

Convergence of IP-Based and Optical Transport Networks

Artur Lason¹, Antonio Manzalini², Giorgos Chatziliadis³, Lampros Raptis³,
Didier Colle⁴, Piet Demeester⁴, Mario Pickavet⁴, Monika Jaeger⁵

¹ AGH – Department of Telecommunications,
Poland

² CSELT - Centro Studi e Laboratori Telecomunicazioni
Italy

³ NTUA - National Technical University of Athens,
Greece

⁴ Ghent University – IMEC
Belgium

⁵ T-Nova Deutsche Telekom Innovationsgesellschaft mbH
Germany

lason@kt.agh.edu.pl
antonio.manzalini@cselt.it
lraptis@telecom.ntua.gr
didier.colle@intec.rug.ac.be
monika.jaeger@telekom.de

Abstract. Today Network and Service Providers are aware of the increasing data traffic volumes and as such they are strategically moving investigations toward a single integrated voice and data infrastructure. In this context IP is gaining the role of the integration layer for multiple services. Nevertheless incumbent NSPs that build a multi-service IP network are going to need connectivity to its preexisting legacy networks (e.g. ATM, SONET, SDH). This reason motivates the introduction of a client-independent Optical Transport Network (OTN) as a missing link to guarantee a smooth evolution from legacy networks to a data-centric OTN. The scope of this paper is to give some guidelines about the definition of functionality and architectures of a multi-layers infrastructure supporting the transport of data and circuit-based services. Particularly, the identification of the different service requirements, as well as the understanding of the allowed degradation, provide a picture of the needed survivability mechanism of IP over OTN scenarios.

1 Introduction

The emerging of new application services and the exponential increasing of data traffic (mainly Internet) pose the problem of the evolution of Network Service Providers' infrastructures to face such trends.

If on one side existing TDM-based infrastructure of incumbent NSPs should evolve to support efficiently the exponential growth of data traffic, on the other side New Comers should deploy cost-effective infrastructures to gain rapidly market

shares. As a matter of fact many new NSPs are entering metropolitan areas with single integrated voice and data infrastructure where IP is gaining the role of integration layer for multiple services. This is a first strong driver.

Another main driver is the introduction of the DWDM technology. WDM techniques, which were originally introduced around '95 to increase transport capacity, have laid the foundations for implementing network functionality directly in the optical layer. This is what is known as Optical Transport Network [6].

Thanks to these two main drivers (increasing of IP traffic and introduction of DWDM), the convergence of IP-based and Optical Transport Networks is becoming one of most strategic areas for NSP.

2 Multi-layers Optical Transport Networks

Historically NSPs have used several layers to build their networks: adopting for example IP routers over ATM switches over PDH or SDH network elements. Figure 1 reports a typical layered architecture based on legacy systems.

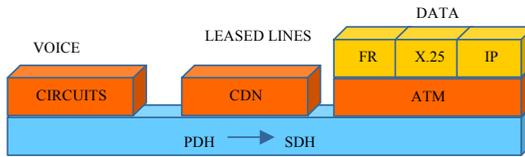


Fig.1 Example of legacy current scenario

Nevertheless even when deploying a new IP-based infrastructure, there is the need to guarantee the connectivity to preexisting legacy networks belonging to the same or to another NSP. SONET/SDH framings and rates seem to be the most common standard to support connectivity to preexisting infrastructures.

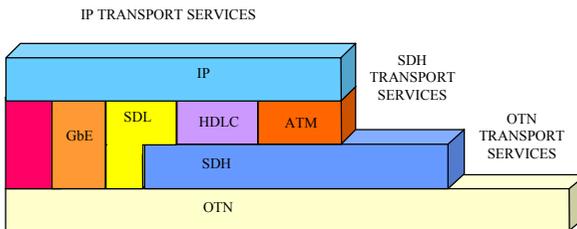


Fig.2 Introduction of the OTN as a server layer network

Furthermore DWDM point-to-point systems have been already introduced in backbone networks to increase transport capacity. Recently DWDM is a technology mature to deploy also networking functionality by means of Optical Network Elements (ONE) such as OADM and OXC. Again the Optical Transport Network (OTN) represents another layer added to the stack (Figure 2). Thanks to DWDM technology, the OTN can provide a large amount of raw bandwidth supporting the

delivery of big volumes of IP traffic. Furthermore it can deliver other data and circuit-based services in a more cost-effective way.

In this context the optical internetwork is defined as a multi-layers transport network composed by two or more connected OTN or client networks connected to one or more OTN. In Figure 3 and Figure 4 respectively show examples of reference scenario and architecture of an optical internetwork.

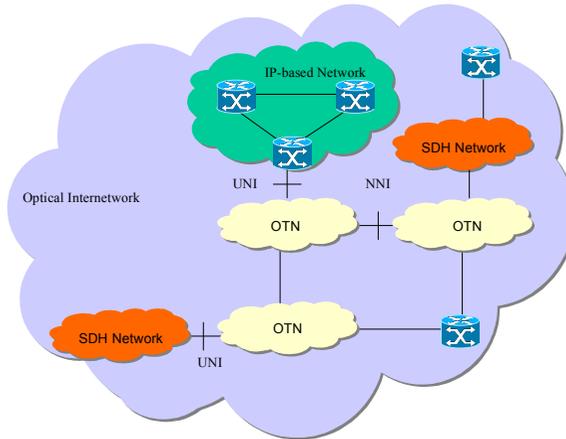


Fig. 3 Reference scenario of an optical internetwork

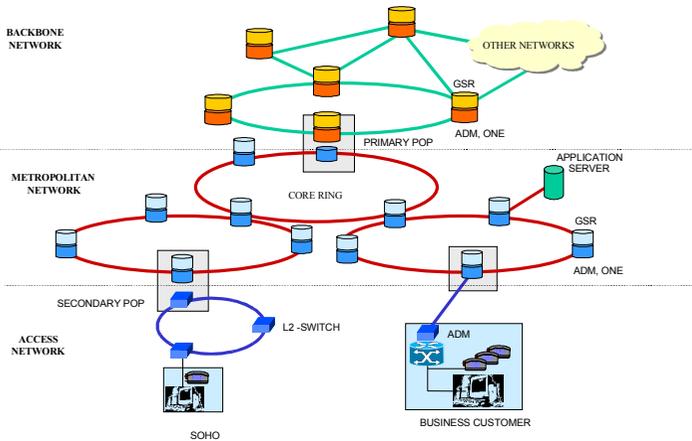


Fig. 4 Architecture of an optical internetwork

3 Application Services

The design of the architecture for the different network segments (access, metropolitan and backbone) of the infrastructure is strictly related to the requirements

of the services to be provided to the customers. The technical requirements of the envisaged application services will impact the choice of the enabling technologies and viceversa the infrastructure capability of supporting certain transport services will impact the providing of new application services.

Applications could be classified into two general categories based on the relative technical requirements, namely Streaming and Elastic Services.

The first category of applications is based on information sent to the customer in a streaming way: the source continuously produces data stream during the end-user session. The source is bursty, mostly due to the adaptive nature of video coding scheme. The application classified into the Streaming Service is sensitive or highly sensitive to the delay introduced by the transport network (Table 1). The Elastic group of applications are characterized as a much less delay sensitive. Data bit rate variation of this group is much higher in comparison to the applications of Streaming Service.

A proposal of assignment of sample applications to the Streaming and Elastic Services is presented in Table 1. The application delay sensitivity has been indicated with the grade ranging from 0 up to 5. The highest grade means that the application is highly delay sensitive, whereas 0 means that the delay in the transport network can be neglected. The same rating has been used for the need for protection.

The need for protection for given applications may vary with the type of end-user. For example the transport of digital video signal between movies server and end-user and between TV studios is characterized by different protection requirements. The most important conclusion from applications analysis is that the Streaming Service generally requires to be supported with protection mechanism of the future transport network. The data bit rate variation of Elastic Service is very high. This effect is observed because Elastic Service applications are in most cases based on information retrieval. Such characteristics of Elastic Service are reflected also in different requirements for protection. Implementation of restoration algorithms in an integrated IP over OTN network would likely be suitable to assure the integrity of Elastic Service.

Each of the applications has also been analyzed with regard to its expected importance in the short and mid-term perspective. It was assumed that the short-term prognosis means the three years perspective and mid-term forecast refers to the application significance in next 10 years. The importance of the application is given in the scale from -5 to +5. The rate of 0 means no changes in the applications importance. The negative ratings is adequate to the forecasted degradation of the application importance. The aggregate rating of the prognosis is higher than zero due to the confidence in continued development of network services. The permanent development of new services should be taken into account in studies on integrated transport services. Data presented in Table 1 suggest that increasing impact of Streaming Services on the integrated transport networks will still be observed in the future.

Table 1 Overview of application and their relationship to the application services

	Application	Bit rate	Bit rate variation	Delay sensitivity	Need for protection	Importance	
						Short-term	Mid-term
Streaming Service	POTS	64 Kbps 32 Kbps	const	5	5	-1	-3
	VoIP	8 Kbps 32 Kbps	const	5	5	3	5
	Video-telephony	256Kbps 1920Kbps	high	5	5	2	3
	Video- conf.	256 Kbps at least	high	5	5	3	4
	Tele-working	64 Kbps 2 Mbps	very high	5	4	3	5
	TV Broadcast	2 Mbps 8 Mbps	high	4	4	1	0
	Distance Learning	64 Kbps 2 Mbps	very high	5	5	2	4
	MoD	750Kbps 4 Mbps	high	4	3	1	3
Elastic Service	News on Demand	64 Kbps	very high	2	2	2	4
	Internet Access	64 Kbps 2 Mbps	very high	1	2	5	5
	TV Listing	64 Kbps	very high	2	2	1	2
	Tele-shopping	64 Kbps 2 Mbps	very high	2	2	5	5

4 Transport Network Services

Network transport services are those functions and utilities supporting connectivity, communications and control required by applications operating across the network. The definition of these network transport services will determine the flexibility of an enabling infrastructure to support current and unforeseen new network applications.

4.1 SDH-Based Transport Services

In principle, an optical internetwork could be able to provide SDH-Section transport services and SDH-VC transport services.

For the SDH-Section transport services the OTN acts as a virtual fiber connection.

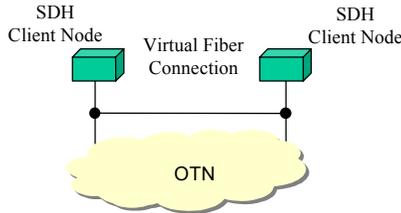


Fig. 5 SDH-Section fiber connection

For SDH-VC transport services, the optical internetwork acts as a virtual container link. For example in order to achieve payload bandwidths larger than the basic VC-4 container, the principle of concatenation has been defined. Concatenation is a procedure whereby a multiplicity of Virtual Containers is associated one with another with the result that their combined capacity can be used as a single container across which bit sequence integrity is maintained [1].

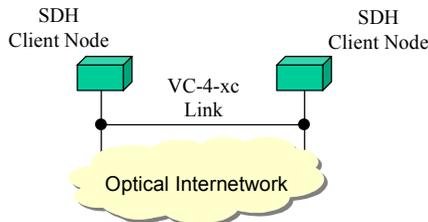


Fig. 6 Example of SDH VC transport service

In [2] SDH-based transport services include PLR, STE and LTE circuits. Particularly they are SONET/SDH rate and framed point-to-point circuit between two UNIs.

A PLR-Circuit is a circuit that preserves all SONET overhead bytes between clients. The SONET/SDH signal may be concatenated or channelized but cannot be SONET/SDH TDM demultiplexed or multiplexed within the optical internetwork.

An STE-Circuit preserves all SONET/SDH line overhead bytes between clients but is not required to preserve the section overhead bytes. The SONET/SDH signal may be concatenated or channelized but cannot be SONET/SDH TDM demultiplexed or multiplexed within the optical internetwork.

An LTE-Circuit preserves the SONET/SDH payload, but is not required to preserve the section or line overhead bytes. The SONET/SDH signal may be concatenated or channelized and may be SONET/SDH TDM demultiplexed or multiplexed within the optical internetwork to allow the subrate circuits to be individually routed, or to allow multiple LTE-Circuits to be multiplexed within the network to better utilize a network link. Thus, an LTE-Circuit implies timing and synchronization requirements not required in PLR-Circuits or STE-Circuits.

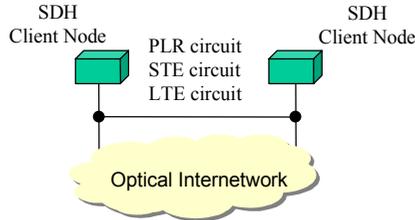


Fig. 7 Example SDH-based transport services

4.2 IP-Based Transport Services

The Internet protocols consist of a suite of communication protocols of which the two best known are the Transmission Control Protocol (TCP) and Internet Protocol (IP).

The IP is a network-layer (Layer 3) protocol that contains addressing information and some control information that enables packets to be routed. IP has two primary responsibilities: providing connectionless, best-effort delivery of datagrams; providing fragmentation and reassembly of datagrams to support data links with different maximum-transmission unit size.

In general, an IP Transport Service could be defined as the capability of an IP-based network to deliver datagram payloads from a Service Access Point to anyone of the interfaces with the IP-address for that SAP. In this sense, an IP Transport Service could be intended as an added value service to the simple data transmission. If the end-user always acts via an application protocol, the Service Access Point of a NSP could be either at the network-layer, or at the transport-layer, via intermediate protocols (e.g. TCP, UDP) or at the application layer via application protocols (FTP, HTTP, SNMP, SMTP, etc).

An IP Transport Service could be qualified by a set of parameters (terms of the Service Level Agreement) such as: access mode, rate of service availability in hours per year, multiple service quality classes, routing configuration indicating the belonging to one or more IP-based VPN, multicasting, throughput management and traffic shaping, security issues, provisioning time is the time required to set-up the service.

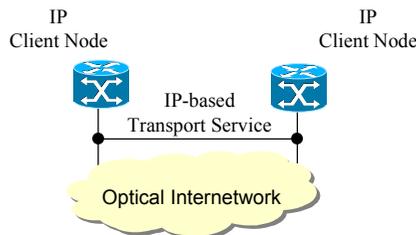


Fig. 8 Example of IP-based transport service

4.3 Optical Transport Services

Three main kinds of Optical Transport Services can be identified:

- Leased OCh service
- Leased Wavelength
- Leased Dark Fiber

Bandwidth management of leased OCh is a further service option considered as to the bandwidth management of leased OChs. This special service might be offered when the inverse multiplexing of OTN, e.g., OCh virtual concatenation is available.

Different potential ways to set-up OCh services are envisaged:

- a permanent set up from the network management system by means of network management protocols;
- a soft permanent set up from the management system, which uses network generated signalling and routing protocols to establish connections;
- a dynamic set up by the customer on demand using signalling and routing protocols (switched optical channel).

Regarding leased wavelength, this transport service is offered to clients equipped with coloured line terminals and in case of Leased Dark Fiber who is providing this service doesn't control the degree of use of the fiber itself.

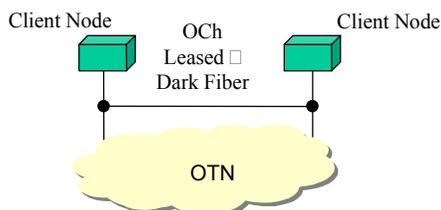


Fig. 9 Example of Optical transport service

5 Resilience of IP over OTN

IP is very dynamic, adaptable and self-healing, whereas OTN has superior link-level protection and restoration capabilities, but is static and slow to provision on a network scale. This prevents the optical layer from effectively addressing the rapid changes in the IP topology.

It is important to provide survivability at multiple layers, in order to recover any service in all expected failure conditions and to combine positive features of the different recovery schemes. In such a case, a proper coordination of the recovery schemes at multiple levels is necessary. A sequential strategy could be implemented with a hold-off timer or a recovery token signal from one layer to the other.

In order to define an efficient, flexible and fast resilience strategy, a clear understanding of the current protection mechanisms available in the different network technologies is needed.

5.1 Restoration in IP Networks

Internet, considered by many as the integrated service layer, was not designed with fast restoration/protection mechanism in mind. IP can recover from any defect in the network, but the time needed is in the order of seconds, making IP unsuitable for streaming applications. It takes IP some time to detect a failure, propagate the information to other routers and then each router compute a new path.

However, there are some techniques that can be used to make IP more efficient. For example equal cost multi-path forwarding (ECMF) enables routers in case of a failure to utilise more than one path for packets that have the same destination. The selection can be done in a per-packet round-robin fashion or on a per-flow basis. Moreover, in order to minimise convergence time of the routing algorithms, the IP network can be segmented into multiple domains. Hierarchical link-state routing protocols like OSPF and IS-IS allow such partitioning, restricting the flooding of the topologic changes in smaller areas of the network.

5.2 Recovery in the OTN

On the other hand, protection/restoration mechanisms for the OTN have already been defined. Many ideas of the SDH protection has been shifted and adopted by the OTN, thus OTN has capabilities similar to the SDH achieving fast protection/restoration within 50 msec. The flexibility of these mechanisms is of vital importance since the disruption of a fiber carrying Terabits of traffic affects thousand of connection. Emerging technologies like DPT, MPLS and MPLambdaS can play a major role in-between the IP and the OTN, allowing a smooth interworking.

5.3 Survivability in MPLS networks

Multiprotocol Label Switching (MPLS) binds packets to a route based on labels. Protection of traffic at the MPLS layer is desirable because MPLS:

- has faster responses in failures compared to IP(layer 3).
- allows the direct integration of IP and WDM layers. The IP packets can be transferred directly over a WDM channel without the need of intermediate layers like SONET/SDH.
- allows finer granularity of protection.
- allows the differentiation of the protection based on the traffic type.

MPLS fast protection switching is similar to the ATM, occupying resources along a back-up path only when needed, combining the advantages of protection (fast recovery) and restoration (capacity efficiency). In addition, label stacking makes it possible to provide a single back-up Label Switched Path (LSP) to protect multiple LSPs, although there are some problems concerning the consistency of the labels inside the back-up LSP. Different protection mechanisms can be identified [4].

Residing at the higher layer, recovery at MPLS level may incorporate more service specific details. For example, along the alternate path low priority traffic (both working and rerouted) will be preempted first (instead of preempting all existing working traffic along the alternate path or not allowing traffic to be rerouted over the alternate path). Also a finer granularity of protected objects can be obtained at this higher layer.

5.4 Deploying DPT Rings for Fast Network Recovery

Dynamic Packet Transport (DPT) is a L2 ring technology, proposed by CISCO Systems. DPT resides between the IP and the OTN and this is why it is mentioned here. WaRP is a protocol that enables the provisioning, routing, protection, and restoration of virtual wavelength paths (VWP). DPT delivers 50 ms restoration timeframes in a mesh network topology, improved fiber utilization via 30% spare capacity reduction, provides rapid end-to-end provisioning on the order of seconds

5.5 Recovery in MPLambdaS Networks

The Multiprotocol Lambda Switching (MPLambdaS) can be considered as the glue between the IP layer and the optical layer. The control plane of OXC can be the same as that of MPLS-capable routers. The recovery in MPLambdaS networks is performed by dynamically setting up back-up optical connections. The issue of dynamic connection set-up is an area of intense research in different standardisation bodies (OIF, IETF, etc). When LSPs are passed to the optical layer, no explicit encapsulation is needed because each wavelength channel represents a LSP label and the encapsulation is done implicitly. Moreover, new fiber-restoration schemes which aggregates (stacks) all the wavelengths of one link into a larger optical LSP.

5.6 Multilayer Network Recovery

The previous paragraphs discussed recovery techniques for each technology independent from each other. However, an IP over OTN network is a typical example of a multi-layer network. Indeed, there is a need to deploy recovery techniques in multiple layers.

Only from a failure-coverage point of view, we can raise following arguments. Only providing recovery in the OTN, would make it impossible to recover from a router failure in an acceptable short timeframe. On the other hand, only relying on the IP restoration capabilities, would make it impossible to restore an affected optical transport service (e.g., a leased OCh service), which have been discussed in section 4.3.

Thus, it is necessary to provide recovery at both IP and OTN level. However, the IP restoration capabilities are not sufficient for all types of traffic, and therefore more advanced techniques as in MPLS or DPT may be required.

5.7 Coordination of Multiple Single Layer Recovery Schemes

As discussed in the previous paragraph, it is recommended to deploy a recovery mechanism in multiple layers. Of course, one has to assure that they work properly together.

A first solution is the most simple and straightforward one. The recovery schemes in the different layers are running in parallel and independent from each other. This may work in some cases, but at least it is inefficient. Although it may be sufficient that the traffic is restored by a single mechanism, both the IP (or MPLS/DPT) and

OTN mechanism are doing their job and thus requiring twice spare resources. Even more, it may be possibly that in some cases (e.g., in severe failure conditions) the OTN has simply to restore the connectivity of its client layer, before this client layer would be able to restore any traffic. For instance, Figure 10 shows a double failure, which requires that MPLS switches over to the backup LSP and that OTN restores the link along the backup LSP. In such a case it is necessary that MPLS does not give up before the OTN restored its backup LSP.

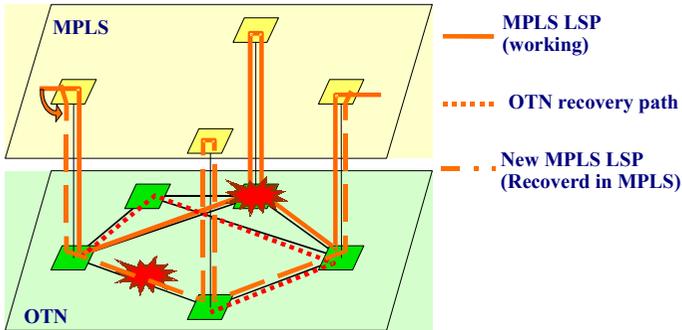


Fig. 10 link + node failure

To solve these problems, one can deploy a sequential strategy: one recovery scheme starts trying to perform the recovery, and only if it fails, the control is handed over to the next recovery scheme. The most intuitive approach, is a bottom-up approach, where the lowest layer (in our case the OTN) tries to restore the traffic. However, the interesting features of e.g. MPLS or DPT may promote a top-down approach, where the recovery starts at the highest layer.

A first way to implement such a sequential approach is to apply a hold-off timer: when a recovery mechanism starts its attempts to restore the traffic, a hold-off timer is launched and only when this timer goes off, the next recovery scheme starts to recover the remaining affected traffic. Although this solution is rather simple to implement, such a timer may introduce a significant delay.

To avoid such an additional delay, one could hand-over the control to the next layer by sending a recovery token signal to that layer. Although it does not introduce a delay, this solution requires a modification of the interface (and the corresponding standards) between those layers.

5.8 Integrating IP and OTN

The fact that the control plane of a MPLambdaS network is similar to the one of a MPLS network, opens up the opportunity to integrate both control planes into a single one. Such an integrated control plane makes it possible to deploy a recovery scheme, covering both the optical and electrical MPLS network, which avoids interworking issues, being discussed in the previous paragraph. Even more, since the control plane now has a full-view of the network (covering both electrical and optical level), new

opportunities are raised to take more intelligent recovery actions. However, one has to make a trade-off between algorithmic complexity (required for more intelligent recovery actions) and recovery speed.

6 Conclusions

The increasing data traffic and the evolution of the WDM technology are driving the convergence of IP-based and Optical Transport Networks. Particularly, the introduction of the OTN will guarantee a smooth evolution from legacy (e.g. SDH, ATM) to a data-oriented architectures, that initially could even coexist in the same infrastructure.

As such, if the first evolutionary step for NSPs is the introduction of the OTN [6], supporting the transport of legacy clients, the next one seems to be the development of interworking and interlayer communications between optical network elements (OADM and OXC) with IP Routers in order to deploy a data-centric OTN.

In a multi-layers scenario it is important to provide survivability at multiple layers, in order to recover any service in all expected failure conditions and to combine positive features of the different recovery schemes. In such a case, a proper coordination of the recovery schemes at multiple levels is necessary. A sequential strategy could be implemented with a hold-off timer or a recovery token signal from one layer to the other. The identification of the different service requirements, as well as the understanding of the allowed degradation of services will give a clear picture of the needed survivability mechanism.

References

1. ITU-T Rec. G.707;
2. OIF-99-161;
3. ITU-T Rec. G.709;
4. Makam et al, work in progress, internet-draft October 1999: Protection/Restoration of MPLS networks. <http://search.ietf.org/internet-drafts/draft-makam-mpls-protection-00.txt>
5. C. Metz in IEEE Internet Computing, March-April 2000: "IP restoration and protection"
6. ITU-T Rec. G.872.

Acknowledgments

This paper has been prepared in the framework of the IST project LION – Layers Interworking in Optical Networks. The Authors wish to thank all project Participants.