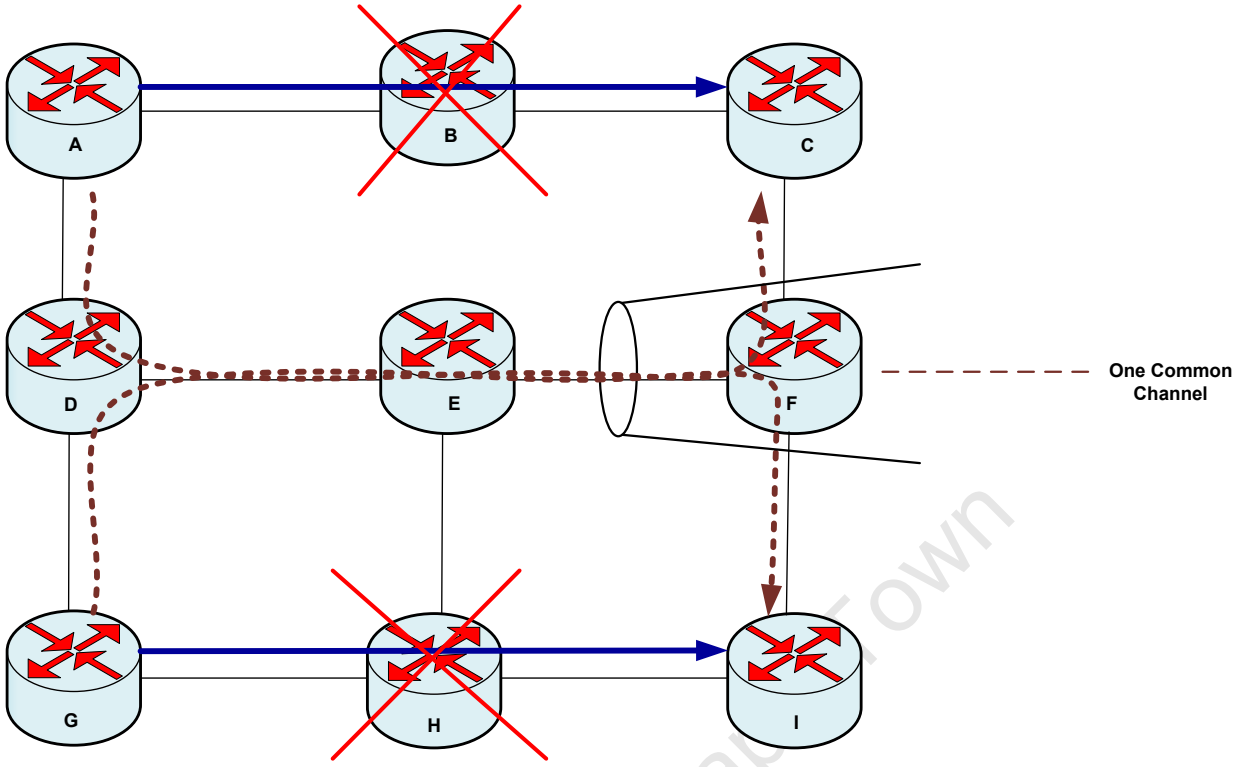

Figure 3.2: Shared Backup Capacity [12]

Figure 3.3 shows a network containing 6 nodes with two primary LSPs, LSP1 and LSP2. LSP 1 from A→B has a backup path A→C→D→B. LSP2 from E→F has a backup path E→C→D→F. Without bandwidth sharing, a total of 6 units of bandwidth would be reserved; one unit on each of the links A→C, D→B, E→C, D→F and 2 units on link C→D. However since LSP1 and LSP2 are failure disjoint, that is, they are not expected to fail at the same time, only one unit of bandwidth must be reserved on the link C→D instead of two. Therefore, 5 units of bandwidth must be reserved in the network instead of 6 thus reducing the backup capacity.

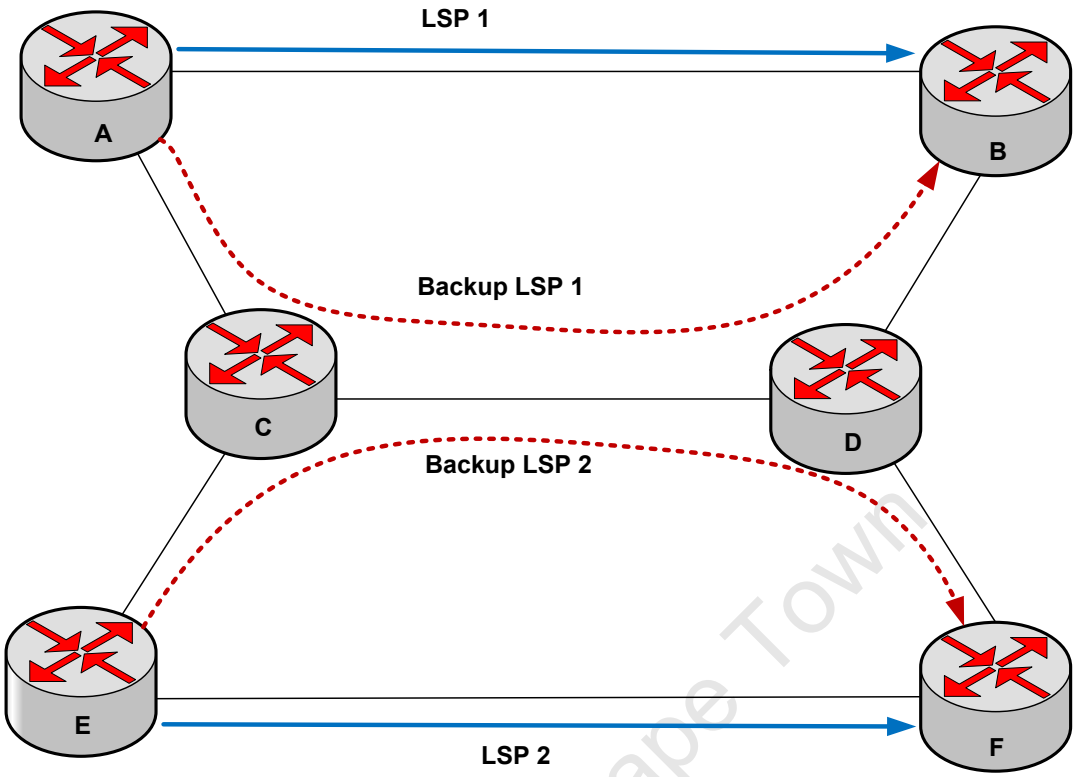

Figure 3.3: Shared Bandwidth Reservation [17]

3.3 RSVP

Resource Reservation Protocol (RSVP) [18] is a signaling protocol used to reserve bandwidth in a network. RSVP was extended for MPLS Tunnels as RSVP-TE [19] to include the features that follow [8]:

- **Label Management**

  RSVP-TE allows for label distribution as the path is established hop-by-hop and bandwidth reservation to be done along the path. The labels are distributed in the path message using the label request object.

- **Control of Explicit routes**

  Signaling of explicit paths is enabled by including an explicit route object in a path or resv message. As the path or resv messages are moved from hop to hop, the explicit route is created. This process is known as route recording.

- **Connectivity Maintenance**

  A new message type, the hello message was added. Adjacent routers exchange hello messages for controlling connectivity between them. This allows a router to know when its neighbor is down.

- **Preemption**

  If insufficient resources are available, preemption of LSPs may be necessary. The holding priority of an LSP determines which LSP can preempt another while the setup priority determines how the LSP is routed and consumes bandwidth.

  Preemption is the removal of an LSP from a given path to accommodate a higher priority LSP. Preemption enables high priority LSPs to be routed through the most favourable paths and to get preferential treatment. Several criteria are used for LSP preemption and these include [20]:

  (i) Preempt LSPs with the least priority.
  (ii) Preempt the least number of LSPs.
  (iii) Preempt the least bandwidth that satisfies the request.
  (iv) Preempt LSPs that will minimise the blocking probability.

RSVP was further extended to include fast reroute in RFC 4090 [21]. Fast reroute was discussed in chapter 2. RSVP is a soft state protocol and therefore periodically refreshes its reservations. Admission control is performed to ensure that enough bandwidth is available to meet the requirements of an LSP. If there is insufficient bandwidth the LSP is not set up. RSVP messages are used to signal, maintain and tear down paths. A description of these RSVP messages is given in table 3.1 [22]. The ResvConf message is not used in RSVP-TE.

Table 3.1: RSVP-TE Messages

Message Type	Description/Purpose
Path	Used for path setup and reservation setup
Resv	Sent upstream in response to path messages to setup path and reservations
ResvConf	Sent in response to resv or resvtear to confirm reservation.
PathTear	Sent downstream and deletes path state
ResvTear	Sent upstream and deletes reservation state
PathErr	Indicates error in path message
ResvErr	Indicates error in resv message
Hello	Detects when neighbor becomes unreachable

3.3.1 RSVP Operation

RSVP sets up and tears down paths and bandwidth reservations in an MPLS network. There are two significant RSVP messages and these are the path and resv messages. RSVP sends periodic path and resv messages to setup and teardown reservations. Path messages are sent downstream from one-hop to another. The path messages store path state as they move from one-hop to the next. The Label Request Object is included in the path message. The Label Request Object indicates that there is a label binding request. When the downstream router receives a path message it performs admission control and checks if the bandwidth requested in the path message is available and passes it to the next hop. The router which is the final destination of the path message sends a Resv message in reply. A label object is included in the Resv message. Resv messages are sent upstream from one-hop to the next thus creating an LSP. Resv messages create and maintain reservation states.

Figure 3.4 shows the RSVP reservation process. The path and resv messages are sent independently from each other. The data flows from receiver to sender are treated independently from receiver to sender.

If a reservation is no longer needed, a teardown message is sent. There are two teardown messages and these are the PathTear and the ResvTear. These teardown messages, delete path state and reservation state in the network. A PathTear message travels downstream towards the receivers deleting path state along the way. A ResvTear message travels upstream toward the senders deleting reservation state along the way.

When an error occurs in the RSVP signaling, error messages are sent. When there is an error in the path message, a PathErr message is sent upstream toward the source of the error. A ResvErr is sent downstream in response to an error in the resv message.

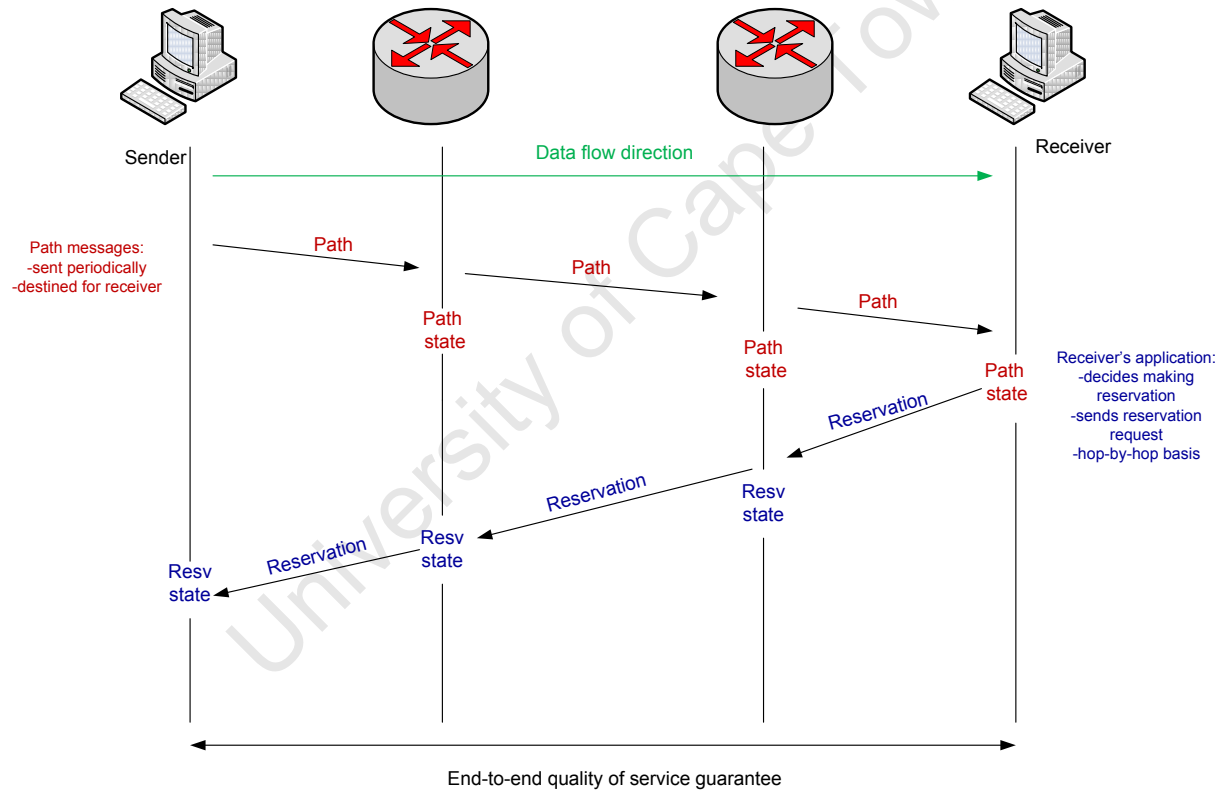

Figure 3.4: RSVP Reservation Process [23]

3.3.2 RSVP Bandwidth Reservation Styles

There are three reservation methods for RSVP and these are discussed in the section that follows [18, 19]:

- **Fixed Filter Style**
  In fixed filter reservation style, each sender reserves bandwidth and this bandwidth is not shared by any other sender. The total bandwidth reserved is the sum of the individual reservations. Each sender is assigned a unique label thereby resulting in a point-to-point LSP.
- **Wildcard Filter**

  In wildcard filter reservation style a single reservation is made by all senders in a session. The bandwidth reserved doesn't change despite the number of senders. A single label is allocated to the senders in a session. This reservation method is suitable for applications that do not all send at the same time. For example, a voice conferencing application, all speakers do not speak at the same. If all senders send at the same time bandwidth reservations are not done well. The reserved bandwidth may be less than what is required closer to the destination and more closer to the senders. Due to this the applicability of Wildcard Filter reservation is restricted for MPLS traffic engineering.

- **Shared Explicit Style**

  Shared explicit reservation method allows a receiver to explicitly specify the senders in a reservation. A single reservation is made for all senders listed. Separate labels are assigned to senders since each sender is explicitly listed in the resv message thereby forming separate LSPs.

3.4 DIFFSERV AWARE MPLS TRAFFIC ENGINEERING (DS-TE)

Diffserv Aware MPLS Traffic Engineering (DS-TE) [24] makes MPLS aware of class of service thereby allowing resource reservation on a per class basis and providing the fault tolerance properties of MPLS. By combining the functionalities of Diffserv and MPLS-TE, network operators can provide services that require strict QoS guarantees like voice while optimizing network resources. DS-TE therefore helps in achieving the objectives mentioned in the section that follows [24]:

- Limiting particular proportion of traffic on a link.
  This helps to ensure that available resources can cater for a particular type of traffic.
- Maintaining relative proportions of traffic on links.
  Proportions of each class type can be set, queue sizes allocated and scheduling policies applied. Traffic engineering can be applied to ensure that traffic complies with available resources. Therefore bandwidth constraints can be applied to different traffic classes.
- Providing guaranteed bandwidth services.
  The aim is to provide the required service level to guaranteed traffic and traffic engineer the best effort traffic.

DS-TE provides resource reservation on a class basis hence available bandwidth for each traffic class can be tracked at each router. In order to track the available bandwidth, a class type CT has been defined by IETF. Eight class types, CT0 to CT7 have been defined and assigned priority of 0 to 7. The combination of the class type and the priority level defines a TE-Class. 8 TE-classes, TE0 to TE7 are defined. CT0 is conventionally mapped to best effort traffic

CSPF takes into account the bandwidth of a class type and the priority and uses this as a constraint during path calculation. The information on the available bandwidth for the different TE classes is carried using the Interior gateway protocol (IGP). After path calculation and signaling, admission control and bandwidth accounting are performed at each hop.

3.5 Bandwidth Constraint Models

Bandwidth constraint models play an important role in determining how bandwidth is allocated to the different classes of traffic. A bandwidth constraint (BC) is the amount of bandwidth that a class type or a group of class types is allocated. The bandwidth constraint model defines the relationship between the class types and the bandwidth constraints. IETF defines three Bandwidth Constraints Models (BCMs) for DS-TE. These are discussed in the next section:

3.5.1 Russian Dolls Model (RDM)

RDM [25] improves bandwidth efficiency over Maximum Allocation Model (MAM) by allowing bandwidth sharing among the class types. CT7 is the class type with the highest priority and CT0 is the best effort traffic. RDM does not provide isolation among the class types hence preemption must be used in order to isolate the class types. Figure 3.5 depicts how RDM works. For simplicity three class types are shown. All LSPs from CT2 use no more than BC2. All LSPs from CT2 and CT1 use no more than BC1. All LSPs from CT2, CT1 and CT0 use no more than BC0.

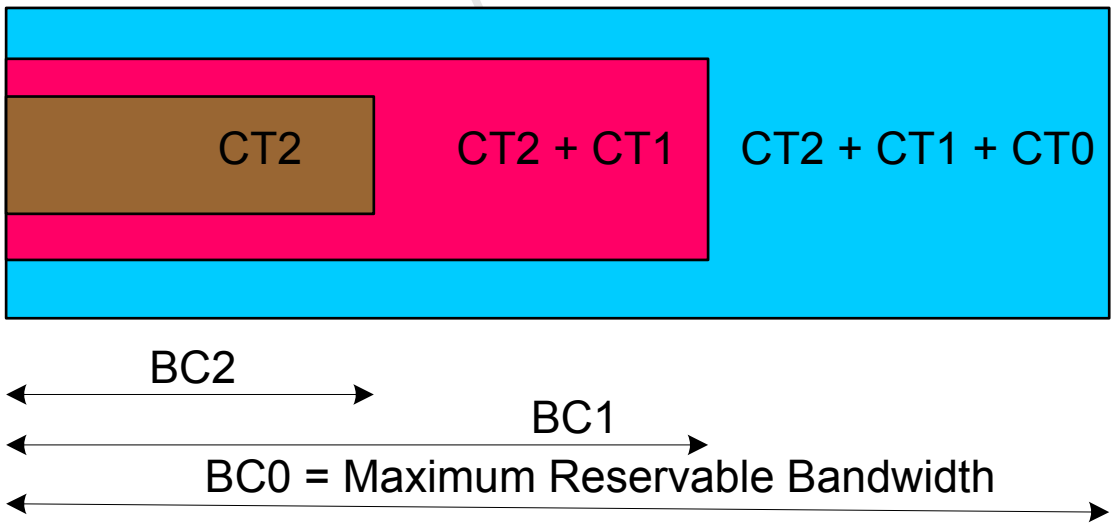

Figure 3.5: RDM Bandwidth Allocation

The total bandwidth reserved by all established LSPs which belong to the class *i* is indicated as R_i

RDM is defined as:

Given *C* Class Types (CTs):

a) Maximum number of BCs is *C*

b) Bandwidth Constraints:

$$\sum_{j=i}^{C-1} R_j \leq BC_i \quad , \forall i \in \{0,1,2,...,C-1\}$$

c) $BC_0 = M$, where M is the maximum reservable bandwidth, therefore the following constraint must be satisfied:

$$\sum_{i=0}^{C-1} R_i \leq M$$

3.5.2 Maximum Allocation Model (MAM)

MAM [26] maps one bandwidth constraint to one class type. The link bandwidth is simply divided among class types. The benefit of MAM is that it provides isolation among the different class types. Priorities therefore do not matter among the LSPs carrying traffic from different class types. The disadvantage of MAM is that it wastes bandwidth as it does not allow sharing of unused bandwidth between class types. Figure 3.6 depicts how MAM works. For simplicity, three class types have are shown.

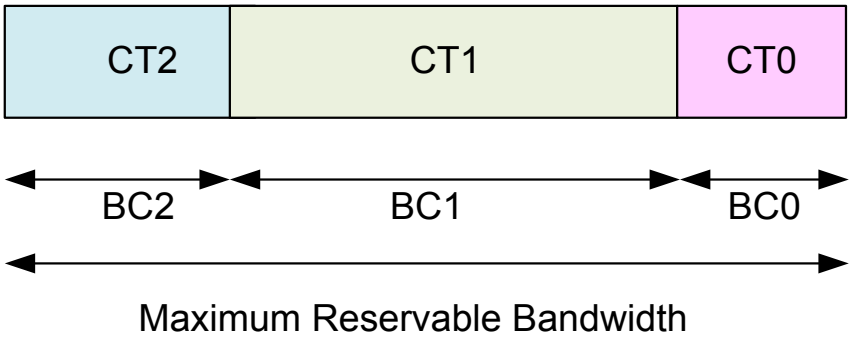

Figure 3.6: MAM Bandwidth Allocation

The total bandwidth reserved by all established LSPs which belong to the class *i* is indicated as R_i.

MAM is defined as:

Given C Class Types (CTs):

a) Maximum number of BCs is *C*

b) $\forall i \in \{0,1,2,...,C-1\}$,

$R_i \leq BC_i \leq M$, where M is the maximum reservable bandwidth.

c) Maximum amount of bandwidth reserved on a link can not exceed *M*

$$\sum_{i=0}^{C-1} R_i \leq M$$

d) To increase bandwidth sharing among CTs, the sum of BCs may exceed *M* therefore:

$$\sum_{i=0}^{C-1} R_i \geq M$$

3.6 Maximum Allocation with Reservation

MAR [27] is similar to MAM except that class types are allowed to exceed their allocated bandwidth in no congestion conditions and revert to their allocations when congestion and overload occur.

An evaluation of the performance of MAM and RDM [28] showed that RDM gives better results for one-way delay and jitter for QoS guarantees. This is mainly due to the bandwidth sharing mechanism of RDM which allows low priority traffic classes to consume unused bandwidth of high priority traffic classes.

RDM is a simple algorithm that doesn't require much processing capability and can be executed in a short time. Therefore RDM is suitable to be used for bandwidth management for real-time applications.

3.7 Current Approaches to MPLS Recovery

MPLS recovery has generated much research due to the failures that communication networks continue to experience and the need to guarantee service protection. This section explores the current research trends and various methods that have been proposed for MPLS recovery

Two schemes that have been developed for MPLS recovery are Haskin [29] and Makam [30]. Haskin combines global repair and local repair. The backup paths are pre-established hence reduces packet loss as it can switch paths quickly, however, the path switching causes packet reordering. It also has high transmission delay due to a longer recovery path. Makam is a global repair scheme and the backup paths are also pre-established. This scheme has higher packet loss as the FIS has to propagate to the ingress for the path switching to occur, however, there is no packet reordering.

Lin et al [31] proposed a scheme based on Haskin and fast reroute. It therefore utilizes RSVP-TE since fast reroute is based on RSVP-TE. The scheme assigns a value called minimum hop to each LSP and a value called decision threshold to classify the LSPs into two categories. If the minimum hop of an LSR is less than or equal to the decision threshold then the LSR applies Haskin scheme if it or its downstream link fails. If the minimum hop of an LSR is greater than

the decision threshold then fast reroute is applied. The performance of the NHF scheme was compared with Haskin and fast reroute in NS2 using end-to-end delay and throughput. The results showed that the NHF scheme was more efficient.

In [32] a recovery mechanism based on the reverse backup path was developed. A comparison of their mechanism with two recovery models, Haskin and Makam showed that it performed better in terms of packet loss and delay.

Hayasaka et al [33] developed a path protection recovery mechanism to guarantee protection of real-time traffic using forward error correction (FEC). FEC is the sending of extra or redundant packets so that lost packets can be recovered using the redundant data. During rerouting of traffic after the occurrence of a failure, some packet loss is experienced. Therefore FEC is used to recover the lost packets due to rerouting of traffic after a failure occurs. The scheme was developed to provide approximately 100% availability for real time traffic. The performance of the scheme was evaluated using the effective packet loss ratio and the occupancy ratio of the FEC traffic. The effective loss ratio is the ratio of the lost packets not recovered even after the use of FEC.

Francisco et al [34] proposed a local protection scheme that utilises dynamic alternative routing. Dynamic alternative routing improves network performance and survivability through rerouting of traffic during periods of congestion. The study was aimed at increasing network performance when a link failure occurs without increasing the protection bandwidth.

El Shazely et al [35] developed schemes based on P-cycles to enhance failure recovery. P-cycles seek to benefit from the merits of ring and mesh based recovery. Ring based recovery is very fast due to its local protection nature. Mesh based recovery provides simple and efficient capacity due to its high level sharing. They proposed 3 p-cycle models namely, capacity planning model, hop limit model and the Hamiltonian p-cycle model. The capacity planning model provides bandwidth guaranteed restoration. Hop limit is needed for the recovery path when there is load balancing in the network. Hamiltonian cycle is when a p-cycle traverses every node once. It helps to provide redundancy. These models are suitable for networks with traffic that is sensitive to packet loss.

In [36] two fast reroute mechanisms, IP fast reroute and MPLS fast reroute were investigated and evaluated. The study was done on a test bed containing Nortel and Juniper routers. The study was aimed at observing the packet loss and convergence time after the occurrence of a failure. The study also investigated the effect of increasing the number of LSPs and prefixes on the packet loss and convergent time in MPLS fast reroute and IP fast reroute respectively. For MPLS fast reroute, it was shown that increasing the number of LSPs increases the convergence time and packet loss. This is due to the extra processing and signaling required by the ingress and the PLR. For IP fast reroute, increasing the prefixes had no effect on the packet loss and the convergence time increases non-linearly.

Among the aspects that MPLS recovery focuses on is reducing the bandwidth reserved for protection. Alicherry et al [37] investigated the problem of determining the least bandwidth to reserve for protection to guarantee fast restoration from link failures. They developed approximate time algorithms whose solution output reserves not more than twice the protection bandwidth reserved by any optimal solution. Wang et al [17] developed a bandwidth management scheme for sharing bandwidth among different service LSPs in one-to-one backup. The scheme was aimed at ensuring that the reserve bandwidth is not more than what is required. This was an extension of RFC 4090 where path merging was used to share bandwidth on common backup paths of the same service LSP. The scheme also includes an algorithm for selecting backup paths that maximize the sharing of bandwidth. In [9] the work of Wang et al was extended by proposing extensions to RSVP-TE signaling and adding functionality to nodes on the backup paths, thereby achieving bandwidth sharing. In [38] first polynomial time algorithms were developed for maximizing throughput for fast restoration. In [39], it was shown that where link capacities are known in advance and the goal is to maximize revenue, local protection should be the recovery scheme of choice because it achieves fast restoration.

MPLS recovery schemes also seek to calculate or compute paths that will achieve efficient bandwidth utilisation. In [40] an integer linear program was used to calculate paths for both global repair and local repair that achieve fast recovery and bandwidth efficiency. The goal was to have path calculation done in a way that minimizes bandwidth consumption and achieves fast restoration. The work considered selecting working and recovery paths that meet the following constraints:

- **Capacity**

  The link capacity must not exceed the total bandwidth required on the links.

- **Protection**

  A working path must be protected by one recovery path or a set of detour paths.

- **Recovery Time**

  The recovery time should be similar to that obtained in Synchronous Optical Network (SONET)/Synchronous Digital Hierarchy (SDH) networks, that is, 50ms.

The solution incorporated bandwidth sharing to achieve efficient bandwidth allocation. In [41] pre-computation of paths that would avoid congestion was investigated. The study also proposed reducing the length of the tunnel lengths to avoid delays and the complexity added to the management of the network. Mathematical models and algorithms on how to minimize the length of pre-computed backup tunnels with reserved bandwidth to reduce chances of congestion during failure conditions were proposed. This concept was applied in [42] where dimensioning was used to determine the backup capacity for protection in facility backup and one-to-one backup. The link capacity required for protection was determined and used to calculate the overall bandwidth required for network resilience. Given a network topology represented by the graph N = (V, E), where V is the set of routers and E the set of links, the degree of protection *B*, is given by:

$$B = \frac{C_s - C_t}{C_t}, \text{ where}$$

C_t is the total network capacity in a protected network for a failure free scenario, *t*.

C_s is the total network capacity in a protected network for a failure scenario, *s*.

.

MPLS recovery is also aimed at guaranteeing QoS protection. In [43] a QoS protection scheme that combines MPLS protection with Diffserv was proposed. Four parameters were combined to form a single metric and weights added to the Diffserv classes. The parameters considered were packet loss, restoration time, resource consumption and link probability. The results showed that the proposed scheme provided better QoS protection compared to the conventional protection methods. In [44] a traffic splitter that redirects traffic onto several backup paths was proposed. The parameters that were used for path selection were bandwidth and end-to-end delay. The scheme increased the reliability and availability of the network thus reducing the recovery time and packet loss.

From the current trends of research on MPLS recovery much of the study is aimed at ensuring that the bandwidth is utilized efficiently and that fast restoration is guaranteed by having shorter recovery times. Some bandwidth allocation algorithms that have been developed are complex and may take long to run as they need more processing. These algorithms may not be ideal for ensuring real-time protection due to the time constraint involved. In [45] the preemption policy was identified as an important factor in the bandwidth reservation and management problem.

This research therefore incorporates preemption and RDM in fast reroute as a solution to guarantee real-time protection of voice traffic. Preemption has been selected because it makes bandwidth available to higher priority LSPs when there is insufficient bandwidth in the network. Since the research focuses on providing real-time protection for voice, preemption will help to make the bandwidth required by voice traffic available. Preemption also provides isolation to the class types when using RDM thus guaranteeing bandwidth to a particular class type. RDM has been selected because it allows for bandwidth sharing when a class type is not using its reserved bandwidth thus achieving efficient bandwidth usage.

3.8 CHAPTER SUMMARY

Resource Reservation Protocol (RSVP) and Diffserv-aware MPLS Traffic Engineering (DS-TE) play a vital role in bandwidth management in MPLS. RSVP is used as a signaling protocol for path setup and bandwidth reservation in MPLS. DS-TE provides QoS and bandwidth guarantees through the use of bandwidth constraint models. The Russian dolls bandwidth constraint model allows for efficient use of bandwidth through bandwidth sharing.

Preemption helps to guarantee bandwidth to higher priority LSPs when there is insufficient bandwidth. It also ensures that high priority LSPs use the most favourable paths in the network. Current approaches to MPLS are aimed at ensuring fast restoration from failure and efficient bandwidth utilisation.

In the next chapter, the proposed solution which incorporates fast reroute, LSP preemption and bandwidth encapsulation or allocation with the Russian dolls model is presented and tested by simulation.

4. SIMULATION SCENARIOS IMPLEMENTATION IN OPNET

4.1 INTRODUCTION

In chapter 3, bandwidth management with regard to RSVP and the Russian dolls bandwidth constraint model was discussed. This chapter looks at the proposed real-time bandwidth encapsulation mechanism to guarantee real-time protection of voice traffic and its implementation in OPNET modeler. The solution utilises fast reroute, RSVP, Russian dolls bandwidth constraint model and LSP preemption.

The chapter begins by discussing the proposed real-time bandwidth encapsulation mechanism in section 4.1. It then proceeds to describe the setup of the system model in section 4.2. Finally the scenarios that were simulated in the research and their setup are described in section 4.3. The objectives of this chapter are therefore to:

- Validate by simulation how the proposed real-time bandwidth encapsulation mechanism guarantees protection to voice traffic.
- Explain the procedure followed in ensuring QoP to Voice traffic in an IP/MPLS network.

4.2 PROPOSED REAL-TIME BANDWIDTH ENCAPSULATION MODEL

The novelty of the research is in the proposal of the real-time bandwidth encapsulation with RDM. In previous work RDM has not been evaluated with regard to real-time protection. This section therefore shows the novelty of the research.

In chapter 3, it was discussed that RDM will be used to allocate bandwidth to the class types in the network. RDM provides efficient bandwidth usage through sharing of unused bandwidth. In this research this process is known as bandwidth encapsulation. The bandwidth encapsulation process involves the reservation and allocation of bandwidth. RSVP is used to reserve the needed bandwidth. When the required bandwidth is available, allocation is done using RDM. If the required bandwidth is insufficient preemption is used to guarantee that bandwidth. Real-time protection will be provided by ensuring that bandwidth is allocated to voice traffic when a failure

occurs. Since traffic should be recovered within 50 ms for voice calls not to be compromised, the process of confirming the bandwidth reserved, bandwidth allocation and switching of voice traffic are expected to be done within 50ms.

In order for a protection scheme to achieve real-time protection some functional requirements are necessary. These are discussed below [46]:

- Protection bandwidth should be reserved on each link. This bandwidth must not be allocated to the working LSPs.
- Failures should be detected by the ingress node or PLR.
- Bandwidth allocation should be done at the time of failure.
- Traffic should be switched from the failed LSP to the protection LSP.
- Recovery should be within bounded time constraints.

4.2.1 Real-Time Bandwidth Allocation

The flow chart in Figure 4.1 shows the proposed protection mechanism operation in order to achieve real-time bandwidth allocation. The steps in this mechanism are discussed below:

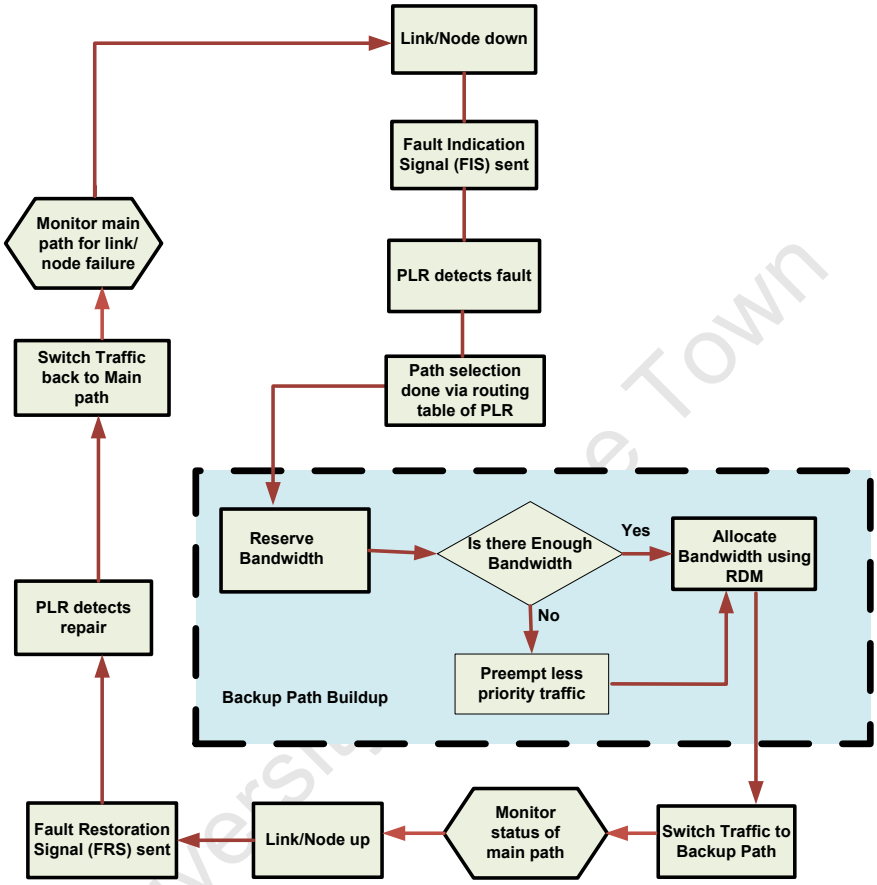

Figure 4.1: Real-Time Bandwidth Encapsulation Flow Chart

1. **Monitor Main Path for Link/Node Failure**

   This stage represents the monitoring of the main or primary path for the occurrence of a failure. The main path or primary path is monitored so that when a link or node failure occurs, it is quickly detected. This is the normal state that the network operates in.

2. Link/Node Down

This stage represents the occurrence of a link or node failure in the network causing the link or node to be down.

3. Fault Indication Signal (FIS) Sent

When the link or node failure occurs, the neighbouring nodes and the node in charge of rerouting or redirecting traffic to an alternative path must be informed. This is done through the FIS. This stage represents the sending of the FIS to the point of local recovery (PLR) node after the link or node has failed.

4. PLR Detects Fault

This stage represents the receiving of the FIS by the PLR node. When the PLR node receives the FIS it detects the fault that has occurred in the network.

5. Path Selection Done Via Routing Table of PLR.

This stage represents the selection of a backup path after the occurrence of a link or node failure. This takes place after the fault has been detected by the PLR node. The PLR has a routing table that contains routes to other nodes in the network. The backup path that will be used after failure is an explicit path to the merge point. This is the path that will be used to bypass the failure point on the primary path.

6. Backup Path Buildup

This stage represents the buildup or setup of the selected backup path. A number of steps are involved in the buildup of the backup path and these are discussed next.

(a) Reserve bandwidth

Protection bandwidth is reserved before the occurrence of a failure. The bandwidth required for the setup of the backup path must be available on the selected route for the path to be setup. This stage therefore represents the request for confirmation on the availability of the requested bandwidth.

(b) Is there Enough Bandwidth

This stage checks whether the requested bandwidth is available for allocation. If the requested bandwidth is available then the bandwidth allocation will be done as requested. If there is insufficient bandwidth the allocation of bandwidth cannot be done unless preemption is done.

(c) Preempt Less Priority Traffic

If the requested bandwidth is not available, less priority traffic will be preempted from the path to provide bandwidth for the higher priority traffic. Preempting less priority LSPs frees up bandwidth which can be used by higher priority LSPs.

(d) Allocate Bandwidth using RDM

The allocation of bandwidth is done when there is sufficient bandwidth to allocate to the higher priority protection traffic. The bandwidth constraint model that is used for the allocation of bandwidth is the Russian dolls model. When the bandwidth has been allocated the path is setup along the selected route from the PLR node to the MP node.

7. Switch Traffic to Backup Path

Once the backup path has been setup, traffic is switched or rerouted to the backup path. The traffic is switched to the backup path by the PLR node and rejoins the primary path at the merge point.

8. Monitor Status of Main Path

After the occurrence of a network failure, the primary or main path is monitored to detect the restoration or recovery of the failed network element. The network remains in this state until the failed network element is restored.

9. Link/Node Up

This stage represents the restoration or repair of the link or node that had failed.

10. Fault Restoration Signal (FRS) Sent

When the failed link or node is restored, a fault restoration signal is sent to the neighbouring nodes and the PLR node.

11. PLR Detects Repair

When the FRS is received by the PLR node, it detects that the link or node that had gone down has been repaired.

12. Switch Traffic Back to Main Path

After the failing network element has been repaired and is stable, traffic is switched back to the primary path by the PLR node.
When traffic is switched back to the main path, the network will continue to be monitored for failures.

The research focused on steps (1) through (7) with emphasis on the backup path buildup process which involves bandwidth reservation, preemption and bandwidth allocation with the Russian dolls model. The timing diagram illustrated in Figure 4.2 depicts the backup path buildup process and traffic switching. The whole process must be completed within 50ms

When the PLR has detected the fault through the FIS, a number of steps take place to begin the buildup of the backup path:

- A path message indicating how much bandwidth is required is sent along the path to be built. It is sent from one hop to the next until it reaches the last router in the path which is the merge point.
- A reservation (resv) message is sent in response to the path message to reserve the requested bandwidth.
- A reservation confirmation message (for RSVP) is sent to confirm the bandwidth reservation.

The bandwidth reservation process is complete by the confirmation of the reservation message. This process from the detection of the fault to the reservation of the bandwidth can take up to 10ms. It has been assumed that the signaling processes involved should be completed within 10ms. Therefore the value of 10ms is part of the research hypothesis that the signaling processes involved during this stage should be completed within 10ms.

Once the bandwidth reservation is confirmed, bandwidth is allocated to the LSPs according to the Russian dolls model (RDM). This can take up to 25ms. It has been assumed that the bandwidth allocation process can take up to 25ms. This is due to the processing involved in allocating bandwidth to the class types in the network. Therefore the value of 25ms is part of the research hypothesis that the bandwidth allocation process with RDM can take up to 25ms.

Once the bandwidth has been allocated traffic is rerouted to the backup path since the backup path has been built and the required bandwidth has been allocated. The traffic reroute time or protection switching time can take up to 15ms. It has been assumed that this process can take up to 15ms due to the traffic rerouting process .Therefore the value of 15ms is part of the research hypothesis that the protection switching or rerouting time can take up to 15ms.The total time is 50ms due to the real-time nature of voice traffic.

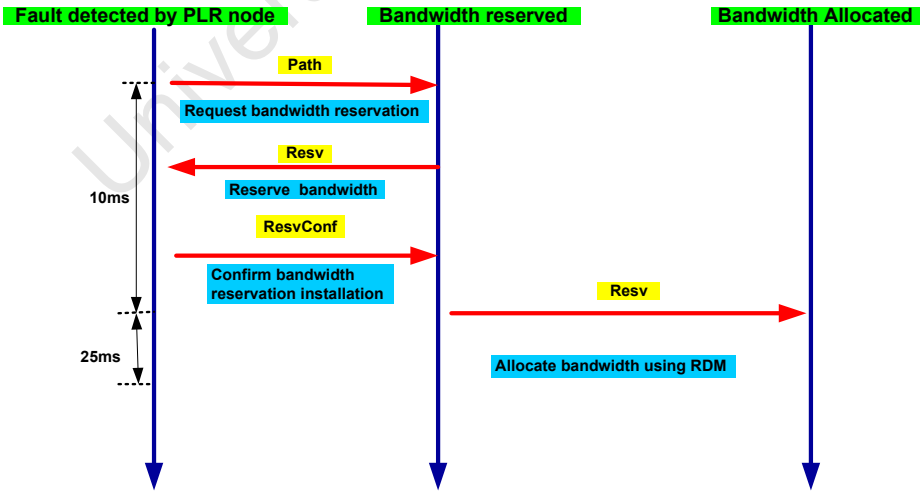

Figure 4.2: Real-Time Bandwidth Encapsulation Timing Diagram

4.3 SYSTEM MODEL

The simulations were done in OPNET Modeler 14.0 simulation software. OPNET Modeler is a discrete event simulator for research and development. It aids in the design and analysis of communication networks, protocols and applications.

The objective of the system model was to simulate an IP/MPLS network that would allow for the investigation of single link and node failures and guarantee QoP to voice traffic. The topology was selected to allow multiple paths for failing elements. The system model consists of 14 MPLS enabled routers, 4 source nodes and 4 destination nodes. The LER A is the ingress router while the LER G is the egress router. The Interior gateway protocol (IGP) configured on the routers is single area Open shortest path first (OSPF). Loopback interfaces were configured on each router. The links between the routers are E3 links (34.368 Mbps). The E3 links were selected to ensure that there was no congestion that would lead to failures due to bottlenecks in the network. The failures considered were those caused by failing elements in the network, that is, a link or a node. The source and destination nodes are connected to the routers by T1 (1.544Mbps) links except for the video source and destination nodes which are linked by an E3 link. All nodes have been assigned class C IPv4 addresses. The system model is illustrated in Figure 4.1.

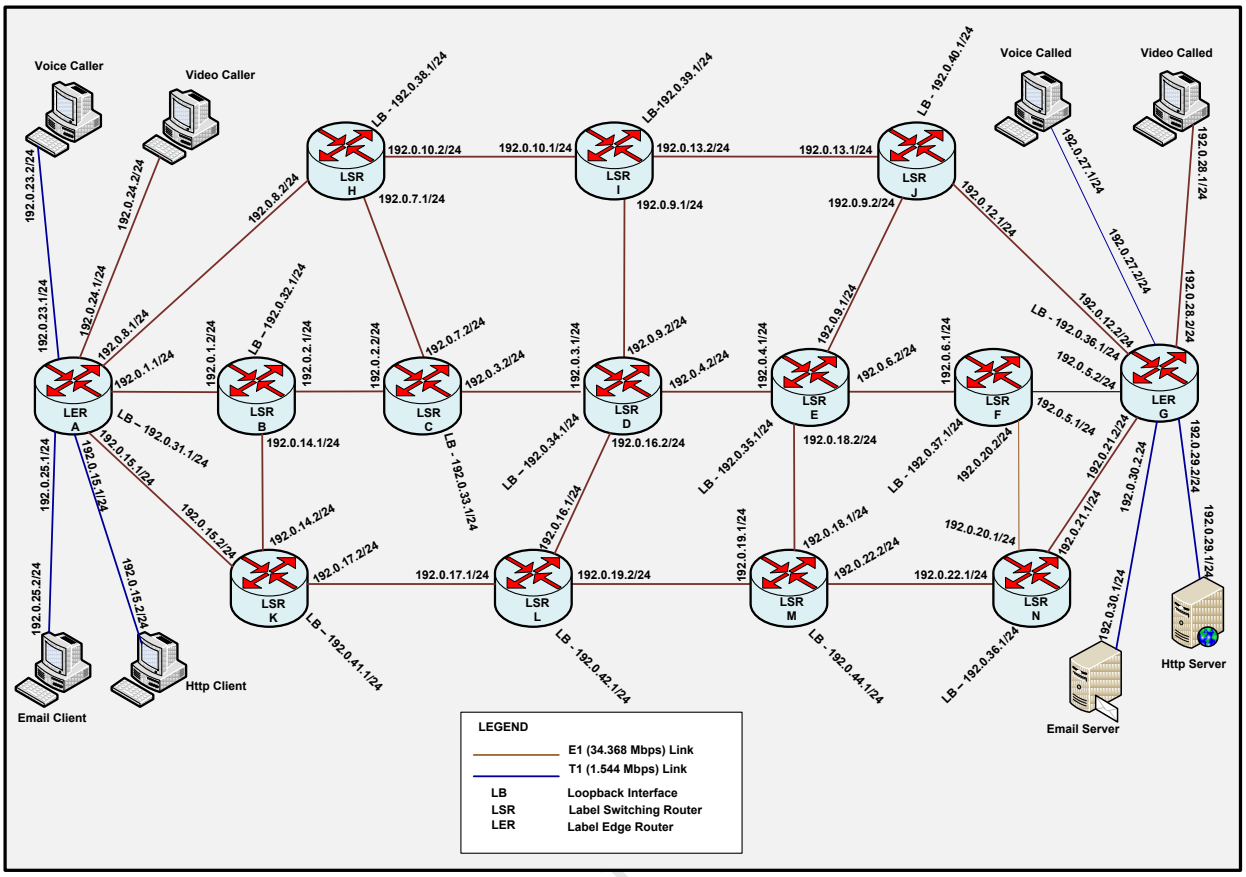

Figure 4.3: System Model

4.3.1 Applications Configuration

Four applications were deployed in the network namely voice, video conferencing, email and HTTP. Each node was running one application and communicating with a corresponding node as depicted in the Figure 4.4.The applications were defined in the application config object. The applications were configured with the attributes described in Table 4.1. The numbers in parenthesis in Table 4.1 represent priority. An application with 0 as the priority has the least priority and an application with 7 as the priority has the highest priority.

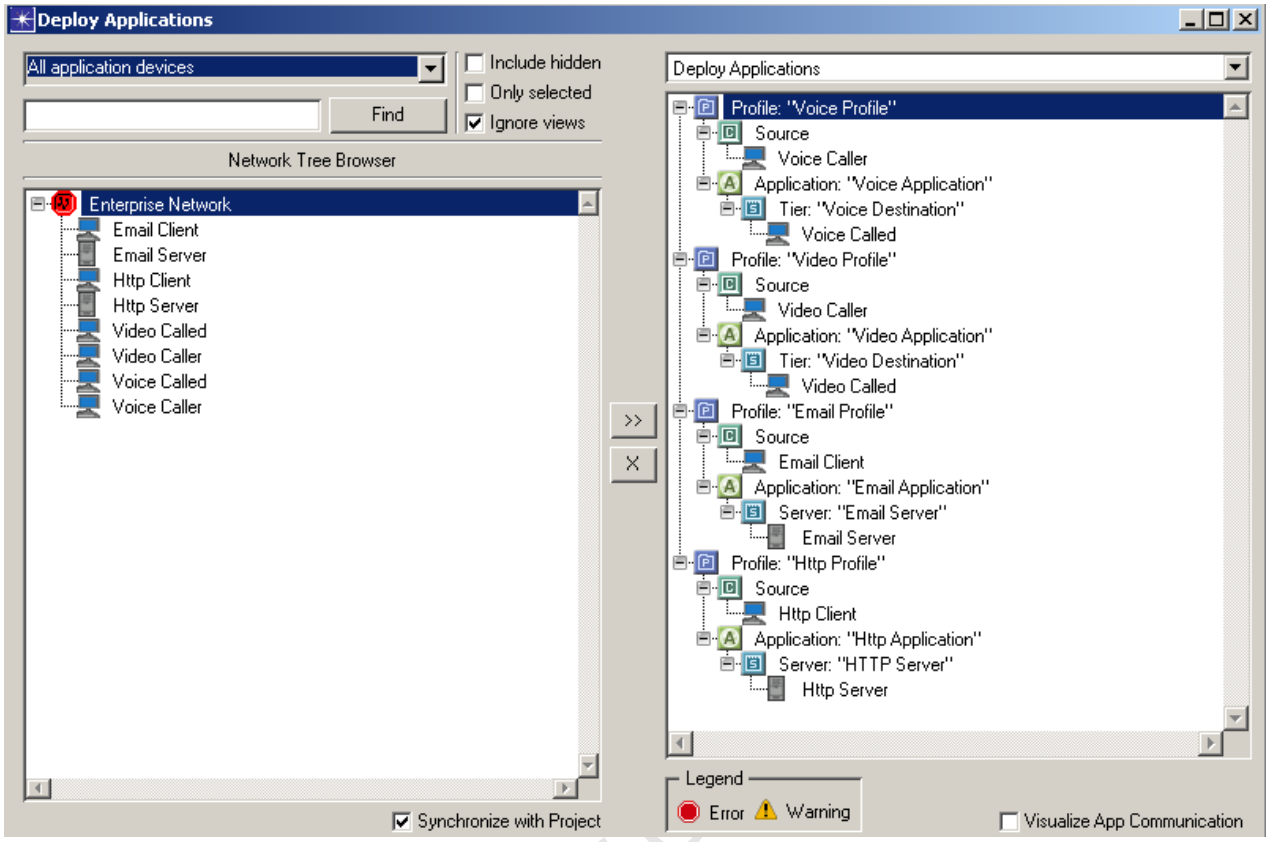

Figure 4.4: Deployed Applications

Table 4.1: Configured Applications

Application Type	Application Attributes
Voice Application	• PCM quality speech • G711 encoding scheme • 64Kbps coding rate • Type of service (ToS) – Interactive voice (6)
Video Application	• Low resolution video • 10 frames/sec • 128 x 120 pixels • ToS – streaming multimedia (4)
Email Application	• High load • 20,000 bytes email size • ToS – Best effort (0)
HTTP Application	• Heavy browsing • 10,000 bytes page size • ToS – Best effort (0)

4.3.2 Application Profiles

Application profiles describe the activity pattern of applications configured in the network. They specify the start time of each application, the duration each application is used and the frequency of use. Four application profiles namely voice profile, video profile, email profile and HTTP profile were configured as shown in the Profiles Configuration Table in Figure 4.5. Each profile was mapped to a corresponding application in the Profile Configuration Table.

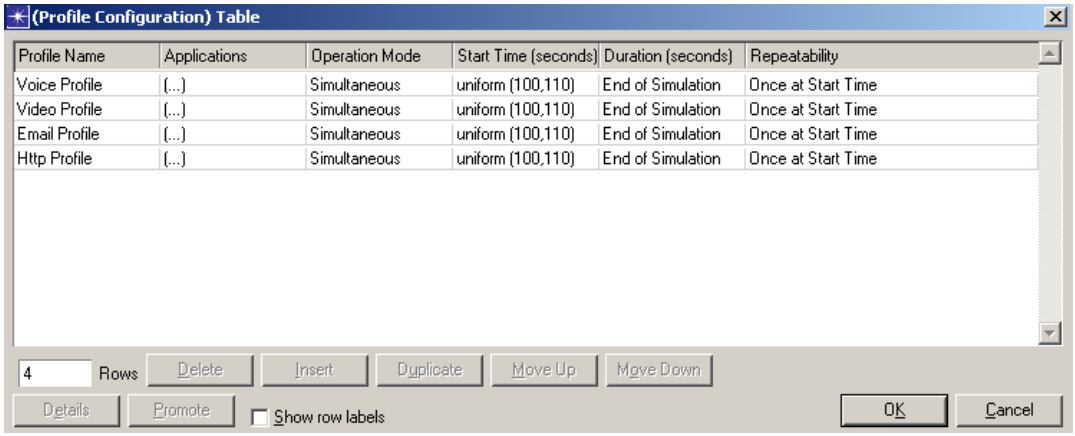

Figure 4.5: Configured Application Profiles

4.4 MPLS Configuration

The MPLS configuration involved configuring the forward equivalence classes (FECs), the traffic trunks, the LSPs and specifying the interfaces through which the traffic enters the ingress router. In order to send traffic through an LSP, traffic mappings are required. Traffic mappings associate traffic with a particular LSP. Static mappings were used to associate traffic with the LSPs. To configure static mappings, FECs and traffic trunks must be configured. The FEC specifications and the traffic trunk profiles were defined in the MPLS config object.

4.4.1 Forward Equivalence Classes (FECs)

Four FECs were configured with the attributes shown in Table 4.2.

Table 4.2: Configured Forward Equivalence Classes

FEC Type	ToS	Transport Protocol	Source	Destination
Voice FEC	Interactive voice (6)	UDP	Voice caller 192.0.19.1	Voice called 192.0.21.1
Video FEC	Streaming multimedia (4)	UDP	Video caller 192.0.20.1	Video called 192.0.22.1
Email FEC	Best effort (0)	TCP	Email client 192.0.23.1	Email server 192.0.25.1
HTTP server	Best effort (0)	TCP	HTTP client 192.0.24.1	HTTP server 192.0.26.1

4.4.2 Traffic Trunk Profiles

Traffic trunks are aggregates of flows belonging to the same class sharing a common QoS requirement placed inside an LSP. Four traffic trunks corresponding to the four FECs were configured. These traffic trunks were configured as follows:

- A voice trunk with Expedited forwarding (EF) as the traffic class,
- Video trunk with Assured Forwarding (AF) 13 as the traffic class,
- Email trunk and HTTP trunk both with Assured Forwarding (AF) 23 as the traffic class.

The traffic profiles were also specified. The traffic profile characterise the traffic flow. The traffic profiles were specified as follows:

- The voice trunk with a traffic profile of 64 Kbps
- The video trunk with a traffic profile of 1.4 Mbps
- The email trunk with a traffic profile of 160,000 bps
- The HTTP trunk with a traffic profile of 80,000 bps

The traffic trunks were configured to remark and transmit packets that violate the traffic profile.

4.4.3 Label Switched Paths (LSPs)

Four LSPs using Resource Reservation protocol (RSVP) as the signaling protocol were configured. The LSPs were configured from the ingress router A to the egress router G. Label switching information was configured by updating the LSP details from the protocols > MPLS menu. The FECs and traffic trunks were mapped on to the corresponding LSPs. The traffic mapping configuration was done on the ingress router A, from the MPLS > MPLS Parameters > Traffic Mapping Configuration menu in Figure 4.6. Each LSP was mapped to its corresponding FEC and traffic trunk and the interface through which traffic enters the LSP was specified.

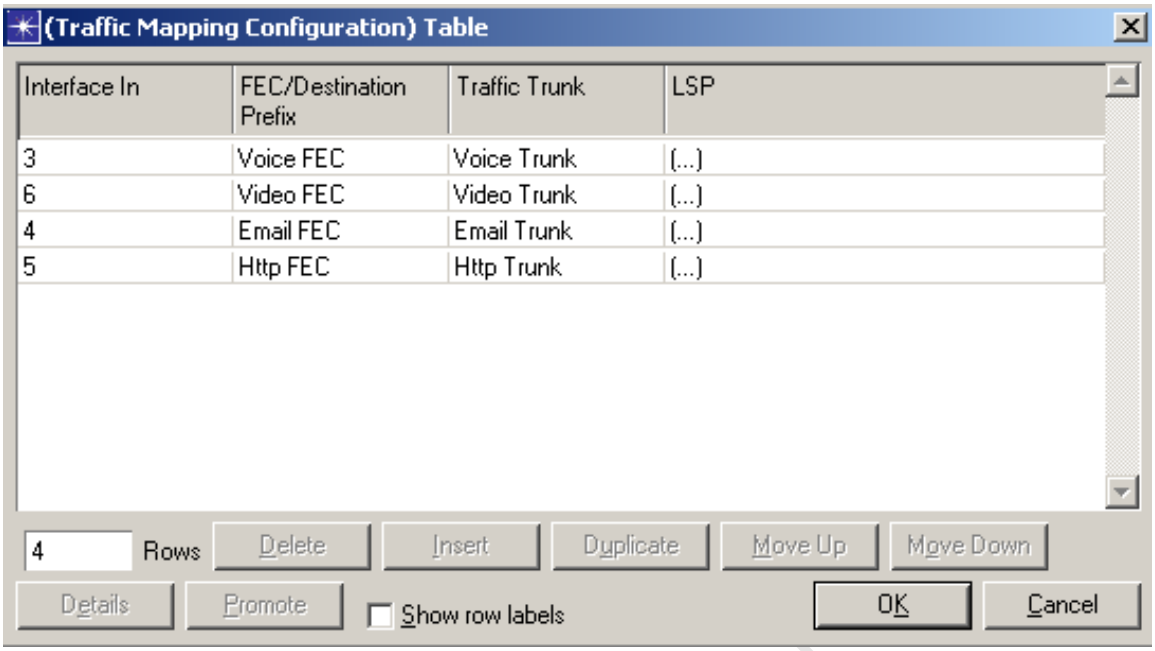

Figure 4.6: Traffic Mapping Configuration

The LSPS configured were:

- Voice LSP with setup and holding priorities of 0. The voice FEC and voice trunk were mapped on to the voice LSP.
- Video LSP with setup and holding priorities of 4. The video FEC and video trunk were mapped on to the video LSP.
- Email LSP with setup and holding priorities of 7. The email FEC and email trunk were mapped on to the email LSP.
- HTTP LSP with setup and holding priorities of 7. The HTTP FEC and HTTP trunk were mapped onto the HTTP LSP.

4.5 SCENARIOS SIMULATED

Several scenarios were simulated in order to achieve the objectives of this research. These scenarios are described in the section that follows:

4.5.1 QoP of Path Protection and Fast Reroute

An investigation of the QoP provided by the two protection switching methods, path protection and fast reroute was done. The investigation involved a single link failure and a single node failure in the network.

(a) Path Protection Configuration

The video, voice, email and HTTP explicit primary LSPs were configured to be setup at 100 seconds from the ingress router A to the egress router G. The voice LSP had an ingress backup LSP that was configured to be setup at 100s. The video, email and HTTP LSPs were not configured with backup LSPs for protection. A failure occurred on the link C→D at 600s and the link was restored at 1200s.

A second scenario was simulated where the node D failed at 600s and was restored at 1200s. The failure and recovery of link C→D and node D were configured from the failure recovery object as shown in Figure 4.7 and Figure 4.8 respectively. The two scenarios are illustrated in Figure 4.9. The simulation time for both scenarios was 30 minutes.

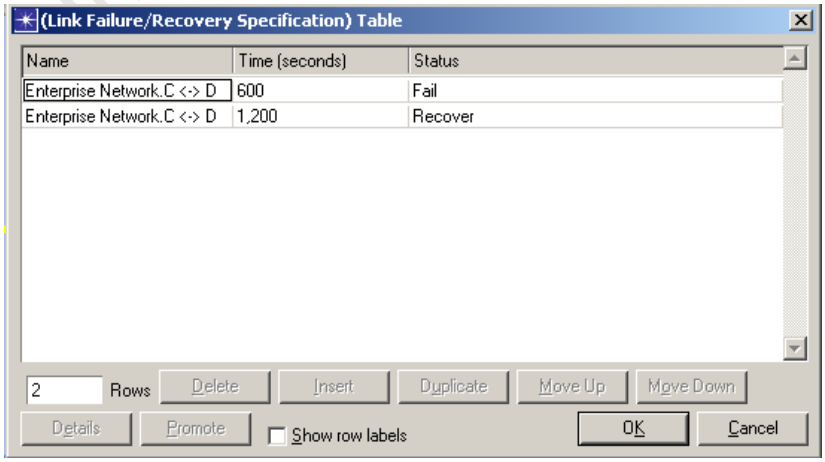

Figure 4.7: Link Failure and Recovery Configuration

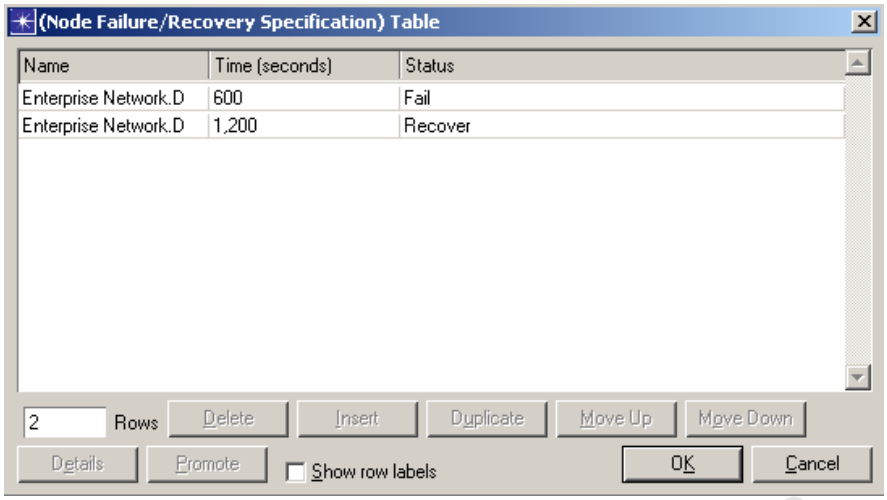

Figure 4.8: Node Failure and Recovery Configuration

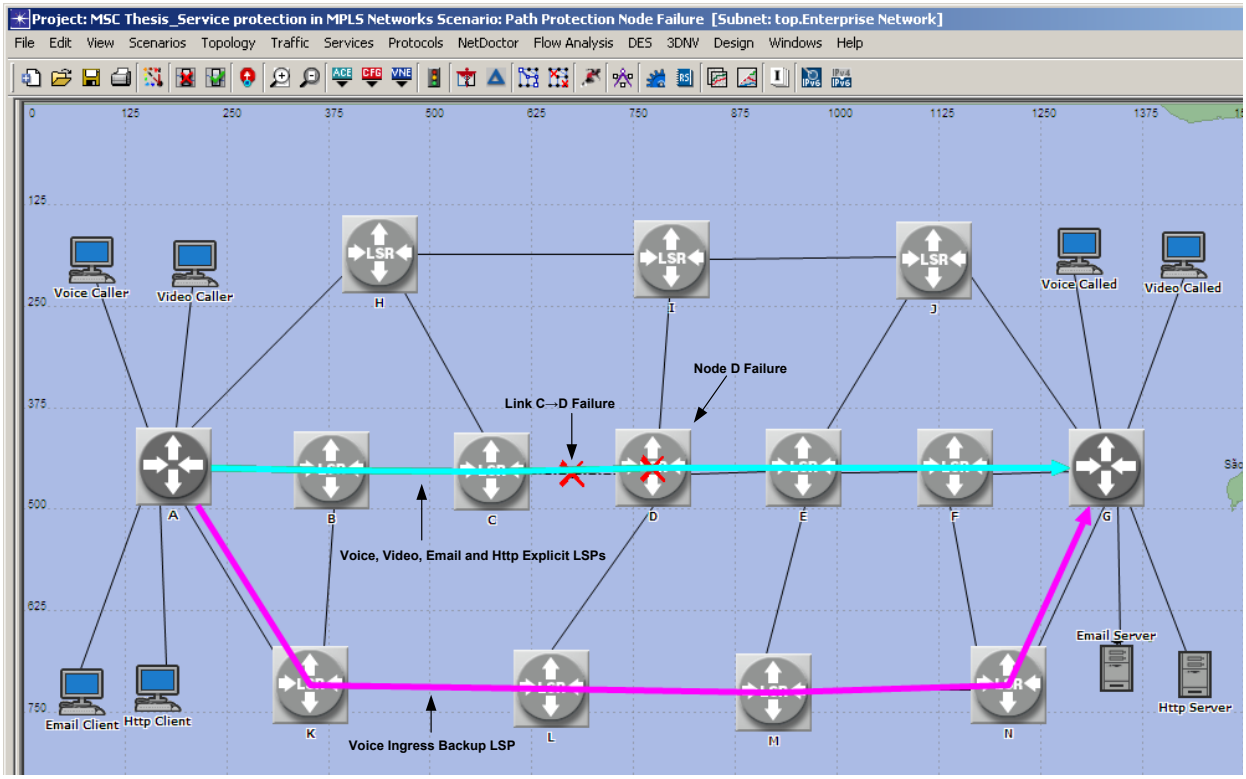

Figure 4.9: Path protection

(b) Fast Reroute Configuration

The voice, video, email and HTTP LSPs were configured to be set up from the ingress router A to the egress router G at 100s just as in the path protection configuration. In the link failure scenario the voice primary LSP was provided with protection by configuring many-to-one protection scheme for link protection. The voice LSP was configured with a bypass tunnel to reroute traffic to in case of failure. Fast reroute configuration for link protection was done on the voice LSP under the recovery parameters as shown in Figure 4.10

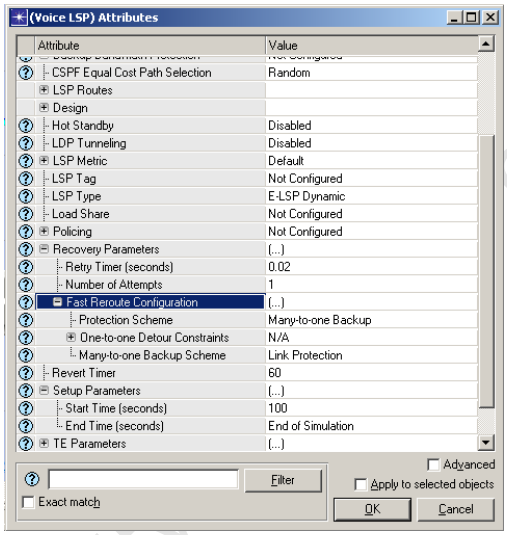

Figure 4.10: Fast Reroute Link Protection Configuration

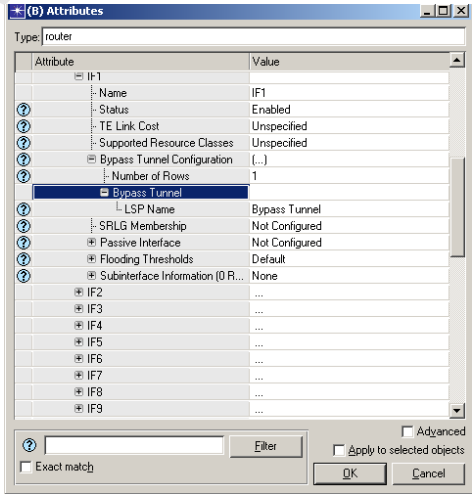

Figure 4.11: Bypass Tunnel Configuration

The bypass tunnel was configured for link protection along the path B→K→L→D. Protection was not provided to the video, email and HTTP LSPs. The bypass tunnel was configured on the outgoing interface of the LSP on router B as shown in Figure 4.11. In this case the outgoing interface of the video and voice LSP was on the interface IF1 with the IP address 192.0.2.1 255.255.255.0. If the bypass tunnel is configured on an interface which is not the outgoing interface of the LSP, the traffic will not be rerouted onto the bypass tunnel. The link C→D failed at 600s and was restored at 1200s. This scenario is illustrated in Figure 4.12.

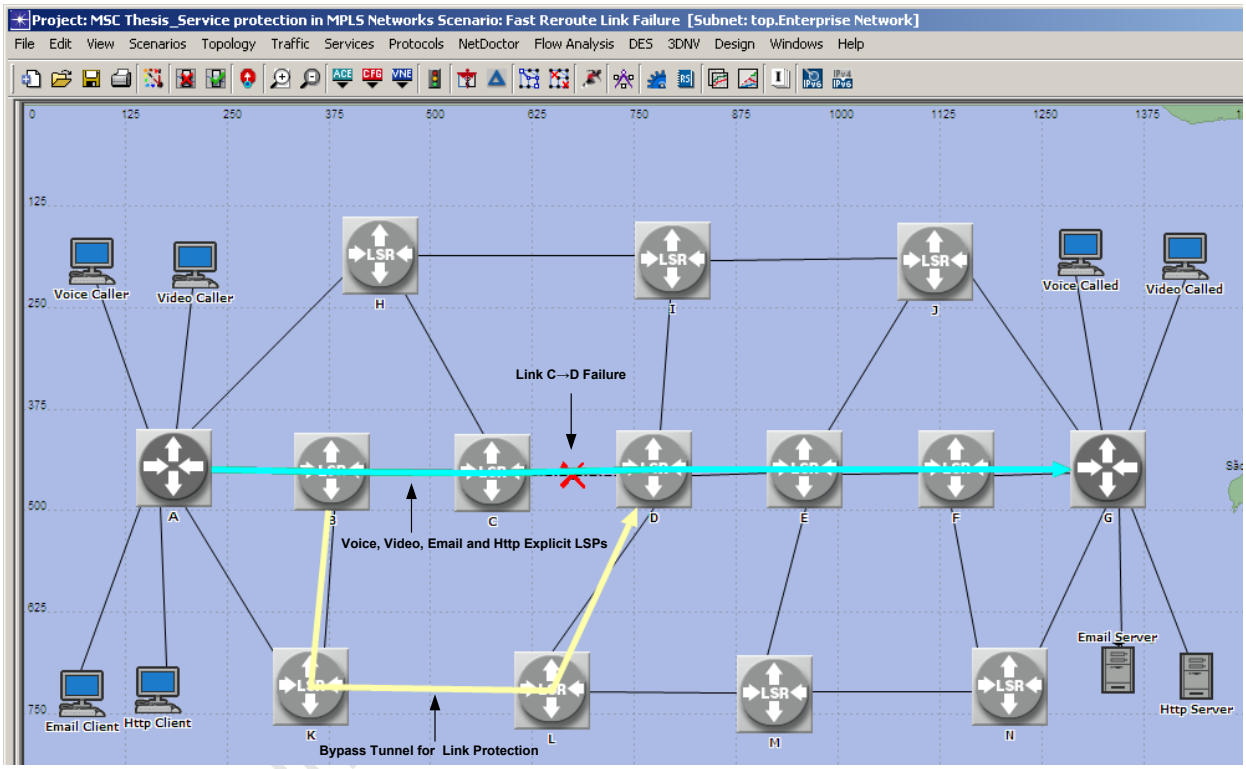

Figure 4.12: Fast Reroute Link protection

In the second scenario, node D failed at 600s and was restored at 1200s. The voice LSP was configured for fast reroute node protection as shown in Figure 4.13. In this case a bypass tunnel was configured for node protection along the path B→K→L→M→E. The bypass tunnel was configured on the outgoing interface of node B. The outgoing interface is IF1 with the IP address 192.0.2.1. This scenario is illustrated in Figure 4.14.The simulation time for both scenarios was 30 minutes.

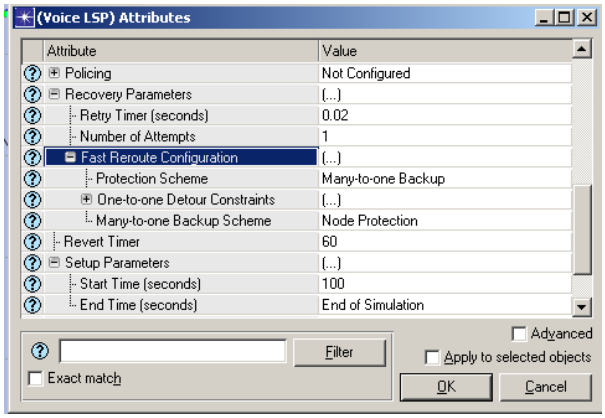

Figure 4.13: Fast Reroute Link Protection Configuration

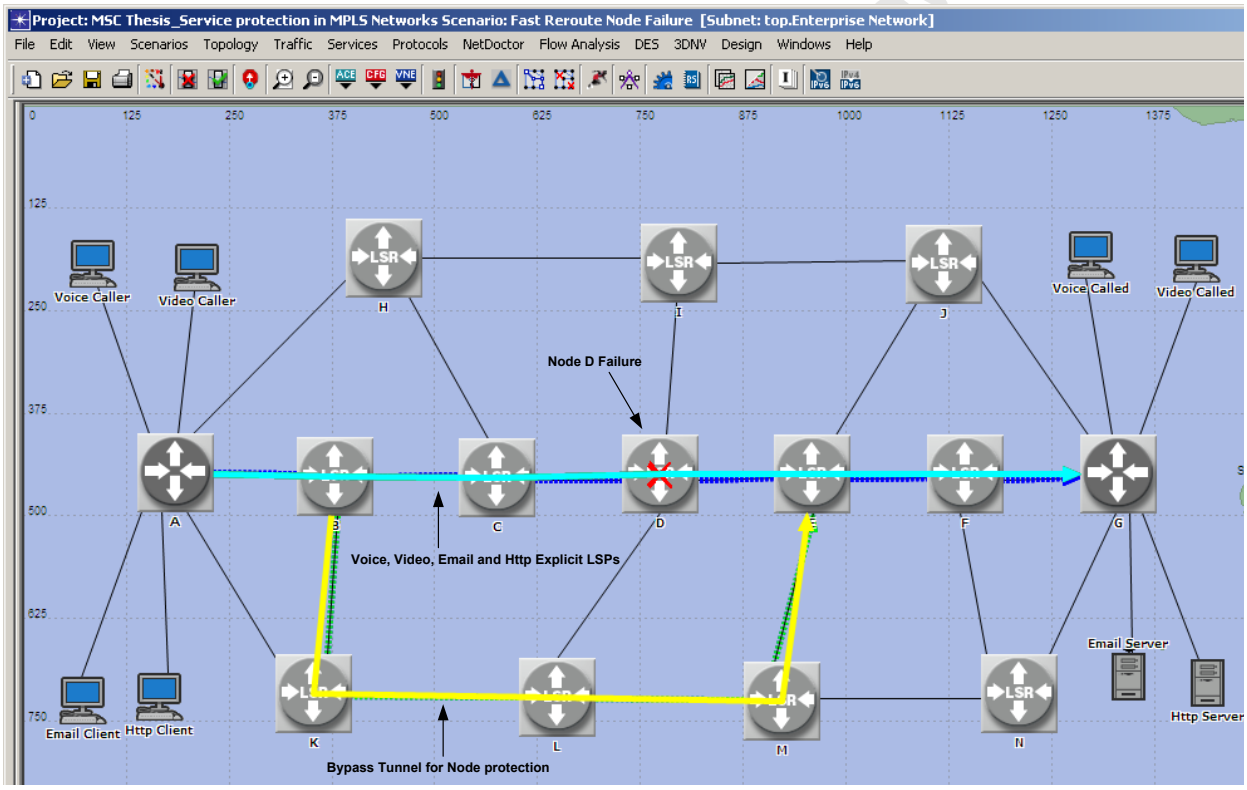

Figure 4.14: Fast Reroute Node Protection

(c) No MPLS Protection Configuration

Two scenarios were simulated with no MPLS protection provided to all the LSPs. The LSPs were configured to be established at 100s. In the first scenario, Link C→D failed at 600s and was restored at 1200s. In the second scenario, node D failed at 600s and was restored at 1200s. These two scenarios are illustrated in Figure 4.15. The simulation time for both scenarios was 30 minutes.

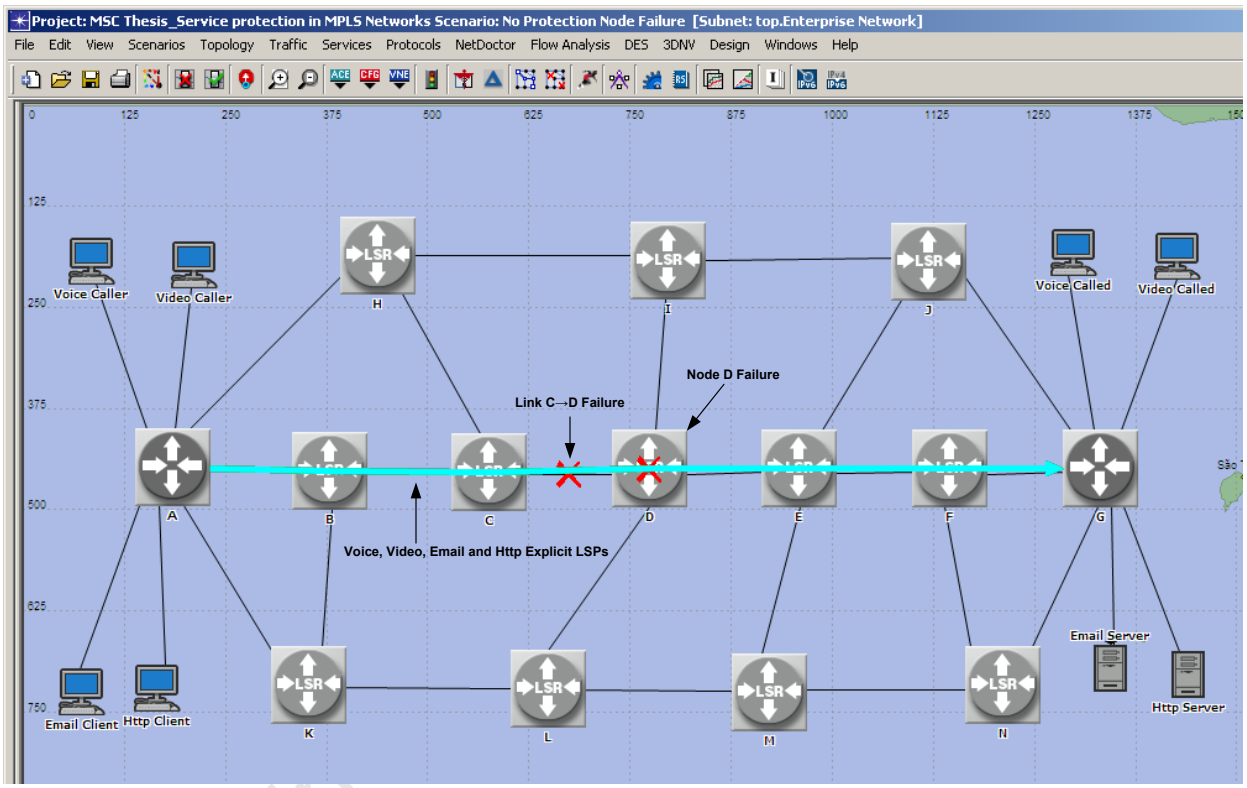

Figure 4.15: No MPLS Protection

4.5.2 Russian Dolls Model and Preemption

In this scenario, the objective was to implement the Russian dolls bandwidth constraint model and preemption of LSPs when there is insufficient bandwidth. RDM configuration involved enabling RSVP on connected interfaces, setting the maximum reservable bandwidth, allocating bandwidth to the bandwidth pools, setting the bandwidth model to RDM on all the routers and the TE class matrix.

RSVP was enabled on all the interfaces by configuring the interface status from the protocols > RSVP menu as shown in Figure 4.16.

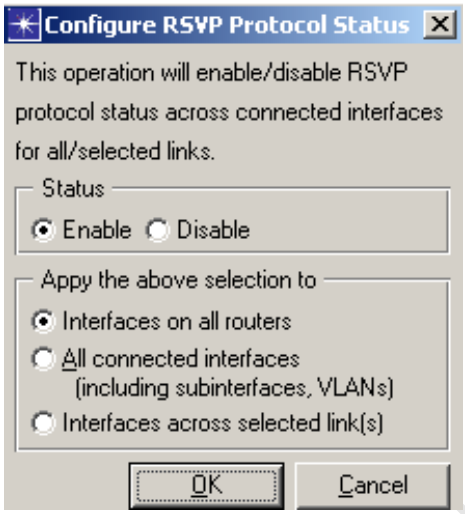

Figure 4.16: Enabling RSVP

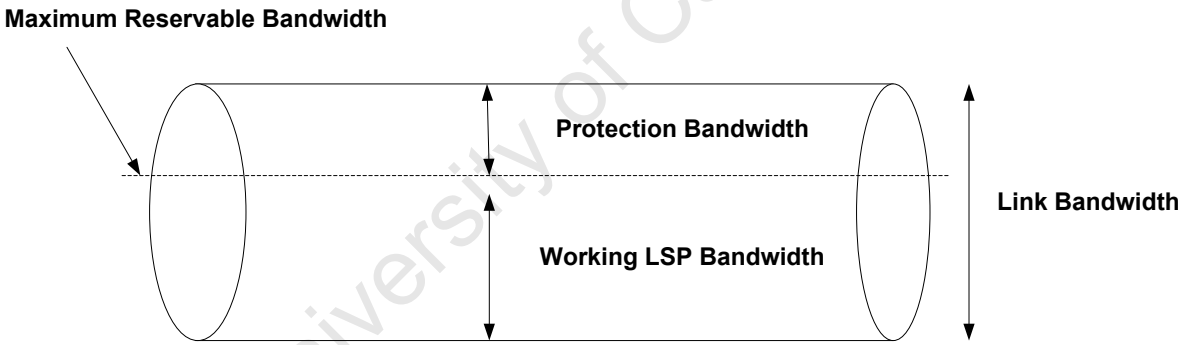

Figure 4.17: Link Bandwidth Allocation

Figure 4.17 shows the allocation of bandwidth on a link. A percentage of the link's bandwidth was reserved for protection in case of failure. The remaining bandwidth was allocated to the working LSPs from the maximum reservable bandwidth. The maximum reservable bandwidth was set by configuring the interface based reservable bandwidth from the protocols menu under RSVP as shown in Figure 4.18.

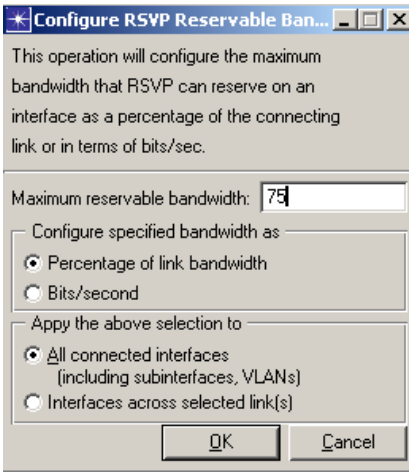

Figure 4.18: Maximum Reservable Bandwidth Configuration

In this scenario,

Link bandwidth = 34.368 Mbps

Maximum reservable bandwidth = 75% of link bandwidth = 25.776 Mbps

Protection Bandwidth = 25% = 8.592 Mbps

The bandwidth allocation to the pools was done on each connected interface under the RSVP > RSVP Protocol Parameters > Interface Information Table on each router. Two bandwidth pools, BC0 (global pool) and BC1 (sub-pool) were configured on the connected interfaces of each router from the bandwidth attribute as shown in Figure 4.19.

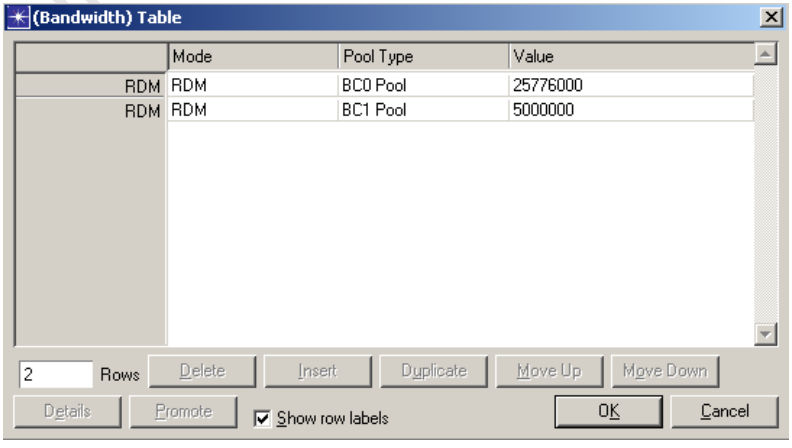

Figure 4.19: Bandwidth Pools Configuration

The bandwidth model was set to “Russian Dolls Model” on all the routers from the MPLS > MPLS Parameters > DiffServ TE Parameters > Bandwidth Model attribute as shown in Figure 4.20. The TE class matrix was also configured from the DiffServ TE attribute as specified in Figure 4.21.

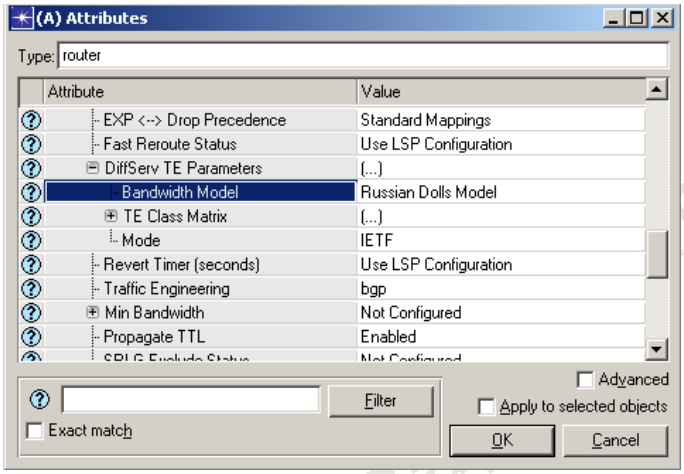

Figure 4.20: Bandwidth Model Configuration

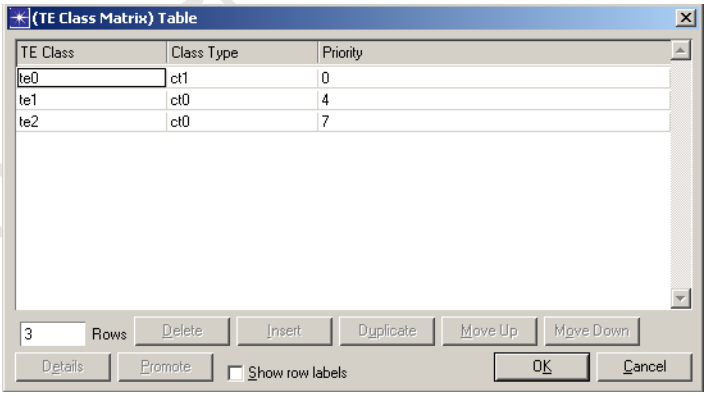

Figure 4.21: Traffic Class Matrix Configuration

The voice, video, email and HTTP LSPs were setup as dynamic LSPs from the ingress router A to the egress router B. The bandwidth allocated to each LSP was used as a constraint for path setup. As defined in the TE class matrix, two class types, CT0 and CT1 were used for classifying the LSPs. CT0 is the least priority traffic while CT1 is the highest priority traffic. According to the Russian Dolls Model definition,

BC0 = CT0 + CT1 = Maximum reservable bandwidth

BC1 = CT1

The maximum reservable bandwidth was allocated to the two bandwidth pools as follows:

BC0 = 25.776 Mbps

BC1 = 5 Mbps

Therefore, CT0 = 20.776 Mbps

CT1 = 5 Mbps

(a) 1st Simulation Run

In the first simulation run, the video, email and HTTP LSPs are set up at 100s and the simulation was run for 5 minutes. Bandwidth was allocated to the LSPs as specified in Table 4.3.

Table 4.3: Run 1 Bandwidth Allocation

LSP Type	Class Type	Priority	Bandwidth
Video LSP	CT0	4	15.776 Mbps
Email LSP	CT0	7	5 Mbps
HTTP LSP	CT0	7	5 Mbps

The video LSP has been allocated the highest bandwidth of 15.776 Mbps because it has the highest bandwidth requirements. The email and HTTP LSPs were allocated 5 Mbps because it is assumed that the allocated bandwidth will be enough to meet the bandwidth requirements of the two LSPs. In this simulation run, there is 5 Mbps available bandwidth which can be used by any of the three LSPs in Table 4.3 should their bandwidth requirements increase or by any new LSP requesting bandwidth. In this case there is 5Mbps bandwidth available should the voice LSP

request to be established in the network. The values all add up to 25.776 Mbps which is the maximum reservable bandwidth.

(b) 2nd Simulation Run

In this simulation, the Voice LSP is included. Two scenarios were run in this simulation. All the four LSPs were set up at100s. The simulation was also run for 5 minutes as in the 1st simulation run. The LSP bandwidth allocation for both scenarios was as specified in Table 4.4. The priorities shown in Table 4.4 were for the first scenario. In the second scenario, all the LSPs had a priority of 7. This was to observe the results when preemption is not possible due to matching priorities.

Table 4.4: Run 2 Bandwidth Allocation

LSP Type	Class Type	Priority	Bandwidth
Voice LSP	CT1	0	5 Mbps
Video LSP	CT0	4	15.776 Mbps
Email LSP	CT0	7	5 Mbps
HTTP LSP	CT0	7	5 Mbps

(c) 3rd Simulation Run

In this simulation, the bandwidth requirement for the voice LSP increased as specified in Table 4.5.

Table 4.5: Run 3 Bandwidth Allocation

LSP Type	Class Type	Priority	Bandwidth
Voice LSP	CT1	0	10 Mbps
Video LSP	CT0	4	15.776 Mbps
Email LSP	CT0	7	5 Mbps
HTTP LSP	CT0	7	5 Mbps

(d) 4th Simulation Run

In this simulation, the bandwidth requirements for the voice, email and HTTP were increased as specified in Table 4.6. Two scenarios were run in this simulation. The first scenario had priorities specified in Table 4.6. In the second scenario all the LSPs had a priority of 7 in order to observe the effect of not having preemption in the network.

Table 4.6: Bandwidth Allocation for Run 4

LSP Type	Class Type	Priority	Bandwidth
Voice LSP	CT1	0	15 Mbps
Video LSP	CT0	4	15.776 Mbps
Email LSP	CT0	7	15 Mbps
HTTP LSP	CT0	7	10 Mbps

4.5.3 Fast Reroute and Preemption

Finally, in this scenario, RDM, preemption and fast reroute were implemented. The objective was to guarantee protection to voice traffic when there is a link or node failure. RDM was setup as follows:

Link Bandwidth = 34.368 Mbps

Maximum Reservable Bandwidth = BC0=75% = 25.776 Mbps

Protection Bandwidth = 25% = 8.592 Mbps

A link bandwidth of 34.368 Mbps (E3) was selected so that there is enough bandwidth to satisfy the bandwidth requirements of the LSPs and no congestion is experienced in the network. The next lower link bandwidth available in the OPNET link models was an E1 link providing 2.048 Mbps bandwidth. If the E1 link were selected, the bandwidth would have been insufficient for the LSPs in the network.

Table 4.7: Bandwidth Allocation for Fast Reroute and Preemption Scenario

LSP Type	Class Type	Priority	Bandwidth
Voice LSP	CT1	0	15 Mbps
Video LSP	CT0	4	15.776 Mbps
Email LSP	CT0	7	25 Mbps
HTTP LSP	CT0	7	10 Mbps

The bandwidth requirements for the voice, video, email and HTTP LSPs were as specified in Table 4.7. In this simulation a failure occurred on link I→J at 600s and the link was restored at 1200s. Protection was provided for the voice traffic by configuring fast reroute for link protection on the voice LSP. A bypass tunnel for link protection was configured on the outgoing interface of router H along the path H→C→D→E→J. The outgoing interface of router H was

IF1 with the IP address 192.0.10.2 255.255.255.0. This scenario is illustrated in Figure 4.22. The bandwidth requirement for the voice LSP was 15 Mbps while the protection bandwidth that was available was 8.592 Mbps. The bypass tunnel bandwidth requirement was 15 Mbps and the protection bandwidth was set as 15 Mbps. The bypass tunnel had holding and setup priorities of 0 and was assigned to the CT1 class. This is to allow it to be able to preempt lower priority LSPs.

In the second scenario the bypass tunnel had holding and setup priorities of 7. All LSPs had 7 as the priority. This includes the setup, holding and class type priorities. The simulation time for both scenarios was 30 minutes.

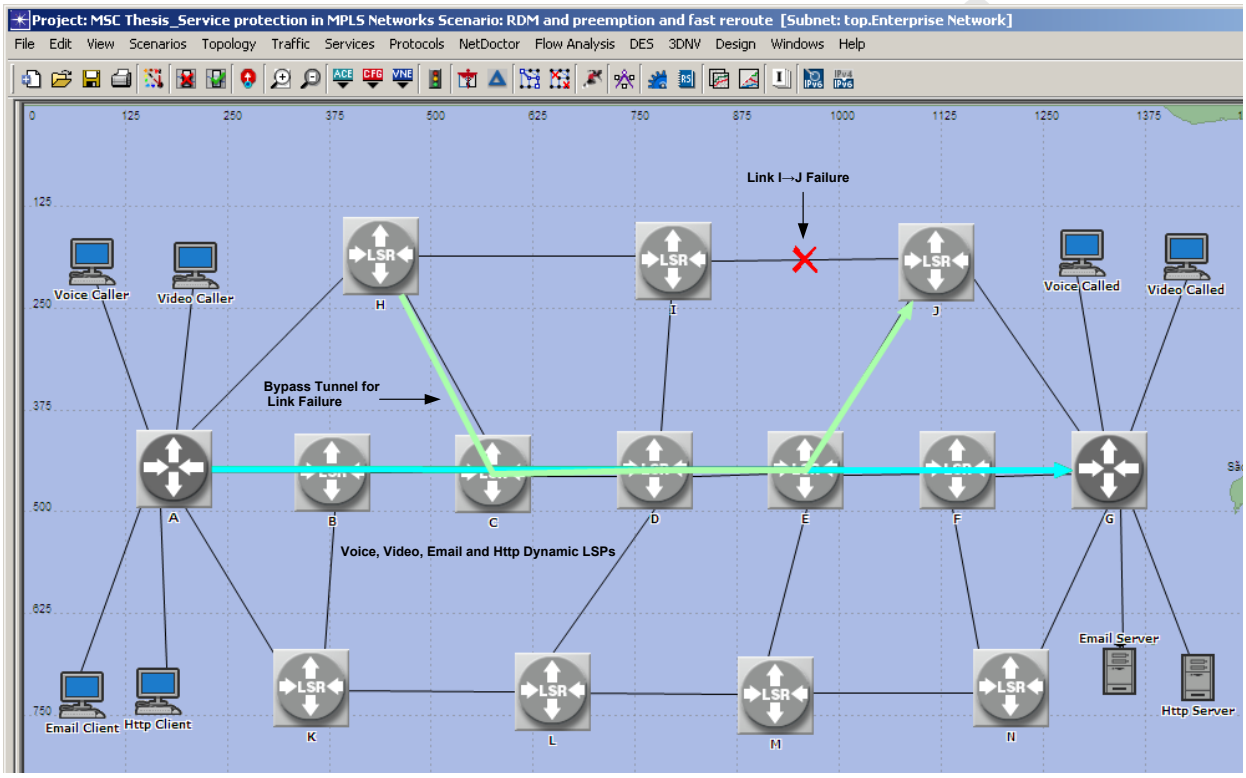

Figure 4.22: Fast Reroute and Preemption Link Protection

4.6 CHAPTER SUMMARY

This chapter presented the proposed real-time bandwidth encapsulation mechanism to guarantee protection of voice traffic during network failure. The proposed solution was tested by simulation in OPNET modeler. The mechanism incorporates LSP preemption and bandwidth encapsulation or allocation through the Russian dolls model.

Several scenarios were simulated to test the performance of the proposed protection scheme. The scenarios simulated were not real world scenarios but theoretical scenarios aimed at showing the real-time nature of the proposed bandwidth encapsulation mechanism for facility backup (many-to-one) protection mechanism. The scenarios were selected to show the changing bandwidth requirements of the voice LSP, the effect of LSP preemption and priority in the network and the performance of the proposed real-time bandwidth encapsulation model.

The first set of scenarios investigated the QoP of path protection and fast reroute. The simulation validated the suitability of fast reroute for the protection of voice applications and the importance of implementing protection in a network.

The effect of LSP preemption on bandwidth allocation and bandwidth utilisation was also tested. After the suitability of fast reroute, preemption and the Russian dolls model was validated, the proposed solution was then tested on a link failure.

The simulations in OPNET did not consider multiple failures occurring in the network but only single link and node failures. The results obtained from the simulations are presented and analysed in chapter 5.

5. SIMULATION RESULTS AND ANALYSIS

5.1 INTRODUCTION

In this chapter the results of the simulations described in chapter 4 are presented and analysed. First, a brief discussion of the performance metrics investigated is given. Then the results obtained from the scenarios simulated are presented and analysed.

As described in chapter 4, several scenarios were simulated. Section 5.2 presents results on the investigation of the QoP of path protection and fast reroute. These two scenarios were compared with a scenario that did not have protection. Section 5.3 presents results on the Russian dolls model and LSP preemption. Finally section 5.4 presents results from the implementation of the Russian dolls model with LSP preemption and fast reroute.

5.2 PERFORMANCE METRICS INVESTIGATED

As discussed in section 2.5 of chapter 2, several criteria or performance metrics are used to assess the performance of a protection scheme. Other performance metrics used were discussed in the literature review. The performance metrics that this research focused on are packet end-to-end delay, LSP traffic reroute time and packet loss.

(a) Traffic Reroute Time

Traffic reroute time is the time taken to switch traffic away from the failed LSP. It is the difference between the time an LSP fails and the time that the ingress LER or PLR switches traffic from the failed LSP.

(b) Packet loss

This is determined by getting the difference between the traffic sent at the source and the traffic received at the destination.

(c) Packet End-End Delay

Packet-end-to-end delay is the time that it takes to transmit packets from the source node to the destination node.

> Voice packet delay = network delay + encoding delay + decoding delay + compression delay + decompression delay.

5.3 PATH PROTECTION AND FAST REROUTE QOP RESULTS

In this set of simulations, the QoP provided by path protection and fast reroute when a link or node fails in the network was investigated. The investigation also included a network without any MPLS protection provided during network failure.

5.3.1 Traffic Reroute Time Results

In this section the results of the traffic reroute time of the voice LSP for path protection, fast reroute and no MPLS protection are presented and discussed. In Figure 5.1 and Figure 5.2 the blue square in the graphs represents the LSP reroute time of the fast reroute scenario, the green triangle represents the LSP reroute time of the path protection scenario and the red diamond in the graphs represents the reroute time of the no MPLS protection scenario.

(a) Link Failure

Figure 5.1 shows the LSP reroute time of the voice LSP when the link C→D failed at 600s (10 m). The traffic reroute time of the path protection scenario was 0.00152s (1.52ms) and that of the fast reroute scenario was 0.000789s (0.789 ms). The voice LSP reroute time of path protection was almost twice that of fast reroute. This is due to the fact that in the path protection scenario, the reroute was done by the ingress router A while in the fast reroute scenario the reroute was done by the point of local recovery (PLR) router B. The reroute time of the no MPLS protection scenario is the same as that of path protection because the rerouting is done by the ingress node A. However, the no MPLS scenario has no backup LSP to reroute the traffic to.

In the path protection scenario, the entire path A→B→C→D→E→F→G was avoided after the link C→D failed and traffic was rerouted to the backup path A→K→L→M→N→G. In the fast

reroute scenario, traffic was rerouted to the bypass tunnel at the PLR router B and rerouted back to the primary path at the merge point (MP) router D. In the no MPLS protection scenario traffic IP rerouting was used to route traffic to the alternative path A→H→I→J→G.

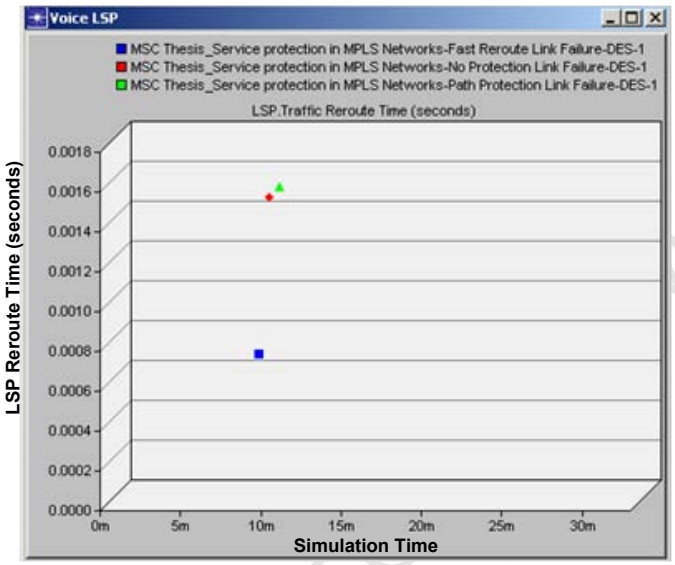

Figure 5.1: Link Failure Voice LSP reroute Time

(a) Node Failure

Figure 5.2 shows the voice LSP reroute time when the router D failed at 600s (10m). The reroute time of path protection and no MPLS protection was 0.001435s (1.435ms) while that of fast reroute was 0.000723s (0.723ms). As in the case of link failure the reroute time of path protection is almost twice that of fast reroute. Traffic on the primary LSP A→B→C→D→E→F→G in path protection was rerouted by the ingress router A to the backup LSP A→K→L→M→N→G. In fast reroute, traffic was rerouted to the bypass tunnel at the PLR router B and rerouted back to the primary path at the MP router E. In no MPLS protection traffic was rerouted along the route A→H→I→J→G by IP rerouting.

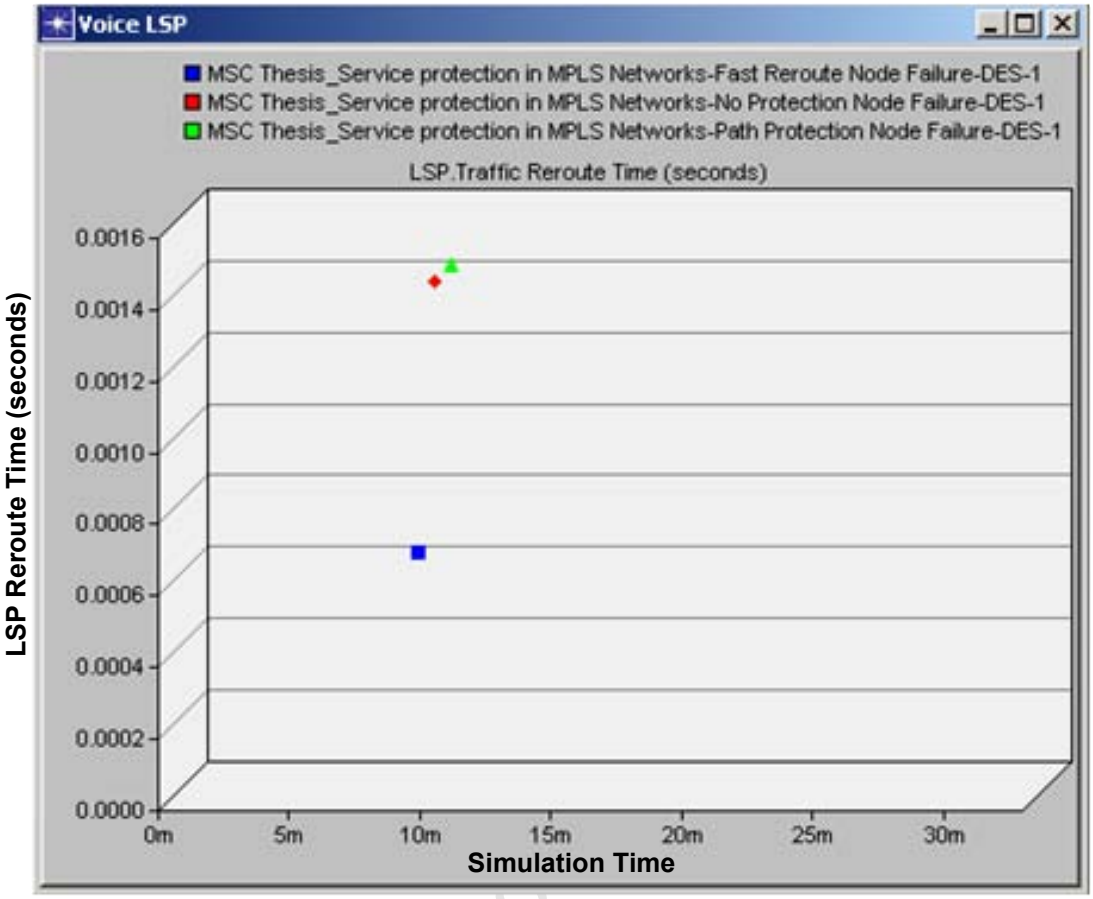

Figure 5.2: Node Failure Voice LSP Traffic Reroute Time

The results presented in this section show that the rerouting or protection switching time was far less than 50ms in all three scenarios. However fast reroute had the lowest reroute values hence is ideal for the protection of voice traffic.

5.3.2 Packet loss Results

In this set of results, the voice traffic received at the destination node, Voice Called, is shown. This was to determine whether there was any packet loss at the receiving node. The scenarios represented are path protection, fast reroute and one without any MPLS protection provided. In Figure 5.3 and Figure 5.4 the blue graph represents fast reroute, the red graph represents no MPLS protection and the green graph represents path protection.

(a) Link Failure

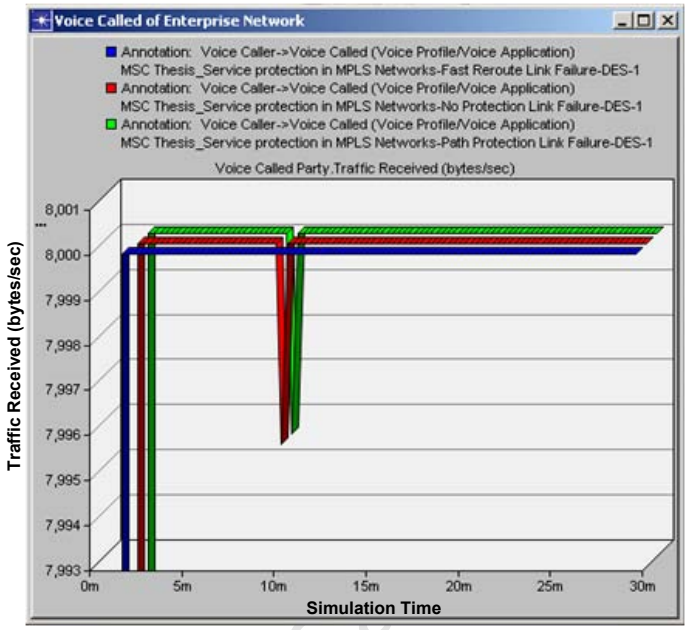

Figure 5.3: Link Failure Traffic Received

Figure 5.3 shows the traffic in bytes/sec received at the voice destination node. It can be seen that when the link C→D failed at 600s (10m), there was a drop in the traffic received at the destination node in path protection (green) and the scenario without MPLS protection (red). There was a drop from 8,000 bytes/sec (64,000bps) to 7,995.6 bytes/sec (63,964.8 bps). There was therefore a packet loss of 4.4 bytes/sec (35.2 bps). However, in the fast reroute scenario (blue) a constant flow of 8000bytes/sec can be seen. There was therefore no packet loss in fast reroute. This was due to the faster reroute time of 0.789ms compared with 1.52ms of path protection. In the scenario without MPLS, the LSP reroute time was the same as that of path protection, however, IP rerouting with OSPF protocol was used to reroute the traffic onto an alternative path hence the packet loss. There was no backup LSP to reroute the traffic to, however, since the network had alternative routes to reroute the traffic to, the route A→H→I→J→G was taken. This was verified by the throughput levels on the links along that route.

(b) Node Failure

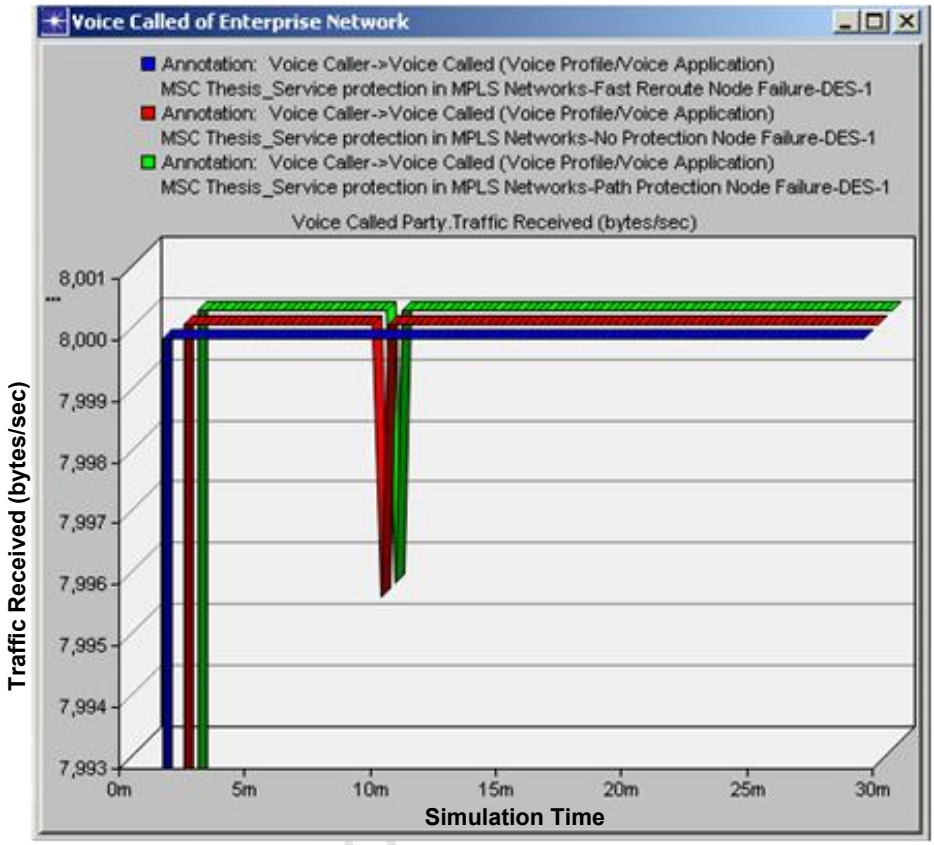

Figure 5.4: Node Failure Traffic Received

Figure 5.4 shows the voice traffic received at the destination node when the router D failed at 600s (10m).The results obtained when router D failed were similar to those obtained when the link C→D failed. It can be seen that just as in the previous results for link failure, there was packet loss in path protection (green) and the scenario without MPLS protection (red) while fast reroute (blue) did not experience packet loss. There was a drop in the received traffic from 8000 bytes/sec (64,000 bps) to 7,995.6 bytes/sec (63,964.8 bps) signifying a packet loss of 4.4 bytes/sec (35.2 bps) in path protection and the scenario with no MPLS protection. Fast reroute showed a constant bit rate of 8,000 bytes/sec (64,000bps). This was due to the shorter reroute time of 0.723ms compared with the longer reroute time of 1.435ms of path protection and the scenario without MPLS protection.

5.3.3 Packet End-to-End Delay Results

The results presented in this section show the voice packet end-to-end delay from the voice source node (Voice Caller) to the voice destination node (Voice Called). In Figure 5.5 and Figure 5.6 the blue graph represents fast reroute, the red graph represents the scenario without MPLS protection and the green graph represents path protection.

(a) Link Failure

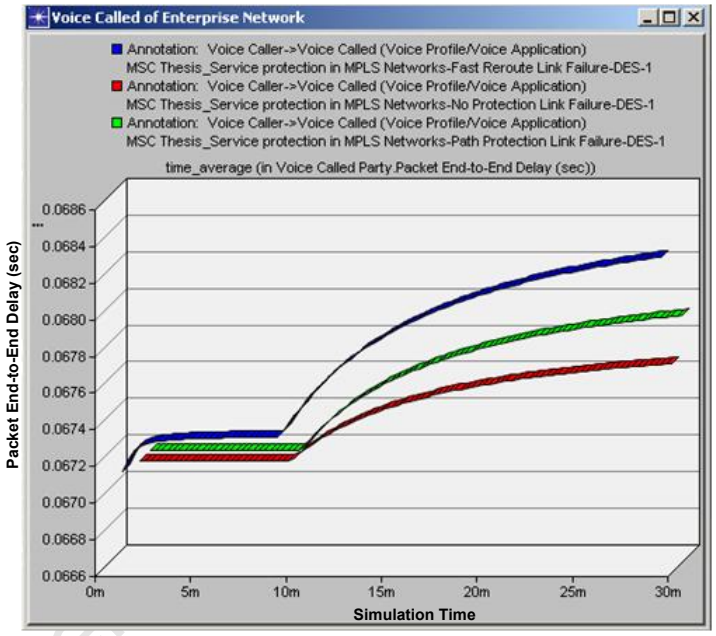

Figure 5.5: Link Failure Packet End-to-End Delay

Figure 5.5 shows the voice packet end-to-end delay for the three scenarios. It can be seen that after the link failure, the packet-end to-end delay increased in all the three scenarios. Fast reroute had the highest packet end-to-end delay of 0.06834s (68.34ms). This was due to the rerouting of the voice traffic through the bypass tunnel. The new path after the failure was A→B→K→L→D→E→F→G making the path longer as it now had 8 nodes from the 7 it had before the failure.

The new path for path protection was A→K→L→M→N→G consisting 0f 6 routers which had 2 routers less than the route in fast reroute. Hence the lower packet end-to-end delay of 0.0679s (67.9ms). The scenario with no MPLS protection had a delay of 0.0677s (67.7ms) which was the

lowest delay. This was due to the rerouting of traffic on the route A→H→I→J→G which was the shortest path from the ingress router A to the egress router G. Since the network was running OSPF which is based on the shortest path algorithm, the traffic was rerouted to that route after the link failure. From the delay values, it can be seen that the difference in the delay for the three scenarios was very minimal.

The results show that the end-to-end delay of fast reroute before the link failure was 0.674s (67.4ms). After the link failure the end-to-end delay increased to 0.0683s (68.3ms) which showed an increase of 0.9ms in delay. The end-to-end delay of the path protection scenario was 0.0672s (67.2ms) before the link failure and increased to 0.0679s (67.9sms) after the link failure. This showed an increase of 0.7ms in delay. The end-to-end delay of the scenario without MPLS protection was 0.672s (67.2ms) before the link failure and increased to 0.0677s (67.7ms) after the link failure. This showed an increase of 0.5ms in delay)

(b) Node Failure

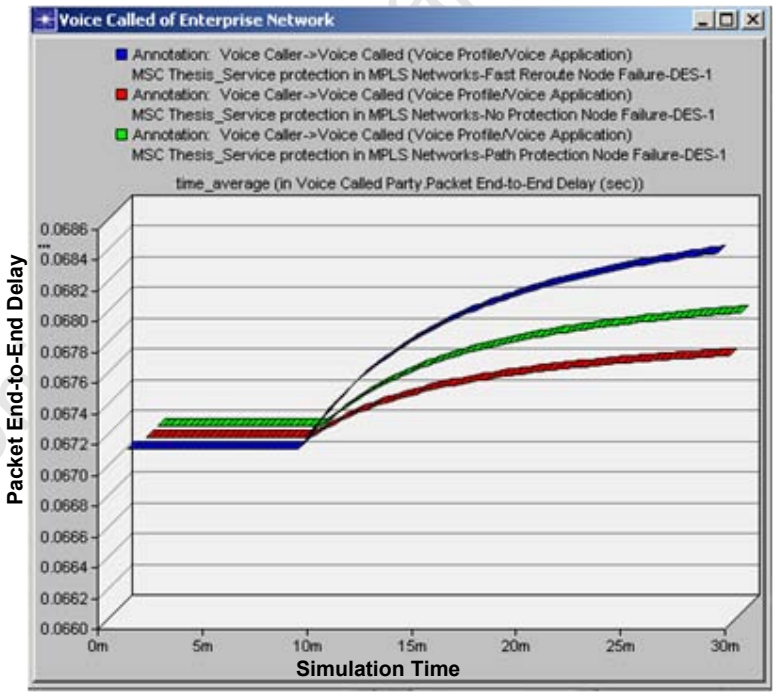

Figure 5.6: Node Failure Packet End-to-End Delay

Figure 5.6 shows the packet end-to-end delay results obtained when node D failed at 600s (10 m). These results were similar to those obtained when the link C→D failed. The end-to-end delay of path protection was 0.0679s (67.9ms) and that of the scenario without MPLS protection was 0.0677s (67.7ms). The end-to-end delay of fast reroute was 0.06844s (68.44). As explained in the previous section, the delay of fast reroute was highest as it had the longest path. After the node failure the route followed was A→B→K→L→M→E→F→G with 8 routers. The routes taken for Path protection and the scenario without MPLS protection were the same as in the link failure scenario. The shortest route was that of the scenario without MPLS hence the lowest delay.

The results show that the end-to-end delay for all three scenarios was 0.0672s (67.2ms) before the node failure. The end-to-end delay of the fast reroute scenario increased to 0.0684s (68.4ms) after the node failure. There was therefore an increase of 1.2ms in delay. The end-to-end delay of path protection increased to 0.0679s (67.9ms) after the node failure. There was therefore an increase of 0.7ms in delay. The end-to-end delay of the scenario without MPLS protection increased to 0.0677s (67.7ms). There was therefore an increase of 0.5ms in delay.

In [46] it was observed that an end-to-end delay of up to 200ms did not cause obvious impairments in the call quality hence was acceptable. The delay values obtained in all three scenarios were far less than 200ms hence were acceptable. It was noticed that longer delays were attributed to longer paths. It is therefore important to ensure that backup paths selected for protection traffic do not degrade the call quality but that they maintain the call quality within acceptable values.

The results of the investigation of the QoP provided by fast reroute and fast reroute showed that fast reroute performed better than path protection with regard to the LSP reroute time and packet loss. Path protection performed better with regard to the packet end-to-end delay. Fast reroute had longer paths after the rerouting of traffic when a network failure occurred hence the longer end-to-end delay. In the scenario without MPLS protection it was shown that packet loss was experienced after both the link and node failure. Although the end-to end delay was the least in this scenario, QoS guarantees provided by MPLS were lost after the network failure.

The LSP reroute time was less than 50ms thus satisfying the requirements of voice traffic to be recovered within 50ms after the occurrence of a network failure. As was shown in the case of fast reroute, due to the fast rerouting of LSP traffic after a network failure, there was no packet loss of the voice traffic. Voice traffic is sensitive to delay and packet loss, therefore fast reroute is ideal for the protection of voice traffic. If voice traffic is not protected, it was shown from the results that packet loss will be experienced. Service protection must therefore be provided to guarantee service continuity during network failure.

5.4 RUSSIAN DOLLS MODEL AND LSP PREEMPTION RESULTS

In this scenario, the Russian dolls model and LSP preemption were implemented. The results show the effect of LSP preemption on bandwidth allocation, bandwidth utilisation and route selection depending on LSP priority and the bandwidth requirements.

(a) 1st Simulation Run Results

In the first simulation run, the video, email and HTTP LSPs were setup from the ingress router A to the egress router G. These LSPs were set up as dynamic LSPs therefore paths were established based on Constraint Shortest Path First (CSPF) calculation. The bandwidth required was used as a constraint for path setup. CSPF uses a routing algorithm based on the SPF calculation. In this model the routing protocol Open Shortest Path First (OSPF) was used. It can be seen from Figure 5.7 that the three LSPs were established along the route A→H→I→J→G. This was the shortest path from the ingress router A to the egress router G, consisting of 5 routers. The route A→H→I→J→G had enough bandwidth to meet the bandwidth requirements of all the three LSPs. The total bandwidth requirement from the three LSPs was 25.776 Mbps and the available bandwidth on each link was 25.776 Mbps. The link bandwidth was 34.368Mbps and 75% of the link bandwidth, that is, 25.776 Mbps was the maximum reservable bandwidth. Since 8.592 Mbps was reserved for protection, only 25.776 Mbps was available for the working LSPs on each link.

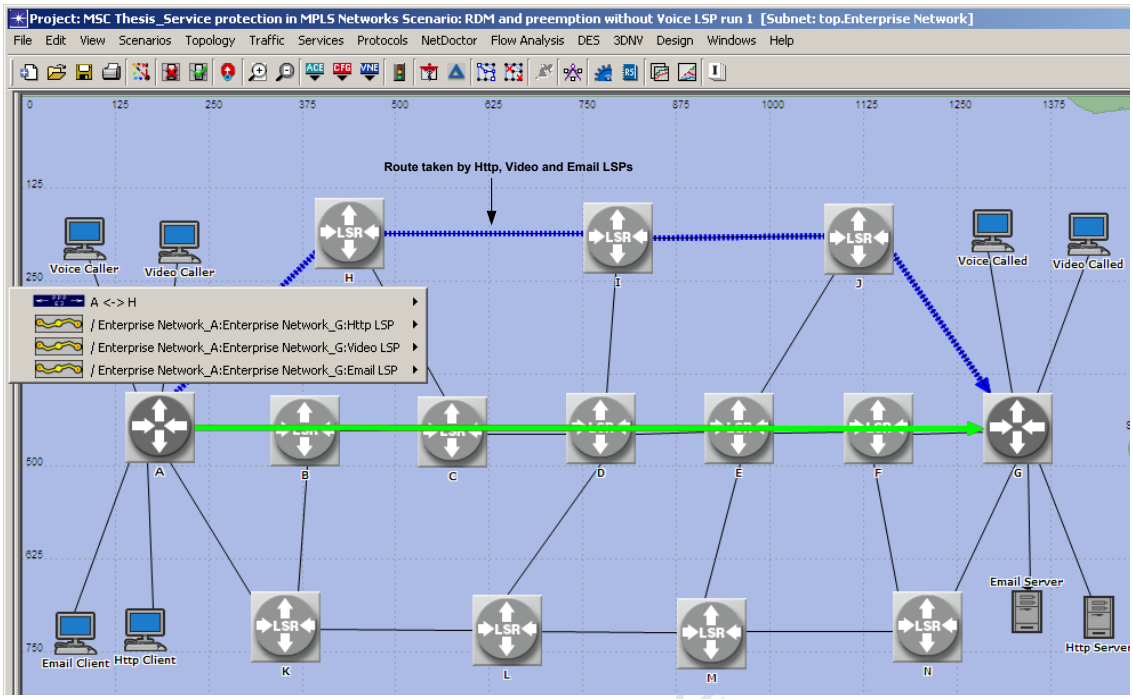

Figure 5.7: First Simulation Run Selected Routes

(b) 2nd Simulation Run Results

Two scenarios were simulated in the second simulation run. In the first scenario, the LSPs had different priorities while in the second scenario all LSPs had the same priorities. In the second simulation run, a voice LSP with a bandwidth requirement of 5Mbps requested to be setup in the network. This represents 62 voice calls of 64 Kbps each and control information.

In the first scenario the voice LSP belonged to the higher priority CT1 traffic class and had the highest setup and holding priorities of 0. The voice LSP was established on the shortest path A→H→I→J→G along with the video and email LSPs. The total bandwidth requirement for all the four LSPs was 30.776 Mbps while the available bandwidth on each link was 25.776 Mbps. The HTTP LSP was preempted from the shortest path A→H→I→J→C and re-established along the next shortest path A→K→L→M→N→G. This route consisted of 6 routers from the ingress router A to the egress router G. The HTTP LSP belonged to the lower priority CT0 traffic class and had the lowest setup and

holding priorities of 7. The video LSP classified as CT0 traffic had higher holding and setup priorities of 4 compared with the HTTP LSP, hence was also established along the shortest path A→H→I→J→C. The email LSP belonged to CT0 traffic and though having the same setup and holding priorities as the HTTP LSP was also established along the shortest path. In OPNET modeler, if LSPs have the same priority they are routed in the order in which they were created, hence the routing of the email LSP on the shortest path.

In OPNET, if an LSP cannot find a suitable path at the first attempt it will keep attempting according to the specified number of attempts until it finds a path. If a path is not found that meets the LSP requirements, the LSP is not setup.

Figure 5.9 shows the setup time of the LSPs. The dark blue square represents the email LSP, the red diamond represents the HTTP LSP, the green triangle represents the video LSP and the light blue triangle represents the voice LSP. It can be seen that the voice, video and email LSPs were all set up at the first attempt at 100s (1m 40s) as specified in the LSP attributes under the setup parameters > Start Time. The HTTP LSP was preempted from the shortest path hence was set up at the second attempt after 10 seconds at 110s (1m 50s). It can be seen that the routing was done in order of priority. The voice LSP was routed first and the time taken for path setup was 0.0099s (9.9ms). The video LSP was routed second and the setup time was 0.0101s (10.1ms). The email LSP was routed third with a setup time of 0.0102s (10.2ms). The HTTP LSP was routed last with a setup time of 0.0108s (10.8s)

In the second scenario all LSPs had the same setup and holding priorities of 7. Since the LSPs all had the same priority the routing was done based on the order in which the LSPs were created and the bandwidth requirement. The video, email and HTTP LSPs were established along the shortest path A→H→I→J→G. The shortest path satisfied the bandwidth requirements of the video, email and HTTP LSPs. The voice LSP was established along the next shortest path A→K→L→M→N→G. The voice LSP did not have higher priority hence could not preempt any LSP. The routes taken by the LSPs are shown in Figure 5.10 and the LSP setup time is shown in Figure 5.11. It can be seen that in contrast to scenario 1, the voice LSP (light blue) was setup last after the second

attempt at 140.02s with a setup time of 0.01078s (10.78ms). The video, HTTP and email LSPs were set up at 100s (1m 40s). The video LSP was routed first with a setup time of 0.0099s (9.9ms). The email LSP was routed second with a setup time of 0.01008s (10.08ms). The HTTP LSP was routed third with a setup time of 0.0102s (10.2ms).

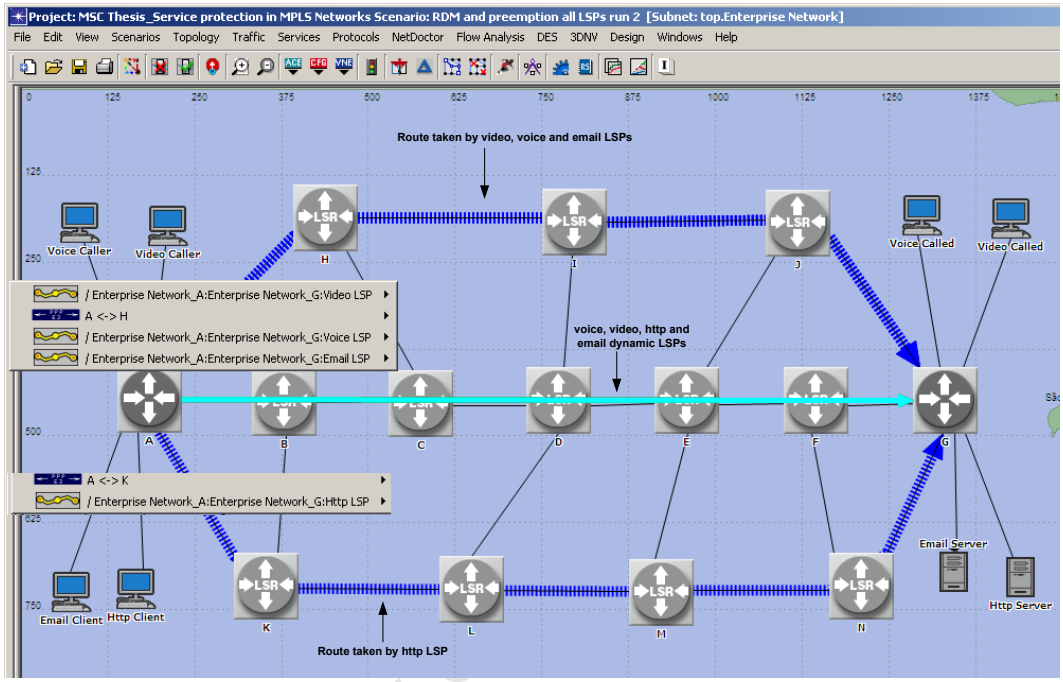

Figure 5.8: Second Simulation Run Selected Routes Scenario 1

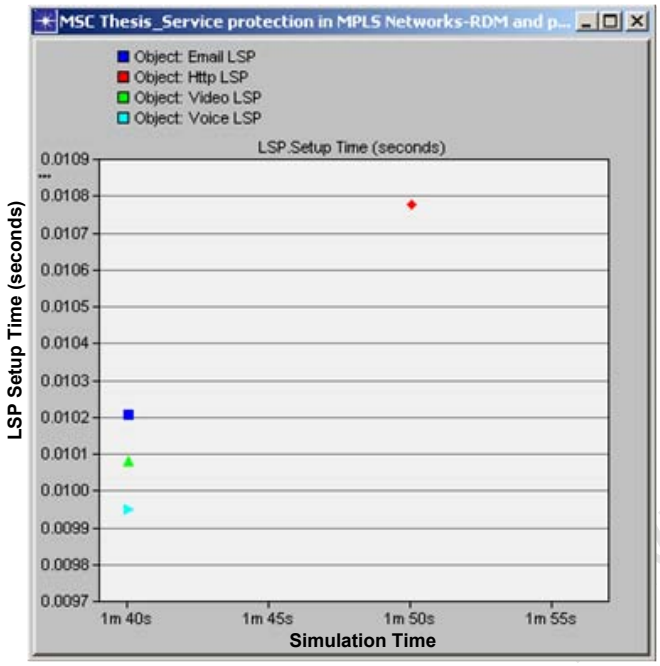

Figure 5.9: Second Simulation Run LSP Setup Time Scenario 1

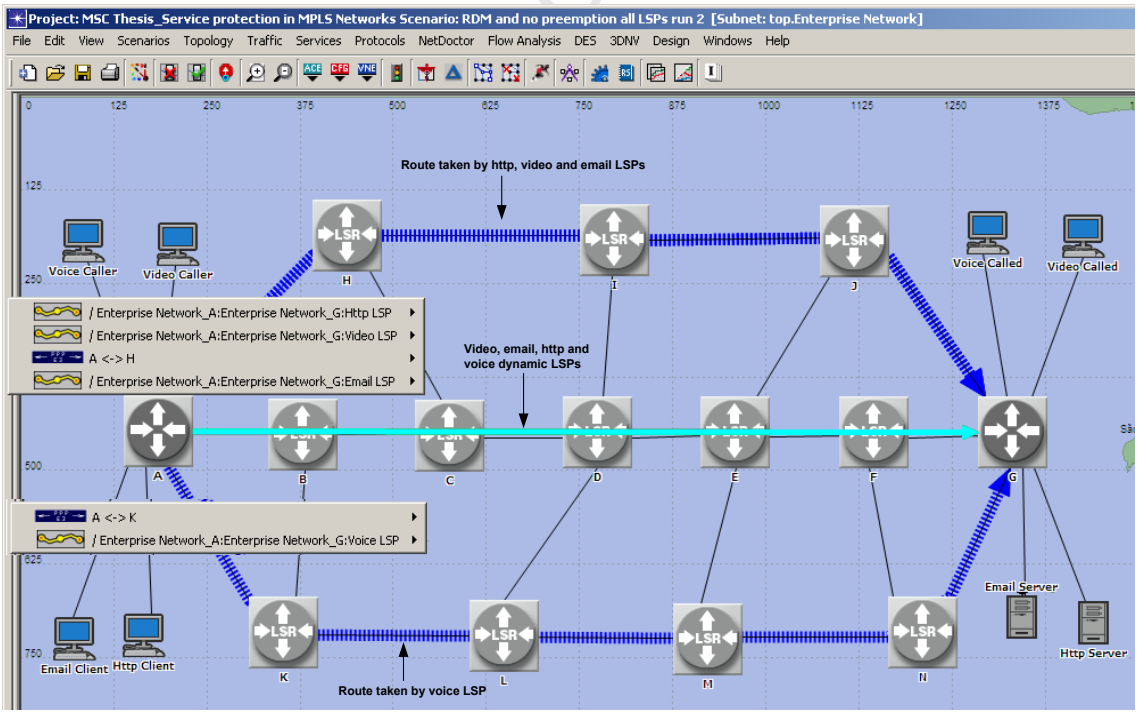

Figure 5.10: Second Simulation Run Selected Routes Scenario 2

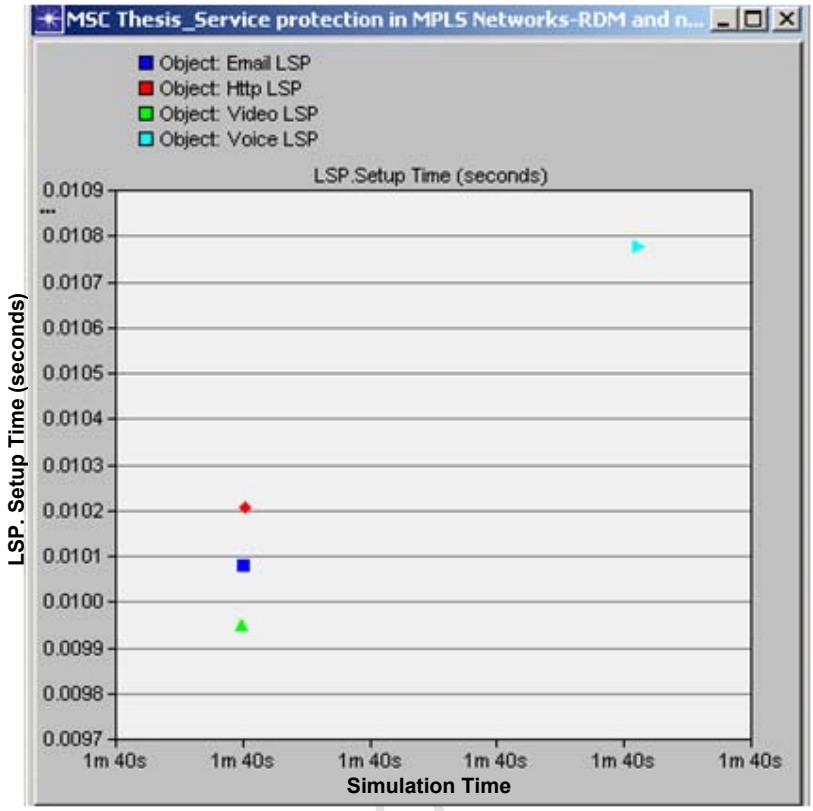

Figure 5.11: Second Simulation Run LSP Setup Time Scenario 2

(c) 3rd Simulation Run Results

In the third simulation run, the bandwidth requirements for the voice LSP increased from 5Mbps to 10 Mbps. This represents 125 voice calls of 64 Kbps each and control information. The total bandwidth requirement for all 4 LSPs was therefore 30.776 Mbps and the available capacity on each link was 25.776 Mbps. The voice and video LSPs being the higher priority LSPs with setup and holding priorities of 0 and 7 respectively were established along the shortest path A→H→I→J→G as shown in Figure 5.12.The email LSP being the lower priority LSP with setup and holding priorities of 7 was preempted from the shortest path and was established on the next shortest path with the HTTP LSP. The total bandwidth requirement for the voice and video LSPs was 25.776 Mbps which was satisfied by the shortest path. The total bandwidth requirement for the

email and HTTP LSPs was 10 Mbps and the next shortest path satisfied this requirement hence the establishment of the two LSPs along this route.

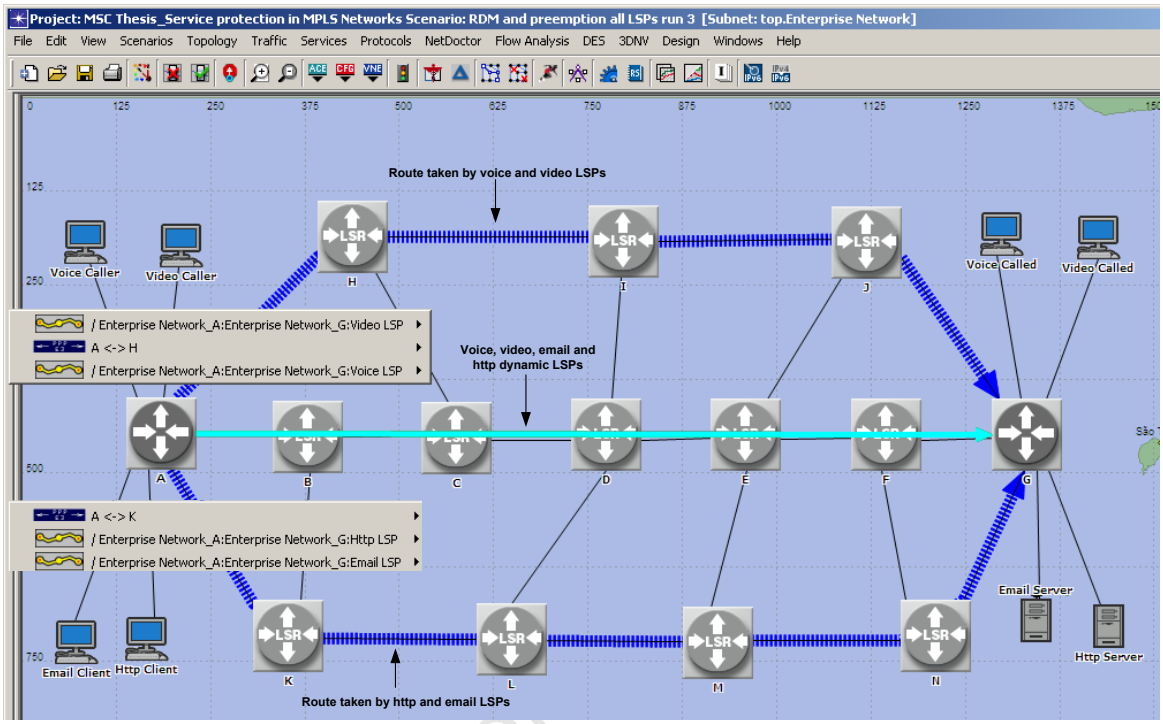

Figure 5.12: Third Simulation Run Selected Routes

Figure 5.13 shows the setup time for the LSPs in the third simulation run. It can be seen that the voice (light blue) and video (green) LSPs were setup first at 100s (1m 40s) as they had higher priority. The voice LSP had a setup time of 0.0099s (9.9ms) and the video had a setup time of 0.01008s (10.08ms). The email (dark blue) and HTTP LSPs (red) were setup at 110s (1m 50s) with setup times of 0.01078s (10.78ms) and 0.01088s (10.88ms) respectively.

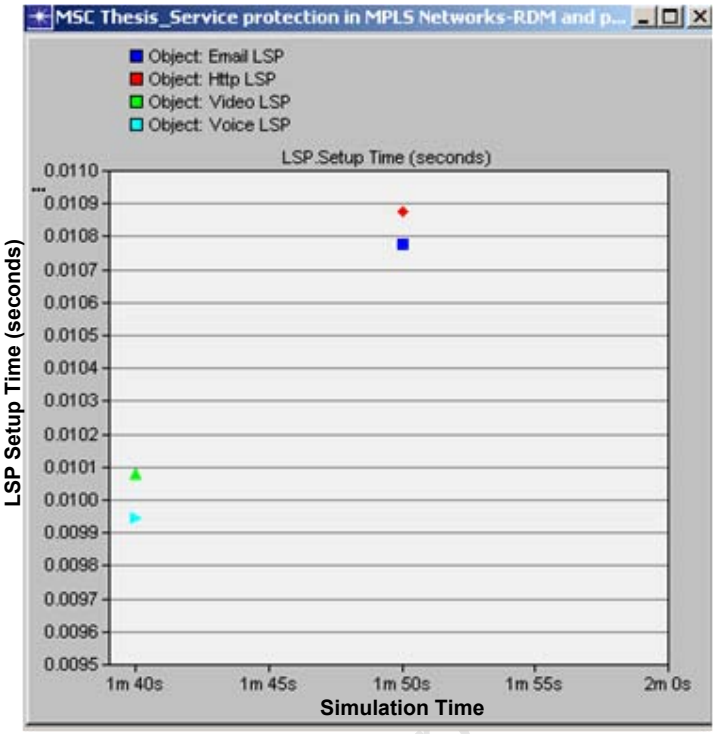

Figure 5.13: Third Simulation Run LSP Setup Time

(d) 4th Simulation Run Results

Two scenarios were simulated in the fourth simulation run. In this simulation run, the bandwidth requirements for the voice, email and HTTP LSPs increased. The voice LSP bandwidth increased from 10 Mbps to 15 Mbps. This represents 187 voice calls of 64 kbps each and control information. The total bandwidth requirement for all the LSPs was 55.776 Mbps.

In the first scenario the voice and HTTP LSPs were established along the shortest path A→H→I→J→G as shown in Figure 5.14. The video LSP was established along the next shortest path A→K→L→M→N→G. The email LSP was preempted from the next shortest path and established along the longest route A→B→C→D→E→F→G with 7 routers.

Figure 5.5 shows the LSP setup time for the LSPs in this scenario. It can be seen that the voice and HTTP LSPs were set up at 100s (1m 40s) with setup times of 0.0099s (9.9ms) and 0.01017s (10.17ms). The video LSP was setup after the second attempt at 110s (1m

50s). The email LSP was set up after the third attempt with a setup time of 0.0089s (8.9ms).

In the second scenario, the HTTP and video LSPs were set up along the shortest path A→H→I→J→G as shown in Figure 5.16. The video and HTTP LSP bandwidth requirement was 15.776 Mbps and 10 Mbps respectively. The total bandwidth requirement of the two LSPs was satisfied by the shortest path A→H→I→J→G hence the establishment of the video and HTTP LSPs along this route. The voice LSP with a bandwidth requirement of 15 Mbps was set up along the next shortest path as the next shortest path A→K→L→M→N→G could not meet the bandwidth requirements of the email and voice LSPs. The email LSP with a bandwidth requirement of 15 Mbps was set up along the longest path A→B→C→D→E→F→G as the next shortest path could not meet the bandwidth requirements of the voice and email LSPs. The voice LSP had a lower retry period of 20ms compared with the 10s for email hence the establishment of the voice LSP on the next shortest path.

Figure 5.17 shows the LSP setup time in the second scenario. The voice LSP (light blue) was setup at the second attempt at 100.02s (1m 40.02s) with a setup time of 0.01078s (10.78ms). The email LSP (dark blue) was also setup at the second attempt at time t = 110s (1m 50s) with a setup time of 0.009s (9ms). The video (green) and HTTP (red) LSPs were setup at 100s (1m 40s) with setup times of 0.0099s (9.9ms) and 0.0101s (10.1ms) respectively.

Since this research was aimed at guaranteeing bandwidth to voice traffic, the two scenarios show that preemption helps to guarantee that bandwidth. When voice traffic is prioritised, it has preference when there is insufficient bandwidth or contention for bandwidth from other types of traffic. Prioritising voice traffic also ensures that the voice traffic is transported along the best route that meet's its requirements thus ensuring QoS. In order to guarantee bandwidth allocation to a class type with the Russian dolls model, preemption must be used to guarantee that bandwidth. If voice traffic is not given

preferential treatment, the QoS is affected which in turn affects the QoP provided in case of network failure.

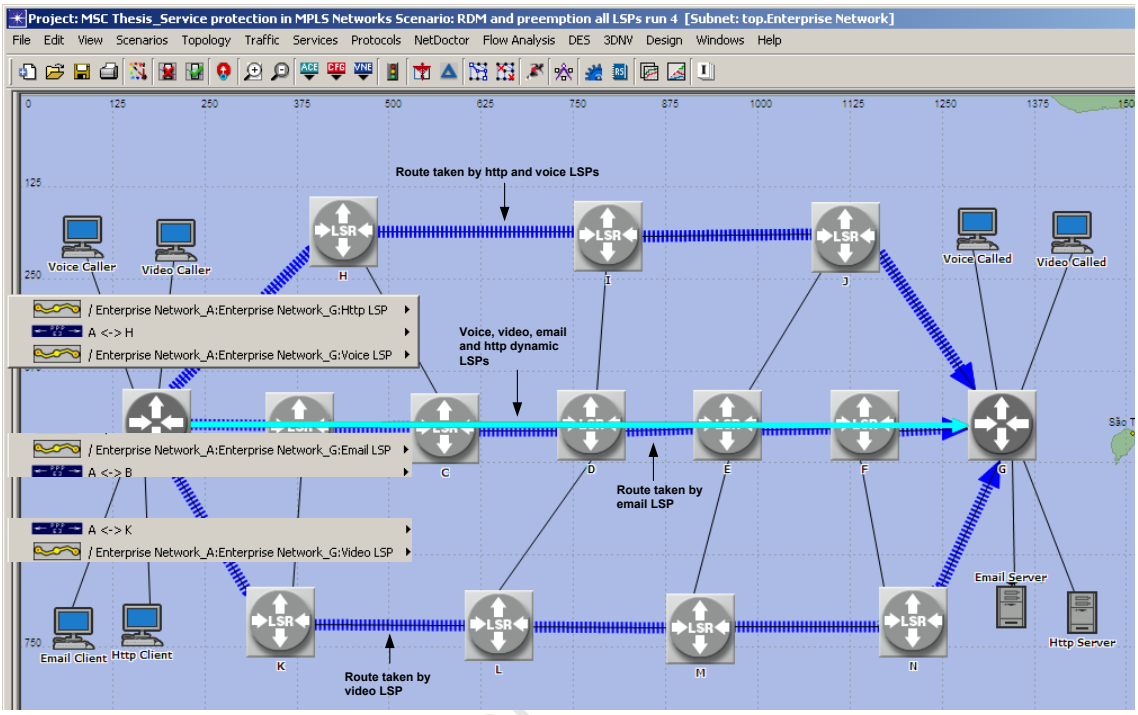

Figure 5.14: Fourth Simulation Run Selected Routes Scenario 1

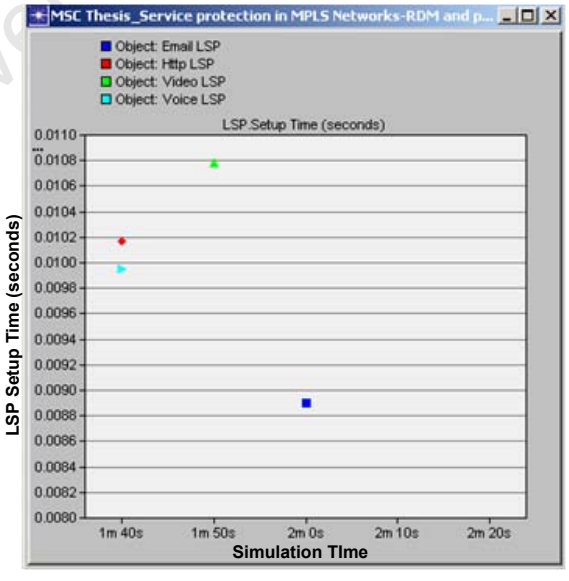

Figure 5.15: Fourth Simulation Run LSP Setup Time Scenario 1

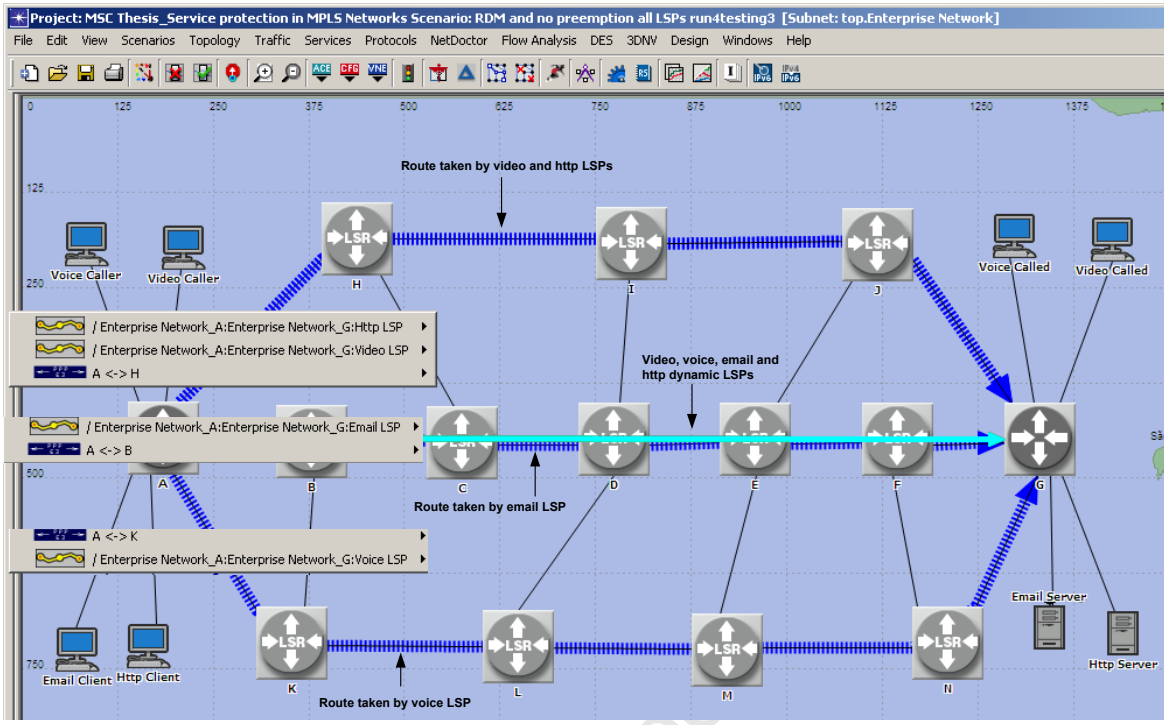

Figure 5.16: Fourth Simulation Run Selected Routes Scenario 2

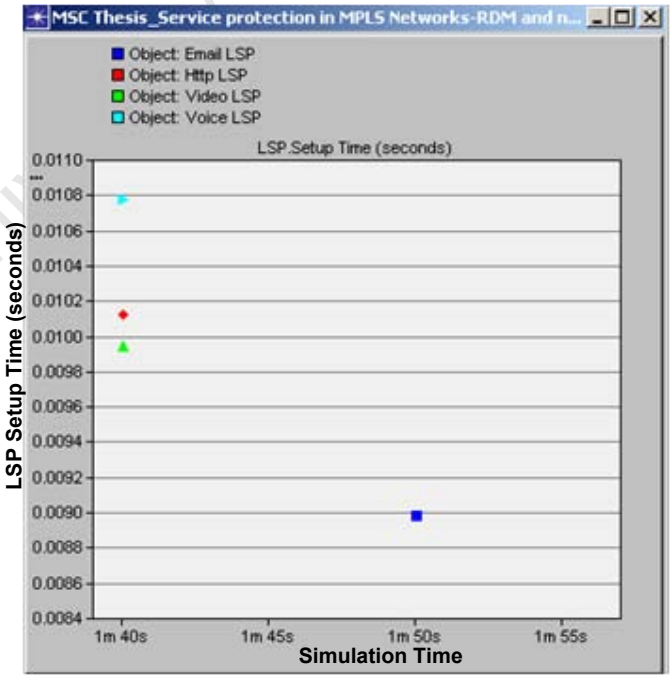

Figure 5.17: Fourth Simulation Run LSP Setup Time Scenario 2

5.5 FAST REROUTE WITH RUSSIAN DOLLS MODEL AND LSP PREEMPTION RESULTS

In the previous section, it was shown that LSP preemption can be used to provide bandwidth to high priority traffic like voice when there is insufficient bandwidth. In this section the results of the implementation of fast reroute with the Russian dolls and LSP preemption are presented.

Two scenarios were run in this simulation. In the first simulation run, there was no failure in the network. The voice and HTTP LSPs with bandwidth requirements of 10 Mbps and 15 Mbps respectively, were set up on the shortest path A→H→I→J→G. The video LSP with a bandwidth requirement of 15.776 Mbps was setup on the next shortest path A→K→L→M→N→G. The email LSP with a bandwidth requirement of 25 Mbps was setup on the longest path A→B→C→D→E→F→G.

The voice LSP bandwidth was 15 Mbps hence the bypass tunnel needed a minimum bandwidth of 15 Mbps along its path for it to protect the voice LSP. The bypass tunnel needed 15 Mbps each on the links H→C, C→D, D→E and E→J. The email LSP had utilised 25 Mbps on the links C→D and D→E along its path. The bypass tunnel needed 6.408 Mbps more bandwidth as only 8.592 Mbps was available on each link for protection.

In the first scenario of the second simulation run, the email LSP was preempted from the path A→B→C→D→E→F→G in order to provide bandwidth for the establishment of the bypass tunnel H→C→D→E→J. Since the email LSP could not find another path that meets its bandwidth requirements, the LSP was not re-established. The email LSP was preempted because it belonged to the lower priority ct0 traffic class. The voice traffic on the bypass tunnel belonged to the higher priority ct1 traffic class hence could preempt the email LSP.

Figure 5.18 shows the setup time for the LSPs. The setup time for the bypass tunnel (dark blue) was 0.00758s (7.58ms), the voice LSP (light blue) setup time was 0.00995s (9.95ms) and the video LSP (green) setup time was 0.01078s (10.78ms).The HTTP LSP (red) was setup initially at 100s (1m 40s) along the path A→H→I→J→G. After the failure at 600s (10m) it was rerouted to the path A→K→L→M→N→G at a setup time of 0.01078s (10.78ms). It can be seen from the graph that the email LSP is not represented on the graph as it was not setup.

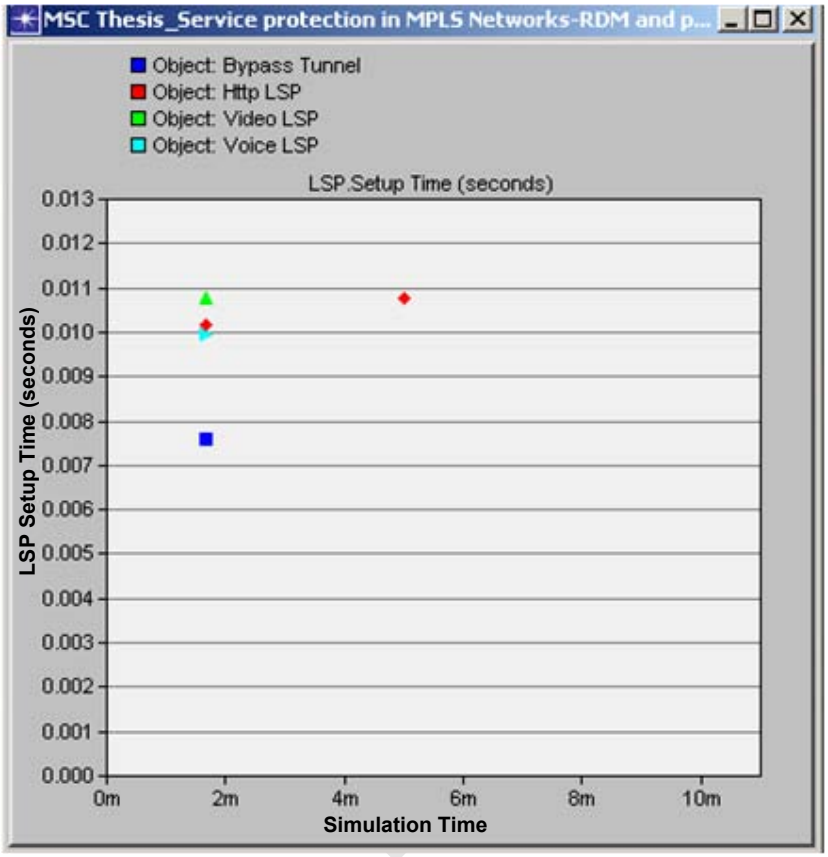

Figure 5.18: Fast Reroute and Preemption Scenario LSP Setup Time

The LSP Reroute time when preemption was used was 0.001329s (1.329ms) while that obtained when preemption was not used was 0.00263s (2.63ms) as shown in Figure 5.19. This shows that preemption reduces the traffic reroute time and not having preemption increases the traffic reroute time.

Figure 5.20 shows the traffic on the voice LSP (red) and the bypass tunnel (blue). It can be seen that there is a constant flow of traffic before and after the failure on the voice LSP. When the link failure occurred at 600s (10m), the traffic was rerouted to the bypass tunnel. There was a constant flow of traffic on the voice LSP because the voice traffic was rerouted to the bypass tunnel at the PLR router H and rerouted back to the main path at the MP router J.

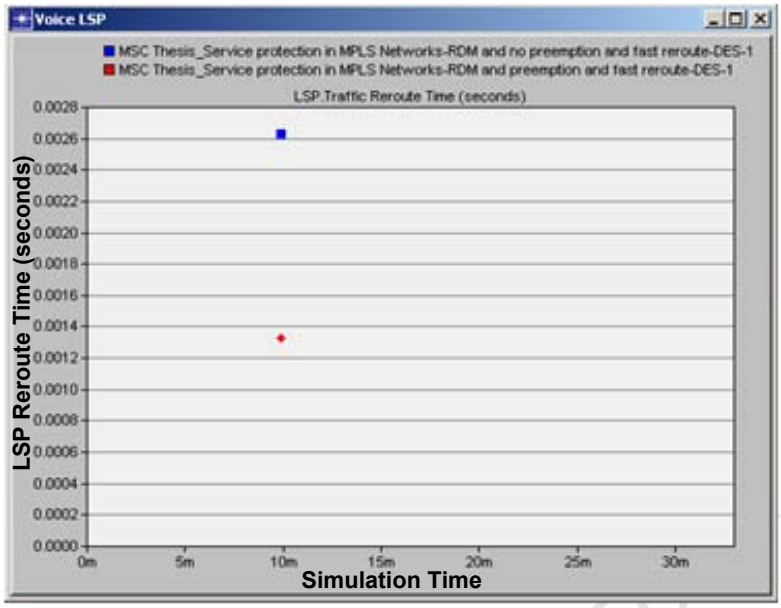

Figure 5.19: Preemption and no Preemption LSP Reroute Time

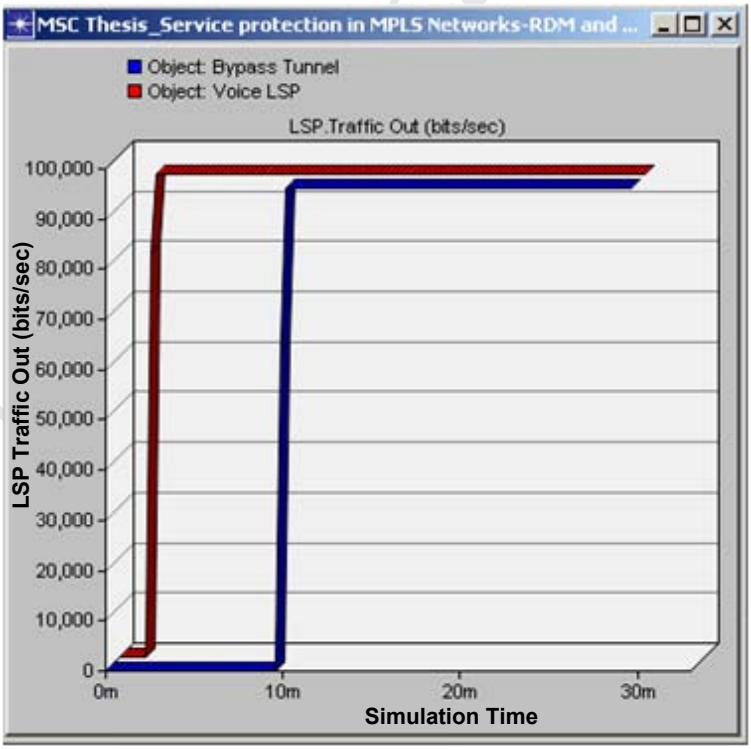

Figure 5.20: Preemption Scenario Voice LSP and Bypass Tunnel Traffic

The traffic sent by the voice caller source node and received by the voice called destination node is shown in Figure 5.21. The graph shows that there was a traffic drop at the receiving node from 8000 bytes/sec (64,000bps) to 7,995.56 bytes/sec (63,964.48 bps). There was a packet loss of 4.44 bytes/sec (35.52 bps) which was 5.5 x 10^{-2} % of the traffic sent.

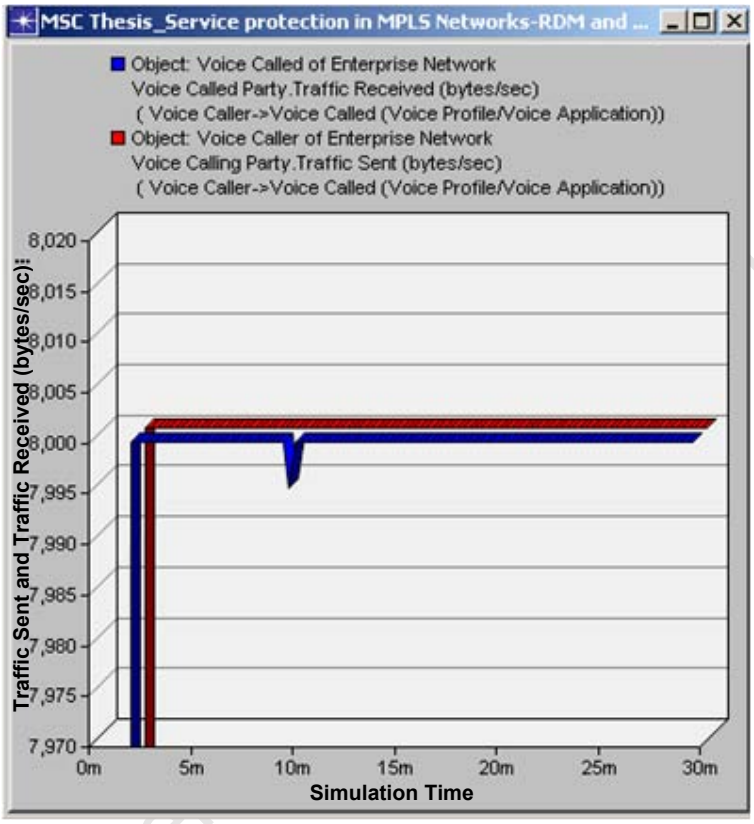

Figure 5.21: Traffic Sent and Traffic Received in Preemption Scenario

In the second scenario, the email LSP was setup on the longest path and the bypass tunnel was not setup. All LSPs had the same priority of 7 hence the email LSP could not be preempted. The voice traffic was not rerouted to the bypass tunnel after the link failure as the bypass tunnel was not setup. The traffic on the voice LSP is shown in Figure 5.22.It can be seen that there was no traffic flow on the voice LSP after the link failure at 600s (10m). The voice LSP had no protection after the link failed hence the receiving node experienced packet loss. The traffic sent by the voice caller (red) source node and the traffic received at the voice called (blue) destination node is shown in Figure 5.23. It can be seen from the graph that the traffic received dropped

from 8000 bytes/sec (64000bps) to 5,786.67 bytes/sec (46,293.36 bps) due to the link failure. There was therefore a packet loss of 2,213.33 bytes/sec (17,706.64 bps) which was 27.67% of the traffic sent. In [47] it was noted that for high quality voice to be maintained packet loss should be less than 1%.

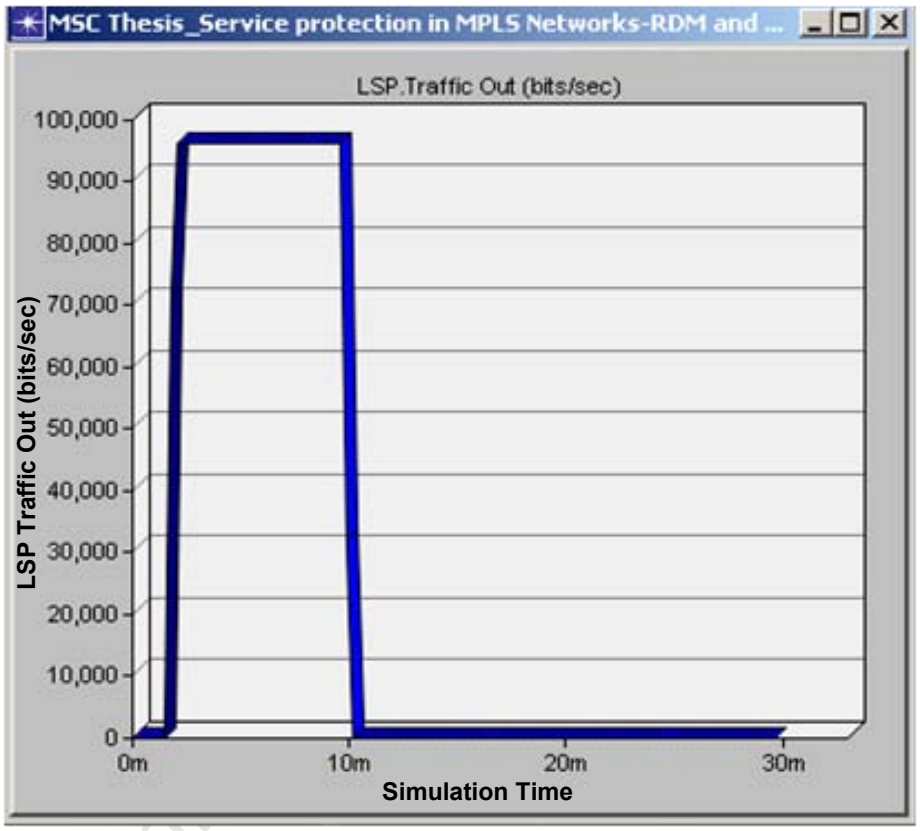

Figure 5.22: No Preemption Scenario Voice LSP Traffic

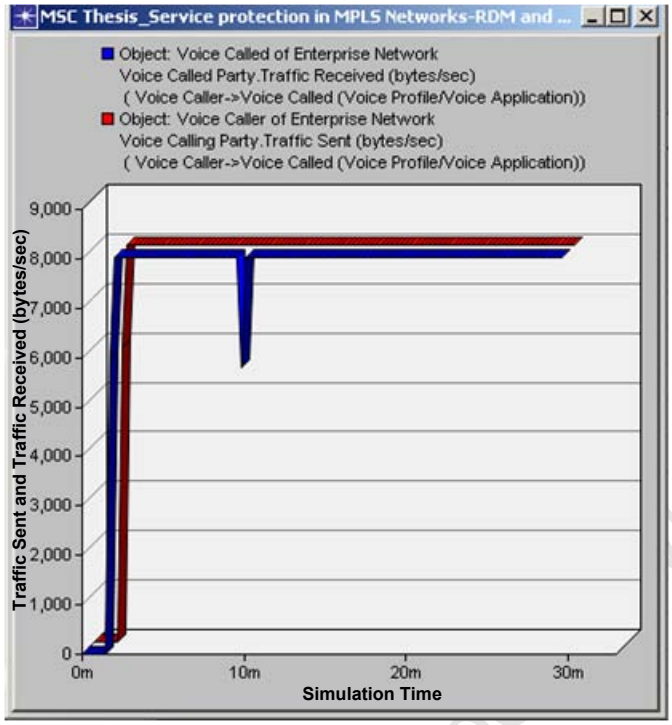

Figure 5.23: Traffic Sent and Traffic Received in No Preemption Scenario

The results in this section show that preemption helps to make bandwidth available for high priority traffic. In cases where preemption is not possible and there is insufficient bandwidth for protection, the traffic will be lost and QoP is not guaranteed to the traffic.

5.6 CHAPTER SUMMARY

In this chapter we presented and analysed the results of the simulations done in OPNET modeler. The QoP of path protection and fast reroute was investigated. The investigation involved a single link and a single node failure. The performance evaluation was based on the LSP traffic reroute time, packet loss and packet end-to-end delay. We found that fast reroute performed better with regard to the LSP reroute time. The LSP reroute time of fast reroute was almost twice that of path protection. This was due to the rerouting of the traffic by the point of local recovery (PLR) node in fast reroute. In path protection, the rerouting of LSP traffic was done by the ingress node hence the longer LSP traffic reroute time. Fast reroute also performed better than path protection with regard to packet loss. In fast reroute, the receiving node did not experience any packet loss

while path protection experienced 5.5 x 10^{-2}% loss in the received traffic. Path protection performed better with regard to packet-end-to-end delay. This was due to the longer paths in fast reroute that were created by the rerouting of traffic to the bypass tunnel thus increasing the number of hops to the destination.

A scenario that had no MPLS protection was also investigated and compared with fast reroute and path protection. We found that when there was MPLS protection, there was a packet loss of 5.5 x 10^{-2}% as was the case with path protection. We also found that the packet end-to-end delay was the lowest. When there was no MPLS protection, IP rerouting with OSPF based on the shortest path algorithm was used. IP rerouting and path protection are too slow to meet the recovery demands of voice traffic which must be recovered within 50ms. When there is no MPLS protection, QoS guarantees provided by MPLS are lost.

We also investigated the effect of LSP preemption on path selection and bandwidth allocation with the Russian dolls model. We found that the priority assigned to traffic and its class type determined whether an LSP will be preempted or be able to preempt other LSPs. When the voice LSP had a lower priority and classified as ct0 traffic, it was not able to preempt any LSP and the path selected was the longer path thus increasing the end to end delay. When voice traffic had the highest priority of 0 and classified as ct1 traffic, the path selected was always the shortest path that met the bandwidth requirements thus reducing the end to end delay.

The final investigation we did was fast rerouting with the Russian dolls model and LSP preemption when a link failure occurred. We found that when the protection bandwidth was insufficient to protect voice traffic, less priority ct0 traffic could be preempted to provide bandwidth for the higher priority ct1 voice traffic on the backup bypass tunnel. When preemption was not possible, the backup bypass tunnel was not setup due to insufficient bandwidth and the voice traffic had no protection. The packet loss experienced when preemption was not possible was 27.67% of the traffic sent while when preemption was possible only 5.5 x 10^{-2}% of the traffic sent was lost. The Russian dolls model implemented with preemption therefore provides a solution for real-time bandwidth encapsulation or allocation to guarantee protection of voice traffic.

The relevance of the results is that they show the efficiency of the proposed real-time bandwidth encapsulation model. The assumed design value of 15ms for switching traffic from the main path to the backup path was much more than the values obtained by simulation. The LSP reroute time obtained by simulation was 1.329ms. It was not possible to obtain the times for bandwidth reservation confirmation and bandwidth allocation from the OPNET simulator to compare them with the assumed design values of 10ms and 25ms respectively. It is assumed that the actual time taken is much less than the assumed design values. The proposed real-time bandwidth encapsulation is therefore an effective solution to guarantee real-time protection of voice traffic.

Chapter 6 concludes the thesis and recommends areas for future research.

6. CONCLUSION

6.1 INTRODUCTION

As communication networks continue to experience link and node failures service protection is vital to guarantee service availability. This research focused on guaranteeing QoP to voice traffic during single link and single node failures. Voice traffic is sensitive to loss and delay hence should be recovered within 50ms so that the call quality is not compromised. MPLS fast reroute is attractive for voice protection because it can provide recovery times of 50ms.

In order to guarantee service availability bandwidth availability is necessary. Bandwidth is a valuable resource and must be utilised efficiently. Bandwidth management is therefore necessary to ensure efficient bandwidth usage. This research proposed guaranteeing QoP to voice traffic by using the Russian dolls model with preemption. The Russian dolls bandwidth constraint model provided bandwidth management through bandwidth allocation to the voice traffic as well as the other traffic classes in the network. LSP preemption guaranteed bandwidth to the voice traffic after failure by preempting less priority traffic.

6.2 THESIS SUMMARY

The research had several objectives to be achieved. The first objective was to investigate single link and node failures in an IP/MPLS network. This objective was achieved by simulating two scenarios each of link failure and node failure in path protection and fast reroute. The results presented in chapter 5 showed that fast reroute achieved better results with regard to packet loss and the LSP reroute time. Path protection performed better with regard to packet-end-end delay. The results obtained for link failure in each protection method were similar to those obtained for node failure. However, a node failure has more impact in that links connected to a router will be affected by the failure. The effect of not having MPS protection in the network was also investigated. The results showed that this caused packet loss in the network. Therefore, service protection is vital to ensure service availability in case of failure and it was validated that fast reroute is ideal for the protection of voice.

The second objective was to investigate the effect of preemption on bandwidth allocation and bandwidth utilisation. This objective was achieved by simulating scenarios with LSPs having different priorities and other scenarios with LSPs having the same priority. The Russian dolls model was implemented for bandwidth allocation to the traffic classes. The results showed that lower priority LSPs could be preempted to create bandwidth for higher priority LSPs. The results also showed that path setup was done in order of priority and along the route with the least number of hops that satisfied bandwidth requirements. Assigning the highest priority to voice traffic guaranteed that it experienced the least end-to-end delay due to the voice LSP being setup along the shortest path to the destination.

The third objective was to investigate bandwidth allocation to guarantee real-time protection of voice traffic and efficient bandwidth utilisation. This objective was achieved by implementing the Russian dolls model for bandwidth allocation to the class types and LSP preemption through simulation. Real-time protection was guaranteed by enabling the voice LSP to preempt less priority LSPs established on links shared with the voice LSP backup path when the protection bandwidth was insufficient in fast reroute. The results showed that when preemption was not possible after a link failure, the backup path could not be established and the voice traffic could not be protected leading to a packet loss of 27.67%. When preemption was used to create bandwidth for the establishment of the voice backup path, the voice traffic was provided with protection and the packet loss due to rerouting was 5.5×10^{-2} %. The results validated that preemption is a useful mechanism to provide bandwidth for higher priority voice traffic for fast reroute.

The final objective was to propose a bandwidth management scheme that would guarantee real-time protection of voice traffic from single link and node failures. This solution was tested and validated by the third objective. The proposed solution uses the Russian dolls model to allocate bandwidth to the different traffic classes in the IP/MPLS network with voice assigned the highest priority. LSP preemption is used to guarantee bandwidth during link or node failure and to ensure that voice is transported along the best route that meets its bandwidth requirements. This solution guarantees minimal packet loss due to rerouting of traffic from the primary path to the backup bypass tunnel.

Table 6.1 gives a summary of the results of the LSP reroute time and packet loss values obtained.

Table 6.1: LSP Reroute Time and Packet Loss Values

Protection Mechanism	**LSP Reroute Time(ms)**	**Packet Loss %**
Fast Reroute Link Protection	0.789	None
Fast Reroute Node Protection	0.723	None
Path protection Link Failure	1.52	5.5×10^{-2}
Path protection Node Failure	1.435	5.5×10^{-2}
No MPLS Protection Link Failure	1.52	5.5×10^{-2}
No MPLS Protection Node Failure	1.435	5.5×10^{-2}
Fast Reroute Link Protection with Preemption	1.329	5.5×10^{-2}
Fast Reroute Link protection without Preemption	2.627	26.67

The results presented in Table 6.1 for Fast Reroute Link and Node Protection, Path Protection Link and Node Failure, No MPLS Protection Link and Node Failure are the results obtained from the simulation runs under Path Protection and Fast Reroute QoP Results in section 5.3. The results obtained are without preemption. The simulations were aimed at determining the quality of protection provided by the different protection mechanisms. The simulations involved a failure of link C→D and a failure of node D as depicted in Figures 4.9, 4.12, 4.14 and 4.15 on pages 61, 63, 64 and 65 respectively.

The results obtained for Fast Reroute Link Protection with Preemption and without Preemption are the results obtained in the simulation runs under Fast Reroute with Russian Dolls Model and LSP Preemption Results in section 5.5. The simulations involved a failure of the link I→J as depicted in Figure 4.22 on page 72. The simulation runs in Section 5.5 are different from those in Fast Reroute Link Failure in section 5.3 in that preemption was not considered in section 5.3 and different links were considered for failure. In section 5.3 the link C→D was considered for failure while in section 5.5 the link I→J was considered for failure. For Fast Reroute Link Protection without Preemption the voice LSP did not have the ability to preempt other LSPs on

the backup path while in Fast Reroute Link Protection with Preemption, the voice LSP had a higher priority and could therefore preempt lower priority LSPs.

6.3 RECOMMENDATIONS FOR FUTURE WORK

This research was validated by simulation in OPNET modeler and can be extending by using a test bed to implement the proposed solution and comparing the results with those obtained in this research. The proposed bandwidth encapsulation can also be tested in a real network to validate its efficiency. Future work can also investigate failure scenarios with multiple faults as this work only considered single link and node failures. As it was mentioned in chapter 1, the study in [1] showed that single failures account for 70% of failures in IP backbones while multiple failures account for 30% of failures in an IP backbone. Multiple failures cause more disruption of traffic compared to single failures and may require more backup paths to deal with the failures. In [48] local recovery mechanisms for single failure recovery were adapted for multiple failure scenarios. This was achieved by grouping failure patterns into clusters and reducing the number of bypass tunnels. In [49] a Label Distribution Protocol (LDP) protection mechanism for transient multiple failures was proposed. More research work on multiple failures can still be done hence the recommendation to extend this work to include multiple failure scenarios.

REFERENCES

[1] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C. Chuah, Y. Ganjali and C. Diot, "Characterization of Failures in an Operational IP Backbone Network," IEEE/ACM Transactions on Networking, vol. 16, no. 4, pp 749-762, August, 2008.

[2] W. D. Grover, "Mesh-Based Survivable Networks: Options and Strategies for Optical, MPLS, SONET and ATM Networking." Prentice Hall PTR, 2003.

[3] E. Rosen, A. Viswanathan, R. Callon, "Multiprotocol Label Switching Architecture," RFC 3031, January, 2001.

[4] M. E Porwal, A. Yadav and S. V. Charhate, "Traffic Analysis of MPLS and Non MPLS Network including MPLS Signaling Protocols and Traffic distribution in OSPF and MPLS," First International Conference on Emerging Trends in Engineering and Technology (ICETET), 187-192, July 16-18, 2008.

[5] MPLS Tutorial, Available: http://www.mplstutorial.com [2011, August 25].

[6] L. He and P. Botham, "Pure MPLS Technology," International Conference on Availability, Reliability and Security, 253-259, March 4-7, 2008.

[7] I. Minei & J. Lucek, "MPLS Enabled Applications, Emerging Technologies and New Technologies," West Sussex, England: John Wiley & Sons, 2005.

[8] B. S Davie & A. Farrel, "MPLS: Next Steps," USA: Morgan Kaufmann, 2008.

[9] Y. Yao, Y. Zhang, C. Lu, Z. Zhang, Y. Zhao and W. Gu, "An Efficient Shared-Bandwidth Reservation Strategy for MPLS Fast Reroute," International Conference on Information Science and Engineering (ICISE), 1644-1647, December 26-26, 2009.

[10] J. A. Zubairi, "Current Practices for MPLS Protection," International Symposium on High Capacity Optical Networks and Enabling Technologies (HONET), 1-5, November 18-20, 2007.

[11] V. Sharma & F. Hellstrand, "Framework for Multi-Protocol Label Switching (MPLS)-based Recovery, RFC 3469, February, 2003.

[12] J. Vasseur, M. Pickavet & P. Dimeester, "Network Recovery, Protection and Restoration of Optical, SONET-SDH, IP and MPLS," USA: Morgan Kaufmann, 2004.

[13] R. Martin and M. Menth, "Backup Capacity Requirements for MPLS Fast Reroute," Symposium on Photonic Networks, 1-8, 27-28 April, 2006.

[14] M. Hadjiona, C. Georgiou and V. Vassiliou, "A Hybrid Fault-Tolerant Algorithm for MPLS Networks," International Conference on Software in Telecommunications and Computer Networks, 369, September 29-October 1, 2006.

[15] E. K. Ali and Y. Habib, "An Efficient Hybrid Recovery Mechanism for MPLS-based Networks," IEEE Symposium on Computers and Communications (ISCC), 474-480, July 5-8, 2009.

[16] C. Chen, "An Adaptive Segment Repair in MPLS Protection," 4th International Conference on Circuits and Systems for Communications (ICCSC), 80-84, May 26-28, 2008.

[17] D. Wang and G. Li, "Efficient Distributed bandwidth Management for MPLS Fast Reroute," IEEE/ACM Transactions on Networking, vol. 16, no. 2, pp 486-495, April 2008.

[18] R. Braden, L. Zhang, S. Berson, S. Herzog & S.Jamin, "Resource Reservation Protocol (RSVP)," RFC 2205, September, 1997.

[19] D. Awduche, L. Berger, D. Gan, T. Li, V. Srinivasan & G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels," RFC 3209, December, 2001.

[20] J. Oliveira, J.P. Vasseur, L. Chen & C. Scoglio, "Label Switched Path (LSP) Preemption Policies for MPLS Traffic Engineering," RFC 4829, April, 2007.

[21] P. Pan, G. Swallow & A. Atlas, "Fast Reroute Extensions to RSVP-TE for LSP Tunnels," RFC 4090, May, 2005.

[22] E. Osborne & A. Simha, "Traffic Engineering with MPLS," USA: Cisco Press, 2003.

[23] "RSVP", OPNET Help Document.

[24] F. Le Faucheur & W. Lai, "Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering," RFC 3564, July, 2003.

[25] F. Le Faucheur, "Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering," RFC 4127, June, 2005.

[26] F. Le Faucheur & W. Lai, "Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering," RFC 4125, June 2005.

[27] J. Ash, "Max Allocation with Reservation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering & Performance Comparisons," RFC 4126, June 2005.

[28] K. Molnar and M. Vlcek, "Evaluation of Bandwidth Constraint Models for MPLS Networks," Available: http://qosip.cs/files/12-evaluation_of_bandwidth_constraint_models_for_mpls_networks.pdf [2011, August, 26].

[29] D. Haskin and R. Krishnan, "A Method for Setting an Alternative Label Switched Paths to Handle Fast Reroute," March, 2000. Available: http://tools.ietf.org/html/draft-haskin-mpls-fast-reroute-03. [2011, November, 06].

[30] K.Owens, S. Makam, V. Sharma, B. Mack-Crane & C. Huang, "A Path Protection/Restoration Mechanism for MPLS Networks," November, 2000. Available: http://tools.ietf.org/html/draft-chang-mpls-path-protection-02. [2011, November, 06].

[31] N. Lin, H. Li and Y. Luo, "A Method of MPLS Fault Restoration," International Conference on Multimedia Technology (ICMT), 1-4, October 29-31, 2010.

[32] Y. Qiu, H. Zhu, Y. Zhou and J. Gu, "A Research of MPLS-Based Network Fault Recovery," 3rd International Conference on Intelligent Networks and Intelligent Systems (ICINIS), 699-702, November 1-3, 2010.

[33] M. Hayasaka and T. Miki "Seamless Failure Recovery for Real-time Premium Traffic in MPLS Networks," 4th IEEE Consumer Communications and Networking Conference, 121-125, January, 2007.

[34] C. Francisco, L. Martins, J. Redol and P. Monteiro, "Dynamic Alternative Routing with Local Protection Paths in MPLS Networks," International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 635-641, October 18-20, 2010.

[35] S. A. El Shazely, O. A. M. Mohsen and K. Shehatta, "Enhancing MPLS Network Recovery using P-Cycle with QoS Protection," 5th International Conference on Information and Communications Technology (ICICT), 197-202, December 16-18, 2007.

[36] A. Hassan, M. Bazama, T. Saad and H. T. Mouftah, "Investigation of Fast Reroute Mechanisms in an Optical Testbed Environment," High Capacity Optical Networks and Enabling Technologies (HONET), 247-251, December 19-21, 2010.

[37] M. Alicherry and R. Bhatia, "Simple Pre-Provisioning Scheme to Enable Fast Restoration," IEEE/ACM Transactions on Networking, vol. 15, no. 2, pp. 400-412, April, 2007.

[38] R. S. Bhatia, M. Kodialam, T.V. Lakshman and S. Sengupta "Bandwidth Guaranteed Routing With Fast Restoration Against Link and Node Failures," IEEE/ACM Transactions on Networking, vol. 16, no. 6, pp. 1321-1330, December, 2008.

[39] R. Cohen and G. Nakibly, "Maximizing Restorable Throughput in MPLS Networks" IEEE/ACM Transactions on Networking, vol. 18, no. 2, pp. 568-581, April 2010.

[40] G. Panza, A. Capone, D. Pinarello and P. Belotti, "Engineering Robust Next Generation Networks," IFIP/IEEE International Symposium on Integrated Network Management-Workshops, June 1-5, 2009.

[41] O. Klopfenstein, "Robust pre-provisioning of Local Protection Resources in MPLS Networks," 6th International Workshop on Design and Reliable Communication Networks, 1-7, October 7-10, 2007

[42] R. Martin, M. Menth and K.Canbolat, "Capacity Requirements for the Facility Backup Option in MPLS in Fast Reroute," 7, Workshop on High Performance Switching and Routing, 2006.

[43] R. Rizk, A. Elmaghraby and M. Mariee, "Protection Otimization for MPLS Networks," 2nd International Conference on Computer and Network Technology (ICCNT), 175-180, April 23-25, 2010.

[44] S. M. Hanshi and W. Al-Khateeb, "Enhancing QoS Protection in MPLS Networks," 2nd International Conference on Network Applications, Protocols and Services (NETAPPS), 95-100, September 22-23, 2010.

[45] M. Zhu, Y. Xing, J. Hu, W.Ye and S. Feng, "A New Preemption Policy for Minimising Path Preemption Cost in MPLS Networks," 6th International Conference on Wireless Communications networking and Mobile Computing (WiCOM), 1-4, September 23-25, 2010.

[46] Draft Revised Recommendation Y.1720 (Protection Switching for MPLS Networks) Available: http://ties.itu.int/ftp/public/itu-t/tsg15opticaltransport/ COMMUNICATIONS/ attached_documents/T05-SG15-061030-TD-PLEN-0296!R1!MSW-E.doc [2011, September 2]

[47] J. H. James, B. Chen and L. Garrison, "Implementing VoIP: A Voice Transmission Performance Progress Report," IEEE Communications Magazine, vol. 42, no. 7, pp 36-41, July, 2004.

[48] M. Tacca, K. Wu, A.Fumagalli and J. Vasseur, "Local Detection and Recovery from Multi-Failure Patterns in MPLS-TE Networks," IEEE International Conference on Communications (ICC), 658-663, June, 2006.

[49] J. Zhang, J. Zhou, J. Ren and B. Wang, "A LDP Fast Protection Switching Scheme for Concurrent Multiple Failures in MPLS Network," International Conference on Multimedia Information Networking and Security (MINES), 259-262, 18-20 November, 2009.

APPENDICES

[1] Project Proposal

[2] SATNAC 2010 Work in Progress Paper

[3] Contents of CD

1. Thesis in PDF Format
2. Project Proposal in PDF Format
3. SATNAC 2010 Work in Progress Paper in PDF Format
4. OPNET V14.0 Simulation Files:

OPNET Project File Name: MSC Thesis_Service Protection in MPLS Network.prj

(i) QoP of Path protection, Fast Reroute and no MPLS Protection Scenario Files

a. Path protection Link Failure
b. Path Protection Node Failure
c. Fast Reroute Link Failure
d. Fast Reroute Node Failure
e. No Protection Link Failure
f. No Protection Node Failure

(ii) Russian Dolls Model and Preemption Scenario Files

a. RDM and Preemption without voice LSP Run 1
b. RDM and Preemption all LSPs Run 2
c. RDM and Preemption all LSPs Run 3
d. RDM and Preemption all LSPs Run 4
e. RDM and no Preemption all LSPs Run 2
f. RDM and no Preemption all LSPs Run 4

(iii) Fast Reroute with Russian Dolls Model and Preemption Scenario Files

a. RDM and Preemption and Fast Reroute before Failure
b. RDM and no Preemption Fast Reroute
c. RDM and Preemption Fast Reroute

Real-time Bandwidth Encapsulation for IP/MPLS Protection Switching

Mampi Lubasi
Department of Electrical Engineering
University of Cape Town, Private Bag X3, Rondebosch 7701, South Africa
Email: mampi.lubasi@uct.ac.za

Abstract- MPLS fast reroute achieves fast protection switching times ideal for the recovery of real-time multimedia traffic. The study proposes to guarantee real-time protection of multimedia traffic by adapting the Russian Dolls Bandwidth Constraints Model to allocate bandwidth to multimedia traffic. The Quality of Protection (QoP) parameters that will be investigated are protection switching time and the bandwidth protection amount.

Index Terms—Bandwidth Encapsulation, Fast reroute, IP/MPLS, Protection Switching

I. INTRODUCTION

IP/MPLS Communication Networks continue to experience an increase in real-time multimedia applications such as Voice over IP (VOIP) and IPTV. Real-time multimedia applications have stringent quality of service (QoS) requirements with regard to delay, jitter, bandwidth and availability [1]. These applications must therefore be provided with prompt recovery during network failures.

In an IP backbone 10% of failures last longer than 20 minutes, 40% last between one minute and 20 minutes, 50% last less than one minute [2]. These failures are caused by factors such as fiber cuts, equipment failures, software problems and maintenance operations. The occurrence of these failures makes it necessary to have mechanisms to recover or protect real-time multimedia traffic during failure conditions. Service protection or network resilience is therefore a vital attribute in communication networks. Service protection guarantees that a network is able to maintain an acceptable level of service during network failures. Quick fault detection and fast switching of traffic to an alternative or backup path is important. Resources in particular, bandwidth, must be available to accommodate this traffic during failure conditions.

This research is aimed at providing real-time protection to multimedia traffic in an IP/MPLS network. An important factor in MPLS network resilience is the quality of Protection (QoP). QoP may be defined as the effectiveness of the failure handling. Two important QoP parameters [3] are protection switching time and bandwidth protection amount. These are the two parameters that will be investigated in this study.

The rest of this paper is organized as follows: Section II discusses MPLS recovery mechanisms. Section III discusses real-time service protection and how it will be achieved in this research. Section IV is the conclusion.

II. MPLS RECOVERY

Multiprotocol label switching (MPLS) recovery mechanisms [4] may be divided into restoration also known as rerouting and protection switching . In restoration, a backup path is established when a failure occurs. In protection switching, the backup path is pre-planned and fully signaled before the failure occurs. Restoration has longer recovery times but is more flexible in the recovery scenarios that it can cover. Protection switching achieves fast recovery and is therefore suitable for the protection of real-time multimedia traffic.

Protection switching mechanisms are divided into global protection and local protection [5].

A. Global Protection

Global Protection is also known as Path Protection. In global protection, when a node or link fails, the entire path from source to destination is bypassed when the backup path is established. The recovery time is hence longer in global protection.

Variants of global protection include 1+1 protection and 1:1 protection. In 1+1 protection, there is one dedicated backup path to protect one primary or working path. Resources on the backup path are dedicated to the protection of the working path and may not be used for anything else. 1+1 protection is efficient and achieves fast recovery times but is expensive in terms of bandwidth usage. In 1:1 protection, there is one dedicated backup path protecting one working path. Low priority traffic may be carried on the backup path. When a failure occurs on the primary path, the low priority traffic is pre-empted from the backup path to accommodate the high priority traffic from the working path. 1:1 protection can be extended to 1:N protection and M:N protection. In 1:N protection, one working path is protected by N backup paths. In M:N protection M working paths are protected by N backup paths.

B. Local Protection

Local Protection is also known as Fast Reroute. In MPLS fast reroute only the failed network elements are bypassed. When a link or node fails, the label switched path (LSP) is rerouted by the upstream node known as the point of local repair (PLR) and terminates at the node known as the merge point (MP). Recovery is done as close to the failed network element as possible. Two techniques for local protection are one-to-one backup and facility backup also known as many-to-one.

Local protection achieves fast recovery times hence is ideal for the protection of real-time multimedia traffic. Real time applications like VOIP must be recovered within 50ms. If the Voice packets do not arrive within 50ms there will be gaps in the conversation. Hence real-time protection must be provided to prevent conversation gaps and reduce packet loss. The protection switching time therefore plays an important role in real-time protection of multimedia traffic. A shorter protection switching time will minimize the time during which traffic is lost.

Figure 1 shows a primary LSP A→B→C→D carrying VOIP traffic. When a failure occurs on the link B→C, node B redirects the VOIP packets onto the backup detour LSP B→E→F→C. In order to do this, the point of local repair (PLR) node B detects the fault and sends the fault indication signal. When the detour path is established, the restoration signal is sent by the Merge point (MP) node C and traffic is redirected on to the detour path. Recovery of the VOIP data takes place within 50ms thus reducing the delay which would lead to gaps in the conversation and packet loss.

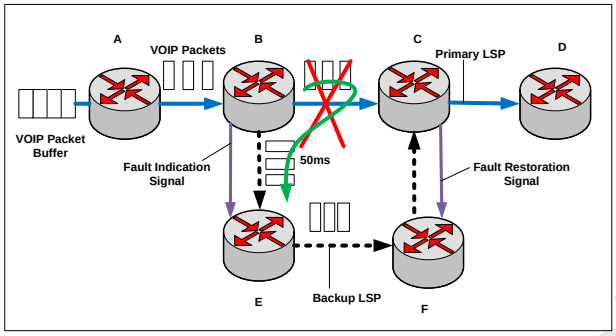

Figure 1: MPLS fast rerouting for real-time protection

III. REAL-TIME SERVICE PROTECTION

Guaranteeing real-time protection of multimedia traffic requires a network to be aware of different classes of traffic. Differentiated services-aware MPLS Traffic Engineering (DS-TE) [6] allows MPLS to be aware of different classes of service. This allows for bandwidth allocation and recovery on a per-class basis.

DS-TE bandwidth constraint models play an important role in determining the bandwidth allocated to traffic classes in an IP/MPLS network. Among the bandwidth constraints models defined is the Russian Dolls Model (RDM) [7].
RDM provides efficient bandwidth usage through sharing of unused bandwidth. This process is called Bandwidth Encapsulation. Pre-emption must be used in order to guarantee bandwidth to a class type as RDM does not provide isolation among the different class types. This research will focus on RDM due to its efficient bandwidth usage.

In order to guarantee bandwidth protection, bandwidth must be reserved on backup paths. Bandwidth protection guarantees that there is enough bandwidth on the protection path to ensure that there is no QoS degradation of the protection traffic.

To achieve real time protection bandwidth must be allocated to multimedia traffic at the time of failure. The protection traffic must be switched onto the backup LSP within 50ms.

In a related work, Yao et al [8] proposed a bandwidth management scheme that allows for bandwidth sharing among backup paths of different service label switched paths thus minimising the protection bandwidth.

An IP/MPLS network will be simulated using OPNET simulation software. Real time service protection will be provided for single link and node failures using MPLS fast reroute. The Russian Dolls Model will be adapted to provide real-time bandwidth allocation for the protection of multimedia traffic when a failure occurs. Pre-emption of low priority best effort traffic will be done to ensure there is enough bandwidth allocated to multimedia traffic. The aim is to achieve fast protection switching times and achieve efficient bandwidth usage.

Bandwidth allocation has been chosen because there must be available bandwidth to accommodate protection traffic during failure conditions. Therefore if real-time allocation of bandwidth is done at the time when a failure occurs, service protection is guaranteed.

IV. CONCLUSION

Service providers are faced with the challenge of providing high availability and reliable services to customers in accordance with service level agreements. End users require guarantee that their multimedia and critical applications will be protected during failure conditions. The solution proposed by this research will prove the consistency and merits of these network resilience approaches and will therefore be very useful.

V. REFERENCES

[1] M. Hayasaka & T. Miki, 'Seamless Failure Recovery for Real-time Premium Traffic in MPLS Networks.' 4th IEEE Consumer Communications and Networking Conference. 121-340. Las Vegas, January 11-13, 2007.

[2] G. Iannaccone, C.Chuah, R. Mortier, S.Bhattacharyya & C. Diot, 'Analysis of Link failures in an IP Backbone.' Proceedings of the 2nd ACM SIGCOMM workshop on Internet Measurement. 237-242. Marseille, November 6-8 2002.

[3] J.A. Zubairi, 'Current Practices for MPLS Protection.' International Symposium on High Capacity Optical Networks and Enabling Technologies. 1-5. Dubai, November 18-20, 2007.

[4] V.Sharma & F. Hellstarnd, Framework for Multi-protocol Label Switching (MLS)- based Recovery, IETF RFC 3469, February 2003.

[5] B. Davie & A. Farrel, MPLS: Next Steps, Massachusetts: Morgan Kaufmann Publishers, pp 165-175. 2008.

[6] F. Le Faucheur & W. Lai, Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering, IETF RFC 3564, July 2003.

[7] F. Le Faucheur, Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering, IETF RFC 4127, June 2005

[8] Y. Yao, Y. Zhang, C. Lu, Z. Zhang, Y. Zhao & W. Gu, 'An Efficient Shared-Bandwidth Reservation Strategy for MPLS Fast Reroute.' 1st International Conference on Information Science and Engineering. 1644-1647. Nanjing, December 26-28, 2009.

Mampi Lubasi received her BSC (Computer Science) degree in 2001 from Copperbelt University, Zambia and is presently studying towards her Master of Engineering (Telecommunications) degree at the University of Cape Town. Her research interests are in network resilience and MPLS networks.

SERVICE PROTECTION IN IP/MPLS NETWORKS

PROJECT PROPOSAL

MAMPI LUBASI

LBSMAM003

PREPARED FOR DR ALEXANDRU MURGU

DATE: MAY 10, 2010

Table of Contents

CHAPTER 1: INTRODUCTION

1.1 Background

IP/MPLS Communication networks today are experiencing an increase in multimedia traffic. Multimedia applications have stringent quality of service (QoS) requirements with regard to delay, bandwidth and availability. These applications must therefore be provided with prompt and efficient recovery from network failures [1].

In an IP backbone [2], 10% of failures last longer than 20 minutes, 40% of failures last between one minute and 20 minutes, and 50 % of failures last less than a minute. These network failures are caused by fiber cuts, equipment failures/upgrades, router reboots, software problems and maintenance operations. Network resilience or service protection is therefore an important attribute in communication networks. Network resilience is the ability of a network to maintain an acceptable level of service during network failures. A resilient network [3] must have:

- Intelligence for rapid detection and localization of failures as well as switching of affected services onto alternative paths.
- Enough resources (bandwidth) to accommodate user traffic during failure conditions.

1.2 Research Definition

As part of contributing to the study of communication networks, this research focuses on service protection in IP/MPLS networks. The focus will be on guaranteeing real-time quality of protection (QoP) for multimedia traffic. QoP can be defined as the effectiveness of the failure handling [4]. The QoP parameters [5] that are used to evaluate the performance of MPLS based recovery schemes include recovery time, packet loss, backup capacity (bandwidth), additive latency and state overhead. As the number of recovery paths grows the information in the individual network elements

also grows. This is what the state overhead refers to. The research will focus on the protection switching time and the protection bandwidth amount.

1.3 Outline of Proposal

The proposal is organized into 6 chapters. Chapter 1 is an introduction to service protection (network resilience) and the research. Chapter 2 gives an overview of MPLS recovery mechanisms. Chapter 3 gives an overview of the three IETF Bandwidth constraint models. Chapter 4 defines the research problem, hypotheses, key questions and objectives. Chapter 5 gives the methodology of how the project will be achieved and the timeline. Chapter 6 is dedicated to the conclusions formulation.

CHAPTER 2: MPLS RECOVERY MECHANISMS

2.1 MPLS Recovery Mechanisms

This chapter gives an overview of MPLS recovery mechanisms.

MPLS recovery is preferred to conventional IP rerouting methods because IP rerouting may be too slow to meet the recovery time of real time traffic. IP rerouting is also not able to provide bandwidth protection to specific traffic flows.

Recovery mechanisms in MPLS can be classified as protection switching and restoration. In protection switching, the backup path is preplanned and fully signaled before a failure occurs. In restoration, a backup path may be preplanned or dynamically allocated, however additional signaling will be required to establish the backup path when a failure occurs. Protection switching has the advantage of fast recovery times. Restoration is more flexible in terms of the failure scenarios that it can recover from. Therefore to achieve fast recovery of protection traffic, protection switching is preferred.

Protection switching mechanisms can be classified as global protection and local protection.

2.1.1 Global Protection

Global protection is also known as path protection. In path protection, when a link or node failure occurs, the entire path from source to destination is bypassed. Global recovery has slower recovery times compared to Local protection. There are several variants of path protection [6] as discussed in the next section:

a) 1+1 Protection

In 1+1 protection, there is one dedicated backup path to protect the working path. Resources on the backup path are dedicated to the protection of the working path and

may not be used for anything else. 1+1 protection achieves fast recovery times, however it is expensive to implement due to high bandwidth usage.

b) 1:1 Protection

In 1: 1 protection, there is one backup path to protect the working path. Low priority traffic may be carried on the backup path. When a failure occurs, the low priority traffic is pre-empted or dropped from the recovery path to accommodate the high priority traffic to be protected.

1:1 protection can be extended to 1: N protection and M: N protection. 1: N protection has 1 working path protected by N number of backup paths. M: N protection has M number of working paths protected by N number of paths.

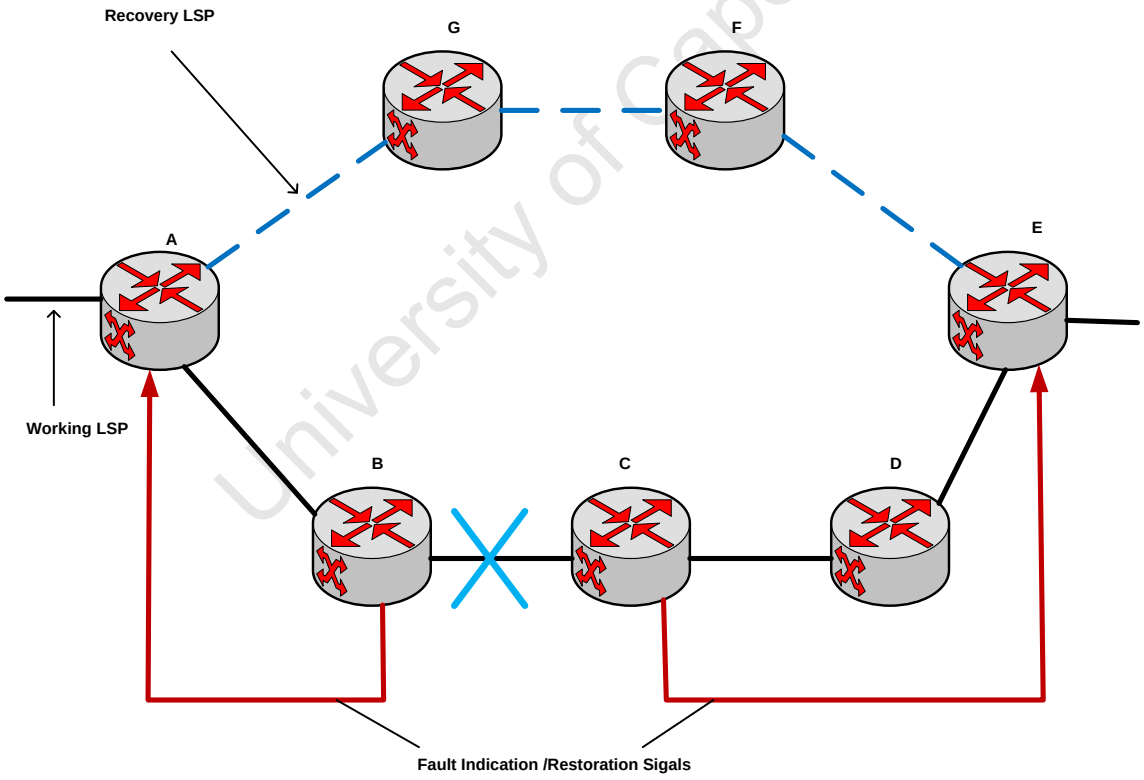

Figure 1: Path protection

Figure 1 shows an example of path protection. The LSP A→B→C→D→E is protected by the LSP A→G→F→E. When the link B→C fails, the entire path is avoided and traffic is redirected onto the path A→G→F→E. Nodes A and E receive the fault indication/notification signals and trigger/coordinate the switch over and switchback processes.

2.1.2 Local Protection

The term Fast reroute is used to refer to local protection. When a node or link failure occurs, the LSP is rerouted by the node that is upstream to the failed network element. This node is called the point of local repair (PLR). The LSP is rerouted at the upstream node closest to the failure. In local protection only the failed network elements are bypassed. In local protection the backup LSPs are set up before a failure occurs. Two techniques for local protection exist and these are one-to-one backup and facility backup. When a backup LSP terminates at the PLR's next hop neighbor, the backup LSP is known as a next-hop (NHOP) backup tunnel. If the backup LSP terminates at the neighbor of the PLR's neighour it is known as a next-next-hop backup tunnel. The node where the backup tunnel terminates is known as the merge point (MP). This is where the backup tunnel rejoins the path of the protected LSP. There are two methods [7] used for local protection and these are one-to-one backup and facility backup.

Local protection achieves fast recovery times hence is ideal for the protection of multi-media traffic which is sensitive to loss and delay. For this reason the research will focus on local protection.

a) One-to-One Backup

In One-to-One backup a backup tunnel is established for each protected LSP. The backup tunnel is known as a detour. To protect an LSP that traverses N nodes, there could be as many as (N-1) detours

In Figure 2, the LSP A→B→C→D→E is protected by the backup tunnel B→F→G→D if node C or the link B→C fails. The LSP H→B→C→D→J is protected by the backup tunnel B→I→D.

b) Facility Backup

In Facility backup, a backup tunnel can protect a set of LSPs. The backup tunnel established is known as bypass. Similarly, there can be (N -1) bypass tunnels to protect an LSP that traverses N nodes. When an NHOP backup tunnel is used this is referred to as link protection and when an NNHOP backup tunnel is used, this is referred to as node protection.

In Figure 4, one NNHOP bypass tunnel is configured on node B to protect the LSPs A→B→C→D→E and H→B→C→D→I from a failure of node C and the link B→C.

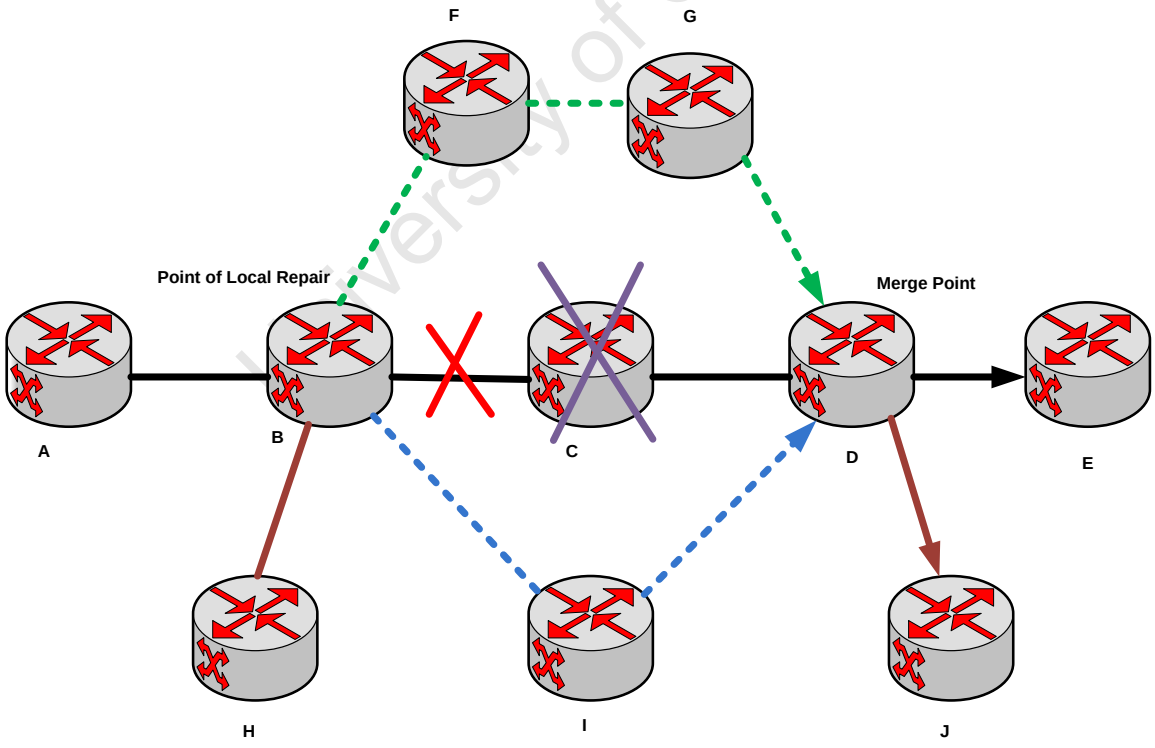

Figure 2: One-to-one backup

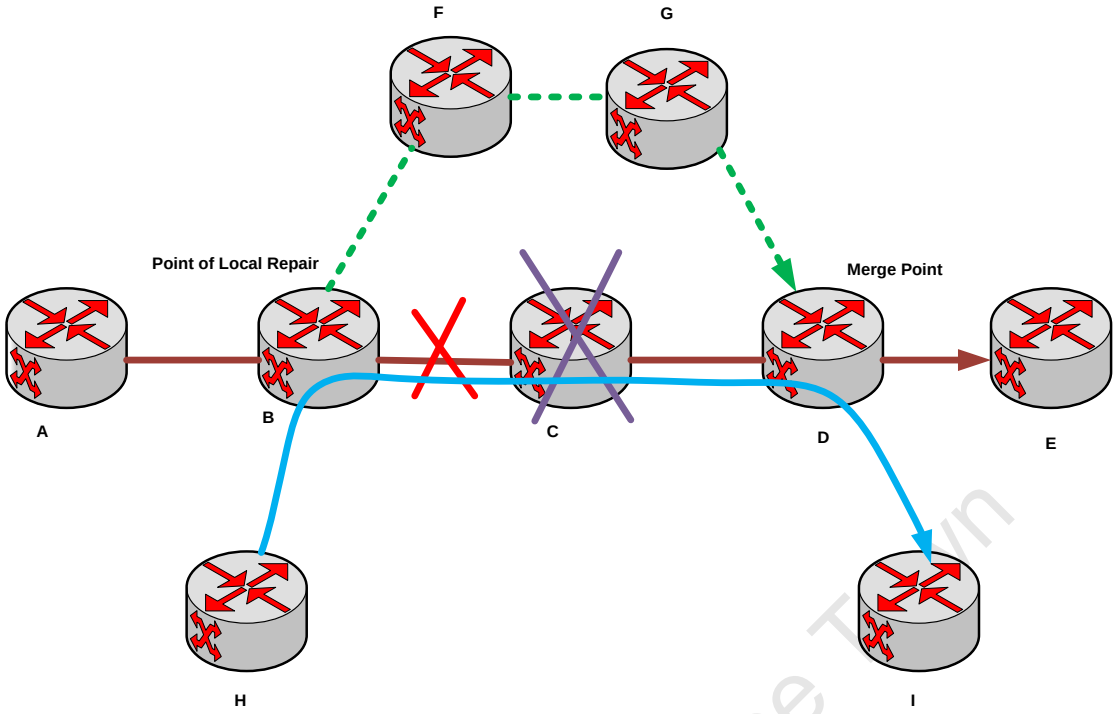

Figure 3: Facility Backup

CHAPTER 3: BANDWIDTH CONSTRAINT MODELS

3.1Bandwidth Allocation

This chapter gives an overview of the bandwidth constraint models that determine the allocation of bandwidth to a traffic class on a link.

Diffserv aware MPLS traffic engineering allows for bandwidth reservation based on class types. Bandwidth constraint models play an important role in determining how bandwidth is allocated to the different classes of traffic. A bandwidth constraint is the amount of bandwidth that a class type or a group of class types is allocated. The bandwidth constraint model defines the relationship between the class types and the bandwidth constraints.

A class type C, is defined as a set of traffic trunks crossing a link and is governed by a set of bandwidth constraints. The reserved bandwidth, R_i for a given class *i* is the total bandwidth reserved by the established LSPs. IETF defines 3 Bandwidth constraint models and these are:

3.1.1 Maximum Allocation Model (MAM)

MAM [8] is defined as:

i. The Maximum number of class types C = Maximum number of bandwidth constraints, MaxBC =8

   Therefore C = MaxBC =8

ii. For each class type C_i,
   $R \leq BC_i \leq M$, where M is the Maximum reservable bandwidth

iii.

iv.

The benefit of MAM is that it isolates the traffic classes and guarantees bandwidth to the traffic classes without the need for pre-emption. The drawback of MAM is that it wastes bandwidth since it does not allow sharing unused bandwidth.

3.1.2 Russian Dolls Model

The Russian dolls model [9] is defined as follows:

i. The Maximum number of class types C = Maximum number of bandwidth constraints, MaxBC =8

   Therefore C = MaxBC =8

ii. For $0 \leq j \leq C$

   Where $j \leq i \leq C$

iii. BC0 = M, where M= Maximum reservable bandwidth

The advantage of RDM is that it provides efficient bandwidth usage through sharing. The drawback is that it does not provide isolation among the different class types and pre-emption must be used to guarantee bandwidth to each class type.

3.1.3 Maximum Allocation with Reservation (MAR)

MAR [10] is similar to MAM except that class types are allowed to exceed their allocated bandwidth in no congestion conditions and revert to their allocations when congestion and overload occur.

This research will adapt the Russian Dolls model for bandwidth allocation to achieve real-time protection of multimedia traffic.

CHAPTER 4: RESEARCH AREA

4.1 Research Aspects

The key aspects regarding bandwidth in service protection relate to:

- Determining the reserve bandwidth to guarantee protection
- Selection of backup paths to ensure efficient bandwidth utilisation
- Allocation of bandwidth to traffic classes to guarantee protection of high priority (multimedia) traffic

4.2 Problem Statement

- Multimedia traffic is sensitive to loss and delay. The challenge is to recover the data upon failure within the shortest possible time that will not degrade the quality of service of the traffic, for example VOIP traffic must be recovered within 50ms. Another challenge is to have sufficient bandwidth allocated for the real time protection of the multimedia traffic.

4.3 Hypotheses

The hypotheses for the research are as follows:

- Bandwidth allocation and pre-emption can guarantee real-time protection of multimedia traffic and fast protection switching times.
- Backup path selection determines bandwidth utilization and protection switching times.

4.4 Research Questions

The key questions for this research are:

- How does bandwidth allocation to backup paths and traffic classes affect protection switching time and bandwidth usage?
- How can backup path selection achieve efficient bandwidth utilisation and fast protection switching times?
- How does pre-emption affect bandwidth allocation to multimedia traffic and protection switching times?

4.5 Research Objectives

The objectives of the research are therefore:

- To investigate how MPLS fast reroute (local protection) techniques handle single link and node failures.
- To investigate bandwidth allocation to backup links and traffic classes to guarantee real-time protection of multimedia traffic and efficient bandwidth utilisation.
- To investigate the effect of pre-emption on bandwidth allocation, bandwidth utilization and the protection switching times.
- To develop a bandwidth allocation scheme that will guarantee real-time protection of multimedia traffic and fast protection switching times from single link and node failures.

CHAPTER 5: METHODOLOGY AND TIMELINE

5.1 Methodology

The methodology of the research will be as follows:

- **Simulation of Network Environment**

  It is necessary to simulate an IP/MPLS network where observations will be made. A number of software simulation tools are available for simulation of various types of networks. OPNET simulation software will be used to simulate the IP/MPLS network as it has an MPLS module with the required functionality. Familiarisation with this tool is vital before simulating the environment.

- **Simulation of Failure Scenarios**

  Single Link and node failures will be introduced into the simulated IP/MPLS network and observations will be made.

  - The two fast reroute techniques will be observed on how they handle link and node failures.
  - The protection switching times and bandwidth utilisation will be observed in both scenarios.

- **Adaptation of Russian Dolls Model for network resilience.**

  The allocation of bandwidth to the different classes will be done based on the Russian Dolls Model. The following scenarios will be simulated:

  - Bandwidth allocation will be made without pre-emption and observations will be made on how this affects real time traffic protection.
  - Bandwidth allocation will be made with pre-emption and observations will be made
  - Reserve bandwidth will be determined and link allocations. Observations will be made on the bandwidth utilization and protection switching times.

- **Comparison with existing works will be used as a benchmark to validate results obtained.**

- **Draw Conclusions**

  Based on the findings conclusions will be made.

  - The results will prove whether pre-emption aids in guaranteeing bandwidth to real time traffic or not.
  - The results must show how backup path selection should be done to ensure efficient resource utilisation.
  - The results must also show the developed bandwidth allocation scheme to guarantee protection to real time traffic and achieve fast protection switching times.

5.2 Timeline

A timeline within which the project must be completed is required. The table and the figure below list the tasks to be carried out and the time in which to complete them.

Table 1: Project Timeline

No.	Task	Period	Duration
1	Literature Review	October - April	7 months
2	Familiarity with OPNET	May	1 month
3	Simulations	June - September	4 months
4	Analysis of Results & Conclusions	October	1 month
5	Thesis write-up	September - December	4 months

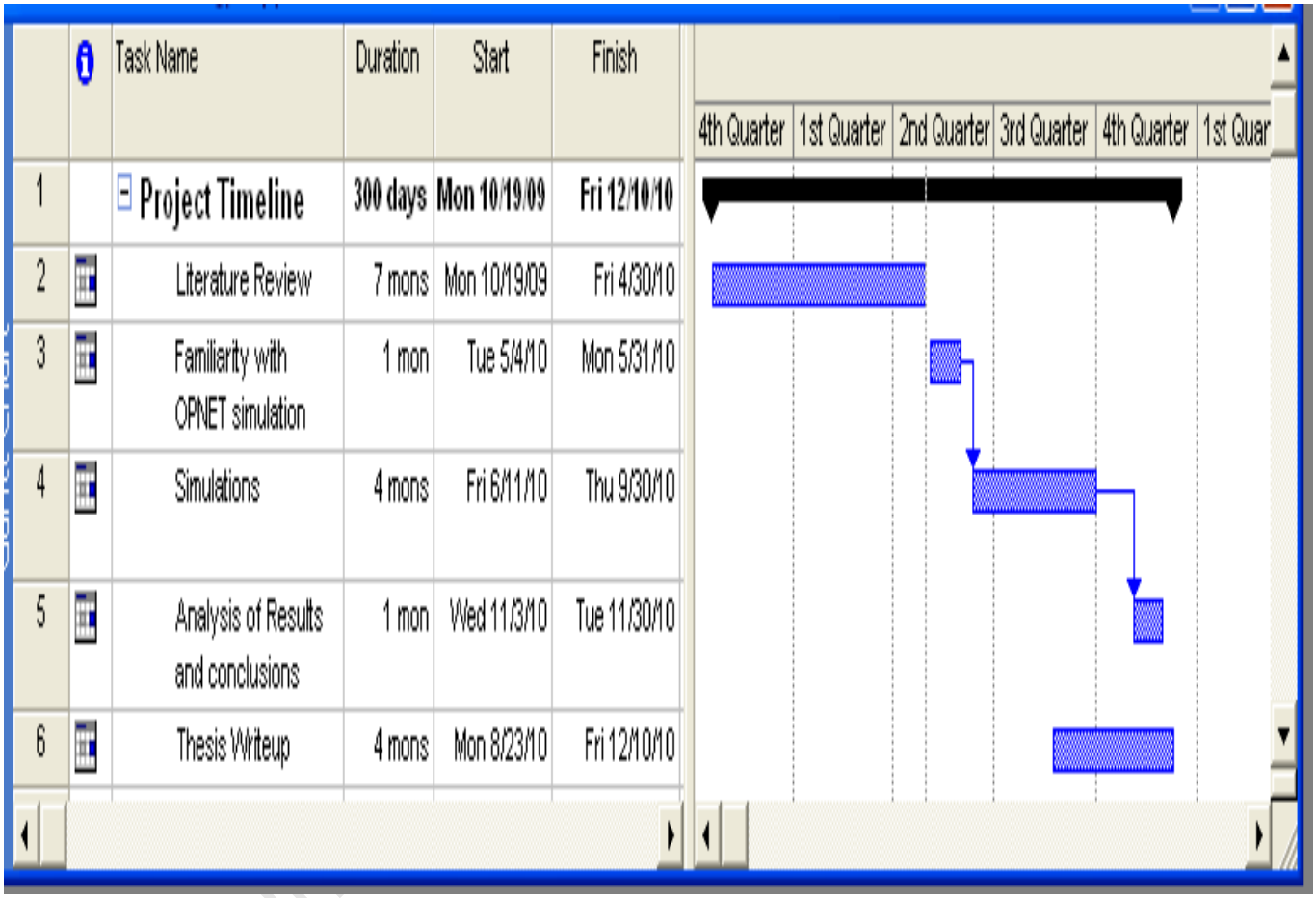

Figure 4: Project schedule

CHAPTER 6: CONCLUSION

In conclusion, undertaking this research will provide a solution for achieving network resilience or service protection with efficient bandwidth utilization. Service providers are faced with the challenge of providing reliable network services to the end user with high availability. Solutions such as the one the research will provide would therefore be useful.

REFERENCES

[1] M. Hayasaka & T. Miki, "Seamless Failure Recovery for Real-time Premium Traffic in MPLS Networks," 4th IEEE Consumer Communications and Networking Conference, 121-125, January, 2007.

[2] G. Iannaccone, C. Chuah, R. Mortier, S. Bhattacharyya & C. Diot, "Analysis of Link Failures in an IP Backbone," Proceedings of the 2nd ACM SIGCOMM Workshop on International Measurement," 2002. Available: http://dl.acm.org [2011, April, 29]

[3] B. Davie & A. Farrel, "MPLS: Next Steps," Massachusetts: Morgan Kaufmann Publishers, p 261. 2008.

[4] J. Zubairi, "Current Practices for MPLS Protection," International Symposium on High Capacity Optical Networks and Enabling Technologies (HONET), 1-5, November, 18-20, 2007.

[5] V. Sharma & F. Hellstarnd, Framework for Multi-Protocol Label Switching (MPLS) - Based Recovery (RFC 3469]. Available at: http://www.ietf.org/rfc/rfc3469.txt [2010, April 28].

[6] J. Vasseur, M. Pickavet, P. Demeester, "Network Recovery: Protection and Restoration of Optical, Sonet-SDH, IP and MPLS," California: Morgan Kaufmann, p 31. 2004.

[7] B. Davie & A. Farrel, "MPLS: Next Steps," Massachusetts: Morgan Kaufmann Publishers, pp 173-176. 2008.

[8] F. Le Faucheur & W. Lai, "Maximum Allocation Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering," RFC 4125, June, 2005.

[9] F. Faucheur, "Russian Dolls Bandwidth Constraints Model for Diffserv-aware MPLS Traffic Engineering, "RFC 4125, 2005.