NTNU
Norwegian University of
Science and Technology

Multi Protocol Label Switching Transport Profile (MPLS-TP) in OpMiGua hybrid network

Christos Katsavos

Master of Telematics - Communication Networks and
Networked Services (2 year)
June 2010
Submission date: Steinar Bjørnstad, ITEM
Supervisor: Harald Øverby, ITEM
Co-supervisor:

Norwegian University of Science and Technology
Department of Telematics

Problem Description

While MPLS is a control-plane driven approach, MPLS-TP adds the functionality of management and monitoring. The Optical Migration Capable Networks with Service Guarantees (OpMiGua) concept (http://www.opmigua.com) has the main objective of combining the best properties from both circuit and packet switched networks into a hybrid solution. In the project, the student shall study how MPLS-TP may be applied in an OpMiGua network. MPLS-TP may be especially suitable for setting up the circuits in the hybrid network. The packet part may also be suited by MPLS-TP. A network-scenario may be proposed, and suitability and functions on MPLS-TP shall be studied in the context of the scenario. This thesis shall evaluate the way that MPLS-TP may be applied in an Opmigua network.

Assignment given: 27. January 2010
Supervisor: Steinar Bjørnstad, ITEM

To my lovely parents George & Helen
and to the unique person,
Danai.

Preface

This Master Thesis is the written result of my studies carried out at the Norwegian University of Science and Technology (NTNU) in Trondheim, Norway. This Thesis is part of the requirements to achieve the MSc in Telematics (Communication Networks and Networked Services) at NTNU.

I would like to thank my professor, Steinar Bjørnstad and my supervisor, Harald Øverby for giving the opportunity to carry out an interesting research and their valuable remarks and ideas to obtain the final result of the project.

Special thanks are given to Stefano Vitelli, Alessandra Palumbo and Francesco Puleio for having shared with me two amazing years in Trondheim.

Trondheim, June 2010

Christos Katsavos

Abstract

This thesis presents the combination of MPLS-TP protocol with an integrated hybrid network, the Opmigua network. It is presented that the MPLS-TP protocol is applicable and follows all the requirements to be compatible with an Opmigua network. Different network scenarios, combining packet and circuit switching properties with MPLS-TP labels, are presented. At the beginning of this thesis, are provided the characteristics and requirements of MPLS-TP protocol which the standardization of this is on going. Furthermore, it is explained how the MPLS-TP management and the forwarding plane work. Some references are also given not only to OAM mechanisms, but also to control plane that the MPLS-TP uses.

We use both, global and local significance MPLS-TP labels for distinguishing the Guaranteed Service Traffic (GST) packets from Statistical Multiplexing (SM) packets. Using this method, we have concluded some results, as it concerns GST and SM traffic. GST packets take a global significance label value until to reach the destination node. On the other hand, SM packets take local significance labels for each path into an Opmigua network which follow Optical Packet Switch (OPS) networks.

We have proposed a new method for differentiation of packets from low to high priority using extension headers of Internet Protocol v6 either Destination Options Header (DOH) or MPLS-TP as an extension header. The result that we have derived is high and low priority packets are differentiated at ingress Opmigua network which GST packets take global significance MPLS-TP label following Optical Cross Connect (OXC) network and SM packets change per each Label Switched Path (LSP) local significance MPLS-TP labels until to reach the destination.

Finally, two MPLS-TP path protection schemes, facility bypass and restoration using detours were combined with Opmigua network to provide failures for both, Guaranteed Service Traffic (GST) packets and Statistical Multiplexing (SM) packets.

Contents

List of Figures

List of Abbreviations

(APS)	*Automatic Protection Switching*
(ARC)	*Alarm Reporting Control*
(ATM)	*Asynchronous Transfer Mode*
(BGP)	*Boarder Gateway Protocol*
(CapEx)	*Capital Expenditures*
(CCh)	*Communication Channel*
(CE)	*Client Edge*
(CoS)	*Class of Service*
(CP)	*Control Plane*
(DCN)	*Data Communication Network*
(DM)	*Delay Measurement*
(DOH)	*Destination Options header*
(DWDM)	*Dense Wavelength Division Multiplexing*
(ECMP)	*Equal Cost Multi - Point*
(EMA)	*Element Management Architecture*
(EMF)	*Equipment Management Function*
(EML)	*Element Management Level*
(EMS)	*Element Management System*
(FCAPS)	*Fault, Configuration, Accounting, Performance and Security*
(FEC)	*Forwarding Equivalent Class*
(FIFO)	*First In First Out*
(G-ACh)	*Generic Associated Channel*

(G-MPLS)	*Generalized MPLS*
(GST)	*Guaranteed Service Traffic*
(IETF)	*Internet Engineering Task Force*
(IP)	*Internet Protocol*
(IPv6)	*Internet Protocol version 6*
(ITU-T)	*International Telecommunication Union*
(LA)	*Local Alarms*
(LCT)	*Local Craft Terminal*
(LDP)	*Label Distribution Protocol*
(LER)	*Label Edge Router*
(LER)	*Label Edge Router*
(LM)	*Loss Measurement*
(LME)	*LSP Maintenance Entity*
(LOC)	*Loss of Continuity Defect*
(LSP)	*Label Switched Path*
(LSR)	*Label Switching Router*
(MAF)	*Management Application Function*
(MCF)	*Message Communication Function*
(MCCh)	*Management Communication Channel*
(ME)	*Maintenance Entity*
(MEF)	*Message Element Function*
(MEG)	*Maintenance Entity Group*
(MEP)	*Maintenance Entity Point*
(MI)	*Management Information*
(MIB)	*Management Information Base*

(MIP)	*Maintenance Entity Group Intermediate Point*
(MP)	*Management Plane*
(MP)	*Management Point*
(MPLS)	*Multi-Protocol Label Switching*
(MPLS-TP)	*Multi-Protocol Label Switching - Transport Profile*
(MS-PW)	*Multi-Segment Pseudo-Wire*
(NE)	*Network Element*
(NEF)	*Network Element Function*
(NEM)	*Network Element Management*
(NGN)	*Next Generation Network*
(NG-SDH)	*Next Generation Synchronous Digital Hierarchy*
(NMS)	*Network Management System*
(OAM)	*Operation Administration and Maintenance*
(OCS)	*Optical Circuit Switch*
(ODU)	*Optical Data Unit*
(OMS)	*Optical Multiplex Section*
(OpEx)	*Operational Expenses*
(OpMiGua)	*Optical Packet-Switched Migration-Capable Networks with service Guarantees*
(OPS)	*Optical Packet Switch*
(OPU)	*Optical Channel Payload Unit*
(OS)	*Operation System*
(OTH)	*Optical Transport Hierarchy*
(OTN)	*Optical Transport Network*
(OTS)	*Optical Transport Section*

(OTU)	*Optical Transport Unit*
(OXC)	*Optical Cross Connect*
(P2MP)	*Point to Multipoint*
(PBC)	*Polarization Beam Combiner*
(PBS)	*Polarization Beam Splitter*
(PC)	*Polarization Combiner*
(PE)	*Provider Edge*
(PolTDM)	*Polarization Time Devision Multiplexing*
(PS)	*Polarization Separator*
(PHP)	*Penultimate Hop Popping*
(PME)	*PW Maintenance Entity*
(PPSTME)	*Path Segment Tunnel Monitoring ME*
(PSTME)	*PST Maintenance Entity*
(PTCME)	*MS-PW Tandem Connection Maintenance Entity*
(PVC)	*Permanent Virtual Circuit*
(PW)	*Pseudo-Wire*
(PW-PDU)	*Pseudo-Wire Protocol Data Unit*
(PWE3)	*Pseudo Wire Emulation Edge to Edge*
(QoS)	*Quality of Service*
(RSVP)	*Resource Reservation Protocol*
(SCN)	*Signaling Communication Network*
(SCCh)	*Signaling Communication Channel*
(SDH)	*Synchronous Digital Hierarchy*
(SM)	*Statistical Multiplexing*
(SME)	*Section Maintenance Entity*

(SONET)	*Synchronous Optical Network*
(SOP)	*State of Polarization*
(S-PE)	*Switching Provider Edge*
(SS-PW)	*Single Segment Pseudo-Wire*
(TE)	*Traffic Engineering*
(T-MPLS)	*Transport MPLS*
(VCI)	*Virtual Circuit Identifier*
(VPI)	*Virtual Path Identifier*
(VPN)	*Virtual Private Network*
(WDM)	*Wavelength Division Multiplexing*
(WRON)	*Wavelength Routed Optical Network*

Chapter 1

Introduction

1.1 Thesis Introduction

These days, as it has been described by IETF and ITU-T, the data traffic is growing more than ten times the rate of voice traffic. The estimation for the future is that data will count 90% of all traffic carried by networks. Because of this rapid change, the obsolete concept of telephone networks that were used to carry data, will be replaced by the data networks concept. Another reason is that circuit switched networks are less cost effective as it concerns the network utilization than IP-based network such as Internet services which they need both, data and voice transmission simultaneously. For these reasons, the telecommunication industry has started to use IP as the bearer of traffic. This scenario, has many consequences as it concerns best effort services. IP based networks have not be able to guarantee reliable packet delivery with low delay for real time services like voice communication. Traditional systems based on SDH/SONET platforms provide low bandwidth network services but high speed transmission speed services. For example, circuit - switched transport network services provide fixed bandwidth 64 Kbps, 1.5 Mbps, 2 Mbps, 150 Mbps etc [1]. From the carriers point of view, there is a desire for reduction of operational expenses (OpEx) and capital expenditures (CapEx) in their networks [1].

Because of the massive number of users and traffic volume, the Internet has grown rapidly and the operational efforts were increased. For this reason, a new more reliable and at the same time cost effective technology has grown [2]. Cisco has developed a technique with tags between layer 2 and layer 3 in the IP stack hierarchy which was named Multi-protocol Label Switching (MPLS). MPLS is considered as a connection -oriented packet transport network technology. Many carriers desire to converge their next - generation core networks to MPLS for their core networks deployment. Organizations like IETF and ITU-T will play key roles in the future development of the MPLS technology [3].

First was Cisco systems that has done a large effort for standardization of a simplified version of MPLS for transport networks [1]. Then, the International Telecommunication Union (ITU-T) in cooperation with the Internet Engineering Task Force (IETF) have become an effort for standardization of a new transport profile for the Multi-protocol Label Switching (MPLS) technology. This technology, should provide the basis for the next generation packet transport network [4]. The main idea of this was the extension of MPLS Operation Administration and Maintenance (OAM) tools to be applied in existing transport network topologies such as Optical Transport Network

(OTN) and SONET/SDH. It also adopts all of the supporting Quality of Service (QoS) and other mechanisms that already defined within the standards.

1.2 Thesis Description and Research Goals

While MPLS is a control-plane driven approach, MPLS-TP adds the functionality of management and monitoring. The “Optical Migration Capable Networks with Service Guarantees” (Opmigua) concept (http://www.Opmigua.com) has the main objective of combining the best properties from both circuit and packet switched networks into an optical hybrid solution. In the project, the student shall study how MPLS-TP may be applied in an Opmigua network. MPLS-TP may be especially suitable for setting up the circuits in the hybrid network. The packet part may also be suited by MPLS-TP.

A network-scenario may be proposed, and suitability and functions on MPLS-TP shall be studied in the context of the scenario. This thesis shall evaluate the way that MPLS-TP may be applied in an Opmigua network.

The main goals of this research are defined as follows:

- Functionalities and mechanisms of MPLS, (Transport) T-MPLS and MPLS-TP (Transport Profile) protocols will be compared.

- MPLS architectural considerations and requirements for a transport profile.

- Presentation of a network scenario will be introduced. Further analysis shall be based on MPLS-TP header and how it is possible to setup Guaranteed Service Traffic (GST) paths and Statistical Multiplexing paths (SM) in Opmigua hybrid network. Another consideration is the identification of each packet into the data forwarding paths.

1.3 Organization of the report

The main study is compromised by five parts.

Initially, in chapter 2, a theoretical point of view for this research project is presented. More specifically, this chapter presents the background for the Opmigua project, MPLS protocol, T-MPLS protocol and finally MPLS-TP protocol.

After the presentation of the Opmigua project and protocols in the previous chapter, the main focus on chapter 3 is the MPLS-TP protocol. It explains the characteristics of management, control, forwarding plane and OAM tool set which is currently under definition at the IETF. A comparison between these protocols is also presented.

Chapter 4, is based on a network scenario and it provides the configuration of GST and SM paths with MPLS-TP protocol. Another aspect that is provided in this chapter is the data forwarding analysis and the identification of each packet inside the network. Furthermore, a combination of two MPLS-TP protection schemes with an Opmigua network is provided.

Chapter 5 provides a summary of proposals and finally, the conclusion and future work are listed in chapter 6.

Chapter 2

Background

This chapter contains the background information needed on the technologies affected in this thesis. It is divided in four subsections. The first one, gives an introduction to the Opmigua project. Furthermore, the second part, provides a basic understanding of MPLS architecture. Part three presents the background of T-MPLS protocol and finally, part four gives the introduction of MPLS-TP which is the main idea of this thesis.

2.1 Opmigua Project Background

A future transport network should be able to serve all types of applications. It must be able to handle the most demanding services with respect to Quality of Service (QoS). There are many applications which are intolerant to delay when using buffering for smoothing of time jitter. Retransmissions of lost packets introduce extra delay and jitter with result these applications like tele - visualizations may not tolerate packet loss [5].

Integrated hybrid networks has been investigated in several projects in the international research community and one these is the Opmigua project. The main aspect of Opmigua project is how to provide service guarantees for demanding applications in a packet switched networks. Hybrid optical circuit and packet switched were introduced to combine the high resource utilization of Optical Packet Switch (OPS) networks with the low processing requirements of Optical Circuit Switch (OCS) networks. Opmigua architecture, has the ability to divide traffic into two service classes. The first is packet switched Statistically Multiplexed (SM) service class and the second one is circuit switched Guaranteed Service Traffic class (GST). As it concerns the Statistical Multiplexing (SM) traffic, is subject to packet loss due to contention of packets inside the packet switch. There is also a small processing delay at each node. From the other side, packets of the GST class follow lightpaths in the Wavelength Routed Optical Network (WRON) and possess a circuit switched quality of service (QoS). GST class guarantees no jitter and no packet loss [6]. Furthermore, for the GST traffic, the Opmigua ensures transparency, high security and high reliability. Because the GST traffic bypasses the packet switches, a reduction of the required size of the packet switch may be possible if transit traffic is handled as GST traffic. Guaranteed service is suitable also for grid applications and for broadcast distribution.

2.1.1 Opmigua Network Layer

Opmigua concept consists of nodes. Each node consists of one optical packet switch (OPS) handling SM traffic and one Optical Cross Connect (OXC) handling high priority GST traffic. The high priority traffic follows G-MPLS Label Switched Paths (LSP) in the Opmigua network. The setup of LSPs is implemented like this: One output wavelength may only receive traffic from one single input wavelength. This technique eliminates the contention between high priority packets. For this reason, the delivery of packets is guaranteed also in the absence of hardware failures. Figure 2-1 presents an Opmigua node as was subdivided into four functional parts. The first part consists of Polarization Separator (PS) at the input node, second part, the Optical Packet Switch (OPS), third part is the Optical Cross Connect (OXC) and finally, the fourth part consists of Polarization Combiners (PC) at the switch output [6][13].

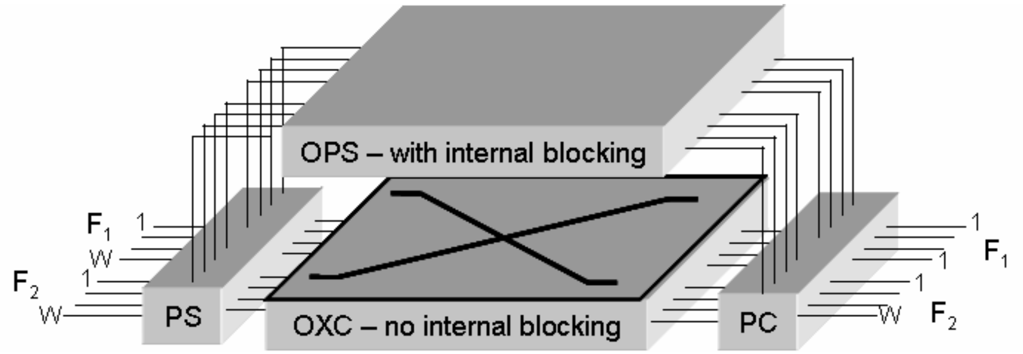


Figure 2-1. An Opmigua node subdivided into four functional blocks [6].

Packet Separator (PS) in figure 2-1, detects the QoS of incoming packets for each input wavelength. Then, it forwards SM packets to the OPS module and GST packets to the OXC. The packets that exist in the OXC have absolute priority over the traffic from the OPS. To achieve this, there is a control - logic which instructs the optical packet switch to treat an output channel as busy whenever a GST packet is present in its packet combiner. Some problems that related to low granularity of the GST LSPs are solved by combining the SM and GST packets to be time division multiplexed on the output wavelengths. Furthermore, an important feature of the Packet Combiner (PC) is a creation of label for each packet according to their service class [6].

As it concerns the four functional blocks, we can conclude some results which are the follows:

- Polarization combiners and separators should be more reliable than the OPS and OXC components.

- A good solution was letting the Packet Switch (PS) support GST traffic in case of Optical Cross Connect (OXC) failure. It was a very good idea because the expenses of this was very small and the increased availability of components used by GST LSPs is valuable.

- Assuming that the OXC is more reliable than the packet switch, there is a duplication of OXC.

- Assuming that the packet switch is the most error - prone, duplication of the packet switch increases the availability of components used by SM packets.

Figure 2-2 depicts a hybrid network model with a packet switches combined with a Wavelength Routed Optical Network (WRON). Packets follow the wavelength paths defined by the Optical Cross Connect (OXC) while the remaining packets are switched in Packet Switches (PS) according to their attached header information [5].

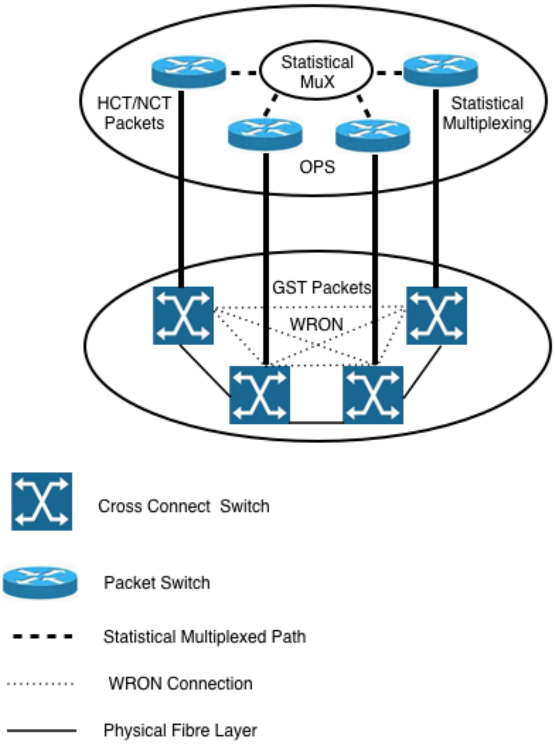


Figure 2-2. Hybrid network model [5].

This model illustrates the efficient sharing of the network layer. If the WRON is an (Static) S-WRON, the cross connect can be a matrix, manually configurable. On the other side, If the network is (Dynamic) D-WRON, then the cross connect should be configured by a control plane.

2.1.2 Opmigua Physical Layer

As it concerns the node design, is explained in figure 2-3 below. The State of Polarization (SOP) is used for separation SM and GST packets inside the node. Polarization Beam Splitters (PBSs) separate by physical way of the SM and GST packets at the input interface. Furthermore, it does not need neither guard band between GST and SM packets nor headers on GST packets but are required processing in the detecting node. At the input node, Automatic Polarization Control (APC) is needed because of the polarization variations in the transmission fibre [5].

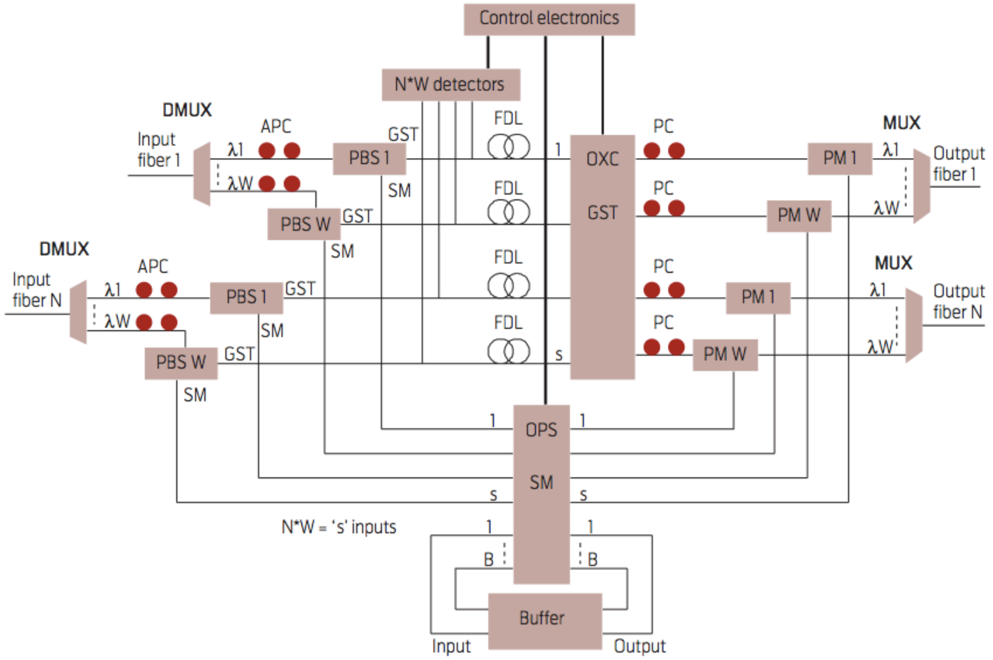


Figure 2-3. Opmigua node design [5].

Figure 2-4 represents the Opmigua hybrid network principle with three nodes and up to two wavelengths per link. Wavelengths λ1 and λ2 are GST lightpaths transporting GST packets (white) from ingress to egress and from core to egress. SM packets (gray) are inserted in gaps at any lightpath passing their next hop, where they are dropped, packet - switched and reinserted in gaps leading towards their destination. Packets, are identified as SM or GST by their state of polarization (SOP) using a Polarization Time Devision Multiplexing scheme (PolTDM) avoiding switches for separating GST and SM packets [6].

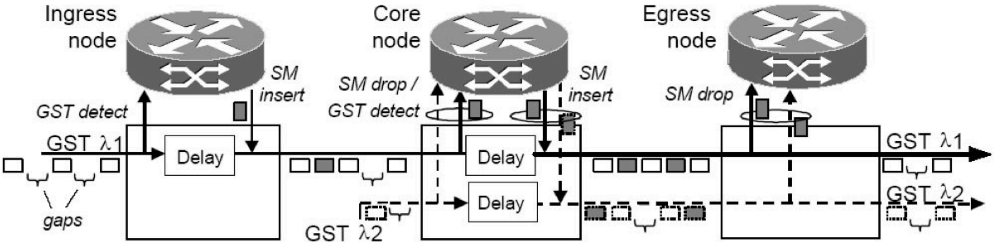


Figure 2-4. Opmigua hybrid network with three nodes. SM packets are processed in the routers while the GST packets are processed in WRON [6].

However, GST packets are transmitted on one SOP and SM packets are transmitted on the orthogonal polarization in a PolTDM scheme. The SOP is random at the input node and fluctuates with time when the environmental conditions change along the optical transmission line. For this reason, polarization control is necessary. The SOP is changed by the controller into the desired state and as a result, different classes can be separated by polarization demultiplexing at node inputs. Figure 2-4 gives how the ingress, core and egress node are connected. The time division multiplexed SM and GST packets are transmitted on orthogonal states of polarization. This enables all-optical identification and separation of the two QoS classes by polarization without optical-to-electrical conversion and complex header processing. Polarization demultiplexing with one controller per wavelength channel is used for separation of packets in core and egress node [6].

2.1.3 Protection Scheme for an Opmigua Node

Hybrid networks are totally different from other network models. They need unique protection strategies and the reason is that SM traffic is handled by an optical packet switch and GST traffic follows WRON paths. One of the advantages of an Opmigua network is the guaranteed transport that provides but it must also be granted in case of a link failure or an equipment failure [14].
There are three protection mechanisms for GST traffic:

- In case of link failure, there is a switching mechanism to an alternative pre-planned link.
- Mechanism for local redundancy of the GST part of the mode.
- Mechanism for switching to a pre-planned alternative network path if the first and second mechanism are failed.

The Statistical Multiplexed (SM) traffic is protected by IP restoration techniques allowing efficient resource utilization but this protection is slow. Figure 2-5, presents the fist mechanism for GST traffic. Here, the main part of the node consists of a OXC and a packet switch and local protection 1+1 for GST packets is achieved by simpler and less expensive redundant part of the node consisting of a passive OXC. If a failure is occurred in the main part of the node, the optical 1x2 switches at the output section will switch all the traffic to the redundant OXC. This change from failure to protecting OXC is achieved by employing fast switches. Furthermore, SM traffic and GST traffic is separated, while in the redundant part of the node, all traffic is forwarded according to the WRON configuration. The result is that there is not protection for SM traffic [14].

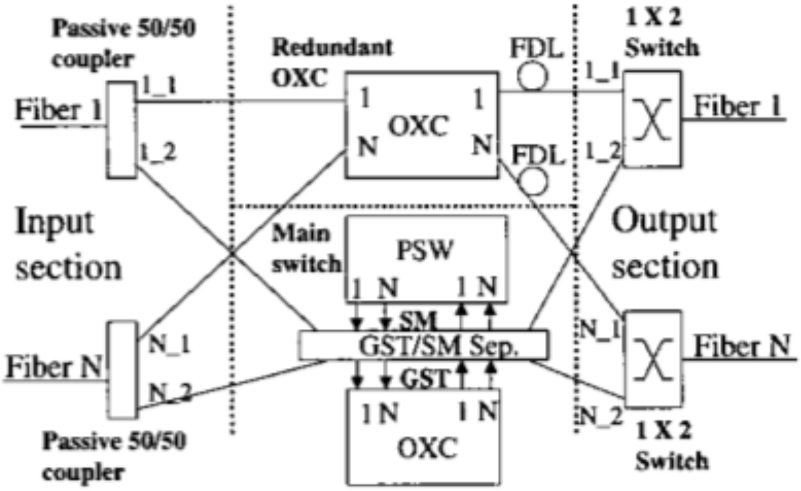


Figure 2-5. Opmigua node with redundant OXC [14].

The second protection mechanism is the link protection. In case of a link failure, the GST traffic is supported by one or more redundant paths. For full protection of GST traffic, in case of x link failures, the total traffic on k redundant GST paths must be lower than the total traffic volume that can be carried on k-x paths. For avoiding packet loss during protection switching there are two mechanisms. The first one is called pre-protection and the second one is called pre-buffering. Pre-protection is the technique that detects failures in the links. When the pre-buffering mechanism is used, data are continuously buffered in the ingress node. If a failure occurs, the data in the buffer are re-transmitted on the backup path [14].

Furthermore, the Opmigua project has two different network layer packet redundancy schemes: The fist one is the RedSM for redundancy packets which are transmitted as SM traffic and second is the RedGST for redundancy packets which are transmitted as GST traffic with lower priority than the original GST data traffic [15].

2.2 MPLS Background

MPLS was originally proposed by a group of engineers from Ipsilon Networks. Cisco Systems, introduced a related proposal, not restricted to ATM transmission, called "Tag Switching". It was a Cisco proprietary proposal, and was renamed "Label Switching". It was handed over to the IETF for open standardization. The IETF work involved proposals from other vendors, and development of a consensus protocol that combined features from several vendors work. The motivation was to allow the creation of simple high-speed switches, since for a significant length of time it was impossible to forward IP packets entirely in hardware. Therefore, the advantages of MPLS primarily revolve around the ability to support multiple service models and perform traffic management.

MPLS is a highly scalable and data-carrying mechanism and it belongs to packet switched networks. In this kind of network, data packets are assigned labels. Packet forwarding decisions are made solely on the contents of this label, without the need to examine the packet itself. This allows one to create circuits across any type of transport medium, using any protocol. The benefit was to eliminate dependence on a particular Data Link Layer technology, like Ethernet and eliminate the need for multiple Layer 2 networks to satisfy different types of traffic.

MPLS operates between Layer 2 - Data Link Layer and Layer 3 - Network layer of OSI network model (figure 2-6). It was designed to provide a data carrying service for both circuit and packet switched based clients. It can be used to carry many different kinds of traffic, such as IP packets, Ethernet and ATM frames. However, MPLS provides the same goals like the previous technologies such as ATM and frame relay but was equipped with some enforcements to face the strengths and weaknesses of ATM mechanism.

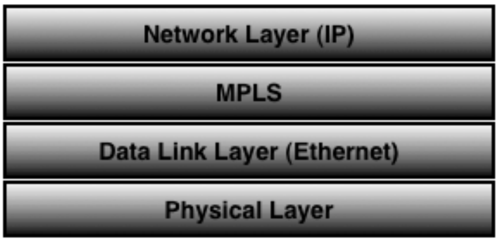


Figure 2-6. MPLS layer into layer hierarchy [9].

MPLS has replaced almost all these technologies in the marketplace [8]. As the packets travel from one router to another, each of these routers make an independent forwarding decision. Each router runs a routing algorithm and does analysis of each packet header to examine where to send it after. For this reason, each router chooses a next hop for each packet based on packet header analysis [9]. A router forwards an IP packet according to its prefix. In a given router, the set of all addresses that have the same prefix, is referred to as the Forwarding Equivalent Class (FEC) and packets that belong to the same FEC, have the same output interface. On the other side, in MPLS technology, each FEC is associated with a different label. This label is a short fixed length identifier and has always local significance. MPLS label is useful for the identification of the output interface of an IP packet without having to look up its IP address every time in the forwarding table. This label has the same functionalities to Virtual Path Identifier/Virtual Circuit Identifier (VPI/VCI) value associated with an Asynchronous Transfer Mode (ATM) cell [20].

MPLS has many benefits which are higher reliability, integration, better efficiency, better way to support multicast and (RSVP), direct classes of service implementation, traffic engineering capabilities, more robust - reduces load on network cores and finally Virtual Private Network (VPN) scalability and manageability [20]. As it concerns the integration, MPLS integrates IP and ATM functionality rather than overlaying IP on ATM. For this reason, the ATM infrastructure is made visible to IP routing and there is not any need for mapping between IP and ATM features. The result is that MPLS does not need ATM addressing and routing techniques. Better efficiency, means when all the Permanent Virtual Circuits (PVCs) are seen by IP routing as a single hop paths with the same cost. Another benefit of MPLS is the higher reliability that was mentioned above. MPLS is an easy solution for integrating routed protocols with ATM. Traditional IP over ATM involves setting up a mesh of Permanent Virtual Circuits (PVCs) between routers around the ATM cloud. With this approach, there are number of problems. The most serious problem is that a single ATM link failure could make several router to router links fail, creating problems with large amounts of routing update and subsequent processing. Direct classes of service implementation is another MPLS benefit. In this situation, MPLS makes use of the ATM queueing and buffering capabilities to provide different Classes of Service (CoS). This allows direct support of IP precedence and CoS on ATM switches without complex translations to the ATM. On the other hand, MPLS provides VPN scalability and manageability. This means that MPLS can make IP VPN services more scalable and more easy to manage. With an MPLS backbone, VPN information can be processed only at the ingress and egress nodes, with MPLS labels carrying packets across a shared backbone to their correct exit point. Moreover, MPLS benefits include Traffic Engineering (TE) capabilities needed for the efficient use of network resources. TE is possible to shift the traffic load from overutilized portions to underutilized portions of the network, according to traffic type, traffic load and traffic destination. Last but not least benefit that the MPLS provides, is the load reduction on core network. MPLS allows access to the internet routing table only at the ingress and exit points of a service provider network. The transit traffic entering at the edge of the provider's autonomous system can be given labels that are associated with specific exit points.

The result is that the internal transit routers and switches need only process the connectivity with the provider's edge routers [20].

An MPLS network consists of MPLS nodes, Label Switching Routers (LSRs) and Label Switching Paths (LSPs). MPLS node is also an LSR but it does not have necessarily the capability to forward IP packets based on prefixes. As it concerns LSR, is an IP router that is capable to run the MPLS protocol. Its LSR is responsible to bind labels to FECs, forward IP packets based on their labels and carry the forwarding decision by carrying out a table look up in the forwarding table using a prefix [10]. Below, in figure 2-7 we can distinguish that there are two MPLS administrative domains and one domain that does not support the MPLS protocol. IP packets, are switched using their MPLS label inside the MPLS domain.

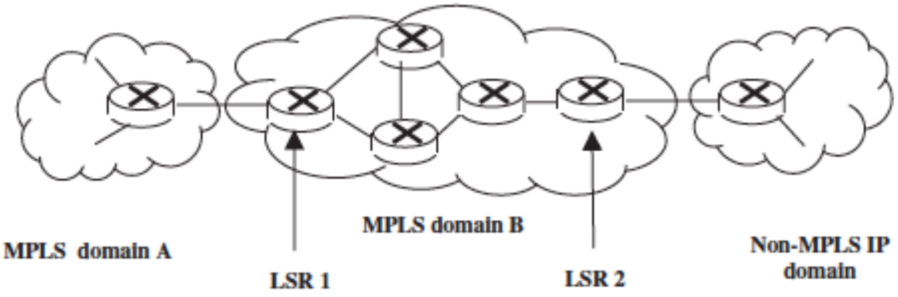


Figure 2-7. MPLS domains, nodes and LSRs [10].

An MPLS domain can be connected to a node outside the domain, which might belong to an MPLS or a non-MPLS IP domain. In figure 2-7 above, the MPLS domain B consists of five routers, two of which are LSRs (LSR 1 and LSR 2). The remaining three routers can be either LSRs or MPLS nodes. For more simplicity, we can assume that all nodes within an MPLS domain are LSRs [10]. MPLS domain B is connected to the MPLS domain A via LSR 1, and is connected to the non-MPLS IP domain via LSR 2. LSRs 1 and 2 are referred to as MPLS edge nodes.

MPLS networks have three main applications. It is possible two or three of these capabilities would be used simultaneously [20].

◉ IP Virtual Private Network (VPN) Services: A VPN service is offered by a provider to many corporate customers and is the infrastructure of a managed Intranet and Extranet service. The MPLS technology in combination with the Boarder Gateway Protocol (BGP), allows one network provider to support thousands of customer's VPNs. This combination offers a very scalable, flexible and manageable way of providing VPN services on both ATM and packet-based equipment.

- IP and ATM Integration: MPLS integrates IP services directly on ATM switches. the IP routing and Label Distribution Protocol (LDP) software resides directly on ATM switches. For this reason MPLS allows ATM switches to optimally support IP multicast, Virtual Private Network (VPN), IP class of service and Resource Reservation Protocol (RSVP). This integration of IP and ATM means that the MPLS is less complex and more scalable.

- IP Explicit Routing and Traffic Engineering (TE): IP networks have lack of ability to finely adjust IP traffic flows to make best use of available network bandwidth. Another problem is the lack to send selected flows down selected paths. Label Switched Paths (LSPs) are used by MPLS and can be used on both ATM and packet-based equipment. IP Traffic Engineering capability of MPLS uses special LSPs to finely adjust IP traffic flows.

2.3 T-MPLS Background

Transport networks have a crucial role for carriers. Service platforms depend on reliable and stable links between elements and nodes. As it concerns transport networks, they provide links and management of physical media and network facilities with different platforms that require connectivity between them. Packet transport networks provide greater flexibility and efficiency than SDH to support next generation networks. The evolution for transport networking was the T-MPLS protocol. Figure 2-8 presents three transport epochs between 1990 and 2005 and how transport technology has re-formulated to provide requirements to a new market.

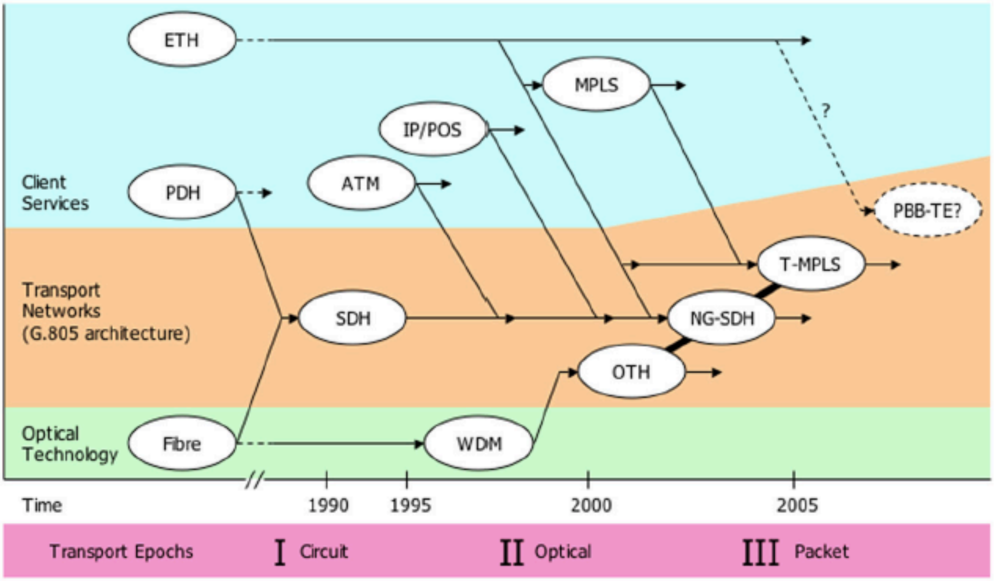


Figure 2-8. Evolution of Transport Networks between three transport epochs [11].

The three transport epochs are: Epoch I is circuit - Synchronous Digital Hierarchy (SDH), Epoch II is optical - Synchronous Digital Hierarchy (SDH) and Optical Transport Hierarchy (OTH) and Epoch III is packet - Next Generation Network (NGN), Transport - Multiprotocol Label Switching (T-MPLS) and Next Generation Synchronous Digital Hierarchy (NG-SDH). In 1990, Synchronous Digital Hierarchy (SDH) was adopted by carriers as the way to deploy circuit transport networks. After ten years (in 2000), another technology which is called Wavelength Division Multiplexing (WDM) was the main interest because the service capacity was increased. These days, Optical Transport Hierarchy/Optical Transport Network (OTH/OTN) architecture which was defined by ITU-T, is followed by all types of optical/WDM equipment. The Optical Transport Network (OTN) also known as Optical Transport Hierarchy (OTH) standard, describes a means of communicating data over an optical network. It was created with the intention of combining the benefits of SONET/SDH technology with the bandwidth expansion capabilities offered by Dense Wavelength Division Multiplexing (DWDM) technology. Furthermore, the OTN consists of many separate parts which are often referred to as layers: Optical Multiplex Section (OMS), Optical Transport Section (OTS), Optical Channel (OCh), Optical Data Unit (ODU), Optical Transport Unit (OTU) and finally Optical Channel Payload Unit (OPU). Each of these elements are distributed along the network and activated when they reach their termination points. Figure 2-9 presents the Optical Transport Network Layer Termination Points [11][21].

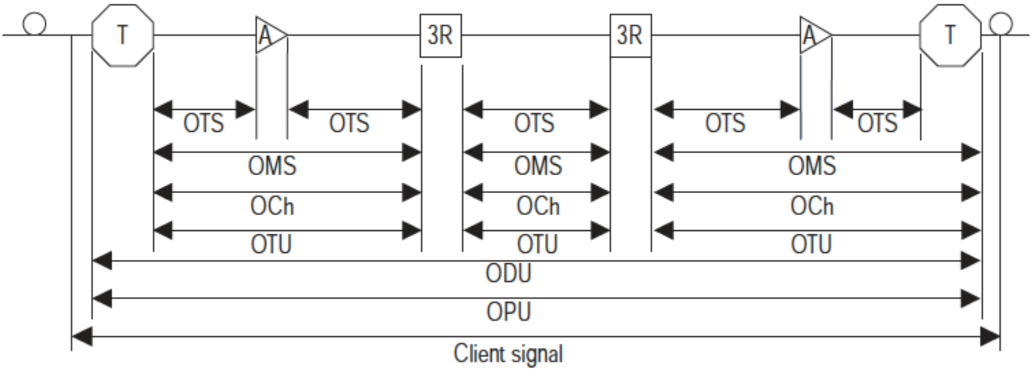


Figure 2-9. Optical Transport Network (OTN) Layer Termination Points (T= Client access point, A= Optical amplifier, 3R= Regeneration, Reshape, Retime) [11].

The termination of Optical Transport Section (OTS), Optical Multiplex Section (OMS) and Optical Channel (OCh) layers is performed at the optical level of the Optical Transport Network (OTN). Further functionality can be added at the termination of Optical Transport Unit (OTU). This layer is also known as digital wrapper and is a digital layer and offers specific overhead to manage the OTN's digital functions. The Optical Transport Unit (OTU) is a new layer to optical networking and it adds Forward Error Correction (FEC) to the network elements, and the result is to allow the network operators to limit the number of required regenerators used in the network. In figure 2-9, the Optical Transport Unit (OTU) encapsulates two additional layers which are the Optical Channel Payload Unit (OPU) and the Optical Data Unit (ODU) which provide access to the payload. The termination of these layers are done at the same location [21].

IETF has originally developed MPLS protocol in order to address core IP router performance issues. While packet networking is increased, the ITU-T was interested in adopting MPLS for making it carrier class network with functions of ITU-T architectural principles. For this reason, the result was the Transport MPLS (T-MPLS) which is a connection oriented packet transport network and is based on MPLS principle which provides managed point to point connections to different client layer networks. T-MPLS does not support a connectionless mode, is more easily managed and less complex than MPLS [11]. The main focus of T-MPLS is based on Ethernet services but also the client - server architecture can handle all packet services like IP/ MPLS.

T-MPLS operates at layer two data plane level. It has borrowed many characteristics and capabilities from IETF - MPLS but is focused on the additional aspects that address the need for any transport layer to provide high availability. Some of the key aspects are:

- Management and control of bandwidth allocation using Label Switched Paths (LSPs).
- Survivability: mechanisms such as protection and restoration. The protection switching is linear with 1+1, 1:1 and 1:N options. Another mechanism is the T-MPLS ring protection switching. Because no control plane is involved protection switching performance can be very fast.
- Improved control of a transport layer's operational state through SDH like OAM (Operation, Administration and Maintenance) which is used for administering and maintaining the network.
- No label reservation. T-MPLS does not reserve labels for its own use independently of MPLS.
- T-MPLS control plane is not used. The management plane will be used for manual or automated provisioning in the same way like OTN/WDM and SDH networks.
- Complete separation of the control and data plane creating full flexibility for network management and signaling which is take place in control plane.

2.4 MPLS-TP Background

MPLS-TP started as a (Transport) T-MPLS at the ITU-T which was renamed based on the agreement that was reached between the ITU-T and the IETF to produce a converged set of standards for MPLS-TP [3]. The first version of Transport MPLS architecture was approved by ITU-T in 2006. Then, in 2008, this technology started to be supported by some vendors in their optical transport products. At the same period, IETF was working on a new mechanism which was called Pseudo Wire Emulation Edge to Edge (PWE3) that emulates the essential attributes of a service such as Frame Relay, TDM, ATM or Ethernet over a Packet Switched Network (PSN) which can be an MPLS network [12]. The future standardization work will focus on defining MPLS-Transport Profile (MPLS-TP) within the IETF using the same functional requirements that drove the development of T-MPLS.

This idea for standardization of a new transport profile for Multiprotocol Label Switching is intended to provide the basis for the next generation packet transport network. The main point of this activity was the extension of MPLS protocol where necessary in order to meet the transport network requirements which are given in figure 2-10 below [1][3].

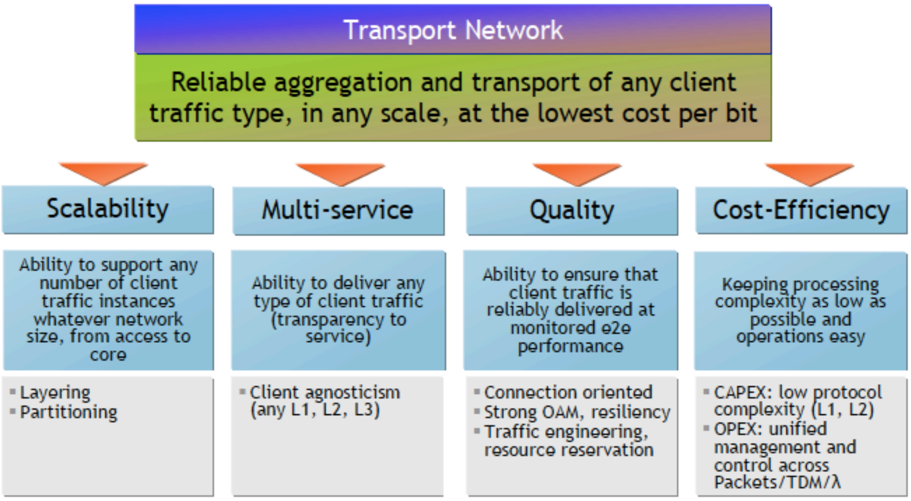

Transport Network
Reliable aggregation and transport of any client traffic type, in any scale, at the lowest cost per bit
Scalability
Multi-service
Quality
Cost-Efficiency
Ability to support any number of client traffic instances whatever network size, from access to core
Ability to deliver any type of client traffic (transparency to service)
Ability to ensure that client traffic is reliably delivered at monitored e2e performance
Keeping processing complexity as low as possible and operations easy
▪ Layering
▪ Partitioning
▪ Client agnosticism (any L1, L2, L3)
▪ Connection oriented
▪ Strong OAM, resiliency
▪ Traffic engineering, resource reservation
▪ CAPEX: low protocol complexity (L1, L2)
▪ OPEX: unified management and control across Packets/TDM/λ

Figure 2-10. Transport Network Requirements [3].

The main goal of MPLS-TP is to provide connection oriented transport for packet and TDM services over optical networks. The essential futures of MPLS-TP defined by IETF and ITU-T are:

- It is able to run over IEEE Ethernet, OTN, SDH/SONET.
- It provides strong Operation, Administration and Maintenance (OAM) functions similar to those available in traditional optical transport networks. OAM are part of the MPLS-TP data plane and are independent from the control plane.
- Several protection schemes at the data plane similar to traditional optical transport networks.
- It uses Pseudo Wire Emulation Edge to Edge (PWE3) architecture.
- Use of Generic Associated Channel (G-ACh) to support FCAPS functions (Fault, Configuration, Accounting, Performance and Security).
- Control Plane: static or dynamic Generalized MPLS (G-MPLS).
- It is strictly connection oriented.
- It is client - agnostic. This means that can carry layer 1, layer 2 and layer 3 services.

Chapter 3

MPLS-TP Architecture

Chapter three provides the background of MPLS-TP and is divided in five sections. The first one, gives some characteristics and requirements of MPLS-TP protocol. Second section, is based on MPLS-TP management and which explains these mechanisms. Furthermore, third section is refereed to MPLS-TP forwarding plane. Finally, section fourth and fifth give some references for Operation Administration and Maintenance (OAM) mechanism and for control plane respectively.

3.1 MPLS-TP Characteristics and Requirements

Optical transport infrastructure like Synchronous Digital Hierarchy (SDH), Synchronous Optical Network (SONET) and Optical Transport Network (OTN) have provided carriers with a high standards of operational simplicity and reliability. To achieve these standards, there are some characteristics of transport technologies which are:

◉ A high level of availability.

◉ Quality of Service (QoS).

◉ Operation Administration and Maintenance (OAM) extension capabilities.

◉ Connection oriented connectivity.

However, carriers wish to evolve this technology for some advantages like cost benefits of packet switching technology, flexibility and efficiency of packet based services support. These days, MPLS plays an important role in transport networks but not all mechanisms and capabilities are needed in a transport network. From the other side of view, there are still characteristics in a transport network technology that are not currently reflected in MPLS. For this reason, there are two objectives for MPLS-TP. The first one is to enable MPLS technology to be supported in transport networks and to be operated in a similar way like the existing transport technologies. Second objective is to enable MPLS to support packet transport services with a similar degree of predictability like the existing transport networks [16]. For achievement of these objectives, there is a need to define a common set of MPLS protocol functions for the use of MPLS in transport networks.

MPLS-TP is considered a connection - oriented packet switched technology and is a subset of MPLS functions (figure 3-1). It is a simplified version of MPLS for transport networks without some of the MPLS functions like Equal Cost Multi - Point (ECMP), Penultimate Hop Popping (PHP) and Label Switched Paths Merge (LSPs). It does not require MPLS control plane capabilities and enables the management plane to setup LSPs manually [1][16].

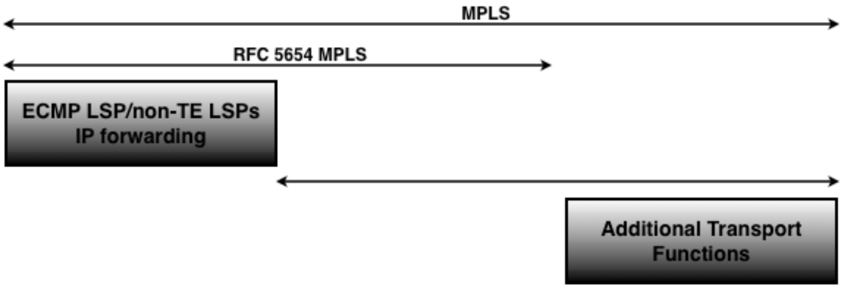


Figure 3-1. Scope of MPLS-TP [16].

The main objective of MPLS-TP, as it considered above, is to enable MPLS to support packet transport services. For this reason, packet transport services inherit a number of characteristics [16][17]:

- The service provided by the MPLS-TP network to the client is guaranteed to do not fail below the agreed level regardless of other client activity.

- Control and Management plane of the MPLS-TP layer network is isolated from the Control and Management plane of a client network layer.

- When MPLS-TP layer network supports a client layer network and the MPLS-TP layer is supported by a server layer network then the operation of the MPLS-TP layer network must be possible without the client and server layer network.

- MPLS-TP addressing and other information are hidden from any client layer networks using packet transport services.

- The set of packets which is generated by a client layer network which is using the packet transport service, may contain packets that are not MPLS packets.

As it concerns the architecture of MPLS-TP, is compromised by some elements like MPLS data plane, Operation Administration and Maintenance (OAM) functions, sections - LSPs and PWs that provide a packet transport service, optional control planes for LSPs and PWs, optional path protection mechanisms and network management functions. MPLS-TP data plane has some components which are: MPLS-TP Label Switched Path (LSP), MPLS-TP Label Switched Router (LSR) and Label Edge Router (LER), MPLS-TP Provider Edge (PE) Router, MPLS-TP Provider (P) Router, Label Edge Router (LER), Edge to Edge LSP and service LSP [16].

An MPLS-TP Label Switched Path (LSP) uses the capabilities of MPLS LSP to meet the requirements of an MPLS transport network. Some characteristics of MPLS-TP LSP are: It is traffic engineered, is either point to point or point to multipoint but multipoint to multipoint and multipoint to point LSPs are not permitted. Another characteristics are included are protection functions 1+1, 1:1 and 1:N, usage of a subset of MPLS OAM tools and LSPs can be maintained and established via management plane or with control plane using GMPLS protocols. As it concerns the MPLS-TP Label Switching Router (LSR) can be either MPLS-TP Provider (P) router or MPLS-TP Provider Edge (PE) router for a given LSP [16][17].

MPLS-TP Provider (P) router switches LSPs which carry client traffic but does not encapsulate the client traffic to be carried over an MPLS-TP LSP. Another thing is that it does not provide MPLS-TP functionality for a given LSP like MPLS-TP Provider Edge (PE) Router. On the other side, MPLS-TP Provider Edge (PE) Router adapts client traffic and encapsulates it to be transported over an MPLS-TP LSP. There are two ways for encapsulation. One way uses pseudo-wire and the other way is simple as a pushing a label [16].

Edge to Edge LSP is a pair of provider edges that transit zero or more provider LSRs. Finally the last element is called Service LSP and it carries a single client service.

The MPLS-TP is used for packet transport network construction and is applicable in any packet transport network context. There are some models that use the MPLS-TP application and are refereed above [16][17]:

- MPLS-TP that is provided by a network supports non MPLS-TP LSPs and PWs.

- MPLS-TP that is provided by a network supports only MPLS-TP LSPs and PWs.

- MPLS-TP acts as a server layer for client layer traffic of MPLS or IP networks which do not use functions of the MPLS transport profile.

The first two models act as a server for other layer 1, layer 2 and layer 3 networks. The third model, for MPLS traffic uses LSPs or PW switching at the provider edge (PE) and terminates the MPLS-TP server layer [16]. Below, figure 3-2 depicts the MPLS-TP LSP which is acting as a server between two Provider Edges (PE1 and PE2) and supports only MPLS-TP.

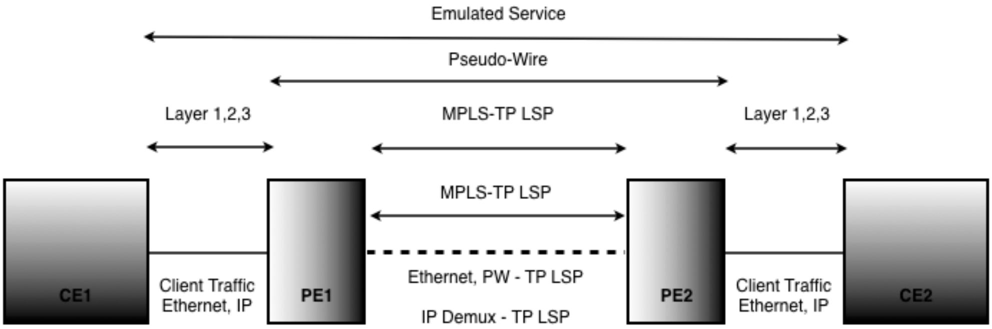


Figure 3-2. MPLS-TP Server Layer Example [16].

On the other side, an MPLS-TP LSP is capable to provide support also to non MPLS-TP functions and it acts as a server for other layer 1, layer 2 and layer 3 networks (figure 3-3). Both figures 3-2 and 3-3 present two Client Edges (CE1, CE2) which are interconnected with two Provider Edges (PE1 and PE2). The connection between a client edge and a provider edge that the client traffic is transmitted can be over IP or Ethernet.

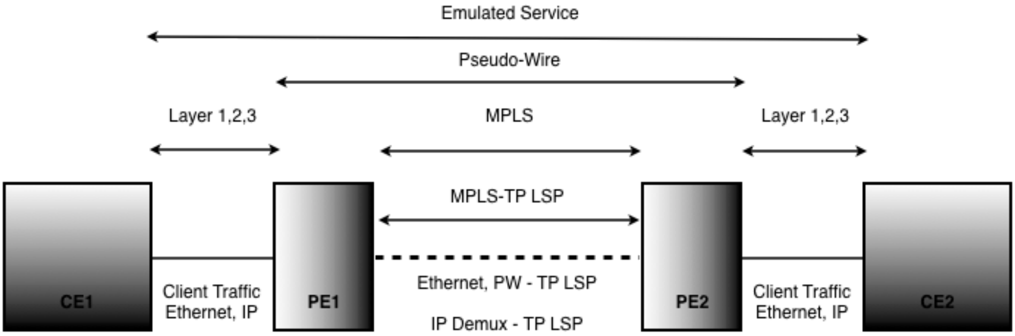


Figure 3-3. MPLS-TP in MPLS Network Example [16].

3.2 MPLS-TP Management Plane

3.2.1 MPLS-TP Management Architecture

The MPLS-TP network could be based on a multi-tiered distributed management systems. As an example of this, each of these tiers defines the level of network management capabilities. The MPLS-TP Network Element (NE) is included on the lowest tier of this model. MPLS-TP network element provides also the Operation System (OS) and the transport service at the Element Management Level (EML) [18].

Management Application Function (MAF) is defined by an application process that participates in a management system. In its entity the MAF can include managers and agents together or only managers and only agents. Furthermore, the management support is provided by the Management Application Function (MAF) with the Operation System (OS) and the Network Element (NE) [18].

Management communication to Network Element (NE) is provided via the Message Communication Function (MCF). The job that the MCF has is to initiate, route, terminate and process management messages over Communication Channel (CCh) or via external interface [18]. It contains communication functions like Management Plane (MP), Control Plane (CP), Local Craft Terminal (LCT), Local Alarms (LA) and finally date and time functions which are related to the outside world. The date and time functions, keep track of the network elements date and time and are used by the FCAPS management functions. Figure 3-4 gives an overview of the functions that are provided by the Message Communication Function (MCF).

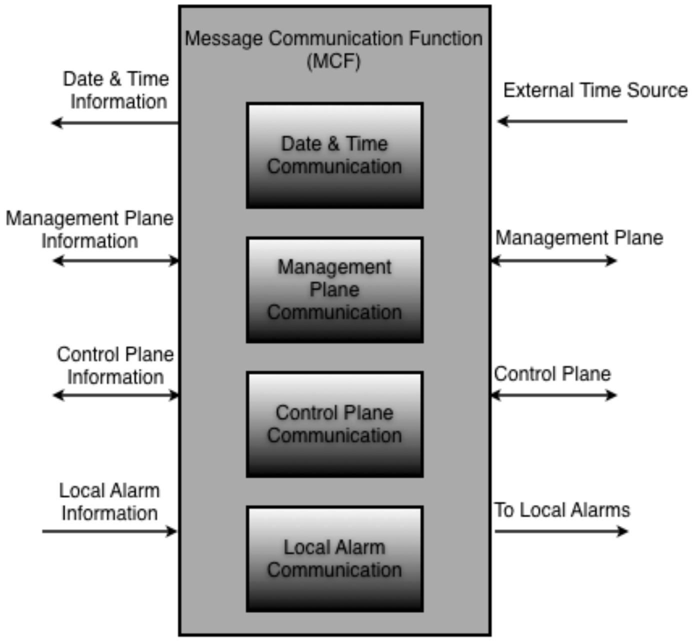

Message Communication Function (MCF)
Date & Time Information
External Time Source
Date & Time Communication
Management Plane Information
Management Plane
Management Plane Communication
Control Plane Information
Control Plane
Control Plane Communication
Local Alarm Information
To Local Alarms
Local Alarm Communication

Figure 3-4. Message Communication Function (MCF) [18].

The user, has the possibility to have access to the management MPLS-TP transport network via a Local Craft Terminal (LCT) which is attached to the network element or to operation system. The management of MPLS-TP network operates independently of any client and server layer management plane and is separated from other technology management networks. For example, it is partitioned into smaller networks which are called MPLS-TP management sub-networks [18]. The reasons that the MPLS-TP management network is partitioned into sub-networks depends on ownership or administrative and for scalability, like geographic reasons, and load-balancing. However, the MPLS-TP management subnetworks are possible to connect with other elements of the management network through Local Craft Terminal (LCT).

The Element Management Architecture (EMA) consists of Network Element Functions (NEF) which is consists of Equipment Management Function (EMF) and Message Communication Function (MCF). The Equipment Management Function (EMF) of MPLS-TP NE provides the means through which a management system manages the NE and contains functions for providing a data reduction mechanism on the information received across the Management Point (MP). It interacts with the NE transport functions by exchanging Management Information (MI) across the Management Point (MP) [18]. Furthermore, the EMF includes some functions like FCAPS (Fault, Configuration, Accounting, Performance, Security), date and time, management and control functions and provides data storage, logging and message processing. One component of the EMF is the management agent which converts management information signals into management application messages and the opposite. Then the agent responds to the management application messages from the Message Communication Function (MCF) by performing some operations on the Managed Objects in a Management Information Base (MIB) [18].

The diagram below (figure 3-5) illustrates the Network Element Function (NEF) and the way that the Equipment Management Function (EMF) and Message Communication Function (MCF) are connected. Here, the Equipment Management Function (EMF) is connected to transport plane for transferring the management information. EMF has four output and input interfaces which are connected to the Message Communication Function (MCF). The first one, which is called date & time interface receives only from the MCF information about date and time. The management and the control plane interface receive and send information to and from MCF and the last interface which is called local alarm interface, sends only information to the MCF. On the other side, the Message Element Function (MEF) has four interfaces that receives and sends information from and to outside the Network Element Function (NEF). The information that is received from outside world is the external time source and sends information about the local alarms. Finally, it both sends and receives management and control plane information.

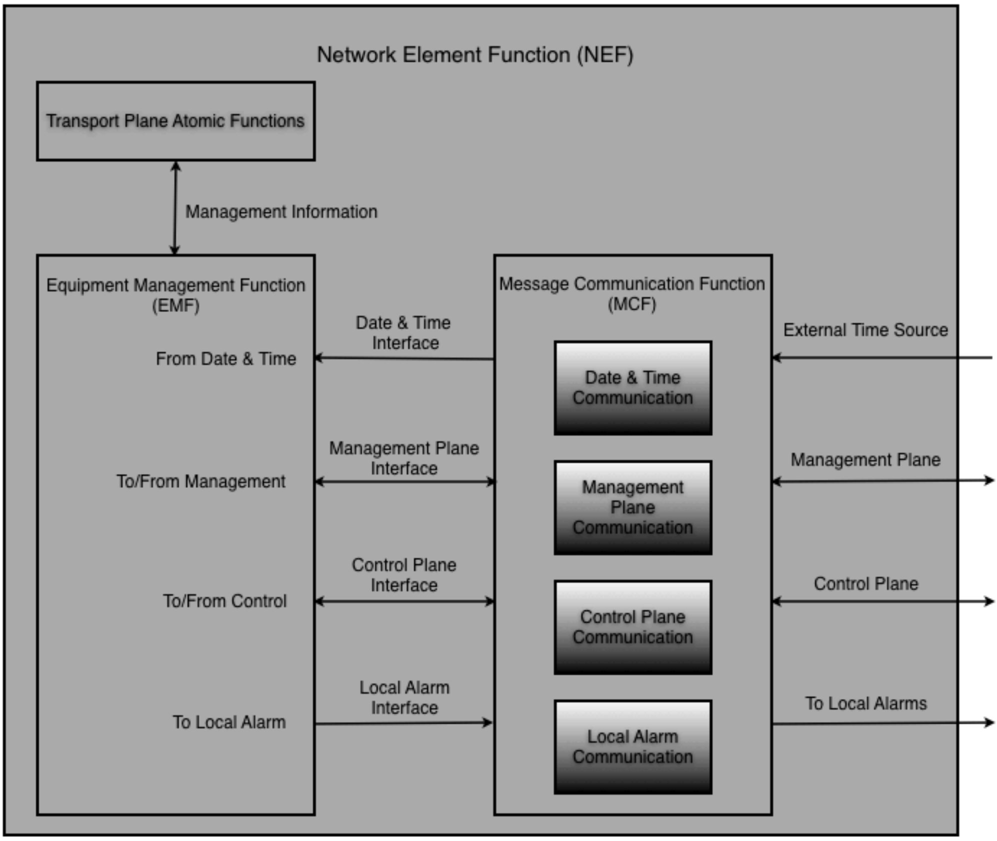

Network Element Function (NEF)
Transport Plane Atomic Functions
Management Information
Equipment Management Function (EMF)
From Date & Time
To/From Management
To/From Control
To Local Alarm
Date & Time Interface
Management Plane Interface
Control Plane Interface
Local Alarm Interface
Message Communication Function (MCF)
Date & Time Communication
Management Plane Communication
Control Plane Communication
Local Alarm Communication
External Time Source
Management Plane
Control Plane
To Local Alarms

Figure 3-5. Network Element Function (NEF) Components [18].

Different types of information like management and signaling information use a common term for the network which is called Data Communication Network (DCN). This information travels between managements systems and network elements, management systems to other management systems, and network elements to other network elements. Data Communication Network (DCN) consists of many parts. Two of these parts are the Management Communication Network (MCN) and the Signaling Communication Network (SCN). The former one, supports the transport of management information for the management plane. On the other hand, Signaling Communication Network (SCN) supports transport for signaling information for the control plane [18]. Each technology has its own technology that is used for the channels that support management and control plane information transfer.

Figure 3-6 presents the communication channel terminology for supporting transport of management information (a), signaling information (b) and common information transport (c). A logical channel between Network Elements (NEs) for transferring signaling and management information is provided by the Communication Channel (CCh).

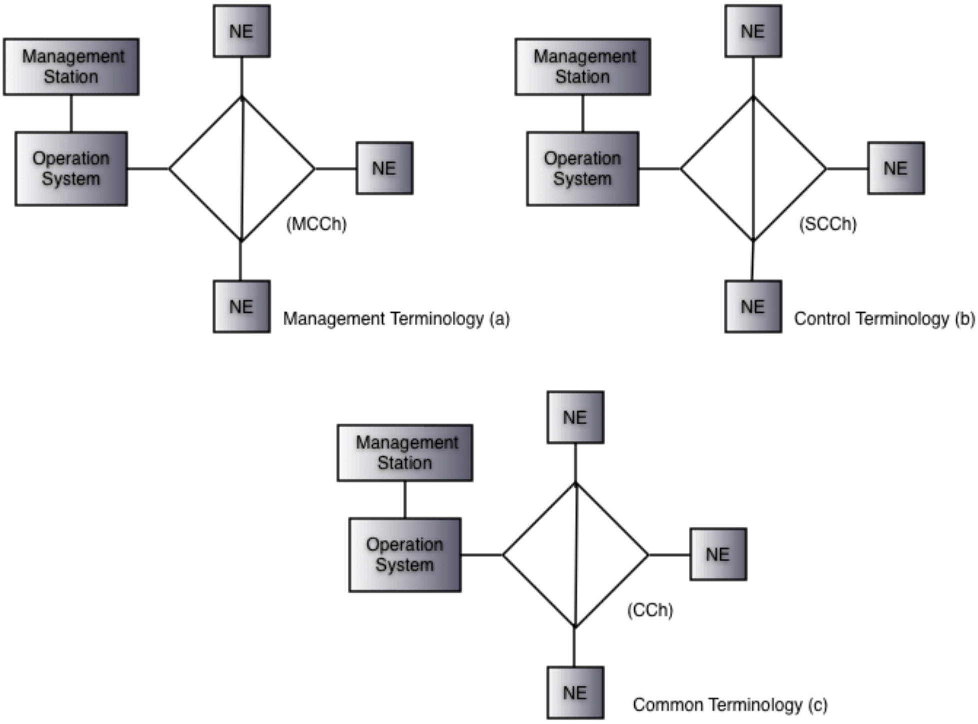


Figure 3-6. Communication Channel Terminology [18].

Some technologies provide separate communication channels for Signaling (SCCh) and Management (MCCh). Furthermore, the Network Elements in figure 3-6 communicate via Data Communication Network (DCN). The DCN, connects NEs with management systems, NEs with NEs, and management systems with management systems. As it concerns the figure 3-6 (a) , NEs are connected between them and use the Management Communication Channel (MCCh) from management information transport. The same exists also in part (b) and (c) in figure 3-6 but the NEs use a Control or Signaling Communication Channel (SCCh) for transport the signaling information and only Communication Channel for common information transport respectively.

3.2.2 MPLS-TP Management Modules

The MPLS-TP like the MPLS management architecture, is divided into multiple management layers. Figure 3-7 below presents the communication between Network Management System layer (NMS) with the Element Management System layer (EMS) and to General Adapter respectively. As it concerns the EMS, it consists of systems and applications that are concerned with managing network elements (NE) on the Network Element Management layer (NEM). Typically, the EMS manages the functions and capabilities within each NE but does not manage the traffic between different NEs in the network. To support management of the traffic between itself and other NEs, the EMS communicates upward to higher-level network management systems (NMS). On the other hand, the NMS talks to the EMS to get the overall view of the network [22]. It is possible many EMSs which belong to different sub-networks to Communicate with one NMS. The Network Management System (NMS) and also the Element Management System(s) (EMS) consist of some modules which are the configuration management, performance management and the fault management [19][22].

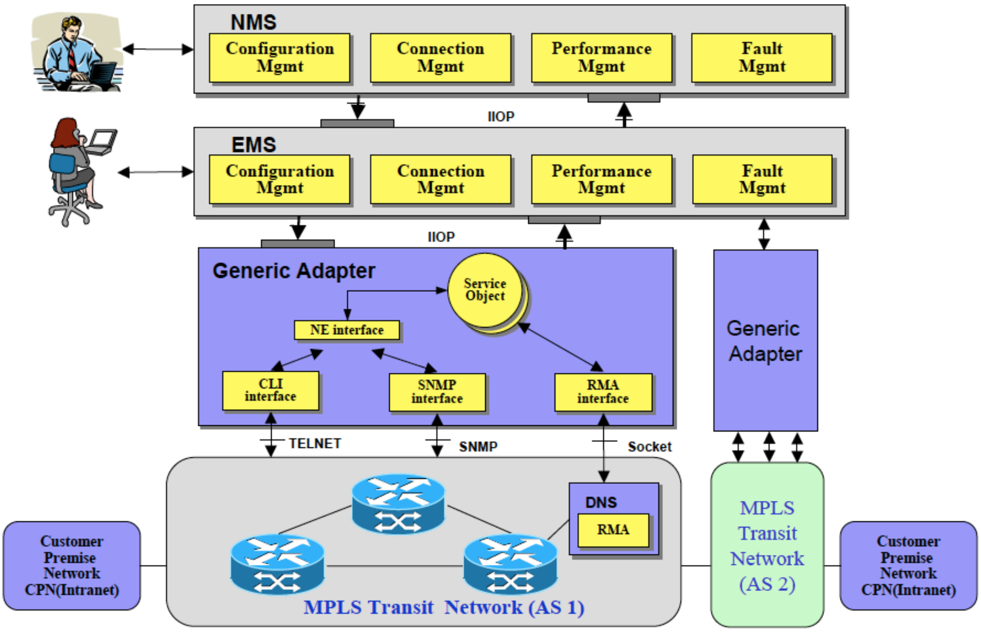


Figure 3-7. Management Architecture Layers. [22]

3.2.2.1 MPLS-TP Configuration Management

MPLS-TP networks can be managed not only by Network Management Systems (NMS) but also by Control Plane (CP) protocols. The control plane is not often used by network operators to make network configuration, Label Switched Path (LSP) and also is not a mandatory requirement [18]. Furthermore, both Control Plane (CP) and Management Plane (MP) are provided in networks and LSPs could be created by either CP or MP. Most of the network operators prefer to have full control of the network resources during the setup phase and then allow the network to be switched automatically by Control Plane. This is achieved by creating LSPs via Management Plane and transferring LSP ownership to the Control Plane. This technique is refereed as ownership handover [18].

The configuration management of MPLS-TP gives the mechanisms for provisioning the MPLS-TP services, provides the destination for fault notifications and performance parameters and setup security for the MPLS-TP services and MPLS-TP network elements. However, it provides functions to identify, collect and provide data from/to Network Elements (NEs). In the management task is also included hardware and software configuration, and Network Elements (NEs) configuration to support transport paths. There are five categories of MPLS-TP management configuration which are: i) Control Plane Configuration, ii) Operation Administration and Maintenance (OAM) Configuration, iii) Path Configuration and iv) Protection Configuration [19]. As it concerns the control plane configuration, the MPLS-TP should support the configuration of MPLS-TP control pane functions by the management plane. For the path configuration, the MPLS-TP should support the configuration of the required path performance characteristics thresholds necessary to support performance monitoring of the MPLS-TP services. For accomplishment this point, the MPLS-TP should support configuration of LSP information and any other information. Another function of path configuration is that MPLS-TP transport paths cannot be statically provisioned using MPLS LSP and PW management tools. Moreover, some of the protection configuration functions that MPLS-TP NE should support are:

- LSPs identification as working or protecting.
- Associations between working and protecting paths.
- Operate and release protection lockout.
- Operate and release manual protection switching .
- Set and retrieve parameters for Automatic Protection Switching (APS).

Moreover, as it concerns the Operation Administration and Maintenance (OAM) configuration, the MPLS-TP should support the capability to configure the OAM functions as part of LSP setup including co-routed bidirectional point to point, unidirectional point to point and also point to multipoint and associated bidirectional point to point connections. However it should support the configuration of maintenance entity identifiers for the purpose of LSP connectivity checking. Finally, another configuration that the MPLS-TP should support is the enabling and disabling of the connectivity check processing. It should support also the provisioning of the identifiers to be transmitted and the expected identifiers [18].

3.2.2.2 MPLS-TP Fault Management

Generally, fault management is the inability of a function to perform a required action [18]. It provides mechanisms for detection, isolation, notification and verification of a fault. There are three functions of the fault management; supervision, validation and alarm handling which are analyzed below.

Supervision function analyses the occurrence of a fault for the purpose of providing an appropriate indication of performance or fault detection condition to maintenance personnel and operation systems [18][19]. It has five basic categories that provide the functionality necessary to detect, notify and verify a fault. The categories are:

- Quality of Service (QoS) Supervision.
- Processing Supervision.
- Transmission Supervision.
- Environment Supervision.
- Hardware Supervision.

Furthermore, the MPLS-TP NE must support the supervision of the OAM mechanisms, the capability to configure data plane forwarding path, the hardware related supervision for interchangeable and non interchangeable unit, power and cable problems. It should also support functions for data plane forwarding, like supervision of failure detection and supervision for loop checking functions for detection of loops in the data plane forwarding path. Finally it must support supervision for software processing faults, storage capacity and corrupted data out of memory problems [19].

As it concerns the validation function, it describes a fault cause as a limited interruption of the required function. It is also used to turn fault causes into failures (alarms). A Fault Cause Indication (FCI) indicates a limited interruption of the required transport function [18][19].

Finally, with alarm handling function, failures can be categorized to these sub functions which are: The alarm severity assignment, alarm suppression, alarm reporting and finally alarm reporting control. For the first one, the MPLS-TP NE should have the ability to assign severity to alarm conditions via configuration. Alarm suppression can be generated from many sources. So, the MPLS-TP should support suppression of alarms based on configuration. Alarm reporting is concerned with the reporting of relevant events and conditions inside the network. Last but not least, Alarm Reporting Control (ARC) supports an automatic internal service provisioning capabilities. It can be turned off on a per managed entity basis to give more time for customer service testing and other activities in this state. The alarm reporting is turned on when a managed entity is ready [18][19].

3.2.2.3 MPLS-TP Performance Management

A management network is overwhelmed by performance statistics and it is important to provide flexible environment that gives control over the amount of performance data to be collected. There are two categories of performance management data. The first one is on demand collection of data measurement and the second is the proactively collection of data measurement. Proactive measurement is used continuously over the time when is being configured with periodicity and storage information. The data that are collected with this method are used for verifying the performance of the service. Performance monitoring has the ability to monitor the process of collecting performance data at a Network Element (NE) and to report this information process to the Operating System (OS). For this reason, the operators would typically limit the services to which proactive performance measurement would be applied to a very selective subset of the services being provided and would limit the reporting of this information to statistical summaries. Furthermore, with on demand measurements, the operator is possible to do performance measurement for maintenance purpose like diagnosis and to provide verification details of this measurement. This method is used on specific LSP service for a limited time for reduction of the impact on network performance in normal operation. For this reason this measurement is not scalable [18][19].

Performance Management provides some functions for the purpose of Quality of Service (QoS), statistics gathering and maintenances. MPLS-TP has two performance management requirements which are path characterization performance metrics and performance measurements instrumentation. As it concerns the path characterization performance metrics, it should be possible to determine when the MPLS-TP based transport service is available or unavailable. A service is unavailable, when there is an indication that the performance threshold has been crossed and the degradation persists long enough. Moreover, MPLS-TP should support collection and reporting of raw performance data that could be used in determining the unavailability of transport service [19]. Also it should be able to support collection of Loss Measurement (LM) statistics and collection of Delay Measurement (DM) statistics.

The other MPLS-TP management requirement is the performance measurement instrumentation and is divided into two parts, measurement frequency and measurement scope. For the fist one, when the performance measurement mechanisms support both on demand and proactive modes, the MPLS-TP should support the capability to operate to these modes. Measurement scope, for bi-directional point to point connections is required proactive measurement of packet loss and loss ratio for each direction and also measurement is required on demand measurement of single ended packet loss and loss ratio. For uni-directional point to point and point to multipoint connection proactive and on demand measurement are required of packet loss, and delay respectively.

3.3 MPLS-TP Forwarding - Data Plane

The MPLS-TP forwarding plane, is based on MPLS data plane functionalities. It includes the following data plane transport entities; Label Switched Paths (LSPs), Sections, and Pseudo-wires.

3.3.1 MPLS-TP Label Switched Paths (LSPs) Entity

Generally, network layer routing is partitioned into two components. The first one is the control component and the second one is the forwarding component. The forwarding component has a set of algorithms that a router uses to make forwarding decision on a packet. It is responsible to forward packets from input to output across the network. A forwarding table that includes all the packet information is used by the forwarding component. On the other side, control component consists of routing protocols, which exchange routing information between routers and algorithms that the router uses to convert routing information into a forwarding table. The responsibility of the control component is the construction and maintenance of the forwarding table. In the network, each router implements both control and forwarding components [23].

Forwarding Equivalence Class (FEC) is a group of IP packets that is forwarded with the same treatment and over the same path. FEC can also be regarded as a traffic policy that examines and classifies traffic flow according to a set of conditions and attributes. The reason that a router forwards all the packets into one FEC is the mapping between the information carried in the network layer header of the packets and the entries in the forwarding table is many to one [23][24]. The result is that the decompression mode of the network layer into forwarding and control components can be also applied to the MPLS label switching approach.

3.3.1.1 MPLS-TP Label Switching Forwarding Component

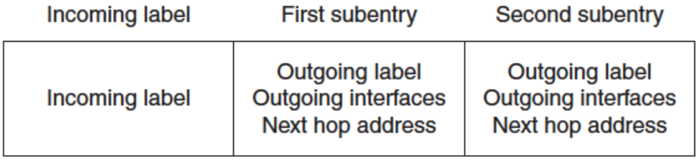
Label switching forwarding component has some key properties which are mentioned below [23]:

- It is possible to support multiple network layer and data link layer protocols.
- It uses a single forwarding algorithm based on label swapping.
- It uses a label which is carried inside the packet header and is a short fixed-length entity that has resource reservation and forwarding semantics.

A Label Switched Path (LSP) in MPLS architecture must be established prior to the forwarding of packets in a given FEC. The LSP functionality defines an ingress and the egress path through a network to be followed by all packets assigned to a particular FEC. The Label Switched Path (LSP) consist of a series of Label Switched Routers (LSRs) that forward packets for a particular FEC. Its LSP is also possible to carry more than one FEC. Furthermore, the algorithm that is used by the label switching function component to make a forwarding decision of the packets, uses two sources of information, the forwarding table maintained by a Label Switching Router (LSR) and the label which is carried in the packet [23][24].

MPLS-TP includes some of the LSP types which are: Point to point unidirectional, point to point associated bidirectional, point to point co-routed bidirectional and point to multipoint unidirectional [22]. Point to point unidirectional LSPs are supported by the basic MPLS architecture and have the same functionalities also in the MPLS-TP. As it concerns point to point associated bidirectional LSP, consists of two unidirectional point to point LSPs between two LSRs, for example LSR A and LSR B. These LSPs are regarded as a pair providing a single-logical bidirectional transport path. Furthermore, a point to point co-routed bidirectional LSP is a point to point associated bidirectional LSP with a modification that is two unidirectional component LSPs follow the same path inside the network. Finally, a point to multipoint unidirectional LSP is the same as point to point unidirectional LSP with some critical differences which are: The LSR can have more than one pair of egress interface and outgoing label, associated with the LSP, and any packet which is transmitted on the LSP is transmitted out all associated egress interfaces [22].

Forwarding table is maintained by an LSR and consists of entries. Each entry consists of incoming labels and one or more sub-entries which include outgoing labels, outgoing interfaces and next hop address. The sub-entries may have different or same outgoing labels. In case of multicast forwarding there may be exist more than one sub-entries, and all the packets arrive on one interface, would need to send out to multiple outgoing interfaces [23]. Figure 3-8, provides an example of the forwarding table entry which is consisted of the incoming label and two sub-entries.

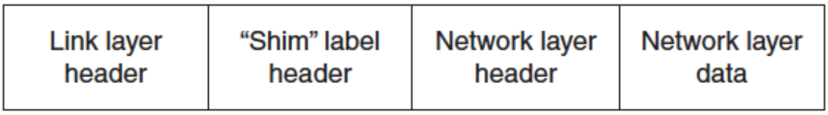


Incoming label	First subentry	Second subentry
Incoming label	Outgoing label Outgoing interfaces Next hop address	Outgoing label Outgoing interfaces Next hop address

Figure 3-8. Forwarding Table Entry [23].

There are two types of Label Switched Routers (LSRs). The edge LSRs and the core LSRs. Core LSRs, forward packets based on labels and they do not examine further the packet header except from the label. On the other side, edge LSRs, reside at the ingress or at the egress of the MPLS network. The responsibility of the ingress LSRs are to receive IP packets, perform packet classifications by grouping packets into FEC, forward the labeled IP packets into the head-end of the LSP and do layer three table lookup [24]. Generally, core routers perform only label swapping, forward packets based on simple label lookups and egress or ingress LSR perform routing lookup and label removal and assignment respectively. A Label Switching Router (LSR), can hold a single forwarding table or a forwarding table per each interface. Single forwarding table, handles a packet which depends solely on the label which is carried inside the packet header. With the latter option, packet handling is determined not only with the label carried inside the packet header but also by the interface that the packet arrives on it [23].

There are many ways for the label switching forwarding component to carry a label in a packet. Data link layer technologies like Ethernet, carry a label as part of their link layer header. One way to support label switching over data link layer when the data link layer cannot be used to carry a label is to carry it in a small label header [24]. This label header can be inserted between data link layer header and network layer header as it is described in figure 3-9 below.



Link layer header	“Shim” label header	Network layer header	Network layer data

Figure 3-9. Topology of the Label header between data link layer header and network layer header [23].

Furthermore, the label switching forwarding component is not specific to a particular network layer. It is possible the same forwarding component to be used for different network layer protocols like IPv4, IPv6, Apple Talk and IPX. With the same way, label switching forwarding component has the ability to operate in a virtual mode over any data link layer protocols like Ethernet. Figure 3-10 presents this ability of the forwarding component, which is described above.

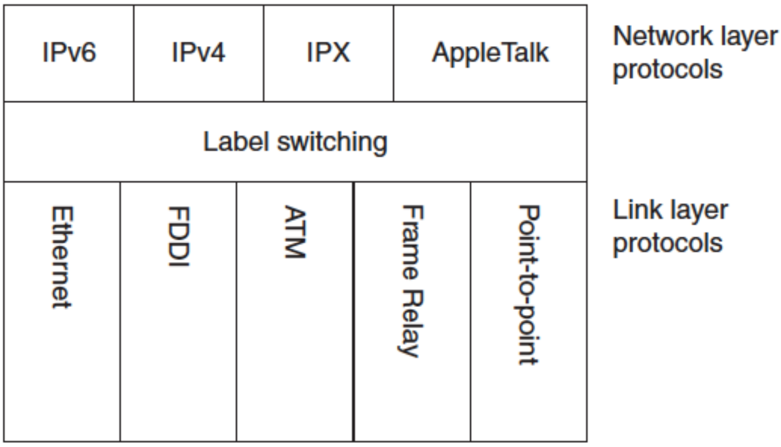


Figure 3-10. Label Switching Forwarding Component between Network layer protocols and Data Link layer protocols [23].

As it concerns the label header, it supports the label switching over point to point, and Ethernet technologies. The label header has 32-bit length (figure 3-11) and is expanded in four fields which are the label (20 bits), experimental bits (3 bits), stack bit (1 bit) and Time To Live (TTL) bits (8 bits) (figure 3-12). The MPLS label which is consisted of 20 bits has a local significant and is used to identify the particular FEC. It is imposed on a particular packet which indicates the FEC to which the packet is assigned.

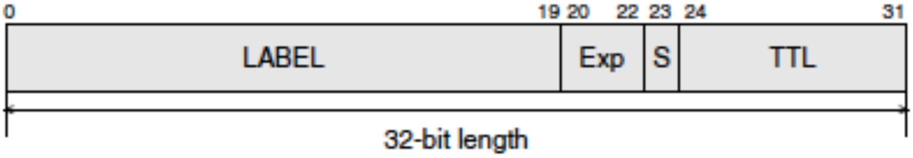


Figure 3-11. Label header length [24].

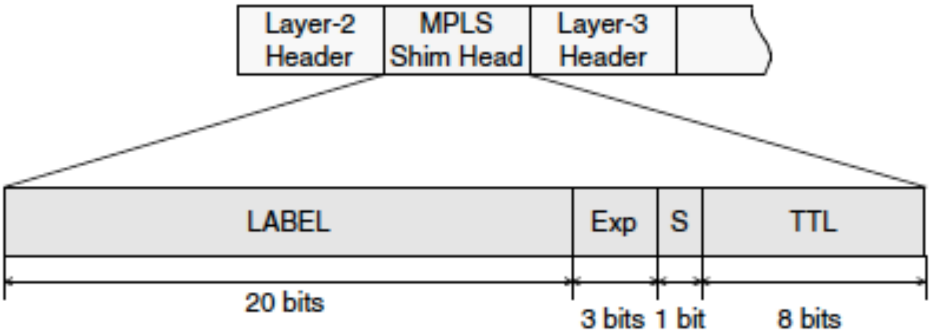


Figure 3-12. Label header structure [24].

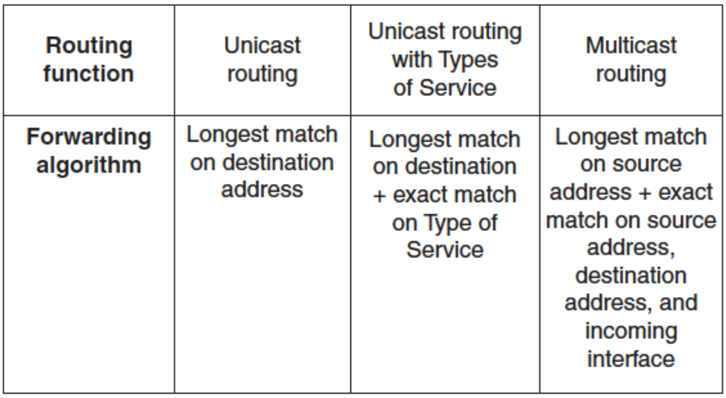
Figure 3-13 below, describes more analytically all the fields that are included into the MPLS header.

MPLS-TP Shim Header Fields	Length	Description
Bottom of stack (S)	1 bit	This bit supports a hierarchical label stack (typically used for nested LSPs) and denotes whether this is the last label in the label stack before the L3 header. It is set to 1 for the last entry in the label stack (bottom of the stack) and 0 for all other label stack entries.
Time to Live (TTL)	8 bits	This field provides traditional IP TTL functionality within the MPLS network. The TTL field is used to prevent forwarding loops and is decremented by a value of 1 on every hop. For more information on MPLS TTL processing, see [RFC3031].
Experimental use (xEp)	3 bits	This field is used to define different classes of service (CoS) that will in turn influence the queuing and discard algorithms applied to the packet as it traverses the MPLS network.

MPLS-TP Shim Header Fields	Length	Description
Label Value	20 bits	This field defines the actual value of the label used, which can range from 0 to 1,048,575 (2^{20}–1). Just like Frame Relay's DLCI, ATM's VPI/VCI, a label typically has only local significance and changes on every hop. Not only do globally unique labels limit the number of usable labels, but they are also difficult to manage.

Figure 3-13. MPLS header fields [24].

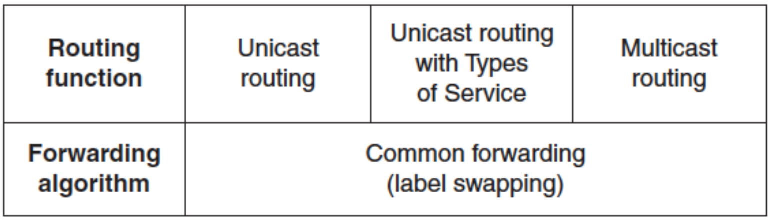
The difference between conventional routing architecture and label switching forwarding architecture is that the former uses multiple forwarding algorithms with its forwarding component (figure 3-14).



Routing function	Unicast routing	Unicast routing with Types of Service	Multicast routing
Forwarding algorithm	Longest match on destination address	Longest match on destination + exact match on Type of Service	Longest match on source address + exact match on source address, destination address, and incoming interface

Figure 3-14. Conventional Routing Architecture [23].

On the other hand, label switching algorithm consists of just one algorithm which is based on label swapping (figure 3-15).



Routing function	Unicast routing	Unicast routing with Types of Service	Multicast routing
Forwarding algorithm	Common forwarding (label swapping)		

Figure 3-15. Label Switching Architecture [23].

MPLS label switching forwarding component supports also the LSPs to be nested and tunneled. This is useful for allowing many LSPs to be forwarded in the same way inside the core network and at the edge nodes to present them as individual entities. This technique improves the manageability of connections across the network. One example of this technique is presented in figure 3-16, which is consisted of hosts, LSRs and one tunnel between LSR W and LSR Z. This protocol which is used on these two LSRs (LSR W and LSR Z) can be presented as a virtual protocol and make forwarding adjacencies between them. The result of this is the allowance of the other LSPs to be tunneled through these trunk LSPs when they step from one LSR to the next. The most easy way is to install a tunnel LSP as an interface between LSR W and LSR Z and to turn it as a virtual link [23].

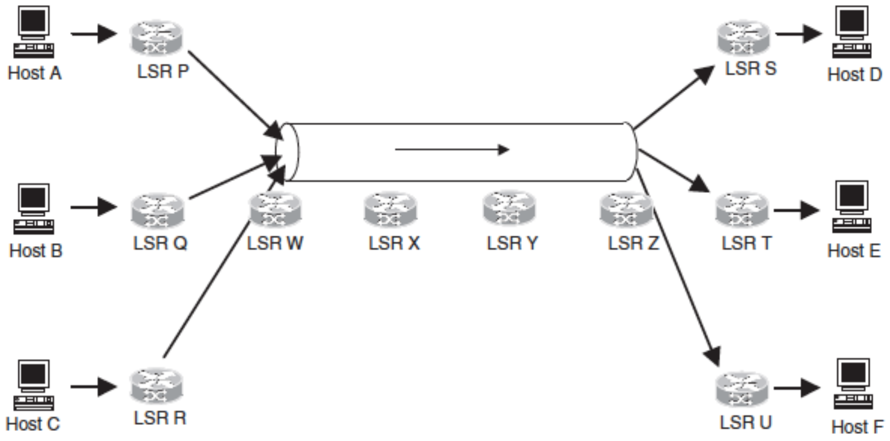


Figure 3-16. LSP tunnel between two LSRs (LSR W and LSR Z) carries multiple LSPs [23].

Its packet assigns only one label header entry. It is possible also additional label header entries may be assigned to packets and are organized as a last-in, first-out buffer by MPLS applications like IP VPNs. This buffer, the last in, first-out is referred to as an MPLS label stack [25]. When a packet enters the tunnel at LSR W (figure 3-16), the label is replaced but is added another label header entry on a packet. This example has packet's label stack depth three which is consisted of top label header entry, label header entry and bottom label header entry (figure 3-17). The top label header entry is used to send packets from LSR W to LSR Z.

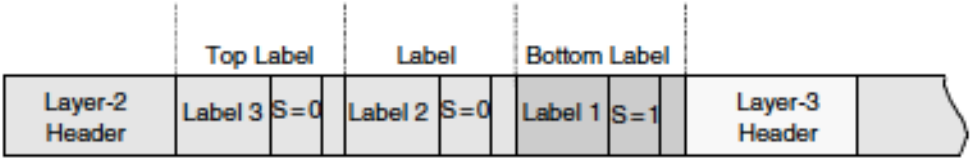


Figure 3-17. Label stack hierarchy [24].

By examining the top label header entry of an incoming packet each LSR along the LSP can examine two fields:

- ◉ The following task that is going to do. Each LSR can replace the label entry at the top of the label stack with a new label, remove the label entry or swap the label entry and add one or more label entries onto the label stack.
- ◉ LSRs can examine the next hop to which the packet is to be forwarded.

Finally, the last header which is the bottom label header entry, when it has the stack bit set, it indicates that it is the bottom of the stack. Finally, at LSR Z in figure 3-17, the top label is popped from the stack, revealing the label of the tunneled LSP [23][24].

3.3.1.2 MPLS-TP Label Switching Control Component

The control component of the MPLS-TP label switching has some responsibilities which are:

- ◉ Routing information distribution between LSRs.
- ◉ Routers use to convert this information into a forwarding table and to be used by the label switching forwarding table.

MPLS-TP label switching control component has many similarities with the conventional component of routing architecture. All the routing protocols which are used by the conventional control component routing architecture are included in the MPLS-TP label switching control component. On the other hand, the conventional routing architecture is not able to support label switching. The structure of the MPLS-TP label switching control component is presented in figure 3-18 below [23][24].

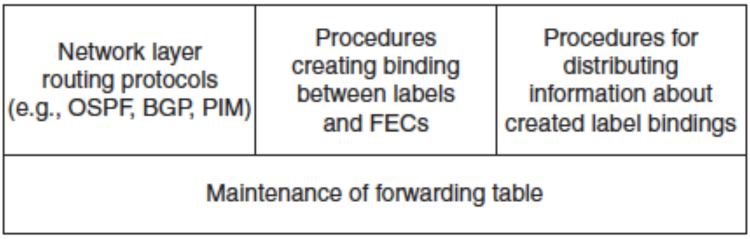

Network layer routing protocols (e.g., OSPF, BGP, PIM)
Procedures creating binding between labels and FECs
Procedures for distributing information about created label bindings
Maintenance of forwarding table

Figure 3-18. Structure of MPLS-TP label switching control component [23][24].

Network layer routing protocols provide to LSRs mapping between FECs and next hop addresses. Procedures for creating label binding between FECs and labels, and distribution this binding information between label switches are done by providing to LSRs with the mapping between FECs and labels [24]. These mappings are combined to provide the information needed to construct forwarding tables and to be used finally by the label switching forwarding table. This procedure is described in figure 3-19.

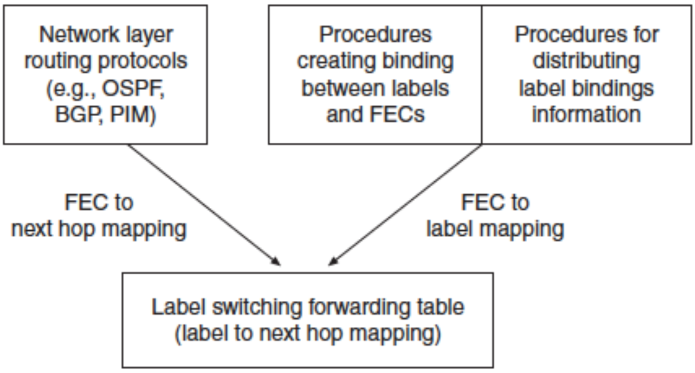

Network layer routing protocols (e.g., OSPF, BGP, PIM)
Procedures creating binding between labels and FECs
Procedures for distributing label bindings information
FEC to next hop mapping
FEC to label mapping
Label switching forwarding table (label to next hop mapping)

Figure 3-19. Mapping combination for construction of label switching forwarding table [23].

Each entry in a forwarding table maintained by an LSR contains one incoming label and one or more outgoing labels. For this reason, the label switching control component provides two types of label bindings. The first type of label binding is called per-interface basis and label bindings can be associated with an interface. A per-interface label space is a separate pool of label values defined for each interface on which the MPLS is enabled and unique labels are assigned to an FEC. The second type is called per-platform basis and label bindings can be associated this time with the router as a whole. The label space in per-platform type is a single global poll of label values defined from the entire router. However, in per-platform basis, a platform unique label is assigned to any particular FEC and announced to all neighbors. This unique label can be used on any interface but also labels that are assigned to different FECs cannot have the same value [23][24]. Label switching control component uses both ways, per-interface basis and per-platform basis to populate its forwarding table with incoming and outgoing labels. There are two ways to achieve this. The first one is when labels from the local binding are used as an incoming labels and labels from remote binding are used as outgoing labels. The second one is exactly the opposite way. When labels from the local binding are used as outgoing labels and remote binding are used as incoming labels [23].

Terms like downstream and upstream are refereed to a particular FEC. Generally, packets that are bound for a particular FEC travel from upstream LSR to the downstream LSR. An example of this is presented in figure 3-20 below. From the downstream point of view, for FEC-2, LSR Aeolus-R11 is a downstream neighbor of LSR Iris-R12, and LSR Iris-R12 is the downstream neighbor of LSR Kastor-R13. Furthermore, for FEC-1, LSR Kastor-R13 is the downstream neighbor of LSR Iris-R12, and LSR Iris-R12 is the downstream neighbor of LSR Aeolus-R11. All of these LSRs learn about their downstream neighbors through the IP routing protocol.

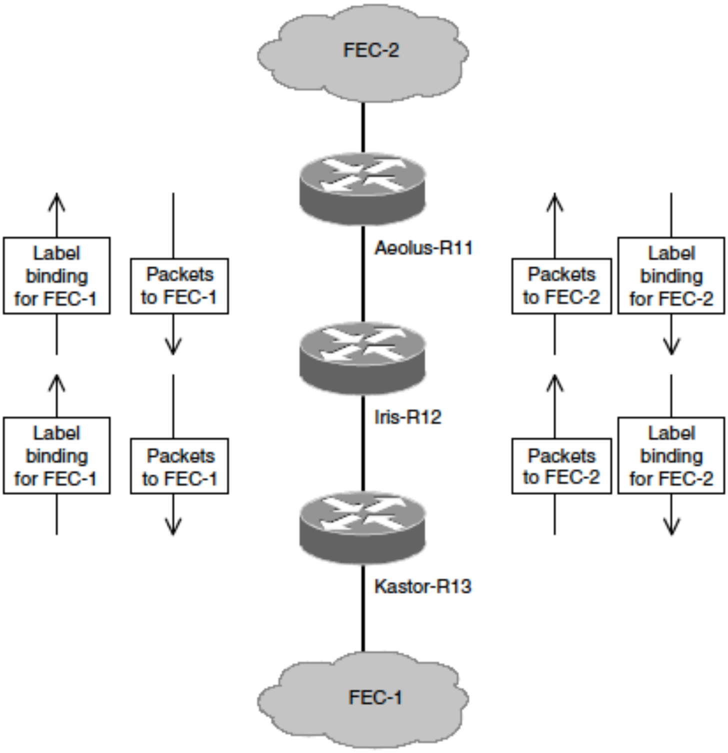


Figure 3-20. Different FECs in Upstream and Downstream LSRs [23].

From the upstream point of view, for FEC-2, LSR Kastor-R13 is the upstream neighbor of LSR Iris-R12 and LSR Iris-R12 is the upstream neighbor of LSR Aeolus-R11. The same is also for FEC-1, which LSR Iris-R12 is the upstream neighbor of LSR Kastor-R13 and LSR Aeolus-R11 is the upstream neighbor of LSR Iris-R12 [23].

There are two techniques that the LSR can distribute label bindings. The first one is the downstream on demand label distribution and the second is called downstream unsolicited label distribution. In the first technique, an LSR requests a label binding for a particular FEC for each downstream next hop and the downstream neighbor distributes the label upon request. As it concerns the downstream unsolicited label distribution, an LSR distributes bindings to other LSRs that they have not made a request. In this situation the label for an FEC is asynchronously allocated and advertised to all neighbors, whether the neighbors are upstream or downstream LSRs for a particular FEC [24].

3.3.2 MPLS-TP Section Entity

Another forwarding data plane transport entity that the MPLS-TP has is called section entity. Two MPLS-TP LSRs are considered to be topologically adjacent at layer n of the MPLS-TP LSP hierarchy if there is a link between them at the next lowest network layer. Figure 3-21 describes a network topology with LSRs or traditional routers and LSPs. LSR-A sends packets to LSR-B via LSPs. These LSPs are consisted of normal routers or LSRs. It is possible some packets to follow the first path which is via router-1, router-2, router-3 and finally LSR-B. Another path that packets follow is via router-1, router-4, router-5, router-6, router-3 to reach the destination which is LSR-B. The lowest network layer consists of routers which have the ability to forward packets based on labels (label header is included) - when router are LSRs and based on destination address only (network layer header only). These routers can support also not only other technologies like Ethernet but also MPLS and MPLS-TP technologies.

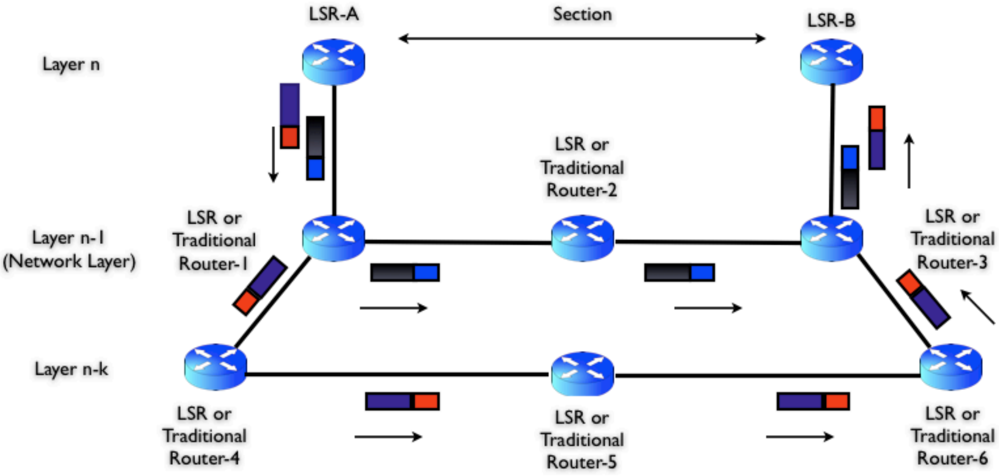

LSR-A
Section
LSR-B
Layer n
LSR or Traditional Router-2
Layer n-1 (Network Layer)
LSR or Traditional Router-1
LSR or Traditional Router-3
Layer n-k
LSR or Traditional Router-4
LSR or Traditional Router-5
LSR or Traditional Router-6

Figure 3-21. Example of section between two LSRs.

For this reason, links are traversed by a layer n-k MPLS-TP are layer n MPLS-TP sections. The MPLS label stack is associated with an MPLS-TP section at layer n and consists of n labels because the MPLS-TP does not support the penultimate hop popping (PHP) [22].

3.3.3 MPLS-TP Pseudo-Wire Entity

The last forwarding data plane transport entity that the MPLS-TP has is called pseudo-wire entity. MPLS-TP supports single-segment pseudo-wires [26], multi-segment pseudo-wires [27], and point to multipoint pseudo-wires [28].

Generally, a pseudo-wire is an emulation of a layer 2 point to point connection oriented service over a packet-switched network (PSN). The pseudo-wire emulates the operation of a transparent wire carrying a service like MPLS and IP protocol over a Packet -Switched Network (PSN) [26]. Figure 3-22 below presents the logical protocol layering model which is consisted of eight layers (payload, encapsulation, PW demultiplexer, PSN convergence, PSN, data-link and physical layer). This model is intended to minimize the differences between PWs operation over different PSN types.

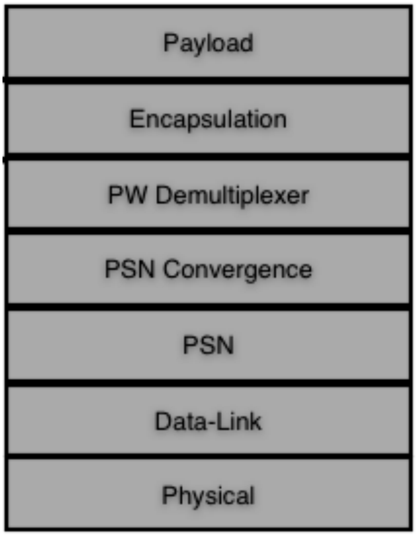


Figure 3-22. Logical Protocol Layering Model [26].

The encapsulation layer, carries any information that is needed by the PW Customer Edge (CE)-bound Provider Edge (PE) interface to send the payload to the CE via the physical interface. Furthermore, the PW demultiplexer layer has the ability to deliver multiple PWs over a single PSN tunnel. The next layer is called PSN convergence and is responsible for providing the enhancements that are needed to make the PSN conform to the assumed PSN service requirement. Mainly, it makes the PW independent of the PSN type [26].

3.3.3.1 MPLS-TP Single-Segment Pseudo-Wires

The MPLS-TP single-segment pseudo-wires is consisted of two Provider Edges (PEs) which have to provide one or more PWs (PW1, PW2) to their Customer Edges (CEs) to enable the clients to communicate between them over the Packet Switched Network (PSN). An example of this model is provided in figure 3-23. Furthermore, a MPLS-TP tunnel is established to provide a data path for the PWs. As it concerns the PW traffic, it is invisible to the core network and also the core network is transparent to the CEs. Packets that arrived via the interfaces between CE1 and PE1 are encapsulated in a Pseudo-Wire Protocol Data Unit (PW-PDU), and then are carried across the underlying network via the MPLS-TP tunnel. PE1 performs the appropriate encapsulation of the PW-PDUs and also the decapsulation is provided by the PE2 [26] [27].

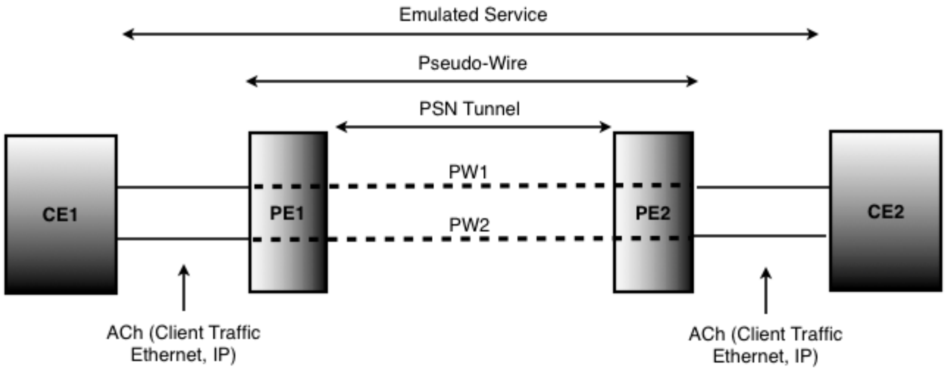

Emulated Service
Pseudo-Wire
PSN Tunnel
PW1
PW2
CE1
PE1
PE2
CE2
ACh (Client Traffic Ethernet, IP)
ACh (Client Traffic Ethernet, IP)

Figure 3-23 . Network Reference Model for point to point PWs [26].

The protocol layering for PWE3 over an MPLS PSN is provided in figure 3-24. Here, the encapsulation layer is divided into three sub-layers which are the payload convergence, timing and sequencing. A control word is used to carry most of the information needed by the PWE3 encapsulation layer. The sequence sub-layer, provides support for both in order payload delivery and a PSN fragmentation service within the PSN convergence layer. Furthermore, an inner MPLS label is used to provide the PW demultiplexing function. The ability of PW demultiplexer layer is to allow multiple PWs to be carried in a single tunnel. This is a good technique for minimizing the complexity of the network and conserving resources [26].

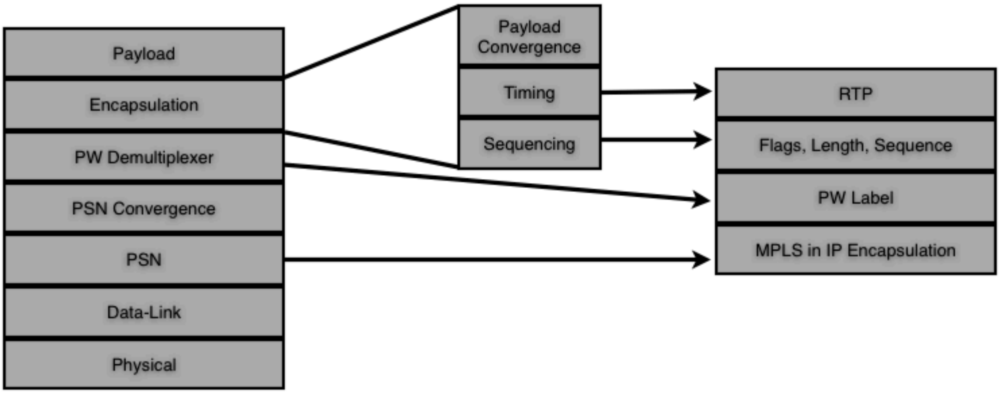


Figure 3-24. PWE3 over an MPLS Packet Switched Network (PSN) using a control word [26].

3.3.3.2 MPLS-TP Multi-Segment Pseudo-Wires

MPLS-TP Multi-Segment Pseudo-Wire (MS-PW) is a set of two or more contiguous PW segments statically or dynamically configured that behave and function as a single point to point pseudo-wire. Each multi-segment pseudo-wire terminates on a terminating provider edge T-PE. When a pseudo-wire segment follow a path of a Packet Switched Network (PSN) tunnel between Switching Provider Edge S-PE, the MS-PW is independent of the PSN tunnel routing [27].

The MS-PWs are applicable to all PW payload types. If each segment of MS-PW are identical in a PSN, then the PW types of each segment must also be identical. If different segments run over different PSN types, the encapsulation may change but the PW segments must be of an equivalent PW type [26][27]. Figure 3-25 presents the Multi-Segment Pseudo-Wire (MS-PW) reference model. Provider Edge 1 (PE1) and

Provider Edge 2 (PE2) provide services to Customer Edge 1 (CE1) and Customer Edge 2 (CE2) which are refereed as Terminating Provider Edge 1 (T-PE1) and Terminating Provider Edge 2 (T-PE2) respectively. There are two Packet Switched Network (PSN) tunnels which the first is extended from T-PE1 to Switching Provider Edge 1 (S-PE1) across PS1 and the second is extended from S-PE1 to T-PE2 across PSN2. The job of pseudo-wires is to connect the Associated Channels (AChs) which are attached to PE1 to the corresponding AChs attached to T-PE2. PW segments on PSN1 tunnel are switched to PW segments on PS2 tunnel at S-PE1 to complete the MS-PW between T-PE1 and T-PE2. The S-PE1 is refereed as PW switching point. An example of this, is that PW segment 2 and PW segment 4 belong to the same MS-PW while PSN1 and PSN2 tunnels are different or same PSN types. However, PW segment 1 and PW segment 3 belong to another MS-PW and should have the same PW types. In this example, there is only one S-PE but it is possible for a PW to transit more than one S-PE along this path [26].

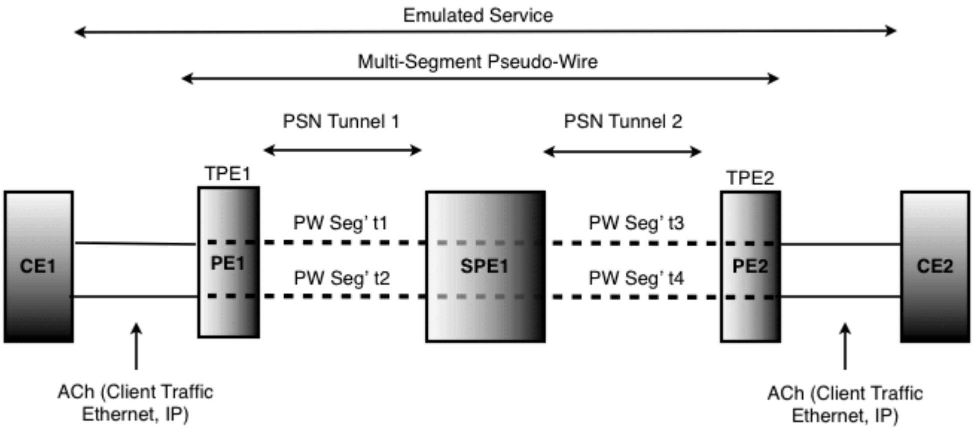


Figure 3-25. MS-PW Reference Model [27].

The MPLS-TP multi-segment pseudo-wire (MS-PW) is consisted of two models which are intra-provider connectivity architecture and inter-provider connectivity architecture.

As it concerns the first model, there is a requirement to deploy PWs edge to edge in large service provider networks. These networks are comprised by hundreds of aggregation devices at the edge side. It is possible the partitioning of this network into smaller networks and core PW domains where the PEs are interconnected by tunnels. The MS-PW reference model in figure 3-25 can be used for intra-provider connectivity architecture with PSN1 and PSN2 to belong to different administrative domains or access, core and metro regions with the same provider's network. There is the possibility PSN1 and PSN2 be a different types. For this reason, the S-PEs are used to connect PW segments of one technology with PW segments of different technology [27]. Furthermore, the intra-provider connectivity architecture uses Associated Channels (AChs) and also Pseudo-Wires (PWs). For the Associated Channels (AChs), the PWs reverts to the native service at the domain boundary PE. This ACh is connected to a separate PW on the same PE. On the other side, PW segments are switched between PSN tunnels of the provider's network without reverting to the native service at the boundary.

The second model is called inter-provider connectivity architecture and PWs can be switched between PSN tunnels at the provider boundary in order to minimize the number of tunnels required to provide PW-based services to CEs to each provider's network. The inter-provider connectivity architecture also supports both AChs and PWs. The inter-provider based on AChs, reverts the PW to the native service at the provider boundary PE. The ACh is connected to a separate PW at the peer provider PE. However the inter-provider architecture which uses PWs is provided in figure 3-26 below, and switches the PW segments between PSN tunnels in each provider's network without reverting to the native service. In this model there are two S-PEs, S-PE1 and S-PE2 which are the provider boarder routers. Here, the PW segment 1 is switched to PW segment 2 at S-PE1. Then the PW segment 2 is carried across an inter-provider PSN tunnel to S-PE2 and is switched to PW segment 3 in PSN2 [27].

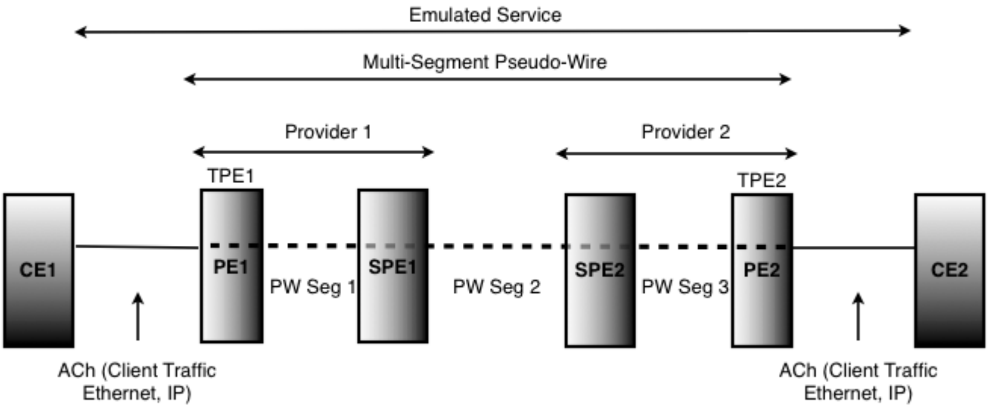

Emulated Service
Multi-Segment Pseudo-Wire
Provider 1
Provider 2
TPE1
TPE2
CE1
PE1
SPE1
SPE2
PE2
CE2
PW Seg 1
PW Seg 2
PW Seg 3
ACh (Client Traffic Ethernet, IP)
ACh (Client Traffic Ethernet, IP)

Figure 3-26. MS-PW Inter-Provider Reference Model [27].

3.3.3.3 MPLS-TP Point to Multipoint Pseudo-Wires

An MPLS-TP Point to Multipoint (P2MP) Pseudo-Wire (PW) is a mechanism that emulates the essential attributes of a P2MP Telecommunications service. The usability of a P2MP PW is to deliver a non-IP multicast service that carries multicast frames from a multicast source to one or more multicast receivers. The MPLS-TP P2MP-PW has some functions which are the encapsulation of service specific PDU which is arrived at an ingress Associated Channel (ACh), and carrying them across a tunnel to one or more egress AChs and managing their timing and order. Furthermore, the MPLS-TP P2MP-PW is divided into two categories. The first one is called MPS-TP Point to Multipoint (P2MP) Single Segment Pseudo-Wire (SS-PW) and the second is the MPS-TP Point to Multipoint (P2MP) Multi Segment Pseudo-Wire (MS-PW) [28].

MPLS-TP Point to Multipoint (P2MP) Single Segment Pseudo-Wire (SS-PW) is a single segment P2MP PW set up between the PE attached to the source and the PEs attached to the receivers. It is relied on P2MP LSP as PSN tunnel. On the other hand, MPS-TP Point to Multipoint (P2MP) Multi Segment Pseudo-Wire (MS-PW) represents an end to end PW segmented by S-PEs. Each of these segments can rely on either P2P LSP or P2MP LSP as PSN tunnel [27][28].

Figure 3-27 below, presents the P2MP SS-PW reference model. Here, it provides a point to multipoint connectivity from a root PE (PE1) which is connected to source (CE1) to the leaf PEs (PE2, PE3, PE4) which are connected to different receivers (CE2, CE3, CE4). In this model, each single copy of PW packet is sent over the P2MP PSN tunnel and is received by all leaf PEs. However, between PE1 and leaf PEs there is a P router which is joining P2MP PSN tunnel operation but is not participating in the signaling of P2MP PW. The P2MP PW is unidirectional but there is a requirement for root PE to receive unidirectional P2P traffic from leaf PEs. It could be also supported bidirectional connectivity between them [28]. For example, for upstream, point to point which any leaf PE sends traffic to root PE and for downstream, point to multipoint which the root PE sends traffic to any leaf PE.

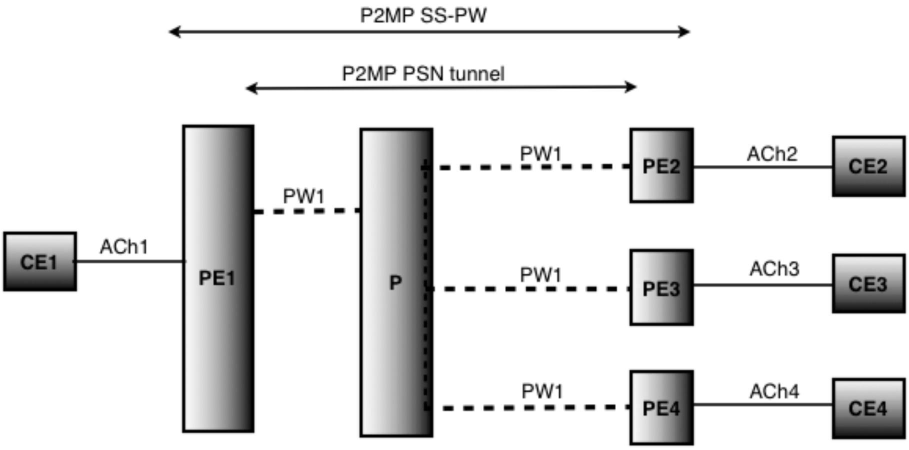


Figure 3-27. P2MP SS-PW Reference Model [28].

The P2MP SS-PW underlaying layer is provided in figure 3-28 and is composed of one root PE and several leaf PEs which are PE1, PE2, PE3 and PE4. The P2MP PW can be supported by multiple P2MP PSN tunnels which must be able to serve more than one P2MP PW [27]. It is also possible P2MP tunnels to belong to different technologies like P2MP MPLS LSP or to have different setup protocols [28].

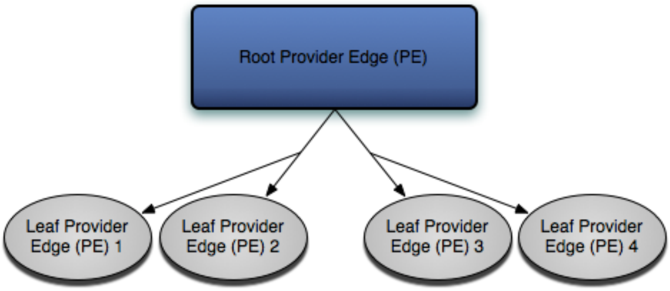

Root Provider Edge (PE)
Leaf Provider Edge (PE) 1
Leaf Provider Edge (PE) 2
Leaf Provider Edge (PE) 3
Leaf Provider Edge (PE) 4

Figure 3-28. P2MP Underlying Layer for P2MP SS-PW [28].

The MPS-TP Point to Multipoint (P2MP) Multi Segment Pseudo-Wire (MS-PW) is depicted in figure 3-29. In this reference model there are two S-PEs (S-PE1 and S-PE2) which are responsible to switch a MS-PW from one input segment to one or several output segments. In the figure below, TPE1 is the root and leaf TPEs are the TPE2, TPE3, TPE4 and TPE5. The leaf TPEs is assumed that they belong to the same PSN which is PSN2 but each PW output is located in a different PSN. However, the role of S-PE1 and SPE2 are used for switching simultaneously the input P2MP PW1 segment to the output P2P PW2, PW3 and PW4 segments. Another thing is that a PW segment belongs to a P2MP MS-PW can also be supported over a P2MP PSN tunnel or a P2P PSN tunnel [28].

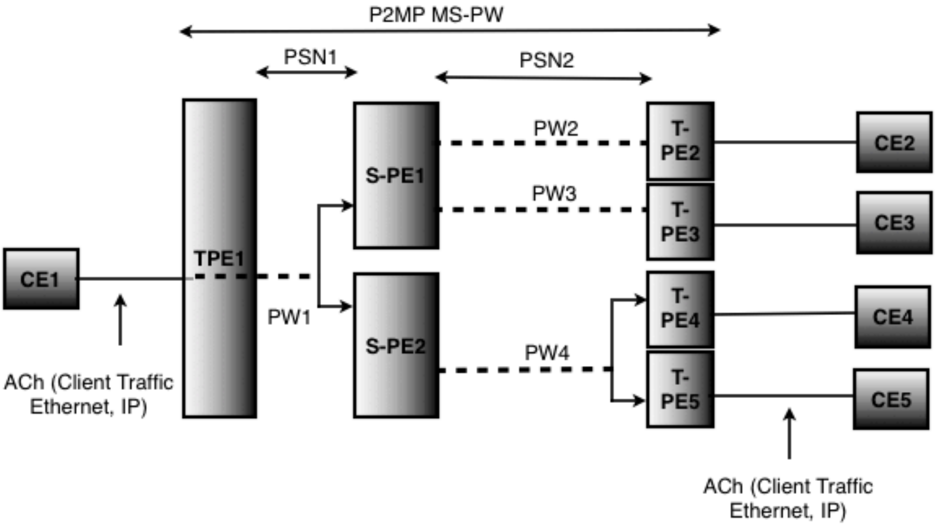


Figure 3-29. P2MP MS-PW Reference Model [28].

P2MP MS-PW topology relying on a combination of both P2P and P2MP LSPs as PSN tunnels is represented in figure 3-30. The PW tree is composed by the root PE, by the branch S-PEs which are S-PE1, S-PE2, S-PE3, S-PE4 and S-PE5 and by several leaf PEs (PE1, PE2, PE3 and PE4). In this case, the traffic replication along the path is performed at the PW level. An example is that the branch S-PE5 must replicate incoming packets which are received from S-PE2 and send them to leaf PE3 and PE4. In this figure, is also presented the case where each segment is supported over a P2P LSP except the S-PE1, S-PE3 and S-PE4 P2MP segment which is conveyed over a P2MP LSP [27][28].

Finally, the configuration of PW tree can be statistically at the PEs and each S-PE crossed. However, the PW tree can be also dynamically configured by allowing the MS-PW segments to be dynamically discovered [28].

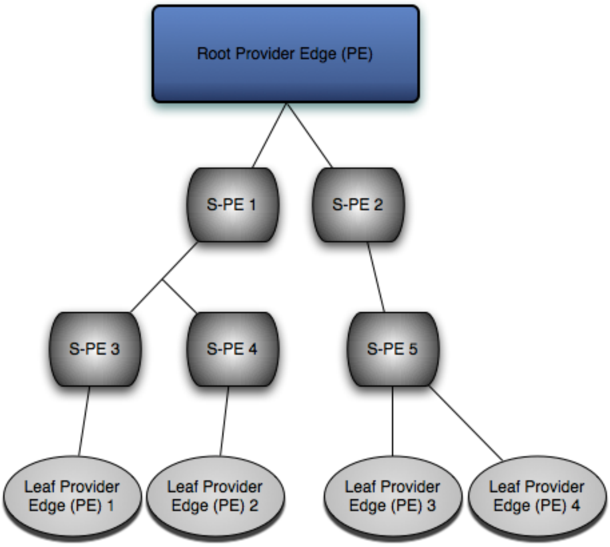

Root Provider Edge (PE)
S-PE 1
S-PE 2
S-PE 3
S-PE 4
S-PE 5
Leaf Provider Edge (PE) 1
Leaf Provider Edge (PE) 2
Leaf Provider Edge (PE) 3
Leaf Provider Edge (PE) 4

Figure 3-30. P2P and P2MP Underlying Layer for P2MP MS-PW [28].

3.4 MPLS-TP OAM Mechanisms

The MPLS-TP OAM mechanisms are applicable to both MS-PWs and LSPs and support co-routed, bidirectional P2P transport paths and unidirectional P2P and P2MP transport paths. MPLS-TP OAM operates in a context of Maintenance Entities (MEs) which are the relationship between two points of a point to point transport path or a root and a leaf point to multipoint transport path to which monitoring and maintenance operations apply. These two points, are called Maintenance Entity Group (MEG) End Points (MEPs). Between these two points there is a possibility to zero or more intermediate points to be existed which are called Maintenance Entity Group Intermediate Points (MIPs). The Maintenance Entity Group (MEG) is defined to monitor the transport path for fault and performance management. In case of associated bidirectional paths, two independent maintenance entities are defined to independently monitor each direction [29].

As it concerns the MEG End Points (MEPs), there are the source and sink points of MEG. For MPLS-TP LSP, only Label Edge Routers (LERs) can implement MEPs while for Path Segment Tunnel (PST), both LERs and LSRs can implement MEPs that contribute to the infrastructure of the transport path. On the other side, for MPLS-TP PW, only T-PEs can implement MEPs while for Packet Segment Tunnels (PSTs) supporting a PW both T-PEs and S-PEs can implement MEPs. The responsibilities of MEPs are to activate and control all the OAM functionalities for the MEG. They are also responsible for origination and termination of OAM messages for fault management and performance monitoring. [29]. A MEP of MPLS-TP transport path (LSP, PW, Section) coincides with transport path termination and monitors it for failures or performance degradation in an end to end scope. Furthermore, the MEPs of path segment tunnel are not necessarily coincident with the termination of the MPLS-TP transport path and monitor some portion of the transport path for failures or performance degradation only within the boundary of the MEG for the path segment tunnel. A MEP can only exist at the beginning and end of a sub-layer. For monitoring some portion of LSPs or PWs, a new sub-layer in the form of a path segment tunnel should be created which permits MEPs and an associated MEG to be created [29][30].

MEG Intermediate Point (MIP) is a point between the MEPs of an MEG. The capability of MIP is to react to some OAM packets and forward all the other OAM packets while ensuring fate sharing with data plane packets. Moreover, it does not initiate packets but is addressed by OAM packets initiated by one of the MEPs of the MEG. MIP is possible to generate OAM packets only in response to OAM packets that are sent on the MEG it belongs to [29].

The MPLS-TP OAM supports five Maintenance Entity Groups (MEGs) which are refereed below:

◉ Section Maintenance Entity Group (SME), between MPLS LSRs, for monitoring and management of MPLS-TP Sections.

- LSP Maintenance Entity Group (LME), between LERs, for monitoring and management of an end to end LSP.

- PW Maintenance Entity Group (PME), between T-PEs, for monitoring and management of end to end Single Segment/Multi Segment SS/MS-PWs.

- PST Maintenance Entity Group (PSTME), between LERs/LSRs along an LSP, for monitoring and management of a path segment tunnel.

- MS-PW Tandem Connection Maintenance Entity (PTCME), between T-PEs/S-PEs along the PW, for monitoring and management of a PW Tandem Connection.

The section Maintenance Entity Group (SME) can be configured on any MPLS section. It is used for monitoring the link between topologically adjacent MPLS LSRs rather than monitoring the individual LSP or PW segments traversing the MPLS section. More analytically, figure 3-31 provides different sections between different LSRs. For example, section 12 ME is associated with the MPLS section between LSR 1 and LSR 2. Furthermore, section 23, between LSR 2 and LSR 3, section 3X between LSR 3 and LSR X, section XY between LSR X and LSR Y and finally, section YZ between LSR Y and LSR Z [29].

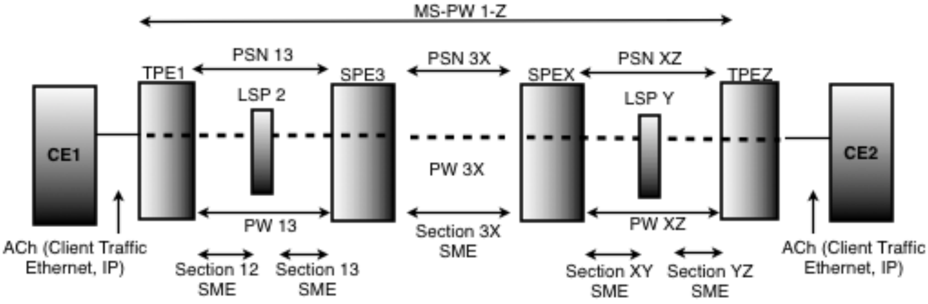


Figure 3-31. Example of MPLS-TP Section MEs (SME) [29].

The second group is called LSP Maintenance Entity Group (LME) and is intended to monitor an end to end LSP between two LERs. It is possible an LME to be configured on any MPLS LSP. However, LME is used in scenarios where it is desirable to monitor an entire LSP between its LERs. Figure 3-32 depicts the MPLS-TP LSP end to end monitoring. More specifically, it presents two LMEs configured in the path between CE1 and CE2. The first one is the PSN 13 LME between LER 1 and LER 3 and the second one is the PSN XZ between LER X and LER Y [29].

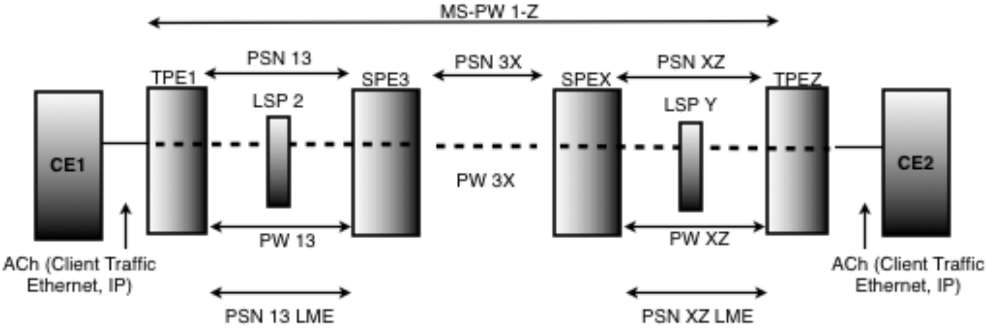


Figure 3-32. Example of MPLS-TP LSP MEs (LME) [29].

An MPLS-TP Path Segment Tunnel ME (LPSTME) is an MPLS-TP maintenance entity intended to monitor an arbitrary part of an LSP between a given pair of LSRs independently from the end to end monitoring (LME). An LPSTME can monitor an LSP segment and it can also include the forwarding engine of the node at the edge of the segment. It is used between the following entities: LER and any LSR of a given LSP and any two LSRs of a given LSP. Furthermore, it is used to monitor the behavior of a part of an LSP or set of LSPs rather than the entire LSP itself. Figure 3-33 gives an example of LPSTME. Here, there are two separate LPSTMEs which are configured to monitor the PSN 1Z LSP. The first LPSTME, monitors the PSN 13 LSP segment on domain 1 and the second one, monitors the PSNXZ LSP segment on domain Z [29].

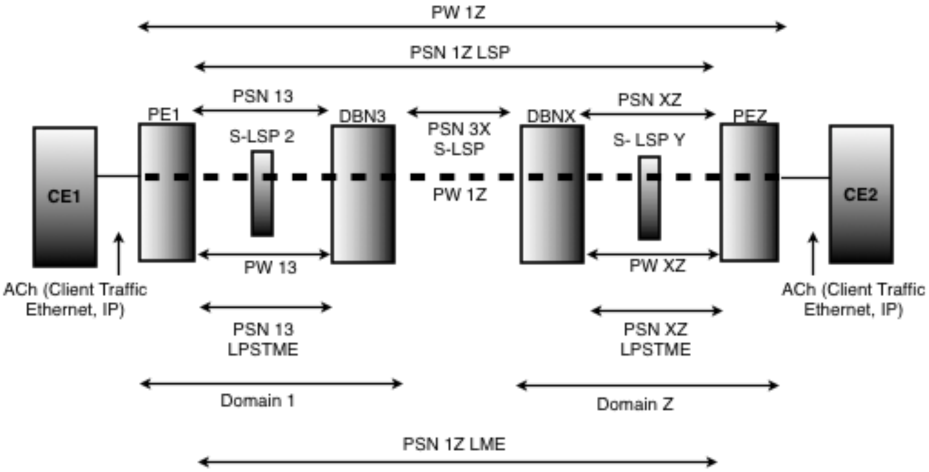


Figure 3-33. Example of MPLS-TP LSP Path Segment Tunnel ME (LPSTME) [29].

An MPLS-TP PW ME (PME) is intended to monitor a SS-PW and MS-PW between a pair of T-PEs. It is possible to be configured on any SS-PW or MS-PW. A PME is deployed in scenarios where it is desirable to monitor an entire PW between a pair of MPLS-TP enabled T-PEs rather than monitoring the LSP aggregating multiple PWs between PEs. Below, figure 3-34 presents a MS-PW (MS-PWIZ) which is consisted of three segments which are: PW13, PW3X and PWXZ [29].

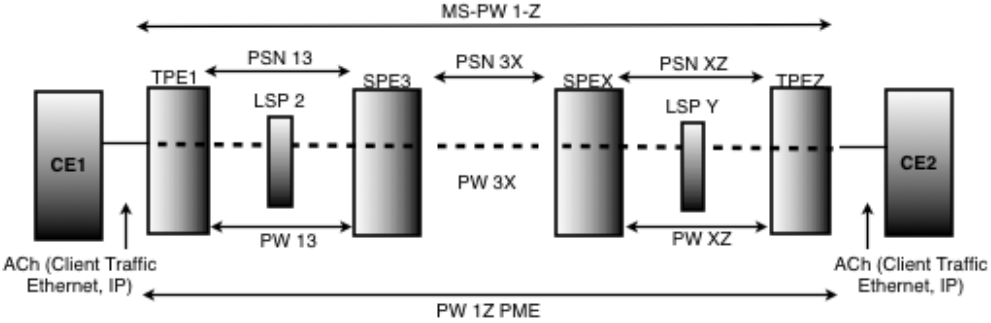


Figure 3-34. Example of MPLS-TP PW ME (PME) [29].

The last group is the MPLS-TP MS-PW Path Segment Tunnel Monitoring ME (PPSTME) which is intended to monitor an arbitrary part of an MS-PW between a pair of PEs independently from the end to end monitoring (PME). Multiple PPSTMEs is possible to be configured on any MS-PW and can be defined between the following entities which are between T-PE and any S-PE of a given MS-PW and any two S-PEs of a given MS-PW. In this scenario above (figure 3-35), there are two separate PPSTMEs configured to monitor fist the PW 13 MS-PW segment on domain 1 and second, the PW XZ MS-PW segment on domain Z [29].

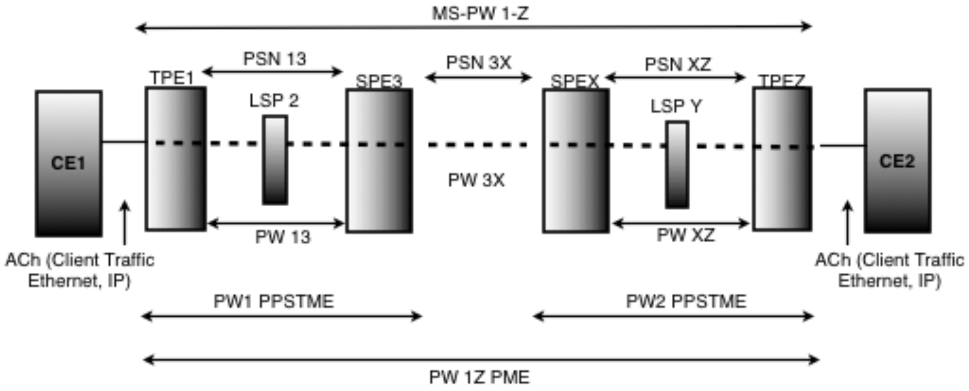


Figure 3-35. Example of MPLS-TP MS-PW Path Segment Tunnel Monitoring (PPSTME) [29].

The OAM mechanism has two functions for monitoring. The first is called proactive monitoring and the second is on-demand monitoring [29][30].

Proactive monitoring is refereed to OAM operations that are either configured to be carried out periodically and continuously or preconfigured for a certain events like alarm signals. It has some functions which are the connectivity check and connectivity verification. As it concerns the proactive connectivity check function, it is used to detect a Loss of Continuity Defect (LOC) between two MEPs in an MEG. On the other side, proactive connectivity verification function is used for detection an unexpected connectivity defect between two MEGs and also an unexpected connectivity within the MEG with an unexpected MEP [29][30].

When there is a bi-directional point to point transport path, a MEP is enabled to generate proactive CC-V OAM packets with a configured transmission rate, it also expects to receive pro-active CC-V OAM packets from its peer MEP at the same transmission rate as a common SLA applies to all components of the transmission path. On the other hand, in a unidirectional transport path, only a source MEP is enabled to generate CC-V OAM packets and only the sink MEP is configured to expect these packets at the configured rate. Furthermore, not only MIPs but also intermediate nodes do not support MPLS-TP OAM and are transparent to the proactive CC-V information and forward these proactive CC-V OAM packets as regular data packets. Applications that use proactive CC-V are fault management, protection switching and performance monitoring [29].

Proactive monitoring is possible to identify different defects with CC-V. Some of the defects are:

- Loss of continuity defect. The loss detection of continuity (LOC) defect by a sink MEP when it fails to receive proactive CC-V OAM packets from the peer MEP.
- Mis-connectivity defect. A sink MEP identifies a mis-connectivity defect when a proactive CC-V OAM packet is received, with its peer source MEP when the received packet carries an incorrect globally source MEP identifier.
- Period misconfiguration defect. If proactive CC-V packets are received with a correct unique source MEP identifier but with a transmission period different that the locally configured reception period, then a CV period misconfiguration defect is detected.

The other function is called on-demand monitoring and is initiated manually and for a limited amount of time usually for operations like diagnosis for investigation a defect condition. Fault management functions are performed by network management, which may invoke periodic on-demand bursts of on-demand CV packets. Another use of on-demand CV is to detect and locate a problem of connectivity when a problem is suspected or based on other tools. However it is based upon generation of on-demand CV packets that should uniquely identify the MEG that is being checked. On-demand CV can be used to check either an entire MEG or between MEP to a specific MIP. This function may not be available for bidirectional paths as the MIP may not have a return to the source MEP for the on-demand CV transaction [29][30].

3.5 MPLS-TP Control Plane

The MPLS-TP uses the Control Plane (CP) protocols for LSPs and PWs. It provides the following functions which are signaling, routing, Traffic Engineering (TE) and constraint-based path computation. Basically, a dynamic control plane is not required in an MPLS-TP because the same procedures are done by the management plane. Some requirements for control plane are [31][32]:

- The MPLS-TP control plane must be able to be operated independent of any particular client or server layer control plane.
- The MPLS-TP control plane should support control plane topology and data plane topology independence. In case of failure of the control plane, it does not affect any failure of the data plane.
- It should support the configuration and modification of OAM maintenance points as well as the activation and deactivation of OAM when the transport path or transport service is established or modified.
- It should support a large number of transport paths, for example node and links.
- Finally, it should support establishing all the connectivity patterns defined for the MPLS-TP data plane (unidirectional P2P, associated bidirectional P2P, co-routed bidirectional P2P, unidirectional P2MP) including configuration of protection functions and any associated maintenance functions.

MPLS-TP control plane is based on existing MPLS and PW control plane protocols. It requires that any signaling be capable of being carried over an out of band signaling network or a signaling control channel. Furthermore, the control planes for LSPs and PWs may be used independently and can be employed with out one each other. For this reason there are four scenarios which are [31]:

- A control plane is used for both LSPs and PWs.
- No control plane is employed.
- A control plane is used for LSPs but not for PWs.
- A control plane is used for PWs but not for LSPs.

For this reason, when client services are provided directly via LSPs, all requirements must be satisfied by the LSP control plane. On the other hand, when client services are provided via PWs, the PW and LSP control planes operate in combination and some functions are satisfied by PW control plane and some others by LSP control plane. Below in figure 3-36, is provided the relationship between the MPLS-TP control plane, forwarding plane, management plane and OAM for point to point MPLS-TP LSPs or PWs [31]. In this example, the NMS may be centralized or distributed but the control plane is distributed. Also the control plane may be transported over the server layer, an LSP or a G-ACh [31]. The control plane in this example is responsible for end to end, segment LSPs and PWs setup and modification, defines and determines primary and backup paths and finally configures the OAM function along the path. The role of OAM is to monitor and drive switches between primary and backup paths for path segments and end to end paths [31][33].

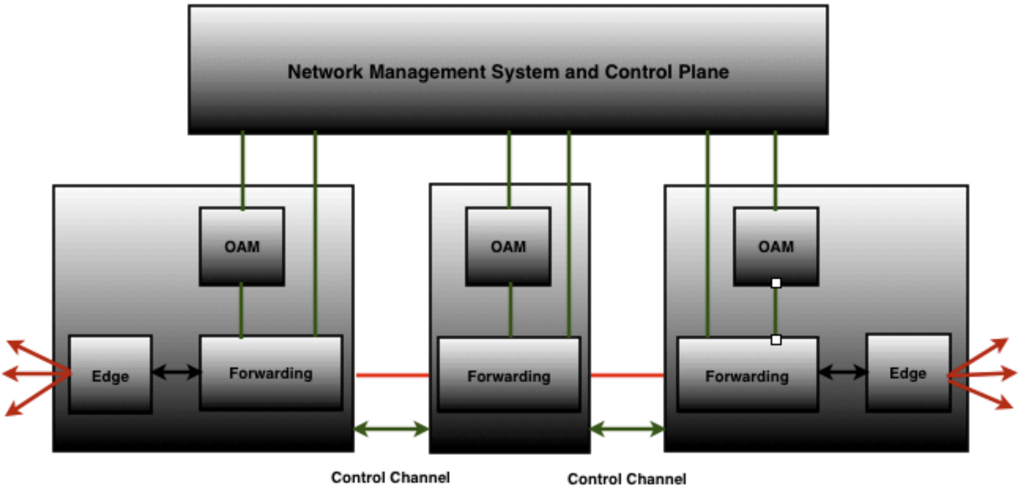
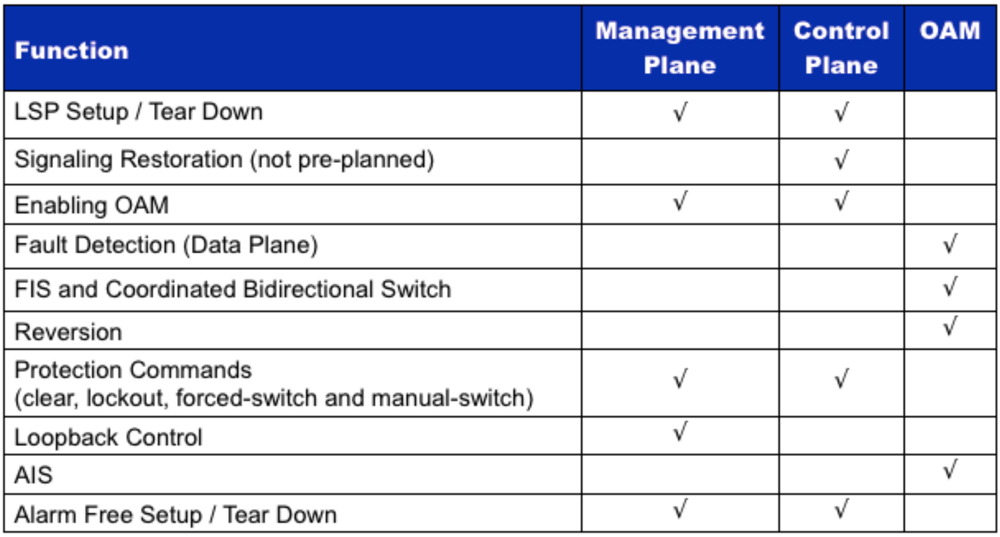


Figure 3-36. MPLS-TP Control Plane Architecture Context [31].

Finally, figure 3-37 below presents functions that are supported and not supported by the management plane, the control plane and OAM. Some of the functions like LSP setup, enabling OAM, protection commands and alarm setup are supported only from management plane and control plane [33].



Function	Management Plane	Control Plane	OAM
LSP Setup / Tear Down	√	√	
Signaling Restoration (not pre-planned)		√	
Enabling OAM	√	√	
Fault Detection (Data Plane)			√
FIS and Coordinated Bidirectional Switch			√
Reversion			√
Protection Commands (clear, lockout, forced-switch and manual-switch)	√	√	
Loopback Control	√		
AIS			√
Alarm Free Setup / Tear Down	√	√	

Figure 3-37. Different supported functions between Management plane, Control plane and OAM [33].

Chapter 4

Applying MPLS-TP in Opmigua Network

Some issues are derived, as it concerns GST and SM packets, when the MPLS-TP protocol is included in Opmigua network. Some of them are:

- Identification of GST and SM Packets.
- The compatibility of GST packets with MPLS-TP.
- A proposal of network scenario and how to configure GST and SM packets and paths into the Opmigua network.
- Protection scenarios of GST and SM paths into the Opmigua network.
- Scalability and compatibility of Opmigua network based on MPLS-TP with other networks.

4.1 Identification of GST and SM packets

As it was mentioned in the previous chapters, in Opmigua, the nodes transmit circuit and packet switched data on orthogonal polarization states on the same wavelength in a polarization and time division multiplexed (PolTDM) scheme. Packets are identified as SM and GST inside the node. Each node is consisted of some elements which are the Packet Separator (PS), Optical Packet Switch (OPS), Optical Cross Connect (OXC) and Packet Combiner (PC). Polarization Beam Splitters (PBSs) separate in a physical way the SM from GST packets at the input interface. A Packet Separator (PS) detects the QoS of incoming packets for each input wavelength and forwards the SM packets to OPS module and the GST packets to OXC module which have more priority that SM packets [6].

The integration of MPLS-TP protocol in the Opmigua network requires some functions for identification of GST and SM packets when are crossed between several nodes. The differentiation of SM packets from GST packets is that the former based on router forwarding table lookup and the MPLS label header, and the latter on the input interface which is known the destination output interface for each packet.

As it concerns the SM packets, are inserted by an Opmigua ingress node and follow a path to Optical Packet Switch (OPS) which are queued and statistically multiplexed. The OPS follows a traditional way for forwarding packets which is achieved by forwarding table lookup to find the next hop. With the integration of MPLS-TP protocol these routers are Label Switched Routers (LSRs) and assign a label with local significance to each packet that passes. More analytically, for the MPLS-TP label header is used the same header as the MPLS protocol uses, and is inserted between data-link layer 2 header and network layer 3 header. In figure 4-1, is presented the procedure of the LSR which takes the incoming packets, examine the network header to find the destination address, run through the forwarding table to do the longest and best match and finally, to forward the packet to the outgoing interface. Before the LSR sends the packet to the outgoing interface, an MPLS shim header is inserted between layer 2 and layer 3 header which includes the label value and is referred to the LSP between this and the next node.

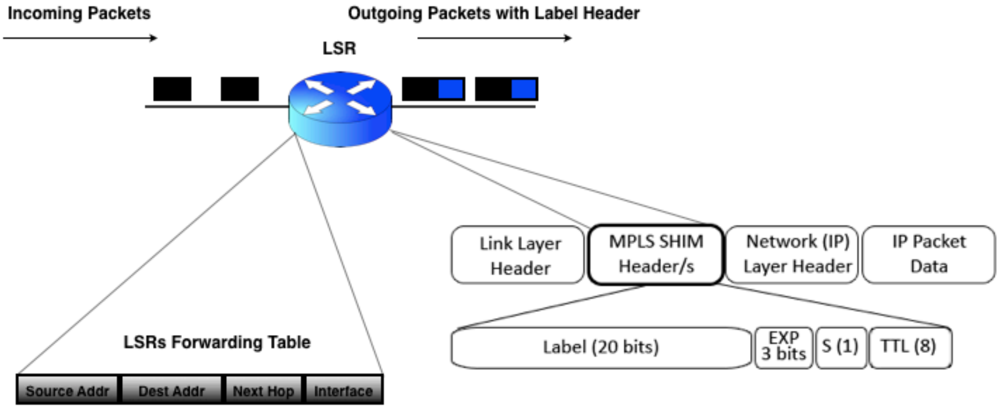


Figure 4-1. Example of LSRs table lookup and MPLS label assignment to each outgoing SM packets.

On the other hand, GST packets follow circuits which are wavelength paths of a WRON through the network. GST packets need absolute priority and this means that packets have no jitter and are not subject of contention. However, a path is possible to support more than one wavelength. Many nodes sharing a wavelength path, are allocated time-slots according to their bandwidth needs. Best effort traffic still accesses unused bandwidth in a statistical multiplexed way, enabling high bandwidth utilization. Next example below, provides (figure 4-2) one link supports wavelengths K1, K2 and K3 between nodes.

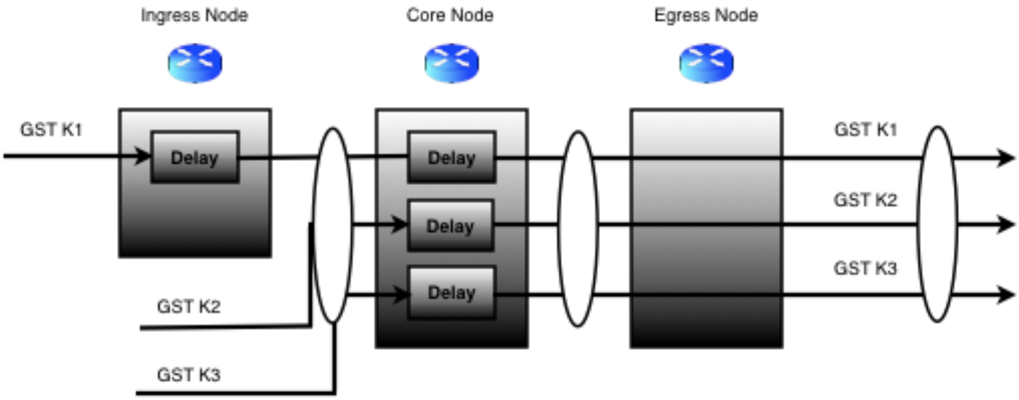


Figure 4-2. GST packets follow a path with three wavelengths K1,K2 and K3 with a small fixed delay.

In the previous example, GST packets follow a circuit switch path through the OXC network, from ingress to egress node, which is consisted of three wavelengths K1,K2 and K3 and there is a small fixed delay between each node. The reason that this delay is added, is that SM packets follow a path through the OPS network for further examination.

4.2 Compatibility of GST packets with MPLS-TP

As it was mentioned in the previous section, GST packets follow a circuit switch path inside a network. For this reason, the input interface knows where the packet is destined for (from the destination IP address) and is not examined by each node to find the next hop.

There are two proposals for being compatible a GST packet with MPLS-TP protocol in Opmigua network. Both of them use the Internet Protocol version 6 (IPv6). The first one uses an extension header which is the Destination Options header (DOH) and the second, the MPLS-TP shim header as an extension header. For achievement of these proposals, GST packets should take at the ingress node of the Opmigua network a label with global significance value until to reach the destination.

As it concerns the fist and the second proposal, a GST packet could be compatible with the MPLS-TP protocol when the Internet Protocol Version 6 (IPv6) is used. In IPv6, the new concept of extension headers is introduced. These headers take the place of many of the predefined IPv4 options. Options, allow the IPv6 datagram to be supplemented with arbitrary sets of information that are not defined in the regular extension headers. They provide maximum flexibility, allowing the basic IPv6 protocol to be extended in ways the designers never anticipated, with the goal of reducing the chances of the protocol becoming obsolete [34]. Optional headers can be placed between the IPv6 header and the upper layer header in a packet. It is possible an IPv6 packet to carry zero, one or more extension headers. Figure 4-3 presents an IPv6 packet with only one extension header.

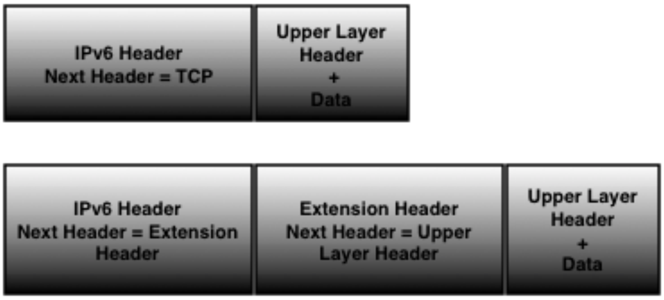

IPv6 Header
Next Header = TCP
Upper Layer Header + Data
IPv6 Header
Next Header = Extension Header
Extension Header
Next Header = Upper Layer Header
Upper Layer Header + Data

Figure 4-3. Example of one IPv6 extension header [34].

One exception, is that extension headers are not examined or processed by any node along a packet's delivery path, until the packet reaches the destination node. There are two types of extension headers which are the hop by hop options header and Destination Options Header (DOH) [34]. For the first proposal, it is used the Destination options header which can be contained options that are intended only to the destination node and is not examined by other nodes. Figure 4-4 presents how a label with global significance value is inserted inside the destination options header of IPv6 packet. The destination options header is consisted of three fields which are next header (8bits), header length (8bits) and options with variable length. Next header field identifies the type of header which is followed by the destination options header and it uses the same values as the IPv4 protocol field. Header length field presents the length of the destination options header in 8-octet units. Last field the options contains more than one TLV-encoded options [34]. The global significance label value uses one bit and could be inserted from the ingress node and to remain unchanged with a unique value until to reach the destination node.

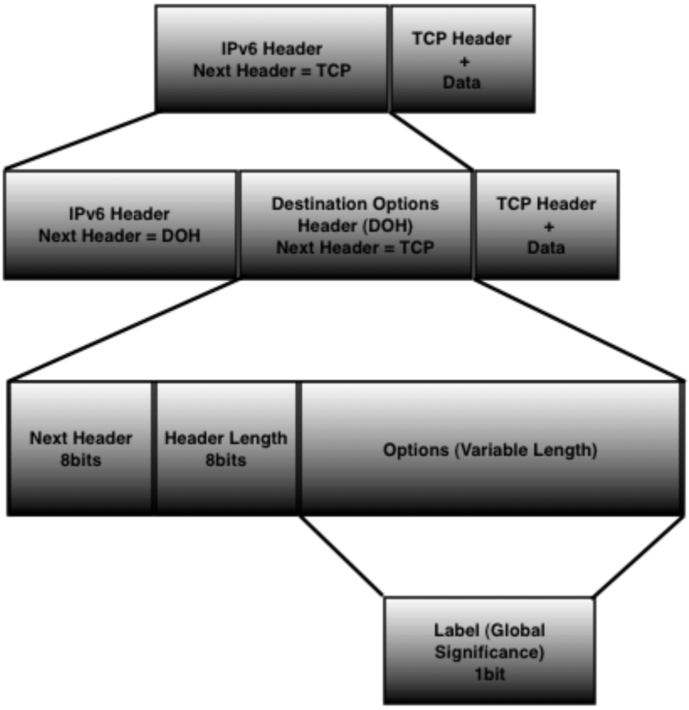


Figure 4-4. Example of global significance label into the destination options header of IPv6 packet.

Second proposal, for the compatibility of GST packets with MPLS-TP protocol as it concerns the IPv6 packet header is that the extension header that is used could be possible be an MPLS-TP shim header. Figure 4-5 presents the fields of MPLS-TP shim header but the label field has also global significance and it remains the same until to reach the destination node.

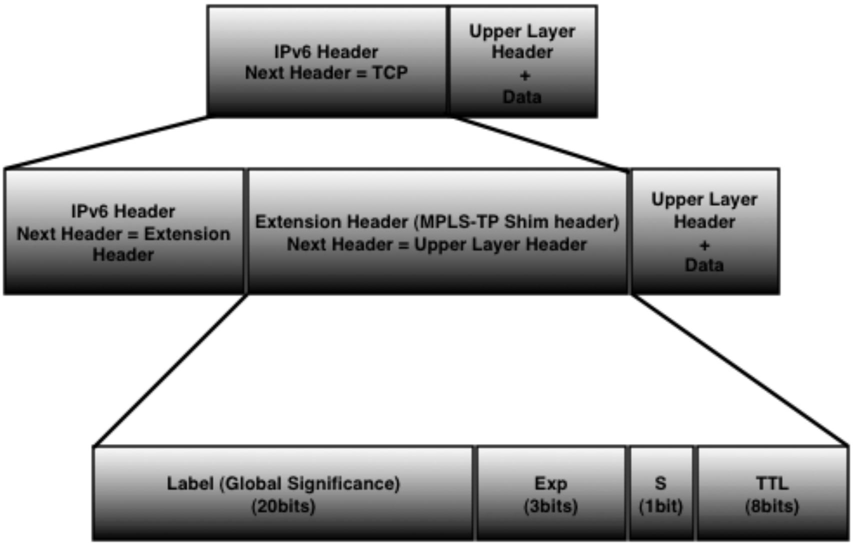

IPv6 Header
Next Header = TCP
Upper Layer Header + Data
IPv6 Header
Next Header = Extension Header
Extension Header (MPLS-TP Shim header)
Next Header = Upper Layer Header
Upper Layer Header + Data
Label (Global Significance) (20bits)
Exp (3bits)
S (1bit)
TTL (8bits)

Figure 4-5. A global significance label into MPLS-TP shim header of IPv6 packet.

For implementation of these proposals that are refereed above, network engineers should also count different consequences. For example, the Opmigua network could be inter-connected with network providers which is unknown or known the topology of their networks and use compatible or incompatible framing technologies (leased lines, MPLS). It could be also inter-connected one Opmigua network with another Opmigua via a third Opmigua network. Its provider uses its own framing techniques and for this reason the best solution for compatibility problems is the tunnel technique. With tunneling, core network which could be another provider or Opmigua network, encapsulates all the traffic into provider's frame and adds an extra header. As a result of this, protocols like MPLS-TP and network protocols (IPv4 - option fields, IPv6 extra headers) are transparent to core networks. MPLS-TP protocol supports this tunnel techniques and is used by many network providers these days. More analysis about tunnel framing technique in Opmigua networks is provided in 4.5 section.

4.3 GST and SM paths Configuration into Opmigua

In this section are presented seven different network schemes into an Opmigua network and the way how SM and GST packets and paths are configured. The seven different schemes are:

- One input interface in ingress Opmigua node with low and high priority (tagged as SM and GST respectively) packets together. Here, the GST packets have the same destination IP address and take the same global significance label.
- One input interface in ingress Opmigua node with also low and high priority (tagged as SM and GST respectively) packets together. The difference from the previous is here GST packets have different IP destination addresses and the result is different global significance labels per packet.
- Two input interfaces in ingress Opmigua node. One interface with high priority packets which are tagged as GST packets (same or different IP destination address) and one interface with low priority packets (tagged SM packets).
- Two input interfaces in ingress Opmigua node. Both interfaces only with high priority packets which are tagged as GST packets (same or different IP destination address).
- One input interface in ingress Opmigua node which receives only packets with low priority (like SM packets) follows GST paths when there are not any GST packets which need high priority.
- Two input interfaces in ingress Opmigua node. One interface receives low priority packets and are tagged as GST low priority packets and a second input interface with few high priority packets (tagged as normal GST packets). Both of them follow GST paths.
- Two input interfaces in ingress Opmigua node. One interface receives high priority packets (tagged as GST packets) and always follow GST paths and a second input interface, which receives low priority packets and are tagged as SM packets or low priority GST packets following a SM and GST paths respectively.

The main issue in this part is how the configuration of GST and SM paths could be established and how the GST and SM packets travel between nodes until to reach the destination node. Figure 4-6 provides an Opmigua network into domainA and presents how the GST and SM packets travel into the internal domain. A wavelength channel from one node to the next contains wavelength-routed circuit switched packets (GST).

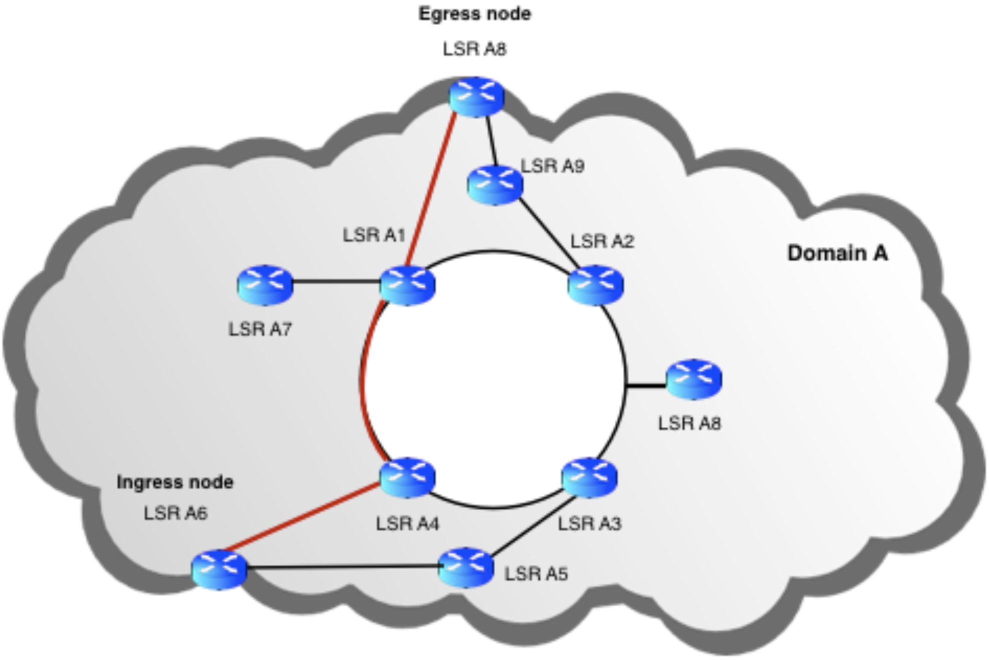


Figure 4-6. Internal Opmigua network (domain A).

The management of this network could be based on MPLS-TP management which support multi-layered distributed management systems. The lowest layer of this organization model includes the MPLS-TP network nodes which are node A1 to node A9. The management support is provided by the Management Application Function (MAF) within the nodes and the Operations System (OS). The MAF at each node can include managers only, agents only, or both managers and agents [18]. Management communication between these nodes into domain A is achieved via the Message Communication Function (MCF). Network operator has access to the MPLS-TP transport network via a Local Craft Terminal (LCT) which is attached to one of these network nodes. Each node in domain A is consisted of two networks, an Optical Packet Switched (OPS) network and an Optical Cross Connect (OXC) network. For better management of this domain, there is a partition of management network into two subnetworks. The Optical Packet Switched (OPS) network is managed by MPLS-TP management subnetwork and the Optical Cross Connect (OXC) network is managed by an OTN management subnetwork. Each subnetwork is separable from the management of the other technology specific networks and operates independently of any particular server of client layer management plane [18]. Furthermore, the Message Communication Function (MCF) of an MPLS-TP node initiates, terminates, routes and process management messages over Communication Channels (CChs) or via external interface.

MPLS-TP nodes into domain A, communicate via the Data Communication Network (DCN). Data Communication Network (DCN) is the common term for the network used to transport Management and Signaling information between nodes [18]. The MPLS-TP network can be managed not only by Management Plane (MP) but also by Control Plane (CP) protocols. Management via Control Plane is not mandatory requirement in MPLS-TP but is used by many network operators for Label Switching Path (LSP) recovery and network configuration. Many times, operators use Management Plane (MP) to have a full control of the network resources during the LSPs setup phase and then allow the network to be automatically maintained by the Control Plane.

When packets arrive to the ingress Opmigua node, it checks each packet to identify if it has high or low priority. This is achieved by the configuration management into the ingress node and sends high priority packets to OXC network and low priority packets to OPS network.

As it concerns the first scheme (figure 4-7), the Opmigua ingress node (LSR A6) tags high priority packets as GST and low priority packets as SM packets due to their class of service (CoS) and send them to the egress node which is LSR A8. Here, the GST packets are supposed to have the same destination IP address and SN packets are inserted into the wavelength channel with different SOP and lower class of service level. There are some intermediate nodes which are LSR A4 and LSR A1. Each Label Switched Path (LSP) takes an MPLS label value like the path between LSR A6 and LSR A4 has the label value 10, path between LSR A4 and LSR A1 label value 7 and path between LSR A1 and LSR A8 label value 4. All of these labels have a local significance and are assigned by LSRs to SM packets only to find the next path until to reach the LSR A8 which takes the label out from the SM packets.

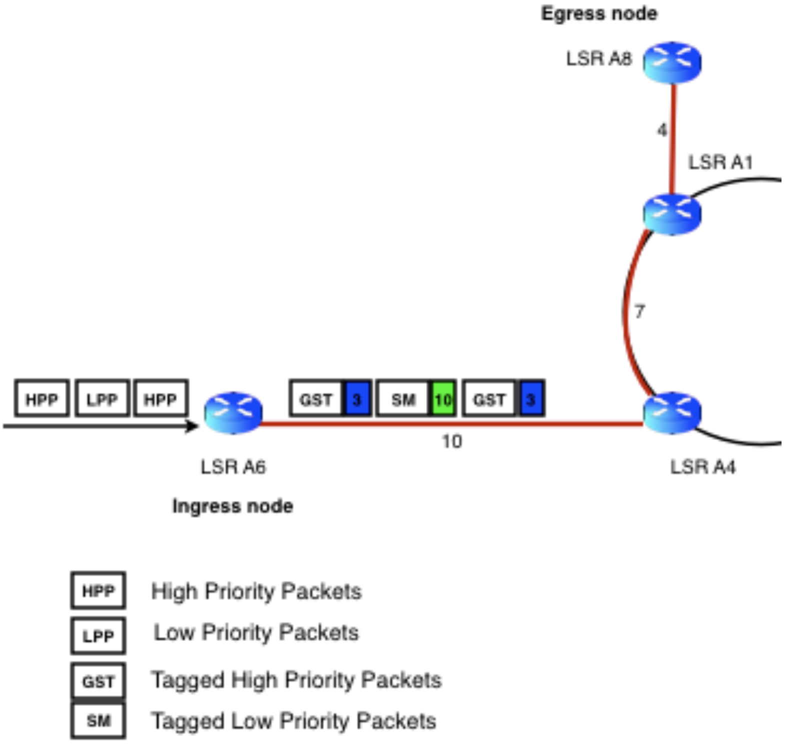


Figure 4-7. GST and SM packets traversing from LSR A6 to LSR A8 inside the domain A. GST packets have the same destination IP address and the are tagged with the same global significance label (3) inside the Opmigua network.

Figure 4-8 below, presents the procedure of the GST packets and SM that follow between LSR A6 and LSR A4. Ingress path is consisted of one wavelength (K1) channel and carries GST packets with a global significance label with value “3” inside the network protocol header. This label remains the same until the GST packet to reach the destination node. As it is refereed above, all of the GST packets have the same destination IP address and for this reason the global significance label remains entirely the same. When LSR A6 detects a high priority packet, which is marked by an optical label as GST packet, a low priority packet (tagged SM packet) is added with an MPLS-TP header and takes a local significance label with value “10”. A Polarization Beam Combiner (PBC) at the output of node 1 ensures that GST and SM packets are launched on orthogonal polarization states, denoted by SOP1 and SOP2, respectively. Until the SM packet to be added in the path, there is a small fixed delay as it concerns the GST packets. SM and GST packets are inserted with different time slots into the wavelength channel. Furthermore, packets are forwarded to the next node which is LSR A4 and SM packets follows the OPS network while the GST packets go directly to OXC network. In OPS network, LSR A4 drops SM packets and take the local significance label off. Then It adds another new SM packets in the GST channel with a new local significance label with value “7”.

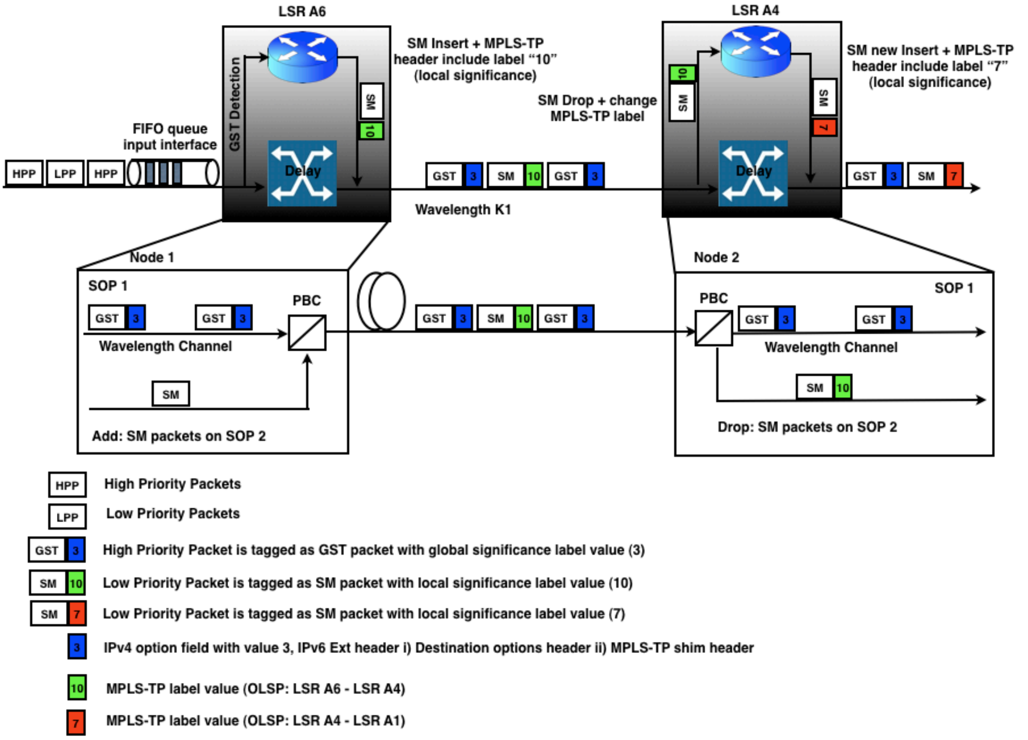

LSR A6
LSR A4
SM Insert + MPLS-TP header include label “10” (local significance)
SM new Insert + MPLS-TP header include label “7” (local significance)
SM Drop + change MPLS-TP label
FIFO queue input interface
GST Detection
Delay
HPP
LPP
HPP
GST 3
SM 10
SM 7
Wavelength K1
Node 1
Node 2
SOP 1
PBC
Wavelength Channel
SM
Add: SM packets on SOP 2
Drop: SM packets on SOP 2
HPP High Priority Packets
LPP Low Priority Packets
GST 3 High Priority Packet is tagged as GST packet with global significance label value (3)
SM 10 Low Priority Packet is tagged as SM packet with local significance label value (10)
SM 7 Low Priority Packet is tagged as SM packet with local significance label value (7)
3 IPv4 option field with value 3, IPv6 Ext header i) Destination options header ii) MPLS-TP shim header
10 MPLS-TP label value (OLSP: LSR A6 - LSR A4)
7 MPLS-TP label value (OLSP: LSR A4 - LSR A1)

Figure 4-8. GST and SM packet analysis and paths from LSR A6 to LSR A4 inside the domain A. GST packets have the same global significance label (3) inside the Opmigua network.

Further analysis of GST and SM packets from LSR A6 to LSR A8 is depicted in figure 4-9 below. LSR A1 does the same procedures with the previous node (LSR A4) and imports a new SM packets with label value “4” into the wavelength channel. Finally, the last node which is the LSR A8 drops the SM packets and forward the procedure of GST packets to the destination address.

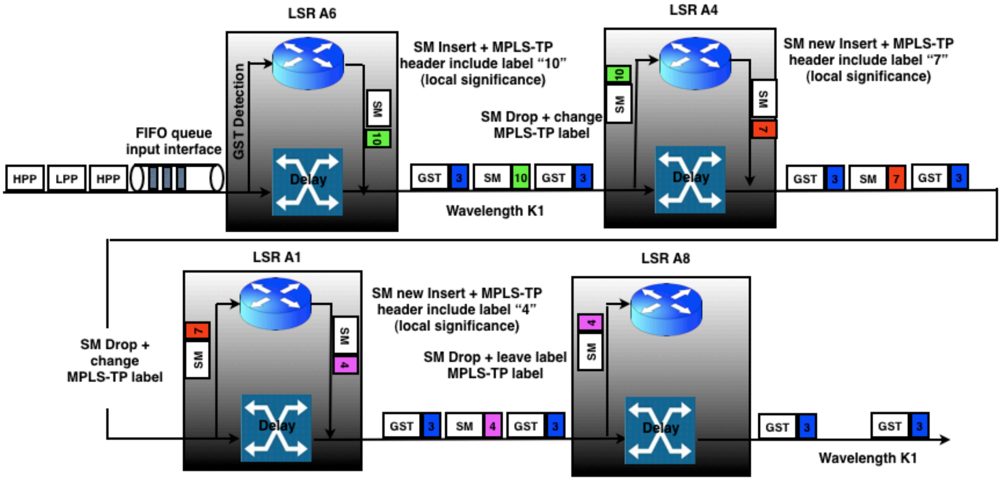

LSR A6
LSR A4
LSR A1
LSR A8
SM Insert + MPLS-TP header include label “10” (local significance)
SM new Insert + MPLS-TP header include label “7” (local significance)
SM new Insert + MPLS-TP header include label “4” (local significance)
SM Drop + change MPLS-TP label
SM Drop + change MPLS-TP label
SM Drop + leave label MPLS-TP label
FIFO queue input interface
GST Detection
HPP
LPP
HPP
Delay
Delay
Delay
Delay
SM
10
SM
7
SM
4
GST
3
SM
10
GST
3
GST
3
SM
7
GST
3
GST
3
SM
4
GST
3
GST
3
GST
3
Wavelength K1
Wavelength K1

Figure 4-9. GST and SM packet analysis and paths from LSR A6 to LSR A8 inside the domain A. GST packets have the same global significance label (3) inside the Opmigua network.

Second scheme that is proposed, is the same with the previous one which is presented in figure 4-7, but the only difference is that the input interface creates different GST packets which have different IP destination addresses and the result is different global significance label per GST packet. Figure 4-10 and 4-11 below presents this scenario and all the other procedures remain the same.

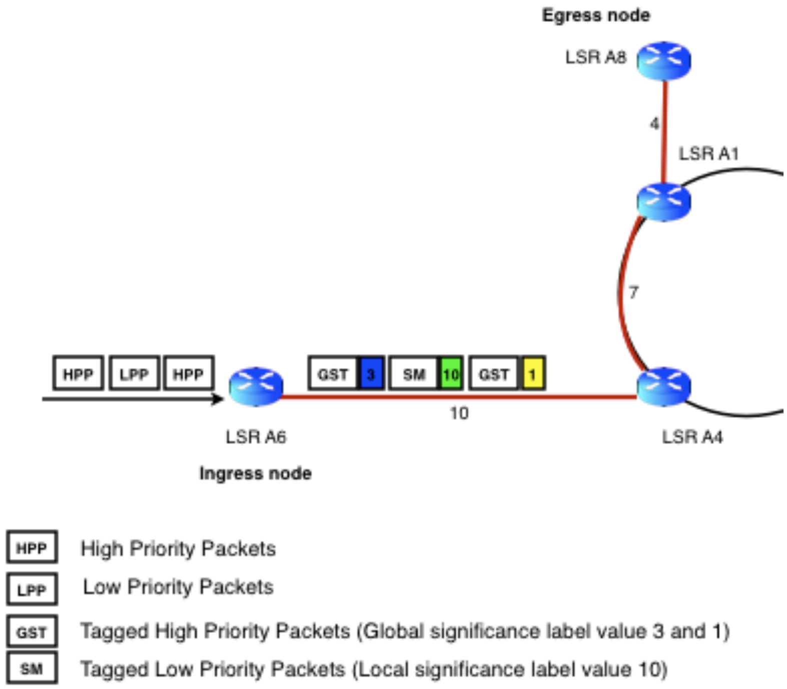

Egress node
LSR A8
4
LSR A1
7
HPP
LPP
HPP
GST
3
SM
10
GST
1
10
LSR A6
Ingress node
LSR A4
HPP High Priority Packets
LPP Low Priority Packets
GST Tagged High Priority Packets (Global significance label value 3 and 1)
SM Tagged Low Priority Packets (Local significance label value 10)

Figure 4-10. GST and SM packets traversing from LSR A6 to LSR A8 inside the domain A. GST packets have different destination IP addresses and the are tagged with different global significance labels (3 and 1) inside the Opmigua network.

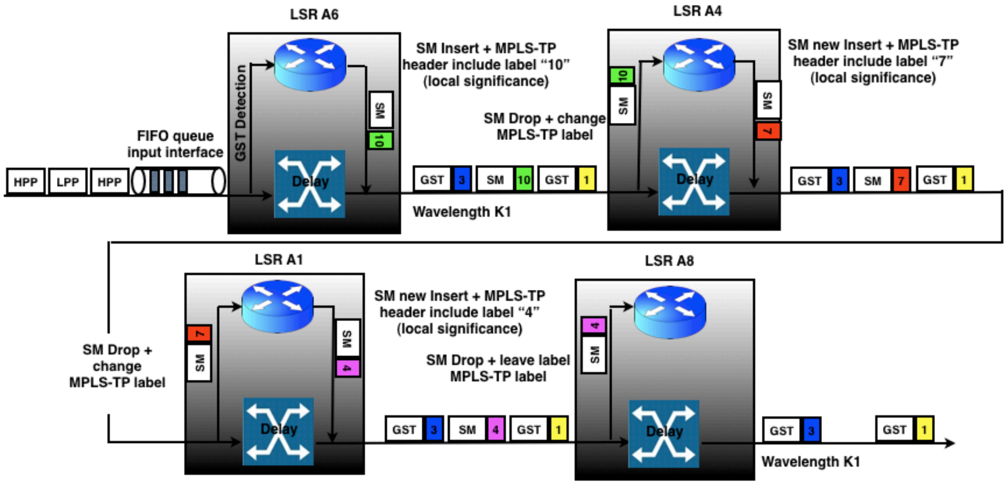

LSR A6
LSR A4
LSR A1
LSR A8
GST Detection
FIFO queue input interface
HPP
LPP
HPP
SM Insert + MPLS-TP header include label "10" (local significance)
SM Drop + change MPLS-TP label
SM new Insert + MPLS-TP header include label "7" (local significance)
SM Drop + change MPLS-TP label
SM new Insert + MPLS-TP header include label "4" (local significance)
SM Drop + leave label MPLS-TP label
Delay
SM
10
7
4
GST
3
1
Wavelength K1
Wavelength K1

Figure 4-11. GST and SM packet analysis and paths from LSR A6 to LSR A8 inside the domain A. GST packets have different global significance labels (3 and 1) inside the Opmigua network.

Another possible scheme is that an Opmigua ingress node (LSR A6) has two different input interfaces which receives packets with high priority (which are tagged after as GST packets) from one interface and from the another interface receives packets with lower priority (tagged as SM packets). High priority packets with the same destination IP address, are tagged as GST packets with the same global significance label value (figure 4-12a) but it is also possible the ingress node to put different global significance label values to packets that are destined to different destination nodes (figure 4-12b). Figure 4-12 presents these schemes below.

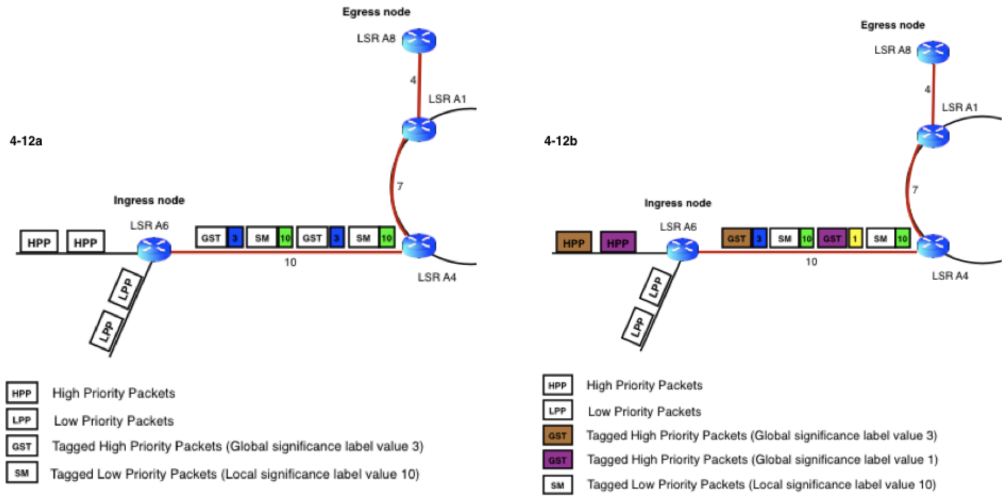
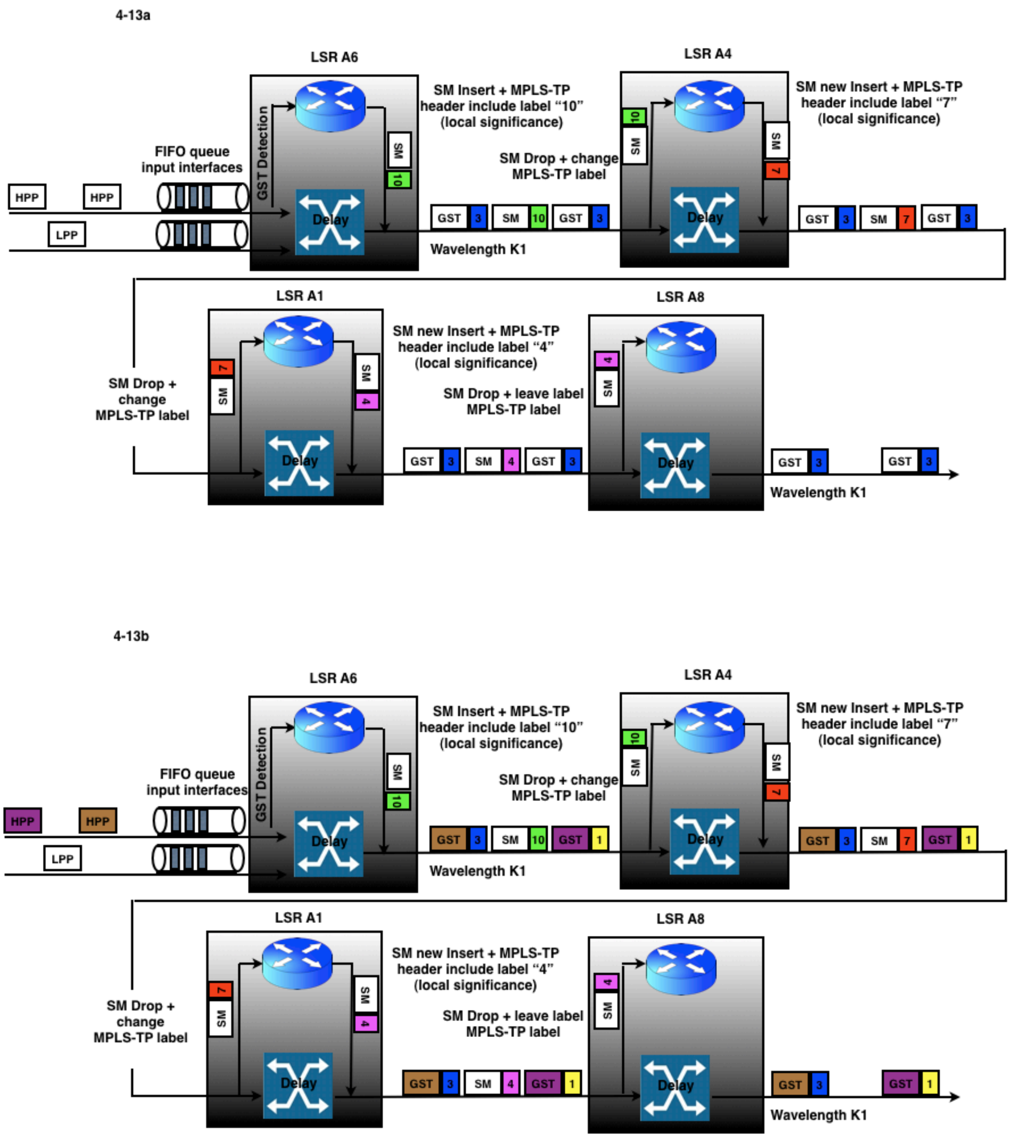

4-12a
Egress node
LSR A8
4
LSR A1
7
Ingress node
LSR A6
HPP
HPP
GST 3
SM 10
GST 3
SM 10
10
LSR A4
LPP
LPP
HPP High Priority Packets
LPP Low Priority Packets
GST Tagged High Priority Packets (Global significance label value 3)
SM Tagged Low Priority Packets (Local significance label value 10)
4-12b
Egress node
LSR A8
4
LSR A1
7
Ingress node
LSR A6
HPP
HPP
GST 3
SM 10
GST 1
SM 10
10
LSR A4
LPP
LPP
HPP High Priority Packets
LPP Low Priority Packets
GST Tagged High Priority Packets (Global significance label value 3)
GST Tagged High Priority Packets (Global significance label value 1)
SM Tagged Low Priority Packets (Local significance label value 10)

Figure 4-12. Opmigua ingress node with two input interfaces (high priority and low priority packets). 4-12a is consisted of GST packets that have the same destination IP addresses. 4-12b is consisted of GST packets with different destination IP addresses.

The previous scheme is analyzed better at the next figures 4-13a and 4-13b respectively. Both figures, present the procedure of the high and low priority packets from different input interfaces into the Opmigua network.


4-13a

4-13b

Figure 4-13. GST and SM packet analysis and paths from LSR A6 to LSR A8 inside the domain A. 63a two input interfaces with high priority packets but with the same destination IP address and low priority packets respectively at the ingress node. 63b two input interfaces, high priority packets with different IP destination addresses and low priority packets.

Next scheme that is proposed in this project, is when the Opmigua ingress node has also two input interfaces but this time, both of these interfaces receive only high priority packets. When the ingress node receives all of these high priority packets from both two input interfaces, it tags them as GST packets and for these packets that have the same destination IP address puts the same global significance label value. For GST packets that are destined to different destination nodes it puts different global significance labels. The presentation of this scenario is provided in figure below (4-14a and 4-14b respectively).

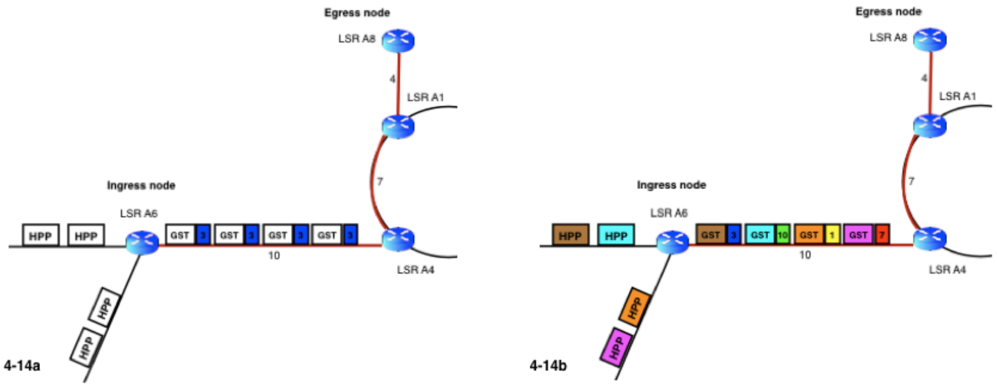


Figure 4-14. Ingress node LSR A6 connected with two input interfaces which have high priority packets only. 4-14a presents GST packets which are sent to the same destination node and 4-14b packets are sent to different destination nodes.

In this scheme, all the packets have high priority and this means that the Optical Packet Switch (OPS) network is not used . The result is all the packets are inserted from the input interfaces of the ingress Opmigua node tagged as GST packets and follow the Optical Cross Connect (OXC) network without any delay between nodes. Previous schemes use a small fixed delay for the insertion of SM packets into the optical path. Figure 4-15a below, presents the procedure of high priority packets with the same destination IP address between the ingress and the egress Opmigua nodes. The ingress node (LSR A6) detects the high priority packets, which each packet has a global significance label with value 3, and send them in a time slot fashion into the optical path. However, buffering of GST packets is avoided, so LSR A6 receives at the same time high priority packets from both input interfaces and the result is small delay at the ingress node. At this scenario, only two nodes take part which are the ingress and the egress node.

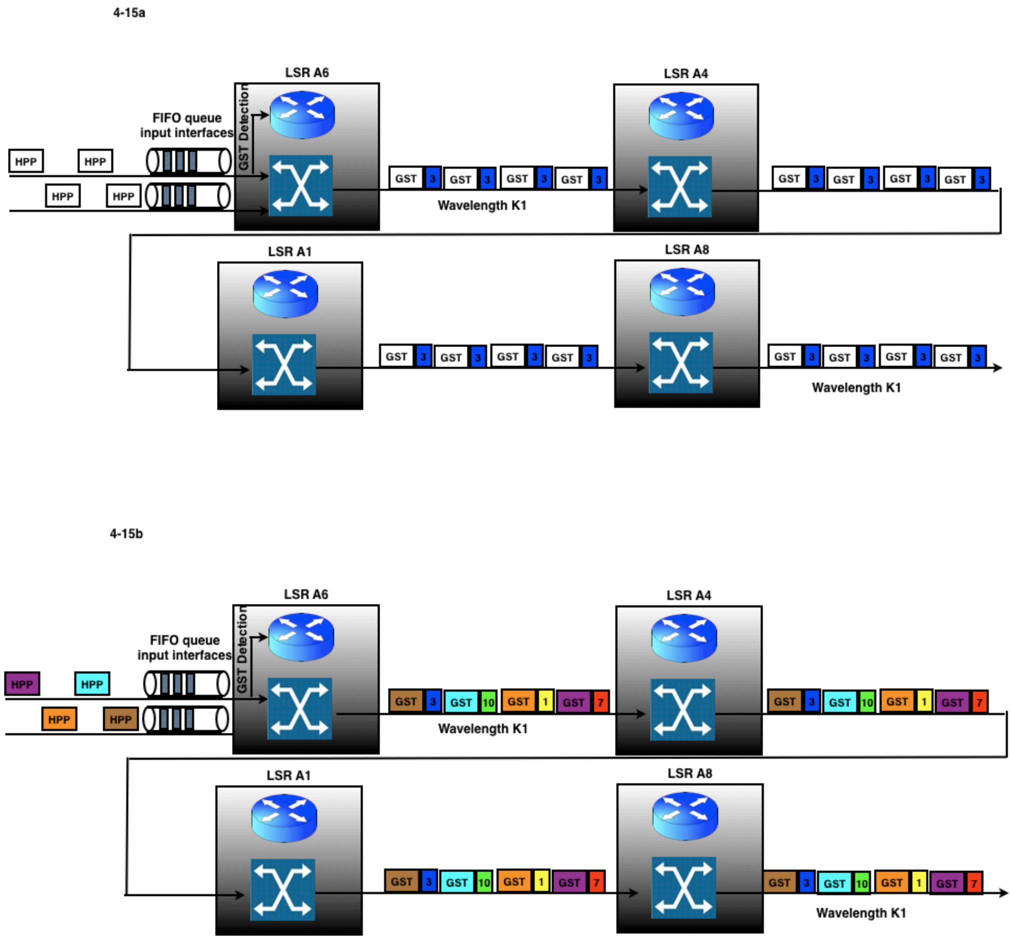


Figure 4-15. GST packet analysis and paths from LSR A6 to LSR A8 inside the domain A. 4-15a two input interfaces with high priority packets but with the same destination IP address. 4-15b two input interfaces, high priority packets with different IP destination addresses.

The same procedure is followed for high priority packets that have different destination IP addresses and is illustrated in figure 4-15b above. Here, the ingress Opmigua node, tags GST packets with different global significance label for each packet.

Another scheme that is proposed is when the Opmigua ingress node has only one input interface and receives low priority packets only. In the previous schemes, packets with low priority are tagged as SM packets but in this scenario packets with low priority could be transmitted as GST packets (with lower priority than normal GST data traffic) if and only if there are not any high priority packets (GST) into the network. This scheme uses the previous Opmigua network into domain A. The ingress Opmigua node receives from an input interface only packets with low priority which have the same destination IP address. With the State of Polarization (SOP) is detected that incoming packets have low priority and no other packets with high priority are existed. Then, the ingress node tags them with global significance label with value 3 (figure 4-16) and send them to the optical wavelength path via Optical Cross Connect (OXC) network as GST packets but with low priority.

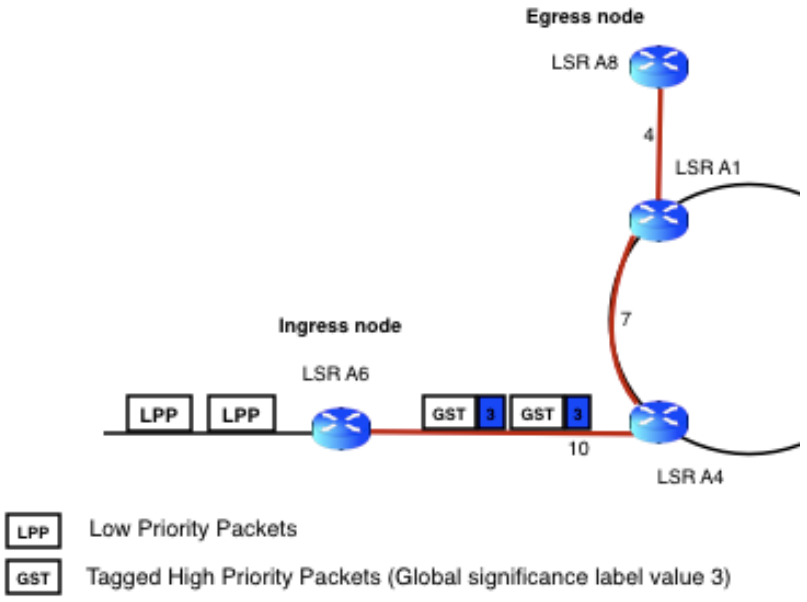


Figure 4-16. Incoming low priority packets are tagged as GST packets with global significance label with the same destination IP address.

Furthermore, the analysis of the previous scenario is illustrated more analytically in figure 4-17 below. Incoming low priority packets are queued to the input interface of the Opmigua ingress node (LSR A6) with First In First Out (FIFO) order, bypass all the intermediate nodes following the OXC network, when there are no high priority packets, and arrived to the egress node (LSR A8). An advantage of this scheme is nodes LSR A4 and LSR A8 do not take part to the packet procedure and there is no fixed and processing delay from OPS network because low priority GST packets are forwarded directly to OXC network and do not take local significance labels to find the next hop until the egress node.

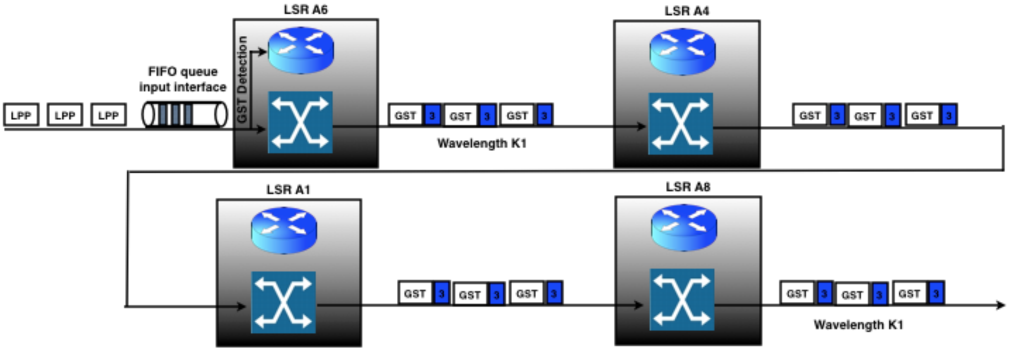


Figure 4-17. Low priority packets are forwarded to OXC network and are tagged as GST packets bypassing the OPS network (same destination IP address).

The same procedure is followed by incoming low priority packets that have different IP destination addresses with the only difference from the previous example is that they take different global significance labels as it is provided in figure 4-18 below.

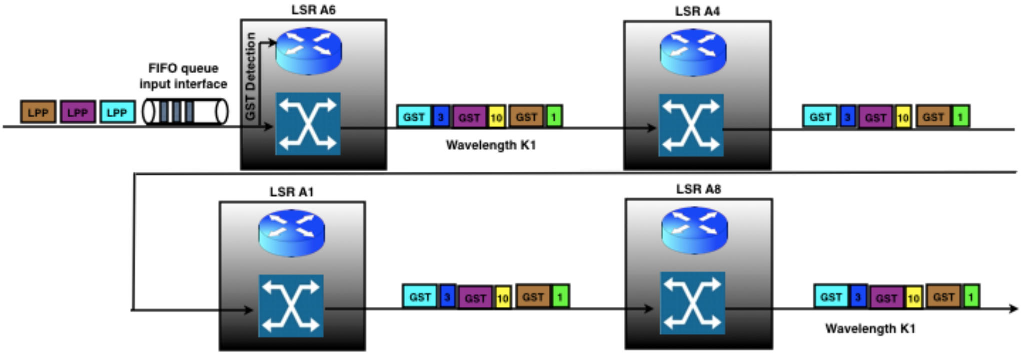


Figure 4-18. Low priority packets are forwarded to OXC network and are tagged as GST packets bypassing the OPS network (different destination IP addresses).

Next scheme, that is proposed in this work is when there are two input interfaces connected with the ingress Opmigua node which the first one, receives only few, high priority packets, and the second, only low priority packets and all the packets follow the OXC network avoiding delays of OPS network (figure 4-19). As it is referred in the previous schemes, the distinction between low and high priority packets is done by MPLS-TP management plane when the packets are inserted to the ingress node. Then, low priority packets are tagged as SM and follow the packet switch network for further analysis, and high priority packets are tagged as GST packets and follow circuit switch network (OXC). For achievement of this scenario, the configuration management that controls the ingress node, identify the high and low priority packets and sends first the GST packets via OXC network to the egress node without delay and then it forwards the low priority packets as GST low priority packets, to the same path (OXC). With this scenario, not only GST high priority packets send with absolute no delay (fixed delay) and jitter to the egress node but also GST low priority packets are sent without delay which is caused by procedures of the OPS network.

However, for this scheme is used the same example like the previous scenarios. High and low priority packets are destined from ingress node LSR A6 to egress node LSR A8 (figure 4-20). High priority packets, have the same destination IP address and also packets with low priority respectively.

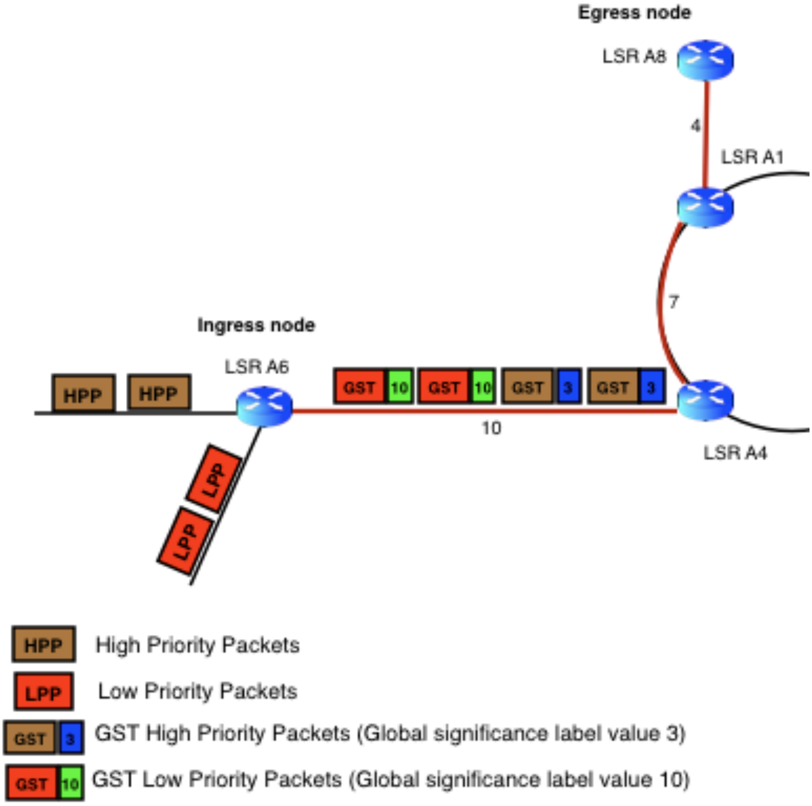

Egress node
LSR A8
4
LSR A1
7
Ingress node
LSR A6
HPP
HPP
GST 10
GST 10
GST 3
GST 3
10
LSR A4
LPP
LPP
HPP High Priority Packets
LPP Low Priority Packets
GST 3 GST High Priority Packets (Global significance label value 3)
GST 10 GST Low Priority Packets (Global significance label value 10)

Figure 4-19. Two incoming interfaces, one with high priority packets and the other low priority packets follow the OXC network.

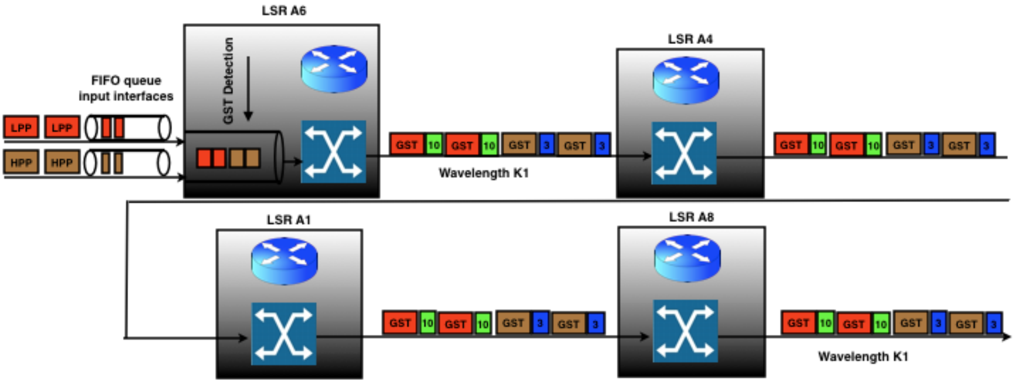


Figure 4-20. GST high and low priority packets are forwarded to OXC network (same destination IP address).

Last scenario, is when an ingress Opmigua node receives high and low priority packets from two input interfaces respectively and aggregate the low priority traffic either to different SM paths or to GST path. Figure 4-21 presents the different paths that follows the SM packets into the Opmigua network from ingress to egress node. GST packets follow circuit switched paths via OXC network from ingress LSR A6 to egress LSR A8 node. All the GST packets inside the GST path, bypass the intermediate nodes which are LSR A4, LSR A1 in a transparent way. The advantage of this is the capacity that is utilized into the circuit switch network remains in low level. Another advantage of GST path is the delay of the packets is minimized. Because nodes LSR A4 and LSR A1 are not used for the examination of GST packets, the processing delay is also minimized. Employing time-slots, the granularity of circuit switched networks is increased. For this reason, GST packets that do not fill the whole capacity of the time-slots, SM packets or low priority GST packets are allowed to be added in the remaining capacity.

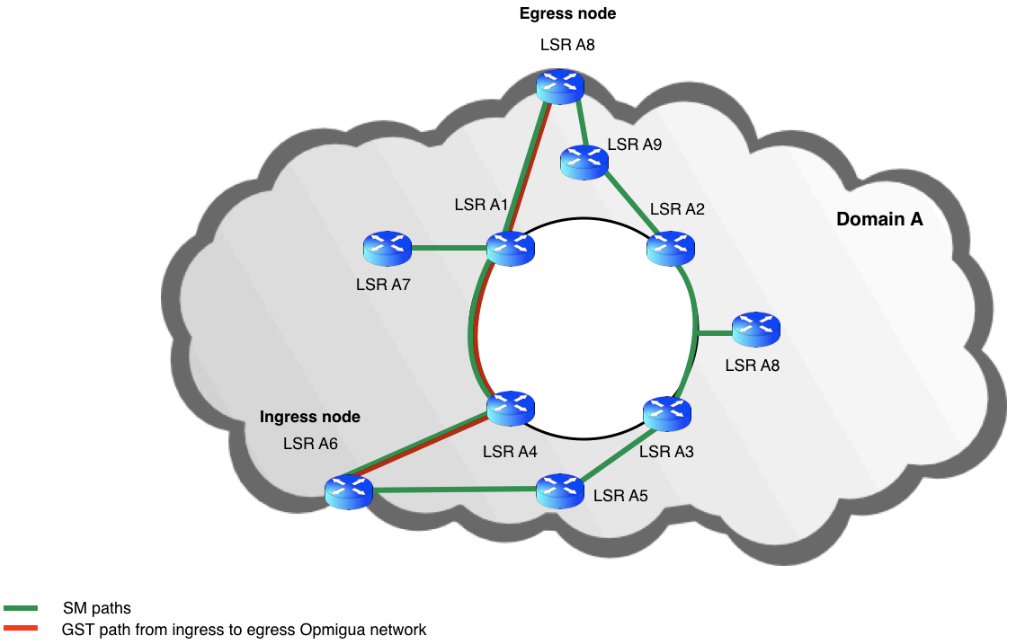


Figure 4-21. Aggregation of low priority packets into GST and SM paths.

It is supposed that the optical path that connects the ingress with egress Opmigua node (LSR A6, LSR A8) has capacity of 100Gb/s and receives high priority packets like voice and video which are not tolerant to any delays. These video on demand packets could be come from a broadcast TV operator that wants to send 100 channel of 5 Mb/s each, which are compressed (MPEG2) via OXC network. The capacity that the optical path carries for these 100 channels is 0.05% of the total. This means that it is possible to send low priority packets to the same path until the capacity is increased and reach some appropriate level. The result is that some SM packets are processed to the Opmigua network and not only follow the Packet Switched Network but also when the utilization capacity of the OXC network is low, they follow the GST path. SM packets are allowed to be scheduled only when: i) there is unused space (capacity) in a time-slot allocated to a GST path and ii) there are time-slots that are not allocated.

Figure 4-22 below, presents the procedure of high, low and lowest priority packets inside the Opmigua ingress node. When the ingress node receives packets, with different priorities, from two different input interfaces, fist the packets are shortened into FIFO queue of each input interface. The aggregation is done by MPLS-

TP configuration management inside the node A6. It identifies the SM class and divides it into several sub classes with different priorities and finally creates different LSPs based on these classes which forwards the SM packets. Each of these packets are distributed either to OPS or to OXC network which are shortened in a time-slot fashion at the output interface of Opmigua ingress node. The procedure remains the same, as it concerns the global significance labels of GST packets. The ingress Opmigua node is also responsible before to forward any high priority packet to do a lookup into the network header of the packet and to add an extra header which are the MPLS-TP or destination options header (with a global significance label value which remain the same) when the Internet Protocol v6 is used.

Low and lowest priority packets are possible to be proceed by OPS and OXC if the capacity of the GST path is low and if there are free time-slots between each GST packet in the path. For these reasons, sometimes are tagged with global significance label if are destined to the egress node bypassing the intermediate nodes and follow the GST path. However, it is possible these packets to have as a destination, intermediate nodes into the Opmigua network, like LSR A7 or LSR A8 (figure 4-21), and to follow SM paths taking MPLS-TP local significance label for each LSP into domain A.

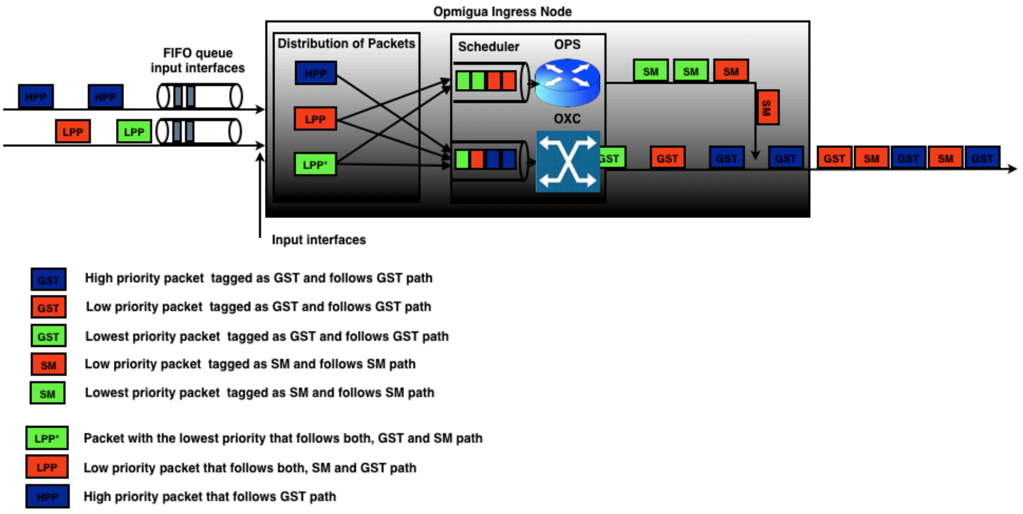

Opmigua Ingress Node
FIFO queue
input interfaces
HPP
HPP
LPP
LPP
Distribution of Packets
HPP
LPP
LPP*
Scheduler
OPS
OXC
SM
SM
SM
SM
GST
GST
GST
GST
GST
SM
GST
SM
GST
Input interfaces
GST High priority packet tagged as GST and follows GST path
GST Low priority packet tagged as GST and follows GST path
GST Lowest priority packet tagged as GST and follows GST path
SM Low priority packet tagged as SM and follows SM path
SM Lowest priority packet tagged as SM and follows SM path
LPP* Packet with the lowest priority that follows both, GST and SM path
LPP Low priority packet that follows both, SM and GST path
HPP High priority packet that follows GST path

Figure 4-22. Distribution of SM, high and low priority GST packets into the ingress Opmigua node.

Moreover, low priority traffic (SM packets) is possible to be aggregated into two different SM paths (figure 4-21) which are, first from A6, A4, A1 and A8 nodes and second the path via node A5, A3, A8, A2, A9 and A8 via OPS network.

As it concerns the monitoring of the packets into the Opmigua network is achieved by MPLS-TP performance management in each node. The only packets that can be monitored are the low priority packets - SM packets because they follow the OPS network which is applicable the MPLS-TP management. GST packets can not be monitored because they follow optical paths via the OXC network. Performance management of SM packets can be achieved in two ways. The first is the measurement of performance data on-demand and the second is with proactively measurement [18].

On-demand measurement, provides the operator of this network to do a performance measurement for maintenance purpose such as diagnosis. This method is used in a specific LSP service instances and is for a limited time. On the other hand, the proactively measurement is used continuously over the time after the path is configured, with periodicity and storage information [18]. The data that are collected from this measurement are used for verifying the performance of the service. This method overwhelms both the process of collecting performance data at a node and the process of reporting this information to the Operations System (OS).

4.4 Protection scenarios for SM and GST paths

In this section are represented two MPLS-TP protection scenarios based on the previous Opmigua network domain. The first is called Facility Bypass and the second restoration using detours (sub-optimal and optimized) [36].

4.4.1 Facility bypass protection

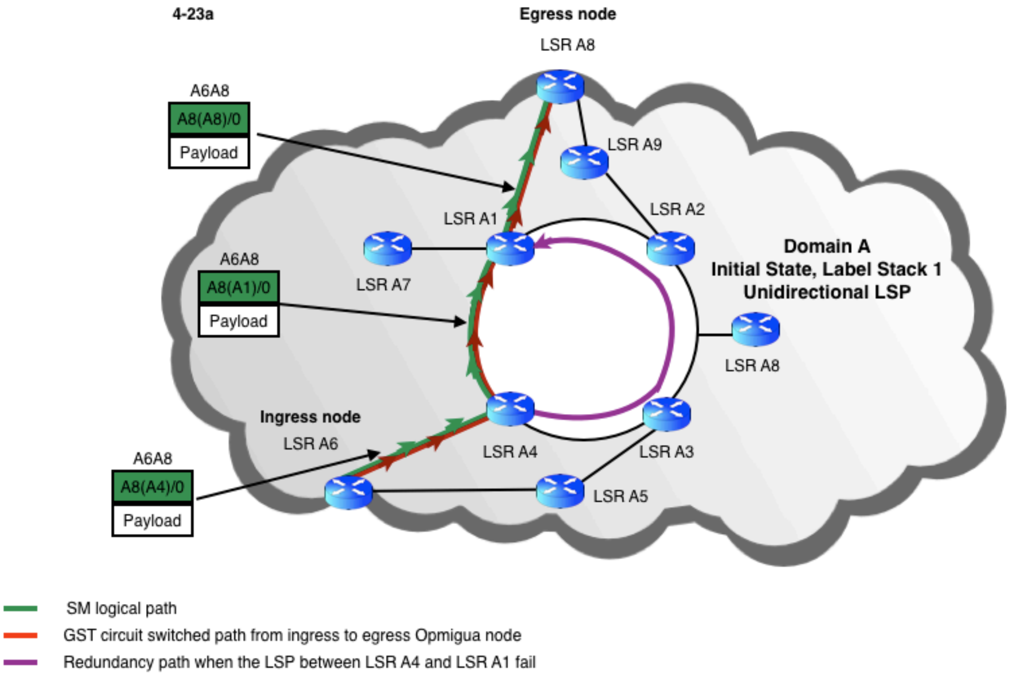
As it concerns the facility bypass protection scenario, it emulates conventional optical ring failure recovery and protects failure of link into the network sending all the traffic to another redundant link path to the merge point. For example, in figure 4-23 below is represented the domain A of Opmigua network. The path that is used to send SM and GST packets from ingress to egress Opmigua node is consisted of two intermediate nodes which are the LSR A4 and LSR A1. A facility bypass path which is between LSR A4, LSR A3, LSR A8 and LSR A2 is established to protect the link between LSR A4 and LSR A1 (figure 4-23a). When this link goes down (figure 4-23b), all SM and GST packets follow the facility bypass protection link and for better scalability this techniques requires two label stack to redirect the LSP around the failure.

MPLS-TP facility bypass uses some labels which are presented in figure 4-23a and 4-24b. These labels are only used by SM packets and not by GST packets. Furthermore, It is considered that the SM path from ingress to egress Opmigua node, is divided into three LSPs. The first one is the LSP between LSR A6 and LSR A4, the second between LSR A4 and LSR A7 and the last LSP is between LSR A1 and LSR A8. Each LSP takes one label (figure 4-24a) for example “A8(A4)/0” between LSR A6 and LSR A4 which means that with “A8” the destination is the LSR A8, “(A4)” uses label that is provided by LSR A4 and finally “/0” means that the Sbit is 0 and this label is not bottom of stack [36].

On the other hand, when the LSP between LSR A4 and LSR A1 fails, the recover path which is consisted of LSR A4, LSR A3,LSR A2 and LSR A1 takes part and uses another label on the top of the label stack as it is provided in figure 4-24b. This label takes part only in redundancy path until to reach the LSR A1 which is connected with broken and redundancy path. However, it has the shape of “A1/(A3)/0” which means that the destination LSR is the A1 and it takes the label that is provided by LSR A3 and the Sbit remains 0.

However, as it concerns GST packets, they use the facility bypass protection taking the redundancy path when the link between LSR A4 and LSR A1 is down but bypassing all the intermediate nodes until to reach the egress node which is the LSR A8.

4-23a


Egress node
LSR A8
A6A8
A8(A8)/0
Payload
LSR A9
LSR A2
LSR A1
A6A8
A8(A1)/0
Payload
LSR A7
Domain A
Initial State, Label Stack 1
Unidirectional LSP
LSR A8
Ingress node
LSR A6
LSR A4
LSR A3
A6A8
A8(A4)/0
Payload
LSR A5
SM logical path
GST circuit switched path from ingress to egress Opmigua node
Redundancy path when the LSP between LSR A4 and LSR A1 fail

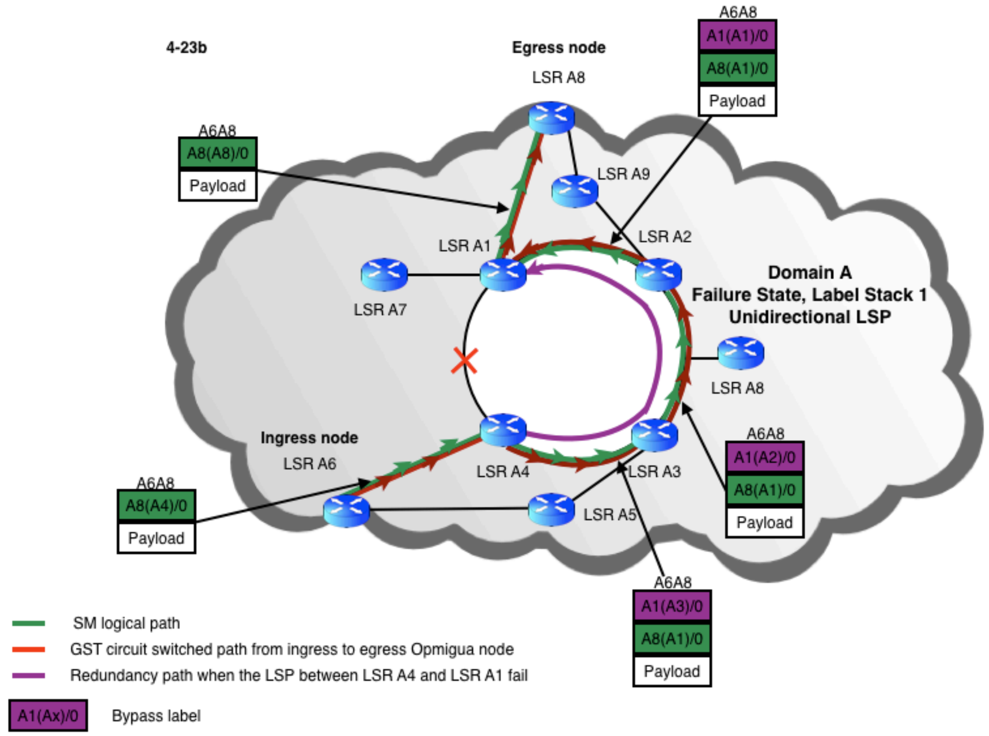
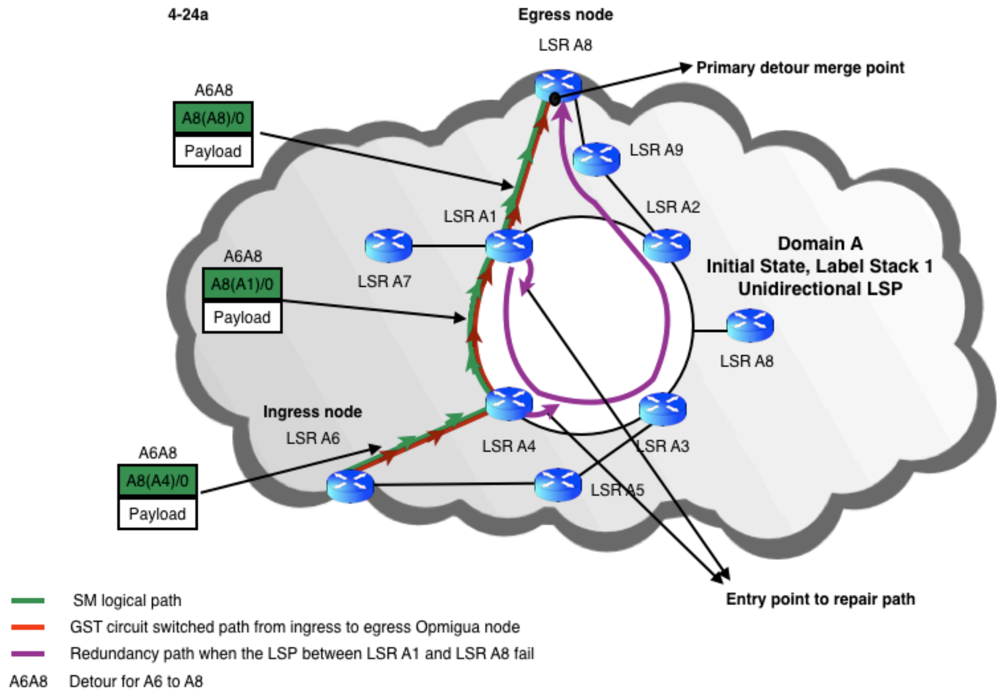


Figure 4-23. Facility bypass protection scenario in Opmigua network (4-23a initial state, 4-23b failure state).

4.4.2 Restoration using detours protection

Detour protection is the other technique which could be used in this network and generally is optimized on conventional optical ring and facility bypass failure recovery. It requires one label stack to redirect the LSP around the failure. However one detour per LSP is required for each working LSP and the detour LSP can be used to protect the failure of any link in the ring [36]. Figure 4-24a and 4-24b presents the initial state and the failure state respectively for unidirectional LSP. In figure 4-24a, LSR A1 and LSR A4 have an entry point to repair path. On the other side, when there is a failure between LSR A1 and LSR A8, all the SM and GST traffic is forwarded by the repair path (figure 4-24b) from LSR A1, LSR A4, LSR A3, LSR A2 to reach finally the egress node which is LSR A8. Because the repair path has as a final destination the egress node, it does not use a label stack but only one label as it is provided in figure 4-24b (purple label).


4-24a
Egress node
LSR A8
Primary detour merge point
A6A8
A8(A8)/0
Payload
LSR A9
LSR A1
LSR A2
A6A8
A8(A1)/0
Payload
LSR A7
Domain A
Initial State, Label Stack 1
Unidirectional LSP
LSR A8
Ingress node
LSR A6
LSR A4
LSR A3
A6A8
A8(A4)/0
Payload
LSR A5
Entry point to repair path
🟩 SM logical path
🟥 GST circuit switched path from ingress to egress Opmigua node
🟪 Redundancy path when the LSP between LSR A1 and LSR A8 fail
A6A8 Detour for A6 to A8

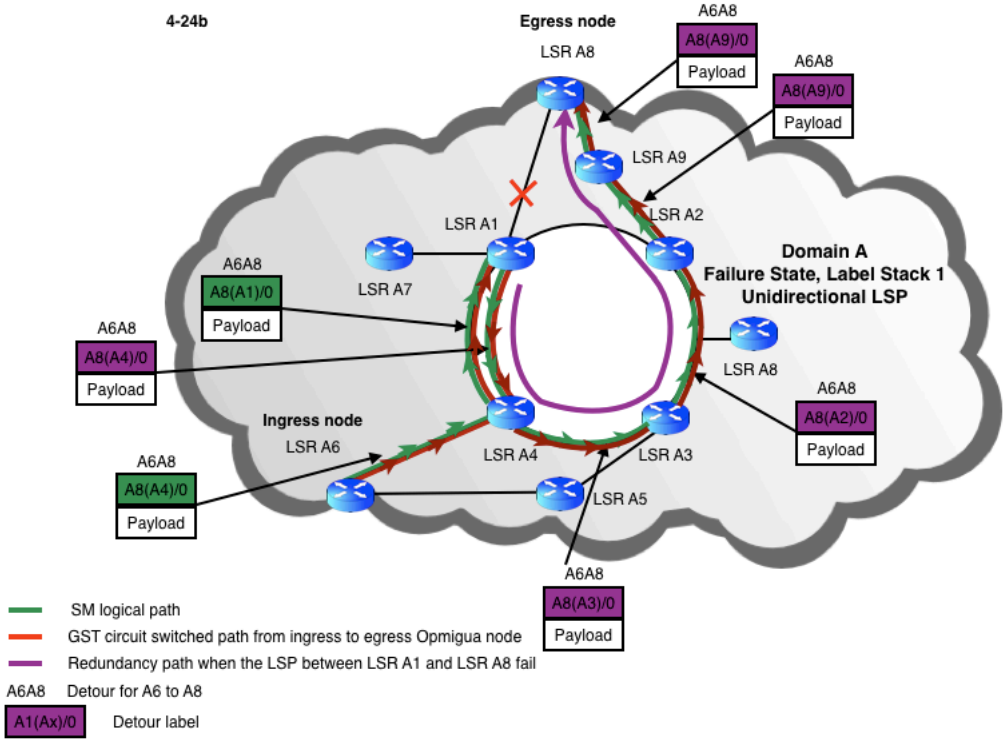


Figure 4-24. Analysis of detour protection of initial state (4-24a) and failure state (4-24b).

4.5 Scalability of Opmigua network with MPLS-TP

In this section is presented how an Opmigua network could be interconnected with other networks or domains with different technologies and characteristics and the way how to transfer GST and SM packets in cooperation with MPLS-TP protocol via these networks.

Below, in figure 4-25 is provided a network with three different domains (domain 1 - Opmigua network 1, domain 2 - provider's network and domain 3 - Opmigua network 2). When packets are imported by ingress node to the Opmigua network 1 with destination Opmigua network 2 are transmitted via provider's network. Provider's network may or may not use the same framing techniques like Opmigua networks and different technologies could be incompatible. For this reason, there is a need for all packets to remain unchanged and to bypass provider's network in a transparent way.

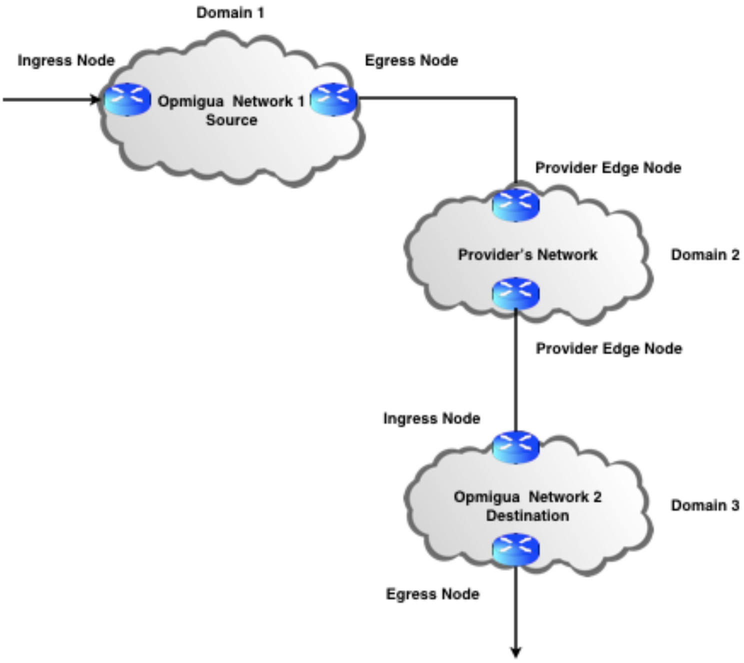


Figure 4-25. Network topology with three different domains (via provider's network).

A solution to these problems is the tunnel mode into provider's network. Providers use techniques like MPLS-TP tunnel mode or other like IP based on Virtual Private Network (VPN) (figure 4-26). As it concerns the MPLS-TP tunnel mode, it is possible to implement a tunnel as LSP and use label switching than network layer encapsulation to cause packets travel through the tunnel.

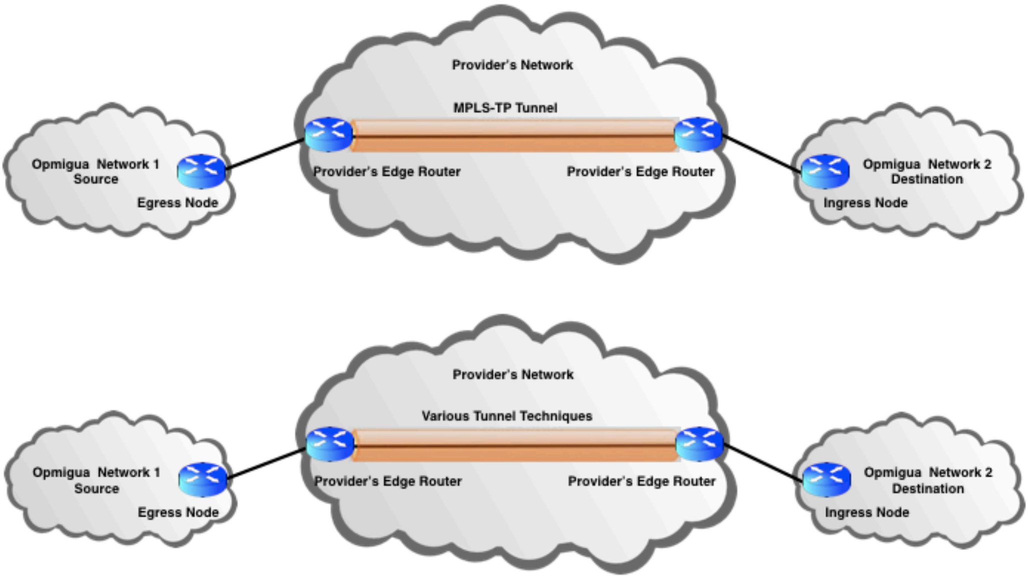


Figure 4-26. Example of tunnel techniques into provider's network.

It is supposed that provider's network uses MPLS-TP tunneling and is consisted of two Provider Edges, which are the ingress PE1 and the egress PE2, and from Provider routers (P) which are LSP1, LSP2, LSP3, LSP4. The procedure is set of packets sent through the LSP tunnel constitutes a FEC and its LSR in the tunnel must assign a label to that FEC. To put a packet into the tunnel, the transmit endpoint pushes a label for the tunnel onto the label stack and sends the labeled packet to the next hop in the tunnel. However, an LSR swaps only the top label stack. The egress LSR continues label disposition in the stack until it finds that the value of the S bit is set to 1 which denotes a bottom of the label stack (figure 4-27). After this procedure, the egress LSR performs a route lookup depending on the information in the IP Layer 3 header and forwards each packet toward the destination.

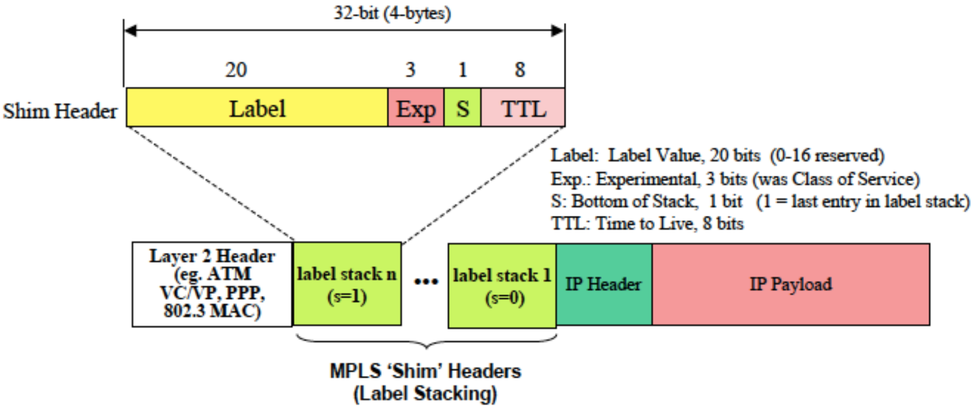

32-bit (4-bytes)
20
3
1
8
Shim Header
Label
Exp
S
TTL
Label: Label Value, 20 bits (0-16 reserved)
Exp.: Experimental, 3 bits (was Class of Service)
S: Bottom of Stack, 1 bit (1 = last entry in label stack)
TTL: Time to Live, 8 bits
Layer 2 Header (eg. ATM VC/VP, PPP, 802.3 MAC)
label stack n (s=1)
•••
label stack 1 (s=0)
IP Header
IP Payload
MPLS 'Shim' Headers (Label Stacking)

Figure 4-27. Hierarchy of MPLS-TP shim headers (Label Stacking) [22].

More analytically, in figure 4-28 is illustrated how the PE1 is connected to PE2. Packets are forwarded via LSP paths with labels 9, 12, 15, 10 respectively. The LSP with label 9 connects the PE1 with the LSR1, LSP with label 12, the LSR1 with LSR2, LSP with label 15, the LSR2 with LSR3 and finally, LSP with label 10 connects the LSR3 with PE2. The traffic that is coming from Opmigua network 1 is encapsulated into a tunnel inside the provider's network with final destination the Opmigua network 2.

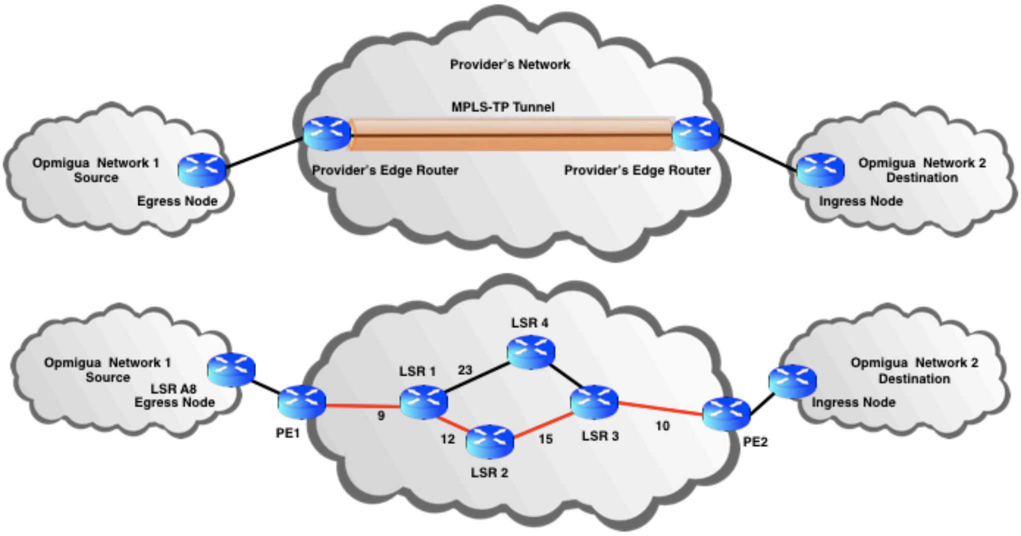


Figure 4-28. MPLS-TP Tunnel analysis into provider's network.

The incoming high priority packets when are inserted to the provider's network and more specifically to the input interface of PE1, carry also with them an MPLS-TP label which has global significance value. This MPLS-TP label, as it is mentioned in the previous section, could be placed in an extra header, if the IPv6 is used.

Figure 4-29 below, presents the procedure of a GST packet that is inserted into the MPLS-TP tunnel provider's network and how the label stack hierarchy is used. At the beginning, the egress node of Opmigua network 1 sends a GST packet via link layer (Ethernet) to the Provider Edge Router 1. At this point, the PE1 pushes one new label on the top of the label stack which is the LSP between PE1 and LSR1 with value 9. From LSR1 to LSR2 the packet is forwarding using this operation: the packet's label stack (with value 9) is replaced with a new label which has value 12. The same operation is used for the LSP between LSR2 and LSR3 which is replaced the previous label stack with a new with value 15. Furthermore, in the label stack hierarchy, the label with value 15 is replaced with a new label (10) and finally, PE2 pops label with value 10 and the GST packet is going out from the MPLS-TP tunnel. This is a decapsulation procedure and because this label is the last on the label stack, which is denoted by the S bit which is set, the GST packet leaves the MPLS-TP tunnel. However, the PE2 must have routing information for the packet's payload to be capable to forward to the destination address. During this procedure, the GST packet remains unchanged and bypass the provider's MPLS-TP tunnel in a transparent mode.

The most interesting here is that the MPLS global significance label does is not taken by any procedure into the provider's tunnel. So it is also transparent.

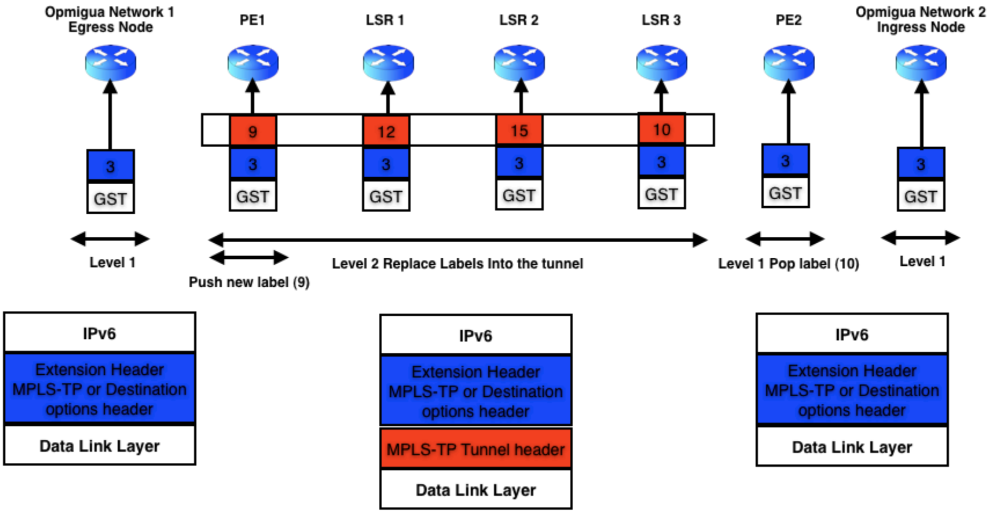


Figure 4-29. Procedure of GST packets into provider's MPLS-TP tunnel.

Another way for forwarding packets from one Opmigua network to another via provider's network is the usage of Pseudo Wires (PWs). A Pseudo Wire (PW) entity is an emulation of layer 2 point to point connection oriented service over a packet switched network. It emulates the operation of a transparent wire carrying service such as MPLS and IP protocol over a packet switched network. As it concerns the PW header is provided in figure 4-30 below. It is consisted of four fields which are flags, fragmenting of the PW payload, length and sequence number. When the PSN path between the PEs includes an Ethernet segment, the PW packet arriving at the CE-bound PE from the PSN may include padding appended by the Ethernet Data Link Layer. The CE-bound PE uses the length field to determine the size of the padding added by the PSN, and extract the PW payload from the PW packet [35].

0000	Flags	FRG	Length	Sequence Number

Figure 4-30. PW header MPLS-TP Control World [35].

However, there is another PW header which is called PW associated header (figure 4-31) and is used when an associated channel is required. Associated channel is a channel that is multiplexed in the PW with user traffic, and thus follows the same path through the PSN as user traffic [35]. It is consisted of four fields which are Version (version number of PWAC), reserved and channel type. The last field has four bits that is used to be distinguished the packet from an IP and PW data packet.

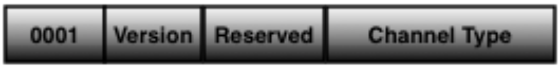


Figure 4-31. PW associated channel header [35].

An example that is provided below in figure 4-32 is an MPLS-TP single segment pseudo wire that connects the edge nodes from Opmigua network 1 and 2. This enables the clients to communicate directly via a virtual wire over a packet switched network (PSN). In this occasion, an MPLS-TP tunnel is established between Provider Edge nodes of provider's network to provide a data path for this pseudo wire. When packets are inserted from the incoming interface of ingress Opmigua node, are encapsulated in a pseudo wire Protocol Data Unit (PW-PDU) with a PW header in front. Then, all packets are carried across the underlying network via the MPLS-TP tunnel which the MPLS-TP tunnel header is inserted in front of the PW header. Next procedure of the packets inside the provider's network is the same as in figure 4-29 until the packets leave the MPLS-TP provider's tunnel. Ingress node of Opmigua network 2 is responsible to make the decapsulation of the PW-PDU and send the packet to the final destination. As it concerns the PW traffic, it is invisible inside the provider's network and as a result packets remain unchanged.

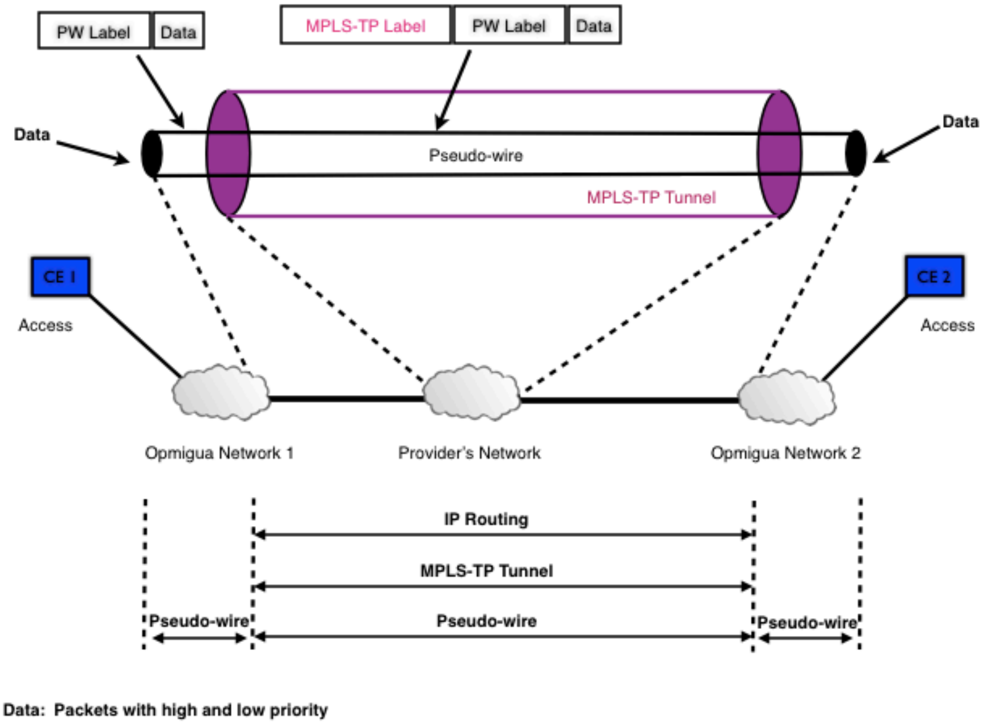


Figure 4-32. Example of Point to point Pseudo Wire between Opmigua network 1 and 2 via Provider's network.

Concerning these two schemes, the MPLS-TP tunnel mode inside the provider's network and point to point Pseudo Wire (PW) between Opmigua network 1 and Opmigua network 2, GST packets may have faced some delay. The reason for this propagation delay is the encapsulation of these high priority packets into MPLS-TP headers, as it concerns provider's tunnel. On the other hand, with Pseudo Wires (PWs), high priority packets take more time to reach the destination because are encapsulated into PW headers and MPLS-TP tunnel headers until to reach the final destination. Another problem is that high priority packets wait for forwarding procedure at the egress node of Opmigua network with result to create queues until to reach the provider's edge node for further forwarding procedure. However, it is possible GST packets to be tolerant to these delays.

For solving these problems, packets with high priority which are not tolerant to these delays should follow circuit switched paths and pure wavelengths into a fiber. In this way, there is not packet delay variation until to reach the destination node.

More techniques that are used by provider's network are Virtual Leased Lines (VLL), Virtual Private Routed Networks (VPRN) and Layer 2 Provider Provisioned VPN (L2PPVPN)/ MPLS [22]. As it concerns the Virtual Leased Lines (VLL), the data link layer type is used to connect the Opmigua network 1 egress node to the provider's ingress node can be any data link layer like Ethernet. On the other hand, Virtual Private Routed Networks (VPRN) inside the provider's network use a mesh of IP tunnels between ingress and egress node with VPN specific routing tables. Another technique that provider uses is the L2PPVPN/MPLS in which are provided pseudo wire service (Virtual Private Wire Service) or emulated LAN service (Virtual LAN Private Service) on provider's network [22]. As a result of these techniques, is that all the MPLS-TP headers of GST packets remain also transparent inside the provider's network.

An Opmigua network is also possible to connect to another Opmigua network via a third Opmigua network. As figure 4-33 presents, the Opmigua network 1 is the source and sends packets to the destination which is the Opmigua network 3 via network 2. The same MPLS-TP tunneling technique like provider's network in the previous section could be established also here inside the Opmigua network 2 for transferring GST and SM packets.

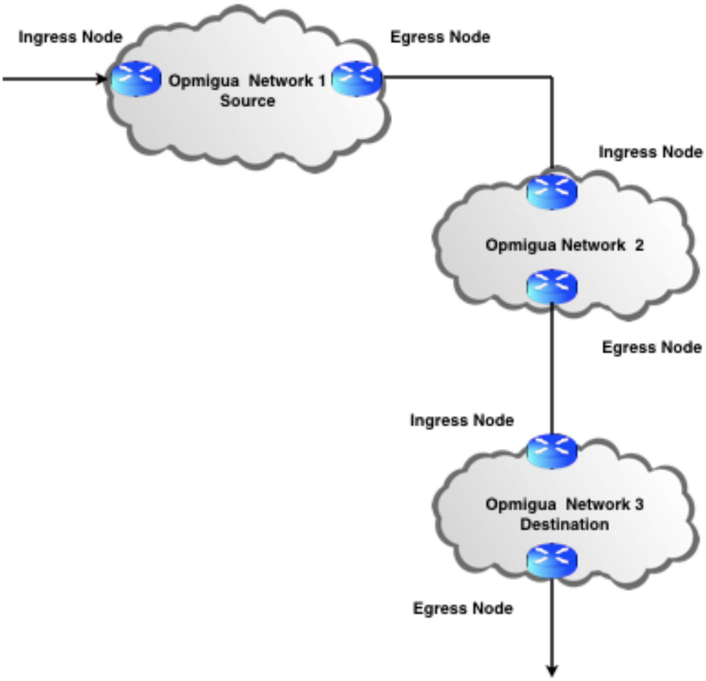


Figure 4-33. Network topology with three different domains (via other Opmigua network).

Opmigua network 2 could use label stack hierarchy techniques to encapsulate in an MPLS-TP tunnel all the packets coming to ingress node until to reach the egress node. This example is presented in figure 4-34 below.

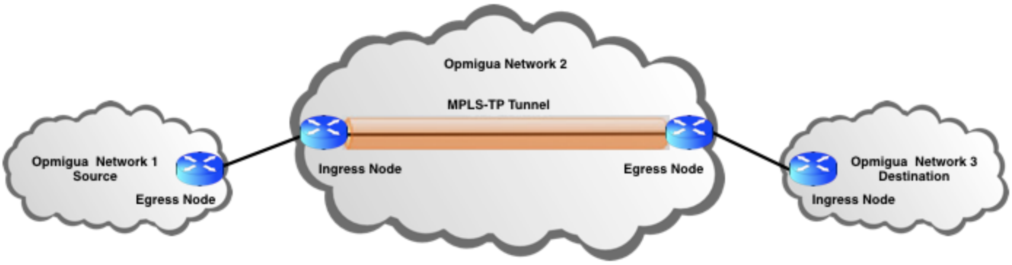


Figure 4-34. Example of tunnel techniques into Opmigua network.

Chapter 5

Summary and Proposals

The issues that have been proposed in this thesis work, as it concerns GST and SM packets, when the MPLS-TP protocol is used by the Opmigua network, are the follow:

- How to identify GST and SM packets into the Opmigua network using MPLS-TP protocol.
- The compatibility of GST packets with MPLS-TP protocol.
- A network scenario proposal and how the configuration of GST and SM packets and paths is done into the Opmigua network.
- Protection scenarios of GST and SM paths.
- Scalability and compatibility of Opmigua network based on MPLS-TP with other networks.

The first issue, describes the differentiation and the identification of SM from GST packets into the Opmigua network. As it concerns SM packets are based on router forwarding table lookup and the MPLS-TP label header and GST packets based on the input interface which is known the destination address for each packets following circuit switches and bypassing all the intermediate nodes until to reach the egress node.

Secondly, in this project are proposed two schemes which explain how GST packets could be compatible with MPLS-TP protocol. Both of these proposals use the extension header of the Internet Protocol v6. The first one, uses the Destination Options Header (DOH) which can be contained options (global significance label value) that are intended only by the destination node and are not examined by the intermediate nodes. The second one, uses as an extension header the MPLS-TP shim header for distribution of global significance label value. These extension headers are added at the ingress Opmigua node and bypass networks in a transparent way without cause any routing faults and are independent of different technologies.

Thirdly, a proposal of network scenarios are presented in this work. These network scenarios are based on the configuration of SM and GST packets and paths into the Opmigua network.

Furthermore, it is proposed the compatibility of two types of MPLS-TP protection scenarios for GST and SM paths into the Opmigua network. The first one is called facility bypass protection which the scalability techniques that uses, are required two label stack to redirect the LSP around the failure link and secondly is the restoration using detours protection. The last technique uses only one label because the repair path has as a final destination the egress node of Opmigua network.

Finally, it is presented how an Opmigua network could be interconnected with other networks or domains with different technologies and characteristics and the way how to transfer GST and SM packets in a transparent mode via these networks in cooperation with MPLS-TP protocol.

Chapter 6

Conclusion and Further work

6.1 Conclusion

This thesis, presents the analysis of the MPLS-TP functionalities in an Opmigua network. While MPLS-TP is a new framework, it is explained the way how the MPLS-TP protocol is applied for integrated hybrid network, and more specifically, in Opmigua network. They have been studied some issues in this thesis. At the beginning of this, is provided the background of the MPLS-TP protocol and more specifically, the characteristics and requirements which is undergoing the process of standardization. Furthermore, It is explained how the MPLS-TP management and the forwarding plane work. Some references are also given not only to OAM mechanisms but also to control plane that the MPLS-TP uses.

The main part of this project is refereed to the combination of MPLS-TP labels with Guaranteed Service Traffic (GST) and Statistical Multiplexing (SM) paths. We have achieved the cooperation of MPLS-TP protocol with the Opmigua network using MPLS-TP labels for setting up circuit and packet switch paths. Using this method, we have proposed a method that each GST packet takes a global significance label value until to reach the destination node. On the other side, SM packets take local significance labels for each path into an Opmigua network which follow Optical Packet Switch (OPS) networks. Another new method that we have proposed for differentiation of packets from low to high priority, is when extension headers of Internet Protocol v6, either Destination Options Header (DOH) or MPLS-TP as an extension header are used. The result is high and low priority packets are differentiated at ingress Opmigua network which GST packets take global significance MPLS-TP label following Optical Cross Connect (OXC) network and SM packets change per each Label Switched Path (LSP) local significance MPLS-TP labels until to reach the destination node.

Finally, two MPLS-TP path protection schemes, facility bypass and restoration using detours were combined with Opmigua network to provide failures not only to Guaranteed Service Traffic (GST) paths but also to Statistical Multiplexing (SM) paths.

6.2 Further work

Following the proposals which are described in this thesis, a further work could be based on performance analysis, reliability and availability of the Opmigua network which MPLS-TP protocol is applied. A performance analysis, employing simulation of GST and SM paths between different domains and technologies, could be achieved for finding the propagation delay and packet loss into the network. Another research work could be the dependability analysis of GST and SM packets, depending on loss ratio which carry global and local significance MPLS-TP labels. Finally, reliability analysis, for packet aggregation between OPS and OXC networks following different paths, could be further studied.

Bibliography

[1] Cisco Systems, Understanding MPLS-TP and Its Benefits, White paper, pages 1-5, 2009. http://www.cisco.com/en/US/technologies/tk436/tk428/white_paper_c11-562013.pdf

[2] Uyless D. Black, MPLS and Label Switching Networks, pages 5-9, January 2001, Prentice Hall PTR, Upper Saddle River, New Jersey.

[3] Dieter Beller, Rolf Sperber, MPLS-TP – The New Technology for Packet Transport Networks, Alcatel-Lucent Deutschland AG. http://www.dfn.de/fileadmin/3Beratung/DFN-Forum2/118.pdf

[4] Bill Michael, MPLS: Breaking Through, A Status Report, Computer Telephony, July 2001. http://www.cconvergence.com/article/CTM20010425S0001

[5] Steinar Bjornstad, Packet Switched Hybrid Optical Networks, ICTON 2004, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1360239&isnumber=29837

[6] The Opmigua Project, http://www.Opmigua.com/index.php?page=front

[7] Peter J. Welcher, Cisco Tag Switching, August 1997, http://www.netcraftsmen.net/resources/archived-articles/491-cisco-tag-switching.html

[8] James E. Goldman & Phillip T. Rawles, Applied Data Communications, 2004 (ISBN 0-471-34640-3)

[9] RFC 3031, Multiprotocol Label Switching Architecture, January 2001 http://www.ietf.org/rfc/rfc3031.txt

[10] Harry G. Perros, Connection-oriented Networks SONET/SDH, ATM, MPLS and Optical Networks, John Wiley & Sons Ltd, 2005 (ISBN 0-470-02163-2)

[11] T-PACK, T-MPLS, a new route to carrier ethernet, June 2007, http://www.tpack.com/fileadmin/user_upload/Public_Attachment/T-MPLS_WP_v2_web.pdf

[12] RFC 3916, Requirements for Pseudo-Wire Emulation Edge-to-Edge (PWE3), http://www.ietf.org/rfc/rfc3916.txt

[13] Martin Nord, Steinar Bjørnstad, Vegard L. Tuft, Andreas Kimsås, Dag Roar Hjelme, Lars Erik Eriksen, Torrid Olsen, Harald Øverby, Aasmund S. Sudbø, Norvald Stol, Oddgeir Austad, Anne-Grethe Kåråsen, Geir Millstein, Marius Clemetsen, The Opmigua project - Final report, 2006, http://www.telenor.com/rd/pub/rep06/r_32_06.pdf (ISBN 82-423-0606-0)

[14] Steinar Bjornstad, Harald Øverby, Norvald Stol, Dag Roar Hjelme, Protecting guaranteed service traffic in an Opmigua hybrid network, 2005 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1576464

[15] A. Kimsas, S. Bjornstad, H. Overby, N. Stol, Improving performance in the Opmigua hybrid network employing the network layer packet redundancy scheme, 2009 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5396276

[16] M. Bocci, Ed. Alcatel-Lucent S. Bryant, Ed. D. Frost, Ed. Cisco Systems L. Levrau, Alcatel-Lucent L. Berger, LabN (IETF MPLS Working Group), A Framework for MPLS in Transport Networks, February 2010 http://tools.ietf.org/html/draft-ietf-mpls-tp-framework-10

[17] B. Niven-Jenkins, Ed. BT D. Brungard, Ed. AT&T M. Betts, Ed. Huawei Technologies N. Sprecher Nokia Siemens Networks S. Ueno NTT Communications, (RFC 5654) Requirements of an MPLS Transport Profile, September 2009 http://www.rfc-editor.org/rfc/rfc5654.txt

[18] S. Mansfield, Ed. E. Gray, Ed. Ericsson H. Lam, Ed. Alcatel-Lucent, MPLS-TP Network Management Framework, January 2010 http://tools.ietf.org/html/draft-ietf-mpls-tp-nm-framework-04

[19] Hing-Kam Lam, Alcatel-Lucent Scott Mansfield, Eric Gray Ericsson, MPLS-TP Network Management Requirements, October 2009 http://tools.ietf.org/html/draft-gray-mpls-tp-nm-req-01

[20] Cisco Systems, Cisco MPLS Controller Software Configuration Guide, April 2000 http://www.ciscosystems.lt/application/pdf/en/us/guest/products/ps525/c2001/ccmigration_09186a00800eadd9.pdf

[21] ITU Recommendation G.709/Y.1331, Interfaces for the Optical Transport Network (OTN), March 2003

[22] Youngtak Kim, Management of MPLS-based VPNs, Advanced Networking Lab. (ANTL), Department of Information & Communication Engineering, Yeungnam University, Korea, 2003 http://www.apnoms.org/2003/slide/Tutorials/tutorial_YTKim.pdf

[22] D.Frost, ed. S. Bryant, Ed. Cisco Systems M. Bocci, Ed. Alcatel-Lucent, MPLS Transport Profile Data PLane Architecture, February 2010 http://tools.ietf.org/html/draft-ietf-mpls-tp-data-plane-00

[23] Davie, Bruce S.; Farrel, Adrian, MPLS: Next Steps, Publisher: Morgan Kaufmann, ISBN: 0123744008, 9780123744005, Chapter 2. Overview of the MPLS Data PLane, 2008

[24] Tan, Nam-Kee, MPLS for metropolitan area networks, ISBN: 084932212x, 084932212x, Chapter 2. Roles of MPLS in Metropolitan Area Networks, 2005

[25] RFC 3032 MPLS Label Stack Encoding, January 2001 http://www.rfc-editor.org/rfc/rfc3032.txt

[26] RFC 3985 Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture, March 2005 http://www.rfc-editor.org/rfc/rfc3985.txt

[27] RFC 5659 An Architecture for Multi-Segment Pseudo Wire Emulation Edge-to-Edge, October 2009 http://tools.ietf.org/html/rfc5659

[28] I-D.ietf-pwe3-p2mp-pw-requirements, Requirements for Point-to-Multipoint Pseudo Wire, January 2010 http://www.ietf.org/id/draft-ietf-pwe3-p2mp-pw-requirements-02.txt

[29] MPLS Working Group, MPLS-TP OAM Framework, December 2009 http://tools.ietf.org/html/draft-ietf-mpls-tp-oam-framework-05

[30] MPLS Working Group, Requirements for OAM in MPLS Transport Networks, December 2009 http://tools.ietf.org/search/draft-ietf-mpls-tp-oam-requirements-06

[31] MPLS Working Group, A framework for MPLS in Transport Networks, February 2010 http://tools.ietf.org/html/draft-ietf-mpls-tp-framework-10

[32] MPLS Working Group, MPLS-TP Requirements, August 2009 http://tools.ietf.org/html/draft-ietf-mpls-tp-requirements-10

[33] UT-STarcom Inc. Broadband Business Unit System Architect, Senior Manager Dr. Wang Yong, Control Protocol and OAM in MPLS-TP Network, Japan 2008 http://www.mpls.jp/1029_yong.pdf

[34] S. Deering Cisco, R. Hinden Nokia, RFC 2460 Internet Protocol Version 6 (IPv6) Specification, December 1998 http://www.faqs.org/rfcs/rfc2460.html

[35] RFC 4385 Pseudo wire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN, February 2006 http://tools.ietf.org/html/rfc4385

[36] ITU-T - IETF Joint Working Team, Dave Ward, Malcolm Betts, ed., MPLS architectural considerations and requirements for a transport profile, April 2008 http://www.ietf.org/MPLS-TP_overview-22.pdf