MPLS Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 19, 2010

M. Bocci, Ed.
Alcatel-Lucent
S. Bryant, Ed.
D. Frost
Cisco Systems
L. Levrau
Alcatel-Lucent

October 16, 2009

Comment [M1]: Should this be moved to the informational track: If so add the "boiler plate text" provided by Adrian.

A Framework for MPLS in Transport Networks
draft-ietf-mpls-tp-framework-06

Status of This Memo

This Internet-Draft will expire on April 19, 2010.

Copyright Notice

Abstract

This document specifies an architectural framework for the application of Multi Protocol Label Switching (MPLS) in transport networks, by enabling the construction of packet switched equivalents to traditional circuit switched carrier networks. It describes a common set of protocol functions - the MPLS Transport Profile (MPLS-TP) - that supports the operational models and capabilities typical of such networks for point-to-point paths, including signaled or explicitly provisioned bi-directional connection-oriented paths, protection and restoration mechanisms, comprehensive Operations, Administration and Maintenance (OAM) functions, and network operation in the absence of a dynamic control plane or IP forwarding support. Some of these functions exist in existing MPLS specifications, while others require extensions to existing specifications to meet the requirements of the MPLS-TP.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [RFC2119].

Although this document is not a protocol specification, these key words are to be interpreted as instructions to the protocol designers producing solutions that satisfy the architectural concepts set out in this document.

Comment [M2]: Add the boiler plate text on ITU-T/IETF cooperation.

Comment [M3]: Are the key words instructions to the protocol designers (like in a requirement document) or instructions to the implementations?

Table of Contents

1. Introduction

1.1. Motivation and Background

This document describes a framework for a Multiprotocol Label Switching Transport Profile (MPLS-TP). It presents the architectural framework for MPLS-TP, defining those elements of MPLS applicable to supporting the requirements in [RFC5654] and what new protocol elements are required.

Historically the optical transport infrastructure (Synchronous Optical Networking (SONET)/Synchronous Digital Hierarchy (SDH), Optical Transport Network (OTN)) has provided carriers with a high benchmark for reliability and operational simplicity. To achieve this transport technologies have been designed with specific characteristics :

- Strictly connection-oriented connectivity, which may be long-lived and may be provisioned ~~manually or~~ by network management.
- A high level of ~~protection and~~ availability.
- Quality of service.
- Extensive~~ded~~ OAM capabilities.

Carriers wish to evolve such transport networks to support packet based services, and to take advantage of the flexibility and cost benefits of packet switching technology. While MPLS is a maturing packet technology that is already playing an important role in transport networks and services, not all of MPLS's capabilities and mechanisms are needed and/or consistent with transport network operations. There are also transport technology characteristics that are not currently reflected in MPLS.

The types of packet transport services delivered by transport networks are ~~very~~ similar to Layer 2 Virtual Private Networks defined by the IETF with two additional objectives:~~.~~

~~There are thus two objectives for MPLS-TP:~~

1. To enable MPLS to be deployed in a transport network and operated in a similar manner to existing transport technologies~~.~~;

and

2. To enable MPLS to support packet transport services with a similar degree of predictability to that found in existing transport networks.

In order to achieve these objectives, there is a need to create a common set of new functions that are applicable to both MPLS networks in general, and those belonging to the MPLS-TP profile.

MPLS-TP therefore defines a profile of MPLS targeted at transport applications and networks. This profile specifies the specific MPLS characteristics and extensions required to meet transport requirements.

1.2. Scope

This document describes an architectural framework for the application of MPLS to transport networks. It specifies the common set of protocol functions that meet the requirements in [RFC5654], and that together constitute the MPLS Transport Profile (MPLS-TP).

The architecture for point-to-point MPLS-TP transport paths is described. The architecture for point-to-multipoint transport paths is outside the scope of this document.

Comment [M4]: Align with RFC 5654

1.3. Terminology

Term	Definition
LSP	Label Switched Path
MPLS-TP	MPLS Transport profile
SDH	Synchronous Digital Hierarchy
ATM	Asynchronous Transfer Mode
OTN	Optical Transport Network
cl-ps	Connectionless - Packet Switched
co-cs	Connection Oriented - Circuit Switched
co-ps	Connection Oriented - Packet Switched
OAM	Operations, Administration and Maintenance
G-ACh	Generic Associated Channel
GAL	Generic Alert Label
MEP	Maintenance End Point
MIP	Maintenance Intermediate Point
APS	Automatic Protection Switching
SCC	Signaling Communication Channel
MCC	Management Communication Channel
EMF	Equipment Management Function
FM	Fault Management
CM	Configuration Management
PM	Performance Management
LSR	Label Switch Router.
MPLS-TP PE	MPLS-TP Provider Edge
MPLS-TP P Router	An MPLS-TP Provider (P) router
PW	Pseudowire
Adaptation	The mapping of client information into the format of the server layer

1.3.1. MPLS Transport Profile.

The MPLS Transport Profile (MPLS-TP) is the subset of MPLS functions that are necessary to meet the requirements in [RFC5654]. Note that MPLS is defined to include any present and future MPLS capability specified by the IETF, including those capabilities specifically added to support the transport network requirement [RFC5654].

1.3.2. MPLS-TP Section

An MPLS-TP Section is defined in Section 1.~~1~~2.2 of [RFC5654].

1.3.3. MPLS-TP Label Switched Path

An MPLS-TP Label Switched Path (MPLS-TP LSP) is an LSP that uses a subset of the capabilities of an MPLS LSP in order to meet the requirements of an MPLS transport network as set out in [RFC5654]. The characteristics of an MPLS-TP LSP are primarily that it:

1. Uses a subset of the MPLS OAM tools defined as described in [I-D.ietf-mpls-tp-oam-framework].

2. Supports ~~only~~ 1+1, 1:1, and 1:N protection functions.

3. Is traffic engineered.

4. May be established and maintained via the management plane or ~~I~~is established and maintained using GMPLS protocols when a control plane is used.

5. LSPs can only be point to point or point to multipoint, i.e. the merging of LSPs is not permitted.

Note that an MPLS LSP is defined to include any present and future MPLS capability include those specifically added to support the transport network requirements.

1.3.4. MPLS-TP Label Switching Router (LSR) and Label Edge Router (LER)

An MPLS-TP Label Switching Router (MPLS-TP LSR) is either an MPLS-TP Provider Edge (MPLS-TP PE) or an MPLS-TP Provider (MPLS-TP P Router) router for a given LSP, as defined below. The terms MPLS-TP PE and MPLS-TP P router describe functions and specific node may undertake ~~both~~ either ~~roles~~role on different LSPs.

Note that the use of the term "router" in this context is historic and neither requires nor precludes the ability to perform IP forwarding.

1.3.4.1. MPLS-TP Provider Edge Router (PE)

An MPLS-TP Provider Edge Router is an MPLS-TP LSR that adapts client traffic and encapsulates it to be carried over an MPLS-TP LSP. Encapsulation may be as simple as pushing a label, or it may require the use of a pseudowire. An MPLS-TP PE exists at the interface between a pair of layer networks. ~~For an~~At a MS-PW stitching point, a~~n~~ MPLS-TP PE is used and it may be either a~~n~~ S-PE or a T-PE.

A layer network is defined in [G.805].

1.3.4.2. MPLS-TP Provider Router (P)

~~An MPLS-TP Provider router is an MPLS-TP LSR that does not provide MPLS-TP PE functionality.~~ An MPLS-TP P router switches LSPs which carry client traffic~~, but~~. It does not adapt the client traffic and encapsulate it to be carried over an MPLS-TP LSP. It may push a label to, for example, multiplex several client MPLS-TP LSPs onto a single server MPLS-TP LSP.

Formatted: Swedish (Sweden)

Comment [j5]: When selection is being performed in a protection function, isn't that a merge function? I believe this is talking about arbitrarily merging traffic from different sources.

Also, is this the implicit requirement for removing PHP? If not, then an additional requirement is needed.

This should be clarified.

Comment [j6]: Istn't it an LER?

Comment [M7]: Please expand these acronyms. Is client adaptation performed at a stitching point if not then why is this a PE function.

Comment [M8]: The MPLS-TP PE also pushes a label…

1.3.5. ~~MPLS-TP~~ Customer Edge (CE)

A~~n MPLS-TP~~ Customer Edge is the client function sourcing or sinking client traffic to or from the MPLS-TP network. CEs on either side of the MPLS-TP network are peers and view the MPLS-TP network as a single point to point or point to multi-point link. These clients have no knowledge of the presence of the intervei~~i~~ning MPLS-TP network.

1.3.6. Additional Definitions and Terminology

Detailed definitions and additional terminology may be found in [RFC5654].

1.4. Applicability

MPLS-TP can be used to construct a packet transport networks and is therefore applicable in any packet transport network application. It is also as an alternative architecture for subsets of a packet network where the transport network operational model is deemed attractive. The following are examples of MPLS-TP applicability models:

1. MPLS-TP provided by a network that only supports MPLS-TP, acting as a server for other layer 1, layer 2 and layer 3 networks (Figure 1) i.e. only MPLS-TP LSPs exist between the LSRs.

2. MPLS-TP provided by a network that also supports non-MPLS-TP functions, acting as a server for other layer 1, layer 2 and layer 3 networks (Figure 2) i.e. both MPLS-TP and "regular" MPLS LSPs exist between the LSRs.

3. MPLS-TP as a server layer for client layer traffic of IP or MPLS networks which do not use functions of the MPLS transport profile (Figure 3).

These models are not mutually exclusive.

Formatted: Swedish (Sweden)

Comment [M9]: The CE is not a part of the MPLS-TP network

Comment [j10]: In a G.800 world, this sounds like the CE is generating MPLS-TP frames and teriminating said frames. I don't believe this is the intent.

I would suggest that the sentance be rewritten as: "A customer Edge provides traffic in a layer above the MPLS-TP network, which will be adapted into MPLS-TP connections by the MPLS-TP PE."

Comment [M11]: The intent is not clear. If MPLS-TP is a part of MPLS how can it be an alternate architecture?

Comment [M12]: But PE2 and PE3 provide some "non" TP functions.

Comment [j13]: I don't see a difference in the two figures. What distinction is trying to be drawn?

Comment [M14]: Not clear how this is different from case 1 above. Is it intended to state that MPLS and MPLS-TP can peer? As implied by figure 3.

MPLS-TP LSP, provided by a network that only supports MPLS-TP, acting as a server
for other layer 1, layer 2 and layer 3 networks.

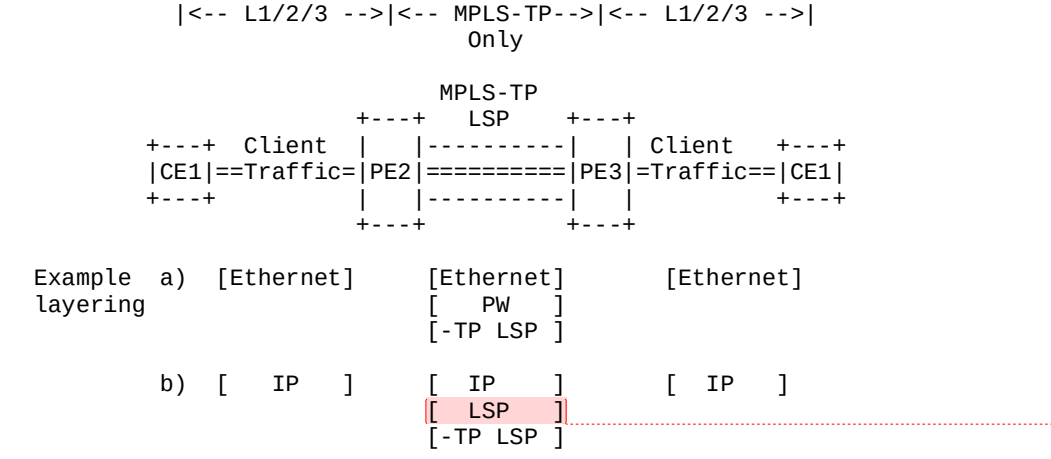


Figure 1: MPLS-TP Server Layer Example

MPLS-TP LSP, provided by a network that also supports non-MPLS-TP functions,
acting as a server for other layer 1, layer 2 and layer 3 networks.

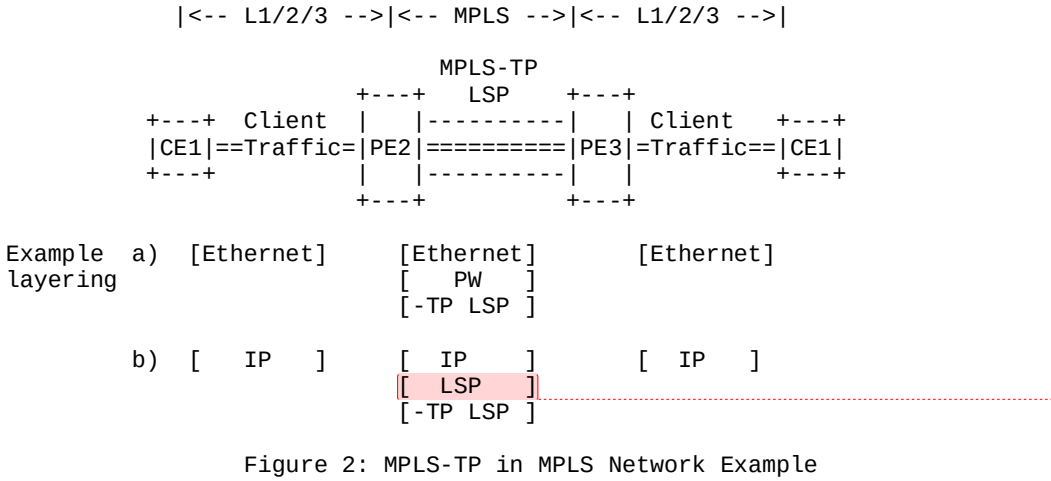


Figure 2: MPLS-TP in MPLS Network Example

Formatted: Swedish (Sweden)

Comment [M15]: Is MPLS the client of MPLS-TP, or is this a MPLS-TP service LSP?

Comment [M16]: Is MPLS the client of MPLS-TP, or is this a MPLS-TP service LSP?

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

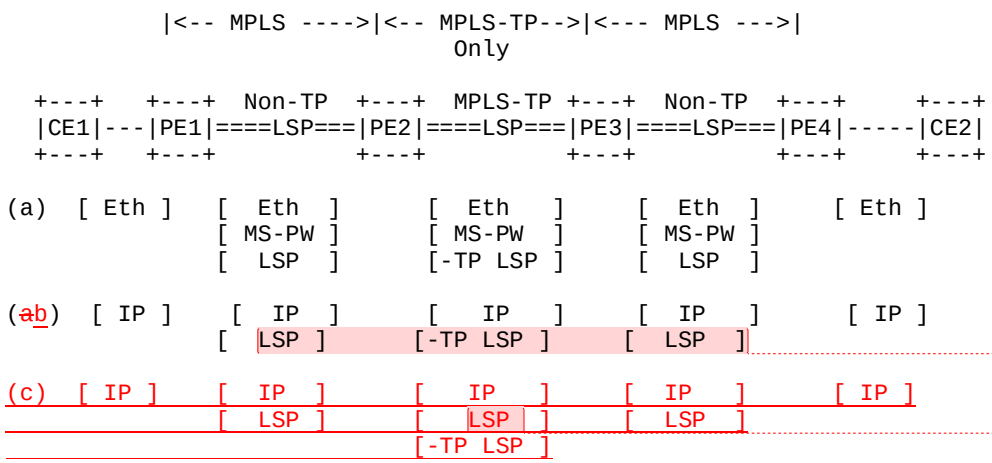


Figure 3: MPLS-TP Transporting Client Service Traffic

2. Introduction to Requirements

The requirements for MPLS-TP are specified in [RFC5654], [I-D.ietf-mpls-tp-oam-requirements], and [I-D.ietf-mpls-tp-nm-req]. This section provides a brief reminder to guide the reader and is therefore not normative. It is not intended as a substitute for these documents.

MPLS-TP must not modify the MPLS forwarding architecture and must be based on existing pseudowire and LSP constructs.

Point to point LSPs may be unidirectional or bi-directional, and it must be possible to construct congruent Bi-directional LSPs.

MPLS-TP LSPs do not merge with other LSPs at an MPLS-TP LSR and it must be possible to detect if a merged LSP has been created.

It must be possible to forward packets solely based on switching the MPLS or PW label. It must also be possible to establish and maintain LSPs and/or pseudowires both in the absence or presence of a dynamic control plane. When static provisioning is used, there must be no dependency on dynamic routing or signaling.

OAM, protection and forwarding of data packets must be able to operate without IP forwarding support.

It must be possible to monitor LSPs and pseudowires through the use of OAM in the absence of control plane or routing functions. In this

Formatted: Swedish (Sweden)

Comment [M17]: Peer relationship?

Comment [M18]: Shows that MPLS may be a client of MPLS-TP

case information gained from the OAM functions is used to initiate path recovery actions at either the PW or LSP layers.

3. Transport Profile Overview

3.1. Packet Transport Services

One objective of MPLS-TP is to enable MPLS networks to provide packet transport services with a similar degree of predictability to that found in existing transport networks. Such packet transport services inherit a number of characteristics, defined in [RFC5654]:

- In an environment where an MPLS-TP layer network is supporting a client layer network, and the MPLS-TP layer network is supported by a server layer network then operation of the MPLS-TP layer network MUST be possible without any dependencies on either the server or client layer network.
- The service provided by the MPLS-TP network to the client is guaranteed not to fall below the agreed level regardless of other client activity.
- The control and management planes of any client network layer that uses the service is isolated from the control and management planes of the MPLS-TP layer network.
- Where a client network makes use of an MPLS-TP server that provides a packet transport service, the level of co-ordination required between the client and server layer networks is minimal (preferably no co-ordination will be required).
- The complete set of packets generated by a client MPLS(-TP) layer network using the packet transport service, which may contain packets that are not MPLS packets (e.g. IP or CNLS packets used by the control/management plane of the client MPLS(-TP) layer network), are transported by the MPLS-TP server layer network.
- The packet transport service enables the MPLS-TP layer network addressing and other information (e.g. topology) to be hidden from any client layer networks using that service, and vice-versa.

Therefore, a packet transport service does not support a connectionless packet switched forwarding mode. However, this does not preclude it carrying client traffic associated with a connectionless service.

Comment [j19]: It isn't clear the difference between the use of "client network" here and "client network" in the next bullet. This may make it hard for agreement to be reached between people familiar with G.800 terminology (which would read these as different in meaning) and people not familiar with G.800 (which may view these as the same).

I suggest that all places where the intent is to talk about nodes in the MPLS-TP switches but are owned by a customer, the term "UNI" be used instead of "client network". This reserves the use of the term "client network" for the purposes defined in G.800.

3.2. Scope of MPLS Transport Profile

Figure 4 illustrates the scope of MPLS-TP. MPLS-TP solutions are primarily intended for packet transport applications. MPLS-TP is a strict sub-set of MPLS, and comprises only those functions that are necessary to meet the requirements of [RFC5654]. This includes MPLS functions that were defined prior to [RFC5654] but that meet the requirements of [RFC5654], together with additional functions defined to meet those requirements. Some MPLS functions defined before [RFC5654] e.g. Equal Cost Multi-Path, LDP signaling used in such a way that it creates multi-point to point LSPs, and IP forwarding in the data plane are explicitly excluded from MPLS-TP by that requirements specification.

Note that this does not preclude the future definition of MPLS functions that do not meet the requirements of [RFC5654] and thus fall outside the scope of MPLS-TP as defined by this document.

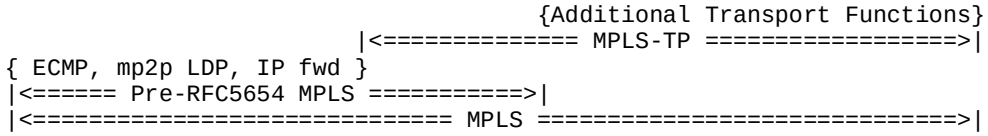


Figure 4: Scope of MPLS-TP

3.3. Architecture

MPLS-TP comprises the following

- Sections, LSPs and PWs that provide a packet transport service for a client network.
- Proactive and on demand Operations Administration and Maintenance (OAM) functions to monitor and diagnose the MPLS-TP network. e.g. connectivity check, connectivity verification, ~~and~~ performance monitoring, fault isolation.
- Optional control planes for LSPs and PWs, as well as static configuration.
- ~~Path~~ Optional path protection mechanisms to ensure that the packet transport service survives anticipated failures and degradations of the MPLS-TP network.

Comment [M20]: The provider may choose to use a control plane and restoration to satisfy the availability objectives.

Formatted: Dutch (Netherlands)

- Network management functions.

The MPLS-TP architecture for LSPs and PWs includes the ~~the~~ following ~~two sets of~~ functions:

- PW adaptation
- PW termination
- MPLS-TP LSP adaptation
- MPLS-TP LSP termination

- MPLS-TP forwarding
- PW stitching

The adaptation functions interface the client service to MPLS-TP. This includes the case where the client service is an MPLS-TP LSP.

Comment [j21]: Is this referring to a client layer? Or is it referring to an service instance generated from a point on the other side of an administrative boundary?

The forwarding functions comprise the mechanisms required for forwarding the encapsulated client over an MPLS-TP server layer network E.g. PW label and LSP label.

3.3.1. MPLS-TP Adaptation

Comment [M22]: Split into LSP and PW

The MPLS-TP adaptation interfaces the client service to MPLS-TP. For pseudowires, these adaptation functions are the payload encapsulation shown in Figure 7 of [RFC3985] and Figure 7 of [I-D.ietf-pwe3-ms-pw-arch]. For network layer client services, the adaptation function uses the MPLS encapsulation format as defined in RFC 3032[RFC3032].

The purpose of this encapsulation is to abstract the client service data plane from the MPLS-TP data plane, thus contributing to the independent operation of the MPLS-TP network.

MPLS-TP is itself a client of an underlying server layer. MPLS-TP is thus also bounded by a set of adaptation functions to this server layer network, which may itself be MPLS-TP. These adaptation functions provide encapsulation of the MPLS-TP frames and for the transparent transport of those frames over the server layer network. The MPLS-TP client inherits its QoS from the MPLS-TP network, which in turn inherits its QoS from the server layer. The server layer must therefore provide the necessary Quality of Service (QoS) to ensure that the MPLS-TP client QoS commitments are satisfied.

3.3.2. MPLS-TP Forwarding Functions

Comment [M23]: Split into LSP and PW

The forwarding functions comprise the mechanisms required for forwarding the encapsulated client over an MPLS-TP server layer network E.g. PW label and LSP label.

MPLS-TP LSPs use the MPLS label switching operations and TTL processing procedures defined in [RFC3031] and [RFC3032]. These operations are highly optimized for performance and are not modified

by the MPLS-TP profile.

In addition, MPLS-TP PWs use the PW and MS-PW forwarding operations defined in[RFC3985] and [I-D.ietf-pwe3-ms-pw-arch]. The PW label is processed by a PW forwarder and is always at the bottom of the label stack for a given MPLS-TP layer network.

Per-platform label space is used for PWs. Either per-platform, per-interface or other context-specific label space may be used for LSPs.

MPLS-TP forwarding is based on the label that identifies the transport path (LSP or PW). The label value specifies the processing operation to be performed by the next hop at that level of encapsulation. A swap of this label is an atomic operation in which the contents of the packet after the swapped label are opaque to the forwarder. The only event that interrupts a swap operation is TTL expiry. This is a fundamental architectural construct of MPLS to be taken into account when design protocol extensions that requires packets (e.g. OAM packets) to be sent to an intermediate LSR.

Further processing to determine the context of a packet occurs when a swap operation is interrupted in this manner, or a pop operation exposes a specific reserved label at the top of the stack. Otherwise the packet is forwarded according to the procedures in [RFC3032].

Point to point MPLS-TP LSPs can be either unidirectional or bidirectional.

It MUST be possible to configure an MPLS-TP LSP such that the forward and backward directions of a bidirectional MPLS-TP LSP are co-routed i.e. they follow the same path. The pairing relationship between the forward and the backward directions must be known at each LSR or LER on a bidirectional LSP.

Comment [j24]: This use of the term “bidirectional LSP” seems to be different than that used in RFC3471.

In normal conditions, all the packets sent over a PW or an LSP follow the same path through the network and those that belong to a common ordered aggregate are delivered in order. For example per-packet equal cost multi-path (ECMP) load balancing is not applicable to MPLS-TP LSPs.

Penultimate hop popping (PHP) is disabled on MPLS-TP LSPs by default.

Comment [j25]: Does this allow for PHP to be enabled? If so, how does it interact with the no merging requirement stated above in item 5 of Section 1.3.3?

Both E-LSP and L-LSP are supported in MPLS-TP, as defined in [RFC3270].

The Traffic Class field (formerly the MPLS EXP field) follows the definition and processing rules of [RFC5462] and [RFC3270].

Only the pipe and short-pipe models are supported in MPLS-TP.

3.4. MPLS-TP Client Adaptation

This document specifies the architecture for two types of client adaptation:

- A PW
- An MPLS Label

When the client is a PW, the MPLS-TP client adaptation functions include the PW encapsulation mechanisms, including the PW control word. When the client is operating at the network layer the mechanism described in Section 3.4.2 is used.

3.4.1. Adaptation using Pseudowires

The architecture for a transport profile of MPLS (MPLS-TP) that uses PWs is based on the MPLS [RFC3031] and pseudowire [RFC3985] architectures. If multi-segment pseudowires are used to provide a packet transport service, motivated by, for example, the requirements specified in [RFC5254] then the MS-PW architecture [I-D.ietf-pwe3-ms-pw-arch] also applies.

Figure 5 shows the architecture for an MPLS-TP network using single-segment PWs.

Formatted: Swedish (Sweden)

Formatted: Portuguese (Brazil)

Comment [M26]: If the client is a PW why is it necessary to include the PW adaptation function?

Comment [j27]: This has an odd interaction with MS-PW, where the S-PE isn't required to understand the PW encapsulation, just switch it from one tunnel to another tunnel.

Comment [M28]: MPLS; MPLS-TP; IP; others?

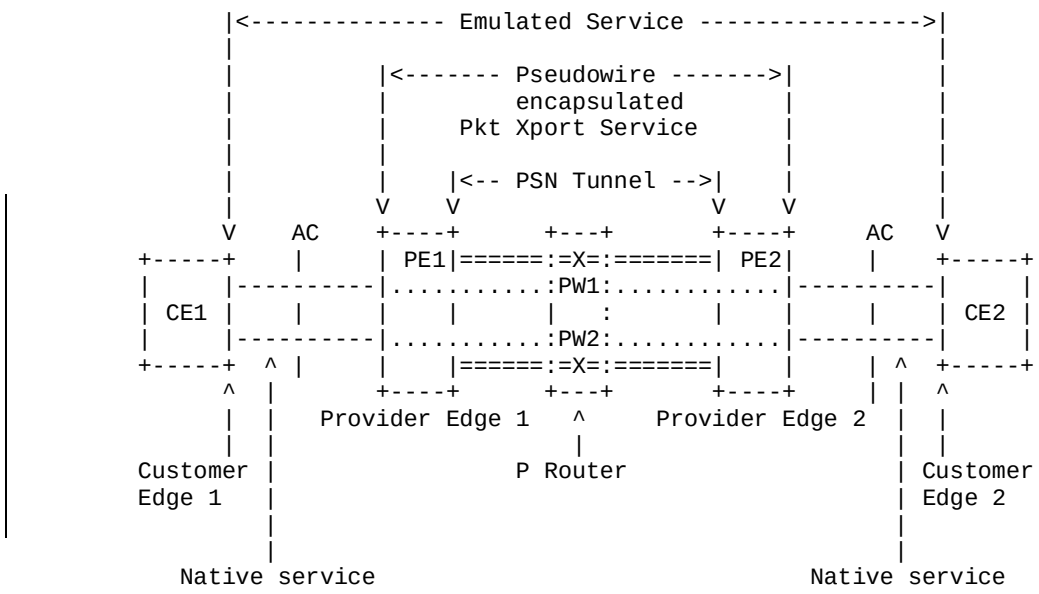


Figure 5: MPLS-TP Architecture (Single Segment PW)

Figure 6 shows the architecture for an MPLS-TP network when multi-segment pseudowires are used. Note that as in the SS-PW case, P-routers may also exist.

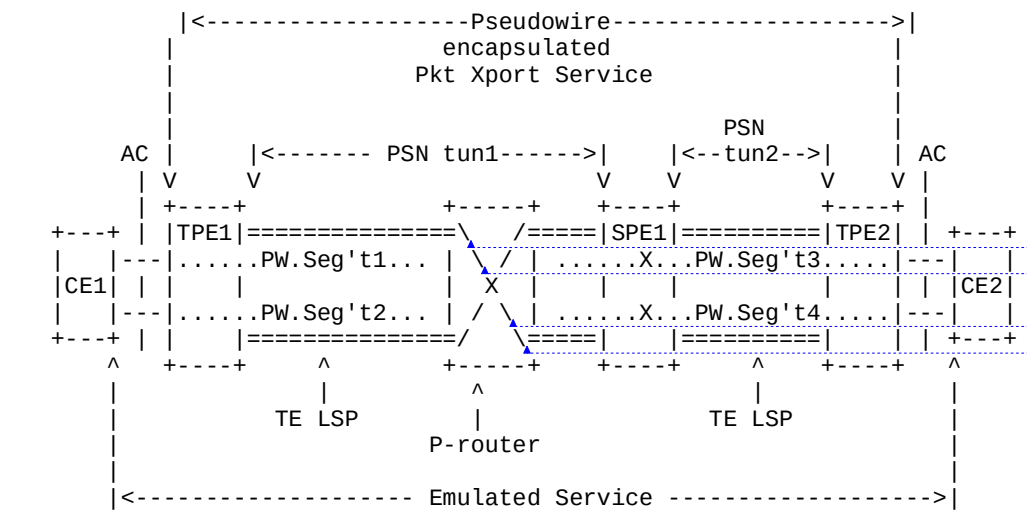
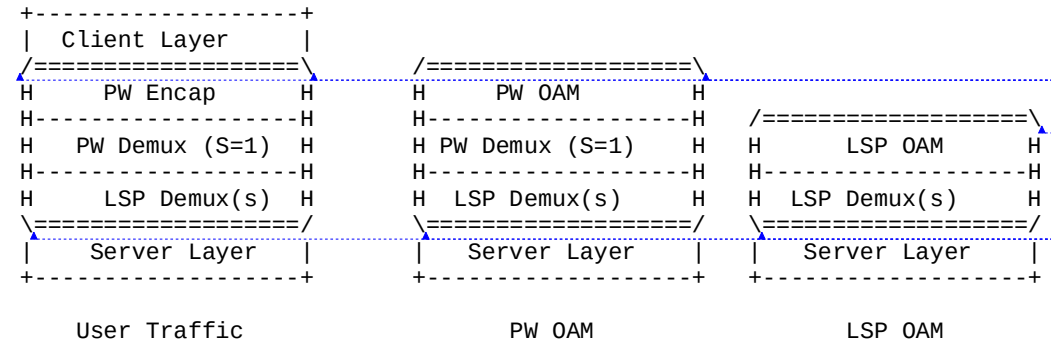


Figure 6: MPLS-TP Architecture (Multi-Segment PW)

The corresponding domain of the MPLS-TP protocol stack including PWs is shown in Figure 7.



Note: Transport Service Layer = PW Demux
Transport Path Layer = LSP Demux

Figure 7: MPLS-TP Layer Network using Pseudowires

When providing a Virtual Private Wire Service (VPWS), Virtual Private Local Area Network Service (VPLS), Virtual Private Multicast Service

Formatted: Swedish (Sweden)
Formatted: Swedish (Sweden)
Formatted: Swedish (Sweden)
Formatted: Swedish (Sweden)
Formatted: Swedish (Sweden)
Formatted: Portuguese (Brazil)
Formatted: Portuguese (Brazil)
Formatted: Portuguese (Brazil)
Formatted: Portuguese (Brazil)
Formatted: Portuguese (Brazil)
Formatted: Portuguese (Brazil)
Formatted: Portuguese (Brazil)

(VPMS) or Internet Protocol Local Area Network Service (IPLS), pseudowires MUST be used to carry the client service. These PWs can be configured either statically or via the control plane defined in [RFC4447].

Note that in MPLS-TP environments where IP is used for control or OAM purposes, IP MAY be carried over the LSP demultiplexers as per RFC3031 [RFC3031], ~~or~~ directly over the server, or over a SCC.

3.4.2. Network Layer Clients

MPLS-TP LSPs can be used to transport network layer clients. Any network layer protocol can be transported between service interfaces. Examples of network layer protocols include IP, MPLS and MPLS-TP.

With network layer transport, the MPLS-TP domain provides a bidirectional point-to-point connection between two customer edge (CE) nodes. Note that a CE may be an an IP, MPLS or MPLS-TP node. As shown in Figure 8, there is an attachment circuit between the CE node on the left and its corresponding provider edge (PE) node that provides the service interface, a bidirectional LSP across the MPLS-TP service network to the corresponding PE node on the right, and an attachment circuit between that PE node and the corresponding CE node for this service.

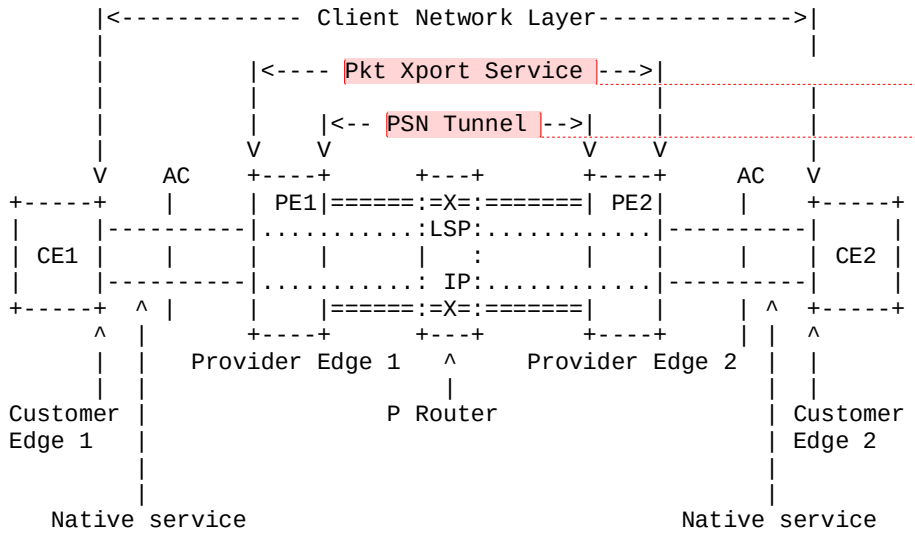


Figure 8: MPLS-TP Architecture for Network Layer Clients

Formatted: Swedish (Sweden)

Comment [M29]: Is this the case described below, if so reference 3.4.2

Comment [M30]: – While the architecture to support PW-encapsulated clients (e.g. clients for which a PW encapsulation is defined) is quite clear, the architecture for supporting Network Layer Client is still not very clear. I can understand different and contradictory ideas in different part of the text below. More detailed comments in line

Comment [M31]: The MPLS-TP connection is between the PE nodes.

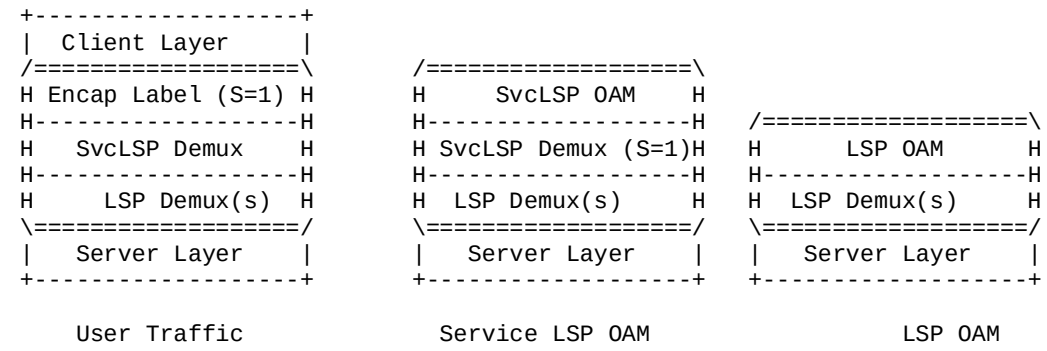
Comment [M32]: The Service LSP is not described. How PE1 maps the AC to the Service LSP and how PE2 maps a Service LSP to an AC is also not described

Comment [M33]: Do we still have an attachment circuit if the client is MPLS or MPLs-TP

Comment [M34]: What is is this service, what is it provided by. Not clear if it can support multiple client protocols or if it is per protocol.

Comment [M35]: Should be PSN tun1 and PSN tun 2 as per PW example above.

At the ingress service interface the PE transforms the ingress packet to the format that will be carried over the transport network, and similarly the corresponding service interface at the egress PE transforms the packet to the format needed by the attached CE. The attachment circuits may be heterogeneous (e.g., any combination of SDH, PPP, Frame Relay etc) and network layer protocol payloads arrive at the service interface encapsulated in the Layer1/Layer2 encoding defined for that access link type. It should be noted that the set of network layer protocols includes MPLS and hence MPLS encoded packets with an MPLS label stack (the client MPLS stack), may appear at the service interface.



Note: Transport Service Layer = SvcLSP Demux
Transport Path Layer = LSP Demux

Note that the functions of the Encap label and the Service Label may represented
by a single label

Figure 9: Domain of MPLS-TP Layer Network for IP and LSP Clients

Within the MPLS-TP transport network, the network layer protocols are carried over the MPLS-TP LSP using a separate MPLS label stack (the server stack). The server stack is entirely under the control of the nodes within the MPLS-TP transport network and it is not visible outside that network. In accordance with [RFC3032], the bottom label, with the 'bottom of stack' bit set to '1', defines the network layer protocol being transported. Figure 9 shows how ~~an~~ a client network protocol stack (which may be an MPLS label stack and payload) is carried over as a network layer transport service over an MPLS-TP transport network.

A label per network layer protocol payload type that is to be

Comment [M36]: From Figure 9, It appears that the pkt Xport Service in Figure 5 is an LSP (called Svc LSP) connecting two ACs. It is not clear whether the Encap Label is an additional label underneath the SvcLSP and used to identify client network layer (PID label).

Comment [M37]: If the S bit =1 is the semantic of the label client protocol identifier (or service identifier) vs. forwarding label when s=0?

transported is REQUIRED. Such labels are referred to as "Service Labels", one of which is shown in Figure 9. The mapping between protocol payload type and Service Label is either configured or signaled.

Service labels are typically carried over an MPLS-TP edge-to-edge LSP, which is also shown in Figure 9. The use of an edge-to-edge LSP is RECOMMENDED when more than one protocol payload type is to be transported. For example, if only MPLS is carried then a single Service Label would be used to provided both payload type indication and the MPLS-TP edge-to-edge LSP. Alternatively, if both IP and MPLS is to be carried then two Service Labels would be mapped on to a common MPLS-TP edge-to-edge LSP.

As noted above, any layer 2 and layer 1 protocols used to carry the network layer protocol over the attachment circuit is terminated at the service interface and is not transported across the MPLS-TP network. This enables the use of different layer 2 / layer 1 technologies at two service interfaces.

At each service interface, Layer 2 addressing must be used to ensure the proper delivery of a network layer packet to the adjacent node. This is typically only an issue for LAN media technologies (e.g., Ethernet) which have Media Access Control (MAC) addresses. In cases where a MAC address is needed, the sending node MUST set the destination MAC address to an address that ensures delivery to the adjacent node. That is the CE sets the destination MAC address to an address that ensures delivery to the PE, and the PE sets the destination MAC address to an address that ensures delivery to the CE. The specific address used is technology type specific and is not covered in this document. In some technologies the MAC address will need to be configured (Examples for the Ethernet case include a configured unicast MAC address for the adjacent node, or even using the broadcast MAC address when the CE-PE service interface is dedicated. The configured address is then used as the MAC destination address for all packets sent over the service interface.)

Note that when the two CEs operating over the network layer transport service are running a routing protocol such as ISIS or OSPF some care should be taken to configure the routing protocols to use point- to-point adjacencies. The specifics of such configuration is outside the scope of this document.

[Editors Note we need to confer with ISIS and OSPF WG to verify that the cautionary note above is necessary and sufficient.]

The CE to CE service types and corresponding labels may be configured or signaled. When they are signaled the CE to PE control channel may

Formatted: Swedish (Sweden)

Comment [M38]: If we have, for example, IP from two different UNI clients how can they be distinguished.

Comment [M39]: Is this a forwarding label or a protocol identifier or both?

Comment [M40]: Is this label stacking, so that we have both a service label and a tunnel label, or are both put into the same LSP (without a service label).

Comment [M41]: Network interworking?

Comment [j42]: This text may be overly specific. The behaviour required is to limit the adjacency to a specific far point user.

Suggest this text be changed to “explicitly configured peer adjacencies”/

Comment [M43]: The label only exists between PEs so what is signalled between the CE and PE?

be either out-of-band or in-band. An out-of-band control channel uses standard GMPLS out-of-band signaling techniques. There are a number of methods that can be used to carry this signalling:

- o It can be carried via an out-of-band control channel. (As is commonly done in today's GMPLS controlled transport networks.)
- o It could be carried over the attachment circuit with MPLS using a reserved label.
- o It could be carried over the attachment circuit with MPLS using a normal label that is agreed between CE and PE.
- o It could be carried over the attachment circuit in an ACH.
- o It could be carried over the attachment circuit in IP.

In the MPLS and ACH cases above, this label value is used to carry LSP signaling without any further encapsulation. This signaling channel is always point-to-point and MUST use local CE and PE addressing.

The method(s) to be used will be described in a future version of the document.

3.5. Identifiers

Identifiers to be used in within MPLS-TP where compatibility with existing MPLS control plane conventions are necessary are described in [draft-swallow-mpls-tp-identifiers-00]. The MPLS-TP requirements [RFC5654] require that the elements and objects in an MPLS-TP environment are able to be configured and managed without a control plane. In such an environment many conventions for defining identifiers are possible. However it is also anticipated that operational environments where MPLS-TP objects, LSPs and PWs will be signaled via existing protocols such as the Label Distribution Protocol [RFC4447] and the Resource Reservation Protocol as it is applied to Generalized Multi-protocol Label Switching ([RFC3471] and [RFC3473]) (GMPLS). [draft-swallow-mpls-tp-identifiers-00] defines a set of identifiers for MPLS-TP which are both compatible with those protocols and applicable to MPLS-TP management and OAM functions.

MPLS-TP distinguishes between addressing used to identify nodes in the network, and identifiers used for demultiplexing and forwarding.

3.6. Operations, Administration and Maintenance (OAM)

~~Whilst IP addressing is used by default,~~ MPLS-TP must be able to operate in environments where IP is not used in the forwarding plane. Therefore, the default mechanism for OAM demultiplexing in MPLS-TP

Comment [M44]: Between the CE and PE, between PEs or between the CEs?

Comment [M45]: Implies a “new” reserved label - Is the intent to used label 13/GAch?

Comment [M46]: How is this carried between PEs

Comment [M47]: Is this the address of the signalling entities or the tunnel end points?

Comment [M48]: We have agreed that MPLS-TP will use a GMPLS control plane

Comment [M49]: These paragraphs should be aligned with the current version of [draft-swallow-mpls-tp-identifiers], that supports both IP-based and ITU-based identifiers for IP and transport applications.

Comment [M50]: Keep in alignment with the OAM framework draft

Comment [M51]: True for pre RFC5317 MPLS. However, after MPLS is extended to include TP then IP addressing cannot be the default for MPLS since MPLS-TP MUST operate in the absence of IP

LSPs and PWs is the generic associated channel
~~. Forwarding based on~~
~~IP addresses for user or OAM packets is not REQUIRED for MPLS-TP.~~

[RFC4379]and BFD for MPLS LSPs [I-D.ietf-bfd-mpls] have defined alert mechanisms that enable an MPLS LSR to identify and process MPLS OAM packets when the OAM packets are encapsulated in an IP header. These alert mechanisms are based on TTL expiration and/or use an IP destination address in the range 127/8. These mechanisms are the default mechanisms for MPLS networks in general for identifying MPLS OAM packets when the OAM packets are encapsulated in an IP header.

MPLS-TP ~~is unable to rely on the availability of IP and thus uses~~MUST be able to operate in an environments where IP forwarding is not supported. Therefore, the GACH/GAL is the default mechanism to demultiplex OAM packets in MPLS-TP.

Comment [M52]: True for pre RFC5317 MPLS. However, after MPLS is extended to include TP then IP addressing cannot be the default for MPLS since MPLS-TP MUST operate in the absence of IP

~~3.6. Operations, Administration and Maintenance (OAM)~~

MPLS-TP supports a comprehensive set of OAM capabilities for packet transport applications, with equivalent capabilities to those provided in SONET/SDH.

MPLS-TP defines mechanisms to differentiate specific packets (e.g. OAM, APS, MCC or SCC) from those carrying user data packets on the same ~~LSP~~transport path (Section, LSP or PW). These mechanisms are described in [RFC5586].

MPLS-TP requires [I-D.ietf-mpls-tp-oam-requirements] that a set of OAM capabilities is available to perform fault management (e.g. fault detection and localization) and performance monitoring (e.g. packet delay and loss measurement) of the LSP, PW or section. The framework for OAM in MPLS-TP is specified in [I-D.ietf-mpls-tp-oam-framework].

MPLS-TP OAM packets share the same fate as their corresponding data packets, and are identified through the Generic Associated Channel mechanism [RFC5586]. This uses a combination of an Associated Channel Header (ACH) and a Generic Alert Label (GAL) to create a control channel associated to an LSP, Section or PW.

3.6.1. OAM Architecture

OAM and monitoring in MPLS-TP is based on the concept of maintenance entities, as described in [I-D.ietf-mpls-tp-oam-framework]. A Maintenance Entity can be viewed as the association of two ~~(or more)~~ Maintenance End Points (MEPs) (see example in Figure 10). Another OAM construct is referred to as Maintenance Entity Group (MEG), which is a collection of one or more MEs that belongs to the same transport path and that are maintained and monitored as a group. A use case for an MEG with more than one ME is point-to-multipoint OAM.The MEPs that form an ME should be configured and managed to limit the OAM responsibilities of an OAM flow within ~~a network or sub- network, or~~the domain of a transport path or segment, in the specific layer network that is

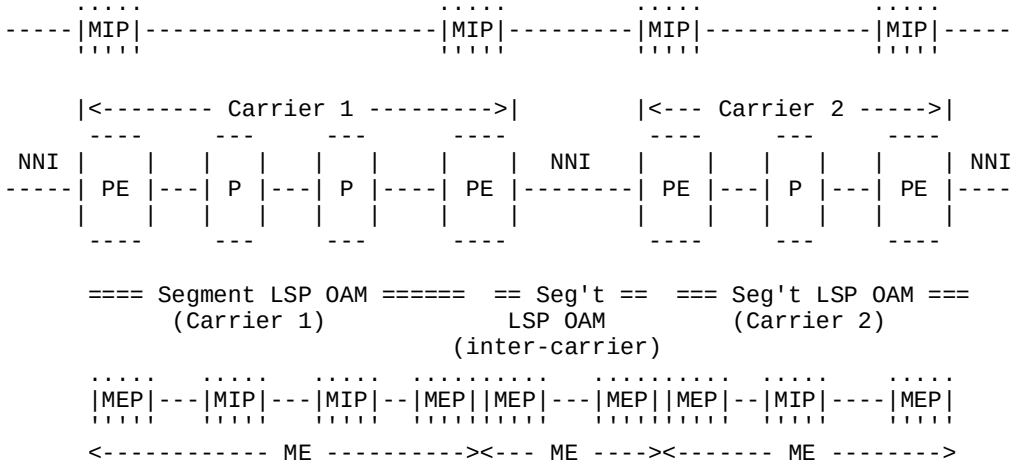
Comment [M53]: Align with OAM framework need to introduce the MEG

being monitored and managed.

Each OAM flow is associated with a single ME. Each MEP within an ME resides at the boundaries of that ME. An ME may also include a set

of zero or more Maintenance Intermediate Points (MIPs), which reside within the Maintenance Entity. Maintenance end points (MEPs) are capable of sourcing and sinking OAM flows, while maintenance intermediate points (MIPs) can only sink or respond to OAM flows from within the MEG.

Comment [M54]: Spontaneous fault notifications (e.g. AIS)

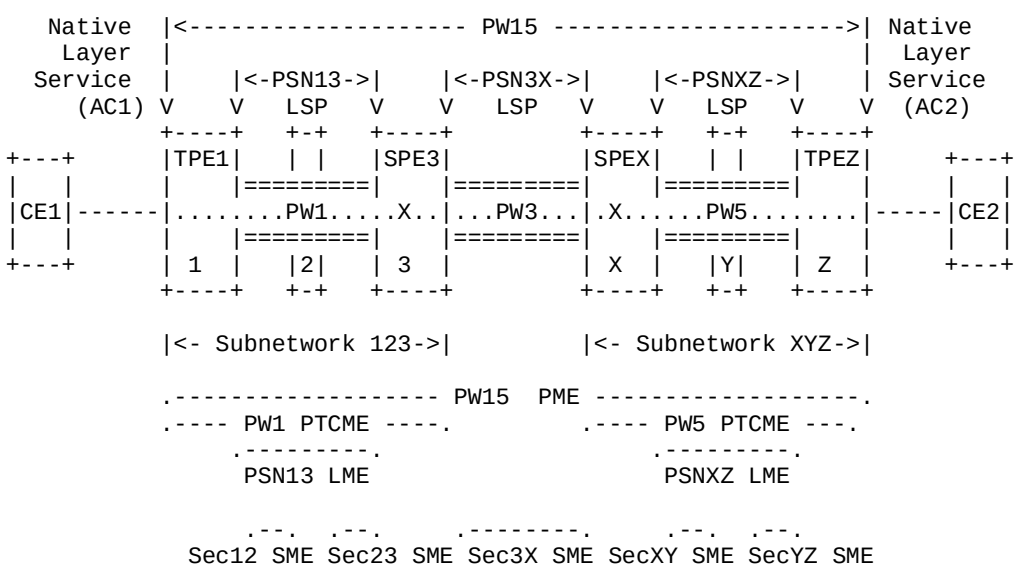


Note: MEPs for End-to-end LSP OAM exist outside of the scope of this figure.

Figure 10: Example of MPLS-TP OAM showing TCM and MIPs

Figure 11 illustrates how the concept of Maintenance Entities can be mapped to sections, LSPs and PWs in an MPLS-TP network that uses MS-PWs.

Formatted: Swedish (Sweden)



TPE1: Terminating Provider Edge 1 SPE2: Switching Provider Edge 3
TPEX: Terminating Provider Edge X SPEZ: Switching Provider Edge Z

.---. ME . MEP ==== LSP .... PW

SME: Section Maintenance Entity
LME: LSP Maintenance Entity
PME: PW Maintenance Entity

Figure 11: Example of PW and MPLS-TP OAM ~~architecture~~

The following MPLS-TP MEs are specified in [I-D.ietf-mpls-tp-oam-framework]:

- A Section Maintenance Entity (SME), allowing monitoring and management of MPLS-TP Sections (between MPLS LSRs).
- A LSP Maintenance Entity (LME), allowing monitoring and management of an end-to-end LSP (between LERs).
- A PW Maintenance Entity (PME), allowing monitoring and management of an end-to-end SS/MS-PWs (between T-PEs).

- An LSP Tandem Connection Maintenance Entity (LTCME), allowing estimation of OAM fault and performance metrics of a single LSP segment or of an aggregate of LSP segments. It also enables any OAM function applied to segment(s) of an LSP to be independent of the OAM function(s) operated on the end-to-end LSP. This can be achieved by including a label representing the LTCME on one or more LSP label stacks for 1:1 or N:1 monitoring of LSPs, respectively. Note that the term Tandem Connection Monitoring has historical significance dating back to the early days of the telephone network, but is equally applicable to the hierarchal architectures commonly employed in todays packet networks.

Individual MIPs along the path of an LSP or PW are addressed by setting the appropriate TTL in the label for the OAM packet, as per [I-D.ietf-pwe3-segmented-pw]. Note that this works when the location of MIPs along the LSP or PW path is known by the MEP. There may be cases where this is not the case in general MPLS networks e.g. following restoration using a facility bypass LSP. In these cases, tools to trace the path of the LSP may be used to determine the appropriate setting for the TTL to reach a specific MIP.

Within an LSR or PE, MEPs and MIPs can only be placed where MPLS layer processing is performed on a packet. The architecture mandates that this must occur at least once.

There is only one MIP on an LSP or PW in each node. That MIP is for all applicable OAM functions on its associated LSP or PW. This document does not specify the default position of the MIP within the node. Therefore, this document does not specify where the exception mechanism resides (i.e. at the ingress interface, the egress interface, or some other location within the node). An optional protocol may be developed that sets the position of a MIP along the path of an LSP or PW within the node (and thus determines the exception processing location).

MEPs may only act as a sink of OAM packets when the label associated with the LSP or PW for that ME is popped. MIPs can only be placed where an exception to the normal forwarding operation occurs. A MEP may act as a source of OAM packets whereever a label is pushed or swapped. For example, on a MS-PW, a MEP may source OAM within an S-PE or a T-PE, but a MIP may only be associated with a S-PE and a sink MEP can only be associated with a T-PE.

3.6.2. OAM Functions

The MPLS-TP OAM architecture support a wide range of OAM functions, including the following

Comment [M55]: Need to also describe for PW – or should all of this be removed and just reference the OAM framework

Comment [M56]: TCM only applies to the 1:1 case – align with the OAM framework (once it is stable).

Comment [M57]: Is TTL expiry valid for a PW?

Comment [M58]: 1) Align with the agreement on 2 MIPs/node in the OAM framework
2) The MIP is optional

- o Continuity Check
- o Connectivity Verification
- o Performance monitoring (e.g. loss and delay)
- o Alarm suppression
- o Remote Integrity

These are applicable to any layer defined within MPLS-TP, i.e. MPLS Section, LSP and PW.

The MPLS-TP OAM toolset needs to be able to operate without relying on a dynamic control plane or IP functionality in the datapath. In the case of MPLS-TP deployment in a network with IP functionality, all existing IP-MPLS OAM functions, e.g. LSP-Ping, BFD and VCCV, may be used. This does not preclude the use of other OAM tools in an IP addressable network.

Comment [M59]: How is this different from the previous sentence?

One use of OAM mechanisms is to detect degradation of the health of an service instance, which may be caused by link failures, node failures and performance outside the required specification which then may be used to trigger recovery actions, according to the requirements of the service.

3.7. Generic Associated Channel (G-ACh)

For correct operation of the OAM it is important that the OAM packets fate share with the data packets. In addition in MPSL-TP it is necessary to discriminate between user data payloads and other types of payload. For example the packet may contain a Signaling Communication Channel (SCC), or a channel used for Automatic Protection Switching (APS) data. Such packets are carried on a control channel associated to the LSP, Section or PW. This is achieved by carrying such packets on a generic control channel associated to the LSP, PW or section.

MPLS-TP makes use of such a generic associated channel (G-ACh) to support Fault, Configuration, Accounting, Performance and Security (FCAPS) functions by carrying packets related to OAM, APS, SCC, MCC or other packet types in band over LSPs or PWs. The G-ACH is defined in [RFC5586] and it is similar to the Pseudowire Associated Channel [RFC4385], which is used to carry OAM packets across pseudowires. The G-ACH is indicated by a generic associated channel header (ACH), similar to the Pseudowire VCCV control word, and this is present for all Sections, LSPs and PWs making use of FCAPS functions supported by the G-ACH.

For pseudowires, the G-ACh use the first nibble of the pseudowire control word to provide the initial discrimination between data packets a packets belonging to the associated channel, as described in [RFC4385]. When the first nibble of a packet, immediately following the label at the bottom of stack, has a value of one, then this packet belongs to a G-ACh. The first 32 bits following the bottom of stack label then have a defined format called an associated channel header (ACH), which further defines the content of the packet. The ACH is therefore both a demultiplexer for G-ACh traffic on the PW, and a discriminator for the type of G-ACh traffic.

When the OAM, or a similar message is carried over an LSP, rather than over a pseudowire, it is necessary to provide an indication in the packet that the payload is something other than a user data packet. This is achieved by including a reserved label with a value of 13 in the label stack. This reserved label is referred to as the 'Generic Alert Label (GAL)', and is defined in [RFC5586]. When a GAL is found anywhere within the label stack it indicates that the payload begins with an ACH. The GAL is thus a demultiplexer for G-ACh traffic on the LSP, and the ACH is a discriminator for the type of traffic carried on the G-ACh. Note however that MPLS-TP forwarding follows the normal MPLS model, and that a GAL is invisible to an LSR unless it is the top label in the label stack. The only other circumstance under which the label stack may be inspected for a GAL is when the TTL has expired. Any MPLS-TP component that intentionally performs this inspection must assume that it is asynchronous with respect to the forwarding of other packets. All operations on the label stack are in accordance with [RFC3031] and [RFC3032].

Comment [M60]: How can the GAL be any where, it must be BoS if it is followed by a ACH – see below.

Comment [M61]: If it is asynchronous how can we support PM?

In MPLS-TP, the 'Generic Alert Label (GAL)' always appears at the bottom of the label stack (i.e. S bit set to 1), however this does not preclude its use elsewhere in the label stack in other applications.

Comment [M62]: How is thias possible – what are the applications.

The G-ACH MUST only be used for channels that are an adjunct to the data service. Examples of these are OAM, APS, MCC and SCC, but the use is not restricted to those names services. The G-ACH MUST NOT be used to carry additional data for use in the forwarding path, i.e. it MUST NOT be used as an alternative to a PW control word, or to define a PW type.

Since the G-ACh traffic is indistinguishable from the user data traffic at the server layer, bandwidth and QoS commitments apply to the gross traffic on the LSP, PW or section. Protocols using the G-ACh must therefore take into consideration the impact they have on the user data that they are sharing resources with. In addition, protocols using the G-ACh MUST conform to the security and congestion

considerations described in [RFC5586]. .

Figure 12 shows the reference model depicting how the control channel is associated with the pseudowire protocol stack. This is based on the reference model for VCCV shown in Figure 2 of [RFC5085].

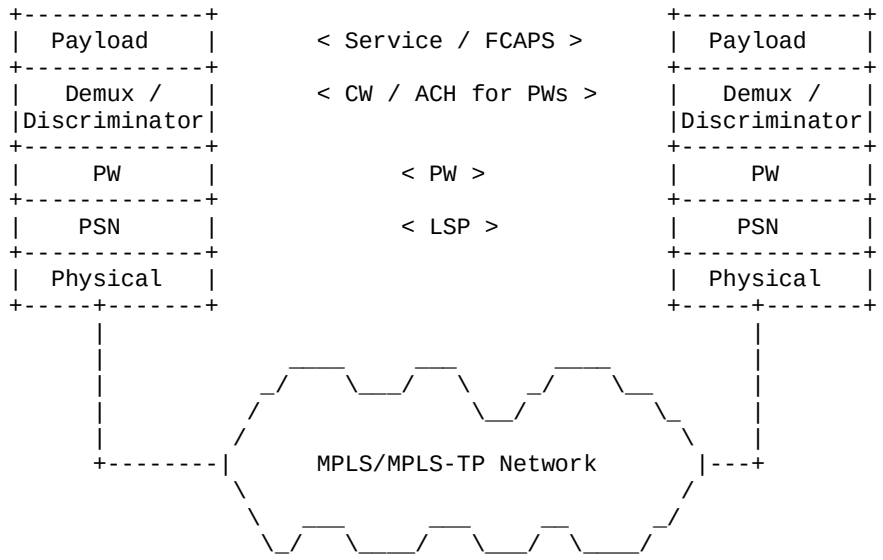


Figure 12: PWE3 Protocol Stack Reference Model including the G-ACh

PW associated channel messages are encapsulated using the PWE3 encapsulation, so that they are handled and processed in the same manner (or in some cases, an analogous manner) as the PW PDUs for which they provide a control channel.

Figure 13 shows the reference model depicting how the control channel is associated with the LSP protocol stack.

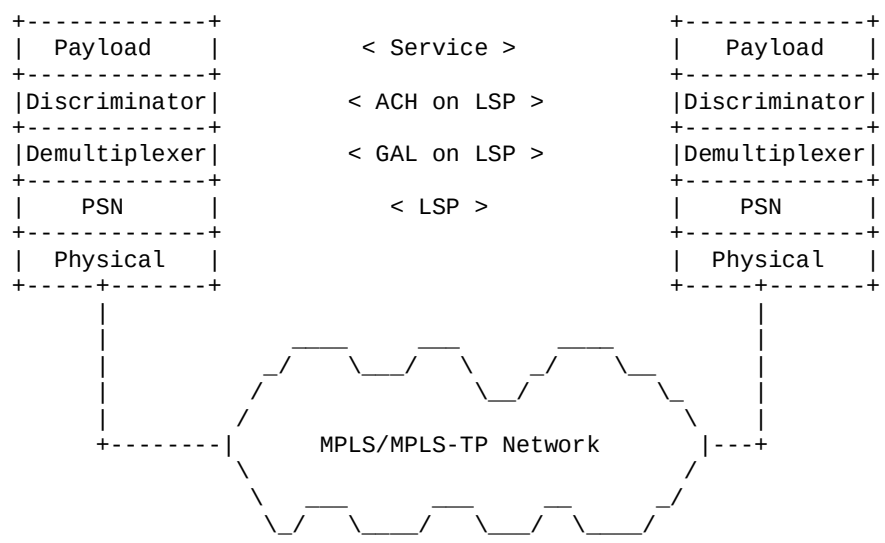


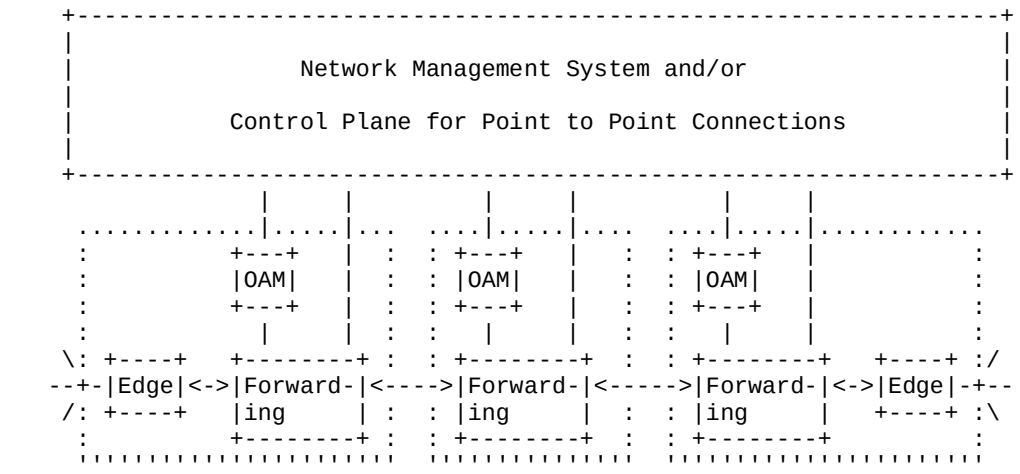
Figure 13: MPLS Protocol Stack Reference Model including the LSP Associated Control Channel

3.8. Control Plane

MPLS-TP should be capable of being operated with centralized Network Management Systems (NMS). The NMS may be supported by a distributed control plane, but MPLS-TP can operated in the absence of such a control plane. A distributed control plane may be used to enable dynamic service provisioning in multi-vendor and multi-domain environments using standardized protocols that guarantee interoperability. Where the requirements specified in [RFC5654] can be met, the MPLS transport profile uses existing control plane protocols for LSPs and PWs.

Figure 14 illustrates the relationship between the MPLS-TP control plane, the forwarding plane, the management plane, and OAM for point-to-point MPLS-TP LSPs or PWs.

Formatted: Swedish (Sweden)



Note:
1) NMS may be centralised or distributed. Control plane is distributed
2) 'Edge' functions refers to those functions present at the edge of a PSN domain, e.g. NSP or classification.
3) The control plane may be transported over the server layer, and LSP or a G-ACh.

Figure 14: MPLS-TP Control Plane Architecture Context

The MPLS-TP control plane is based on a combination of the LDP-based control plane for pseudowires [RFC4447] and the RSVP-TE based control plane for MPLS-TP LSPs [RFC3471]. Some of the RSVP-TE functions that are required for LSP signaling for MPLS-TP are based on GMPLS.

The distributed MPLS-TP control plane may provide~~s~~ the following functions:

o Signaling

o Routing

Comment [M63]: May use NMS for routing initial requests and control plane for routing for restoration.

o Traffic engineering and constraint-based path computation

In a multi-domain environment, the MPLS-TP control plane supports different types of interfaces at domain boundaries or within the domains. These include the User-Network Interface (UNI), Internal Network Node Interface (I-NNI), and External Network Node Interface

(E-NNI). Note that different policies may be defined that control the information exchanged across these interface types.

The MPLS-TP control plane is capable of activating MPLS-TP OAM functions as described in the OAM section of this document Section 3.6 e.g. for fault detection and localization in the event of a failure in order to efficiently restore failed transport paths.

The MPLS-TP control plane supports all MPLS-TP data plane connectivity patterns that are needed for establishing transport paths including protected paths as described in the survivability section Section 3.10 of this document. Examples of the MPLS-TP data plane connectivity patterns are LSPs utilizing the fast reroute backup methods as defined in [RFC4090] and ingress-to-egress 1+1 or 1:1 protected LSPs.

The MPLS-TP control plane provides functions to ensure its own survivability and to enable it to recover gracefully from failures and degradations. These include graceful restart and hot redundant configurations. Depending on how the control plane is transported, varying degrees of decoupling between the control plane and data plane may be achieved.

3.8.1. PW Control Plane

An MPLS-TP network provides many of its transport services using single-segment or multi-segment pseudowires, in compliance with the PWE3 architecture ([RFC3985] and [I-D.ietf-pwe3-ms-pw-arch]). The setup and maintenance of single-segment or multi- segment pseudowires uses the Label Distribution Protocol (LDP) as per [RFC4447] and extensions for MS-PWs [I-D.ietf-pwe3-segmented-pw] and [I-D.ietf-pwe3-dynamic-ms-pw].

3.8.2. LSP Control Plane

MPLS-TP provider edge nodes aggregate multiple pseudowires and carry them across the MPLS-TP network through MPLS-TP tunnels (MPLS-TP LSPs). Applicable functions from the Generalized MPLS (GMPLS) protocol suite supporting packet-switched capable (PSC) technologies are used as the control plane for MPLS-TP transport paths (LSPs).

The LSP control plane includes:

- RSVP-TE for signalling
- OSPF-TE or ISIS-TE for routing

RSVP-TE signaling in support of GMPLS, as defined in [RFC3473], is

used for the setup, modification, and release of MPLS-TP transport paths and protection paths. It supports unidirectional, bi-directional and multicast types of LSPs. The route of a transport path is typically calculated in the ingress node of a domain and the RSVP explicit route object (ERO) is utilized for the setup of the transport path exactly following the given route. GMPLS based MPLS-TP LSPs must be able to inter-operate with RSVP-TE based MPLS-TE LSPs, as per [RFC5146]

OSPF-TE routing in support of GMPLS as defined in [RFC4203] is used for carrying link state information in a MPLS-TP network. ISIS-TE routing in support of GMPLS as defined in [RFC5307] is used for carrying link state information in a MPLS-TP network.

3.9. Static Operation of LSPs and PWs

A PW or LSP may be statically configured without the support of a dynamic control plane. This may be either by direct configuration of the PEs/LSRs, or via a network management system. Static operation is independent for a specific PW or LSP instance – for example it should be possible for a PW to be statically configured, while the LSP supporting it setup by a dynamic control plane.
~~The collateral damage that loops can cause during the time taken to detect the failure may be severe.~~ When static configuration mechanisms are used, care must be taken to ensure that loops ~~to~~ are not ~~form~~created.

3.10. Survivability

Survivability requirements for MPLS-TP are specified in [I-D.ietf-mpls-tp-survive-fwk].

A wide variety of resiliency schemes have been developed to meet the various network and service survivability objectives. For example, as part of the MPLS/PW paradigms, MPLS provides methods for local repair using back-up LSP tunnels ([RFC4090]), while pseudowire redundancy [I-D.ietf-pwe3-redundancy] supports scenarios where the protection for the PW can not be fully provided by the PSN layer (i.e. where the backup PW terminates on a different target PE node than the working PW). Additionally, GMPLS provides a well known set of control plane driven protection and restoration mechanisms [RFC4872]. MPLS-TP provides additional protection mechanisms that are optimised for both linear topologies and ring topologies, and that operate in the absence of a dynamic control plane. These are specified in [I-D.ietf-mpls-tp-survive-fwk].

Different protection schemes apply to different deployment topologies and operational considerations. Such protection schemes may provide different levels of resiliency. For example, two concurrent traffic paths (1+1), one active and one standby path with guaranteed bandwidth on both paths (1:1) or one active path and a standby path that is shared by one or more other active paths (shared protection).

Comment [M64]: Keep in alignment with this dratf

Comment [M65]: How can the path be shared if it is a 1:1 relationship. The resources used by the standby path may be shared

The applicability of any given scheme to meet specific requirements is outside the current scope of this document.

The characteristics of MPLS-TP resiliency mechanisms are listed below.

- Optimised for linear, ring or meshed topologies.
- Use OAM mechanisms to detect and localize network faults or service degenerations.
- Include protection mechanisms to coordinate and trigger protection switching actions in the absence of a dynamic control plane. This is known as an Automatic Protection Switching (APS) mechanism.
- MPLS-TP recovery schemes are applicable to all levels in the MPLS-TP domain (i.e. MPLS section, LSP and PW), providing segment and end-to- end recovery.
- MPLS-TP recovery mechanisms support the coordination of protection switching at multiple levels to prevent race conditions occurring between a client and its server layer.
- MPLS-TP recovery mechanisms can be data plane, control plane or management plane based.
- MPLS-TP supports revertive and non-revertive behavior.

3.11. Network Management

Comment [M66]: Should reference the NM framework and should be kept in alignment with the NM framework.

The network management architecture and requirements for MPLS-TP are specified in [I-D.ietf-mpls-tp-nm-req]. It derives from the generic specifications described in ITU-T G.7710/Y.1701 [G.7710] for transport technologies. It also incorporates the OAM requirements for MPLS Networks [RFC4377] and MPLS-TP Networks [I-D.ietf-mpls-tp-oam-requirements] and expands on those requirements to cover the modifications necessary for fault, configuration, performance, and security in a transport network.

The Equipment Management Function (EMF) of a MPLS-TP Network Element (NE) (i.e. LSR, LER, PE, S-PE or T-PE) provides the means through which a management system manages the NE. The Management Communication Channel (MCC), realized by the G-ACh, provides a logical operations channel between NEs for transferring Management information. For the management interface from a management system to a MPLS-TP NE, there is no restriction on which management protocol should be used. It is used to provision and manage an end-to-end connection across a network where some segments are create/managed,

Comment [M67]: Can only manage nodes – for example a node can be configured to provide one end of a segment.

for examples by Netconf or SNMP and other segments by XML or CORBA interfaces. Maintenance operations are run on a connection (LSP or PW) in a manner that is independent of the provisioning mechanism. An MPLS-TP NE is not required to offer more than one standard management interface. In MPLS-TP, the EMF must be capable of statically provisioning LSPs for an LSR or LER, and PWs for a PE, as per Section 3.9.

Comment [M68]: And any associated MEPs/MIPs

Fault Management (FM) functions within the EMF of an MPLS-TP NE enable the supervision, detection, validation, isolation, correction, and alarm handling of abnormal conditions in the MPLS-TP network and its environment. FM must provide for the supervision of transmission (such as continuity, connectivity, etc.), software processing, hardware, and environment. Alarm handling includes alarm severity assignment, alarm suppression/aggregation/correlation, alarm reporting control, and alarm reporting.

Configuration Management (CM) provides functions to control, identify, collect data from, and provide data to MPLS-TP NEs. In addition to general configuration for hardware, software protection switching, alarm reporting control, and date/time setting, the EMF of the MPLS-TP NE also supports the configuration of maintenance entity identifiers (such as MEP ID and MIP ID). The EMF also supports the configuration of OAM parameters as a part of connectivity management to meet specific operational requirements. These may specify whether the operational mode is one-time on-demand or is periodic at a specified frequency.

The Performance Management (PM) functions within the EMF of an MPLS-TP NE support the evaluation and reporting of the behaviour of the NEs and the network. One particular requirement for PM is to provide coherent and consistent interpretation of the network behaviour in a hybrid network that uses multiple transport technologies. Packet loss measurement and delay measurements may be collected and used to detect performance degradation. This is reported via fault management to enable corrective actions to be taken (e.g. Protection switching), and via performance monitoring for Service Level Agreement (SLA) verification and billing. Collection mechanisms for performance data should be should be capable of operating on-demand or proactively.

4. Security Considerations

The introduction of MPLS-TP into transport networks means that the security considerations applicable to both MPLS and PWE3 apply to those transport networks. Furthermore, when general MPLS networks that utilise functionality outside of the strict MPLS-TP profile are used to support packet transport services, the security

considerations of that additional functionality also apply.

For pseudowires, the security considerations of [RFC3985] and [I-D.ietf-pwe3-ms-pw-arch] apply.

Packets that arrive on an interface with a given label value should not be forwarded unless that label value was previously ~~assigned~~ allocated~~to~~ ~~an~~ for use by a LSP or PW that has been configured to be delivered to ~~a peer LSR or PE that it reachable via~~ that interface.

Each MPLS-TP solution must specify the additional security considerations that apply.

5. IANA Considerations

IANA considerations resulting from specific elements of MPLS-TP functionality will be detailed in the documents specifying that functionality.

This document introduces no additional IANA considerations in itself.

6. Acknowledgements

The editors wish to thank the following for their contribution to this document:

- Rahul Aggarwal
- Dieter Beller
- Lou Berger
- Malcolm Betts
- Italo Busi
- John E Drake
- Hing-Kam Lam
- Marc Lasserre
- Vincenzo Sestito
- Martin Vigoureux

Formatted: Swedish (Sweden)

Comment [M69]: In the past there was some discussion regarding the need to check that the label is received from the interface/server LSP it is expected to be received. Some text needs to be added.

Formatted: Portuguese (Brazil)

Formatted: Italian (Italy)

7. Open Issues

This section contains a list of issues that must be resolved before last call.

- Add addition detail on survivability architectures.
- Consider whether there is too much detail in the OAM, network management, identifiers and control plane sections. Should this framework document reduce the discussion on these topics in order to minimise the dependency on other components not yet ready for publication.
- There is some text missing from the network layer clients section. Text is invited covering the use of out of band signaling on the AC.
- Need text to address how the LSR next hop MAC address is determined for Ethernet link layers when no IP (i.e. ARP) is available. If statically configured, what is the default?
- Are there any other invariants of a typical LSR/PE architecture that need to be clarified in the context of MPLS-TP.

Comment [M70]: Suggest that the level of detail is reduced and reference the survivability framework

Comment [M71]: Level of detail should be reduced.

Comment [M72]: If the signalling is out of band how can it be “on” the AC?

8. References

8.1. Normative References

[G.7710] "ITU-T Recommendation G.7710/ Y.1701 (07/07), "Common equipment management function requirements"", 2005.

[G.805] "ITU-T Recommendation G.805 (11/95), "Generic Functional Architecture of Transport Networks"", November 1995.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3031] Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, January 2001.

[RFC3032] Rosen, E., Tappan, D., Fedorkow, G., Rekhter, Y., Farinacci, D., Li, T., and A. Conta, "MPLS Label Stack Encoding", RFC 3032, January 2001.

[RFC3270] Le Faucheur, F., Wu, L., Davie, B., Davari, S., Vaananen, P., Krishnan, R., Cheval, P., and J. Heinanen, "Multi-Protocol Label Switching (MPLS) Support of Differentiated Services", RFC 3270, May 2002.

[RFC3471] Berger, L., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Functional Description", RFC 3471, January 2003.

[RFC3473] Berger, L., "Generalized Multi-Protocol Label Switching (GMPLS) Signaling Resource ReserVation Protocol-Traffic Engineering (RSVP-TE) Extensions", RFC 3473, January 2003.

[RFC3985] Bryant, S. and P. Pate, "Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture", RFC 3985, March 2005.

[RFC4090] Pan, P., Swallow, G., and A. Atlas, "Fast Reroute Extensions to RSVP-TE for LSP Tunnels", RFC 4090, May 2005.

[RFC4203] Kompella, K. and Y. Rekhter, "OSPF Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", RFC 4203, October 2005.

[RFC4385] Bryant, S., Swallow, G., Martini, L., and D. McPherson, "Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN", RFC 4385,

February 2006.

[RFC4447] Martini, L., Rosen, E., El-Aawar, N., Smith, T., and G. Heron, "Pseudowire Setup and Maintenance Using the Label Distribution Protocol (LDP)", RFC 4447, April 2006.

[RFC4872] Lang, J., Rekhter, Y., and D. Papadimitriou, "RSVP-TE Extensions in Support of End-to-End Generalized Multi-Protocol Label Switching (GMPLS) Recovery", RFC 4872, May 2007.

[RFC5085] Nadeau, T. and C. Pignataro, "Pseudowire Virtual Circuit Connectivity Verification (VCCV): A Control Channel for Pseudowires", RFC 5085, December 2007.

[RFC5307] Kompella, K. and Y. Rekhter, "IS-IS Extensions in Support of Generalized Multi-Protocol Label Switching (GMPLS)", RFC 5307, October 2008.

[RFC5332] Eckert, T., Rosen, E., Aggarwal, R., and Y. Rekhter, "MPLS Multicast Encapsulations", RFC 5332, August 2008.

[RFC5462] Andersson, L. and R. Asati, "Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field", RFC 5462, February 2009.

[RFC5586] Bocci, M., Vigoureux, M., and S. Bryant, "MPLS Generic Associated Channel", RFC 5586, June 2009.

8.2. Informative References

[I-D.ietf-bfd-mpls] Aggarwal, R., Kompella, K., Nadeau, T., and G. Swallow, "BFD

For MPLS LSPs", draft-ietf-bfd-mpls-07 (work in progress), June 2008.

[I-D.ietf-l2vpn-arp-mediation] Rosen, E., Shah, H., Heron, G., and V. Kompella, "ARP Mediation for IP Interworking of Layer 2 VPN", draft-ietf-l2vpn-arp-mediation-12 (work in progress), June 2009.

[I-D.ietf-mpls-tp-nm-req] Gray, E., Mansfield, S., and K. Lam, "MPLS TP Network Management Requirements", draft-ietf-mpls-tp-nm-req-05 (work in progress), September 2009.

[I-D.ietf-mpls-tp-oam-framework] Busi, I. and B. Niven-Jenkins, "MPLS-TP OAM Framework and Overview", draft-ietf-mpls-tp-oam-framework-01 (work in progress), July 2009.

[I-D.ietf-mpls-tp-oam-requirements] Vigoureux, M., Ward, D., and M. Betts, "Requirements for OAM in MPLS Transport Networks", draft-ietf-mpls-tp-oam-requirements-03 (work in progress), August 2009.

[I-D.ietf-mpls-tp-rosetta-stone] Helvoort, H., Andersson, L., and N. Sprecher, "A Thesaurus for the Terminology used in Multiprotocol Label Switching Transport Profile (MPLS-TP) drafts/RFCs and ITU-T's Transport Network Recommendations.", draft-ietf-mpls-tp-rosetta-stone-00 (work in progress), June 2009.

[I-D.ietf-mpls-tp-survive-fwk] Sprecher, N., Farrel, A., and H. Shah, "Multiprotocol Label Switching Transport Profile Survivability Framework", draft-ietf-mpls-tp-survive-fwk-00 (work in progress), April 2009.

[I-D.ietf-pwe3-dynamic-ms-pw] Martini, L., Bocci, M., Bitar, N., Shah, H., Aissaoui, M., and F. Balus, "Dynamic Placement of Multi Segment Pseudo Wires", draft-ietf-pwe3-dynamic-ms-pw-09 (work in progress), March 2009.

[I-D.ietf-pwe3-ms-pw-arch] Bocci, M. and S. Bryant, "An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge", draft-ietf-pwe3-ms-pw-arch-07 (work in progress), July 2009.

[I-D.ietf-pwe3-redundancy] Muley, P. and M. Bocci, "Pseudowire (PW) Redundancy", draft-ietf-pwe3-redundancy-01 (work in progress), September 2008.

[I-D.ietf-pwe3-segmented-pw] Martini, L., Nadeau, T., Metz, C., Duckett, M., Bocci, M., Balus, F., and M. Aissaoui, "Segmented Pseudowire", draft-ietf-pwe3-segmented-pw-13 (work in progress), August 2009.

[RFC0826] Plummer, D., "Ethernet Address Resolution Protocol: Or converting network protocol addresses to 48.bit Ethernet address for transmission on Ethernet hardware", STD 37, RFC 826, November 1982.

[RFC2390] Bradley, T., Brown, C., and A. Malis, "Inverse Address Resolution Protocol", RFC 2390, September 1998.

[RFC2461] Narten, T., Nordmark, E., and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)", RFC 2461, December 1998.

[RFC3122] Conta, A., "Extensions to IPv6 Neighbor Discovery for Inverse Discovery Specification",

RFC 3122, June 2001.

[RFC4377] Nadeau, T., Morrow, M., Swallow, G., Allan, D., and S. Matsushima, "Operations and Management (OAM) Requirements for Multi-Protocol Label Switched (MPLS) Networks", RFC 4377, February 2006.

[RFC4379] Kompella, K. and G. Swallow, "Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures", RFC 4379, February 2006.

[RFC5146] Kumaki, K., "Interworking Requirements to Support Operation of MPLS-TE over GMPLS Networks", RFC 5146, March 2008.

[RFC5254] Bitar, N., Bocci, M., and L. Martini, "Requirements for Multi-Segment Pseudowire Emulation Edge-to-Edge (PWE3)", RFC 5254, October 2008.

[RFC5654] Niven-Jenkins, B., Brungard, D., Betts, M., Sprecher, N., and S. Ueno, "Requirements of an MPLS Transport Profile", RFC 5654, September 2009.

Authors' Addresses

Matthew Bocci (editor)
Alcatel-Lucent
Voyager Place, Shoppenhangers Road
Maidenhead, Berks SL6 2PJ
United Kingdom

Phone:
EMail: matthew.bocci@alcatel-lucent.com

Stewart Bryant (editor)
Cisco Systems
250 Longwater Ave
Reading RG2 6GB
United Kingdom

Phone:
EMail: stbryant@cisco.com

Dan Frost
Cisco Systems

Phone:
Fax:
EMail: danfrost@cisco.com
URI:

Lieven Levrau
Alcatel-Lucent
7-9, Avenue Morane Sulnier
Velizy 78141
France

Phone:
EMail: lieven.levrau@alcatel-lucent.com