ATTACHMENT
TO COM 15-LS 136

Formatted: Centered

MPLS Working Group M. Bocci, Ed.
Internet-Draft Alcatel-Lucent
Intended status: Informational S. Bryant, Ed.
Expires: August 8, 2010 D. Frost, Ed.
Cisco Systems
L. Levrau
Alcatel-Lucent
L. Berger
LabN
February 4, 2010

Comment [M1]: Add note for RFC editor to add boiler plate text on approved via IETF consensus process.

A Framework for MPLS in Transport Networks
draft-ietf-mpls-tp-framework-10

Abstract

This document specifies an architectural framework for the application of Multiprotocol Label Switching (MPLS) to the construction of packet-switched transport 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, 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 are defined in existing MPLS specifications, while others require extensions to existing specifications to meet the requirements of the MPLS-TP.

This document defines the subset of the MPLS-TP applicable in general and to point-to-point paths. The remaining subset, applicable specifically to point-to-multipoint paths, are out of scope of this document.

This document is a product of a joint Internet Engineering Task Force (IETF) / International Telecommunications Union Telecommunications Standardization Sector (ITU-T) effort to include an MPLS Transport Profile within the IETF MPLS and PWE3 architectures to support the capabilities and functionalities of a packet transport network as defined by the ITU-T.

Status of This Memo

ATTACHMENT
TO COM 15-LS 136

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at http://www.ietf.org/ietf/1id-abstracts.txt.

The list of Internet-Draft Shadow Directories can be accessed at http://www.ietf.org/shadow.html.

This Internet-Draft will expire on August 8, 2010.

Copyright Notice

Table of Contents

1. Introduction

1.1. Motivation and Background

This document describes an architectural framework for the application of MPLS to the construction of packet-switched 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) for point-to-point paths. The remaining MPLS-TP functions, applicable specifically to point-to-multipoint paths, are out of scope of this document.

Historically the optical transport infrastructure - Synchronous Optical Network/Synchronous Digital Hierarchy (SONET/SDH) and 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 (i.e. configuration of the node via a command line interface) or by network management.
- A high level of availability.
- Quality of service.
- Extensive OAM capabilities.

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

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.
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 define a common set of MPLS protocol functions - an MPLS Transport Profile - for the use of MPLS in transport networks and applications. Some of the necessary functions are provided by existing MPLS specifications, while others require additions to the MPLS tool-set. Such additions should, wherever possible, be applicable to MPLS networks in general as well as those that conform strictly to the transport network model.

This document is a product of a joint Internet Engineering Task Force (IETF) / International Telecommunications Union Telecommunications Standardization Sector (ITU-T) effort to include an MPLS Transport Profile within the IETF MPLS and PWE3 architectures to support the capabilities and functionalities of a packet transport network as defined by the ITU-T.

1.2. Scope

This document describes an architectural framework for the application of MPLS to the construction of packet-switched 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) for point-to-point MPLS-TP transport paths. The remaining MPLS-TP functions, applicable specifically to point-to-multipoint transport paths, are out of scope of this document.

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	G-ACh 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 Switching Router
MPLS-TP PE	MPLS-TP Provider Edge LSR
MPLS-TP P	MPLS-TP Provider LSR
PW	Pseudowire
AC	Attachment Circuit
Adaptation	The mapping of client information into a format suitable for transport by the server layer
Native Service	The traffic belonging to the client of the MPLS-TP network
T-PE	PW Terminating Provider Edge
S-PE	PW Switching provider Edge

Comment [M2]: The MPLS-TP OAM framework draft uses the MEG . MEP is a Maintenance entity group End Point. MIP is a MEG Intermediate Point. Please align with the latest version of the MPLS-TP OAM framework draft.

1.3.1. Transport Network

A Transport Network provides transparent transmission of client user plane traffic between attached client devices by establishing and maintaining point-to-point or point-to-multipoint connections between such devices. The architecture of networks supporting point to multipoint connections is out of scope of this document. A Transport Network is independent of any higher-layer network that may exist between clients, except to the extent required to supply this transmission service. In addition to client traffic, a Transport Network may carry traffic to facilitate its own operation, such as that required to support connection control, network management, and

Operations, Administration and Maintenance (OAM) functions.

See also the definition of Packet Transport Service in Section 3.1.

1.3.2. MPLS Transport Profile

The MPLS Transport Profile (MPLS-TP) is the subset of MPLS functions that 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 transport network requirements [RFC5654].

1.3.3. MPLS-TP Section

An MPLS-TP Section is defined in Section 1.2.2 of [RFC5654].

1.3.4. 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 1+1, 1:1, and 1:N protection functions.

3. Is traffic engineered.

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

5. Is either point-to-point or point-to-multipoint. Multipoint to point and multipoint to multipoint LSPs are not permitted.

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

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

An MPLS-TP Label Switching Router (LSR) is either an MPLS-TP Provider Edge (PE) router or an MPLS-TP Provider (P) router for a given LSP, as defined below. The terms MPLS-TP PE router and MPLS-TP P router describe logical functions; a specific node may undertake only one of these roles on a given LSP.

Comment [M3]: The text below states that a LER is a type of LSR.

Comment [M4]: Text added below to clarify where push/pop/swap are performed.

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

1.3.5.1. MPLS-TP Provider Edge (PE) Router

An MPLS-TP Provider Edge (PE) router is an MPLS-TP LSR that adapts client traffic and encapsulates it to be transported 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 MS-PW, an MPLS-TP PE may be either an S-PE or a T-PE, as defined in [RFC5659]. A PE pushes or pops a label and is therefore a LER.

1.3.5.2. MPLS-TP Provider (P) Router

An MPLS-TP Provider router is an MPLS-TP LSR that does not provide MPLS-TP PE functionality for a given LSP. An MPLS-TP P router switches LSPs which carry client traffic, but does not adapt client traffic and encapsulate it to be carried over an MPLS-TP LSP. A P router only pushes or pops a label if it is at the end of a PST, in this case it is an LER otherwise it only performs a swap operation.

1.3.5.3. Label Edge Router (LER)

An LSR that exists at the endpoints of an LSP and therefore pushes or pops a label, i.e. does not perform a label swap on the particular LSP under consideration.

1.3.6. Customer Edge (CE)

A Customer Edge (CE) is the client function sourcing or sinking native service 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-multipoint~~ link.

Comment [M5]: Scope is point to point only: Will this definition be extended in the p2mp framework. Should also include rooted multi point links.

1.3.7. Edge-to-Edge LSP

An Edge-to-Edge LSP is an LSP between a pair of PEs that may transit zero or more provider LSRs. When carrying PWs, the edge-to-edge LSP is equivalent to the PSN Tunnel LSP in [RFC 385] terminology.

1.3.8. Service LSP

A service LSP is an LSP that carries a single client service.

1.3.9. Layer Network

A layer network is defined in [G.805] and described in [RFC5654].

1.3.10. Additional Definitions and Terminology

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

1.4. Applicability

MPLS-TP can be used to construct packet ~~transport~~ networks and is therefore applicable in any packet ~~transport~~ network context. ~~It~~ A subset of MPLS-TP is also applicable to ~~subsets of a~~ packet transport networks, as defined by the ITU-T 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 LSPs and PWs (i.e. Only MPLS-TP LSPs and PWs exist between the PEs or LSRs), acting as a server for other layer 1, layer 2 and layer 3 networks (Figure 1).

2. MPLS-TP provided by a network that also supports non-MPLS-TP LSPs and PWs (i.e. both LSPs and PWs that conform to the transport profile and those that do not, exist between the PEs), acting as a server for other layer 1, layer 2 and layer 3 networks (Figure 2).

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. For MPLS traffic, the MPLS-TP server layer network uses PW switching [RFC5659] or LSP stitching [RFC5150] at the PE that terminates the MPLS-TP server layer (Figure 3).

These models are not mutually exclusive.

Comment [M6]: Clarify that the ITU-T applications only use a subset of the full MPLS-TP capabilities.

ATTACHMENT
TO COM 15-LS 136

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.

```
           |<-- L1/2/3 -->|<-- MPLS-TP-->|<-- L1/2/3 -->|
                                Only

                              MPLS-TP
                        +---+   LSP    +---+
          +---+  Client  |   |----------|   | Client   +---+
          |CE1|==Traffic=|PE2|==========|PE3|=Traffic==|CE1|
          +---+          |   |----------|   |          +---+
                        +---+          +---+

  Example  a)  [Ethernet]     [Ethernet]     [Ethernet]
  layering                    [   PW   ]
                              [-TP LSP ]

           b)  [   IP   ]     [  IP    ]     [  IP   ]
                              [ Demux  ]
                              [-TP LSP ]
```

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.

```
           |<-- L1/2/3 -->|<-- MPLS -->|<-- L1/2/3 -->|

                              MPLS-TP
                        +---+   LSP    +---+
          +---+  Client  |   |----------|   | Client   +---+
          |CE1|==Traffic=|PE2|==========|PE3|=Traffic==|CE1|
          +---+          |   |----------|   |          +---+
                        +---+          +---+

  Example  a)  [Ethernet]      [Ethernet]     [Ethernet]
  layering                     [   PW   ]
                               [-TP LSP ]

           b)  [   IP   ]      [  IP    ]     [  IP   ]
                               [ Demux  ]
                               [-TP LSP ]
```

Figure 2: MPLS-TP in MPLS Network Example

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.

```
             |<-- MPLS ---->|<-- MPLS-TP-->|<--- MPLS --->|
                                   Only

   +---+   +-----+  Non-TP  +-----+  MPLS-TP +-----+  Non-TP  +-----+   +---+
   |CE1|---|T-PE|====LSP===|S-PE|====LSP===|S-PE|====LSP===|S-PE|---|CE2|
   +---+   +-----+          +-----+          +-----+          +-----+   +---+
                     (PW switching)  (PW switching)

 (a)  [ Eth ]   [    ~~Eth~~  ]       [  Eth   ]      [  ~~Eth~~  ]      [ Eth ]
                [ PW Seg ]       [ PW Seg ]      [ PW Seg ]
                [   LSP  ]       [-TP LSP ]      [   LSP  ]



           |<-- MPLS ---->|<-- MPLS-TP-->|<--- MPLS --->|
                                 Only

   +---+   +-----+  Non-TP  +-----+  MPLS-TP +-----+  Non-TP  +-----+   +---+
   |CE1|---| PE |====LSP===| PE |====LSP===| PE |====LSP===| PE |---|CE2|
   +---+   +-----+          +-----+          +-----+          +-----+   +---+
                     (LSP stitching) (LSP stitching)

 (b)  [ IP ]       [  ~~IP~~  ]       [  IP   ]      [  ~~IP~~   ]      [ IP  ]
                   [  LSP ]       [-TP LSP ]      [  LSP   ]
```

Figure 3: MPLS-TP Transporting Client Service Traffic

Comment [M7]: Clarify that Eth is edge to edge and is not visible in the S-PE nodes

Comment [M8]: Clarify that IP is not visible at the LSP stitching points

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

3. MPLS 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 the client network layer is considered to be the native service of the MPLS-TP 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 CLNS packets used by the control/management plane of the client MPLS(-TP) layer network), are transported by the MPLS-TP server layer network.

- o 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.

These characteristics imply that 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.

Such packet transport services are very similar to Layer 2 Virtual Private Networks as defined by the IETF.

3.2. Scope of the 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 subset 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] such as Equal Cost Multi-Path, LDP signaling used in such a way that it creates multipoint-to-point LSPs, and IP forwarding in the data plane are explicitly excluded from MPLS-TP by that requirements specification.

Note that MPLS as a whole will continue to evolve to include additional functions that do not conform to the MPLS Transport Profile or its requirements, and thus fall outside the scope of MPLS-TP.

```
 |<============================== MPLS ==============================>|


 |<============= Pre-RFC5654 MPLS ================>|
   {      ECMP       }
   { LDP/non-TE LSPs }
   {     IP fwd      }

                     |<================ MPLS-TP ====================>|
                                                { Additional }
                                                {  Transport }
                                                {  Functions }
```

Figure 4: Scope of MPLS-TP

3.3. Architecture

MPLS-TP comprises the following architectural elements:

- A standard MPLS data plane [RFC3031] as profiled in [I-D.fbb-mpls-tp-data-plane].
- 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, such as connectivity check, connectivity verification, performance monitoring and fault localisation.
- Optional control planes for LSPs and PWs, as well as support for static provisioning and configuration.
- Optional path protection mechanisms to ensure that the packet transport service survives anticipated failures and degradations of the MPLS-TP network.
- Network management functions.

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

- MPLS-TP client adaptation
- MPLS-TP forwarding

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

The forwarding functions comprise the mechanisms required for forwarding the encapsulated client traffic over an MPLS-TP server layer network, for example PW and LSP labels.

3.3.1. MPLS-TP Client Adaptation Functions

Formatted: English (United States)

The MPLS-TP native service adaptation functions interface the client service to MPLS-TP. For pseudowires, these adaptation functions are the payload encapsulation described in Section 4.4 of [RFC3985] and Section 6 of [RFC5659]. For network layer client services, the adaptation function uses the MPLS encapsulation format as defined in [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 Quality of Service (QoS) from the MPLS-TP network, which in turn inherits its QoS from the server layer. The server layer must therefore provide the necessary QoS to ensure that the MPLS-TP client QoS commitments can be satisfied.

3.3.2. MPLS-TP Forwarding Functions

The forwarding functions comprise the mechanisms required for forwarding the encapsulated client over an MPLS-TP server layer network, for example PW and LSP labels.

MPLS-TP LSPs use the MPLS label switching operations and TTL processing procedures defined in [RFC3031], ~~and~~ [RFC3032] and [RFC3443]. These operations are highly optimised for performance and are not modified by the MPLS-TP profile.

In addition, MPLS-TP PWs use the SS-PW and optionally MS-PW forwarding operations defined in [RFC3985] and [RFC5659]. ~~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 [RFC5331] 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 designing protocol extensions that require 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, or the packet is received with the GAL (Section 3.6) at the top of stack.

Comment [M9]: As defined in draft fbb-mpls-tp-data-plane

Comment [M10]: PW forwarder is not mentioned in this draft.

Comment [M11]: Do we need the next 3 paragraphs, a reference to fbb-mpls-tp-data-plane may be more appropriate

ATTACHMENT
TO COM 15-LS 136

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. 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.

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.

MPLS-TP supports Quality of Service capabilities via the MPLS Differentiated Services (DiffServ) architecture [RFC3270]. Both E-LSP and L-LSP MPLS DiffServ modes are supported. The Traffic Class field (formerly the EXP field) of an MPLS label follows the definition and processing rules of [RFC5462] and [RFC3270]. Note that packet reordering between flows belonging to different traffic classes may occur if more than one traffic class is supported on a single LSP or PW.

Only the Pipe and Short Pipe DiffServ tunnelling and TTL processing models described in [RFC3270] and [RFC3443] are supported in MPLS-TP.

3.4. MPLS-TP Native Services

This document describes the architecture for two native service adaptation mechanisms, which provide encapsulation and demultiplexing for native service traffic traversing an MPLS-TP network:

- A PW

- An MPLS Label

Formatted: Spanish (Spain, Traditional Sort)

A PW provides any emulated service that the IETF has defined to be provided by a PW, for example Ethernet, Frame Relay, or PPP/HDLC. A registry of PW types is maintained by IANA. When the native service adaptation is via a PW, the mechanisms described in Section 3.4.2 are used.

An MPLS LSP Label can also be used as the adaptation, in which case any native service traffic type supported by [RFC3031] and [RFC3032] is allowed. Examples of such traffic types include IP, and MPLS-labeled packets. Note that the latter case includes TE-LSPs [RFC3209] and LSP based applications such as PWs, Layer 2 VPNs [RFC4664], and Layer 3 VPNs [RFC4364]. When the native service adaptation is via an MPLS label, the mechanisms described in Section 3.4.3 are used.

3.4.1. MPLS-TP Client/Server Relationship

The MPLS-TP client server relationship is defined by the MPLS-TP network boundary and the label context. It is not explicitly indicated in the packet. In terms of the MPLS label stack, when the client traffic type of the MPLS-TP network is an MPLS LSP or a PW, then the S bits of all the labels in the MPLS-TP label stack carrying that client traffic are zero; otherwise the bottom label of the MPLS-TP label stack has the S bit set to 1 (i.e. there can only one S bit set in a label stack).

The data plane behaviour of MPLS-TP is the same as the best current practise for MPLS. This includes the setting of the S-Bit. In each case, the S-bit is set to indicate the bottom (i.e. inner-most) label in the label stack that is contiguous between the MPLS-TP server and the client layer. Note that this best current practise differs slightly from [RFC3032] which uses the S-bit to identify when MPLS label processing stops and network layer processing starts.

The relationship of MPLS-TP to its clients is illustrated in Figure 5.

```
   PW-Based              MPLS Labelled                IP
   Services                 Services                Transport
 |------------|  |-----------------------------|  |------------|

   Emulated        PW over LSP      IP over LSP         IP
   Service
                  +------------+
                  | PW Payload |
                  +------------+  +------------+              (CLIENTS)
                  |PW Lbl(S=1) |  |     IP     |
 +------------+   +------------+  +------------+  +------------+
 | PW Payload |   |LSP Lbl(S=0)|  |LSP Lbl(S=1)|  |     IP     |
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
 |PW Lbl (S=1)|   |LSP Lbl(S=0)|  |LSP Lbl(S=0)|  |LSP Lbl(S=1)|
 +------------+   +------------+  +------------+  +------------+
 |LSP Lbl(S=0)|
 +------------+                                               (MPLS-TP)
```

~~~~~~~~~~~ denotes Client <-> MPLS-TP layer boundary

Note that in the PW over LSP case the client may omit its LSP Label if penultimate hop popping has been agreed with ~~its~~ the peer CE.

Comment [M12]: Editorial – clarify that the peer must be another CE

Figure 5: MPLS-TP - Client Relationship

~~The data plane behaviour of MPLS-TP is the same as the best current practise for MPLS. This includes the setting of the S-Bit. In each case, the S-bit is set to indicate the bottom (i.e. inner-most) label in the label stack that is contiguous between the MPLS-TP server and the client layer.~~

Comment [M13]: Editorial – same text in first paragraph of 3.4.1

Note that the label stacks shown above are divided between those inside the MPLS-TP Network and those within the client network when the client network is MPLS(-TP). They illustrate the smallest number of labels possible. These label stacks could also include more labels.

3.4.2. Pseudowire Adaptation

The architecture for an MPLS-TP network that provides PW emulated services is based on the MPLS [RFC3031] and pseudowire [RFC3985] architectures. Multi-segment pseudowires may optionally be used to provide a packet transport service, and their use is consistent with
~~~~~~~~~~~

the MPLS-TP architecture. The use of MS-PWs may be motivated by, for example, the requirements specified in [RFC5254]. If MS-PWs are used, then the MS-PW architecture [RFC5659] also applies.

Figure 6 shows the architecture for an MPLS-TP network using single-segment PWs.

```
         |<--------------- Emulated Service ----------------->|
         |                                                     |
         |          |<-------- Pseudowire -------->|          |
         |          |      encapsulated, packet    |          |
         |          |      transport service       |          |
         |          |                              |          |
         |          |    |<------ LSP ------->|    |          |
         |          V    V                    V    V          |
         V    AC    +----+      +-----+       +----+     AC   V
   +-----+    |     | PE1|=======\   /========| PE2|     |    +-----+
   |     |----------|.......PW1.| \ / |...........|----------|     |
   | CE1 |    |     |    |      |  X  |       |    |     |    | CE2 |
   |     |----------|.......PW2.| / \ |...........|----------|     |
   +-----+  ^ |     |    |=======/   \========|    |     | ^  +-----+
         ^  |       +----+      +-----+       +----+       |  ^
         |  |   Provider Edge 1    ^     Provider Edge 2   |  |
         |  |                      |                       |  |
   Customer |                  P Router                    | Customer
    Edge 1  |                                              |  Edge 2
            |                                              |
            |                                              |
      Native service                                Native service
```

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

Figure 7 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.

Comment [M14]: Figure 9 labels this as a PSN tunnel: Other places in the document call it an edge to edge LSP. Also see comment on figure 7. Please select a single term

```
           |<----------- Pseudowire encapsulated ------------->|
           |             packet transport service              |
           |                                                   |
           |                                                   |
           |                                                   |
       AC  |     |<-------- LSP1 -------->|    |<--LSP2-->|    | AC
         | V     V                        V    V          V    V |
         | +-----+              +-----+    +-----+          +----+ |
   +---+ | |TPE1|===============\   /=====|SPE1|==========|TPE2| | +---+
   |   |---|......PW1-Seg1.... | \ / | ......X...PW1-Seg2......|---|   |
   |CE1| | |    |              |  X  |     |    |          |    | | |CE2|
   |   |---|......PW2-Seg1.... | / \ | ......X...PW2-Seg2......|---|   |
   +---+ | |    |===============/   \=====|    |==========|    | | +---+
       ^   +-----+     ^        +-----+    +-----+     ^    +----+   ^
       |               |           ^                   |             |
       |           TE LSP          |               TE LSP            |
       |                       P-router                              |
       |                                                             |
       |<-------------------- Emulated Service ------------------->|
```

PW1-segment1 and PW1-segment2 are segments of the same MS-PW,
while PW2-segment1 and PW2-segment2 are segments of another MS-PW

Figure 7: MPLS-TP Architecture (Multi-Segment PW)

The corresponding MPLS-TP protocol stacks including PWs are shown in Figure 8. In this figure the Transport Service Layer [RFC5654] is identified by the PW demultiplexer (Demux) label and the Transport Path Layer [RFC5654] is identified by the LSP Demux Label.

Comment [M15]: Is this a PSN tunnel or edge to edge LSP

```
 +--------------------+     /====================\   /====================\
 |  Client Layer      |     H      OAM PDU       H   H      OAM PDU       H
 /====================\     H--------------------H   H--------------------H
 H      PW Encap      H     H       GACh         H   H       GACh         H
 H--------------------H     H--------------------H   H--------------------H
 H   PW Demux (S=1)   H     H PW Demux (S=1)     H   H    GAL (S=1)       H
 H--------------------H     H--------------------H   H--------------------H
 H   edge-to edge     H     H   edge-to edge     H   H   edge-to edge     H
 H      LSP Demux(s)  H     H  LSP Demux(s)      H   H  LSP Demux(s)      H
 \====================/     \====================/   \====================/
 |    Server Layer    |     |   Server Layer     |   |   Server Layer     |
 +--------------------+     +--------------------+   +--------------------+

     User Traffic                  PW OAM                  LSP OAM
```

Note: H(ighlighted) indicates the part of the protocol stack we are considering in this document.

Figure 8: MPLS-TP ~~Layer Network~~label stack using Pseudowires

LSP or PWs and their associated labels may be configured or signaled. See Section 3.11 for additional details related to configured service types. See Section 3.9 for additional details related to signaled service types.

3.4.2.1. Pseudowire Based Services

When providing a Virtual Private Wire Service (VPWS) , Virtual Private Local Area Network Service (VPLS), Virtual Private Multicast Service (VPMS) or Internet Protocol Local Area Network Service (IPLS), pseudowires must be used to carry the client service. VPWS, VLPS, and IPLS are described in [RFC4664]. VPMS is described in [I-D.ietf-l2vpn-vpms-frmwk-requirements].

3.4.3. Network Layer Adaptation

MPLS-TP LSPs can be used to transport network layer clients. This document uses the term Network Layer in the same sense as it is used in [RFC3031] and [RFC3032]. The network layer protocols supported by [RFC3031] and [RFC3032] can be transported between service interfaces. Examples are shown in Figure 5 above. Support for network layer clients follows the MPLS architecture for support of network layer protocols as specified in [RFC3031] and [RFC3032].

With network layer adaptation, the MPLS-TP domain provides either a uni-directional or bidirectional point-to-point connection between two PEs in order to deliver a packet transport service to attached customer edge (CE) nodes. For example, a CE may be an IP, MPLS or

Comment [M16]: Align with figure 7

Comment [M17]: Editorial: Should this be moved to section 1.3 definitions.

ATTACHMENT
TO COM 15-LS 136

MPLS-TP node. As shown in Figure 9, there is an attachment circuit between the CE node on the left and its corresponding provider edge (PE) node which provides the service interface, a bidirectional LSP across the MPLS-TP 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.

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.

```
                |<------------- Client Network Layer ------------->|
                |                                                  |
                |          |<---- Pkt Xport Service --->|          |
                |          |                            |          |
                |          |    |<-- PSN Tunnel -->|    |          |
                |          V    V                  V    V          |
                V     AC   +----+      +---+       +----+   AC     V
          +-----+     |    |PE1 |      |   |       |PE2 |   |      +-----+
          |     |     |LSP |    |      |   |       |    |   |      |     |
          | CE1 |----------|    |========X=========|    |----------| CE2 |
          |     |  ^  |IP  |    |  ^   |   |   ^   |    |   |  ^   |     |
          +-----+  |  |    |    |  |   |   |   |   |    |   |  |   +-----+
                ^  |       +----+  |   +---+   |   +----+      |   ^
                |  |     Provider  |     ^     |  Provider     |   |
                |  |       Edge    |     |     |   Edge        |   |
          Customer |         1     | P-router  |     2         | Customer
          Edge 1   |            TE            TE               | Edge 2
                   |            LSP           LSP              |
                   |                                           |
           Native service                             Native service
           Attachment Circuit                        Attachment Circuit
```

Figure 9: MPLS-TP Architecture for Network Layer Clients

At the ingress ~~service~~ interface on the attachment circuit the client packets are received .
The PE pushes one or more labels onto the client packets which are then label switched over the transport network. Correspondingly the egress PE pops any labels added by the MPLS-TP networks and transmits the packet for delivery to the attached CE via the egress ~~service~~ interface to the attachment circuit.

Comment [M18]: Align with terminology in figure 6 & 7

Comment [M19]: Add a second client to align with the example in figure 6

Formatted: Spanish (Spain, Traditional Sort)

Comment [M20]: Editorial – align terminology with the text above.

Comment [M21]: Editorial

Comment [M22]: Editorial

Formatted: English (United States)

Formatted: English (United States)

ATTACHMENT
TO COM 15-LS 136

```
                           /====================\
                           H      OAM PDU       H
 +--------------------+    H--------------------H   /====================\
 |  Client Layer      |    H       GACh         H   H      OAM PDU       H
 /====================\    H--------------------H   H--------------------H
 H    Encap Label     H    H       GAL (S=1)    H   H       GACh         H
 H--------------------H    H--------------------H   H--------------------H
 H   SvcLSP Demux     H    H SvcLSP Demux (S=0) H   H     GAL (S=1)      H
 H--------------------H    H--------------------H   H--------------------H
 H     edge-to edge   H    H     edge-to edge   H   H     edge-to edge   H
 H      LSP Demux(s)  H    H  LSP Demux(s)      H   H  LSP Demux(s)      H
 \====================/    \====================/   \====================/
 |   Server Layer     |    |   Server Layer     |   |   Server Layer     |
 +--------------------+    +--------------------+   +--------------------+

     User Traffic            Service LSP OAM              LSP OAM
```

Note: H(ighlighted) indicates the part of the protocol stack we are considering in this document.

Figure 10: ~~Domain of~~ MPLS-TP ~~Layer Network~~labels used for IP and LSP Clients

In this figure the Transport Service Layer [RFC5654] is identified by the Service LSP (SvcLSP) demultiplexer (Demux) label and the Transport Path Layer [RFC5654] is identified by the LSP Demux Label. ~~Note that the functions of the Encapsulation label and the Service Label shown above as SvcLSP Demux may be represented by a single label stack entry.~~ Additionally, the S-bit will always be zero when the client layer is MPLS labelled.

Within the MPLS-TP transport network, the network layer protocols are carried over the MPLS-TP network using a logically 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. Figure 10 shows how a client network protocol stack (which may be an MPLS label stack and payload) is carried over a network layer client service over an MPLS-TP transport network.

~~A label per network layer protocol payload type that is to be transported is required.~~ When multiple protocol payload types are to be carried over a single service LSP a unique label stack entry must be present for each payload type. Such labels are referred to as "Encapsulation Labels", one of which is shown in Figure 10. Encapsulation Label may be either configured or signaled. Encapsulation labels are regular labels (i.e. they are not reserved labels).

~~Both an Encapsulation Label and a Service Label should be present in~~

Comment [M23]: This is not clear, the Service Label is not identified in the figure. The description below is better, suggest that this text is deleted.

Comment [M24]: Contradicts the statement 2 paragraphs below.

Comment [M25]: Technical: Reserved labels e.g. IPV4 Explicit Null lable cannot be used as an Encap label – is this correct?

Comment [M26]: Editorial: Duplicate text

ATTACHMENT
TO COM 15-LS 136

~~the label stack when a particular packet transport service is supporting more than one network layer protocol payload type.~~ For example, if both IP and MPLS are to be carried, as shown in Figure 9, then the two Encapsulation Labels are mapped on to a common Service Label.

Note: The Encapsulation Label may be omitted when the ~~transport~~ Service LSP is supporting only one network layer protocol payload type. For example, if only MPLS labeled packets are carried over a service, then the Service Label (stack entry) provides both the payload type indication and service identification.

Service labels are typically carried over an MPLS-TP LSP edge-to-edge (or transport path layer). An MPLS-TP edge-to-edge LSP is represented as an LSP Demux label as shown in Figure 10. An edge-to-edge LSP is commonly used when more than one service exists between two PEs.

Note that the service label ~~edge-to-edge LSP~~ may be omitted when only one service exists between two PEs. For example, if only one service is carried between two PEs then a single ~~Service~~ LSP Label could be used to provide both the service indication and the MPLS-TP edge-to-edge LSP. Alternatively, if multiple services exist between a pair of PEs then a per-client Service Label would be mapped on to a common MPLS-TP edge-to-edge LSP.

Comment [M27]: The edge to edge LSP must always be present

As noted above, the layer 2 and layer 1 protocols used to carry the network layer protocol over the attachment circuits are not transported across the MPLS-TP network. This enables the use of different layer 2 and layer 1 protocols on the two attachment circuits.

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 specified 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 destination MAC address for all packets sent over the service interface.)~~

Comment [M28]: This detail should be in the data plane draft

Note that when two CEs, which peer with each other, operate over a network layer transport service and run a routing protocol such as IS-IS 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. See [RFC5309] for additional details.

~~The CE to CE service types and corresponding labels may be configured or signaled . See Section 3.11 for additional details related to configured service types. See Section 3.9 for additional details related to signaled service types.~~

Comment [M29]: 3.9 and 3.11 describe the MPLS-TP control plane and static operation. Service configuration is not described and should be out of scope.

3.5. Identifiers

Identifiers are used to uniquely distinguish entities in an MPLS-TP network. These include operators, nodes, LSPs, pseudowires, and their associated maintenance entities.
MPLS-TP defines two sets of identifiers: a set that is compatible with IP-based operations and another set that is compatible with ITU-T transport-based operations. The definition of these sets of identifiers is outside the scope of this document and it is provided by [I-D.ietf-mpls-tp-identifiers]~~ defines a set of identifiers that are compatible with existing MPLS control plane identifiers, as well as a set of identifiers that may be used when no IP control plane is available.~~

Comment [M30]: Clarify the rational for two sets of identifiers. The ITU set may be used when IP is present.

3.6. 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 MPLS-TP it is necessary to discriminate between user data payloads and other types of payload. For example, a packet may be associated with a Signaling Communication Channel (SCC), or a channel used for Automatic Protection Switching (APS) data. 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 or sections. The G-ACh is defined in [RFC5586] and is similar to the Pseudowire Associated Channel [RFC4385], which is used to carry OAM packets over pseudowires. The G-ACh is indicated by a generic associated channel header (ACH), similar to the Pseudowire VCCV control word; this header is present for all Sections, LSPs and PWs making use of FCAPS functions supported by the G-ACh.

Comment [M31]: Align with previous paragraph, also added section below.

For pseudowires, the G-ACh uses the first four bits of the pseudowire control word to provide the initial discrimination between data packets and packets belonging to the associated channel, as described in [RFC4385]. When this first nibble of a packet, immediately following the label at the bottom of stack, has a value of '1', 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 other control message is carried over ~~an~~ a section or a 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 'G-ACh Label (GAL)', and is defined in [RFC5586]. When a GAL is found, it indicates that the payload begins with an ACH. The GAL is thus a demultiplexer for G-ACh traffic on the section or 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 [M32]: This is implementation specific internal box behaviour and cannot be specified. It would be reasonable to state that inspection of the GAL after TTL expiry may be asynchronous with respect to the forwarding of other packets.

In MPLS-TP, the 'G-ACh Label (GAL)' always appears at the bottom of the label stack (i.e. its S bit is set to 1).

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 these 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.

At the server layer, bandwidth and QoS commitments apply to the gross traffic on the LSP, PW or section. Since the G-ACh traffic is indistinguishable from the user data traffic, protocols using the G-ACh must take into consideration the impact they have on the user data that they are sharing resources with. Conversely, capacity must be made available for important G-ACh uses such as protection and OAM. In addition, protocols using the G-ACh must conform to the security and congestion considerations described in [RFC5586].

Figure 11 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].

ATTACHMENT
TO COM 15-LS 136

```
         +-------------+                               +-------------+
         |  Payload    |           < FCAPS >           |  Payload    |
         +-------------+                               +-------------+
         |   Demux /   |        < ACH for PW >         |   Demux /   |
         |Discriminator|                               |Discriminator|
         +-------------+                               +-------------+
         |     PW      |            < PW >             |     PW      |
         +-------------+                               +-------------+
         |    PSN      |            < LSP >            |    PSN      |
         +-------------+                               +-------------+
         |  Physical   |                               |  Physical   |
         +-----+-------+                               +-----+-------+
               |                                             |
               |             ____     ___       ____         |
               |           _/    \___/   \    _/    \__      |
               |          /               \__/         \_    |
               |         /                               \   |
               +--------|      MPLS/MPLS-TP Network       |---+
                         \                               /
                          \   ___      ___     __      _/
                           \_/   \____/   \___/  \____/
```

Comment [M33]: This draft is describing MPLS-TP

Figure 11: PWE3 Protocol Stack Reference Model showing 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 12 shows the reference model depicting how the control channel is associated with the LSP protocol stack.

```
          +-------------+                              +-------------+
          |  Payload    |          < FCAPS >           |   Payload   |
          +-------------+                              +-------------+
          |Discriminator|        < ACH on LSP >        |Discriminator|
          +-------------+                              +-------------+
          |Demultiplexer|        < GAL on LSP >        |Demultiplexer|
          +-------------+                              +-------------+
          |    PSN      |           < LSP >            |    PSN      |
          +-------------+                              +-------------+
          |  Physical   |                              |  Physical   |
          +-----+-------+                              +-----+-------+
                |                                            |
                |              ____     ___       ____       |
                |            _/    \___/   \    _/    \__    |
                |           /               \__/         \_  |
                |          /                               \ |
                +--------|      ~~MPLS/~~MPLS-TP Network       |---+
                          \                               /
                           \   ___      ___     __      _/
                            \_/   \____/   \___/  \____/
```

Figure 12: MPLS Protocol Stack Reference Model showing the LSP Associated Control Channel

3.7. Operations, Administration and Maintenance (OAM)

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 LSPs and PWs is the Generic Associated Channel (Section 3.6). 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 for IPv4 and that same range embedded as IPv4 mapped IPv6 addresses for IPv6 [RFC4379]. When the OAM packets are encapsulated in an IP header, these mechanisms are the default mechanisms for MPLS networks in general for identifying MPLS OAM packets. MPLS-TP must be able to operate in an environments where IP forwarding is not supported, and thus the G-ACh/GAL is the default mechanism to demultiplex OAM packets in MPLS-TP.

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 transport path (i.e. section, LSP or PW). These mechanisms are described in [RFC5586].~~

Comment [M34]: Redundant, already described in 3.6

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 localisation) 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 G-ACh Label (GAL) to create a control channel associated to an LSP, Section or PW.

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 Maintenance End Points (MEPs). A Maintenance Entity Group (MEG) is a collection of one or more MEs that belongs to the same transport path and that are maintained and monitored as a group. The MEPs that form an ME limit the OAM responsibilities of an OAM flow to within the domain of a transport path or segment, in the specific layer network that is being monitored and managed.

An MEG may also include a set of Maintenance Intermediate Points (MIPs). Maintenance End Points (MEPs) are capable of sourcing and sinking OAM flows, while Maintenance Intermediate Points (MIPs) can only ~~sink or respond~~react to OAM flows received from within a MEG~~,~~. ~~or~~ Intermediate nodes can originate notifications to the MEPs as a result of specific network conditions.

Comment [M35]: Text aligned with agreed changes that are being included in the MPLS-TP OAM framework draft.

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

~~o A Section Maintenance Entity (SME), allowing monitoring and management of MPLS-TP Sections (between MPLS LSRs).~~

~~o A LSP Maintenance Entity (LME), allowing monitoring and management of an edge-to-edge LSP (between LERs).~~

~~o A PW Maintenance Entity (PME), allowing monitoring and management of an edge-to-edge SS/MS-PWs (between T-PEs).~~

~~o An LSP Tandem Connection Maintenance Entity (LTCME).~~

~~A G-ACh packet may be directed to an individual MIP along the path of an LSP or MS-PW by setting the appropriate TTL in the label for the G-ACh packet, as per the traceroute mode of LSP Ping [RFC4379] and the vccv-trace mode of [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 circumstances where this is not the case, 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.~~

~~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 wherever a label is pushed or swapped. For example, on an 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.~~

Comment [M36]: This is not fully aligned with the ITU architecture. However, this level of detail should only be included in the MPLS-TP OAM framework. So the concern can be addressed by deleting the text

~~The MPLS-TP OAM architecture supports a wide range of OAM functions to check continuity, to verify connectivity and to monitor the preformance of the path, to generate, filter and manage local and remote defect alarms. These functions are applicable to any layer defined within MPLS-TP, i.e. to MPLS-TP Sections, LSPs and PWs.~~

Comment [M37]: Redundant text

The MPLS-TP OAM tool-set must be able to operate without relying on a dynamic control plane or IP functionality in the datapath. In the case of an MPLS-TP deployment in a network in which IP functionality is available, all existing IP/MPLS OAM functions, e.g. LSP-Ping, BFD and VCCV, may be used.

3.8. ~~LSP~~ Return Path

Comment [M38]: PWs and out of band are also described. The text in this section should be generalized to include PWs

Management, control and OAM protocol functions may require response packets to be delivered from the receiver back to the originator of a message exchange. This section provides a summary of the return path options in MPLS-TP networks. In this section the case of a MPLS-TP LSP is described, however this is also applicable to a PW.

In this discussion we assume that A and B are terminal LSRs (i.e. LERs) for an MPLS-TP LSP and that Y is an intermediate LSR along the LSP. In the unidirectional case, A is taken to be the upstream and B the downstream LSR with respect to the LSP. We consider the following cases for the various types of LSPs:

Case 1. Packet transmission from B to A

Comment [M39]: To link to the text below

Case 2. Packet transmission from Y to A

Case 3. Packet transmission from B to Y

Note that a return path may not always exist, and that packet transmission in one or more of the above cases may not be possible. In general the existence and nature of return paths for MPLS-TP LSPs is determined by operational provisioning.

3.8.1. Return Path Types

There are two types of return path that may be used for the delivery of traffic from a downstream node D to an upstream node U either:

a. The LSP between U and D is bidirectional therefore D ~~maintains~~ has an MPLS-TP LSP back to U which ~~is specifically~~can be used ~~designated~~ to carry return traffic for the original LSP, or

b. D has some other unspecified means of directing traffic back to U.

Comment [M40]: Can this exist if the LSP is bidirectional?

The first option is referred to as an "in-band" return path, the second as an "out-of-band" return path.

There are various possibilities for "out-of-band" return paths. Such a path may, for example, be based on ordinary IP routing. In this case packets would be forwarded as usual to a destination IP address associated with U. In an MPLS-TP network that is also an IP/MPLS network, such a forwarding path may traverse the same physical links or logical transport paths used by MPLS-TP. An out-of-band return path may also be indirect, via a distinct Data Communication Network (DCN) (provided, for example, by the method specified in [RFC5718]); or it may be via one or more other MPLS-TP LSPs.
It is also possible that no “out-of-band” return path exists or that an operator disables, by policing decision, the usage of an "out-of-band" return path.

3.8.2. Point-to-Point Unidirectional LSPs

Case 1 In this situation, either an in-band or out-of-band return path may be used to deliver traffic from B back to A.

It is ~~therefore~~ recommended for reasons of operational simplicity that point-to-point unidirectional LSPs be provisioned as associated or co-routed bidirectional LSPs~~—~~ whenever return traffic from B to A is required. Note that the two directions of such an LSP may have differing bandwidth
In ~~the in-band~~this case there is in essence an associated or co-routed bidirectional LSP between A and B, and the discussion for

such LSPs below applies. ~~It is therefore recommended for reasons of operational simplicity that point-to-point unidirectional LSPs be provisioned as associated bidirectional LSPs (which may also be co-routed) whenever return traffic from B to A is required. Note that the two directions of such an LSP may have differing bandwidth~~

Comment [M41]: Moved text to improve flow allocations and QoS characteristics.

Case 2 In this case only the out-of-band return path option is available. However, an additional out-of-band possibility is worthy of note here: if B is known to have a return path to A, then Y can arrange to deliver return traffic to A by first sending it to B along the original LSP. The mechanism by which B recognises the need for and performs this forwarding operation is protocol-specific.

Case 3 In this case only the out-of-band return path option is available. However, if B has a return path to A, then in a manner analogous to the previous case B can arrange to deliver return traffic to Y by first sending it to A along that return path. The mechanism by which A recognises the need for and performs this forwarding operation is protocol-specific.

3.8.3. Point-to-Point Associated Bidirectional LSPs

For Case 1, B has a natural in-band return path to A, the use of which is typically preferred for return traffic, although out-of-band return paths are also applicable.

For Cases 2 and 3, the considerations are the same as those for point-to-point unidirectional LSPs.

3.8.4. Point-to-Point Co-Routed Bidirectional LSPs

For all of Cases 1, 2, and 3, a natural in-band return path exists in the form of the LSP itself, and its use is typically preferred for return traffic. Out-of-band return paths, however, are also applicable, primarily as an alternative means of delivery in case the in-band return path has failed.

3.9. Control Plane

A distributed dynamic control plane may be used to enable dynamic service provisioning in an MPLS-TP network. Where the requirements specified in [RFC5654] can be met, the MPLS Transport Profile uses existing standard control plane protocols for LSPs and PWs.

Note that a dynamic control plane is not required in an MPLS-TP network. See Section 3.11 for further details on statically configured and provisioned MPLS-TP services.

Figure 13 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.

```
 +-------------------------------------------------------------------+
 |                                                                   |
 |                Network Management System and/or                   |
 |                                                                   |
 |           Control Plane for Point to Point Connections            |
 |                                                                   |
 +-------------------------------------------------------------------+
               |     |         |     |          |     |
  .............|.....|...  ....|.....|....  ....|.....|...........
  :          +---+   |  :  : +---+   |   :  : +---+   |          :
  :          |OAM|   |  :  : |OAM|   |   :  : |OAM|   |          :
  :          +---+   |  :  : +---+   |   :  : +---+   |          :
  :            |     |  :  :   |     |   :  :   |     |          :
 \: +----+   +--------+ :  : +--------+  :  : +--------+   +----+ :/
--+-|Edge|<->|Forward-|<---->|Forward-|<----->|Forward-|<->|Edge|-+--
 /: +----+   |ing     | :  : |ing     |  :  : |ing     |   +----+ :\
  :          +--------+ :  : +--------+  :  : +--------+          :
  ''''''''''''''''''''''  ''''''''''''''  ''''''''''''''''''''''
```

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, an LSP or a G-ACh.

Figure 13: MPLS-TP Control Plane Architecture Context

The MPLS-TP control plane is based on existing MPLS and PW control plane protocols and fits within the ASON architecture. MPLS-TP uses Generalized MPLS (GMPLS) signaling ([RFC3945], [RFC3471], [RFC3473]) for LSPs and Targeted LDP (T-LDP) [RFC4447] [I-D.ietf-pwe3-segmented-pw][I-D.ietf-pwe3-dynamic-ms-pw] for pseudowires.

MPLS-TP requires that any ~~signaling~~ control plane traffic be capable of being carried over an out-of-band signaling network or a signaling control channel such as the one described in [RFC5718]. Note that while T-LDP signaling is traditionally carried in-band in IP/MPLS networks, this does not preclude its operation over out-of-band channels. References to T-LDP in this document do not preclude the definition of alternative PW control protocols for use in MPLS-TP.

Comment [M42]: This also applies to other control plane traffic e.g. routing.

PW control (and maintenance) takes place separately from LSP tunnel signaling. The main coordination between LSP and PW control will

occur within the nodes that terminate PWs. The control planes for PWs and LSPs may be used independently, and one may be employed without the other. This translates into the four possible scenarios: (1) no control plane is employed; (2) a control plane is used for both LSPs and PWs; (3) a control plane is used for LSPs, but not PWs; (4) a control plane is used for PWs, but not LSPs. The PW and LSP control planes, collectively, must satisfy the MPLS-TP control plane requirements reviewed in the MPLS-TP Control Plane Framework [I-D.abfb-mpls-tp-control-plane-framework]. When client services are provided directly via LSPs, all requirements must be satisfied by the LSP control plane. When client services are provided via PWs, the PW and LSP control planes operate in combination and some functions may be satisfied via the PW control plane while others are provided to PWs by the LSP control plane.

Note that if MPLS-TP is being used in a multi-layer network, a number of control protocol types and instances may be used. This is consistent with the MPLS architecture which permits each label in the label stack to be allocated and signaled by its own control protocol.

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

- Signaling

- Routing

- 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 3.7, e.g. for fault detection and localisation 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 Section 3.12. Examples of the MPLS-TP data plane connectivity patterns are LSPs utilising 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. In all cases, however, the control plane is logically decoupled from the data plane such that a control plane failure will not cause any existing transport paths to be impacted.

3.10. Inter-domain Connectivity

A number of methods exist to support inter-domain operation of MPLS-TP including the data plane, OAM and configuration aspects, for example:

- o Inter-domain TE LSPs [RFC4216]
- o Multi-segment Pseudowires [RFC5659]
- o LSP stitching [RFC5150]
- o back-to-back attachment circuits [RFC5659]

An important consideration in selecting an inter-domain connectivity mechanism is the degree of layer network isolation and types of OAM required by the operator. The selection of which technique to use in a particular deployment scenario is outside the scope of this document.

3.11. 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. Thus it should be possible for a PW to be statically configured, while the LSP supporting it is set up by a dynamic control plane. When static configuration mechanisms are used, care must be taken to ensure that loops are not created.

3.12. 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 cannot be fully provided by the underlying LSP

(i.e. where the backup PW terminates on a different target PE node than the working PW in dual homing scenarios, or where protection of the S-PE is required). 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 can 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:

- o Two concurrent traffic paths (1+1).
- o one active and one standby path with guaranteed bandwidth on both paths (1:1).
- o one active path and a standby path the resources or which are shared by one or more other active paths (shared protection).

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 as follows:

- o Optimised for linear, ring or meshed topologies.
- o Use OAM mechanisms to detect and localise network faults or service degenerations.
- o 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.
- o 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.
- o 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.
- o MPLS-TP recovery mechanisms can be data plane, control plane or management plane based.
- o MPLS-TP supports revertive and non-revertive behaviour.

3.13. Path Segment Tunnels

Comment [M43]: Technical issue: We have not discussed the QoS implications of the use of the PST to support the TCM function. This draft must be updated to reflect the agreements on this issue. See email from Italo Busi "PST QoS model in draft-ietf-mpls-tp-framework-10"

In order to monitor, protect and manage a portion of an LSP, a new architectural element is defined called the Path Segment Tunnel (PST). A PST is a hierarchical LSP [RFC3031] which is defined and used for the purposes of OAM monitoring, protection or management of LSP segments or concatenated LSP segments.

A PST is defined between the edges of the portion of the LSP that needs to be monitored, protected or managed. ~~Maintenance message~~OAM messages can be initiated at the edge of the PST and sent to the peer edge of the PST or to ~~an intermediate point~~ MIP along the PST by setting the TTL value at the PST level accordingly.

Comment [M44]: Section 3.7 uses the term OAM messages

Comment [M45]: Section 3.7 uses the term MIP

For example in Figure 14, three PSTs are configured to allow monitoring, protection and management of the LSP concatenated segments. One PST is defined between PE1 and PE2, the second between PE2 and PE3 and a third PST is set up between PE3 and PE4. Each of these three PSTs may be monitored, protected, or managed independently.

```
 ========================== End to End LSP =============================

    |<--------- Carrier 1 --------->|       |<----- Carrier 2 ----->|

 ---| PE1 |---| P |---| P |---| PE2 |-------| PE3 |---| P |---| PE4 |---

    |============= PST =============|==PST==|========= PST =========|
               (Carrier 1)                          (Carrier 2)
```

Comment [M46]: Edge to Edge? Where are the end points? In the CE?

Comment [M47]: Not consistent with the definition of PE in 1.3.5.

Comment [M48]: Is a new label pushed for this PST

Comment [M49]: Is this one PST or three PSTs

Figure 14: PSTs in inter-carrier network

The end-to-end traffic of the LSP, including data traffic and control traffic (OAM, Protection Switching Control, management and signaling messages) is tunneled within the PST by means of label stacking as defined in [RFC3031].

Comment [M50]: Is the PST edgae to edge between PE1 and PE4

The mapping between an LSP and a PST can be 1:1, in which case it is similar to the ITU-T Tandem Connection element [G.805]. The mapping can also be 1:N to allow aggregated monitoring, protection and management of a set of LSP segments or concatenated LSP segments. Figure 15 shows a PST which is used to aggregate a set of concatenated LSP segments for the LSP from PEx to PEt and the LSP from PEa to PEd. Note that such a construct is useful, for example, when the LSPs traverse a common portion of the network and they have the same Traffic Class.

```
   |PEx|--|PEy|-+                                     +-|PEz|--|PEt|
                |                                     |
                |  |<---------- Carrier 1 --------->|  |
                |  +-----+   +---+   +---+    +-----+  |
                +--|     |---|   |---|   |----|     |--+
                   | PE1 |   | P |   | P |    | PE2 |
                +--|     |---|   |---|   |----|     |--+
                |  +-----+   +---+   + P +    +-----+  |
                |  |============= PST ==============|  |
   |PEa|--|PEb|-+            (Carrier 1)              +-|PEc|--|PEd|
```

Figure 15: PST for a Set of Concatenated LSP Segments

3.13.1. Provisioning of PST

PSTs can be provisioned either statically or using control plane signaling procedures. The make-before-break procedures which are supported by MPLS allow the creation of a PST on existing LSPs in-service without traffic disruption. A PST can be defined corresponding to one or more end-to-end tunneled LSPs. New end-to-end LSPs which are tunneled within the PST can be set up. Traffic of the existing LSPs is switched over to the new end-to-end tunneled LSPs. The old end-to-end LSPs can then be torn down.

3.14. Pseudowire Segment Tunnels

Pseudowire segment tunnels are for further study.

Comment [M51]: Experience with other technologies e.g. SDH has shown that adding TCM at a later stage in the definition of a technology causes the design to be inefficient.
At a minimum a high level outline for PW TCM should be provided.

3.15. Network Management

The network management architecture and requirements for MPLS-TP are specified in [I-D.ietf-mpls-tp-nm-framework] and [I-D.ietf-mpls-tp-nm-req]. These derive 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 an 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), realised by the G-ACh, provides a logical operations channel between NEs for transferring Management information. For the management interface from a management system to an MPLS-TP NE, there is no restriction on which management protocol is used. The ~~MCC~~ NMS is used to provision and manage an end-to-end connection across a network where some segments are created/managed by, for example, Netconf [RFC4741] or SNMP [RFC3411] 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 well as any associated MEPs and MIPs, as per Section 3.11.

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 capable of operating on-demand or pro-actively.

4. Security Considerations

Comment [M52]: Liaison from IETF suggested that G.8110.1 should reference draft-ietf-mpls-mpls-and-gmpls-security-framework.

The introduction of MPLS-TP into transport networks means that the security considerations applicable to both MPLS and PWE3 apply to

ATTACHMENT
TO COM 15-LS 136

those transport networks. Furthermore, when general MPLS networks that utilise functionality outside of the strict MPLS Transport 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 [RFC5659] apply.

Packets that arrive on an interface with a given label value should not be forwarded unless that label value is assigned to an LSP or PW to a peer LSR or PE that is reachable via that interface.

Comment [M53]: In the past there was some discussion and early review comments regarding the need to check that the label is received from the interface/ (lower level) LSP it is expected from.. This text does not appear to cover this issue.

Comment [M54]: This text is not clear. If the label value is received how can it be assigned to a LSP that is going to a peer LSR or PE?

Each MPLS-TP solution must specify the additional security considerations that apply. This is discussed further in [I-D.fang-mpls-tp-security-framework].

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:

Formatted: Spanish (Spain, Traditional Sort)

- Rahul Aggarwal
- Dieter Beller
- Malcolm Betts
- Italo Busi
- John E Drake
- Hing-Kam Lam
- Marc Lasserre
- Vincenzo Sestito
- Nurit Sprecher

Formatted: French (Switzerland)

Formatted: French (France)

o Martin Vigoureux

o Yaacov Weingarten

o The participants of ITU-T SG15

Formatted: French (France)

~~7. Open Issues~~

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

~~o~~

8. References

8.1. Normative References

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

Formatted: French (France)

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

Formatted: French (France)

[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.

Formatted: French (France)

[RFC3270] Le Faucheur, F., Wu, L., Davie, B., Davari, S., Vaananen, P., Krishnan, R., Cheval, P., and J. Heinanen, "Multi-Protocol Label Switching (MPLS)

Formatted: French (Switzerland)

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.

[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.

Formatted: English (Canada)

Formatted: English (United States)

Formatted: French (France)

Formatted: French (France)

[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.

[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.abfb-mpls-tp-control-plane-framework] Andersson, L., Berger, L., Fang, L., Bitar, N., Takacs, A., and M. Vigoureux, "MPLS-TP Control Plane Framework", draft-abfb-mpls-tp-control-plane-framework-01 (work in progress), July 2009.

[I-D.fang-mpls-tp-security-framework] Fang, L. and B. Niven-Jenkins, "Security Framework for MPLS-TP", d raft-fang-mpls-tp-security-framework-00 (work in progress), July 2009.

[I-D.fbb-mpls-tp-data-plane] Frost, D., Bryant, S., and M. Bocci, "MPLS Transport Profile Data Plane Architecture", draft-fbb-mpls-tp-data-plane-00 (work in progress), February 2010.

[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-vpms-frmwk-requirements] Kamite, Y., JOUNAY, F., Niven-Jenkins, B., Brungard, D., and L. Jin, "Framework and Requirements for Virtual Private Multicast Service (VPMS)", draft-ietf-l2vpn-vpms-frmwk-requirements-02 (work in progress), October 2009.

[I-D.ietf-mpls-tp-identifiers] Bocci, M. and G. Swallow, "MPLS-TP Identifiers", draft-ietf-mpls-tp-identifiers-00 (work in progress), November 2009.

[I-D.ietf-mpls-tp-nm-framework] Mansfield, S., Gray, E., and H. Lam, "MPLS-TP Network Management Framework", draft-ietf-mpls-tp-nm-framework-04 (work in progress), January 2010.

[I-D.ietf-mpls-tp-nm-req] Mansfield, S. and K. Lam, "MPLS TP Network Management Requirements", draft-ietf-mpls-tp-nm-req-06 (work in progress), October 2009.

[I-D.ietf-mpls-tp-oam-framework] Allan, D., Busi, I., and B. Niven-Jenkins, "MPLS-TP OAM Framework", draft-ietf-mpls-tp-oam-framework-04 (work in progress), December 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-04 (work in progress), December 2009.

[I-D.ietf-mpls-tp-survive-fwk] Sprecher, N. and A. Farrel, "Multiprotocol Label Switching Transport Profile Survivability Framework", draft-ietf-mpls-tp-survive-fwk-03 (work in progress), November 2009.

[I-D.ietf-pwe3-dynamic-ms-pw] Martini, L., Bocci, M., Balus, F., Bitar, N., Shah, H., Aissaoui, M., Rusmisel, J., Serbest, Y., Malis, A., Metz, C., McDysan, D., Sugimoto, J., Duckett, M., Loomis, M., Doolan, P., Pan, P., Pate, P., Radoaca, V., Wada, Y., and Y. Seo, "Dynamic Placement of Multi Segment Pseudo Wires", draft-ietf-pwe3-dynamic-ms-pw-10 (work in progress), October 2009.

[I-D.ietf-pwe3-redundancy] Muley, P. and V. Place, "Pseudowire (PW) Redundancy", draft-ietf-pwe3-redundancy-02 (work in progress),

Formatted: French (France)

October 2009.

[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.

[RFC3209] Awduche, D., Berger, L., Gan, D., Li, T., Srinivasan, V., and G. Swallow, "RSVP-TE: Extensions to RSVP for LSP Tunnels", RFC 3209, December 2001.

[RFC3411] Harrington, D., Presuhn, R., and B. Wijnen, "An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks", STD 62, RFC 3411, December 2002.

[RFC3443] Agarwal, P. and B. Akyol, "Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks", RFC 3443, January 2003.

[RFC3945] Mannie, E., "Generalized Multi-Protocol Label Switching (GMPLS) Architecture", RFC 3945, October 2004.

[RFC4216] Zhang, R. and J. Vasseur, "MPLS Inter-Autonomous System (AS) Traffic Engineering (TE) Requirements", RFC 4216, November 2005.

[RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, February 2006.

[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.

[RFC4664] Andersson, L. and E. Rosen, "Framework for Layer 2 Virtual Private Networks (L2VPNs)", RFC 4664, September 2006.

[RFC4741] Enns, R., "NETCONF Configuration Protocol", RFC 4741, December 2006.

[RFC5150] Ayyangar, A., Kompella, K., Vasseur, JP., and A. Farrel, "Label Switched Path Stitching with Generalized Multiprotocol Label Switching Traffic Engineering (GMPLS TE)", RFC 5150, February 2008.

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

[RFC5309] Shen, N. and A. Zinin, "Point-to-Point Operation over LAN in Link State Routing Protocols", RFC 5309, October 2008.

[RFC5331] Aggarwal, R., Rekhter, Y., and E. Rosen, "MPLS Upstream Label Assignment and Context-Specific Label Space", RFC 5331, August 2008.

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

[RFC5659] Bocci, M. and S. Bryant, "An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge", RFC 5659, October 2009.

[RFC5718] Beller, D. and A. Farrel, "An In-Band Data Communication Network For the MPLS Transport Profile", RFC 5718, January 2010.

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 (editor)
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

Lou Berger
LabN

Phone: +1-301-468-9228
Fax:
EMail: lberger@labn.net
URI:

Formatted: English (Canada)

ATTACHMENT
TO COM 15-LS 136