CCIT Report #596 July 2006

Designing Low-Capacity Backup Networks for Fast Restoration

ABSTRACT

There are two basic approaches to allocate protection resources for fast restoration. The first allocates resources upon the arrival of each connection request; yet, it incurs significant set-up time and is often capacity-inefficient. The second approach allocates protection resources during the network configuration phase; therefore, it needs to accommodate *any* possible arrival pattern of connection requests, hence calling for substantial *over-provisioning* of resources. In this study we establish a novel protection approach that overcomes all the above drawbacks.

During the network configuration phase, we construct an (additional) low-capacity *backup network*. Upon a failure, traffic is rerouted through a bypass in the backup network. We establish that, with proper design, backup networks induce *minor* capacity overhead. We further impose several design requirements (e.g., hop-count limits) on backup networks and their induced bypasses, and prove that, commonly, they also incur minor overhead. Our approach offers additional benefits, most notably: traffic demands can be routed in an *unprotected* fashion, using standard routing schemes; moreover, upon a failure, control effort and congestion on the (primary) network are *small* and *localized* since affected traffic is immediately rerouted through the backup network. Motivated by these findings, we design efficient algorithms for the construction of backup networks.

Keywords

Fast-Restoration, Network Design, Graph-Theory.

1. INTRODUCTION

Transmission capabilities have increased to rates of 10 Gbit/s and beyond [10]. With this increase, any failure may lead to a vast amount of data loss. Accordingly, fast restoration has become a central requirement in the design of high-capacity networks e.g., optical mesh networks. It has been recognized that, for many practical settings, the speed and capacity of the involved links do not allow to activate restoration mechanisms *after* the failure. Thus, *protection resources* must be allocated in advance i.e., *before* a failure occurs [13].

There are two basic approaches to allocate protection resources. In the first approach, resources are allocated *on demand* i.e., upon the arrival of every bandwidth request, thus incurring a significant overhead in terms of connection set-up time. Consequently, this approach presents a clear tradeoff between the efficiency of the resulting solution in terms of capacity usage and the time needed to compute it; furthermore, its corresponding solutions are usually based on *only* partial (or no) information regarding the network state and future connection requests. A different approach is to pre-allocate the protection resources *during the configuration phase* of the network. While this approach enables to perform computations offline, it requires allocating protection resources for *any* potential pattern of connection requests; hence, it usually calls for a substantial *over-provisioning* of protection resources.

In this study we introduce a novel protection approach, which overcomes all the above drawbacks and incurs a negligible toll of protection resources. The proposed approach is based on allocating *dedicated resources* to be used *exclusively* for handling failures. In essence, given a *primary network* that is used in normal operation mode to route demands (in an unprotected manner), we propose to establish a (low-capacity) *backup network* that can protect against *any single failure* experienced by the primary network; i.e., upon a failure of any primary link $e=(u,v)$, the traffic on e is rerouted from u to v through bypass paths that exclusively belong to the backup network. We formulate this notion as a network design problem with the objective of minimizing the total spare capacity of the backup network. The following example illustrates this idea.

Example 1: Considering Fig. 1, the solid lines represent the connectivity in a given (unprotected) primary network. Assume that the network is undirected and the capacity of all links (in each direction) is 1 except for the (bold) links (a,f) and (f,e) that have a capacity of 5. The dashed lines with indicated capacities represent a backup network. It is easy to verify that this backup network indeed provides protection against any single link failure in the primary network. For example, upon a failure of the (unit capacity) link (b,e), it is possible to reroute (exclusively over the backup network) one flow unit through the bypass path (b,c,d,e). Similarly, when link (a,f) that has a capacity 5 fails, it is possible to send one flow unit over the bypass path (a,e,f) and 4 flow units over the bypass path (backup link) (a,f). Note that bypass paths that protect

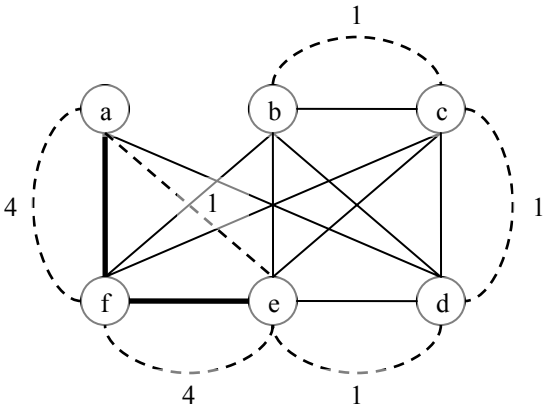

Fig. 1: A primary network and a corresponding backup network.