Service Level Agreement Framework for Differentiated Survivability in GMPLS-based IP-over-Optical Networks

David Harle,Saud Albarrak, Fuead Ali
University of Strathclyde, Glasgow, UK
{ d.harle,Sbarrak,fuead@eee.strath.ac.uk }

Anna Urra, Eusebi Calle, Jose L. Marzo
University of Girona, Spain
{ anna.urra, eusebi, joseluis.marzo@udg.es}

Abstract: **In the next generation optical internet, GMPLS-based IP-over-optical networks, ISPs will be required to support a wide variety of applications each having their own requirements. These requirements are contracted by means of the SLA. This paper describes a recovery framework that may be included in the SLA contract between ISP and customers in order to provide the required level of survivability. A key concern with such a recovery framework is how to present the different survivability alternatives including recovery techniques, failure scenario and layered integration into a transparent manner for customers. In this paper, two issues are investigated. First, the performance of the recovery framework when applying a proposed mapping procedure as an admission control mechanism in the edge router considering a smart-edge simple-core GMPLS-based IP/WDM network is considered. The second issue pertains to the performance of a pre-allocated restoration and its ability to provide protected connections under different failure scenarios.**

Index Terms- **Multi-layer survivability, quality of restoration, recovery mechanisms.**

1 INTRODUCTION

The use of optical technology has enabled operators to meet the rapidly growing demand for data traffic by taking advantage of the huge capacity offered by optical fibre. Due to their high capacity and flexibility, optical networks are the right choice for the next-generation optical Internet networks to transport high-speed IP traffic. The integration of the IP and optical layer is facilitated by the development of Generalized Multi-Protocol Label Switching (GMPLS) [1]. GMPLS relies on a peer model in which all network elements share the same unified control and signalling plane providing efficient management and use of the network resources. GMPLS provides instruments for traffic engineering, constraint-based routing and many other services required by future Internet applications. In this network architecture, survivability has become a key issue to improve and satisfy the increasing requirements of Quality of Service (QoS) and Quality of Restoration (QoR) [2]. Although not all the applications require the same level of reliability, current networks do not offer a large set of differentiated recovery methods. Moreover, some clients/applications are more stringent about their QoR requirements than others. In many cases, improving the fault recovery involves very expensive mechanisms in terms of resource consumption, such as 1+1 protection, which cannot be deployed throughout the whole network.

Internet Service Providers (ISPs) obviously aim to achieve the required level of survivability with minimum resource consumption and network cost. ISPs should determine the most suitable recovery mechanism for each application/customer by means of the Service Level Agreement (SLA) [3]. With the SLA, customers define and contract the service that ISPs should provide. The survivability parameters that customers contract are the accepted/expected recovery time and availability. No particular resilience scheme (restoration, protection, 1+1, etc.) is indicated by the customer; this decision pertains to the operator and should be transparent to the client. Based on client requirements, ISPs determine an appropriate recovery mechanism according to the contracted availability and recovery time coupled with the considerations of low network cost (in terms of spare capacity), scalability, and simplicity.

In this paper, a service level agreement framework, focusing upon the trade-off between the various aspects of survivability performance parameters and the customer/application requirements is presented. The proposed framework, by providing a range of possibilities for customer survivability parameters (availability and recovery time), allows ISPs to embed survivability within the SLA. Different aspects pertinent to survivability such as survivability techniques, layer integration and different failure scenarios are considered.

2 SURVIVABILITY OVERVIEW

2.1. Survivability techniques

Numerous survivability techniques have been previously proposed and can be broadly classified into protection, restoration and pre-allocated restoration techniques [2,4]. The distinction between these techniques is based on the timing of spare capacity allocation and the timing of backup route calculations; each offering different fault recovery times. The protection technique describes recovery schemes that are pre-planned for both spare capacity and backup paths. It is clear that protection schemes achieve the shortest recovery time. However, protection mechanisms require more network resources since they must pre-allocate spare capacity for pre-established backup paths. The reservation of the spare capacity may be either dedicated or shared. In shared protection, the spare capacity of the backup path may be shared with other backup paths, saving potentially large amounts of spare capacity. In dedicated protection, the spare capacity is not shared and identical traffic may be transmitted simultaneously on both working and backup paths (1+n protection). Another issue concerning protection mechanisms is their scalability when multiple failure scenarios are considered. Restoration techniques overcome these drawbacks by planning both spare capacity and backup routes after failure occurrences. Thus, restoration is

1-4244-0353-7/07/$25.00 ©2007 IEEE

flexible in terms of resource utilization and coping with various failure scenarios [5,6]. However, restoration schemes offer lower recovery time and do not guarantee the recovery of all traffic affected by the failure. The recovery action may not always be successful as there may be insufficient network resources available.

A survivability scheme that falls between the protection and restoration techniques is the pre-allocated restoration scheme [7]. This scheme only uses pre-planned spare capacity; additional capacity specifically for survivability purposes is embedded in the network. The restoration capacity is effectively invisible to routing algorithms under normal operational (no-failure) conditions. Moreover, the pre-allocated restoration technique is more flexible in terms of resource utilization and coping with various failure scenarios. Survivable routing computation and resource allocation are involved only when the failure has been notified

2.2. Failure coverage

Another emerging issue for ISPs is to provide survivability under different failure scenarios. In most previous work the dominant failure scenario is the single-link case. However, the dual-link failure scenario has now emerged as a real motivation for both designers of survivable networks and ISPs [2]. The main reason is that, as a result of the physical topology constraints and long-distance fibre link installations, the occurrence of dual-link failures in large-scale networks is now more probable. Another motivation arises from the improvement of optical layer functionality whereby a significant proportion of functions are facilitated through a GMPLS-based distributed control plane rather than any centralized management unit. Since some applications require high availability, ISPs should also guarantee recovery against dual-link failures. The failure coverage is a parameter that is transparent to the customer; it is not normally explicitly defined in the SLA. Therefore, SLA customer parameters should be properly defined in order to appropriately represent the failure quality that an ISP must provide to the customer when utilising network resources. Note that, for instance, by applying 1+n protection under dual link failure scenarios (i.e. n=2), two disjoint backup paths are established to protect the connection; resulting in possible inefficient use of network resources.

2.3. Application Identification

In response to the applied survivability techniques and required failure coverage, ISPs may extend the SLA in order to represent application survivability requirements and enable efficient use of network resources. From higher to lower, in terms of recovery resource costs, ISPs may differentiate between protected, best effort, unprotected and pre-empted traffic. Table 1 summarizes, from the ISP perspective, the characteristics of each application. Scalability in terms of management cost and implementation (network resources used) as well as the economic cost in terms of technology equipment necessary to offer the survivability technique are also depicted.

2.4. Multi-layer Survivability

Survivability may be provided at either IP or optical domains. Each network layer generally deploys its own recovery mechanisms. The characteristics presented in Table I is independent of the layer that recovers the traffic. The same table may be used to identify the relative costs for applications when survivability is applied at either optical or IP domain. However, recovering an application at either IP or optical domains has different implications in terms of scalability, spare capacity and recovery time; due to the granularity of the recovery strategy. Diverse switching granularity levels exist in the IP-over-optical network scenario: from coarse to fine - fibre, lightpath and label switch path (LSP). Recovering at the optical layer recovers affected connections in-group; thus, the recovery action is also fast and easier to manage than when individually recovering each affected connection at the IP layer. On the other hand, IP's finer granularity results in better resource consumption (spare capacity). Therefore, a SLA should integrate the multi-layer scenario in a transparent way for the customers. Basically, this may be done in terms of recovery time (faster at the optical layer) and price (more expensive at the optical layer). The SLA helps ISPs to identify the layer where recovery mechanisms will be applied to recover failed applications.

Table 1. Application identification and characteristics.

<table>
<tr><th colspan="2">Applications</th><th>Survivability scheme</th><th>restorability</th><th>Scalability</th><th>Economic cost</th><th>Spare Capacity</th><th>Recovery time</th><th>Normal oper.</th></tr>
<tr><td rowspan="6">Non pre-empted</td><td rowspan="4">Protected</td><td>Dedicated protection (1+n)</td><td rowspan="4">guaranteed recovery</td><td>Complex</td><td>Most expensive</td><td>Very high</td><td>Fastest</td><td>No pre-emptive traffic</td></tr>
<tr><td>Dedicated protection (1:1,1:2)</td><td>Complex</td><td>Quite expensive</td><td>High</td><td>Fast</td><td rowspan="3">Spare capacity is used by pre-emptive traffic</td></tr>
<tr><td>Shared protection (n:m)</td><td>Medium</td><td>Expensive</td><td>Medium</td><td>Medium</td></tr>
<tr><td>Pre-allocated restoration</td><td>Simple</td><td>Regular</td><td>Low</td><td>Slow</td></tr>
<tr><td>Best Effort</td><td>Restoration</td><td>No guaranteed recovery</td><td>Simple</td><td>Cheap</td><td>None</td><td>Slowest</td><td>N/A</td></tr>
<tr><td>Unprotected</td><td>none</td><td>No recovery</td><td>Simple</td><td>Very cheap</td><td>None</td><td>N/A</td><td>N/A</td></tr>
<tr><td>Pre-empted</td><td>none</td><td>No recovery</td><td>Simple</td><td>Cheapest</td><td>Pre-emptable</td><td>N/A</td><td>N/A</td><td></td></tr>
</table>

2.4. Survivability Measurements

The survivability measurement parameters can be classified into explicit measurement parameters such as restorability and recovery time or implicit measurement parameters such as availability. The explicit parameters reflect the network performance when failures actually do occur while the implicit parameters estimate the performance independent of the failure occurrence.

In general, availability can be viewed from two perspectives; the resource availability and the connection availability. The resource availability determines the probability of maintaining that connection when no links fail. Based on this definition, connections may be classified into pre-emptable and non pre-emptable. The pre-emptable connections carry only, under no-failure conditions, low priority or extra traffic using the spare capacity allocated for survivability purposes.

The connection availability (A_c) is defined as the probability that the connection will be found in the operation state at a random time in the future [8]. Moreover, it depends on the availability of a set of sequence elements (S) crossed by the connection. Therefore, the availability of an unprotected connection is obtained using formula (1) where (A_i) indicates the availability of element (i).

$$A_c = \prod_{i \in S} A_i \tag{1}$$

The availability of any element can be obtained based on two key parameters; the mean time between failure (MTBF) and the mean time to repair (MTTR). This paper considers only link availability and assumes that all the other elements are ideal (always available). Therefore, the link availability can be calculated using equation (2) based on three parameters which include MTTR and MTBF specified by fibre vendor and total link length (L) [9].

$$A_i = \left(\frac{MTBF}{MTBF + MTTR} \right)^L \tag{2}$$

In order to increase the connection availability a protection mechanism is essential. In case of protection, a connection is presented as a set of paths including the working path with availability (A_w) and the backup paths (A_{bi}). The connection availability of different protection schemes is calculated as follows:

- Dedicated protection (1+1, 1:1) :

$$A_c = 1 - (1 - A_w) * (1 - A_b) \tag{3}$$

- Dedicated protection (1+2, 1:2) :

$$A_c = 1 - (1 - A_w) * (1 - A_{b1}) * (1 - A_{b2}) \tag{4}$$

- Shared protection (1:1) :

$$A_c = 1 - (1 - A_w) * (1 - A_s * A_{b1}) \tag{5}$$

- Shared protection (1:2) :

$$A_c = 1 - (1 - A_w) * (1 - A_{s1} * A_{b1}) * (1 - A_{s2} * A_{b2}) \tag{6}$$

The shared resources availability (A_s) depends on the availability of the other working paths which share the same resource. Therefore, the shared resources are available for the current connection when it is not used by the other connections; in other words, when all the other connections are available. Consequently, the value of (A_s) is obtained using formula (7).

$$A_s = \prod_{i \in N} A_i \tag{7}$$

where N is the number of connections which share the same resources and (A_i) indicates the availability of connection(i).

On the other hand, the recovery time is one of the key survivability performance measurements and it affects directly the level of quality of service. A full discussion of different aspects of the recovery time is presented Calle et al [10].

3 PROBLEM DISCUSSION

ISP survivability concerns motivate the definition of a more accurate recovery framework that can be included in the SLA. ISPs may then more easily identify a suitable survivability technique to deploy that can recover the applications under failure conditions while making better use of the network resources. The incorporation of a recovery framework in the SLA is important, firstly, because survivability has become a key issue for the next generation optical internet, where single and dual link failures are highly probable in large-scale networks. Secondly, survivability parameters have not been taken into account in current SLAs. Finally, the improvement in optical layer functionality such that many functions are facilitated through a GMPLS-based distributed control plane make possible the move towards differentiated multi-layer survivability schemes rather than relying on single layer survivability schemes.

A prime concern in such a recovery framework is how to present the different survivability alternatives including recovery techniques, failure scenario and layered integration into a manner that is transparent to customers. The proposed framework considers two key components: customer requirements in terms of QoR and ISP requirements in terms of the implementation capability. From the customer perspective, the survivability parameters assigned to customers are simply availability under normal and failure situations and the recovery time as shown in Table 2. Survivability is classified into four classes: protected, best effort, unprotected and pre-empted classes. The higher the survivability requirements in terms of availability and recovery time, the higher the cost.

From the ISP perspective, to meet QoR requirements, ISPs should identify and implement the recovery mechanisms suitable to the customer at the lowest possible network cost by exploiting the variety of possible survivability techniques within the differentiated multi-layer survivability concept. This challenge can be met by mapping the application and survivability characteristics (Table 1) into the SLA framework (Table 2) when considering both IP and optical layers. Such a mapping procedure directly impacts both network cost and QoR.

Table 2. SLA customer perspective

Application	Availability under normal operation	Availability under failure operation	Price
Protected	100% guaranteed availability	100% guaranteed availability	Expensive
		Premium availability	
		High availability	
Best effort	100% guaranteed availability	Availability is not guaranteed	
Unprotected	100% guaranteed availability	No availability	
Pre-empted	Availability is not guaranteed	No availability	Cheap

Application	Recovery time	Price
Protected	Very fast recovery time ≅ 0	Expensive
	Fast recovery time 10's ms	
	Medium recovery time 100's ms	
	Slow recovery time from ms to s	
Best effort	Very slow recovery time from s to minutes	
Unprotected	No recovery action	
Pre-empted	No recovery action	Cheap

4 MODEL IMPLEMENTATION

This work uses the OMNeT++ (Objective Modular Network Testbed in C++) discrete-event simulation platform which supports modelling of distributed mesh topologies.

4.1. Model structure

The structure consists of a set of nodes connected by a set of paired fibre links. Internally, each node consists of an edge router connected to an optical cross connection (OXC) as shown in Figure 1. The router and OXC may be placed in a separate location or they may be combined to form a single node with a common control plane. The network structure can be seen from two perspectives: a data plane and a control plane. The data plane is an overlay model with three topologies: link, lightpath, and Label Switched Path (LSP) topology. Lightpaths and LSPs are diverse in terms of granularity and capacity ranges; lightpath granularity is more coarse than LSP granularity and lightpath capacity is represented in discrete units while LSP capacity is presented as a continuous variable with a defined range. Moreover, an LSP may traverse more than one lightpath. However, lightpath and LSP connections exhibit a degree of similarity in terms of provisioning

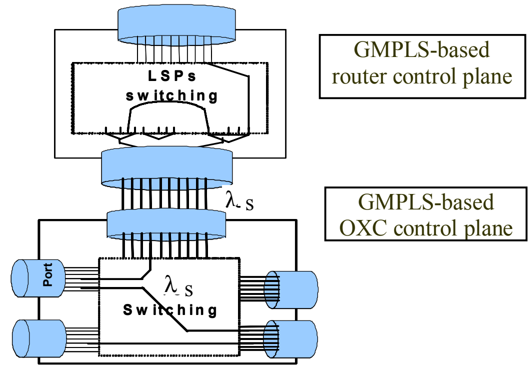

Figure 1: network node structure.

procedure, recovery notification and providing an end-to-end path. In the context of this paper, the term "connection" is used to refer to both LSP and lightpath connections indistinctly, when mechanisms that can be implemented at IP and optical layer are explained. Moreover, the term "path" is used to describe working and backup paths are associated with a connection.

The control planes, in both edge routers and OXCs, consist of three units: the signalling, the routing and the recovery units. The functionalities of the signalling and routing units are implemented using standard GMPLS protocols as described in the Internet drafts [10]. This work focuses on the implementation of the recovery unit functions in conjunction with other protocols. The node units require particular information in order to efficiently implement their functionality. Specifically, several data tables are maintained in each node. These tables can be updated by either signalling or routing protocols. The signalling protocol facilitates table updating to maintain local information such as wavelength routing, lightpath information, forwarding and LSP information tables. On the other hand, tables that maintain global information including the link resource availability and logical topology tables are updated by means of the routing protocol.

In order to analyse the recovery time, this model considers three delay components; the link propagation delay, the link transmission delay and the nodal process delay. The link propagation delay is the latency in propagating the bits along the link and is a function of the link propagation speed and the link length. The link transmission delay is the time needed to transfer/pump data onto a link and is calculated as a function of the link capacity and the message size. The nodal process delay describes the time between the node receiving a message though the input port and when the message is sent to the output port and includes the time taken to examine a message, to calculate a new route and to perform wavelength switching

4.2. Model assumptions under no-failure conditions

At the IP layer, LSP connections are requested and terminated randomly with arriving requests based on a Poisson process. The LSP parameters include the source, the destination and the capacity selected randomly based upon a uniform distribution. Four classes of services (protected, best-effort, unprotected and pre-empted) are also generated based upon a uniform distribution. From the routing calculation perspective, this model adopts the source explicit routing concept and the n-step constraint-based shortest-path-first algorithm. The former considers the provision of an explicit route at the source nodes, therefore, this route cannot be modified during the signalling phase. The latter algorithm provides an efficient method to compute the working and backup paths for any connection. The IP routing unit determines the explicit route based on the amount of available capacity in each lightpath while the optical layer determines the explicit route based on the number of free wavelengths in each link. Therefore, in the first step, the working path is computed. The second step computes the first backup path considering the SRLG of the working path. Next, step 2 is repeated n-2 times in order to compute the remaining n-2 backup paths. For each iteration of step 2, the SRLG associated with each previous computed backup path is considered in the computation of the new backup path.

New LSP requests may be accommodated either by requesting a protected lightpath, an unprotected lightpath or by determining a route within the existing lightpath topology depending on the LSP class of service. The lightpath-create-first policy [12] is used by edge routers to handle and manage the traffic classes associated with best-effort class and unprotected class. Lightpath-create-first policy with n-steps routing algorithm is applied for the protected applications not included in the previous policy. The pre-empted LSP request is accommodated only within the existing spare capacity in the network including the backup lightpaths and the pre-allocated spare capacity. The shared capacity protection is implemented using the partial information strategy explained in detail elsewhere [13]. A request is blocked if there are no available resources along its route. It is assumed that no repeat behaviour is considered. Therefore, the admission control is aware of the situation when the working path for a connection is established while its backup path is rejected and vice versa.

4.3. Model assumptions under failure conditions

Failures are generated randomly. The inter-arrival time and holding time of failures are generated based on an exponential distribution. Links selected for failures are obtained using a uniform distribution. The dual link failure scenario considered in this work is when two random links fail simultaneously. The path-level recovery (end-to-end recovery) is applied as this provides better resource utilisation than link-level. The recovery procedure can be classified into three key processes: fault notification, failed connection teardown and recovery.

- Notification process: The notification process starts at the upstream node, which is responsible for sending a notify message to the source node. It is possible to aggregate many failed connections that belong to the same source node on one notify message. The optical layer is responsible for notifying the IP layer about any unrecovered or unprotected lightpath. The cooperation between layers is shown in Figure 2.

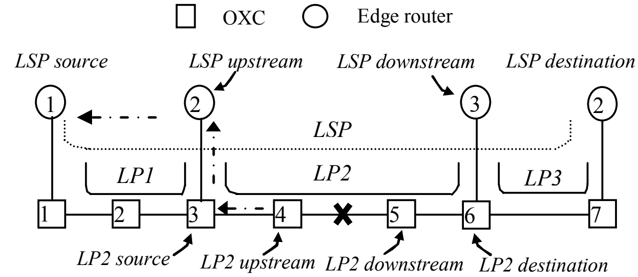

Figure 2: Notify messages delivery from the optical to IP layer.

- Teardown process: The teardown process starts at both upstream and downstream nodes. The upstream node is responsible for tearing down the upstream segment while the downstream node is in charge of the teardown of the downstream segment.
- Recovery process: The recovery process starts at the source node of any failed connection. It ranges from doing nothing to switching traffic onto an alternative connection depending on the recovery scheme associated with each class of service. There are no associated recovery schemes with the pre-empted and unprotected connection.
  - Protected connection using protection: the recovery process requires only switchover synchronization signalling between the source and destination of a failed connection. The reason being that the bidirectional backup path of a connection is used to transfer pre-empted traffic
  - Protected connection using pre-allocated restoration: the recovery process requires the provisioning of an alternative connection. Therefore, the admission control, at the source node, meets this challenge by using existing protected and unprotected lightpaths including the pre-allocated spare capacity. The pre-allocated spare capacity is reserved Using 'a link partitioning' method. In the 'lightpath partitioning' method, the spare capacity is allocated between all active lightpaths whereby the total lightpath capacity is partitioned into two parts; working capacity and restoration capacity [14].
  - Best effort connection: the recovery process requires the provisioning of an alternative connection. Therefore, the admission control must delay this class for a certain pre-set time in order to give precedence to pre-allocated restoration traffic.

5 PERFORMANCE RESULTS

This section presents results for a number of simulation-based experiments. The performance metrics of interest are the availability, restoration ratio, recovery time and blocking probability. The availability of a connection is obtained as explained in section 2.4 with MTBF=300 years/km and MTTR=8 hours [9]. The restoration ratio gives the ratio of the number of restored connections over the number of failed connections in the network. The recovery time is defined as the ratio of the total restoration time of restored connections over the number of restored connections. The blocking probability is calculated as the ratio of the number of rejected connections to the number of requested connections in the network. The offered load indicates the traffic load expressed in Erlangs. It is assumed that all links have the same number of wavelengths (8 wavelengths) with 10 Gb of capacity. The topology adopted by this work is the NSFnet network topology where link length is represented by values derived from previous work[6]. The process delay is 3ms for the Path and Reservation messages and 1ms for other messages. The OXC reconfiguration time is 1ms. It is assumed that LSP capacity varies continuously between 1Mb to 2.5 Gb. The mean failure inter-arrival time is 5 time units and the mean repair time is one time unit. These particular values were adopted primarily as a result of experimental expediency in order to set limits for the experimental work. It is recognised that the numerical values maybe lower or different than those experienced in practical networks; the results attained represent reasonable limits under the consideration to provide multiple failure events. It is assumed that the hold-off time is 60ms. The techniques are investigated progressively with the same network load value (400 Erlangs). Each performance value is an average of 10 different simulation runs.

The main interest in this set of experiments is the protected class. Based on the framework, there are two techniques used to provide protected connections; protection and pre-allocated restoration. Thus, the first experiment investigates the performance of the recovery schemes that are included in the recovery framework. The aim of this experiment is to evaluate the required spare capacity, the range of recovery time, the availability, and the blocking probability, in particular, for the protected class in both optical and IP layer. The second experiment considers the pre-allocated restoration technique. It is clear that the protection techniques provide 100% restorability whereby the recovery from failure is pre-planned. The aim is then to investigate, specifically, the ability of the pre-allocated restoration to achieve 100% restorability.

Figure 3 presents a performance comparison between different survivability techniques including dedicated, shared and restoration under different single- and dual-link failure scenarios. As expected, protection at the optical domain results in better performance in terms of recovery time and availability than at the IP layer. On the other hand, the IP layer achieves better resource utilisation in terms of blocking probability and required spare capacity. It can be seen that the restoration achieves lowest availability value and the highest recovery time while providing the best resource utilisation in terms of spare capacity. Moreover, the figures show clearly that dual- link failure protection is inefficient in terms of required spare capacity and blocking ratio. The high blocking ratio arises from a number of different reasons; lack of resources, routing calculation whereby it is not simple to find three disjoint paths between particular pairs, and message contention, in particular, with distributed network.

Therefore, it is suggested that the protection technique be applied to specific connections which required certain QoS, rather than adopt the protection technique wholesale to provide survivability for the entire network.

Figure 3-b presents the delay which considers only the notification and the recovery time. The results show that the recovery time of 1:2 and 1:1 shared protection are at the same level with a similar outcome for dedicated protection. The reason being that the recovery time relies on the

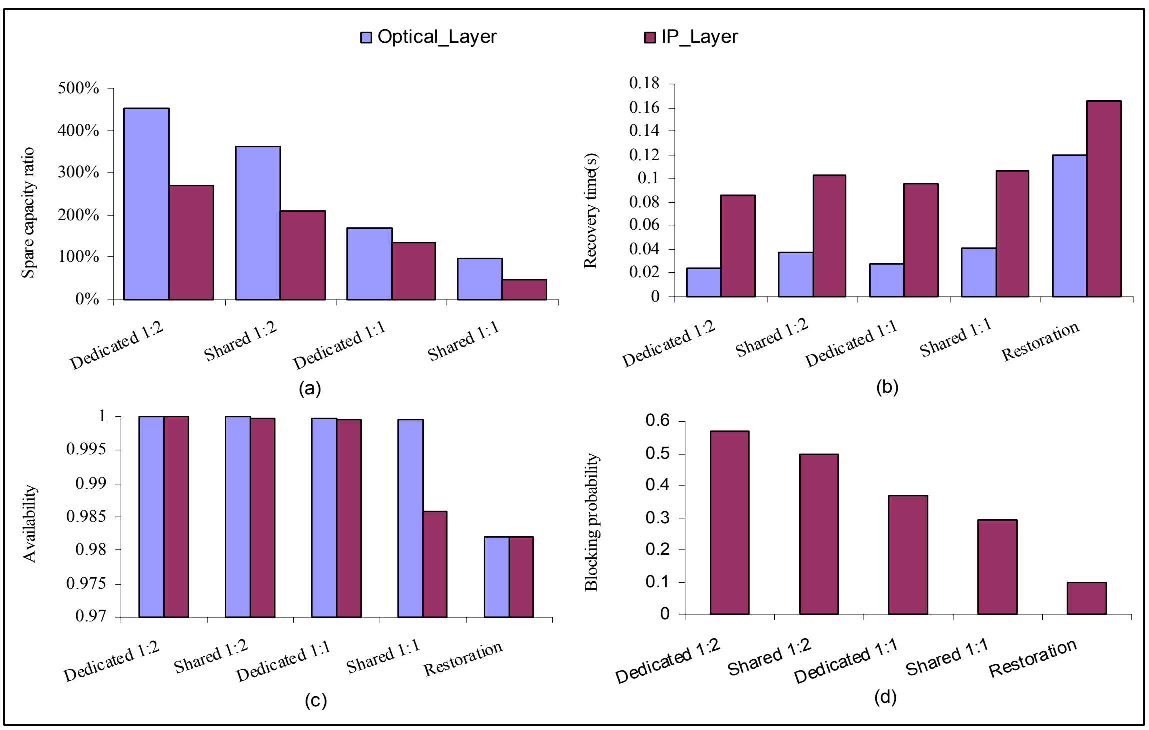

Figure 3: performance comparison between different survivability techniques. (a) Spare capacity ratio, (b) Recovery time, (c) Availability and (d) Blocking probability.

applied signalling method between pairs, regardless of single- or dual-link failure protection. On the other hand, the figure gives only an indication for comparison between different techniques under the same assumptions whereby the absolute recovery time values are hard to obtain.

Figure 3-d illustrates only the blocking ratio for the IP layer; the blocking probability of the optical layer is constant regardless the applied technique. The reason is that the optical layer is fully controlled by the IP layer which adopts the lightpath-create-first policy [12] to mange the lightpath request. Adopting such a policy, the number of requested lightpaths is relatively high compared to the number of established lightpaths.

The second experiment considers the pre-allocated restoration technique. The aim here is to investigate the ability of the pre-allocated restoration to achieve 100% restorability using the retrial method. Figure 4 presents the restoration ratio for the lightpath partitioning method under single- and dual-link failures with and without retrial methods. The experimental results show that the restoration ratio is improved when the amount of pre-reserved capacity increases; clearly an expected result. Additionally, this experiment demonstrates clearly the effect of contention problems in the GMPLS-based distributed network model, in which the restoration ratio of dual-link failures with retrials exceeds that of the restoration ratio for single-link failures without retrial. Moreover, the method achieves full single-link and dual-link failure recovery with relatively low use of spare capacity when the retrial method is applied. The results show clearly that, the pre-allocated restoration technique is an efficient technique that can be applied to provide protected connections against different failure scenarios requiring spare capacity in the range of 25-35% of the total network capacity (2-3 Gb/s).

Figure 5 illustrates the Pre-allocated restoration recovery time with different retrial values under dual-link failures. The graph shows that the restoration time is improved when the amount of pre-reserved capacity increases, the reason being that, when the spare capacity increases the recovery routes become shorter.

The experimental results show that there is a trade-off between the pre-allocated restoration performance parameters when the retrial method is applied. While the restoration ratio is improved significantly under the retrial method (with 1ms delay), the restoration time is increased significantly. However, based on the suggested framework, it is assumed that the pre-allocated restoration is adopted for the connections that are not particularly sensitive in terms of recovery time.

6 PROPOSAL AND CONCLUSION

From the results obtained, a simple and efficient mapping procedure is proposed in Table 3. The aim of this mapping is to provide the recovery process at the IP layer when the required QoR is guaranteed, taking advantage of the better use of the network resources.

In this paper, two issues have been investigated. Firstly, the performance of pre-allocated restoration and its ability to provide protected connections has been investigated under different failure scenario. Secondly, the performance

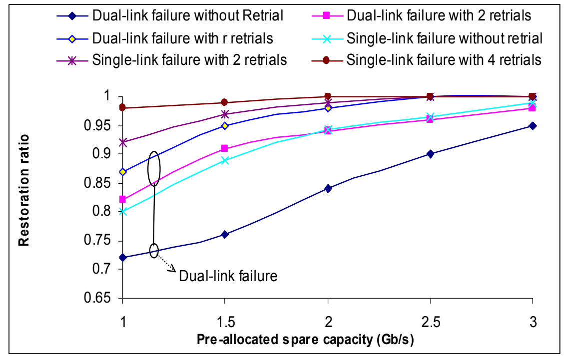

Figure 4: Pre-allocated restoration ratio with and without retrial under single- and dual-link failure.

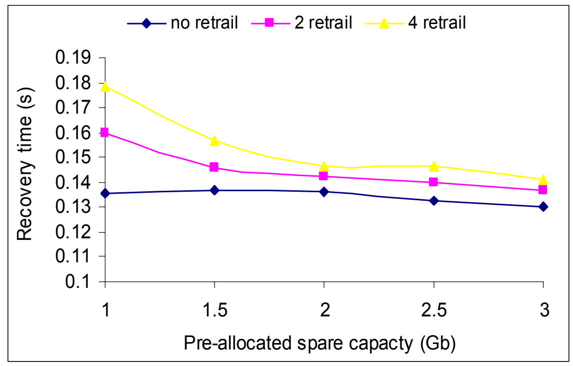

Figure 5: Pre-allocated restoration recovery time with different retrial values under dual-link failure.

of the recovery framework has been investigated by applying the proposed mapping procedure as an admission control mechanism in the edge router considering a smart-edge simple-core GMPLS-based IP/WDM network.

Thus, ISPs can embed survivability within the SLA by providing a range of possibilities for the customer survivability parameters (availability and recovery time). The framework considers two prime factors: customer requirements in terms of QoR and ISPs requirements in terms of the implementation capability. Moreover, the challenge can be seen from the perspective of mapping the customer requirements into the proposed framework.

In this paper, the performance of the proposed framework was obtained based on a simulation model built using OMNET++ considering a distributed GMPLS-based IP/WDM network model. Two issues were investigated. Firstly, the performance of pre-allocated restoration is investigated under different failure scenario. The simulation results show that the pre-allocated restoration technique can provide protected connections by embedded spare capacity in the network and applying the retrial method. Secondly, the performance cooperation between different schemes to provide a protected class was presented. As expected, the results show that, even though a protected connection can be provided using either protection or pre-allocated restoration techniques, there is a trade-off between these techniques when they are applied at either the optical or IP layers.

Table 3. **Mapping procedure**

Application	Availability	Recovery time	Recovery techniques
Protected	100% guaranteed availability	≅ 0	1+2 IP protection
	Premium availability	10's ms	1:2 optical protection
		100's ms	1:2 IP protection
	High availability	10's ms	1:1 optical protection
		100's ms	1:1 IP protection
		from ms to s	Pre-allocated restoration with retrial
Best effort	Availability is not guaranteed	ms to minutes	Restoration

Acknowledgements

This collaborative work was carried out in-part under the auspices of Spanish Education Ministry project (Ref:) MCyT [TIC2003-05567] and DURSI consolidated research group AEDS (ref. SGR-00296); the authors gratefully acknowledge the support provided.

7 REFERENCES

[1] E. Mannie, "Generalized Multi-Protocol Label Switching ({GMPLS}) Architecture,'' IETF RFC 3945, Oct. 2004.

[2] J. Zhang and B. Mukherjee, "A Review of Fault Management in WDM Mesh Networks: Basic Concepts and Research Challenges,'' in IEEE Networks Magazine, Mar. 2004.

[3] W. Fawaz et al., "Service Level Agreement and Provisioning in optical networks", in IEEE Comm. Mag., pp. 36-43, Jan. 2004.

[4] C. (Sam) Ou, K. Zhu, H. Zang, L. H. Sahasrabuddhe, and B. Mukherjee, "Traffic Grooming for Survivable WDM Networks-Shared Protection," IEEE Journal on Selected Areas in Communications, vol. 21, no. 9, pp. 1367-1383, Nov. 2003.

[5] D. Colle et al., "Data-centric optical networks and their survivability,'' in IEEE Journal on Sel. Areas in Comm., vol.20, no.1, pp. 6-20, Jan. 2002.

[6] J.Wang, L. Sahasrabuddhe and B. Mukherjee, "Path vs. subpath vs. link restoration for fault management in IP-over-WDM networks: performance comparisons using GMPLS control signalling," in IEEE Communications Magazine, vol.40, no 11, pp.80-87, Nov. 2002.

[7] W.D. Grover, "The protected working capacity envelope concept: an alternate paradigm for automated service provisioning," in IEEE Communications Magazine, vol.42, no.1, pp.62- 69, Jan 2004.

[8] Jing Zhang, Keyao Zhu, Hui Zang, and Biswanath Mukherjee, "A New Provisioning Framework to Provide Availability-Guaranteed Service in WDM Mesh Networks" IEEE ICC 2003.

[9] Schupke D.A., and Prinz R.G., Capacity Efficiency and Restorability of Path Protection and Rerouting in WDM Networks Subject to Dual Failures, in Photonic Network Communications, Vol. 8, No.2, pp 191-207, Sep 2004.

[10] Eusebi Calle, Anna Urra and Jose L. Marzo," Failure Recovery Time in Multi-layer GMPLS-based Networks" , V Workshop in GMPLS Networks. WGN5 Girona April 2006.

[11] J. Lang, "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVPTE) Extensions," January 2003.

[12] S. Albarrak and D. Harle, "An Edge Admission Control in a Distributed GMPLS-Based IP/WDM Network," IV GMPLS Workshop, Spain, 21st Apil, 2005.

[13] Kodialam M. and Lakshman, T.V. , Restorable dynamic quality of service routing, in IEEE Communications Megazine, Vol.40, No.6, pp.72-81, June 2002

[14] S. Albarrak and D. Harle, "Spare Capacity Allocation in a Distributed GMPLS-Based IP/WDM Mesh Network," International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS'06), Canda, July 31, 2006.