Present Issues & Challenges in Survivable WDM Optical Mesh Networks

Amitava Mukherjee

School of Computer Science and Engineering
University of New South Wales
Sydney 2052, Australia
amitavam@cse.unsw.edu.au

Asidhara Lahiri

IBM Global Services
Salt Lake, Calcutta 700 091, India
asidhara.lahiri@in.ibm.com

Debashis Saha

MIS & Computer Science Group
Indian Institute of Management (IIM) Calcutta
Joka, Kolkata 700 104, India
ds@iimcal.ac.in

January 2004

UNSW-CSE-TR-0405

Abstract

The design of survivable optical networks is obtained by exploiting *restoration* and/or *protection* schemes in the WDM and IP layers. In this paper, we discuss the different restoration and protection techniques available at the IP and WDM layers. Upon network failure, a restoration scheme dynamically looks for backup paths of spare capacity in the network. A protection scheme reserves, in advance, dedicated backup paths and wavelengths in the network. The former scheme is commonly available at higher layers (e.g., the IP layer). The latter scheme is commonly used at the transport (e.g., WDM) layer. The WDM predefined protection scheme is broadly divided into link-based and path-based protection. Predesigned protection schemes are so far the most studied for WDM networks. Because of the multichannel traffic, the design algorithms used in a WDM network are more complex than those used in non-WDM systems. The survivability schemes available at the network layer, such as IP (IP/MPLS), have the capability to recover multiple faults and operate at small traffic granularity. A primary concern for this approach is the slow convergence and response time of IP link failure detection and routing algorithms that renders them unsuitable for use with critical or premium services. This paper discusses the recent works on the restoration and/or protection schemes in the WDM and IP layers and few future research issues.

I. Introduction

The today's telecommunication networks can provide fast and high quality services to end users with the integration of computer and communication technologies and the fast maturation of fiber optic communication techniques. This service type is right from voice to different types of multimedia services. Internet traffic will grow between 50 and 300 percent yearly. The aggregate bandwidth required in the backbone networks will shortly surpass hundreds of terabits per second in the near future. In the backbone networks, optical communication network will play a key role to provide diverse array of services to end-users. As more and more mission-critical business users are involved, the 99% up-time of services for those users is a must. As such, how to provide uninterrupted services to these users, and reduce the loss of service to a minimum if interruption is inevitable, becomes a critical design issue; that is, *survivability* must be considered in designing optical communication network. The survivability of a communication network refers to a network's capability to provide uninterrupted continuous service to users in the presence of node/link failures.

I (a) Protection and Restoration Schemes for IP/WDM layers

Optical transport networks are compatible with existing transport and switching solutions, such as synchronous digital hierarchy (SDH)/synchronous optical network (SONET), asynchronous transfer mode (ATM), and Internet Protocol (IP). Optical fiber has become the dominant transport medium in the backbone networks because of its advantages in capacity, reliability, scalability and cost. An attractive feature of optical fiber is its extremely large capacity, on the order of a few terabits per second. A new multiplexing technique such as wave-length-division multiplexing (WDM) divides this large bandwidth of a fiber into many nonoverlapping wavelengths, called WDM channels or *ligthpaths*. An optical crossconnect (OXC) can switch the optical signal on a WDM channel from an input port to an output port without undergoing signal to any optoelectronic conversion. If an OXC is equipped with wavelength converters, then the OXC can also change the wavelength of an incoming optical signal as it passes through the switch. A lightpath is a point-to-point path of light that may be established between node pair (e.g., IP routers) that may not be physically adjacent (i.e., not connected by a single fiber hop), thus increasing the logical network connectivity. Using OXCs at intermediate nodes and via appropriate routing and wavelength assignment, a lightpath can create virtual (or logical) neighbors out of nodes that are geographically far apart in the network; thus, a set of lightpaths embeds a virtual (or logical) topology on the network. In the virtual topology, a lightpath carries not only the direct traffic between the nodes it interconnects but also traffic between nodes that are not directly connected in the virtual topology by employing the multihop approach, namely, by using electronic packet switching at the intermediate nodes in the virtual topology. IP routers, leading to an IP-over-WDM, can provide this electronic packet-switching functionality.

The design of survivable optical networks is obtained by exploiting *restoration* and/or *protection* schemes in the WDM and IP layers. In this paper, we discuss the different restoration and protection techniques available at the IP and WDM layers. Upon network failure, a restoration scheme dynamically looks for backup paths of spare capacity in the network. A protection scheme reserves, in advance, dedicated backup paths and wavelengths in the network. The former scheme is commonly available at higher layers (e.g., the IP layer). The latter scheme is commonly used at the transport (e.g., WDM) layer.

The basic types of network failures generally considered are link and node failure. Link failure usually occurs because of cable cuts; node failure is due to equipment failure at network nodes. Besides node and link failures, which are common failure situations in any communication network, channel failure is also possible in WDM optical networks. A channel failure is usually caused by the failure of transmitting and/or receiving equipment operating on that channel (wavelength). Initial work on survivability in WDM optical networks has focused mostly on the recovery from a single link or node failure. *Link-based protection schemes* can be further classified as dedicated or shared link protection. In WDM path protection, during the call setup of a lightpath, a backup lightpath is set up as well so that in the event of a fiber failure, all the traffic on the primary lightpath can be diverted to the backup lightpath. Path protection comes in two flavors that are shared-path protection and dedicated-path protection. *Restoration schemes*, where backup resources are deployed dynamically only when failures occur.

Survivability using dynamic restoration methods in WDM optical networks has received much less attention than predesigned protection schemes. In spite of this we review on any existing work dynamic protection schemes available for WDM networks.

The next-generation optical Internet can be viewed as a collection of autonomous networks, which may be considered as of different sizes from a small corporate network to a large backbone network. Each autonomous network consists of a set of routers that belong to the same administrative domain. Routers within an autonomous network exchange routing information by employing an interior gateway protocol (IGP). By using an IGP, an autonomous network can combat a link failure—i.e., when a link fails along a primary path between two nodes/routers in the autonomous network, the IGP can dynamically find an alternate path between the two nodes. IP/WDM networking architecture is shifted from a static point-to-point architecture toward more dynamic reconfigurable and switched architectures. This shift is away from static planned resource allocation and service provisioning, toward dynamic on-demand resource allocation and service provisioning. This shift is also away from centralized management and off-line optimization strategies toward distributed control and on-line incremental heuristics in network and traffic management. We present a survey of available protection/restoration schemes for IP layer that may be used in networks with arbitrary (mesh) topology of IP/WDM architecture.

I (b) Organization of the paper

The Section I is an Introduction section. The section II describes the survivability in WDM networks. The Section III focuses on the survivability schemes in IP layer. The Sections II and III have several subsections. The Section IV summaries the recent studies while Section V discusses the future research issues.

II. Survivability in WDM Networks

WDM systems being widely used in the backbone network today as these technologies divide the vast transmission bandwidth available on a fiber into several nonoverlapping wavelength channels and enable data transmission over these channels simultaneously. The deployment of optical switches and all optical components introduces a network layer that is called optical layer or WDM layer in the layered topology. Here, a message is transmitted between two nodes using a lightpath without requiring any electro-optical conversion and buffering at the intermediate nodes. This is known as *wavelength routin*g. A wavelength and a physical path uniquely identify a lightpath. At the optical layer, lightpaths are established between a subset of node pairs, forming a *virtual topolog*y. The optical layer is formed between the lower physical media layer and the higher circuit layer in the layered network architecture. This layer is protocol-transparent, and can support different kinds of services and protocols at the higher layer such as synchronous optical network (SONET)/synchronous digital hierarchy (SDH), asynchronous transfer mode (ATM), and Internet protocol (IP). The higher circuit layer is also known as the c*lient layer* because the optical layer serves it. According to the layered structure of a network, survivability can be offered at the WDM layer or higher layers. The higher-layer services, such as IP and ATM, actually have their own protection/restoration mechanisms, while some may not have recovery mechanisms incorporated in the protocols. Under this situation, the WDM layer should be able to offer them. However, WDM layer survivability cannot protect against failures at higher layers, and some survivability must be provided at higher client layers as well. Incorporating survivability mechanisms at multiple layers leads to the issues of assigning functions to each layer and coordinating the layers in effecting recovery from a fault.

In a WDM network, the failure of a fiber link can cause the failure of all lightpaths that traverse the failed link. SONET operating over WDM systems has its own survivability schemes that have the protection times on the order of milliseconds and the higher layers, IP/ATM, have their own fail-over procedures to recover from link failures. An IP network recovers from link failures by rerouting data packets around the failed link and the recovery time in this higher layer is still in the order of seconds. The survivability schemes differ in their assumption about the functionality of cross-connects, traffic demand, performance metric, and network control. The lightpath that carries traffic during normal operation is known as the *primary lightpat*h. When a primary lightpath fails, the traffic is rerouted over a new lightpath known as the *backup lightpat*h. The traffic demand can be two different types either static or dynamic. In static traffic demand, the set of demands (or connection requests) is given a priori. In a dynamic traffic environment, the demands arrive at a network one by one in a random manner.

The survivability scheme may assume either centralized or distributed control. The distributed control is preferred over centralized control for large backbone WDM networks. Several control messages are exchanged between nodes in a distributed control protocol. Also two simultaneous attempts to find paths can create conflict for the possibility of reservation for these paths. The survivability schemes can be classified as illustrated in Fig. 1. They are broadly classified as protection and restoration schemes. The restoration scheme is the simplest way of recovering from failures. In this method, when an existing lightpath fails, a search is initiated to find a new lightpath, which does not use the failed components. This has an advantage of low overhead in the absence of failures. However, this does not guarantee successful recovery, since the attempt to establish a new lightpath may fail due to resource shortage at the time of failure recovery. Also, in case of distributed implementation, contention among simultaneous recovery attempts for different failed lightpaths may require several retries to succeed, resulting in increased network traffic and restoration time. In a protection scheme, backup lightpaths are identified, and resources are reserved along the backup lightpaths at the time of establishing the primary light-path itself. In doing so, this method yields a 100 percent survivability guarantee. This metric refers to the guarantee that a failed path finds its backup path readily available upon failure. The backup lightpath takes over the role of the primary lightpath when it fails. Since the backup lightpath is established before a failure actually occurs, one can use it immediately upon occurrence of a failure on the primary, without invoking the time-consuming connection reestablishment process. Hence, the restoration time of a protection scheme is much lower, leading to fast recovery. The protection technique uses preassigned capacity to ensure survivability, while the restoration technique reroutes the affected traffic after failure occurrence by using available capacity. A protection or restoration method is either *link-based* or *path-based*. The link-based method employs *local detourin*g, while the path-based method employs *end-to-end detourin*g. The link-based method reroutes traffic around the failed component. When a link fails, a new path is selected between the end nodes of the failed link. This path, along with the working segment of the primary path, will be used as the backup path. The choice of backup paths is limited; also, the backup paths are usually longer. Also, in wavelength selective networks, the backup path must necessarily use the same wavelength as the primary path since its working segment is retained. Sometimes protection and restoration schemes are called proactive and reactive methods respectively. In link protection/restoration all the connections that traverse the failed link are rerouted around that link. In link protection, back-up paths and wavelength are reversed around each link of primary path. In link restoration, the end-nodes of the failed link dynamically find a route around the link for each wavelength that traverses the link.

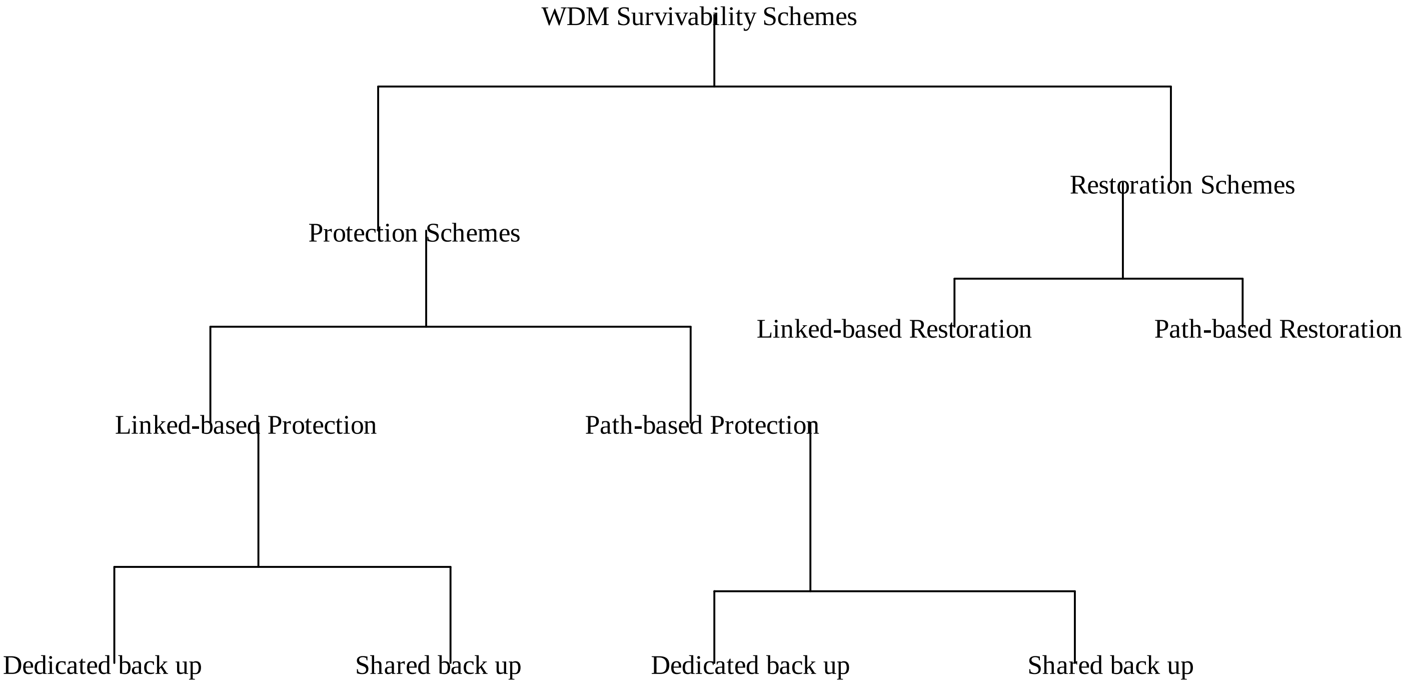

Figure 1: WDM Survivable Schemes

The procedure to set up restoration paths are either *dedicated* to or *shared* with individual source-destination (s-d) pair whose working paths fail by network component failures, which occur independently. In the dedicated case a restoration path has been established for each working path. Switching from the working path to the corresponding restoration path is then simply performed by exchanging signaling messages between the s–d pair over the control channel accommodated by the restoration path. In the shared case each restoration path is set up with a signaling procedure only if the corresponding working path fails in the following way. We assume that each link accommodates a signaling channel to connect a pair of controllers in adjacent core nodes terminating the link. As soon as an s–d pair receives an alarm indication signal for its working path, one node of the s–d pair generates a signaling message to set up the corresponding restoration path. This message is transferred on the signaling channel and processed by each node along its route to reserve the wavelengths in each link on the route. When the s–d pair succeeds in setting up the restoration path, the pair switches demand from the failing working path to its restoration path.

II (a) WDM-layer Protection

This section will give us different approaches to survive single-link failure in WDM-layer. In point-to-point WDM systems, 1 + 1, 1:1, and 1:N optical protection are used for automatic protection switching (APS) that is happened in the optical domain. In WDM systems, due to the availability of multiple wavelengths in a single fiber, protection methods can be more flexible. Either a whole fiber or only some wavelengths in the fiber can be dedicated to protection purposes. Of course, the multiplicity in wavelengths also makes the protection schemes more complicated. As WDM system deployment advances beyond the upgrading of existing non-WDM systems, mesh topologies using OXCs are likely to emerge. In such situations, protection can be provided by the OXCs. WDM self-healing ring (SHR) architectures operate along the same lines as SONET SHRs. Researchers have recently started studying WDM mesh network survivability. Most of the studies so far have considered only single-link failures. The fault detection/localization is an important issue in the WDM-layer survivability and is a prerequisite to error recovery process. Using frame overhead bytes and electronic monitoring facilities carry out this localization error detection in SONET. As the similar types of techniques are not maturing in the optical layer, few supervisory techniques on optical channels are used for this purpose. Instead, the electronic monitoring techniques at all nodes in the network are used intermittingly. Although electronic monitoring techniques remove full transparency, the electronic processing is done at bit level. Hence, protocol transparency can still be provided. At present the fault localization cannot be done effectively as full transparency within the optical core is required. When a lightpath fails, the network edge routers may be able to detect the fault, but the exact location of the fault cannot be determined. Fault recovery in such situations is not clearly understood at this time. For the sake of the simplicity of our review, the fault detection/ localization can be assumed to happen and focused on WDM-layer protection. To be sure, however, the failure of even a single link in a WDM system causes the failure of several channels simultaneously, a much more serious situation than in non-WDM systems. Furthermore, fiber cuts are among the most common failure scenarios.

II (b) Protection from Single-Link Failures

The WDM predefined protection scheme is broadly divided into link-based and path-based protection. Predesigned protection schemes are so far the most studied for WDM networks. Because of the multichannel traffic, the design algorithms used in a WDM network are more complex than those used in non-WDM systems.

Path Protection: The path protection for each s-d pair during call set-up refers to the reservation of a protection path and wavelength on an end-to-end basis for each working wavelength path and link failure. When link fails, the s-d nodes of each failure connection are shifted to the predesigned wavelength path. The path-based protection needs a mechanism to notify the affected connection end nodes of the failure and should be disjoint with the affected link. The path-based protection technique can be dedicated or shared.

In *dedicated path protectio*n (also called 1+1 protection), the backup wavelength on the links of a protection path is reserved for a specific working connection. This implies that two overlapping protection paths must use different wavelengths even if the working paths do not overlap. The backup wavelength reserved on the links of the backup path are dedicated to that call, and are not shared with other back paths. Dedicated path protection requires a large amount of extra capacity for protection purposes, and when there is no failure, the protection resources are kept idle. It is able to provide recovery from not only single-link failures, but also *some* multilink failures.

Shared path protection allows the use of the same wavelength on a link for two different protection paths if the corresponding working paths are link-disjoint. As a result, backup channels are multiplexed among different failure scenarios and therefore the shared-pat protection is more capacity efficient when compared with dedicated-path protection.

Only one wavelength on this link has to be reserved for protection, as opposed to two for dedicated path protection.

Link Protection: In the link-based protection, a protection path is reserved for each link, and when the link fails, traffic is rerouted (looped back) around the failed link. In a WDM network, each link carries many channels, and the failure of a single link causes the failure of all the channels on the link. In link protection, during call setup, backup paths and wavelengths are reversed around each link of the primary path. The protection wavelength paths used for different working wavelengths on the same link may use different paths and/or different wavelengths.

Shared link protection allows different protection paths to share a wavelength on the overlapping portion if the corresponding working channels are on different links. Shared link protection utilizes capacity more efficiently than dedicated link protection, and can provide 100 percent recovery from single-link failures. *Dedicated link protection* means that a protection wavelength path is dedicated to a working channel on a particular link. Therefore, if the protection paths for (some wavelengths on) two different links overlap, different wavelengths must be assigned to the protection path on the overlapping portion even if the working wavelengths on the two links are the same.

II (c) Dynamic Restoration

The *dynamic restoration* refers the discovery of excess capacity dynamically in the WDM network to restore the affected services; that is, the resources used for recovery are not reserved during call setup between s-d nodes, but are chosen from available resources such as fibers, wavelengths, switches, and so on when the failure occurs. This is typically more efficient than pre-designed protection from the viewpoint of resource utilization. On the other hand, the restoration time is usually longer, and 100 percent service recovery cannot be guaranteed because sufficient spare capacity may not be available at the time of failure. The dynamic restoration schemes in WDM layer can again be divided into link- and path- restoration schemes. In the *path restoration* scheme, the s-d pair of each connection that traverses a failed link dynamically discovers a back-up path for end-to-end basis after the link fails. In the *link restoration*, the end-nodes of the failed link discover dynamically a path around the link for each wavelength that traverses the link.

In the following section, we will highlight the different schemes used by different researchers for single link failure recovery.

II (d) Recent Research on WDM Survival Schemes

In [1], the planning is done in two steps: first, routing and working capacity assignment are optimized and second, the spare capacity is assigned. The outcome is a dimensioned network with an optimized number of working and spare fibers (or channels) on each link and the most appropriate working paths on which to route the demand and restoration routes on which to recover from a single link failure. Protection strategies are, in the first instance, considered for point-to-point links and in ring structures. In meshed networks, rerouting strategies can be applied more efficiently; spare capacity is not really dedicated to protect working entities, but the spare resources are shared among several working entities. In this paper three rerouting strategies are considered for single link failures. Two optimization techniques: integer linear programming (ILP) and simulated annealing (SA) are used to optimize the routing in the network and allocate of working and spare fiber resources, and minimize the total network cost. The planning approach described in this paper has as its starting point the location of the optical crossconnects, a set of candidate links between these crossconnects, and the demand between each pair of nodes, expressed in the number of wavelength channels.

In [2], the proposed algorithm presents the disjoint alternate path (DAP) algorithm, an algorithm using tabu search for placing CC's in order to maximize design protection while trying to enforce link capacity constraints. This will try to place a proposed virtual topology onto the physical one. It will give a list of CC's (Clear Channel) that may not be protected in case of failure. The virtual topology may then be changed to include this feedback. The global algorithm will be run until a virtual topology that satisfies the design protection criterion is found. The difference is that the routes of a CC and its associated alternate path must be node-disjoint (instead of link-disjoint for link failure protection). The only achievable protection is against failure propagation for the remaining CC's. The virtual topology consists of a graph representing all the CC's that are present in the network. It is the only view of the network available to the higher layer switches. The physical topology is the real network, composed of optical links and photonic nodes. The mapping between these two topologies (i.e., the assignment of the CC's within this network) is performed by the design algorithm. Physical protection provides a reliable transport capability to the higher level networks. For physical protection, it is the photonic network that is responsible for performing the necessary reconfiguration following a failure. The algorithm for design protection uses the physical and virtual topologies, which are supplied to it.

This paper [3] formulates design problems to optimally select combinations of a working path and the corresponding restoration path, which is independent of failure locations. By using these restoration paths, each s–d pair can set up a restoration path as soon as the s–d pair detects the corresponding working path failing due to a span or node failure in any location. In such a restoration process, optical cross-connect (OXC) systems play an important role of setting up restoration paths. It is therefore significant to optimize the total facility cost including cross-connection cost as well as transmission cost. Since the cost structure for WDM transmission systems and OXC systems will vary as these technologies advance, the design problems for several values of a cost parameter with respect to both systems have been solved. The impact of the cost parameter on several items such as total fiber length, the total number of OXC's, and total optical channel length has then been evaluated. The relationship between optical path and optical channel in this paper is equivalent to that between virtual path and virtual channel in ATM networks. This paper used a demand matrix and assumed wavelength translation in each OXC, nonrelease of wavelengths assigned to working paths, which fail, and 100% restoration against any single span failure. A set of candidates for combinations of a working path and its corresponding restoration path for each s–d pair has been generated by all permutations of first three successively shortest span-disjoint paths for each s–d pair.

In [4], they have studied the relationship between failure localization and the properties of link restoration algorithms. They have employed a quantitative measure of a network's ability to recover from two-link failures, i.e., failures in which two independent links in a network graph fail concurrently. Although multiple link failures are less likely than single failures, a two-link failure model allows considering issues of failure localization that cannot be addressed through models that assume only single failures. Based on the relationship between algorithmic properties and restoration failures, a failure classification hierarchy is prepared. Finally, they have applied this classification scheme to three networks from the literature and discuss the results in terms of their importance for link restoration algorithms. They have found that the topological constraints on restoration paths required by algorithms that embed rings within mesh networks result in significant degradation of failure localization. The pre-selection of restoration paths (as opposed to selection at the time of failure) also has a negative impact, although it is not as significant as the topological effect. Algorithms that make use of the mesh topology and dynamically route around existing failures come close to an inherent limit imposed by the complexity of additional algorithmic advances. In this paper, they have limited discussion to algorithms that successfully recover from all one-link failures, thus we assume that recovery from the first failure is always successful. None of the fibers in a failed network link remain usable; all primary and backup arcs through that link are broken.

This paper [4] deals with the problem of routing logical links (lightpaths) on a physical network topology in such a way that the logical topology remains connected in the event of single physical link failures (e.g., fiber cut). In this paper they have addressed the problem of routing the lightpaths of a logical topology on a given physical topology so that the logical topology can withstand a physical link failure. They have used the ILP formulation to find survivable routings for a variety of network topologies. The results show that this new formulation is able to offer a degree of protection when compared to shortest path routing. This added protection, of course, comes at the expense of additional network resources. They attempted to embed all possible 6 and 10 node logical rings on the 6 and 10 nodes physical rings and used the ring ILP to determine survivable routings for all of these topologies.

In [5], they have considered the routing and wavelength assignment problem in survivable WDM transport network without wavelength conversion and assumed the single-link failure and a path protection scheme in optical layer. When a physical network and a set of working paths are given, the problem is to select a link-disjoint protection path for each working path and assign a wavelength for each working and protection path. The predetermined protection path for each working path is independent to the location of the failure. In other words, a working path and the corresponding protection path are link-disjoint. They have given an integer programming formulation of the problem and proposed an algorithm to solve it.

This paper [6] considers the problem of dynamically establishing dependable connections (D-connections) with specified failure restoration guarantees in wavelength-routed wavelength-division multiplexed (WDM) networks. They have used a proactive approach to fault tolerance wherein a D-connection is identified with the establishment of a primary and a backup lightpath at the time of honoring the connection request. The algorithms are developed to select routes and wavelengths to establish D-connections with specified failure restoration guarantees. They consider the single-link failure model in their study and use a technique called primary-backup multiplexing for dynamically establishing dependable connections with specified failure restoration guarantees combining the advantages of both the proactive and reactive methods. They have estimated the average number of connections per link, which do not have their backups readily available upon occurrence of a single link failure. This measure is used for selecting suitable primary and backup lightpaths for a connection. The simulation networks considered are the 21-node ARPA-2 network with 26 duplex links and 16- node Mesh-tours network with 32 duplex links.

This paper [7] proposes a methodology for performing automatic protection switching (APS) in optical networks with arbitrary mesh topologies in order to protect the network from fiber link failures. In the scenario considered, the layout of the protection fibers and the setup of the protection switches are implemented in nonreal time, during the setup of the network. When a fiber link fails, the connections that use that link are automatically restored and their signals are routed to their original destination using the protection fibers and protection switches. Under normal operation, the network supports a number of active source-destination connections, whose paths are determined by the settings of the optical switches. In these networks, a typical link consists of a pair of unidirectional working fibers and a pair of unidirectional protection fibers that are terminated by four protection switches. When a fiber link is cut, rerouting their optical signals around the fault using the protection fibers and protection switches automatically restores connections using that link. In the first part, showing how to solve the APS problem in mesh networks. The second part demonstrates how this approach is implemented in an optical network to provide full protection capabilities against a fiber link failure. A complete solution of this problem is presented for networks with planar or Eulerian (planar/nonplanar) topologies, together with algorithmic methods for extending it to networks with arbitrary nonplanar topologies.

This paper [8] is concerned with fast-distributed restoration and provisioning for generic mesh-based optical networks. They have considered two problems of practical importance: determining the best restoration route for each wavelength demand, given the network topology and the capacities and primary routes of all demands, determining primary and restoration routes for each wavelength demand to minimize network capacity and cost. The approach they propose for both problems is based on precomputing. For each problem, they describe traffic algorithms used for computing routes and also describe endpoint-based failure detection, message flows, and cross-connect actions for execution of fast restorations. The proposed restoration strategy is different from the 1+1 protection, which works at the link level, and the so-called 1+1 restoration (in which the source node bridges two copies of signal-one along each route). In particular, the restoration route (the alternate path) in their strategy does not need dedicated capacity reservations. If the service (primary) routes of two demands are disjoint, no single failure will affect both demands simultaneously. This means that the restoration routes of these demands can share link capacities, because these two routes will not be activated at the same time. They have proposed algorithms for simultaneous computation of primary route (for provisioning) and restoration route (to be invoked for restoration). This approach to distributed provisioning and restoration will speed up provisioning and will pave the way for dynamic reconfigurability of the entire optical layer network.

This investigation [9] considers optical networks which employ wavelength cross-connects that enable the establishment of WDM channels, between node pairs. This study examines different approaches to protect mesh-based WDM optical networks from single-link failures. These approaches are based on two basic survivability paradigms: (a) path protection/restoration, and (b) link protection/restoration. In path- and link-protection schemes, backup paths and wavelengths are reversed in advance at the time of call setup. Path and link restoration schemes are dynamic schemes in which backup paths are discovered (from the spare capacity in the network) upon the occurrence of a failure. The network resources used in dedicated-resource protection may be dedicated for each failure scenario, alternatively, the dedicated network resources used for protection against failures may be shared among different failure scenarios. In dynamic restoration, the spare capacity available within the network is utilized for restoring services affected by a failure. In this paper, they have examined the wavelength capacity requirements, and routing and wavelength of primary and backup paths for different protection schemes for a static traffic demand. The network topology and demand matrix (consisting of number of connections to be established between each node-pair) are given. They also assume that the set of alternate routes (that are satisfied any demand) between each node pair is precomputed and are given.

III. Survivability schemes in IP layer

The survivability schemes available at the network layer, such as IP (IP/MPLS), have the capability to recover multiple faults and operate at small traffic granularity. A primary concern for this approach is the slow convergence and response time of IP link failure detection and routing algorithms that renders them unsuitable for use with critical or premium services. However, these schemes are generally slow, as they require online processing upon failure occurrence. The networking functions such as routing and switching for service provisioning and restoration are performed at the network service layers (IP and MPLS) by the edge and core routers. Likewise, LSP failure detection can take a long time, since notification messages are propagated and processed hop-by-hop along the LSP back to the ingress router. However, these concerns may be addressed by suitable modification to the IP layer protocol behaviors. Another concern has to do with the scalability and efficiency of the approach. As WDM channels approach OC-192 rates (10 Gb/s) and beyond, there is a huge amount of traffic to be protected and rerouted in the event of a single wavelength channel (not to mention fiber) failure. Therefore, instead of rerouting individual fine grain IP flows, it is much more scalable if a server layer protection mechanism can be engineered. It is worth mentioning that IP layer protection can be made much finer grain and, therefore, affords much more focused protection, without wasting unnecessary bandwidth for those flows not needing protection. The next concern is that in a purely IP-based approach, there is no way to assure physical WDM layer path diversity between the primary and the backup paths setup by an IP/MPLS protection/restoration algorithm. Obtaining such an assurance requires knowledge of the WDM layer physical layout. For carrier grade operations, it is certainly desirable (in fact necessary) to have reliable protection and restoration schemes in place. However, for many IP data applications that assume a best effort IP datagram service, many have argued that a pure IP based recovery approach is in fact sufficient. In fact, recent study has indicated that much faster IP routing convergence may indeed be possible [10]. However, more detailed studies are needed to discern if a pure IP-based approach can usefully augment WDM layer protection and restoration. Recently, MPLS-based protection and restoration schemes are being actively pursued in the IETF MPLS working group, and some initial approaches have already been proposed [11], [12]. For the augmented and the peer models that adopt a unified control plane based on GMPLS, it would be possible to setup alternate lambda switched paths (SPs) [13]. This will allow fast backup switching when faults occur to provide uninterrupted end-to-end communications. In essence, the protection and restoration schemes in this category are analogous to the WDM server layer based approach and share the same properties. The main advantage is that the backup SPs are now visible to the IP layer, promising more effective coordination across the layers. Furthermore, physical path diversity can be directly enforced if the MP s control has access to the WDM layer's conduit layout information, in addition to the fiber topology. Dynamic routing and MPLS protection switching [14] are schemes currently considered to achieve network survivability at the IP (IP/MPLS) layer.

III (a) IP Dynamic (Survivable) Routing

Traditional IP networks employ destination-based shortest path first (SPF) routing such as RIP [15], OSPF [16], and IS-IS [17], to forward traffic from source to destination. The drawback is that it is traffic independent and does not support diverse routes. The shortest paths from different source-destination pairs in general will overlap at intermediate links causing congestion and packet loss. A recent enhancement to the SPF paradigm is to allow multiple equal-cost paths to a destination, and split the traffic between the multiple paths. For example, the latest OSPF specification allows for equal cost multipath routing (ECMP). However, even ECMP is traffic independent in the sense that there is no load balancing between the multiple paths, because there is also no feedback between the traffic load and the routing algorithm. A further enhancement to ECMP for load balancing, called optimized multipath routing (OMP), has been proposed recently. OMP utilizes and extends a link-state routing protocol like OSPF to periodically broadcast link loading information. Recently, in MPLS, the routing and forwarding functions in IP are separated. MPLS supports constraint based routing, including in particular explicit routing, thereby allowing direct control on the exact paths of IP traffic flows. Therefore, MPLS can be used to perform multipath load balancing of IP traffic. Using MPLS, IP traffic load balancing can be effected by rerouting selected LSPs away from congested links. In an IP over reconfigurable WDM network, traffic engineering can also be affected through wavelength circuit reconfiguration that adapts the IP network (virtual) topology to the evolving traffic pattern. By exploiting the WDM layer's reconfigurability, we can change the IP network's virtual topology to better match the ensuing traffic demand pattern.

With dynamic routing, reachable active routers are found dynamically, thus adapting IP routing to possible network faults. This task is accomplished by exchanging, between adjacent routers, control messages that are used to update the routers' routing tables, thus enabling IP packets to be dynamically rerouted around link and node failures. This protocol guarantees network wide survivability, independent of the underlying physical network. The routers can detect the faults in the network either explicitly or implicitly [18]. Explicitly, faults are detected at the local level and signaled to the neighboring routers through regular exchange of routing protocol control messages, such as Internet Control Message Protocol (ICMP). Otherwise, the expiration of timers on background messaging implicitly signals the presence of faults. Once a router detects a line fault, it recalculates the affected routes and updates its routing tables. Then it propagates the occurred changes to its neighboring routers using UPDATE messages such as Open Shortest Path First (OSPF) link state advertisement (LSA) or Border Gateway Protocol-4 (BGP-4). The dynamic routing protocol efficiently uses spare network resources and is flexible to topological changes. However, it is usually slow, from tens of seconds to minutes, and its behavior is unpredictable. Some enhancements of the protocol have been proposed [19] to overcome the former drawbacks.

III (b) MPLS Protection Switching

An alternative approach, MPLS protection switching, circumvents the latency drawback of dynamic routing. This approach is enabled through LSPs by prepending a stack of labels or tags to packet headers. The MPLS protection switching techniques, dynamic and prenegotiated, can be performed on a line basis by rerouting a portion of the LSP around the failed line, or link rerouting, or a path basis by rerouting the entire LSP, or edge-to-edge rerouting. In general, dynamic protection increases resource utilization but requires longer restoration times than preestablished protection. Link rerouting is faster than edge-to-edge rerouting because, in the latter case, the failure notification must reach the head-ends of all the LSPs affected by the failure.

A. 1+ 1 Dedicated MPLS Protection

The 1+ 1 dedicated MPLS protection is achieved by diverse LSPs, and no sharing of restoration capacity is attained. In this restoration approach, each OC-48c signal out of the edge routers is dual-fed into the duplicated core routers (via 0 1 interfaces), aggregated in OC-192c channels and diverse routed, via node and link disjoint physical paths, to the core routers at the destination end. Also, the OC-192c connections are transmitted from source to destination without any processing at the intermediate nodes. Therefore, in this architecture, intermediate nodes perform *static* wavelength routing, interconnecting wavelength channels from incoming to outgoing optical layer systems. Since switching functionality is not required at intermediate nodes, the simplest approach is to have thru channels (optically) bypassing the core routers via patch-panel connections. This leads to a large saving in router ports and switching capacity, resulting in the cheapest way to implement this architecture. However, this architecture provides only limited packet-level reconfigurability via the routers at the source and destination. Moreover, since the traffic is simultaneously fed to both primary and secondary paths, the 1+1 dedicated MPLS architecture does not support any preemptable traffic

B. 1: 1 Dedicated MPLS Protection

As for the 1+ 1 dedicated MPLS protection architecture, in the 1: 1 case each OC-48c connection is assigned physically disjoint primary and secondary paths. However, in this case, in fault-free state, the secondary LSP carries preemptable traffic so that the destination edge router receives both primary and preemptable traffic, increasing the network bandwidth efficiency. In the case of a failure in the primary LSP or core router, the destination edge router switches to the secondary LSP after having requested the source edge router to perform the same operation. This results in the preemptable traffic being dropped. This approach requires an MPLS signaling mechanism between the source and destination edge routers, and thus the restoration time is expected to be longer than the 1+1 case. As the traffic demand increases, this solution may become extremely complex to manage and the increasing amount of edge router signaling could flood the network if a fiber cut occurs. From a network design perspective, the 1+1 and 1: 1 cases are the same architecture.

III (c) Recent Research on Survivability schemes in IP layer

This paper [20], presents new algorithms for dynamic routing of locally restorable bandwidth guaranteed paths. This locally restorable on-line routing problem is becoming particularly important in optical networks and in MPLS based networks due to the trend toward dynamic provisioning of bandwidth guaranteed or wavelength paths. They developed efficient dynamic routing algorithms for bandwidth guaranteed paths that are locally restorable under single link or node failure. The routing is done using a sequence of shortest path computations, and it permits sharing of backup paths between requests as well as between the backup paths for different network elements for the same request. To prevent excessive resource usage for backup paths, and to satisfy the implicit service provider requirement of optimizing network resource utilization so as to increase the number of potential future demands that can be routed, it is desirable to judiciously share backup paths while still maintaining local restorability. The best sharing performance is achieved if the routing algorithm knows the routing of every path in progress in the network at the time of a new path set-up. However, this requires maintenance of nonaggregated or per-path information, which is not often desirable particularly when distributed routing is preferred. We show that a partial information scenario, which uses only aggregated and not per-path information provides sufficient information for efficient dynamic routing of locally restorable bandwidth guaranteed paths. In this partial information scenario the routing algorithm only knows what fraction of each link's bandwidth, is currently used by active paths, and is currently used by backup paths. Obtaining this information is feasible using proposed traffic-engineering extensions to routing protocols. They only have considered the case of protection against single link (node) failures. This is because the backup path is likely to be used only for a short time until a new active path is set-up. Secondly, protection against multiple failures requires multiple backups and this is too expensive in backup resource requirements.

In [21] the authors have described a restoration strategy called virtual protection cycles (p-cycles) for restoration in IP networks. The aim of the paper is to explain the basic p-cycle concept and its adaptation to both link and node restoration in the IP transport layer. In an IP router-based network, p-cycles are implemented with virtual circuits techniques such as an MPLS label switched path, or other means to form closed logical loops that protect a number of IP links, or a node. In the event of failure, packets, which would normally have been lost, are encapsulated with a p-cycle IP address and reenter the routing table, which diverts them onto a protection cycle. They travel by normal forwarding or label switching along the p–cycle until they reach a node where the continuing route cost to the original destination is lower than that at the p-cycle entry node. Diverted packets are deencapsulated (dropped from the p-cycle) at that node and follow a normal (existing) route from there to their destination. The p-cycle thus provides an immediate real-time detour, preventing packet loss, until conventional global routing reconvergence occurs. The first class of failures, which p-cycles can restore, is the loss of a logical IP link sometimes also called an IP trunk or IP logical span or just a "link" between a pair of adjacent routers. This could be caused by a failure at the physical/transport layer, such as a transmission span cut, or by the failure of an interface card. For physical layer failures, the failure will appear in the IP layer only if there is no physical layer restoration mechanism or its capability is exceeded for some reason. p-cycle restoration of logical link failures in an IP network is envisaged as follows. When an IP link failure has been detected, the router ports, which terminate the failed link, will be marked as dead and the usual link-state advertisement update process will be triggered. Until a global routing up-date is affected, any packet whose next hop, as indicated by the normal routing table entry for the packet's destination address, would have been directed into the dead port, is instead deflected onto a -cycle, which has been assigned to protect the link. A number of relaxations and heuristics are being considered for practical application on large networks. For research purposes, however, we have obtained completely optimal solutions for three networks, of up to 20 nodes and 31 links. Each test network was provisioned with link capacities that just met the working demand requirements of the shortest-path mapped demand matrix plus an amount of excess (or "spare") capacity given by an optimized "span restorable mesh" network.

In [22], the authors have considered an IP-over-WDM network in which network nodes employ optical crossconnects and IP routers. Nodes are connected by fibers to form a mesh topology. Any two IP routers in this network can be connected together by an all-optical wavelength-division multiplexing (WDM) channel, called a lightpath, and the collection of lightpaths that are set up form a virtual topology. In this paper, they investigated the maximum guaranteed network capacity and recovery times for two fault-management techniques for IP-over-WDM networks: WDM shared-path protection and IP restoration. The mathematical formulations of these fault-management techniques are developed, which turn out to be integer linear programs. They also developed heuristics for both of the techniques and compared the maximum guaranteed network capacity for the two techniques by plotting the traffic load factor versus the number of wavelengths for a network of interconnected rings typically used in the metro-area telecom environment. They developed analytical formulas for the recovery times for WDM shared-path protection and IP restoration and found that the recovery times for WDM shared-path protection are much faster than the recovery times for IP restoration.

IV. Summary of recent studies

This section summaries the work done so far.

Work Name	Layer	Link/Path protection/restoration	Shared/Dedicated protection/restoration	Proactive/Reactive	Static/Dynamic	Solution Methodology
[1]	Optical Layer	1) Link restoration 2) Path restoration	Shared	Proactive	Static	Two optimization techniques: integer linear programming (ILP) and simulated annealing (SA)
[2]	Photonic layer/ Network layer	Link/Path restoration	Shared/Dedicated	Proactive	Static	Disjoint Alternative Path (DAP) Algorithm and Simulation
[3]	Optical Layer	Path restoration/ protection	Shared/Dedicated	Proactive	Static	Integer programming and Simulation
[20]	Network Layer	MPLS path protection	Dedicated	Proactive	Dynamic	Integer linear programming and Simulation
[4]	Optical Layer	Link protection	Shared	Proactive	Static	Integer programming and Simulation
[5]	Optical Layer	Path protection	Shared/Dedicated	Proactive	Static	Integer programming and Simulation
[6]	Optical Layer/ Network Layer	Link protection	Dedicated	Proactive/ Dynamic	Dynamic	Algorithm/ Simulation
[7]	Optical Layer	Link protection	Dedicated	Reactive	Dynamic	Algorithm/ Simulation
[8]	Optical Layer	Path restoration	Shared/Dedicated	Proactive	Static	Integer programming and Simulation
[9]	Optical Layer	(a) path protection/restoration and (b) link protection/restoration	Shared/Dedicated	Proactive	Static	Integer programming and Simulation
[23]	Optical Layer	(a) path protection/restoration and (b) link protection/restoration	Shared/Dedicated	Proactive/ Reactive	Static/Dynamic	Because it is review paper for, different types of solution algorithms have been discussed.
[24]	Optical Layer	(a) path protection/restoration and (b) link protection/restoration	Shared/Dedicated	Proactive/Reactive	Static/Dynamic	Because it is review paper for, different types of solution algorithms have been discussed

Table I: Summary of present research works

V. Future Research Problem

Discussion for Future Study

Some pointers of the future problem are given:

1. Detection of the fault: to pinpoint the exact location of the fault in either the line or the node; some investigation regarding the methodology by which it would be possible
2. Both protection in the IP layer and restoration in the physical layer have their respective advantages. If a scheme can be developed which would encompass the advantages of both in such a way that the time and cost are both optimized, then ensuring survivability would be an easier task
3. One way to do this might be to have a path protection strategy for critical applications/users so that the fault can be restored fast and in a sure manner and have a restoration strategy, which is used for the rest of the non-critical applications
4. Carry out a study about such a scheme and develop the solution space with the help of Simulated Annealing or maybe ILP or maybe some heuristic method

References

[1] V Caenegem, W V Parys, F De Turck and P M. Demeester, "Dimensioning of Survivable WDM Networks" IEEE JSAC Sep 1998

[2] Crochat and J-Y Le Boudec, "Design Protection for WDM Optical Networks" IEEE JSAC Sep 1998

[3] Yasuhiro Miyao and Hiroyuki Saito, "Optimal Design and Evaluation of Survivable WDM Transport Networks", IEEE JSAC Sep 1998

[4] Eytan Modiano and Aradhana Narula-Tam, "Survivable routing of logical topologies in WDM networks" Proceedings of INFOCOM 2001

[5] Taehan Lee and Sungsoo Park, "Routing and Wavelength Assignment in Survivable WDM Networks", Proceedings of INFOCOM 2001

[6] G. Mohan and Arun K. Somani, "Routing Dependable Connections With Specified Failure Restoration Guarantees in WDM Networks", Proceedings of INFOCOM 2000

[7] Georgios Ellinas, Aklilu Gebreyesus Hailemariam, and Thomas E. Stern) Protection Cycles in Mesh WDM Networks JSAC Oct-200

[8] Bharat T. Doshi, Subrahmanyam Dravida, P. Harshavardhana, Oded Hauser and Yufei Wang, “ Optical Network Design and Restoration”, Bell Labs Tech Journal-Jan-Mar '99

[9] S. Ramamurthy and B. Mukherjee, “Survivable WDM Mesh Networks, Part I – Restoration”, Proceedings of INFOCOM-99

[10] C. Alaettinoglu *et al*.. (2000, Nov.) Toward millisecond IGP convergence. IETF Internet Draft. [Online]. Available: http://www.water-springs. org/pub/id/draft-alaettinoglu-isis-convergence-00.txt.

[11] V. Sharma *et al*.. (2001, July) Framework for MPLS based recovery. IETF Internet Draft. [Online]. Available: http://www.ietf.org/internet-drafts/ draft-ietf-mpls-recovery-frmwrk-03.txt.

[12] R. Doverspike and J. Yates, “Challenges for MPLS in optical network restoration,” *IEEE Commun. Mag*., vol. 39, pp. 89–97, Feb. 2000.

[13] G. Li *et al*., “Experiments in fast restoration using GMPLS in optical/ electronic mesh networks,” in *Proc. OFC’200*1, Anaheim, CA,

[14] T. M. Chen and T. H. Oh, “Reliable Services in MPLS,” *IEEE Commun. Mag*., vol. 37, no. 12, Dec. 1999, pp. 58–62.

[15] G. Malkin, “RIP version 2,” IETF, RFC 2453, Nov. 1998.

[16] J. Moy, “OSPF version 2,” IETF, RFC 2328, Apr. 1998.

[17] D. Oran, “OSI IS-IS intra-domain routing protocol,” IETF, RFC 1142, Feb. 1990.

[18] J. Anderson *et al*., “Protocols and Architectures for IP Optical Networking,”*Bell Labs Tech. Journa*l, vol. 4, no. 1, Jan.–Mar. 1999, pp. 105–24.

[19] C. Metz, “IP Protection and Restoration,” *IEEE Internet Comp*., vol. 4, no. 2, Mar.-Apr. 2000, pp. 97-102

[20] Murali Kodialam and T. V. Lakshman, “Dynamic Routing of Locally Restorable Bandwidth Guaranteed Tunnels using Aggregated Link Usage Information” Proceedings of INFOCOM 2000

[21] Demetrios Stamatelakis, and Wayne D. Grover, “IP Layer Restoration and Network Planning Based on Virtual Protection Cycles” JSAC Oct 2000

[22] L. Sahasrabuddhe, S. Ramamurthy, and B.Mukherjee, “Fault Management in IP-Over-WDM Networks: WDM Protection Versus IP Restoration” JSAC Jan 2002

[23] Dongyun Zhou and Suresh Subramaniam, “Survivability in Optical Networks” IEEE Networks -Dec 2000

[24] Gurusamy Mohan and C. Siva Ram Murthy, “Lightpath Restoration in WDM Optical Networks” IEEE Networks Dec 2000