©2006 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. The definitive version of this paper has been published in IEEE International Conference on Broadband Communication, Networks, and Systems (BROADNETS), 2006, 10.1109\/broadnets.2006.4374358.

Capacity Requirements for the One-to-One Backup Option in MPLS Fast Reroute

Ruediger Martin, Michael Menth, and Korhan Canbolat
Department of Distributed Systems, Institute of Computer Science, University of Würzburg, Germany
Email: {martin,menth}@informatik.uni-wuerzburg.de

***Abstract*— MPLS fast reroute (MPLS-FRR) mechanisms deviate the traffic in case of network failures at the router closest to the outage location to achieve an extremely fast reaction time. We review the one-to-one backup and the facility backup that are options for MPLS-FRR to deviate the traffic via a detour or a bypass around the failed elements, respectively. Basically, the backup paths can take the shortest path that avoids the outage location from the point of local repair to the tail-end router or to the merge point with the primary path. We suggest two simple modifications that lead to a new path layout which can be implemented by one-to-one and by facility backup. We evaluate the backup capacity requirements, the length of the backup paths, and the number of backup paths per primary path in a parametric study regarding the network characteristics. Our proposals save a considerable amount of backup capacity compared to the standard mechanisms. They are suitable for application in practice since they are simple and conform to the standards.**

Keywords: protection and restoration, MPLS fast reroute, capacity planning

I. Introduction

The operations for multiprotocol label switching (MPLS) fast reroute (MPLS-FRR) mechanisms have been standardized recently by the IETF [1]–[3]. In case of a network failure, they deviate the traffic at the router closest to the failure location. This can be done by two basically different mechanisms: one-to-one and facility backup. The one-to-one backup deviates the traffic directly from the outage location to its destination while the facility backup just bypasses the traffic around the outage location to repair the original primary paths. The facility backup concept deviates several label switched paths (LSPs) by a single backup path around the failure location while the one-to-one concept needs a private backup path for each LSP. Thus, the facility backup leads to a lower configuration overhead but introduces other configuration problems.

The standards provide only the protocol mechanisms to implement a detour or a bypass but the path layout is not determined. Thus, operators have many degrees of freedom to set up the backup paths. Usually, the default path layout for the backup paths follows the shortest path that avoids the outage location [4]. The authors of [5] suggest a mixed integer linear program (MILP) formulation to find optimum backup paths for the one-to-one mechanism. However, the solution of MILPs is complex and it may be difficult and very time consuming for medium-size or large networks. The authors of [6] present a distributed online algorithm for one-to-one backup path layout that can be used when LSPs are set up and torn down on demand.

In this paper, we discuss the path layout for both one-to-one and facility backup paths. We consider different outage scenarios, i.e., single router failures only, single link failures only, and single link or router failures. We suggest simple modifications to the default shortest path layout both for the one-to-one and the facility backup concept and obtain new MPLS-FRR mechanisms that can be implemented by existing protocols. While we calculated the required capacity for our proposed MPLS-FRR facility backup concepts in [7], we here calculate the required capacity for our proposed MPLS-FRR one-to-one backup concepts considering various networks and outage scenarios and compare it to other protection methods. Our comparison shows that traffic distribution by backup paths helps a lot to reduce the required capacity. The proposed new mechanisms require less capacity than standard solutions since they take advantage of that fact.

This paper is structured as follows. Section II gives a brief overview on resilience mechanisms in general. Section III describes protocol issues specifically for MPLS-FRR, it reviews the default layout of the backup paths and suggests modifications. Section IV compares the required backup capacity for the proposed MPLS-FRR one-to-one backup mechanisms and the required configuration overhead. Finally, Section V summarizes this work and gives an outlook on further research.

II. Overview on Resilience Mechanisms

In this section we give a brief overview on resilience mechanisms to classify MPLS-FRR. A broader and more complete overview can be found, for instance, in [8]. Resilience mechanisms can be divided into restoration and protection schemes. Restoration sets up a new paths after a failure while protection switching pre-establishes backup paths in advance.

A. IP Restoration

Usually, restoration is applied by IP rerouting. IP networks have the self-healing property, i.e., their routing re-converges after a network failure by exchanging link state advertisements (LSAs) such that all but the failed nodes can be reached after a while if a working path still exists. In addition, the equal cost multipath (ECMP) option of the most widely used interior gateway routing protocols (IGPs) OSPF [9] and IS-IS [10] distributes traffic over several alternative paths of equal cost to destinations. Thus, especially after the routing reconvergence

due to failures, normal and rerouted traffic can be spread more equally over the network. This reduces the required bandwidth as we will see in Section IV. Another example for restoration besides IP rerouting are backup paths in MPLS that are set up after a network failure.

The disadvantage of such methods is obvious: they are slow. In particular, the interval length to exchange the LSA updates cannot be reduced to arbitrarily small values [11] and the computation of the shortest paths that are needed to construct the routing tables based on the new LSAs requires a substantial amount of time. This time overhead is tolerable for elastic traffic but not for realtime traffic or even high-precision telematic or tele-surgery applications. However, the reconvergence of the IP routing algorithm is a very simple and robust restoration mechanism [12], [13].

B. Protection Switching Mechanisms

Protection addresses the problem of slow reconvergence speed. It is usually implemented in multiprotocol label switching (MPLS) technology due to its ability to pre-establish explicitly routed backup paths in advance. Depending on the place where the reaction to failures is done, protection switching mechanisms can be distinguished into end-to-end and local protection.

1) End-to-End Protection Switching: In case of end-to-end protection switching the reaction to a failure along a path is executed at the path ingress router.

a) Primary and Backup Paths: Backup paths are set up simultaneously with primary paths and in case of a failure, the traffic is just shifted at the path ingress router of a broken primary path to the corresponding backup path.

b) Self Protecting Multipath (SPM): The self-protecting multipath (SPM) consists of disjoint label switched paths (LSPs) and provides at the source several alternatives to forward the traffic to the destination. The SPM has been presented first in [14]. The traffic is distributed over all alternative paths according to a traffic distribution function (see Figure 1). If one of the paths fails, the traffic is transmitted over the working paths according to another precomputed traffic distribution function. Thus, traffic distribution functions can be optimized a priori to minimize the required backup capacity in the network.

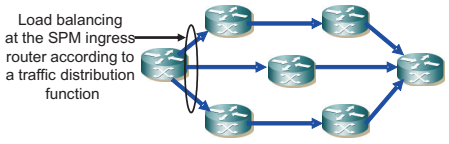


Fig. 1. The SPM performs load balancing over disjoint paths according to a traffic distribution function which depends on the working paths.

End-to-end protection switching is faster than restoration methods but the signalling of the failure to the path ingress router takes time within which traffic is lost.

2) Local Protection Switching: Local protection schemes tackle the problem of lost traffic in case of end-to-end protection. Backup paths towards the destination are set up not only at the ingress router of the primary path but at almost every node of the path. Then, a backup path is immediately available if the path breaks at some location. Local protection switching can be implemented by MPLS-FRR [1]–[3]. Currently, fast reroute mechanisms are also discussed for IP networks. Several solutions are being discussed but a preferred method is not yet established [15]–[18].

III. Mechanisms for MPLS Fast Reroute

MPLS fast reroute mechanisms protect primary LSPs by local repair methods. A primary LSP is said to be protected at a given hop if it has one or multiple associated backup tunnels originating at that hop. In this work, we want to protect the primary LSP along all intermediate routers of its path. Thus, each intermediate router is a so-called point of local repair (PLR) that serves as head-end router for at least one backup path. There are two basically different methods for local repair: one-to-one backup and facility backup. In the following, we review these concepts, we explain simple and obvious options for the layout of the backup path, and propose slightly more complex options that reduce the number of required backup paths or the required backup capacity.

A. Local Repair Options in the MPLS Fast Reroute Framework

We briefly introduce the one-to-one backup and the facility backup together with mandatory conditions regarding the path layout for the protection of link or router failures.

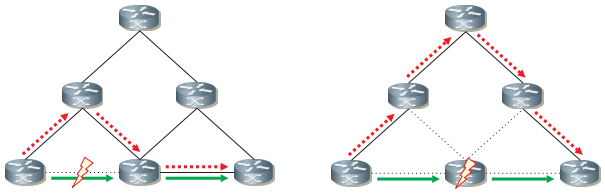
1) One-to-One backup Using Detour LSPs: The one-to-one backup sets up a backup path from the PLR to the tail-end of the protected LSP. This backup path is called detour LSP. Each detour LSP protects exactly one primary LSP, but the primary LSP may be protected by several detour LSP starting at different PLRs. If a detour LSP intersects its protected path further upstream, it may be merged with the primary path at a so-called detour merge point (DMP) to reduce the LSP states in the routers further downstream. However, we disregard this possibility in the following. Modes are defined in which detour LSPs may contain elements of the protected LSP and others are defined in which such elements are forbidden. In the following, we point out only mandatory constraints to protect against link or router failures.

a) Link Detour: To protect a primary path against a link failure, the router preceding the failed link acts as PLR by redirecting the traffic onto a detour LSP towards the tail-end router r_{tail} of the primary path. The backup path must not contain the failed link, but it may contain the adjacent routers of the failed link. We call this type of backup path $LinkDetour(PLR, r_{tail})$.

b) Router Detour: To protect a primary path against a router failure, the router preceding the failed router acts as PLR by redirecting the traffic onto a detour LSP towards the tail-end router r_{tail} of the primary path. The backup path must not contain the failed router and all its adjacent links. We call this type of backup path $RouterDetour(PLR, r_{tail})$. Note

that the primary path cannot be protected against the failure of its head-end or tail-end label switched router (LSR).

Figures 2(a) and 2(b) show that the backup path $LinkDetour(PLR, r_{tail})$ and $RouterDetour(PLR, r_{tail})$ from the same PLR within the same flow can take different shortest paths due to their specific requirements.



(a) $LinkDetour(PLR, r_{tail})$. (b) $RouterDetour(PLR, r_{tail})$.

Fig. 2. One-to-one backup using detours.

2) Facility Backup Using Bypass LSPs: The facility backup sets up a backup path from the PLR to an upstream router of the protected LSP. This router is called merge point (MP) as it merges the backup path with the protected LSP. Since the backup path bypasses the failure location, it is called bypass LSP. Unlike detour LSPs, a bypass LSP can protect multiple primary LSPs that share the same PLR and MP. In the following, we point out the placement of the MP to protect against link or router failures.

a) Link Bypass: To protect a primary path against a link failure, the router preceding the failed link acts as PLR by redirecting the traffic onto a bypass LSP towards the next hop (NHOP) LSR of the PLR. Thus, the adjacent routers of the link are the head-end and the tail-end LSRs of the bypass LSP which must not contain the failed link. We call this type of backup path $LinkBypass(PLR, NHOP)$.

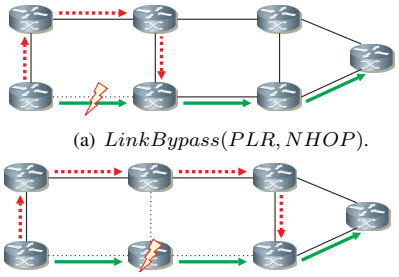
b) Router Bypass: To protect a primary path against a router failure, the router preceding the failed router acts as PLR by redirecting the traffic onto a bypass LSP towards the next-next hop (NNHOP) LSR of the PLR. Thus, the neighboring routers of the failed router within the primary path are the head-end and the tail-end LSRs of the bypass LSP which must not contain the failed router and all its adjacent links. We call this type of backup path $RouterBypass(PLR, NNHOP)$. Like above, the primary path cannot be protected against the failure of its head-end or tail-end LSR.

The $LinkBypass(PLR, NHOP)$ in Figure 3(a) and the $RouterBypass(PLR, NNHOP)$ in Figure 3(b) from the same PLR within the same flow take different paths due to their specific requirements.

B. Backup Path Configuration for Detour and Bypass LSPs

In this section we consider the backup path configuration for detour and bypass LSPs. We consider three different options. They differ in the number of installed backup paths, their use, and their path layout.

1) Backup Path Configuration based on Shortest Paths: An intuitive and obvious approach is characterized by setting up backup LSPs according to the shortest path principle. Each potential PLR, i.e. each intermediate LSR of an LSP, has separate backup paths for the protection against the failure of the next link and the next router, respectively.



(a) $LinkBypass(PLR, NHOP)$.

(b) $RouterBypass(PLR, NNHOP)$.

Fig. 3. Facility backup using bypasses.

This very simple approach obviously leads to a large number of backup paths that we are trying to assess now for one-to-one backup and facility backup. We assume n routers and m bidirectional links in the network as well as a fully meshed LSP overlay, i.e., there are $n \cdot (n-1)$ protected LSPs. The length of a specific primary path p is given by $len(p)$ in terms of links and the average number of links per primary path is denoted by $\overline{len}$. The number of adjacent links of router r is given by its node degree $deg(r)$. The average node degree in a network is $deg_{avg} = \frac{2 \cdot m}{n}$

a) Number of Required Detour LSPs: The one-to-one backup concept requires $len(p)$ link detour LSPs to protect it against all link failures and $len(p)$–1 detour LSPs to protect it against all router failures of the primary path. Thus, $2 \cdot len(p)$–1 detour LSPs are required altogether for its protection. As a consequence, $n \cdot (n-1) \cdot (2 \cdot \overline{len}-1)$ detours are needed in the network.

b) Number of Required Bypass LSPs: The network requires $2 \cdot m$ link bypasses to protect against the failures of m different links in each direction since these backup LSPs can protect multiple primary paths. In addition, router bypass LSPs are needed for the protection against the failure of each of the n routers. We consider a specific router r with $d = deg(r)$ adjacent bidirectional links, from which traffic can be received and to which traffic can be forwarded by that router. If all combinations are possible, $d \cdot (d-1)$ different backup paths are needed to protect possible LSPs carried over r. Thus, $d \cdot (d-1)$ different router bypass LSPs are required for the protection against the failure of this router. As a consequence, a rough guess for the number of required backup path is $2 \cdot m + n \cdot deg_{avg} \cdot (deg_{avg}-1) = 2 \cdot m \cdot deg_{avg}$. This expression proposes that considerably fewer bypasses than detours are required to protect the network against all single link and router failures.

2) First Modification: Reducing the Number of Backup Paths: It is obvious that the number of required backup paths of the naive backup path configuration approach can be reduced if the backup paths for the protection of link failures are substituted by the backup paths for router failures if possible.

a) Backup Paths Reduction for Detour LSPs: A link failure can be protected by a $LinkDetour(PLR, r_{tail})$ but it can also be protected by the $RouterDetour(PLR, r_{tail})$.

The latter one just has more stringent requirements for the layout of its backup path. Such backup paths exist for all links but the last one within the primary path. Thus, $len-1$ link failures can be protected by a $RouterDetour(PLR, r_{tail})$ and the failure of the last one must be protected by a $LinkDetour(PLR, r_{tail})$.

b) Backup Paths Reduction for Bypass LSPs: A link failure can be protected by a $LinkBypass(PLR, NHOP)$ but it can also be protected by the $RouterBypass(PLR, NNHOP)$. The latter one just has different requirements for the layout of its backup path. Such backup paths exist for all links but the last one within the primary path. Thus, $len-1$ link failures can be protected by a $RouterBypass(PLR, NNHOP)$ and the failure of the last one must be protected by a $LinkBypass(PLR, NHOP)$.

3) Second Modification: Push Back Mechanism to Increase the Traffic Spreading: We will see in Section IV that traffic distribution in failure cases reduces the required backup capacity. This can be achieved by a simple push back mechanism: the idea is to deviate the traffic at least one hop prior to the outage location.

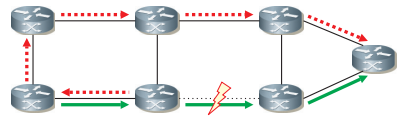
a) Push Back Mechanism for Detour LSPs: When routers fail, the previous router acts as PLR and redirects the traffic onto its backup paths. Thus, there are several different PLRs that deviate the traffic and, therefore, the traffic can be spread well across the network. As a consequence, $RouterDetour(PLR, r_{tail})$ LSPs do not need to be changed.

In contrast, when a link fails, only a single PLR redirects the traffic over backup paths, regardless of whether $LinkDetour(PLR, r_{tail})$ or $RouterDetour(PLR, r_{tail})$ are used. Pushing the traffic back by one link to the previous router within the primary path and deviating it from there leads to the same situation like for router failures: the traffic can be distributed from different locations. This leads to the following rule. If the first link within the primary path fails, it is not possible to push the traffic back. If another link within the primary path fails, the traffic is pushed back and deviated at the previous router. This leads to a new kind of backup path, the $PushedBackDetour(PLR, r_{tail})$. Note that this backup path starts at the PLR and visits the previous router before heading to the destination r_{tail}.

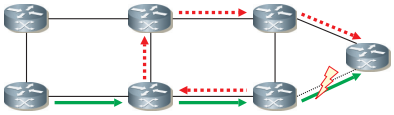
b) Push Back Mechanism for Bypass LSPs: Again, when routers fail, the previous router acts as PLR and redirects the traffic onto its backup paths. Thus, there are several different PLRs that deviate the traffic and, therefore, the traffic can be spread well across the network. As a consequence, $RouterBypass(PLR, NNHOP)$ backup paths do not need to be changed.

When a link fails and the primary path contains only a single link, a normal $LinkBypass(PLR, NHOP)$ is the only option. When a $RouterBypass(PLR, NNHOP)$ is used to protect against a link failure, the traffic of different primary paths is deviated to several different NNHOP routers. This leads already to a certain traffic distribution. However, this cannot be applied to the last link within a primary path that must be protected by an explicit $LinkBypass(PLR, NHOP)$. Again, we push the traffic back to the previous router within the primary path such that it can be deviated from different locations to the NHOP router. We call this structure $PushedBackBypass(PLR, NHOP)$, which starts also at the normal PLR and just visits the router previous to the outage location before heading tho the NHOP router.

Figure 4(a) shows the push back mechanism for a $PushedBackDetour(PLR, r_{tail})$ which can be applied for the protection against the failure of any link except the first one within the primary path. Figure 4(b) shows the $PushedBackBypass(PLR, NHOP)$ which is only applied for the protection against the failure of the last link within the primary path provided that at least two links exist.



(a) $PushBackDetour(PLR, r_{tail})$.



(b) $PushBackBypass(PLR, NHOP)$.

Fig. 4. Application of the push back concept to detour- and bypass-LSPs.

IV. Performance Comparison

In this section we investigate the performance of the above discussed options for the one-to-one backup by parametric studies regarding different network characteristics. First, we explain our evaluation methodology, then we study the required backup capacity, the path lengths, and the number of backup paths per primary path before we compare their efficiency with other well known resilience mechanisms.

A. Evaluation Methodology

We first explain the network dimensioning approach that we use to calculate the required backup capacity. Then, we describe the foundation of our parametric study which is based on artificially generated random networks.

1) Calculation of the Required Backup Capacity: The required backup capacity is the major performance measure in this study. We obtain it as follows for a given network topology, a given traffic matrix, and a given resilience mechanism. The network topology is given by a graph $\mathcal{N} = (\mathcal{V}, \mathcal{E})$ where $\mathcal{V}$ is the set of routers and $\mathcal{E}$ is the set of links. We first compute the capacity $c(l)$ of all links $l \in \mathcal{E}$ in the network that is required to carry the traffic according to the shortest path principle. The sum of these capacities yields the required network capacity $C_\emptyset = \sum_{l \in \mathcal{E}} c(l)$ for the failure-free scenario $\emptyset$. The network must be protected against the failures of a set of failure scenarios $\mathcal{S}$ that contains always the failure-free scenario $\emptyset$. Resilience mechanisms require sufficient backup capacity on the links to carry the traffic in each protected failure scenario. We first determine the link capacity $c(s, l)$

that is required to carry the traffic in each protected failure scenario $s \in \mathcal{S}$ according to the routing which has been changed according to the resilience mechanism. We use it to calculate the required capacity for the resilient network by $C_{\mathcal{S}} = \sum_{l \in \mathcal{E}} max_{s \in \mathcal{S}}(c(s,l))$. Note that traffic aggregates are inactive in failure scenarios if their source or destination node fails. We express the required backup capacity relative to the capacity needed for shortest path routing by $B = \frac{C_{\mathcal{S}} - C_{\emptyset}}{C_{\emptyset}}$. This methodology can be viewed as a network dimensioning approach. Another option is to calculate, e.g., blocking or QoS violation probabilities for networks with given link capacities. However, we take the network dimensioning approach since it is simpler than the second one, and it is fairer since it grants the capacity to the links where it is needed by each considered resilience mechanism.

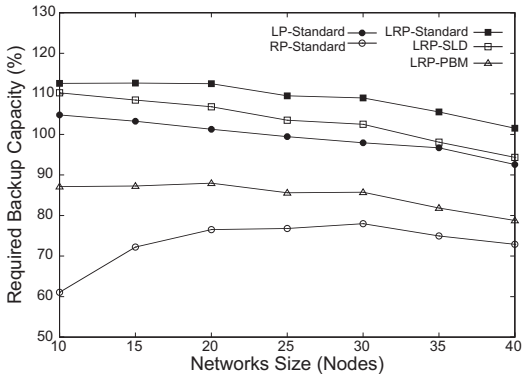
2) Parametric Study: In our parametric study we assume that every network node serves as border router with transit capabilities. We have a fully meshed overlay network and a homogenous traffic matrix. We showed in [19] that the heterogeneity of the traffic matrix has a significant impact on the required backup capacity but an investigation of this issue in this context is beyond the scope of this paper. We consider three different failure scenarios: all single router failures, all single bidirectional link failures, and all single router and bidirectional link failures. Mainly we use the latter one since 30% of all network failures are due to router failures and 70% are due to link failures [20].

We use sample networks in our study. Most important network characteristics for resilient networks are the network size in terms of nodes $|\mathcal{V}| = n$ and in terms of links $|\mathcal{E}| = m$. They define the average node degree $deg_{avg} = \frac{2 \cdot m}{n}$ that indicates the average number of adjacent links of a node and is thereby an indirect measure for the network connectivity. In addition, the minimum and the maximum node degree deg_{min} and deg_{max} are also important measures. Since today's well established topology generators cannot control deg_{min} and deg_{max}, we use our own topology generator which is described in [14] and which incorporates features of the well known Waxman model [21], [22]. It allows direct control over n, deg_{avg}, and the maximum deviation deg_{dev}^{max} of the individual node degrees from their predefined average value. It generates connected networks and avoids loops and parallels. We consider networks of size $n \in \{10, 15, 20, 25, 30, 35, 40\}$ nodes with an average node degree $deg_{avg} \in \{3, 4, 5, 6\}$ and a maximum deviation from the average node degree of $deg_{dev}^{max} \in \{1, 2, 3\}$. We generate 5 networks of each combination randomly. This leads in sum to 420 sample networks. For each of them we calculated the required backup capacity for each of the following resilience mechanisms.

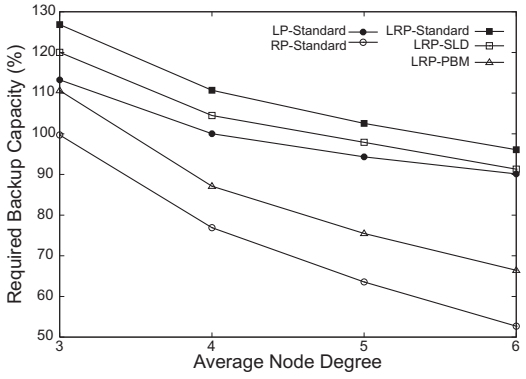
- To provide only link protection (LP), we used the standard $LinkDetour(PLR, r_{tail})$; the set of protected failure scenarios comprises only single link failures. *(LP-Standard)*
- To provide only router protection (RP), we used the standard $RouterDetour(PLR, r_{tail})$; the set of protected failure scenarios comprises only single router failures. *(RP-Standard)*
- To provide link and router protection (LRP), we used both the standard $LinkDetour(PLR, r_{tail})$ and the standard $RouterDetour(PLR, r_{tail})$ for the link and router failures respectively; the set of protected failure scenarios comprises both single link and single router failures. *(LRP-Standard)*
- As an alternative to the previous scenarios, we substitute the link detours by existing router detours (cf. Section III-B.2) wherever possible. Note that this is the standard path layout approach for the detour concept as proposed in [4]. *(LRP-SLD)*
- As another alternative, we use the push back mechanism $PushBackDetour(PLR, r_{tail})$ for link detours (cf. Section III-B.3) wherever possible. *(LRP-PBM)*

In the following these abbreviations indicate the protected failures and the applied method.

B. Backup Capacity Requirements for MPLS-FRR-Detour



(a) Backup capacity requirements depending on the network size.



(b) Backup capacity requirements depending on the network connectivity.

Fig. 5. Impact of the network characteristics, the protected failures, and the resilience mechanism on the required backup capacity for one-to-one backup only.

We compare the backup capacity requirements depending on the network size for the 5 above defined investigation scenarios. Each point in Figure 5(a) represents the average

backup capacity for all 60 networks of a specific size and the respective investigation scenario while each point in Figure 5(b) represents the average backup capacity for all 105 networks of a specific average node degree and the respective investigation scenario. In both figures, the chosen resilience mechanism has a significant impact on the required backup capacity.

The required backup capacity increases in the order RP-Standard, LRP-PBM, LP-Standard, LRP-SLD, and LRP-Standard. Thus, router protection only, requires less resources than link protection only, although router failures affect also several adjacent links. There are two reasons to explain that phenomenon. The curve for RP-Standard increases for small networks in Figure 5(a) in contrast to the one of LP-Standard. This is due to inactive aggregates whose source or destination failed because of the router failure. However, this affects only $\frac{2}{n}$ of the entire traffic and, therefore, this effect shrinks with an increasing network size. Another reason for the reduced backup capacity requirements of RP-Standard compared to LP-Standard is the improved traffic distribution around the outage location. The $LinkDetour(PLR, r_{tail})$ backup paths of LP-Standard have a single point of local repair (PLR) while the $RouterDetour(PLR, r_{tail})$ backup paths have different PLRs. Thus, the traffic is deviated over a larger number of different links starting from different locations in the network, which is illustrated in Figure 6. As a consequence, the deviated traffic uses less backup capacity on a larger number of different links for the same scenario which increases the potential for backup capacity sharing for different scenarios. Therefore, the difference between the required backup capacity of RP-Standard and LP-Standard increases in Figure 5(b) with an increasing average node degree.

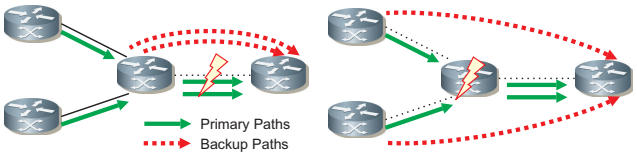
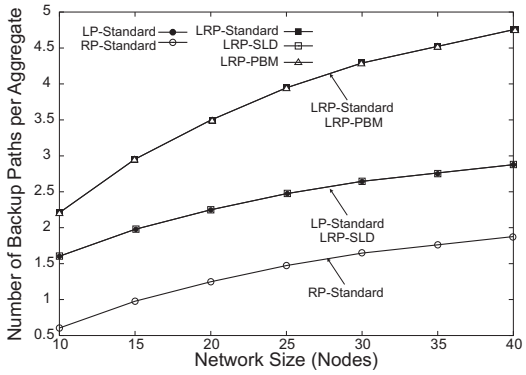


Fig. 6. In case of router failures the traffic is deviated from different locations in the network which leads to a better traffic distribution than in case of link failures.

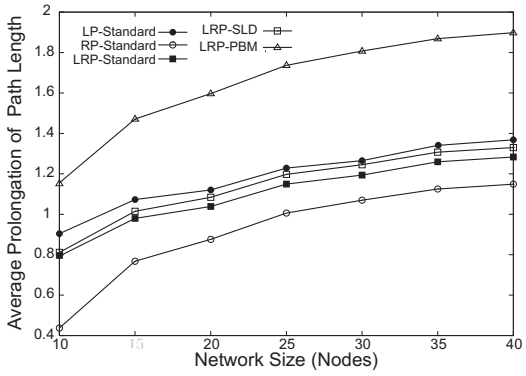
LRP-Standard uses the backup paths of both RP-Standard and LP-Standard and requires clearly more capacity than their maximum. Hence, LP-Standard allocates its capacity at different locations than RP-Standard. As a consequence, the substitution of the $LinkDetour(PLR, r_{tail})$ backup paths through suitable $RouterDetour(PLR, r_{tail})$ backup paths where possible (SLD) leads to a notable reduction of required backup capacity in Figures 5(a) and 5(b). However, the last links of the primary paths cannot be protected by suitable router detours. This motivated the push back mechanism (PBM). It requires 10 to 30% less capacity than LRP-Standard and LRP-SLD although it protects against exactly the same failures. The substitution of the $LinkDetour(PLR, r_{tail})$ for the last link on the primary paths in LRP-SLD by a $PushBackDetour(PLR, r_{tail})$ in LRP-BPM leads to this significant performance gain due to a better traffic distribution around the outage location. This effect is similar to the effect seen for RP-Standard that is illustrated in Figure 6. Note that LRP-PBM requires even clearly less capacity than LP-Standard where only link failures are protected. The impact of this improvement increases also with the average node degree. In general, Figure 5(a) illustrates that the network size has a rather small impact on the required backup capacity while Figure 5(b) shows that the network connectivity in terms of the average node degree reduces the required backup capacity significantly, in particular if backup capacity sharing is enforced through mechanisms that support load distribution around the outage location.

C. Configuration Overhead: Path Length and Number of Backup Paths

As mentioned above, resilience mechanisms differ regarding their configuration overhead. The number of the paths and their length contribute to the number of connection states in the network. Therefore, we compare these measures for the investigated scenarios. In addition, extremely long backup paths delay the traffic which may be even prohibitive for stringent QoS.



(a) Average number of detour-LSPs per primary path.



(b) Average prolongation of the path length through detour-LSPs.

Fig. 7. Impact of the network size, the protected failures, and the protection method on the configuration overhead.

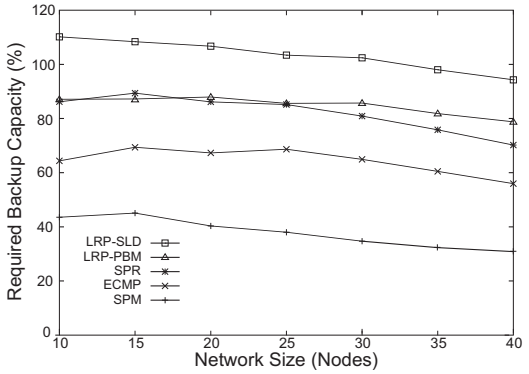
Figure 7(a) shows the average number of detour-LSPs per

primary LSP depending on the network size. The number of backup path for LP-Standard is exactly the average path length in the network and increases with the network size. The number of intermediate routers along a path is smaller by one than the number of links and, thus, the number of backup paths for RP-Standard is smaller by exactly one than for LP-Standard. LRP-Standard uses both all link detours from LP-Standard and all router detours from RP-Standard and, therefore, its number of backup paths is their sum. LRP-BPM has the same number of backup paths since it uses separate detour-LSPs for link and router failures. LRP-SLD uses all router detours from RP-Standard to substitute appropriate link detours in LP-Standard which leads to a protection of link and node failures while keeping the number of backup paths as low as for LP-Standard.

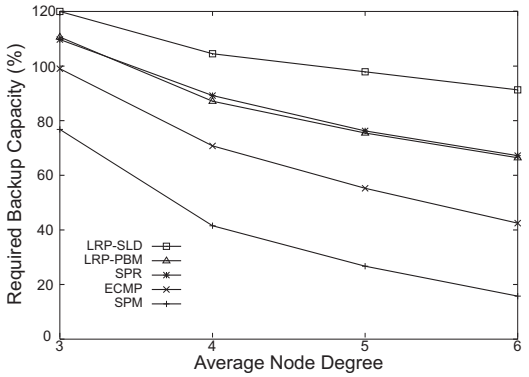
We now consider the path lengths for the detour-LSPs. In case of a failure, the primary LSPs hit by failed elements are split into two parts. The part from the source to the PLR can still be used and a detour-LSP must be found for the part from the PLR to the destination. The detour-LSP is at least as long as the part from the PLR to the destination and mostly prolongs the path. For a primary path p of length $len(p)$, the average length of the part from the PLR to the destination is $\frac{len(p)}{2}+1$ taking into account only all router failures and it is $\frac{len(p)}{2}+\frac{1}{2}$ taking into account only all link failures. Since the average prolongation of short paths through a detour is longer than the one for a long path, router failures lead to shorter path prolongations than link failures. Therefore, the average prolongation of the path length caused by the detours in all failure scenarios is smaller for RP-Standard than for LP-Standard as shown in Figure 7(b). The impact of this effect is reduced with an increasing network size since the path lengths $len(p)$ increase and the relative difference between $\frac{len(p)}{2}+1$ and $\frac{len(p)}{2}+\frac{1}{2}$ becomes smaller. LRP-Standard falls in between RP- and LP-Standard as it is a combination of both concepts. The backup paths for LRP-SLD are slightly longer than the ones for LRP-Standard because the $LinkDetour(PLR, r_{tail})$ are partly replaced by $RouterDetour(PLR, r_{tail})$ at the same PLR and may be longer due to more constraints. (cf. Figures 2(a) and 2(b)). The $PushBackDetour(PLR, r_{tail})$ of PBM are clearly prolonged compared to simple link or router detours and, therefore, the average path length for LRP-BPM is notably larger than for the other methods. However, the difference of the average path length is less than one link since LRP-BPM uses mostly also normal link and router detours.

D. Comparison of the Required Backup Capacity for Restoration, End-to-End Protection, and Local Protection

In previous work [14] we investigated the backup capacity requirements for the self-protecting multipath (SPM) and for shortest path rerouting (SPR). We consider them and also equal-cost multipath (ECMP) rerouting for a comparison with one-to-one backup regarding the required backup capacity. All single link and node failures are protected.



(a) Backup capacity requirements depending on the network size.



(b) Backup capacity requirements depending on the network connectivity.

Fig. 8. Impact of the network characteristics, the protected failures, and the resilience mechanism on the required backup capacity for restoration, end-to-end protection, and local protection.

Figures 8(a) and 8(b) show the averages of their required backup capacity depending on the network characteristics. The SPM requires by far the least capacity, followed by ECMP, and SPR. Surprisingly, LRP-BPM requires about the same backup capacity like SPR, but the one-to-one backup reacts within tens of milliseconds while the restoration mechanism reacts only within seconds. LRP-SLD comes with less configuration overhead than LRP-BPM, but it requires more backup capacity. Like above, the network size has only little impact while an increasing average node degree leads to a considerable reduction of backup capacity especially for ECMP and SPM that support traffic distribution explicitly. The SPM seems to be the most attractive resilience mechanism since it requires the least capacity and it is relatively fast as it implements end-to-end protection. However, in contrast to the one-to-one backup, it needs load balancing capabilities and it is not a standardized approach.

V. Summary and Conclusion

We first gave an overview of restoration and protection mechanisms for packet-switched networks. Then we explained the MPLS-FRR framework introduced by the IETF which

is intended for fast local protection. It only standardizes protocol signaling issues and the behavior of the label switched routers (LSRs) in case of network element failures. It does not recommend the layout of the backup paths themselves, which is still an open research issue. These backup paths should be short, easy to configure, easy to calculate, and they should require only little additional backup capacity when backup capacity sharing is possible.

The MPLS-FRR framework specifies two different protection types: one-to-one backup using detour LSPs and facility backup using bypass LSPs. We first clarified the requirements for these backup structures and considered a simple standard mechanism that sets up link and router detours and bypasses, respectively, for all single link and node failures. The backup paths take the shortest paths that avoid the outage location. Then, we proposed a link detour and link bypass substitution (SLD, SLB) approach to reduce the number of required backup paths. In addition, we suggested an additional push back mechanism (PBM) for link detours and bypasses to reduce the required backup capacity. All these modifications are simple, they can be implemented by the framework [1], and they use the shortest paths principle, i.e., they do not require complex and time consuming optimization algorithms.

We evaluated the required backup capacity, the average path length, and the number of backup paths per primary path for the above discussed options of the one-to-one backup. To that end, we conducted a parametric study taking into account 420 artificial networks of different size in terms of nodes, different node degree, and different regularity (deg_{dev}^{max}). Our results showed that both the proposed SLD and in particular the PBM modification reduce the required backup capacity compared to the standard approach due to a better distribution of the backup traffic in failure cases for which we considered single link and node failures. This happens at the expense of slightly longer backup paths. Compared to the standard approach, the SLD modification reduces the number of backup paths and thereby the configuration complexity while the PBM needs exactly the same number of backup paths. Finally, a comparison with other resilience mechanisms showed that the self-protecting multipath (SPM) requires by far the least backup capacity, followed by shortest equal-cost multipath rerouting (ECMP) and single shortest path rerouting (SPR). Surprisingly, our new PBM-based one-to-one backup requires about the same amount of backup capacity like SPR although it reacts within milliseconds while restoration through SPR takes up to several seconds.

Our findings have shown that very simple heuristics for the layout of the backup paths already yield a significant reduction of the required backup capacity which may stimulate more complex and efficient heuristics to obtain further savings.

ACKNOWLEDGEMENT

The authors would like to thank Prof. Phouc Tran-Gia for his valuable discussion and the stimulating environment which was a prerequisite for that work.

REFERENCES

[1] P. Pan, G. Swallow, and A. Atlas, "RFC4090: Fast Reroute Extensions to RSVP-TE for LSP Tunnels," May 2005.

[2] R. Cetin and T. D. Nadeau, "Multiprotocol Label Switching (MPLS) Traffic Engineering Management Information Base for Fast Reroute," http://www.ietf.org/internet-drafts/draft-ietf-mpls-fastreroute-mib-04.txt, August 2005.

[3] J.-P. Vasseur, Z. Ali, and S. Sivabalan, "Definition of an PRO node-id subobject," http://www.ietf.org/internet-drafts/draft-ietf-mpls-nodeid-subobject-07.txt, November 2005.

[4] J.-P. Vasseur, M. Pickavet, and P. Demeester, *Network Recovery*. Elsevier, 2004, pp. 397–422.

[5] H. Saito and M. Yoshida, "An Optimal Recovery LSP Assignment Scheme for MPLS Fast Reroute," in *International Telecommunication Network Strategy and Planning Symposium (Networks)*, June 2002, pp. 229–234.

[6] D. Wang and G. Li, "Efficient Distributed Solution for MPLS Fast Reroute," in 4^{rd}*IFIP-TC6 Networking Conference (Networking)*, Waterloo, Onatrio, Canada, May 2005, pp. 502 – 513.

[7] R. Martin, M. Menth, and K. Canbolat, "Capacity Requirements for the Facility Backup Option in MPLS Fast Reroute," in *IEEE High Performance Switching and Routing (HPSR)*, Poznan, Poland, June 2006.

[8] A. Autenrieth and A. Kirstädter, "Engineering End-to-End IP Resilience Using Resilience-Differentiated QoS," *IEEE Communications Magazine*, vol. 40, no. 1, pp. 50–57, Jan. 2002.

[9] J. Moy, "RFC2328: OSPF Version 2," April 1998.

[10] ISO, "ISO 10589: Intermediate System to Intermediate System Routing Exchange Protocol for Use in Conjunction with the Protocol for Providing the Connectionless-Mode Network Service," 1992.

[11] G. Iannaccone, C.-N. Chuah, S. Bhattacharyya, and C. Diot, "Feasibility of IP Restoration in a Tier-1 Backbone," *IEEE Network Magazine (Special Issue on Protection, Restoration and Disaster Recovery)*, March 2004.

[12] A. Nucci, B. Schroeder, S. Bhattacharyya, N. Taft, and C. Diot, "IGP Link Weight Assignment for Transient Link Failures," in 18^{th}*International Teletraffic Congress (ITC)*, Berlin, Sept. 2003.

[13] B. Fortz and M. Thorup, "Robust Optimization of OSPF/IS-IS Weights," in *International Network Optimization Conference (INOC)*, Paris, France, Oct. 2003, pp. 225–230.

[14] M. Menth, "Efficient Admission Control and Routing in Resilient Communication Networks," PhD thesis, University of Würzburg, Faculty of Computer Science, Am Hubland, July 2004.

[15] M. Shand and S. Bryant, "IP Fast Reroute Framework," http://www.ietf.org/internet-drafts/draft-ietf-rtgwg-ipfrr-framework-04.txt, October 2005.

[16] A. Atlas and A. Zinin, "Basic Specification for IP Fast-Reroute: Loop-free Alternates," http://www.ietf.org/internet-drafts/draft-ietf-rtgwg-ipfrr-spec-base-04.txt, July 2005.

[17] G. Schollmeier, J. Charzinski, A. Kirstädter, C. Reichert, K. J. Schrodi, Y. Glickman, and C. Winkler, "Improving the Resilience in IP Networks," in *IEEE Workshop on High Performance Switching and Routing (HPSR)*, Torino, Italy, June 2003.

[18] M. Menth and R. Martin, "Network Resilience through Multi-Topology Routing," in *The* 5^{th} *International Workshop on Design of Reliable Communication Networks*, Island of Ischia (Naples), Italy, Oct. 2005.

[19] M. Menth, J. Milbrandt, and A. Reifert, "Sensitivity of Backup Capacity Requirements to Traffic Distribution and Resilience Constraints," in 1^{st}*Conference on Next Generation Internet Networks Traffic Engineering (NGI)*, Rome, Italy, Apr. 2005.

[20] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, and C.-N. Chuah, "Characterization of Failures in an IP Backbone," in *IEEE Infocom*, Hongkong, Mar. 2004.

[21] B. M. Waxman, "Routing of Multipoint Connections," *IEEE Journal on Selected Areas in Communications*, vol. 6, no. 9, pp. 1617–1622, 1988.

[22] E. W. Zegura, K. L. Calvert, and M. J. Donahoo, "A Quantitative Comparison of Graph-Based Models for Internet Topology," *IEEE/ACM Transactions on Networking*, vol. 5, no. 6, pp. 770–783, 1997.