Photonic Network Communications, 4:3/4, 251–269, 2002

Optical Network Survivability: Protection Techniques in the WDM Layer

Guido Maier
CoreCom, Via Ampere 30, 20131 Milano, Italy
E-mail: maier@corecom.it

Achille Pattavina
Department of Electronics and Information, Politecnico di Milano, P.za Leonardo da Vinci 32, 20133 Milan, Italy
E-mail: pattavina@elet.polimi.it

Simone De Patre
CoreCom
E-mail: depatre@corecom.it

Mario Martinelli
CoreCom and Department of Electronics and Information, Politecnico di Milano
E-mail: martinelli@corecom.it

Abstract. This paper is an introduction to survivability of WDM networks. All the main optical protection techniques proposed as far as now for the WDM layer are classified and reviewed. In particular, commonly adopted protection strategies for ring and mesh networks are explained. Moreover, off-line planning of WDM networks able to support path protection is briefly introduced. Finally, an example of heuristic network-capacity optimization is presented, discussing results obtained by considering a case-study network.

Keywords: survivability, WDM

1 Introduction

Nowadays survivability of optical connections has grown into an issue of greatest importance for the wavelength division multiplexing networks (WDM). What stated above is due to the obvious reason that the interruption of a high-speed optical connection operating at such bit rates as 10 Gbit/s or higher, even for few seconds, means a huge waste of data information. The network operators of the new generation have therefore to face their customers' requirements, which are very stringent on the outage periods.

Network ''survivability'' is not purely an academic subject in the real telecommunication networks, failures happen quite frequently and with catastrophic consequences. The impact of the network outage can be normally measured in terms of customer-minutes, defined as the outage in minutes multiplied by the number of affected customers. Failures in an optical network can be distinguished depending whether they damage links or switching devices. In the first situation, faults often result from external causes: cable cuts are very frequent especially in terrestrial networks since fiber cables often share other utility transport conduits, such as gas or water pipes and electrical cables. Equipment failures in the network nodes are mainly due to internal causes, such as hardware degradation or management-software inefficiency. They can result also from exceptional events such as natural phenomena, power blackouts, bombing or terrorists attacks (this latter menace has become a very serious issue after the tragic events of September 2001). However, forecasting and statisti-

cally characterizing external causes is so difficult that they are not usually taken into account in network design.

Equipment malfunctions proved to be less common on average than transmission-link failures: on the other hand, the former can have devastating consequences since they can interrupt all the connections that traverse the failed node. Still no analysis, to our knowledge, has been published assessing the entity of damages caused to networks by the recent disaster in New York City (it is well known, however, that several links and nodes in Manhattan and in the proximity of the WTC were severely damaged). Another episode of the past can be mentioned. The most devastating failure in U.S. telecommunication history occurred in 1988 when a fire broke out in the Illinois Bell's Hinsdale switching office [1]. The consequences were worsened by the Mother's day holiday, which is considered the busiest day of the year, as far as telephone traffic is concerned. It took more than one month to completely restore connectivity.

In the past, failures were manually solved by temporarily re-routing the broken connections and sending teams to repair the damaged equipment *in situ*. Today, optical networks that still require manual re-routing can be considered as unprotected. The outage periods due to traffic recovery based on the human intervention are unacceptable, even if nowadays the apparatus of a digital telephone network can be remotely re-configured from an operative headquarters, a doubtless advantage compared to pre-digital telephone systems. At present no optical network operator is willing to accept unprotected facilities: survivability must be always guaranteed by adopting efficient techniques of automatic recovery from failures, that is to say re-routing broken connections automatically [2].

In this paper we intend to review the most widespread strategies up to now proposed to manage survivability in WDM networks. A preliminary work on the classification of protection techniques for WDM networks has already been presented [3]. In Section 2 the basic concepts underlying lightpath switching and the protocol architecture of the optical transport network are introduced. Section 3 briefly describes the protection techniques of the electronic protocol layers and discusses the motivations to introduce analogous techniques in the WDM layer. Section 4 presents a general classification of the possible strategies to guarantee survivability to the WDM network. The following three sections, 5, 6 and 7, describe in detail the main protection techniques known today to implement WDM protection in ring and mesh networks, respectively. Then, in Section 8 the particular case of path-protection is discussed more in depth, presenting a heuristic tool that we have developed to design and optimize WDM survivable mesh networks.

2 WDM Networks: Basic Concepts

Modern optical networks are complex systems designed according to a layered approach. Higher layers are fully managed by electronic equipment. Several protocols can be stacked one over the other in various combinations (IP over SDH, IP over ATM, ATM over Ethernet, IP over PPP, ATM over SDH, and so on). It has become a universally accepted concept that the WDM optical layer must behave as a common platform able to carry all the possible protocol combinations. This is the main reason why the WDM layer has been standardized as a circuit-switching oriented multi-protocol transport level. It is understood that multi-protocol refers to the ability of transparently supporting many different upper-layer protocol stacks. The main task of the WDM layer is connectivity and bandwidth provisioning to the electronic layers in a client–server relationship (Fig. 1). The provisioning service offered by WDM consists of setting up optical point-to-point circuits in order to fulfill requests of a point-to-point connection issued by the upper layer. Such a request defines a so-called virtual connection (or logical connection by some other authors), while an optical circuit is named lightpath. A lightpath is set up by reserving to the

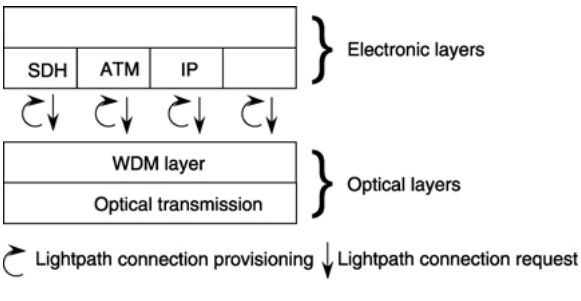


Fig. 1. Lightpath provisioning: a client–server relationship in a multiprotocol environment.

virtual connection a sequence of WDM channels linking the source to the destination node throughout the optical network. Each lightpath carries a high bit-rate digital stream. It is added and dropped by electro-optical devices interfacing the WDM layer to the higher electronic layers and it is transparently switched by each WDM switching device it crosses along its path. WDM switching is performed either by optical add-drop multiplexers (OADMs) or by optical cross-connects (OXCs), according to the type of network architecture we are considering (ring or mesh).

The WDM protocol layer is the set of protocols created to control and manage the so-called optical transport network (OTN). It is articulated in several sub-layers. This allows an easier implementation of the main WDM functions. According to the ITU-T Recommendation G.872 [4], WDM layer is divided into four sublayers: the optical channel sublayer (OCh), the optical multiplex section sublayer (OMS), the optical transmission section sublayer (OTS) and the physical media sublayer (Fig. 2). (The stack has been further complicated in a recent Recommendation still in a draft version [5], but we will not discuss it in this paper.)

The main entity managed by the optical channel sublayer is the lightpath. OCh takes care of all the end-to-end networking functions: routing and wavelength assignment, connectivity check, fault recovery. OCh signaling is carried by an optical supervisory channel (OCh-OSC): several techniques to associate the OCh-OSC information to each lightpath have been proposed in the past [6]; recently, the TDM technique (digital wrapper) prevailed and was included in the G.709 ITU-T Recommendation [5].

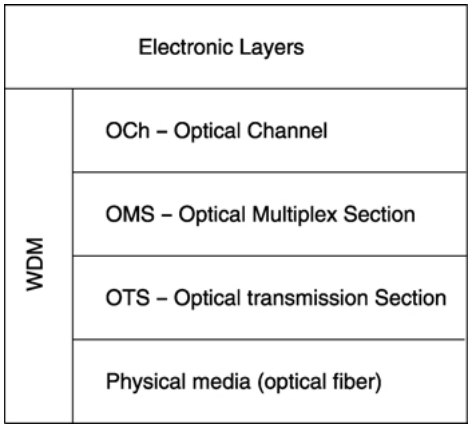


Fig. 2. Optical-transport-network protocol architecture: sublayers of the WDM layer.

The optical multiplex section sublayer controls not a single lightpath but the multiplex of all the WDM channels that transit on a single fiber, each one carried by a particular wavelength. Therefore its functions are not performed by the end-to-end lightpath terminations, as for OCh, but locally by each individual link terminations. OMS mainly performs WDM multiplex monitoring (i.e., checking of multiplex integrity and wavelength stability). Signaling for OMS is provided by an optical supervisory channel, normally transmitted by using a dedicated wavelength. Finally, the optical transmission section sublayer absolves all the control operations required to manage and supervise the optical transmission devices (amplifiers, transponders, regenerators and so on). The managed entity, as for OMS, is the WDM aggregate traveling on each fiber [7]. OTS signaling is provided by exploiting the same OSC used by OMS in time-sharing.

3 Survivability in the ''Classical'' Transport Network

Let us go back to WDM network survivability. This issue arose in telecommunication long before the definition of a WDM layer. Thus the main electronic layers of the transport network are today provided with standardized well-known protection mechanisms. For example, recovery techniques for a circuit- and a packet-switching environment have been defined for SHD/SONET and IP, respectively. The former are based on automatic IP-routing-table reconfiguration or on flexible load-sharing mechanisms: these two functions are supported by all the main IP routing protocols such as OSPF (open shortest path first), BGP (border gateway protocol) [8].

Even if in the future the direct implementation of IP over WDM becomes a reality, in most transport networks nowadays the SDH/SONET layer is the client of the WDM layer. For this reason, before WDM protection was defined, SDH/SONET protection mechanisms were mainly adopted to guarantee optical network survivability. Several of these mechanisms have been standardized, both for SDH [9] and SONET systems, to fully protect the network at tributary (path protection) or frame level (section protection), and for different network architectures:

point-to-point links (MS linear trail protection), rings (MS-SPRings) and mesh (SNC-P). When the WDM layer was created, ensuring the maximum compatibility with the legacy systems was a primary condition. Thus, the optical networks survivability techniques are based on many elements of SDH/SONET protection. For this reason some of the WDM-layer protection techniques that we are going to describe next are very similar to SDH/SONET, especially in the case of ring networks.

Given the existence of widespread and effective protection standards in the electronic layers, a natural question is why the introduction of other protection functions in the new WDM layer can be justified. As many authors point out [10], one of the main motivations is the possibility of exploiting optical layers to reduce the fault-recovery time below the values obtainable with SDH/SONET. SDH protection schemes have typical recovery-time from 60 to 100 ms. Beating this performance is the target of WDM protection. Improving the recovery time, in some cases by orders of magnitude, will indeed be possible in the near future with suitably designed schemes and advanced optical-switching technology (though already some papers have been published referring to WDM systems with sub-50-ms recovery times [11]). However, the other strong reason justifying WDM protection is that in general a failure should preferably be solved in the layer in which it occurs. Managing optical protection at a low protocol layer, just above the physical layer, implies that the control system has a direct knowledge of the physical topology and behavior of the network. For instance, information regarding optical-circuit performance (such as bit-error-rate, optical power, wavelength value, etc.) need not to be mediated through many layers: this reduces the total bandwidth consumed by the network control system overhead, simplifies signaling-data formats, and so on. All these benefits contribute to increase speed and effectiveness of the protection procedures.

4 Optical Layer Survivability

Having presented the protocol environment and discussed the motivations of WDM survivability, the details of the various protection techniques that have been proposed in literature can now be reviewed. Some general and ''orthogonal'' criteria can be assumed in order to classify these techniques.

A first classification criterion regards the particular sublayer of the WDM layer in which a given protection mechanism operates. Two alternatives exist: optical channel sublayer or optical multiplex section sublayer. In the first case the lightpath is the entity to be protected, so that OCh protection is also called path protection. In case of failure each single interrupted lightpath is switched on its protection path [12,13]. Recovery operations are activated by the OCh apparatus hosted in the end-nodes (source and destination) of the lightpath. These systems also have the duty of monitoring lightpaths for failure detection. The protected entity is called working lightpath, while after the failure the optical circuit is switched over a protection lightpath. This lightpath can be pre-allocated or dynamically established as is explained later on.

As mentioned above, the OMS-sublayer managed entity is the multiplex of WDM channels transmitted on a fiber. Thus, at this sublayer, fault recovery regards each network link individually, for which reason this is also called link protection [1]. The OMS apparatus in the termination of the fibers that compose a single link locally manages fault-detection and protection switching. Protection mechanism reacts to a failure by diverting the interrupted WDM multiplex to an alternative path, thus bypassing the damaged components. The main difference from path protection is that all the lightpaths traveling along a broken fiber are simultaneously re-routed together. Link protection is commonly implemented adopting one of two alternative modes: four-fiber and two-fiber mode. The choice between the two implementations is strictly dependent on the physical design of the network. The optical cables composing a typical WDM transmission link are usually bidirectional: that is to say the cable contains a set of fiber pairs, one fiber per each propagation direction. In a link protected by a four-fiber OMS system, for each fiber pair employed in the bi-directional transmission of the working traffic, a second pair is reserved for backup traffic of some other link in case of failure. In two-fiber OMS systems, instead, on each fiber of a couple of fibers in one direction, half of the WDM channels carry the working traffic, while the other half are used as spare resources to protect some other link. On the fiber of the pair in the opposite direction, the role of each wavelength is inverted: if it was a working

wavelength in the other fiber now has turned into a protection wavelength and vice versa.

According to a second classification criterion, WDM protection mechanisms can be divided on the basis of their ability to guarantee that the network survives only to link failures or both to link and node failures. A special type of node failure is the malfunction of a transmitting or receiving line card: in this case, providing the node with a redundant number of line cards (span protection) can ensure resilience. Apart from this simple technique, a node is protected if the network is able to withstand a failure in its switching subsystems. Usually survivability to node general failures is achieved by employing a more complex technique and a large amount of spare resources than the simple link protection. A protection technique for node failures is frequently also able to recover a link failure.

A third important aspect by which WDM survivable networks can be grouped concerns the dynamic management of the protection capacity. About this characteristic, two radically different approaches are possible [13]. The most widespread approach in the real commercial applications is preplanning: spare resources are pre-allocated when a lightpath is established (on-line) or, if the traffic is purely static, during the planning of the network (off-line). The network is in a sense ''ready'' to react to a failure: after such an event has been detected, the nodes have to perform simple switching operations, often without the need of any intervention of the network management system. This feature allows us to obtain a fast recovery; the drawback is that each WDM channel is rigidly allocated to serve as working or spare resource. At least, some preplanned schemes exist in which, in absence of failures, the spare channels can be used to transmit low priority traffic (pre-emptive) that can be interrupted or lost to recover high priority traffic. The alternative to preplanning is provisioning (also called restoration) [13]. In this case the network is in general planned with an amount of resources that exceeds the real working-traffic requirements and no spare capacity is allocated. When a failure occurs, the network activates new connections to restore the faulty ones. Provisioning has the advantage of increasing flexibility to the network system, potentially improving resource utilization for the working traffic. A second advantage is that it gives the network some chances to survive multiple simultaneous failures (e.g., as in the case of a large-scale environmental disaster). A preplanned survivable network, on the opposite, because of the rigid association between protection resources and working lightpaths, is not able to face an unknown number of simultaneous faults. (Some works analyze the effects of multiple failures on WDM network with preplanned protection [14,34] and complex preplanned protection techniques are under study that are able to recover some simultaneous failures—for simplicity we will not consider these events any more in the rest of this paper.) Provisioning, however, suffers the disadvantage of not being completely safe: in fact there is no guarantee that after a failure there are enough spare resources to accommodate all the new protection lightpaths. A second major drawback is that provisioning requires an intense activity of the network management system to set up new connections and therefore the recovery time is long. The recent evolution of the WDM control plane, aimed to efficiently support dynamic traffic (automatic switched optical networks, ASON), seems to make protection by provisioning more feasible than in the past.

A final classification criterion can be applied to the preplanned techniques only. Preplanned protection can be implemented as dedicated protection or shared protection. The simplest and most conservative preplanning procedure is the reservation of a set of spare resources exclusively to one working entity (a lightpath in OCh protection or a link in OMS protection). This is the so-called dedicated protection: it reduces the complexity of failure recovery, but requires that at least 50% WDM channels cannot be used by the (non-preemptive) working traffic. Since preplanned protection is based on the assumption that a multiple failure is a very unlikely event, two or more protection entities (lightpaths or fiber sequences for OCh and OMS protection, respectively) can actually share some resources (WDM channels or fibers, respectively). This is possible provided that the corresponding working entities cannot be simultaneously involved by a single failure event (they cannot belong to the same shared risk group, a concept introduced in recent literature [15–19]). Shared-protection strategy exploits this property by preplanning the network so that some WDM channels or fibers are shared by more protection entities. Shared protection allows one to sensibly reduce the amount of spare resources and to improve network utilization for working traffic, at the cost of increasing the recovery

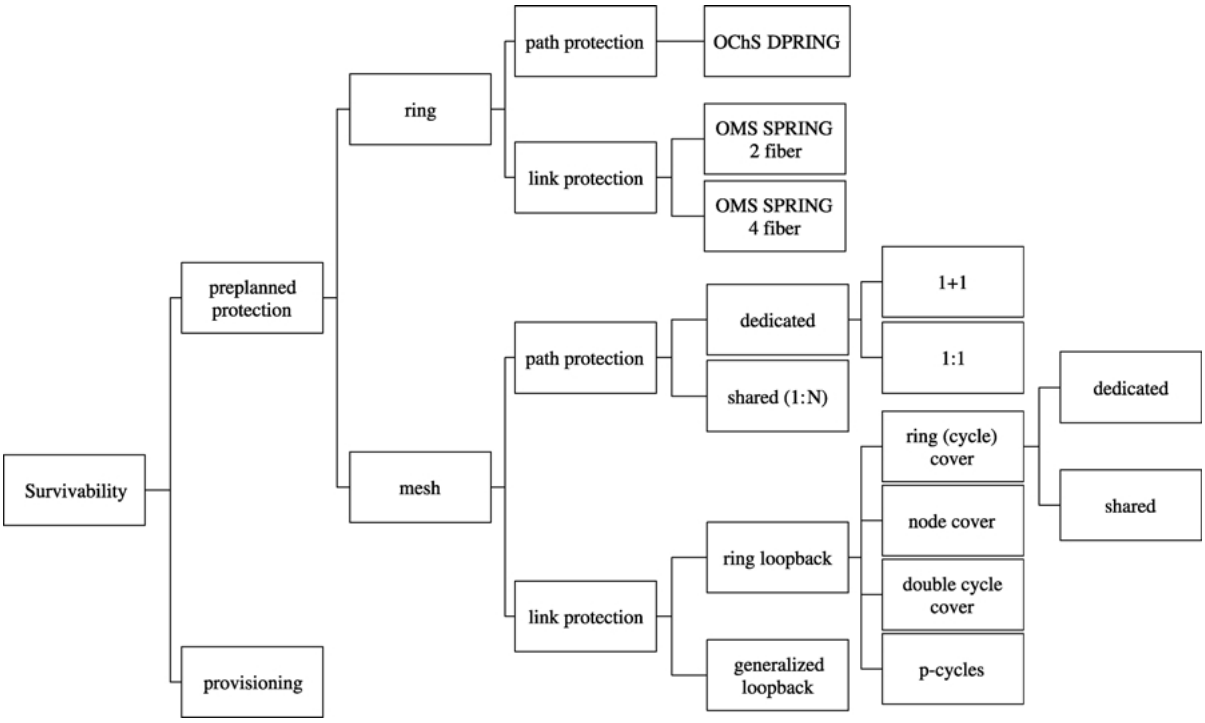


Fig. 3. General classification scheme of the protection techniques implementing survivability in the WDM layer.

procedure complexity (we will discuss this point further on).

A general classification of the survivability schemes in the WDM optical networks is shown in Fig. 3. In the following sections of the paper the most important protection mechanisms for ring and mesh architectures will be described in detail. Mainly preplanned protection will be considered, leaving provisioning for future works.

5 WDM Ring Network Protection

Most WDM optical networks today are based on the ring topology, especially in metro or regional areas. For its simplicity and its easy integration with SDH structures, WDM ring can be considered historically the second stage in the optical network architecture evolution (the first being point-to-point) and the environment in which WDM protection techniques were standardized. For this reason well-known simple and tested solutions exist since a long time (it should be noted that ring nodes have degree 2, the minimum necessary to support survivability).

For path protection, the OCh dedicated protection ring (OCh-DPRing) scheme has been defined: it is applied to rings that use two fibers to propagate the signals in opposite directions (Fig. 4). Path protection is designed using both the fibers to establish two counter-propagating lightpaths around the ring. The source node splits the signal in two identical copies transmitting them simultaneously on the two different lightpaths. The receiver node selects the signal with the best quality. This scheme is defined as $1 + 1$ dedicated protection (also protection switching) and the architecture is also known as WDM self-healing

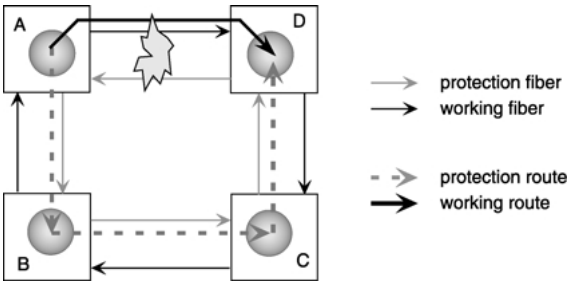


Fig. 4. OCh dedicated protection ring (OCh-DPRing): $1 + 1$ protection of the lightpath AD.

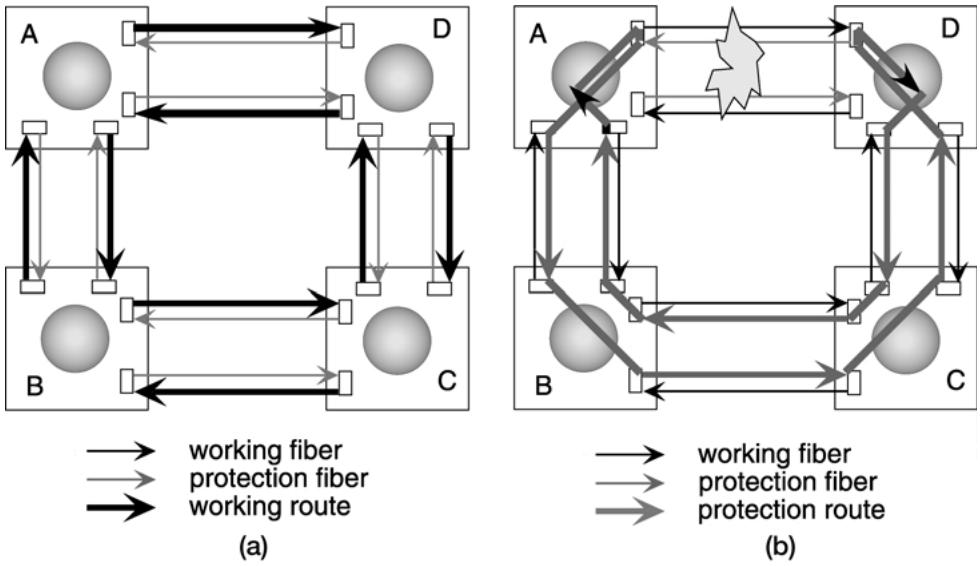


Fig. 5. OMS shared protection ring (OMS-SPRing), four-fiber implementation. The ring is represented in working conditions (a) and after a loopback (b) due to a failure on link AD.

ring. In case of failure no optical switching device has to be reconfigured: only the electronic receiver has to make the best choice. No signaling is necessary. Recovery time is then very fast and protection requires exactly 50% of the installed physical resources (in the $1 + 1$ case spare capacity sharing is not possible).

In the OMS sublayer two schemes of link protection are standardized and they are called shared protection ring (OMS-SPRing) for two- and four-fiber ring topology. In both the cases, protection switching is carried out by 2×2 optical switches with large optical bandwidth, able to switch the multiplex of WDM signals from one fiber to another. Switching occurs very fast, in the range of microseconds in case of opto-mechanical technology. These devices (two and four in the two- and four-fiber schemes, respectively) are usually hosted into the optical add-drop multiplexers (OADM). Fig. 5 represents the four-fiber scheme. In case of link failure, the two OADMs adjacent to the failed link, recover the connectivity by closing the ring (loopback operation) and rerouting the traffic on the fibers or the wavelengths reserved to protection. OMS-SPRings are able to react also to a node failure: in such case the 2×2 optical switches inside the failed node itself operate the loopback. Reverting (normally preferred) or non-reverting implementations are possible, according on the fact that the system returns to its original state after the failure has been recovered. Protection needs again the 50% of the physical resources: in this case sharing does not give an actual advantage over the DPRing in terms of resources utilization. Signaling between the two terminations of the faulty link is required to coordinate the loopback operation.

6 WDM Mesh Network Protection

Though the ring is the most common physical topology today, WDM mesh networks are beginning to assume more importance, especially thanks to the development and improving of the OXC, the optical switching device in the mesh architectures. In a mesh network, survivability is a more complex problem than in a ring topology because of the greater number of routing and design decisions that has to be taken [6,20,21]. Besides, no WDM mesh protection mechanism has been commercially deployed on a large scale yet, and therefore all the techniques that we are going to discuss in this section are equally likely to become the best choice in the future.

Path protection at OCh layer is obviously well applicable to mesh networks [22]. To satisfy each connection request a pair composed of a working and a protection lightpath has to be established (Fig. 6a). For the protection mechanism to be effective against

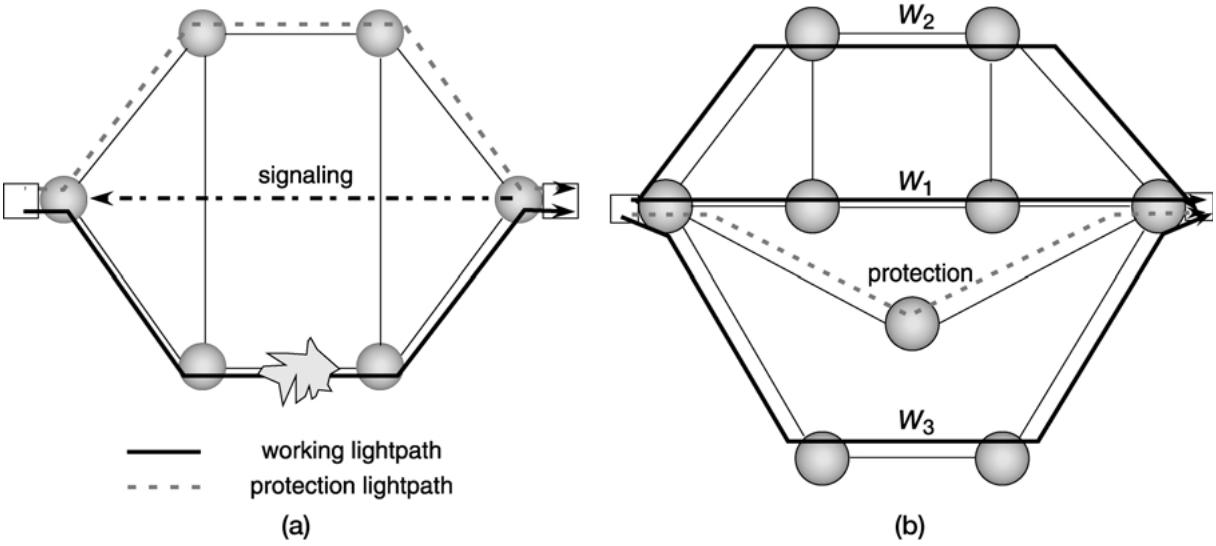


Fig. 6. Path protection in a mesh network: (a) 1:1 dedicated protection; (b) 1:3 shared protection.

link failures, the links of the working and protection lightpaths must be independent in the sense of failure occurrence. In many cases, this condition is satisfied by setting up the two lightpaths in physical-route diversity: the primary and backup paths cannot share any link (link disjointness[1]). If protection against node faults is also required, node independence between work and protection paths is also necessary. Again, in most cases this is guaranteed by preventing sharing of a node by the two lightpaths: routing must be performed under the node-disjointness constraint (this latter, of course, implies link-disjointness).[2] Both the $1+1$ dedicated path protection and 1:1 dedicated path protection are possible [24]. In the second case (also called protection transferring), low priority traffic can be transmitted on the protection lightpath in absence of failure, but end-to-end signaling becomes necessary (Fig. 6a). Dedicated path protection is quite resource-consuming in mesh networks because of the physical route diversity constraint. Sharing of WDM channels among protection paths may reduce the physical resources employed for protection. Shared protection may be applied in an end-to-end sense using a single protection lightpath for N working lightpaths with the same source-destination node pair (Fig. 6b). This technique is a special case of sharing in which N protection lightpaths share all their WDM channels, and is also known as 1:N protection. Obviously 1:N protection requires that $N+1$ link-disjoint (or node-disjoint) paths are available between the source and the destination nodes of the connection.

Shared path protection can also be implemented in a wider sense on a mesh network by allowing partial sharing among the protection lightpaths. In this case the additional constraint that we mentioned in Section 4 must be taken into account: protection lightpaths sharing WDM channels must be associated with working lightpaths that are mutually link disjoint (or node disjoint) [12,20]. It is important to notice that sharing allows savings in terms of transmission resources, but it also requires a more complicated management. In 1:1 and in 1:N protection, when a failure occurs, only the end-nodes are involved in the recovery process because the protection lightpaths are completely set up in advance. When shared-path protection is adopted in the wide sense in a mesh network, the fault event activates a more complex recovery procedure that requires a lot of signaling among several network elements. It is, in fact, necessary to reconfigure all the OXCs that are terminations of shared WDM channels (see Fig. 7) according to which particular working lightpath needs to be recovered. This inevitably increases the recovery delay, which will be limited by the time taken by the signaling messages to reach all the involved elements plus the time taken to reconfigure all the OXCs. Since shared protection is still preplanned, the recovery operation could be controlled in a distributed rather than in a centralized way, thus eliminating the

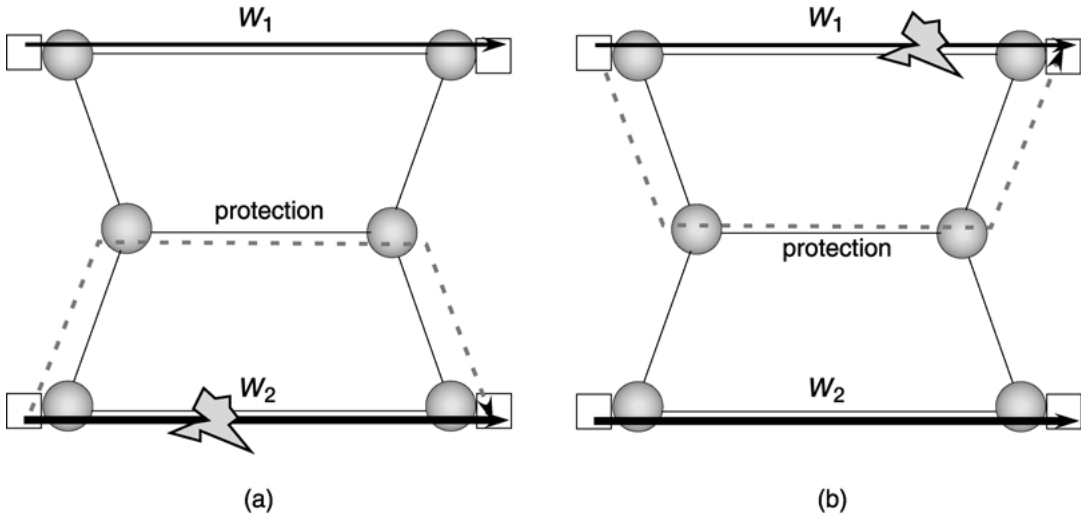


Fig. 7. Shared path protection in a mesh network. Different network configurations when a failure affects the lightpath w_1 (a) or the lightpath w_2 (b), whose protection-lightpaths share a common fiber.

intervention of the network management system and reducing the amount of signaling. In this case, the OXCs must be able to autonomously identify the faulty working lightpath in order to switch accordingly. The first operation requires real-time detection of the lightpath identity and it is one of the main motivations that fostered the definition of an OCh identifier in the framework of the standardization of the OCh supervisory channel [4,5,25].

In WDM mesh networks, link protection at the OMS sublayer (Fig. 8) under some aspects can be preferable to path protection. In a complex topology, a local recovery mechanism, more suitable to distributed than to centralized control, is easier to manage than an end-to-end mechanism. Link protection on a mesh network can be carried out in various ways [22,26]. We will not consider link protection based on provisioning. Rather, we are going to describe the two

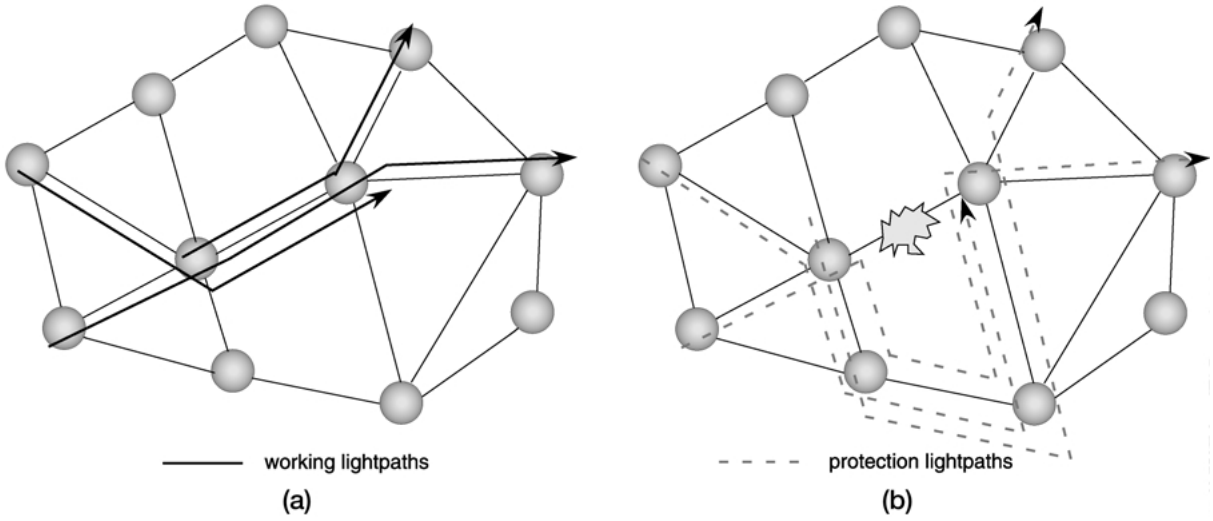


Fig. 8. Link protection in a mesh network. All the lightpaths crossing a link (a) are rerouted on a common protection route (b) when the link is down.

main known approaches to preplanned link protection: one is based on the loopback-by-rings concept while the other, more recently proposed, on the generalized-loopback technique.

A mesh network can be naturally created by simply interconnecting several rings: this is actually how most of the existing WDM networks are managed today. Switching between the rings in such networks is performed electronically often by SDH/SONET digital cross-connects. Survivability in WDM multi-ring networks is therefore often guaranteed by SDH/SONET protection techniques (which, in particular, exploit redundancy of the inter-ring interconnections). Some of these techniques will probably migrate also to the WDM layer (e.g., for the special case of submarine WDM multi-rings, see Desbrulais et al. [27]). In the following, however, we would like to drop the multi-ring architecture and focus on the ''actual'' WDM mesh networks, i.e., those created starting from a mesh physical topology and which exploit OXCs to perform optical switching throughout the whole network. This future-proof architectures ring decomposition serves only to the survivability.

The loopback-by-rings principle can be applied to a ''actual'' WDM mesh network as follows. First the network is decomposed in several sets of fibers, each set managed as a single ring. Once decomposition is made, each ring is equipped with an OMS protection system exactly like an OMS-SPRing. Each ring becomes, therefore, a protected system that reacts against failures looping back the faulty connections. Normally the four-fiber ring-protection implementation is the best choice, since the two-fiber implementation might require wavelength converters in several nodes. A clear advantage of this approach is that it allows distributed recovery: each ring is an automatic and autonomous recovery system. This implies that recovery time is bounded only by the ring size (in path-protection, instead, the source-to-destination propagation delay must be taken into account). Moreover, fault management is confined to the faulty ring.

The main design problem concerning the loopback-by-rings approach is how to perform ring decomposition of the meshed network topology [28]. In fact, provided that the physical topology of the network is at least two-edge connected, recovery is possible if a family of directed cycles can be defined over the network. This operation is carried out under the following constraints: minimizing the network resources, realizing a distributed control and fast recovery, protecting as many links as possible and ensuring good scalability of the protection mechanisms if the network is expanded. Attempting to solve this problem by inspection is possible but extremely difficult, given that the design constraints are apparently in conflict. Some systematic approach is required to obtain effective decompositions. Some techniques that have been proposed to satisfy these requirements will now be briefly reviewed.

The first mesh-ring decomposition is known as node cover [29]: the set of rings is chosen in a way that each node belongs to one or more rings and each link belongs at most to one ring. A node cover does not necessarily cover all the links and the uncovered links remain without protection. This problem is avoided using the ring cover, based on the following ring decomposition condition: each link must at least belong to one ring. Such a necessary condition assures that all the links are protected but does not constrain spare resource redundancy: each link could belong to any number of rings. An optimization technique must be therefore exploited to identify the minimal ring cover of a given topology.

Cycle cover is a four-fiber ring-cover technique, based on the assumption that each network link comprises a pair of counter-propagating working and a pair of counter-propagating protection fibers [28]. A family of directed cycles must be identified which fully cover all the protection fibers, under the constraint that each protection fiber is used exactly once. In the particular case of a planar topology, finding the optimal ring cover is simple. In fact, each cycle corresponds to a face of the graph, chosen with the proper orientation so that each link is covered on both the directions (Fig. 9a). In a planar graph there are always $f - 1$ internal faces plus one external face. f is the Euler number of the graph: $f = 2 + E - N$, where E is the number of edges and N is the number of nodes [1,28]. Based on the cycle decomposition of the topology, cycles of protection fibers are identified on the network (Fig. 9b). In this way each working fiber in the network has a backup path (Fig. 9b). The recovery operation (also called automatic protection switching, APS), carried out by the switching devices inside the nodes, is very similar to the OMS-SPRing recovery operation.

Unfortunately in the general case cycle cover is difficult to apply. Finding the minimal ring cover in non-planar networks is an NP-hard problem and it is

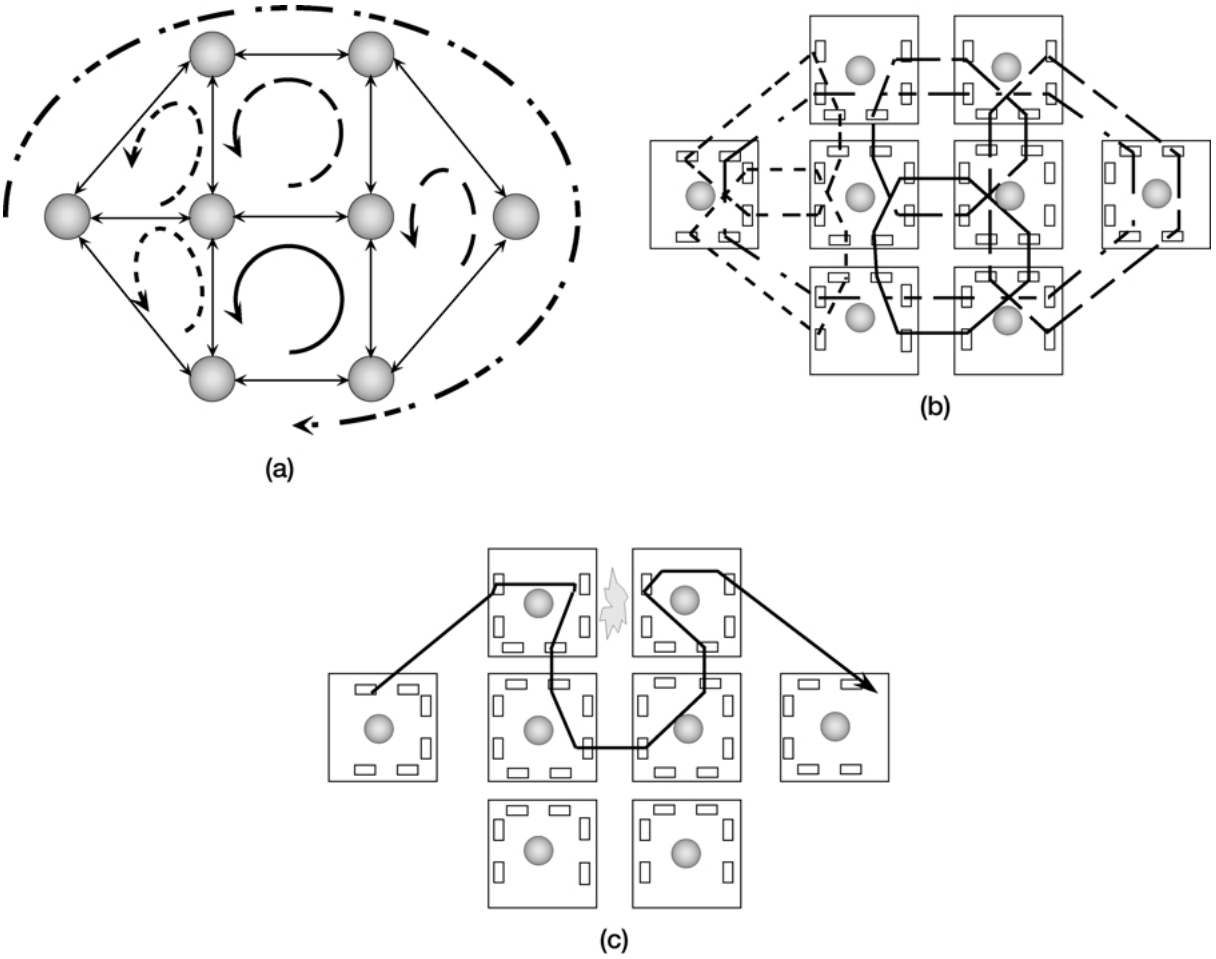


Fig. 9. (a) Mesh-topology decomposition by the cycle-cover technique. (b) Protection cycles defined by the decomposition. (c) Recovery of a lightpath after a link failure.

also not scalable: for instance, if a new node is added, the network must be completely reconfigured. (Another case in which the minimal ring cover can be found in polynomial time comprises networks having an Eulerian physical topology [28].)

A second ring cover technique is the so-called multiple WDM self healing ring protection (M-WSHR) [30]. Designing a survivable network based on M-WSHR requires three steps: first, all the working traffic is routed, without specifying the spare capacity (WL-step); secondly, a ring cover is defined on the network (RC-step); finally, the spare capacity is ring-by-ring dimensioned (SW-step). The last step can be performed in a dedicated or shared mode. In the dedicated mode, each link of the ring is protected by its own set of backup lightpaths, one per working lightpath crossing the link. In this mode, full survivability is achieved but the amount of spare WDM channels is very large. In the shared mode, instead, each ring is arranged as a four-fiber OSM-SPRing. All the spare fibers having a clockwise direction are equipped with a number of wavelengths equal to the number of WDM channels allocated to working traffic on the most loaded working fiber in the counter-clockwise direction. The same procedure is applied to the fibers in the opposite directions. Beside protection-wavelength sharing inside each ring, more rings can also share protection fibers, provided that they employ different protection-wavelength sets. The M-WSHR protection technique can by applied only to networks supporting full-wavelength conversion.

A possible alternative to the ring cover is the double cycle cover [28,31]: cycles are chosen in such a way

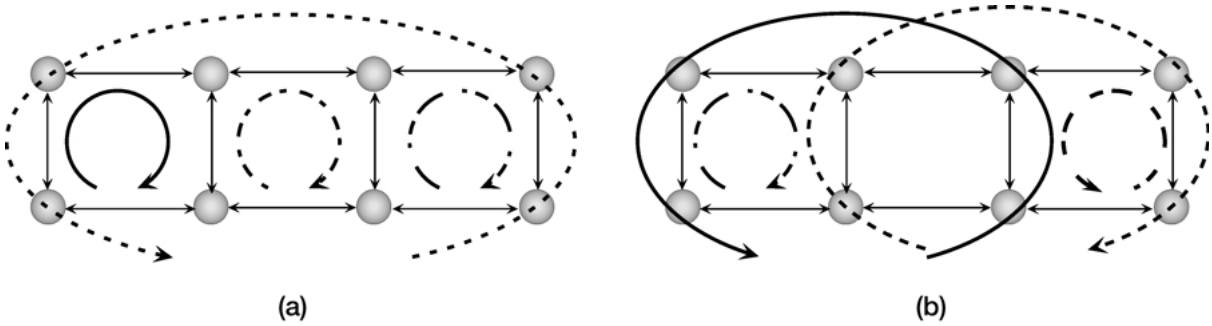


Fig. 10. Two possible (planar)-mesh-topology decompositions obtained by applying the double-cycle-cover technique.

that each link appears exactly in two rings (Fig. 10). In case of planar topology, an optimal double cycle cover can be found in a polynomial time; very efficient heuristic methods exist for the non-planar case (though the existence of a double cycle cover can only be conjectured): for this reason this method is often preferred to cycle cover. In theory double cycle cover can be adopted both in four-fiber and in two-fiber implementations. In practice, however, only the four-fiber version is feasible. The main difficulty in the two-fiber version is wavelength assignment under the constraint that the backup wavelengths all along the backup path of a given link are the same as the working wavelengths on that link. This is impossible on most networks without adding wavelength converters in some nodes (for example, both the covers represented in Figs 10a and 10b require converters). Finding the double cycle cover that minimizes the number of wavelength converters to be added is a very difficult problem.

Recently the preconfigured protection cycle (p-cycle) technique has been proposed [32]. It is based on the property of a ring to protect not only its own links, but also any possible chordal link (a link connecting two non-adjacent ring nodes) (Fig. 11). Actually, chordal links result to be double-protected, since two different restoration paths are available on the p-cycle (Fig. 11b). P-cycles allow savings in spare resources and are recognized to be the most efficient protection structures as for capacity minimization. However, p-cycle planning is an NP-hard problem and is not scalable.

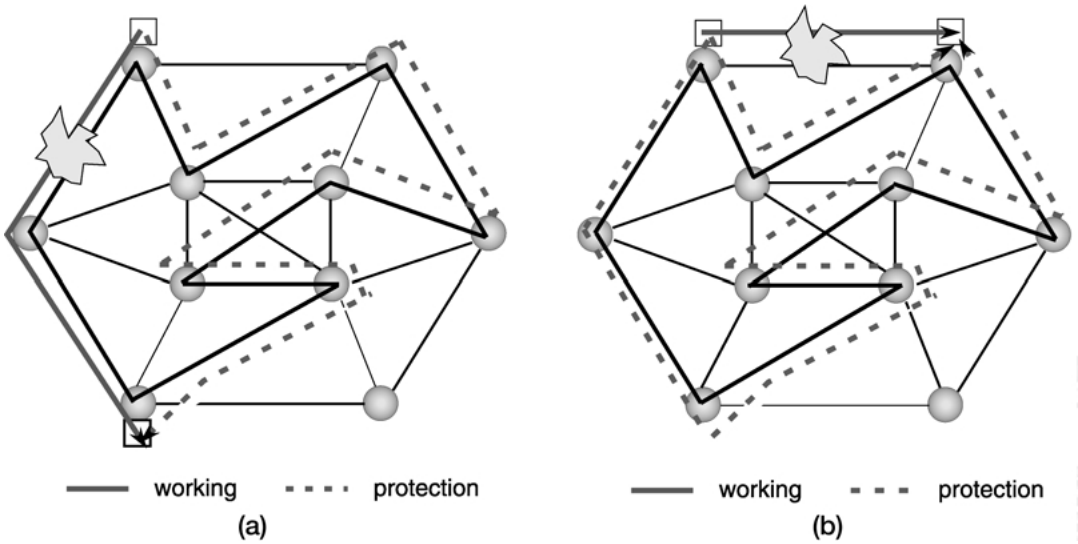


Fig. 11. P-cycle protection design. A ring is able to recovery either one of its links (a) or one of its chords (b).

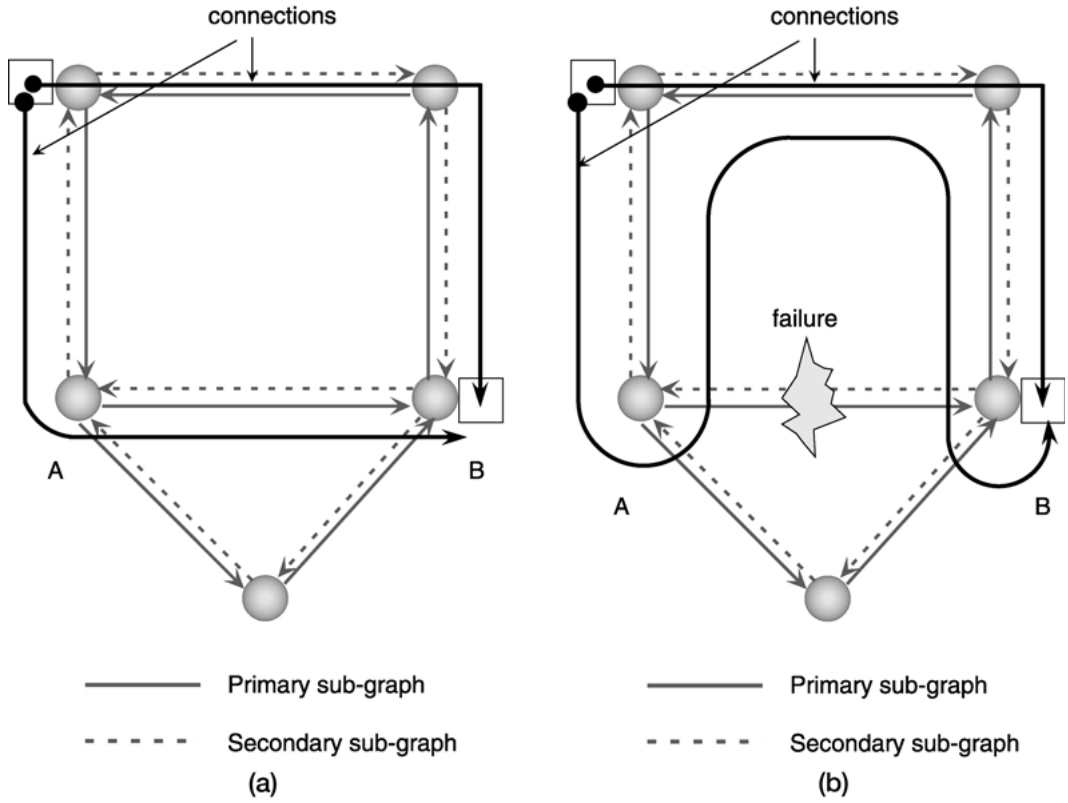


Fig. 12. Generalized-loopback protection. Two lightpaths are represented before (a) and after (b) the failure of link AB.

Link protection implemented in mesh networks exploiting the generalized loopback principle [33] is radically different from the previous cases. Let us consider a network having two fibers per link, for simplicity. The graph modeling such a network can be divided in two directed and conjugate subgraphs, in such a way that each link is crossed by one arc of each subgraph in the two opposite directions (Fig. 12a). One of the two subgraphs is chosen to represent the working network resources, while the other is reserved for protection and is kept idle in normal conditions. In case of link failure, the upstream node operates the loopback diverting all the working channels over a fiber belonging to the protection subgraph; the recovered optical signals then propagate by flooding through the network. Since the subgraphs are conjugate there is the guarantee that at least a copy of the original signal reaches the node downstream of the faulty link. This node then performs an inverse loopback, re-inserting the signals in the working subgraph, thus restoring connectivity (Fig. 12b). Generalized loopback is very efficient in terms of network resources and it is suitable to distributed control. It is also scalable since it allows the network to grow without the need of entirely reconfiguring the protection mechanisms.

7 Some Concluding Remarks

This overview of different protection techniques is mainly supported by qualitative considerations. A complete survey would have also to compare the techniques on the basis of quantitative numerical data, obtained e.g., by simulation of a certain number of case studies. Such a work goes beyond the scope of the present paper, as it is a very difficult task deserving another entirely dedicated article. Works in literature dedicated to this task are quite rare and compare only some of the techniques presented above [1,34]. The great difficulties in carrying out such a comparison lies not only on the heavy modeling and computation burden that must be faced, but also on the problem of comparing so different cases and scenarios.

To conclude our discussion, we can, however, suggest a set of performance parameters that would have to be considered while comparing WDM protection techniques. The first important parameter is the spare network capacity, i.e., the amount of extra transmission resources dedicated to protection in excess of those strictly sufficient to build the network with no protection. Other parameters are: switching speed of connection recovery, cost of protection equipment and protection mechanism control complexity (including, for example, the amount of bandwidth consumed by signaling).

These parameters are linked by various trade-offs. We have already underlined the trade-off between spare resources and control complexity (e.g., dedicated vs. shared protection). Other obvious trade-offs exist, for example, between control complexity and switching speed, between equipment cost, control complexity and switching speed, and so on. Survivable network optimization is the problem of evaluating the best solutions in these trade-offs, given a certain network scenario: the choice of the best protection technique is the result that can be obtained after an objective function has been determined by suitably weighting the parameters reported above according to the needs and the priorities of the network operator. As in every optimization problem, another part of the definition, beside the objective function, is represented by the constraints. Besides constraints coming from the network system, there are others which depend on the reliability of the network itself. Most of the studies today employ simple ''hard'' constraints such as requiring that all the connections or all the links of the network are protected by simple redundancy. However, a more complex and more general way to define protection constraint is to define a parameter that allows a ''soft'' measurement of network reliability. The most commonly used parameter is network availability (or its complement unavailability), defined as the amount of time a system is working over a given lifetime period [35]. A target availability can be assigned in the form of minimum connection availability or mean network availability [36]. Availability evaluation of optical devices, switching systems, point-to-point links and SDH/SONET ring networks have been extensively studied [27,37]. Pioneering studies focusing the whole WDM network have introduced the similar concepts of quality of protection [38] and differentiated reliability [39,40]. The optimal design of survivable WDM networks assuming availability as a constraint or as cost function is, however, still a green research field. Very few (if any) systematic approaches have been proposed that are applicable to a very ample range of network scenarios.

8 WDM Network Heuristic Design with Path Protection

In this section we would like to concentrate on one of the protection techniques that have been quickly reviewed in the previous sections, in order to offer an insight on the issue of planning a survivable WDM network. In particular we chose to discuss the preplanned path protection case on a mesh topology. Clearly, survivability requires the network infrastructure to be provided with extra capacity reserved to backup, which increases the costs sustained by the network operator compared to an unprotected system. It is therefore extremely important that protection mechanisms are designed with care in order to minimize the required spare capacity. This brings optimization under survivability constraints into the foreground as a major problem of network design. As real WDM networks scale in size and connectivity, this problem can no longer be manually solved. Automatic tools and systematic optimization procedures become important aids to planning. The most important features of the tools are: simple implementation, ability to find good (optimal or quasi-optimal) solutions in a reasonable computational time, possibility to model several network environments. Network design tools should also give the operators the chance to explore a range of alternatives in the trade-off between network costs and quality of protection. In this context, we proposed a planning and optimization tool for survivable WDM mesh networks based on a heuristic approach [41–43].

In our approach the optical connections, requested by the upper transport protocol layers, are known *a priori*, and the physical network-topology (multifiber WDM links and OXC nodes) is given. Connections are established by suitably configuring optical switching nodes and by allocating network transmission resources to the various lightpaths. Allocation is jointly solved with network dimensioning with the goal of minimizing a given network cost parameter.

If a connection has to be protected, then its activation corresponds to the setup of a working/

protection lightpath-pair; otherwise only the working lightpath is established. The developed tool simultaneously finds the route and assigns fibers and wavelengths to the lightpath(-pair) (routing fiber and wavelength assignment, RFWA). In particular, the tool exploits multiple RFWA criteria, obtained by applying a set of traditional RWFA individual criteria, such as shortest-path and least-loaded (for routing), first-fit and most-used (for fiber and wavelength assignment), etc., according to a prefixed priority order (e.g., first shortest-path, then first-fit, then least-loaded, and so on). When two alternative lightpaths (lightpath-pairs) are equally good according to a certain criterion of the set, the next criterion in the set is selected in order to break the tie. The application of a prioritized set of RFWA criteria improves the heuristic efficiency. The connection requests are served by the tool one after the other, once the given set of requests has been sorted according to a particular order. Also request sorting is obtained by applying a heuristic rule: requests between nodes that are farthest apart and require the largest amount of connections are served first.

The first design phase is completed when all the connections requested to the network have been satisfied by performing RFWA. Network resources at this point are used with low efficiency, since the lightpaths were setup in a greedy way. Therefore, an iterative optimization cycle begins in which the network is scanned several times to spot under-utilized resources: the tool tries to reallocate lightpaths occupying such resources so that they can be completely freed and removed from the network. This approach, which proved to be quite computationally efficient, is called ''deterministic heuristic.'' When an alternative solution is found in the cycle that decreases the chosen cost function, this solution is deterministically accepted. The adoption of probabilistic strategies which can lower the chance of getting stuck in local minima (e.g., simulated annealing) will be considered as future improvement of our tool. The results shown in this paper concern minimization of the total number of fibers required to support all the connections with the given protection strategy. The tool, however, allows to choose other cost functions (e.g., the total fiber mileage).

An interesting feature of the particular heuristic algorithm we adopted to solve RFWA concerns routing of the working/protection-lightpath pair. This problem is basically equivalent to the search of the minimum-cost pair of link-(node-)disjoint routes between two nodes. An easy but non-optimal solution is to assign the best route (e.g., the shortest path) to the working lightpath and then the second best alternative to the protection lightpath. This approach is greedy: there are situations in which it fails to establish the working/protection lightpath pair even if there are enough unused resources. To overcome this obstacle, we have studied an algorithm which is able to compute the minimum-cost pair of link-(node) disjoint routes in one single step, thus simultaneously identifying both the working and the protection lightpaths. If enough resources are available, the search is always successful and the identified route-pair is actually minimal. The algorithm we have developed is an adaptation of Bhandari algorithm [23] to a WDM network environment (modeled by a wavelength layered graph).

Thanks to the flexibility of heuristics we were able to model several physical network environments, such as networks with different wavelength conversion capability (no converters, converters everywhere, converters somewhere, etc.). Moreover, the low computational effort required by heuristic optimization makes our tool applicable to fairly complex network topologies. On the contrary, exact methods that return the precise optimal solution become impractical for realistic size networks. Though it is based on efficient integer linear programing (ILP) techniques, the optimal design of a survivable WDM network is an NP-hard problem that requires a number of operations increasing roughly exponentially with the network dimensions.

We tested our tool by optimizing the NSF-Net, a well-known case-study network (Fig. 13); we assumed a static traffic matrix derived from real

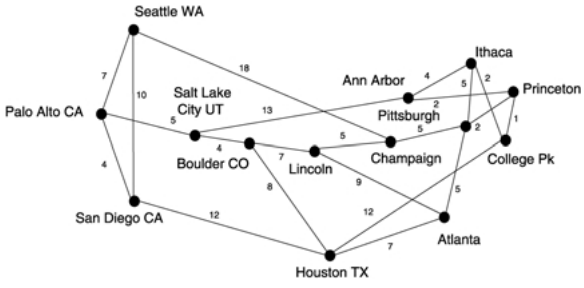


Fig. 13. NSF-Net, used as a case-study network for a heuristic design and optimization tool. Links are labeled with their normalized length.

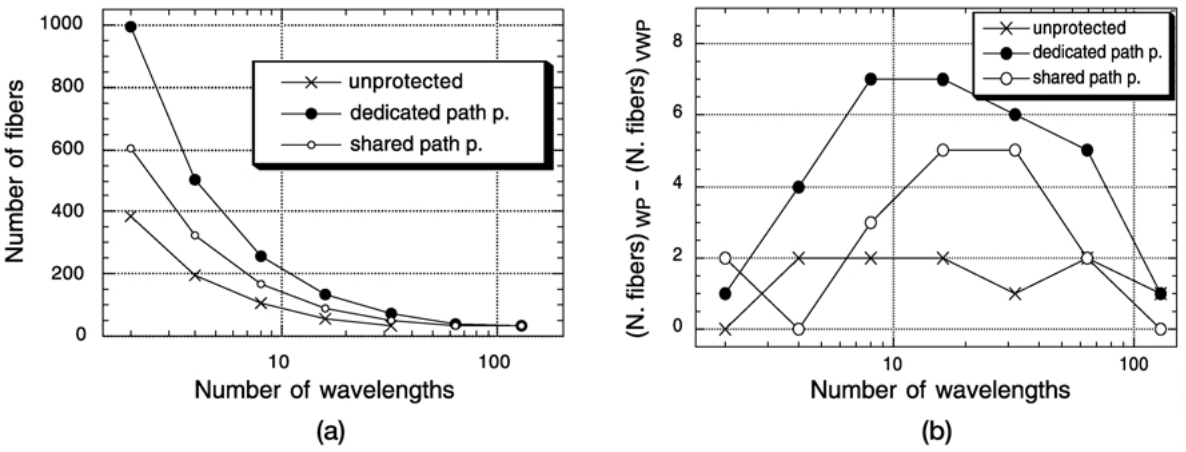


Fig. 14. Heuristic optimization of the NSF-Net with different path-protection implementations: (a) total number of fibers in the VWP scenario; (b) advantages of wavelength conversion on the total number of fibers.

measurements. Both physical topology and traffic data were taken from Miyao and Saito [6].

Fig. 14a shows the performance of our heuristic algorithm when applied to the NSF-Net adopting various path-protection cases. The curves represent the total number of fibers in the optimized network necessary to route all the requested connections while guaranteeing full survivability (the non-protected case is also reported for comparison); this parameter is plotted as a function of the maximum number of wavelengths per fiber. By comparison of the unprotected case to the curve obtained when dedicated path-protection is adopted for all the connections, it can be noticed that this scheme, when applied to a mesh network, requires more than 100% extra-fibers. The intermediate curve indicates instead that shared path-protection on the mesh topology has a good efficiency, requiring just roughly 50% extra-fibers. The network is assumed to have full wavelength-conversion capability: this condition is called virtual wavelength path (VWP) scenario, to distinguish it from the wavelength path (WP) scenario, in which the network has no wavelength conversion capability.

Fig. 14b shows the advantages that the adoption of wavelength converters implies in terms of the difference between the total number of fibers in the WP and VWP scenarios. The three curves are referred to the unprotected, dedicated path-protection and shared path protection cases, respectively. The plotted values indicate that converters are more useful when protection has to be guaranteed, compared to the unprotected case. However, it can be noticed that the conversion advantage in general is modest, as expected in the case of a WDM network optimized under static traffic conditions.

The results we obtained were in good accordance with Miyao and Saito [6] and other works published in literature. Moreover, Table 1 allows us to compare the results of our heuristic approach to the optimal

Table 1. Minimization of the total number of fibers M performed with ILP and heuristic techniques (NSF-Net, VWP network scenario).

	Unprotected			Dedicated path protection		
W	M_{ILP}	M_{Heu}	$\Delta\%$	M_{ILP}	M_{Heu}	$\Delta\%$
2	374	382	2.14	983	995	1.22
4	189	199	5.30	492	505	2.64
8	96	106	10.42	248	256	3.23
16	51	58	13.73	125	134	7.20
32	30	35	16.67	65	73	12.31
64	—	24	—	—	41	—

solutions of the same problems found (with a much larger computational time) by ILP (details on our ILP approach can be found in Maier et al. [44]). Also this comparison confirmed that our heuristic algorithms are able to find quasi-optimal solutions, as the mean difference $\Delta\%$ between optima and sub-optima is below 10% and below 6% in the unprotected and path-dedicated protection cases respectively. Missing ILP data are due to the impossibility to reach convergence of ILP because of memory overflow.

9 Conclusions

This work is intended as an introduction to survivability of WDM optical networks. After presenting some general classification criteria, we reviewed the main protection and restoration strategies that can be adopted for the WDM network. We outlined the simplest and fastest schemes more promising for the next future necessary to recover the failed connections. We have also discussed a heuristic method we proposed to optimize a resilient WDM mesh network in a static environment when dedicated or shared path protection is implemented. We presented some results of this method concerning a case-study and we took the opportunity to compare different protection techniques in terms of the amount of extra spare capacity they require.

Notes

1. The term ''link (node) disjoint paths'' has entered the common usage in literature, to indicate the condition of preventing physical resource sharing (see Refs. [1,23], etc.). The term disjoint is not entirely appropriate, since in probability mathematics it refers to events not happening at the same time: independent should be use instead. We will, however, follow the common convention in this paper.
2. Care must be taken when imposing physical route diversity. A network topology simply representing fibers or cables as separated arcs may be misleading. Strand et al. [16] discusses cases in which distinct arcs of the physical topology share the same infrastructure (e.g., two different fiber cables crossing a river on the same bridge).

References

[1] T. E. Stern, K. Bala, Multiwavelength optical networks—a layered approach (Addison Wesley Longman, Inc., 1999).

[2] O. Gerstel, R. Ramaswami, Optical layer survivability: a service perspective, IEEE Communications Magazine, vol. 3, no. 38, (March 2000), pp. 104–113.

[3] G. Maier, A. Pattavina, S. De Patre, M. Martinelli, Tecniche di protezione per la rete WDM, in: Proc. of Reti ottiche di nuova generazione: architetture e tecnologie, IEEE-LEOS Italian Chapter Workshop (in Italian) (2001), pp. 37–45.

[4] ITU-T Recommendation G.872, Architecture of Optical Transport network (OTN), (1999).

[5] ITU-T Recommendation G.709, Network node interface for the optical transport network (OTN), (2001).

[6] Y. Miyao, H. Saito, Optimal design and evaluation of survivable WDM transport network, IEEE J. on Sel. Areas Comm., vol. 16, (vol. 7, Sept. 1998), pp. 1190–1198.

[7] J. Armitage, O. Crochat, J.-Y. Le Boudec, Design of a survivable WDM photonics network, in: Proc. IEEE INFOCOM'97, (Kobe, Japan, April 1997), vol. 1, pp. 244–252.

[8] C. Huitema, Routing in the Internet, Second edn (Prentice Hall PTR, 2000).

[9] ITU-T Recommendations G.774, Synchronous Digital Hierarchy (SDH), (2001).

[10] G. Mohan, C. S. R. Murthy, Lightpath restoration in WDM optical networks, IEEE Network Magazine, vol. 6, no. 14, (Nov/Dec. 2000), pp. 24–32.

[11] P. Gadiraju, H. T. Mouftah, Channel protection in WDM mesh networks, in: Proc. 2001 IEEE Workshop on High Performance Switching and Routing, (2001), pp. 26–30.

[12] S. Ramamurthy, B. Mukherjee, Survivable WDM mesh networks, Part I-Protection, in: Proc. IEEE INFOCOM'99, (New York, NY, March 1999), vol. 2, pp. 744–751.

[13] S. Ramamurthy, B. Mukherjee, Survivable WDM mesh networks, Part II-Restoration, in: Proc. IEEE ICC'99, (Vancouver, Canada, June 1999), vol. 3, pp. 2023–2030.

[14] W. D. Grover, High availability path design in ring-based optical networks, IEEE/ACM Transactions on Networking, vol. 4, no. 7, (Oct. 1999), pp. 558–574.

[15] R. Ramamurthy, et al., Capacity performance of dynamic provisioning in optical networks, IEEE Journal Lightwave Technology, vol. 19, no. 1, (Jan. 2001).

[16] J. Strand, A. L. Chiu, R. Tkach, Issues for routing in the optical layer, IEEE Communications Magazine, vol. 2, no. 39, (Feb. 2001), pp. 81–87.

[17] I. P. Kaminow, T. L. Koch, Optical Fiber Telecommunications IIIA (Academic Press, Inc., 1997).

[18] R. Doverspike, J. Yates, Challenges for MPLS in optical network restoration, IEEE Communic. Magazine, vol. 2, no. 39, (Feb. 2001), pp. 89–96.

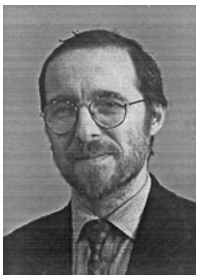
[19] S. Yan, J. Jue, A heuristic routing algorithm for shared protection in connection-oriented networs, in: SPIE Proc. OptiComm 2001, vol. 4599, Denver, CO (August 2001), pp. 142–152.

[20] R. J. Gibbens, S. Baroni, P. Bayvel, K. Korotky, Analysis and design of resilient multifiber wavelength-routed optical transport networks, IEEE Journal of Lightwave Technology, vol. 17, no. 5, (May 1999), pp. 743–758.

[21] V. Anand, C. Qiao, Static versus dynamic establishment paths in WDM networks, Part I, in: Proceedings of IEEE ICC'00, (New Orleans, LA, June 2000), vol. 1, pp. 198–204.

[22] S. Baroni, Routing and Wavelength Allocation in WDM Optical Networks, Ph.D. thesis, Department of Electronic and Electrical Engineering, UCL London.
[23] R. Bhandari, R. Survivable networks—algorithms for diverse routing (Kluwer Academic Publishers, Inc., 1999).
[24] J. Spath, H. Weißschuh, Investigation of protection strategies: problem complexity and specifics aspects for WDM networks, in: Proc. NOC'99, (Delft, Netherlands, June 1999), vol. 2, pp. 58–74.
[25] ITU-T Recommendation G.798, Characteristics of OTN Hierarchy Equipment Functional Blocks (under discussion), (1999).
[26] S. S. Lumetta, M. Medard, Toward a deeper understanding of link restoration algorithms for mesh networks, in: Proc. IEEE INFOCOM'01 (Anchorage, AL, April 2001), vol. 1, pp. 367–375.
[27] S. Desbrulais, V. Lemaire, L. Le Gall, C. Mathieu, Association of submarine cable reliability and network protection for very high availability transoceanic transmission networks, in: SPIE Proc. Reliability of optical fibers and optical fiber systems, vol. CR73, (1999), pp. 255–283.
[28] G. Ellinas, A. G. Hailermariam, T. E. Stern, Protection cycles in mesh WDM networks, IEEE Journal on Selected Areas in Comm., vol. 18, no. 10, (Oct. 2000), pp. 1924–1937.
[29] O. J. Wasem, An algorithm for designing rings for survivable fiber networks, IEEE Trans. Rel., vol. 3, (1991), pp. 57.5.1–57.5.7.
[30] A. Fumagalli, L. Valcarenghi, Fast optimization of survivable WDM mesh networks based on multiple self-healing rings, in: Proc. SPIE Conference on All-Optical Networking, vol. 3843, (1999), pp. 44–55.
[31] F. Jaeger, A survey of the double cycle cover conjecture, Cycles in Graphs, Annals of Discrete Mathematics, vol. 115, (1985).
[32] W. D. Grover, D. Stamatelakis, Cycle-oriented distributed preconfiguration: Ring-like speed with mesh-like capacity for self-planning network reconfiguration, in: Proc. IEEE ICC'98 (Atlanta, GA, June 1998), vol. 1, pp. 537–543.
[33] M. Medard, S. G. Finn, R. A. Barry, WDM loop-back recovery in mesh networks, in: Proc. IEEE INFOCOM'99 (New York, NY, March 1999), vol. 2, pp. 752–759.
[34] S. S. Lumetta, M. Medard, Y. C. Tseng, Capacity versus robustness: a tradeoff for link restoration in mesh networks, IEEE Journ. of Lightwave Techn., vol. 18, no. 12, (Dec. 2000), pp. 1765–1775.
[35] E. E. Lewis, Introduction to reliability engineering (John Wiley & Sons, Inc., 1987).
[36] A. Antonopoulos, J. J. O'Reilly, P. Lane, A framework for the availability assessment of SDH transport networks, in: Proc second IEEE Symposium on Computers and Communications, (1997), pp. 666–670.
[37] M. To, P. Neusy, Unavailability analysis of long-haul networks, IEEE Journal on Selected Areas in Comm., vol. 1, no. 12, (Dec. 1994), pp. 100–109.
[38] O. Gerstel, G. Sasaki, Quality of Protection (QoP): a quantitative unifying paradigm to protection service grades, in: SPIE Proc. OptiComm 2001, vol. 4599, (2001a), pp. 12–23.
[39] A. Fumagalli, M. Tacca, Optimal design of optical ring networks with differentiated reliability (DiR), in: Proc. Int. Workshop on QoS in multiservice IP networks (2001b).
[40] A. Fumagalli, M. Tacca, Differentiated reliability (DiR) in WDM rings without wavelength converters, in: Proc. IEEE ICC 2001 (Helsinki, Finland, June 2001), vol. 9, pp. 2887–2891.
[41] G. Maier, A. Pattavina, L. Roberti, T. Chich, Static-lightpath design by heuristic methods in multifiber WDM networks, in: Proc. Opticomm 2000 SPIE Conf., Richardson, TX (Oct. 2000), pp. 64–75.
[42] G. Maier, A. Pattavina, L. Roberti, T. Chich, A heuristic approach for the design of static multifiber WDM networks: principles and applications, Optical Network Magazine, accepted for publication.
[43] A. Dacomo, S. De Patre, G. Maier, A. Pattavina, M. Martinelli, Design of static resilient WDM mesh networks with multiple heuristic criteria, in: Proc. IEEE INFOCOM'02 (New York, NY, April 2002), accepted for publication.
[44] G. Maier, A. Pattavina, M. Tornatore, WDM network optimization by ILP based on source formulation, in: Proc. IEEE INFOCOM'02 (New York, NY, April 2002), accepted for publication.

Guido Maier received his Laurea degree in Electronic Engineering at Politecnico di Milano, Italy, in 1995 and his Ph.D. degree in Telecommunication Engineering at the same university in 1999. He is researcher at CoreCom, where he has the position of Head of the Optical Network Laboratory. His main areas of interest are optical network modeling, design and optimization and photonic ATM and WDM switching architectures. He has been author of more than 20 papers in the area of optical networks published in international journals and conference proceedings.



Achille Pattavina received the degree in Electronic Engineering (Dr. Eng. degree) from the University ''La Sapienza'' of Rome, Italy, in 1977. He was with the same university until 1991 when he moved to the ''Politecnico di Milano'', Milan, Italy, where he is now full Professor. In the last ten years he has been involved in researches on the design and performance evaluation of fast packet switching architectures for broadband networks. He has been author of more than 80 papers in the area of communications networks published in international journals and conference proceedings. He has been author of the book *Switching Theory, Architectures and Performance in Broadband ATM Networks* (John Wiley & Sons). He has been a Co-Guest Editor of Special Issues on ATM Switching Systems for B-ISDN for the *Journal on Selected Areas in Communications* (IEEE) and the *Transactions on Communications* (IEICE). He has been Editor for *Switching Architecture Performance of the IEEE Transactions on*

Communications since 1994 and Managing Editor of the *European Transactions on Telecommunications* since 1997. He is a Senior Member of the IEEE Communications Society. His current research interests are in the area of optical networks and wireless networks.

Simone De Patre was born in Atri (Teramo), Italy, in 1974. He received his degree in Telecommunications Engineering (Laurea in Ingegneria delle Telecomunicazioni) from the Politecnico di Milano, Italy, in 2001. From the graduation he joined CoreCom at the Optical Networks Lab. His main research area is planning and optimization of WDM networks and WDM-layer survivability.

Mario Martinelli was born in Mantova in 1952. He received the Laurea Degree in Nuclear-Electronics Engineering from Politecnico di Milano, Italy in 1976. In 1978 he joined the Quantum Electronics Department of CISE Advanced Technologies, Milan, Italy. In 1991 he has been appointed Associate Professor of Optical Communications by Politecnico di Milano, where he activated the Italian first related course, and in 1993 founded the Photonic Lab at the Electronics and Information Department. Since 1995 he has been Director of CoreCom, a research consortium between Politecnico di Milano and Pirelli Cables, whose main area of activity is in the field of optical processing and photonic switching.