End-to-End Dedicated Protection in Multi-Segment Optical Networks

Srinivasan Seetharaman, Admela Jukan and Mostafa Ammar
Georgia Institute of Technology, Atlanta, GA
Email: {srini, ajukan, ammar}@cc.gatech.edu

***Abstract* - In this paper, we analyze the blocking probability of end-to-end protected lightpath setups in large-scale, interconnected optical networks. The networks we are focusing at are composed of multiple heterogeneous segments, interconnected by gateways. The networking segments refer to any portion of an optical path that requires special consideration for wavelength routing, such as separate administrative domains, sub-networks characterized by different levels of traffic aggregation (e.g. access and regional networks), or different optical technology networks. Based on the network model with segment, we study the following protection schemes: End-to-end link disjoint, End-to-end Gateway-Disjoint, Segment-Disjoint, and Concatenated Segments, and study their relative merits on the basis of segment-specific resources, traffic characteristic, gateway location and adaptation capabilities. For each of the proposed schemes, we analyze the benefits with respect to the above characteristics and present numerical results of blocking performances of different routing and protection algorithms.**

I.INTRODUCTION

The migration of real-time and high-priority traffic to IP networks means that modern IP networks increasingly carry mission-critical business data, and must therefore provide reliable transmission. Current routing algorithms can take a substantial amount of time to recover from a failure, which can be on the order of several seconds to minutes and can cause serious disruption of service in the interim. This is unacceptable for many applications that require highly reliable service, and has motivated network providers to give serious consideration to the issue of network survivability. Thus one of the important functions of the optical control plane is to restore network operation in the event of a failure.

Recently, end-to-end optical paths that involve various segments of optical networks, e.g. access, metro, backbone, have received attention. Segments of end-to-end optical paths refer to any portion of an optical path that requires particular consideration for wavelength routing. The segments (or, domains) are the result of partitioning of a network for administrative reasons, scalability of routing schemes, security and reliability, or technology differences in the systems of different domains. This division enables the handling of individual segments autonomously and makes the characteristics of the sub-networks homogenous. Usually, when dealing with multi-vendor interoperability, a networking segment represents part of the network in the data plane that comes from the same vendor. The policy constraints cause incompatibility between adjacent segments.

Various routing options are possible in multi-segment optical networks [4]. The End-to-end (E2E) scheme is suitable for networks, which possess complete global information. It performs optimal with regards to the blocking probability and the network utilization, but is not very scalable. Segment-specific schemes can be either hierarchical or based on concatenation of the shortest paths in each single segment. For the latter methods, by increasing the number of gateways and by altering their location and adaptation capabilities, the performance of an E2E scheme can be achieved, by keeping the routing information local and scalable.

Based on the multi-segment network model, this paper considers protection schemes where provisioning a dedicated backup path is done at the time of the time of the working path set-up. With such a scheme, an optical connection can perform protection switching in three different ways:

1) Local (span) protection - refers to the protection of the link between two neighboring switches.
2) Segment protection - refers to the recovery of a lightpath between the boundary-nodes of the segment.
3) End-to-end protection - refers to the recovery of an entire lightpath from the ingress to the egress port.

Each of the above methods involves different routing and signaling models. For example, the first two methods of protection do not require any external information. Most of the multi-segment issues arise in the case of end-to-end protection or restoration. The type of repair (mentioned above) is recommended to be globally uniform.

This paper concentrates on the last method, end-to-end protection and presents the following protection schemes: Basic End-to-End Link-Disjoint, Gateway-Disjoint, Segment-Disjoint, and Concatenated Segments, and study their relative merits on the basis of segment-specific resources, traffic characteristic, gateway location and adaptation capabilities. For each of the proposed schemes, we analyze the benefits with respect to the segments' characteristics and present numerical results of blocking performances of different routing and protection algorithms.

A. Related Work

Overall, very little research effort has been spent on analyzing an interconnected all-optical infrastructure, which would allow fully protected all-optical end-to-end paths. The initial work on multi-segment WDM networks was inspired by [9], which to the best of our knowledge is the only paper that so far has considered all-optical network interconnection based on WDM. The research effort in this paper tends to complement the multi-segment routing schemes in [4]. The network model and other assumptions developed for routing are similar to that of protection, as we have chosen the 1+1 dedicated backup path.

There is substantial research done in the field of sub-path protection. The basic idea behind this scheme is to concatenate different protection domains [5] [6] [7] [8], so that service recovery can be provided end-to-end. A given service may cross multiple networks and these may employ different recovery mechanisms. It is considered that the recovery mechanisms in different domains may operate autonomously, and that multiple points of attachment may be used between domains (to ensure there is no single point of failure). Clearly, computational complexity will decrease drastically as the network size grows larger.

In [10], various methods to calculate the so-called service restorability are shown. The method of 1+1 protection at the connection set-up is shown is evaluated in terms of blocking probability and restorability. The focus was on service-differentiated protection.

II. End-to-End Dedicated Protection Schemes

The key objective of this research effort is to develop protection mechanisms for multi-segment paths with segment-specific properties. This section briefly explains the network model adopted for analysis and describes the proposed schemes. No traffic preemption is assumed for dedicated protection paths.

A.Network model

The network model adopted in this research is similar to that used in [4]. The model is a general tool to estimate the blocking probability of multi-segment lightpath provisioning and is capable of capturing the following unique properties:

1) Segment-specific properties, such as particular network topology per segment and particular location of the gateways between them, network load per segment, wavelength capacity and type of wavelengths, or different wavelength converter density per segment.
2) Global (inter-segment) and local (intra-segment) traffic.
3) Gateway adaptation on segment boundaries, e.g. adaptation between different numbers of wavelengths.

In multiple WDM networks interconnected by gateways, traffic may originate from and be destined to any network. The proportion of global or local calls affects the blocking probability of all connections. The gateway is a logical entity, which acts as the interface between two adjacent segments. Each network has a number of gateways to each of its neighbors. The gateway has its own wavelength shifting ability, adaptation capabilities and traffic load constraints. Fig.1 illustrates a typical multi-segmented optical network. The link *B*-*E* is a gateway link and for purposes of analysis is considered as a single node. Nodes *B* and *E* are the border routers of the network-to-network interface (NNI) and Node *G* is an example of an internal node. This model doesn't support multi-homing i.e., each border router connects a single other border router. The number of wavelengths per link, i.e. wavelength capacity is assumed to be uniform on all links within each segment. Different segments can have different wavelength capacity, provided there is an overlap.

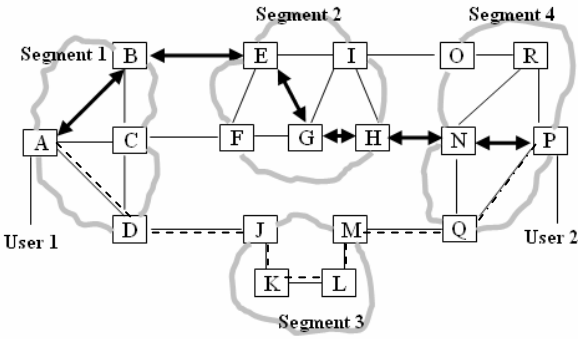

Fig.1. Typical scenario to illustrate multi-segment optical protection. The bold arrows indicate the working path of *User1–A–B–E–G–H–N–P–User2* and the double lines indicate a link disjoint backup path of *User1–A–D–J–K–L–M–Q–P–User2*

Following the example shown in Fig.1, we will next illustrate three different backup path computation strategies. They have been identified based on the different hierarchies involved. The schemes have been explained based on the sample topology of Fig.1, with only link disjointedness taken into consideration.

- **Basic End-to-End (BE2e)** – Each node has complete information about the whole system. The backup path computation proceeds like it were a single-segment scenario. The scheme isn't as scalable and works well in case of an unified management system. This declares the next best path from *User1* to *User2* in Fig.1 as the backup path. (E.g.: *User1–A–C–F–G–I–O–R–P–User2*)
- **Disjoint Segment (DS)** – The backup path does not have any segments common with the primary path. A top layer view is adopted while performing the routing operation. The aggregated or summary information of each segment is sufficient. It is subject to any special policy constraints between segments. The only condition is that the source and destination segment should be the same. In Fig. 1, the backup path is routed through *Segment 3*, *e.g. User1–[A–D]–[J–K–L–M]–[Q–P]–User2*)
- **Concatenated segment (CS)** – The backup path follows the same sequence of segments as the working path and adopts the same gateway nodes, too. The alternate path is computed for each segment and appropriately activated. This scheme is considered to be segment conserving. Based on the notification option and segment properties, the restoration is segment specific or end-to-end. The path computation probability is the same in either case. Generally, the fault is managed within the particular segment without external interaction. Unlike sub-path protection [5], it considers multi-segment issues for path computation and fault management. In Fig.1, the backup path is computed on a per-segment basis, e.g. *User1–[A–C–B]–[E–I–H]–[N–R–P]–User2*

The blocking probability for establishing the backup path in the above-mentioned schemes is discussed in the next section. While there are different kinds of redundancy – N:M shared or 1:1, 1+1 dedicated, the mode adopted for performance analysis is 1+1 dedicated path protection. This means that the switchover is guaranteed in the event of a failure. For Fig.1, if there is a fault in link *E-G*, the traffic will be routed through:

- BE2e scheme : *F-G-I*
- DS scheme : *Segment 3*
- CS scheme : *E-I-H*

B.Disjointedness constraints

To ensure that the traffic switchover is successful, the working path and the backup path should have no resources common. This eliminates the single point of complete failure. IETF defines a Shared Risk Link Group (SRLG) set for each connection. The system computes the backup paths by running the RWA problem with few extra constraints.

a) The working and protection lightpaths must be node and link disjoint for the protection mechanism to be effective.
b) No two working paths that share the same SRLG values can have the same protection path. This constraint has been imposed to remove the resource conflict in the event of a node / link failure.

Fig.1 lists the backup path computed with each of the three schemes having only links disjoint. Table I lists the possible routes considering disjointedness with nodes and gateways. Backup paths computed by CS can only be link disjoint.

TABLE I. Backup paths for the network topology given earlier, with different disjointedness constraints.

Prot. Type = BE2e	
Link + Node Disjoint	User1–A–D–J–K–L–M–Q–P–User2 (Increased blocking probability; Possibility of backup path being locked out)
Link + Gateway Disjoint	User1–A–C–F–G–I–O–R–P–User2 (No extra change, unless gateway has one-to-many connections)
Prot. Type = DS	
Link + Node Disjoint	User1–[A–D]–[J–K–L–M]–[Q–P]–User2 (Increased blocking probability owing to reduced resources in src and dest domain)
Link + Gateway Disjoint	User1–[A–D]–[J–K–L–M]–[Q–P]–User2 (Not much of a change, unless enforced across the UNI)

C.Interworking between routing and protection

Both routing and protection schemes can be different in different segments and interoperate within the same category (A, B or C) as mentioned in Table II. The working path is computed by any type of routing algorithm [4]:

- End-to-end global – The system has global information and path is computed as if it were just a single segment.
- Hierarchical – Similar to that used in OSPF with the segments having summary information of other neighboring segments over the local information.
- Concatenated – The segment has no external information and route computation follows a greedy algorithm. The path is computed in each segment and fused together.

For a given routing scheme, there can be a mix of different protection scheme for the different connections existing. We can define a set {a, b, c, d} where 'a' represents the percentage of connections not protected, 'b' corresponds to scheme BE2e, 'c' refers to DS and 'd' connections have CS. The system administrators need to find the optimal 'a', 'b', 'c', 'd' such that the utilization, blocking probability, restoration time and other administrative constraints are met.

TABLE II. Interworking between routing & protection

Index	Routing	Protection	Code
A	Global (Pseudo-single domain)	None (0)	1_0
		BE2e (1)	1_1
		DSP (2)	1_2
		CSP (3)	1_3
B	Hierarchical (Like OSPF) Have local info + Summary of neighbors	None (0)	2_0
		DSP (2)	2_2
		CSP (3)	2_3
C	Concatenated Have only local info	None (0)	3_0
		CSP (3)	3_3

III.SIMULATION RESULTS

This section presents the simulation results for blocking performance. Since the paper considers 1+1 dedicated backup path, the blocking probability is of foremost concern. The schemes proposed are simulated in a network, as shown in Fig.2, and compared qualitatively. The adopted network has 8 segments with 4 being bi-directional rings at the metro edge of the network and the remaining 4 being mesh-torus at the core. The physical topology of the metro ring consists of 36 nodes and that of the mesh-torus core consists of 7x7 nodes. For illustration, the core is partitioned into 4 segments. All segments in the network have a capacity of 8 wavelengths per link. The metro rings serve as the user and the mesh serves as the optical network. The routing and protection schemes are applied over both the user-to-network interface and the NNI.

The different schemes perform the same for intra-segment calls. Hence, the proportion of global traffic is set at 100% for accurate comparison. The gateway is selected at random, redundancy is set at 100%, wavelength conversion is restricted inside a segment, and only link disjointedness is considered for initial comparison.

In the blocking probability measurements, the connection requests arrive according to a Poisson process. Call durations are independent and exponentially distributed All calls are equally likely to arrive at any node within the source segment, and equally likely to be destined to any other node

within any other segment. A call is blocked if either the path or the wavelengths for allocation cannot be found. Each data point in the simulation was obtained using 10 x 10^4 call arrivals after a transient state of 1 x 10^4 call arrivals. Intermediate nodes are not capable of doing wavelength shifting while gateways are assumed to do full shifting. The experiment does not simulate faults and calculates blocking probability assuming safe operation.

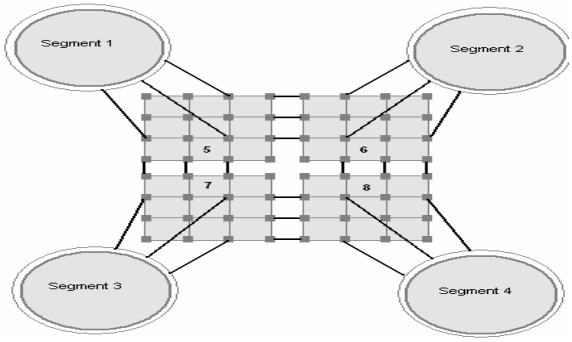

Fig.2. Logical topology of the network with triple gateway interconnection. The dark lines indicate the gateway links.

The simulation experiment compares the performance of the previously mentioned schemes, with 1:1 (or) 1+1 dedicated protection being the mode. In that scenario, each call requests two constrained paths from the network. The constraints reflect the type of protection in place and characteristics of the network. The working path and the dedicated backup path should be devoid of any overlap in resources (e.g. in terms of links, nodes, or gateways). The call setup consists of path calculation and wavelength allocation for the working and dedicated backup path. The other protection modes, like shared restoration, are out of the scope of this paper. The backup path is not used for sending any extra traffic and assumed to be unusable by other calls.

The six different combinations (as indicated in Table I), with dedicated protection, perform identically when the global probability is zero. This means that in the case where the network has only local calls, the different protection schemes behave in a similar manner. To accurately compare the performance of the different schemes, we take into account the case with global calls only. These calls necessarily have different source and destination domains. More the gateway interconnections, the better the probability of establishing calls. The number of gateways does not matter much with the CSP scheme because the working and backup paths share the same gateways in each of the segment it traverses. The DSP scheme depends more on the number of neighboring segments.

Fig.3 and Fig.4 present the relative blocking performance of each of the combinations in the simulated network with only link disjointedness. The joint blocking probability is plotted against the increasing segment load. The naming convention for each of the plot is as described in Table I. Fig.3 represents the blocking probability taking into account the wavelength occupancy. The path computation is dynamic and considers capacity of each link. This provides a better chance for a successful backup path. Fig.4 represents the blocking probability for shortest path based static routing. The backup path is computed using Dijkstra's algorithm, without any wavelength considerations. Wavelength allocation is not guaranteed, thereby causing an increased blocking probability relative to dynamic routing.

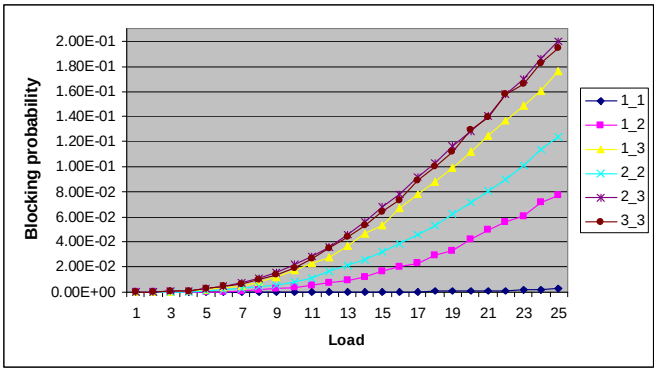

Fig.3. Joint blocking probability for dynamic path routing

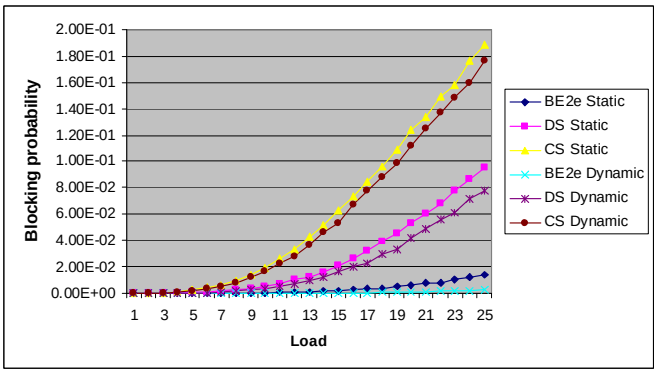

Fig.4. Joint blocking probability of Dynamic vs. Static protection path. The routing scheme is end-to-end global.

Irrespective of the routing scheme adopted, the BE2e protection scheme performs the best. This is attributed to the fact that the global information provides better chances for a successful backup path. The CSP scheme performs the worst among all methods because it needs to adopt the same gateway link as the working path. This has a higher probability for blocking owing to unavailability of free wavelengths. The DSP scheme performs intermediate because of reduced candidate gateways at the intermediate segments relative to the BE2e scheme.

The effort in this paper tries to highlight the behavior of a system requesting 1+1 protection service and helps choose a good combination of routing and protection schemes. This joint selection is crucial for the success of the call. Not all systems are capable of supporting BE2e protection scheme. The system needs to possess global information and tends to be unscalable. The global control of individual segments tends to be complicated. The DS and CS schemes can provide a closer approximation to BE2e by modifying gateway level

parameters, thereby reducing the computational complexity, storage requirements etc. DS backup paths bring in higher disjointedness making the system more fault tolerant. CS backup paths can be activated on a segment basis leading to a shorter restoration time.

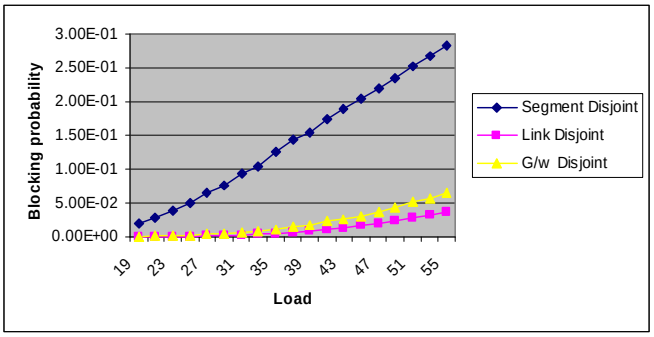

Fig.5. Blocking probability for BE2e Gateway Disjoint scheme relative to BE2e Link Disjoint, Segment Disjoint

In multi-segment networks, the gateway can increase the blocking probability considerably, owing to minimum amount of resources and less number of gateway uplinks. Moreover, the gateway can serve as a single axis of failure in most cases. Hence, forcing the backup path to take a route having no gateway in common with the working path has inherent advantages (like increase in the fault tolerance level). Fig.5 indicates that the blocking probability does not increase substantially when gateway disjointedness is enforced over link disjointedness. However, having the backup path segment disjoint incurs a much higher penalty.

TABLE III. Resource utilization for different combinations

Protection	Avg. overuse factor	Avg. working hop count	Avg. backup hop count
Routing = End-to-end			
BE2e Link disjoint	2.558	10.394	21.966
BE2e G/w disjoint	2.588	10.394	22.220
DSP	6.200	10.394	53.671
CSP	8.684	10.394	76.196
Routing = Hierarchical			
DSP	2.529	25.270	49.978
CSP	3.373	25.270	64.947
Routing = Concatenated			
CSP	4.836	19.054	71.258

Table III lists the average overuse factor and the hop count values for the different combinations. For the topology adopted in our discussion, it can be noted that BE2e-link-disjoint performs the best with regard to resource usage, closely followed by BE2e-gateway-disjoint. The BE2e protection schemes are capable of choosing the next best path on an end-to-end basis with no extra constraints. The restoration latency is high for BE2e as the notification of end users takes substantial time. The constraints of choosing a particular segment sequence seem to increase the overuse factor in DSP and CSP. The average backup hop count of each scheme explains the extra resources (links) used. This is more dependent on the topology and is always greater than the working path length.

The blocking probability of each scheme was observed to improve when wavelength-shifting facility was provided within all segments. The concept of an optical service can also be introduced, as in [10]. However, when the simulation was performed for a multi-service system of the same characteristics, with one in 10 connections requesting for protection, the blocking probability distribution was observed to have the same behavior.

IV. CONCLUSIONS

In this paper we presented three protection schemes for usage in the multi-segment optical networks. The schemes perform differently based on different factors like protection mode, wavelength reachability, topology, gateway selection, and proportion of global traffic. On the basis of blocking probability and resource utilization, the BE2e (both link disjoint and gateway disjoint) was noticed to be the best performing scheme, followed by DSP and then CSP. This is attributed to the absence of constraints and presence of global information. However, BE2e schemes tend to be unscalable and inherit high restoration times. The fault management issues and shared protection forms of the scheme are reserved for future study. The results of the simulation are particular to the adopted topology and are a first step towards analyzing protection schemes for multi-segment networks.

REFERENCES

[1] Lang, J., Rajagopalan, B., et al, *"Generalized MPLS Recovery Functional Specification,"* Internet Draft draft-bala-gmpls-recovery-functional-00.txt, August 2002

[2] E.Mannie et al., *"Recovery (Protection and Restoration) Terminology for GMPLS,"* Internet Drafts draft-ietfccamp-gmpls-recovery-terminology-00.txt, Jun 2002.

[3] S.Makam et al., *"Building a reliable MPLS networks using a path protection mechanism,"* IEEE Communications Magazine, March 2002.

[4] Y. Zhu, A. Jukan and M. Ammar, *"Multi-segment Wavelength Routing in Large-scale Optical Networks,"* ICC2003.

[5] C.Ou, H.Zang and B.Mukerjee, *"Sub-path protection for scalability and fast recovery in WDM mesh networks,"* Proc. OFC 2002, March 2002.

[6] Pin-Han Ho, H.T. Mouftah, *"SLSP: A new path protection scheme for the optical Internet,"* OFC2001, TuO1-1

[7] Anand, S. Chauhan and C. Qiao, *"Sub-path Protection: A New Framework for Optical Layer Survivability and its Quantitative Evaluation,"* Technical report, Feb 2002.

[8] Todimala and B. Ramamurthy, *"A Dynamic Partitioning Sub-Path Protection Routing Technique in WDM Mesh Networks,"* ICCC '02, Aug. 2002

[9] A. R. Hajare, *"Simulating Multi-Segment LANs,"* IEEE Infocom 1994.

[10] A. Jukan, *"QoS-Based Wavelength Routing in Multi-Service WDM Networks,"* Springer Verlag, New York-Vienna, 2001.