MPLS Working Group
Internet Draft
Intended status: Informational

I. Busi (Ed)
Alcatel-Lucent
B. Niven-Jenkins (Ed)
BT
D. Allan (Ed)
Ericsson

Expires: September 5, 2010

March 5, 2010

MPLS-TP OAM Framework
draft-ietf-mpls-tp-oam-framework-05.txt

Abstract

Multi-Protocol Label Switching (MPLS) Transport Profile (MPLS-TP) is based on a profile of the MPLS and pseudowire (PW) procedures as specified in the MPLS Traffic Engineering (MPLS-TE), pseudowire (PW) and multi-segment PW (MS-PW) architectures complemented with additional Operations, Administration and Maintenance (OAM) procedures for fault, performance and protection-switching management for packet transport applications that do not rely on the presence of a control plane.

This document describes a framework to support a comprehensive set of OAM procedures that fulfills the MPLS-TP OAM requirements [12].

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.

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 September 5, 2010.

Copyright Notice

Table of Contents

Editors' Note:

This Informational Internet-Draft is aimed at achieving IETF Consensus before publication as an RFC and will be subject to an IETF Last Call.

[RFC Editor, please remove this note before publication as an RFC and insert the correct Streams Boilerplate to indicate that the published RFC has IETF Consensus.]

1. Introduction

As noted in [8], MPLS-TP defines a profile of the MPLS-TE and (MS-)PW architectures defined in RFC 3031 [2], RFC 3985 [5] and [7] which is complemented with additional OAM mechanisms and procedures for alarm, fault, performance and protection-switching management for packet transport applications.

In line with [13], existing MPLS OAM mechanisms will be used wherever possible and extensions or new OAM mechanisms will be defined only where existing mechanisms are not sufficient to meet the requirements.

The MPLS-TP OAM framework defined in this document provides a comprehensive set of OAM procedures that satisfy the MPLS-TP OAM requirements [12]. In this regard, it defines similar OAM functionality as for existing SONET/SDH and OTN OAM mechanisms (e.g. [16]).

The MPLS-TP OAM framework is applicable to both LSPs and (MS-)PWs and supports co-routed and bidirectional p2p transport paths as well as unidirectional p2p and p2mp transport paths.

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.

1.1. Contributing Authors

Dave Allan, Italo Busi, Ben Niven-Jenkins, Annamaria Fulignoli, Enrique Hernandez-Valencia, Lieven Levrau, Dinesh Mohan, Vincenzo Sestito, Nurit Sprecher, Huub van Helvoort, Martin Vigoureux, Yaacov Weingarten, Rolf Winter

2. Conventions used in this document

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 RFC-2119 [1].

2.1. Terminology

AC Attachment Circuit

DBN Domain Border Node

FDI Forward Defect Indication

LER Label Edge Router

LME LSP Maintenance Entity

LSP Label Switched Path

LSR Label Switch Router

LPSTME LSP packet segment tunnel ME

ME Maintenance Entity

MEG Maintenance Entity Group

MEP Maintenance Entity Group End Point

MIP Maintenance Entity Group Intermediate Point

PHB Per-hop Behavior

PME PW Maintenance Entity

PPSTME PW path segment tunnel ME

PST Path Segment Tunnel

PSN Packet Switched Network

PW Pseudowire

SLA Service Level Agreement

SME Section Maintenance Entity

2.2. Definitions

Note - the definitions in this section are intended to be in line with ITU-T recommendation Y.1731 in order to have a common, unambiguous terminology. They do not however intend to imply a certain implementation but rather serve as a framework to describe the necessary OAM functions for MPLS-TP.

Data plane loopback: it is an out-of-service test where an interface at either an intermediate or terminating node in a path is placed into a data plane loopback state, such that it loops back all the packets (including user data and OAM) it receives on a specific MPLS-TP transport path.

Domain Border Node (DBN): An LSP intermediate MPLS-TP node (LSR) that is at the boundary of an MPLS-TP OAM domain. Such a node may be present on the edge of two domains or may be connected by a link to an MPLS-TP node in another OAM domain.

Loopback: see data plane loopback and OAM loopback definitions.

Maintenance Entity (ME): Some portion of a transport path that requires management bounded by two points, and the relationship between those points to which maintenance and monitoring operations apply (details in section 3.1).

Maintenance Entity Group (MEG): The set of one or more maintenance entities that maintain and monitor a transport path in an OAM domain.

MEP: A MEG end point (MEP) is capable of initiating (MEP Source) and terminating (MEP Sink) OAM messages for fault management and performance monitoring. MEPs reside at the boundaries of an ME (details in section 3.3).

MEP Source: A MEP acts as MEP source for an OAM message when it originates and inserts the message into the transport path for its associated MEG.

MEP Sink: A MEP acts as a MEP sink for an OAM message when it terminates and processes the messages received from its associated MEG.

MIP: A MEG intermediate point (MIP) terminates and processes OAM messages and may generate OAM messages in reaction to received OAM messages. It never generates unsolicited OAM messages itself. A MIP resides within an MEG between MEPs (details in section 3.3).

OAM domain: A domain, as defined in [11], whose entities are grouped for the purpose of keeping the OAM confined within that domain.

Note - within the rest of this document the term "domain" is used to indicate an "OAM domain"

OAM flow: Is the set of all OAM messages originating with a specific MEP that instrument one direction of a MEG.

OAM information element: An atomic piece of information exchanged between MEPs in MEG used by an OAM application.

OAM loopback: it is the capability of a node to intercepts some specific OAM packets and to generate a reply back to their sender. OAM loopback can work in-service and can support different OAM functions (e.g., bidirectional on-demand connectivity verification).

OAM Message: One or more OAM information elements that when exchanged between MEPs or between MEPs and MIPs performs some OAM functionality (e.g. connectivity verification)

OAM Packet: A packet that carries one or more OAM messages (i.e. OAM information elements).

Path: See Transport Path

Signal Fail: A condition declared by a MEP when the data forwarding capability associated with a transport path has failed, e.g. loss of continuity.

Tandem Connection: A tandem connection is an arbitrary part of a transport path that can be monitored (via OAM) independent of the end-to-end monitoring (OAM). The tandem connection may also include the forwarding engine(s) of the node(s) at the boundaries of the tandem connection.

This document uses the terms defined in RFC 5654 [11].

This document uses the term 'Per-hop Behavior' as defined in [14].

3. Functional Components

MPLS-TP defines a profile of the MPLS and PW architectures ([2], [5] and [7]) that is required to transport service traffic where the characteristics of information transfer between the transport path endpoints can be demonstrated to comply with certain performance and quality guarantees.

In order to describe the required OAM functionality, this document introduces a set of high-level functional components.

3.1. Maintenance Entity and Maintenance Entity Group

MPLS-TP OAM operates in the context of Maintenance Entities (MEs) that are a relationship between two points of a point to point transport path or a root and a leaf of a point to multipoint transport path to which maintenance and monitoring operations apply. These two points are called Maintenance Entity Group (MEG) End Points (MEPs). In between these two points zero or more intermediate points, called Maintenance Entity Group Intermediate Points (MIPs), MAY exist and can be shared by more than one ME in a MEG.

The abstract reference model for an ME with MEPs and MIPs is described in Figure 1 below:

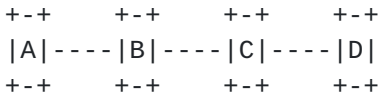


Figure 1 ME Abstract Reference Model

The instantiation of this abstract model to different MPLS-TP entities is described in section 4. In this model, nodes A, B, C and D can be LER/LSR for an LSP or the {S|T}-PEs for a MS-PW. MEPs reside in nodes A and D while MIPs reside in nodes B and C. The links connecting adjacent nodes can be physical links, (sub-)layer LSPs/PSTs, or serving layer paths.

This functional model defines the relationships between all OAM entities from a maintenance perspective, to allow each Maintenance Entity to monitor and manage the (sub-)layer network under its responsibility and to localize problems efficiently.

Another OAM functional component is referred to as Maintenance Entity Group, which is a collection of one or more MEs that belongs to the same transport path and that are maintained and monitored as a group. An MPLS-TP Maintenance Entity Group may be defined to monitor the transport path for fault and/or performance management.

The MEPs that form an MEG are configured and managed to limit the scope of an OAM flow within the MEG that the MEPs belong to (i.e. within the domain of the transport path that is being monitored and managed). A misbranching fault may cause OAM packets to be delivered to a MEP that is not in the MEG of origin.

In case of unidirectional point-to-point transport paths, a single unidirectional Maintenance Entity is defined to monitor it.

In case of associated bi-directional point-to-point transport paths, two independent unidirectional Maintenance Entities are defined to independently monitor each direction. This has implications for transactions that terminate at or query a MIP as a return path from MIP to source MEP does not necessarily exist in a unidirectional MEG.

In case of co-routed bi-directional point-to-point transport paths, a single bidirectional Maintenance Entity is defined to monitor both directions congruently.

In case of unidirectional point-to-multipoint transport paths, a single unidirectional Maintenance entity for each leaf is defined to monitor the transport path from the root to that leaf.

The reference model for the p2mp MEG is represented in Figure 2.

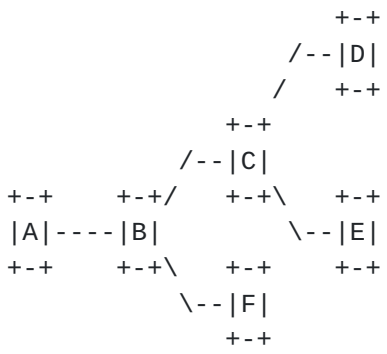


Figure 2 Reference Model for p2mp MEG

In case of p2mp transport paths, the OAM operations are independent for each ME (A-D, A-E and A-F):

- Fault conditions - some faults may impact more than one ME depending from where the failure is located;
- Packet loss - packet dropping may impact more than one ME depending from where the packets are lost;
- Packet delay - will be unique per ME.

Each leaf (i.e. D, E and F) terminates OAM flows to monitor the ME from itself and the root while the root (i.e. A) generates OAM

messages common to all the MEs of the p2mp MEG. Nodes B and C MAY implement a MIP in the corresponding MEG.

3.2. Nested MEGs: Path Segment Tunnels and Tandem Connection Monitoring

In order to verify and maintain performance and quality guarantees, there is a need to not only apply OAM functionality on a transport path granularity (e.g. LSP or MS-PW), but also on arbitrary parts of transport paths, defined as Tandem Connections, between any two arbitrary points along a transport path.

Path segment tunnels (PSTs), as defined in [8], are instantiated to provide monitoring of a portion of a set of co-routed transport paths (LSPs or MS-PWs). Path segment tunnels can also be employed to meet the requirement to provide tandem connection monitoring (TCM).

TCM for a given portion of a transport path is implemented by first creating a path segment tunnel that has a 1:1 association with portion of the transport path that is to be uniquely monitored. This means there is direct correlation between all FM and PM information gathered for the PST AND the monitored portion of the E2E transport path. The PST is monitored using normal LSP monitoring.

There are a number of implications to this approach:

1) The PST would use the uniform model of TC code point copying between sub-layers for diffserv such that the E2E markings and PHB treatment for the transport path was preserved by the PST.

2) The PST would use the pipe model for TTL handling such that MIP addressing for the E2E entity would be not be impacted by the presence of the PST.

3) PM statistics need to be adjusted for the encapsulation overhead of the additional PST sub-layer.

A PST is instantiated to create an MEG that monitors a segment of a transport path (LSP or PW). The endpoints of the PST are MEPs and limit the scope of an OAM flow within the MEG the MEPs belong to (i.e. within the domain of the PST that is being monitored and managed).

The following properties apply to all MPLS-TP MEGs:

- They can be nested but not overlapped, e.g. an MEG may cover a segment or a concatenated segment of another MEG, and may also include the forwarding engine(s) of the node(s) at the edge(s) of the segment or concatenated segment, but all its MEPs and MIPs are no longer part of the encompassing MEG. It is possible that MEPs of nested MEGs reside on a single node.

- It is possible for MEPs of nested MEGs to reside on a single node.

- Each OAM flow is associated with a single Maintenance Entity Group.

- OAM packets that instrument a particular direction of a transport path are subject to the same forwarding treatment (i.e. fate share) as the data traffic and in some cases may be required to have common queuing discipline E2E with the class of traffic monitored. OAM packets can be distinguished from the data traffic using the GAL and ACH constructs [9] for LSP and Section or the ACH construct [6]and [9] for (MS-)PW.

3.3. MEG End Points (MEPs)

MEG End Points (MEPs) are the source and sink points of an MEG. In the context of an MPLS-TP LSP, only LERs can implement MEPs while in the context of a path segment tunnel (PST) both LERs and LSRs can implement MEPs that contribute to the overall monitoring infrastructure for the transport path. Regarding MPLS-TP PW, only T-PEs can implement MEPs while for PSTs supporting a PW both T-PEs and S-PEs can implement MEPs. In the context of MPLS-TP Section, any MPLS-TP LSR can implement a MEP.

MEPs are responsible for activating and controlling all of the OAM functionality for the MEG. A MEP is capable of originating and terminating OAM messages for fault management and performance monitoring. These OAM messages are encapsulated into an OAM packet using the G-ACh as defined in RFC 5586 [9]: in this case the G-ACh message is an OAM message and the channel type indicates an OAM message. A MEP terminates all the OAM packets it receives from the MEG it belongs to. The MEG the OAM packet belongs to is inferred from the MPLS or PW label or, in case of MPLS-TP section, the MPLS-TP port the OAM packet has been received with the GAL at the top of the label stack.

OAM packets may require the use of an available "out-of-band" return path (as defined in [8]). In such cases sufficient information is required in the originating transaction such that the OAM reply packet can be constructed (e.g. IP address).

Once an MEG is configured, the operator can configure which OAM functions to use on the MEG but the MEPs are always enabled. A node at the edge of an MEG always supports a MEP.

MEPs terminate all OAM packets received from the associated MEG. As the MEP corresponds to the termination of the forwarding path for an MEG at the given (sub-)layer, OAM packets never "leaks" outside of a MEG in a fault free implementation.

A MEP of an MPLS-TP transport path (Section, LSP or PW) coincides with transport path termination and monitors it for failures or performance degradation (e.g. based on packet counts) in an end-to-end scope. Note that both MEP source and MEP sink coincide with transport paths' source and sink terminations.

The MEPs of a path segment tunnel are not necessarily coincident with the termination of the MPLS-TP transport path (LSP or PW) and monitor some portion of the transport path for failures or performance degradation (e.g. based on packet counts) only within the boundary of the MEG for the path segment tunnel.

An MPLS-TP MEP sink passes a fault indication to its client (sub-)layer network as a consequent action of fault detection.

It may occur that the MEPs of a path segment tunnel are set on both sides of the forwarding engine such that the MEG is entirely internal to the node.

Note that a MEP can only exist at the beginning and end of a layer i.e. an LSP or PW. If we need to monitor some portion of that LSP or PW, a new sub-layer in the form of a path segment tunnel MUST be created which permits MEPs and an associated MEG to be created.

We have the case of an intermediate node sending msg to a MEP. To do this it uses the LSP label - i.e. the top label of the stack at that point.

3.4. MEG Intermediate Points (MIPs)

A MEG Intermediate Point (MIP) is a point between the MEPs of an MEG.

A MIP is capable of reacting to some OAM packets and forwarding all the other OAM packets while ensuring fate sharing with data plane packets. However, a MIP does not initiate unsolicited OAM packets, but may be addressed by OAM packets initiated by one of the MEPs of the MEG. A MIP can generate OAM packets only in response to OAM packets that are sent on the MEG it belongs to.

An intermediate node within a MEG can either:

o support per-node MIP (i.e. a single MIP per node)

o support per-interface MIP (i.e. two or more MIPs per node on both sides of the forwarding engine)

When sending an OAM packet to a MIP, the source MEP should set the TTL field to indicate the number of hops necessary to reach the node where the MIP resides. It is always assumed that the "pipe"/"short pipe" model of TTL handling is used by the MPLS transport profile.

The source MEP should also include Target MIP information in the OAM packets sent to a MIP to allow proper identification of the MIP within the node. The MEG the OAM packet is associated with is inferred from the MPLS label.

A node at the edge of an MEG can also support per-interface MEPs and per-interface MIPs on either side of the forwarding engine.

Once an MEG is configured, the operator can enable/disable the MIPs on the nodes within the MEG. All the intermediate nodes host MIP(s). Local policy allows them to be enabled per function and per LSP. The local policy is controlled by the management system, which may delegate it to the control plane.

3.5. Server MEPs

A server MEP is a MEP of an MEG that is either:

o defined in a layer network that is "below", which is to say encapsulates and transports the MPLS-TP layer network being referenced, or

o defined in a sub-layer of the MPLS-TP layer network that is "below" which is to say encapsulates and transports the sub-layer being referenced.

A server MEP can coincide with a MIP or a MEP in the client (MPLS-TP) (sub-)layer network.

A server MEP also interacts with the client/server adaptation function between the client (MPLS-TP) (sub-)layer network and the server (sub-)layer network. The adaptation function maintains state on the mapping of MPLS-TP transport paths that are setup over that server (sub-)layer's transport path.

For example, a server MEP can be either:

- A termination point of a physical link (e.g. 802.3), an SDH VC or OTN ODU, for the MPLS-TP Section layer network, defined in section 4.1;

- An MPLS-TP Section MEP for MPLS-TP LSPs, defined in section 4.2;

- An MPLS-TP LSP MEP for MPLS-TP PWs, defined in section 4.4;

- An MPLS-TP PST MEP used for LSP segment monitoring, as defined in section 4.3, for MPLS-TP LSPs or higher-level LSP PSTs;

- An MPLS-TP PST MEP used for PW segment monitoring, as defined in section 4.5, for MPLS-TP PWs or higher-level PW PSTs.

The server MEP can run appropriate OAM functions for fault detection within the server (sub-)layer network, and provides a fault indication to its client MPLS-TP layer network. Server MEP OAM functions are outside the scope of this document.

3.6. Configuration Considerations

When a control plane is not present, the management plane configures these functional components. Otherwise they can be configured either by the management plane or by the control plane.

Local policy allows to disable the usage of any available "out-of-band" return path, as defined in [8], to generate OAM reply packets, irrespectively on what is requested by the node originating the OAM packet triggering the request.

PSTs are usually instantiated when the transport path is created by either the management plane or by the control plane (if present). Sometimes PST can be instantiated after the transport path is initially created (e.g. PST).

3.7. P2MP considerations

All the traffic sent over a p2mp transport path, including OAM packets generated by a MEP, is sent (multicast) from the root to all the leaves. As a consequence:

- To send an OAM packet to all leaves, the source MEP can send a single OAM packet that will be delivered by the forwarding plane to all the leaves and processed by all the leaves.

- To send an OAM packet to a single leaf, the source MEP sends a single OAM packet that will be delivered by the forwarding plane to all the leaves but contains sufficient information to identify a target leaf, and therefore is processed only by the target leaf and ignored by the other leaves.

- In order to send an OAM packet to M leaves (i.e., a subset of all the leaves), the source MEP sends M different OAM packets targeted to each individual leaf in the group of M leaves. Better mechanisms are outside the scope of this document.

P2MP paths are unidirectional, therefore any return path to a source MEP for on demand transactions will be out of band.

A mechanism to scope the set of MEPs or MIPs expected to respond to a given "on demand" transaction is useful as it relieves the source MEP of the requirement to filter and discard undesired responses as normally TTL exhaust will address all MIPs at a given distance from the source, and failure to exhaust TTL will address all MEPs.

4. Reference Model

The reference model for the MPLS-TP framework builds upon the concept of an MEG, and its associated MEPs and MIPs, to support the functional requirements specified in [12].

The following MPLS-TP MEGs are specified in this document:

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

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

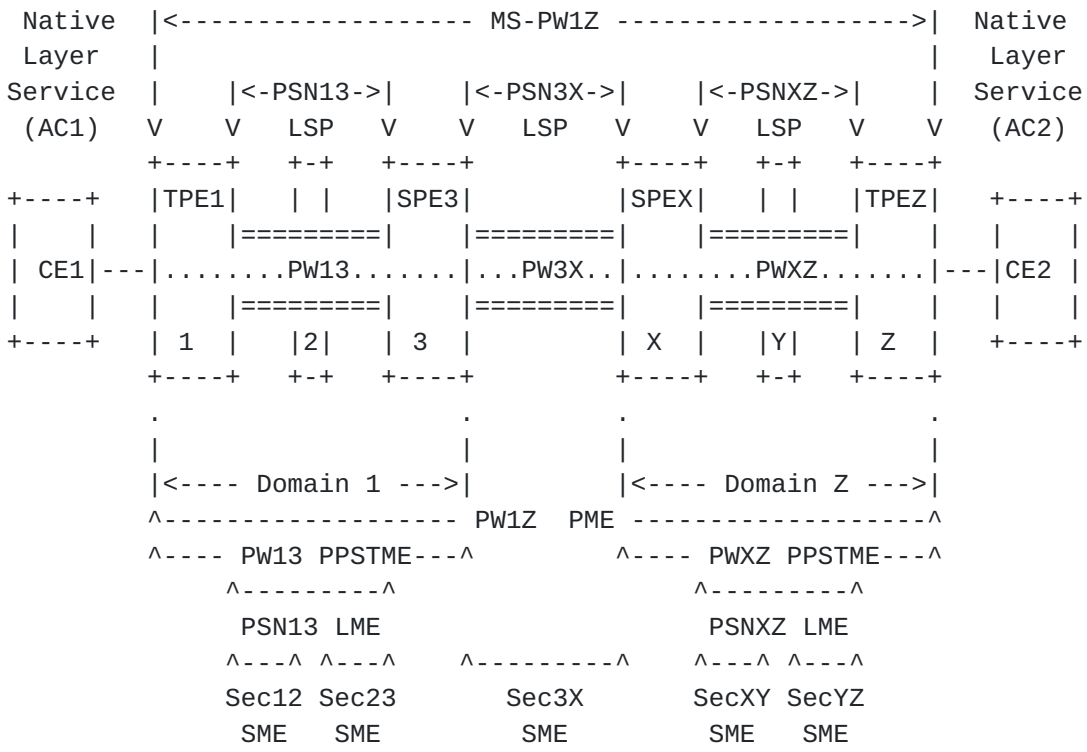
- A PW Maintenance Entity Group (PME), allowing monitoring and management of an end-to-end SS/MS-PWs (between T-PEs).

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

- A MS-PW PST Maintenance Entity (PPSTME), allowing monitoring and management of an MPLS-TP path segment tunnel (between any T-PEs/S-PEs along the (MS-)PW).

The MEGs specified in this MPLS-TP framework are compliant with the architecture framework for MPLS-TP MS-PWs [7] and LSPs [2].

Hierarchical LSPs are also supported in the form of path segment tunnels. In this case, each LSP Tunnel in the hierarchy is a different sub-layer network that can be monitored, independently from higher and lower level LSP tunnels in the hierarchy, on an end-to-end basis (from LER to LER) by a PSTME. It is possible to monitor a portion of a hierarchical LSP by instantiating a hierarchical PSTME between any LERs/LSRs along the hierarchical LSP.



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

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

Figure 3 Reference Model for the MPLS-TP OAM Framework

Figure 3 depicts a high-level reference model for the MPLS-TP OAM framework. The figure depicts portions of two MPLS-TP enabled network domains, Domain 1 and Domain Z. In Domain 1, LSR1 is adjacent to LSR2 via the MPLS Section Sec12 and LSR2 is adjacent to LSR3 via the MPLS Section Sec23. Similarly, in Domain Z, LSRX is adjacent to LSRY via the MPLS Section SecXY and LSRY is adjacent to LSRZ via the MPLS Section SecYZ. In addition, LSR3 is adjacent to LSRX via the MPLS Section 3X.

Figure 3 also shows a bi-directional MS-PW (PW1Z) between AC1 on TPE1 and AC2 on TPEZ. The MS-PW consists of three bi-directional PW Segments: 1) PW13 segment between T-PE1 and S-PE3 via the bi-directional PSN13 LSP, 2) PW3X segment between S-PE3 and S-PEX, via the bi-directional PSN3X LSP, and 3) PWXZ segment between S-PEX and T-PEZ via the bi-directional PSNXZ LSP.

The MPLS-TP OAM procedures that apply to an MEG are expected to operate independently from procedures on other MEGs. Yet, this does not preclude that multiple MEGs may be affected simultaneously by the same network condition, for example, a fiber cut event.

Note that there are no constrains imposed by this OAM framework on the number, or type (p2p, p2mp, LSP or PW), of MEGs that may be instantiated on a particular node. In particular, when looking at Figure 3, it should be possible to configure one or more MEPs on the same node if that node is the endpoint of one or more MEGs.

Figure 3 does not describe a PW3X PPSTME because typically PSTs are used to monitor an OAM domain (like PW13 and PWXZ PPSTMEs) rather than the segment between two OAM domains. However the OAM framework does not pose any constraints on the way PSTs are instantiated as long as they are not overlapping.

The subsections below define the MEGs specified in this MPLS-TP OAM architecture framework document. Unless otherwise stated, all references to domains, LSRs, MPLS Sections, LSPs, pseudowires and MEGs in this section are made in relation to those shown in Figure 3.

4.1. MPLS-TP Section Monitoring (SME)

An MPLS-TP Section ME (SME) is an MPLS-TP maintenance entity intended to an MPLS Section as defined in [11]. An SME may be configured on any MPLS section. SME OAM packets must fate share with the user data packets sent over the monitored MPLS Section.

An SME is intended to be deployed for applications where it is preferable to monitor the link between topologically adjacent (next hop in this layer network) MPLS (and MPLS-TP enabled) LSRs rather than monitoring the individual LSP or PW segments traversing the MPLS Section and the server layer technology does not provide adequate OAM capabilities.

Figure 3 shows 5 Section MEs configured in the network between AC1 and AC2:

1. Sec12 ME associated with the MPLS Section between LSR 1 and LSR 2,

2. Sec23 ME associated with the MPLS Section between LSR 2 and LSR 3,

3. Sec3X ME associated with the MPLS Section between LSR 3 and LSR X,

4. SecXY ME associated with the MPLS Section between LSR X and LSR Y, and

5. SecYZ ME associated with the MPLS Section between LSR Y and LSR Z.

4.2. MPLS-TP LSP End-to-End Monitoring (LME)

An MPLS-TP LSP ME (LME) is an MPLS-TP maintenance entity intended to monitor an end-to-end LSP between two LERs. An LME may be configured on any MPLS LSP. LME OAM packets must fate share with user data packets sent over the monitored MPLS-TP LSP.

An LME is intended to be deployed in scenarios where it is desirable to monitor an entire LSP between its LERs, rather than, say, monitoring individual PWs.

Figure 3 depicts 2 LMEs configured in the network between AC1 and AC2: 1) the PSN13 LME between LER 1 and LER 3, and 2) the PSNXZ LME between LER X and LER Y. Note that the presence of a PSN3X LME in such a configuration is optional, hence, not precluded by this framework. For instance, the SPs may prefer to monitor the MPLS-TP Section between the two LSRs rather than the individual LSPs.

4.3. MPLS-TP LSP Path Segment Tunnel Monitoring (LPSTME)

An MPLS-TP LSP Path Segment Tunnel ME (LPSTME) is an MPLS-TP maintenance entity intended to monitor an arbitrary part of an LSP between a given pair of LSRs independently from the end-to-end monitoring (LME). An LPSTMEE can monitor an LSP segment or concatenated segment and it may also include the forwarding engine(s) of the node(s) at the edge(s) of the segment or concatenated segment.

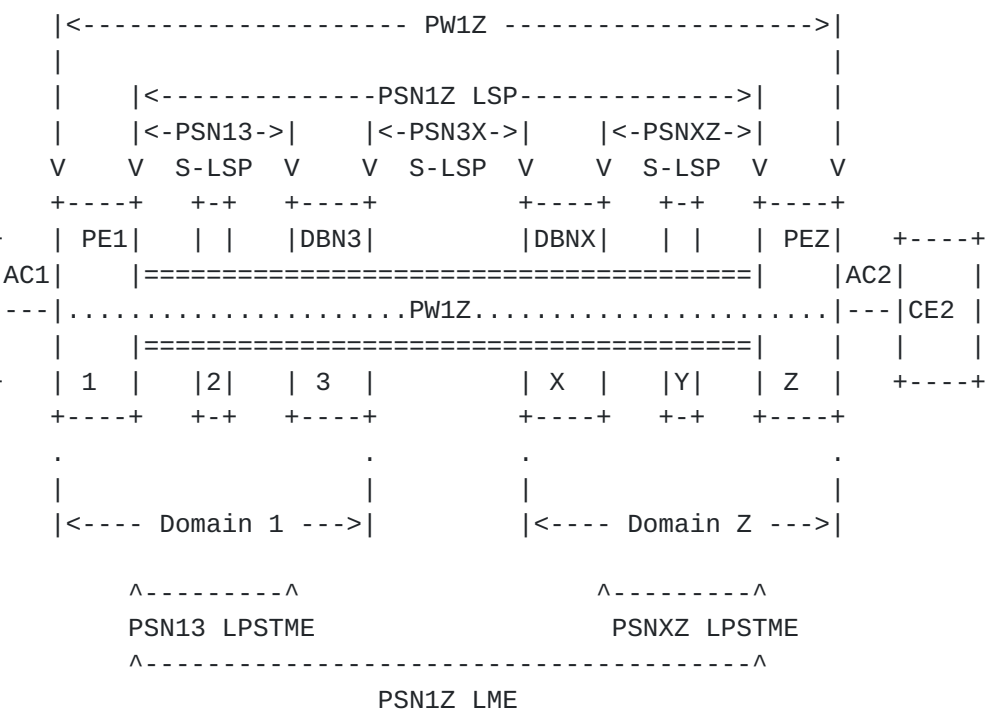
Multiple LPSTMEs MAY be configured on any LSP. The LSRs that terminate the LPSTME may or may not be immediately adjacent at the MPLS-TP layer. LPSTME OAM packets must fate share with the user data packets sent over the monitored LSP segment.

A LPSTME can be defined between the following entities:

o LER and any LSR of a given LSP.

o Any two LSRs of a given LSP.

An LPSTME is intended to be deployed in scenarios where it is preferable to monitor the behaviour of a part of an LSP or set of LSPs rather than the entire LSP itself, for example when there is a need to monitor a part of an LSP that extends beyond the administrative boundaries of an MPLS-TP enabled administrative domain.



DBN: Domain Border Node

Figure 4 MPLS-TP LSP Path Segment Tunnel ME (LPSTME)

Figure 4 depicts a variation of the reference model in Figure 3 where there is an end-to-end PSN LSP (PSN1Z LSP) between PE1 and PEZ. PSN1Z LSP consists of, at least, three LSP Concatenated Segments: PSN13, PSN3X and PSNXZ. In this scenario there are two separate LPSTMEs configured to monitor the PSN1Z LSP: 1) a LPSTME monitoring the PSN13 LSP Concatenated Segment on Domain 1 (PSN13 LPSTME), and 2) a LPSTME monitoring the PSNXZ LSP Concatenated Segment on Domain Z (PSNXZ LPSTME).

It is worth noticing that LPSTMEs can coexist with the LME monitoring the end-to-end LSP and that LPSTME MEPs and LME MEPs can be coincident in the same node (e.g. PE1 node supports both the PSN1Z LME MEP and the PSN13 LPSTME MEP).

4.4. MPLS-TP PW Monitoring (PME)

An MPLS-TP PW ME (PME) is an MPLS-TP maintenance entity intended to monitor a SS-PW or MS-PW between a pair of T-PEs. A PME MAY be configured on any SS-PW or MS-PW. PME OAM packets must fate share with the user data packets sent over the monitored PW.

A PME is intended to be deployed in scenarios where it is desirable to monitor an entire PW between a pair of MPLS-TP enabled T-PEs rather than monitoring the LSP aggregating multiple PWs between PEs.

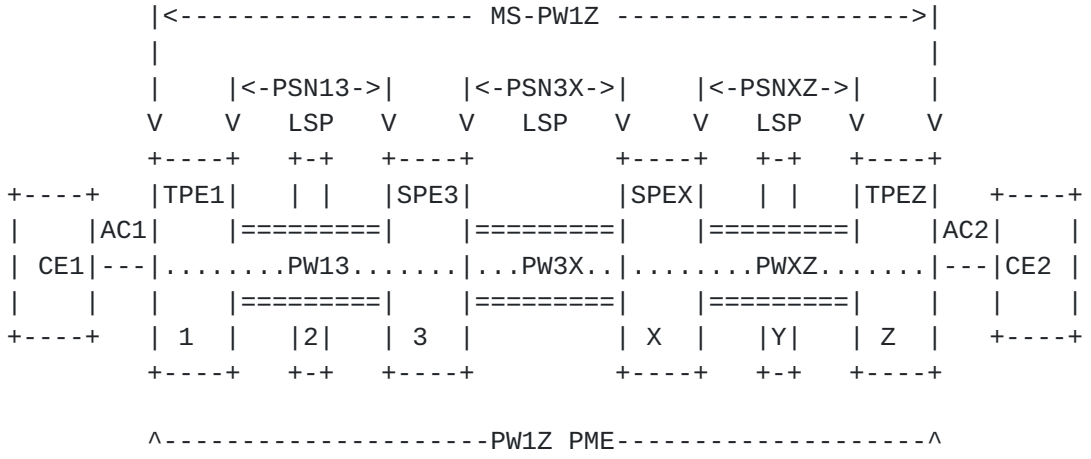


Figure 5 MPLS-TP PW ME (PME)

Figure 5 depicts a MS-PW (MS-PW1Z) consisting of three segments: PW13, PW3X and PWXZ and its associated end-to-end PME (PW1Z PME).

4.5. MPLS-TP MS-PW Path Segment Tunnel Monitoring (PPSTME)

An MPLS-TP MS-PW Path Segment Tunnel Monitoring ME (PPSTME) is an MPLS-TP maintenance entity intended to monitor an arbitrary part of an MS-PW between a given pair of PEs independently from the end-to-end monitoring (PME). A PPSTME can monitor a PW segment or concatenated segment and it may also include the forwarding engine(s) of the node(s) at the edge(s) of the segment or concatenated segment.

Multiple PPSTMEs MAY be configured on any MS-PW. The PEs may or may not be immediately adjacent at the MS-PW layer. PPSTME OAM packets fate share with the user data packets sent over the monitored PW Segment.

A PPSTME can be defined between the following entities:

o T-PE and any S-PE of a given MS-PW

o Any two S-PEs of a given MS-PW. It can span several PW segments.

A PPSTME is intended to be deployed in scenarios where it is preferable to monitor the behaviour of a part of a MS-PW rather than the entire end-to-end PW itself, for example to monitor an MS-PW Segment within a given network domain of an inter-domain MS-PW.

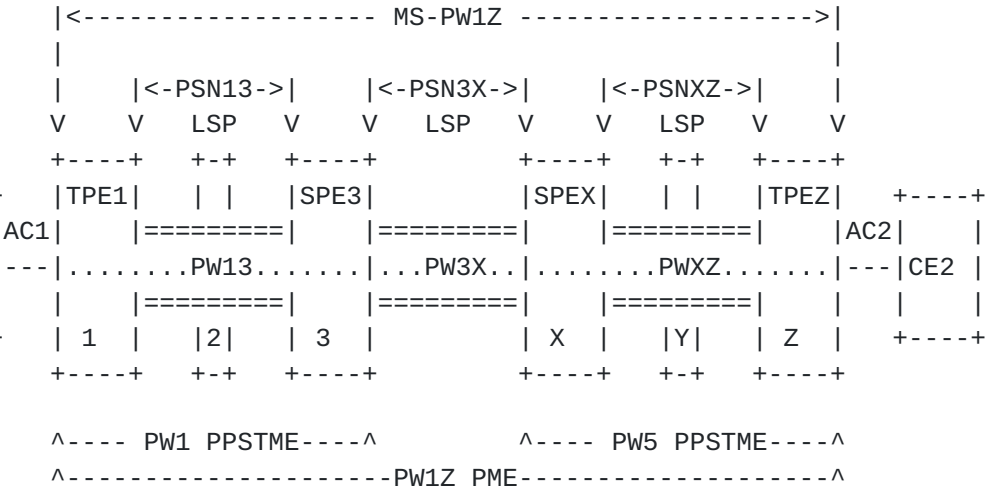


Figure 6 MPLS-TP MS-PW Path Segment Tunnel Monitoring (PPSTME)

Figure 6 depicts the same MS-PW (MS-PW1Z) between AC1 and AC2 as in Figure 5. In this scenario there are two separate PPSTMEs configured to monitor MS-PW1Z: 1) a PPSTME monitoring the PW13 MS-PW Segment on Domain 1 (PW13 PPSTME), and 2) a PPSTME monitoring the PWXZ MS-PW Segment on Domain Z with (PWXZ PPSTME).

It is worth noticing that PPSTMEs can coexist with the PME monitoring the end-to-end MS-PW and that PPSTME MEPs and PME MEPs can be coincident in the same node (e.g. TPE1 node supports both the PW1Z PME MEP and the PW13 PPSTME MEP).

5. OAM Functions for proactive monitoring

In this document, proactive monitoring refers to OAM operations that are either configured to be carried out periodically and continuously or preconfigured to act on certain events such as alarm signals.

Proactive monitoring is frequently "in service" monitoring. The control and measurement implications are:

1. Proactive monitoring for a MEG is typically configured at transport path creation time.

2. The operational characteristics of in-band measurement transactions (e.g., CV, LM etc.) are configured at the MEPs.

3. Server layer events are reported by transactions originating at intermediate nodes.

4. The measurements resulting from proactive monitoring are typically only reported outside of the MEG as unsolicited notifications for "out of profile" events, such as faults or loss measurement indication of excessive impairment of information transfer capability.

5. The measurements resulting from proactive monitoring may be periodically harvested by an EMS/NMS.

5.1. Continuity Check and Connectivity Verification

Proactive Continuity Check functions, as required in section 2.2.2 of [12], are used to detect a loss of continuity defect (LOC) between two MEPs in an MEG.

Proactive Connectivity Verification functions, as required in section 2.2.3 of [12], are used to detect an unexpected connectivity defect between two MEGs (e.g. mismerging or misconnection), as well as unexpected connectivity within the MEG with an unexpected MEP.

Both functions are based on the (proactive) generation of OAM packets by the source MEP that are processed by the sink MEP. As a consequence these two functions are grouped together into Continuity Check and Connectivity Verification (CC-V) OAM packets.

In order to perform pro-active Connectivity Verification function, each CC-V OAM packet MUST also include a globally unique Source MEP identifier. When used to perform only pro-active Continuity Check function, the CC-V OAM packet MAY not include any globally unique Source MEP identifier. Different formats of MEP identifiers are defined in [10] to address different environments. When MPLS-TP is deployed in transport network environments where IP addressing is not used in the forwarding plane, the ICC-based format for MEP identification is used. When MPLS-TP is deployed in IP-based environment, the IP-based MEP identification is used.

As a consequence, it is not possible to detect misconnections between two MEGs monitored only for continuity as neither the OAM message type nor OAM message content provides sufficient information to disambiguate an invalid source. To expand:

- For CC leaking into a CC monitored MEG - undetectable

- For CV leaking into a CC monitored MEG - presence of additional Source MEP identifier allows detecting the fault

- For CC leaking into a CV monitored MEG - lack of additional Source MEP identifier allows detecting the fault.

- For CV leaking into a CV monitored MEG - different Source MEP identifier permits fault to be identified.

CC-V OAM packets MUST be transmitted at a regular, operator's configurable, rate. The default CC-V transmission periods are application dependent (see section 5.1.3).

Proactive CC-V OAM packets are transmitted with the "minimum loss probability PHB" within a single network operator. This PHB is configurable on network operator's basis. PHBs can be translated at the network borders by the same function that translates it for user data traffic. The implication is that CC-V fate shares with much of the forwarding implementation, but not all aspects of PHB processing are exercised. On demand tools are used for finer grained fault finding.

In a bidirectional point-to-point transport path, when a MEP is enabled to generate pro-active CC-V OAM packets with a configured transmission rate, it also expects to receive pro-active CC-V OAM packets from its peer MEP at the same transmission rate as a common SLA applies to all components of the transport path. In a unidirectional transport path (either point-to-point or point-to-multipoint), only the source MEP is enabled to generate CC-V OAM packets and only the sink MEP is configured to expect these packets at the configured rate.

MIPs, as well as intermediate nodes not supporting MPLS-TP OAM, are transparent to the pro-active CC-V information and forward these pro-active CC-V OAM packets as regular data packets.

It is desirable to not generate spurious alarms during initialization or tear down; hence the following procedures are recommended. At initialization, the MEP source function (generating pro-active CC-V packets) should be enabled prior to the corresponding MEP sink function (detecting continuity and connectivity defects). When disabling the CC-V proactive functionality, the MEP sink function should be disabled prior to the corresponding MEP source function.

5.1.1. Defects identified by CC-V

Pro-active CC-V functions allow a sink MEP to detect the defect conditions described in the following sub-sections. For all of the described defect cases, the sink MEP SHOULD notify the equipment fault management process of the detected defect.

5.1.1.1. Loss Of Continuity defect

When proactive CC-V is enabled, a sink MEP detects a loss of continuity (LOC) defect when it fails to receive pro-active CC-V OAM packets from the peer MEP.

- Entry criteria: if no pro-active CC-V OAM packets from the peer MEP (i.e. with the correct globally unique Source MEP identifier) are received within the interval equal to 3.5 times the receiving MEP's configured CC-V reception period.

- Exit criteria: a pro-active CC-V OAM packet from the peer MEP (i.e. with the correct globally unique Source MEP identifier) is received.

5.1.1.2. Mis-connectivity defect

When a pro-active CC-V OAM packet is received, a sink MEP identifies a mis-connectivity defect (e.g. mismerge, misconnection or unintended looping) with its peer source MEP when the received packet carries an incorrect globally unique Source MEP identifier.

- Entry criteria: the sink MEP receives a pro-active CC-V OAM packet with an incorrect globally unique Source MEP identifier.

- Exit criteria: the sink MEP does not receive any pro-active CC-V OAM packet with an incorrect globally unique Source MEP identifier for an interval equal at least to 3.5 times the longest transmission period of the pro-active CC-V OAM packets received with an incorrect globally unique Source MEP identifier since this defect has been raised. This requires the OAM message to self identify the CC-V periodicity as not all MEPs can be expected to have knowledge of all MEGs.

5.1.1.3. Period Misconfiguration defect

If pro-active CC-V OAM packets are received with a correct globally unique Source MEP identifier but with a transmission period different than the locally configured reception period, then a CV period mis-configuration defect is detected.

- o Entry criteria: a MEP receives a CC-V pro-active packet with correct globally unique Source MEP identifier but with a Period field value different than its own CC-V configured transmission period.

- o Exit criteria: the sink MEP does not receive any pro-active CC-V OAM packet with a correct globally unique Source MEP identifier and an incorrect transmission period for an interval equal at least to 3.5 times the longest transmission period of the pro-active CC-V OAM packets received with a correct globally unique Source MEP identifier and an incorrect transmission period since this defect has been raised.

5.1.2. Consequent action

A sink MEP that detects one of the defect conditions defined in section 5.1.1 MUST perform the following consequent actions.

If a MEP detects an unexpected globally unique Source MEP Identifier, it MUST block all the traffic (including also the user data packets) that it receives from the misconnected transport path.

If a MEP detects LOC defect that is not caused by a period mis-configuration, it SHOULD block all the traffic (including also the user data packets) that it receives from the transport path, if this consequent action has been enabled by the operator.

It is worth noticing that the OAM requirements document [12] recommends that CC-V proactive monitoring is enabled on every MEG in order to reliably detect connectivity defects. However, CC-V proactive monitoring MAY be disabled by an operator on an MEG. In the event of a misconnection between a transport path that is pro-actively monitored for CC-V and a transport path which is not, the MEP of the former transport path will detect a LOC defect representing a connectivity problem (e.g. a misconnection with a transport path where CC-V proactive monitoring is not enabled) instead of a continuity problem, with a consequent wrong traffic delivering. For these reasons, the traffic block consequent action is applied even when a LOC condition occurs. This block consequent action MAY be disabled through configuration. This deactivation of the block action may be used for activating or deactivating the monitoring when it is not possible to synchronize the function activation of the two peer MEPs.

If a MEP detects a LOC defect (section 5.1.1.1), a mis-connectivity defect (section 5.1.1.2) or a period misconfiguration defect (section

5.1.1.3), it MUST declare a signal fail condition at the transport path level.

5.1.3. Configuration considerations

At all MEPs inside a MEG, the following configuration information needs to be configured when a proactive CC-V function is enabled:

- o MEG ID; the MEG identifier to which the MEP belongs;
- o MEP-ID; the MEP's own identity inside the MEG;
- o list of peer MEPs inside the MEG. For a point-to-point MEG the list would consist of the single peer MEP ID from which the OAM packets are expected. In case of the root MEP of a p2mp MEG, the list is composed by all the leaf MEP IDs inside the MEG. In case of the leaf MEP of a p2mp MEG, the list is composed by the root MEP ID (i.e. each leaf MUST know the root MEP ID from which it expect to receive the CC-V OAM packets).
- o PHB; it identifies the per-hop behaviour of CC-V packet. Proactive CC-V packets are transmitted with the "minimum loss probability PHB" previously configured within a single network operator. This PHB is configurable on network operator's basis. PHBs can be translated at the network borders.
- o transmission rate; the default CC-V transmission periods are application dependent (depending on whether they are used to support fault management, performance monitoring, or protection switching applications):
    - o Fault Management: default transmission period is 1s (i.e. transmission rate of 1 packet/second).
    - o Performance Monitoring: default transmission period is 100ms (i.e. transmission rate of 10 packets/second). Performance monitoring is only relevant when the transport path is defect free. CC-V contributes to the accuracy of PM statistics by permitting the defect free periods to be properly distinguished.
    - o Protection Switching: default transmission period is 3.33ms (i.e. transmission rate of 300 packets/second), in order to achieve sub-50ms the CC-V defect entry criteria should resolve in less than 10msec, and complete a protection switch within a subsequent period of 50 msec.

It SHOULD be possible for the operator to configure these transmission rates for all applications, to satisfy his internal requirements.

Note that the reception period is the same as the configured transmission rate.

For statically provisioned transport paths the above information are statically configured; for dynamically established transport paths the configuration information are signaled via the control plane.

The operator SHOULD be able to enable/disable some of the consequent actions defined in section 5.1.2.

5.2. Remote Defect Indication

The Remote Defect Indication (RDI) function, as required in section 2.2.9 of [12], is an indicator that is transmitted by a MEP to communicate to its peer MEPs that a signal fail condition exists. RDI is only used for bidirectional connections and is associated with proactive CC-V activation. The RDI indicator is piggy-backed onto the CC-V packet.

When a MEP detects a signal fail condition (e.g. in case of a continuity or connectivity defect), it should begin transmitting an RDI indicator to its peer MEP. The RDI information will be included in all pro-active CC-V packets that it generates for the duration of the signal fail condition's existence.

A MEP that receives the packets with the RDI information should determine that its peer MEP has encountered a defect condition associated with a signal fail.

MIPs as well as intermediate nodes not supporting MPLS-TP OAM are transparent to the RDI indicator and forward these proactive CC-V packets that include the RDI indicator as regular data packets, i.e. the MIP should not perform any actions nor examine the indicator.

When the signal fail defect condition clears, the MEP should clear the RDI indicator from subsequent transmission of pro-active CC-V packets. A MEP should clear the RDI defect upon reception of a pro-active CC-V packet from the source MEP with the RDI indicator cleared.

5.2.1. Configuration considerations

In order to support RDI indication, this may be a unique OAM message or an OAM information element embedded in a CV message. In this case the RDI transmission rate and PHB of the OAM packets carrying RDI should be the same as that configured for CC-V.

5.3. Alarm Reporting

The Alarm Reporting function, as required in section 2.2.8 of [12], relies upon an Alarm Indication Signal (AIS) message used to suppress alarms following detection of defect conditions at the server (sub-)layer.

- o A server MEP that detects a signal fail conditions in the server (sub-)layer, will notify the MPLS-TP client (sub-)layer adaptation function, which can generate packets with AIS information in a direction opposite to its peers MEPs to allow the suppression of secondary alarms at the MEP in the client (sub-)layer.

A server MEP is responsible for notifying the MPLS-TP layer network adaptation function upon fault detection in the server layer network to which the server MEP is associated.

Only the client layer adaptation function at an intermediate node will issue MPLS-TP packets with AIS information. Upon receiving notification of a signal fail condition the adaptation function SHOULD immediately start transmitting periodic packets with AIS information. These periodic packets, with AIS information, continue to be transmitted until the signal fail condition is cleared.

Upon receiving a packet with AIS information an MPLS-TP MEP enters an AIS defect condition and suppresses loss of continuity alarms associated with its peer MEP. A MEP resumes loss of continuity alarm generation upon detecting loss of continuity defect conditions in the absence of AIS condition.

For example, let's consider a fiber cut between LSR 1 and LSR 2 in the reference network of Figure 3. Assuming that all the MEGs described in Figure 3 have pro-active CC-V enabled, a LOC defect is detected by the MEPs of Sec12 SME, PSN13 LME, PW1 PPSTME and PW1Z PME, however in transport network only the alarm associate to the fiber cut needs to be reported to NMS while all these secondary alarms should be suppressed (i.e. not reported to the NMS or reported as secondary alarms).

If the fiber cut is detected by the MEP in the physical layer (in LSR2), LSR2 can generate the proper alarm in the physical layer and suppress the secondary alarm associated with the LOC defect detected on Sec12 SME. As both MEPs reside within the same node, this process does not involve any external protocol exchange. Otherwise, if the physical layer has not enough OAM capabilities to detect the fiber cut, the MEP of Sec12 SME in LSR2 will report a LOC alarm.

In both cases, the MEP of Sec12 SME in LSR 2 notifies the adaptation function for PSN13 LME that then generates AIS packets on the PSN13 LME in order to allow its MEP in LSR3 to suppress the LOC alarm. LSR3 can also suppress the secondary alarm on PW13 PPSTME because the MEP of PW13 PPSTME resides within the same node as the MEP of PSN13 LME. The MEP of PW13 PPSTME in LSR3 also notifies the adaptation function for PW1Z PME that then generates AIS packets on PW1Z PME in order to allow its MEP in LSRZ to suppress the LOC alarm.

The generation of AIS packets for each MEG in the client (sub-)layer is configurable (i.e. the operator can enable/disable the AIS generation).

AIS packets are transmitted with the "minimum loss probability PHB" within a single network operator. This PHB is configurable on network operator's basis.

A MIP is transparent to packets with AIS information and therefore does not require any information to support AIS functionality.

5.4. Lock Reporting

The Lock Reporting function, as required in section 2.2.7 of [12], relies upon a Locked Report (LKR) message used to suppress alarms following administrative locking action in the server (sub-)layer.

A server MEP is responsible for notifying the MPLS-TP layer network adaption function upon locked condition applied to the server layer network to which the server MEP is associated.

Only the client layer adaptation function at an intermediate node will issue MPLS-TP packets with LKR information. Upon receiving notification of a locked condition the adaptation function SHOULD immediately start transmitting periodic packets with LKR information. These periodic packets, with LKR information, will continue to be transmitted until the locked condition is cleared.

Upon receiving a packet with LKR information an MPLS-TP MEP enters an LKR defect condition and suppresses loss of continuity alarm associated with its peer MEP. A MEP resumes loss of continuity alarm generation upon detecting loss of continuity defect conditions in the absence of LKR condition.

The generation of LKR packets is configurable in the server (sub-)layer (i.e. the operator can enable/disable the LKR generation).

LKR packets are transmitted with the "minimum loss probability PHB" within a single network operator. This PHB is configurable on network operator's basis.

A MIP is transparent to packets with LKR information and therefore does not require any information to support LKR functionality.

5.5. Packet Loss Measurement

Packet Loss Measurement (LM) is one of the capabilities supported by the MPLS-TP Performance Monitoring (PM) function in order to facilitate reporting of QoS information for a transport path as required in section 2.2.11 of [12]. LM is used to exchange counter values for the number of ingress and egress packets transmitted and received by the transport path monitored by a pair of MEPs.

Proactive LM is performed by periodically sending LM OAM packets from a MEP to a peer MEP and by receiving LM OAM packets from the peer MEP (if a bidirectional transport path) during the life time of the transport path. Each MEP performs measurements of its transmitted and received packets. These measurements are then transactionally correlated with the peer MEP in the ME to derive the impact of packet loss on a number of performance metrics for the ME in the MEG. The LM transactions are issued such that the OAM packets will experience the same queuing discipline as the measured traffic while transiting between the MEPs in the ME.

For a MEP, near-end packet loss refers to packet loss associated with incoming data packets (from the far-end MEP) while far-end packet

loss refers to packet loss associated with egress data packets (towards the far-end MEP).

5.5.1. Configuration considerations

In order to support proactive LM, the transmission rate and PHB associated with the LM OAM packets originating from a MEP need be configured as part of the LM provisioning procedures. LM OAM packets should be transmitted with the same PHB class that the LM is intended to measure. If that PHB is not an ordered aggregate where the ordering constraint is all packets with the PHB being delivered in order, LM can produce inconsistent results.

5.6. Client Failure Indication

The Client Failure Indication (CSF) function, as required in section 2.2.10 of [12], is used to help process client defects and propagate a client signal defect condition from the process associated with the local attachment circuit where the defect was detected (typically the source adaptation function for the local client interface) to the process associated with the far-end attachment circuit (typically the source adaptation function for the far-end client interface) for the same transmission path in case the client of the transport path does not support a native defect/alarm indication mechanism, e.g. AIS.

A source MEP starts transmitting a CSF indication to its peer MEP when it receives a local client signal defect notification via its local CSF function. Mechanisms to detect local client signal fail defects are technology specific.

A sink MEP that has received a CSF indication report this condition to its associated client process via its local CSF function. Consequent actions toward the client attachment circuit are technology specific.

Either there needs to be a 1:1 correspondence between the client and the MEG, or when multiple clients are multiplexed over a transport path, the CSF message requires additional information to permit the client instance to be identified.

5.6.1. Configuration considerations

In order to support CSF indication, the CSF transmission rate and PHB of the CSF OAM message/information element should be configured as part of the CSF configuration.

5.7. Packet Delay Measurement

Packet Delay Measurement (DM) is one of the capabilities supported by the MPLS-TP PM function in order to facilitate reporting of QoS information for a transport path as required in section 2.2.12 of [12]. Specifically, pro-active DM is used to measure the long-term packet delay and packet delay variation in the transport path monitored by a pair of MEPs.

Proactive DM is performed by sending periodic DM OAM packets from a MEP to a peer MEP and by receiving DM OAM packets from the peer MEP (if a bidirectional transport path) during a configurable time interval.

Pro-active DM can be operated in two ways:

- One-way: a MEP sends DM OAM packet to its peer MEP containing all the required information to facilitate one-way packet delay and/or one-way packet delay variation measurements at the peer MEP. Note that this requires synchronized precision time at either MEP by means outside the scope of this framework.

- Two-way: a MEP sends DM OAM packet with a DM request to its peer MEP, which replies with a DM OAM packet as a DM response. The request/response DM OAM packets containing all the required information to facilitate two-way packet delay and/or two-way packet delay variation measurements from the viewpoint of the source MEP.

5.7.1. Configuration considerations

In order to support pro-active DM, the transmission rate and PHB associated with the DM OAM packets originating from a MEP need be configured as part of the DM provisioning procedures. DM OAM packets should be transmitted with the PHB that yields the lowest packet loss performance among the PHB Scheduling Classes or Ordered Aggregates (see RFC 3260 [15]) in the monitored transport path for the relevant network domain(s).

6. OAM Functions for on-demand monitoring

In contrast to proactive monitoring, on-demand monitoring is initiated manually and for a limited amount of time, usually for operations such as e.g. diagnostics to investigate into a defect condition.

On-demand monitoring covers a combination of "in service" and "out-of service" monitoring functions. The control and measurement implications are:

1. A MEG can be directed to perform an "on demand" functions at arbitrary times in the lifetime of a transport path.

2. "out of service" monitoring functions may require a-priori configuration of both MEPs and intermediate nodes in the MEG (e.g., data plane loopback) and the issuance of notifications into client layers of the transport path being removed from service (e.g., lock-reporting)

3. The measurements resulting from on-demand monitoring are typically harvested in real time, as these are frequently craftsperson initiated and attended. These do not necessarily require different harvesting mechanisms that that for harvesting proactive monitoring telemetry.

6.1. Connectivity Verification

In order to preserve network resources, e.g. bandwidth, processing time at switches, it may be preferable to not use proactive CC-V. In order to perform fault management functions, network management may invoke periodic on-demand bursts of on-demand CV packets, as required in section 2.2.3 of [12].

Use of on-demand CV is dependent on the existence of either a bi-directional MEG, or the availability of an out of band return path because it requires the ability for target MIPs and MEPs to direct responses to the originating MEPs.

An additional use of on-demand CV would be to detect and locate a problem of connectivity when a problem is suspected or known based on other tools. In this case the functionality will be triggered by the network management in response to a status signal or alarm indication.

On-demand CV is based upon generation of on-demand CV packets that should uniquely identify the MEG that is being checked. The on-demand functionality may be used to check either an entire MEG (end-to-end) or between a MEP to a specific MIP. This functionality may not be available for associated bidirectional transport paths, as the MIP may not have a return path to the source MEP for the on-demand CV transaction.

On-demand CV may generate a one-time burst of on-demand CV packets, or be used to invoke periodic, non-continuous, bursts of on-demand CV packets. The number of packets generated in each burst is configurable at the MEPs, and should take into account normal packet-loss conditions.

When invoking a periodic check of the MEG, the source MEP should issue a burst of on-demand CV packets that uniquely identifies the MEG being verified. The number of packets and their transmission rate should be pre-configured and known to both the source MEP and the target MEP or MIP. The source MEP should use the mechanisms defined in sections 3.3 and 3.4 when sending an on-demand CV packet to a target MEP or target MIP respectively. The target MEP/MIP shall return a reply on-demand CV packet for each packet received. If the expected number of on-demand CV reply packets is not received at source MEP, the LOC defect state is entered.

On demand CV should have the ability to carry padding such that a variety of MTU sizes can be originated to verify the MTU capacity of the transport path.

6.1.1. Configuration considerations

For on-demand CV the MEP should support the configuration of the number of packets to be transmitted/received in each burst of transmissions and their packet size. The transmission rate should be configured between the different nodes.

In addition, when the CV packet is used to check connectivity toward a target MIP, the number of hops to reach the target MIP should be configured.

The PHB of the on-demand CV packets should be configured as well. This permits the verification of correct operation of QoS queuing as well as connectivity.

6.2. Packet Loss Measurement

On-demand Packet Loss Measurement (LM) is one of the capabilities supported by the MPLS-TP Performance Monitoring function in order to facilitate diagnostic of QoS performance for a transport path, as required in section 2.2.11 of [12]. As proactive LM, on-demand LM is used to exchange counter values for the number of ingress and egress packets transmitted and received by the transport path monitored by a pair of MEPs.

On-demand LM is performed by periodically sending LM OAM packets from a MEP to a peer MEP and by receiving LM OAM packets from the peer MEP (if a bidirectional transport path) during a pre-defined monitoring period. Each MEP performs measurements of its transmitted and received packets. These measurements are then correlated evaluate the packet loss performance metrics of the transport path.

6.2.1. Configuration considerations

In order to support on-demand LM, the beginning and duration of the LM procedures, the transmission rate and PHB associated with the LM OAM packets originating from a MEP must be configured as part of the on-demand LM provisioning procedures. LM OAM packets should be transmitted with the PHB that yields the lowest packet loss performance among the PHB Scheduling Classes or Ordered Aggregates (see RFC 3260 [15]) in the monitored transport path for the relevant network domain(s).

6.3. Diagnostic Tests

6.3.1. Throughput Estimation

Throughput estimation is an on-demand out-of-service function, as required in section 2.2.5 of [12], that allows verifying the bandwidth/throughput of an MPLS-TP transport path (LSP or PW) before it is put in-service.

Throughput estimation is performed between MEPs and can be performed in one-way or two way modes.

This test is performed by sending OAM test packets at increasing rate (up to the theoretical maximum), graphing the percentage of OAM test packets received and reporting the rate at which OAM test packets start begin dropped. In general, this rate is dependent on the OAM test packet size.

When configured to perform such tests, a MEP source inserts OAM test packets with test information with specified throughput, packet size and transmission patterns.

For one way test, remote MEP sink receives the OAM test packets and calculates the packet loss. For two way test, the remote MEP loopbacks the OAM test packets back to original MEP and the local MEP sink calculates the packet loss.

6.3.1.1. Configuration considerations

Throughput estimation is an out-of-service tool. The diagnosed MEG should be put into a Lock status before the diagnostic test is started.

An MEG can be put into a Lock status either via NMS action or using the Lock Instruct OAM tool as defined in section 6.6.

At the transmitting MEP, provisioning is required for a test signal generator, which is associated with the MEP. At a receiving MEP, provisioning is required for a test signal detector which is associated with the MEP.

A MIP is transparent to the OAM test packets sent for throught estimation and therefore does not require any provisioning to support MPLS-TP throghtput estimation.

6.3.2. Data plane Loopback

Data plane loopback is an out-of-service function, as required in section 2.2.5 of [12], that permits traffic originated at the ingress of a transport path to be looped back to the point of origin by an interface at either an intermediate node or a terminating node.

If the loopback function is to be performed at an intermediate node it is only applicable to co-routed bi-directional paths. If the loopback is to be performed end to end, it is applicable to both co-routed bi-directional or associated bi-directional paths.

Where a node implements data plane loopback capability and whether it implements more than one point is implementation dependent.

6.4. Route Tracing

It is often necessary to trace a route covered by an MEG from a source MEP to the sink MEP including all the MIPs in-between after e.g., provisioning an MPLS-TP transport path or for trouble shooting purposes, it.

The route tracing function, as required in section 2.2.4 of [12], is providing this functionality. Based on the fate sharing requirement of OAM flows, i.e. OAM packets receive the same forwarding treatment as data packet, route tracing is a basic means to perform connectivity verification and, to a much lesser degree, continuity check. For this function to work properly, a return path must be present.

Route tracing might be implemented in different ways and this document does not preclude any of them.

Route tracing should always discover the full list of MIPs and of the peer MEPs. In case a defect exist, the route trace function needs to be able to detect it and stop automatically returning the incomplete list of OAM entities that it was able to trace.

6.4.1. Configuration considerations

The configuration of the route trace function must at least support the setting of the number of trace attempts before it gives up.

6.5. Packet Delay Measurement

Packet Delay Measurement (DM) is one of the capabilities supported by the MPLS-TP PM function in order to facilitate reporting of QoS information for a transport path, as required in section 2.2.12 of [12]. Specifically, on-demand DM is used to measure packet delay and packet delay variation in the transport path monitored by a pair of MEPs during a pre-defined monitoring period.

On-Demand DM is performed by sending periodic DM OAM packets from a MEP to a peer MEP and by receiving DM OAM packets from the peer MEP (if a bidirectional transport path) during a configurable time interval.

On-demand DM can be operated in two ways:

- One-way: a MEP sends DM OAM packet to its peer MEP containing all the required information to facilitate one-way packet delay and/or one-way packet delay variation measurements at the peer MEP.

- Two-way: a MEP sends DM OAM packet with a DM request to its peer MEP, which replies with an DM OAM packet as a DM response. The request/response DM OAM packets containing all the required information to facilitate two-way packet delay and/or two-way packet delay variation measurements from the viewpoint of the source MEP.

6.5.1. Configuration considerations

In order to support on-demand DM, the beginning and duration of the DM procedures, the transmission rate and PHB associated with the DM OAM packets originating from a MEP need be configured as part of the LM provisioning procedures. DM OAM packets should be transmitted with the PHB that yields the lowest packet delay performance among the PHB

Scheduling Classes or Ordering Aggregates (see RFC 3260 [15]) in the monitored transport path for the relevant network domain(s).

In order to verify different performances between long and short packets (e.g., due to the processing time), it SHOULD be possible for the operator to configure of the on-demand OAM DM packet.

6.6. Lock Instruct

Lock Instruct (LKI) function, as required in section 2.2.6 of [12], is a command allowing a MEP to instruct the peer MEP(s) to put the MPLS-TP transport path into a locked condition.

This function allows single-side provisioning for administratively locking (and unlocking) an MPLS-TP transport path.

Note that it is also possible to administratively lock (and unlock) an MPLS-TP transport path using two-side provisioning, where the NMS administratively put both MEPs into ad administrative lock condition. In this case, the LKI function is not required/used.

6.6.1. Locking a transport path

A MEP, upon receiving a single-side administrative lock command from NMS, sends an LKI request OAM packet to its peer MEP(s). It also puts the MPLS-TP transport path into a locked and notify its client (sub-)layer adaptation function upon the locked condition.

A MEP, upon receiving an LKI request from its peer MEP, can accept or not the instruction and MUST reply to the peer MEP with an LKI reply OAM packet indicating whether it has accepted or not the instruction.

If the lock instruction has been accepted, it also puts the MPLS-TP transport path into a locked and notify its client (sub-)layer adaptation function upon the locked condition.

Note that if the client (sub-)layer is also MPLS-TP, Lock Reporting (LKR) generation at the client MPLS-TP (sub-)layer is started, as described in section 5.4.

6.6.2. Unlocking a transport path

A MEP, upon receiving a single-side administrative unlock command from NMS, sends an LKI removal request OAM packet to its peer MEP(s).

The peer MEP, upon receiving an LKI removal request, can accept or not the removal instruction and MUST reply with an LKI removal reply OAM packet indicating whether it has accepted or not the instruction.

If the lock removal instruction has been accepted, it also clears the locked condition on the MPLS-TP transport path and notify this event to its client (sub-)layer adaptation function.

The MEP that has initiated the LKI clear procedure, upon receiving a positive LKI removal reply, also clears the locked condition on the MPLS-TP transport path and notify this event to its client (sub-)layer adaptation function.

Note that if the client (sub-)layer is also MPLS-TP, Lock Reporting (LKR) generation at the client MPLS-TP (sub-)layer is terminated, as described in section 5.4.

7. Security Considerations

A number of security considerations are important in the context of OAM applications.

OAM traffic can reveal sensitive information such as passwords, performance data and details about e.g. the network topology. The nature of OAM data therefore suggests to have some form of authentication, authorization and encryption in place. This will prevent unauthorized access to vital equipment and it will prevent third parties from learning about sensitive information about the transport network.

Mechanisms that the framework does not specify might be subject to additional security considerations.

8. IANA Considerations

No new IANA considerations.

9. Acknowledgments

The authors would like to thank all members of the teams (the Joint Working Team, the MPLS Interoperability Design Team in IETF and the T-MPLS Ad Hoc Group in ITU-T) involved in the definition and specification of MPLS Transport Profile.

The editors gratefully acknowledge the contributions of Adrian Farrel, Yoshinori Koike and Luca Martini for per-interface MIPs and MEPs description.

The editors gratefully acknowledge the contributions of Malcolm Betts, Yoshinori Koike, Xiao Min, and Maarten Vissers for the lock report and lock instruction description.

The authors would also like to thank Malcolm Betts, Stewart Bryant, Rui Costa, Adrian Farrel, Liu Gouman, Feng Huang, Yoshionori Koike, Yuji Tochio, Maarten Vissers and Xuequin Wei for their comments and enhancements to the text.

This document was prepared using 2-Word-v2.0.template.dot.

10. References

10.1. 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., Callon, R., "Multiprotocol Label Switching Architecture", RFC 3031, January 2001

[3] Rosen, E., et al., "MPLS Label Stack Encoding", RFC 3032, January 2001

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

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

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

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

[8] Bocci, M., et al., "A Framework for MPLS in Transport Networks", draft-ietf-mpls-tp-framework-10 (work in progress), February 2010

[9] Vigoureux, M., Bocci, M., Swallow, G., Ward, D., Aggarwal, R., "MPLS Generic Associated Channel", RFC 5586, June 2009

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

10.2. Informative References

[11] Niven-Jenkins, B., Brungard, D., Betts, M., sprecher, N., Ueno, S., "MPLS-TP Requirements", RFC 5654, September 2009

[12] Vigoureux, M., Betts, M., Ward, D., "Requirements for OAM in MPLS Transport Networks", draft-ietf-mpls-tp-oam-requirements-06 (work in progress), March 2010

[13] Sprecher, N., Nadeau, T., van Helvoort, H., Weingarten, Y., "MPLS-TP OAM Analysis", draft-ietf-mpls-tp-oam-analysis-01 (work in progress), March 2010

[14] Nichols, K., Blake, S., Baker, F., Black, D., "Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers", RFC 2474, December 1998

[15] Grossman, D., "New terminology and clarifications for Diffserv", RFC 3260, April 2002.

[16] ITU-T Recommendation G.707/Y.1322 (01/07), "Network node interface for the synchronous digital hierarchy (SDH)", January 2007

[17] ITU-T Recommendation G.805 (03/00), "Generic functional architecture of transport networks", March 2000

[18] ITU-T Recommendation G.806 (01/09), "Characteristics of transport equipment - Description methodology and generic functionality ", January 2009

[19] ITU-T Recommendation G.826 (12/02), "End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections", December 2002

[20] ITU-T Recommendation G.7710 (07/07), "Common equipment management function requirements", July 2007

[21] ITU-T Recommendation Y.2611 (06/12), " High-level architecture of future packet-based networks", 2006

Authors' Addresses

Dave Allan (Editor)
Ericsson

Email: david.i.allan@ericsson.com

Italo Busi (Editor)
Alcatel-Lucent

Email: Italo.Busi@alcatel-lucent.com

Ben Niven-Jenkins (Editor)
BT

Email: benjamin.niven-jenkins@bt.com

Contributing Authors' Addresses

Annamaria Fulignoli
Ericsson

Email: annamaria.fulignoli@ericsson.com

Enrique Hernandez-Valencia
Alcatel-Lucent

Email: Enrique.Hernandez@alcatel-lucent.com

Lieven Levrau
Alcatel-Lucent

Email: Lieven.Levrau@alcatel-lucent.com

Dinesh Mohan
Nortel

Email: mohand@nortel.com

Vincenzo Sestito
Alcatel-Lucent

Email: Vincenzo.Sestito@alcatel-lucent.com

Nurit Sprecher
Nokia Siemens Networks

Email: nurit.sprecher@nsn.com

Huub van Helvoort
Huawei Technologies

Email: hhelvoort@huawei.com

Martin Vigoureux
Alcatel-Lucent

Email: Martin.Vigoureux@alcatel-lucent.com

Yaacov Weingarten
Nokia Siemens Networks

Email: yaacov.weingarten@nsn.com

Rolf Winter
NEC

Email: Rolf.Winter@nw.neclab.eu