Multi-layer resilience schemes and their control plane support

Victor Lopez, Juan Pedro Fernandez Palacios
Telefónica I+D/GCTO
c/Ronda de la Comunicación s/n, 28050
Madrid, Spain
Email: victor.lopezalvarez@telefonica.com

Thomas Szyrkowiec, Mohit Chamania
ADVA Optical Networking
Germany

Domenico Siracusa
Fondazione Bruno Kessler
Trento Italy

***Abstract*— Network operators design and manage IP/MPLS and optical networks on a per-layer basis, to the point that they are run as different business areas within the operator. However, there are clear CAPEX and OPEX savings that network operators can achieve by simplifying the network infrastructure. Moreover, the evolution of optical equipment and the introduction of network programmability are accelerating the adoption of multi-layer schemes in real networks.**

This paper revisions the planning process considering resilience schemes for IP and optical networks. It also presents an evolutionary view on the control plane and SDN paradigms that enable the support of multi-layer schemes in real networks.

Keywords— Network planning; multi-layer architecture; SDN; control plane; Path Computation

I. INTRODUCTION

Core networks have experienced a clear simplification process in the last decade. MPLS technology applied ATM concepts to the emerging packet switching paradigm and MPLS became the current standard in packet core networks. More recently, WDM/OTN networks with GMPLS control plane emerges as the next generation transport network, combining the scalability of WDM technologies with the dynamicity provided by a control plane. Moreover, even though IP/MPLS and WDM/OTN still represent two significantly different domains, a critical mass of experts is working towards further integration as the next natural step in network architecture evolution [1]. Authors in [2,3] demonstrate that significant CAPEX savings could be obtained by a rational combination of optical and electronic switching for transit traffic.

Even though the network operators are migrating towards an IP/MPLS over WDM architecture, there is still a separation of the IP and optical management layers, which leads to highly redundant and un-coordinated protection schemes. In current typical network operator's deployments, there are protection and restoration mechanisms for each layer. Moreover, each IP link is designed with peak load link utilization around 30-50%, to ensure enough capacity in the IP network in case recovery in the transport network fails. As there is no information exchange between them, it is not possible to coordinate the process. Each layer carries out its own protection mechanisms without information exchange between the layers. Each connection used to provision an IP link in the transport network is protected using a dedicated 1+1 protection scheme, and each IP router and card is duplicated to protect from single failures. These means that the resources for protection remains high even though there is a huge pressure to reduce the CAPEX in the networks.

Multi-layer survivability mechanisms is a topic with high interest in the research community. Multi-layer in an ATM over SDH/WDM architecture was studied in [4]. Moreover, when the the network architecture changed to IP/MPLS over WDM networks, similar studies were done considering the new technological capabilities. The work has considered several topics: new metrics to recover from failures like in [5], CAPEX reduction like in [6], routing mechanisms suitable for multi-layer restoration as stated in [7], or analytical and simulation results to demonstrate the benefits on multi-layer restoration [8].

Control plane architectures for multi-layer networks is a topic analysed in different publications. These work compares three control plane architectures: UNI, Path Computation Element and Software Defined Network. The UNI architecture was demonstrated at [9], creating new IP links as well as MPLS services. The authors in [10] shows how multi-layer scenarios can be performed using a multi-layer Path Computation Element coordination. Finally, [11] presents the first SDN demonstration using the Netphony controller from Telefonica [12]. Let us highlight a very detailed survey about the Network Management in mult-layer scenarios.

This paper is structured as follows: Section II describes a reference network architecture, based on current network deployments. Section III presents the resilience schemes and the multi-layer alternatives. Section IV explains two advance multi-layer operations: Multi-layer Re-Route and Multi-Layer Shared Backup Router. Section V presents which are the alternatives to support multi-layer operations. Section VI explains which are the steps in an SDN architecture to support the multi-layer operations. Finally, Section VII concludes this paper.

ISBN 978-3-8007-4383-4

TABLE I. SERVICE UNAVAILABLE DURING A YEAR DEPENDING ON THE NUMBER OF NINES

Availability Target	99.9%	99.99%	99.999%	99.9999%
Hours without service in a year	525.6	52.56	5.256	0.5256

II. REFERENCE NETWORK

This section introduces a packet-optical reference network used in this work, based on an IP/MPLS over WSON architecture.

A. IP/MPLS Layer

The IP/MPLS core network of the operators is based on a hierarchical structure [9]. This network has three levels: (1) access level, (2) transit level and (3) interconnection level. The access level is the first aggregation level in the core network, where a big number of final users are connected (typically 50k to 100k). This access level is meant to handle small cities or districts in big cities. The goal of the transit level is to interconnect multiple access routers in different regions. Each region has a transit node (duplicated in case of using 1+1 protection scheme) which is connected to other regions by direct links between the transit routers allowing inter-region traffic. The transit level also aggregates traffic towards interconnection which is also known as "internet traffic". The interconnection level aggregates all operator traffic which needs to be driven to other operators or other countries. Fig. 1 presents an example of hierarchical core network. Depending on the operator's size, the network can have more than one transit level. For this work, a single transit level is assumed.

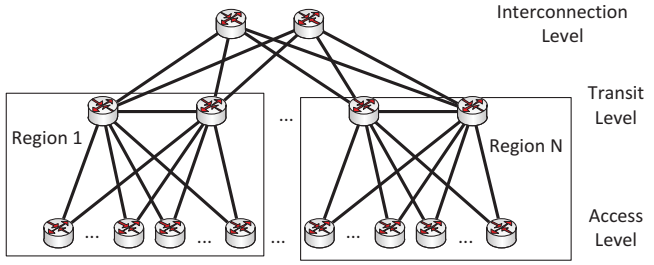


Fig. 1. Hierarchical IP/MPLS Network

Typically, operators present 1+1 protection in each network level and all of them are dimensioned to drive all the traffic of each region. In this structure, the traffic is routed thanks to inter-domain routing protocols and other techniques to make the switching more efficient (such as MPLS). The incoming traffic from the edges of the IP network (interconnection or access nodes) crosses the IP network through the transit nodes to reach the other edges (interconnection or access nodes). Each of the links between two routers (IP links) is set up using the different transport technologies (WSON in this study).

B. WSON Transport Network

Operators have deployed transport network with a GMPLS control plane and a WSON mesh to have a reconfigurable core network. A dynamic photonic mesh with a control plane allows the operator to perform multi-layer restoration operations. UNI interface is important for these multi-layer procedures, since the IP/MPLS layer can request to connections to the WSON mesh via this interface. Fig. 2 depicts an IP/MPLS over WSON topology. Each IP/MPLS router is connected to ROADMs or OXCs in the transport layer.

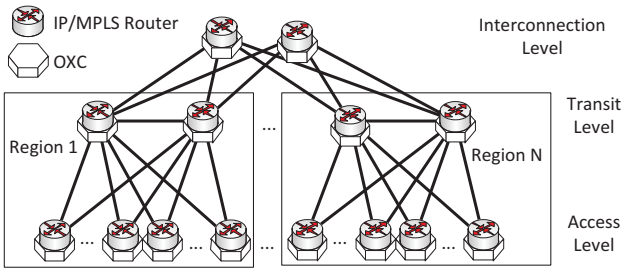


Fig. 2. Hierarchical IP/MPLS over WSON network

C. Hierarchical IP/MPLS Network

As can be seen in Fig. 2, each region can reach other region's transit routers by transport layer links. As each transit router is dimensioned to handle the traffic of its region, other regions transit routers may restore the connectivity when a double failure occurs in one region. This work studies the availability of this multi-layer restoration use case, where the access routers can connect to other regions and restore traffic in case of double failures.

III. SURVIVABILITY MECHANISMS

The survivability concept is the ability of systems to continue operating in case of failures independently of what causes these failures. Attending to communication networks, this concept applies to the capability of the network, in case of failures, to continue providing connectivity to the users. To measure how "survivable" a network is, the availability concept is defined as how long a user can access to the services provided by the network. Equation 1 presents the availability parameter calculation.

$$Availability = 1 - \frac{Time\ unaccessible}{Total\ operating\ time} \quad (1)$$

Based on the Service Level Agreements (SLAs), operators are bound to provide a specific level of availability to each of the provided services. Typically, the availability target is calculated as the ratio between the time in which the service is accessible and the total operating time and is defined in terms of nines e.g. 3 nines is equal to 99.9%. Depending on the type of service, the availability target is different. For instance, the connections of regular customers to the Internet can have enough availability

ISBN 978-3-8007-4383-4

with three or four nines, while critical services related with the factories of the future, e-health, or other industries in the field of commerce (e.g. financial institutions) require from five to six nines availability. It is important to notice that different penalties are applied if the operator does not comply with the agreed SLA, and, usually, in the case of critical services, these penalties are really high.

In order to ensure survivability, operators have three main options: (1) acquire robust equipment, (2) reduce the time to repair and (3) deploy survivability algorithms. If the operator deploys robust equipment, the chances that it fails are limited, thus also ensuring that fewer error-prone network configurations are carried out by the technicians. This defines the first important parameter in a survivability analysis, which is the mean time between failures (MTBF). Robust equipment increases the MTBF and, consequently, the network availability.

The second option is to repair the network quickly. However, in the case of five nines target, this is unrealizable with human intervention. As a consequence, automated control plane solutions (as the ones described in this paper) can be adopted to ease network operations and to promptly react to network failures. This defines the second important parameter in availability studies: the mean time to repair (MTTR), i.e., the time the operator needs to repair a failure.

As robust equipment fails and as high availability targets are becoming more and more relevant (especially considering the new wave of services that will be introduced by the deployment of 5G infrastructures), the operators need survivability methods ensuring that services are minimally impacted by any possible network failure, so that they can be (almost) continuously and consistently provided. To this account, the two main survivability mechanisms that are exploited are protection and restoration.

A. Protection

Protection includes a set of proactive mechanisms based on deploying more equipment than needed in order to have backup resources already reserved and immediately usable in case of failure. With protection, backup resources are totally disjoint from primary ones, allowing to recover the traffic when a failure appears on the primary resources. In order to ensure that all the traffic (or at least, the most critical services) can be protected, the network operator has to carefully carry out the network planning, by taking into account the required additional resources.

There are different protection schemes defined according to the way resources are used: 1+1 schemes consist on splitting the traffic between the resources (50% each); 1:1 mechanisms use all the resources in the primary path, while the backup path uses no resources; N:M schemes operate the same way as 1:1 schemes, but with M options to recover N resources. The different protection models are shown in Fig. 3. Backup resources in protection schemes are pre-defined by the operator to protect the nominal resources and they cannot be used by another network resource to recover traffic.

Protection can be carried out either at the IP/MPLS or at the optical layer. Both options are very effective in terms of the time needed to switch from the primary to the backup paths; such effectiveness is paid in terms of CAPEX, due to the additionally installed equipment.

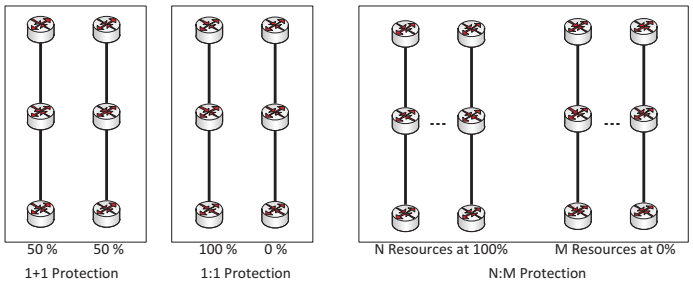


Fig. 3. Network protection schemes

B. Restoration

Restoration is a reactive mechanism in which a new connection is established after the failure happened. Therefore, it does not require any additional resource to be deployed. By doing so, restoration allows to reduce the cost of survivability with respect to protection, since the latter maintain some or all backup resources unused. However, due to the fact that the new path is dynamically computed and provisioned when the failure occurs, it may happen that backup resources are not available. Furthermore, due its reactive nature, restoration commonly needs more time to switch from the primary to the backup resources, thus introducing longer service disruption. In addition to that, the network behaviour is less predictable, making the network planning process more complex.

Like protection, restoration may be applied at either the IP or the optical layer. Optical restoration involves re-routing an existing optical connection around a failure in the optical layer. Due to intrinsic issue given by the technology (such as power equalization processes), optical restoration is relatively slow (in the order of seconds). In IP restoration, existing IP links are exploited to reroute the restored traffic. IP restoration is faster than optical one, but it requires that backup paths have sufficient capacity to support the re-routed traffic.

The two restoration strategies present trade-offs in the form of cost, responsiveness and offered capacity. However, the benefits of both mechanisms can be combined by managing resiliency at both layers.

IV. Multi-Layer Restoration

The idea behind multi-layer restoration is to extend the restoration mechanism to all the network layers involved in the restoration process. Indeed, two layers acting separately with their own resilience mechanisms may create resource inefficiencies. In some cases, failures may not be even recovered due to the lack of inter-layer communication and coordination.

The typical example of a failure that is not possible to recover with single layer survivability mechanisms is the failure of inter-layer connections. For instance, a failure on the fibre or the cards connected between two layers may start single layer actions, but in many cases the system is not able to recover from that failure. A solution to this type of failures is to use other resources in both layers to reach the same endpoints. However, as there is no multi-layer coordination, the network is unable to realize such possibility.

ISBN 978-3-8007-4383-4

Moreover, in order to increase the effectiveness of the resiliency process, multi-layer restoration can be applied by immediately reacting to a failure and recovering the traffic via IP layer restoration, and then apply optical layer restoration, thus establishing a new connection at the optical layer (ensuring the required capacity) in which the traffic is finally forwarded.

Multi-layer restoration operations are more resource efficient that restoration at just the IP or the optical layer. Multi-layer restoration involves coordinated operations across the layers to which is more efficient as compared to restoration operations at individual layers working to restore the same failure in an uncoordinated fashion. The authors in [14] shows how the optical restoration and multi-layer optimization can improve the CAPEX investment for network operators.

This section presents two advance multi-layer resilience operations: Multi-layer Re-Route and Multi-Layer Shared Backup Router.

A. Multi-layer Re-Route

Multi-layer restoration idea is an extension of the restoration mechanism where multiple layer resources are involved in the restoration process. Since protection schemes and restoration schemes are defined in scenarios where all nodes, links and path are in the same layer, the network operators use combination of protection and restoration mechanisms in each layer separately. Having more than one layer resources involved in the restoration process, a multi-layer path must be computed to recover failures that with single layer protection and restoration schemes may be unable to be restored.

The multi-layer reroute uses a common pool of additional resources in the form of extra transponders at each router to restore failures by creating new IP adjacencies. The additional transponders facilitate the restoration in case of failures that cannot be recovered via traditional mechanisms. This mechanism can reduce the number of ports for restoration as presented in [14].

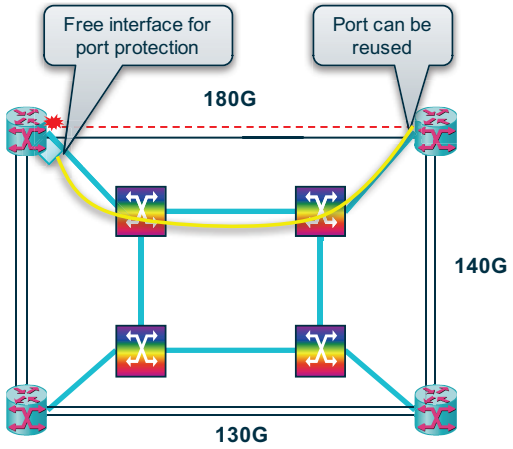


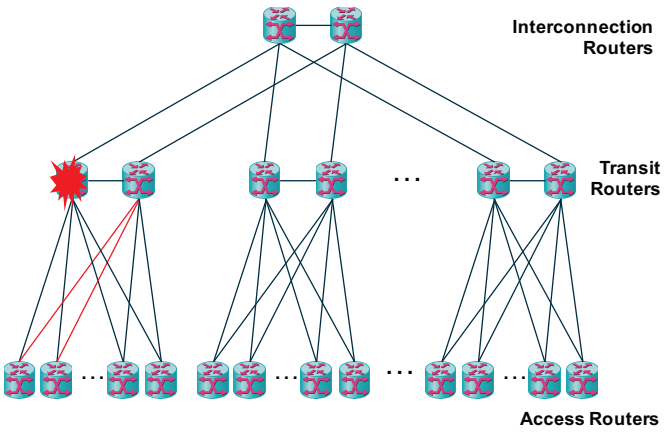
Fig. 4. Multi-layer Re-Route resilient mechanism

Consider the example in Fig. 4. In case of a fibre cut between 2 optical switches, the connection may be recovered via optical restoration only, but in case of a port/transponder failure, optical restoration cannot help recover from this failure. However, via the multi-layer reroute mechanism, the extra transponder available at the routers are used in case of a failure to create a new IP adjacency on-demand.

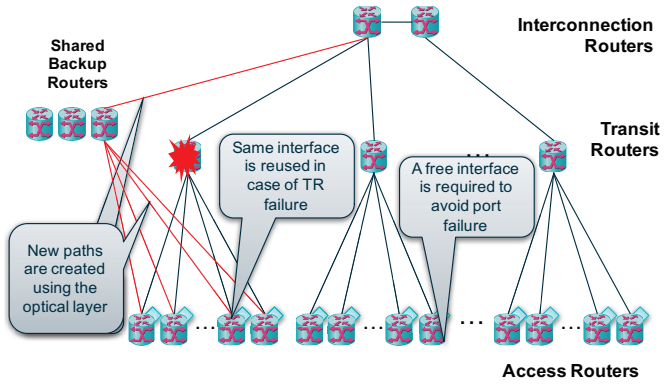
B. Multi-Layer Shared Backup Router

The multi-layer shared backup router (MLSBR) [8] is the natural extension to the multi-layer reroute mechanism to protect against router failures. In the case of hierarchical IP networks, typical deployments (Fig. 5a) involve duplication of routers at each level to protect against equipment failures. This technique compared with the common design of today's networks, where two IP planes are created in order to deal with node failure, reduces the investment in IP routers [15].

As seen with IP ports in the last mechanism, the MLSBR proposes to use a common shared pool of routers to protect against router failures. In case of a router failure, configuration from the failed router is copied onto a shared backup router, and connectivity to other routers is restored via multi-layer provisioning operations. Fig. 5b presents an example MLSBR restoration operation, where the network recovers from a failure of a transit router using a shared backup router. As shown in the figure, we see that IP ports on remote endpoints for the failed links can be re-used to create connections to the shared backup router, further reducing the dimensioning cost associated with this operation.



(a) Dual-plane Protection



(b) MLSBR

Fig. 5. Resilience schemes in a hierarchical topology.

ISBN 978-3-8007-4383-4

C. Drawbacks of Multi-Layer Restoration Mechanisms

It is evident that multi-layer restoration mechanisms can significantly reduce redundant equipment costs when dimensioning a network capable of recovering from equipment failures. However, the operations involved in multi-layer restoration are usually hindered by the large provisioning timescales associated with operations like light-path setup and router configurations. As a result, these operations can potentially only be employed for protecting best-effort traffic or used in conjunction with protection schemes to support recoveries from multiple failures in the network.

V. SDN and Control Plane Architectures

This section presents three approaches to support the multi-layer advance mechanisms.

A. UNI Control Plane

The control plane has three main interfaces the Internal-Network to Network Interface (I-NNI), the External NNI (E-NNI) and the User to Network Interfaces (UNI). The I-NNI is the interface between two elements of the same technology in the same domain (Fig. 6). The E-NNI is the interface between two elements of the same technology in the two different domains. Finally, The UNI is the control plane interface from the routers to the optical equipment, as shown in Fig. 6.

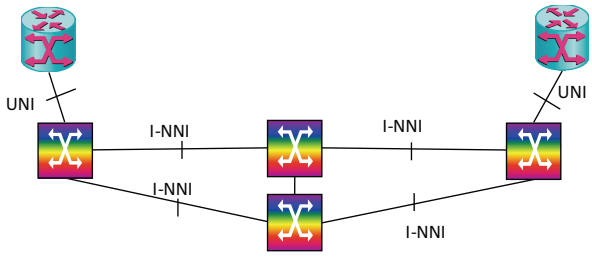


Fig. 6. Multi-layer scenario based on UNI

There are different models for the control plane to be used in this environment with UNI. The "peer" model and "overlay" model are the two main approaches, but current operator's networks typically use "overlay" because of the lack of multi-vendor interoperability between layers. The "overlay" model for multi-layer networks works as a client/server model. The IP/MPLS upper layer can be considered as the client layer, while the Transport layer works as the server layer. In this context, the client layer requests a connection to the transport layer through the UNI.

UNI works with RSVP-TE (and the extensions to GMPLS) for resource reservation, and OSPF-TE to notify the new adjacencies in the client layer after the resource reservation in the transport layer. The router can request the creation of a lightpath using RSVP.

B. Path Computation Element

The original definition of the PCE was stateless in the sense that a network element queries the PCE to obtain the path for a connection. A stateful PCE knows which are the connections on the network and can make decisions based on this information. An active stateful PCE goes a step further and it is a path computation entity, which can maintain the sessions for the LSPs and can even create LSPs in the network.

With this approach, the network operator enters in the PCE and it can set-up a connection on the network via a PCInitate message which is sent to the network elements. The lightpath is signaled using RSVP with the constraints sent by the PCE in the PCInitiate message. Once the message is RSVP Resv message is received, the network element sends a PCReport to the PCE. The PCE can learn the topology using different protocols like an IGP (OSPF, ISIS) or BGP-LS.

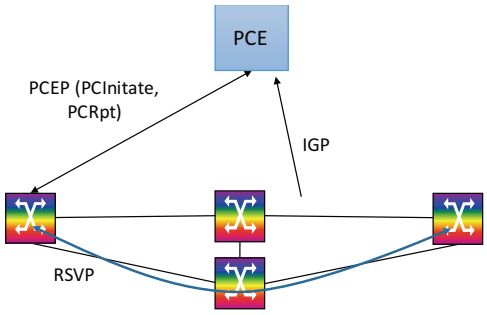


Fig. 7. PCE control plane architecture

C. Software-Defined Networks

Software Define Network (SDN) concept is based on the idea of decoupling the control and data plane. This concept is inherent to the optical networks as the signaling as done always via an out of band channel. The NMS was the controller, which configures the optical equipment and there was not standard interface from the NMS to the devices. The utilization of open and standard interfaces to enable interoperability is the first advantage of this architecture.

The SDN architecture is based on hierarchical entities, which configure each technological domain (MW, Optical or IP) and have an orchestrator on top to enable the E2E provisioning of services and an interface with the OSS. Fig. 8 shows the SDN architecture.

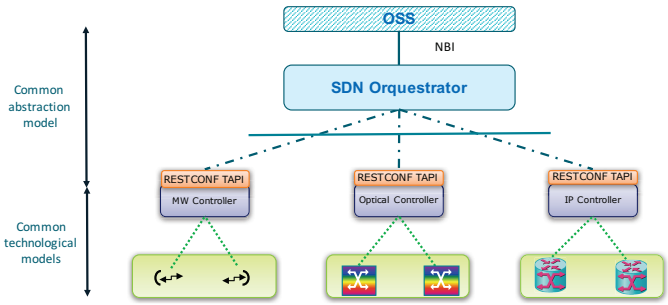


Fig. 8. SDN control plane architecture

D. Comparison

Even though the three previous architectures can enable multi-layer operations, there are some differences between them.

- **UNI control plane** enables the request of connections from the routers to the optical devices. However, this approach only has a local view of the network. This means that it could start a multi-layer restoration process without the whole network visibility. Moreover, this architecture does not

ISBN 978-3-8007-4383-4

consider the configuration of the routers, which requires some configuration after a multi-layer process. This can be solved via NMS provisioning.

- **Path Computation Element** is a technology that has the central intelligence to provision optimal network configuration and create operations that will consider the network on an end-to-end basis. This approach does not cover the router set-up, even though there are some extensions to map a template into an LSP configuration. Such templates must be configured beforehand in the router via an NMS. Moreover, this architecture lacks of an abstract interface to get/provide configuration to the OSS.
- **Software Defined Networks** can use the benefits of the PCE architecture and enhance it with the utilization of an IP controller with YANG models for the router configuration. Moreover, the SDN architecture is based on the utilization of REST/APIs which can easily interface the OSS of the network operators. These APIs can be abstracted or detailed depending on the use cases and the hierarchy of the controller.

VI. Multi-layer Operations Using SDN Approach

Following network operations are selected, because they are multi-layer. This means that both layers the IP and the optical must be coordinated during the process. There are situations like failures or congestion, that are solved in a single layer. For instance, a failure in a ROADM is solved by means of restoration or protection using GMPLS. We can manage this situation from a SDN controller, but network operators already have GMPLS networks to solve these issues.

A. IP Link Provisioning

The provisioning of an IP link between two routers is the basic multi-layer operation. We assume that the routers are connected via an optical network composed of ROADMs. New IP links are deployed in the network every year to increase the network capacity. Once the equipment is installed in the network and operator creates the request to create a new IP link between two locations, the SDN orchestrator receives the notification from the OSS and requests the lower layer to set-up an optical connection. This process can be done using the PCE architecture sending an PCInitiate message to the head-end node or triggering the process from the vendor NMS.

Once the optical layer is configured, the IP controller must configure the routers with the proper IP configuration. Depending on the IGP and services that can be instantiated in this port, the IP SDN controller must send the configuration using Netconf/YANG models. The models can be proprietary of the vendor or it can follow IETF or OpenConfig models [16].

B. Multi-layer Re-Route

In order to perform multi-layer re-route operation, let us remark that there must be a floating port for backup purposes. The SDN IP controller must send an alarm notifying the SDN orchestrator that there was a failure on an IP port. Based on this trigger, the SDN orchestrator must set-up a new IP link between the original port at the destination router and the floating port at the router with the failed interface. To follow this procedure, the SDN optical controller can use the PCE messages to create the lightpath, or the NMS in legacy scenarios without an optical SDN controller.

After the optical layer configuration, the IP SDN controller copies the configuration of the failed interface in the floating interface. Depending on the router position, it can be as easy as setting up the routing protocols like in a P router or the services if the failure happens on an PE router. As stated in the previous network operation, the preferred mechanism is Netconf/YANG using standard models like in IETF or OpenConfig.

C. Multi-layer Shared Backup Router

The latest operation is the Multi-layer Shared Backup Router. This operation consists on replacing a router in the network by another router located remotely after a failure. The first step is that the IP SDN controller notifies the SDN orchestrator that there was a failure in a router. Once the failure is detected, the SDN orchestrator sets up all the optical connections required to reach the new router and remove the previous ones if required.

To do so, the Optical SDN controller can use the PCE or NMS to carry out such operation. The IP SDN controller must copy the router configuration in the new backup router in order to enable the same configurations. Therefore, there must be a copy of the router configuration to deal with this situation. This process can be easier in P routers, but it can be very complex in PE routers with several access ports.

VII. Conclusions

This paper reviews the planning process taking into account resilience schemes not only IP and optical networks, but also multi-layer. Moreover, it presents an evolutionary view on the control plane and SDN paradigms that enable the support of multi-layer schemes in real networks.

Acknowledgment

The work on this paper is partially funded by the European Commission within the H2020 Research and Innovation program, ACINO project, Grant Number 645127, www.acino.eu.

References

[1] J.E. Gabeiras, V. López, J. Aracil, J.P. Fernández Palacios, C. García Argos, Ó. González de Dios, F.J. Jiménez Chico and J.A. Hernández: “Is Multi-layer Networking Feasible?”, in Elsevier Journal on Optical Switching and Networking, April 2009, Vol. 6, Issue 2, Pages 129-140.

[2] Sidnei de Oliveira, et al.: “Economic Analysis for Transport Network Evolution”, in the 8th Conference on Telecom, Internet and Media Techno-Economics (CTTE), June 2009.

[3] O. Gonzalez, J. Jimenez, J. Fernandez-Palacios, S. Oliveira, and M. Callejo, "CAPEX Savings by a Scalable IP Offloading Approach," in Optical Fiber Communication Conference (OFC), paper OTuR5, March 2011.

[4] P. Demeester et all., “Resilience in Multilayer Networks”, IEEE Communication Magazine, Vol. 37, no. 8, pp. 70-76, August 1999.

[5] K. Lee, E. Modiano, H.W. Lee, “Cross-Layer Survivability in WDM-Based Networks”, IEEE/ACM Transactions on Networking, vol.19, no.4, pp.1000-1013, Aug. 2011.

[6] M. Ruiz, O. Pedrola, L. Velasco, D. Careglio, J. Fernández-Palacios, and G. Junyent, “Survivable IP/MPLS-Over-WSON Multilayer Network Optimization”, IEEE/OSA Journal of Optical Communications and Networking, Vol. 3, pp. 629-640, 2011.

[7] Eiji Oki, Kohei Shiomoto and Daisaku Shimazaki, "Dynamic Multilayer Routing Schemes in GMPLS-Based IP+Optical Networks," IEEE Communications Magazine, pp. 108-144, January 2005.

[8] F. Muñoz, V. López, Ó. González de Dios and J. P. Fernández-Palacios: Multi-layer Restoration in Hierarchical IP/MPLS over WSON Networks, in Networks and Optical Communications (NOC), Jun 2012.

[9] F. Muñoz, R. Muñoz, J. Rodríguez, V. López, O. González de Dios and J.P. Fernández-Palacios, "End-to-end service provisioning across MPLS and IP/WDM domains", in the International Workshop on Network Management Innovations co-located with the 4th IEEE Technical CoSponsored International Conference on Smart Communications in Network Technologies, Jun 2013.

[10] O. Gonzalez de Dios, V. López, M. Cuaresma, F. Muñoz, M. Chamania and A. Jukan: Coordinated Computation and Setup of Multi-layer Paths via Inter-layer PCE Communication: Standards, Interoperability and Deployment, in IEEE Communications Magazine, December 2013, Vol. 51, pp. 144 - 154.

[11] A. Aguado, V. López, J. Marhuenda, Ó. González de Dios and J. P. Fernández-Palacios: ABNO: a feasible SDN approach for multi-vendor IP and optical networks , in Journal of Optical Communications and Networking, February 2015, Vol. 7, Iss. 2, pp. A356–A362.

[12] Netphony Suite, https://github.com/telefonicaid/netphony-abno/wiki

[13] A. Martínez, M. Yannuzzi, V. Lopez, D. López, W. Ramírez, X. Masip-Bruin, R. Serral-Gracià, M. Maciejewski, J. Altmann: Network Management Challenges and Trends in Multi-Layer and Multi-Vendor Settings for Carrier-Grade Networks, in IEEE Communications Surveys and Tutorials, June 2014, Issue 99.

[14] O. Gerstel, C. Filsfils, T. Telkamp, M. Gunkel, M. Horneffer, V. Lopez and A. Mayoral: Multi-Layer Capacity Planning for IP-Optical Networks, in IEEE Communications Magazine Feature Topic "Advances in Network Planning", January 2014, Vol. 52, Issue. 1, pp. 44-51.

[15] A. Mayoral, V. López O. Gerstel, E. Palkopoulou, J. P. Fernández-Palacios and Ó. González de Dios: Minimizing resource protection in IP over WDM networks: Multi-layer Shared Backup Router , in Proc. Optical Fiber Conference (OFC), M3B.1, Mar 2014.

[16] OpenConfig project, http://www.openconfig.net/

ISBN 978-3-8007-4383-4