MULTILAYER PROTECTION AND SURVIVABILITY IN WDM OPTICAL NETWORK

Refat Kibria, Md. Aminul Haque Chowdhury, Md. Ali Ahsan Razib,
Uzzal Shyam and Mustafa Amir Faisal
Department of Computer Science and Engineering
Shah Jalal University of Science and Technology, Sylhet, Bangladesh
E-mail: refat-cse@sust.edu, aminul.babor@gmail.com, razib.ahsan@gmail.com, uzzal_shyam@yahoo.com, mafaisal@gmail.com

Abstract: *Optical networks require a number of security and survivability methods as any other network does. These methods are more important for a WDM network since it carries far greater amount of data than any other network. In the multilayer networking approach, protection mechanism is more technical compared to the non-layered network. To attain high performance and quick recovery, a well-considered coordination between different layers is mandatory. This paper provides an overview of multilayer recovery issues for WDM optical network and also focuses on how these techniques can be applied to make the next generation WDM networks more fault tolerant and survivable.*

Keywords: *OTN, SONET, WDM, ATM, OXC, WXC.*

1. Introduction

WDM is the emerging technology believed to provide the ultimate solution of bandwidth for present and future. It exploits optical fiber's unlimited (approximately) bandwidth. WDM has been a reality for a couple of decades and various implementations (e.g. Broadcast and Select, Point-to-Point, Wavelength Routing) of WDM give network designers opportunity to design cost effective and *fault tolerant* network. Like every network WDM networks are prone to failures of components such as links, nodes, and Wavelength Cross-Connects (WXC). Since these networks carry high volumes of traffic, failures may have severe consequences. Therefore, it is imperative that these networks have the capability of fault tolerance.

Fault tolerance refers to the ability of the network to reconfigure and reestablish communication upon failure. A related term *restoration* refers to the process of rerouting affected traffic on a component failure. A network with restoration capability is known as *survivable* network or a restorable network. It requires redundant capacity or spare resources. Restoration can be provided at the optical path layer or at the higher service layer each of which has its own merits. This layer-wise protection of network is called *Multilayer Protection*. A multilayer transport network typically consists of a stack of single-layer networks. There is usually a client–server relationship between the adjacent layers of this stack. Each of these network layers may have its own (single-layer) recovery schemes. As will be shown in the following sections, it is important to be able to combine recovery schemes in several layers in order to cope with the variety of possible failures in an efficient way and to benefit from the advantages of the schemes in each layer. It is worth mentioning that implementing a multilayer recovery strategy does not necessarily mean that all the recovery mechanisms will be used at every layer. The process of assigning network resources to traffic demand is known as *provisioning* a network. Given a set of demands, the provisioning problem is to allocate resources (wavelength, fibers) to the primary network and the restoration network so as to minimize the capacity required. The capacity is measured in terms of the number of wavelengths for a single-fiber network and number of fibers in a multi-fiber network.

2. Multilayer Protection in WDM Networks

In the backbone network, WDM systems are being widely deployed. A new network layer called the *optical layer* has been introduced into the layered architecture. This layer supports different higher-layer services, such as SONET connections, Asynchronous Transfer Mode (ATM) virtual circuits, and IP-switched datagram traffic. As we know from the layered structure of a network, survivability can be offered at the WDM layer or higher layers. The higher-layer services, such as SONET and ATM, have their own protection mechanisms. Some higher layer services may not have recovery mechanisms incorporated in the protocols. So, the WDM layer should be able to offer survivability. However, at higher layers, WDM layer survivability cannot protect against failures and so we have to provide some survivability 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. Escalation or inter-working strategy is the set of rules describing the point of origination of the fault recovery process and the interaction between the various layers.

There are two escalation strategies which have been proposed [1] based on the layer at which the fault recovery process is initiated. Recovery starts at the layer closest to the failure in the bottom-up strategy, and escalates upward upon expiration of a hold-off timer. Before triggering recovery mechanisms at a higher layer, this timer allows the lower layers time to recover from a fault (if possible). This strategy activates the recovery process very quickly. On the other hand, recovery always starts at the uppermost layer and escalates downward in the top-down strategy. We do not need hold-off timers in this strategy, but a disadvantage is that potentially large number of traffic streams must be restored at the higher layers.

Another strategy starts the recovery process at some intermediate layer and based on the received alarms and survivability statistics escalate either upward or downward. A cost-performance comparison of the escalation strategies, reported in [1] for an ATM-over-synchronous digital hierarchy (SDH) network, found that the bottom-up approach was better in terms of both equipment cost and recovery time. However, a main attraction of the top-down strategy is that it can provide differentiated QoS for survivability to different users. The next sections suggest that WDM layer survivability is desirable. The advantages of providing survivability functionality at the WDM layer are [2, 3]:

- Speed: As the nodes can act quickly upon the occurrence of failures and do not have to wait for higher-layer indication signals, recovery at the WDM layer is much faster.
- Simplicity: It is simple because it needs less coordination than recovery at higher layers.
- Effectiveness: Because of sharing resources among different service layers, Optical restoration makes more efficient use of restoration capacity.
- Transparency: The wavelength routing protection technique does not depend on the protocols used in higher layers.

3. Different Types of Survivability in Optical Networks

3.1 Survivability at the Bottom Layer

In this technique, recovery of a failure is always done at the bottom layer of the multilayer network. For example, this implies that the 1 + 1 optical protection scheme, or any other recovery scheme that is deployed at the OTN layer, attempts to restore the affected traffic in case of a failure in an IP over- OTN network. This strategy has the benefit that it treats only a simple root failure and that the number of required recoveryactions are minimal (the recovery actions are performed on the coarsest granularity). Before triggering any recovery action, failures do not need to propagate through multiple layers. It cannot handle problems that occur due to failures in a higher network layer. If a node failure occurs in the OTN layer [such as an optical-cross-connect (OXC) failure], the OTN-layer recovery mechanism will only be able to restore the affected traffic that transits the failed bottom-layer node (being the OXC). Due to the failure of the OXC underneath, the collocated higher-layer IP router will become isolated. So, in the lower (optical) layer all traffic treated by this IP router cannot be restored. We have illustrated this in the example of Figure 1. In this paper, top-level nodes are represented in lower case and the bottom-layer nodes are represented in upper case.

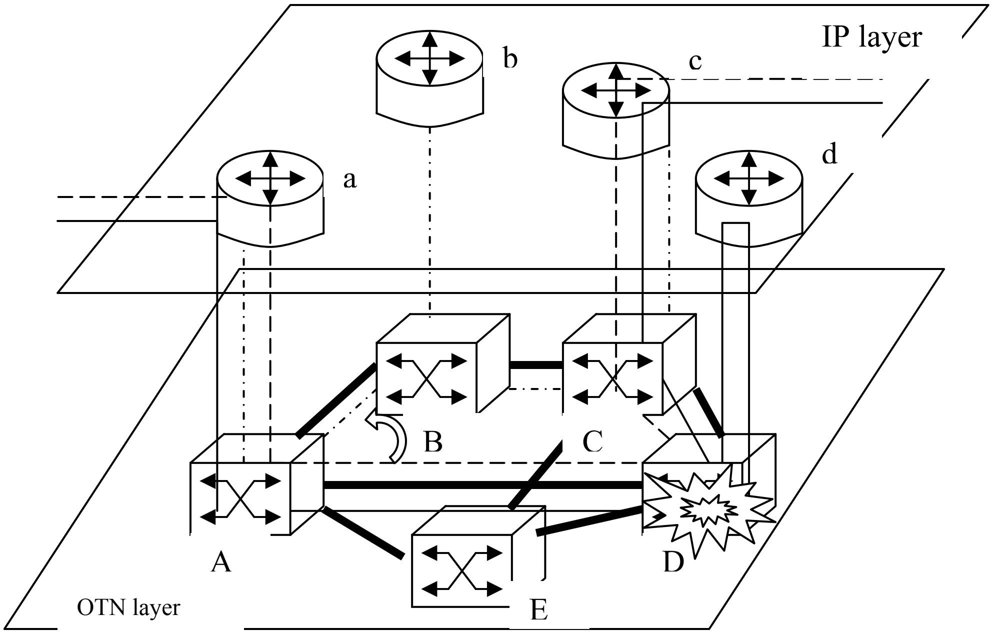


Figure 1. Survivability at the bottom layer.

There are two traffic flows between client-layer nodes *a* and *c* in this network. One traffic flow (*a–d–c*, indicated with a full line) transits the client-layer node *d* (using links *a–d* and *d–c*), while the other traffic flow (*a–c*, indicated with a dashed line) uses a direct logical link from *a* to *c* and only transits the server-layer node D. Now we consider a failure being occurred in the bottom layer at node D. We see that the server layer cannot recover the first traffic flow *a–d–c*. The client-layer node *d* is isolated because of the failure of D. And this terminates both logical links *a–d* and *d–c*. At the higher layer, this failure can only be resolved. However, over a direct logical link between nodes *a* and *c* the second traffic flow *a–c* is routed. This logical link transits only the failing node D in the bottom layer. And in this way this traffic flow (dotted line in Figure 1) can be restored by the bottom-layer recovery scheme.

3.2 Survivability at the Top Layer

There is another strategy which provides survivability in a multilayered network. It provides the survivability at the top layer of the network. In the example of an IP-over-OTN network, this could be the IP restoration technique or MPLS-based restoration (see [4] for a detailed overview of IP and MPLS recovery techniques). It can also cope with higher-layer failures which are the main advantages of this strategy. The prime disadvantage of this strategy is that it requires a lot of recovery actions, because of the finer granularity of the flow entities at the top layer. As a consequence of a single root failure in the lower layer, in the higher network layer a complex scenario of secondary failures is typically induced. This is illustrated in Figure 2, where the failure of an optical link in the bottom layer corresponds with the simultaneous failure of three logical IP links in the top layer. Hence, these three logical IP links are part of a shared risk link group

(SRLG) [5]. This implies that the recovery scheme in the top layer will have to recover from three simultaneous link failures which is a quite-complex failure scenario. This is in clear contrast with a recovery scheme at the bottom layer that would only have to cope with the simpler scenario of a single link failure. Another disadvantage of a recovery at the top layer only is that the traffic injected directly in the lower layer cannot be recovered by the optical-network operator, even if the failure happens in the optical layer itself.

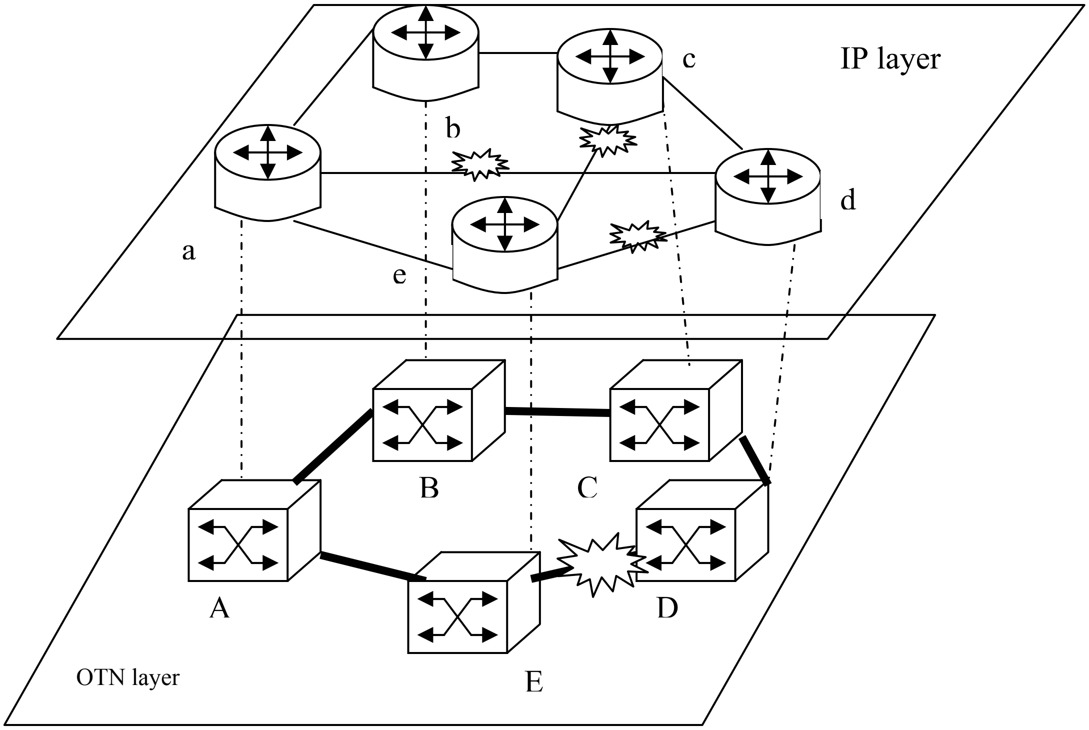


Figure 2. Survivability at the top layer.

3.3 Variants

A different variant on the strategy is the survivability at the lowest detecting- layer strategy. It applies survivability at the bottom layer. The lowest detecting layer is the lowest layer in the layered network hierarchy which is able to detect the failure. Multiple layers in the network will now deploy a recovery scheme using this method, but recovery actions are taken by the (single) layer that detects only the root failure. With this strategy, the problem of the bottom layer recovery scheme not detecting a higher-layer failure is avoided, because the higher layer will detect the failure and will recover the affected traffic. However, this strategy requires that we determine which layer is the lowest detecting layer (to avoid the condition where higher layers also react upon a lower-layer failure). Moreover, it cannot restore any traffic transiting higher layer equipment isolated by a node failure in the layer below. By using this strategy, the client layer in the example (Figure 1) will deploy a recovery scheme, but the considered traffic flow *a–d–c* is still lost since this client-layer recovery scheme is not triggered by the occurrence of the node failure in the server layer. Therefore, it is still considered as a single layer survivability strategy in a multilayer network although this strategy considers the deployment of recovery schemes in multiple layers due to the fact that the responsibility to recover all traffic is situated in only one layer (being the lowest one detecting the failure) for each failure scenario. Another strategy is the survivability at the highest possible layer strategy that offers survivability at the top layer. As not all traffic have to be injected (by the customer) at the top layer, with this strategy, a traffic flow is recovered in the layer in which it is injected; in other words, the highest possible layer for this traffic flow. This means that this highest possible layer is to be determined on the basis of per-traffic-flow. For providing survivability in a multilayer network this survivability at the highest-possible layer strategy is also considered as a single-layer survivability strategy. But recovery schemes in multiple layers are considered by it. And we know the recovery schemes in multiple layers will never recover the same traffic flow. Actually, for each traffic flow this strategy deploys the survivability at the top layer strategy individually.

4. WDM-Layer Protection

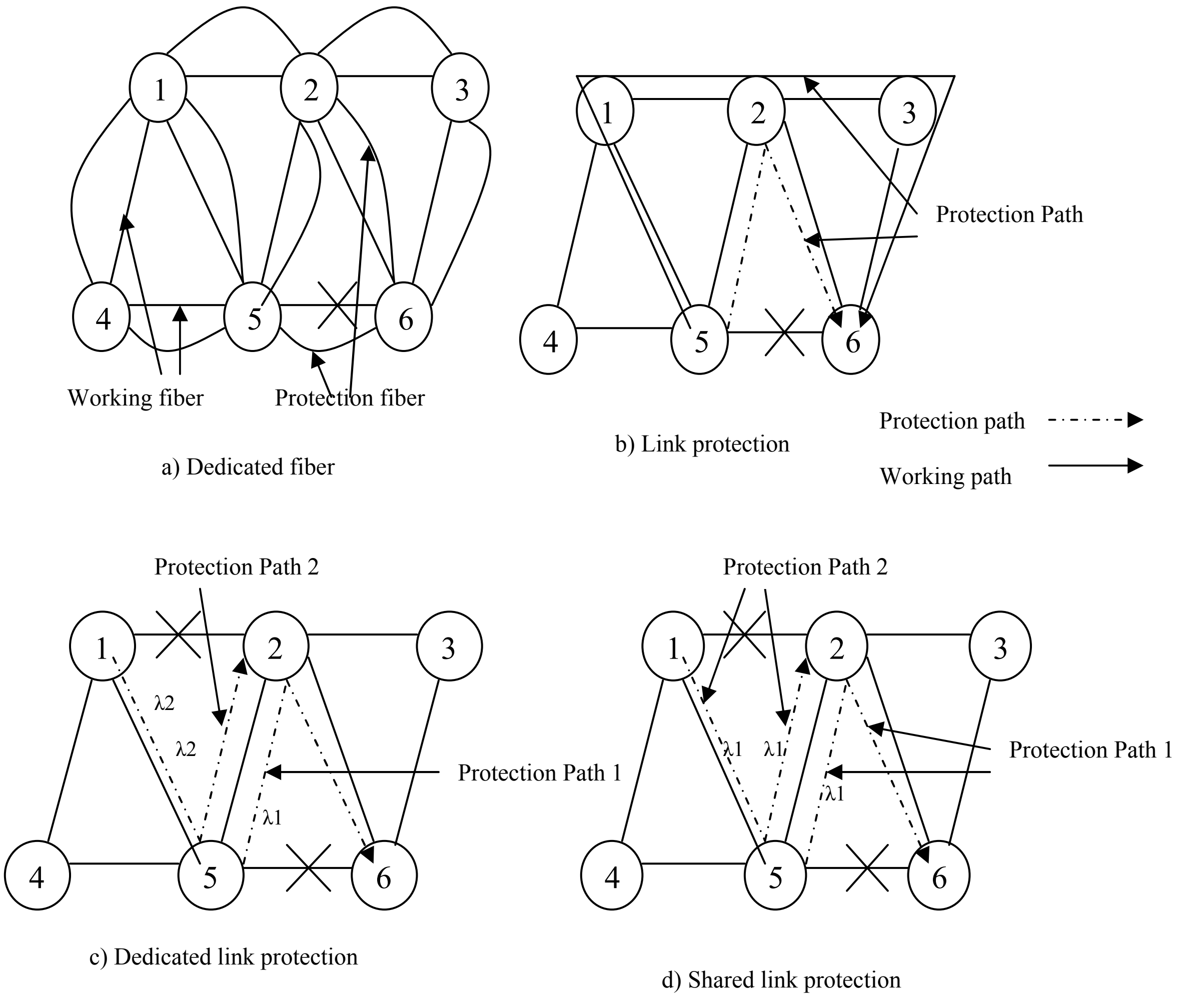
The ideas used in WDM-layer protection are very similar used in SONET systems. The main reason for this is that WDM technology has been used to upgrade the existing optical networks, thus keeping the network topologies largely unchanged i.e. for minimum number of change. It is natural to find protection schemes similar to existing techniques and use them in the upgraded networks. For example, in point-to-point WDM systems, 1 + 1, 1:1, and 1:N optical protection are used in a way similar to APS in SONET systems, except that switching is done in the optical domain. Here the difference is in the electronic and optical switching capability. WDM SHR (Self healing ring) architectures also operate along the same lines as SONET SHRs. In WDM systems, we have multiple wavelengths and so the protection and restoration methods are more easy, flexible and compact. 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. For example, if the BSHR/2 architecture is used in *WDM* systems, the wavelengths used for protection have to be chosen carefully to avoid wavelength conversion in the nodes, because of high cost of wavelength converter. The wavelengths used on the two rings can be chosen to overlap (i.e., some wavelengths are used as working channels on both rings) or non-overlapped (i.e., the wavelengths used as working channels on one ring are not used as working channels on the other ring). Non-overlapped wavelength assignment has the advantage that when a failure occurs, the nodes doing loopback do not have to deal with wavelength conversion, because the affected channels can always use the same wavelengths reserved for them on the other ring.

As WDM system deployment advances beyond the upgrading of existing non-WDM systems, mesh topologies using optical cross-connects (OXCs) are likely to emerge. In such situations, protection can be provided by the OXCs, much like DCSs in SONET networks. Most of the studies so far have considered only single-link failures. 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. In the following, we will survey the different schemes used for single-link failure recovery.

Considering the single-link failure scenario in mesh networks, a simple way to provide survivability is the dedicated fiber scheme. Here each link in the network has its dedicated backup link. Upon a link failure, traffic is simply routed over its backup link, as shown in the example of Figure 3a in which the link between nodes 5 and 6 has failed. Because most link failures are due to fiber cable cuts, the backup fiber is required to be diversely routed. This is a complicated task for network design and realization, and is obviously a waste of capacity and also concern of cost. Pre-designed protection schemes are by far the most studied for WDM optical networks. Because of the multi-channel traffic, the design algorithms used in a WDM network are more complicated compared to those used in non-WDM systems.

There are two main pre-designed protection techniques against single-link failures in WDM networks. They are:

- Link-based protection
- Path-based protection.



a) Dedicated fiber

b) Link protection

c) Dedicated link protection

d) Shared link protection

Figure 3. Link-based protection

4.1 Link-Based Protection

The basic idea of link-based protection is that a protection path is reserved for each link, and when the link fails, traffic is rerouted (looped back) around the failed link. As an example, in Figure 3b, after a link failure between nodes 5 and 6, the affected traffic is rerouted through the backup path 5–2–6. Here, the end nodes of the failed link (i.e., nodes 5 and 6) are responsible for recovery.

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-based protection, each working channel has a protection wavelength path (a path with one wavelength’s worth of capacity). The protection wavelength paths used for different working wavelengths on the same link may use different paths and/or different wavelengths. For example, Figure 3b shows two different protection paths (5–2–6 and 5–1–2–3–6) for the same link 5–6. Link-based protection schemes can be further classified as dedicated or shared link protection.

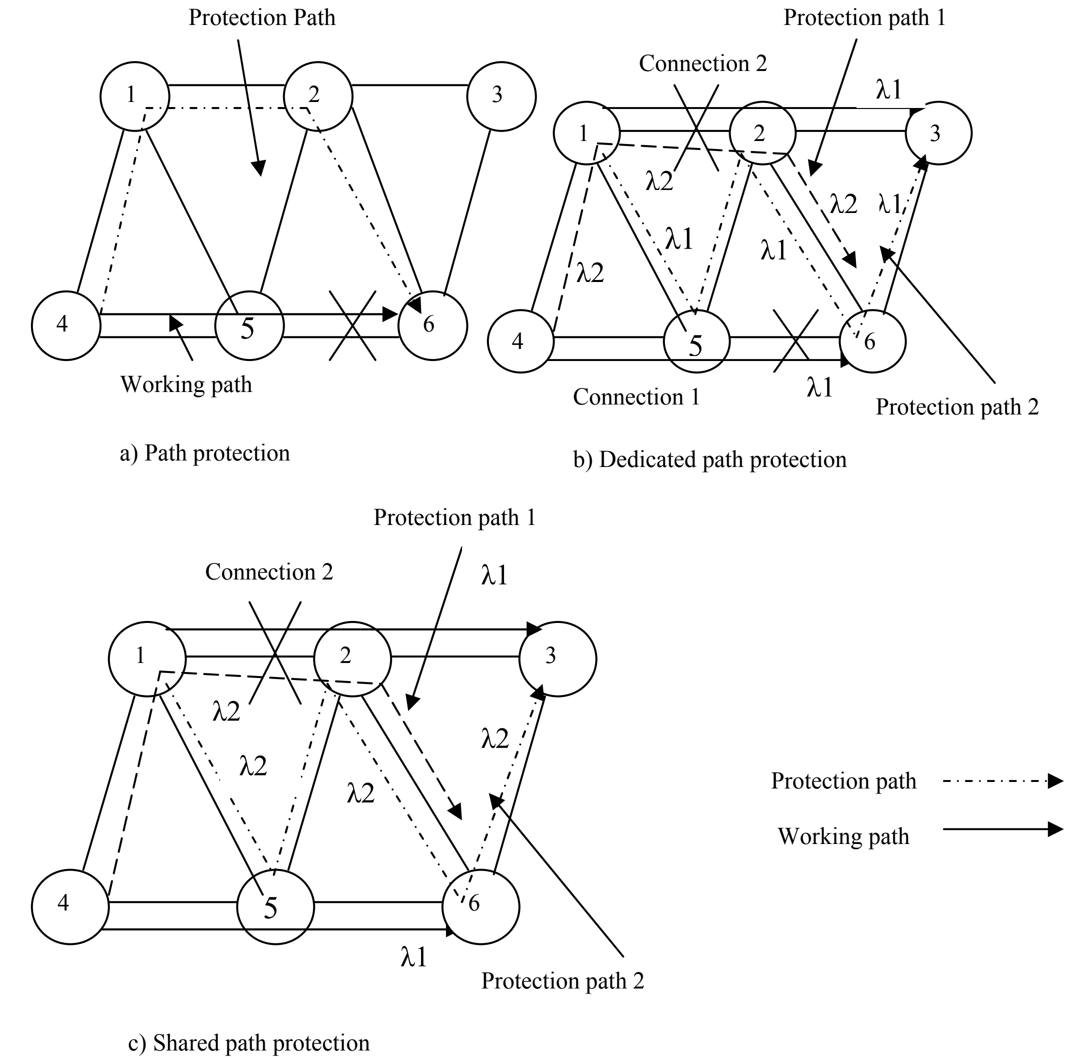
Dedicated link protection means that a protection wavelength path is dedicated to a working channel on a particular link. Therefore, if the protection paths for (some wavelengths on) two different links overlap, different wavelengths must be assigned to the protection path on the overlapping portion even if the working wavelengths on the two links are the same. As an example, consider Figure 3c. Let λ_1 on path 5–2–6 (labeled protection path 1) be the protection wavelength path for a working channel on link 5–6, and the protection path for a working channel on link 1–2 be 1–5–2 (labeled protection path 2). Then a different wavelength, say λ_2, must be assigned to protection path 2, even if the working wavelengths on links 5–6 and 1–2 are the same, say λ_1. Note that this requires wavelength conversion if link 1–2 fails. This example indicates the difficulty in designing efficient protection schemes in large networks. Efficient design is especially difficult if wavelength conversion facilities are unavailable. On the other hand, dedicated link protection may offer protection against the failure of multiple links. For example, in Figure 3c both working channels can be recovered if both links 1–2 and 5–6 fail simultaneously. However, note that recovery of working channel 5–6 is not possible if both links 5–2 and 5–6 fail at once.

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. Figure 3d shows an example of shared link protection. Protection paths 1 and 2 (used to protect a working channel on links 5–6 and 1–2, respectively) can share wavelength λ_1 on link 5–2. Note, however, that a different wavelength must be used to protect a different working channel on link 5–6 if protection path 1 is used for that working channel.

4.2 Path-Based Protection

In WDM systems, path-based protection refers to the reservation of a protection path and wavelength (protection wavelength path) for each working wavelength path and each link failure. Upon failure of a link, the source and destination nodes of each affected connection switch to the corresponding protection wavelength paths. As opposed to link-based protection, which involves only the nodes adjacent to the link failure, path-based protection needs a mechanism to notify the affected connection end nodes of the failure. This requires the cooperation of several network nodes, and may not be easily achievable. The protection wavelength paths for every link failure are usually reserved at connection setup, and should be disjoint with the failed link. Upon link failure, the wavelength paths reserved for this failure scenario are activated. As a special case, when a protection wavelength path is disjoint with every link of the working path, the same wavelength path can be used to restore a connection upon any single-link failure along the working path. Note that in this case, the identification of the failed link is not required to initiate recovery. An example of the special case is shown in Figure 4a, where the working path is 4–5–6. When the link between nodes 5 and 6 fails, nodes 4 and 6 switch the connection to the protection path 4–1–2–6. The wavelength used on the protection path can be the same as or different from the working wavelength. Also, the protection paths used for different connections using the same working path can be different. Similar to link-based protection, path-based protection can be dedicated or shared.

In *dedicated path 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. For example, Figure 4b shows two working paths, 4-5-6 and 1–2–3, both using λ_1. The protection wavelength path for connection 1 is λ_2 on 4–1–2–6 (λ_1 is a working wavelength on link 1–2 and cannot be used for protection). The protection wavelength path for connection 2 is 1–5–2–6–3. Since these two protection paths have the common link 2–6, and λ_2 is assigned to protection path 1, protection path 2 has to be assigned a different wavelength (e.g., λ_1). 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. The positive aspect is that 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. Thus, it is possible to utilize the capacity more efficiently, while still achieving 100 percent recovery from



a) Path protection

b) Dedicated path protection

c) Shared path protection

Figure 4. Path-based protection

single-link failures. An example of shared path protection is given in Figure 4c. The two backup paths can now share λ_2 on link 2–6. Therefore, only one wavelength on this link has to be reserved for protection, as opposed to two for dedicated path protection.

5. Concluding Remarks

A network cannot be complete if it is not fault tolerant and restorable. These are serious drawbacks of an optical network since a failure may force a network to be in disjoint parts. For WDM network the reconfiguration due to the failure of a component is flexible because of multiple channels but at the same time is complicated due to wavelength assignment constraints. However this is not a big deal for the networks where the techniques discussed above are implemented properly. We believe that future optical networks will be more error free, fault tolerant as well as restorable and hopefully we will be able to meet the ever-increasing bandwidth requirement in the generations to come.

References

[1] P. Demeester *et al.*, “Resilience in Multilayer Networks,” *IEEE Commun. Mag.*, vol. 37, no. 8, Aug. 1999, pp. 70-76.

[2] O. Gerstel, R. Ramaswami, and G. H. Sasaki, “Fault Tolerant Multiwavelength Optical Rings

with Limited Wavelength Conversion," *IEEE JSAC*, vol. 16, no. 7, Sept. 1998, pp. 1166–78.

[3] O. Crochat and J. Y. Le Boudec, "Design Protection for *WDM* Optical Networks," *IEEE JSAC*, vol. 16, no. 7, Sept. 1998, pp. 1158–65.

[4] J. P. Vasseur, M. Pickavet, and P. Demeester, *Network Recovery,* San Francisco, CA: Morgan Kaufmann, 2004.

[5] D. Papadimitriou *et al.*, "*Shared Risk Link Groups Encoding and Processing*", June 2002, http://www.ietf.org.

[6] ITU-T Recommendation G.807/Y.1302, "*Requirements for automatic switched transport networks (ASTN)"*, Geneva, Switzerland, ITU-T Standardization Org., July 2001, http://www.itu.int.

Refat Kibria, born in 1981, an Electrical and Electronic Engineer, graduated from Islamic University of Technology, Dhaka, Bangladesh, in 2003.

He is now working as a lecturer of Department of Computer Science and Engineering, Shah Jalal University of Science and Technology and his research interest includes WDM Networks, Dynamically Reconfigurable WDM Networks, IP over WDM and Wireless Networks etc.

Md. Aminul Haque Chowdhury completed his Graduation in Computer Science and Engineering from Shah Jalal University of Science and Technology, Sylhet, Bangladesh, in 2006.

Currently Aminul is the Supervisor of Network Operations Center (NOC) support team of Data Tech Labs, Latvia. He was a regular contestant of ACM UVA and solved lots of Algorithmic and Mathematical problems. He was also a regular contestant of CSE SUST, and ranked top in a number of occasions in his undergraduate career. His primary interests are optical communications and WDM systems, Artificial Intelligence, fiber optic communications, RFID, Networking, and Database systems.

Md. Ali Ahsan Razib received the BSc. Engineering degree from Shah Jalal University of Science and Technology, Sylhet, Bangladesh, in 2006, in Computer Science and Engineering.

Currently, he is an Executive in Research and Development in Synchronous ICT, Sylhet, Bangladesh. Being top ranked among the batch in his undergraduate career, he has always been eager to contribute to the optical communications industry. Therefore he conducted his undergraduate thesis on Wavelength Division Multiplexed (WDM) Systems. He has also written a paper proposing necessary protocols for survivable wide area network architecture. His current research interests include WDM architecture and protocols, optical components, and protection and survivability techniques.

Uzzal Shyam received the B.Sc. Engineering degree from Shah Jalal University of Science and Technology, Sylhet, Bangladesh, in 2006, in Computer Science and Engineering.

He pursued his undergraduate research on Fiber optic based Wavelength Division Multiplexing (WDM) Technology with a view to have a significant contribution to the telecommunications arena. His written research papers also have focus on optical communications and wide area WDM networks. He is interested to research in Networking and Communications sectors, especially in WDM networks and survivability concepts.

Mustafa Amir Faisal received the B.Sc. Engineering degree from Shah Jalal University of Science and Technology, Sylhet, Bangladesh, in 2006, in Computer Science and Engineering.

Currently, he is a Software Support Engineer in REVE Systems, Dhaka, Bangladesh. His current research interests include Telecommunications, WD M systems, and software engineering.