IP Over WDM Network Control: Network Addressing and Restoration

Refat Kibria[1] and Syed Reza[2]
[1]Department of Computer Science and Engineering, Shah Jalal University of Science & Tech., Bangladesh
[2]HUAWEI Technologies, Bangladesh

Abstract: *There are some common network control issues in IP over WDM(IP/ WDM) which includes network addressing, neighborhood discovery, routing behavior, connection setup and tear down, signaling mechanism, network access control and IP/ WDM protection and restoration. Among them network addressing and restoration are two major research area. In this paper these two issues have been discussed. This paper also contains two different case studies based on lightpath provisioning and segment restoration.*

Keywords: *Optical cross-connector, shared-risk link group, open shortest path first, link state advertisement, label switched path, resource reservation protocol.*

Received June 15, 2006; accepted June 13, 2007

1. Introduction

IP/ WDM network is designated to transmit IP traffic in a WDM-enabled optical network to leverage both IP universal connectivity and massive WDM bandwidth capacity. Combining IP and WDM means, in the data plane, one can assign WDM optical network resources to forward IP traffic efficiently, and in the control plane, one can construct a unified control plane, presumably IP-centric, across IP and WDM networks. IP over WDM will also address all levels of interoperability issues on intra- and inter-WDM optical networks and IP networks.

For interoperability across IP-centric WDM networks, a fundamental issue is addressing. Possible addressing entities in WDM networks include switch interface, wavelength ports, optical links, physical fibers, and optical channels (wavelengths). The issue here is how granular the identification should be as far as network control is concerned [1, 2].

Another important network operational issue is restoration that aims at a resilient network providing network survivability. Restoration can be implemented in two fashions, provisioned and non-provisioned. Provisioned restoration is also known as protection. Protection copes with predetermined failure recovery since protection resources are reserved beforehand. It can be used by low priority traffic if pre-emption is allowed. Non-provisioned restoration deals with dynamic discovery of alternate routes from the spare network resources for disrupted traffic once the failure is detected.

Section 2 of this papers presents a brief discussion on network addressing in particular overlay addressing and peer addressing scheme. Section 3 contains the presentation of IP/ WDM restoration technique. It also includes two different case study based on lightpath provisioning and subnet segment restoration.

2. IP/ WDM Network Addressing

It is unreasonable to assume that every wavelength channel or termination port should have a unique IP address. Also, the routing of a lightpath within the WDM network may not depend on the precise termination point information, but rather on the terminating Optical Cross-Connector (OXC) [3]. This suggests an identification scheme whereby OXCs are identified by a unique IP address, and a selector identifies further fine-grain information of relevance at an OXC. This, of course, does not preclude the identification of these termination points directly with IP addresses (with a null selector). The selector can be formatted to have an adequate number of bits and a structure that expresses port, channel, and other identifications.

Another entity that must be identified is the Shared-Risk Link Group (SRLG). An SRLG is an identifier assigned to a group of optical links that share a physical resource. For instance, all optical channels routed over the same fiber could belong to the same SRLG. Similarly, all fibers routed over a conduit could belong to the same SRLG. The notable characteristic of SRLG is that a given link could belong to more than one SRLG, and two links belonging to a given SRLG may individually belong to two other SRLGs.

Finally, optical link between adjacent OXCs may be bundled for advertisement in a link state protocol. The component links within the bundle must be identifiable. In concert with SRLG identification, this information is necessary for correct (protection) path computation.

Address translation in an overlay IP/ WDM addressing is likely to become a performance bottleneck. So far, the main reason for using IP address in the WDM layer is to leverage the control mechanisms such as routing and signaling protocols developed in the IP environment. To support a common, peer control plane, both IP over WDM networks need to have global IP addresses.

2.1. **Overlay Addressing**

An overlay IP/ WDM network can use IP addresses in the IP and the WDM layer, but these addresses in different layers are not visible to each other. WDM layer IP addresses can be considered as an example of layer 2 addresses [4]. As such, there is a need for address resolution between IP layer addresses and WDM layer IP addresses. Deploying IP addresses in the WDM layer enables the use of IP control protocols. The IP layer can be controlled by an IGP protocol. The WDM layer can be controlled by the Open Shortest Path First (OSPF) protocol with WDM extensions. This also implies that although both IP over WDM layer may use OSPF, the IP OSPF and the optical OSPF are separate OSPF instances.

Figure 1 shows the IP layer addressing in IP/ WDM networks, where there are four IP routers, each with two point-to-point interfaces and one ethernet interface. In IP working over reconfigurable WDM networks, the old lightpath topology needs to be migrated to the new
lightpath topology. However, conventional IP topology is static and a network convergence takes time. In addition, dynamic IP topology reconfiguration (such as changing IP interface addresses) may have impact on network stability and cause packet drop [5, 6]. An alternative to dynamically assigned IP addresses is pre-assigning multiple IP addresses to one interface. Different IP addresses for the same interface from different IP subnets, but only one IP subnet is active at a time.

In the WDM layer, the control channel is separated from the data channel as shown in Figure 2 an out-of-band channel is used to transport the control messages. The data channel represents the data plane WDM network, where the WDM Network Element (NE) interfaces can use physical addresses. The IP addressed control channel carries the corresponding WDM link information. A control channel is related to one or more data channel links between a pair of neighboring switches. A link group identified by a link group ID can be formed by links according to the following criteria:

- Links having the same set of SRLGs.
- Links having the same encoding format, for example, OC-192.
- Links having the same protection type, for example, 1+1.

Link bundling saves IP address, which in turn reduces the number of routing adjacencies between neighboring nodes. The data channel's link state information is flooded in the control channel using OSPF in the format of an opaque Link State Advertisement (LSA).

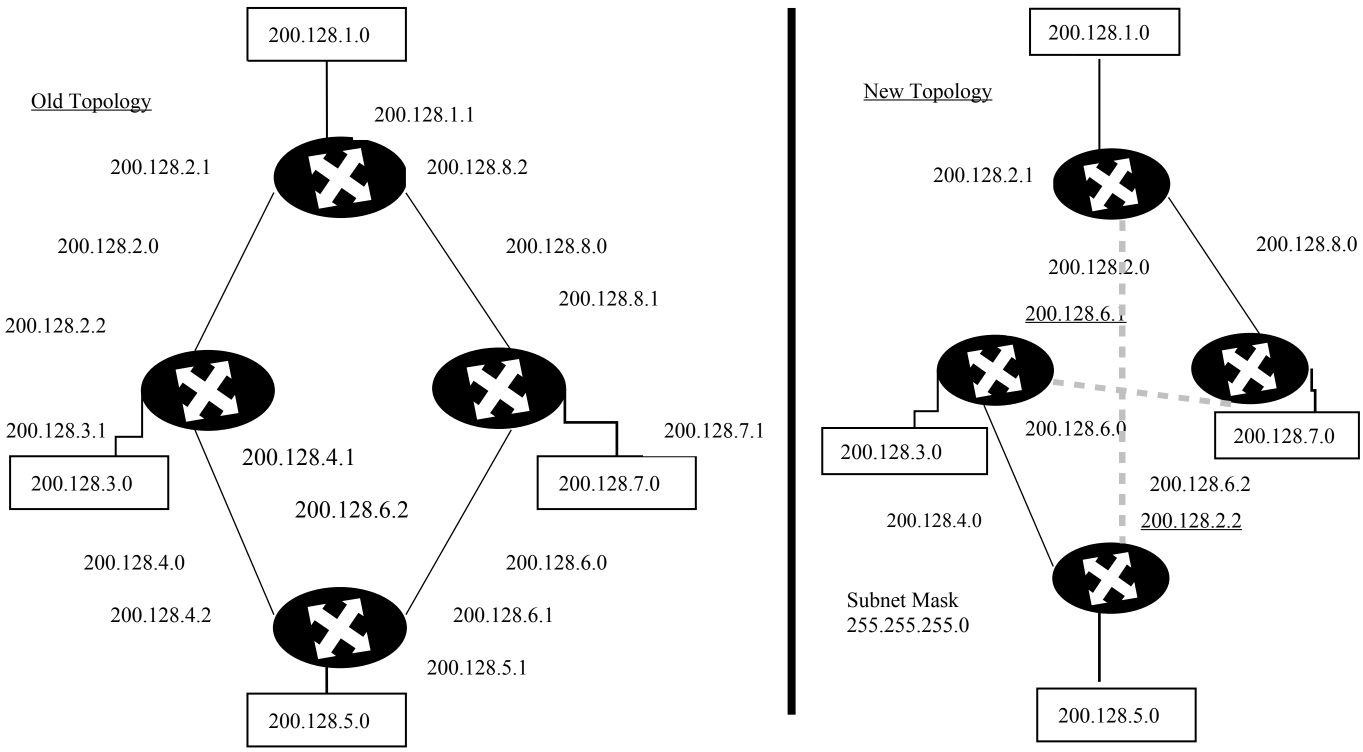

Figure 1. IP layer addressing in an IP over reconfigurable WDM network.

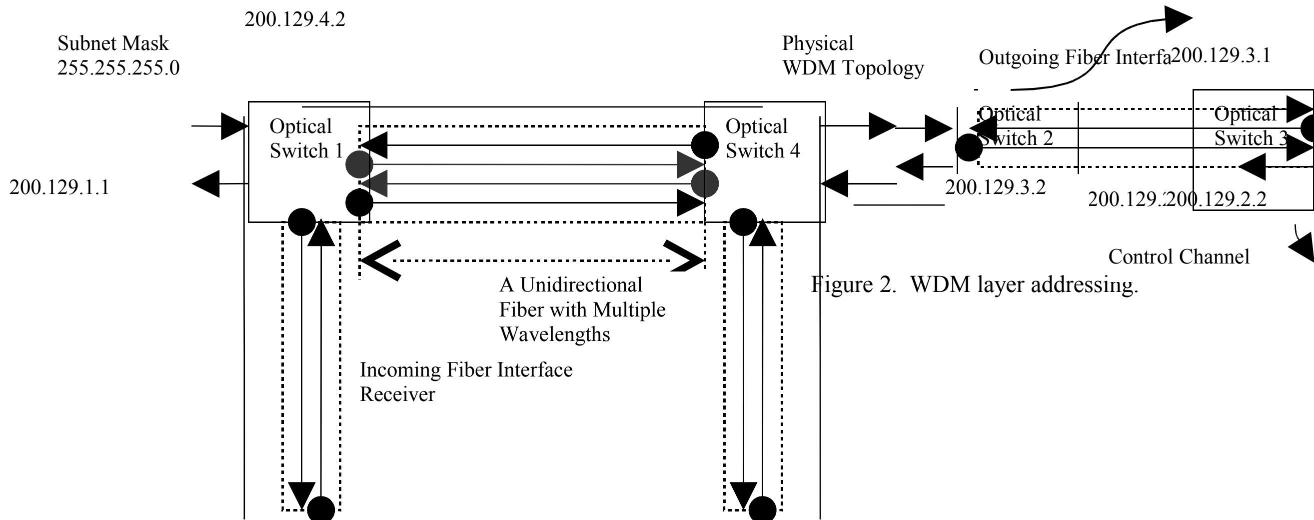

Figure 2. WDM layer addressing.

An IP link in the data channel is associated with one bi-directional wavelength channel. The WDM layer IP address can be assigned to the outgoing WDM link to its neighbor switch. The WDM layer control channel is assigned with IP addresses, as shown in Figure 2. There are four optical switches interconnected by WDM links. The data channel information is associated with the control channel and transported over the control channel. This kind of addressing is suitable for IP over a reconfigurable WDM network in which there is no data plane IP function in the WDM layer.

2.2. Peer Addressing

IP working over reconfigurable WDM can also foster a peer model in the control plane in which WDM layer IP-addressed switches are peers to IP layer routers. Since reconfigurable WDM can only support circuit switching, there is no need to support IP functions in the WDM data plane. WDM layer IP addressing is the same as the overlay addressing except that the WDM address has a peer-to-peer relationship to an IP network address. The WDM layer can employ the link building to assign a pair of IP addresses to the link between neighbor switches.

IP over switched WDM always supports peer addressing in the control plane. An IP over an OLSR network has an independent data-forwarding plane that is different from the IP destination-based forwarding. Hence, an OLSR network may not implement the IP data plane functions. This implies, from a data plane point of view, IP working over switched WDM still forms an overlay network. IP over OPR forms a peer network between IP and WDM networks in both the control plane and the data plane. In all cases, link bundling is used to save IP addresses and reduce routing adjacencies.

3. IP/ WDM Restoration

In a multi-layered IP/ WDM network, restoration can be provided either in a single layer or in a coordinated fashion among different layers. Lower layer protection uses primitive protection scheme, such as automatic fiber switching in SONET, whereas higher layer restoration aims at service level restoration.

Figure 3 shows several types of IP/ WDM restoration. In the WDM-D network in the Figure, each fiber link is protected by a backup fiber in the ring. This type of fiber protection needs only a simple network control and management mechanism and provides fast restoration, for example, less than 50 ms. However, this approach has low utilization as only 50% of the network capacity is used for the traffic. Another type of IP/ WDM restoration is path protection/ restoration [7], which is more bandwidth-efficient but slower in terms of restoration time. Path restoration is enforced by the Network Management System (NMS) either as user requested or as QoS mechanisms provided by the network. In a WDM network, path protection can be offered in a finer granularity, i.e., the lambda (λ) channel. In IP/MPLS/ WDM networks, path protection can be designed for virtual channels.

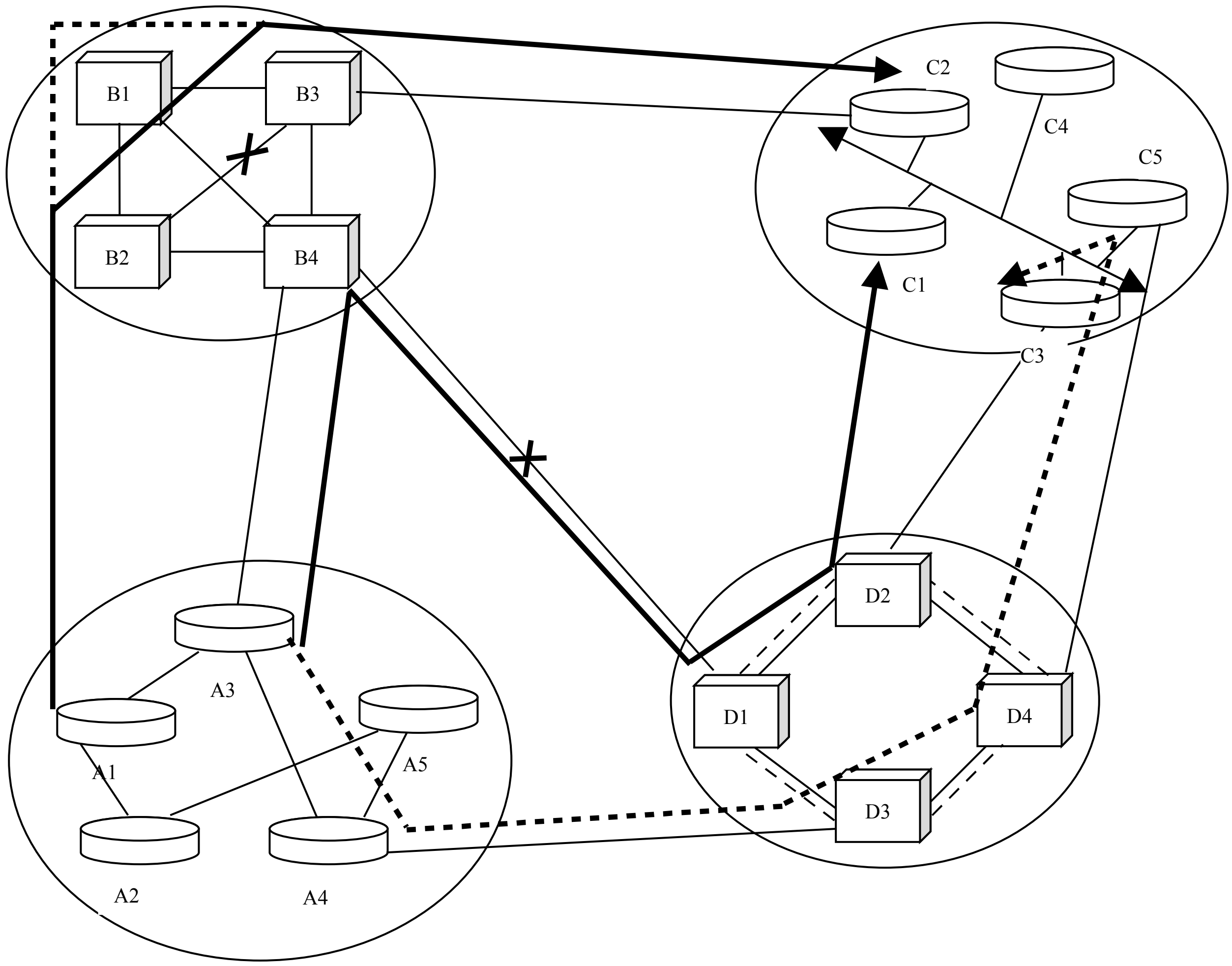

Figure 3. IP/WMD Restoration.

In principle, dynamic restoration can be applied to sub-wavelength channels or very fine-granularity virtual channels, but that level of restoration usually generates a significant amount of control traffic and therefore hinders its 'real time' performance and subsequently scalability. Path protection/ restoration has three variants:

- Link protection restoration: in link protection, a dedicated link disjoint backup route is set up in advance during the lightpath or Label Switched Path (LSP) creation process for the primary link. In case of link failure, once its adjacent nodes detect it , the upstream node switches to the backup path if there is a protection path or dynamically computes a route to replace the damaged link. LSP1 in Figure 3 shows an example of link restoration.
- Lightpath or LSP protection/ restoration*:* when a link failure is detected, its adjacent nodes notify the ingress and egress nodes of the lightpaths of LSPs traversing the failed link. The ingress and egress nodes either use the provisioned end-to-end backup path or compute a new end-to-end path based on the current network capacity and condition. Once the backup path is established, the ingress and egress nodes switch from the failed primary path to the backup path. A special kind of lightpath restoration is disjoint-link path restoration, which is designed for multiple simultaneous failures on the primary path. LSP 2 in Figure 3 shows an example of disjoint-link LSP restoration.
- Partial protection/ restoration*:* partial protection/ restoration provides restoration for a segment of the entire path or several links. In terms of protection scope, it is in between link and lightpath restoration.

Path protection can use dedicated paths or shared paths. Both 1+1 and 1:1 have dedicated protection paths, whereas 1:N and M:N employ shared protection paths. The computation of a primary route for a lightpath within a WDM network is essentially a constraint-based routing problem. The computation of a backup path is essentially a disjoint path problem. In terms of graph theory, there are two levels of disjoint: (1) Link disjoint and (2) Node disjoint. A path traverses a set of nodes. If there is no single node common to the two

wavelengths on each unidirectional fiber. Each link on the figure represents a bidirectional fiber. Let us also assume that all the wavelength channels on a fiber link

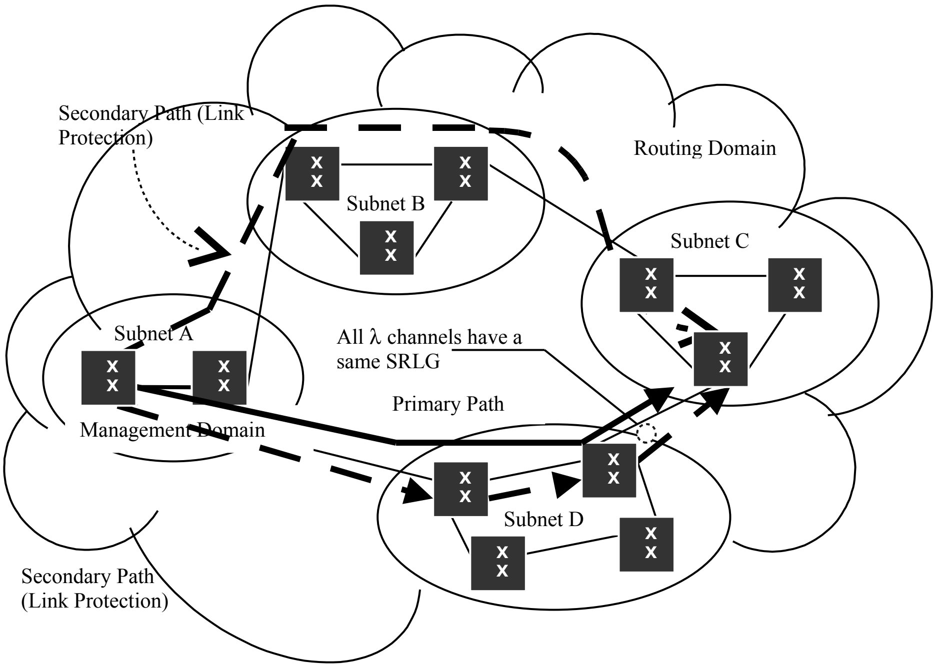

Figure 4. Light path protection vs. link protection.

have a same SRLG.

nodes sets each of which is traversed by a path, these two paths are node disjoint. Obviously, node disjoint is more diverse than link disjoint.

The primary path can be computed first, and the backup is computed next based on the SRLGs chosen for the primary path. The primary path computation procedure can output a series of link group's that the path is routed over. Since a link group is uniquely identified with a set of SRLGs, the alternate path can be computed right way based on this knowledge. However, if the primary path setup does not succeed for a lack of resources in a chosen link group, the primary and backup paths must be recomputed. In another case, if the backup path setup does not succeed for lack of resources under the SRLGs constraint, the primary, and consequently the backup path, may be recomputed.

3.1. Provisioning Case Study

Figure 4 shows an example of lightpath provisioning and link provisioning. The Figure uses an IP-centric control plane in which each switch is IP addressed and controlled by OSPF and ReSource reserVation Protocol (RSVP) [8]. With respect to routing, the switches are grouped into sub-networks, for example, according to geographical locations. Each subnet has an Element Management System (EMS). The crown network is managed by a Network Management System (NMS). Although network control can be purely distributed, it is reasonable to assume that network management is hierarchical. There are 8

In the case of lightpath protection, NMS receives a connection request from a client, decides the protection scheme (for example, 1+1, 1:1, 1-1), and notifies the edge switch for path setup. The notation '1-1' is used to refer to a secondary path which is computed but the secondary path is not signaled. The edge switch computes the end-to-end primary and secondary path based on its local routing table maintained by OSPF, and signals the primary (and secondary if 1+1 or 1:1 protection) lightpath setup using RSVP.

If failure occurs on the primary path during 1:1 transmission, the edge switch will switch over to the secondary path. If the 1-1 protection scheme is implemented, the secondary path needs to be signaled before data can be transmitted.

In the case of link protection, NMS receives a connection request, decides the protection scheme, and notifies the edge switch for path setup. The edge switch computes the end-to-end primary path and the first hop secondary path, and signals the primary path setup using RSVP. Hop by hop, the secondary path is computed. If the 1:1 protection scheme is requested, each hop is also responsible for its secondary path segment setup using RSVP. If failure occurs on the primary path during transmission, the intermediate switch to the failure spot will switch over to the secondary path segment. If the 1-1 protection scheme is implemented, the secondary path segment needs to be signaled before data can be transmitted. Note in our example in the Figure the link protection secondary path computation does not take into account SRLG.

3.2. Restoration Case Study

Figure 5 shows an example of subnet segment restoration and network restoration. For subnet segment restoration, the primary path is computed and set up by the edge switch. There is no secondary path signaled or computed. Once failure occurs on a subnet of the primary path, the intermediate switch to the failure link is responsible for computing and signaling a secondary path dynamically. In the absence of active fault management mechanisms in IP/ WDM networks, RSVP will detect the failure. This is shown in the Figure as event 1-subnet fiber cut. The intermediate switch consults its local routing table, computes a disjoint path based on SRLG, and signals the disjoint path using RSVP. Then, it consistency, it sends an alarm to NMS once the fiber cut is detected and sends a notification to NMS once the switchover is performed.

For network restoration, the primary path is computed and signaled first. If failure occurs on a segment of the primary path, using RSVP, the failure information (including its affected SRLG) is revealed to the edge switch. Then, the edge switch decides a secondary path, signals the path, and performs switchover to the path. The edge switch should also send an alarm and a notification to NMS for courtesy. This is shown in the Figure as event 2- network fiber cut. Once the edge switch receives the RSVP failure message, it computes and sets up a secondary end-to-end lightpath.

4. Concluding Remarks

This paper has represented the structure of network addressing and protection and restoration in IP/ WDM network. In order to clarify the concepts, two different case studies based on light path along with link provisioning and subnet segment restoration presented in this paper. Three variants of path protection and restoration scheme are shown. The applications of these techniques are however subject of future research.

References

[1] Baroni S., Eaves J., Kumar M., Qureshi M., Rodriguez-Moral A., and Sugerman D., "Analysis and Design of Backbone Architecture Alternatives for IP Optical Networking," *IEEE Journal in Selected Areas in Communications*, vol. 18, no. 10, pp. 1980-1994, 2000.

[2] Fumagalli A. and Valcarenghi L., "IP Restoration vs. WDM Protection: Is There an Optimal Choice," *IEEE Network Magazine*, vol. 14, no. 6, pp. 34-41, 2000.

[3] Gerstel O. and Ramaswami R., "Optical Layer Survivability an Implementation Perspective," *IEEE Journal Selected Areas in Communications*, vol. 18, no. 10, pp. 1885-1899, 2000.

[4] Liu K., Wilson B., and Wei J., "A Management and Visualization Framework for Reconfigurable WDM Optical Networks," *IEEE Network Magazine*, vol. 14, no. 6, pp. 8-15, 2000.

[5] Liu K., Wilson B., Pastor J., Roy A., and Wei J., "Performance and Testbed Study of Topology Reconfiguration in IP over WDM Networks," *IEEE Transactions on Communications*, vol. 50, no. 10, pp. 1662-1679, 2002.

[6] Wausters N. and Demeester P., "Design of the Optical Path Layer in Multiwavelength Cross-Connected Networks," *IEEE Journal Selected Areas in Communications*, vol. 14, no. 5, pp. 881-892, 1996.

[7] Wei J., Liu C., Park S., Liu K., Ramamurthy S., Kim H., and Maeda M., "Network Control and Management for the Next Generation Internet," *IEICE Transactions on Communications*, vol. E83B, no. 10, pp. 2191-2209, 2000.

[8] Wilson B., Stofel N., Post M., Pastor J., Liu K., Li T., Walsh K., Wei J, and Tsai Y., "Network Control and Management for Multiwavelength Optical Networks," *IEEE Journal Lightwave Technology*, vol. 18, no. 12, pp. 2038-2057, 2000.

[9] Zhang L., Deering S., Estrin D., Shenker S., and Zappala D., "RSVP: A New Resource Reservation Protocol," *IEEE Network Magazine*, vol. 7, no. 5, pp. 8-18, 1993.

Refat Kibria is an electrical and electronic engineer, he graduated from Islamic University of Technology, Dhaka, Bangladesh, in 2003. He is working for the Department of Computer Science and Engineering, Shah Jalal University of Science & Technology. His research interest includes WDM networks, dynamically reconfigurable WDM networks, IP over WDM, multi media communication and signal processing and wireless networks, and he has also acquired national and international publications in these fields. Refat is currently serving as a research assistant at Information and Communication Engineering Department of the INHA University, Inch eon South Korea under the KOREAN Govt. IT Scholarship Program.

Syed Reza is an electrical and electronic engineer, he graduated from Islamic University of Technology, Dhaka, Bangladesh, in 2003. Now working as a product manager of HUAWEI Technologies Bangladesh Limited. His research interest includes CDMA networks, WDM networks, dynamically reconfigurable WDM networks, IP over WDM, and wireless networks. He has national and international trainings on CDMA and very much eager in working with R and D.