Optical Switching and Networking 9 (2012) 271–285

Contents lists available at SciVerse ScienceDirect

Optical Switching and Networking

journal homepage: www.elsevier.com/locate/osn

Resource efficient network design and traffic grooming strategy with guaranteed survivability

Arunita Jaekel, Ataul Bari *, Quazi Rahman, Ying Chen, Subir Bandyopadhyay, Yash Aneja

School of Computer Science, University of Windsor, 401 Sunset Avenue, Windsor, ON, N9B 3P4, Canada

ARTICLE INFO

Article history:
Received 18 May 2010
Received in revised form 5 April 2012
Accepted 16 April 2012
Available online 16 May 2012

Keywords:
Optical network
Traffic Grooming
Logical topology design

ABSTRACT

In WDM networks, path protection has emerged as a widely accepted technique for providing guaranteed survivability of network traffic. However, it requires allocating resources for backup lightpaths, which remain idle under normal fault-free conditions. In this paper, we introduce a new design strategy for survivable network design, which guarantees survivability of all ongoing connections that requires significantly fewer network resources than protection based techniques. In survivable routing, the goal is to find a Route and Wavelength Assignment (RWA) such that the logical topology remains connected for all single link failures. However, even if the logical topology remains connected after any single link fault, it may not have sufficient capacity to support all the requests for data communication, for all single fault scenarios. To address this deficiency, we have proposed two independent but related problem formulations. To handle our first formulation, we have presented an Integer Linear Program (ILP) that augments the concept of survivable routing by allowing rerouting of sub-wavelength traffic carried on each lightpath and finding an RWA that maximizes the amount of traffic that can be supported by the network in the presence of any single link failure. To handle our second formulation, we have proposed a new design approach that integrates the topology design and the RWA in such a way that the resulting logical topology is able to handle the *entire* set of traffic requests after any single link failure. For the second problem, we have first presented an ILP formulation for optimally designing a survivable logical topology, and then proposed a heuristic for larger networks. Experimental results demonstrate that this new approach is able to provide guaranteed bandwidth, and is much more efficient in terms of resource utilization, compared to both dedicated and shared path protection schemes.

1. Introduction

Recent advances in wavelength division multiplexing (WDM) allow a single lightpath [1,2] to support data rates of up to 40 Gbps (OC-768) or even higher in current networks. Individual requests, on the other hand, require much lower rates, typically in the range of 155 Mbps (OC-3) to 622 Mbps (OC-12). Therefore, to ensure effective resource utilization, it is essential to share the capacity of a lightpath among several low-speed requests. *Traffic grooming* techniques [3–10] for optical networks have been introduced to effectively handle the capacity mismatch between individual traffic requests and the lightpaths over which these low-speed traffic requests must be routed. In this context, traffic grooming strategies can be classified into two broad categories—*static traffic grooming* [8] and *dynamic traffic grooming* [10]. Static grooming is used when the traffic requests are known in advance and do not change significantly over relatively long periods of time. In this case, it is reasonable to spend a considerable time to determine an optimal grooming strategy. Dynamic

[*] Corresponding author.
E-mail addresses: arunita@uwindsor.ca (A. Jaekel), ataulbari@gmail.com, bari1@uwindsor.ca (A. Bari), rahmanq@uwindsor.ca (Q. Rahman), chen13r@uwindsor.ca (Y. Chen), subir@uwindsor.ca (S. Bandyopadhyay), aneja@uwindsor.ca (Y. Aneja).

1573-4277/$ – see front matter © 2012 Elsevier B.V. All rights reserved.
doi:10.1016/j.osn.2012.04.004

grooming is appropriate when the pattern of user requests is not known and connections must be set up on arrival of requests. In this paper, we address the static traffic grooming problem.

A highly simplified model of the *physical topology* of an optical network is a graph $G_P = (V_P, E_P)$, where V_P denotes the set of nodes in the network and E_P denotes the set of edges in the network [1]. Here each node is either a *router node* or an *end-node* and each edge is a single unidirectional link in the network, representing a fiber from one node to another. Once the lightpaths have been deployed, only the optical connections need to be considered for traffic grooming. It is convenient to view the network as a set of connections at the optical layer level, where each connection is a lightpath and is best represented by a *logical topology* (also called *virtual topology*) [1,2]. A logical topology is defined by a graph $G_L = (V_L, E_L)$, where V_L denotes the set of end-nodes in the network and E_L denotes the set of logical edges in the network [1]. If there is a logical edge $x \rightarrow y$ in G_L, there is at least one lightpath from end-node x to end-node y in the network.

Since each fiber can carry 100 or more lightpaths, the failure of a single fiber typically results in the disruption of several lightpaths where each lightpath is carrying an enormous amount of data, it is clear that disruption of this traffic, even for a brief period of time, is a serious event. Many schemes have been proposed to handle such faults in WDM networks [11–17]. A standard approach for handling single link failures (in most cases resulting from a fiber cut [14]) is the use of *path protection* techniques [15,18]. In this approach, for every logical edge in the network, resources for two edge-disjoint lightpaths—a *primary lightpath* and a *backup lightpath* are allocated at design time. In *dedicated protection*, the resources allocated to a backup path cannot be shared with any other primary or backup path. *Shared path protection* improves resource utilization by allowing resource sharing among two or more backup paths, if the corresponding primary paths are edge-disjoint [19]. Both dedicated and shared path protection schemes require resources to be reserved for backup paths, which typically remain idle during normal fault-free operations. Approximately 50% of network resources remain idle in fault-free operations in dedicated path protection schemes. This is reduced to some extent in the case of shared path protection. An alternative to the path protection schemes is the *restoration scheme*, which involves a search for spare resources to set up lightpaths to replace the lightpaths disrupted by a fault. Although restoration schemes lead to more efficient resource utilization, they typically do not guarantee survivability of all ongoing connections. It is important to note that, if a path protection scheme is used, the logical topology *does not change* when there is a single link failure, since each primary lightpath that uses the failed link is replaced by the corresponding backup lightpath [18]. Similarly, if a restoration is successful, we note that the logical topology does not change, since each disrupted lightpath, say from source s_i to destination d_i, is replaced by a new lightpath, also from s_i to d_i.

An alternative approach to fault-tolerant network design uses the concept of *survivable routing* (SR). Given a logical topology (or a set of lightpaths) and an underlying physical fiber network, a survivable routing of the lightpaths ensures that the Route and Wavelength Assignment (RWA) [20] of the lightpaths is done in such a way that a single link failure does not disconnect the network [21]. However, there may be multiple survivable routings (or none at all) for a given topology. It is quite possible that some of these are capable of supporting more traffic, in the case of a fault, and hence are more “desirable” compared to others.

We have taken advantage of the fact that the amount of traffic that can be supported by a network, in the presence of faults, can be significantly increased by modifying the grooming strategy in response to a fault. In other words, when there is an link fault, we may reroute some (or all, if possible) individual (sub-wavelength) traffic requests to avoid disrupted lightpaths. Traditional SR techniques simply focus on maintaining a connected topology by properly choosing a RWA scheme for the lightpaths and do not exploit the possibility of modifying the traffic grooming techniques to ensure that the entire set of requests for data communication can be handled in the case of a fault. In the approaches explored in this paper, we do not protect or restore a lightpath in the case of a link failure. When there is a fault, we allow the logical topology to change since the lightpaths which use the faulty link are no longer operational. We have studied the extent to which the network can handle traffic requests, in the case of a fault, by a proper choice of:

(i) the logical topology,
(ii) the RWA and
(iii) a traffic grooming strategy for each fault scenario.

For a specified physical topology of the network and the sub-wavelength traffic requirements that have to be supported, we have looked at the following related problems:

Problem (1) Given a logical topology, find a RWA and a traffic grooming strategy, for every single (physical) link failure, that maximizes the total amount of weighted[1] traffic that the network can handle, under all single link failure scenarios.
Problem (2) Given a physical topology, the capacity of a lightpath and the number of transceivers at different end-nodes, find a logical topology, the corresponding RWA and a traffic grooming strategy that guarantees that the entire set of requests for communication can be supported by the network under any single link failure in the physical layer.

It is important to note that problem 1 and problem 2 are two *separate and independent problems* and should not be viewed as two sequential steps in a two-step design process. Problem 2 is the complete, generalized problem, solved in an integrated manner, for an optimal solution.[2] Problem 1 is a subset or simplification of

[1] The weight of a request for communication denotes the priority given to that request.

[2] We have used an integer linear program (ILP2 described in Section 4) for an optimal solution and have suggested H-STG as a heuristic to handle larger networks.