

Instituto de Engenharia de Sistemas e Computadores de Coimbra
Institute of Systems Engineering and Computers
INESC - Coimbra

Catarina Francisco, Lúcia Martins,
João Redol, Paulo Monteiro

**A previous study on Dynamic Alternative Routing
with Local Protection Paths in MPLS networks**

No.4

2010

ISSN: 1645-2631

Instituto de Engenharia de Sistemas e Computadores de Coimbra
INESC - Coimbra
Rua Antero de Quental, 199; 3000-033 Coimbra; Portugal
www.inescc.pt

A previous study on Dynamic Alternative Routing with Local Protection Paths in MPLS networks

Catarina Francisco^{1,2}, Lúcia Martins^{1,3}, João Redol²,
Paulo Monteiro²

¹ Departamento de Engenharia Electrotécnica e de Computadores
Pólo II da Universidade de Coimbra

Morada: Pinhal de Marrocos, 3030-290 COIMBRA, Portugal

² Nokia Siemens Networks S.A.

Morada: Rua Irmãos Siemens 1, 2720-093 AMADORA, Portugal

³ INESC-Coimbra

Morada: Rua Antero de Quental 199, 3000-033 COIMBRA, Portugal

Email: catarina.francisco@nsn.com, lucia@deec.uc.pt, joao.redol.ext@nsn.com

paulo.1.monteiro@nsn.com

Abstract

MPLS is a core technology for nowadays and future networks, and must meet the needs of real-time applications for which network survivability is critical. Dynamic alternative routing has already been proposed several times to increase MPLS network performance. In this paper, a proposal of a protection scheme to be used with dynamic alternative routing is presented and its performance is evaluated through a simulation study. Our study uses three representative topologies as our test networks in order to understand the impact of these different topologies in our routing algorithm performance.

1 Introduction

Best-effort architecture does not meet the requirements of the current Internet carrying heterogeneous traffic flows. MPLS (Multi Protocol Label Switching) is a backbone technology that takes the best out of both connection-oriented traffic engineering (TE) techniques and packet networks in order to solve one of the main problems in an IP-based network which is the assurance of QoE and QoS in supported services.

On the other hand, some real time services like high-quality video present critical requirements in terms of packet loss and delay and impose a stringent recovery time in case of failure. Traditional restoration mechanism at the IP layer may take seconds and it will allow the users to be aware that a problem has occurred. This failure recovery time is not acceptable even for some applications like VoIP (ITU-T recommends in its standard G.114 that the end-to-end delay for VoIP should be kept below 150 ms to maintain an acceptable conversation quality [16]) and, as such, MPLS will have to use a faster IP independent recovery mechanism.

Network survivability in MPLS Networks can be improved in several ways [9, 24]. One possibility is to enforce path diversity at the time of flow allocation, namely employing diversity constraints, where the volume of traffic is split into more than one path. In fact, in the advent of a failure, there is only a partial loss of end-to-end traffic volume.

However, in the previous strategy, traffic in progress is lost. Traffic rescue can only be accomplished by recovery mechanisms where a pair of link-disjoint paths (primary and backup) are provided between each source and destination and, in the advent of a failure, affected traffic is switched to the backup path. Network restoration establishes backups only after the failure occurs, which is an advantage in terms of bandwidth usage but it incurs setup time delay. On the other hand, protection mechanisms previously establish (not necessarily with bandwidth reservation) both primary and backup paths and, in case of failure, the protection is immediate. A lot of work in these areas has been accomplished [27], namely in global and local approaches [19, 18], bandwidth management [28] and, in case of restoration, fast convergence routing protocols [6, 1].

MPLS was designed to meet the needs of real-time applications and, for that reason, IETF's MPLS working group has developed a local protection mechanism (Fast Reroute - FRR) that provides recovery in SONET time (50 ms). In local protection, it is the node immediately upstream the failing facility that redirects the affected traffic to their backup.

Current MPLS Fast Reroute approaches are either fixed, non-adaptive approaches, or periodically updated optimized approaches. In addition, in order to enable a fast protection mechanism, all approaches usually imply bandwidth reservation which translates into some waste of bandwidth. On the

other hand, current implementations use one backup path (possibly shared) to carry both ongoing and incoming traffic affected by a link failure, which can lead to local congestion in the advent of a failure.

Dynamic alternative routing was widely used in ISDN and has been proposed for optical [23] and MPLS networks in order to improve network performance [22, 26, 21]. Additionally, dynamic alternative routing also improves network survivability because of its ability to reroute traffic in congestion situations [4].

In this work 'alternative route' regards to the second chance route a connection request may have and not to a path backup to save a connection in a failure situation (as often designated in literature).

Here, we present a well-known event-dependent dynamic alternative routing algorithm associated with an adapted scheme for local protection in order to improve network performance also in case of link failure.

1.1 Contents of the Report

In section 2 is presented an overview of principles learned with circuit-switched voice networks that have been extended to MPLS networks. In section 3 are explained the fundamentals of MPLS and its local protection mechanism (Fast Reroute). In section 4 are presented routing algorithms with link protection and a new protection scheme is proposed to be used with dynamic alternative routing. In Section 5 it is presented a network environment for a simulation study in order to compare the previous routing algorithms in terms of network performance, with and without a link failure. Finally, in section 6, conclusions and future work are presented.

2 Dynamic Alternative Routing

Routing policy is one of the key aspects when talking about network performance. In fact, the set of rules that decide how incoming connections are carried throughout the network is very important in terms of the minimization of resources allocation and the fulfillment of connection's QoS requirements.

As mentioned in [3], much of the principles learned with circuit-switched voice networks have been extended to packet switching networks. Therefore, some circuit-switched routing fundamental concepts will be reviewed. Generally, routing methods may be categorized in four types, according to how routing tables are updated: fixed routing (FR), time-dependent routing (TDR), state-dependent routing (SDR) and event-dependent routing (EDR) [2]. In a FR scheme there is a pre-configured route for each pair of nodes in the network, which is maintained on a fixed basis. As such, it is easy to understand that offering no adaptability FR lacks robustness to handle changes in the network. On the other hand, TDR methods update routing tables periodically. However, because routes are computed off-line, TDR is not capable of instantly react to changes in the network. Finally, SDR updates paths

automatically according to network state, and EDR schemes update their routing tables according to whether a connection request succeeds or fails to be established.

As stated in [3], one of the lessons learned with circuit-switching is that EDR should be preferred over SDR (that implies network flooding with state information) to allow scalable networks.

The Dynamic Alternative Routing (DAR) used in this work is one of the simplest and efficient event-dependent routing methods and has been proposed for several network technologies, such as ATM [8], optical [23], IP [17] and MPLS [26, 21].

Opposed to fixed routing which offers no adaptability, dynamic routing has a more flexible behaviour, taking advantage of available bandwidth in certain network areas, when there is congestion elsewhere, maximizing network performance. DAR was developed at British Telecom (BT) and it improves network throughput based on isolated learning in the switches. DAR behaves in the following manner: a connection is offered to the first-choice route (usually the direct link) and, if there are no available resources, the connection may overflow to an alternative route [12]. If this alternative routes fails, a new alternative route is randomly selected from within a set of admissible alternative routes, and DAR sticks with it as long as it is successful (sticky random principle).

In [21] are described the assumptions to have alternative routing in MPLS networks, namely regarding the connection admission control mechanism [7], which must exist in order to allow alternative routing.

Another key aspect to remember from circuit-switching is bandwidth reservation when alternative routing is employed. Usually, second-choice (alternative) paths are second best or longer paths when comparing to the first-choice paths and, as such, when bandwidth usage approaches a given threshold limit value, it is advisable to prohibit the use of alternative paths so that a bigger number of first-choice paths is allowed. This is a first-choice path protection mechanism that is important when network approaches an overload situation in order to prevent the network to be overtaken by second-choice paths (snowball effect) leading to a bigger congestion.

3 MPLS

The entry and exit points of a MPLS network are called Label Edge Routers (LER), which, respectively, push a MPLS label onto an incoming packet and pop it off from an outgoing packet. At an ingress router, an unlabeled packet needs to go through a MPLS tunnel, and the router first determines the forwarding equivalence class (FEC) the packet should be in. Consequently, a FEC is a group of IP packets which are forwarded in the same manner (e.g., over the same path and with the same label) and for that reason they belong to the same label switched path (LSP). The packet is then passed on to the next hop router after the tunnel. When a labeled packet is received by a MPLS router the

topmost label is examined and, based on the contents of the label a swap, a push or a pop operation can be performed on the packet's label stack. In conclusion, packet processing simply relies on the lookup of the topmost label in the incoming packet which makes this process very quick and protocol independent, as the contents of the packet below the MPLS label stack are not examined [13].

One very important characteristic of MPLS TE is that the head end router in the network controls the path taken by the traffic flows to any particular destination in the network.

Regarding MPLS, each explicit LSP is treated as a point-to-point path that, for a given time duration, has a constant bandwidth. In MPLS, if an explicit path specified with a 'non-mandatory' preference rule attribute value is not feasible, an alternative path may be chosen [5]. This way, if a flow request does not find available the resources it needs in the first choice path, a second chance will be given to that flow as it will be possible to try a pre-computed alternative path.

3.1 MPLS Fast Reroute

Failure protection can be implemented by global or local mechanisms. With global protection, rerouting is performed by the head end, which means that the origin node of the failing path has to receive the failure notification before rerouting the affected traffic onto their respective backup paths. In local protection, it is the node immediately upstream the failing facility that redirects the affected traffic to their backups. In terms of recovery time, the bigger and sparser the network is, the bigger the propagation delay in a global mechanism. MPLS was designed to meet the needs of real-time applications and, for that reason, a local protection mechanism must be used. IETF's MPLS working group has developed a local protection mechanism (Fast Reroute) that provides recovery in SONET time (50 ms). In MPLS local protection each LSP passing through a facility is protected by a backup path which originates at the node immediately upstream to that facility. This node which redirects the traffic onto the preset backup path is called the Point of Local Repair (PLR), and the node where a backup LSP merges with the primary LSP is called Merge Point (MP).

This mechanism (local protection) provides faster recovery (redirection of traffic must occur within 50 ms, in the event of a failure) because the decision of recovery is strictly local.

There are two distinct approaches to local protection. In the one-to-one backup method, a PLR computes a separate backup LSP for each LSP that the PLR protects. In the facility backup method, the PLR creates a single bypass tunnel that can be used to protect multiple LSPs. In both cases, only one protection path exists for a failing facility for a given LSP.

Another important issue regards to what happens to the LSPs after the failure recovery. There are two ways of dealing with this: one is the 'local revertive mode', where every LSP is switched back to the previous path. The other possibility is the 'global revertive mode', where the head-end LSR of

each tunnel is responsible for finding the optimal path for each LSP after the failure recovery.

Finally, it is important to remark that loops may arise in a LSP path whose failing link is protected by a facility backup method. In fact, when a PLR detects a local link failure, immediately starts using a previously computed backup path to get rid of the failure. Because this is a local decision and PLR has no knowledge of the complete path of each LSP that traverses the failing link, the backup path may have one or more nodes in common with each primary LSP. However, in [14] this problem is evaluated and the solution proposed was to prevent the triggering of the LSP loop detection procedure in order not to discard the LSP.

4 Routing Algorithms with Local Link Protection

The most common routing paradigm in MPLS networks is fixed single path routing, where there is only one LSP for each origin-destination pair of nodes and for each type of traffic. In this case, if facility backup method is used, a single LSP is configured in PLR to back up the set of LSPs that traverse the link it protects. In order to do this efficiently there are several studies available, as is the case, for instance, of [20].

An extension of the facility backup method can also be based in the traffic splitting concept as was already applied to path protection and presented in [10], in the context of a global protection strategy. Using this technique in local protection facility backup, PLR is allowed to split the traffic of the failing LSPs into pre-assigned LSPs, as a way to improve network performance.

On the other hand, alternative routing can improve network performance if network topology allows at least two paths (with a maximal number of links) for each origin-destiny pair and type of flows. This type of networks are typical of core networks where MPLS is mainly implemented and survivability is more critical. As previously mentioned, DAR offers more than one path possibility to an incoming request. In that sense, in the advent of a link failure, connections in progress are lost however, even if no protection is implemented, new incoming connections are routed over an alternative path. This source routing behavior can be achieved with the association of RSVP to DAR, and it is a way to implement a sort of network restoration.

In this work we present a new approach that introduces a protection mechanism in networks with alternative routing in order to increase survivability and to save not only the incoming connections, which is typical of alternative source routing, but also connections in progress in the failing link, which is the new achievement with this strategy. In this context, in the same way that network topology is suitable for alternative routing, it is also suitable for more than one bypass tunnel. Doing this we try to distribute more evenly the ongoing traffic in the failed link which is split into more than one bypass tunnel, allowing the alternative routing mechanisms to route the new traffic according to the

new network condition.

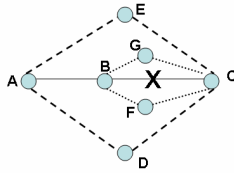


Figure 1: DARMP protection mechanism

Our methodology is explained in figure 1. In the advent of a failure in link B-C, LSPs that go through the failing link are backed up by both B-G-C and B-F-C bypass tunnels. Regarding new incoming connections, they will be carried by one of the alternative (shorter) paths (A-D-C or A-E-C), according to the dynamic alternative routing algorithm (and its sticky random principle) which allows traffic to be better adjusted to current network situation.

One important aspect related to alternative routing methods is the trunk reservation mechanism. In this work we use a known rule of thumb to define the trunk reservation level for each link [23].

5 Study Environment

In order to evaluate our Dynamic Alternative Routing with local Multiple paths Protection (DARMP) strategy, we have also implemented two other fixed routing with local protection approaches. The first approach implements a facility backup method, where PLR has a single bypass tunnel. In this approach, designated in this report by Fixed Routing with Single Protection (FRSP), the bypass tunnel is chosen as the second shortest-path (using hop count metric) between the failure end nodes.

Our second approach, designated in this report by Fixed Routing with Multiple Protection (FRMP), has multiple bypass tunnels. In this case, in the advent of a link failure, ongoing traffic is rescued by several pre-configured paths. In the same manner, newly arrived traffic is also carried by these paths. In this approach the computation of the bypass tunnels is the same as in DARMP.

A discrete-event simulator was used to evaluate network performance. For our study, it is assumed the following: all traffic flows are homogeneous Poissonian and independent, and service times are negative exponentially distributed. For each simulation scenario, we performed 10 independent simulation runs, and results presented are within a 97.5% confidence interval.

5.1 Test network A

The first test network used in our study is based on Network I in [26]. Network I is derived from an MPLS service provider network, it comprises 15 nodes, connected by 58 links, and all sources of traffic have direct links between them.

In [26], work has been developed in order to discuss whether different controls that can be deployed in an MPLS environment for TE are actually beneficial from a network performance point of view. In that sense, because one of the aims with TE is to assure certain classes of traffic, giving better grade-of-service to priority classes, the traffic for the network model is comprised of more than one service classes. In fact, there are four service classes each having different loads between each pair of nodes. In addition, three service models were implemented: fixed rate (FR), uniform fixed rate (UFR) and variable rate on-off model (VR). All these models require specification of the Erlang load to be generated and the flow duration.

In our work, we intend to introduce a dynamic alternative routing algorithm with multiple paths protection in order to show that the combination of multiple paths to save ongoing flows and the existence of alternative paths to carry incoming traffic is an advantage in terms of network survivability in case of link failure. With that in mind, we adjusted Network I to consider one service alone, in order to simplify our study.

Erlang's function $B(\lambda, C)$ gives us the blocking probability that occurs when Poisson traffic of intensity λ is offered to a link with capacity C . According to the inverse of Erlang-B formula (which gives us the number of circuits needed to carry Poisson traffic λ with blocking probability at most B), for a low value of B , the bigger the value of the offered load and the closer it becomes of the number of circuits.

Total capacity regarding active node pairs in Network I is 75573 Mbps. As such, we will make an assumption and considerer that the offered load to the network is approximately 75573 Mbps.

According to the ratio of the overall effective load, service 1, 2, 3 and 4 are responsible for 3544.3737 Mbps, 3461.2434 Mbps, 68552.2683 Mbps and 15.1146 Mbps, respectively.

Regarding service 2 which is implemented under a fixed rate model, with $\lambda=6$ connections/minute and average duration of 3 minutes, we can conclude that offered load by each active node pair is 18 Erlang. Because there are 37 service 2 active node pairs, each pair offers an average of 3461.2434 Mbps/37 = 93.547 Mbps of traffic load, which leads us to approx. 93.547 Mbps/18=5.2 Mbps per circuit. In conclusion, we get 4 amounts of capacity: 933 Mbps (180 circuits), 1866 Mbps (2*180=360 circuits), 2799 Mbps (3*180=540 circuits) and 3732 (4*180=720 circuits).

As previously stated, our intention is to simulate one service alone. We have considered LSPs only for a video service based on service 4 whose effective bandwidth (EBW) is based on the fluid-flow model given in [15] and, considering an Active Burst Length of 1 second and Cell Loss Ratio of 0.01%, we came to conclude that $EBW = 0.8740 \times \text{Peak Flow Rate}$. To be possible to use an effective bandwidth of 5.2 Mbps, we are talking about Peak Flow Rate of approx. 6 Mbps, which is a likely value for video applications [11].

So, considering that each connection occupies one circuit of 5.2 Mbps, we need to calculate the amount of effective load that we intend to offer to the network as coming from service 4 but that corresponds, in the situation presented in [25], to all the other services: service 1 has 3544.3737 Mbps of effective load (681.61 Erlang of service 4 will be offered to the network instead), service 2 offers 18 Erlang of traffic (as already calculated), service 3 has 68552.2683 Mbps of effective load (13183.13 Erlang of service 4) and, finally, service 4 has 15.1146 Mbps of effective load (2.91 Erlang).

Because there are 36 pairs of active nodes generating service 1 and service 3 traffic, we have 18.93 and 366.20 Erlang of service 4 traffic equivalents to service 1 and 3, respectively. There are also 37 active node pairs of service 2 offering 18 Erlang each, and 6 active node pairs generating service 4 traffic, which corresponds to 0.485 Erlang. In conclusion, the total amount of offered traffic to the network would be 14533.65 Erlang.

This way, we calculated the amount of traffic it was offered to the network in paper [25]. A small change will be made regarding each link capacity because 933.12 Mbps is the data rate on OC-18 in optical carriers, and we are not interested on that technology. We will use rounded values (see table 1), which correspond to the circuits in table 2. The test network was engineered with one video service,

O-D Pair	Cap(Mbps)	O-D Pair	Cap(Mbps)	O-D Pair	Cap(Mbps)	O-D Pair	Cap(Mbps)
1-2	1000	1-3	1000	1-5	2000	1-7	2000
1-8	2000	1-9	1000	1-10	1000	1-11	2000
1-13	2000	1-15	2000	2-3	2000	2-6	2000
2-7	1000	2-8	2000	2-9	2000	2-12	1000
3-5	1000	3-6	1000	3-7	3000	3-9	4000
3-10	2000	3-11	1000	3-13	1000	3-14	3000
3-15	1000	4-5	1000	4-8	2000	4-9	1000
4-10	1000	4-13	1000	5-7	3000	5-9	3000
5-11	2000	5-14	3000	6-7	1000	6-8	2000
6-10	1000	7-8	1000	7-11	1000	7-13	3000
7-14	1000	8-9	2000	8-10	1000	8-11	1000
8-12	2000	9-11	2000	9-13	4000	9-14	1000
10-11	1000	10-12	2000	10-15	1000	11-13	1000
11-14	3000	12-13	2000	12-15	2000	13-14	4000
13-15	1000	14-15	2000				

Table 1: Test Network A, in terms of Mbps

with the required effective bandwidth of 5.2 Mbps and call durations of 3 minutes.

The resulting network A presents a 5.6% blocking probability in our DARMP routing model. This is a situation where the network is already under stress and in our study we will call it HIGH_LOAD situation. We would also like to analyze this network with a lower blocking probability value, in order to allow our protection against failures mechanism to succeed more efficiently. As such, in LOW_LOAD situation, we decreased the average value for each pair offered load of 17% and we obtained a 1% blocking probability network performance for DARMP.

O-D Pair	Cap(circuits)	O-D Pair	Cap(circuits)	O-D Pair	Cap(circuits)	O-D Pair	Cap(circuits)
1-2	193	1-3	193	1-5	386	1-7	386
1-8	386	1-9	193	1-10	193	1-11	386
1-13	386	1-15	386	2-3	386	2-6	386
2-7	193	2-8	386	2-9	386	2-12	193
3-5	193	3-6	193	3-7	579	3-9	772
3-10	386	3-11	193	3-13	193	3-14	579
3-15	193	4-5	193	4-8	386	4-9	193
4-10	193	4-13	193	5-7	579	5-9	579
5-11	386	5-14	579	6-7	193	6-8	386
6-10	193	7-8	193	7-11	193	7-13	579
7-14	193	8-9	386	8-10	193	8-11	193
8-12	386	9-11	386	9-13	772	9-14	193
10-11	193	10-12	386	10-15	193	11-13	193
11-14	579	12-13	386	12-15	386	13-14	772
13-15	193	14-15	386				

Table 2: Test Network A, in terms of circuits

5.2 Test network B

Our original study was accomplished with test network A. Nevertheless, we would like to understand the impact of different topologies in our routing algorithms performance. As such, we used one more representative topology: a fully meshed network (table 3).

Test network B is a 10 nodes fully meshed network with 45 links and it was chosen because DAR was designed for fully-connected circuit-switched voice networks. It was engineered with one service and call durations of 3 minutes. All pairs of nodes offered to the network the same average erlang load, and traffic was considered asymmetric. Link capacities and offered load were not engineered by a specific algorithm. Instead, they were adjusted by simulation in order to obtain a 1% blocking probability network performance for DARMP (to be possible to compare with LOW_LOAD situation in network A). In conclusion, link capacities are the ones presented in table 3, and the average erlang demand for each pair of nodes is equal to 45.

O-D Pair	Cap(circ.)	O-D Pair	Cap(circ.)	O-D Pair	Cap(circ.)	O-D Pair	Cap(circ.)	O-D Pair	Cap(circ.)
1-2	104	2-3	104	3-5	102	4-8	103	6-8	104
1-3	106	2-4	105	3-6	104	4-9	102	6-9	105
1-4	103	2-5	103	3-7	101	4-10	102	6-10	101
1-5	105	2-6	105	3-8	102	5-6	101	7-8	102
1-6	102	2-7	103	3-9	103	5-7	102	7-9	102
1-7	102	2-8	100	3-10	105	5-8	102	7-10	99
1-8	100	2-9	101	4-5	100	5-9	103	8-9	101
1-9	100	2-10	103	4-6	100	5-10	103	8-10	102
1-10	100	3-4	106	4-7	100	6-7	103	9-10	102

Table 3: Test Network B - 10 nodes fully meshed network

It is important to remind that in neither of these two networks was protection against failures involved in network dimensioning.

5.3 Framework

5.3.1 Finding the subset of admissible LSPs and bypass tunnels

The first step is to find the set of LSPs that will be used to carry traffic for each pair of nodes and to store them. These LSPs are chosen in ascending order of hop count metric and must comply simultaneously with 3 parameters: maximum number of admissible paths (MAP), maximum number of hops in the path (MHP) and, finally, the maximum number of hops exceeding the shortest path hop count for that pair of nodes (MHSP). All these 3 parameters must be adjusted according to each test network degree of connectivity and they are very important in order to prevent congestion due to the use of large size LSPs. Network A was configured with MAP=8, MHP=3 and MHSP=2. The 10 nodes fully meshed network B, which has one direct path and nine two-link disjoint paths between all pairs of nodes, was configured with MAP=10, MHP=2 and MHSP=1.

Secondly, we must find, for each link, the set of bypass tunnels that will be used to back up traffic in case of failure. These bypass tunnels must obey to the same parameters mentioned before for the original LSPs.

The number of times a given LSP or bypass tunnel is used is inversely proportional to its hop count.

In DARMP, each router has a multi-path routing table: a direct path (which is the first-choice path), and a list of second-choice paths. Additionally, there will be a list with all admissible bypass tunnels (and their usage probabilities), for each one of its adjacent links.

A remark must be made: we had previously thought of accepting only link-disjoint backup paths but this solution lead to very bad performance results because the number of bypass tunnels presented a significant decrease and this approach was abandoned.

5.3.2 Route selection in DARMP

When a connection request arrives at a given router, it attempts to carry that connection through the first-choice path. If that request is denied in that path, a second chance is given to that flow that may attempt an alternative path. Regarding the second-choice path, DARMP is event-dependent, that is, if this second-choice path is denied, another path from within the pool of admissible paths takes its place for future requests, and this particularly connection is lost. If incoming requests are satisfied by this alternate path, the path is not changed (sticky principle). The substitution of the alternative path is random, but smaller paths have higher probability of being chosen. For example, if we only have alternative paths with 2 or 3 nodes; paths with 2 nodes will be chosen with a probability that is twice the probability of choosing paths with 3 nodes. However, paths with the same length have the same probability of being picked.

If a link failure happens, ongoing connections in affected LSPs are switched over to bypass tunnels, according to each tunnel probability, and new incoming connections are carried by their alternative LSPs. It is important to remind that the use of alternative paths to carry new incoming requests allows the use of smaller paths during link failure instead of the longer paths resulting from the adoption of bypass tunnels through local protection mechanisms.

5.4 Analysis of simulation results

We will analyze network performance in both networks with FRSP, FRMP and DARMP algorithms. It is important to recall that FRSP and FRMP behave the same way and they will be treated as equal, when no link protection mechanism is activated.

5.4.1 Network A

We will analyze the network performance with FRSP, FRMP and DARMP algorithms in HIGH_LOAD and LOW_LOAD situations. As we can see in table 4, where B represents network mean blocking probability in normal network operation, DARMP presents higher performance (translated by a lower blocking probability) than FRSP/FRMP). This can be easily explained due to the fact that FRSP/FRMP give one chance alone to each connection request, while our alternative routing scheme in DARMP gives a second chance to connection requests whose first-choice paths were blocked. In addition, the event-dependent nature of our dynamic alternative routing scheme allows our routing tables to be continuously adapted to current network conditions without the burden of global signalling mechanisms, because decisions are strictly local, simply relying on whether previous connection requests were fulfilled or not. Our study is about the evaluation of DARMP network performance and, consequently, we need first to quantify how much multiple protection paths (FRMP) increase network survivability when comparing to single protection paths (FRSP) and, finally, we want to see the increased gain with the introduction of alternative paths. For that purpose, we have done network

	FRSP/FRMP	DARMP
B (HIGH_LOAD)	$0.1155 \pm 2.8 \times 10^{-4}$	$0.0556 \pm 2.2 \times 10^{-4}$
B (LOW_LOAD)	$0.0610 \pm 1.4 \times 10^{-4}$	$0.0106 \pm 7.3 \times 10^{-5}$

Table 4: Blocking probability when there is no failure

simulations in failure conditions (with and without link protection activated) for FRSP, FRMP and DARMP routing schemes. It is important to note that we did not increase overall network bandwidth because we would like to avoid the waste of resources and we want to understand how these algorithms behave in a network that was not dimensioned having in mind protection against failures.

In tables 5 and 6 we can see the results obtained with a 5 minutes failure in link 3-9 (one of the biggest in terms of both carried traffic and capacity [11]) in HIGH_LOAD situation (without and with protection, respectively). The 5 minutes failure may be the necessary time for a reboot.

B_F represents the mean network blocking probability during the failure; $Conv$ is the number of seconds, after the failure resolution, that the network takes to reach a stable value which is 1% apart from the initial blocking probability before the failure; O_F is the number of ongoing connections that went through the failing link in the failure time instant; S_F and F_F are the number of connections that in failure time instant were saved and failed, respectively. C_x represents the number of ongoing connections on network x that were carried by FRSP/FRMP routing methods and that traversed the failing link in the time instant that the failure occurred. We will start by analyzing the results with no

	Without Protection Mechanism Activated	
	FRSP/FRMP	DARMP
B_F	$0.1438 \pm 1.1 \times 10^{-3}$	$0.0684 \pm 2.9 \times 10^{-3}$
$Conv$	300.46 ± 40.5	293.46 ± 76.9
O_F	C_A	$1.44 \times C_A$
S_F	0	0
F_F	C_A	$1.44 \times C_A$

Table 5: No protection mechanism activated, in HIGH_LOAD situation

protection activated. Regarding FRSP/FRMP, blocking probability during failure rises approx. 25% when comparing to a situation where no failure occurs. This can be explained due to the fact that these routing schemes present a fixed single path routing table, which is translated into a total loss of traffic in both ongoing and incoming paths that traverse the failing link. On the other hand, blocking probability during failure rises 23% when DARMP is implemented. However, this value continues to be much better than the one presented with FSPP/FSPMP, as expected. It is also important to observe convergence time values; DARMP takes about 293 seconds and FRSP/FRMP takes 300.46 seconds. In the case where protection is activated, we can see that FRSP presents a blocking probability during

	With Protection Mechanism Activated		
	FRSP	FRMP	DARMP
B_F	$0.1437 \pm 1.1 \times 10^{-3}$	$0.13335 \pm 3.1 \times 10^{-3}$	$0.0737 \pm 3.5 \times 10^{-3}$
$Conv$	300.47 ± 12.8	312.614 ± 15.8	437.1 ± 236.9
O_F	C_A	C_A	$1.44 \times C_A$
S_F	$0.48 \times C_A \pm 2.23$	$0.51 \times C_A \pm 0.03$	$0.54 \times C_A \pm 2.72$
F_F	$0.52 \times C_A \pm 2.23$	$0.49 \times C_A \pm 0.03$	$0.90 \times C_A \pm 2.72$

Table 6: Protection mechanism activated in HIGH_LOAD situation

failure which is quite the same when comparing to the situation where no protection was activated, FRMP experiences an approx. 1% decrease and DARMP has an increase of 1%. These values can be

explained by their behaviours in the advent of a failure. FRSP presents one bypass tunnel path for all traffic that would be carried through the failing link. Consequently, only one path becomes congested; all other incoming connections (that do not need to go through any of the links of the bypass tunnel) are not affected.

When it comes to FRMP, in the advent of a failure, multiple bypass tunnels are used simultaneously (according to their usage probabilities) to save ongoing traffic. As such, a decrease in blocking during failure when compared to FRSP was already expected.

When it comes to the implementation of DARMP, in the failure time instant, its behaviour is equal to the one presented in FRMP. The main difference relies on the number of connections that it has to save. As presented in table 5, DARMP has to rescue almost 50% more connections than FRSP or FRMP. This results from the fact that DARMP has a much lower blocking probability and, as such, carries more traffic in the same network and, consequently, in the advent of a failure, there is more traffic to be saved. If we consider both the greater link usage at failure time instant as a result from the dynamic alternative routing scheme employed, and the sudden increase in bypass tunnels occupation, it is easy to understand how DARMP mean network blocking during failure increases. However, it is important to remark that the number of saved connections in FRMP and DARMP is very similar (with DARMP achieving the best value and the lowest mean blocking probability during failure). Notice, once again, that there is no bandwidth reservation for protection mechanisms in neither of the routing schemes and that the network is already under stress.

	Without Protection	
	FRSP/FRMP	DARMP
B_F	$0.0900 \pm 3.2 \times 10^{-3}$	$0.0116 \pm 1.6 \times 10^{-3}$
$Conv.$	306.1 ± 3.5	577.5 ± 324.7
O_F	C_A	$1.46 \times C_A$
S_F	0	0
F_F	C_A	$1.46 \times C_A$

Table 7: No protection mechanism activated, in LOW_LOAD situation

In tables 7 and 8, simulation results are presented for the LOW_LOAD situation. As expected,

	FRSP	With Protection	
		FRMP	DARMP
B_F	$0.0884 \pm 3.4 \times 10^{-3}$	$0.0707 \pm 3.4 \times 10^{-4}$	$0.0135 \pm 1.7 \times 10^{-5}$
$Conv.$	306.1 ± 3.5	305.2 ± 2.9	711.355 ± 634.9
O_F	C_A	C_A	$1.46 \times C_A$
S_F	$0.58 \times C_A \pm 0.02$	$0.78 \times C_A \pm 0.03$	$0.96 \times C_A \pm 0.05$
F_F	$0.42 \times C_A \pm 0.02$	$0.22 \times C_A \pm 0.03$	$0.50 \times C_A \pm 0.05$

Table 8: Protection mechanism activated in LOW_LOAD situatio

performances improved because there is more available bandwidth for protection in all cases. It is

important to note that DARMP saves more connections than FRMP, and that this number is almost the equivalent of total connections in danger with FRMP.

5.4.2 Network B

We will now analyze the network performance of FRSP, FRMP and DARMP with network topology B. As expected, DARMP presents lower mean blocking probability (B) than FRSP/FRMP when no failure occurs (table 9). This improved performance in network B was already expected because DAR was designed for fully meshed networks.

	FRSP/FRMP	DARMP
B	$0.0195 \pm 1.7 \times 10^{-4}$	$0.0101 \pm 1.6 \times 10^{-4}$

Table 9: Network B - mean blocking probability when there is no failure

In table 10 we can see the results obtained with a 5 minutes failure in biggest link in terms of both carried traffic and capacity (link 1-3), when no protection is implemented. A bigger increase in terms of blocking during failure is already expected for DARMP (when comparing to FRSP/FRMP) because traffic flows that would normally be carried by paths traversing the failing link are now carried by their alternative (longer) paths. FRSP/FRMP experienced a 116% and DARMP a 165% increase in its blocking probability during failure, comparing to a normal network situation. Because alternative paths in use in this fully meshed network are limited to two-link paths, blocking probability has a moderate increase.

Regarding convergence DARMP takes more time than FSRP/FRMP to return to the stable state, as expected.

	Without Protection	
	FRSP/FRMP	DARMP
B_F	$0.0422 \pm 2.2 \times 10^{-3}$	$0.0268 \pm 2.6 \times 10^{-3}$
$Conv.$	415.4 ± 193.2	582.5 ± 277.4
O_F	C_B	$1.04 \times C_B$
S_F	0	0
F_F	C_B	$1.04 \times C_B$

Table 10: Network B - no protection mechanism activated

We are now going to analyze our algorithms performance when protection is implemented. We recall that FRSP, FRMP and DARMP in network A save $0.58 \times C_A$, $0.78 \times C_A$ and $0.96 \times C_A$ connections, respectively (table 8). However, this can only be possible because we are referring to a network with several links that are under-utilized as they are only used by alternative paths. We wish to understand to which extent a balanced network in terms of its resources occupation is able to deal with failures

without the burden of over provisioning.

FRSP presents a very bad performance in terms of both blocking during failure and number of LSPs saved in failure time instant. This results from the fact that single bypass tunnel did not have enough available capacity to deal with all failing LSPs. On the other hand, FRMP takes advantage of multiple bypass tunnels to efficiently distribute traffic in danger the most evenly possible in the network, saving almost 70% of the LSPs traversing the failing link in failure time instant. DARMP saves a little less LSPs than FRMP (due to the fact that it has more carried traffic in the network which leads to less available capacity); however, it is once more the protection approach with the lowest blocking probability during failure.

Again, DARMP is the algorithm that takes more time to return to the stable state, as expected.

	With Protection Mechanism Activated		
	FRSP	FRMP	DARMP
B_F	$0.0421 \pm 2.5 \times 10^{-3}$	$0.0390 \pm 2.6 \times 10^{-3}$	$0.0285 \pm 3.0 \times 10^{-3}$
$Conv$	405.7 ± 190.6	415.4 ± 193.2	582.2 ± 282.6
O_F	C_B	C_B	$1.04 \times C_B$
S_F	$0.10 \times C_B \pm 3.5$	$0.69 \times C_B \pm 8.1$	$0.60 \times C_B \pm 10.4$
F_F	$0.90 \times C_B \pm 3.5$	$0.31 \times C_B \pm 8.1$	$0.40 \times C_B \pm 10.4$

Table 11: Network C - protection mechanism activated

6 Conclusions and Future work

In this report a protection scheme to be used with dynamic alternative routing is presented. This scheme allows networks to become more efficient in link failure situations because it eliminates bandwidth reservation in bypass tunnels and the excess of necessary bandwidth that comes with it, increases network adaptability and load balancing because it uses an event-dependent dynamic alternative routing scheme and the protection mechanism for ongoing traffic splits it among several paths while incoming connections are carried by continually updated alternative paths.

The performance of this scheme was presented for two different representative topologies and can be improved for less loaded networks. We also believe that it is an appropriated approach for real-time traffic.

The percentage of saved connections with DARMP is not 100% and, indeed, it does not have to be. In real networks, premium traffic would have priority in the protection treatment and the failed traffic flows would correspond to classes of service previously recognised as less important.

References

- [1] C. Alaettinoglu, V. Jacobson, and H. Yu. Towards Millisecond IGP Convergence. *NANOG 20*, March 2000.
- [2] G. R. Ash. *Dynamic Routing in Telecommunications Networks*. McGraw-Hill, New York, 1998.
- [3] G. R. Ash and P. Chemouil. 20 years of dynamic routing in circuit-switched networks: Looking backward to the future. *IEEE Global Communications Newsletter*, pages 1–4, October 2004.
- [4] J. Ash. *Traffic Engineering and QoS Optimization of Integrated Voice & Data Networks*. The Morgan Kaufmann Series in Networking. Elsevier, 2007.
- [5] Q. Awduche, J. Malcolm, J. Agogbua, M. O’Dell, and J. McManus. Requirements for traffic engineering over mpls. Internet (www.icft.crri.reston.va.us/...), September 1999.
- [6] A. Basu and J. Riecke. Stability issues in OSPF routing. In *SIGCOMM ’01: Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 225–236, New York, NY, USA, 2001. ACM.
- [7] K. Chan, A. Charny, and P. Eardley. Pre-congestion notification failure problem statement: Internet draft, work in progress. 2006.
- [8] M. Conte. *Dynamic Routing in Broadband Networks*. Klumwer Academic, 2003.
- [9] R. Cotter and D. Medhi. Survivable Design of Reconfigurable MPLS VPN Networks. In *Proc. of 7th International Workshop on the Design of Reliable Communication Networks (DRCN 2009)*, Washington, DC, October 2009.
- [10] A. Dana, A. Zadeh, M. Kalantari, and K. Badie. A traffic splitting restoration scheme for mpls network using case-based reasoning. *IEEE Communications*, 2:763–766, September 2003.
- [11] Catarina Francisco, Lúcia Martins, João Redol, and Paulo Monteiro. A previous study on Dynamic Alternative Routing with local protection paths in MPLS networks. Technical Report ISSN:1645-2631, INESC-Coimbra, May 2010.
- [12] R. Gibbens. *Dynamic Routing In Circuit-Switched Networks: The dynamic alternative routing strategy*. PhD thesis, University of Cambridge, 1988.
- [13] IETF Network Working Group, RFC 2702, Q. Awduche, J. Malcolm, J. Agogbua, M. O’Dell, and J. McManus. Requirements for traffic engineering over MPLS, September 1999.
- [14] IETF Network Working Group, RFC 4090, P. Pan, G. Swallow, and A. Atlas. Fast reroute extensions to rsvp-te for lsp tunnels, March 2005.
- [15] R. Guérin, H. Ahmadi, and M. Naghshineh. Equivalent capacity and its application to bandwidth allocation in high-speed networks. *IEEE Journal on Selected Areas in Communications*, 9(7):968–981, September 1991.
- [16] International Telecommunication Union. ITU-T Recommendation G.114 (2003) One-way transmission time. Technical report, ITU-T, Geneva - Switzerland, 2003.
- [17] A. Kist and R. Harris. Scheme for alternative packet overflow routing (SAPOR). In *Workshop on High Performance Switching and Routing, HPSR*, pages 269 – 274. IEEE, June 2003.
- [18] M. Kodialam and T. Lakshman. Dynamic Routing of Locally Restorable Bandwidth Guaranteed Tunnels Using Aggregated Link Usage Information. In *In Proceedings of IEEE INFOCOM*, pages 376–385, 2001.

- [19] G. Li and D. Wang. Efficient Restoration Capacity Design in MPLS Networks. *10th Asia-Pacific Conference on Communications and 5th International Symposium on Multi-Dimensional Mobile Communications*, 2004.
- [20] Rüdiger Martin, Michael Menth, and Korhan Canbolat. Requirements for the Facility Backup Option in MPLS Fast Reroute. In *IEEE High Performance Switching and Routing (HPSR)*, Poland, October 2006.
- [21] Lúcia Martins, Catarina Francisco, João Redol, José Craveirinha, J. Clímaco, and Paulo Monteiro. *NETWORKING 2009*, volume 5550 of *Lecture Notes in Computer Science*, chapter Evaluation of a Multiobjective Alternative Routing Method in Carrier IP/MPLS Networks (Work in Progress), pages 195–206. Springer Berlin / Heidelberg, 2009.
- [22] D. Medhi. QoS routing computation with path caching: A framework and network performance. *IEEE Communications Magazine*, 40(12):106–113, December 2002.
- [23] D. Medhi and I. Katib. Adaptive alternate routing in wdm networks and its performance tradeoffs in the presence of wavelength converters. In *Optical and Switching Networks*, March 2009.
- [24] M. Pióro and D. Medhi. *Routing, Flow and Capacity Design in Communication and Computer Networks*. Elsevier Inc., 2004.
- [25] S. Srivastava, G. Agrawal, and D. Medhi. Dual-based link weight determination towards single shortest path solutions for ospf networks. In *Proceedings of 19th International Teletraffic Congress*, Beijing, China, Aug 29 - Sep 2 2005.
- [26] S. Srivastava, B. Krithikaivasan, C. Beard, and D. Medhi et al. Benefits of traffic engineering using qos routing schemes and network controls. *IEEE Computer Communication Magazine*, 27:387–399, 2004.
- [27] Jean-Philippe Vasseur, Mario Pickavet, and Piet Demeester. *Network Recovery: Protection and Restoration of Optical, SONET-SDH, IP, and MPLS*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 2004.
- [28] D. Wang and G. Li. Efficient Distributed Bandwidth Management for MPLS Fast Reroute. *IEEE/ACM Transactions on Networking*, 16(2), April 2008.