Protection Based QoS in WDM Mesh Networks

Sun-il Kim
University of Illinois at Urbana-Champaign
CS Department
Coordinated Science Laboratory
sunilkim@crhc.uiuc.edu

Steven S. Lumetta
University of Illinois at Urbana-Champaign
ECE Department
Coordinated Science Laboratory
lumetta@uiuc.edu

***Abstract*— Quality of service (QoS) provisioning on wavelength division multiplexed (WDM) networks is an increasingly important issue in network design and management. One important performance metric in a QoS optical network is survivability. The choice of protection algorithm directly affects survivability of a network and can be differentiated based on the needs of different clients. Differentiating services based on protection affects both availability and data loss due to a failure. Network operation cost in terms of provisioned capacity (wavelength channels) needs to be considered in QoS routing and resource allocation, and an efficient classification scheme based on protection classes along with optimized capacity assignment algorithms can help reduce costs.**

Based on different protection requirements of network clients, a protection based classification scheme for QoS support in optical networks is proposed. We also introduce an optimization technique based on protection resource sharing among two different protection classes. We compare different classification schemes and quantify the benefits of having protection differentiated classes in terms of network capacity cost.

Our results show that, on average over five sample networks, online provisioning with the proposed protection based QoS scheme allows up to 30% savings in terms of capacity cost compared to a network without such classification, and roughly a 7.6% savings compared with a network that provides only two classes while providing better reliability.

Keywords: optical communication, optical fiber communication, WDM network, optical network, differentiated services, QoS, class of service, quality of service, protection, survivability

I. Introduction

As demand increases for more robust and fluid communications to support our growing reliance on rapid access to information, the need for efficient and reliable networks becomes critical. The use of WDM technology in the backbone networks has enabled us to meet these demands by taking advantage of the huge capacity of optical fibers. Numerous protection schemes exist for these networks, but in practice most networks use only one or two such schemes, roughly classifying customers into those that need robust connectivity and those that do not. In this paper, we examine the potential benefits of using a broader system of protection classifications to support data traffic and present a novel approach to optimization across classes that reduces the protection capacity necessary to support a given traffic load.

The material presented in this paper is based in part upon work supported by National Science Foundation grants ANI 01-21662 ITR and ACI 99-84492 CAREER. The content of the information does not necessarily reflect the position or the policy of that organization.

Most WDM backbones still carry primarily SONET (Synchronous Optical NETwork) streams, which in turn consist mostly of virtual ATM (Asynchronous Transfer Mode) circuits. IP (Internet Protocol) packets are then layered atop ATM, with virtual circuits providing the links between routers. However, within the last two years, as projected in [1], the volume of data communications in the wide area overtook the volume of voice communications. Data communication volume continues to grow exponentially, while voice has grown only linearly for several decades. Within a few years, voice transmissions will account for only a tiny fraction of total traffic, making the use of protocols designed to carry such traffic questionable.

SONET and ATM were both designed more than a decade ago by the telephony industry at a time when data traffic was essentially irrelevant in the wide area. While they are both mature, well-established and well-tested protocols, they do not necessarily do a good job in addressing the needs of data traffic. One issue in particular is the inclusion of recovery functionality at all four layers mentioned, leading to inefficient use of physical resources and complex synchronization schemes to avoid interference between layers when a problem occurs.

Many researchers have thus begun to investigate the possibility of coupling the IP layer more closely to the WDM layer, removing most of the replicated functionality in SONET and ATM and moving the rest into IP, WDM, or a slim layer between the two [2]. If the layers are reorganized, the proper layer for protection functionality is unclear. These issues are currently addressed in markedly different ways in the two layers. Restoration time has long been considered an aspect of quality-of-service (QoS) in many circuit-switched networks like ATM [3], [4]. WDM protection schemes offer fast restoration, often on the order of the 60-millisecond restoration requirement imposed for SONET self-healing rings. In sharp contrast, recovery through Internet routing protocols, whether within an Autonomous System (AS) using Open Shortest Path First (OSPF) or between them using BGP-4 [5], can currently take minutes [6], [7]. Some claim that these long times are not fundamental to the protocols themselves, but in practice, security concerns with automatic routing updates have dramatically slowed the propagation of failure information with BGP-4, in which information is usually only forwarded to neighbors every 30 seconds [5].

We believe that protection functionality must be supported in both layers. WDM schemes that support restoration over several autonomous, independently-managed domains have

yet to be developed, and are unlikely to be simple. Such recovery must occur within the IP framework. When possible, however, recovery should be fast to support applications that need high availability, such as air traffic control, remote surgery, and certain types of transactions. Protection at the physical layer must thus also be made available, and customers allowed to differentiate themselves according to their needs. As with most optimization problems, relaxing constraints by allowing additional protection options reduces the protection capacity requirements for a WDM network. Schemes in which IP controls nearly all WDM-layer functionality [8] may be feasible, but a diverse set of protection schemes is attractive.

A WDM network that supports several compatible protection schemes also offers opportunities to optimize across connections using different schemes. In addition to exploring the benefits of increased protection service differentiation, this paper describes an optimization for networks that offer both dedicated (one-for-one, or 1:1) and shared (one-for-N, or 1:N) protection that allows capacity costs to be reduced by as much as 15% when only these two schemes are supported, and by 5-10% in a network with more protection schemes.

The remainder of the paper is organized as follows. In Section II, we describe related background material in more detail. Section III outlines our approach to protection-differentiated QoS and introduces our protection classifications. Section IV describes our methodology for evaluating the benefits of differentiation and introduces an interesting optimization for 1:1/1:N protection. Section V gives our results and a discussion of their meaning. Finally, we provide our conclusions and outline future work in Section VI.

II. Background

A. QoS under WDM Networks

The idea of supporting protection differentiation in optics is not novel, but neither has it been thoroughly explored. Early work in this area [9], [10] primarily addressed issues of physical signal quality and blocking probability. More recently, a study proposed leveraging the emerging Multiprotocol Label Switching (MPLS) standards, which support the identification of the customer or group of customers behind a particular packet in a traffic flow through the use of labels within headers [11]. In coordination with the optics, the MPLS flow classification can then include a resilience class. This study [11] fairly clearly demonstrates the benefits of supporting multiple resilience classes for reducing protection capacity, but assumes that all unprotected traffic can be preempted in the event of a failure and performs off-line routing and optimization. We split unprotected traffic into preemptable and non-preemptable classes, as we believe that the increased vulnerability due to preemption will be unattractive to many customers. In IP/MPLS over WDM networks, many paths in the optical layer will be provisioned without any protection, therefore, preempting these traffic my have undesirable effects on the upper layer protocols (IP/MPLS, TCP etc.). In addition, off-line optimization is used in [11]. As both the size and the complexity of networks increases, especially in IP/MPLS over WDM networks, dynamic routing becomes more attractive than static routing as lightpaths will be required to be setup and torn down dynamically to meet the communication demands. We therefore perform online routing which does not allow off-line optimization that can aid in reducing cost in terms of capacity usage. We also present results on the average number of connections broken by a failure and the percentage of traffic that were protected for free (with zero capacity cost), thus providing more insight into these tradeoffs. A more direct comparison appears in Section V.

B. Survivability

Failures in optical networks result in loss of enormous data and revenue. Some of these failures include channel failures, link failures and failures of optical crossconnects (OXC). Channel failures caused by card failures at a port of an optical switch are the most common type of failures in optical networks. Links failures (fiber cuts caused by wayward backhoes, amplifier failures etc.) are also common, and can result in failures of all the channels that are carried on the fiber. Node (OXC) failures are less common, but can cause failures of all the links that are adjacent to the node.

Protection and Restoration are the two main approaches that address failures in optical networks [12], [13]. Restoration addresses failures by locating free λ-channels for backup after a failure occurs. Protection preplans backup routes that are used in the event of a failure. Protection and restoration offer a tradeoff between the speed of recovery and efficiency in terms of the use of spare capacity [14], [15]. However, protection can be implemented in a capacity efficient manner [16], [17], [18], [19], [20] and can offer much faster recovery than restoration with the absence of the signaling delay needed for dynamic route discovery [21], [22], [23]. Restoration schemes find a recovery route dynamically, which takes about 2 seconds, whereas protection schemes can achieve complete recovery in the order of tens of milliseconds [24]. We therefore focus on protection, and for the rest of this paper, we use the terms restoration and protection interchangeably to mean protection as defined above.

There are two types of protection: local (link/node) protection and path protection. Path protection requires the knowledge of the whole path and selection of a backup path that is shared risk group (SRG) disjoint from the primary path. In 1+1 protection, traffic is sent out over both paths and the receiving node simply switches to the backup stream in the event of a failure [24]. 1+1 protection offers very fast recovery with little data loss because no signaling is required between the source and the destination nodes, but is inefficient in terms of capacity requirements. 1:1 protection is same as 1+1 except the data stream is not actively sent out, but switched after a failure. In shared path protection schemes, the end nodes of a lightpath signal the intermediate nodes to establish the backup route. Capacity reserved for backup can be shared among different connections that do not share same SRGs, or can also be used to carry low priority (unprotected) traffic, which is preempted in the event of a failure. The signaling and configuration of the intermediate PXCs render shared mesh protection slow compared to 1+1/1:1 protection. In link protection, nodes that

Class	Priority (Class A)	Protected (Class B)	Reroutable (Class C)	Unprotected (Class D)	Pre-emptable (Class E)
Protection Scheme	1:1 or 1+1	1:N	Best-effort rerouting	None	[Pre-emption]
Recovery Time	20∼50ms	90ms	seconds	Duration of the failure	Duration of the failure
Data Loss	20ms	90ms	seconds	Duration of the failure	Duration of the failure

TABLE I
PROTECTION BASED QOS CLASSES.

Scheme	Traffic Demand Ratio (Protection Class)
S1: 5 classes - Optimized	1(A):2(B):4(C):2(D):1(E)
S2: 5 classes	1(A):2(B):4(C):2(D):1(E)
S3: 2 classes	0(A):3(B):0(C):7(D):0(E)
S4: 2 classes	3(A):0(B):0(C):7(D):0(E)
S5: 1 class	0(A):0(B):0(C):10(D):0(E)
S6: 1 class	0(A):10(B):0(C):0(D):0(E)
S7: 1 class	10(A):0(B):0(C):0(D):0(E)

TABLE II
PROTECTION BASED QOS CLASSES.

are adjacent to the failure initiate recovery by reserving spare capacity and signaling and configuring the intermediate nodes after a failure in a manner akin to path protection. However, recovery of failures usually involves the use of more local resources compared to path protection. Recovery is usually faster because it is initiated by the end nodes of the failed link compared to path protection, but link protection is more inefficient in terms of spare capacity usage [17], [19].

III. PROTECTION DIFFERENTIATED QOS

Different network clients and applications have different survivability needs ranging from mission critical applications requiring immediate recovery with minimized data loss to lower-end user traffic with no survivability needs. Different protection algorithms offer different protection capabilities such as speed of recovery, data loss, provisioning costs and management overhead. Utilizing link protection and dynamic restoration for different classes of traffic can provide sufficient differentiation among traffic classes with different survivability needs, but at the cost of having two different protocols to operate and manage. In order to reduce management overhead, we choose to utilize a single class of protection algorithms. For this reason, we focus on path protection to meet our goal to lower operation costs through protection differentiated QoS. In this section we propose a five classification schemes and discuss the details of each protection class.

A. Protection Classes

Table I shows the proposed classification scheme for protection based QoS support in optical notworks. We next briefly explain each protection differentiated class.

1) Priority Class (Class A): Mission critical traffic that require high availability, low loss service can utilize lightpaths of this class. Dedicated path protection (1:1 or 1+1) is used for this class of service and achieves the highest level of protection. Recovery of a link failure takes about 20ms for 1+1 or 40ms for 1:1. Up to about 20ms (failure detection and switching time at the end nodes, and possibly propagation delay) of data is lost after the failure. Protection resources are pre-allocated and the recovery paths are preconfigured (paths are computed and the switches along the paths are pre-set). Less data is lost when 1+1 is used, but 1+1 is more expensive operate compared to 1:1 because traffic needs to be actively duplicated and sent out over two live paths in the network. When 1:1 protection is used, protection paths can be used to carry the pre-emptable class traffic to reduce capacity cost.

2) Protected Class (Class B): Service classes with a lower level of protection requirement can be assigned to Class B. Shared path protection (1:N) is used for this class. Recovery paths are computed, but the switches along the paths are not preconfigured. This flexibility allows sharing of protection resource among different lightpaths and reduces capacity cost. Recovery takes about 90ms to complete with 50 to 90ms of data loss.

3) Reroutable Class (Class C): Reroutable traffic are given shortest path working paths and have no protection resource allocated for use. However, best effort rerouting may be done after a failure to recover some of the Class C traffic. Rerouting is done using the unused protection resources allocated for Class A and B after the Class A and B traffic are fully recovered. The average number of Class C traffic that cannot be rerouted after a failure is given in Section 5. Network service providers may reserve additional capacity to increase the recovery ratio. Shortest paths are assigned for this type of traffic to reduce total capacity cost. Rerouting can begin immediately after a failure and can take up to several seconds.

4) Unprotected Class (Class D): Class D traffic are also assigned shortest available paths in the network to reduce capacity cost. They have no protection from failures and cannot be rerouted. Data is lost during the entire lifetime of the failure, until a physical repair is made.

5) Pre-emptable Class (Class E): Pre-emptable class traffic are the cheapest to provision. Routing can take advantage of resources that are already provisioned for protection of either Class A or B traffic to reduce capacity cost. Furthermore, Unprotected traffic can be pre-empted to make room for rerouting class C traffic in case of a failure. Generally, data is lost until a physical repair is made, but more data can be lost if lightpaths were pre-empted to make room for Class A or B's recovery. Lightpaths that were pre-empted are brought back only after having the Class A or B traffic restored to their original working paths.

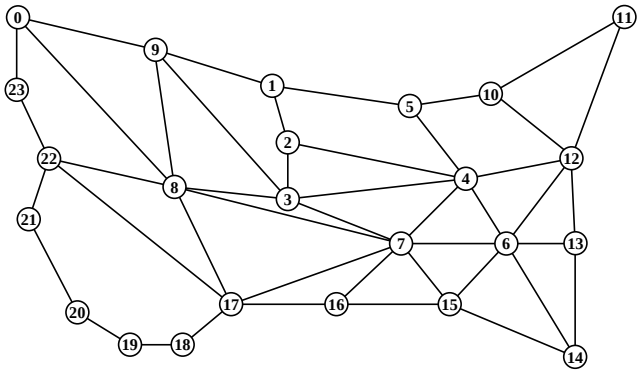

Fig. 1. The National network.

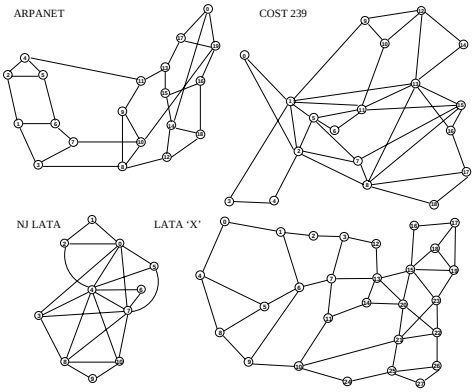

Fig. 2. Example Network

B. Classification Scheme

Table II shows 7 different protection based differentiation schemes that we evaluate. S1 and S2 represent 5 class differentiation scheme we propose for QoS routing at the optical layer. S1 improves capacity performance over S2 by using a novel sharing optimization explained in the next section. S3 and S4 consist of two classes of traffic differentiated by whether or not protection is provided. They only differ in the choice of protection algorithm used for the protected class traffic. S5–S7 are based on single class traffic. In S5, all lightpaths are unprotected. In S6 and S7, all lightpaths are protected. Like S3 and S4, S6 and S7 differ only by the choice of protection algorithm used.

IV. Capacity Assignment

An important motivation for having protection based QoS is to reduce network operation costs. An efficient capacity assignment scheme for protection based QoS is needed as the classification and the choice of protection services directly affect cost in terms of provisioned network capacity.

A. Routing and Wavelength Assignment

We assume uniform traffic demands which can effectively aid in capturing the different characteristics of the classification schemes. In the simulations, we perform dynamic on-line provisioning with uniformly distributed full-mesh traffic demands scaled by a factor of 10. Dynamic provisioning means that we have no knowledge of future demands, and cannot reroute existing connections on the network to optimize provisioning upon receipt of a new request. Each request is assumed to be a bidirectional connection with a uniformly distributed demand of 1 lightpath between each source and destination. Table II shows the traffic ratios between each class of traffic for the different classification schemes where 1 equals a uniformly distributed demand of full-mesh, $(N\times(N\text{-}1))/2$, bidirectional requests. Traffic demands are routed in random order to simulate an on-line provisioning process. Although, in practice, the demands may not be uniformly distributed among different requests, we believe that studying uniformly distributed traffic demands is sufficient in that it shows the characteristics of different protection schemes for comparison purposes. We assume that each λ-channel has a cost of 1 in terms of calculating capacity. The total cost of capacity is therefore the sum of the overall of working paths and the total number of the reserved protection λ-channels.

For both Class A and Class B with 1+1/1:1 and 1:N protection, we utilize a joint path selection method similar to the one used in [16]. The working and protection paths are selected together to minimize the capacity cost. We always route classes C and D using shortest paths. If Class E exists in the classification scheme, then routing depends on whether or not protection resources are reserved in the network. Class E lightpath are routed over an existing dedicated protection paths with the same source and destination. If protection resources are allocated to protect Class B, we find paths such that the cost is minimized via sharing with Class B's protection resources. If no sharing is possible, the algorithm automatically will choose shortest paths.

B. Sharing Optimization

The key to our optimization algorithm is the sharing of protection resources between two different protection differentiated classes utilizing dedicated path protection (Class A, 1:1/1+1) and shared path protection (Class B, 1:N). Preconfiguration of switches is the main difference between 1:1/1+1 and 1:N protection. Since switches are not preconfigured, 1:N algorithm can allow sharing between multiple protection paths as long as their working paths do not share a common failure mode. Paths protected by the 1:1/1+1 scheme cannot share resources with other 1:1/1+1 schemes because the switches must be preconfigured in order to provide rapid recovery.

We assign protection resources such that resources can be shared between protection paths if their working paths do not share common failure modes. 1:N, Class B, protection paths can share resources with any other protection path(s). In the optimized version of the sharing algorithm, a single Class A lightpath can share a protection channel with any number Class B lightpaths. Switches are then preconfigured to support recovery of the Class A lightpath, and when needed, reconfigured to support recovery of Class B lightpaths. The advantage of this optimization is discussed in the next section.

V. Performance Evaluation

Figure 3 shows the results of on-line provisioning performed on the National network (US Backbone with 24 nodes and 44

Network	S1	S2	S3	S4	S5	S6	S7
National	17414 (1.00)	18788 (1.079)	18862 (1.083)	22894 (1.315)	16000 (0.919)	25380 (1.457)	39000 (2.340)
Arpanet	11314 (1.00)	12270 (1.084)	12252 (1.083)	15164 (1.340)	10460 (0.925)	16334 (1.444)	26180 (2.314)
Cost 239	8286 (1.00)	8964 (1.082)	8944 (1.080)	10906 (1.316)	7660 (0.924)	11818 (1.426)	18480 (2.230)
Lata X	27004 (1.00)	29038 (1.075)	29360 (1.087)	35430 (1.312)	24840 (0.920)	39810 (1.474)	60140 (2.227)
NJ Lata	2134 (1.00)	2260 (1.059)	2294 (1.074)	2682 (1.257)	1920 (0.900)	2930 (1.373)	4460 (2.089)

TABLE III
TOTAL CAPACITY COST FOR DIFFERENT CLASSIFICATION SCHEMES NORMALIZED TO S1.

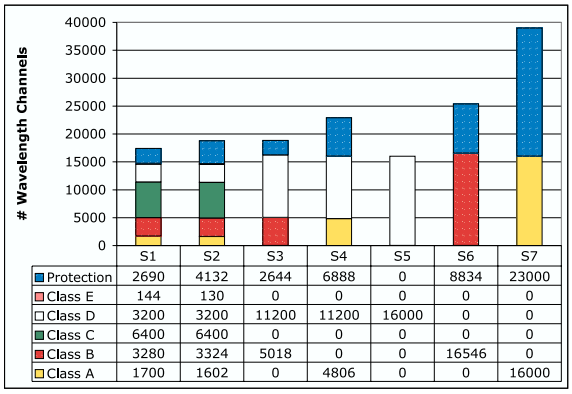

Fig. 3. On-line capacity provisioning results on the National network.

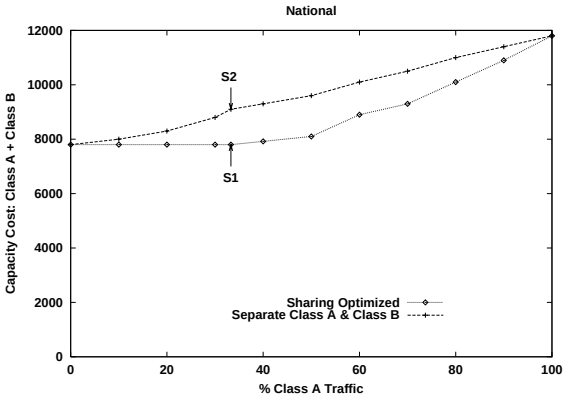

Fig. 4. Capacity for Class A and Class B traffic with varying percentage of Class A traffic for National. Arrows point to data at 1:2 ratio corresponding to data shown in Figure 1.

links, shown in Figure 1) with the seven different classification schemes previously explained in section 3.B. Protection requirements for all Class A and B traffic can be met with 8.8%(S1) and 17.4%(S2) additional capaciy compared to S5,which employs all unprotected traffic. S6 and S7 requires over 148% additional capacity compared to S1. Note that Class D traffic can be converted to Class C traffic on S3 and S4 at no additional capacity.

It is interesting to note that protection capacity on S1 is very close to protection capacity on S3. S3 consists of all Class B traffic, and therefore the are showing that the sharing optimization allows enough sharing of protection resources between Class A and Class B traffic that the efficiency is equivalent to using all 1:N protection. Figure 4 more directly shows the benefit of the optimization. The total traffic shown on Figure 4 is consistent with the demand used for results on Figure 3. The ratio between Class A and Class B is varied from 0 to 100 to show the optimization. At 33.3%, pointed by the arrows, the overall capacity cost is improved by 7.9% as also shown in Table III. We also measured the on-line provisioning cost in terms of capacity using the classification scheme provided in [11]. All demands can be provisioned with an addition of less than1% capacity over S5. The improvement comes from assuming that all unprotected traffic belong Class E (preemptable). Grouping all unprotected traffic to Class E is not attractive because lightpaths provisioned under Class E are susceptible to failures of other lightpaths.

We also simulated on-line provisioning using four other sample networks shown in Figure 2. Table III shows the total

	S1	S2	S3	S4	S5	S6	S7
Class E	$\frac{20.1}{20.1}$	$\frac{19.8}{19.8}$	—	—	—	—	—
Class D	$\frac{67.9}{67.9}$	$\frac{249.6}{249.6}$	$\frac{244.6}{244.6}$	$\frac{361.9}{361.9}$	—	—	—
Class C	$\frac{91.0}{137.9}$	$\frac{45.3}{135.6}$	—	—	—	—	—
Class B	$\frac{0}{74.5}$	$\frac{0}{75.5}$	$\frac{0}{114.0}$	—	—	$\frac{0}{376.0}$	—
Class A	$\frac{0}{38.6}$	$\frac{0}{36.4}$	—	$\frac{0}{109.2}$	—	—	$\frac{0}{363.6}$

TABLE IV
AVG # OF FAILED LIGHTPATHS / AVG. # OF LIGHTPATHS AFFECTED BY A LINK FAILURE (AVG. LINK LOAD).

capacity results for different classification under each network. Results show that the benefits of the differentiation via protection classification is consistent for the five sample networks used where S1 provides 7.4 to 8.4 percent improvement in capacity cost over S3.

Table IV shows the average failure count of each class of traffic under different protection differentiated classifications. The average number of lightpaths that are affected by a single link failure (average link load) for each protection class is also shown. Since recovery for Class C utilizes rerouting over

existing protection capacity, reducing capacity cost through sharing optimization reduces the available recovery resources for Class C. For S1, 91.0 out of 137.9 Class C lightpaths cannot be rerouted whereas for S2, 45.3 out of 135.6 Class C lightpaths are left unrestored.

VI. Conclusions

A protection differentiated classification scheme based on five protection classes was proposed. We also introduced a novel sharing optimization method that allows sharing of protection capacity between two different classes of traffic. We showed that using protection based classification can reduce network capacity cost by up to 130% on average over five sample networks. Results showed that about 8% additional capacity cost can be reduced by using our sharing optimization under protection differentiated classification.

References

[1] A. Dwivedi and R. E. Wagner, "Traffic model for usa long-distance optical network," in *Proceedings of the Optical Fiber Communication Conference*. OSA, March 2000, pp. 156–8, TuK1.

[2] J. Wu and H. T. Mouftah, "Integrated slip layer for ip over WDM," in *2000 Digest of the LEOS Summer Topical Meeting on Broadband Optical Networks*, July 2000, pp. 37–8.

[3] K. Murakami and H.S. Kim, "Virtual path routing for survivable atm networks," *IEEE/ACM Transactions on Networking*, vol. 4, 1996.

[4] D.J. Pai and H.L. Owen, "An algorithm for bandwidth management with survivability constraints in atm networks," in *Proceedings of IEEE ICC*, 1997, vol. 1, pp. 261–6.

[5] Y. Rekhter and T. Li, "A border gateway protocol 4 (bgp-4)," in *Internet Engineering Task Force RFC 1771*, March 1995.

[6] A. Bose C. Labovitz, A. Ahuja and F. Jahanian, "Delayed internet routing convergence," in *Proceedings of ACM SIGCOMM Conference*, 2000, pp. 175–87.

[7] R. Watterhofer C. Labovitz, A. Ahuja and S. Venkatachary, "The impact of internet policy and topology on delayed routing convergence," in *Proceedings of IEEE INFOCOM*, 2001.

[8] G. Hjálmtýsson A. Greenberg and J. Yates, "Smart routers - simple optics - a network architecture for ip over WDM," in *Proceedings of the Optical Fiber Communication Conference*. OSA, March 2000, ThU3.

[9] A. Monitzer A. Jukan and H. R. van As, "Service-specific recovery of wavelength connections in WDM networks," in *Proceedings of the Optical Fiber Communication Conference*. OSA, 1999, TuL1.

[10] H. R. van As A. Jukan, "Service-specific resource allocation in WDM networks with quality constraints," *IEEE JSAC*, vol. 18, no. 10, pp. 2051–61, October 2000.

[11] A. Autenrieth and A. Kirstädter, "Engineering end-to-end ip resilience using resilience-differentiated qos," *IEEE Communications Magazine*, vol. 40, no. 1, pp. 50–7, January 2002.

[12] S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks, part i: Protection," in *Proceedings of IEEE INFOCOM*, 1999, vol. 2, pp. 744–51.

[13] S. Ramamurthy and B. Mukherjee, "Survivable WDM mesh networks, part ii: Restoration," in *Proceedings of IEEE ICC*, 1999, vol. 3, pp. 2023–39.

[14] D. Johnson G. N. Brown M. C. Sinclair M. J. O'Mahony R. S. K. Chang, C. P. Botham and I. Hawker, "A multi-layer restoration strategy for reconfigurable networks," in *Proceedings of IEEE GLOBECOM*, 1994, vol. 3.

[15] H. Kobrinski and M. Azuma, "Distributed control algorithms for dynamic restoration in dcs mesh networks: Performance evaluation," in *Proceedings of IEEE GLOBECOM*, 1993, vol. 3, pp. 1584–8.

[16] S. Dixit C. Xin, Y. Ye and C. Qiao, "A joint working and protection path selection approach in WDM optical networks," in *Proceedings of IEEE GLOBECOM*, 2001, vol. 4, pp. 2165–8.

[17] A. Fumagalli and L. Valcarenghi, "The preplanned weighted restoration scheme," in *IEEE Workshop on High Performance Switching and Routing*, 2001, pp. 36–41.

[18] X. Su and C. Su, "An online distributed protection algorithm in WDM networks," in *Proceedings of IEEE ICC*, 2001, vol. 5, pp. 1571–5.

[19] B. Wauters B. Caenegem and P. Demeester, "Spare capacity assignment for different restoration strategies in mesh survivable networks," in *Proceedings of IEEE ICC*, 1997, vol. 1, pp. 288–92.

[20] S .Samieian D .Saha B. Rajagopalan S. Sengupta S. Chaudhuri R Ramamurthy, Z. Bogdanowicz and K. Bala, "Capacity performance of dynamic provisioning in optical networks," *OSA JLT*, vol. 19, no. 1, pp. 40–8, 2001.

[21] H. Fujii and N. Yoshikai, "Double search self-healing algorithm and its characteristics," in *Electronics and Communications in Japan-Part 1*, 1994, vol. 77, pp. 75–8.

[22] W. D. Grover, "The selfhealing network," in *Proceedings of IEEE GLOBECOM*, 1987, vol. 2, pp. 1090–5.

[23] T. H. Wu, "A passive protected self-healing mesh network architecture and applications," *IEEE/ACM Transactions on Networking*, vol. 2, no. 1, pp. 40–52, February 1994.

[24] T. E. Stern and K. Bala, *Multiwavelength Optical Networks; A Layered Approach*, Prentice-Hall, Upper Saddle River, NJ, 2000.