Using SRLGs to Enhance Backup Path Computation

Mohand Yazid SAIDI [a] Bernard COUSIN [b] Jean-Louis LE ROUX [c]

[a]IRISA/INRIA, Université de Rennes I - Campus de Beaulieu, 35042 Rennes, France
msaidi@irisa.fr

[b]IRISA, Université de Rennes I - Campus de Beaulieu, 35042 Rennes, France
bcousin@irisa.fr

[c]France Télécom, 2 Avenue Pierre Marzin, 22300 Lannion, France
jeanlouis.leroux@orange-ftgroup.com

Abstract

To cope quickly with all types of failure risks (link, node and Shared Risk Link Group (SRLG)), each router detecting a failure on an outgoing interface activates locally all the backup paths protecting the primary paths which traverse the failed interface. With the observation that upon a SRLG failure, some active backup paths are inoperative and don't really participate to the recovery (since they don't receive any traffic flow), we propose a new algorithm (SRLG Structure Exploitation Algorithm or SSEA) exploiting the SRLG structures to enhance the admission control and improve the protection rate.

With our algorithm, more flexibility is provided for the backup path selection since a backup path which protects against the failure of a link belonging to a SRLG does not systematically bypass all the links of that SRLG. Moreover, our algorithm permits to save more bandwidth because it does not allocate the bandwidth for the inoperative backup paths even if they are activated.

Simulations show that our algorithm SSEA decreases the ratio of rejected backup paths and, it reduces in distributed environments the average number of messages sent to manage the bandwidth information necessary for the backup path computation.

Key words: network, local protection, SRLG, bandwidth sharing, path computation

---

With the advent of MPLS (MultiProtocol Label Switching) [3] in the last decade, local protection is provided in efficient manner. In fact, MPLS offers a great flexibility for path (Label switched Path or LSP) selection and provides mechanisms allowing resource[1] reservations[2] and backup path preconfigurations[3]. Moreover and contrarily to the local protection in low layers (e.g. p_cycles [4]), MPLS permits permits the separation of the traffic in several classes and to choose the classes of traffic to be protected.

In order to cope with any physical failure[4] in a logical (MPLS/IP) level, three types of failure risks are defined: link, node and Shared Link Risk Group (SRLG). The first type of failure risk corresponds to the risk of a logical link failure due to the breakdown of an exclusive physical component of the logical link. The second type of failure risk corresponds to the risk of a logical node failure due to the breakdown of an exclusive physical component of the logical node. Finally, the third type of risk corresponds to a set of logical links that share a common physical component (optical fiber, crossconnect, etc.) whose failure may impact all links in the set [5–7].

Two types of backup LSP are defined for MPLS local protection [8]: Next HOP (NHOP) LSP and Next Next HOP (NNHOP) LSP. A NHOP LSP (resp. NNHOP LSP) is a backup path protecting against link failure (resp. node failure); it is setup between a primary node called Point of Local Repair (PLR) and one primary node downstream to the PLR (resp. to the PLR next-hop) called Merge Point (MP). Such backup LSP bypasses the link (resp. the node) downstream to the PLR on the primary LSP. When a link failure (resp. node failure) is detected by a node, this later activates locally all its NHOP and NNHOP (resp. its NNHOP) backup LSPs by switching traffic from the affected primary LSPs to their backup LSPs.

In order to ensure that there is enough bandwidth after a failure (i.e. to guarantee the communication repair success), the backup paths should reserve the bandwidth they need beforehand. Besides, to decrease the bandwidth allocations and accept much more connection establishments, the practical hypothesis of single failure is often adopted [9,6,10,11,7,12,13]. With such hypothesis, all the backup paths protecting against failures of different components can share their bandwidth allocations (on their common links) since they cannot be active at the same time.

Several classical approaches [9,6,10,11,7,12,13] are developed to optimize the bandwidth allocated to the backup paths (called also protection bandwidth). In such apthat a backup path is activated if its head-end router detects a failure on the protected link or node. As only the activate backup paths can really use their resources, the classical approaches propose to allocate the maximum of cumulative bandwidths of backup paths which could be active at the same time on each link.

Contrarily to the protection against link and node failure risks which uses only one backup path for each primary path, the protection against a SRLG risk employs several backup paths, one for each link which belongs to the primary protected path and to the SRLG. Moreover, for fast recovery from a SRLG failure, all the backup paths which protect against the failure of links belonging to the failed SRLG will be activated simultaneously. With the observation that some activated backup paths don't really use their resources (bandwidth) after a SRLG failure (because the traffic of the primary paths they protect was switched towards other backup paths which bypass their head-end routers), we propose in this article to enhance the protection quality and increase the bandwidth sharing by extending its application to some activated backup paths. In our approach, we explore the SRLG structures to determine the active backup paths which do not really use their resources after certain SRLG failures. Such active backup paths are in reality inoperative after such failures since they don't consume the bandwidth. In order to decrease the protection bandwidth that is allocated on each link, we propose to limit the concurrence for protection bandwidth to the backup paths which can be operative at the same time. In our proposition, more flexibility is provided for backup path selection since a backup path does not systematically bypass all the links sharing a SRLG with the protected link.

The rest of this article is organized as follows: In section 2, we review some works related to the bandwidth sharing. In section 3, we give a SRLG structure based classification of the backup paths that permits to improve the backup path computation. In our classification, the backup paths are grouped into two sets: the operative backup paths which receive the rerouted traffic after a failure, and the inoperative backup paths which do not receive any traffic after a failure, although they are active. In section 4, we propose and describe a new algorithm (SRLG Structure Exploitation Algorithm or SSEA) which decreases the protection bandwidth allocations and provides more flexibility for the backup path selection. In section 5, we give some ideas and propositions for the implementation of the SRLG structure exploitation algorithm in both centralized and distributed environments. In the next section, we present and analyze some simulation results and we give, in section 7, computing the backup paths. To minimize the quantity of bandwidth allocated on links while avoiding the bandwidth constraint violation (bandwidth insufficiency), the Backup Path Computation (BPC) algorithms require the knowledge of some information like the primary and backup paths, bandwidth allocations and protected risks.

Depending on the number of simultaneous failures that we would tolerate, the quantity of bandwidth reserved on each link for protection can be high (large number of simultaneous failures) or low (small number of simultaneous failures). Indeed, the number of simultaneous failures that can be processed successfully determine all the failure scenarios, which in turn control the number and structures of the backup paths which provide the protection. Due to the rarety of multiple failures[5] and the complexity to protect (in local and proactive manner) against this type of failure, and in order to increase the bandwidth availability (increase the bandwidth sharing), most of works in the literature consider only single failures [9,6,10,11,7,12,13]. With such type of failure (i.e. a single failure), the quantity of bandwidth that should be reserved on each link for protection, depends on the cumulative bandwidth of the paths which could be active at the same time after any single failure occurrence. Two strategies of bandwidth sharing are defined to reduce the protection bandwidth allocations: backup-backup bandwidth sharing and backup-primary bandwidth sharing.

In the first strategy (backup-backup bandwidth sharing), the quantities of protection bandwidth allocated on links are decreased significantly with the application of the bandwidth sharing between the backup paths [9,6,10,11,7,12,14]. This type of bandwidth sharing is made possible thanks to the hypothesis of single failures which ensures that some backup paths cannot be active (they don't use their bandwidth) at the same time. Thus, only the backup paths protecting against a same risk can be in concurrence for bandwidth allocation.

When a new backup path is being computed, control admission is applied on all its links to verify the bandwidth constraints. Two concepts are defined in [6] to ensure the respect of the protection bandwidth constraints: protection failure risk group and protection cost.

The protection failure risk group of a backup path b, denoted PFRG (b), is a set

$$(b,r) \mapsto y = \begin{cases} 1 & \text{if } b \text{ is active upon the failure of } r \\ 0 & \text{otherwise} \end{cases}$$

We determine the protection failure risk group of a backup path b as follows:

$$PFRG(b) = \{r \mid r \in Risks \text{ and } Act(b,r) = 1\} \qquad (1)$$

The protection cost of a risk r on a link λ, denoted δ_r^λ, corresponds to the cumulative bandwidth of the backup paths which will be activated on the unidirectional link λ upon a failure of the risk r. It is computed as follows ($bw(b)$ is the bandwidth required by the backup path b):

$$\delta_r^\lambda = \sum_{b \in BPaths \wedge \lambda \in b} Act(b,r) \times bw(b) \qquad (2)$$

For a SRLG risk $srlg$ composed of link risks $(l_1, l_2, \ldots, l_n)$, the protection cost on a link λ verifies always the following equality: $\delta_{srlg}^\lambda = \sum_{0<i\leq n} \delta_{l_i}^\lambda$.

To compute a new backup path b, only the unidirectional links λ verifying the following inequality can be used:

$$Pr_\lambda + Max_{r \in PFRG(b)}(\delta_r^\lambda) + bw(b) \leq C_\lambda \qquad (3)$$

where Pr_λ is the the cumulated bandwidth of the backup paths traversing the arc λ and C_λ is the capacity of the arc λ.

To cope successfully with any single failure, the amount of protection bandwidth Bk_λ that should be reserved on each link λ is determined as follows:

$$Bk_\lambda = Max_r(\delta_r^\lambda) \qquad (4)$$

The backup-backup bandwidth sharing strategy improves substantially the bandthis bandwidth information before its advertisement in the network could give some interesting and practical solutions [9,11,7,12,14]. For instance, to decrease the size and frequency of the advertisement messages, the Kini's heuristic [9] suggests to approximate all the protection costs on a given unidirectional link by the highest protection cost on that link (i.e. $8(\prod\ r) :\ \pm_r^{\prod}$ is approximated by $Max_r\ (\pm_r^{\prod})$). In this way, a given unidirectional link $\prod$ can be used to establish a new backup path b if it verifies the following inequality: $Pr_{\prod} + Max_r\ (\pm_r^{\prod}) + bw(b) \sum C_{\prod}$.

In the second strategy (backup-primary bandwidth sharing), another style of bandwidth sharing (bandwidth sharing between the primary and backup paths) is applied to decrease the protection bandwidth allocated on links. This type of sharing was proposed for the first time in [13]. It suggests to (pre)allocate the bandwidth freed by the deactivated (or bypassed) primary path segments upon a failure of a risk r to the backup paths which will be activated to recover from that failure. For instance, when a protected link (resp. an unprotected link) u-v traversed by a primary path p fails, a quantity of bandwidth equal to the bandwidth of p is freed on all the links located between the end nodes of the backup path repairing the primary path p (resp. on all the links located between the failed link and the destination node of the primary path p). Such freed bandwidth is then assigned to the backup paths which will be activated to recover from the failure of link u-v.

To avoid the violation of the bandwidth constraints with this second strategy, only the unidirectional links $\prod$ verifying the following inequality can be selected to be in a new backup path b:

$$Pr_{\prod} + Max_{r2PFRG(b)}\ (\pm_r^{\prod} + bw(b)\ °\ F_r^{\prod}; 0) \sum C_{\prod} \qquad (5)$$

To cope successfully with any single failure, the amount of protection bandwidth $Bk_{\prod}$ that should be reserved on each link $\prod$ is determined as follows:

$$Bk_{\prod} = Max_r\ (\pm_r^{\prod}\ °\ F_r^{\prod}; 0) \qquad (6)$$

where $F_r^{\prod}$ is the total primary bandwidth freed on the link $\prod$ after a failure of the risk r.

of the second strategy of bandwidth sharing requires the knowledge of the quantities of primary bandwidth freed on the links for all single failures.

Although there are some activated backup paths which do no receive any traffic after a SRLG failure, both the bandwidth sharing methods of the first and the second strategies allocate them bandwidth. This wastes bandwidth and blocks uselessly some protection requests.

3 Motivations

For fast recovery, each router detecting a failure on one of its outgoing interfaces activates locally all the backup paths which protect the primary paths traversing the failed interface. Although active, some backup paths (inoperative backup paths) do not participate to the recovery of the affected communications because the traffic was already redirected by upstream routers onto other backup paths (operative backup paths) bypassing their head-end routers.

By limiting the concurrence for the protection bandwidth to the operative backup paths, we decrease the protection bandwidth allocations. Besides, with the restriction of the protection failure risk group of a backup path b to the risks whose failure operates the backup path b, we provide more flexibility for the path selection.

Before describing our improvement propositions, we show in the next subsection the difference between the set of the active backup paths and the set of the operative paths, upon failure. Next, we propose and describe an algorithm permitting the determination of the operative backup paths, by using the structures of the SRLGs.

3.1 Active backup paths vs operative backup paths

Due to the difficulty to distinguish quickly between the types of failure (node, link or SRLG), each router detecting a failure on an outgoing interface activates all the backup paths which protect the primary paths traversing[6] the affected interface.

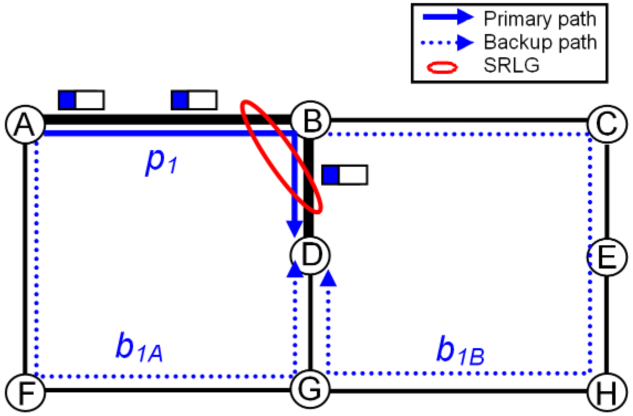
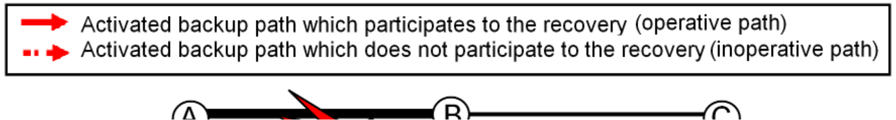
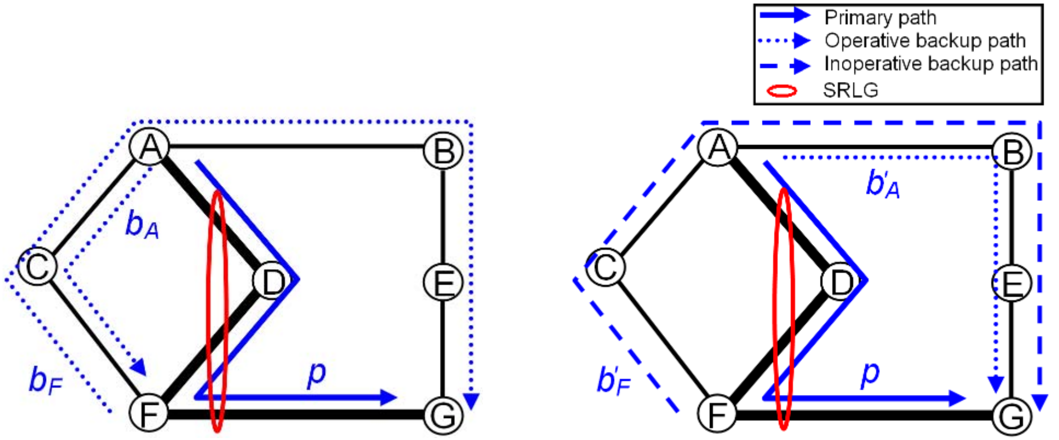


Fig. 1. Local protection of a primary path

really use its resources (particularly the bandwidth). Hence, the bandwidth allocated for such inoperative path can be freed and reallocated to other paths. Contrarily to the backup path b_1, the other backup path b_2 really participates to the recovery since it reroutes the traffic of the affected primary path. This path is considered as operative. Its resources (particularly the bandwidth) cannot be reallocated to other paths.

In figure 1, two backup paths b_{1A} (A! F! G! D) and b_{1B} (B! C! E! H! G! D) are setup to protect the primary path p_1 (A! B! D) against the failure of the four following risks: node B, link A-B, link B-D and SRLG srlg = (A-B, B-D). When the router A (resp. router B) detects a failure on the interface leading to its adjacent router B (resp. router D), it activates locally the backup path b_{1A} (resp. b_{1B}) which protects the unique primary path traversing the failed interface. Hence, for the failure of node B or the failure of link A-B (resp. the failure of link B-D), traffic of the affected primary path p_1 will be switched onto the unique activated backup path b_{1A} (resp. b_{1B}). As only one outgoing interface of the primary path routers can be affected upon a single link or a single node failure, we conclude that at most one backup path per primary path could be activated. As a result, all the backup paths activated to recover from a link or node failure really receive and reroute the traffic





(a) Two operative backup paths upon the SRLG failure

(b) One operative backup path upon the SRLG failure

Fig. 3. Operative backup paths

of the affected primary paths.

With risks of type SRLG however, some activated backup paths do not receive or reroute the traffic of the affected primary paths. For instance, when the SRLG srlg in figure 1 fails, all the end routers of the srlg's links (i.e. routers A, B and D) will detect a failure. As a result, all the backup paths protecting an affected primary path and whose head-end router is an end router of the links belonging to the failed SRLG will be activated (cf. figure 2). Typically, the backup path b_{1A} (resp. b_{1B}) will be activated since it protects the affected primary path (p_1) and its head-end router A (resp. B) is an end router of a link A-B (resp. B-D) belonging to the affected SRLG srlg. As the traffic switching toward a backup path results in the bypassing of a primary path segment located between the head-end and the tail-end routers of the backup path, we deduce that only the backup path b_{1A} receives and reroutes the traffic of the affected primary path p_1 after the recovery from the failure of the SRLG srlg. Indeed, after the activation of the backup path b_{1A}, the traffic of the primary path p_1 is forwarded on the path A! F! G! D: the head-end router B of the second activated backup path b_{1B} is bypassed and thus, no packet traverses this backup path.

(1) The backup path b protects against the failure of a link belonging to the SRLG srlg.
(2) There is no backup path b’ (b’ 6= b) such as:
  ≤ b’ protects the primary path p against the failure of a link belonging to the SRLG srlg,
  ≤ the sub-path of p located between the end routers of b’ contains, as transit router, the head-end router of the backup path b.

To better understand the procedure of determination of the operative backup paths upon a SRLG failure, let us consider an example. In figure 3, a primary path p (A! D! F! G) traversing the unique SRLG srlg = (A-D, D-F, F-G) of the network is established. To protect this primary path against the failure of link F-G, we setup a same NHOP backup path F! C! A! B! E! G in both sub-figures (b_F in the sub-figure 3(a) and b^0_F in the sub-figure 3(b)). To protect the primary path p against the failure of node D (and against the failure of link A-D), we used a different backup path in each sub-figure. Hence, in sub-figure 3(a), we setup the backup path b_A (A! C! F) and in sub-figure 3(b), we configured the backup path b^0_A (A! B! E! G).

Upon a failure of the SRLG srlg, the nodes A and F activate the backup paths b_A and b_F in the sub-figure 3(a) (resp. the backup paths b^0_A and b^0_F in the sub-figure 3(b)) for recovery. In figure 3(a), both the backup paths b_A and b_F become operative after the recovery from the SRLG failure. In fact, the backup path b_A (resp. b_F) protects the primary path p against the failure of a srlg’s link A-D (resp. F-G) and its head-end router A (resp. F) does not belong to the primary path segment located between the end routers F and G (resp. A and F) of the unique other backup path b_F (resp. b_A) protecting the primary path p (against the failure of a link in the same SRLG srlg). In figure 3(b) however, only the backup path b^0_A becomes operative (for the same reasons as b_A in figure 3(a)) upon the failure of the unique network SRLG srlg. The second backup path b^0_F is inoperative upon the failure of the SRLG srlg since there is another backup path b^0_A verifying these two conditions: 1) b^0_A protects the primary path p (i.e. the same primary path as the one protected by b^0_F) against the failure of a link (A-D) belonging to srlg. 2) the sub-path (A! D! F! G) of p located between the end routers (A and G) of b^0_A contains, as transit router, the head-end router (F) of the backup path b^0_F.

backup paths. Besides, we provide more flexibility for the backup path selection by restricting the set of failure risks that should be bypassed by the backup paths.

4.1 Decreasing the bandwidth allocation

Instead of using the activity state of backup paths to allocate the protection bandwidth, we propose here to exploite the operativity state of backup paths to reduce the protection bandwidth allocations. Before showing how to utilize the operativity state of backup paths to enhance the protection bandwidth allocation, let us defining a new function Op as follows:

$$\begin{aligned} Op : BPaths \times Risks &\rightarrow \{0, 1\} \\ (b, r) &\mapsto y = \begin{cases} 1 & \text{if } b \text{ is operative upon the failure of } r \\ 0 & \text{otherwise} \end{cases} \end{aligned}$$

where: $BPaths$ is the set of all the backup paths and $Risks$ is the set of all the network failure risks.

As only the operative backup paths receive traffic upon failure, we propose to limit the concurrence for the protection bandwidth allocation to the operative backup paths. In this way, the protection bandwidth allocations are reduced since a backup path which is inoperative after a failure of a given SRLG does not require to reserve any unit of bandwidth to cope with the failure of that SRLG.

To manage the set of risks whose failure operates a backup path b, we reduce the protection failure risk group of b and define the Restricted Protection Failure Risk Group of b (or RPFRG (b)) as follows:

$$RPFRG(b) = \{r \mid r \in Risks \text{ and } Op(b, r) = 1\} \tag{7}$$

In addition to the reduction of the protection failure risk group set, we modify (2) to exploit the operative/inoperative state information when the backup paths are in (3), (4), (5) and (6), we obtain the formulas ensuring the respect of the bandwidth constraints and allowing the computation of the minimal protection bandwidth to be allocated on each unidirectional link.

Concretely, with the backup-backup bandwidth sharing, we have:

$$Pr_{\prod} + Max_{r2RPFRG(b)}(\propto_r^{\prod}) + bw(b) \sum C_{\prod} \tag{9}$$

$$Bk_{\prod} = Max_r(\propto_r^{\prod}) \tag{10}$$

With the primary-backup bandwidth sharing, we have:

$$Pr_{\prod} + Max_{r2RPFRG(b)}(\propto_r^{\prod} + bw(b) \circ F_r^{\prod}; 0) \sum C_{\prod} \tag{11}$$

$$Bk_{\prod} = Max_r(\propto_r^{\prod} \circ F_r^{\prod}; 0) \tag{12}$$

Since the set of the operative backup paths is included in the set of the activated backup paths (i.e. $8b\ 2\ BPaths : RPFRG(b)\ \mu\ PFRG(b)$)), we deduce that all the protection prices are lower or equal to their corresponding protection costs ($8(r;\prod) : \propto_r^{\prod} \sum \pm_r^{\prod}$). As a result, much more protection bandwidth is saved.

Example: Let us applying the backup-backup bandwidth sharing to the link A! B in figure 3(b).

Without the exploitation of the SRLG structures, we compute the minimal protection bandwidth $Bk1_{AB}$ allocated on the link A! B as follows:
$Bk1_{AB} = Max(\pm_{AD}^{AB}; \pm_{D}^{AB}; \pm_{FG}^{AB}; \pm_{srlg}^{AB}) = \pm_{srlg}^{AB} = 2 \pounds\ bw(p)$

With the exploitation of the SRLG structures, we compute the minimal protection bandwidth $Bk2_{AB}$ allocated on the link A! B as follows:
$Bk2_{AB} = Max(\propto_{AD}^{AB}; \propto_{D}^{AB}; \propto_{FG}^{AB}; \propto_{srlg}^{AB}) = \propto_{srlg}^{AB} = bw(p)$

4.2 Providing flexibility for the backup path selection

In addition to the protection bandwidth decrease, the exploitation of the SRLG structures in the BPC has another important advantage: it provides more flexibility for the backup path selection and improves the quality of protection (i.e. the number of protected risks on a primary path is increased) by reducing the set of risks that a backup path must bypass. In our approach, a new backup path b does not systematically bypass all the SRLGs containing the link to be protected. Instead, only the node and link to be protected and the SRLGs whose failure operates the new backup path b should be bypassed (i.e. only the risks in RPFRG (b)).

Since the set of links (and nodes) that a backup path should bypass must be known before the start of its computation, to apply our approach it would be necessary to determine beforehand whether a backup path is operative or not after a failure of any risk. By analyzing the sufficient conditions (cf. section 3.2) allowing the determination of the operative backup paths, we deduce that the links traversed by a backup path have no incidence on the operative state of that backup path upon failure. Indeed, only (1) the protected link and node, (2) the head-end router of the backup path b in computation, and (3) all the backup paths protecting a same primary path as b against the failure of an upstream link (which belongs to the same SRLG as the protected link) to the link to be protected, are used to deduce the operative state of b upon any given failure. Thus, the risks forming the restricted protection failure risks group of any backup path can be deduced before its computation, in condition that the backup paths protecting against the failures of upstream links are completely determined.

In figure 3(b) for instance, any computed backup path b^0_D protecting the primary path p against the failure of the link $D \rightarrow F$ is inoperative upon the failure of the SRLG srlg. Indeed, upon such failure, the traffic is switched by the router A onto the backup path b^0_A which joins the primary path p on a router G downstream to

4.3 SRLG structure exploitation algorithm (SSEA)

In order to decrease the protection bandwidth allocations (cf. section 4.1) and to offer more flexibility for the backup path selection (cf. section 4.1), we propose a new algorithm SSEA (cf. algorithm 1) taking into account the SRLG structures to enhance the BPC. Thus, to compute a new backup path b, we determine in the first step of our algorithm SSEA the restricted protection failure risk group of the backup path b (i.e. RPFRG (b)). This restricted protection failure risk group is formed of all the elements in PFRG (b) except the risks whose failure does not operate the backup path b. In order to denote the elements of RPFRG (b), we say that a given risk is really protected by the backup path b if and only if such risk is in RPFRG (b).

In the second step of our algorithm SSEA, we eliminate from the network topology all the links and nodes which belong to the risks in RPFRG (b). In this way, no failure risk can affect simultaneously both a primary path and one of its backup paths. Obviously, since the set of risks to be bypassed by each new backup path is reduced, more flexibility is provided for the path selection.

In order to ensure the respect of the bandwidth constraints, we apply in the third step

---

Algorithm 1 Computation of a backup path b with the SRLG structure exploitation algorithm

---

```
inputs
  A graph G = (V, E) corresponding to the network topology. V is the set of vertices
  (routers) and E is the set of edges (links)
begin_algorithm
  1. f Determination of the set RPFRG (b) which is composed of the risks whose
  failure operates the backup path bg
  RPFRG (b) √ f r n Op(b; r) = 1g
  2. f Determination of the links which should be bypassed by the backup path bg
  E” √ f ∏2 E n 9 r 2 RPFRG (b): ∏2 rg
  f Determination of the nodes which should be bypassed by the backup path bg
  V” √ f n 2 V n 9 r 2 RPFRG (b): n 2 rg
  3. f Determination of the links verifying the bandwidth constraintsg
  if backup_backup_sharing_only then
    E’ √ f ∏n ∏2 E ^ Pr∏ + Max_r2RPFRG(b) (∝∏_r) + bw(b) ∑ C∏g
```

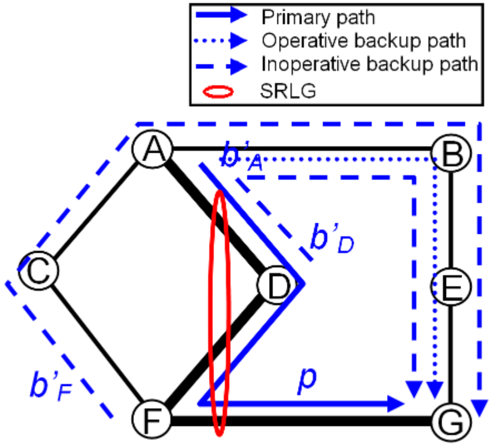


Fig. 4. A backup path traversing a link of a SRLG containing the protected link

of our algorithm SSEA inequality 9 (for the backup-backup bandwidth sharing) or inequality 11 (for the primary-backup bandwidth sharing) to select the links which can be used for the next backup path computation. Clearly, all the links which do not satisfy inequality 9 (or inequality 11 for the primary-backup bandwidth sharing) are pruned from the network topology before the BPC starts.

In the last step of our algorithm SSEA, we deduce one backup path providing the desired protection by running any path computation algorithm (e.g. CSPF) with the use of any local protection technique (one-to-one backup protection or facility backup protection [8]). Thus, our algorithm is generic and compatible with any path computation algorithm and any local protection technique.

To better understand our algorithm, let us consider the example in figure 3(b). Suppose that we are trying to compute a new backup path b_D^0 protecting the primary path p against the failure of the node F and link D-F. Assume also that all the network links have a capacity of one unit. Independently on the chosen local protection technique, the backup path b_D^0 must interconnect node D to node G.

With the application of the classical BPC algorithms, no path can support b_D^0 since such path would bypass all the links (A-D, D-F, F-G) belonging to the SRLG srlg (note that srlg is in PFRG (b_D^0) and srlg includes the protected link D-F). With our algorithm SSEA however (step 1 of algorithm 1), the probability to determine a termine the unique backup path D → A → B → E → G interconnecting node D to node G (figure 4).

Note that the three backup paths b_A^0, b_D^0, and b_F^0 (in figure 4) share totally their bandwidth on the common path segment A → B → E → G although they protect against the failure of links belonging to the same SRLG. This sharing does not induce any bandwidth constraint violation because the three backup paths b_A^0, b_D^0, and b_F^0 cannot be operative at the same time.

5 Implementation requirements for the SRLG structure exploitation algorithm

With a centralized implementation of the SRLG structure exploitation algorithm, the unique BPCE can store all the information about the network topology, the SRLG structures and the path properties (traversed links, type, bandwidth, etc.). From such information, the centralized BPCE determines the bandwidth parameter values of each link (cumulative primary bandwidth, protection prices, primary bandwidth freed) and deduces the best backup paths.

We note that to improve the protection quality, the centralized BPCE should establish a computation order for the backup paths protecting a same primary path. Indeed, to determine the final operative state of each backup path (cf. section 3.2), the BPCE should begin with the protection of the links closest to the head-end router of each primary path.

With a distributed implementation of the BPC taking account of the SRLG structures, a comparable information as that transmitted in the classical approaches [9,6,10,7,12,13] is sufficient to avoid the violation of the bandwidth constraints. For instance, the information advertised with the approach described in [6,10,12] is sufficient to decrease the bandwidth allocation. However, a very slight transformation of the advertised information (replacement of the protection cost values by the corresponding protection price values) is required with [9,7,13].

To enhance the protection quality with the distributed approaches, it is necessary order of backup paths can be imposed. Concretely, each PLR can notify[7] its downstream routers of the accomplishment of the configuration of its backup path. Thus, to guarantee the respect of the backup path computation order, each PLR should wait for the notifications of all its upstream routers before it starts to compute its backup path.

6 Analysis and simulation results

6.1 Simulation model

In order to evaluate the performances of the SRLG structure exploitation algorithm (SSEA), we compared it to the Kini's heuristic and TDRA algorithm. We chose the Kini's heuristic for its practicability whereas we opted for the TDRA algorithm for its efficiency to determine the backup paths reducing the protection bandwidth allocation.

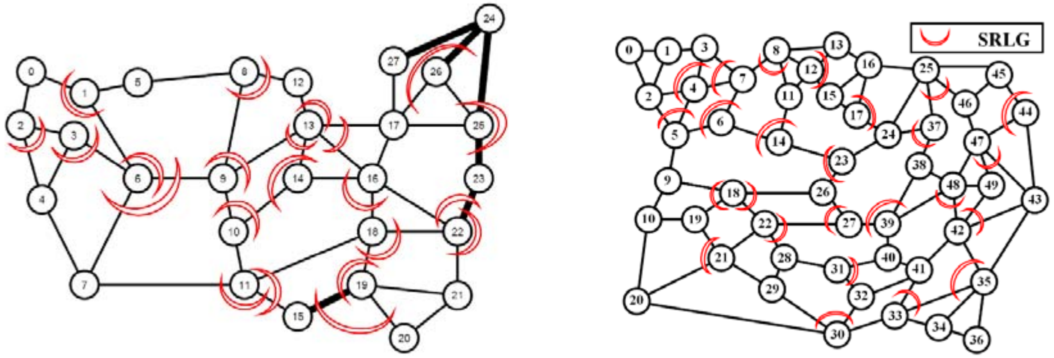
6.1.1 Comparison metrics

Four metrics are used for the comparison: ratio of rejected backup paths (RRP), relative gain in backup path rejection (RGR), normalized SRLG bandwidth (NSB) and average number of messages (ANM) transmitted in the network per configured backup path.

The first metric measures the ratio of backup paths that are rejected because of the lack of protection bandwidth on the network links. It corresponds to the ratio between the number of backup path requests that are rejected and the total number of backup path requests (RRP = #rejected protection requests / #protection requests).

The second metric calculates the gain in the RRP values obtained by using a new BPC method instead of an old one. It is determined as follows: RGR (newMeth, oldMeth) = (RRP (oldMeth) - RRP (newMeth)) / RRP (oldMeth).

The third metric measures the amount of bandwidth allocated on links to protect



(a) Medium size topology (95 risks)

(b) Large size topology (162 risks)

Fig. 5. Test topologies

For the TDRA algorithm and the Kini's heuristic, we have:
NSB = $\sum_{(r \text{ is a SRLG};\, \ell \in E)} (\delta_r^{\ell}) \,/\, \sum_{(r \text{ is a link};\, \ell \in E)} (\delta_r^{\ell})$

The fourth metric counts the (average) number of messages traversing the network links, after each backup path establishment, to maintain and update the protection bandwidth information necessary for the BPC (ANM = $\sum_{\ell \in E}$ #messages traversing (ℓ) / #accepted protection requests where E is the set of network unidirectional links).

Contrarily to the values of the metrics RRP, RGR and NSB, those of the metric ANM depend strongly on the implementation type (centralized or distributed) and on the mechanism distributing the information necessary for the BPC (flooding or targeted advertisements). In a centralized environment, any BPC demand is transmitted to the centralized server which processes it and sends back the computation results to the requesting router. Hence, independently on the bandwidth sharing strategies and on the BPC algorithms, the number of messages transmitted in the network to process a set of requests is always the same. Accordingly, it is pointless to compare the ANM of our proposition to those of the classical centralized BPC

6.1.2 Topologies, SRLGs and traffic matrix generation

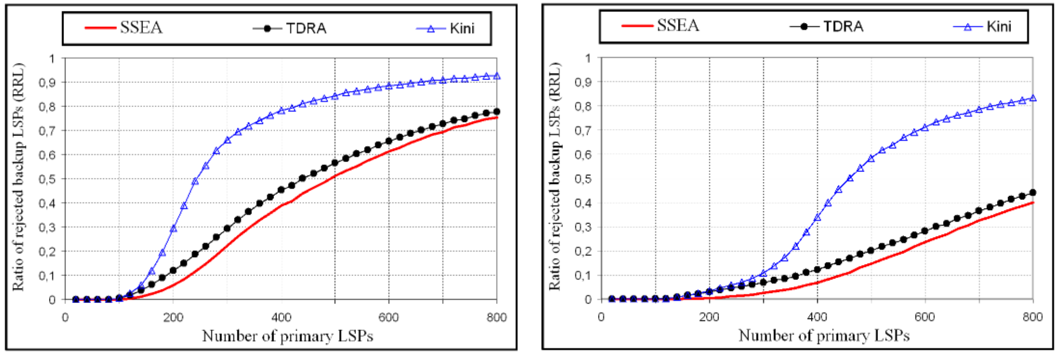
Two well known network topologies are used for our simulation. The first topology (USA network), depicted in figure 5(a), is composed of 28 routers and 45 bidirectional links. It is a network topology of a medium size where the average degree of nodes is equal to 3.21. To take SRLG failures into account, we added to the topology in figure 5(a) 22 SRLGs. These SRLG are generated so that the protection against the failure of any risk remains physically possible. The second topology, depicted in figure 5(b), is composed of 50 routers and 87 bidirectional links. It is a network topology of a large size where the average degree of nodes is equal to 3.48. To take SRLG failures into account, we added to this topology (figure 5(b)) 25 SRLGs. These SRLG are generated so that the protection against the failure of any risk remains physically possible.

The traffic matrix is generated randomly and consists of requests arriving one by one and asking for quantities of bandwidth uniformly distributed between 1 and 10. The head-end and tail-end routers of each primary path are chosen randomly among the network routers.

6.1.3 Primary and backup path computations

To focus only on the impact of our proposition on the protection bandwidth allocation and on the protection quality, we separated the task of primary path computation from that computing the backup paths (i.e. the task computing the primary path is independent from that computing the backup paths). For this to be possible, we divided the capacity of each unidirectional link in two disjoint pools: primary pool and protection pool. The primary pool is used to allocate the bandwidth for the primary paths whereas the protection pool is used for backup path bandwidth allocations.

In our simulations, we considered that the primary pool capacities are sufficient to satisfy all the requests of primary path establishment. In this manner, the same primary paths, which are computed according to the shortest path first algorithm (SPF with unitary weights), are used to compare SSEA, TDRA and Kini’s heuristic.



(a) Medium size topology (b) Large size topology

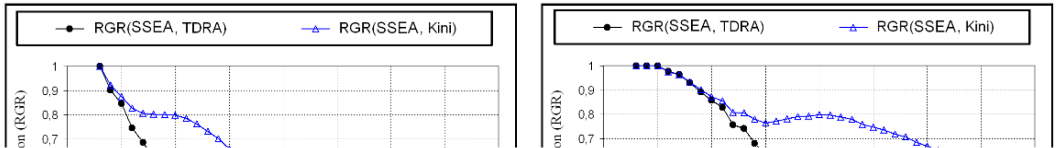
Fig. 6. Ratio of rejected backup paths (RRP)

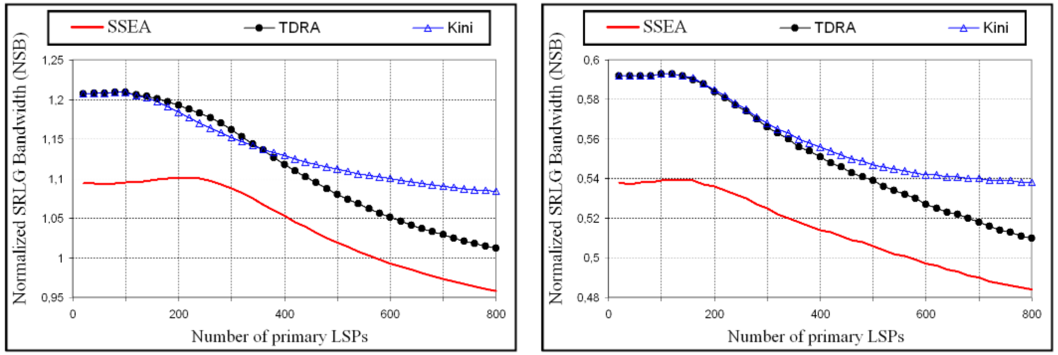
Each primary node, different from the destination node and its upstream node, computes a NNHOP backup path to protect against both its next link and node on the primary path. The upstream node of the primary path destination node uses a NHOP backup path to protect against the failure of its next link.

At each establishment of 20 primary paths, the four metrics RRP, RGR, NSB and NMN are computed for all the compared methods. We note that our results correspond to average values over 1000 runs.

6.2 Results and analysis

Figure 6 and figure 7 depict the evolution of RRP and RGR respectively as a function of the number of primary paths setup in the network (i.e. as a function of the network load). The figure 6 shows clearly that the RRP values of SSEA algorithm are lower and better (except for the 40 first primary paths where the RRP values of the three compared methods are null) than those of TDRA algorithm which are in turn lower than those of Kini's heuristic.



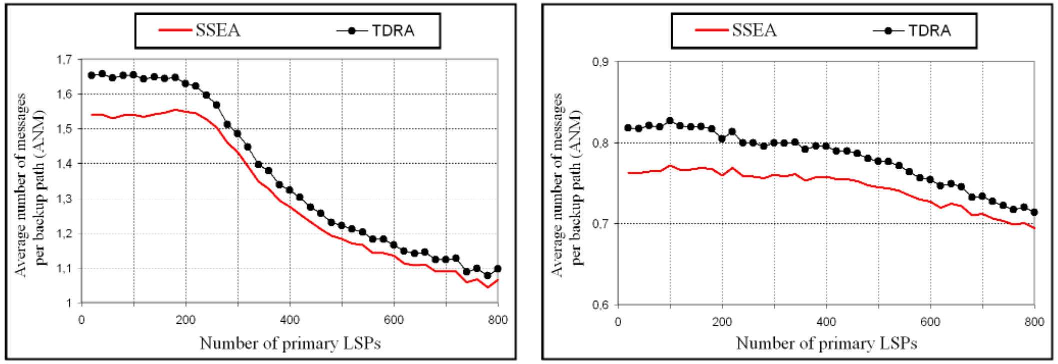


(a) Medium size topology

(b) Large size topology

Fig. 8. Normalized SRLG Bandwidth (NSB)

The wide difference in the RRP values between the Kini's heuristic and the SSEA algorithm is essentially due to the partial knowledge of the protection bandwidth information with the Kini's heuristic whereas the SSEA algorithm utilizes and has a complete knowledge of the protection bandwidth parameter information. Thus, the Kini's heuristic overestimates the bandwidth parameters required for the BPC whereas the SSEA algorithm uses exact values of these parameters in its computations. Obviously, the wide difference in the RRP values between the Kini's heuristic and the SSEA algorithm explains also the large relative gain in backup path rejection (i.e. RGR (SSEA, Kini)) when the SSEA algorithm is used instead of the Kini's heuristic. Concerning the comparison between the RRP values of TDRA and those of SSEA, we note that the difference is significant although it is not high in relation to the total number of protection requests. For instance, the difference of the RRP values in figure 6(a) varies between 5.16% and 5.76% when the number of primary paths is between 380 and 540 whereas it varies in figure 6(b) between 5% and 7.3% when the number of primary paths is between 180 and 520. In fact, for practical RRP values located between 0 and 0.1 (the number of primary paths is lower than 380 in figure 6(a) and lower than 200 in figure 7(b)), the relative gain of using SSEA instead of TDRA is larger than 56% in figure 7(a) and larger than 68% in figure 7(b) (i.e. more than 68% of the number of protection requests rejected by TDRA are satisfied with SSEA in figure 7(b)). When rejection of the protection requests is not allowed, figure 6(a) and figure 6(b) shows that the adoption of SSEA algorithm instead of TDRA permits to increase the number of protected primary paths from 60 to 80 and from 60 to 120 respectively.



(a) Medium size topology

(b) Large size topology

Fig. 9. Average number of messages sent in the network per backup path (ANM)

risks to be bypassed by each backup path (see section 4.2) with SSEA (contrarily to TDRA algorithm and Kini's heuristic which waste the protection bandwidth and bypass more risks).

Another important point to highlight concerns the high difference between the normalized SRLG bandwidth values obtained on the two test topologies. Indeed, for the same number of primary paths, the normalized SRLG bandwidth in figure 8(a) is often twice higher than that obtained in figure 8(b). This can be explained essentially by the density of SRLGs[8] in figure 5(a) (equal to 0.48) which is higher than than that obtained in figure 5(b) (equal to 0.28). According to our simulations[9], we conclude that SSEA saves more protection bandwidth and reject less backup paths than TDRA and Kini's algorithm, when the density of SRLGs is high. Indeed, larger the density of SRLGs is, more different the behaviors of SSEA and TDRA (or Kini's heuristic) are.

In figure 9, the evolution of the average number of messages transmitted in the network (ANM) as a function of the number of primary paths setup in the network is shown. In this performance study, we focused only on the SSEA and TDRA algorithms. The ANM values of the Kini's heuristic are not represented because they are very high (see [12] for details about the comparaison between the TDRA algorithm and the Kini's heuristic).

As shown in figures 9(a) and 9(b), the SSEA algorithm sends in average less mestween the SSEA algorithm and TDRA algorithm decreases slightly as the number of setup primary paths increases. This comes from the augmentation of the SRLG protection prices which induces in its turn the reduction of the rate of protected SRLGs.

Note that the performances of the SSEA algorithm can be improved by favouring primary paths which traverse more links of the same SRLGs. Moreover, designing the network topologies could take SRLGs into account to enhance the backup path computation (the location of SRLGs should be chosen so that the blocking probability is decreased and the network deployment is minimized).

7 Conclusion

In this paper, we proved that it is possible to ensure the recovery from any single failure without forcing the (new) backup paths to bypass all the SRLGs containing the links to be protected. In fact, it is possible that a first active backup path does not receive traffic upon a SRLG failure since the traffic was already rerouted onto a second active backup path bypassing the head-end router of the first backup path. In such a case, the first backup path does not require any resource (bandwidth) and acts as an inoperative backup path upon that SRLG failure. However, the second backup path acts as an operative backup path that requires the bandwidth to reroute the traffic of the affected primary path. Obviously, only the operative paths (instead of all the activated backup paths) upon a failure of a SRLG should protect against the failure of that SRLG and can be in concurrence for a resource.

As the operative state of a backup path can be determined beforehand by taking the SRLG structures into account, we proposed a new and efficient approach to compute the backup paths. Our approach permits to increase the bandwidth availability (it decreases the protection bandwidth allocations) and provides more flexibility for the backup path selection (i.e. it improves the protection quality). It can be applied in both centralized and distributed environments. It also allows efficient design of networks since an effective combination of SRLGs can permit a significant reduction of the deployment cost without a decrease (or with a slight decrease) of the

References

[1] P. Meyer, S. Van Den Bosch, N. Degrande, High Availability in MPLS-based Networks, Alcatel telecommunication review, Alcatel (4th Quarter 2004).

[2] S. Ramamurthy, B. Mukherjee, Survivable WDM Mesh Networks (Part I - Protection), in: Proceedings of 18th IEEE International Conference on Computer Communications (INFOCOM 2001), Vol. 2, 1999, pp. 744–751.

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

[4] W. Grover, D. Stamatelakis, Cycle-Oriented Distributed Preconfiguration: Ring-like Speed with Mesh-like Capacity for Self-planning Network Restoration, in: Proceedings International Conference on Communications, 1998, pp. 537–543.

[5] K. Kompella, Y. Rekhter, Routing Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS), RFC 4202 (October 2005).

[6] J. L. Le Roux, G. Calvignac, A Method for an Optimized Online Placement of MPLS Bypass Tunnels, Internet Draft draft-leroux-mpls-bypass-placement-00.txt, IETF (February 2002).

[7] M. Y. Saidi, B. Cousin, J. L. Le Roux, A Distributed Bandwidth Sharing Heuristic for Backup LSP Computation, in: Global Telecommunications Conference, 2007 (IEEE GLOBECOM '07), Washington (USA), 2007, pp. 2477–2482.

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

[9] S. Kini, K. Kodialam, T. V. Lakshman, S. Sengupta, C. Villamizar, Shared Backup Label Switched Path Restoration, Internet Draft draft-kini-restoration-shared-backup-01.txt, IETF (May 2001).

[10] J. P. Vasseur, A. Charny, F. Le Faucheur, J. Achirica, J. L. Le Roux, Framework for PCE-based MPLS-TE Fast Reroute Backup Path Computation, Internet Draft draft-leroux-pce-backup-comp-frwk-00.txt, IETF (July 2004).

[11] M. S. Kodialam, T. V. Lakshman, Dynamic Routing of Locally Restorable Bandwidth Guaranteed Tunnels using Aggregated Link Usage Information, in: Proceedings

[14] M. Y. Saidi, B. Cousin, J. L. Le Roux, Distributed PLR-Based Backup Path Computation in MPLS Networks, in: IFIP Networking 2008.

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

Mohand Yazid SAIDI has obtained a master degree from the univerity of Lille 1 (France) in 2005. He is actually a PHD student, working at the IRISA laboratory in Rennes (France). His research topics and interests include protection, MPLS and high speed networks, resource optimization, routing, QoS, multicast.

SAIDI PHOTO

Click here to download high resolution image

Bernard Cousin is a Professor of Computer Science at the University of Rennes 1, France. Bernard Cousin received in 1987 his PhD degree in computer science from the University of Paris 6.

He is, currently, member of IRISA (a CNRS-University-INSA joint research laboratory in computing science located at Rennes). More specifically, he is at the head of a research group on networking.

He is the co-author of a network technology book: "IPV6" (Fourth edition, O'Reilly, 2006) and has co-authored a few IETF drafts in the areas of Explicit Multicasting and Secure DNS.

His research interests include dependable networking, high speed networks, traffic engineering, multicast routing, network QoS management, network security, sensor networks and multimedia distributed applications.

Cousin Photo

Jean-Louis joined France Telecom eight years ago, and is currently working as Senior Architect in domotic networks and IP/MPLS networks. He is working on short-term design and deployment activities and on longer term research and development projects. He is actively contributing to the IETF, where he has been editing and co-authoring several Internet Drafts and RFCs. Jean-Louis is a frequent speaker in international conferences.

His interests are Traffic Engineering, Fast Rerouting, Multi-Layer Routing as well as Multicast Transport. Jean-Louis holds an engineering degree from the Ecole Nationale Supérieure des Télécommunications de Bretagne, France.