

Differentiated Service Survivability in WDM Backbone Networks

Chen-Shie Ho*, Chang Woei **

*Department of Healthcare Administration, Oriental Institute of Technology, Banqiao City, Taipei County, Taiwan, R.O.C.

** Department of Computer Science and Information Engineering, Vanung University, Chung-Li, Tao-Yuan, Taiwan, R.O.C.

FL007@mail.oit.edu.tw, jungwoei@mail.vnu.edu.tw

Abstract— Traditionally the protection switching are performed in the manner of ignoring the class of service flows in a connection because of the cost and complexity considerations. In this paper, we will study the protection and restoration mechanisms for flows with different priorities in each connection. The simulation results show that the proposed mechanism can achieve significant improvement on several performance parameters.

Keywords— protection, restoration, WDM, survivability.

I. INTRODUCTION

Wavelength divisions multiplexing (WDM) networks provide high transmission rate and large bandwidth to deliver huge amounts of data over single fiber, and are deployed as the backbones by many network service providers for their fruitful business activities [1]. Since any cut in such a fiber may lead to huge data loss and cause a lot of traffic being blocked, WDM survivability becomes an important issue and has been well-studied in such optical mesh backbone networks. For this reason, methods and mechanisms of protection should be implemented to minimize the data loss when the failure occurs. In general, a proactive scheme called survivable routing and wavelength assignment (SRWA) process is executed when a connection request arrives [2][3]. It attempts to find a pair of paths (the working path and the protection path) and corresponding wavelengths used by them to convey the data for the request. The service stream will be assigned to the working path if the required resources are allocated. If no available path or wavelength resource can be found under this establishment phase, the request will be rejected. Several network protection methods based on such kind of resource reservation have been proposed, including the path protection, link protection, segment (sub-path) protection and cycle protection. The protection schemes have advantages on faster restoration time and provide guarantees of restoration capability compared to the dynamic restoration schemes. The goals of these schemes include increasing the number of recovered connections or improving the utilization of network resource during the service recovery phase, and speeding up the

connection setup process or increasing the acceptance ratio during the establishment phase.

After the working and spare resource are prepared, the data stream is transmitted from the source node to the destination node along the working path by using the pre-assigned working wavelength. Once a link along the path fails, all the data flow on the path will be transferred to the same protection path. With service operator's standpoint, performing protection switching for all the traffic flows to the protection path simultaneously is economic and easier to implement. On the other hand, the service providers who rent the infrastructure look forward to afford the quality of service which corresponds with their service level agreement or matches their service priority. In other words, the traffic flows include various type of service are differentiated in essential. Regarding all the traffic flow to single and same priority and performing protection switching for all of them simultaneously will be unreasonable and impractical.

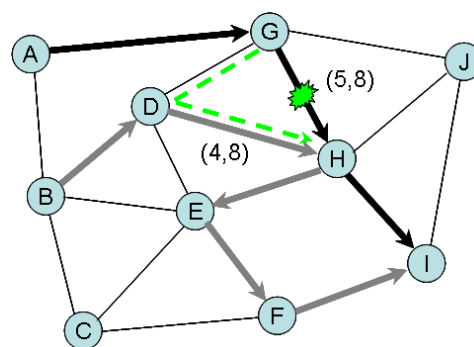


Figure 1. Illustration of the service recovery for the connection

Figure 1 shows an example to illustrate the link restoration in a sample network. The link usage is denoted as (c_u, c_l) pair where c_u and c_l indicates the used capacity and link capacity, respectively. Once the link G-H fails, the whole flow pre-assigned to that link will be tried to switch to the alternative route G-D-H. Since the aggregated flow of two connections on link D-H will exceed the capacity of that link, the route G-D-H will be discarded and the G-J-H will be chosen as candidate route. But if only the traffic flow with high priority is reallocated to route G-D-H, the successful probability of

switching will be increased and the resource of route G-J-H will be left to be used for other network connections. The automatic and adaptive mechanisms to identify the network status and distribute the flows to available resource of the network properly are necessary to be developed to improve the network operation efficiency.

In this paper, we will consider the differentiated recovery mechanism for service flows with different priorities on WDM backbone networks. Different class of service traffic will be assigned with different quality of restoration according to their priority. The protection paths for different type of traffic belonging to the same working path will be established if proactive strategy is adopted. Since it is not realistic to mix too many different class of services are to a single flow, the complexity of route computation and influence on resource utilization won't be significant in most cases. We will consider the mixing of static and dynamic traffic requests simultaneously. Long-term, high-volume and stable traffic streams always presents as the static traffic loads, and optimal capacity allocation can be achieved for this type of traffic. The dynamic traffic are suitable for connections with variable loads, and can be allocated with available network resource depends on the latest network status. The assumption that each node in the network is equipped with wavelength conversion capability is made. We also assume only single failure will occur at any moment, and no other failure exists during the MTTR period.

II. RESTORATION-BASED MECHANISM

We will first consider the reactive strategy in this article. The goal of the differentiated restoration is to let the disrupted traffic can be recovered by their priority, and increase the recovery ratio of traffic with high priorities. The trade-off will be made between the network resource occupied by the traffic and the restoration cost (including restoration time and switching cost). By limiting the path length and recovery time, the restoration paths are established dynamically and stored at the intermediated nodes along the working path. To achieve the distributed dynamical differentiated restoration, the data stored in each node for each working path will be replaced from the single flow information to multiple service information. The protection switching table records the next hop of rerouting link for each service flow. Once a request message enters the node in next hop, the service type is retrieved and stored at the node. So the intermediate nodes in the working path are aware of how many service types exist in the current flow. During the data transmission period, these nodes have to find alternative route and wavelength to successive hops towards the destination node. The length of the alternative route depends on the available network resource can be found. The protection discovery process consists of two steps. The first step is to find protection resource for high priority service streams, and the length of the protection path will be unlimited. The node which has found the shortest path with associated wavelength will stop its process. This process at a node without finding the protection path will be re-activated

after it receives the link dissemination message. The second step is to find protection resource for the dynamic low priority traffic. To increase the efficiency of resource utilization, share protection scheme is adopted for the dynamic traffic. Also, the path length is unlimited under the premise of maximal resource sharing. The performance of this kind of strategy will be verified later in the simulation study.

III. PROACTIVE STRATEGIES

Contrary to the reactive method, the proactive strategy can provide the guarantee to survive the connections upon failures. The goal of the differentiated protection is to achieve higher request acceptance ratio under the survivable routing and wavelength assignment operation. That is, the proposed strategy will try to accommodate as most connection requests, and each of the established connection can be restored once single failure occurs. For each request, the SRWA mechanism will work as the two-step operation. First the working path will be found for the request, and then the protection resource corresponding to this working path is explored. These two steps also form the connection establishment stage. The request will be rejected if any one of these steps fails to complete.

As in the reactive method, the information about the service type is recorded at the network nodes and exchanged between the nodes when they disseminate the link status messages. The request and acknowledgement messages also contain the service flow number. The request message includes all traffic type information in a connection request, and the acknowledgement message will return all protection routes information for all services upon the failures. To achieve this, each intermediate node along the working path has to find the protection route for each type of service traffic according the current network status when it receives the message. Since the traffic types are classified into several classes of service, providing the differentiated protection for various services with their restoration requirements is reasonable.

The working path is selected by shortest-first criteria. The source node has to determine the working path after it receives all acknowledgment messages from the downstream direction. To speed up the connection establishment process, especially on finding the protection path, the backup tree is constructed at each node along the working path. The backup tree is built according to the working tree, and has various sizes depending on the associated working path and current network status. Not the same as the conventional multi-way search tree, the tree also stores the available capacity and the level number of each branch. Each node maintains the backup tree, and the tree size decreases along the downstream direction towards the destination node. When the node receives the update message from its neighbouring node, the backup tree will be adjusted to reflect the latest network status. After the protection path is determined, the information is recorded to the tree and floods to other nodes in the network. When a node detects the failure of a link, it disseminates the update message and deletes the link in the backup tree. In the same way, when the node finds the capacity of a link is empty, it deletes the link from the tree to avoid link traversal in the protection establishment process.

To implement the differentiated protection, we classify the protection modes by different degree of overlapping, and use the path protection scenario as the protection scheme. We discuss these classifications as follows.

A. Fully differentiated protection

The protection path is node-disjoint with the working path for any type of the service flow. Besides, the protection path for each flow is node-disjoint although it can be multiplexed with the working or protection paths of other connections. Since the protection path for each flow is separated physically, the protection switching can be accomplished in dedicated way for each disrupted flow.

B. Differentiated protection with partial overlapping

The protection paths are allowed to be overlapped on several portions of the paths. The overlapping causes better capacity utilization but slightly increases the switching complexity inevitably. Also, several protection paths may be damaged when a link or node failure occurs. As the overlapping degree increases, the maintenance for each flow in the node will become more complicated.

C. Differentiated protection with limited overlapping

Some of the protection paths are allowed to be overlapped but some are not in this model. That is, the number of overlapped protection path is limited. The constraint criteria are optional to the network operator, and can be selected by the priority of each flow, by the link utilization limitations, by maximal sharing principle for overall network resource, or by the occupied resource of current connection. For the last criterion, the length of protection path is limited to a fixed number, which makes the overlapping is restrained automatically. In our implementation, the protection paths for static traffic are node-disjoint but the protection paths for dynamic traffic are shared multiplexing with each other. Since the failure may occur at any link along the working path randomly, the restoration efficiency will depend on the location of the failure.

The proposed scheme in differentiated protection with partial overlapping can be regarded as a variation of $M:N$ protection, which means that M working paths are protected by N spare paths against the failure. The difference between these two schemes is the source node will not be the same in the proposed model. The protection rerouting can be made from any intermediate node in the working path, which forms the node-disjoint subpath to protect different class of service.

The SRWA procedure will be terminated after the working-protection path pair for a connection request is found. In distributed-controlled network, the link status including the information about the current load is delivering on the control plane unceasingly. The failure of a link on a working path will generate protection switching for the disrupted connection. It also makes some protection paths associated with other working paths which connections are not affected be altered. Under the assumption of single failure condition, the protection paths for undisrupted

working paths will be restored though the unaffected traffic will loss the protection temporarily. If single failure condition cannot be obeyed due to some environment factors, dynamic multiple restoration for all affected paths will be made. The failure notification message will be delivered to the adjacent node of the link, which will activate the protection re-established process. Since it is possible no available route parallel to the failed link can be found, the node will send the notification message to next hop along both sides towards the end nodes of a connection. During the re-established process, no incoming request will be allowed to pass through the nodes progress the reconstruction. The request will be pending until the process is completed.

Another observation is about the protection switching scheme. The link protection makes more overlapping and complexity when finding the backup routes, but it is beneficial to recover the flow in faster way. In the protection mechanism allows the dynamic recovery, the determination of switching point to perform protection switching transition is critical for optimal protection resource allocation problem. On the other hand, the discussion above is from the perspective of single connection protection. In fact, more than one connection will exist in the network at any instant, and the connections may cross several autonomous domains in hierarchical network infrastructure. For such circumstance, to maintain the same quality of protection, the service layer protocol has to exchange about the class of services between the border routers. Since the working path is divided into several segments, each domain will be responsible for keeping the same restoration capabilities.

Finally, as more services types and lease solutions will be carried out by service providers, not all static or dynamic traffic can be classified into high or low priority explicitly. The provisional customer who rent the service may have higher priority due to higher pay. Whether the priority or the classification is determined in which manner, the strategies to deal with the SRWA will remain. That is, after the working path is found, the selected protection scheme and model are then applied to the protection establishment process for flows with different priorities.

IV. EXPERIMENT RESULTS

To evaluate the effectiveness of the proposed mechanism, we conducted simulations on the EON mesh network. The EON network has 19 nodes and 76 links. Each link has 32 wavelengths, which means the node in the network will select the working and protection wavelengths from these wavelengths from them. The traffic requests arrive at the network following the Poisson process and hold with exponential distribution. The performance parameter will be observed in restoration-based mechanism is the recovery ratio. The parameters will be inspected in proactive-based mechanism include the total acceptance ratio and capacity utilization for all loads. The total acceptance ratio is defined as the requests which have been established successfully over all injected traffic requests. The capacity utilization is calculated by summing total shared wavelength ratio for all links in the network. The failures are generated with random distribution

function. The level of service type is assumed with four different priorities and are random distributed inserted into the traffic queue to the network. Two higher services are static traffic and other services are dynamic. The ratio of the traffic is 1:1.

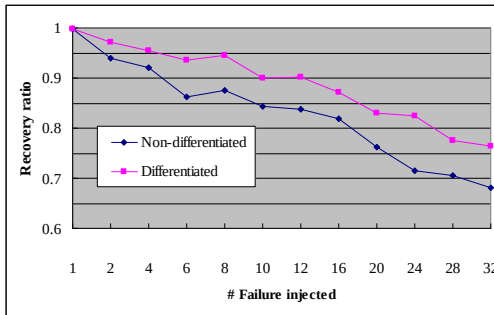


Figure 2. Performance of the restoration-based mechanism

The recovery ratio of the restoration-based mechanism is plotted in figure 2. We only plot the successful ratio for connections with higher priorities for non-differentiated mechanism in the figure. The difference of these two mechanisms reaches about ten percent at high loads condition. The non-differentiated mechanism switches all the flows in a connection to its protection path once a failure occurs, and therefore requires to find the route with identical capacity with the original one. The differentiated scheme tries to recover the flow with higher priorities first, and then restores the dynamic traffic by searching the available resource by the current network status. The recovery ratio for these two types of traffic is about 8:2 after 100 runs of the simulation.

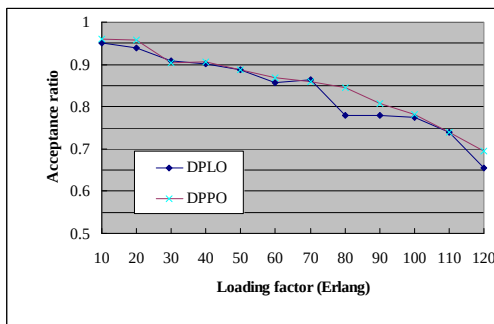


Figure 3. Performance result of acceptance ratio

Figure 3 shows the result about the acceptance ratio of differentiated protection with partial overlapping (DPPO) and differentiated protection with limited overlapping (DPLO) proactive mechanism, and figure 4 shows the result about the capacity utilization. DPPO can achieve better capacity utilization, produce more spare resource for dynamic traffic, and hence increase the acceptance of the request with lower priorities. The result is significant under high load conditions. The average path length of the connections is 5 links, and the average overlapping degree is 4.8. The reason of the cave in DPLO is resulted from the fact

that several dynamic requests attempting to compete the shared segment with insufficient capacity. This phenomenon can be eliminated even by allow more longer path length for these traffic or increase the wavelength number of each link for the fixed network topology.

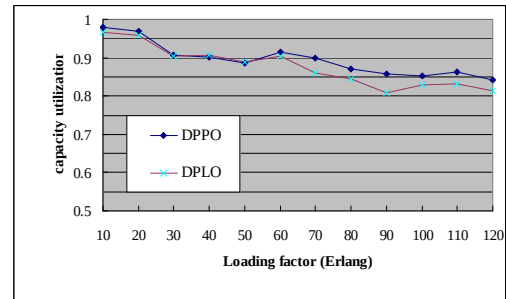


Figure 4. Performance result of capacity utilization

V. CONCLUSIONS

In this paper, we investigate the problem of differentiated protection and restoration for flows within the same connection. The restoration-based mechanism by given some constraint for different traffic is discussed. The protection strategies include the differentiated protection with partial overlapping and differentiated protection with limited overlapping are proposed. Under the assumption of single failure condition, the simulation results reveal that the differentiated service recovery will become more reasonable and equitable solution to achieve survivability for traffic with distinct priorities.

REFERENCES

- [1] R. Ramaswami and K. N. Sivarajan, *Optical Networks: A Practical Perspective*. Second Edition, San Mateo, CA: Morgan Kaufmann, 2002.
- [2] H. Zang, J. P. Jue, and B. Mukherjee, "A Review of Routing and Wavelength Assignment Approaches for Wavelength-Routed Optical WDM Networks," *SPIE/Baltzer Optical Networks Magazine (ONM)*, vol. 1, no. 1, pp. 47-60, Jan. 2000.
- [3] S. Yuan and J. P. Jue, "A Shared Protection Routing Algorithm for Optical Networks," *Optical Networks Magazine*, vol. 3, no. 3, pp. 32-39, May/June 2002.
- [4] Xi Yang, Lu Shen, and Byrav Ramamurthy, "Survivable Lightpath Provisioning in WDM Mesh Networks Under Shared Path Protection and Signal Quality Constraints," *J. Lightwave Technol.* 23, pp. 1556-1567, 2005.
- [5] G. Mohan, C. S. R. Murthy, and A. K. Somani, "Efficient Algorithms for Routing Dependable Connections in WDM Optical Networks," *IEEE/ACM Trans. on Networking*, vol. 9, pp. 553-566, Oct. 2001.
- [6] C. Ou, H. Zang, and B. Mukherjee, "Sub-path protection for scalability and fast recovery in optical WDM mesh networks," *Proc. OFC*, pp. 495-496, Mar. 2002.
- [7] 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.
- [8] W. D. Grover and D. Stamatelakis, "Cycle-oriented distributed pre-configuration: Ring-like speed with mesh-like capacity for self-planning network restoration," in *Proceedings of IEEE ICC'98*, pp. 537-543, 1998.
- [9] G. Shen and W. D. Grover, "Segment-based approaches to survivable translucent network design under various ultra-long-haul system reach capabilities," *OSA Journal of Optical Networking*, vol. 3, no. 1, pp. 1-24, Jan. 2004.
- [10] S. Ramamurthy, L. Sahasrabudhe, and B. Mukherjee, "Survivable WDM Mesh Networks", *IEEE Journal of Lightwave Technology*, vol. 21, no. 4, pp. 870-883, Apr. 2003.