PART II: Multi-layer TE in Metropolitan Area Networks

Traffic Engineering is concerned with the performance and resources optimization in response to dynamic traffic demands and/or node and link failures [41].

In this second part of the Ph.D. Thesis, we concentrate on the design and evaluation of efficient resilience strategies to face with different failure scenarios which can occur in the networks. Specifically, we concentrate on an IP/MPLS over Resilient Packet Ring (RPR) over optical transport network scenario for metropolitan area networks. We present the DHOT coordination approach between the protection mechanisms provided by the RPR technology and the ones defined in the optical layer. The novelty of the suggested approach relies on the required interworking between the RPR and the optical layer.

Firstly we introduce the multi-layer resilience concept, highlighting the related work on this topic. Then, we describe the strength and weakness of the recent standardized packet-based RPR technology and finally it is presented the DHOT approach, discussing its characteristics and its performance evaluation. An interworking strategy between RPR and the optical layer, based on taking benefits from the automatic switching of optical connections capability to optimize the RPR bandwidth utilization, is also presented and discussed.

5 Multi-layer Resilience

The failures occurrences produce a strong impact on network performance. When failures occur in the network, there is the need of rerouting/switching the affected traffic along alternative routes. For example, this possibly implies longer routes and therefore higher propagation delays and thus higher end-to-end delays. For time-sensitive applications (e.g. multimedia applications, voice over IP), this is an important factor in assessing the performance of the recovery strategy.

In case of failures, the optimization of the utilization of the network resources is very critical. Indeed, network survivability/recovery/resilience, namely the capability of the network to recover traffic affected by failures, has become of vital importance in current and next generation networks [25], [26], [88] and [89]. With the growth of data traffic that has to be transported, the networks need to be very robust to face the different kinds of failures that can occur. Therefore, network operators have to take special precautions in order to do networks survivable. Since it is difficult to prevent failures in the network infrastructure (equipment failures, cable breaks, etc.) the network design objective is to maintain services availability even under failure conditions. In order to make the networks more reliable, they have to be reconfigurable and such reconfiguration has to be fast in order to minimize the traffic lost and services interruptions. At the same time, the recovery strategies have to optimise the utilisation of the network resources while, from the Network Operator's point of view, they should not increase too much the network cost (CAPEX and OPEX).

In the case of metropolitan area networks, the emerging Resilient Packet Ring (RPR) technology provides powerful protection mechanisms which minimize the time needed to restore the traffic and, thus, the traffic lost due to the failures. RPR recovery mechanisms do not need to pre-allocate spare network resources to be used in case of failures.

This second part of the Ph.D. Thesis deals with the design and performance evaluation of multi-layer resilience strategies to be used in an IP/MPLS over RPR over intelligent optical networks.

5.1 Network Survivability

With the exponential growth of the traffic that has to be transported, network resilience has gained a critical role in the design of telecommunication networks. The failures can occur at different layers composing the network architecture and it is very important to decide at which layer the recovery is implemented. This is due to the fact that, for example, lower layers could not aware of failure occurred at the higher layers. The recovery mechanisms have to be designed basically with the aim to be simple from the implementation point of view, to minimize the traffic losses due to the failures and finally to optimize the utilization of the network resources, reaching TE objectives.

Among others, some of the most common failures that have to be taken into account in order to design a survivable network are [25]:

- **Node Failure:** A node can fail because of different reasons such as power down or heat. Thus, the connections that use that node are interrupted and the communications to the neighbouring nodes are lost.
- **Link Failure:** Link failure is a common failure, which interrupts the communication between two neighbouring nodes. The failure of a link can be detected at several layers.
- **Router Failure:** This failure occurs at the IP layer and therefore the detection and recovery is done at this layer. This failure can be detected by timeouts and then, a backup router replaces the failed router.
- **Optical Path failure:** Optical path failure interrupts the communication between the sending and receiving nodes of the light path. This failure can be caused by a bad functioning of lasers, by a bad-established switch connection, etc. This failure affects one optical path and therefore, only the data belonging to this interrupted path have to be restored.

To make a network survivable, two approaches can be used, namely the protection and restoration approaches [90], [3]. The first one is much quicker than the second one and it implies the use of fixed, pre-calculated routes and pre-allocated spare capacity, eventually used to transport low priority traffic. Specifically, in point-to-point links, basically two types of protection

mechanisms are used namely 1+1 and 1:1 (more generally 1:N). In 1+1 protection, traffic is sent simultaneously on two different physically disjoint paths between source and destination nodes; one of the path is called working path while the second is called protection (recovery) path. The destination node, in absence of failures, selects one of the two paths for reception. In the case the failure of that path is produced, the receptor node switches to the other path. In such a mechanism, no signalling between nodes to recovery from the failure is required. In 1:1 protection, two paths are available between source and destination nodes. In this case, the data are sent only through the working path. In case a failure occurs, both the source node and the destination node switch to the other pre-defined path. In this case, a signalling mechanism is required between the source and the destination node. However, the advantage is that in absence of failure, the second path can be used to transmit, for example, low priority traffic.

On the other hand, the restoration approach implies the rerouting of the affected traffic calculating an alternative route once the failure has occurred. It is based on using any available capacity in the network. The restoration mechanisms are much more efficient that protection in terms of network resource utilization since no spare resources are needed to be pre-allocated for recovery purposes; however, since the affected traffic has to be rerouted, this leads to higher recovery times, which is the time needed to recover from the failure [3].

In the current multi-layers networks, each layer (e.g. IP, SONET/SDH) has its own protection mechanism built in, independent from the other layers [25], [91]. Reliability basically relies on protection at the SONET/SDH network layer. Indeed, different protection mechanisms have been designed for survivable SONET/SDH networks that allow fast recovery within the target of 50 ms [92], [93]. Nevertheless, SONET/SDH protection is mainly limited to ring topologies and it is not able to distinguish between different priorities of traffic and it has not vision of higher layer failures. On the other hand, the IP layer has limited recovery functionalities (i.e., rerouting). The routing protocols can reroute the traffic in case of failures, but the time needed for the routing algorithms to re-converge is in the order of seconds. Thus, this rerouting time compared to the 50 ms of the SONET/SDH is extremely poor, especially in the case of real time applications. MultiProtocol Label Switching (MPLS) technology can be used to enhance the survivability of IP networks. Basically, mechanisms defined for protection in MPLS rely on pre-established protection LSPs, used as backups for the working LSPs, achieving better protection switching times than IP networks [94]. The backup (or alternative) LSPs are set-up (signalled) at the moment the failure is detected by the IP/MPLS router. These mechanisms rely on the control plane functionalities of MPLS [31].

5.2 Multi-layer resilience: Related Work

As before mentioned, in the current multi-layers networks each layer has its own protection mechanism built in. Various technologies at different layers may provide protection and/or restoration capabilities at different temporal granularities (i.e., in terms of time scales) and at different bandwidth granularity (from packet-level to circuit level) [90]. The recovery actions rely on a single-layer strategy, which means that a single layer takes the responsibility to recovery from the failure. These are taken either in the lowest (bottom) layer or in the highest (top) layer. The resilience single-layer strategy is very simple from the implementation point of view. Its major drawback concerns that it may not be able to recover the network from all kind of failures that can occur within the network [26]. Moreover, deciding at which layer the recovery actions have to be carried out is very challenging.

A more efficient approach, consisting on to combine recovery mechanisms in more than one layer, has been proposed in [88]. Recovery at multiple layers (multi-layer resilience) increases the reliability of the multi-layer networks, since the network is very robust to a wider range of failures scenario. It is beneficial in order to avoid contention between the different single-layer recovery schemes and it takes benefits from the advantages of each layer recovery mechanism.

Indeed, the definition of multi-layer resilience approaches/strategies leads to decrease the investments costs required to ensure a certain survivability target and leads to overall better utilization of the network resources after the network reconfiguration [88].

Generally speaking, to evaluate the effectiveness of multi-layer resilience strategies, an important issue deals with the definition of their actual performance parameters.

In [25], the authors defined the cost, the complexity and the feasibility of the recovery strategy.

The cost is strictly dependent on the properties of the used resilience techniques such as the extra resources (spare resources) required to enable the recovery actions. This is closely related to the planning of the network, which must enable the provisioning of network connections throughout occurring network failures.

Aside from the actual complexity of the resilience mechanisms, routes have to be calculated and set up, and this may increase the complexity even though the resilience protocol itself can be fairly simple (like for example the protection mechanisms).

Finally, feasibility is related to complexity, but is to be considered on a more general level and considers whether a resilience strategy is feasible/achievable to be applied.

When considering multi-layer resilience, the simplest way to implement it is to run the different mechanisms in parallel and independently from each other; it is called the *uncoordinated approach* [88], [94]. As each layer detects the failure, it starts to run its own recovery mechanism.

Such solution is very simple from the implementation point of view since no standardization of coordination signals between layers is required. It is also simple from the operational point of view. The most important drawback is that multiple layers can start the recovery action contemporarily leading in such a way to potential networks instability (above all at the higher network layers) and unnecessary reduction of the overall available bandwidth. Thus, coordination among the different recovery mechanisms is required.

A way for the coordination of the recovery mechanisms relies on using the so-called sequential approach, namely one layer tries to restore the traffic and the following layer only takes over if the current layer does not succeed in recovery the traffic.

Specifically, two sequential approaches have been proposed in [89], namely:

- ***The bottom-up approach***: The lower layer starts the recovery actions. In the case that it cannot restore all the traffic, then higher layer actions are triggered.

- ***The top-down approach***: Recovery actions are initiated at the top/highest possible layer and only if the higher layer cannot restore all traffic, lower layer actions are triggered. An advantage of this approach is that a higher layer can more easily differentiate traffic with respect to the service classes (service-based recovery) and thus it may try to recover high priority traffic first and then try to restore low priority traffic. A major drawback is that a lower layer may not detect whether a higher layer is able to restore traffic or not and thus an explicit signal between the layers is required for this purpose.

The implementation of these multi-layer resilience strategies implies the need to define some rules to coordinate the recovery actions between the different network layers. Authors in [94], [95] and [96] have proposed the following three different rules.

The first one is based on the hold-off timer concept. It can be applied both for the bottom-up and top-down approaches. Specifically, a hold-off timer is set at the moment the server (client) layer starts attempting to restore the traffic. If this hold-off timer expires and the traffic is not restored, then the client (server) layer will take over the recovery actions while the server (client)

layer ceases its attempts. It does not require any interworking between layers. Therefore, it is probably less appropriate for the top-down approach, since the lower layer should be notified with an explicit signal whether the higher layer managed to restore the traffic or not. The main drawback of a hold-off timer is that higher (lower) layer recovery actions are always delayed, independent of the failure scenario.

To overcome this delay, a second strategy, based on using a recovery token signal between layers, has been proposed [26], [94]. It is based on the fact that the server layer sends the recovery token, by means of an explicit signal, to the client layer from the moment that it knows that it cannot restore traffic anymore. Contrarily to the hold-off timer approach, it requires the interworking between the layers involved in the recovery. Moreover, when comparing the recovery token approach with the hold-off timer one, its major drawback consists on that a recovery token signal needs to be incorporated in the standardization of the interface between network layers. Therefore, even though its complexity is rather low, its feasibility is rather high.

Finally, in [94], a third possible strategy, namely the integrated approach, has been proposed. It is based on a single integrated multi-layer recovery scheme. This implies that this has a full overview of all the network layers and that it can decide when and in which layer (or layers) to take the appropriate recovery actions. Although it is the most flexible coordination mechanism, the major issue is its implementation. It is unlikely to develop a single recovery scheme, controlling and having an overview of all network layers, in current overlay-based networks. The integrated approach might represent an interesting solution if a peer-to-peer network model is used.

5.3 Problem addressed in this Ph.D. Thesis

The second part of this Ph.D. Thesis is related with the design and evaluation of a multi-layer resilience strategy for metropolitan area networks. Specifically it takes benefits from the characteristics of the recovery mechanisms of the emerging Resilient Packet Rings layer 2 technology and the ones designed for the optical layer. The proposed strategy/mechanism is based on the definition of interworking rules between the RPR layer and the optical layer with the aim to recovery faster from failures while achieving the optimization of the utilization of the network resources, reaching in such a way traffic engineering objectives. Specifically, firstly, the double hold-off timer approach, which improves the hold-off timer one, is presented and its performance evaluation discussed.

Secondly, if the failure is recovered at the RPR layer, this recovery action implies the substantial reduction of the bandwidth available at the logical level. To avoid such bandwidth reduction, the automatic provisioning of connections capability provided by the intelligent optical layer (i.e., ASON/GMPLS networks) is used. Specifically, we present and discuss an algorithm based on monitoring the traffic load carried by the light path connecting two IP/RPR routers and, on the basis of such monitoring, the request for a switched connection to be used temporarily as additional light path connecting the routers is triggered.