# 9

# CONCLUSIONS AND FUTURE WORK

This chapter concludes the thesis with a summary of the contributions of our research and proposes several topics that should be considered by future work.

## 9.1 CONCLUSIONS

The objectives set out for this thesis have been achieved. This thesis was aimed to develop mechanisms capable of providing a reliable and fast restoration from network component failure in an MPLS-based network for multimedia streaming with strict real time requirements in a better way than existing proposals in order to guarantee service continuity.

The main contributions are summarized in the following paragraphs.

- **Fast rerouting mechanism**. As we discuss throughout this thesis, the main drawback of MPLS technology, as a connection-oriented architecture, is its slow response time from network component failure due to the time needed to establish a new LSP to carry the affected traffic.

  Link failures are a common cause of service disruption in computer networks. Failures in high capacity links or between backbone routers, may seriously affect multimedia streaming and strict real-time application services and protocols. To alleviate this problem the Fast Rerouting approach was adopted as a solution.

  Fast Rerouting relies on pre-planning and requires that a backup LSP be computed, advertised and setup before a link failure is detected. The backup LSP combined with local repair aims to minimize packet losses during the restoration period. We presented an enhanced Fast Rerouting mechanism for MPLS-based networks which reroutes traffic over a backup LSP when a link/node of the protected LSP fails. The goal is to provide quality of service for the traffic carried by the protected LSP, even in case of failure and during recovery, until it is rerouted. Non-protected LSPs may be rerouted but without guarantees (best effort). Our proposal performs better compared to previous proposals in terms of both packet delay and packet disorder. We provide a simple and concise novel algorithm in the intermediate LSRs that operates in a distributed manner, introducing additional functionality to avoid packet re-ordering and to reduce unnecessary additional delay.

  The proposed mechanism can be used for quality of service (QoS) provision. This is possible because the algorithm is capable of handling criteria other than link failure detection for its activation. Once a given LSR detects congestion or a situation that leads to a Service Level Agreement (SLA) or QoS agreement being violated, it may start a fast reroute of a protected LSP. To extend our mechanism to the congestion problem, only a guarantee that the LSR is aware of the congestion problem is needed. Just as in the case of a link fault, the flow can be diverted to an alternative LSP once the congestion situation is detected.

  The proposed algorithm has been evaluated through simulation and the results have shown an improvement in the average latency or average packet delay. The

proposal eliminates packet re-ordering, improving end-to-end performance (overall performance), and has a shorter restoration period (i.e., fast network resources release) compared to Haskin's proposal.

The results of this work were published in the proceedings of the IEEE International Conference on Computer Communications and Networks (I3CN'01), October, 2001 [HD01].

- **Reliable and Fast Rerouting (RFR) mechanism**. This proposal addresses the packet loss issue during network component failure, which remains unsolved and affects the performance of fast rerouting mechanisms as well as our enhanced fast rerouting mechanism presented before. The parameters that affect the performance of any recovery scheme are traffic recovery delay (Full Restoration Time), packet disorder, and packet losses. In the previous proposal we addressed the first two issues.

  The main idea of RFR is to try to find solutions to the problem of packet losses during the failure, more precisely lost packets on the protected LSP. Up to now, packet loss due to node or link failure was considered to be "inevitable". It has always been assumed that the transport layer would somehow take care of the retransmission of lost packets through transmission control protocol (TCP). Our main interest is to protect multimedia and realtime traffic that usually do not benefit from retransmission. Furthermore, we have observed that the retransmission process due to packet loss significantly affects the throughput of TCP traffic due to the startup behavior (slow-start) of TCP. For this reason, critical services (premium traffic) will be affected by packet losses and, for TCP traffic, lost packets trigger retransmission requests, and hence the gains due to the decrease in restoration time achieved by previous the proposal (fast rerouting mechanism) may become negligible. As a consequence, bad performance and degraded service delivery will be experienced and QoS parameters will be seriously affected during the restoration period.

  The RFR mechanism proposes a novel recovery algorithm with small local buffers in each LSR node within the protected path to provide some preventive action against the packet loss problem by storing a copy of the packets in order to elim-

inate *packet loss* due to link/node failure. This buffer is also used to avoid *packet disorder* during the restoration period. This results in a significant throughput improvement for premium traffic.

In this proposal we eliminate packet losses while maintaining the benefits of our previous proposal, making link failures unnoticeable to all end users.

*** Buffer requirement analysis for RFR**. As our mechanism introduces an additional buffer requirement, for the proper operation of the proposal it is important to know the required additional buffer size, especially in the ingress LSR (i.e., ingress buffer). For this purpose and to validate the simulation results, we did an analytical study of buffer requirements and recovery times to justify the additional cost of the buffers that our proposal introduces. The results demonstrate that the buffer requirement is within a justifiable range compared to the benefit gained in network survivability and QoS guarantee for protected traffic.

The results of this work were published in the proceedings of the IEEE GLOBECOM'02, November, 2002 [HD02d].

- Although TCP traffic is not the main aim of this thesis, the RFR proposal was also evaluated for TCP traffic. The simulation results show that the RFR proposal gives support even for traffic using reliable transport protocols (TCP).

  Because RFR avoids packet losses and packet disorder for the protected flows, TCP connections experience neither losses nor disordered packets and may run at the maximum throughput even during the restoration period of the protected LSP.

  The results of this work were published in the proceedings of the IEEE International Conference on Networking (ICN'02), August, 2002 [HD02a].

- **Multiple fault tolerance**. In this work we extend our proposal from single link/node failure tolerance to multiple link/node failures on a protected LSP. The main idea presented in this proposal is the combination of existing proposals: segment protection, path protection and local repair. The significant change is made by the incorporation of the segment protection scheme. This allows the restoration of the failure to take place closer to the point of failure.

As the length of the protection path is a main quantitative measure of the quality of a protection scheme, the protection path length is used as an indication of the delay that the rerouted traffic will experience after a link failure. In addition to the delay, the length of the protection path reflects the amount of resources required to protect an LSP.

The simulation results show a significant reduction of the protection path length by merging the alternative LSP made by the local restoration decision in each segment protection domain, into the alternative LSP used for global restoration in the entire MPLS domain. This improves the main disadvantage of local restoration schemes.

Furthermore, rerouting of traffic is performed close to the failure point, increasing the restoration speed. In consequence, the proposed scheme provides a significant reduction of the LSP blocking problem. At the same time it provides better recovery (protection) in terms of path length. As a result, we achieve better network resource utilization and less delay for the rerouted traffic.

Finally, the proposed mechanism improves the main disadvantage of the previous proposals, packet loss in Makam's scheme and packet reordering in Haskin's scheme. Thereby the combined approach gives a better restoration mechanism than either of the mechanisms applied separately.

- **Optimal and Guaranteed LSP**. One of the main disadvantages of using the fast rerouting (preplanned) schemes is that the preplanned alternative LSP established at the time the protected LSP was set up may become a non-optimal alternative path after the occurrence of failure. For this reason a *dynamic and fast rerouting hybrid* approach was proposed. The proposal gains the advantages of both schemes: fast restoration time from the fast rerouting scheme by rerouting the affected traffic to the preplanned alternative LSP and the use of the possible optimal alternative path, if one exists, by using the dynamic restoration scheme. Note that the time that the dynamic scheme process takes to find the new alternative using the current network information does not affect the restoration time because the protected traffic is immediately rerouted using the fast rerouting mechanism.

The other problem that we address in this proposal is related to vulnerability. This problem appears when the preplanned alternative LSP is converted to the new protected LSP carrying the rerouted traffic on it and it is not protected from further failures. To give a solution to this, we compute a new alternative LSP. Then it is compared with the alternative LSP that is being used currently by the protected traffic. If the new alternative is "better", in terms of path length, then it is considered to be the new protected LSP and the traffic is rerouted through it. The previous alternative LSP remains as alternative LSP.

This method provides a guarantee of an alternative LSP at any time for the protected LSP, avoiding the vulnerability problem for the protection path.

The results of this work have been presented in a paper submitted for an international conference. At the time of writing this dissertation the reviewing process is not yet finished. [HD02c].

- **Adaptive LSP**. MPLS provides an integrated approach to traffic engineering, but it lacks flexibility due to its connection-oriented forwarding behavior. Long duration LSP connections may suffer from non-optimal resource utilization due to the fact that at setup the load of the network forced a non-optimal route. This affects interactive multimedia flows and delay-sensitive applications due to long end-to-end delays along the LSP.

  The proposed adaptive LSP, composed of a bandwidth threshold and released LSP procedures, allows more flexibility in network resource allocation and utilization by adapting the LSP to variations in the overall network load. The release of an LSP frees allocated bandwidth that may be used to update a non-optimal LSP. The mechanism is based on monitoring both a significant decrement of aggregated traffic on the established non-optimal LSP and the release of any LSP in the network. The adaptation is based on two aspects: dynamic bandwidth management for an LSP and rerouting traffic from a non-optimal LSP to an optimal one.

The preliminary results in this mechanism show an improvement of network resource utilization while reducing end-to-end delay and minimizing traffic blocking problems when setting up a new LSP.

The results of this work have been presented in a paper submitted for an international conference. At the time of writing this dissertation the reviewing process is not yet finished. [HD02b].

## 9.2 FUTURE WORK

There are several open issues related to the proposals presented in the PhD thesis that need further study. In the following paragraphs an outline of the immediate future work to be done is presented.

An aspect that requires more study is related to the definition of Segment Protection Domain, (SPD). Besides the administrative decisions (i.e., autonomous systems), some the criteria to determine and define SPDs are needed. The available buffer size and the maximum delay allowed for protected traffic can be used as additional criteria for SPD setup. From the study for buffer requirements at the ingress LSR presented in Chapter 4 we find a tradeoff between the amount of memory at the ingress LSR and the length of the protected LSP. This gives a first approach to the coverage of an SPD. This needs further study in different topologies and traffic characteristics.

Related to the proposed Reliable and Fast Rerouting mechanism, it seems simple to implement in existing devices; however, to determine the feasibility of this proposal it is important to adapt the Label Distribution Protocol (LDP) and the routing protocols to support our mechanism. For this purpose, the implementation of the proposal in a PC-based platform might be useful to observe the real behavior and determine the modifications needed. Furthermore, an analysis of the number of LDP messages required for the setup of the alternative and backup LSP is needed. For this study a simulation platform based on the MPLS Network Simulator (MNS) would suffice.

As we mentioned in Chapter 8, the open issues in adaptive LSP are to determine the threshold value of the aggregated bandwidth, the waiting time, and the frequency of LSP setup, their dependencies, and their results in providing the optimal protected LSP and the aggregated alternative LSP. This evaluation may be performed via simulation using MNS, running simulations for large networks with many LSR and links. Obviously, the best way to determine these values is the use of real MPLS traffic traces from some authoritative sources as input data for the number of LSPs, inter-arrival time for new LSPs, mean duration of LSPs, etc. Unfortunately, these traces are not available at this time.

Finally, we considered in our proposals all protected LSPs on a link as an LSP (aggregated LSPs) to gain scalability and strictly follow the MPLS architecture. The extension of MPLS for optical networks, Generalized Multi-Protocol Label Switching (GMPLS), gives the possibility to carry individual protected LSP per lambda (DWDM). An interesting topic to be considered in the future is the possibility of handling each protected LSP individually, using the fast rerouting mechanism with preplanned alternative LSPs which are disjoint among them. This approach may allow both the benefit of survivability and the possibility of load balancing in the network. At the same time the approach must establish some regulation to balance the tradeoff of advantages between scalability and load balancing.