Capacity Requirements for the Facility 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 which is closest to the outage location to achieve an extremely fast reaction time. We review the facility backup that is an option for MPLS-FRR that deviates the traffic via a bypass around the failed elements. Basically, the backup path can take the shortest path that avoids the outage location from the point of local repair to the merge point with the primary path. We suggest two new simple modifications that lead to a new path layout which can be implemented by the facility backup. We evaluate the backup capacity requirements, the length of the backup paths, and the number of backup paths 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 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 path. The facility backup concept deviates several label switched paths (LSPs) over a single bypass 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.

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 for setting 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 time consuming for medium-size or large networks. The authors of [6] present a distributed online algorithm for the one-to-one backup that can be used when LSPs are set up and torn down on demand. Guidelines for the setup of good backup paths for the facility backup and an analysis thereof are still needed.

In this paper, we discuss the path layout for the facility backup. 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 for the facility backup concept and obtain new MPLS-FRR mechanisms that can be implemented by existing protocols. We calculate the required capacity for our proposed MPLS-FRR facility 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 take advantage of that fact and require less capacity than standard solutions.

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 facility 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 [7]. 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 [8] and IS-IS [9] 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 [10] 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 [11], [12].

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 [13]. 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.

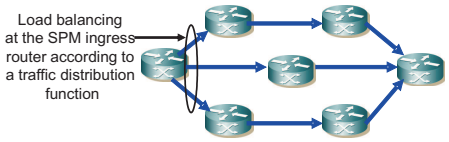


Fig. 1. The SPM performs load balancing over disjoint paths according to a traffic distribution function which depends on the working paths.

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 [14]–[17].

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.

A. Local Repair Options in the MPLS Fast Reroute Framework

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 LSPs 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. To protect a primary path against a link or router failure, the router preceding the failed element 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 element. In case of a link failure, this is the only constraint. In case of a router failure, the backup path must additionally not contain all links adjacent to the failed router. Note that the primary path cannot be protected against the failure of its head-end or tail-end label switched router (LSR). The one-to-one backup concept requires at least one separate backup path per primary LSP at each PLR. This leads to a large number of backup paths.

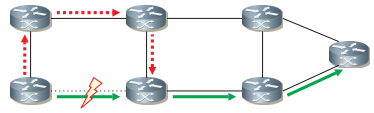
The facility backup in contrast sets up a backup path from the PLR to an upstream router of the protected LSP. This router is called merge point (MP) as it merges the backup path with the protected LSP. Since the backup path bypasses the failure location, it is called bypass LSP. Unlike detour LSPs, a bypass LSP can protect multiple primary LSPs that share the same PLR and MP, which has a large potential to reduce the number of required backup paths. In the following, we point out the placement of the MP to protect against link or router failures.

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

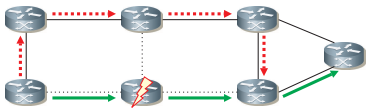
b) Router Bypass: To protect a primary path against a router failure, the router preceding the failed router acts as PLR by redirecting the traffic onto a bypass LSP towards the next-next hop (NNHOP) LSR of the PLR. Thus, the neighboring

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 2(a) and the $RouterBypass(PLR, NNHOP)$ in Figure 2(b) from the same PLR within the same flow take different paths due to their specific requirements.



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



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

Fig. 2. Facility backup link and router bypasses.

B. Backup Path Configuration for Bypass LSPs

In this section we consider the backup path configuration for 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 [4]. 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.

We now approximate the number of required backup paths for the 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 number of adjacent links of router r is given by its node degree $deg(r)$. The average node degree in a network is $deg_{avg} = \frac{2 \cdot m}{n}$. The network requires $2 \cdot m$ link bypasses to protect against the failures of m different links in each direction. 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, $n \cdot d \cdot (d-1)$ 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 to protect against all single link and router failures is $2 \cdot m + n \cdot deg_{avg} \cdot (deg_{avg} - 1) = 2 \cdot m \cdot deg_{avg}$.

2) First Modification: Substituting Link Bypasses with Router Bypasses: A link failure can be protected by a $LinkBypass(PLR, NHOP)$ from the PLR to the NHOP. But in most cases it can also be protected by the $RouterBypass(PLR, NNHOP)$ from the PLR to the NNHOP. This is possible for all links within a primary path except the last one since the latter has no NNHOP. The advantage of substituting the link bypasses with suitable router bypasses if possible will become clear in Section IV. The naive mechanism deviates all traffic carried over the failed link via a single bypass $LinkBypass(PLR, NHOP)$ to a single NHOP. In contrast, this modification distributes the traffic over several bypasses $RouterBypass(PLR, NNHOP)$ since different primary LSPs may have different NNHOPs. It leads to a better traffic distribution in failure cases. Besides, the router bypasses are already required for the protection against router failures.

3) Second Modification: Push Back Mechanism to Increase the Traffic Spreading: An increased traffic spreading also for the last link within an LSP can be achieved by a simple push back mechanism: the idea is to deviate the traffic one hop prior to the outage location.

When the link fails and the primary path contains only a single link, a normal $LinkBypass(PLR, NHOP)$ is the only option. Otherwise, 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 $PushBackBypass(PLR, NHOP)$, which starts also at the normal PLR and just visits the router previous to the outage location before heading to the NHOP router.

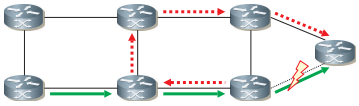


Fig. 3. $PushBackBypass(PLR, NHOP)$ – the push back concept for bypass-LSPs.

Figure 3 shows the $PushBackBypass(PLR, NHOP)$ 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.

IV. Performance Comparison

In this section we investigate the performance of the above discussed options for the facility 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 [18] 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. We mainly use the latter one since 30% of all network failures are due to router failures and 70% are due to link failures [19].

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 [13] and which incorporates features of the well known Waxman model [20], [21]. 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 $LinkBypass(PLR, NHOP)$; the set of protected failure scenarios comprises only single link failures. *(LP-Standard)*
- To provide only router protection (RP), we used the standard $RouterBypass(PLR, NNHOP)$; 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 $LinkBypass(PLR, NHOP)$ and the standard $RouterBypass(PLR, NNHOP)$ 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 bypasses by existing router bypasses (cf. Section III-B.2) wherever possible. *(LP-SLB)*
- As another alternative, we use the push back mechanism $PushBackBypass(PLR, NHOP)$ for link bypasses (cf. Section III-B.3) wherever possible. *(LP-PBM)*

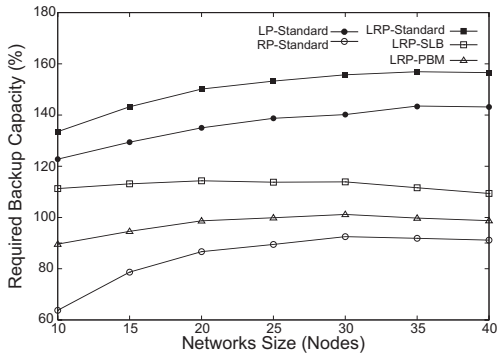
In the following these abbreviations indicate the protected failures and the applied method.

B. Backup Capacity Requirements for MPLS-FRR-Bypass

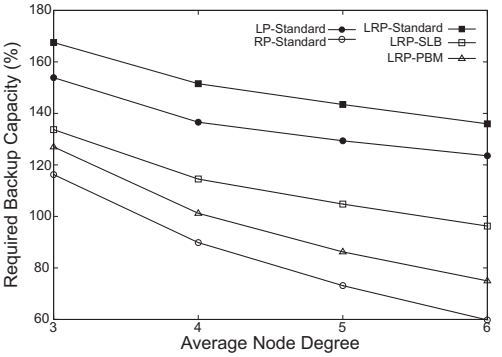
We compare the backup capacity requirements depending on the network size for the 5 above defined investigation scenarios. Each point in Figure 4(a) represents the average backup capacity for all 60 networks of a specific size and the respective investigation scenario while each point in Figure 4(b) 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.

Router protection only with RP-Standard requires the least resources, in particular less resources than link protection only. This is at first counterintuitive since router failures affect also several adjacent links, but there are two reasons to explain that phenomenon.

The curve for RP-Standard increases significantly for small networks in Figure 4(a). 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 $LinkBypass(PLR, NHOP)$ backup paths of LP-Standard have a single point of local repair (PLR) and a single merge point (MP) at the next hop (NHOP) while the $RouterBypass(PLR, NNHOP)$ backup paths have different PLRs or different MPs at the next next hop (NNHOP).



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



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

Fig. 4. Impact of the network characteristics, the protected failures, and the resilience mechanism on the required backup capacity for facility backup.

Thus, the traffic is deviated over a larger number of different bypasses starting from and ending at different locations in the network, which is illustrated in Figure 5. As a consequence, the required backup capacity for the same scenario is distributed over a larger number of different bypasses 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 4(b) with an increasing average node degree.

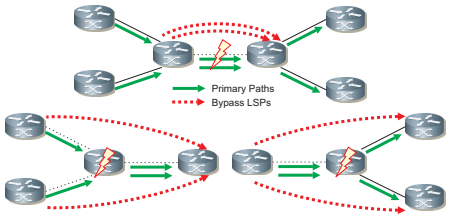


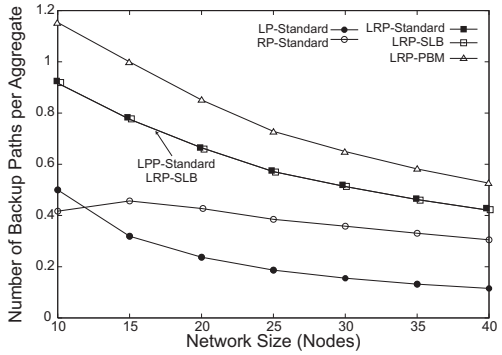
Fig. 5. In case of router failures the traffic is deviated from/to different locations in the network which leads to a better traffic distribution than in case of link failures.

LRP-Standard uses the backup paths of both RP-Standard and LP-Standard. Since link bypasses allocate their capacity at different locations than router bypasses, it requires clearly more capacity than their maximum. The increased traffic distribution that lead to reduced backup capacity requirements with RP-Standard (cf. Figure 5) motivated the substitution of link bypasses (SLB) concept. The substitution of the $LinkBypass(PLR, NHOP)$ backup paths by suitable $RouterBypass(PLR, NNHOP)$ backup paths – where possible – leads to a notable reduction of required backup capacity in Figures 4(a) and 4(b). Here, different NNHOPs act as MPs and increase the backup capacity sharing potential. The LRP-SLB concept requires 22-49% less capacity than LRP-Standard although it protects against exactly the same failures. However, the last links of the primary paths cannot be protected by suitable link bypasses. Hence, the push back mechanism (PBM) increases the traffic spreading through the $PushBackBypass(PLR, NHOP)$ also for the last link if the path contains more than one link. It requires additional 10 to 22% less capacity than LRP-SLB. Note that LRP-SLB and LRP-PBM require 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 4(a) illustrates that the network size has a small impact on the required backup capacity while Figure 4(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.

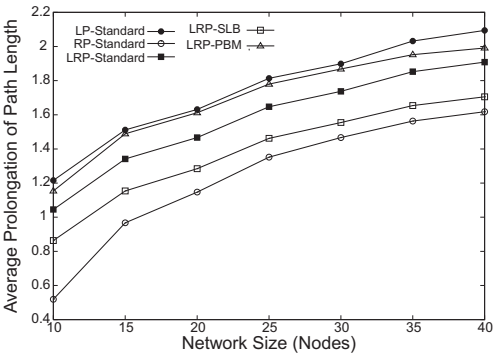
C. Configuration Overhead: Path Length and Number of Backup Paths

As mentioned above, resilience mechanisms differ regarding their configuration overhead. The number of the backup 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.

Figure 6(a) shows the average number of bypass LSPs per primary LSP depending on the network size. The number of backup path for LP-Standard is exactly the number of links m. This yields an average per aggregate of $\frac{m}{n \cdot (n-1)}$ and decreases with the network size. In Section III-B.1 we approximated the number of backup paths for RP-Standard as $n \cdot deg_{avg} \cdot (deg_{avg} - 1)$. The results of our evaluation in Figure 6(a) reveal that this is an upper bound only. Not all routers serve as transit nodes and not all combinations to transport transit traffic over the adjacent links of a node are actually used. This effect is extremely strong for small networks where many aggregates are direct connections between neighboring nodes. LRP-Standard uses both all link bypasses from LP-Standard and all router bypasses from RP-Standard and, therefore, its number of backup paths is their sum. LRP-SLB substitutes link bypasses with router bypasses for all links within a primary LSP except the last one. Since each link is at least once the last link within the primary LSP that consists of exactly one link connecting neighboring nodes, this does not reduce the number of required backup paths. Finally, LRP-BPM uses additional bypasses for the last link within primary LSPs that consist of more than one link and thus increases the number of backup



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



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

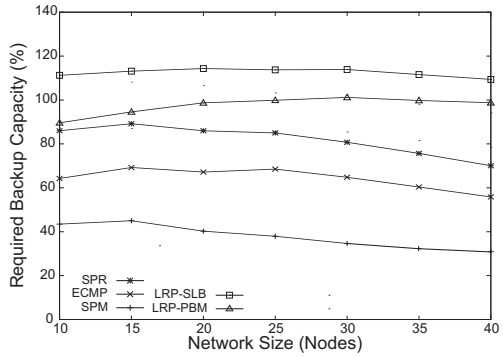
Fig. 6. Impact of the network size, the protected failures, and the protection method on the configuration overhead.

LSPs slightly. However, the number of backup paths remains clearly below one LSP per aggregate for all bypass concepts and most networks. This emphasizes the strength of the facility backup option to keep the configuration overhead small.

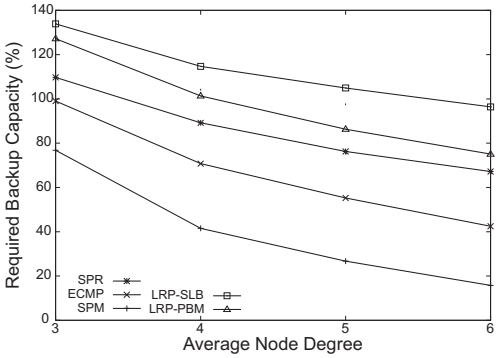
We now consider the path lengths for the bypass-LSPs. In case of a failure, the part of the primary LSPs from the PLR to the MP cannot be used anymore and the traffic is deviated over a bypass. This deviation around the outage location mostly prolongs the path. In case of a link failure, LP-Standard replaces one link that directly connects two nodes by a $LinkBypass(PLR, NHOP)$. No alternative connection between PLR and NHOP can be found that is shorter than two links since our networks have no parallels. Therefore, the bypass prolongs the original paths at least by one link as shown in Figure 6(b). In case of a router failure, RP-Standard replaces two links by a $RouterBypass(PLR, NNHOP)$. Here, it is possible to find a bypass of equal length. Hence, the prolongation caused by the bypasses for RP-Standard is much smaller than for LP-Standard and on average below 1 for small networks. LRP-Standard falls in between RP- and LP-Standard as it is a combination of both concepts. The substitution of the $RouterBypass(PLR, NNHOP)$ for the $LinkBypass(PLR, NHOP)$ by LRP-SLB reduces the path length relative to LRP-Standard since again two links of the original path are replaced by a bypass of possibly the same length. The $PushBackBypass(PLR, NHOP)$ inserts an additional link to push the traffic backwards and must increase the path length further. However, the path prolongation is still smaller than for LP-Standard. In general, in larger networks it becomes more unlikely to find bypasses of the same length as the original bypassed part. The backup path length increases with the network size.

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

In previous work [13] 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 facility 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. 7. 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 7(a) and 7(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. Both sophisticated facility backup concepts LRP-SLB and LRP-BPM require more backup capacity than the simple SPR mechanism, but the facility backup reacts within tens of milliseconds while the restoration mechanism reacts only within seconds. LRP-SLB 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 facility 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 which was introduced by the IETF 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 contrasted both options briefly and then we considered a simple standard mechanism that sets up link and router bypasses for the facility backup for all single link and node failures, respectively. The backup paths take the shortest paths that avoid the outage location. Then, we proposed a link bypass substitution (SLB) approach and an additional push back mechanism (PBM) to reduce the required 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 facility backup. To that end, we conducted a parametric study taking into account 420 artificial networks with different topological properties. Our results showed that the proposed modifications SLB and in particular PBM reduce the required backup capacity compared to the standard approach due to a better distribution of the backup traffic in failure cases. This happens at virtually no cost for LRP-SLB and even reduces the path length while LRP-PBM uses slightly longer backup paths. Remarkably, LRP-SLB and LRP-PBM protect both link and router failures with less backup capacity than LP-Standard that protects only link failures. 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). All facility backup mechanisms require more backup capacity than SPR, but they react 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.

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] 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.

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

[9] 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.

[10] 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.

[11] 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.

[12] 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.

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

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

[15] 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.

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

[17] 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.

[18] 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.

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

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

[21] 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.