Dynamic survivable RWA strategy on IP over WDM networks

Chen-Shie Ho[1]
Department of Electrical Engineering
National Taiwan University
Taipei, Taiwan
hocs@lion.ee.ntu.edu.tw

Sy-Yen Kuo
Department of Electrical Engineering
National Taiwan University
Taipei, Taiwan
sykuo@cc.ee.ntu.edu.tw

Abstract **To provide the robust message delivery capability with traffic flows in the networks, survivability become a key issue for the service provider to guarantee the service level agreement to the customers. In this paper, we propose the group-based routing and wavelength assignment policy for dynamic traffic demands under WDM optical networks on IP/GMPLS/WDM environment. We consider the survivable routing and wavelength assignment strategy for dynamic traffic demands under static partitioned network. The extensive simulation results show the efficiency of the proposed protection approach.**

***Index Terms*—protection, GMPLS, WDM, dynamic traffic**

I. Introduction

Wavelength-routed WDM (WRWDM) networks are the promising candidates for next-generation Internet and telecommunication backbones. In such a network, a failure of a network component (link or node) can lead to a severe disruption in the traffic. The service providers usually provide a pair of risk-independent working and protection paths for each connection request to protect the network against the failure situation [1-5]. Among all the existing survivability approaches, shared mesh protection has proven to be practical and cost-efficient [6-8]. In shared protection, several protection paths can share a wavelength resource on a wavelength channel if their working paths are risk-disjoint. When a traffic request arrives, the process to determine the risk-independent routes and assign the wavelengths for them is called as the survivable RWA (SRWA) problem. Efficient SRWA algorithms may make trade-off between the capacity utilization and restoration speed. In the mean while, IP based real-time and high-priority critical applications and services are still the mainstream data volume on the Internet. By supporting of the proposed Generalized Multiprotocol Label Switching (GMPLS) and its attendant protocol suite, a unified control plane is provided for the network devices equipped optical switching capability. Signaling of new connections in GMPLS-capable networks is accomplished by using either the RSVP-TE or CR-LDP protocols. To achieve higher level fast recovery of IP services, MPLS/GMPLS protocols also support restoration functionality to provide the network survivability [10]. We depicted the relationship between the 3 layer architecture in Fig. 1.

On the other hand, the future Internet, with the support of the next version of the Internet Protocol, IPv6, has been foreseen as a much large-scale network than today's Internet. IPv6 provides a greatly increased addressing space, improved mobility support, integrated security, quality-of-service support, and facilitates new delivery modes like anycast function. Anycast [9] is a technique used to deliver a packet to one of many hosts. A group of possibly distributed hosts respond to the same anycast address. A packet destined for an anycast address will be delivered to one of the hosts with that address, ideally the closest one. Any anycast destined packet should always be delivered to the appropriate destination once the underlying routing algorithms can find the lowest-cost path to the destination. Since the anycast operation has not been limited to one-to-many destination hosts, we can extend it to one-to-many group data delivery in order to find the protection group with the highest priority which means high efficiency in spare capacity.

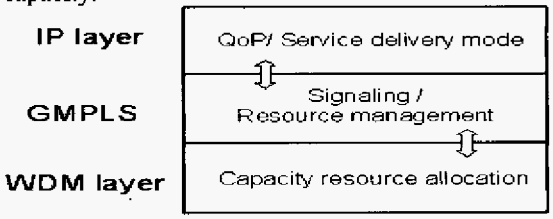

IP layer
QoP/ Service delivery mode
GMPLS
Signaling / Resource management
WDM layer
Capacity resource allocation

Fig. 1. Relationship between IP/GMPLS/WDM architecture.

In this paper, we will propose the IPv6/GMPLS group-based protection scheme for survivable WDM network design. It's main idea [11] is to partition the whole network into several autonomous protection system based on some metrics, then the SRWA process for each arriving traffic demand can be achieved by using the IPv6 anycasting to select the protection group which can provide the most promising spare capacity to meet the quality of restoration when any failure occurs along the working path. We present the network model under discussion in Section II, and we will give an example in section III to illustrate the basic concept of our method, and the proposed SRWA strategy under this architecture will be described in section IV. The simulation results will be examined in section V and section VI concludes this paper.

[1] Chen-Shie Ho is also with Department of CSIE, Van Nung University, Chung-Li, Tao-Yuan, Taiwan, R.O.C. E-mail: hocs@vnu.edu.tw

0-7803-8932-8/05/$20.00 © 2005 IEEE

II. Network Model

We plot the network model under assumption in Fig. 2. In the example network, the bold lines form the protection groups which are in charge of the protection switching for the disrupted connections in its own group domain. The entire intelligent optical cross-connects (IOXCs) are interconnected and linked to a local access station for providing client IP services. The nodes of the network are partitioned to different group set, and will be classified to inner node set and boundary node set for each group. We assume the nodes located at the boundary of the group have the capability to perform wavelength conversion, that is, the connections which crossing adjacent groups don't require following the wavelength continuity constraint (SCC). The connection requests are initiated from any access station and aggregated demands are delivered to the IOXC by the differentiation of quality of protection. The IOXC first recognize the traffic level, and determine to perform the SRWA if it is a dependable connection request. If it is a no-protected request, only RWA process is necessary to be carried out and this type of connections will be preempted when restoration is proceeded for dependable connections under failure conditions.

The concept of topology partition protection is proposed in [7]. In there, the subpath protection strategy use the idea to partitioning the network into several fixed but not same sized domains to protect each working lightpath segments in each domain area separately. It has advantages in multiple failure recovery, ILP scalability and fast recovery time, and suitable for low connection loading and traffic distribution conditions. In [9], we proposed the dynamic sub-mesh restoration scheme to further consider the resource utilization benefit and recovery speed from the viewpoint of multi-flow topology partitioning. In this paper, we will investigate the SRWA procedure for dynamic traffic demands under static group partition scenario on WDM mesh backbone networks. Note that the partition configuration will have great effects on provisioning and restoration performance, and it is the duty of network planner or operator to determine the optimal network capacity allocation for resource usage efficiency. The difference between this network architecture with core WDM network without partition is that the nodes (or links) of the network is cut into different set with various size, and therefore possesses different potential capacity and routes flexibility. How to perform the SRWA effectively for each connection is critical for achieving highly resource utilization and recovery speed.

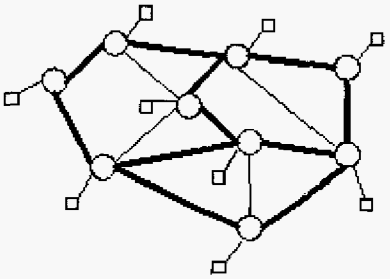


Fig. 2. Network model considered in this paper.

III. Basic Concept of the Mechanism

Restoration can be provided by either the client service layer or directly the optical layer. In transparent WDM network architecture with optical cross-connects (OXCs) equipped, a connection may not need to remain the same wavelength on all the links along its path, and hence more efficient wavelength resource can be achieved. In group switching restoration scenario, the traffic connection path is divided into several segments with unequal hop-length and located into several distinct group area. The path segmentation will be determined by group partition criteria. The group partition methods can be static or dynamic, which has the different influence to the quality of survivability. This paper will mainly consider the dynamic traffic condition on the wide area wavelength routed mesh topology based backbone environment with sparse wavelength conversion capability.

We denote the traffic request in our network model as a quadruple (s,d,b,p), where s and d is the source node and destination node, respectively; b indicates the bandwidth requirement, and p indicates the class of quality of protection specified by the service provider and this information will be incorporated to the request packet in IPv6 header. The network is partitioned into t groups $G_1, G_2, \ldots, G_t$, and we use V_{Gi} and E_{Gi} to denote the number of node and link in group G_i. Let the working path and protection path from s to d is W_{sd} and P_{sd} respectively. We define the intra-group connection as the demand request which $(s,d) \in V_{Gi}$ and $W_{sd}, P_{sd} \in E_{Gi}$; (Note that this may not hold in subpath protection because the protection path can be across multiple groups.) and the inter-group connection as the demand request which $(s,d) \in V_{Gi} \cup V_{Gj}$, $i \neq j$ and $W_{sd}, P_{sd} \in \cup E_{Gi}$, where i means all group indexes the W_{sd}, P_{sd} pass through. We denote the sets of boundary internetworking (as boundary ingress and egress) nodes in each adjacent group pair i and j as $G_B(i,j)$.

Consider a inter-group traffic request in node s in group G_i. First of all, the ingress node determined by GMPLS flow control will be found and the next hop will be selected by anycast result by aggregating the reply packet return from all adjacent $G_B(i,j)$, $i \neq j$. The selection phase on group G_i and routing process on next hop G_k can be performed in parallel. If node s find the route through one of it adjacent group would meet the QoP requirement, then it provisions this path segment as the working segment. It then tries to find the protection segment corresponding to this working segment. In group protection, the protection segment is chosen along the group boundary link set E_{Gi}, plus the extra segment from node s to the boundary of the group. The protection path for this connection can be done by joint or separate (2-step) RWA process and the local resource utilization will be optimized if the maximum sharing scheme is adopted. Since in each group the backup routes are preserved in priori corresponding to each segment of the working path, the protection switching rail is fixed so that no extra signaling overhead will be pay. In addition to the adaptation of segment protection by automatic separation of grouping, one can also exploit the protection by group disjoint paths. Since it is possible that there exists many groups established dynamically and distributed everywhere in the networks, the group-disjoint protection-based scheme has benefit on load distribution (although the load-balancing decision can also be made by GMPLS control signaling). The protection segment may be assigned to be the shortest path or the least load alternate route, which can be determined by the group provider's policy. Group switching can be viewed as the partition of the mesh transport network into groups to enhance the management efficiency and failure restoration.

The SRWA complexity can be further reduced if the group hierarchy scenario is used to assist the group routing. The load information in each node will be flooded in its own group, and the latest network resource usage status is stored in each node including the boundary nodes of the group. The source node of each connection request will first find a group which has the least load node within its boundary nodes. Then the anycast operation will be employed to find a target node as the next hop node in the same group. Once the next hop boundary node is determined, the next segment in next group will be fixed since the least load routing policy is adopted and this information is stored in all the boundary nodes corresponding to each group.

Besides, in static group partition scenario, the whole deployed transport network will be partitioned into several fixed-size groups. The boundary location and the dimension of the group can be determined depending on the network topology, the traffic patterns and the protection strategies. Here we adopt the method proposed in [11] because it is simple in implementation and can be easily modified to accommodate varying traffic demands and adapt to different quality of protection. The internal nodes within the group will be purely the IP/OXC without the routing overhead, that is, only the boundary nodes could be the ingress/egress LSR which have the responsibility to perform the RWA decision. The priority of each static group can be defined by the following two categories:

(a) *Fixed priority*: The priority and group size assigned to each group is fixed depending on the consideration by the network provider. The RWA will become the fixed and dedicate routing for each connection request and the setup or restoration delay can be estimated readily once the priority has been determined. The operator can change the group size and priority anytime or even multiplex the flows into several groups simultaneously. In this scenario, the working and protection paths are all located on the same group to assure complete restorability. The resource shortage condition can be improved if hierarchical protection layer has been defined and deployed. In this case, nodes belong to one layer will form a protection group. The group will no longer be formed by the geographical region. The efficiency on resource utilization will be improved further.

(b) *Variable priority*: In this scenario, to improve the efficiency of RWA computation, we define the priority of each group as follows, where l means the link within a group, w and s indicates the working and spare capacity, the l_w and l_s indicates the links along the working and protection path, respectively:

$$P_{G_i} = \frac{total\ capacity}{total\ capacity - assigned\ capacity} = \frac{\sum_l C_l / l}{\sum_l C_l / l - \sum_l (w_i + s_i)/(l_w + l_s)}$$

Once all the nodes compute and record the priorities, the RWA problem will be made when there arrives the connection request. Since the priority of each group will vary as the dynamic traffic demands be provisioned, the working and protection path pair will be cross same or different groups, which makes the restorability and recovery latency more unpredictable. The advantage of this group priority assignment scenario is its high resource utilization. The group classification will proceed after the group priority process was complete. The traffic demand which has different QoP will be routed on different group class whether the groups are classified in physically or logically. Since we do not consider the shared risk link group (SRLG) deployment here, the QoP of each connection will be achieved by provisioning physically resource disjoint paths.

In dynamic traffic environment, since the connection provisioned is short-lived, the group boundary will then change dynamically. Nodes within the same group will share all the resource in a group. Sometimes the groups will be merged not due to the resource insufficiency but when some connections or groups intersect with the others. In these cases the shared protection capacity will be re-computed to satisfy all the working paths in the merged group. The nodes in each group will record available resource and group priority information to be used as the routing decision. If global routing decision has to be made, each node in the network has to know the current group distribution status, which can be afforded by information exchanged using OSPF/ISIS signaling protocol. On the other hand, if suboptimal routing decision is to be made, the partial routing information collected by neighbor discovery will be enough. The forwarding table and protection table which store the working-protection port and occupied resource can be merged to further save the node processing space resource. The reconfiguration process, which is mainly composed of the rerouting mechanism, will be performed periodically or by event driven manner. The anycast group selection will be performed when new connection request arrives. RWA decision will be made in ingress source node. The final provisioned LSP pair will be determined after the aggregated from ingress nodes in each group by extended GMPLS protocols.

IV. SIMULATION STUDY

A. Simulation environment

We evaluate the effectiveness of the proposed dynamic partition algorithms by performing simulation. We list the characteristics of simulated networks in Table 1. We used GMPLS Lightwave Agile Switching Simulator (GLASS) developed by NIST as a simulation tool. TCP traffic request with 1Mbytes size is generated repeated and are assumed to arrive at hosts according to a Poisson process with a rate of 0.5. The traffics are classified into four QoS classes: premium, gold, medium and low. A duplex link is comprised of two simplex links in the opposite directions and consists of 32 wavelength channels. Every node has the same probability to be a source or a destination node for a connection request. Two types of failures, link and node failures ware injected to the network in a random manner during the simulation and then we inspect the failure recovery metrics for all affected traffics to examine the restorability. We examine 3 metrics, resource utilization, restoration penalty, and recovery ratio to measure the performance of the proposed mechanism. The restoration penalty can be evaluated either by restoration time estimation or by counting the total amount of exchanged messages. We examine restoration penalty by summing all the control messages including which generated in the failure recovery duration.

Table 1. Sample network topology information

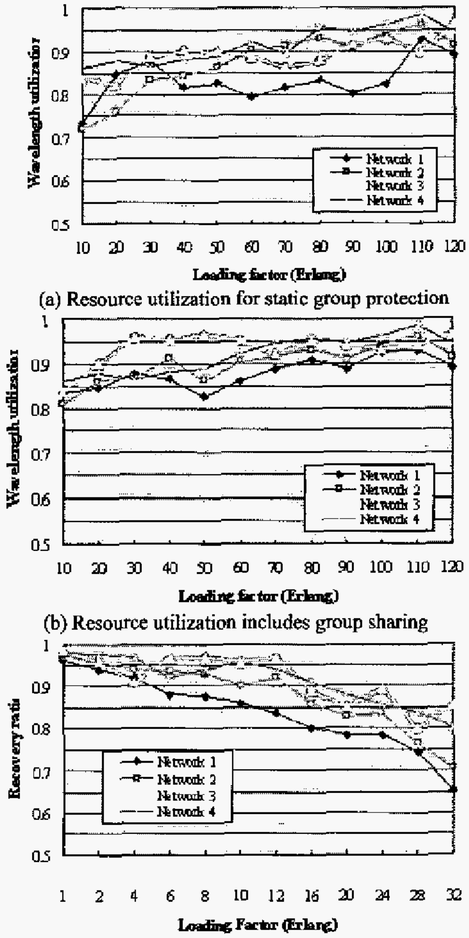
Target network	Node number	Edge number	Average nodal degree
(1)Spain	40	60	3.0
(2)Poland	47	70	2.98
(3)French	122	214	3.51
(4)Germany	73	130	3.56

B. Simulation results

The wavelength utilization ratio versus loading factor (in Erlang unit) is plotted in Fig. 3(a). From there we can see that higher wavelength resource utilization can be achieved in denser network and smaller oscillation appears which means the loads are more balanced in such networks. This value is calculated by averaging all the local capacity utilization by the working and protection segments within each group. Here the load balance means the capacity usage is fairer between the groups. It is beneficial if the SRWA procedure can be made by constraint routing decision. The round-robin load distribution scheme can be selected instead of the least-load or shortest distance routing when assign the anycast metrics. It needs to make trade-off between setup speed and resource utilization efficiency.

We also plot the result allowing group sharing for static grouping in Fig. 3(b), i.e., partial links or nodes in one group can be shared by multiple groups which attempting to exploit the resource more efficient. About 2%~15% efficiency can be achieved if the sharing size constraint is limited to 30%. The full sharing which overlapping adjacent groups increases the routing flexibility but also lengthen the protection path, which degrades the restoration efficiency. The dynamic sharing scheme seems a feasible solution to incorporate the resource availability and fault management into consideration in the same time.

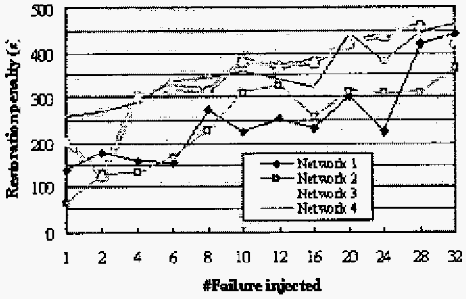
In order to verifying the efficiency of restoration, we apply 4-types of failures with different attribute which are intra-group link/node failures and inter-group link/node failure. From the plotting of restorability analysis in Fig. 3(c), the recovery ratio decays more than linearly because of the contention of dynamic resource setup/release, and resource shortage by bounded group size. This value is also related to the locations where failures occur. Some failures which gather at one area will make the resource no longer be available and disrupt all the traffics along this area. Advanced modification on group selection policy and control protocol will improve the recovery efficiency. The restoration penalty (in second) versus loading factor is plotted in Fig. 3(c). To get the numerical results during the simulation, we assume that the failure detection time is 15 μs, the unit propagation delay is 0.5 ms, the message processing time is 20 ms, the OXC setup time is 10 ms. As seen from the figure, the amount of exchanged message grows quickly under the heavy load condition after the failure occurred. It consists of group operation messages exchanged in normal condition and messages required for failure recovery. We use source-based signaling scheme on restoration, which can be substituted by parallel intermediate node signaling strategy to speed up the recovery process. The effect of link and node failure has different influence on the restoration performance. The rerouting mechanism considered in his paper is targeted to the node failure which makes the protection resource is over-reserved in average. On the other hand, multiple failures distributed in several groups can be deal with simultaneously if they are spare resource independent.



(a) Resource utilization for static group protection

(b) Resource utilization includes group sharing

(d) Recovery ratio in multiple failures



(e) Restoration penalty in time

Fig. 3. Various simulation parameters vs. loading factors.

V. Conclusion

This paper describes a novel approach to resolve static protection switching under IP/GMPLS/WDM network environment. This approach has benefits on simple survivable RWA implementation and restoration resource efficiency and availability, and has the capability to handle multiple failures. The proposed group switching preserves capacity for different priority level of service connection. Also, the performance can be further improved if dynamic reconfiguration and capacity optimization techniques are employed. For multiple failures condition, multiple restoration LSP can be issued simultaneously instead of paying tedious recovery processing delay. The investigation of our simulation results has shown that the improvement in bandwidth utilization can be effectively realized by our method if rerouting functionality scheme are incorporated into the switching module.

References

[1] H. Zang, J. P. Jue, and B. Mukherjee, "A review of routing and wavelength assignment approaches for wavelength-routed optical WDM networks," Optical Networks Magazine, vol. 1, no. 1, January 2000, pp. 47–60.

[2] B. T. Doshi, S. Dravida, P. Harshavardhana, O. Hauser, and Y. Wang, "Optical network design and restoration," Bell Labs. Technical Journal, Jan.–Mar. 1999, pp. 58–84.

[3] S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks, Part II--Restoration," Proc. ICC, Vol. 3, 1999, pp. 2023—2030.

[4] S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks, Part I—protection," Proc. IEEE INFOCOM, 1999, pp. 744—751.

[5] G. Mohan and Arun K. Somani, "Routing Dependable Connections with Specified Failure Restoration Guarantees in WDM Networks," in Proc. IEEE INFOCOM, vol. 3, 2000, pp. 1761 -1770.

[6] V. Anand, et al., "Sub-path protection: a new framework for optical layer survivability and its quantitative evaluation," UB CSE Technical Report, Jan. 2002.

[7] C. Qu, et al., "Sub-path protection for scalability and fast recovery in WDM mesh networks," Proc. OFC'02', Anaheim, CA, Mar. 2002, pp. 495-497.

[8] P. H. Ho and T. M. Hussein, "A framework for service-guaranteed shared protection in WDM mesh networks," IEEE Communication Magazine, Feb. 2002, 40(2), pp. 97-103.

[9] S. Weber and L. Cheng, "A survey of anycast in IPv6 networks", IEEE Communication Magazine, Jan. 2004, pp. 127-132. .

[10] D. W. Griffith and S. K. Lee, "Dynamic expansion of M:N protection groups in GMPLS optical networks", IEEE International Conference on Parallel Processing Workshops, Aug. 2002, pp. 171 – 176.

[11] C. S. Ho, Ing-Yi Chen and S. Y. Kuo, "Dynamic sub-mesh protection under dynamic traffic demands in dense WDM networks," AINA'04, Fukuoka, Japan, Mar. 2004, pp. 1164-1170.