MPLS Working Group
Internet-Draft
Intended status: Informational
Expires: May 31, 2009

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

November 27, 2008

A Framework for MPLS in Transport Networks
draft-ietf-mpls-tp-framework-00

Status of This Memo

Abstract

This document specifies an archiectectural framework for the application of MPLS in transport networks. It describes a profile of MPLS that enables operational models typical in transport networks networks, while providing additional OAM, survivability and other maintenance functions not currently supported by MPLS.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT",

"SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC2119 [1].

Table of Contents

1. Introduction

1.1. Motivation and Background

Existing transport technologies (e.g. SDH, ATM, OTN) have been designed with specific characteristics:

- Strictly connection oriented
  - Long-lived connections
  - Manually provisioned connections
- High level of protection and availability
- Quality of service
- Extended OAM capabilities

The development of MPLS-TP has been driven by the carriers needing to evolve SONET/SDH networks to support packet based services and networks, and the desire to take advantage of the flexibility and cost benefits of packet switching technology.

There are three objectives:

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.
3. To create a common set of new functions that are applicable to both MPLS networks in general, and those blonging to the MPLS-TP profile.

MPLS-TP defines a profile of MPLS targeted at transport applications. This profile specifies the specific MPLS characteristics and extensions required to meet transport requirements. An equipment conforming to MPLS-TP must support this profile. An MPLS-TP conformant equipment MAY support additional MPLS features. A carrier may deploy some of those additional features in the transport layer of their network if they find them to be beneficial.

Figure 1 illustrates the range of services that MPLS-TP is intended to address. Networks supporting MPLS-TP are intended to support a range of layer 1,layer 2 and layer 3 services, and are not limited to

layer 3 services only.

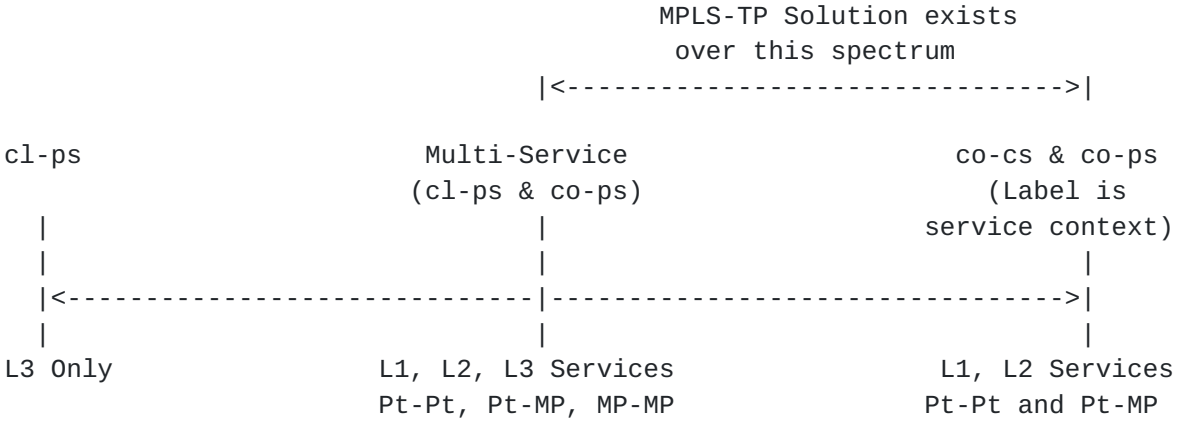


Figure 1: MPLS-TP Service Spectrum

1.2. Scope

This document specifies the high-level functionality of MPLS-TP required for adding transport-oriented capabilities to MPLS

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, Adminitration and Maintenance
G-ACH	Generic Associated Channel Header
GAL	Generic Alert Label
MEP	Maintenance End Point
MIP	Maintenance Intermediate Point
APS	Automatic Protection Switching
SCC	Signaling Communication Channel
MCC	Management Communication Channel
EMF	Equipment Management Function
FM	Fault Management
CM	Configuration Management
PM	Performance Management

2. Summary of Requirements

This section summarizes the requirements for the MPLS transport profile. Such requirements are specified in more detail in [20], [21], and [22].

Solutions MUST NOT modify the MPLS forwarding architecture.

Solutions MUST be based on existing pseudowire and LSP constructs.

New mechanisms and capabilities added to support transport networks must be able to interoperate or interwork with existing MPLS and pseudowire control and forwarding planes.

Point to point LSPs MAY be unidirectional or bi-directional. It MUST be possible to construct congruent Bi-directional LSPs. Point to multipoint LSPs are unidirectional.

MPLS-TP LSPs do not merge with other LSPs at an MPLS-TP LSR. It is possible to detect that 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. Transport Profile Overview

3.1. Architecture

The architecture for a transport profile of MPLS (MPLS-TP) is based on the MPLS-TE [2], pseudowire [3], and multi-segment pseudowire [4] architectures, as illustrated in Figure 2. The primary constructs of the transport profie for MPLS are LSPs, while PWs are the primary client layer.

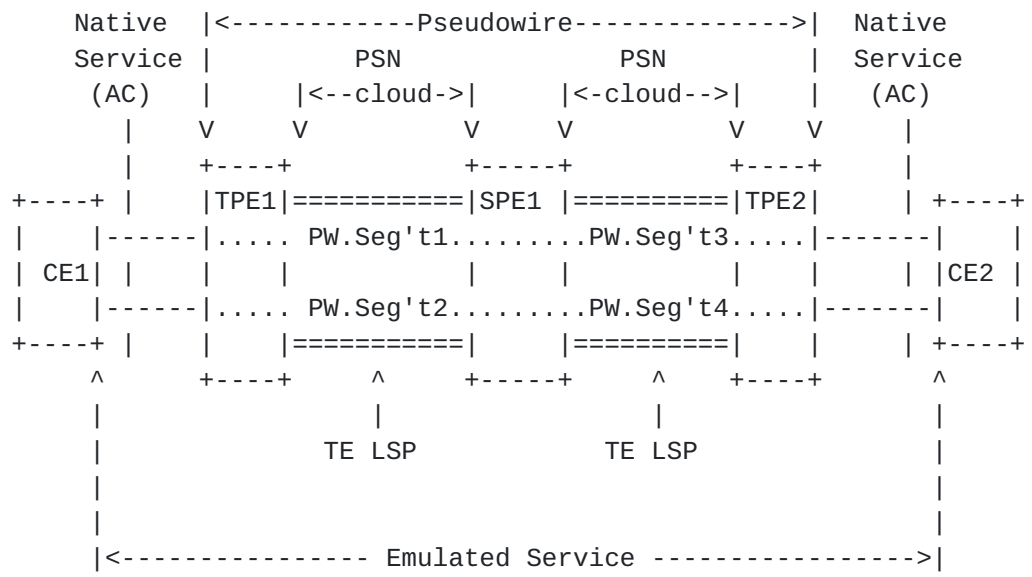


Figure 2: MPLS-TP Architecture

The MPLS-TP forwarding plane is a profile of the MPLS LSP PW, and MS-PW forwarding architecture as detailed in section Section 3.3.

MPLS-TP supports a comprehensive set of OAM and protection-switching capabilities for packet transport applications, with equivalent capabilities to existing SONET/SDH OAM and protection, as described in sections Section 3.4 and Section 3.7. MPLS-TP may be operated with centralized Network Management Systems with or without the support of a distributed control plane as described in sections Section 3.5 and Section 3.8.

MPLS-TP defines mechanisms to differentiate specific packets (e.g. OAM, APS, MCC or SCC) from those carrying user data packets on the same LSP. These mechanisms are described in sections Section 3.4.2and Section 3.4.1.

3.2. Addressing

MPLS-TP distinguishes between adressing used to identify nodes in the network, and identifiers used for demultiplexing and forwarding. This distinction is illustrated in Figure 3.

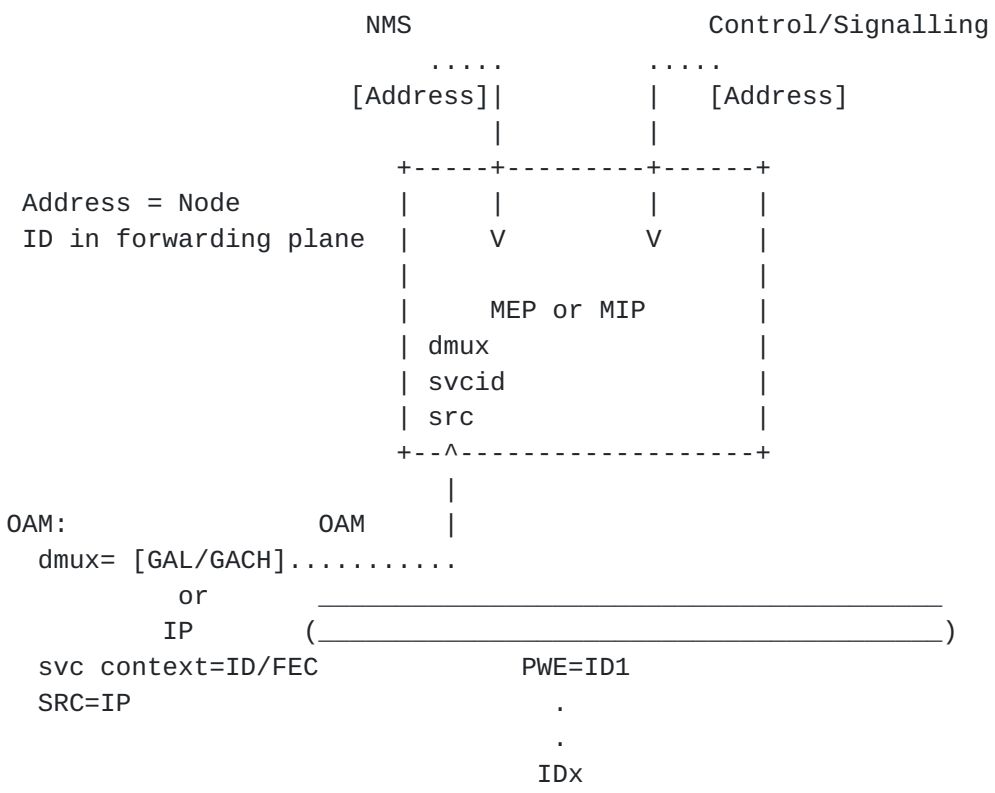


Figure 3: Addressing in MPLS-TP

Ediror's note: The figure above arose from discussions in the MPLS-TP design team. It will be clarified in a future verson of this draft.

IPv4 or IPv6 addresses are used to identify MPLS-TP nodes by default for network management and signaling purposes.

In the forwarding plane, identfiers are required for the service context (provided by the FEC), and for OAM. OAM requires both a demultiplexer and an address for the source of the OAM packet.

For MPLS in general where IP addressing is used, IPv4 or IPv6 is used by default. However, 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. Forwarding based on IP addresses for user or OAM packets is NOT REQUIRED for MPLS-TP.

RFC 4379 [23]and BFD for MPLS LSPs [24] have defined alert mechanisms that enable a MPLS LSR to identify and process MPLS OAM packets when the OAM packets are encapsulated in an IP header. These alert mechanisms are based on TTL expiration and/or use an IP destination address in the range 127/8. These mechanisms are the default mechanisms for MPLS networks in general for identifying MPLS OAM

packets when the OAM packets are encapsulated in an IP header. MPLS-TP must not rely on these mechanisms, and thus relies on the GACH/GAL to demultiplex OAM packets.

3.3. Forwarding

MPLS-TP LSPs use the MPLS label switching operations defined in [2]. These operations are highly optimized for performance and are not modified by the MPLS-TP profile.

During forwarding a label is pushed to describe the processing operaton to be performed at 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 circumstance that disrupts a swap operation is TTL expiry, in which case the packet may be discarded or subjected to further scrutinity within the LSR. Operations on a packet with an expired TTL are asynchronous to the other packets in the LSP. Thus the only way to cause a P (intermediate) LSR to inspect a packet (for example for OAM purposes) is to set the TTL to expiry at that LSR.

MPLS-TP PWs support the PW and MS-PW forwarding operations defined in[3] and [4].

The Traffic Class field (former MPLS EXP field) follows the definition and processing rules of [5] and [6]. Only the pipe and short-pipe models are supported in MPLS-TP.

The MPLS encapsulation format is as defined in RFC 3032[7]. Per-platform or the per-interface label space can be selected. Standard PW encapsulation mechanisms are applicable to the different client layers as defined by the IETF PWE3 WG.

MPLS-TP LSPs can be unidirectional or bidirectional point-to-point. As for MPLS, point-to-multipoint MPLS-TP LSPs are unidirectional.

Point-to-multipont PWs are currently in definition in the IETF and may be incorporated in MPLS-TP if required.

It MUST be possible to configure an MPLS-TP LSP such that the forward and backward directions of bidirectional MPLS-TP LSPs congruent: i.e. they follow the same path. The pairing relationship between the forward and the backward directions must be known at each MEP, MIP or segment protection endpoint on a bidirectional LSP.

Per-packet equal cost multi-path (ECMP) load balancing is not applicable to MPLS-TP LSPs, however PWs or LSPs that emulate link bundles may be employed, for example [25]

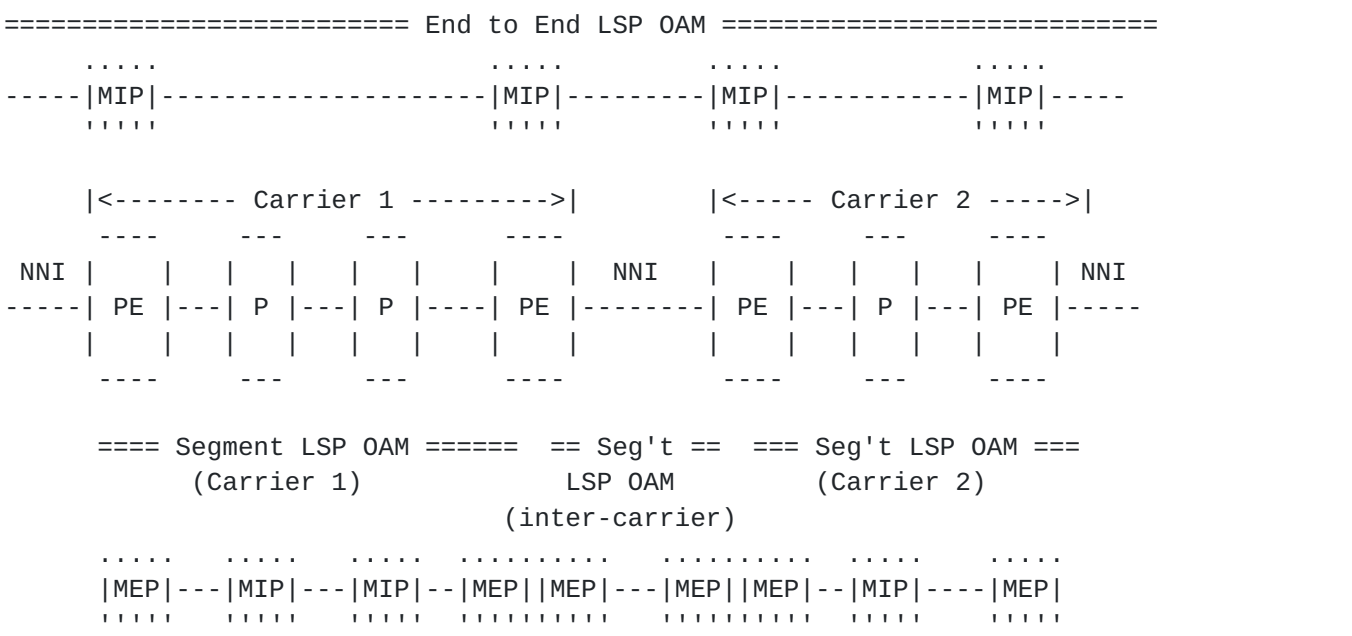
Penultimate hop popping (PHP) is disabled on MPLS-TP LSPs by default. The applicability of PHP to both MPLS-TP LSPs and MPLS networks in general providing paket transport services will be clarified in a future version of this draft.

Both E-LSP and L-LSP are supported in MPLS-TP, as defined in RFC 3270 [6].

3.4. Operations, Administration and Maintenance (OAM)

MPLS-TP requires [21] that a set of OAM capabilities is available to perform fault management (e.g. fault detection and localization) and performance monitoring (e.g. signal quality measurement) of the MPLS-TP network and the services. These capabilities are applicable at the section, LSP and PW layer. The framework for OAM in MPLS-TP is specified in [26].

OAM and monitoring in MPLS-TP is based on the concept of maintenance entities, as described in [26]. A Maintenance Entity can be viewed as the association of two (or more) Maintenance End Points (MEPs) (see example in Figure 4). The MEPS that form an ME should be configured and managed to limit the OAM responsibilities of an OAM flow within a network or sub-network in the specific layer network that is being monitored and managed. Each OAM flow is associated to a unique ME. Each MEP within an ME resides at the boundaries of that ME. An ME may also include a set of zero or more Maintenance Intermediate Points (MIPs), which reside within the Maintenance Entity. Maintenance end points (MEPs) are capable of sourcing and sinking OAM flows, while maintenance intermediate points (MIPs) can only sink or respond to OAM flows.

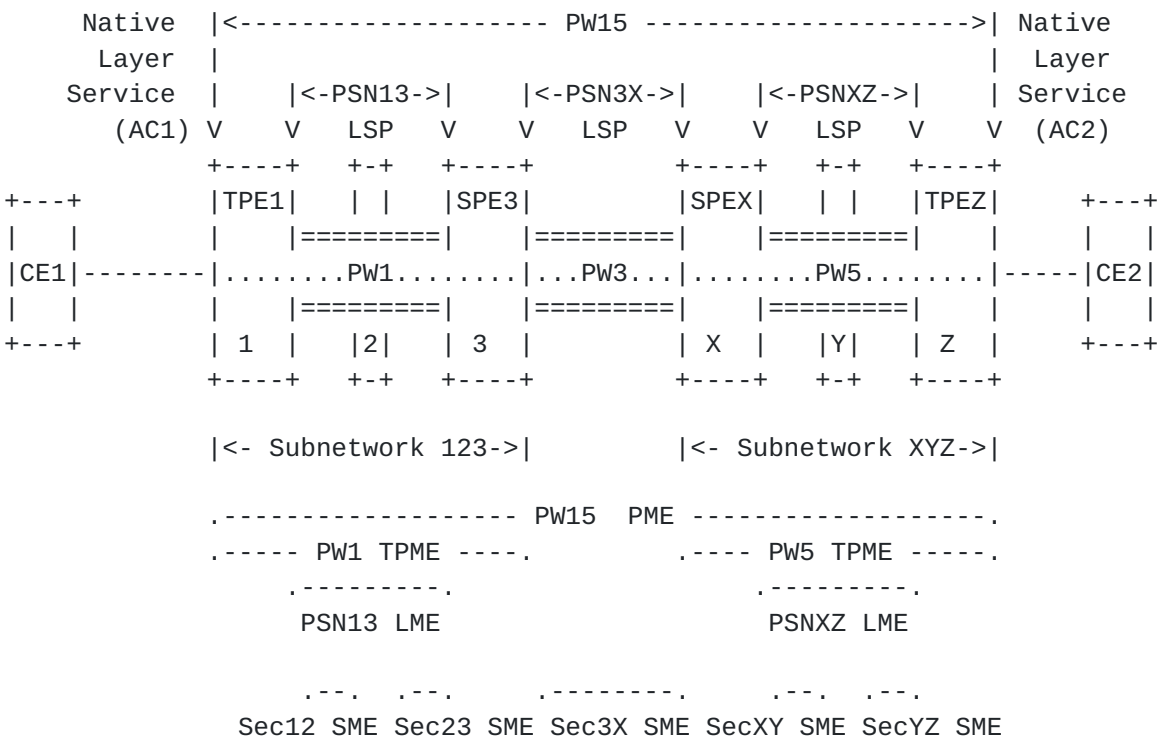


Note: MEPs for End-to-end LSP OAM exist outside of the scope of this figure.

Figure 4: Example of MPLS-TP OAM

Editor's note: The above diagram will be clarified in the next version of this draft.

The OAM architecture for MPLS-TP is illustrated in Figure 5.



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

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

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

Figure 5: MPLS-TP OAM archtecture

The following MPLS-TP MEs are specified in [26]:

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

Segment) between any LER/LSR along the LSP. o A MS-PW Tandem Connection Maintenance Entity (TPME), allows monitoring and management of a SS/MS-PW Tandem Connection (or PW Segment) between any T-PE/S-PE along the (MS-)PW.

Individual MIPs along the path of an LSP or PW are addressed by setting the appropriate TTL in the label for the OAM packet, as per [27]. Note that this works when the location of MIPs along the LSP or PW path is known by the MEP. There may be cases where this is not the case in general MPLS networks e.g. following restoration using a facility bypass LSP.

The following is a high level summary of the classes of OAM functions that MPLS-TP supports. These are intended to be applicable to any layer defined within MPLS- TP, i.e. MPLS Section, LSP and PW:

- Continuity Check
- Connectivity verification
- Performance monitoring
- Alarm suppression
- Remote Integrity

For all of the above listed functions except alarm suppression, both "continuous" and "on-demand" operation SHOULD be supported.

Performance monitoring includes means for both "packet loss measurement" and "delay measurement".

It is REQUIRED that MPLS-TP OAM packets share the same fate as their corresponding data packets and that a means exists to identify OAM packets. The document[8] proposes specific mechanisms relying on the combination of the 'Generic Alert Label (GAL)' and Generic Associated Channel Header for MPLS Sections and LSPs and using the Generic Associated Channel Header only for MPLS PWs. This is described in more detail elsewhere in this document Section 3.4.1 and Section 3.4.2.

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

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

3.4.1. Generic Associated Channel (G-ACH)

MPLS-TP makes use of a generic associated channel (G-ACH) to support Fault, Configuration, Accounting, Performance and Security (FCAPS) functions by carrying packets related to OAM, APS, SCC, MCC or other packet types in band over LSPs or PWs. The G-ACH is defined in [8]and it is similar to the PWE3 Associated Channel, which is used to carry OAM packets across pseudowires. The G-ACH is indicated by a generic associated channel header, similar to the PWE3 VCCV control word, and this is present for all LSPs and PWs making use of FCAPS functions supported by the G-ACH.

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 resticted to those names services. The G-ACH MUST NOT be used to carry additional data for use in the forwarding path, i.e. it MUST NOT be used as an alternative to a PW control word, or to define a PW type.

The messages transfered over the G-ACH MUST conform to the security and congestion considerations described in [8]. They must also take into consideration the throughput, latency and congestion requirements of the main data channel.

Figure 1 shows the reference model depicting how the control channel is associated with the pseudowire protocol stack, as per [9].

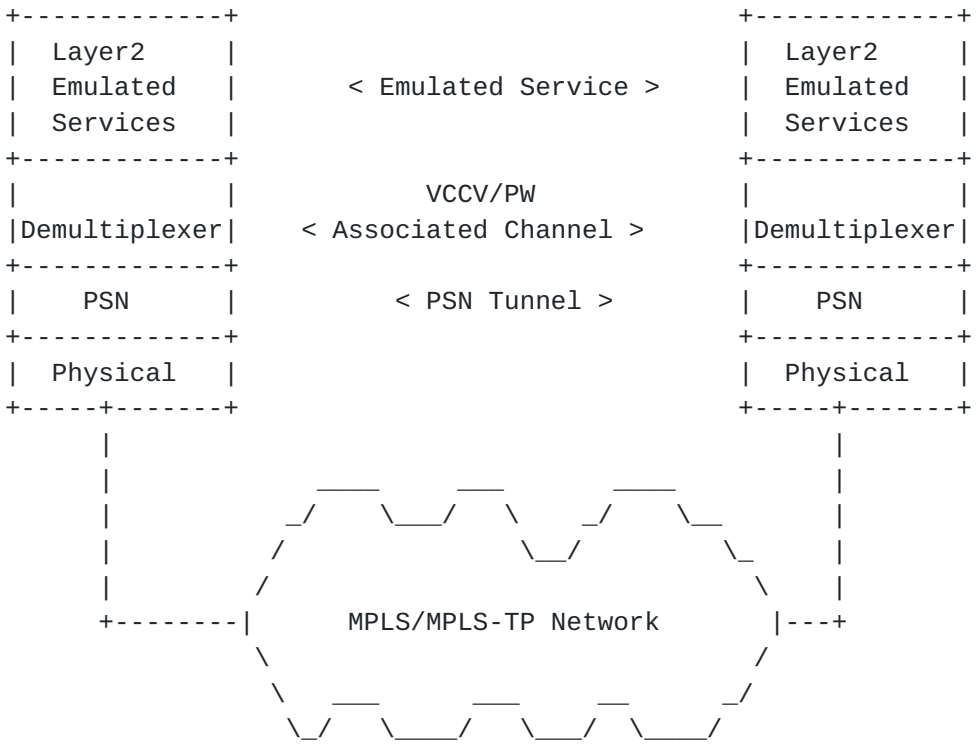


Figure 6: PWE3 Protocol Stack Reference Model including the PW Associated Control Channel

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

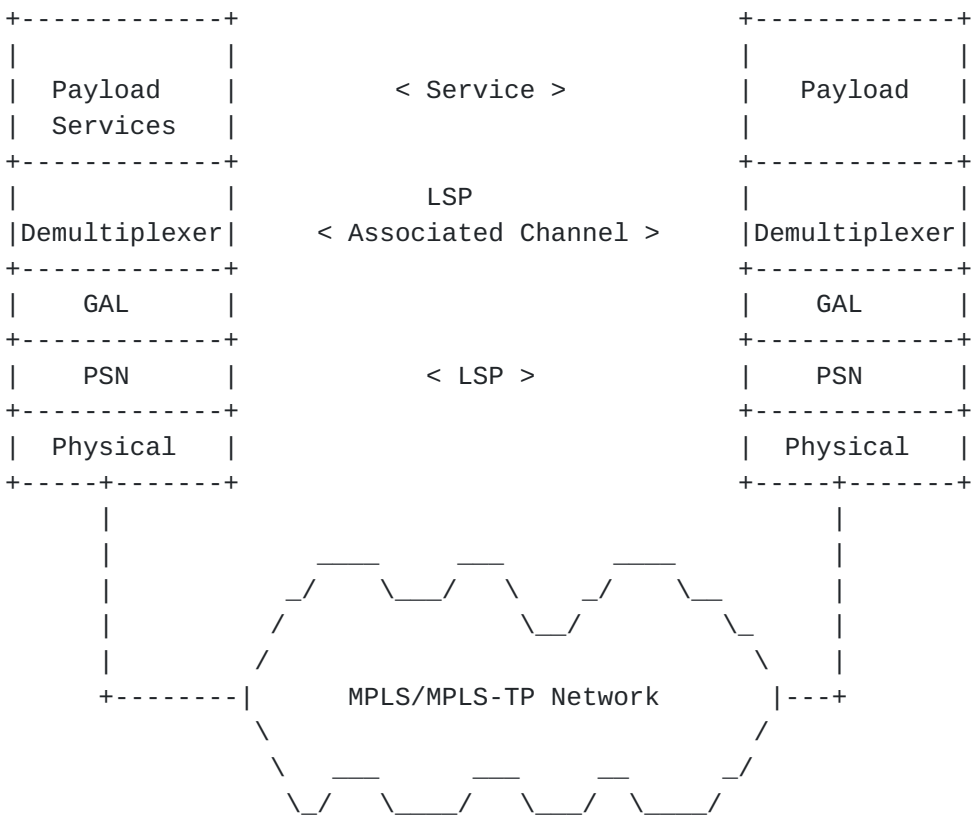


Figure 7: MPLS Protocol Stack Reference Model including the LSP Associated Control Channel

LSP associated channel messages are encapsulated using a generic associated control channel header (G-ACH). The presence of the GE-ACH is indicated by the inclusion of an additional 'Generic Alert Label (GAL)'. This arrangement means that both normal data packets and packets carrying an ACH are carried over LSPs in a similar manner.

Note that where a traffic engineered LSP is used the paths will be identical. If for any reason a non-traffic engineered path (for example an LDP path) were to be used the ECMP behaviour may be modified by the presence of the GAL.

3.4.2. Generic Alert Label (GAL)

For correct operation of the OAM it is important that the OAM packets fate share with the data packets. In addition in MPSL-TP it is necessary to indicate that the payload carried over an LSP is not user data. For example the packet may contain Signaling Communication Channel (SCC), or Automatic Protecton Switching (APS) data. The presence of the ACH indicates that the packet is not user data and identifies its type.

PWE3 uses the first nibble of the control word to provide the initial discrimination between data packets and "other" packets [10]. When the first nibble of a pseudwire packet has a value of one, then the first 32 bits that follow the bottom of stack have a defined format called an ACH, and which further defines the content of the pseudowire packet. For MPLS-TP this mechanism is further generalized to apply to also apply to LSPs and MPLS sections [8].

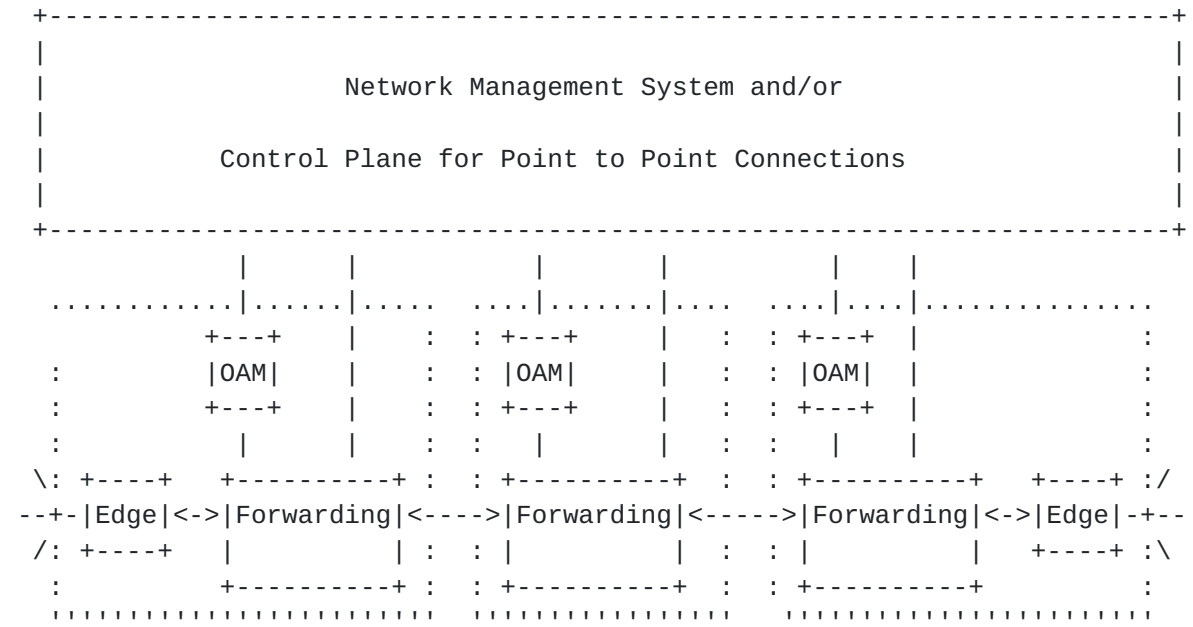
When the OAM, or a similar message is carried over an LSP, rather than over a pseudowire, it is necessary to provide an indication in the packet that the payload is something other than a regular data packet. This is acheived by including ia new reserved label in the label stack. This reserved label is referred to as the 'Generic Alert Label (GAL)', and is defined in [8]. When a GAL is found anywhere within the label stack it indicates that the payload begins with an 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 label being popped. The only circumstance under which the label stack may be inspected for a GAL is when the TTL has expired. Any MPLS-TP component which intentionally triggers this inspection must assume that the inspection to be asynchronous with respect to the forwarding of other packets.

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

3.5. Control Plane

The MPLS-TP may utilize a distributed control plane to enable fast, dynamic and reliable service provisioning in multi-vendor and multi-domain environments using standardized protocols that guarantee interoperability.

Figure 8 illustrates the relationshop between the MPLS-TP control plane, the forwarding plane, the management plane, and OAM.



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) OAM functions are described in more detail below.

Figure 8: MPLS-TP Control Plane Architecture Context

The MPLS-TP control plane is based on a combination of the MPLS control plane for pseudowires and the GMPLS control plane for MPLS-TP LSPs, respectively. More specifically, LDP is used for PW signaling and GMPLS based RSVP-TE for LSP signaling. The distributed MPLS-TP control plane provides the following basic functions:

- Signaling
- Routing
- Traffic engineering and constraint-based path computation

In a multi-domain environment, the MPLS-TP control plane may provide different types of interfaces at domain boundaries or within the domains such as UNI, I-NNI, and E-NNI where different policies are in place that control what kind of information is exchanged across these different types of interfaces.

Editor's note: Isn't the following a managment plane operation. I can't think of a routing protocol triggering an OAM message. Or do

we mean that the control plane is capable of reacting to OAM events? Control plane and OAM are independent.

The MPLS-TP control plane is capable of activating MPLS-TP OAM functions as described in the OAM section of this document Section 3.4 e.g. for fault detection and localization in the event of a failure in order to efficiently restore failed transport paths.

The MPLS-TP control plane supports all MPLS-TP data plane connectivity patterns that are needed for establishing transport paths including protected paths as described in the survivability section Section 3.7 of this document. Examples of the MPLS-TP data plane connectivity patterns are LSPs utilizing the fast reroute backup methods as defined in [11] and ingress-to-egress 1+1 or 1:1 protected LSPs.

Moreover, the MPLS-TP control plane needs to be capable of performing fast restoration in the event of network failures.

The MPLS-TP control plane provides features to ensure its own survivavbility and to enable it to recover gracefully from failures and degredations. These include graceful restart and hot redundant configurations. The MPLS-TP control plane is largely decoupled from the MPLS-TP data plane such that failures in the control plane do not impact the data plane and vice versa.

3.5.1. PW Control Plane

An MPLS-TP packet transport network provides many of its transport services in the form of single-segment or multi-segment pseudowires following the PWE3 architecture as defined in [3] and [4] . The setup and maintenance of single-segment or multi- segment pseudowires is based on the Label Distribution Protocol (LDP) as per [12] and the use of LDP in this manner is applicable to PWs used to provide MPLS transport services.

It shall be noted that multi-segment pseudowire signaling is still work in progress. The control plane supporting multi-segment pseudowires is based on [13].

3.5.2. LSP Control Plane

Editors note: The following must be reviewed by a CP specialist. Lou will review and provide comments.

MPLS-TP provider edge nodes aggregate multiple pseudowires and carry them across the MPLS-TP network through MPLS-TP tunnels (MPLS-TP LSPs). The generalized MPLS (GMPLS) protocol suite already supports

packet-switched capable (PSC) technologies and is therefore used as control plane for MPLS-TP transport paths (LSPs). The LSP control plane includes:

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

RSVP-TE signaling in support of GMPLS as defined in [14]is used for the setup, modification, and release of MPLS-TP transport paths and protection paths. It supports unidirectional, bi-directional and multicast types of LSPs. The route of a transport path is typically calculated in the ingress node of a domain and the RSVP explicit route object (ERO) is utilized for the setup of the transport path exactly following the given route. GMPLS based MPLS-TP LSPs must be able to interoperate with RSVP-TE based MPLS-TE LSPs, as per [28]

OSPF-TE routing in support of GMPLS as defined in [15] is used for carrying link state information in a MPLS-TP network.

For routing scalability reasons, parallel physical links in an MPLS-TP network are typically bundled into TE-links as defined in [16]and the OSPF-TE routing protocol disseminates link state information on a TE-link basis.

3.6. Static Operation of LSPs and PWs

Where a control plane is not used to set up and manage PWs or LSPs, the following considerations apply. Static configuration of the PW or LSP, either by direct configuration of the PEs/LSRs, or via a network management station must take care that loops to not form on an active LSP. The OAM would normally detect a break in end to end connectivity as a consequence of a loop, and withdraw the LSP from use. However the colateral damage that a loop can during the time taken to detect the failure is severe. Therefore an LSP should not be brought into operation until it certain that loops do not exist.

3.7. Survivability

Survivability requirements for MPLS-TP are apecified in [29].

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 ([11]), while pseudowire redundancy [17]supports scenarios where the protection for the PW can not be

fully provided by the PSN layer (i.e. where the backup PW terminates on a different target PE node than the working PW). Additionally, GMPLS provides a set of control plane driven well known protection and restoration mechanisms [14]. Finally, as part of the transport networks and applications paradigms, APS-based linear and ring protection mechanisms are defined in [18]and [30].

These schemes have different scopes. They are protecting against link and/or node failures and can be applied end-to-end or on a segment of the considered connection.

These protection schemes propose different levels of resiliency (e.g. 1+1, 1:1, shared).

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

MPLS-TP resiliency mechanisms characteristics are listed below

- Linear, ring and meshed protection schemes are supported.
- As with all network layer protection schemes, MPLS-TP recovery mechanisms (protection and restoration), rely on OAM mechanisms to detect and localize network faults or service degenerations.
- APS-based protection mechanisms (linear and ring) rely on MPLS-TP APS mechanisms to coordinate and trigger protection switching actions.
- MPLS-TP recovery schemes are designed to be applicable at various levels (MPLS section, LSP and PW), providing segment and end-to-end recovery.
- MPLS-TP recovery mechanisms support means for avoiding race conditions in switching activity triggered by a fault condition detected both at server layer and at MPLS-TP layer.
- MPLS-TP recovery mechanisms can be data plane, control plane or management plane based.
- MPLS-TP allows for revertive and non-revertive behavior
- Multiple resiliency mechanisms can be applied to any connection

3.8. Network Management

The network management architecture and requirements for MPLS-TP are specified in [22]. It derives from the generic specifications described in ITU-T G.7710/Y.1701 [19]for transport technologies. It also leverages on the OAM requirements for MPLS Networks [31] and MPLS-TP Networks [21]and expands on the requirements to cover the modifications necessary for fault, configuration, performance, and security.

The Equipment Management Function (EMF) of a MPLS-TP NE provides the means through which a management system manages the NE. The Management Communication Channel (MCC), realized by the G-ACH, provides a logical operations channel between NEs for transferring Management information. For the management interface from a management system to a MPLS-TP NE, there is no restriction on which management protocol should be used. It is allowed to provision and manage an end-to-end connection across a network where some segments are create/managed, for examples by Netconf or SNMP and other segments by XML or CORBA interfaces. It is allowed to run maintenance operations on a connection which is independent of the provisioning mechanism. An MPLS-TP NE is not required to offer more than one standard management interface. In MPLS-TP. the EMF MUST be capable of statically provisioning LSPs for an LSR or LER, and PWs for a PE, as per Section 3.6.

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

Configuration Management (CM) provides functions to exercise control over, 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 configuration of the OAM parameters as part of connectivity management to meet specific operational requirements, such as whether one-time on-demand or periodically based on a specified frequency.

The Performance Management (PM) functions within the EMF of an MPLS-TP NE supports the evaluation and reporting upon the behaviour of the

equipment, NE, and network with the objective of providing coherent and consistent interpretation of the network behaviour, in particular for hybrid network which consists of multiple transport technologies. Packet loss measurement and delay measurement are collected so that they can be used to detect performance degradation. Performance degradation is reported via fault management for corrective actions (e.g. protection switch) and via performance monitoring for Service Level Agreement (SLA) verification and billing. The performance data collection mechanisms should be flexible to be configured to operate on-demand or proactively.

4. Security Considerations

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

Specific security considerations for MPLS-TP will be detailed in documents covering specific aspects on the MPLS-TP architecture.

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:

- Dieter Beller
- Italo Busi
- Hing-Kam Lam
- Marc Lasserre
- Vincenzo Sestito
- Martin Vigoureux

7. References

7.1. Normative References

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

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

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

[4] Bocci, M. and S. Bryant, "An Architecture for Multi-Segment Pseudowire Emulation Edge-to-Edge", draft-ietf-pwe3-ms-pw-arch-05 (work in progress), September 2008.

[5] Andersson, L. and R. Asati, ""EXP field" renamed to "Traffic Class field"", draft-ietf-mpls-cosfield-def-07 (work in progress), November 2008.

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

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

[8] Vigoureux, M., Bocci, M., Ward, D., Swallow, G., and R. Aggarwal, "MPLS Generic Associated Channel", draft-bocci-mpls-tp-gach-gal-00 (work in progress), October 2008.

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

[10] 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.

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

[12] 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.

[13] Martini, L., Bocci, M., Bitar, N., Shah, H., Aissaoui, M., and F. Balus, "Dynamic Placement of Multi Segment Pseudo Wires", draft-ietf-pwe3-dynamic-ms-pw-08 (work in progress), July 2008.

[14] 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.

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

[16] Kompella, K., Rekhter, Y., and L. Berger, "Link Bundling in MPLS Traffic Engineering (TE)", RFC 4201, October 2005.

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

[18] "ITU-T Recommendation G.8131/Y.1382 (02/07) " Linear protection switching for Transport MPLS (T-MPLS) networks"", 2005.

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

7.2. Informative References

[20] Niven-Jenkins, B., Brungard, D., Betts, M., and N. Sprecher, "MPLS-TP Requirements", draft-jenkins-mpls-mpls-tp-requirements-01 (work in progress), October 2008.

[21] Vigoureux, M., Ward, D., Betts, M., Bocci, M., and I. Busi, "Requirements for OAM in MPLS Transport Networks", draft-vigoureux-mpls-tp-oam-requirements-01 (work in progress), November 2008.

[22] Mansfield, S., Lam, K., and E. Gray, "MPLS TP Network Management Requirements", draft-gray-mpls-tp-nm-req-01 (work in progress), October 2008.

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

[24] Aggarwal, R., Kompella, K., Nadeau, T., and G. Swallow, "BFD

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

[25] Bryant, S., Filsfils, C., and U. Drafz, "Load Balancing Fat MPLS Pseudowires", draft-bryant-filsfils-fat-pw-02 (work in progress), July 2008.

[26] Busi, I. and B. Niven-Jenkins, "MPLS-TP OAM Framework and Overview", draft-busi-mpls-tp-oam-framework-00 (work in progress), October 2008.

[27] Nadeau, T., Metz, C., Duckett, M., Bocci, M., Balus, F., and L. Martini, "Segmented Pseudo Wire", draft-ietf-pwe3-segmented-pw-09 (work in progress), July 2008.

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

[29] Sprecher, N., Farrel, A., and V. Kompella, "Multiprotocol Label Switching Transport Profile Survivability Framework", draft-sprecher-mpls-tp-survive-fwk-00 (work in progress), July 2008.

[30] "Draft ITU-T Recommendation G.8132/Y.1382, "T-MPLS shared protection ring", http://www.itu.int/md/T05-SG15-080211-TD-PLEN-0501/en", 2005.

[31] 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.

Authors' Addresses

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

Phone: +44-207-254-5874
EMail: matthew.bocci@alcatel-lucent.com

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

Phone: +44-208-824-8828
EMail: stbryant@cisco.com

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

Phone: +33-6-33-86-1916
EMail: lieven.levrau@alcatel-lucent.com

Full Copyright Statement

Intellectual Property