A Review of Fault Management in WDM Mesh Networks: Basic Concepts and Research Challenges

Jing Zhang and Biswanath Mukherjee, University of California

Abstract

This article first presents a broad overview of the fault management mechanisms involved in deploying a survivable optical mesh network, employing optical crossconnects. We review various protection and restoration schemes, primary and backup route computation methods, sharability optimization, and dynamic restoration. Then we describe different parameters that can measure the quality of service provided by a WDM mesh network to upper protocol layers (e.g., IP network backbones, ATM network backbones, leased lines, virtual private networks), such as service availability, service reliability, restoration time, and service restorability. We review these concepts, the factors that affect them, and how to improve them. In particular, we present a framework for cost-effective availability-aware connection provisioning to provide differentiated services in WDM mesh networks. Through the framework, the more realistic scenario of multiple near-simultaneous failures can be handled. In addition, the emerging problem of protecting low-speed connections of different bandwidth granularities is also reviewed.

With the maturing of wavelength-division multiplexing (WDM) technology, one single strand of fiber can provide tremendous bandwidth (potentially a few tens of terabits per second) by multiplexing many nonoverlapping wavelength channels (WDM channels). Each wavelength channel can be operated asynchronously and in parallel at any desirable speed (e.g., peak electronic speed of a few gigabits per second). In a wavelength-routed WDM network, an optical crossconnect (OXC) can switch the optical signal on a WDM channel from an input port to an output port without any optoelectronic conversion of the signal; thus, a lightpath may be established from a source node to a destination node, and it may span multiple fiber links.

A fiber cut usually occurs due to a duct cut[1] during construction or destructive natural events, such as earthquakes, etc. All the lightpaths that traverse the failed fiber will be disrupted so a fiber cut can lead to tremendous traffic loss. Other network equipment (OXC, amplifier, etc.) may also fail. Table 1 shows some typical data on network component (transmitter, receiver, fiber link [cable], etc.) failure rates and failure repair times according to Bellcore (now Telcordia) [1]. In Table 1, failure-in-time (FIT) denotes the average number of failures in 10^9 hours, Tx denotes optical transmitters, Rx denotes optical receivers, and MTTR means mean time to repair.

With the frequent occurrence of fiber cuts and the tremendous traffic loss a failure may cause, network survivability becomes a critical concern in network design and real-time operation. As networks migrate from stacked rings to meshes because of the poor scalability of interconnected rings and the excessive resource redundancy used in ring-based fault management schemes, designing and operating a survivable WDM mesh network have received increasing attention [2–6]. Most of the research work on survivability in WDM networks focuses on recovery from a single link or node failure, where one failure is repaired before another failure is assumed to occur in the network. Nevertheless, as our knowledge on this subject has matured, the more realistic scenario of multiple near-simultaneous failures should now be considered (e.g., more than one link may be affected when a natural disaster such as an earthquake occurs).

Meanwhile, as our knowledge of resource management in survivable network design and real-time operation continues to mature, more and more researchers are shifting their attention to a service perspective. Naturally, how to provide a certain quality of service (QoS) per a customer's requirement and how to guarantee the service quality become critical concerns. The rationale behind this is as follows. A WDM mesh network may provide services for IP network backbones, asynchronous transfer mode (ATM) network backbones, leased lines, virtual private networks (VPNs), and so on. The QoS requirements for these services can be very different because of their diverse characteristics; for example, online trading, military applications, and banking services will require strin-

This work has been supported by the National Science Foundation (NSF) under Grant No. ANI-9805285, and by Sprint Advanced Technology Laboratories (ATL).

[1] *A duct is a bidirectional physical pipe between two nodes. In practice, fibers are put into cables, which are buried into ducts under the ground.*

gent reliability, while IP best effort packet delivery service may be satisfied without a special constraint on reliability. Service quality can be measured in many different ways such as signal quality, service availability, service reliability, restoration time, and service restorability. Signal quality is mainly represented by the optical signal-to-noise ratio (OSNR), bit error rate (BER), and other factors, and is affected by the transmission equipment characteristics. This is a problem in all-optical networks, and is out of the scope of our current discussion.

Our interest is in the availability of service paths in WDM mesh networks. Usually, availability is defined as the probability that the service or connection will be found in the operating state at a random time in the future [7]. Connection availability can be computed statistically based on the failure frequency and failure repair rate, reflecting the percentage of time a connection is "alive" or "up" during its entire service period. Although the problem of how connection availability is affected by network failures is currently attracting more research interest [1, 7–9], we still lack a systematic methodology to quantitatively estimate a connection's availability, especially when protection schemes are applied to the connection. In this review we shall discuss the rationale and challenges for availability analysis in WDM mesh networks. In particular, we shall present a framework for a generic connection provisioning problem with due consideration of network component failure characteristics so that all possible network failure scenarios and their effects can be incorporated.

The objective of this article is to present a broad overview of the fault management issues involved in designing an optical mesh network employing OXCs and real-time network operation including dynamic connection provisioning. We introduce the basic concepts in fault management schemes: various protection and restoration schemes, primary and backup route computation methods, sharability optimization, and dynamic restoration. Then we present a framework for availability-aware connection provisioning to provide differentiated services in a mesh network and handle multiple failures. We also outline other criteria that may affect service quality such as service reliability, restoration time, and service restorability. Online algorithms for protecting low-speed connections are also reviewed.

Metric	Telcordia statistics
Equipment MTTR	2 h
Cable-cut MTTR	12 h
Cable-cut rate	4.39/yr/1000 sheath mi
Tx failure rate	10,867 FIT
Rx failure rate	4311 FIT

■ Table 1. *Failure rates and repair times (Telcordia) [1].*

Basic Concepts in Fault Management

There are two types of fault recovery mechanisms [3]. If backup resources (routes and wavelengths) are precomputed and reserved in advance, we call it a *protection* scheme. Otherwise, when a failure occurs, if another route and a free wavelength have to be discovered dynamically for each interrupted connection, we call it a *restoration* scheme. Generally, dynamic restoration schemes are more efficient in utilizing network capacity because they do not allocate spare capacity in advance and provide resilience against different kinds of failures (including multiple failures); but protection schemes have faster recovery time and can guarantee recovery from service disruptions against which they are designed to protect (a guarantee restoration schemes cannot provide).

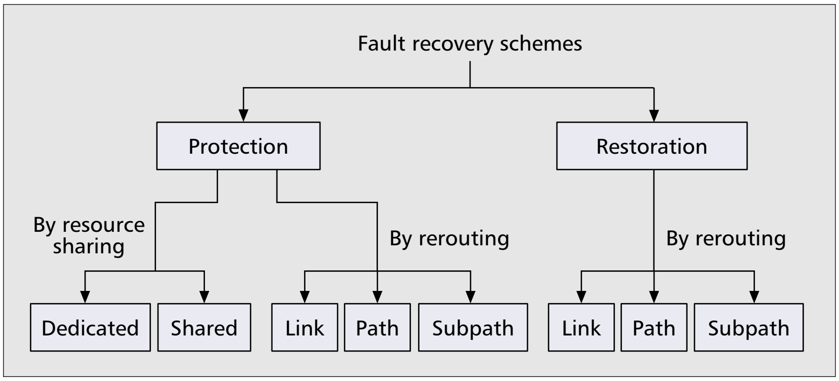
Protection schemes can be classified as ring protection and mesh protection. Ring protection schemes include Automatic Protection Switching (APS) and Self-Healing Rings (SHR). Both ring and mesh protection can be further divided into two groups: path and link protection. In *path protection*, the traffic is rerouted through a backup route (*backup path*) once a link failure occurs on its working path (*primary path*). The primary and backup paths for a connection must be link disjoint so that no single link failure can affect both paths. In *link protection*, the traffic is rerouted only around the failed link. While path protection leads to efficient utilization of backup resources and lower end-to-end propagation delay for the recovered route, link protection provides shorter protection switching time. Recently, researchers have proposed the idea of *subpath protection* in a mesh network by dividing a primary path into a sequence of segments and protecting each segment separately (or dividing the whole network into different domains where a lightpath segment in one domain must be protected by the resources in the same domain) [10, 11]. Compared to path protection, subpath protection can achieve high scalability and fast recovery time for a modest sacrifice in resource utilization.

Note that node failures can also be considered by calculating node disjoint routes. However, one should also note that carrier-class OXCs in network nodes must be 1 + 1 (master/slave) protected in the hardware for both the OXC's switch fabric and its control unit. The OXC's port cards, however, do not have to be 1 + 1 protected since they take up the bulk of the space (perhaps over 80 percent) and cost of an OXC; also, a port card failure can be handled as link and/or wavelength channel failure(s). However, node failures are important to protect against in scenarios where an entire node (or a collection of nodes in a part of the network) may be taken down, possibly due to a natural disaster or by a malicious attacker.

Link, subpath, and path protection schemes can be dedicated or shared. In *dedicated protection* there is no sharing between backup resources, while in *shared protection* backup wavelengths can be shared on some links as long as their protected segments (links, subpaths, paths) are mutually diverse. OXCs on backup paths cannot be configured until the failure occurs if shared protection is used. Thus, recovery time in shared protection is longer but its resource utilization is better than dedicated protection.

Dynamic restoration [3, 12] can also be classified as link-, subpath-, or path-based depending on the type of rerouting. In *link restoration* the end nodes of the failed link dynamically discover a route around the link for each connection (or "live" wavelength) that traverses the link. In *path restoration* when a link fails, the source and destination nodes of each connection that traverses the failed link are informed about the failure (possibly via messages from the nodes adjacent to the failed link). The source and destination nodes of each connection independently discover a backup route on an end-to-end basis. In *subpath restoration*, when a link fails, the upstream node of the failed link detects the failure and discovers a backup route from itself to the corresponding destination node for each disrupted connection. Link restoration is fastest and path restoration is slowest of the above three schemes; subpath restoration time lies between. Figure 1 summarizes the classification of protection and restoration schemes.

We discuss the main problems in fault management and some appropriate techniques to solve them in the following subsections. Network traffic can be static, dynamic, or incremental; and these techniques can be applied to different provisioning scenarios according to different network characteristics.



■ Figure 1. *Different protection and restoration schemes in WDM mesh networks.*

Survivable Routing and Wavelength Assignment

If wavelength converters are equipped in OXCs, a lightpath can be assigned to different wavelengths on the links it traverses. Such a network is known as a *wavelength-convertible* network. If wavelength converters are not equipped in OXCs, we require that, when establishing a lightpath, the same wavelength be allocated on all links in the path. This requirement is known as the *wavelength continuity constraint* and such a network is known as a *wavelength-continuous* network. In a wavelength-continuous WDM mesh network employing end-to-end path protection, the problem of finding a link disjoint primary-backup path pair and assigning a proper wavelength channel to each path is known as the survivable routing and wavelength assignment (S-RWA) problem and has been extensively studied.

Usually a path pair with least cost from a source to a destination is preferred to carry the traffic. Similar to the path cost for an unprotected lightpath, defined to be the sum of the costs of the links on the path, the path cost of a dedicated-path-protected connection is the sum of the costs of the primary and backup lightpaths.

When shared path protection is applied, the cost of a connection t is the sum of the cost of t's primary lightpath and the costs of the *additional* backup links on which the wavelength is reserved by connection t but is not shared by other existing connections. The path pair can be either selected from a set of preplanned alternate routes or dynamically computed according to current network state. Depending on different traffic engineering considerations, different cost functions can be applied to network links, such as constant 1 (to minimize hop distance), length of the links (to minimize delay), fraction of available capacity on the links (to balance network load), network cost (total equipment cost plus operational cost) on the links (to minimize cost), and so on.

The wavelength assignment (WA) problem can be considered after the routing of the pair of primary-backup paths has been fixed. Different WA heuristics have been proposed and studied in the literature [13]. WA can also be jointly considered with the route computation of both primary and backup paths. It has been proven that the problem of computing a pair of link disjoint paths in a WDM network with the wavelength continuity constraint is NP-complete [13]. When a network has full wavelength conversion capability, the problem is reduced to an optimal routing problem for a link disjoint path pair, which can be solved using existing algorithms such as Suurballe's algorithm [14].

Besides different S-RWA heuristics, linear program (LP)-based approaches are used to attack the problem. The LP approach can be used to either precompute a set of candidate routes or compute a pair of primary-backup paths according to current network state in an on-demand manner. Although an LP-based scheme is not very scalable because it is computation-intensive, such an approach can provide valuable insights for designing efficient heuristic algorithms. Different approximation schemes have been proposed for LP-based approaches that make them suitable for use in a practical network with a reasonable volume of traffic demands.

Sharability Optimization

One of the key advantages of WDM mesh networks against legacy SONET-based interconnected ring networks is that WDM mesh networks are capable of supporting differentiated protection schemes and can be more efficient than those in SONET ring networks. Particularly, through path-based shared protection, optical WDM mesh networks may only require 40–60 percent extra capacity to protect against any single failure in the network, compared to a 100 percent spare capacity requirement in SONET-ring-based protection schemes [3]. In a shared protection scheme, network resources along the backup path can be shared between primary paths of different connections, as long as only one connection will revert its traffic from the primary path to the backup path when a network failure occurs. There are several investigations on how to maximize resource sharability for the shared protection scheme in WDM mesh networks in order to optimize network resource efficiency [4]. It is generally assumed that:

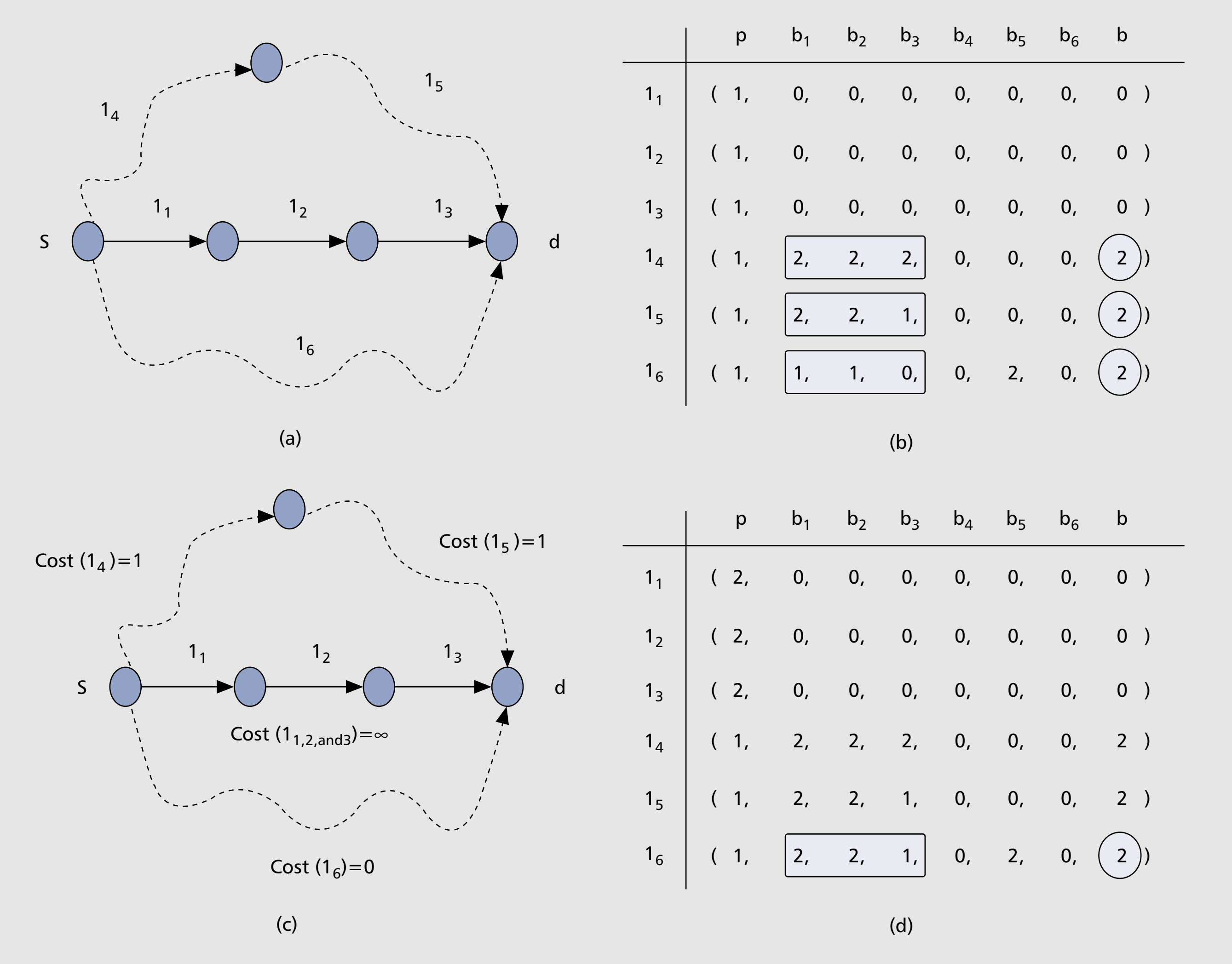
- Link failure is the dominant network failure scenario.
- There is at most a single link failure at any time, and it is repaired before the next failure occurs, so the multiple-failure scenario is a relatively rare event in the network.

The following approaches and considerations have been investigated for maximizing resource sharability with or without the wavelength continuity constraint.

Backup Route Optimization — One way to achieve high resource sharability is to spread the primary path of different connections as much as possible, and simultaneously plan their backup paths such that they will share the same resources extensively. This joint optimization is a very hard problem; hence, we lack effective approaches. An alternative approach is to fix the primary path according to current network state (e.g., minimal cost route) while optimizing the backup route for a connection request. This can be realized by adjusting the link costs based on current resource usage information of network links. For instance, let $l_j(p, b_1, b_2, \ldots, b_i, \ldots, b_N, b)$ denote the resource usage information of link j (i.e., link vector) in a full wavelength-convertible network, where p denotes the number of wavelength channels allocated for the primary paths (connections) on link j; b_i denotes the number of wavelength channels allocated on link j to protect against the failure of link i ($1 \le i \le N$, and N is the number of links in the network, i.e., when link i fails, there are b_i connections originally supported by link i that will be reverted to link j); and b denotes the total number of allocated spare wavelength channels for protection purposes. Under the assumptions that there is a single link failure at any time and shared path protection is employed in the network, b is equal to the maximal value of b_i ($1 \le i \le N$). When the primary path of a connection traverses links $l_{m1}, l_{m2}, \ldots, l_{mn}$, the link cost of l_j can be adjusted to

$$Cost(l_j) = \begin{cases} \infty & \text{if } l_j \text{ is on the primary path,} \\ 0 & \text{if } b_{m1} < b, \ldots \text{ and } b_{mn} < b, \\ 1 & \text{otherwise.} \end{cases} \qquad (1)$$

Note that, using this link cost adjustment function, the link cost is set to 0 if no new wavelength channel needs to be allocated;



(b)

	p	b_1	b_2	b_3	b_4	b_5	b_6	b
1_1	(1,	0,	0,	0,	0,	0,	0,	0)
1_2	(1,	0,	0,	0,	0,	0,	0,	0)
1_3	(1,	0,	0,	0,	0,	0,	0,	0)
1_4	(1,	2,	2,	2,	0,	0,	0,	2)
1_5	(1,	2,	2,	1,	0,	0,	0,	2)
1_6	(1,	1,	1,	0,	0,	2,	0,	2)

(d)

	p	b_1	b_2	b_3	b_4	b_5	b_6	b
1_1	(2,	0,	0,	0,	0,	0,	0,	0)
1_2	(2,	0,	0,	0,	0,	0,	0,	0)
1_3	(2,	0,	0,	0,	0,	0,	0,	0)
1_4	(1,	2,	2,	2,	0,	0,	0,	2)
1_5	(1,	2,	2,	1,	0,	0,	0,	2)
1_6	(1,	2,	2,	1,	0,	2,	0,	2)

■ Figure 2. *An example of backup sharing optimization.*

otherwise, link cost is set as 1.[2] After each network link has been assigned a proper link cost, the backup path can be computed using any shortest path algorithm (e.g., Dijkstra's algorithm).

Figure 2 illustrates an example of how to compute a backup path that can optimize resource sharability when the primary path is known. Figure 2a shows the state of a part of a network where only a few network nodes and links are shown. There is a connection request between node pair (s,d), whose primary path traverses links l_1, l_2, and l_3, as shown by the solid lines in Fig. 2a. It is straightforward to see that the candidate backup path for the connection request traverses either links l_4 and l_5, or link l_6. (Note that each backup link in Fig. 2a can be a collection of links. To simplify the example, we just use one or two links on each candidate backup path.) Assuming that there are enough wavelength channels on each link, Fig. 2b shows the link vector for each network link. Based on this resource usage information and the cost function shown in Eq. 1, Fig. 2c shows the network state with adjusted link cost from which a resource-sharability-optimized backup route can be calculated for the given primary path using a standard shortest path algorithm. Finally, Fig. 2d illustrates the updated link vectors after both primary and backup paths have been fixed for the connection request.

Such a backup resource optimization technique can be applied to different provisioning scenarios based on different network characteristics. Network traffic can be static, dynamic, or incremental. It may also be combined with different S-RWA schemes.

A Physical Constraint on Backup Route Optimization — Although the backup route optimization technique can greatly improve resource efficiency, one problem may arise. When this approach is extensively used, a connection may have a backup path traversing long (hop) distances even though the primary path is short [3]. A long backup path may lead to a signal quality degradation problem, especially in an all-optical WDM network. In such a network, transmission and switching impairments can accumulate along the lightpath, and may affect the signal quality at the destination node. As a result, after an optical signal travels a long distance, the BER at the destination node may not be tolerable for services at upper network layers. Therefore, when a network failure occurs, even though a preplanned backup path can be used to restore each affected connection, an unexpectedly long backup path can potentially degrade signal quality or even fail to restore the connection.

Recently, different research groups have started to investigate such a problem. The authors in [15] proposed an ILP-based model to jointly compute the shared protected primary-backup path pair for dynamic traffic. The model takes both network resource usage and backup path distance

[2] *This method assumes that minimizing the number of wavelength links used in the network is the optimization objective.*

into consideration. The idea of such a model is to incorporate one additional cost component μ to the link cost, such that the link cost reflects both the extra resources the backup path may use and the distance it may traverse.

Failure-Independent Backup Routing vs. Failure-Dependent Backup Routing — Another possible approach to improve backup resource sharability is failure-dependent backup routing (FDBR). In such a scheme, one backup route can be computed according to a certain network failure on the primary path. That is, if the primary path traverses *m* links, there may exist *m* backup paths, one for each failure of the *m* links. In a failure-independent backup routing (FIBR) scheme, a single backup path will be used independent of the failed link; FIBR is the dominant method used by most approaches in the research literature today. It is easy to see that FIBR is a special case of FDBR in the sense that the *m* backup paths are the same. The *m* backup paths in FDBR may share resources with other backup paths or even between themselves. The resources along the primary path may also be reused by the *m* backup paths. In this way, FDBR may further improve resource sharability among the backup paths and eventually increase overall network resource efficiency.

Dynamic Restoration

Besides protection schemes, traffic restoration schemes have also been an important area of research interest. The following performance metrics have been used to evaluate a restoration scheme:

- *Restoration success rate (RSR)* denotes the ratio between the number of successfully restored connections and the number of affected connections after a network failure occurs.
- *Restoration time (RT)* denotes the average time needed to successfully restore an affected connection request.

There are different considerations under study for restoration schemes in optical WDM mesh networks.

Distributed Control vs. Centralized Control — In a distributed control system, the source node of each interrupted connection can restore the service following either a precomputed or dynamically computed route. Since the connections are restored in a distributed manner, it is possible that resource contention may occur on some network link. Although such contentions can be resolved through restoration retries, they may affect RSR and RT performance. In a centralized control system, connections will be restored one by one, so resource contention is avoided, but this scheme may affect the RT performance of some connections. Compared to distributed control, a centralize controlled restoration scheme may achieve better RSR since it can perform global optimization of network resource usage.

Preplanned Restoration Routes vs. Online Dynamically Computed Restoration Routes — In a distributed control system, the restoration routes can be preplanned or dynamically computed. In a preplanned scheme, a candidate restoration route set can be precomputed for each connection. When a connection fails, one route from this set can be selected as the restoration path without online computation. Other candidate routes can also be tried if the restoration on the selected route fails. This scheme may improve RT performance. The route set may be periodically updated according to different network states in order to improve the probability of successful restoration.

Path vs. Subpath vs. Link Restoration — As mentioned before, restoration schemes can be classified into path-based, subpath-based, and link-based schemes, according to which an alternative path is chosen, and how the new path is routed to bypass the failed link. The work in [12] compared the performance trade-off of these different restoration mechanisms under a distributed control and signaling system using generalized multiprotocol label switching (GMPLS).

IP Restoration vs. WDM Protection — It has been well accepted that IP traffic is the dominant traffic in today's Internet. The IP-over-WDM network architecture has gained significant attention and been widely studied. In such a network architecture, different network layers may employ different fault management schemes. For example, it may not be cost effective to employ all fault management schemes at every network layer. The authors in [16, 17] have investigated the trade-offs of different fault management schemes at different layers. It is reported that a network may have better performance if restoration schemes are employed at the IP layer and protection schemes at the optical WDM layer. Although there is growing interest in this research topic, more in-depth study is still needed to design and develop such IP-over-WDM network infrastructures.

Current Research Trends and Future Challenges

As our knowledge of resource management in survivable network design and real-time operation keeps maturing, more and more researchers are shifting their interest to a services perspective. How to provide a certain QoS based on a customer's requirements and how to guarantee service quality are becoming critical concerns. In this section we briefly describe these network-failure-related QoS metrics: service availability, service reliability, restoration time, and service restorability. In addition, the emerging problem of protecting low-speed connections of different bandwidth granularities is also discussed.

Availability is defined as the probability that a system (in this case a connection) will be found in the operating state at a random time in the future. Connection availability can be computed statistically based on the failure frequency and failure repair rate of the underlying network components the connection is using, reflecting the percentage of time a connection is "alive" or "up" during its entire service period.

Reliability is the probability that a system will operate without any disruption for a period of time. Service reliability can be represented by the number of hits or disruptions in a period of time. Availability and reliability are different measures of service quality. For example, a connection is disrupted once during the period from time T_1 to time T_2. If the disruption holds for 50 ms or 5 s, the availability of the connection will differ by two orders of magnitude for the two cases, while the connection reliability is the same (i.e., one failure during period $T_2 - T_1$) for both cases.

Restoration time defines the exact disruption holding time, which should be minimized as much as possible.

Service restorability is usually a network-wide parameter representing the capability of a network to survive a specific failure scenario.

Service Availability

It should be clear that a protection scheme will help to improve a connection's availability since traffic on the failed primary segment (link/path/subpath) will be quickly switched to the backup segment. For example, a path-protected connection will have 100 percent availability[3] in the presence of any single failure. Nevertheless, when the more realistic scenario of multiple, near-simultaneous failures is considered, connection availability depends intimately on the precise details of the failures (locations, repair times, etc.), how much backup resources are reserved (i.e., single backup route or multiple backup routes), and how the backup resources are allocated (i.e., dedicated or shared). Intuitively, the more backup resources (paths) there are, the higher is the connection availability, while more backup sharing leads to lower connection availability. What we need now is a systematic methodology to quantitatively estimate a connection's availability, especially when various (dedicated or shared) protection schemes are applied to the connection. Such a methodology can essentially help us to understand how well a connection is protected and whether or not a service quality can be guaranteed instead of simply stating that a connection is protected.

As we discussed above, a customer of an optical network operator may buy some bandwidth with certain service-quality requirements. Availability is one of them, which is usually defined in a service-level agreement (SLA). The SLA is a contract between the network operator and a customer. (Normally, the customer pays for the services provided by the network operator.) An SLA violation may cause a certain amount of penalty to be paid by the network operator according to the contract (e.g., providing free services for one additional month). Although overprovisioning may help a network operator to avoid such a penalty, extra resource (or cost) consumption will be introduced, which may not be necessary if the connection is provisioned properly. Thus, a cost-effective, availability-aware, connection-provisioning scheme is very desirable such that, for each customer's service request (static or dynamic), a proper protection scheme (dedicated, shared, or unprotected) is designed and the degree of sharing is consciously controlled (in shared-protection case) so that the SLA-defined availability requirement can be guaranteed and high overall resource efficiency can be achieved. Through such a scheme, differentiated protection services are also inherently provided in optical WDM mesh networks.

A network component's availability is a relatively static value since it is based on the component's failure rate and average time to fix a failure. One may notice that a connection's availability is also a static value as long as the routes of the connection's primary and backup paths have been fixed and there is no resource correlation between two connections (which means no resource sharing). Hence, some candidate routes can be predesigned, and the availability of each of them can be calculated. Then, in on-line provisioning, one of the routes will be picked to carry a new connection as long as its availability is larger than that required by the customer. This strategy can also be applied in offline network design with a given set of traffic demands which need to be set up simultaneously. We can formulate the problem into an ILP and solve it for moderate problem sizes.

However, connection availability becomes a dynamic value when the connection (t) is sharing some wavelengths on its backup path with others. Let St contain all the connections that share some backup wavelength on some link with t. We denote S_t as the sharing group of t. Each time a new connection joins S_t, the availabilities of all the connections in the group will be affected. Meanwhile, there are various backup-sharing-related operational decisions which also affect connection availability. For example, if there are multiple failures in the network that, unfortunately, affect more than one connection in S_t, some questions will arise such as which connection will be chosen to restore and how to deal with other failed connections. Usually, connection t's traffic can be switched back to its primary path after the failure on the primary path is repaired, which is called *reverting*; or the traffic can stay on the backup path for the remaining service time, which is called *nonreverting*. A network operator may choose their desired policies based on operational cost and service characteristics. Each of these policies will have an effect on the availability analysis.

Protection schemes	Connection availability
Unprotected	$A_t = \Pi_{j \in G_t} a_j$
Dedicated path protected	$A_t = 1 - (1 - A_p) \times (1 - A_b)$
Shared path protected	$A_t = A_p + (1 - A_p) \times A_b \times \Sigma_{i=0}^{N} \delta_\tau^2 \times p_i$

■ Table 2. *Connection availability computation.*

Availability Analysis in WDM Mesh Networks — We present an availability analysis for a connection with different protection schemes (which could be unprotected, dedicated path protected, or shared path protected) in a WDM mesh network. We assume that different network components fail independently; and, for any component, the up times, or mean time to failure (MTTF), and the repair times, or mean time to repair (MTTR), are independent memoryless processes with known mean values. Upon failure of a component, it is repaired and restored to be "as good as new." This procedure is known as an *alternating renewal process*. Consequently, the availability of a network component j (denoted a_j) can be calculated as follows:

$$a_j = \frac{MTTF}{MTTF + MTTR}. \tag{2}$$

Particularly, fiber cut statistics are used to derive the distance-related fiber cut rates. If connection t is only carried by one single path, given the route of the path, the availability of t (denoted A_t) can be calculated based on the known availabilities of the network components along the route. Connection t is available only when all the network components along its route are available. Let a_j denote the availability of network component j. Let G_t denote the set of network components used by path t. Then A_t can be computed as follows:

$$A_t = \prod_{j \in G_t} a_j. \tag{3}$$

If t is dedicated path protected, t is down only when both primary path (p) andß backup path (b) are unavailable, so A_t can be computed as follows:

$$A_t = 1 - (1 - A_p) \times (1 - A_b), \tag{4}$$

where A_p and A_b denote the availabilities of p and b, respectively. Note that a connection may also have multiple backup paths. Assuming that all the backup paths are disjoint, the availability of the connection can be derived following a principle similar to that in Eq. 4. Table 2 shows how to calculate the availability for an unprotected or dedicated path protected connection.

As discussed above, the availability of connection t (A_t) will be affected by the size of S_t and the availabilities of the connections in S_t if shared path protection is applied. For illustration purposes, we present here a preliminary connection availability analysis for a shared path protected connection. A shared path protected connection t will be available if p is available; or p is unavailable, b is available, and p can get the backup resources when the other paths in the sharing group S_t have also failed. Therefore, A_t can be computed as follows (it is also shown in Table 2):

[3] *Here, the contribution of the reconfiguration time to unavailability is disregarded since it is relatively small compared to failure repair time and the connection's holding time.*

$$A_t \quad A_p + (1 - A_p) \times A_b \times \sum_{i=0}^{N} \delta_t^i \times P_i, \tag{5}$$

where A_p and A_b denote the availability of p and b, respectively; N is the size of S_t; δ_t^i is the probability that t can get the backup resources when both p and the other i primary paths in S_t fail; and p_i is the probability that exactly i primary paths in S_t are unavailable. We can enumerate all the possible i connection failures to compute p_i. For δ_t^i, we use a continuous-time Markov chain to derive it. Please see [9] for the Markov model and the corresponding state transition diagram for the Markov chain, which are skipped here due to lack of space.

Note that the analysis for connection availability may be different under different backup sharing policies. More study is required in this relatively unchartered field of availability analysis for shared protected connections. These policies impact not only the connection availability, but also the overall network blocking probability, resource efficiency, and provisioning strategy design (e.g., if a nonreverting model is employed, recomputing the backup paths after a failure occurs may be needed for connections that are in the sharing group of the failure-affected connection). Provisioning strategies should be properly designed according to each policy.

Provisioning Strategies — Based on the analytical model, we propose some availability-aware connection provisioning approaches in which an appropriate level of protection is provided to each connection according to its predefined availability requirement. Both formal optimization techniques and heuristic strategies are studied for a given set of traffic demands. Our goal is to determine the route for each connection request and protect them (if necessary) while satisfying their availability requirements and minimizing the total network cost (wavelength links, particularly).

To optimize network resource usage, we first classify the connection requests into two categories: T_1 (containing *one-path-satisfiable* connections whose availability requirements can be satisfied without using any backup paths) and T_2 (containing *protection-sensitive* connections for which backup paths are necessary); then we provide different treatments to different connection sets:

- For a connection in T_1, one path is needed to carry each of them. We use an ILP to find the routes that can satisfy the connections' availability requirements while minimizing the consumed resources (wavelength links).
- Protection schemes are necessary for connections in T_2. The problem of providing dedicated path protection while satisfying the connections' availability requirements is mathematically formulated. Due to the nonlinearity of the formulations, we propose two schemes to approximately solve them. Several heuristic algorithms are studied since mathematical formulations are not scalable when the network size and number of connection requests increase. To further improve resource efficiency, we incorporate a failure-independent shared-path protection scheme into the heuristics.

Our preliminary results demonstrate that availability-aware provisioning strategies are promising; hence, further research is very encouraging to undertake.[4]

Service Reliability, Restoration Time, and Service Restorability

Service Reliability — Disruption Rate — Service disruption rate is not only affected by the failure rate but also by operation policies. For example, traffic will be disturbed twice in the reverting strategy, which may be highly undesirable for some services such as online trading. However, if nonreverting strategy is employed, the backup paths for the connections that are sharing backup resources with connection t may need to be rearranged since some resources on parts of their backup paths may be taken by t after t is switched to its backup path. These connections become vulnerable during their backup recomputation and resource reservation; furthermore, their successful backup rearrangement is not guaranteed, especially when network load is high, so nonreverting may result in unpreferable service degradation. Hence, the operation policies need to be carefully selected according to the customers' requirements and network resource utilization.

Restoration Time — Service restoration time varies according to different fault management schemes. In dedicated (link, path, or subpath) protection, OXCs on the backup paths can be preconfigured when the connection is set up. Then no OXC configuration is necessary when the failure occurs. This type of recovery can be very fast. If traffic is not transmitted on both paths, the destination node needs to wait until the source node is notified, and the source node switches traffic to the backup path. Thus, the restoration time will include time for failure detection, time for failure notification, and propagation delay. In shared protection the OXCs on the backup paths cannot be configured until a failure occurs. The restoration time is longer in this case. For dynamic restoration, the service restoration time includes the time for route computation and resource discovery besides failure detection, notification, OXC reconfiguration, and propagation delay.

Network partitioning has been proposed to achieve high network scalability and fast fault restoration time. The idea is to partition a large network into several smaller domains, and then provide protection to each connection such that an intradomain segment of a lightpath does not use resources of other domains, and the primary and backup paths of an interdomain lightpath exit a domain (and enter an adjacent domain) through a common egress (or ingress) domain border node [10]. When a failure occurs, only the affected domain will activate its protection subpath, so the restoration time is reduced due to the reduced path length.

Service Restorability — Service restorability is usually a network-wide parameter representing the capability of a network to survive a specific failure scenario. The restorability $R_f(i)$ of a network for a specific f-order ($f \geq 1$) failure scenario (i) is defined as the fraction of failed working capacity that can be restored by a specified mechanism within the spare capacity provided in a network [7]. The restorability R_f of a network as a whole is the average value of $R_f(i)$ over the set of f-order failure scenarios. For example, the network-wide ratio of restorable capacity to failed capacity over all single-failure (dual-failure) scenarios is called the single-failure (dual-failure) network restorability, R_1 (R_2), in [7].

Network restorability is an important criterion in network design that can be used to evaluate the quality of a specific mechanism (e.g., a protection scheme). Suppose we have two protection schemes, P_1 and P_2, both of which consume the same amount of spare capacity to provide 100 percent R_1 to the network. We can essentially compare R_2 of the network under P_1 and P_2 to distinguish between their qualities for the dual failure scenario. Obviously, the one with higher R_2 is preferred since it can provide higher network restorability when

[4] *Please see [9] for the connection classification technique, detailed mathematical formulations, heuristic algorithms, and results from ILP and heuristics, which are skipped here due to lack of space.*

dual failures occur. The work in [7] showed that R_1-designed mesh restorable networks inherently have high levels of dual-failure restorability (R_2) using an adaptive restoration process. However, how to efficiently design a network with $R_1 = 100$ percent and restore connections for dual failures play important roles in R_2 evaluation, which needs further study.

Protecting Low-Speed Connections of Different Bandwidth Granularities

Here, we briefly discuss algorithms for routing and protecting low-speed connections with different bandwidth granularities. The bandwidth of a wavelength channel is quite high (10 Gb/s, OC-192, today, and expected to grow to 40 Gb/s, OC-768, soon). However, only a fraction of customers are expected to need such high bandwidth (where customers mean Internet service providers and large institutional users of bandwidth). Many customers will be content with lower bandwidth — STS-1 (51.84 Mb/s), OC-3, OC-12, OC-48, and so on — for their applications. Since different connections may prefer different fault management schemes, the network operator has to trade off between protecting each connection individually (protection at connection level, PAC) or grooming (i.e., efficiently packing several lower-speed connections onto high-capacity wavelength channels) and then protecting them as a whole (protection at lightpath level, PAL) [18].

A low-speed connection can be routed through some existing lightpaths as long as there is enough available bandwidth on these lightpaths. Under PAL, a backup lightpath must be computed when establishing a new primary lightpath; thus, backup paths are given by default when a connection is routed through some existing lightpaths. Under PAC, a connection is routed via link disjoint working and backup paths, each of which traverses a sequence of lightpaths. Therefore, backup paths still need to be computed even though the connection is routed through existing lightpaths.

The fundamental difference between PAL and PAC is that PAL provides end-to-end protection with respect to a lightpath, while PAC provides end-to-end protection with respect to a connection.

Essentially, PAL performs at an aggregate level (lightpath) and PAC works on a per-flow basis (connection). Note that under both PAL and PAC, protection resources can be dedicated or shared depending on customers' requirements. Both of these schemes incorporate additional constraints on backup resource sharing, which need further study. PAL appears to be simpler to implement than PAC. When backup sharing is allowed, both PAL and PAC need routing information of all *existing lightpaths* to provision a new connection request. PAL does not require any information about the *existing connections*. PAC, however, requires detailed routing information of all existing connections.

Concluding Remarks

Fault management in WDM mesh networks is an important and exciting research area. This article reviews the fault management mechanisms involved in deploying a survivable optical mesh network using OXCs. Specifically, we examine various protection and restoration schemes, primary and backup route computation methods, sharability optimization, and dynamic restoration. Different parameters such as service availability, service reliability, restoration time, and service restorability, which can measure the QoS provided by a WDM mesh network to upper network layers, are discussed. In particular, a framework for cost-effective availability-aware connection provisioning to provide differentiated services in WDM mesh networks is presented. In addition, the emerging problem of protecting low-speed connections of different bandwidth granularities is reviewed. More study is required in designing and operating a survivable WDM mesh network to provide differentiated services and efficiently provide service quality guarantees.

References

[1] M. To and P. Neusy, "Unavailability Analysis of Long-Haul Networks," *IEEE JSAC*, vol. 12, Jan. 1994, pp. 100–09.

[2] G. Ellinas, A. Hailemariam, and T. E. Stern, "Protection Cycles in Mesh WDM Networks," *IEEE JSAC*, vol. 18, Oct. 2001, pp. 1924–37.

[3] S. Ramamurthy, L. Sahasrabuddhe, and B. Mukherjee, "Survivable WDM Mesh Networks," *IEEE/OSA J. Lightwave Tech.*, vol. 21, Apr. 2003, pp. 870–83.

[4] G. Mohan, C. S. R. Murthy, and A. K. Somani, "Efficient Algorithms for Routing Dependable Connections in WDM Optical Networks," *IEEE/ACM Trans. Net.*, vol. 9, Oct. 2001, pp. 553–66.

[5] R. Ramamurthy *et al.*, "Capacity Performance of Dynamic Provisioning in Optical Networks," *IEEE/OSA J. Lightwave Tech.*, vol. 19, Jan. 2001, pp. 40–48.

[6] O. Gerstel and R. Ramaswami, "Optical Layer Survivability – An Implementation Perspective," *IEEE JSAC*, vol. 18, Oct. 2000, pp. 1885–99.

[7] M. Clouqueur and W. D. Grover, "Availability Analysis of Span-Restorable Mesh Networks," *IEEE JSAC*, vol. 20, May 2002, pp. 810–21.

[8] A. Fumagalli *et al.*, "Shared Path Protection with Differentiated Reliability," *Proc. IEEE ICC*, Apr. 2002, pp. 2157–61.

[9] J. Zhang *et al.*, "Service Provisioning to Provide Per-Connection-Based Availability Guarantee in WDM Mesh Networks," *Proc. OFC*, Mar. 2003, expanded version in *ICC*, May 2003.).

[10] C. Ou, H. Zang, and B. Mukherjee, "Sub-path Protection for Scalability and Fast Recovery in Optical WDM Mesh Networks," *Proc. OFC*, Mar. 2002, pp. 495–96.

[11] V. Anand, S. Chauhan, and C. Qiao, "Sub-path Protection: A New Framework for Optical Layer Survivability and Its Quantitative Evaluation," Dept. of Comp. Sci. and Eng., SUNY Buffalo, Tech. rep. 2002-01, Jan. 2002.

[12] J. Wang, L. Sahasrabuddhe, and B. Mukherjee, "Path vs. Subpath vs. Link Restoration for Fault Management in IP-over-WDM Networks: Performance Comparisons using GMPLS Control Signaling," *IEEE Commun. Mag.*, vol. 40, Nov. 2002, pp. 2–9.

[13] J. Zhang *et al.*, "On The Study Of Routing And Wavelength-Assignment Approaches for Survivable Wavelength-routed WDM Mesh Networks," *SPIE Opti. Nets. Mag.*, Nov./Dec., 2003.

[14] J. W. Suurballe and R. E. Tarjan, "A Quick Method For Finding Shortest Pairs of Disjoint Paths," *Networks*, vol. 14, 1984, pp. 325–36.

[15] C. Qiao, Y. Xiong, and D. Xu, "Novel Models For Efficient Shared-Path Protection," *Proc. OFC*, Mar. 2002, pp. 546–47.

[16] L. Sahasrabuddhe, S. Ramamurthy, and B. Mukherjee, "Fault Management in IP-over-WDM Networks: WDM Protection Versus IP Restoration," *IEEE JSAC*, vol. 20, Jan. 2002, pp. 21–33.

[17] A. Fumagalli and L. Valcarenghi, "IP Restoration vs. WDM Protection: is There An Optimal Choice?," *IEEE Network*, vol. 14, Nov./Dec. 2000, pp. 34–41.

[18] C. Ou *et al.*, "Traffic Grooming for Survivable WDM Networks – Shared Protection," *IEEE JSAC*, vol. 21, Nov. 2003, pp. 1367–83.

Biographies

JING ZHANG (zhangj@cs.ucdavis.edu) received a B.S. degree from Peking University, Beijing, China, in 1998 and an M.S. degree from the University of California (UC), Davis in 2001. Currently, she is a Ph.D. student in the Computer Science Department, UC Davis, where she works as a research assistant in the network research laboratory. Her research interests include fault management, algorithm design and performance evaluation, and reliability analysis in optical WDM networks.

BISWANATH MUKHERJEE (mukherje@cs.ucdavis.edu) received a B.Tech. (Hons) degree from Indian Institute of Technology, Kharagpur in 1980 and a Ph.D. degree from the University of Washington, Seattle, in June 1987. At Washington he held a GTE Teaching Fellowship and a General Electric Foundation Fellowship. In July 1987 he joined UC Davis, where he has been a professor of computer science since July 1995, and chairman of Computer Science since September 1997. He is co-winner of paper awards presented at the 1991 and 1994 National Computer Security Conferences. He serves on the editorial boards of *IEEE/ACM Transactions on Networking*, *IEEE Network*, *ACM/Baltzer Wireless Information Networks*, *Journal of High-Speed Networks*, *Photonic Network Communications*, and *Optical Networks Magazine*. He also served as Editor-at-Large for optical networking and communications for the IEEE Communications Society. He served as Technical Program Chair of IEEE INFOCOM '96, and is the author of *Optical Communication Networks* (McGraw-Hil, 1997), which received the Association of American Publishers, Inc.'s 1997 Honorable Mention in Computer Science. His research interests include lightwave networks, network security, and wireless networks.