Link Management Protocol extensions for OMS protection in GMPLS-based optical ring networks

Luis Velasco, Salvatore Spadaro, Jaume Comellas, Gabriel Junyent
Optical Communications Group, Signal Theory and Communications Dept.
Universitat Politècnica de Catalunya (UPC), C/ Jordi Girona, 31 08002 Barcelona, Spain
{luis.velasco, spadaro, comellas, junyent}@tsc.upc.edu

Abstract. *In this paper we propose a mechanism to provide dedicated section protection in ring-based optical networks. It is based on extensions to GMPLS Link Management Protocol (LMP) and its performance is experimentally evaluated.*

Introduction

Currently, only Optical Channel (OCh) resilience is supported by the GMPLS recovery framework [1-2]. In this paper we propose the GMPLS Automatic Protection Switching (GAPS) mechanism, which provides dedicated section protection (hereafter OMS-DPRing) in GMPLS-based optical ring networks and it is based on extensions to GMPLS LMP [3]. GAPS aims to provide service recovery within 50ms after the fault detection.

Network scenario

An OMS-DPRing consists of two counter-rotating rings, each transmitting in opposite directions relative to each other (Fig. 1a). In the normal state, the working sections in the transport plane carry regular traffic. When a network component fails a switch event occurs and the working section is protected using protection sections.

The failure in a section implies a Loss of Light (LoL) detection and it can be corrected by its adjacent nodes. These nodes are called switching nodes and they use the bridge and switch actions for the protection of the working section (Fig. 1b). When a node detects a failure through LoL, it notifies the failure to the Optical Connection Controller (OCC) in the GMPLS-based control plane which becomes the head end. Conversely, an OCC that is notified of a failure becomes the tail end and its transport plane associated node executes a bridge.

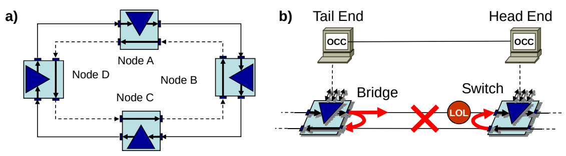

Fig. 1 a) OMS DPRing. b) Bridge and Switch actions

The GAPS mechanism

A failure can be due to a span or a node failure. Firstly, let us assume a span failure. When an OCC receive a notification of failure, it sends a switching request, which includes the detecting node Id, to the OCC of the adjacent node over the control network on both the short and the long path. The short path connects head and tail OCCs directly, while the long path connects them through intermediate OCCs using the opposite side of the ring.

Fig. 2 shows the details of the GAPS mechanisms. The initial state of the ring is the normal state. In this state, all OCCs in the ring have interchanged messages 1-4 (omitted in Fig. 2) with its neighbors.

At time T1, node A detects a LoL on its working section and notifies it to its OCC. It becomes a switching node and its OCC becomes the head end. Head end OCC sends a bridge request. All intermediate OCCs on the long path enter full pass-through state. OCC D, upon reception of the bridge request from OCC A on the short path, transmits a LoL ring bridge. OCC D, upon reception of the bridge request from OCC A on the long path, executes a bridge, and updates its status. OCC A, upon reception of the ACK from OCC D on the long path, executes a ring switch, and updates its status. Signaling reaches steady-state.

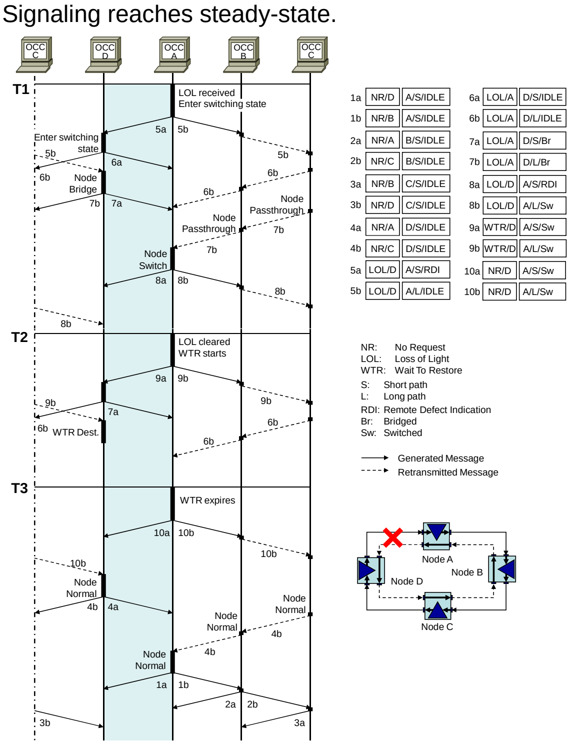

Fig. 2 GAPS messages for a LOL situation

At time T2, the LOL clears. Node A notifies this to its OCC, and OCC A enters the Wait-To-Restore (WTR) state, signaling its new state. OCC D, upon the reception of the WTR bridge request on the short path, sends out WTR. At time T3, the WTR interval expires. OCC A sends out No Request codes. OCC D, upon reception of the No Request code from OCC A on the long path, drops its bridge, and generates the Idle code. OCC A, upon reception of the Idle code on the long path, drops its switch and also generates the Idle code. All OCCs then return to the idle state.

Since the protection channels are shared among all spans, contention among the nodes may arise when multiple simultaneous failures occur. In these cases request with the lowest head node Id has priority.

Let us now analyze how to differentiate between span and node failure. When a LoL is detected, the detecting OCC cannot know at this stage whether the span or the adjacent node has failed. Assuming a span failure, the initiating OCC identifies the destination node as the one known to be on the other side of the assumed failed link. The identifier of the destination node is included in the message. When the relayed message reaches the other end of the failure, it will either find itself as the nominated destination node, in which case the failure was indeed a link failure as assumed, or it will find itself as the node one short of the destination identified, in which case the unreachable destination is a failed node.

In contrast to other protection schemes, in OMS-DPRing connections do not run the risk of misconnection in case of a node failure. Thus, connections ending at that node are not squelched.

LMP extension definition

We define GAPS as an LMP extension running in the control plane of ASON/GMPLS networks. GAPS protocol manages protection messages signaling, being complementary to the automatic provisioning functionalities.

GAPS protocol uses control channel management functionalities provided by LMP protocol. Once a control channel is activated between two adjacent nodes, the LMP Hello protocol can be used to maintain control channel connectivity between the nodes. Our proposal for extending LMP with GAPS consists in the definition of a new LMP Message. This message is used to transmit GAPS information when the LMP adjacency is part of an OMS-DPRing structure GAPS controlled. The GAPS object contains the source and destination node Id, the request type, the path (long or short) and the status of the protection switch.

Performance Evaluation

The performance of the GAPS mechanisms has been experimentally evaluated over rings with up to 18 nodes over the ASON/GMPLS CARISMA network testbed [4]. The evaluation comprises both the performance of the GAPS mechanisms and its scalability. Our objective has been to compare the experimental results with the general network objectives defined for SDH MS-SPRing. According to [5], the maximum number of nodes on a MS-SPRing ring is sixteen and the end-to-end switch completion time must be within 50ms after detection of a fault for a SDH ring of less than 1200 km of fiber.

Let us define switch completion time (T_{DPRing}) as the interval from the decision to switch to the completion of the switch operation at the node initiating the bridge request. It includes notification from the initiating optical node to its OCC (T_{config}), the propagation delay in each control network link (T_{link}), the processing time in each OCC ($T_{control}$), the time to configure (T_{config}) each optical node in the ring to perform the switching action and the time to switch itself (T_{switch}). Then, T_{DPRing} can be expressed as:

$$T_{DPRing} = 2T_{config} + T_{switch} + (2n-1)T_{control} + 2(n-1)T_{link} \quad (1)$$

From the experimental tests we obtained that T_{config} is 5ms, T_{switch} is 1ms and $T_{control}$ is about 0.25ms. Finally, T_{link} depends on the length of the links (L) of the ring. Fig. 3 shows the switch completion time for GAPS protocol as a function of the number of nodes (n) in the ring and for several lengths of the links in the ring. It also shows the scalability of GAPS when the number of nodes in the ring is increased.

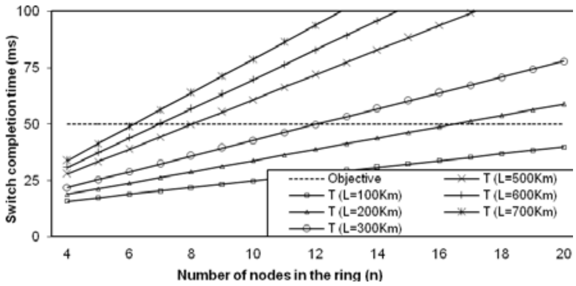

Fig. 3 Switch completion time

The maximum number of nodes in the ring ranges from 6 to 26 for links with length (L) ranging from 700 km to 100 km. In the worst case, the total length of the ring is 2600 km, outperforming in such a way the 1200 km specified for SDH networks.

Conclusions

We have presented GAPS, a protocol based on the extension of the standardized GMPLS LMP protocol in order to support efficient protection for OMS-DPRing. The experimental results allow concluding that the GAPS mechanism is able to provide efficient protection even in large optical rings.

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

References

1. L. Berger, et al., RFC 4873, (2007).
2. J.P. Lang, et al., RFC 4872, (2007).
3. J. Lang, RFC 4204 (2005).
4. E. Escalona, et al., ICTON 2 (2005), 21-24.
5. ITU-T Rec. G.841 (1998).