

A Perspective on Network Restoration

Deep Medhi

Abstract

An important issue in the design and deployment of communication networks is the issue of network restoration to address for various types of failures. In this exposition, we consider a variety of networks and networking technology and argue that networks can be broadly classified as either traffic networks or transport networks. We then present optimization models for network protection for link failures and discuss how they fit into this classification. We then discuss the process of network restoration and interaction between the traffic and the transport network. Finally, we also discuss situations and failures for which restoration is difficult to model—an area that requires further exploration.

Index Terms

IP networks, circuit-switched networks, optical networks, traffic and transport networks, multi-layer networks, network optimization modeling, network protection design.

I. INTRODUCTION

Network restoration refers to the ability of a network to restore or recover from a failure. The difficulty with this subject is that there are diverse issues such as how capable the network is to do restoration (and the capability the network has), to what extent the network can do it (fully or partially), what type of failure it is, the cost of network restoration and protection. To complicate matter, we have different types of networks as well as networks of networks; furthermore, technological changes are happening almost every day.

Often, we also tend to look at network restoration from the point of view of a specific technology, for example, how do we restore an IP network, or how do we restore a SONET network. However, as capabilities change, the technological distinction and functionalities have made it difficult to see what to do and where to do in terms of restoration. We also need to understand the role of protection (especially pre-planned) in network restoration. In this paper, our interest is primarily about network restoration from a link failure for different types of networks. We start with a simple example about considering a failure in a network and then discuss different technologies. We then argue that most networks can be broadly classified either as traffic networks or transport networks. After that, we present a representative set of optimization models that can be applicable in a traffic or transport network setting for protection and restoration design. This is followed by considering a sample of different networks and discussing possible approaches for network restoration. Finally, we discuss different types of failures faced by a network; in particular, we discuss the issue of failure propagation (usually from one network to another) and how that can impact recovery from a failure.

II. A SIMPLE ILLUSTRATION

Consider a three-node network (Figure 1) where we have average traffic demand of 20 units between each pair of nodes. The nodes are connected by links, each with capacity of 150 units.

November 2004, revised January 2005.

D. Medhi is with the Department of Computer Science and Electrical Engineering, University of Missouri–Kansas City, MO 64110 USA (e-mail: dmedhi@umkc.edu).

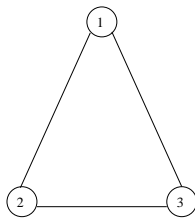


Fig. 1. Three-node network

Suppose a link fails in the network, say it is the link 2-3. In this case, the traffic between nodes 2 and 3 which normally would use the link 2-3 could be routed via path 2-1-3. This however depends on whether the network has the ability to switch (re-route) traffic from one route to another route. In other words, whether node 2, on knowing that the link 2-3 has failed, can switch traffic quickly to path 2-1-3. If we assume that the network has this capability, then the traffic would be rerouted without any perceived effect since there is plenty of bandwidth (capacity) available on links 1-2 and 1-3 to carry the traffic between 2 and 3. Thus, in this case, the link 2-3 is not necessarily needed to be restored (at least immediately) and the failure may not be perceived in the network at the user level.

Consider now for a moment that dynamic rerouting is not available in this network, i.e., the network has only static routes where routes are only direct-link routes. In this case, with the link failure of 2-3, the traffic between 2-3 can not be restored. The only way to address this case is to bring the link 2-3 up (somehow). These two situations illustrate two important points. If the network has enough bandwidth¹ and the network has dynamic routing capability, then traffic restoration is almost immediate and not perceived without requiring the link to be physically repaired. On the other hand, if the network does not have dynamic routing capability, i.e., it only has static routing, then this is not possible.² These two observations often hold in most communication networks, irrespective of the actual technology as long as the networks property described (dynamic routing or static routing) is available.

Consider next a slightly different traffic loading scenario. That is the traffic demand between nodes 2 and 3 is 140 units while all the other values remain the same as before. In this case, under the normal scenario, the network has the capacity to carry all traffic; however, this is not so if any of the links fails. If the goal of the network is to provide 'full' restoration, then the only way to do this would be to have restoration (or protection) capacity in the network ahead of time so that when the failure occurs, the network can bank on this protection capacity to route the traffic.

There are several aspects that the simple example discussed so far does not cover. For example, how does the above hold when the network is large? Are there other factors that play a role (or roles)? How about the actual technology of a network? And so on. In order to delve more into these aspects, we need to understand certain properties of different networking technologies.

III. TECHNOLOGY OVERVIEW

We can see from the illustration in the previous section that a closely intertwined topic with restoration is network routing. This also helps us to define the domain of our work here: we consider here network restoration for networks where routing (either dynamic or static) is applicable. In other words, local area networks based on Ethernet/Fast Ethernet, more specifically "networks" that are set up as spanning trees

¹While bandwidth is not always plenty in real life, this is not unusual in a network with the drop in bandwidth capacity cost, especially within a geographical proximity such as a campus or enterprise network.

²See Section IV for a modification of this statement when considered in a two-layer network architecture framework.

(or bus) would not be covered here; instead, our work here is primarily applicable to wide-area networks. However, we do clarify that our work is also applicable to access networks that are not simply spanning tree-based or bus-type networks; for example, campus or enterprise (access) networks that have backbone networks consisting of multiple routers and switches; this would fall under the domain we are discussing here. Also, our coverage in this paper is for wired networks; that is, wireless networks restoration is outside the scope of this paper. In this backdrop, we now review a few key technologies and networks.

A. IP Network

Internet is based on the IP networking technology. Contents for applications such as web, email are broken down into small chunks (called packets or IP datagrams) at the end computers which are routed through the IP network. An IP network consists of a set of nodes, commonly referred to as routers. In reality, a large IP network is really networks of networks, as a packet traversing from one computer to another computer (server) goes from an IP network run by an Internet service provider (ISP)³ to another IP network run by another ISP, and then to another, until the packet reaches the destination computer. IP networks can be broken into two main components: access networks, and core networks consisting of multiple ISPs; in either case, the entire Internet is a collection of autonomous systems (AS) where an autonomous system is connected to one or more autonomous systems and where each autonomous system consists of multiple routers that are maintained by the ISP in charge of it.⁴ Each ISP runs an intra-domain routing protocol for routing traffic within its network (autonomous system) or traffic that transitions through its network (autonomous system); the most common intra-domain routing protocols are OSPF and IS-IS⁵. Another protocol called BGP is used for the purpose of inter-domain routing that connects different autonomous systems managed by various ISPs. A pictorial view of intra-domain and inter-domain relation is shown in Figure 2.

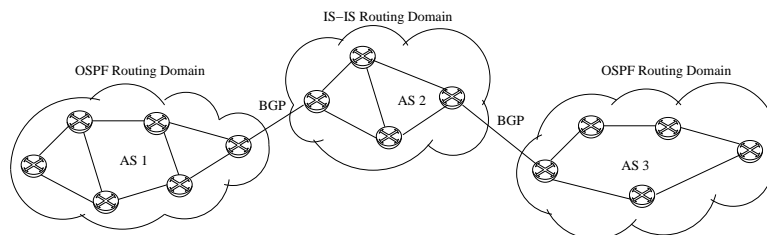


Fig. 2. IP Network Routing Architecture

Both OSPF and IS-IS are link-state protocols that are similar in spirit and use Dijkstra’s shortest-path routing; the shortest path is determined based on the “state” information, e.g., cost of links in the network. It is important to note that the routing protocol does not define the metric value for the link; that is, the provider is left to decide on its own the link cost metric whether it is to be based just on hop counts, or delay, or some other measure. Presumably, an ISP uses a metric based on network goals such as minimizing average delay or minimizing congestion on any link. It may be noted that while a provider may chose the link metric, it may not necessarily want to update the values of the link metric frequently or periodically, unless there is a failure of a link in the network. When a failure occurs, the cost of the

³Our definition of an ISP is broad: a campus network is also considered to be an ISP.

⁴While multiple autonomous systems can possibly fall under the jurisdiction of a single ISP (for example, due to merger of providers), we assume here that each ISP covers an autonomous system.

⁵See appendix for the list of acronyms.

failed link is set to infinity and this information is distributed as link-state advertisement to every router in the network.

The inter-domain routing protocol BGP works on the notion of exchange of reachability information. For the purpose of routing determination, it considers each autonomous system as if it is a mega-node, and the routing is determined based on minimum number of mega-nodes visited.

B. Circuit-Switched Voice Telephone Network

The voice service⁶ is primarily provided through a circuit-switched network where a dedicated circuit with a fixed amount of bandwidth (64Kbps) is set up for the duration of a voice call and is teared down when the call is over. Different telephone service providers (TSP) play different roles in carrying a call. A call originates in an access TSP, a “Local-exchange carrier (LEC)”, where the call starts from a switching node called the end office (or the central office). If the call is destined for another user in the same LEC, then the call is routed within its network. When a call starts from one LEC and is destined to terminate in another LEC, then the call typically goes through an inter-exchange carrier (IXC) before entering the destination LEC (see Figure 3).

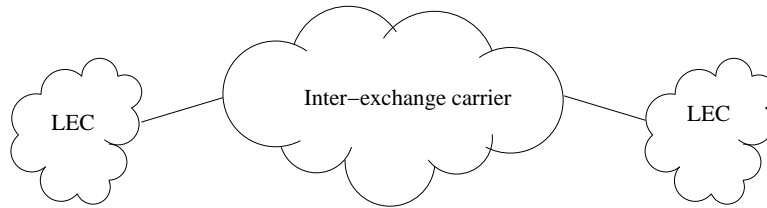


Fig. 3. Telephone Network Architecture

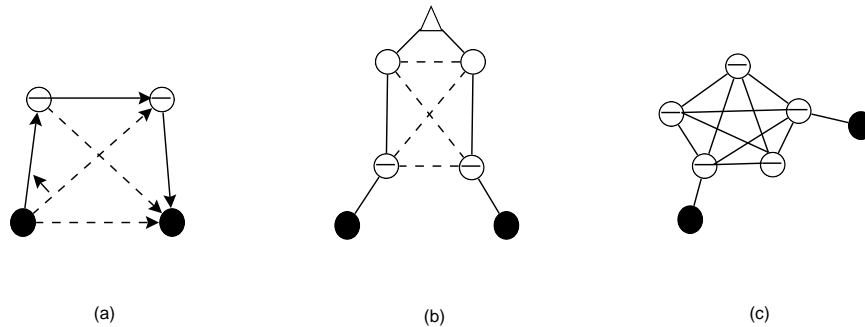


Fig. 4. Telephone Network Routing: (a)Local Exchange Carrier: Two level fixed hierarchical routing, (b)Inter-exchange Carrier: hierarchical, (c) Inter-exchange Carrier: fully-connected dynamic routing

In most cases, LECs use a two level fixed hierarchical routing architecture with call overflow from the lower level to the upper level (see Figure 4a). An IXC can either deploy fixed hierarchical routing or dynamic routing (Figures 4b and 4c); if the network does provide dynamic routing, then the part of the call that falls within its network uses at-most two links for routing between the ingress switch and the egress switch within its network.⁷ A link between two telephone switches is referred to as trunkgroups, or inter-machine trunks. Unless a call terminates in a different country, there is usually at most one IXC involved

⁶Carrying voice traffic on Internet that uses VoIP technology is gaining popularity; this won't be discussed in this paper.

⁷In other words, at the level of end-offices, a call traverses through multiple links that includes at most two links when dynamic routing is used in the IXC part for this call [2].

between the access LECs. For a call going from one country to another country, the call may go through the second country's inter-exchange provider or equivalent before reaching the destination address in another access carrier. In many countries, both the access service and the inter-exchange/long-distance service are provided by the same provider; regardless, a fixed hierarchical routing is commonly deployed in access LECs.

C. MPLS Network

Multi-protocol Label Switching (MPLS) is a relatively recent networking technology that is capable of carrying multiple protocols in the same data networks which may be of different types and may have different quality-of-service requirements. Certainly, the IP service is a primary candidate for MPLS networks, but other services such as voice or Ethernet services can also be handled directly by the MPLS technology.

MPLS provides a functionality called 'labels' so that different protocols/services (with differing quality-of-service requirements) can be carried separately without inter-mixing them (or some of them may be combined, if needed); the ingress and egress nodes in an MPLS network provide the translation functionality from an external protocol for use in an MPLS network. Nodes in an MPLS are called label-switched routers (LSR). Between LSRs, labeled-switched paths (LSP) can be set up. Label-Distribution protocol (LDP) is used for communicating label information for LSPs. The actual decision of how many or what labels to set for different services and usage of LSP functionality is left to the MPLS network provider.

There are several different usage of MPLS technology. An MPLS network can be deployed where LSPs are set up on a permanent or a semi-permanent basis. For example, LSPs can be set up to carry IP traffic; in this case, this LSP will act as a logical link between two IP network routers for the IP network.

MPLS also provides the capability to do constraint-based routing. This means that a service which may have different "constraint" requirements such as bandwidth requirements, or delay requirement may be taken into account in routing decision. This may be on a per "call" basis for a particular service. In that sense, this function has similarity to the circuit-switched voice service, with the important distinction that each call can be of differing bandwidth requirement (instead of just a fixed 64Kbps, in the case of voice circuit-switching) and may also have other requirements such as inter-packet delay, and so on.

There is another usage of MPLS that may be possible. In this case, the LSPs are to be setup and teared down on a on-demand basis based on customer requests, rather than being of permanent or semi-permanent nature. That is, demand requests arrive randomly requesting to set up LSPs with specific bandwidth; this usage of MPLS is essentially similar to the circuit-switched voice service.

A pre-cursor to MPLS technology is ATM (Asynchronous Transfer Mode) where packets are of fixed length called cells. ATM provides virtual path (VP) services which are similar to the notion of label-switched paths.

D. Telecommunications Cross-Connect Network

The role of the telecommunication cross-connect network ([33]) has been that of a bearer network to provide permanent or semi-permanent capacity for 'logical' services such as circuit-switched voice, or for private line service between geographically separated locations of large companies, or more recently, for IP networks. For example, the actual physical routes for trunkgroups for the circuit-switched voice network or a link in the IP network is provided in the cross-connect network as bulk capacity service (such as, 24 voice circuits as T1). The nodes in this networks are cross-connects, or digital cross-connects

(DCS) systems; they can be thought of as ‘slow’ switches since they do not address on-demand real time connection requests. In the literature, such networks are also referred to as transmission networks, transmission facilities networks, facilities networks, or simply as transport networks.

Through DCS functionally, a logical trunkgroup between two switches, that are in far apart places such as Los Angeles and New York (which are two extremes of continental US), can be physically provisioned through cross-connects and transmission network links. To address the economy of scale, such bulk capacities are multiplexed up at grooming nodes, such as from T1 (1.54Mbps, 24 voice circuits) to T3 (45 Mbps, 28 T1s); thus, within the transport network, a hierarchy of rates that feeds from one to another is available.

E. Optical Network

The first generation of optical networks are essentially an extension of the digital cross-connect network where links are over fiber-optic cables. With optical networks, many new layers of rate hierarchy have been defined going from OC-3 (155.52Mbps) to OC-192 (9.9 Gbps) using SONET/SDH standard.

An early implementation of SONET is in the form of rings which are self-healing, in that it can address a single cut failure very quickly, usually in less than 40 ms. A transport network encompassing a large geographical network can be formed by putting together a collection of interconnecting SONET self-healing rings (see Figure 5); it is important to ensure that two rings are not connected at just one point to avoid single point failure which can result in losing both the rings.

Over the past decade, the use of optical cross-connects (OXC) to form mesh transport networks has gained popularity. Recently, there has been interest in providing on-demand optical level services at high data rates (OC-3 or higher) that can be requested much like circuit-switched voice on demand and can be set up and teared down almost instantaneously through signalling functionality.

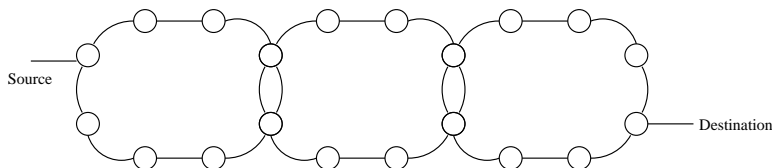


Fig. 5. Network of SONET rings

In recent years, wave-division multiplexing (WDM) concept is gaining momentum where multiple light-waves can be multiplexed on a fiber, thereby increasing capacity without needing to add new fibers in the ground. With WDM, a node may or may not have converter; the role of converter is to switch from one frequency to another (if it is available).

F. Network Hierarchy

Traditionally, network hierarchy consists of the telephone network over the underlying transmission facility made of digital cross-connect networks. Over time, the traditional transmission facility has been replaced by SONET/SDH networks. Similarly, IP networks are provided over SONET network using Packet over SONET (PoS) technology to create IP network links. Thus, an architecture where circuit-switched voice and IP services are offered over the SONET network can be envisioned as shown in

Figure 6. With the advent of WDM, SONET networks are strong candidates for replacement with WDM technology.⁸

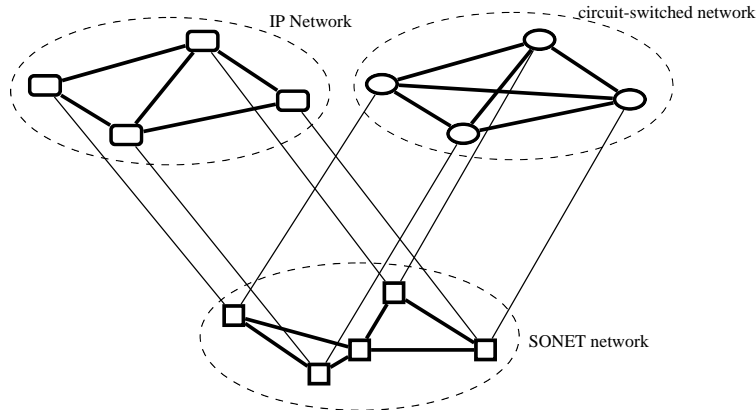


Fig. 6. Multi-Layer Architecture

It is worth mentioning that network hierarchy can consist of more than two layers; for example, MPLS can be put in between the IP and the SONET layer. In reality, below the SONET layer, there is a duct layer where the actual fiber is deployed. When we consider one network on top of another network, the term “overlay network” is also used to indicate the network at the top layer.

G. Distinguishing between Traffic and Transport Networks

Based on the technology discussion so far along with the functionalities available or emerging, we make an important distinction on how to view networks; this view can be broadly classified as *traffic networks* and *transport networks*. We argue that this classification is more powerful than taking a purely technological point of view.

Our use of these two terminologies is as follows: a network is a traffic network if the service request are on-demand (stochastic) and requests are switched or routed on a per-unit basis and are of short duration. A routed entity in the traffic network would be referred to as *packets* or *calls*. A network is considered to be a transport network if requests are scheduled to be activated on a periodic basis and such requests when routed in the network are set up on a permanent or a semi-permanent basis. A “routed” entity in the transport network would be referred to as *circuits*. From the point of view of network restoration, the one for the traffic network can be called *traffic restoration* since traffic is rerouted whereas the one for the transport restoration can be called *link restoration* or *path restoration* (whether dedicated or shared) since either a transport link is restored or an end-to-end path is restored.

Clearly, IP networks and circuit-switched voice networks are traffic networks. Similarly, digital cross-connect networks are clearly transport networks. On the other hand, MPLS and optical networks can not be labeled directly in either category; instead, we need to look at the specific functionality or service provided by such technology based on which we can classify them into these two categories.

Consider MPLS first. MPLS can be used for setting up semi-permanent or permanent label-switched tunnels—if it is used this way, then this particular MPLS network can be classified as a transport network. If MPLS tunnels are set up on demand (virtually with minimal set-up delay), are of short duration and can

⁸Note that this is only in theory; in practice, replacing an existing (live) network with another technology is not very easy—in the end, multiple technologies are in place at one point of time when a new technology is being rolled in while another is not yet fully rolled out. This makes network restoration complicated in practice due to co-existence of multiple transport technologies.

be teared down quickly, then the behavior of this MPLS network is closer to the circuit-switched voice network and hence, in this case, this MPLS network can be thought of as a traffic network. Similarly, depending on how constraint-based routing is used for services provided in an MPLS network (i.e., on demand or semi-permanent/permanent basis), the proper categorization under either traffic or transport network can be done.

Now consider optical networks. An optical network based on WDM or SONET/SDH technology is a transport network. If the optical network uses optical cross-connects (OXC's), then this would fall under the transport network. On the other hand, an on-demand high-rate optical service with optical switching capability that can be set up for short duration and then can be teared down (with minimal set-up/tear-down delay) would fit into services in a traffic network setting.

From the discussion about MPLS and optical networks, it is important to recognize that instead of purely looking at them as technologies, the service functionality provided by them can help us see whether to put each one under the traffic network or the transport network classification. There are several important benefits of this broad classification that has implications for network protection and restoration as well:

- In traffic networks, there is no distinction between working and backup capacity for network protection and restoration, while in transport networks there is often a distinction between working paths/capacity and backup paths. A corollary of this observation is that under no failure, the excess capacity provided in the traffic network serves as additional revenue-bearing capacity for the provider.
- In traffic networks, the restoration would mean being able to restore traffic in general (perhaps at a degraded performance) while for the transport network, restoration would mean whether we have the actual capacity to restore lost capacity and ability to set up paths.
- In a traffic network, the restoration would be on traffic basis while in the transport network, the restoration can be on a bulk capacity basis.
- An effected unit of traffic in a traffic network may not necessarily be recoverable when a failure occurs; for example, consider a packet in transit in an IP network, or an existing call in the circuit-switched voice network—they could both be dropped if a failure occurs⁹. In the case of transport network, the restoration is done for affected circuits.
- There are certain failures inherent to a traffic network that can not be perceived by the underlying transport network. For example, a line card failure at an IP network router would not be recognized by the underlying transport network. Reverse is not necessarily true. That is, it is indeed true that a self-healing SONET ring can restore a failed link without the traffic network above it perceiving it; on the other hand, in a cross-connect network where there is a delay in restoration time, the failure will be perceived by the traffic network above it.
- In a multi-layer network (say, three layers), if we have more than two layers of technology, then only the top layer is the traffic network, and the second and the bottom layer would be (cascaded) transport networks. For example, consider IP over MPLS over SONET. In this case, MPLS would be set up as permanent tunnels¹⁰ for IP network links and serves the function of a (virtual) transport network. It is neither possible nor desirable to setup MPLS in this case as a traffic network; such usage of MPLS would mean quick setup/tear down of tunnels (and associated bandwidth) that would cause the IP network routing to oscillate undesirably. An important corollary is that a transport network, especially an intermediate one, can still be a logical network.

⁹Certainly, this depends on whether the failure is perceived by the traffic network; for example, a SONET self-healing ring can restore a failed link without an IP network or circuit-switched voice network perceiving it.

¹⁰Note that, from a technology point of view, ATM virtual paths can be set up instead of MPLS tunnels in the middle layer in this architecture.

- Network design models can be of different types depending on whether this is addressed for a traffic network or a transport network (see Section V).

While the traffic network and the transport network classification has several benefits, we want to emphasize that this is a broad classification. It can not capture how to do or what to do for all types of failure, for example when a failure propagates from one network to another, or certain intricacies between different types of traffic networks (or, for different types of transport networks). In the rest of the discussion, we also bring out some of the limitations of this classification as and when applicable.

IV. REVISITING THE THREE-NODE EXAMPLE

First consider the three-node network again; this time as an IP network with three routers, where each router pairs have 20 Mbps of traffic on average and the link speed is 155 Mbps. With OSPF protocol, when link 2-3 fails, the routers will use link state update. Through this process, node 2 can find out that path 2-1-3 exists. In a data network such as the IP network, an important goal is that the delay is minimized, or utilization is kept as low as possible¹¹. For example, ISPs often try to keep utilization lower than 50% on average in the normal operating condition. In this case, with re-routing, still the link utilization is at $(20 + 20)/155 = 25.81\%$, and thus, the failure may not be perceived by the user.

We now discuss the case if we were to consider a circuit-switched voice network consisting of three switches; assume that each node pair has 20 Erlangs of offered traffic and the link capacity is 150 voice trunks. If the circuit-switched network has dynamic routing,¹² then this is not different than the IP network with dynamic routing since there is plenty of bandwidth on the alternate path to route traffic. In the case of the telephone network, another possible case is when, of the three nodes, one is at a higher level of the hierarchy than the other two (e.g. two are end office switches, while the third one is used for alternate routing.). In this case, if nodes 2 and 3 are at the lower level, and node 1 is at a higher level, then for link 2-3 failure, the network can do alternate routing via node 1. On the other hand, if nodes 1 and 2 are at the lower level and node 3 is at the higher level, then for link 2-3 failure the telephone network can not do any alternate routing (thus, relying on the underlying transport network for recovery). Finally, if three switches are at the top level of a telephone switching hierarchy without dynamic routing, this would be similar to the case of the IP network with static routing. In other words, the routing capability does make a difference in a traffic network's ability to restore from a failure.

Let us consider the case of static routing in the traffic network (be it IP or circuit-switched voice), that is, only direct link route allowed for each pair of nodes. In this case, when traffic link 2-3 fails, then traffic between nodes 2 and 3 can not communicate. On the other hand, recall from previous section that links for IP networks are set up over a transport network. Now suppose that there is a SONET ring that connects traffic link 2-3 as shown in Figure 7a. Thus, in this case, a traffic link failure is really a transport link that is affected in the SONET network; for example, the traffic link failure 2-3 is really due to the failure of transport link 2-4. Here, in the transport network itself, transport link 2-4 will be restored by routing around the SONET ring immediately without the traffic (IP or circuit switched voice) network perceiving it. Based on this observation, we now modify one of the observations we discussed earlier in Section II: in a traffic network with static routing, restoration may be possible either partially or fully depending on the capability of the underlying transport network.

¹¹There is a strong relation between utilization and delay; for example, if we assume M/M/1 queueing model, the average delay, T , is related to utilization ρ by the relation $T = \frac{1}{\mu(1-\rho)}$ where μ is the effective bandwidth of the link.

¹²In the case of telephone network, this usually means that switches in the network are at the same level of hierarchy and employ dynamic routing.

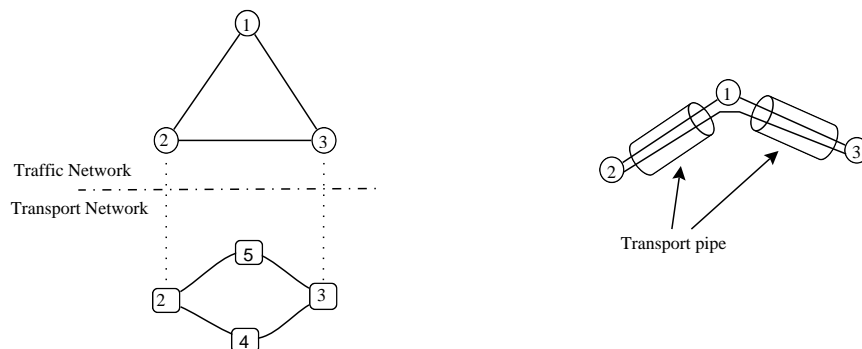


Fig. 7. (a) Transport level diversity through ring, (b) no transport level diversity

Another important variation to consider is the following: when the perceived diversity in the traffic network is not really diverse when viewed from the transport network. For example, consider again the three node IP network with dynamic routing. Thus, for a link failure, we assume that the traffic can be routed over the alternate path. Now suppose the underlying transport capacity for the IP network is over the same fiber as shown in Figure 7b. In this case, if a fiber cable cut occurs, one router in the IP network will be completely isolated from the other two. This illustrates that a single fiber link (or transport link) failure can actually translate to multiple (two in this case) link failures in the IP network. There are following important observations that come out of this aspect:

- Logical diversity in the traffic network can be misleading.
- With the dynamic routing capability in the traffic network, it can restore services in its network more effectively if the underlying transport network has diversity.
- Developing a design model for network restoration based on a single-link failure assumption may not always be realistic if the network under consideration is especially a traffic network.

Finally, the notion of static routes for the traffic network is similar to the idea of permanent static circuits being setup in the transport network with cross-connects. Thus, for a transport network with permanent cross-connect circuits, back up circuits on diverse paths needs to be set up for recovery. However, for a logical transport network (intermediate layer in a multi-layer network, e.g., MPLS between IP and SONET), the underlying physical transport network must provide physical diversity even if backup paths are set up in the intermediate transport network.

V. NETWORK PROTECTION

No matter where it lies in the network hierarchy, the notion of traffic and transport network provides us a good way to address network protection in terms of optimization model development. In this section, we present formulations for certain specific scenarios. The reader is directed to [31] (especially, Chapters 9 and 12) for a wide variety of different optimization models that can be used for network protection design. We also present a short overview on algorithmic approaches.

A. Traffic Network Protection

From the discussion earlier, it is clear that networks such as IP networks, circuit-switched voice networks, on-demand MPLS network, or on-demand optical networks—all fall under the traffic network as per our broad classification.

Assume that h_d is the average traffic volume for demand identifier d ($d = 1, 2, \dots, D$) between two nodes i and j in a traffic network. Let $p = 1, 2, \dots, P_d$ be the possible paths for demand d to carry this

demand volume h_d . Let x_{dp} be the unknown (to be determined) for flow allocated to path p for demand d . Note that since we are considering a traffic network, the flow on a path here reflects the average amount of traffic to be allocated to this path; secondly, due to traffic nature, we can assume the flow variables to take continuous values. We denote the links in the network by $e = 1, 2, \dots, E$. Due to path p and link e , we also introduce the indicator δ_{edp} which is set to 1 if path p for demand d uses link e ; 0, otherwise. Let ξ_e be the cost of adding capacity of modular unit M on link e , and let variable y_e denote incremental number of capacity units needed on link e (given that the link already has c_e units). Then, the basic capacity design problem can be written as the following mixed-integer linear programming multi-commodity flow model:

$$\begin{aligned}
& \text{minimize}_{x,y} && \sum_{e=1}^E \xi_e y_e \\
& \text{subject to} && \sum_{p=1}^{P_d} x_{dp} = h_d, && d = 1, 2, \dots, D \\
& && \sum_{d=1}^D \sum_{p=1}^{P_d} \delta_{edp} x_{dp} \leq M(c_e + y_e), && e = 1, 2, \dots, E \\
& && x_{dp} \geq 0, \\
& && y_e \geq 0 \text{ and integer.}
\end{aligned} \tag{1}$$

In the above model, the first set of constraints, called demand constraints, is to indicate that demand volume is to be satisfied by the path flow variables. The second set of constraints, called capacity constraints, is to determine how much capacity is needed on each link to carry traffic taking that link. Finally, the objective function minimizes the cost of incremental capacity y_e .

It may be noted that this multi-commodity flow model is based on the link-path representation which suits communication networks well since there are often restrictions on the length of paths and also due to any restriction imposed by network engineers based on their knowledge of an operational network. For example, for dynamic routing circuit-switched networks, a path is restricted to at most two links.

In order to address failures, we consider S states $s = 1, 2, \dots, S$ and consider the normal state as $s = 0$. We also introduce the parameter α_{es} to denote 0 if the link e is affected due to failure s and 1 if it is not affected.¹³ Let h_{ds} be the traffic volume to be carried in state s for demand d . Note that $s = 0$ denotes the normal state of the network; thus, we have $h_{d0} = h_d, d = 1, 2, \dots, D$. Extending x_{dp} , for each state s we indicate flow variables as x_{dps} for path p and demand identifier d . Then the protection capacity design problem to address for any failure s can be written as follows:

$$\begin{aligned}
& \text{minimize}_{x,y} && \sum_{e=1}^E \xi_e y_e \\
& \text{subject to} && \sum_{p=1}^{P_d} x_{dps} = h_{ds}, && d = 1, 2, \dots, D \\
& && && s = 0, 1, \dots, S \\
& && \sum_{d=1}^D \sum_{p=1}^{P_d} \delta_{edp} x_{dps} \leq \alpha_{es} M(c_e + y_e), && e = 1, 2, \dots, E \\
& && && s = 0, 1, \dots, S \\
& && x_{dps} \geq 0, \\
& && y_e \geq 0 \text{ and integer.}
\end{aligned} \tag{2}$$

¹³Parameter α_{es} can be allowed to take a value between 0 and 1 if a link is partially available; for example, see [31].

In the above model, the first set of constraints, called demand constraints, is to indicate that demand volume is to be satisfied by the path flow variables for each state s . The second set of constraints, called capacity constraints, is to determine how much capacity is needed on each link to carry traffic taking that link for each failure state s . The goal is to minimize the cost that addresses any link failure. The above model is quite powerful due to the following reasons:

- The failure states can be either all single link failures (each considered independently), or multiple link failures, or one can consider only a subset of key links that is of interest to a network provider. Depending on the failure which is indicated by s , the corresponding α_{es} can be set to zero, and thus, a variety of failures including multi-link failures can be captured as well.
- Since in a failure state s , we have $\alpha_{es} = 0$, the right hand side of the capacity constraints is forced to be zero. Consequently, this forces the associated x_{dps} to be zero. Furthermore, this says that for each demand pair we do not necessarily need to consider a separate set of paths for each failure state from the normal states (thus, we have kept the number of candidate paths for demand d at P_d , instead of needing to introduce a new P_{ds}).
- Traffic volume can be appropriately captured depending on specific types of traffic network considered; accordingly, modular value M can be adjusted. We discuss below two cases:
 - For an intra-domain IP network running the OSPF/IS-IS protocol, h_d represents traffic in Gbps for average packet traffic from router at node i to router at node j ; then, h_{ds} is an appropriately adjusted volume in state s . The quantity, M , is a combination of two factors: acceptable utilization times the capacity module (such as OC-12). Note that multi-commodity flow x_{dps} on path p would be positive in state s only if path p is the shortest path as imposed by the link metric (weight) system $w_{es}, e = 1, 2, \dots, E$ for state $s = 0, 1, \dots, S$. Thus, in the above formulation, we need to replace x_{dps} by $x_{dps}(w_{es})$ to properly reflect the induced dependency on flow due to the link weight system. It is important to point out that protection design model (2), with explicitly writing $x_{dps}(w_{es})$ (instead of just flow x_{dps}), is no longer a mathematical programming formulation. On the other hand, the solution to the dual of the original problem (2) is related to the optimal link weight system; see [1], [31], [32], [39]. Certainly, this relationship between dual solution and the original optimal solution holds also for the basic design case of OSPF networks (i.e., no failure).
 - For a circuit-switched voice network with dynamic routing,¹⁴ h_d can be approximated as follows: $h_d = \mathcal{E}^{-1}(a_d, B)$, where \mathcal{E}^{-1} is the inverse Erlang-B formula¹⁵ applied to traffic load a_d Erlangs for an acceptable blocking level (grade-of-service), B . For each state s , traffic load h_{ds} is an appropriately adjusted volume due to possibly different acceptable blocking level for each state s . In this case, M would be the capacity in terms of modular trunk units (such as 24 voice trunks/T1).

B. Transport Network Protection

An important problem in transport network protection is to provide a back-up path for every path with positive demand flow. The idea is that since the back-up path exists, the demand can take the back-up path automatically in case of a failure,¹⁶ and the restoration is instantaneous. For this illustration, we assume

¹⁴Network design formulation for dynamic routing circuit switched networks is more accurately captured through non-linear optimization formulation; for example, see [14]. With the advent and availability of high-valued modular capacity units as well as drop in per unit cost of network capacity, a mixed-integer linear programming model such as (2) adequately captures network's need in term of capacity.

¹⁵That is, we need to find the smallest h such that $\mathcal{E}(a, h) \leq B$ where $\mathcal{E}(a, h) = \frac{a^h/h!}{\sum_{k=0}^h a^k/k!}$.

¹⁶For example, this is applicable to an MPLS network deployed as a virtual transport network with the fast-reroute option.

that we are addressing protection design for a traffic network link. It is important to understand that bandwidth required for a traffic link is routed on a transport network on a permanent or semi-permanent basis (as circuits); thus, from the perspective of the transport network, this protection can be thought of as an end-to-end or path protection.

Consider now Figure 8. In this network, if the demand between 1 and 2 is routed on path 1-3-4-2, then a complete link and node-disjoint back-up path can be setup on 1-6-2; alternately, if the demand between 1 and 2 is routed on 1-3-5-2, then 1-6-2 can also be the back-up path. We can see that when we combine a pair of main path and the back-up path that are disjoint, we can form a cycle; for example, in this case, for demand between 1 and 2, we have two cycles: 1-3-4-2-6-1, and 1-3-5-2-6-1. Either of them is a candidate to be chosen for this demand pair—which one to chose would certainly depend on the network goal. Before we discuss the network goal, we want to point out the following: i) for a network to provide disjoint back ups, we assume that the topology allows us to find at least a pair of primary and back-up paths—otherwise, this is not possible (imagine a linear network), ii) there are already algorithms available for finding a pair of disjoint paths (for example, see [36], [37])—such an algorithm can be used for generating a set of pre-processed candidate cycles for a demand pair to be used in the protection design phase.

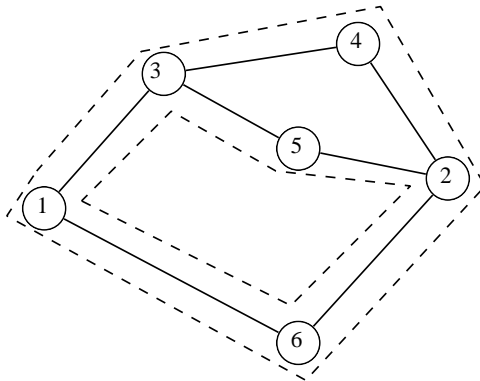


Fig. 8. Network with multiple disjoint paths forming cycles

In order to use the notion of cycle, in a link-path multi-commodity formulation, we make an important observation: a path can be replaced by a cycle since a cycle can be thought of as a series of links much like a path [26]. Thus, for demand identifier e connecting two end points of a traffic link, we can consider a set of candidate cycles in the transport network identified as $q = 1, 2, \dots, Q_e$. Note again that the output capacity of the traffic network is now the demand volume for the transport network. Thus, a traffic network link is now a demand pair for the transport network (hence, we chose to use the notation e for the same entity to show this connection). A transport network link would be identified by g where $g = 1, 2, \dots, G$. We use γ_{geq} as the indicator that takes the value 1 if cycle q for demand e takes the transport link g ; 0, otherwise. Since, we are providing back-up paths in the transport network,¹⁷ we want the demand volume for a demand e to be assigned to just one cycle out of a set of possible cycles; we use the binary variable u_{eq} for making this decision.

Our goal is to minimize the cost of transport network capacity ($z_g, g = 1, 2, \dots, G$) for providing the primary-back up paths for demand volume given as $\hat{c}_e, e = 1, 2, \dots, E$; this can be formulated as follows:

¹⁷If completely disjoint back-up path is not achievable, then a possible approach is to provide demand splitting on diverse paths in the transport network for a demand arising for a traffic network link.

$$\begin{aligned}
& \mathbf{minimize}_{u,z} && \sum_{g=1}^G \eta_g z_g \\
& \mathbf{subject\ to} && \sum_{q=1}^{Q_e} u_{eq} = 1, && e = 1, 2, \dots, E \\
& && \sum_{e=1}^E \sum_{q=1}^{Q_e} \gamma_{geq} \hat{c}_e u_{eq} \leq N z_g, && g = 1, 2, \dots, G \\
& && u_{eq} \text{ binary} \\
& && z_g \geq 0 \text{ and integer.}
\end{aligned} \tag{3}$$

In the above formulation, η_g is the unit cost of transport network capacity on link g in modular units of N . Here, the first set of constraints indicated that only a single cycle is to be determined for each demand pair e . For the cycles chosen, the load on links needs to be less than the capacity which is indicated in the second set of constraints. Note that this is an integer linear multi-commodity flow model.

In many cases, available capacity on a transport network link is known due to the planning cycle for such capacity determination being on a different time window than the planning cycle for the traffic network. In this case, the goal of a protection design problem can be to maximize residual capacity¹⁸ (so that future demand can take advantage of the residual capacity) given that \hat{C}_g is the currently available capacity in transport network link g .

$$\begin{aligned}
& \mathbf{maximize}_u && \sum_{g=1}^G \left(\hat{C}_g - \sum_{e=1}^E \sum_{q=1}^{Q_e} \gamma_{geq} \hat{c}_e u_{eq} \right) \\
& \mathbf{subject\ to} && \sum_{q=1}^{Q_e} u_{eq} = 1, && e = 1, 2, \dots, E \\
& && \sum_{e=1}^E \sum_{q=1}^{Q_e} \gamma_{geq} \hat{c}_e u_{eq} \leq \hat{C}_g, && g = 1, 2, \dots, G \\
& && u_{eq} \text{ binary.}
\end{aligned} \tag{4}$$

While it may not be obvious to the reader from either (3) or (4), we do point out that for most transport network design (protection or without protection) cases, the flow variables usually take integer¹⁹ values since the flows for transport networks is to route permanent or semi-permanent circuits. This is another subtle and important distinction between traffic and transport networks and their impact on network modeling formulation. Certainly, this does not rule out the possibility that an integer programming model can be relaxed to linear programming counter part for ease of solving a model towards generating a set of usable solution.

Models (3) and (4) illustrate just one way to address for network protection, namely through pre-configuration of stand-by backup paths. It is fairly easy to see that such an approach comes at the price of high protection capacity while achieving quick restoration through back-up. Depending on the functional capability of the transport network, protection capacity can be sharable that would lead to reduction in capacity required. Often, however, this reduction in shared capacity comes at the price of the actual restoration time being more pronounced.

So far, we have not clearly stated what should be the demand volume \hat{c}_e for the transport network. There are two possibilities in light of the design models presented for the traffic network. If \hat{c}_e is set to

¹⁸Formulation (4) can be easily transformed to a minimization problem.

¹⁹Obviously, relaxation of flow variables to be continuous to solve the overall model can be done to arrive at a good approximate solution. However, this is done primarily to address the issue of solvability of a model.

be the total capacity from model (2), i.e., $\hat{c}_e = M(c_e + y_e^*)$, $e = 1, 2, \dots, E$ (where y_e^* is the solution of (2)), and if the back-up capacity in the transport network is designed using (3), then it is very clear that we are double-dipping on spare capacity for network protection—once in the traffic network and then again in the transport network! Unfortunately, this double-dipping is not always avoidable since in many instances traffic and transport networks are provided by different network providers; thus, when a traffic network provider requests capacity \hat{c}_e from the transport network provider, the transport network provider has no way to know whether the quantity, \hat{c}_e , requested by the traffic network has already built-in protection capacity or not (recall that in the traffic network, there is no distinction between working and spare protection capacity).

If both the traffic network and the transport network are provided by the same network provider, then the provider can coordinate its own network design steps to avoid double-dipping on capacity. Such a model is discussed in the next section.

C. Multi-Layer Model

In this section, we present a two-layer model that considers a traffic network and a transport network together. As we have discussed so far, we assume that the back-up path method described above in Section V-B is used for protection in the transport network part along with normal capacity design for the traffic network part. In this model, we assume that the available capacity in the transport network is given and our design goal is to minimize the total cost due to capacity for the traffic network and routing (primary and backup) in the transport network. The formulation is presented below:

$$\begin{aligned}
& \mathbf{minimize}_{x,u,y} && \sum_{e=1}^E \xi_e y_e + \sum_{e=1}^E \sum_{q=1}^{Q_e} \zeta_{eq} u_{eq} \\
& \mathbf{subject\ to} && \sum_{p=1}^{P_d} x_{dp} = h_d, && d = 1, 2, \dots, D \\
& && \sum_{d=1}^D \sum_{p=1}^{P_d} \delta_{edp} x_{dp} \leq M(c_e + y_e), && e = 1, 2, \dots, E \\
& && \sum_{q=1}^{Q_e} u_{eq} = 1, && e = 1, 2, \dots, E \\
& && \sum_{e=1}^E \sum_{q=1}^{Q_e} \gamma_{geq} M y_e u_{eq} \leq \hat{C}_g, && g = 1, 2, \dots, G \\
& && x_{dp} \geq 0, \\
& && u_{eq} \text{ binary} \\
& && y_e \geq 0 \text{ and integer.}
\end{aligned} \tag{5}$$

The common notations are the same as used earlier in Sections V-A and V-B except for a few. This model combines (1) and (3) in an integrated model. In this model, the unit routing cost for a pair of primary and backup paths is given by ζ_{eq} , and the transport network protection is shown only for the incremental capacity of the traffic network capacity y_e . Thus, this model captures the fact that often network providers do not want to re-arrange traffic network capacity already installed from a previous planning cycle, as well as how that capacity is provisioned in the transport network. There is however a different problem with the above model: this is a mixed integer *non-linear* programming model due to the product term $y_e u_{eq}$. On the other hand, this non-linearity can be avoided if a new shadow flow variable v_{eq} associated with the binary variable for selection of cycle u_{eq} in the transport network is introduced.

We also need an artificially high positive number H to capture the relation between v_{eq} and u_{eq} ; as a guideline, H needs to be more than $\max_{e=1,2,\dots,E} \{My_e\}$. A model equivalent to (5) is shown below:

$$\begin{aligned}
\mathbf{minimize}_{x,u,v,y} \quad & \sum_{e=1}^E \xi_e y_e + \sum_{e=1}^E \sum_{q=1}^{Q_e} \zeta_{eq} u_{eq} \\
\mathbf{subject\ to} \quad & \sum_{p=1}^{P_d} x_{dp} = h_d, & d = 1, 2, \dots, D \\
& \sum_{d=1}^D \sum_{p=1}^{P_d} \delta_{edp} x_{dp} \leq M(c_e + y_e), & e = 1, 2, \dots, E \\
& \sum_{q=1}^{Q_e} u_{eq} = 1, & e = 1, 2, \dots, E \\
& \sum_{q=1}^{Q_e} v_{eq} = My_e, & e = 1, 2, \dots, E \\
& v_{eq} \leq H u_{eq}, & e = 1, 2, \dots, E \\
& & q = 1, 2, \dots, Q_e \\
& \sum_{e=1}^E \sum_{q=1}^{Q_e} \gamma_{geq} v_{eq} \leq \hat{C}_g, & g = 1, 2, \dots, G \\
& x_{dp} \geq 0, \\
& u_{eq} \text{ binary} \\
& v_{eq} \geq 0, \\
& y_e \geq 0 \text{ and integer.}
\end{aligned} \tag{6}$$

Note that for each e , only one u_{eq} takes the value 1—the rest are zero; this forces the associated v_{eq} to be zero except for the one corresponding to the specific u_{eq} that takes the value 1. In the above model, capacity constraints in the transport network are linear constraints.

Through the above integrated model, we have shown the following: i) indeed, traffic and transport network protection design can be modeled through an integrated optimization model, ii) depending on the requirement in the transport network protection, it is possible to arrive at models with non-linear product terms; on the other hand, through the introduction of addition variables such product terms can be avoided.

D. Algorithmic Approaches

In the previous subsections, we have presented a set of optimization models to address the protection and restoration design for traffic and transport networks. Approaches for solving different models cover a vast area in itself; we now briefly discuss algorithmic approaches.

The optimization models presented so far are multi-commodity flow models, specifically mixed-integer linear programming models for the traffic network, and integer linear programming models for the transport network; also, design models for multi-layer protection design can be cast as mixed-integer linear programming models. Furthermore, we have commented earlier that often link-path formulation suits telecommunication network modeling well since network designers and engineers can use their prior knowledge of the network and network properties to determine a set of pre-processed candidate paths using k -shortest paths methods (and pruning paths not wanted), or determining pairs of disjoint-paths for protection.²⁰

²⁰See references such as [23], [31] for generating k shortest paths, and [36], [37] for generating disjoint-path pairs.

Despite having pre-generated candidate paths, such formulations are hard and time consuming to solve for large-size networks, especially if a commercial mixed-integer programming solver is used. Fortunately, these models are multi-commodity flow models with special structures; for example, requirement for routing can be decoupled on a per commodity (i.e., demand) basis, flow and capacity variables are coupled only on certain type of constraints; for a multi-layer model, there is also a connection due to one network's capacity being related to another network's demand.

Based on our experience over the years, we have found that Lagrangian relaxation-based dual subgradient (LRBDS) approach can be a very effective method for solving many such problems for very large networks. The main idea behind LRBDS is to consider the original problem in the dual space by relaxing a set of constraints of the original problem so that it allows us to decouple the problem into different “like-minded” variables (e.g., flow variables, capacity variables); such relaxation leads to generating a set of subproblems which are not only decoupled, but can be solved very efficiently. On the other hand, such subproblems depend on knowing the dual solution. Since we would not know the dual solution to begin with, we need to iterate through the dual space. Furthermore, the dual problem is continuous, but non-differentiable at many points; thus, the iterative dual approach is based on obtaining a subgradient (instead of gradient) of the dual function at each dual iteration to compute a direction. Such a subgradient is readily available from solving a series of subproblems. Thus, the entire process iterates back and forth between the dual multiplier update and solving large number of subproblems efficiently. The interested reader can find more details about how LRBDS can be applied to different network design problems in [31].

We do want to point out that when the traffic network is the IP network with shortest path routing, then the goal is to determine link weights—we have commented earlier that this is not a direct mathematical programming formulation. For such a design problem, several approaches have been proposed such as local search heuristic ([11], [12], [40]), genetic algorithm ([6], [9]), and a variant of the LRBDS approach ([31], [34]).

E. Remarks

Although from a modeling point of view integrated protection model as described in Section V-C is possible, a network provider may still decide to do completely decoupled design for its traffic and transport networks for practical reasons: i) the network management and provisioning system needed to implement such a model can be cumbersome, and often a hindrance, ii) the transport network may provide transport function for many different upper layer ‘logical’ transport networks,²¹ each of which may also fall under different planning cycles, iii) traffic and transport network design are done by different business units (partly because of item-ii) for large telecommunications network providers.

We conclude this section by noting that the traffic and transport network design models presented here are to give some flavor of models applicable. The reader is directed to [31] (especially Chapters 9 and 11) for an extensive variety of optimization models and approaches.

VI. APPROACH TO RESTORATION

In this section, we present approaches for restoration in different networks. By no means, this list is exhaustive. Our attempt here is to make the reader aware of the necessity to take different approaches to network restoration. It is important to understand that for this part we assume that protection capacity

²¹Consider a telecommunications transport network provider that provides its own traffic network service, e.g., for voice telephony, IP networks, and virtual private network services for automated teller machine networks for banking institutions; each can be considered as a mid-level logical transport network.

(whether partial or full) is already provided through the protection design models presented in the previous section.

A. Large-Scale intra-domain IP network

In the three-node IP network discussed earlier in Section IV, any link-state update can be performed quickly. When an intra-domain IP network is very large (say 100 nodes or more), then communicating about a link failure can take certain amount of time as this is being disseminated throughout the network to every router. Once this information is received, then each router employs shortest path routing (by setting the affected link with infinite cost) to compute next hop for shortest paths. There is an important issue to consider here. Most large IP networks are traffic engineered for optimal movement of packets through the network [11]; often, such traffic engineering requires considering traffic snapshot and capacity of links to determine an optimal (or, near optimal) set of link weights for links of the IP network so that congestion is minimized in the network. Such weight determination is computed off-line and disseminated back to each router in the network. When a link failure occurs, affected traffic will be re-routed on the newly computed shortest path (based on old link weights except for the affected link) which may result in significant congestion on some links, thereby affecting the delay perceived by users. This suggests that determination of a *new* optimal link weight system after a failure could conceivably minimize such congestion.

While theoretically the idea of determining new link weights after each specific failure is desirable, we need to understand the basic steps in the restoration process which can be summarized as follows:

failure occurs → *indicate failure to all nodes* → *determine new weight systems* → *compute shortest path* → *update routing table*

Furthermore, in order to determine the new weight system, network measurements to get a snapshot of traffic demand in the network may be necessary, followed by running an optimization algorithm for determining new link weights; i.e., in reality, the new weight determination step involves two sub-steps. We can now see that the actual time to restoration starts adding up as we consider various steps involved. Finally, we need to understand something about types of failure. It has been reported that 50% of failures last for < 1 minute, and 80% of failures last for < 10 minutes for a large inter-domain IP network [30]; such short-lived failures are referred to as transient failures.

Given the observation about transient failures, there is another important issue to consider; even if a new link weight system under a specific failure might be optimal, the network may be required to revert back to the old weight system (that existed prior to the failure) for most of the transient failure scenarios—this itself can cause undesirable oscillatory behavior in the network, not to mention additional impact on computational time to obtain them for a live network. The approach proposed in [30] and [40] (also discussed in [31, Chapter 7]) is elegant: instead of trying to compute a new weight system *every time* after a failure, determine *ahead* of time a robust weight system that works for *both* normal network condition as well as under likely transient failures; in other words, after a transient failure, it is not necessary to determine new traffic snapshot²² and no new weight computation is necessary; instead, the failure of the link is communicated through the link state advertisement—each router can then compute a new shortest path preferably only for affected destinations using the robust link weights already determined except for using infinite cost for the affected link; this itself reduces computation time in each router instead of computing complete routing tables to all destinations.

²²Determining traffic demand in an IP network can be time consuming, see [10].

We now briefly describe the off-line modeling approach for computation of link metric values that can work for both under the normal condition and transient failures. Consider that we are interested in the goal of minimizing maximum link utilization; now, minimizing maximum link utilization under no failure and transient failures can be given different priority by constructing an objective function that gives weights to each scenario (no failure or transient failures); this then can be formulated as a composite optimization problem (see [30]; also, see [31, Chapter 7] for a different formulation). Another approach would be to consider no failure and failures as a bi-criteria optimization problem for which Pareto optimal solution can be obtained (see [40]). Thus, off-line optimization model to understand how to determine link metric that works for no failure and transient failures is an important usage of optimization models in networking. Finally, we point the reader to the recent work [17] that discusses feasibility of restoration in IP networks taking into account practical issues.

B. Large Dynamic Routing Circuit-Switched Networks

Most implementations of dynamic routing for circuit-switched voice networks (usually deployed by inter-exchange TSPs) have two important features: the network is almost fully-connected with the length of a call path (within its network) consisting of maximum two-links²³ and multiple possible paths are cached (instead of just the shortest path) for each pair of source-destination switches. Note that paths are updated periodically or almost on-demand; exchanges of link status information is usually done through an out-of-band network. The path list is kept in a pre-defined priority order, for example from most available bandwidth to the least available bandwidth. When a call arrives and can not find bandwidth on the first path, it can try the second path in the list, and so on.²⁴

To be able to compute path ordering quickly, most dynamic routing implementations such as real-time network routing (RTNR) and dynamically controlled routing (DCR) use heuristic algorithms based on the status of link bandwidth availability (see [2], [4], [14]). This operation is followed during the normal network condition; if failure occurs, status of the failed link is updated to non-availability. Since multiple paths are cached for each source-destination pair and assuming a failure does not affect all paths in cache, the path set need not be updated immediately. Rather, for a new call that arrives, a path with the affected link would be attempted (without success), and depending on crankback capability, the call will then attempt the next path available in the list (until all paths in the cache are exhausted). Thus, this functionality provides the traffic restoration capability in the network. The actual performance of the network and its adaptability would depend on built-in traffic restoration capacity in the network.

Since a dynamic routing circuit-switched network is almost fully-connected, a lower layer transport network link failure is likely to affect multiple links in the traffic network; this is an important point to note. Thus, trunk diversity along with restoration capacity design is needed for graceful recovery from a failure [27].

C. Transport Network Restoration

If the transport network is a SONET/SDH ring-based network, then the self-healing property of such a ring can address any single link failure. As we have discussed earlier, a large transport network is often made up of a series of rings where two adjacent rings are usually interconnected in two different points

²³This length limitation was originally done to reduce complexity of switching software along with the realization that the marginal gain was negligible when additional paths with more than two-link paths are used if the network grade-of-service were to be maintained below 1% call blocking; see [3].

²⁴Due to a feature called trunk reservation or state protection, a call may not be allowed on a link even if there is available capacity; see [14].

to reduce the impact of a node failure on two rings. It is commonly understood that the overall capacity needed in a SONET ring network is much higher than if the entire network is set up as a mesh transport network. On the other hand, the benefit of immediate restoration possible with a SONET/SDH ring can be of paramount importance to a network provider; this benefit may have much higher weight than the cost of the capacity over provisioned through a series of rings. Thus, it is up to the service provider to decide on this trade-off between the high cost ring architecture and the restoration speed, and to make the best strategic decision.

Now consider a mesh transport network. With technological advantages, increasingly more intelligence is being pushed to a transport network node than it was possible before. Thus, for the rest of the discussion in this section, we will consider only mesh transport networks in general and provide specific network cases as applicable, for example, when an MPLS network serves as a transport network.

Mesh transport network restoration clearly depends on availability of protection capacity, as well as ability to compute back-up paths. If a transport network is designed without any hot-standby back-up paths (either for path or link restoration), then after a failure some algorithm is required to be solved to determine restoration paths. Determination of restoration of transport paths after a failure in the path restoration framework can be modeled as a multi-commodity flow problem ([18], [28]). However, solving a multi-commodity flow model in its entirety after a failure can be time consuming; thus, a heuristic approach is desirable to arrive quickly at an acceptable solution. Arriving at such a solution, however, depends on whether the protection capacity in the network is tight. A general sense is that if the protection capacity is plenty, then determining such a solution through a heuristic is usually less time consuming.

In many transport networks, a back-up path is pre-provisioned corresponding to a deployed primary path. We have already discussed earlier protection capacity design for such an environment. For an MPLS network that provides transport network services, a functionality called “MPLS fast-reroute” provides signalling capacity for restoration from a failure by switching from a primary path to a backup path quickly. In addition, automatic protection switching (APS) concept has been around for sometime to address for quick restoration in a transport network for link restoration.

It may be noted that the concept of p -cycle ([16]) which can be implemented at the signalling level of a mesh optimal network for restoration can be a very attractive method that brings the advantage of a SONET-ring like restoration functionality in a mesh network environment; for details, see [15], [16].

The above discussion is to provide a glimpse into the vast area of transport network protection. For additional details on transport network protection, see two recent books: [16], [38].

D. Combined Traffic and Transport Network Restoration

Usually, large telecommunication network service providers operate both traffic networks such as circuit-switched voice and IP networks along with underlying optical transport networks. Thus, in such a situation, the question of combined or integrated protection arises. As we have discussion earlier in the context of protection capacity design model, such combined effort can lead to less capacity required for providing protection.

From the point of view of actual restoration, it is helpful to understand the impact of a severe transport network failure and staggered restoration in the transport network for overall recovery of the traffic network. To illustrate this, we consider a specific traffic/transport network scenario²⁵ where the traffic network is fully-connected with dynamic call routing capability (with multiple routes cached)—this traffic network is provided over a mesh transport network and the capacity required (including protection capacity)

²⁵See [28] for details.

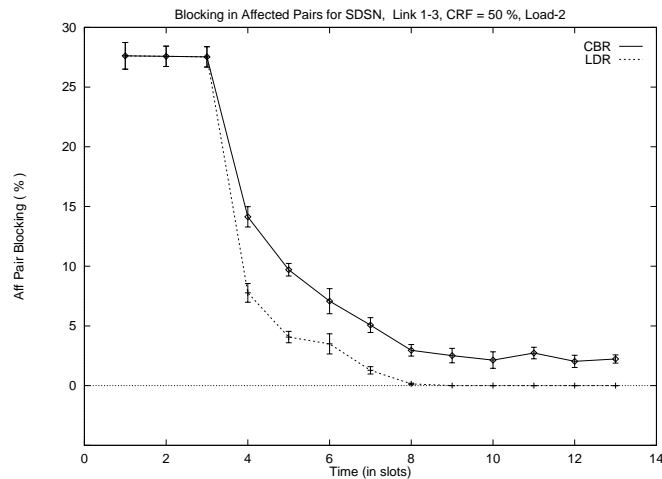


Fig. 9. Impact on Performance due to staggered restoration

for the traffic network is diversely routed in the transport network. In this example, a single link failure in the transport network affected multiple links in the traffic network (almost 40% of the total number of traffic network links); since the logical traffic network is fully-connected, a traffic link impacted means the traffic that uses the direct link path is always impacted.

To show the severity of a transport network failure, we report impact on the affected²⁶ node pairs in the traffic network and where we assume that the transport capacity is not fully recoverable from a failure. We found that dynamic routing can still find available capacity to reroute calls and bring down the blocking significantly (from being nearly 100% blocking) due to built-in transport network diversity. Through staggered recovery in the transport network, if we bring up the affected traffic links in a staggered manner,²⁷ blocking gradually improves. This is illustrated in Figure 9. Specifically, we have indicated two lines to illustrate recovery; the solid line represents when the transport network path restoration is recovered without any knowledge of the current traffic volume in the traffic network, whereas the dashed line represents prioritized transport network path restoration allocation that is aided by the knowledge of the current traffic volume in the traffic network along with dynamic routing capability—it is important to note that when the transport network restoration is over (in this case, capacity only partially recoverable due to assumption on the lack of enough protection capacity in the transport network) the traffic network is not fully recovered in the former case, but is fully recovered in the latter case.

Finally, integrated restoration, especially, IP over optical networks, and its implication on traffic engineering is a growing area of interest; for example, see [13], [24], [29], [35].

E. Lessons Learned

Eventually, the question arises about what can we learn in regard to network restoration for traffic and transport networks when done independently, and also in regard to integrated traffic and transport network restoration. We also need to understand how the speed of restoration impacts what we may do in terms of restoration. Incidentally, Figure 9 allows us to understand several different dimensions about network restoration, especially when we interpret that the x-axis represents unit of time without being specific about what the actual value is. Here are some important lessons:

²⁶Instead of all node pairs, we consider only the affected node pairs to show the “worst” case scenario.

²⁷Note that from the transport network point of view, a traffic link restoration is equivalent to a path restoration in the transport network.

- If the transport network consists of self-healing rings with restoration capability in milliseconds (e.g., SONET/SDH rings), then the failure is not perceived in the traffic network; in other words, the intermediate steps shown in the plot in terms of time is instantaneous, and may not trigger any specific traffic network level recovery.
- If transport network capacity is not recoverable, then at least some level of transport diversity should be provided in the routed circuits for traffic network capacity; this can provide some flexibility for the traffic network to address traffic restoration through re-routing. Secondly, traffic restoration protection capacity may be addressed in the traffic network; with this, the end state in the plot can be arrived at almost instantaneously. This situation also essentially applies for traffic network providers who do not own the underlying transport network, i.e., leases capacity from a transport network provider.
- Traffic network restoration can be fully recoverable without requiring fully recovery in the transport network *if* certain information exchange between the traffic network and the transport network is possible regarding a failure—for this to work smoothly, an integrated network management functionality to coordinate between two layers is needed.
- In a mesh transport network, if a dedicated back-up path is provided for every provisioned path, then depending on the speed of the switching logic to move to the back-up path, the failure may or may not be perceived in the traffic network.
- In a mesh transport network, the recovery process may have some delay due to calculation of restored paths. This graph allows us to see how the traffic network may be impacted depending on the speed of this recovery.
- Speed of restoration in the transport network can be the driver in the right combination to do between the traffic and transport network, especially in terms of restoration capacity.
- When a failure in the transport network is recognized by the traffic network (e.g., due to delay in recovery in the transport network), the traffic network starts its own restoration process by rerouting (and possibly new computation of the routing table). As the transport network starts to recover, the traffic network may start changing routing again, thus possibly causing instability in routing and traffic flow behavior during the transient period. Good understanding of protocol interactions with state information exchange is required through further study to determine an appropriate action to take.

A closely related issue with speed of restoration is the cost associated with restoration. The cost of restoration has primarily three major cost components: i) protection capacity cost, ii) switching functionality cost, iii) operational cost. In Section V, we have shown how optimization models can be used for determining protection capacity cost. In many instances, switching functionality cost can be modeled in these optimization models since unit link cost can be thought of as summation of the unit distance-based cost and the unit switching gear cost. Secondly, the formulation of the model is independent of actual component costs for different technologies; thus, the appropriate unit cost can be used for a specific technology without fundamentally needing to change the optimization models. Operational cost is however very hard to model; often a general understanding is that more automated a network is, the less is the operational cost for a failure; on the other hand, it is hard to differentiate between day-to-day cost of normal operation of a network and what is specifically needed whenever a failure occurs. Finally, there is another important cost we need to be aware of which can be called “opportunity” cost: if a provider has a network down often or for a long period of time, then customers may chose to move to other providers—this cost is difficult to model solely within the framework of an optimization model for protection. It may be noted that there can be other costs as well for failures not considered here; for example, redundancy in power to address for a power failure.

VII. TYPES OF FAILURE, AND FAILURE PROPAGATION

Our discussion here has primarily centered around link failures in networks. In many cases, the result is also applicable to node failures when we consider that a node failure in abstract means that all the links connected to the failed node is not available any more. At the same time, it is more appropriate to consider node failure in a network as a separate design problem. For example, large IP networks [17] use redundant routers at a point-of-presence (PoP) to address for any router failure.

In general, it is important to realize that a network may have many different types of failures. There are no recent study available in regard to sources of failure in the public switched telephone network; the last reported study was by Kuhn ([20]). Regarding sources of failure in IP networks, the first one was by Labovitz *et. al.* ([21]), while there has been a series of recent works by researchers at Sprint [5], [17], [25]. It is worth noting that IP network availability is a growing area of interest (see also [7], [19]).

The study for the PSTN was based on reporting required to be submitted to Federal Communication Commission (FCC) by a provider when the provider has a failure that lasts for more than 30 minutes affecting at least 30,000 customers;²⁸ thus, these failures can be considered major failures and do not include short transient failures that the network has managed to heal based on capabilities such as routing. It was reported that errors due to cable cuts constitute about one-fourth of total errors while affecting the network 14% of the time in terms of downtime minutes. Interestingly, while failures due to overload were only 6% in terms of occurrence, it contributed to more than two-fifth in terms of downtime minutes. Hardware failure that included loss of power supply accounted for 19% of the time being only 6% of the total downtime-minutes. It was also reported that software failure was not a big factor. Regardless, Kuhn stated that during the period studied, the PSTN network was very reliable, being up 99.999% of the time; he attributed this reliability due to software reliability and dynamic routing capability of the network to re-route around a failure.

The report by Labovitz *et. al.* on the source of failure in the Internet was based on the trouble ticket log of a regional Internet service provider (which leases the transport capacity from telecommunication providers). Certainly, this report can not be generalized to the entire Internet or other ISPs; on the other hand, this report can serve primarily as indicators of the type of failures than the actual values. Nevertheless, specific values can provide some guideline on what to focus on in terms of reliability objective. The report stated that 16% of the failure were due to maintenance while another 16% were due to power outage. However, they also reported that 15% of failure were due to the underlying transport network (e.g., fiber cut) which the ISPs have little control over. Based on this report, it can be inferred that a traffic network provider such as an ISP can not completely rely on the underlying transport provider to be reliable; thus, an ISP must engineer traffic restoration capacity in its network and request trunk diversity from its transport network provider so that with robust link metric setting (see Section VI-A), it can circumvent most transport network failures.

The series of reports from the Sprint research group is the most recent study available about failure characterization and restoration of an operational IP network based on measurements over a six-month window. It may be noted that in Sprint's case, the optical transport network is also provided by Sprint (but by a different organizational/business unit). They made the following important remark: "failures are part of everyday operation and affect a variety of links" [25]. They reported that 20% of failures occurred during scheduled maintenance activities, although the maintenance window was only for 5% of the time every week. Of the rest of the failures, 30% were shared failures (16.5% were router-related while 11.4% optical related which affected multiple IP network links), and the rest were individual link failures. They

²⁸A limitation of such reporting is that it can not capture the benefit of protection capacity already deployed in the network which may have resulted in the ability to provide services gracefully despite some failures.

also reported that 50% of the failures were of up to a minute duration, 81% were of up to ten minute duration (which they classify as “transient” failures); only 10% of the failures were longer than 45 minutes duration. By clever use of forward path re-computation of shortest paths (after a failure) and adjustment of various timers, they were able to bring down the recovery time to less than one second [17] for failures “seen” by the IP network. It is worthwhile to note that Sprint deploys networks of SONET rings in most of its optical transport network; despite this feature, it is clear that there are many failure events still seen by the IP network (which uses this transport network), and thus, the development of design and restoration mechanisms independently for the traffic and the transport network is evidently important.

Finally, we conclude this section with an example of failure propagation somewhat typical to Internet routing architecture. Recall that Internet routing architecture is a federation of autonomous systems connected by BGP. Through BGP, reachability information is communicated about a network connected to the Internet where a network is identified by an IP-prefix.²⁹ When a BGP router³⁰ faces a problem (for example, due to router CPU overload³¹), keep-alive messages (which are used for indicating that two neighboring BGP routers are in communication) may not be communicated on a timely basis—this can make one router think that the other router is not available any more, much like as if the link between the routers has gone down. Each router can then generate a series of messages to indicate about non-reachability which can cascade from one autonomous system to another one; due to the path vector protocol nature of the BGP protocol and to avoid route looping problem, finding another path through other autonomous systems can take a long time (sometimes, in the order of 15 minutes). A second problem is that when the CPU overload subsides and both the routers determine that they can talk to each other again (that means the link is up again)—this can cause another storm of activities in regard to re-updating reachability information thus causing an instable behavior. For a specific example of CPU overload, consider the impact of a recent virus on the routing infrastructure. Routers usually cache forwarding path for commonly routed IP addresses to provide fast lookup and fast packet routing. During the Code Red and Nimda virus attack [8], instances of the virus started random IP port scanning; this resulted in cache misses as well as router error messages³² leading to extensive CPU overload in routers, thus causing the instable behavior just described.

VIII. SUMMARY

Network restoration is a critical area to understand in the design and deployment of communication networks. In this exposition, we have considered a variety of networks and networking technologies to argue that classification of networks into two broad categories, traffic network and transport network, provides us with a systemic way to consider network protection design models and associated restoration techniques to address for a network failure. In particular, we have shown how this classification impacts the development of appropriate optimization models.

In general, existence of multiple layers (to address for different purpose) makes network protection and restoration a difficult problem. On either extremes are the scenarios where the restoration is done only in the traffic network or is only in the transport network. Certainly, a combination of strategies give the best option to address for many different types of failures which also depends on the capability available in a network and the associated cost of doing it. Finally, we point out that besides a link (or a node) failure,

²⁹A network identified through IP-prefix is based on higher order bits of the IP address along with a subnet mask; such a network should not be confused with an autonomous system.

³⁰A BGP router is also referred to as a BGP speaker.

³¹See [22]; while router vendors have made progress on how to handle keepalive messages during CPU overload, this is a good example to understand the basics of Internet routing instability.

³²through ICMP error messages.

there are other types of failures that a network regularly faces for which a provider needs to develop an appropriate restoration strategy based on its reliability objective. Many of these problems are difficult to model since there are conflicting interests and strategies involved while ensuring that network instability can be avoided—this is an area that requires further exploration.

APPENDIX: ACRONYMS

APS := Automatic Protection Switching
 ATM := Asynchronous Transfer Mode
 AS := Autonomous System
 BGP := Border Gateway Protocol
 DCR := Dynamically Controlled Routing
 DCS := Digital Cross-Connect System
 FCC := Federal Communication Commission
 ICMP := Internet Control Message Protocol
 IS-IS := Intermediate System-to-Intermediate System
 ISP := Internet Service Provider
 IXC := Inter-exchange Carrier
 LDP := Label Distribution Protocol
 LEC := Local-exchange Carrier
 LSP := label Switched Path
 LSR := Label Switched Router
 MPLS := Multi-Protocol Label Switching
 OC := Optical Carrier
 OXC := Optical Cross-connects
 OSPF := Open Shortest Path First
 PoS := Packet over SONET
 PSTN := Public Switched Telephone Network
 RTNR := Real-Time Network Routing
 SDH := Synchronous Digital Hierarchy
 SONET := Synchronous Optical Network
 TSP := Telephone Service Provider
 VP := Virtual Path
 WDM := Wave Division Multiplexing

ACKNOWLEDGMENTS

This work in some sense is a reflection of my interest to understand network protection and restoration for more than fifteen years for many different types of networks. During this period, I have benefited from funding provided by DARPA (Agreement no. F30602-97-1-0257), NSF (grant no. NCR-9506652), the University of Missouri Research Board, and Sprint Corporation. Needless to say, my interest in this area initially piqued during my employment at the AT&T Bell Laboratories (1987–1989).

I have personally benefited from communication/discussion with several people over the years in regard to traffic and transport networks, and network protection and restoration; for that, I like to thank Jerry Ash, Supratik Bhattacharyya, Robert Doverspike, Wayne Grover, Hadriel Kaplan, Karen Medhi, Jim Pearce, Michał Pióro, John Strand, and David Tipper. Finally, I like to thank Balaji Krithikaivasan for drawing several figures included in this paper, and Amit Sinha for carefully reading a draft of this paper.

REFERENCES

- [1] R. K. Ahuja, T. L. Magnanti, and J. B. Orlin. *Network Flows: Theory, Algorithms, and Applications*. Prentice Hall, 1993.
- [2] G. R. Ash. *Dynamic Routing in Telecommunication Networks*. McGraw-Hill, 1997.
- [3] G. R. Ash, R. H. Cardwell, and R. P. Murray. Design and optimization of networks with dynamic routing. *Bell System Technical Journal*, 60:1787–1820, 1981.
- [4] G. R. Ash and P. Chemouil. 20 years of dynamic routing in telephone networks: Looking backward to the future. *IEEE Global Communications Newsletter*, pages 1–4, October 2004. (appears as insert in IEEE Communication Magazine, October 2004 issue).
- [5] S. Bhattacharyya and G. Iannaccone. Availability and survivability in IP networks. Tutorial presented at the 11th IEEE International Conference on Network Protocols (ICNP), November 2003.
- [6] L. S. Buriol, M. G. C. Resende, C. C. Ribeiro, and M. Thorup. A hybrid genetic algorithm for the weight setting problem in OSPF/IS-IS routing. *Networks*, 2005. In press.
- [7] R. Callon. Availability & security for IP data networks. Tutorial presented at the 4th International Workshop on Design of Reliable Communication Networks (DRCN), Banff, Canada, October 2003.
- [8] J. Cowie and A. Ogielski. Global routing instabilities during Code Red 2 and Nimda worm propagation. Presentation at NANOG23 Meeting, Oakland, CA, October 2001.
- [9] M. Ericsson, M. G. C. Resende, and P. M. Pardalos. A genetic algorithm for the weight setting problem in OSPF routing. *Journal of Combinatorial Optimization*, 6(3):229–333, 2002.
- [10] A. Feldmann, A. Greenberg, C. Lund, N. Reingold, J. Rexford, and F. True. Deriving traffic demands for operational IP networks: methodology and experience. *IEEE/ACM Transactions on Networking*, 9:265–279, 2001.
- [11] B. Fortz and M. Thorup. Internet traffic engineering by optimizing OSPF weights. In *Proc. 19th IEEE Conference on Computer Communications (INFOCOM'2000)*, pages 519–528, 2000.
- [12] B. Fortz and M. Thorup. Increasing internet capacity using local search. *Computational Optimization and Applications*, 29(1):13–48, 2004. Preliminary short version of this paper published as *Internet Traffic Engineering by Optimizing OSPF weights*, in Proc. 19th IEEE Conf. on Computer Communications (INFOCOM 2000).
- [13] A. Fumagalli and L. Valcarenghi. IP restoration vs. WDM protection: Is there an optimal choice? *IEEE Network*, 14(6):34–41, November 2000.
- [14] A. Girard. *Routing and Dimensioning in Circuit-Switched Networks*. Addison-Wesley, Reading, MA, 1990.
- [15] W. Grover and D. Stametaelakis. Bridging the ring-mesh dichotomy with p-cycles. In *Proc. Design of Reliable Communication Networks (DRCN'2000)*, Munich, pages 92–104, 2000.
- [16] W. D. Grover. *Mesh-based Survivable Networks: Options and Strategies for Optical, MPLS, SONET and ATM Networking*. Prentice Hall, 2004.
- [17] G. Iannaccone, C.-N. Chuah, S. Bhattacharyya, and C. Diot. Feasibility of IP restoration in a tier-1 backbone. *IEEE Network*, 18(2):13–19, March-April 2004.
- [18] R. R. Iraschko, M. MacGregor, and W. D. Grover. Optimal capacity placement for path restoration in STM or ATM mesh survivable networks. *IEEE/ACM Trans. on Networking*, 6:325–336, 1998.
- [19] H. Kaplan. Resilient IP network design. Tutorial presented at the 3th IEEE Workshop on IP Operations & Management (IPOM), Kansas City, Missouri, USA, October 2003.
- [20] D. R. Kuhn. Sources of failure in public switched telephone network. *IEEE Computer*, 30(4):31–36, April 1997.
- [21] C. Labovitz, A. Ahuja, and F. Jahanian. Experimental study of Internet stability and wide-area network failures. In *Proceedings of Twenty-Ninth Annual International Symposium on Fault-Tolerant Computing (FTCS99)*, pages 278–285, Madison, Wisconsin, June 1999.
- [22] C. Labovitz, G. R. Malan, and F. Jahanian. Internet routing instability. *IEEE/ACM Transactions on Networking*, 6:515–528, 1998.
- [23] E. L. Lawler. *Combinatorial Optimization: Networks and Metroids*. Holt, Rinehart, and Winston, 1976.
- [24] Y. Lee and B. Mukherjee. Traffic engineering in next-generation optical networks. *IEEE Communications Surveys*, 6(3):16–33, 2004.
- [25] A. Markopoulou, G. Iannaccone, S. Bhattacharyya, C.-N. Chuah, and C. Diot. Characterization of failures in an IP backbone. In *Proc. of 23rd IEEE Conference on Computer Communication (INFOCOM'2004)*, pages 2307–2317, Hong Kong, March 2004.
- [26] D. Medhi. Diverse routing for survivability in a fiber-based sparse network. In *Proc. IEEE International Conference on Communication (ICC'91)*, pages 672–676, Denver, Colorado, June 1991.
- [27] D. Medhi. A unified approach to network survivability for teletraffic networks: Models, algorithms and analysis. *IEEE Trans. on Communications*, 42:534–548, 1994.
- [28] D. Medhi and R. Khurana. Optimization and performance of network restoration schemes for wide-area teletraffic networks. *Journal of Network and Systems Management*, 3(3):265–294, 1995.
- [29] D. Medhi and D. Tipper. Multi-layered network survivability – models, analysis, architecture, framework and implementation: An overview. In *Proc. DARPA Information Survivability Conference and Exposition (DISCEX'2000)*, volume I, pages 173–186, Hilton Head Island, South Carolina, USA, January 2000.
- [30] A. Nucci, B. Schroeder, S. Bhattacharyya, N. Taft, and C. Diot. IGP link weight assignment for transient link failures. In *Proc. 18th International Teletraffic Congress (ITC18)*, pages 321–330, Berlin, Germany, September 2003.
- [31] M. Pióro and D. Medhi. *Routing, Flow and Capacity Design in Communication and Computer Networks*. Morgan Kaufmann Publishers, 2004.

- [32] M. Pióro, A. Szentesi, J. Harmatos, A. Jüttner, P. Gajowniczek, and S. Kozdrowski. On OSPF related network optimization problems. *Performance Evaluation*, 48:201–223, 2002.
- [33] R. F. Rey. (ed.) *Engineering and Operations in the Bell System – 2nd Edition*. AT&T Bell Laboratories, Murray Hill, New Jersey, 1983.
- [34] S. Srivastava, G. Agrawal, M. Pióro, and D. Medhi. Determining link weight system under various objectives for OSPF networks using a Lagrangian relaxation-based approach. *(IEEE) e-Trans. Network and Systems Management*, 2005. In press.
- [35] J. Strand. Converging protection and restoration strategies of the IP and optical layers to support the survival of IP services. MPLS Summit, January 2001.
- [36] J. W. Suurballe. Disjoint paths in a network. *Networks*, 4:125–145, 1974.
- [37] J. W. Suurballe and R. E. Tarjan. A quick method for finding shortest pairs of disjoint paths. *Networks*, 14:325–336, 1984.
- [38] J.-P. Vasseur, M. Pickavet, and P. Demeester. *Network Recovery: Protection and Restoration of Optical, SONET-SDH, IP, and MPLS*. Morgan Kaufmann Publishers, 2004.
- [39] Y. Wang, Z. Wang, and L. Zhang. Internet traffic engineering without full mesh overlaying. In *Proc. 20th IEEE Conference on Computer Communications (INFOCOM'2001)*, pages 565–571, New York, USA, 2001.
- [40] D. Yuan. A bi-criteria optimization approach for robust OSPF routing. In *Proc. IEEE Workshop on IP Operations and Management (IPOM'2003)*, pages 91–98, Kansas City, USA, October 2003.