Bridging the Interoperability Gap Between the Internet and Optical Network Management Systems

M. Yannuzzi*, X. Masip-Bruin*, O. González de Dios†, C. García Argos†, M. Maciejewski‡, and J. Altmann§
*Advanced Network Architectures Lab (CRAAX), Technical University of Catalonia (UPC), Spain
†Telefónica I+D, Spain
‡ADVA Optical Networking, Poland
§Seoul National University, Korea

***Abstract*—Despite the efforts made towards the convergence of packet and circuit switched technologies, the isolation between the Internet and the optical Network Management Systems (NMSs) remains unsolved. Today, carriers have nothing but manual means to coordinate the provisioning between the routers and L1 switches, and much less to communicate and coordinate policy rules, or failures between the IP networks and Ethernet/optical networks. In this paper, we outline the strengths of an easy-to-deploy solution, which can overcome the current separation between the IP and the optical NMSs. The solution consists of an adapter (a middle-box), especially designed to provide a simple, reliable, and automated communication channel between the two management layers. The adapter that we conceive will enable automated interoperability between the IP and the optical NMSs, in support of coordinated actions such as: i) IP service provisioning; ii) IP/MPLS offloading; and iii) coordinated self-healing. We contend that our approach not only eliminates the need for large scale integration into a single multi-layer management system, but also bridges the communication gap between two management ecosystems that are currently isolated.**

I. Introduction

Over the last years, the research and industrial communities have devoted significant efforts toward the convergence of IP and optical networks. Despite this, the practical segmentation of the IP router infrastructure from the optical transport network has not only led to the carriers organizational separation, but also to a fragmentation of technical competencies and networking solutions. At present, the IP and optical transport networks are two separate ecosystems within a telecom carrier, up to the point that the management systems and tools used for the administration of these networks have become completely isolated. In this context, even simple tasks involving operations in both the IP and the optical transport networks require multiple human-assisted configurations. This not only creates management expenditures and significant delays, but is also error prone and hinders the integration of emergent multi-layer management sub-systems, such as the Path Computation Element (PCE) [1].

To address these issues, different initiatives have tried to develop a unified multi-layer Network Management System (NMS), capable of managing Network Elements (NE) in the IP as well as in the optical layer. Although there are ongoing efforts in this direction (see e.g., [2]), as yet this integration has not succeeded in practice, and it remains to be seen if a fully-integrated solution would be adopted by telecom carriers.

In light of this, we propose a pragmatic and easy-to-deploy solution aimed at enabling communication and coordinated actions between the two management planes, without requiring the fusion of NMSs into a unified solution. More specifically, we outline the advantages of developing a communication adapter between the IP and the optical NMSs, targeted at facilitating specific coordinated multi-layer operations such as automated provisioning of IP services over transport circuits and multi-layer self-healing operations. Figure 1 illustrates the interoperability envisioned with the adapter. Consider a carrier network, which typically has both IP and transport network infrastructures, with the former composed of IP/MPLS routers, and the latter of optical and possibly carrier-grade Ethernet switches. The transport network is assumed to be managed by one or more Transport Net-

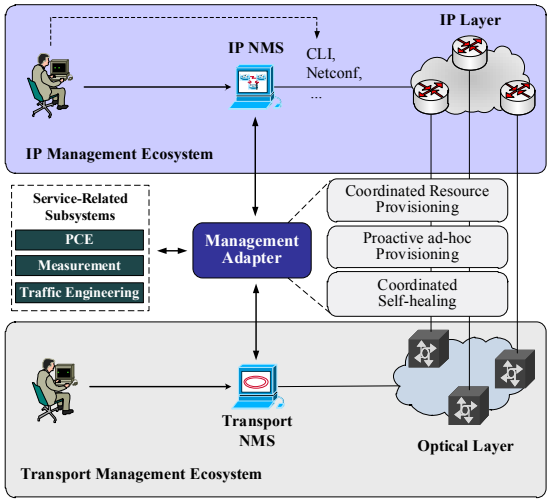

Fig. 1. Interoperability envisioned with the management adapter.

work Management Systems (TNMSs), which are typically provided by the vendor of the transport equipment, such as ADVA's Optical Networking FSP Service Manager [3]. The IP network devices, on the other hand, are typically managed by one or more IP NMSs, such as HP's OpenView [4], or are configured directly by network administrators using the Command Line Interface (CLI) [5] or NETCONF [6].

In this scenario, the management adapter shall be able to communicate with the TNMSs and the IP NMSs (e.g., using web services over a standardized interface like the Multi-Technology Operations System Interface (MTOSI) [7]). In case that the carrier lacks a proper IP NMS solution or relies on a set of proprietary tools, the administrators of the IP network could interact directly with the adapter, issuing high-level requests which will be interpreted and adapted to the appropriate semantics and syntax of the corresponding TNMS.

Under these assumptions, which are representative of current carrier networks, this paper presents how the management adapter can facilitate automated multi-layer operations for three well-defined use cases which entail automated provisioning and configurations in both networks and encompass:

1) The automated provisioning of IP links and services demanding resources from the optical layer.
2) IP traffic offloading over optical bypass triggered by pre-configured policies.
3) Coordinated multi-layer self-healing actions.

A management adapter that could provide the functionality listed above is being prototyped in the framework of the FP7 European project ONE [8]. This adapter does not intend to replace the functions of current IP and transport NMSs, but rather to offer an interface capable of interpreting requests and coordinating actions between these management systems. We emphasize that our approach does not seek the integration of various NMSs, but to foster the evolution of automated interoperability between the Internet and a broad category of emerging carrier-grade NMSs, including those designed for carrier-grade Ethernet standards and optical systems. As shown in Fig. 1, the adapter will also facilitate the interactions with external management sub-systems, such as a PCE, a measurement system, or a policy-based Traffic Engineering (TE) system.

II. Coordinated operation using the Management Adapter

The proposed management adapter will interact with the IP NMS and the TNMS and will coordinate the automated configuration of NEs in both networks. Since neither the IP-NMS nor the TNMS inherently identifies the other network, the management adapter must communicate with other external subsystems as shown in Fig. 1. A simple example in case here is the fact that neither the IPNMS nor the TNMS currently contains inter-layer interconnectivity information which can be easily mapped to the other network. Currently, this information is stored in a separate database, and as a result even a simple IP link provisioning requires multiple manual interactions to retrieve the necessary information to match a transport circuit to its IP interfaces. We assume the presence of three primary control sub-systems to provide: 1) multi-layer topology information, 2) network measurement information, and 3) traffic engineering information. We now present use cases to expose the ability of the management adapter to facilitate multi-layer operations.

A. Use case 1: IP Service Provisioning

This use case focuses on eliminating the need for manual interactions between the IP and the transport layer departments by automating the provisioning process. The role of the adapter in this case is to interpret the carrier's IP (link/service) requests and convert them into comprehensible and unambiguous transport layer resource requests, which are required to provision the desired IP service in an automated fashion. This use case could be split into two primary scenarios, where the adapter is used to automate the provisioning of: i) a new IP link; ii) an IP service which requires additional resources from the transport layer (e.g., a new VPN).

1) Automated IP Link Provisioning: As shown at the top of Fig. 2, an administrator of the IP network could request a new IP link between a pair of routers in the IP network. In order to automate the provisioning process, the adapter will first check for free interfaces at the IP routers in question and will identify the corresponding transport network switches (1). If interfaces are available, the adapter will request the TNMS to reserve a circuit between the corresponding transport network end-points (2). Upon successful reservation, the adapter will configure data-plane mappings at the inter-layer interconnects, and will then configure the interfaces at the routers to set the IP addresses and routing rules as defined by the operator to initialize the new IP link (3).

2) Automated Multi-layer IP Service Provisioning: In this commonly occurring scenario (see the bottom of Fig. 2), the provisioning of an IP service (e.g. VPNs or IPTV) requires additional capacity installation in the IP network. To this end, the administrator of the IP network could request the adapter to initiate the required inter-layer interactions to provision the service request. Assuming that a planning tool was previously used to determine the location and capacity for the IP links required to accommodate the service (step (1) at the bottom of Fig. 2), upon receiving the request, the adapter will contact a PCE to compute the paths, and, if the computation is successful, the adapter will then initiate the IP link provisioning processes (2) (as described in the previous scenario) and will then instruct the IP NMS to initiate service provisioning along the computed paths (3).

Note that both the IP link and service provisioning processes can be used in combination to facilitate more complex operations. For example, a coordinated sequence of IP link and service provisioning processes can be used

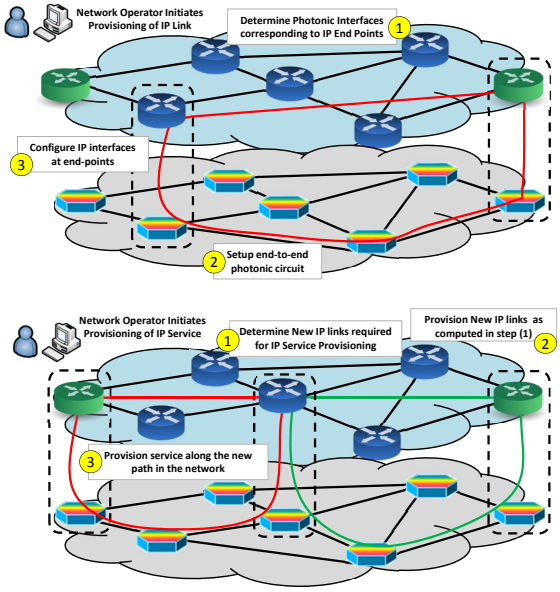

Fig. 2. (Top) Automated provisioning of a new IP link; (Bottom) Automated provisioning of a new multi-layer IP service.

to execute a network re-planning operation for an IP network, where the new IP links are first established and services then migrated before old links are decommissioned.

B. Use case 2: IP/MPLS Offloading

While the previous use case describes the coordination of actions initiated by the operator, in this use case, we focus on the capability of the adapter to automatically drive multi-layer operations based on policies defined by the network operator. We use the example of "IP offloading" [9], to show the ability of the adapter to facilitate automated policy-driven processes in a multi-layer network. In the IP offloading paradigm, the network responds to the increase in traffic of a particular service or segment in the IP network by offloading IP traffic onto optical circuits, thereby reducing the load on intermediate IP routers and links. The decision process driving IP offloading is complex and is constrained by a set of rules to reduce costs (OpEx) while ensuring network stability. The basic rules governing IP offloading are:

- A circuit may be established to offload individual application or aggregate service traffic across overloaded network segments.
- Routing rules must be configured at the ingress and egress of the established circuit to ensure that only specific traffic (as determined by the offloading logic) is offloaded onto the circuit, and that routing of other flows remains unaffected.
- Creation of new connections and enabling new interfaces should not pose a threat to the adjacency scalability in terms of possible flooding upon element failures.
- The logic used to calculate bypasses should account for costs incurred both in the IP/MPLS and transport network layers to optimize overall cost.

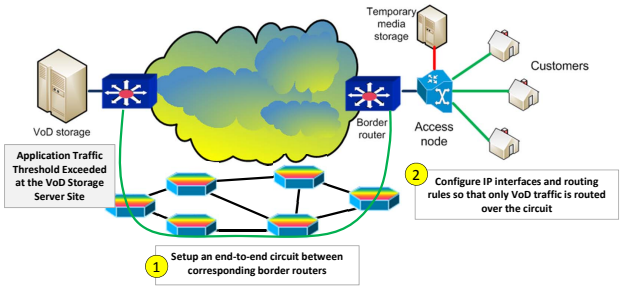

Fig. 3. IP offloading use case (VoD scenario).

The offloading operation should initiate automatically when a critical traffic load is reached in the network. Thereafter, using available network information such as IP link loads and the multi-layer topology information, the offloading logic must determine: a) the application/service traffic to be offloaded; b) the routers/links which should be bypassed; and c) the required bandwidth for the circuit(s) to support the offloaded traffic. We exemplify this use case through two possible scenarios: i) application-based traffic; and ii) aggregated IP traffic.

1) Application-based traffic offloading: Consider the scenario for a commercial Video-on-Demand (VoD) application shown in Figure 3, where on-demand video is served by the VoD server across the core network up to the access network. The characteristics of VoD traffic make it a good candidate for offloading end-to-end across the core network. Thus, when the VoD traffic increases beyond a pre-defined threshold, the adapter could coordinate an offloading process using an optical circuit. In this setting, the adapter could be notified by an external entity if the application exceeds a critical load threshold (e.g., a monitoring system assessing the application load). Once notified, the adapter will first identify the edge routers associated with the application end-points and will check if these end-points have available IP interfaces. If available, the adapter will initiate the IP link provisioning process as described in the previous scenario. To ensure that the introduction of the new link does not lead to routing changes, the adapter will assign the interfaces IP addresses from a private address pool outside the OSPF/ISIS routing area, and will configure routing rules on the edge routers to offload VoD traffic onto the newly established link. In this way, only application specific traffic is offloaded onto the bypass and IP routing in the core remains unaffected.

2) Aggregated IP Traffic Offloading: In this scenario, no single application/service may justify the cost for being offloaded over an optical circuit, but traffic aggregated over multiple services/applications can better justify the cost for deploying a new optical circuit. Given the high traffic volumes in the core network, the offloading operation will typically offload aggregate MPLS tunnels. In this scenario, and similarly to the previous one, the adapter will first compute and configure a new IP link to be used for offloading inside the core network. However, instead of using IP routing rules which are difficulty to

match in the core, the adapter will modify the MPLS forwarding entries at the ingress and the egress routers of the established optical circuits, in order to offload the aggregate MPLS tunnels.

C. Use case 3: Coordinated Self-healing

The lack of coordination in current IP/MPLS and optical networks means that protection resources are typically duplicated in both the IP as well as the transport network, and protection timescales are preset with optical network protection triggered in $< 50\ ms$, while IP protection is triggered in the order of 10s of seconds. In this use case, we discuss how the proposed adapter can support coordination to recover from simple and complex network failures. We contend that coordinated self-healing processes can help to reduce the Capital Expenditures (CapEx) as well as the operational costs of carriers, while improving the network availability.

1) Coordinated Recovery Process: In this scenario, we present the capability of the adapter to coordinate recovery in a multi-layer environment. We first consider a network setting where optical circuits employ a shared path/segment protection variant, and therefore may not always be protected from a failure in the network. The IP network is also designed with smaller headroom (peak load link utilization $\approx$ 60%). In case of a failure in the optical network, the adapter is notified by the TNMS, and waits for the recovery mechanism in the optical layer to finish recovery. In case the circuit cannot be recovered, the adapter then instructs the IP NMS to initiate recovery. Coordination of recovery mechanisms could bring significant savings both in time and capacity. Finally, if a critical service cannot be restored using existing available capacity, the adapter can initiate the service provisioning process to add additional capacity to the IP network.

2) Recovery from Unplanned Double Failures: These failures are becoming less rare events in large telecom carriers, mainly due to the amount and heterogeneity of devices present in their networks. In light of this, some carriers are considering alternatives, such as increasing the redundancy beyond the classical 1+1 protection. In this scenario, we show how the adapter can help recovery from unplanned double failures in the network without increasing the redundancy in protection. As shown in Fig. 4, the failure of routers $T1_a$ and $T1_b$ leads to a disconnection of AC_{11} and AC_{12} from the Internet. As recovery in the transport layer cannot recover from these router failures, and recovery in the IP layer is not possible, in this scenario, the adapter will compute new possible adjacencies ($T2_a$ in Fig. 4) and will setup IP links in order to reroute Internet service traffic from AC_{11}.

III. Conclusion

In this paper, we have outlined the strengths and potential application of a management adapter, which can be a true enabler to foster the evolution of automated interactions between the Internet and a broad category

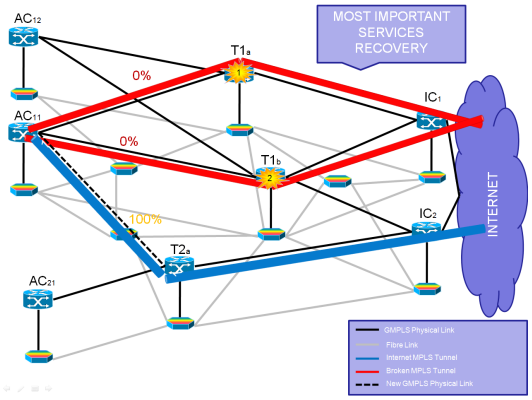

Fig. 4. Self-Healing use case (double failure scenario).

of emerging carrier-grade network management systems, including those designed for carrier-grade Ethernet standards, optical switching, as well as third party systems such as the PCE [1]. It is worth noting that, as many of the operations described in this paper are potentially intrusive, the adapter may be configured to suggest a possible solution, and wait for approval from the network operator before initiating configuration and provisioning tasks. The adapter along with the functionality described in this paper is being prototyped in the framework of the FP7 European project ONE [8]. The ONE adapter will use an ontology mapper as a basic functional block, for interpreting requests and dealing with the semantics necessary to unambiguously automate management actions and properly drive the configuration of devices in both in the IP and optical layers.

Acknowledgements

The authors would like to thank Mohit Chamania and Admela Jukan for the support received. This work was supported in part by the European Commission through the ONE project in the FP7 Program, contract number INFSO-ICT-258300. UPC authors also acknowledge the support received by Spanish Ministry of Science and Innovation under contract TEC2009-07041, and by the Catalan Research Council (CIRIT) under contract 2009 SGR1508.

References

[1] A. Farrel, J. P. Vasseur, and J. Ash, "A Path Computation Element (PCE)-Based Architecture," IETF RFC 4655, August 2006.
[2] CYAN, Multi-Layer Management System, http://cyaninc.com/.
[3] ADVA Optical Networking, FSP Service Manager, http://www.advaoptical.com/.
[4] HP OpenView, http://www.hp.com/.
[5] Cisco Systems "Using the Cisco IOS Command-Line Interface," April 2010.
[6] R. Enns, "NETCONF Configuration Protocol," IETF RFC 4741, December 2006.
[7] Multi-Technology Operations System Interface (MTOSI), release 2.0, Tele-Management Forum, http://www.tmforum.org.
[8] FP7 Project ONE (INFSO-ICT-258300): "Towards Automated Interactions between the Internet and the Carrier-Grade Management Ecosystems," http://www.ict-one.eu/.
[9] M. Chamania, A. Jukan, O. González de Dios, J. Jiménez Chico, "Offloading Excess IP Traffic with Optical Bypass–A Simple Capacity Upgrade, or More?" ONTC PRISM Newsletter, vol. 1, no. 3, Aug. 2010.