Real-Time OCh-OMS Protection Scheme Selection

Luis Velasco, Salvatore Spadaro, Jaume Comellas, Gabriel Junyent
Optical Communications Group, Signal Theory and Communications Department
Universitat Politècnica de Catalunya (UPC), C/ Jordi Girona, 1-3, 08034 Barcelona, Spain
Tel: +34 93 401 6999, Fax: +34 93 401 7102,
e-mail: {luis.velasco, spadaro, comellas, junyent}@tsc.upc.edu

ABSTRACT
Optical channel (OCh) shared protection is considered the best scheme to implement protection in optical networks due to its high efficiency. Moreover, protection resources can be used to transport extra-traffic under normal conditions. Nevertheless, the switching time of the currently available Wavelength Selective Switches (WSS), the key component to build reconfigurable optical nodes, prevents from protecting the complete set of affected lightpaths within 50 ms after fault detection. In this paper we propose a real-time mechanism to decide, on the basis of the current number of lightpaths to protect, whether the protection scheme to apply is either at the OCh level or at the link level. When protecting at the OCh level, some part of the not affected extra-traffic will be saved, whereas all extra-traffic will be pre-empted protecting at the link level. The objective of the proposed mechanism is to maximize the total transported traffic while keeping the protection times under the 50 ms objective. The performance of the proposed mechanism has been experimentally evaluated.

Keywords: ASON/GMPLS, Shared Path Protection, extra-traffic.

1. INTRODUCTION
Dense Wavelength Division Multiplexing (DWDM) transmission technology allows multiplexing an increasing number of data-channels in a single optical fiber, each channel transporting huge amount of traffic. Moreover, in core transport networks most of the carried traffic must be provided with a high availability guaranteed.

On the one hand, the GMPLS recovery framework defines OCh protection, providing RSVP-TE extensions for both end-to-end [1] and segment cases [2]. Three protection schemes have been specified: 1+1 dedicated protection, 1:N (N >= 1) shared protection with extra-traffic, and pre-planned rerouting without extra-traffic. In the 1:N scheme, N working lightpaths are protected by one shared lightpath; all lightpaths with the same origin and destination. In the pre-planned label switched path (LSP) rerouting, two disjoint LSPs are established between the end nodes: the working LSP, and the protecting LSP. However, while the working LSP is implemented in the transport plane, the resources of the protecting LSP are only pre-reserved in the control plane and therefore an explicit signaling to instantiate them in the transport plane is required. This gives the opportunity of reusing the protection reserved resources to accommodate extra-traffic.

On the other hand, protection schemes at the optical layer can work also at the Optical Multiplex Section (OMS) level [3]. Protecting at the OMS layer allows recovering the complete bundle of multiplexed optical channels in a fiber with only one protection action. In this sense, the authors have designed the GMPLS Automatic Protection Switching (GAPS) mechanism [4], which is based on extensions to GMPLS LMP [5]. It provides service recovery within 50ms after fault detection, even in large (OMS dedicated or shared) rings.

The efficiency of OCh and OMS shared schemes can be further improved by supporting the use of protection (or spare) capacity to transport extra-traffic when that capacity is not needed to protect working capacity. Nevertheless, in case of failure, when protecting at the OMS layer, the totality of extra-traffic will be preempted, whereas when protecting at the OCh layer, only that extra-traffic which is transported by resources that have to be used to protect working traffic, will be preempted.

Commercially available WSSs provide switching times close to 2 ms [6]. Besides the WSS switching time, some additional time is needed in the equipment to generate the specific command to the WSS. Telecom equipments are usually based on cards, where one card represents the interface with the control plane, and another card includes the WSS component and such cards are interconnected through a bus. Based on experimental results [4], we assume that the time from the reception of the command from the control plane to the WSS command is generated is about 1.5 ms. Thus, the actual OADM switching time is about 3.5 ms. This restriction limits the number of LSP which can be protected within 50 ms.

In this paper we propose a real-time mechanism which selects the scheme to be applied (OCh or OMS) as a function of the current number of protected LSPs in order to maximize the total carried traffic. We call the OCh shared protection scheme, also known as Shared Path Protection (SPP), as OCh SPRing when is applied to optical GMPLS-based ring networks. We have implemented OCh SPRing with extra-traffic using the pre-planned LSP rerouting extensions to RSVP-TE. Note that, in this case, a protection action is needed for each

This work has been partially founded by i2Cat Foundation through TRILOGY project and by Spanish Science Ministry through TEC-2005-08051-C03-02 RINGING project.

978-1-4244-2626-3/08/$25.00 ©2008 IEEE
protected lightpath impacted by a failure, in order to activate the pre-reserved protection LSP. Its performance has been experimentally evaluated over the ASON/GMPLS CARISMA network test-bed [7].

The remainder of the paper is organized as follows: Section 2 describes the OCh SPRing protection scheme. In Section 3 we design the joint OMS + OCh protection with real-time scheme selection. Finally, in Section 4 we draw the main conclusions of this work.

2. OCH SPRING

In the OCh SPRing scheme, the total capacity of each fiber is divided in two wavebands (B1, B2), as shown in Fig. 1a. One waveband on each fiber –B1 clockwise and B2 counter-clockwise– is reserved to transport working channels while the other is used to transport protection channels. Working connections in one fiber are protected by the available capacity in the other fiber, in the opposite direction of the ring. This way no wavelength converters are needed when moving channels from working to protection bands.

Both directions of a bidirectional lightpath are routed along the same side of the ring, in different fibers (connection A-D in Fig. 1a). Thus, the same wavelength can be reused to accommodate a connection between other nodes, whose route does not overlap the existing connection. Under normal conditions, spare resources can be used to carry extra-traffic (connection E-F in Fig. 1a).

![Fig. 1. OCh SPRing transporting two lightpaths, a) before and b) after a failure in the link B-C.](image)

When a link failure is detected (Fig. 1b) protection paths are created using spare resources to protect the affected working lightpaths and the extra-traffic in those spare resources is preempted. The protection resources are shared among working lightpaths being necessary a protocol to ensure the correct use of the shared protection capacity. This fact makes the implementation of OCh SPRing to be complex.

However, this kind of protection presents a very high efficiency in terms of transported traffic/used resources ratio (here we consider the working and the protecting capacity, as one resource). For example, if we use 1+1 protection this ratio is always 1/2 = 50%. In OCh SPRing this ratio is, at least, (1+1)/2 = 100% due to the extra-traffic effect. In fact, since the protection resources can be associated to transport extra-traffic whose end point can different from the working traffic, this ratio can be much better. For instance, if we consider the lightpath A-D in Fig. 1a), the ratio will reach (1+3)/2 = 200% when 3 additional preemtatable LSPs are carried.

We have implemented the OCh SPRing protection scheme using the pre-planned LSP rerouting, specified in [1]. After the failure in a link, the adjacent OADMs measure optical power levels under a threshold and advertise of that condition to their Optical Connection Controller (OCC) in the GMPLS control plane. The OCC looks for lightpaths using that link. For every lightpath to be protected, the OCC looks for the address of the OCC which has to be notified. That information was received in the NOTIFY_REQ object in the RSVP-TE Path message. If the OCC to be notified is not the current OCC, a RSVP-TE Notify message is send to that OCC with the corresponding error. If the OCC is the one to be notified or upon the reception of the RSVP-TE Notify message, the protection LSP signaling starts. The protection lightpath signaling process consists on sending a RSVP-TE Path message to eliminate the extra-traffic from the resources which the protection lightpath needs and sending a RSVP-TE Resv message to effectively activate the protection lightpath in the transport plane.

Taking advantage of its shared nature and that the protection lightpaths are created in a failure-driven way, it is possible to reuse the protection capacity to transport extra-traffic. In the event of a link failure, the extra-traffic can be preempted by the working traffic. In such a case, only the protection resources needed to protect the working traffic are released. All other extra-traffic using resources which are not strictly needed for the protection of that failure are not released and can continue transporting traffic.

To determine the number of LSPs that can be protected within 50ms after the fault detection let us denote $t_{CLI}$ as the communication time between the OADM and the OCC, $t_{OCC}$ as the time to process a single RSVP-TE message, $t_{link}$ as the propagation delay in each link, and $t_{switch}$ as the time from the reception of a request in the OADM to the time when that request is physically performed. Let us define the protection time ($t_{OCh}$) in an $n$ nodes ring with pre-planned rerouting, as the interval from the detection of the failure to the completion of the switching operation for every single optical connection for every lightpath to be protected. Let us denote $r$ as the
number of LSPs to be restored. WSS components perform one connection at a time, so if we need to perform several connections (e.g., \( r \)) we need to wait for \( r \cdot t_{\text{switch}} \).

We always use the shortest route for the working LSP. Then, all lightpaths, independently of their end nodes, have their protection routes through the nodes which are at a distance of \( \text{round}(n/2) \)-1 hops of the nodes adjacent to the failure. Therefore, those OADMs have to perform \( r \) connections sequentially. We assume that the time to travel from a node to the adjacent through the opposite side of the ring (in the case where the end nodes of a lightpath are adjacent to the failure) is lower than the time needed to perform the \( r \) connections (\( r \cdot t_{\text{switch}} > (2n-2)(t_{\text{link}} + t_{\text{OCC}}) \)). Thus, the time to protect all the affected traffic due to the coincidence of multiple connections in those nodes (\( t_{\text{OCCh}} \)), can be expressed as:

\[
t_{\text{OCCh}} = 2t_{\text{CCI}} + t_{\text{OCC}} + \left( \left\lfloor \frac{n}{2} \right\rfloor + 1 \right) (t_{\text{link}} + t_{\text{OCC}}) + r \cdot t_{\text{switch}}
\]

The protection mechanism has been experimentally evaluated over the ASON/GMPLS CARISMA network test-bed [7]. In our implementation, we have obtained the following times: \( t_{\text{CCI}} = 1 \) ms, \( t_{\text{OCC}} = 0.5 \) ms. Therefore, the maximum number of LSPs that can be protected within 50 ms after fault detection is 11.

### 3. OCH+OMS SHARED PROTECTION

In [4] we presented OMS protection which is also suitable for GMPLS-based optical ring networks. Protecting at the OMS layer allows recovering the complete bundle of multiplexed optical channels in a fiber with only one protection action. This allows keeping the protection time under 50 ms, even in the case of very large rings, and independently of the number of working LSPs.

OMS shared protection also allows using the protection resources to transport extra-traffic. However, conversely to the OCh protection, in OMS protection all extra-traffic is preempted to recover the protected traffic, after a failure in a link.

OMS and OCH protection schemes can coexist in the same ring. In fact, OMS SPRing also divides the total capacity of each fiber in two wavebands. This way, wavebands can be used to support OCh or OMS SPRing.

In order to support the OCh SPRing scheme with extra-traffic, we have designed the OADM block shown in Fig. 2a. The basic components are splitters/couplers (S) and WSS. The incoming DWDM signal in the East and West ports can either pass-through or be dropped to any port. The local traffic can be added either to the East or to the West outgoing DWDM signals. To the OADM block in Fig. 2a, we have added the support to the OMS SPRing scheme, a set of optical switches, splitters/couplers, and band splitters (BS), and the additional hardware to monitor the incoming optical power, as shown in Fig. 2b.

![Fig. 2. OADM design supporting a) OCh and b) OMS protection, with extra-traffic.](image)

Using the designed OADM, we propose a real-time mechanism to decide which protection scheme is appropriated to perform upon the detection of a failure, in base to the number of LSPs, \( r \), to be restored at this concrete time: if \( r \leq 11 \), then OCh protection can be performed, keeping the protection time under 50 ms, while maximizing the total traffic transported by the ring, as some preemptable LSP can continue working; if \( r > 11 \) the protection time cannot be kept under the limit, so OMS protection is performed instead although all extra-traffic will be preempted.

To illustrate the impact of the protection method chosen over the spare resources, let us assume uniformly distributed traffic to be transported by the ring. The shortest route is always used for the working LSP. In the six-node ring example (Fig. 1) a particular link (e.g. B-C) can transport working paths of 1, 2, and 3 hops long. Depending on the end nodes, several distinct paths for the same hop count may exist (Fig. 3). The probability of transporting each different path, therefore, can be estimated (Table 1). In case of failure, we can calculate the
number of spare data-channels that will be used to protect the working traffic as the product of the number of
hops used for protection and the probability of each type of path. Thus, in average, the number of data-channels
used for the protection of one LSP in our example is \(0.83 \times 1.33 + 1.5 = 3.67\). Using OMS protection, the
number of data-channels used for the protection of the link the example, is \((6-1) \times 20 = 100\).

### Table 1. Data-channels used for protection.

<table>
<thead>
<tr>
<th>Hops working</th>
<th>Hops protection</th>
<th>Distinct paths</th>
<th>Prob.</th>
<th>Data-channels</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>5</td>
<td>1</td>
<td>0.167</td>
<td>0.83</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>2</td>
<td>0.333</td>
<td>1.33</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>3</td>
<td>0.5</td>
<td>1.5</td>
</tr>
</tbody>
</table>

Fig. 3a) Distinct paths. b) Spare capacity used as a function of the number of protected lightpaths.

Fig. 3b shows the number of spare data-channels that are preempted, in average, as a function of the number of
protected lightpaths for different ring sizes. When the number of lightpaths to protect is low, \(r \leq 11\), OCh shared
protection is performed; the spare capacity used grows linearly with the number of lightpaths. When the number
of lightpaths to protect is greater than the threshold, \(r > 11\), OMS shared protection has to be applied in order to
keep the protecting time within 50ms; in this case, the whole spare capacity is used. Fig. 3b also shows, in
percentage, the evolution of the spare data-channels that continue working after the protection is performed.

### 4. CONCLUSIONS

In this paper we have presented a real-time mechanism which, on the basis of the number of protected lightpaths,
decides the protection scheme to apply: OMS or OCh shared protection. The decision is taken to provide
protection within 50ms after the detection of a failure. We have shown that both methods can coexist and we
have designed a new OADM which support protection at both levels.

Starting from the experimental results and taking into account the currently available components, we have
analytically found the number of lightpaths which can be protected within 50ms. This threshold is 11. When the
number of protected lightpaths is higher than the threshold, OMS shared protection is applied in order to provide
protection times within 50 ms.

Finally, we have shown the spare capacity that is necessary to be preempted to recover the protected traffic in
case of failure. Using OCh shared protection, only a portion of the spare capacity is used, whereas using OMS
shared protection all spare capacity need to be used.

### REFERENCES

  ring networks”, Accepted for publication in Computer Networks, 2008.