Chapter 4. Network Failures

Network performance has become a critical issue in the area of computer networks and the contemporary communications field. There is a greater need than ever before for reliable service due to several factors: an increasing dependence of end-users on telecommunications; a greater demand for high-quality performance; the need for assured service; and the special reliability needs for government, emergency and military organizations. These demands have resulted in much work on categorizing, classifying, and analyzing network failures as well as studies in areas of network survivability performance, network survivability characterization and restoration [20].

4.1. Classification

Although somewhat ambiguous, classification of failures has received a lot of attention from the research community and telecommunications standards-setting bodies. Based on the work of ANSI Technical Subcommittee T1A1, three features of an outage in a network can be used to describe outage categories [1].

The three features are: 1) unservability (U), which represents a percentage of failed links or circuits in circuit switched networks, percentage of lost or unusable packets delivered in a packet switched network and a percentage of failed service units for leased lines; 2) duration (D), or a time period for which unservability lasts and 3) weight (W) which represents a population or geographic area in which the unservability exceeds a certain threshold [1].

The (U, D, W) triple can be graphed in three-dimensional space. The values of U, D and W for a particular failure would then define a region as shown in Figure 4.1 [1].

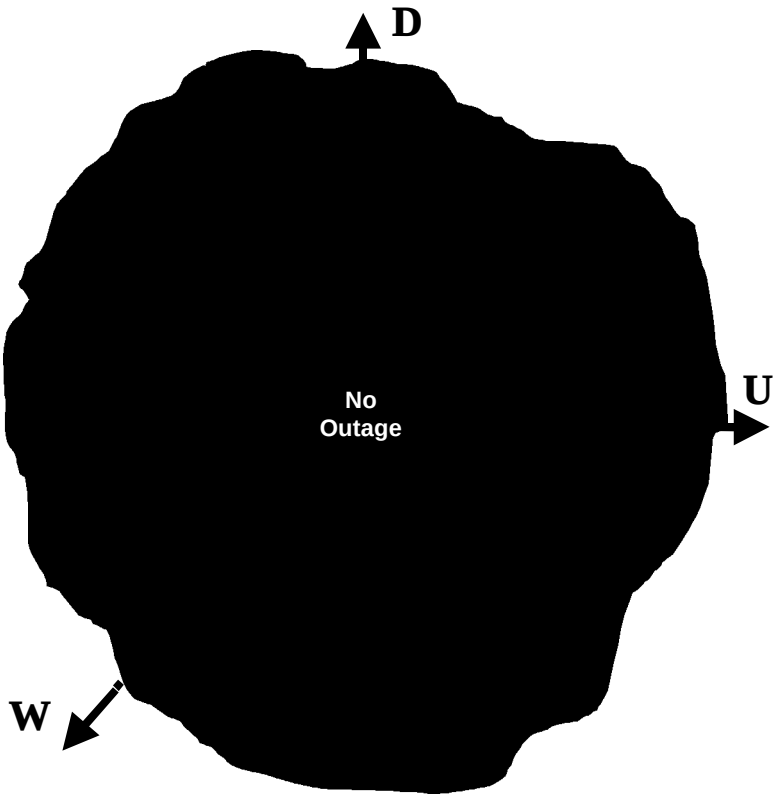

Figure 4.1 Failure regions for U, D, and E

The failure categories that can be defined based on the three features are catastrophic, major or minor [1]. Catastrophic network failures are often triggered by such disastrous occurrences as earthquakes, floods, tornadoes, power grid failures, or war. Major cable backbone failures can happen as a result of fire, terrorism, or tandem switch failure. Minor single link or path failures often are due to fiber failure, equipment failure, and shelf or unit failure. It

should be pointed out that these failures are all hard failures and assume a complete failure of a part of a network no matter how small a role the part plays.

4.2. Restoration Techniques

Today, most of the solutions for these hard failures have been incorporated in the lower layers of networks, particularly in SONET/SDH. ITU-T has released many recommendations for SONET/SDH restoration techniques such as automatic protection switch (APS), self-healing ring (SHR) and self-healing network (SHN). ITU-T has also begun working on standardizing restoration and self-healing techniques for ATM networks, which include slight modifications of the same methods implemented in SONET/SDH, as well as new ones unique to ATM, such as failure-resistant virtual path (FRVP) [21].

The main drive behind ITU-T's continued work toward expending restoration capabilities into the higher network layers is the one way dependency between the protocol layers. In other words, the lower layers cannot see the defects occurring at the higher ones while the higher ones will always be affected by defects in the lower layers. Thus, SONET/SDH offers very fast restoration performance from fiber failures but does not protect against defects in the ATM layer because ATM cell defects are invisible to the SONET/SDH defect-detection mechanism [22]. As newer technologies emerge as potential new layers there will be a continuing need to study and later standardize their survivability/restoration schemes, as well as define their roles in the multi-layered networks as a whole.

4.2.1. Single-Layer Network Restoration

Just as classification of network failures is somewhat ambiguous, so is the classification of network restoration methods. The two largest categories that cover most, if not all network restoration methods are centralized and distributed control schemes.

4.2.1.1. Centralized Control Schemes

Centralized control schemes include one main center that oversees the entire network and is responsible for the entire network survivability process, from detection of failures to finding an alternate route. Since the control center has an overview of the entire network, it has a better chance of finding the best alternate route, as well as distributing the extra load from the failed network elements most efficiently. Centralized control schemes can be implemented in SONET/SDH as well as in an ATM layer. However, the big drawback is the complexity of such centralized management, and the relatively slow speed of restoration. Examples of implemented centralized control schemes are AT&T's FASTAR and NTT's SUCCESS [23, 21].

4.2.1.2. Distributed Control Schemes

Distributed control schemes use a decentralized approach to network survivability issues, where many or all network elements play some role in detecting failures and selecting the best and the quickest alternate route. The three largest categories of implementing distributed control schemes are APS, SHR and SHN [21]. However, in order to provide full restoration capabilities

APS systems require 100% redundancy, and SHRs require 100% or more redundancy. Certain SHNs, such as mesh-restorable networks, can achieve lower redundancy levels than SHRs [24].

APS comes in many flavors and is the simplest and most popular distributed control restoration mechanism. The basic premise for all APS systems relies on a set of working and a set of backup links. 1+1 (parallel) APS is based on parallel transmission of the same data on a working as well as a backup link, and, in case of a detected failure, the receiver shifts from a working link to a backup link. 1:1 (non-parallel) APS also uses one working and one backup link, only in this case nothing is being transmitted over a backup link until the failure is detected, after which both transmitter and receiver switch to the backup link. Then there is m:n APS which is just an extension of the 1:1 APS system. In order to lower some redundancy levels, generally m (the number of working links) would be smaller than n (the number of backup links). APS can easily be implemented in ATM either through means of its VPs or VCs. 1:1 VP-APS has even been discussed in ITU-T as a basic restoration function in ATM networks [21].

SHR is a high-speed restoration scheme for ring topology SONET/SDH networks and is similar to 1:1 or 1+1 APS methods. An example would be a Bi-directional Line Switched Ring (BLSR), which can be implemented either on two or four fibers and guarantees 60 ms restoration performance [22]. SHRs can also be implemented in the ATM layer, but since ATM does not depend as much on the layout of the fiber and network's physical topology, this method does not offer any cost advantage over VP-APS.

SHN is an expansion of SHR without topological restrictions. Most commonly the best alternate route in an SHN is found by message transmission

between the network nodes, often employing flooding algorithms. The clear disadvantage is that these topology update algorithms can generate many messages, and are therefore limited to restoration over small geographical areas [22].

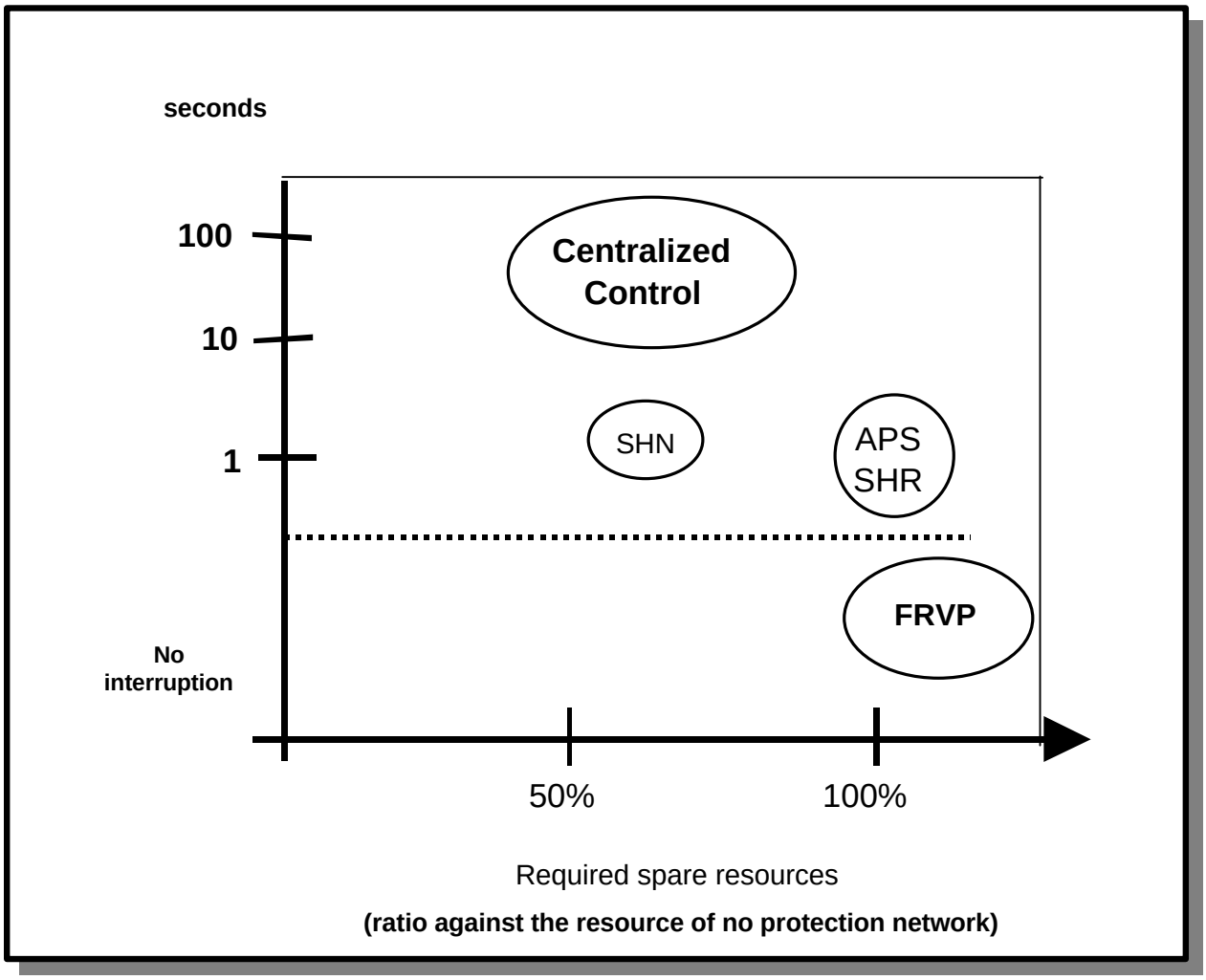

Figure 4.2 Network Restoration Schemes

FRVP realizes failure free transmission even under network failure and thus offers no interruption of service, as shown in Figure 4.2 [21]. In FRVP the transmitter would duplicate all the outgoing traffic and send it over the multiple VPs, each routed over a separate physical link. The receiver would constantly compare the cells arriving from separate VPs, choose the cells without error, and then pass the cells without error onto the user [21].

4.2.2. Multi-Layer Network Restoration

The multilayered nature of computer networks (for example, WDM-SONET-ATM-IP) makes the problem of network restoration more complex. Although each layer has its own ways of dealing with failures, and each has advantages and disadvantages (see Figure 4.3), the question becomes how efficient is the overall network restoration system. Identifying solutions to this problem of overall network protection in an efficient manner, while taking into account the individual restoration mechanisms of each layer, has been on the main agenda of projects such as ACTS' PANEL [25]. However, solutions such as layer escalation, subnetwork escalation, and scheme escalation have been offered.

Layer escalation involves a restoration process that begins at the lowest layer; if the first layer is unable to eliminate the failure, then the process proceeds layer-by-layer up the protocol stack until all the failures are removed.

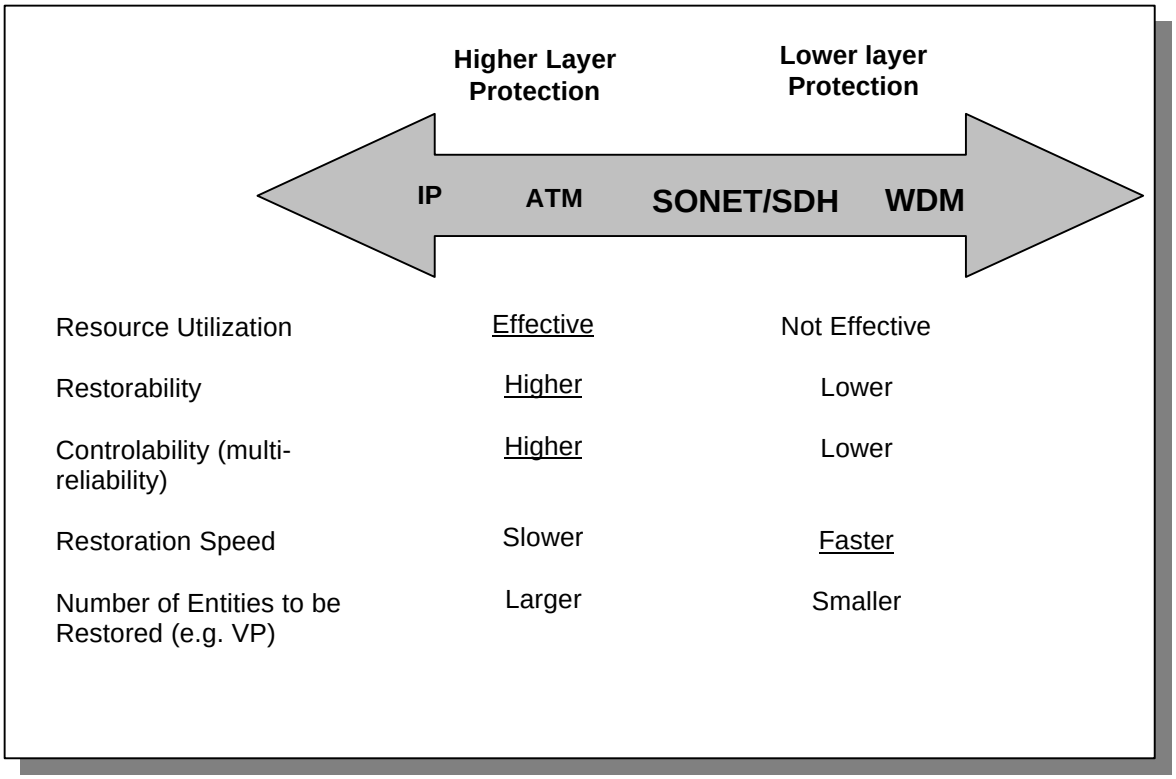

Figure 4.3 Characteristics of Each Layer

Subnetwork escalation schemes involve a restoration process starting physically close to the failed network element; if the subnetwork does not have an alternate route or additional resources, the process continues to expand the restoration until an alternate route and / or resources are found.

Scheme escalation involves restoration according to a set plan. An example would be an initial restoration attempt by a certain preplanned scheme; in the event that the plan does not eliminate all the failures, then the dynamic planned scheme would be employed [21].

4.3. Soft Failures

Soft failures are not as clear to define and have not yet been studied extensively. Soft failures can include wide variety of component or system malfunctions components where performance is compromised without triggering hard failure alarms. For example, it is possible to have several components performing at a marginal or suboptimal level where the overall performance of the system may be degraded. Therefore it is a goal of this project to dynamically load and stress the system, and to then observe its performance just before the initiation of the built in protection mechanisms, such as those previously described. The intention is to gain an insight into this area of marginal network performance where no particular layer, protocol or hardware is obviously malfunctioning, but overall performance has decreased as observed by the end user.