Optical Layer Survivability: A Post-Bubble Perspective

Ori Gerstel and Rajiv Ramaswami, Cisco Systems

ABSTRACT

We revisit the topic of optical layer protection from a motivation and deployment perspective. We first discuss the changes that have occurred in optical networking in general and the implications for protection. We then discuss scenarios where optical protection makes sense, recognizing that other fast protection schemes at the client layer provide viable alternatives in certain cases. Our conclusion is that optical protection makes sense for metro networks, as long as they are based on simple dedicated schemes. When it gets to more complex shared ring and mesh protection, we believe that OEO-based schemes are more viable, whether crossconnect-based or packet-switch-based.

THE STATE OF THE OPTICAL LAYER

Much has been said and written about the state of optical networking after the burst of the telecom bubble. Huge investments during the bubble years yielded significant advances on both the component and system fronts. However, with the current business conditions, carriers are not deploying new technologies unless there is a sound near-term return on investment potential. This has caused them to focus more on deploying infrastructure closer to the edges of the network in response to direct user demands, and a dramatic slowdown in long-haul deployments.

The fundamental realities reflected in our original article [1] are still valid and perhaps even more significant today. Business continuance and disaster recovery applications rely heavily on network survivability, and have become even more important after 9/11. IP, synchronous optical network/synchronous digital hierarchy (SONET/SDH), and various storage-related protocols such as Fibre Channel continue to be the main client layers of the optical layer. The leading survivability mechanisms are still relatively simple and limited in scope: basically, various forms of dedicated 1 + 1 protection (see Table 1 for a summary of the different protection schemes from [1]).

Within this context, optical layer protection has been deployed primarily in metro WDM networks serving storage applications. In fact, it is hard to sell a metro WDM system today that does not support various forms of simple optical layer protection. Long-haul WDM networks, on the other hand, have relied primarily on SONET/SDH layer protection, with some rare exceptions.

OPTICAL LAYER SURVIVABILITY: WHY AND WHY NOT

The main reason for having survivability at the optical layer, rather than leaving it to the higher layers, has not changed: protection at the optical layer is more cost effective for high-bandwidth services that lack their own robust protection mechanisms. The obvious candidates here are storage networking protocols, which do not have adequate survivability built in. As a result, these applications rely almost entirely on optical layer protection to handle fiber cuts and failure of the networking equipment; this is perhaps the single major reason for commercial deployment of optical layer survivability to date.

In other applications, however, new fast and bandwidth-efficient protection schemes in the client layers have reduced the need for optical layer protection. For instance, mesh protection is now implemented in SONET/SDH layer optical crossconnects, and a few carriers have deployed this capability in their network.

Resilient Packet Ring (RPR) technology provides another good example of more efficient client layer protection schemes that reduce the need for optical layer protection. Under normal operation the entire ring bandwidth is available to carry traffic, and in the event of a failure half the bandwidth around the ring is utilized for protection of higher-priority traffic while dropping lower-priority traffic. However, the optical layer manages bandwidth at the wavelength

 0163-6804/03/$17.00

Acronym	Name	Explanation
OBLSR	Optical bidirectional line switched ring	A shared ring protection scheme, in which the entire DWDM signal is looped back around the ring to recover from a failure
OBPSR	Optical bidirectional path switched ring	A shared ring protection scheme, in which each lightpath is separately routed along the alternate path to recover from a failure
	1 + 1 linear optical multiplex section (OMS) protection	A dedicated point-to-point protection scheme in which the WDM signal is split over two fibers at the upstream OADM and selected from at the downstream OADM
	1 + 1 lightpath protection	A dedicated protection scheme in which two copies of the same lightpath are routed over diverse routes and selected from at the egress node
	SONET/SDH ring protection	This refers to legacy SONET/SDH schemes, either shared protection in the form of bidirectional line switched rings (BLSRs) or dedicated protection in the form of unidirectional path switched rings (UPSR)
	SONET/SDH mesh protection	A family of protection schemes that operate on the entire mesh network instead of breaking it into rings; these schemes could be at the SONET/SDH line level or SONET/SDH path level
RPR	Resilient packet ring	A shared packet-level ring scheme that provides bandwidth-efficient and fast protection for routers or Ethernet switches in ring configurations

Table 1. *A summary of protection schemes.*

level, not at the packet level. In the event of a failure, the optical layer cannot figure out how to keep high-priority packets while dropping lower-priority packets. Therefore, we cannot implement an RPR-like scheme within the optical layer.

Another stimulus for optical layer protection not mentioned in our article is the complexity of mapping client layer connections onto the optical layer. The complexity arises from the fact that the mapping must be done so that a single failure at the optical layer does not result in an irrecoverable failure at the client layer. This task rapidly gets out of hand once the mapping needs to be tracked across multiple technologies, multiple network layers (conduit, fiber, optical, SONET, IP), and their respective network management systems [2, 3]. Obtaining working paths and protection paths from different carriers does not guarantee resilience, as those paths may still share common physical right of way and may fail together in a catastrophic event. Protection switching at the optical layer makes it easier to track how the resources at that layer directly map into fibers and conduits.

What Has Been Deployed?

Among the various protection schemes we considered in the original article (Table 1), the ones being deployed include client protection, 1 + 1 lightpath protection, and 1 + 1 linear OMS protection. Client protection particularly makes sense for SONET/SDH networks deployed over the optical layer, and in some cases for IP routers connected using optical layer equipment. 1 + 1 lightpath protection has been implemented in a variety of ways, some of which protect against both fiber cuts and transponder (optical-electronic-opticalOEO) failures, while others protect only against fiber cuts.

The more sophisticated schemes we described (OBPSR, OBLSR, and optical mesh protection) have not seen much real deployment for a variety of reasons. Many WDM networks today operate at low utilization levels, with the number of deployed wavelengths (4–8) much smaller than the maximum capacity for which the systems are designed (32–64 typically). In this scenario, saving wavelengths using shared protection does not buy much. Second, shared protection schemes, particularly in the optical layer, may require more expensive equipment (additional amplifiers or regenerators to deal with the longer protection paths, optical switches to automate the switchover, etc.) and more complex operations (wavelength planning, dynamic routing to account for link budget impairments, etc.) than dedicated protection schemes, offsetting some of their benefits. Third, the protection switching time achievable may not be in the 50 ms range, due to inherent settling time limitations within the optical layer equipment, making it harder to argue that optical protection is a simple replacement for SONET/SDH ring protection.

Finally, from a service class perspective, we speculated that a variety of service classes would be offered. The reality today is that essentially two types of services are offered: fully protected lightpaths and unprotected lightpaths. There is a fair bit of talk about whether the protection switching time requirement of 50 ms can be relaxed to hundreds of milliseconds in some applications, and this may indeed be the case in the future.

The Road Forward

We believe that deployment of optical layer protection will continue to grow in both metro and long-haul networks, and will be a significant part of any equipment offering. At the same time, we do not think that sophisticated *shared* protection schemes at the *optical* layer

are likely to be deployed significantly anytime soon. This is because of the complexity of implementing such fast-reacting schemes in the optical domain and because the granularity of services does not yet justify the equipment that enables the necessary switching functionality.

However, the client layers will continue to offer more sophisticated protection schemes, such as reliable IP rerouting, RPR, MPLS fast reroute, or SONET/SDH layer mesh protection. In fact, we expect many of the techniques that have been discussed in the context of optical protection to be applied to SONET/SDH mesh protection instead. A good example of this is generalized multiprotocol label switching, which is more readily applicable at the SONET/SDH layer (see [3] for some of the complexities of implementing it at the optical layer).

References

[1] O. Gerstel and R. Ramaswami, "Optical Layer Survivability — A Service Perspective," *IEEE Commun. Mag.*, Mar. 2000.

[2] O. Crochat, J-Y. Le Boudec, and O. Gerstel, "Protection Interoperability for WDM Optical Networks," *IEEE/ACM Trans. Net.*, June 2000.

[3] J. Strand, A. Chiu, and R. Tkach, "Issues for Routing in the Optical Layer," *IEEE Commun. Mag.*, Feb. 2001.

Biographies

ORI GERSTEL [SM'01] (ogerstel@cisco.com) is a senior network architect for the Optical Networking Group at Cisco. Until recently he was a senior systems architect for Nortel Networks' photonic crossconnect product. Before joining Xros/Nortel, he was the systems and software architect for the Optical Networking Group at Tellabs. Prior to that, he performed early optical networking research at IBM Research. He has authored over 50 papers and patents on optical networks, and served on the program committee of OFC and other conferences and journals. He also teaches the Optical Protection short course at OFC. He received his Ph.D. degree from the Technion, Israel, in 1995. His interests include fault tolerance in optical networks and network planning.

RAJIV RAMASWAMI [F] joined Cisco Systems as CTO of the Optical Networking Group in September 2002. Prior to joining Cisco, he was vice president for photonic switching at Xros within the Optical Long Haul Group of Nortel Networks. From 1997 through 1999, he was director of the Optical Networking Group at Tellabs, responsible for development and marketing of Tellabs' metro optical networking products. Before the Tellabs acquisition, he spent nine years at the IBM T. J. Watson Research Center. Some of his notable accomplishments include being a recipient of the IEEE W. R. Bennett and W.R.G. Baker prize paper awards, an Outstanding Innovation award from IBM, a Distinguished Alumnus of the Indian Institute of Technology (IIT), Madras, 25 patents issued or pending, co-author of *Optical Networks — A Practical Perspective* (Morgan Kaufmann, 1998/2001), General Chair of OFC 2000 and Technical Program Chair in 1998. He received a B.Tech. degree from IIT Madras and M.S. and Ph.D. degrees in electrical engineering and computer science from the University of California, Berkeley.

We expect many of the techniques that have been discussed in the context of optical protection to be applied to SONET/SDH mesh protection instead. A good example of this is GMPLS, which is more readily applicable at the SONET/SDH layer