# Supporting differentiated survivability services in WDM optical networks

**Anna Tzanakaki, Senior Member IEEE, George Markidis, Kostas Katrinis**
*Athens Information Technology (AIT) 19,5km Markopoulou Avenue 68, 1900 2 Athens, Greece*
*Tel: (30)210 668 2766, Fax: (30)210 668 2730, e-mail: atza@ait.gr*

## ABSTRACT

Optical networks are currently widely employed to support a variety of telecommunications and other applications. In order to provide the increased bandwidth needed by the existing and emerging applications, optical networks rely extensively on wavelength division multiplexing (WDM). In these networks, WDM is not only used to satisfy capacity requirements, but it can be also exploited to offer advanced features and functionalities such as service differentiation, varying QoS guarantees etc. This paper studies the use of WDM in core optical networks with focus on resilience issues. More specifically the use and suitability of WDM to support differentiated survivability requirements of traffic generated by different applications are investigated. The proposed approach combines various routing and wavelength assignment schemes with the aim to facilitate efficient resource sharing, thus leading into significant enhancement of the spare capacity utilization, as demonstrated by our evaluation results. At the same time, routing and wavelength assignment can be used to differentiate various classes of services based on their survivability requirements. Simulations have shown significant network performance improvement through the proposed approach compared to conventional solutions that do not include survivability differentiation between services.

**Keywords**: optical networks, WDM, routing, wavelength assignment, resilience, survivability.

## 1. INTRODUCTION

It is widely accepted that telecommunications networks and the Internet have grown from infrastructures that were initially only supporting some level of connectivity between end users into a very powerful economic/business paradigm with a significant socioeconomic impact for the whole globe. It is true to say that, when considering the extent and nature of the use of Today's and Future Internet, including activities such as commerce and businesses, a fundamental requirement that needs to be satisfied is to provide secure and trusted access to the end users. It is becoming increasingly important to offer the ability to carry out a wide spectrum of activities through a trustworthy network infrastructure—ensuring the security, reliability, and stability of increasingly critical and pervasive applications and services.

Optical networking exploiting wavelength division multiplexing (WDM) is currently extensively used in existing telecommunications infrastructures and is expected to play a significant role in next generation networks and the future Internet supporting a large variety of services having very different requirements in terms of bandwidth, latency, reliability and other features. When focusing on reliability one could easily identify different requirements requested by various applications supported by the network. It is clear that providing 100% resilience guarantee to all types of traffic supported by the network would be ideally desirable but this may be unnecessary and wasteful in terms of resource utilization resulting in cost inefficiencies. In this context a more efficient resilience scheme suitable for a network supporting a variety of applications would be a scheme that provides different level of network survivability to different traffic types in accordance with the respective Service Level Specifications (SLS) maximizing the network utilization. Therefore, in a network environment such as the new global and business oriented internet an important requirement will be to provide differentiated survivability services to different types of traffic enabling higher priority demands to exploit higher network availability [1].

. The deployment of WDM technology enables the routing of multiple lightpath connections utilizing different wavelength channels in an optical fiber. In this environment fault-tolerance is an essential requirement as a single link failure causes loss of services that carry enormous amounts of information that may lead to significant revenue losses. Therefore it is indispensable for WDM networks to have in place resilience mechanisms to reroute/restore the affected traffic upon a failure. Different approaches of addressing resilience in WDM optical networks have been extensively reported in the literature [2].

The provision of resilience in optical WDM networks is realized by either proactive protection [3] or reactive restoration [4]. The first computes one or more alternative paths to the primary routing path (backup paths) and the required network resources are reserved for it at the time of establishing the primary lightpath. A backup path is then activated at the occurrence of a failure on the primary path. On the other hand, restoration acts only after the detection of a failed path by computing and provisioning a new path that circumvents the point of failure. This procedure may fail in identifying a backup lightpath due to lack of network available capacity and therefore does not guarantee successful recovery.

A further classification of the pre-designed protection method is performed based on link or path protection schemes. In the link based method the failed link is replaced by a new path which however includes the unaffected portion of the primary path. This method constraints the choice of the backup paths and requires more spare resources than the path-based method [5], which computes a complete end-to-end backup path from the source to the destination of the failed primary path. In the path-based method, wavelength channels on the backup path can be either dedicated or shared. If dedicated the wavelength channels assigned to a specific backup path cannot be assigned to other backup paths. On the other hand in the shared method, backup paths can share wavelength channels under the single link failure assumption, if their primary paths are link-disjoint which is known as backup multiplexing and provides improved resource utilization [4].

The above and other design choices create interesting trade-offs, like for instance the balance between overall cost and degree of resilience in shared vs. dedicated protection [6]. The algorithm proposed in this paper employs path-based protection in an effort to combine manageable complexity with higher spare bandwidth availability [7]. More specifically, survivability is provided by implementing the backup multiplexing technique under dynamic traffic demands where existing lightpaths cannot be rerouted and future lightpath requests are not known. In addition, traffic demands are assigned three classes of service with regards to network recovery and adopt the concept of resilience priority classes to maximize network resource utilization. The three types of lightpaths considered are: 1) high priority protected lightpaths, 2) unprotected lightpaths and 3) low priority preempted lightpaths. A high priority protected lightpath has a working path and a diversely routed backup path. Both the working and the backup lightpaths are identified before the provisioning of the working path according to the back-up multiplexing scheme. An unprotected lightpath is not protected with a backup path and upon any failure along the lightpath a dynamic restoration mechanism is initiated to provide an alternative route without any guarantees. Finally low priority preempted lightpaths are unprotected lightpaths that can use the backup routes of the high priority lightpaths. In case of high priority lightpath failure preemption of this low priority traffic takes place.

## 2. ALGORITHM SPECIFICATION

The work presented in this paper solves the online version of the RWA/resilience problem, i.e. traffic requests arrive and get served sequentially without knowledge of future incoming requests. This makes this contribution valid for usage both in the network design and – most importantly – the traffic engineering field. In addition it is assumed that only a single link could fail at any instance of time and re-routing of already established connections is not allowed. Last, the model does not take into consideration any wavelength conversion capability of the network and thus wavelength continuity across any path is a tight constraint in the problem definition.

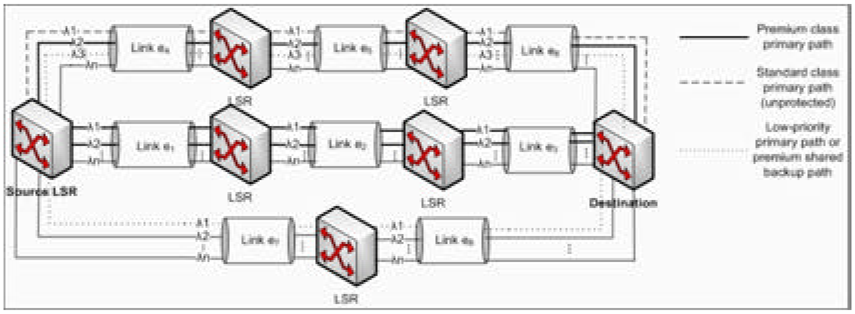

λ1
λ2
λ3
λn
Link $e_4$
Link $e_5$
Link $e_6$
Link $e_1$
Link $e_2$
Link $e_3$
Link $e_7$
Link $e_8$
LSR
Source LSR
Destination
Premium class primary path
Standard class primary path (unprotected)
Low-priority primary path or premium shared backup path

*Fig. 1. Sample network topology*

As already mentioned, the proposed algorithm provides for differentiated services with regard to survivability. This is realized through the definition of the following **three classes of service**:

- A premium class (class-1) offering one dedicated primary path plus one shared but diversely routed backup path
- A standard class (class-2) providing for one unprotected but dedicated primary path that can be restored dynamically in case of failure and
- A low-priority class (class-3) offering a single path that may share links with class-1 backup paths and can be pre-empted in the case of a class-1 primary path failure to allow for activation of the backup mechanism.

The routing of primary paths belonging to either dass-1 or class-2 is accomplished as follows: using global network knowledge, the algorithm assigns costs to all network links: a) infinite cost is assigned to a link, if all its wavelengths are occupied and otherwise b) a link is assigned a cost value that is inversely proportional to its current residual bandwidth $R_i$. The residual bandwidth of a link is defined as the difference between the capacity bandwidth $C_i$ of the link and the already reserved bandwidth on the link for primary (denoted by $A_i$) and shared (denoted by $B_i$) paths, i.e. $R_i= C_i-A_i- B_i$. After costs are assigned to network links, a widest shortest path algorithm is executed on the graph, resulting in a single chosen shortest path, namely the one with the minimum number of hops and satisfying the wavelength continuity constraint. If no such path can be found, the connection request is rejected. Otherwise, the calculated path is provisioned using the first available wavelength.

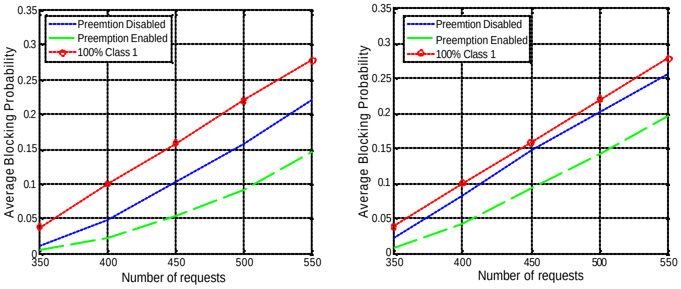
To increase intuition, consider the sample network topology shown in Figure 1. Assume that initially only wavelength ?1 is free on links $e_7$ and $e_8$ (e.g. through manual configuration for the sake of presentation), whereas the rest of the links are completely unloaded. A premium-class request from source to destination is then not routed via the minimum hop path (via links $e_7$ and $e_8$), but through the path $e_1$- $e_2$- $e_3$, which is a shorter path in terms of spare bandwidth costs compared to the $e_7$- $e_8$ path. The served request in the figure is finally assigned wavelength ?1 on the $e_1$- $e_2$- $e_3$ path. Similarly, a newly arrived standard-class request is routed through the path $e_4$- $e_5$- $e_6$ using wavelength ?1.

Backup paths and low-priority primary paths are routed in a similar manner, however with a few amendments to the previously described scheme. Due to allowing link sharing among those paths, the residual bandwidth $R_i$’ in this case includes the bandwidth already reserved for shared paths on a link, i.e. $R_i$’= $C_i$-$A_i$. Additionally, particularly to the case of backup paths, every link on a shortest path is checked to ensure that no backup path uses this link to protect primary (premium-class) paths that are not disjoint to the primary path that is to be protected by the backup path of focus. Consider applying this constraint in the example network of Figure 1. Suppose that we start with the instance, where the primary connections $e_1$- $e_2$- $e_3$ on ?1 and $e_4$- $e_5$- $e_6$ on ?1 are already established. Additionally, a backup path $e_7$- $e_8$ on ?1 is set up to protect the premium class $e_1$- $e_2$- $e_3$ on ?1connection. Assume that the next premium class request between source and destination is routed via $e_4$- $e_5$- $e_6$ on ?2. The already provisioned backup path $e_7$- $e_8$ on ?1 can also be used to protect the newly routed request, since the two primary paths do not share links. Consider now the arrival of the next premium class request, which happens to be routed on ?2 via $e_1$- $e_2$- $e_3$. Since this new path shares links (actually is identical here) with another (class-1 or class-2) primary path, links $e_7$ and $e_8$ can not be used on the same wavelength for protection. Was this the case, then upon failure of a single link, e.g. link $e_2$, both failed connections would use the same link on their backup path and thus fail to operate as desired.

From the above, it follows that our algorithm achieves to avoid saturated links and strives to balance bandwidth utilization among fiber links (load balancing). For a more strict specification of the algorithm please refer to [1].

## 3. PERFORMANCE STUDY

Simulations of dynamic provisioning on several representative backbone mesh topologies have been performed. The results presented here are generated based on the Pan-European test network defined by COST 239 [8] that comprises 11 nodes and 26 links. Links are considered bidirectional and if a link failure occurs the traffic flow in both directions will be disrupted. Lightpaths comply with the wavelength continuity constraint and connections requests are equally likely to have any of the network nodes as its source or destination. Also we assume that calls arrive one by one and their holding time is long enough to consider that accepted calls do not leave (incremental traffic). A connection is blocked if either a primary or a backup path can not be established. The results shown in the following figures are the average values over 20 independent experiments.

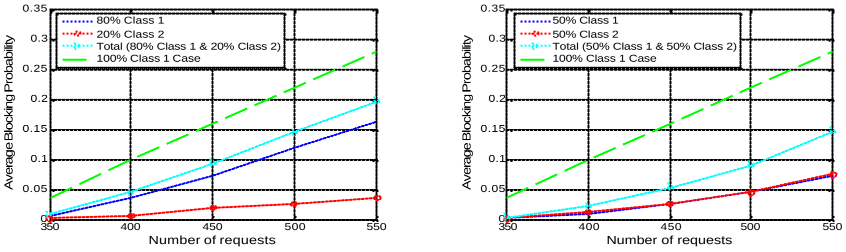


(a) (b)

*Figure 2 Average blocking probability when (a) 50% and (b) 80% of the requested connections are assigned as class 1 traffic and LF scheme is used for C=16*

Figure 2 illustrates the results obtained by considering the coexistence of both class 1 and class 2 traffic, with the preemption authority disabled and enabled. More specifically in this case two scenarios are compared: one for which the class 1 traffic is 50% and one for which 80% of the total requests. These two cases are compared with the case in which all the traffic is considered as class 1 traffic. The benefit offered by the preemption enabled scheme is up to 12% when half of the incoming traffic is assigned as class 1 and up to 8% when 80% is set us class 1.

For the non preemptive scheme the benefit reduces to 5% and 3% respectively indicating the superiority of the preemptive approach in terms of network performance. This improvement offered by the preemptive scheme is at the expense of the reliable provisioning of low priority traffic, which can be tolerated for many non-real time applications. The preemptive scheme although utilizing a smaller number of links compared to the non preemptive case provides an increase in the link reuse percentage since it allows the low priority class 2 traffic to be shared among the backup paths of the higher priority traffic. When no preemption is allowed the number of possible shared paths is significantly reduced since only 50% of the total demands require backup paths resulting in inefficient backup resource utilization with considerable impact on the network performance.



(a) (b)

*Figure 3 Analyzing the blocking probabilities of the different classes in the network when (a) 80% and (b) 50% of class1 traffic is requested.*

Finally in figure 3 we analyze the blocking probabilities of the different classes coexisting in the network when preemption is allowed. In fig 4.a 80% of the total traffic is considered as class 1 and 20% as class 2. The blocking probability of the class 1 traffic is high compared to the low priority traffic (a difference of about 10% is observed) although the overall blocking is reduced when considering this differentiation scheme. In fig 4.b the same percentage of class 1 and class 2 demands is assumed and almost the same blocking probability is observed for the two classes, causing a higher reduction in the overall blocking probability. Also in this case the blocking probability of high priority traffic is reduced considerably at least for heavier network loadings (around 8%) whereas the blocking of the lower priority traffic is increased in a much smaller scale (about 4%).

## 4. CONCLUSIONS

In this paper we addressed the problem of efficiently provisioning lightpaths with different protection requirements in a dynamic WDM network environment. The incoming traffic is differentiated to classes of service according to their survivability requirements and the preemption of low priority traffic by higher priority demands in the event of a link failure is proposed. In case of the use of pre-emption detailed simulation results demonstrate significant network improvement of up to 12% and considerable decrease in the blocking probability of the high priority traffic.

## ACKNOWLEDGEMENTS

The authors would like to acknowledge the FP6 EU funded integrated project PHOSPHORUS, IST-034115 and COST291 for providing support for this work.

## REFERENCES

[1] A. Fumagalli and M. Tacca,"Differentiated Reliability (DiR) in Wavelength Division Multiplexing Rings", IEEE/ACM Trans. Netw. 14, 159-168 (2006)

[2] G. Mohan and C. Murthy, "Lightpath Restoration in WDM Optical Networks," IEEE Netw. 14, 24-32 (2000)

[3] S. Ramamurthy and B. Mukherjee, "Survivable WDM Mesh Networks, Part I - Protection," in *Proceeding of IEEE conference on Computer and Communication Societies* (IEEE, 1999), pp. 744-751.

[4] B. T. Doshi., "Optical Network Design and Restoration," Bell Labs Tech. J. 58-84,(1999).

[5] M. Kodialam, T. V. Lakshma: Dynamic Routing of Bandwidth Guaranteed Tunnels with Restoration, in Proceeding of IEEE Conference on Computer Communication, pp. 902-911, 2000.

[6] J. Li, K. L. Yeung , "A Novel Two-Step Approach to Restorable Dynamic QoS Routing" J. Lightw. Tech. 23, 3663-3670 (2005).

[7] Markidis, G. and A. Tzanakaki: Network Performance Improvement through Differentiated Survivability Services in WDM Networks, to appear in Journal of Optical Networking, 2008.

[8] Batchelor,P. et al. "Study on the Implementation of Optical Transparent Transport Networks