
Question(s): 10/15

Geneva, 15-26 February 2016

TD**Source:** Editor G.8113.1/Y.1372.1**Title:** Draft revised Recommendation ITU-T G.8113.1/Y.1372.1 (for Consent, 26 February 2016)

This document provides draft revised G.8113.1/Y.1372.1 (edition 2) for consent based on:

- The output from the 2-6 March 2015 Q10/15 interim meeting;
- In force G.8113.1/Y.1372.1 (2012) Amd. 1 (08/2013);
- In force G.8113.1/Y.1372.1 (11/2012).

The diff-marks show the differences from G.8113.1/Y.1372.1 (11/2012) by incorporating the amendment 1 (08/2013) and the output from the 2-6 March 2015 Q10/15 interim meeting.

Contact:	Han Li China Mobile Communications P.R. China	Tel: +86-10-15801696688-33092 Fax: +86-10-63601087 Email: lihan@chinamobile.com
-----------------	---	--

Contact:	Jia He Huawei Technologies Co., Ltd. P.R.China	Tel: +86-755-28972597 Fax: +86-755-28979835 Email: hejia@huawei.com
-----------------	--	---

Attention: This is not a publication made available to the public, but an **internal ITU-T Document** intended only for use by the Member States of ITU, by ITU-T Sector Members and Associates, and their respective staff and collaborators in their ITU related work. It shall not be made available to, and used by, any other persons or entities without the prior written consent of ITU-T.

Draft revised Recommendation ITU-T G.8113.1/Y.1372.1

Operations, administration and maintenance mechanisms for MPLS-TP in packet transport networks

Summary

Recommendation ITU-T G.8113.1/Y.1372.1 specifies mechanisms for user-plane operations, administration and maintenance (OAM) in multi-protocol label switching transport profile (MPLS-TP) networks to meet the MPLS-TP OAM requirements defined in IETF RFC 5860. It also specifies the MPLS-TP OAM packet formats, syntax and semantics of MPLS-TP OAM packet fields.

The OAM mechanisms defined in this Recommendation assume common forwarding of the MPLS-TP user packets and MPLS-TP OAM packets. In transport networks, the OAM return path is always in-band.

The MPLS-TP OAM mechanisms described in this Recommendation apply to co-routed bidirectional point-to-point MPLS-TP connections. Unidirectional point-to-point and point-to-multipoint MPLS-TP connections will be addressed in a future version of this Recommendation.

This Recommendation is compliant with the transport profile of MPLS as defined by the IETF. In the event of a misalignment in MPLS-TP-related architecture, framework, and protocols between this ITU-T Recommendation and the normatively referenced IETF RFCs, the RFCs will take precedence.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T G.8113.1/Y.1372.1	2012-11-20	15	<u>11.1002/1000/11323</u>
<u>1.1</u>	<u>ITU-T G.8113.1/Y.1372.1 (2012) Amd. 1</u>	<u>2013-08-29</u>	<u>15</u>	<u>11.1002/1000/12032</u>
<u>2.1</u>	<u>ITU-T G.8113.1/Y.1372.1 (xx/2015)</u>	<u>TBD</u>	<u>15</u>	<u>TBD</u>

* To access the Recommendation, type the URL <http://handle.itu.int/> in the address field of your web browser, followed by the Recommendation's unique ID. For example, <http://handle.itu.int/11.1002/1000/11830-en>.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at <http://www.itu.int/ITU-T/ipr/>.

© ITU 2013

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

	Page
1 Scope.....	1
2 References.....	1
3 Definitions	2
3.1 Terms defined elsewhere.....	2
3.2 Terms defined in this Recommendation.....	2
4 Abbreviations and acronyms	3
5 Conventions	5
6 Functional components.....	5
6.1 Maintenance entity (ME).....	5
6.2 Maintenance entity group (MEG)	6
6.3 MEG end points (MEPs)	6
6.4 MEG intermediate points (MIPs)	8
6.5 Server MEP	10
7 OAM functions	10
7.1 Identification of OAM packets from user-traffic packets	10
7.2 OAM functions specification	11
8 OAM packet formats	15
8.1 Common OAM packets.....	15
8.2 OAM PDU formats based on [ITU-T G.8013]	16
8.3 Management communication channel (MCC)	24
8.4 Signalling communication channel (SCC)	24
9 MPLS-TP OAM procedures	24
9.1 MPLS-TP OAM procedures based on ITU-T G.8013 PDUs.....	24
Annex A – MPLS-TP OAM for a packet transport network (PTN) applicability statement..	33
Appendix I – MPLS-TP network scenarios	34
I.1 MEG nesting example	34
Bibliography.....	35

Draft revised Recommendation ITU-T G.8113.1/Y.1372.1

Operations, administration and maintenance mechanism for MPLS-TP in packet transport networks

1 Scope

This Recommendation specifies mechanisms for operations, administration and maintenance (OAM) for multi-protocol label switching transport profiles (MPLS-TPs) that can be applied in packet transport networks (PTN). It defines mechanisms for user-plane OAM in MPLS-TP networks to meet the MPLS-TP OAM requirements defined in [IETF RFC 5860]. It also specifies the MPLS-TP OAM packet formats, syntax and semantics of MPLS-TP OAM packet fields.

The OAM mechanisms defined in this Recommendation assume common forwarding of the MPLS-TP user packets and MPLS-TP OAM packets. In transport networks, the OAM return path is always in-band.

The MPLS-TP OAM mechanisms described in this Recommendation are applicable in network scenarios, as described in Annex A, and apply to co-routed bidirectional point-to-point MPLS-TP connections. Unidirectional point-to-point and point-to-multipoint MPLS-TP connections will be addressed in a future version of this Recommendation.

This Recommendation provides a representation of the MPLS-TP technology using the methodologies that have been used for other transport technologies (e.g., synchronous digital hierarchy (SDH), optical transport network (OTN) and Ethernet).¹

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

- [ITU-T G.805] Recommendation ITU-T G.805 (2000), *Generic functional architecture of transport networks*.
- [ITU-T G.806] Recommendation ITU-T G.806 (2004), *Characteristics of transport equipment – Description methodology and generic functionality*.
- [ITU-T G.826] Recommendation ITU-T G.826 (2002), *End-to-end error performance parameters and objectives for international, constant bit-rate digital paths and connections*.
- [ITU-T G.7710] Recommendation ITU-T G.7710/Y.1701 (2007), *Common equipment management function requirements*.
- [ITU-T G.7712] Recommendation ITU-T G.7712/Y.1703 (2010), *Architecture and specification of data communication network*.

¹ This ITU-T Recommendation is intended to be aligned with the IETF MPLS RFCs normatively referenced by this Recommendation.

- [ITU-T G.8010] Recommendation ITU-T G.8010/Y.1306 (2004), *Architecture of Ethernet layer networks*, plus Amendment 1 (2006).
- [ITU-T G.8013] Recommendation ITU-T G.8013/Y.1731 (2011), *OAM functions and mechanisms for Ethernet based networks*.
- [ITU-T G.8021] Recommendation ITU-T G.8021/Y.1341 (2010), *Characteristics of Ethernet transport network equipment functional blocks*.
- [ITU-T G.8110.1] Recommendation ITU-T G.8110.1/Y.1370.1 (2011), *Architecture of MPLS Transport Profile (MPLS-TP) layer network*.
- [ITU-T M.20] Recommendation ITU-T M.20 (1992), *Maintenance philosophy for telecommunication networks*.
- [ITU-T M.1400] Recommendation ITU-T M.1400 (2006), *Designations for interconnections among operators' networks*.
- [IETF RFC 3031] IETF RFC 3031 (2001), *Multiprotocol Label Switching Architecture*.
- [IETF RFC 3032] IETF RFC 3032 (2001), *MPLS Label Stack Encoding*.
- [IETF RFC 4385] IETF RFC4385 (2006), *Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN*.
- [IETF RFC 3443] IETF RFC 3443 (2003), *Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks*.
- [IETF RFC 5462] IETF RFC 5462 (2009), *Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field*.
- [IETF RFC 5586] IETF RFC 5586 (2009), *MPLS Generic Associated Channel*.
- [IETF RFC 5654] IETF RFC5654 (2009), *Requirements of an MPLS Transport Profile*.
- [IETF RFC 5718] IETF RFC5718 (2010), *An In-Band Data Communication Network For the MPLS Transport Profile*.
- [IETF RFC5860] IETF RFC5860 (2010), *Requirements for Operations, Administration, and Maintenance (OAM) in MPLS Transport Networks*.
- [IETF RFC 6371] IETF RFC6371 (2011), *Operations, Administration and Maintenance Framework for MPLS-Based Transport Networks*.
- [ISO 3166-1] ISO 3166-1:2013 alpha-2, Codes for the representation of names of countries and their subdivisions – Part 1: Country codes.

3 Definitions

This Recommendation introduces terminology that is required to discuss the functional network components associated with OAM. These definitions are consistent with ITU-T G.805 terminology.

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined in [ITU-T G.806]:

- **defect**
- **failure**

3.2 Terms defined in this Recommendation

This Recommendation defines the following term:

3.2.1 MPLS transport profile: A set of multi-protocol label switching (MPLS) functions used to support packet transport services and network operations.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

IDM	One-way Delay Measurement
A	Adaptation function
ACH	Associated Channel Header
AIS	Alarm Indication Signal
AP	Access Point
APS	Automatic Protection Switching
C	Customer
CC	Continuity Check
CCM	Continuity Check Message
C-DCI	Client - Defect Clear Indication
CFI	Client Failure Indication
CSF	Client Signal Fail
CV	Connectivity Verification
DCC	Data Communication Channel
DM	Delay Measurement
DMM	Delay Measurement Message
DMR	Delay Measurement Reply
DT	Diagnostic Test
ES	Experimental Specific
EXM	Experimental OAM Message
EXP	Experimental
EXR	Experimental OAM Reply
FC	Frame Count
G-ACh	Generic Associated Channel
GAL	G-ACh Label
IANA	Internet Assigned Numbers Authority
ICC	ITU-T Carrier Code
ID	Identifier
IETF	Internet Engineering Task Force

IF	Interface
IO	Intermediate Operator
IP	Intermediate Provider
LBM	Loopback Message
LBR	Loopback Reply
LCK	Locked Signal
LER	Label Edge Router
LM	Loss Measurement
LMM	Loss Measurement Message
LMR	Loss Measurement Reply
LOC	Loss Of Continuity
LSE	Label Stack Entry
LSP	Label Switched Path
LSR	Label Switch Router
MCC	Management Communication Channel
ME	Maintenance Entity
MEG	Maintenance Entity Group
MEL	MEG Level
MEP	MEG End Point
MIP	MEG Intermediate Point
MMG	Mismerge
MPLS	Multi-Protocol Label Switching
MPLS-TP	MPLS Transport Profile
N	Network
NE	Network Element
Num	Number
O	Operator
OAM	Operation, Administration and Maintenance
OpCode	Operations Code
OSS	Operations Support System
OTN	Optical Transport Network
P	Provider
PD	Packet Delay
PDU	Protocol Data Unit
PDV	Packet Delay Variation

PHB	Per-Hop Behaviour
PRBS	Pseudo-Random Bit Sequence
PSN	Packet Switched Network
PW	PseudoWire
PWE3	PseudoWire Emulation Edge-to-Edge
RDI	Remote Defect Indication
RFC	Requests for Comments
<u>RT</u>	<u>Route Tracing</u>
Rx	Receive
S	Stack
SCC	Signalling Communication Channel
SDH	Synchronous Digital Hierarchy
Sk	Sink
SLA	Service Level Agreement
So	Source
SPME	Sub-Path Maintenance Entity
SRV	Server
TC	Traffic Class
TCM	Tandem Connection Monitoring
TLV	Type, Length, and Value
TrCP	Traffic Conditioning Point
TSB	Telecommunication Standardization Bureau
TST	Test
TTL	Time To Live
Tx	Transmit
UNI	User Network Interface
UNL	Unexpected (MEG) Level
UNM	Unexpected MEP
UNP	Unexpected Period
UNPr	Unexpected Priority
VCCV	Virtual Circuit Connectivity Verification
VS	Vendor-Specific
VSM	Vendor Specific (OAM) Message
VSR	Vendor Specific (OAM) Reply

5 Conventions

The diagrammatic conventions for maintenance entity group end point (MEP) and MEG intermediate point (MIP) compound functions are those of [ITU-T G.8010].

The values of the OAM protocol data unit (PDU) fields are expressed in decimal format.

6 Functional components

6.1 Maintenance entity (ME)

A maintenance entity (ME) can be viewed as the association between two MEG end points (MEPs) that applies maintenance and monitoring operations to a network connection or a tandem connection.

In the case of a co-routed bidirectional point-to-point connection, a single bidirectional ME is defined to monitor both directions congruently.

6.2 Maintenance entity group (MEG)

A maintenance entity group (MEG) is a set of one or more MEs that belong to the same connection and are maintained and monitored as a group.

6.2.1 Tandem connection monitoring (TCM)

Tandem connection monitoring (TCM) can be supported by the instantiation of a sub-path maintenance entity (SPME), as described in [IETF RFC 6371], that has a 1:1 relationship with the monitored connection. The SPME is then monitored using normal label switched path (LSP) monitoring.

When an SPME is established between non-adjacent nodes, the edges of the SPME become adjacent at the client sub-layer network and any intermediate node that was previously in-between becomes an intermediate node for the SPME.

TCMs can nest but not overlap.

6.3 MEG end points (MEPs)

A MEG end point (MEP) marks the end point of a MEG which is responsible for initiating and terminating OAM packets for fault management and performance monitoring.

A MEP may initiate an OAM packet to be transferred to its corresponding peer MEP, or to an intermediate MIP that is part of the MEG.

As the MEP corresponds to the termination of the forwarding path for a MEG at the given (sub-) layer, OAM packets never leak outside of a MEG in a properly configured error-free implementation.

A MEP may be a per-node MEP or a per-interface MEP.

Per-node MEP is a MEP which is located somewhere within one node. There is no other MEG intermediate point (MIP) or MEP in the same MEG within the same node.

Per-interface MEP is a MEP which is located on a specific interface within the node. In particular a per-interface MEP is called "Up MEP" or "Down MEP" depending on its location relative to the connection function², as shown in Figure 6-1.

² The connection function is called a forwarding engine in [IETF RFC 6371]

NOTE – It is possible that two Up MEPs of a MEG are set, one on each side of the connection function, such that the MEG is entirely internal to the node.

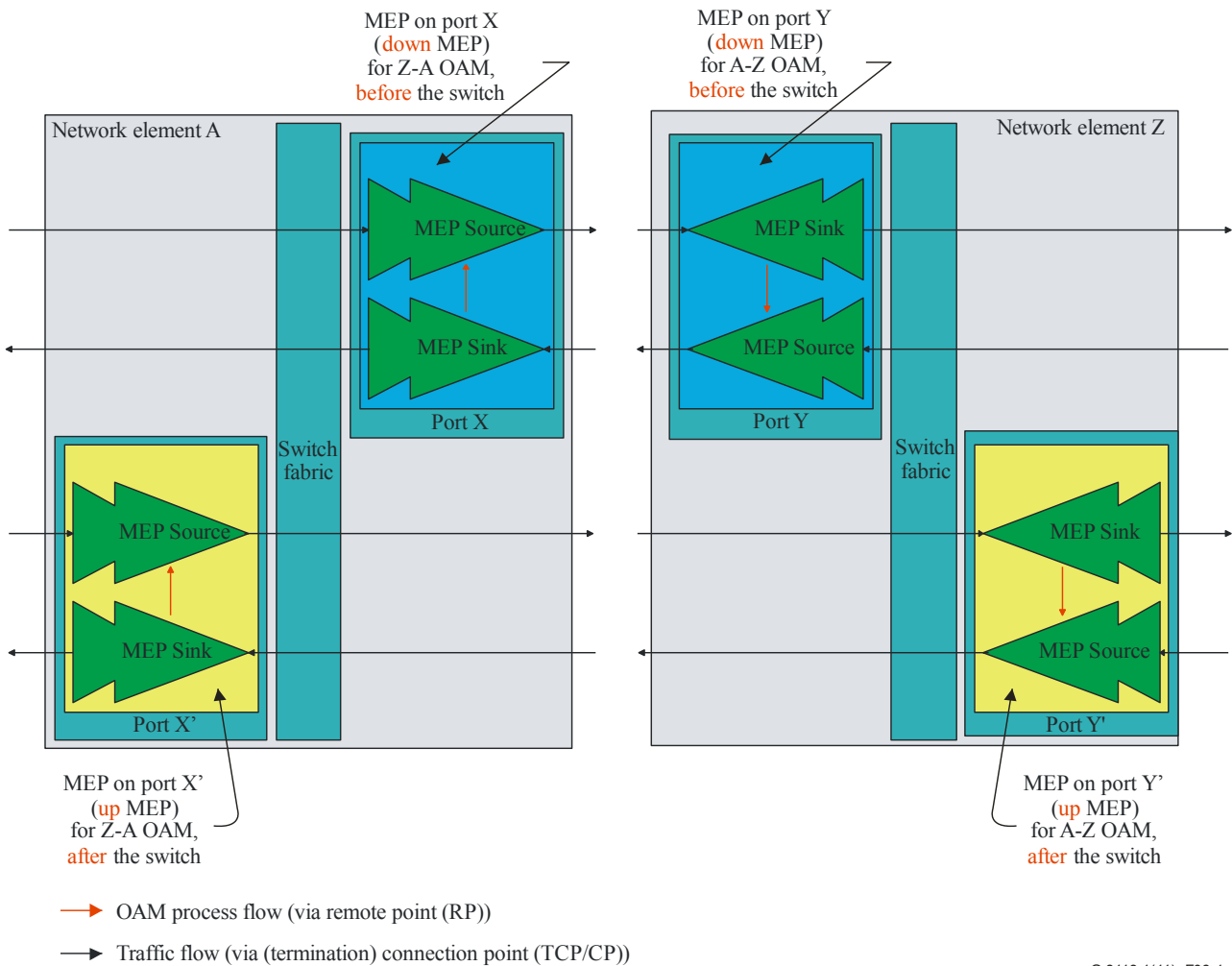


Figure 6-1 – Up/Down MEPs

In Figure 6-1 above, the MEP of the transport entity traversing interface port X of NE-A is a Down MEP. Similarly the MEP of interface port Y of NE-Z is also a Down MEP. Note that an interface port may support multiple transport entities. In the figure, only one transport entity is shown. For simplicity, refer to these two MEPs as MEP_{AX} and MEP_{ZY}. If these two MEPs belong to the same MEG (i.e., they peer to each other), OAM flow (e.g., loopback OAM packets) from the MEP_{AX} to MEP_{ZY} will be processed (looped back) by MEP_{ZY} and the connection function of NE-Z is not involved in this OAM flow. Similarly, OAM packets from MEP_{ZY} to MEP_{AX} will be processed by MEP_{AX} and do not transit the connection function of NE-A.

In Figure 6-1 above, the MEP of the transport entity traversing interface port X' of NE-A is an Up MEP. Similarly the MEP of interface port Y' of NE-Z is also an Up MEP. If these two MEPs (MEP_{AX'} and MEP_{ZY'}) belong to the same MEG, OAM packets (e.g., loopback packets) from MEP_{AX'} to MEP_{ZY'} will traverse through the connection function of NE-Z and then be processed by MEP_{ZY'} and therefore the connection function of NE-Z is involved in this OAM flow. Similarly, the OAM packets from MEP_{ZY'} to MEP_{AX'} will be processed by MEP_{AX'} and transit the connection function of NE-A.

More details are described in [IETF RFC 6371].

6.4 MEG intermediate points (MIPs)

A MEG intermediate point (MIP) is an intermediate point between the two MEPs within a MEG that is capable of reacting to some OAM packets and forwarding all the other OAM packets while ensuring fate-sharing with user-plane packets.

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.

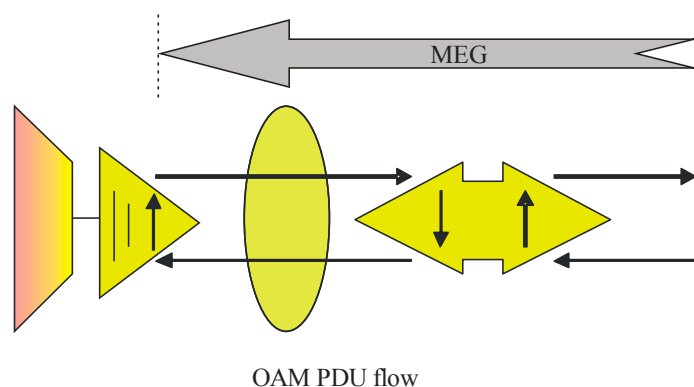
MIPs are unaware of any OAM flows running between MEPs or between MEPs and other MIPs. MIPs can only receive and process OAM packets addressed to them.

A MIP may be a per-node MIP or a per-interface MIP.

Per-node MIP is a MIP which is located somewhere within one node. There is no other MIP or MEP on the same MEG within the same node.

Per-interface MIP is a MIP which is located on a node interface, independently from the connection function³. The MIP can be placed at the ingress interface or at the egress interface of any node along the MEG.

A node at the edge of a MEG that has a per-interface Up MEP can also support a per-interface MIP on the other side of the connection function, as illustrated in Figure 6-2.



G.8113.1(11)_F06-2

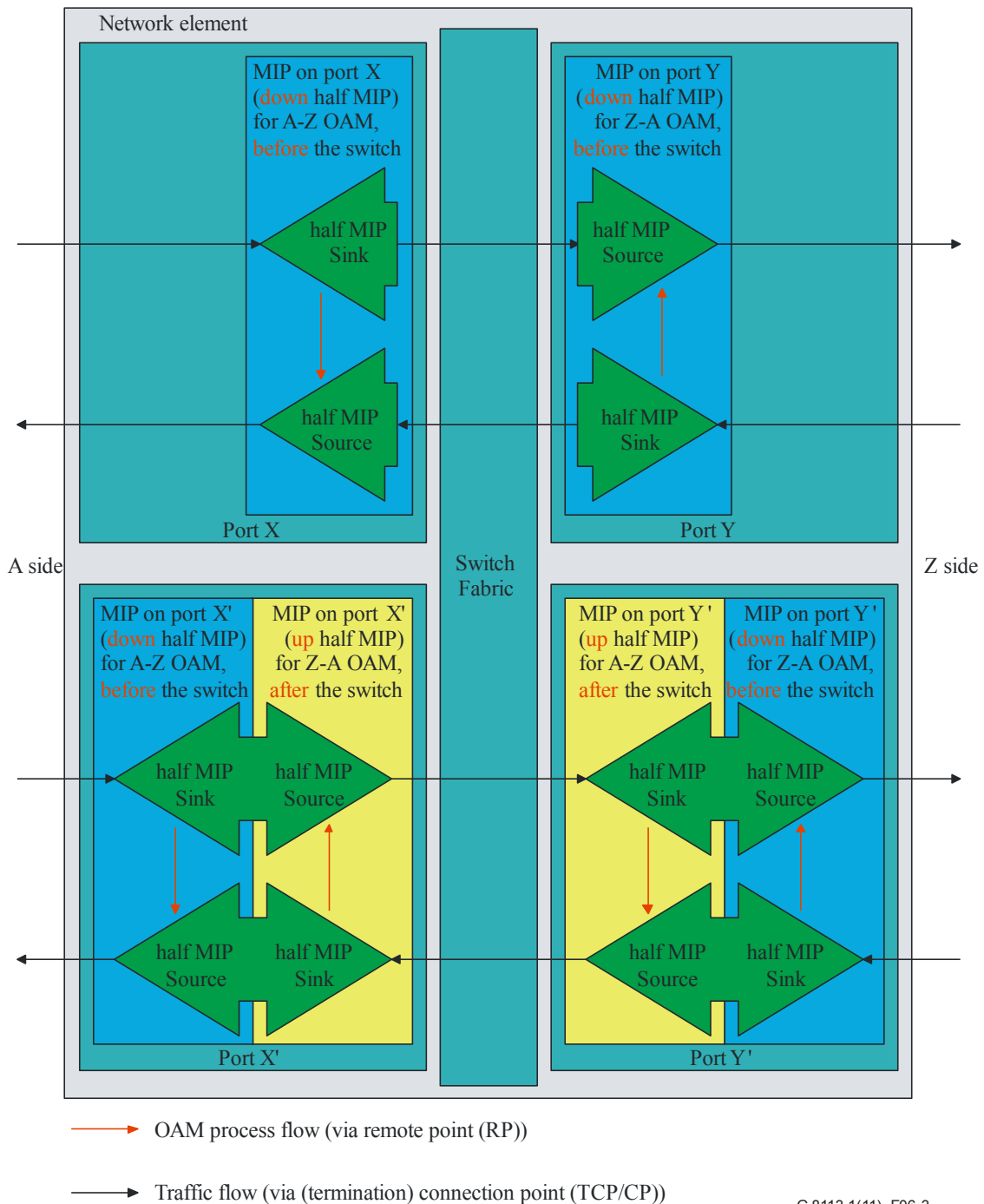
Figure 6-2 – Per-interface Up MEP and MIP in a node at the edge of a MEG

An intermediate node within a MEG can either:

- support per-node MIP (i.e., a single MIP per node in an unspecified location within the node);
- support per-interface MIPs (i.e., two MIPs per node, one on each side of the forwarding engine, for co-routed point-to-point bidirectional connections).

According to [ITU-T G.8110.1], a MIP is functionally modelled as two back-to-back half MIPs as illustrated in Figure 6-3.

³ The connection function is called forwarding engine in [IETF RFC 6371]



G.8113.1(11)_F06-3

Figure 6-3 – Up/Down half MIPs

In Figure 6-3 above, MIP_{AX} is on the interface port X on the A-side of the NE, MIP_{ZY} is on the interface port Y on the Z-side of the NE, $MIP_{AX'}$ is on the interface port X' on the A-side of the NE, and $MIP_{ZY'}$ is on the interface port Y' on the Z-side of the NE.

MIP_{AX} is a Down half- MIP. It can respond to OAM flow coming from the A-side and targeted to it. It cannot respond to OAM flow coming from the Z-side, even when targeted to it.

MIP_{ZY} is a Down half MIP. It can respond to OAM flow coming from the Z-side and targeted to it. It cannot respond to OAM flow coming from the A-side, even when targeted to it.

MIP_{AX'} is a full MIP, which consists of a Down half MIP and an Up half MIP. It can respond to OAM flow coming from the A-side and targeted to it. It can also respond to OAM flow targeted to it coming from the Z-side and traversing the connection function.

MIP_{ZY'} is a full MIP, which consists of a Down half MIP and an Up half MIP. It can respond to OAM flow coming from the Z-side and targeted to it. It can also respond to OAM flow targeted to it coming from the A-side and traversing the connection function.

6.5 Server MEP

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

- defined in a layer network that is "below", which is to say encapsulates and transports the MPLS-TP layer network being referenced, or
- 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 provides server layer OAM indications to the server/MPLS-TP adaptation function. The adaptation function maintains state on the mapping of MPLS-TP connections that are setup over that server (sub-)layer's trail.

The server MEP is expected to run OAM mechanisms specific to its (sub-)layer.

7 OAM functions

7.1 Identification of OAM packets from user-traffic packets

In order to ensure proper operational control, MPLS-TP network elements exchange OAM packets that strictly follow the same path as user traffic packets; that is, OAM packets are subject to the exact same forwarding schemes (e.g., fate-sharing) as the user traffic packets. These OAM packets can be distinguished from the user traffic packets by using the generated associated channel (G-Ach) and the G-Ach label (GAL) constructs, as defined in [IETF RFC 5586].

The G-ACh is a generic associated control channel mechanism for Sections, label switched paths (LSPs) and pseudowires (PWs), over which OAM and other control messages can be exchanged.

The GAL is a label-based exception mechanism to alert label edge routers (LERs)/label switch routers (LSRs) of the presence of an associated channel header (ACH) after the bottom of the stack.

Time to live (TTL) expiration is another exception mechanism to alert intermediate LSRs of the presence of an OAM packet that requires processing.

7.1.1 G-Ach

The Generic associated channel (G-ACh) is similar to the virtual circuit connectivity verification (VCCV); a control channel associated with a PW that carries OAM and other control messages, except that it is generic and can carry such messages over either a section, a PW, an LSP or a tandem connection..

Specifically, the VCCV uses an associated channel header (ACH) to provide a PW-associated control channel between a PW's end points for exchanging OAM and other control messages. The G-ACh is an associated control channel that generalizes the applicability of the ACH to LSPs and Sections, while maintaining compatibility with the PW-associated channel. The ACH, specified in [IETF RFC 4385], may be used with additional code points to support additional OAM functions on

the G-ACh and is common to Sections, LSPs, PWs and tandem connections. The format of the G-ACh is specified in clause 8.1 in alignment with [IETF RFC 5586].

7.1.2 GAL

A G-ACh alert label (GAL) is used to flag the G-ACh. Specifically, the GAL is used to indicate that a packet contains an ACH followed by a non-service payload (i.e., the G-ACh packet payload), thus generalizing the associated control channel mechanism to LSPs, Sections, PWs and tandem connections.

The GAL provides an alert based exception mechanism to:

- differentiate G-ACh packets (e.g., OAM, DCC, APS, etc.) from those of user traffic packets
- indicate that the ACH appears immediately after the bottom of the label stack.

One of the reserved label values defined in [IETF RFC 3032] is assigned for this purpose: the reserved label value assigned is 13. ~~The GAL must always be at the bottom of the label stack (i.e., S bit set to 1).~~ The format of the GAL is specified in clause 8.1 in alignment with [IETF RFC 5586].

NOTE – Using GAL for PW in MPLS-TP is specified in [b-IETF RFC 6423]. In MPLS-TP, the GAL MUST be used with packets on a G-Ach on LSPs, Sections, and tandem connections, and MAY be used with PWs.

7.2 OAM functions specification

Table 7-1 – OAM functions

Application	OAM function	
Fault management	Pro-active	Continuity check and connectivity verification (CC/CV)
		Remote defect indication (RDI)
		Alarm indication signal (AIS)
		Client signal fail (CSF) ⁴
	On-demand	Connectivity verification (CV)
		<u>Route tracing (RT)</u>
		Diagnostic test (DT)
Locked signal (LCK) ⁵		
Performance management	Pro-active	Loss measurement (LM)
		Delay measurement (DM)
	On-demand	Loss measurement (LM)
		Delay measurement (DM)
Other applications	Automatic protection switching (APS)	
	Management communication channel/Signalling communication channel (MCC/SCC)	
	Vendor-specific (VS)	

⁴ Client signal fail (CSF) is called client failure Indication (CFI) in [IETF RFC 5860].

⁵ Locked signal (LCK) is called lock reporting in [IETF RFC 5860].

Experimental (EXP)

7.2.1 OAM Functions for fault management

7.2.1.1 Proactive OAM functions for fault management

7.2.1.1.1 Continuity check and connectivity verification

The source MEP sends continuity check (CC)/connectivity verification (CV) OAM packets periodically at the configured rate. The sink MEP monitors the arrival of these CC/CV OAM packets at the configured rate and detects the defect of loss of continuity (LOC).

The following connectivity verification defects are also detected by this function:

- a) Mismatch: unintended connectivity between two MEGs.
- b) Unexpected MEP: unintended connectivity within the MEG with an unexpected MEP.

The following misconfiguration defect is also detected by this function:

- a) Unexpected period: CC/CV OAM packets are received with a period field value that is different from the configured CC/CV OAM packet rate.

CC/CV is mainly used for the fault management, performance monitoring and protection switching. A MEP periodically transmits the proactive CC/CV OAM packet at the configured transmission period. In transport networks, the following default transmission periods are defined:

- a) 3.33 ms: default transmission period for protection switching application (transmission rate of 300 packets/second);
- b) 100 ms: default transmission period for performance monitoring application (transmission rate of 10 packets/second);
- c) 1 s: default transmission period for fault management application (transmission rate of 1 packet/second).

Other transmission periods are not precluded, however the behaviour of the intended application is not guaranteed unless the default values are used.

7.2.1.1.2 Remote defect indication

Remote defect indication (RDI) is an indicator that is transmitted by a MEP to communicate to its peer MEPs that a signal fail condition exists. When a MEP detects a signal fail condition, it sends an RDI to its peer MEP.

An RDI is only used for bidirectional connections and is associated with proactive CC/CV activation.

7.2.1.1.3 Alarm indication

The alarm indication (AI) function is mainly used to suppress alarms following detection of defect conditions at the server (sub-)layer. When a server MEP asserts LOC or signal fail, it sets a flag that results in generation of OAM packets with alarm indication signal (AIS) information that are forwarded in the downstream direction to the sink MEP in the client (sub-)layer, which allows the suppression of secondary alarms (LOC, etc.) in the client (sub-)layer.

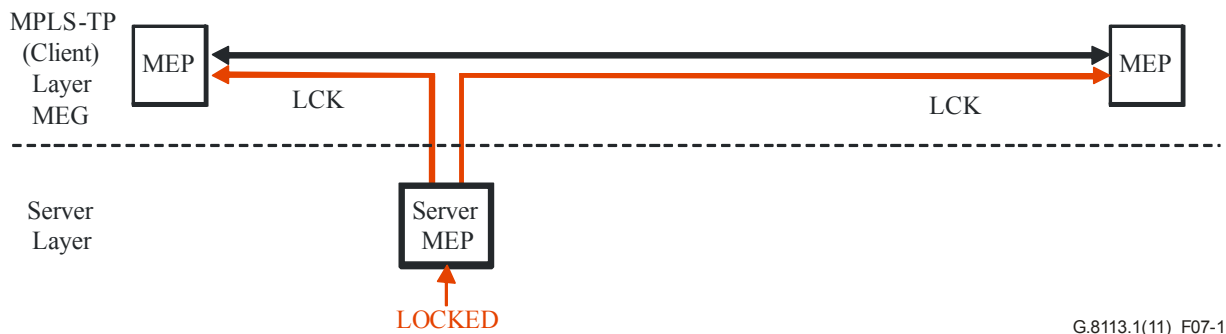
7.2.1.1.4 Locked signal

The locked signal (LCK) function is used to communicate to the client (sub-)layer MEPs the administrative locking of a server (sub-)layer MEP and consequential interruption of data traffic forwarding in the client (sub-)layer. It allows a client (sub-)layer MEP receiving packets with LCK information to differentiate between a defect condition and an administrative locking action at the

server (sub-)layer MEP. An example of an application that would require administrative locking of a MEP is the out-of-service diagnostic test, as described in clause 7.2.1.2.2.

When a server MEP is administratively locked, it sets a flag that results in generation of OAM packets with LCK information that are forwarded in both upstream and downstream directions to the client (sub-)layer MEPs until the administrative lock condition is removed (see Figure 7-1).

NOTE – When a server MEP is administratively locked, the server (sub-)layer is blocked from carrying user traffic. The server MEP source blocks any client (sub-)layer traffic received from upstream from being forwarded over the server (sub-)layer; however it allows locally-generated client (sub-)layer LCK packets to be sent over the server (sub-)layer. The server MEP sink blocks any client (sub-)layer traffic received from the server layer MEG from being forwarded downstream.



G.8113.1(11)_F07-1

Figure 7-1 – Example of LCK transmission

7.2.1.1.5 Client signal fail

This function is used to process client defects and propagate a client signal defect to the associated remote MEP using OAM packets. This function is usually used when the client of the MPLS-TP trail does not support a native defect/alarm indication mechanism.

7.2.1.2 On-demand OAM functions for fault management

7.2.1.2.1 Connectivity verification

On-demand connectivity verification (CV) allows detection of failures in the path for trouble shooting purposes. The on-demand CV can be used to check either the entire MEG (end-to-end) or just between a MEP and a specific MIP. When the on-demand CV function is invoked on a MEP, an OAM CV request packet is sent from the MEP to the target MIP or MEP within the MEG. The originating MEP expects to receive an OAM packet with the CV reply information from the target MIP or MEP. Upon reception of OAM CV request packet information, the receiving MIP or MEP validates it and transmits an OAM packet with CV reply information to the originating MEP.

7.2.1.2.2 Diagnostic test

The diagnostic test (DT) function is used to perform diagnostic tests such as bandwidth throughput, packet loss, and bit errors estimation, etc., by sending OAM diagnostic test packets on one direction of the MEG.

- a) When an out-of-service test is performed, the source MEP configured for the out-of-service test transmits LCK packets to suppress the secondary alarms; the client data traffic is disrupted in the MEG and the OAM diagnostic test packets are sent to realize this function.

NOTE – When the out-of-service test is performed, the MEP also generates LCK packets at the immediate client (sub-)layer in the same direction as the diagnostic test (DT) packets are

transmitted (see Figure 7-1). This needs to be taken into account when performing throughput measurement tests.

- b) When in-service test function is performed, data traffic should not be disrupted and the OAM diagnostic test packets have to be transmitted in such a manner that a limited portion of the service bandwidth is utilized.

NOTE – When the in-service test is performed, the DT packets can impact the data traffic.

When the diagnostic test function is invoked on a MEP, a test signal generator associated with the MEP can transmit OAM diagnostic test packets as often as the test signal generator configuration. Each DT packet is transmitted with a specific sequence number. A different sequence number must be used for every DT packet, and no sequence number from the same MEP may be repeated within one minute.

When a MEP receives OAM diagnostic test packets, it examines them to ensure that they are valid. If the receiving MEP is configured for the diagnostic test function, the test signal detector associated with the MEP detects bit errors from the pseudo-random bit sequence of the received DT packets and reports such errors. Further, when the receiving MEP is configured for an out-of-service test, it also generates LCK packets at the client (sub-)layer in the direction in which the DT packets are received.

7.2.1.2.3 Route tracing

Route tracing (RT) enables a MEP to discover the ordered sequence of MIPs (if any) and MEP(s) within a MEG.

The Route tracing (RT) OAM function can be implemented using the LBM OAM PDU with the "Discovery ingress/node MEP/MIP" and/or the "Discovery egress MEP/MIP" TLVs in the target MEP/MIP ID TLV which are defined in clause 8.2.2. However detailed procedures for implementing the RT OAM function are for further study in this version of the Recommendation.

7.2.2 OAM functions for performance monitoring

7.2.2.1 Proactive OAM functions for performance monitoring

7.2.2.1.1 Proactive loss measurement

The proactive loss measurement function is for performance monitoring purposes. It is performed continuously and its result is used for verifying the performance of the connection against the service level agreement (SLA). This function is used to measure packets loss on a connection. To perform the loss measurement function (LM), the MEP periodically sends OAM packets with LM information to the peer MEP and similarly receives packets with LM information from the peer MEP. Each MEP performs packet loss measurements which contribute to unavailable time. Since a bidirectional service is defined as unavailable if either of the two directions is declared unavailable, LM must allow each MEP to perform near-end and far-end packet loss measurements.

NOTE – For a MEP, near-end packet loss refers to packet loss associated with ingress data packets while far-end packet loss refers to packet loss associated with egress data packets. Both near-end and far-end packet loss measurements contribute to near-end severely errored seconds (near-end SES) and far-end severely errored seconds (far-end SES) respectively which together contribute to unavailable time, in a manner similar to [ITU-T G.826] and defined in [ITU-T G.7710].

7.2.2.2 On-demand OAM functions for performance monitoring

7.2.2.2.1 On-demand loss measurement

The on-demand loss measurement (LM) function is for maintenance purpose. It is performed during a configured specific time interval and its result can be used for diagnosis and analysis. This function is used to measure packets loss on a connection. To perform the LM function, the MEP sends OAM packets with LM information to the peer MEP and similarly receives packets with LM information from the peer MEP. Each MEP performs packet loss measurements, but the measurements do not contribute to the SES and unavailable time of the connection.

For a MEP, near-end packet loss refers to packet loss associated with ingress data packets while far-end packet loss refers to packet loss associated with egress data packets.

7.2.2.2.2 On-demand delay measurement

The on-demand delay measurement (DM) function is for maintenance purposes. It is performed during a configured specific time interval and its result can be used for diagnose and analysis. This function is used to measure packet delay and packet delay variation on a connection. The DM function can be performed in two fashions: one-way DM and two-way DM.

When a MEP is invoked to perform the on-demand delay measurement function (DM), it periodically sends DM packets with DM information (such as timestamps) to its peer MEP. It also expects to receive packets with DM information from its peer MEP. Packet delay (PD) and packet delay variation (PDV) measurements are derived from the DM information in the DM packets. The individual raw measurements of PD and PDV, instead of the summary statistics, will be reported to the maintenance system or crafted for analysis and diagnosis.

The processing details of performing on-demand DM are similar to those of proactive DM.

7.2.3 Other functions

7.2.3.1 Automatic protection switching (APS) communications

Automatic protection switching (APS) communications allows MPLS-TP nodes to exchange protection switching control via the generalized associated channel (G-ACh).

The specific use of APS communications is outside the scope of this Recommendation.

7.2.3.2 Management communication channel/signalling communication channel

The management communication channel (MCC) and the signalling communication channel (SCC) allow MPLS-TP nodes to exchange management-plane and control-plane messages via the generalized associated channel (G-ACh).

The specific use of MCC and SCC is outside the scope of this Recommendation.

NOTE – MPLS-TP MCC and SCC are defined in [ITU-T G.7712] and [IETF RFC 5718].

7.2.3.3 Vendor-specific

Vendor-specific (VS) functions can be used by a vendor across its equipment. Interoperability of the vendor-specific functionality is not expected across different vendor's equipment.

The protocol design allows different vendor-specific protocols to be distinguished/separated from standard protocols and experimental protocols, as well as from other vendor-specific protocols.

The specific application of vendor-specific functions is outside the scope of this Recommendation.

7.2.3.4 Experimental

Experimental (EXP) functions can be used within an administrative domain on a temporary basis. Interoperability of experimental functionality is not expected across different administrative domains.

The protocol design allows different experimental protocols to be distinguished/separated from standard protocols and vendor-specific protocols, as well as from other experimental protocols.

The specific application of experimental functions is outside the scope of this Recommendation.

8 OAM packet formats

8.1 Common OAM packets

The format of GAL is described in Figure 8-1 below:

1								2								3								4							
1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
Label (13)																TC		S	TTL												

Figure 8-1 – GAL format

The value of GAL is 13, as defined in [IETF RFC 5586].

The traffic class (TC) field (formerly known as the EXP field) of the label stack entry (LSE) containing the GAL follows the definition and processing rules specified and referenced in [IETF RFC 5462].

S bit is set to 1. GAL is always at the bottom of the label stack.

The time to live (TTL) field of the LSE that contains the GAL MUST be set to at least 1 and follow the definition and processing rules specified in [IETF RFC 3443].

The format of associated channel header is described in Figure 8-2 below:

1				2				3				4			
1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
0001				Version(0)				Reserved (0)				Channel Type			

Figure 8-2 – ACH format

The first nibble is set to 0001b to indicate a control channel associated with a PW, an LSP or a Section as defined in [IETF RFC 5586].

The Version field is set to 0 as defined in [IETF RFC 5586].

The Reserved field is set to 0 and ignored on reception as defined in [IETF RFC 5586].

Channel type indicates the specific OAM protocol carried in the associated control channel.

The registry of the allocated channel type values is maintained by IANA [b-IANA PW Reg]. The values used in this Recommendation are described in Table 8-1 below:

Table 8-1 – Channel type values

Channel type value	Description	Reference clause
0x0001	Management communication channel (MCC)	8.3
0x0002	Signalling communication channel (SCC)	8.4
0x8902	ITU-T G.8113.1-based OAM	8.2

8.2 OAM PDU formats based on [ITU-T G.8013]

This clause describes the information elements and formats for different OAM PDU types used to meet the requirements of OAM functions described in clause 7 that are inherited from [ITU-T G.8013].

This clause describes the use of the CC and ICC based MIP and MEP identifiers. MPLS-TP also supports IP-based formats for MIP and MEP identifiers⁶. The possible mixing of CC and ICC based formats and IP based formats within an operator domain is for further study. The encoding of the IP-based formats is also for further study.

Within the MPLS-TP OAM framework [IETF RFC 6371], OAM packets are distinguished from user data packets using the G-ACh construct (see clause 7.1) and they are addressed to MEPs or MIPs using existing MPLS forwarding mechanisms (i.e., label stacking and time to live (TTL) expiration). It is therefore possible to reuse the OAM PDUs defined in [ITU-T G.8013] within MPLS-TP and encapsulate them within the G-ACh.

A single ACH channel type (0x8902) is required to identify the presence of the OAM PDU. Within the OAM PDU, the OpCode field, defined in [ITU-T G.8013], identifies the specific OAM PDU, as described in Figure 8-3 below:

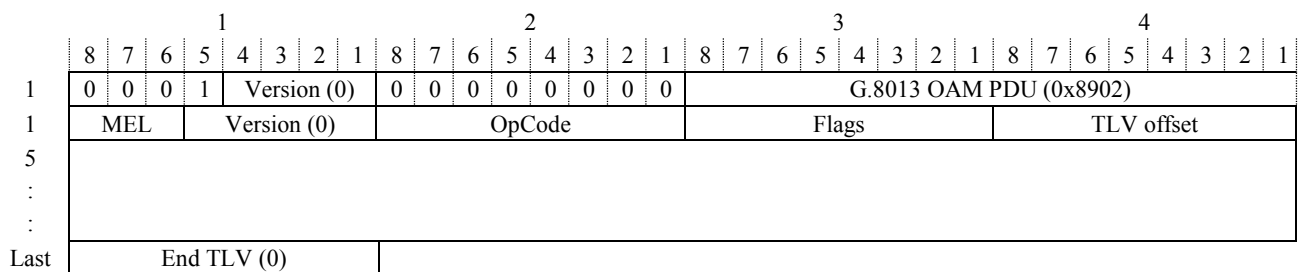


Figure 8-3 – Common OAM packet format based on [ITU-T G.8013]

The MEL field is configurable. It is set to the default value "111" on transmission and checked at reception for compliancy with [ITU-T G.8013].

The OpCode field identifies the type of the OAM PDU. The Registry of the allocated OpCode values is maintained by ITU-T in [ITU-T G.8013]. The values used in this Recommendation are described in Table 8-2 below:

⁶ The semantics for IP-based identifiers for MIP and MEP are defined in [b-IETF RFC 6370].

Table 8-2 – OpCode values

OpCode value	OAM PDU type	OpCode relevance for MEPs/MIPs
1	CCM	MEPs
3	LBM	MEPs and MIPs (connectivity verification)
2	LBR	MEPs and MIPs (connectivity verification)
33	AIS	MEPs
35	LCK	MEPs
37	TST	MEPs
39	APS	MEPs
43	LMM	MEPs
42	LMR	MEPs
45	IDM	MEPs
47	DMM	MEPs
46	DMR	MEPs
49	EXM	Outside the scope of this Recommendation
48	EXR	Outside the scope of this Recommendation
51	VSM	Outside the scope of this Recommendation
50	VSR	Outside the scope of this Recommendation
52	CSF	MEPs

The setting of the Version, Flags and type, length, and value (TLV) Offset is OpCode specific and described in [ITU-T G.8013].

The generic format of TLVs is defined in Figure 9.1-2 of [ITU-T G.8013].

The Registry of the allocated type values is maintained by ITU-T in [ITU-T G.8013]. The values used in this Recommendation are described in Table 8-3 below:

Table 8-3 – Type values

Type value	TLV name
0	End TLV
3	Data TLV
32	Test TLV
33	Target MEP/MIP ID TLV
34	Replying MEP/MIP ID TLV
35	Requesting MEP ID TLV

8.2.1 Continuity check message (CCM)

The CCM PDU is defined in [ITU-T G.8013]. When encapsulated within MPLS-TP, as described in clause 8.2, it can be used to support the following MPLS-TP OAM functional requirements:

- Pro-active continuity check (section 2.2.2 of [IETF RFC 5860]).
- Pro-active connectivity verification (section 2.2.3 of [IETF RFC 5860]).

- Pro-active remote defect indication (section 2.2.9 of [IETF RFC 5860]).
- Pro-active packet loss measurement (section 2.2.11 of [IETF RFC 5860]).

Procedures for generating and processing CCM PDUs are defined in clause 9.1.1.

In order to perform pro-active connectivity verification, the CCM packet contains a globally unique identifier of the source MEP, which is the combination of a globally unique MEG ID with a MEP ID that is unique within the scope of the maintenance entity group.

The generic format for MEG ID is defined in Figure A.1 of [ITU-T G.8013]. Different formats of MEG ID are allowed: the MEG ID format type is identified by the MEG ID format field.

The formats of both the ICC-based MEG ID and the CC- and ICC-based global MEG ID are defined in Annex A of [ITU-T G.8013]. ~~Both of these~~ This formats are applicable to MPLS-TP Sections, LSPs and PWs. If a globally unique MEG ID is required the CC- and ICC-based MEG ID must be used.

~~MPLS-TP supports also IP-based format for MEG ID. These formats are outside the scope of this version of the Recommendation.⁷~~

8.2.2 OAM loopback (LBM/LBR)

The loopback message/loopback reply (LBM/LBR) PDUs are defined in [ITU-T G.8013]. When encapsulated within MPLS-TP, as described in clause 8.2, they can be used to support the following MPLS-TP OAM functional requirements:

- On-demand bidirectional connectivity verification (section 2.2.3 of [IETF RFC 5860]).
- Bidirectional in-service or out-of-service diagnostic test (section 2.2.5 of [IETF RFC 5860]).

Procedures for generating and processing LBM and LBR PDUs are defined in clause 9.1.2.

In order to allow proper identification of the target MEP/MIP to which the LBM is addressed, the LBM PDU is required to include the target MEP/MIP ID TLV: this TLV is always present in an LBM PDU and it is always located at the top of the TLVs (i.e., it starts at the offset indicated by the TLV Offset field).

To allow proper identification of the actual MEP/MIP that has replied to an LBM PDU, the LBR PDU is required to include the replying MEP/MIP ID TLV: this TLV is always present in an LBR PDU and it is always located at the top of the TLVs (i.e., it starts at the offset indicated by the TLV Offset field).

NOTE – In order to simplify hardware-based implementations, these TLVs have been defined to have a fixed position (as indicated by the TLV Offset field) and a fixed length (see clause 8.2.2.1).

It is worth noting that the MEP/MIP identifiers used in the target MEP/MIP ID and in the replying MEP/MIP ID TLVs are required to be unique within the scope of the MEG. When LBM/LBR OAM is used for connectivity verification purposes, there are some misconnectivity cases that could not be easily located by simply relying upon these TLVs. In order to locate these misconnectivity configurations, the LBM PDU can carry a requesting MEP ID TLV that provides a globally unique identification of the MEP that has originated the LBM PDU. When the requesting MEP ID TLV is present in the LBM PDU, the replying MIP/MEP is required to check that the received requesting MEP identifier matches with the expected requesting MEP identifier before replying. In this case, the LBR PDU is required to carry the requesting MEP ID TLV to confirm to the MEP the LBR

⁷ ~~The IP-based format for MEG ID is under definition in IETF: see [b-IETF-tp-id].~~

PDU is sent to that the requesting MEP ID TLV in the LBM PDU has been checked before replying.

When LBM/LBR OAM is used for bidirectional diagnostic tests, the requesting MEP ID TLVs are never included.

The format of the LBM and LBR PDUs are shown in Figure 8-4 and in Figure 8-5.

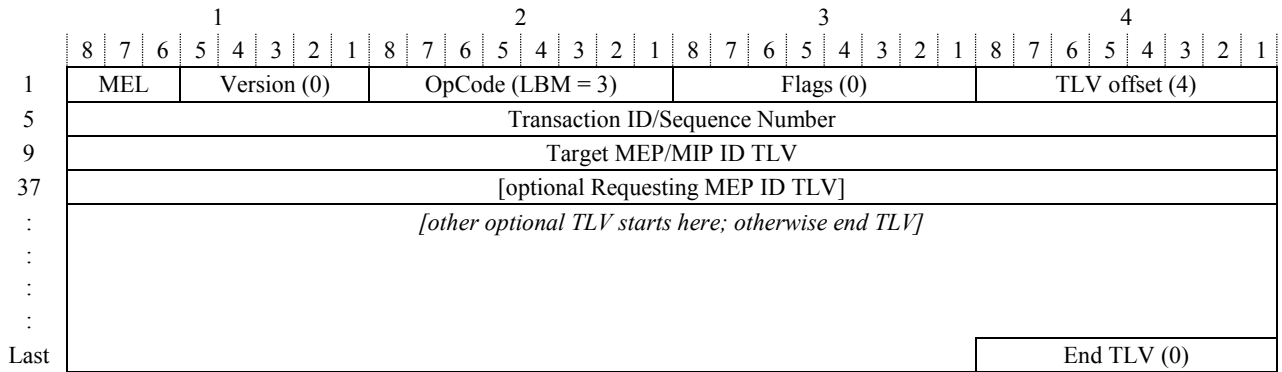


Figure 8-4 – LBM PDU format

The target MEP/MIP ID TLV is always present as the first TLV within the LBM PDU. When present, the requesting MEP ID TLV always follows the target MEP/MIP ID TLV within the LBM PDU.

NOTE – When the LBM packet is sent to a target MIP, the source MEP knows the hop count to the target MIP and sets the TTL field accordingly as described in [IETF RFC 6371].

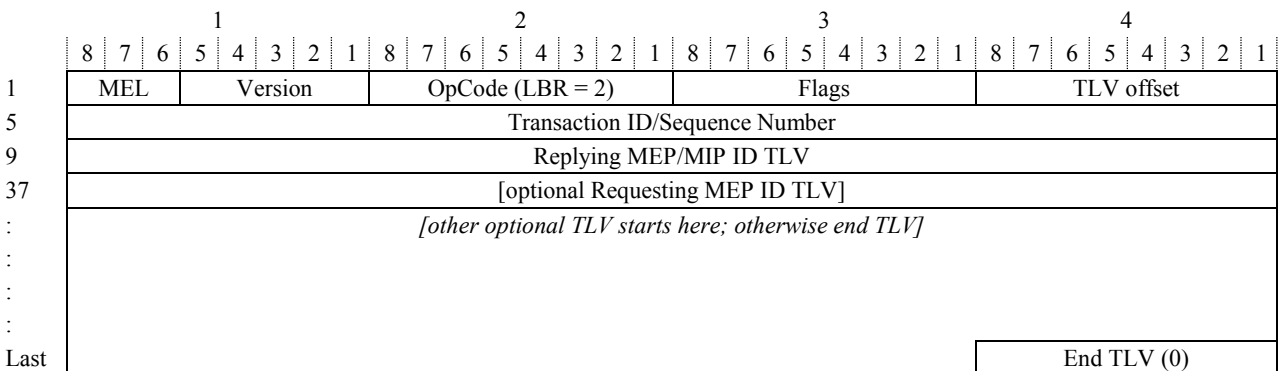


Figure 8-5 – LBR PDU format

The replying MEP/MIP ID TLV is always present as the first TLV within the LBR PDU. When present, the requesting MEP ID TLV always follows the replying MEP/MIP ID TLV within the LBR PDU.

8.2.2.1 Target and replying MEP/MIP ID TLVs

The format of the target and replying MIP/MEP ID TLVs are shown in Figures 8-6 and 8-7.

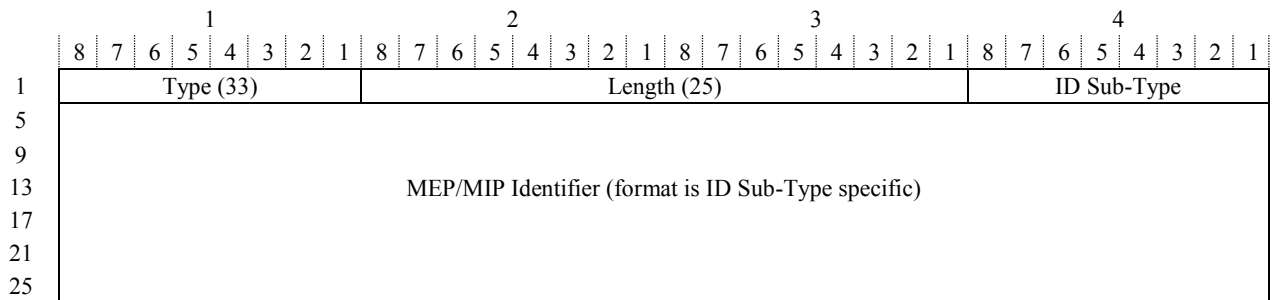


Figure 8-6 – Target MEP/MIP ID TLV format

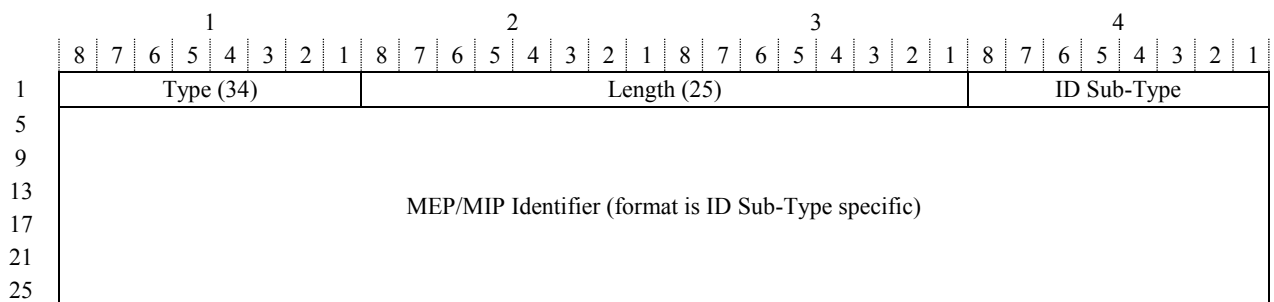


Figure 8-7 – Replying MEP/MIP ID TLV format

Different formats of MEP/MIP identifiers can be defined: the format type is described by the MEP/MIP ID sub-type field (see Table 8-4).

Table 8-4 – MEP/MIP identifier sub-type values

ID Sub-Type	MEP/MIP identifier name	MEP/MIP identifier length
0x00	Discovery ingress/node MEP/MIP	0
0x01	Discovery egress MEP/MIP	0
0x02	ICC-based MEP ID	2 bytes
0x03	ICC-based MIP ID	146 bytes
0x04-0xFF	Reserved	

The "Discovery ingress/node MEP/MIP" and the "Discovery egress MEP/MIP" identifiers can only be used within the LBM PDU (and cannot appear in an LBR PDU) for discovering the identifiers of the MEPs or of the MIPs located at a given TTL distance from the MEP originating the LBM PDU.

The format of the target MEP/MIP ID TLV carrying a "Discovery ingress/node MEP/MIP" is shown in Figure 8-8.

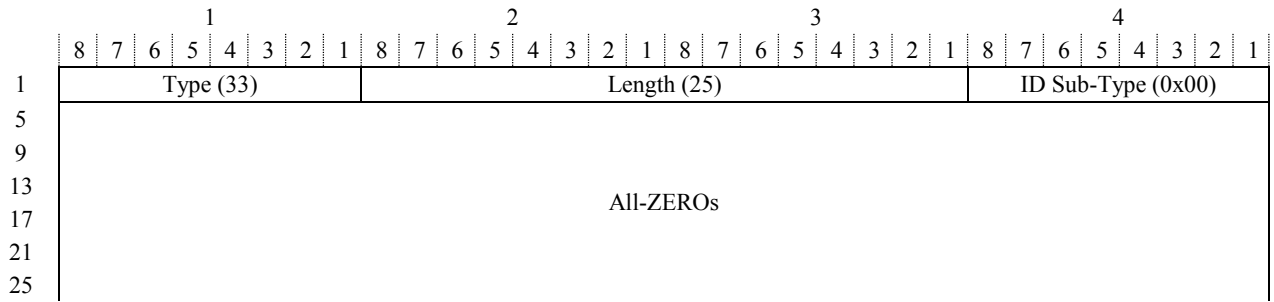


Figure 8-8 – Target MEP/MIP ID TLV format for ~~(Discovery ingress/node MEP/MIP)~~

The format of the target MEP/MIP ID TLV carrying a "Discovery egress MEP/MIP" is shown in Figure 8-9.

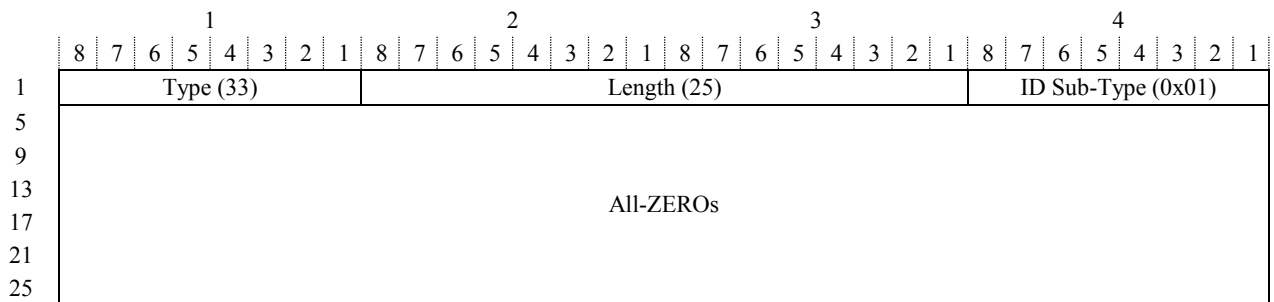


Figure 8-9 – Target MEP/MIP ID TLV format for ~~(Discovery egress MEP/MIP)~~

The format of the target or replying MEP/MIP ID TLV carrying an "ICC-based MEP ID" is shown in Figure 8-10.

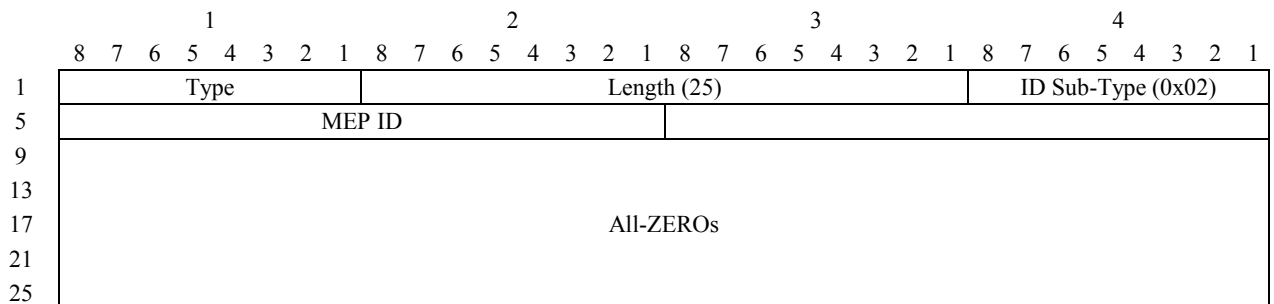


Figure 8-10 – Target or replying MEP/MIP ID TLV format ~~(ICC-based)~~ for MEP ID)

The MEP ID is a 16-bit integer value identifying the transmitting MEP within the MEG.

The format of the target or replying MEP/MIP ID TLV carrying an "ICC-based MIP ID" is shown in Figure 8-11.

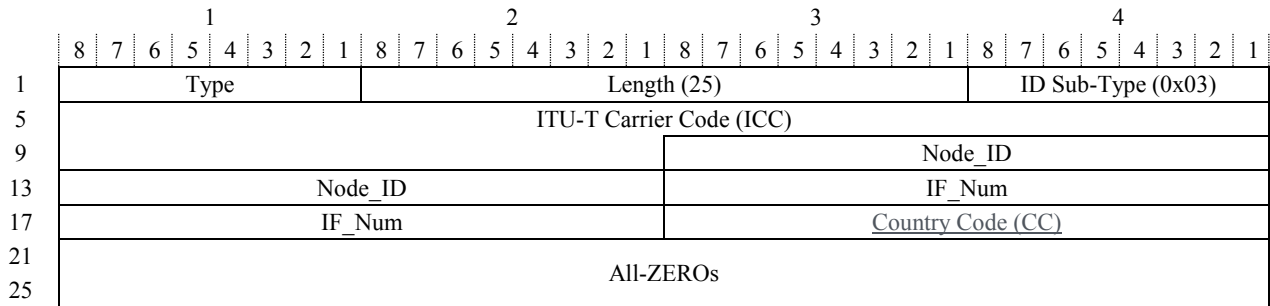


Figure 8-11 – Target or replying MEP/MIP ID TLV format (ICC based for MIP ID)

The ITU-T Carrier Code (ICC) is a code assigned to a network operator/service provider and maintained by the ITU-T Telecommunication Standardization Bureau (TSB) as per [ITU-T M.1400]. The ITU field in Figure 8-11 consists of between 1 and 6 left-justified characters with trailing NULLs completing the ICC field.

For backward compatibility, in cases where global uniqueness is not required, the CC field may be All ZEROs.

The Node_ID is a numeric identifier of the node where the MIP is located. Its assignment is a matter for the organization to which the ICC has been assigned, provided that uniqueness within that organization is guaranteed.

The IF_Num is a numeric identifier of the access point (AP) toward the server layer trail, which can be either an MPLS-TP or a non-MPLS-TP server layer, where a per-interface MIP is located. Its assignment is a matter for the node where the MIP is located, provided that uniqueness within that node is guaranteed. Note that the value 0 for IF_Num is reserved to identify per-node MIPs.

~~MPLS-TP supports also IP based format for MIP and MEP identifiers. These formats are outside the scope of this version of the Recommendation.&~~

The Country Code (alpha-2) is a string of 2 alphabetic characters represented with upper case letters (i.e., A-Z). The Country Code format is defined in [ISO 3166-1].

8.2.2.2 Requesting MEP ID TLV

The format of the requesting MEP ID TLVs is shown in Figure 8-12.

~~& The IP based format for MIP and MEP identifiers are under definition in IETF: see [b-IETF-tp-id]~~

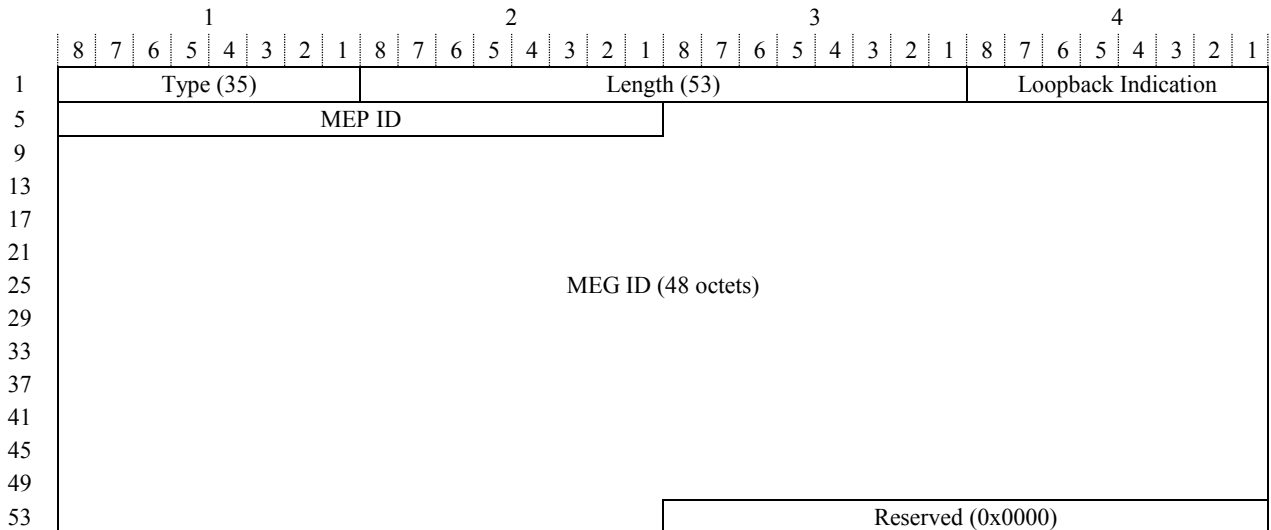


Figure 8-12 – Requesting MEP ID TLV format

~~The MEP ID and MEG ID carry the globally unique MEP ID as defined in clause 8.2.1. The globally unique identifier for a MEP can be provided by the combination of a globally unique MEG ID with a MEP ID as defined in clause 8.2.1.~~

The reserved bits are set to all-ZEROes in transmission and ignored in reception.

The loopback indication is set to 0x0000 when this TLV is inserted in a loopback message (LBM) PDU and set to 0x0001 in the LBR PDU. This is used to indicate that the value of this TLV has been checked by the node that generated the LBR PDU.

8.2.3 Alarm indication signal (AIS)

The AIS PDU is defined in [ITU-T G.8013]. When encapsulated within MPLS-TP, as described in clause 8.2, it can be used to support the alarm reporting MPLS-TP OAM functional requirement (section 2.2.8 of [IETF RFC 5860]).

Procedures for generating and processing AIS PDUs are defined in clause 9.1.3.

8.2.4 Locked signal (LCK)

The LCK PDU is defined in [ITU-T G.8013]. When encapsulated within MPLS-TP, as described in clause 8.2, it can be used to support the lock reporting MPLS-TP OAM functional requirement (section 2.2.7 of [IETF RFC 5860]).

Procedures for generating and processing LCK PDUs are defined in clause 9.1.4.

8.2.5 Test (TST)

The TST PDU is defined in [ITU-T G.8013]. When encapsulated within MPLS-TP, as described in clause 8.2, it can be used to support the unidirectional in-service or out-of-service diagnostic tests MPLS-TP OAM functional requirement (section 2.2.8 of [IETF RFC 5860]).

Procedures for generating and processing TST PDUs are defined in clause 9.1.5.

8.2.6 Loss measurement message/loss measurement reply (LMM/LMR)

Loss measurement message/loss measurement reply (LMM/LMR) PDUs are defined in [ITU-T G.8013]. When encapsulated within MPLS-TP, as described in clause 8.2, they can be used

to support both the on-demand and pro-active packet loss measurement MPLS-TP OAM functional requirement (section 2.2.11 of [IETF RFC 5860]).

Procedures for generating and processing LMM and LMR PDUs are defined in clause 9.1.6.

8.2.7 One-way delay measurement (1DM)

The 1DM PDU is defined in [ITU-T G.8013]. When encapsulated within MPLS-TP, as described in clause 8.2, it can be used to support both the on-demand and pro-active one-way packet delay measurement MPLS-TP OAM functional requirement (section 2.2.12 of [IETF RFC 5860]).

Procedures for generating and processing 1DM PDUs are defined in clause 9.1.7.

8.2.8 Two-way delay measurement)

The delay measurement message/delay measurement reply (DMM/DMR) protocol data units (PDUs) are defined in [ITU-T G.8013]. When encapsulated within MPLS-TP, as described in clause 8.2, they can be used to support both the on-demand and pro-active two-way packet delay measurement MPLS-TP OAM functional requirement (section 2.2.12 of [IETF RFC 5860]).

Procedures for generating and processing DMM/DMR PDUs are defined in clause 9.1.8.

8.2.9 Client signal fail (CSF)

The CSF PDU is defined in [ITU-T G.8013]. When encapsulated within MPLS-TP, as described in clause 8.2, it can be used to support the client failure indication MPLS-TP OAM functional requirement (section 2.2.10 of [IETF RFC 5860]). Procedures for generating and processing CSF PDUs are defined in clause 9.1.9.

8.2.10 Automatic protection switching (APS)

The APS PDU supports the requirement for MPLS-TP protection switching coordination.

The common formats for APS PDUs are defined in [ITU-T G.8013]. The complete format of the APS PDUs and the associated procedures are outside the scope of [ITU-T G.8013] and of this Recommendation.

8.2.11 Experimental (OAM) message/experimental (OAM) reply (EXM/EXR)

The EXM/EXR PDUs support the requirement for support of MPLS-TP experimental functions.

The common formats for EXM/EXR PDUs are defined in [ITU-T G.8013]. The complete format of the EXM/EXR PDUs and the associated procedures are outside the scope of [ITU-T G.8013] and of this Recommendation.

8.2.12 Vendor-specific OAM message/vendor specific OAM reply (VSM/VSR)

The VSM/VSR PDUs support the requirement for support of MPLS-TP vendor-specific functions.

The common formats for VSM/VSR PDUs are defined in [ITU-T G.8013]. The complete format of the VSM/VSR PDUs and the associated procedures are outside the scope of [ITU-T G.8013] and of this Recommendation.

8.3 Management communication channel (MCC)

The packet format for carrying management communication (i.e., MCC packets) over an ACH, and associated procedures, are defined in [ITU-T G.7712] and [IETF RFC 5718].

8.4 Signalling communication channel (SCC)

The packet format for carrying signalling communication (i.e., SCC packets) over an ACH, and associated procedures, are defined in [ITU-T G.7712] and [IETF RFC 5718].

9 MPLS-TP OAM procedures

9.1 MPLS-TP OAM procedures based on ITU-T G.8013 PDUs

The high level procedures for processing ITU-T G.8013 OAM PDUs are described in [ITU-T G.8013]. The technology-independent procedures are also applicable to MPLS-TP OAM.

More detailed and formal procedures for processing ITU-T G.8013 OAM PDUs are defined in [ITU-T G.8021]. Although the description in [ITU-T G.8021] is Ethernet-specific, the technology-independent procedures are also applicable to MPLS-TP OAM.

This clause describes the MPLS-TP OAM procedures based on the technology-independent ones defined in [ITU-T G.8013] and [ITU-T G.8021].

9.1.1 Continuity check message (CCM) procedures

The CCM PDU format is defined in clause 8.2.1.

When CCM generation is enabled, the MEP generates CCM OAM packets with the periodicity and the PHB configured by the operator:

- The MEL field is set to the configured value (see clause 8.2).
- The Version field is set to 0 (see clause 8.2).
- The OpCode field is set to 01 (see clause 8.2.1).
- The RDI flag is set, if the MEP asserts signal file. Otherwise, it is cleared.
- The Reserved flags are set to 0 (see clause 8.2.1).
- The Period field is set according to the configured periodicity (see Table 9-3 of [ITU-T G.8013]).
- The TLV Offset field is set to 70 (see clause 8.2.1).
- The Sequence number is set to 0 (see clause 8.2.1).
- The MEP ID and MEG ID fields are set to carry the configured values.
- The TxFCf field is set with the current value of the counter for in-profile data packets transmitted towards the peer MEP, when proactive loss measurement is enabled. Otherwise it is set to 0.
- The RxFCb field is set with the current value of the counter for in-profile data packets received from the peer MEP, if proactive loss measurement is enabled. Otherwise it is set to 0.
- The TxFCb field is set with the value of TxFCf of the last received CCM PDU from the peer MEP, if proactive loss measurement is enabled. Otherwise it is set to 0.
- The Reserved field is set to 0 (see clause 8.2.1).
- The end TLV is inserted after the Reserved field (see clause 8.2.1).

NOTE 1 – The transmission period of the CCM is always the configured period and does not change unless the operator reconfigures it. The period field in CCM PDU is transmitted with a value of the transmission period configured at the transmitting MEP.

When a MEP receives a CCM OAM packet, it checks the various fields (see Figure 8-19 of [ITU-T G.8021]). The following defects are detected as described in clause 6.1 of [ITU-T G.8021]: loss of continuity defect (dLOC); unexpected MEG level defect (dUNL)⁹; mismerge defect (dMMG); unexpected MEP defect (dUNM); unexpected periodicity defect (dUNP); unexpected priority defect (dUNPr); and remote defect indication defect (dRDI).

If the Version, MEL, MEG and MEP fields are valid and the pro-active loss measurement is enabled, the values of the packet counters fields are processed as described in clause 8.1.7.4 of [ITU-T G.8021].

The CCM packet also allows measurement of proactive dual-ended packet loss for co-routed point-to-point bidirectional MPLS-TP connections.

When configured for proactive loss measurement, a MEP periodically transmits CCM packets with the following information elements: TxFCf, RxFCb, TxFCb, as described above.

When configured for pro-active loss measurement, a MEP, upon receiving a CCM packet, uses the following values to make near-end and far-end loss measurements:

- **Received CCM** packet's TxFCf, RxFCb and TxFCb values and local counter RxFCI value at the time this CCM packet was received. These values are represented as TxFCf[tc], RxFCb[tc], TxFCb[tc] and RxFCI[tc], where tc is the reception time of the current frame.
- Previous CCM packet's TxFCf, RxFCb and TxFCb values and local counter RxFCI value at the time the previous CCM packet **was received. These values are represented as** TxFCf[tp], RxFCb[tp], TxFCb[tp] and RxFCI[tp], where tp is the reception time of the previous packet.

$$\text{packet loss}_{\text{far-end}} = |\text{TxFCb}[\text{tc}] - \text{TxFCb}[\text{tp}]| - |\text{RxFCb}[\text{tc}] - \text{RxFCb}[\text{tp}]|$$

$$\text{packet loss}_{\text{near-end}} = |\text{TxFCf}[\text{tc}] - \text{TxFCf}[\text{tp}]| - |\text{RxFCI}[\text{tc}] - \text{RxFCI}[\text{tp}]|$$

NOTE 2 – For dual-ended loss measurement, the counters do not count on-demand OAM packets for LBM/LBR, LMM/LMR, DMM/DMR, 1DM, TST and CCM. However, proactive OAM packets for APS are counted.

9.1.2 Loopback message/loopback reply (LBM/LBR) procedures

The loopback message/loopback reply (LBM/LBR) PDU formats are defined in clause 8.2.2.

When an out-of-service OAM loopback function is performed, client data traffic is disrupted in the diagnosed ME. The MEP configured for the out-of-service test transmits LCK packets in the immediate client (sub-) layer, as described in clause 9.1.4.

When an in-service OAM loopback function is performed, client data traffic is not disrupted and the packets with LBM/LBR information are transmitted in such a manner that a limited part of the service bandwidth is utilized. The periodicity for packets with LBM/LBR information is pre-determined.

NOTE 1 – The maximum rate at which packets with LBR/LBM information can be sent without adversely impacting the client data traffic for an in-service LBR/LBM is outside the scope of this Recommendation. It may be mutually agreed between the user of the LBM/LBR function and the user of the service.

NOTE 2 – Additional configuration information elements may be needed, such as the transmission rate of LBM/LBR information, the total interval of the test, etc. These additional configuration information elements are outside the scope of this Recommendation.

⁹ The dUNL defect will not be raised if the default value for MEL is used.

The LBM/LBR PDU formats are defined in clause 8.2.2 and described in details in clauses 9.3 and 9.4 of [ITU-T G.8013].

When on-demand OAM loopback is enabled at a MEP, the (requesting) MEP generates and sends to one of the MIPs or the peer MEP, LBM OAM packets with the periodicity and the per-hop (forwarding) behaviour (PHB) configured by the operator:

- The MEL field is set to the configured value (see clause 8.2).
- The Version field is set to 0 (see clause 8.2).
- The OpCode field is set to 03 (see clause 8.2.2).
- The Flags field is set to all-ZEROes (see clause 8.2.2).
- The TLV Offset field is set to 4 (see clause 8.2.2).
- The Transaction field is a 4-octet field that contains the transaction ID/sequence number for the loop back measurement.
- The target MEP/MIP ID is set to carry the configured value.

NOTE 3 – When performing a discovery function, the target MEP/MIP-ID is configured to be the "Discovery ingress/node MEP/MIP" or the "Discovery egress MEP/MIP".

- The originator MEP-ID TLV is inserted if configured, and it is set to carry the configured value.

NOTE 4 – When performing a bidirectional diagnostic test function, the originator MEP ID is configured not to be sent.

- Optional TLV field whose length and contents are configurable at the requesting MEP. The contents can be a test pattern and an optional checksum. Examples of test patterns include pseudo-random bit sequence (PRBS) ($2^{31}-1$) as specified in clause 5.8 of ITU-T O.150, all '0' pattern, etc. For bidirectional diagnostic test application, configuration is required for a test signal generator and a test signal detector associated with the MEP.
- End TLV field is set to all-ZEROes (see clause 8.2.2).

Whenever a valid LBM packet is received by a (receiving) MIP or a (receiving) MEP, an LBR packet is generated and transmitted by the receiving MIP/MEP to the requesting MEP:

- The MEL field is set to the value which is copied from the last received LBM PDU.
- The Version field is set to the value which is copied from the last received LBM PDU.
- The OpCode field is set to 2 (see clause 8.2.2).
- The Flags field is set to the value which is copied from the last received LBM PDU.
- The TLV Offset field is set to the value which is copied from the last received LBM PDU.
- The Transaction field is set to the value which is copied from the last received LBM PDU.
- The target MEP/MIP ID and originator MEP ID fields are set to the value which is copied from the last received LBM PDU.
- The Optional TLV field is set to the value which is copied from the last received LBM PDU.
- The end TLV field is inserted after the last TLV field; it is set to the value which is copied from the last received LBM PDU.

NOTE 5 – The transmission period of the LBR is always the same as the period of the LBM.

9.1.3 Alarm indication signal (AIS) procedures

The AIS PDU format is described in clause 8.2.3.

When the server layer trail termination sink asserts signal fail, it notifies the server/MT_A_Sk function that raises the aAIS consequent action. The aAIS is cleared when the server layer trail termination clears the signal fail condition and notifies the server/MT_A_Sk.

When the aAIS consequent action is raised, the server/MT_A_Sk continuously generates MPLS-TP OAM packets carrying the AIS PDU until the aAIS consequent action is cleared:

- The MEL field is set to the configured value (see clause 8.2).
- The Version field is set to 0 (see clause 8.2).
- The OpCode is set to 33 (see clause 8.2.3).
- The Reserved flags are set to 0 (see clause 8.2.3).
- The Period field is set according to the configure periodicity (see Table 9-4 of [ITU-T G.8013]).
- The TLV Offset is set to 0 (see clause 8.2.3).
- The end TLV is inserted after the TLV Offset field (see clause 8.2.3).

It is recommended that AIS be generated once per second.

The generated AIS packets are inserted in the incoming stream, i.e., the output stream contains the incoming packets and the generated AIS packets.

When a MEP receives an AIS packet with the correct MEL value, it detects the alarm indication signal defect (dAIS), as described in clause 6.1 of [ITU-T G.8021].

9.1.4 Locked signal (LCK) procedures

The LCK PDU format is described in clause 8.2.4.

When the access to the server layer trail is administratively locked by the operator, the server/MT_A_So and server/MT_A_Sk functions raise the aLCK consequent action. The aLCK is cleared when the access to the server layer trail is administratively unlocked.

When the aLCK consequent action is raised, the server/MT_A_So and server/MT_A_Sk continuously generate, on both directions, MPLS-TP OAM packets carrying the LCK PDU until the aLCK consequent action is cleared:

- The MEL field is set to the configured value (see clause 8.2).
- The Version field is set to 0 (see clause 8.2).
- The OpCode is set to 35 (see clause 8.2.4).
- The Reserved flags are set to 0 (see clause 8.2.4).
- The Period field is set according to the configure periodicity (see Table 9-4 of [ITU-T G.8013]).
- The TLV Offset is set to 0 (see clause 8.2.4).
- The end TLV is inserted after the TLV Offset field (see clause 8.2.4).

It is recommended that LCK be generated once per second.

When a MEP receives an LCK packet with the correct MEL value, it detects the dLCK defect as described in clause 6.1 of [ITU-T G.8021].

9.1.5 Test (TST) procedures

The TST function allows performing on-demand in-service or out-of-service one-way diagnostic tests between a pair of peer MEPs in point-to-point MPLS-TP connections. This includes verifying bandwidth throughput, detecting bit errors, etc.

The TST PDU format is described in clause 8.2.5 and defined in detail in clause 9.9 of [ITU-T G.8013].

When an out-of-service TST function is performed, client data traffic is disrupted in the diagnosed ME. The MEP configured for the out-of-service test transmits LCK packets, as described in clause 9.1.4, in the immediate client (sub-) layer.

When an in-service TST function is performed, client data traffic is not disrupted and the packets with TST information are transmitted in such a manner that a limited part of the service bandwidth is utilized. The periodicity for packets with TST information is pre-determined.

NOTE 1 – The maximum rate at which packets with TST information can be sent without adversely impacting the client data traffic for an in-service TST is outside the scope of this Recommendation. It may be mutually agreed between the user of the MS-TST function and the user of the service.

NOTE 2 – Additional configuration information elements may be needed, such as the transmission rate of TST information, the total interval of the test, etc. These additional configuration information elements are outside the scope of this Recommendation.

A MIP is transparent to the TST packets and therefore does not require any configuration information to support the TST functionality.

When on-demand diagnostics test is enabled at a MEP, it periodically generates and transmits TST OAM packets to its peer MEP in the same ME. The receiving MEP detects these TST OAM packets and makes the intended measurements.

The TST PDU format is defined in clause 8.2.5.

The requesting MEP generates and sends the TST OAM packets with the periodicity and the PHB configured by the operator.

- The MEL field is set to the configured value (see clause 8.2).
- The Version field is set to 0 (see clause 8.2).
- The OpCode field is set to 37 (see clause 8.2).
- The Flags field is set to all-ZEROes.
- The TLV Offset field is set to 4 (see clause 8.2.5).
- The Sequence Number field: A 4-octet value containing the sequence number which is incremented in successive TST PDUs.
- The test TLV field: Test TLV as specified in clause 8.2.5 and described in Figure 9.3-4 of [ITU-T G.8013]. Test TLV whose length and contents are configurable at the requesting MEP. The contents can be a test pattern and an optional checksum. Examples of test patterns include pseudo-random bit sequence (PRBS) ($2^{31}-1$) as specified in clause 5.8 of ITU-T O.150, all '0' pattern, etc.
- The end TLV field is set to all-ZEROes.

9.1.6 Loss measurement message/loss measurement reply (LMM/LMR) procedures

The loss measurement message/loss measurement reply (LMM/LMR) function allows measurement of on-demand and pro-active single-ended packet loss for point-to-point bidirectional MPLS-TP connections.

The LMM/LMR PDU formats are described in clause 8.2.6 and defined in detail in clauses 9.12 and 9.13 of [ITU-T G.8013].

When on-demand or pro-active loss measurement is enabled at a MEP, the MEP (i.e., the requesting MEP) generates and sends to its peer MEP the LMM OAM packets with the periodicity and the PHB configured by the operator:

- The MEL field is set to the configured value (see clause 8.2).
- The Version field is set to 0 (see clause 8.2).
- The OpCode field is set to 43 (see clause 8.2).
- The Reserved bits of the Flags field (see clause 8.2) are set to 0 (see clause 9.12.2 of [ITU-T G.8013]).
- The LSB bit (Type) of the Flags field (see clause 8.2) is set according to the type (pro-active or on-demand) of the operation (see clause 9.12.2 of [ITU-T G.8013]). ~~The Flag field is set to all-ZEROes.~~
- The TLV Offset field is set to 12 (see clause 8.2.6).
- The TxFCf field is set to the current value of the counter for in-profile data packets transmitted by the MEP towards its peer MEP, at the time of LMM packet transmission.
- The Reserved fields for RxFCf and TxFCb are set to 0 (see clause 8.2.6).
- The end TLV is set to all-ZEROes (see clause 8.2). No TLVs other than the end TLV are present in the LMM PDU.

NOTE – For LMM/LMR, the counters do not count on-demand OAM packets for LBM/LBR, LMM/LMR, DMM/DMR, 1DM and TST. Instead, CCM and APS packets are counted.

An LMM packet with a valid MEG level is considered to be a valid LMM packet. An LMM packet is discarded if not valid. Whenever a valid LMM packet is received by a MEP (i.e., the receiving MEP), an LMR packet is generated and transmitted by the receiving MEP to the requesting MEP as follows:

- The MEL field is set to the value which is copied from the last received LMM PDU.
- The Version field is set to the value which is copied from the last received LMM PDU.
- The OpCode field is set to 42 (see clause 8.2).
- The Flag field is set to the value which is copied from the last received LMM PDU.
- The TLV Offset field is set to the value which is copied from the last received LMM PDU.
- The TxFCf field is set to the value which is copied from the last received LMM PDU.
- The RxFCf field is set to the value of the counter of in-profile data packets received by the MEP (receiving MEP) from its peer MEP (requesting MEP), at the time of receiving last LMM packet from that peer MEP.
- The TxFCb field is set to the value of the counter of in-profile data packets transmitted by the MEP (receiving MEP) towards its peer MEP (requesting) at the time of LMR packet transmission.
- The end TLV is set to all-ZEROes. No TLVs other than the end TLV are present in the LMR PDU.

Upon receiving an LMR packet, a MEP (the requesting MEP) uses the following values to make near-end loss measurement (i.e., loss associated with ingress data packets) and far-end loss measurements (i.e., loss associated with egress data packets):

- Received LMR packet's TxFCf, RxFCf and TxFCb values and local counter RxFCI value at the time this LMR packet was received. These values are represented as TxFCf[tc], RxFCf[tc], TxFCb[tc] and RxFCI[tc], where tc is the reception time of the current reply packet.

- Previous LMR packet's TxFCf, RxFCf and TxFCb values and local counter RxFCI value at the time the previous LMR packet was received. These values are represented as TxFCf[tp], RxFCf[tp], TxFCb[tp] and RxFCI[tp], where tp is the reception time of the previous reply packet.

$$\text{packet loss}_{\text{far-end}} = |\text{TxFCf}[t_c] - \text{TxFCf}[t_p]| - |\text{RxFCf}[t_c] - \text{RxFCf}[t_p]|$$

$$\text{packet loss}_{\text{near-end}} = |\text{TxFCb}[t_c] - \text{TxFCb}[t_p]| - |\text{RxFCI}[t_c] - \text{RxFCI}[t_p]|$$

9.1.7 One-way delay measurement (1DM) procedures

The 1DM function allows measurement of on-demand and pro-active one-way packet delay and packet delay variation for point-to-point unidirectional or bidirectional MPLS-TP connections.

The 1DM PDU format is described in clause 8.2.7 and defined in details in clause 9.14 of [ITU-T G.8013].

When on-demand or pro-active packet delay measurement is enabled at a MEP, it periodically generates and transmits 1DM OAM packets to its peer MEP in the same ME. It also expects to receive 1DM OAM packets from its peer MEP in the same ME.

The transmitting MEP generates and sends the 1DM OAM packets with the periodicity and the PHB configured by the operator:

- The MEL field is set to the configured value (see clause 8.2).
- The Version field is set to 0 (see clause 8.2).
- The OpCode field is set to 45 (see clause 8.2).
- The Reserved bits of the Flags field (see clause 8.2) are set to 0 (see clause 9.14.2 of [ITU-T G.8013]). The Flag field is set to all-ZEROes.
- The LSB bit (Type) of the Flags field (see clause 8.2) is set according to the type (pro-active or on-demand) of the operation (see clause 9.14.2 of [ITU-T G.8013]).
- The TLV Offset field is set to 16 (see clause 8.2.7).
- The TxTimeStampf field is set to the timestamp at the transmission of the 1DM packet. The format of TxTimeStampf is equal to the TimeRepresentation format in [IEC 61588].
- The Reserved field is set to all-ZEROes.
- The end TLV is set to all-ZEROes (see clause 8.2). No TLVs other than the end TLV are present in the 1DM PDU.

Upon receiving a valid 1DM packet, the receiving MEP can compare the TxTimeStampf value in the received 1DM packet with the RxTimeef, the time at the reception of the 1DM packet and calculate the one-way packet delay. A 1DM packet with a valid MEG level is considered to be a valid 1DM packet. The one-way packet delay is calculated as:

$$\text{Packet Delay} = \text{RxTimeef} - \text{TxTimeStampf}$$

Packet delay variation measurement is calculated based on the difference between subsequent packet delay measurements.

Consideration regarding impact of clock synchronization on one-way packet delay measurement is described in clause 8.2 of [ITU-T G.8013].

9.1.8 Two-way delay measurement message/delay measurement reply (DMM/DMR) procedures

The delay measurement message/delay measurement reply (DMM/DMR) function allows measurement of on-demand and pro-active two-way packet delay and packet delay variation for point-to-point bidirectional MPLS-TP connections.

The DMM/DMR PDU formats are described in clause 8.2.8 and defined in detail in clauses 9.15 and 9.16 of [ITU-T G.8013].

When on-demand or pro-active two-way packet delay measurement is enabled at a MEP (the requesting MEP), it periodically generates and transmits DMM OAM packets to its peer MEP in the same ME with the periodicity and the PHB configured by the operator:

- The MEL field is set to the configured value (see clause 8.2).
- The Version field is set to 0 (see clause 8.2).
- The OpCode field is set to 47 (see clause 8.2).
- The Reserved bits of the Flags field (see clause 8.2) are set to 0 (see clause 9.15.2 of [ITU-T G.8013]).
- The LSB bit (Type) of the Flags field (see clause 8.2) is set according to the type (pro-active or on-demand) of the operation (see clause 9.15.2 of [ITU-T G.8013]).
- ~~– The Flag field is set to all-ZEROes.~~
- The TLV Offset field is set to 32 (see clause 8.2.8).
- The TxTimeStampf field is set to the timestamp at the transmission of the DMM packet. The format of TxTimeStampf is equal to the TimeRepresentation format in [IEC 61588].
- The Reserved field is set to all-ZEROes.
- The end TLV is set to all-ZEROes (see clause 8.2). No TLVs other than the end TLV are present in the DMM PDU.

A DMM packet with a valid MEG level is considered to be a valid DMM packet. A DMM packet is discarded if not valid. Whenever a valid DMM packet is received by a MEP (i.e., the receiving MEP), a DMR packet is generated and transmitted by the receiving MEP to the requesting MEP as follows:

- The MEL field is set to the value which is copied from the last received DMM PDU.
- The Version field is set to the value which is copied from the last received DMM PDU.
- The OpCode field is set to 46 (see clause 8.2).
- The Flag field is set to the value which is copied from the last received DMM PDU.
- The TLV Offset field is set to the value which is copied from the last received DMM PDU.
- The TxTimeStampf field is set to the value which is copied from the last received DMM PDU.
- The RxTimeStampf field is optional. If used, it is set to the timestamp of DMM reception. If not used, it is set to all-ZEROes.
- The TxTimeStampb field is optional. If used, it is set to the timestamp of DMR transmission. If not used, it is set to all-ZEROes.
- The Reserved field is set to all-ZEROes.
- The end TLV is set to all-ZEROes. No TLVs other than the end TLV are present in the DMR PDU.

Upon receiving a DMR packet, the requesting MEP can compare the TxTimeStampf value in the received DMR packet with the RxTimeb, the time at the reception time of the DMR packet and calculate the two-way packet delay as:

$$\text{Packet Delay} = \text{RxTimeb} - \text{TxTimeStampf}$$

If the optional timestamps are carried in the DMR packet, which is determined by non-zero values of the RxTimeStampf and TxTimeStampb fields, the more precise two-way packet delay (i.e., excluding the local processing time at the receiving MEP) is calculated to be:

$$\text{Packet Delay} = (\text{RxTimeb} - \text{TxTimeStampf}) - (\text{TxTimeStampb} - \text{RxTimeStampf})$$

Packet delay variation measurement is calculated based on the difference between subsequent packet delay measurements.

9.1.9 Client signal fail (CSF) procedures

The CSF function is used to propagate an indication from the ingress of an ME to the egress of the same ME that a failure of the ingress client signal has been detected. This is used in case the client layer itself does not support an alarm suppression mechanism, e.g., AIS. This supports the application described in Appendix VIII of [ITU-T G.806].

CSF packets with CSF information can be issued by a MEP, upon receiving signal fail information from its client layer. Detection rules for client signal fail events are by definition client-specific and outside the scope of this Recommendation. Upon receiving signal fail indication from its client layer, the MEP can immediately start transmitting periodic CSF packets. A MEP continues to transmit periodic packets with CSF information until the client layer signal fail indication is removed.

Transmission of CSF packets can be enabled or disabled on a MEP. The period of CSF generation is client layer specific and outside the scope of this Recommendation.

Upon receiving a CSF packet, a MEP detects the client layer signal fail condition and forwards this as a signal fail indication to its client layer.

The clearing conditions of CSF are client layer specific and outside the scope of this Recommendation.

Upon receiving the clearing of the signal fail indication from its client layer the MEP communicates this condition to its peer MEP by:

- ceasing the transmission of CSF packets and starting to forward client PDUs; or
- transmitting CSF packets with client defect clear indication (C-DCI) information.

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

The CSF PDU format is defined in clause 8.2.9.

The requesting MEP generates and sends the CSF OAM packets with the periodicity and the PHB configured by the operator.

- The MEL field is set to the configured value (see clause 8.2).
- The Version field is set to 0 (see clause 8.2).
- The OpCode field is set to 52 (see clause 8.2).
- The Flags field consists of:
 - reserved bits set to all-ZEROes;
 - type field set according to CSF condition (see Table 9-5 of [ITU-T G.8013]);

- period field configured by operator.
- The TLV Offset field is set to 0 (see clause 8.2.9).
- The end TLV field is set to all-ZEROes.

10 Security

According to clause 6.3 of this Recommendation packets originating outside the MEG are encapsulated by the MEP at the ingress and transported transparently through the MEG. This encapsulation significantly reduces the risk of an attack from outside the MEG. The MEP at the egress also prevents OAM packets from leaving a MEG.

The use of the CV tool improves network integrity by ensuring traffic is not misconnected or mismerged between LSPs. The expected MEP ID is provisioned at the sink MEP. This allows the received MEP ID to be verified with a high degree of certainty, which significantly reduces the possibility of an attack.

The use of globally unique identifiers for MEPs by the combination of a globally unique MEG ID with a MEP ID provides an absolute authoritative detection of persistent misconnection between LSPs. A globally unique MEG ID should be used when an LSP between the networks of different national operators crosses national boundaries since non-uniqueness can result in undetected misconnection in a scenario where two LSPs use a common MEG -ID.

For the use of any other OAM tools it is assumed that MEPs and MIPs that start using the tools verify the integrity of the path and the identity of the source MEP. If a misconnection is detected the tool in use shall be disabled immediately.

Annex A

MPLS-TP OAM for a packet transport network (PTN) applicability statement

(This annex forms an integral part of this Recommendation.)

This annex provides options and configurations of MPLS-TP in a packet transport network (PTN) application.

- 1) This application is intended to include the deployment of multi-technology transport nodes that may include MPLS-TP, Ethernet, optical transport network (OTN) and synchronous digital hierarchy (SDH) transport technologies.
- 2) Multiple transport layers may be supported by a common node.
- 3) In a network where the primary requirements are driven by a desire for consistency from the perspective of transport network (SDH/OTN) operational behaviour, operational functionality and operational process.
 - a) In particular compatibility with the existing OAM and protection switching paradigm for SDH, OTN, Ethernet. i.e., provide the same controls and indications.
 - b) Compatibility (consistency) means that the same management information model is be used. This enables upgrades of the operations support system (OSS) infrastructure in which it is only necessary to recognize the new type of layer network technology.
 - c) Minimize the impact on the workforce that operates the existing transport network. e.g., retraining about the same as for SDH to OTN.
- 4) [ITU-T G.7710], [ITU-T G.806], [ITU-T G.808.1] and [b-ITU-T G.808.2] describe the common behaviour (also see [b-IETF RFC 5951] for [ITU-T G.7710]).
- 5) Transport network: A connection-oriented network whose connections provide connectivity between service switches.
- 6) Currently connections are limited to a point-to-point co-routed bidirectional transport path.
 - a) Future requirement to support unidirectional point to multipoint.
- 7) Independence between services and transport i.e., the transport network is service agnostic
 - a) Provides a transport path for a PW or a LSP.

Appendix I

MPLS-TP network scenarios

(This appendix does not form an integral part of this Recommendation.)

I.1 MEG nesting example

Figure I.1 provides an example scenario, using the default MEG level, of nested MEGs for customer, provider and operator roles. In the figure, triangles represent MEPs, circles represent MIPs, and diamonds represent traffic conditioning points (TrCPs).

Figure I.1 shows an example of network implementation; MEPs and MIPs should be configured per interface, not per node. Upside-down triangles (▼) indicate Down MEPs and normal triangles (▲) indicate Up MEPs.

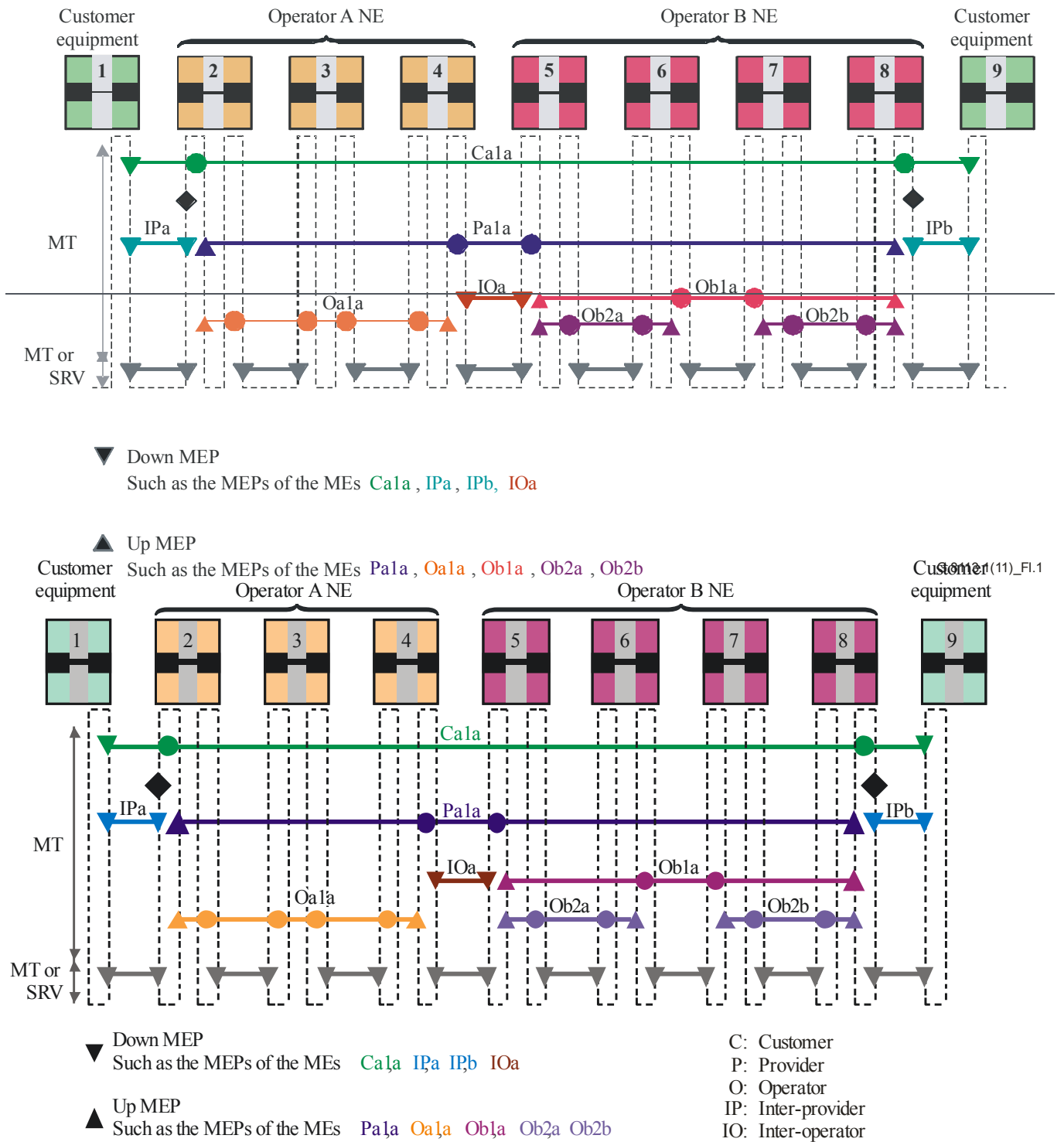


Figure I.1 – Example MEG nesting

- UNI_C to UNI_C customer ME (Ca1a).
- UNI_N to UNI_N provider ME (Pa1a).
- End-to-end operator MEs (Oa1a and Ob1a).
- Segment operator MEs in operator B's network (Ob2a and Ob2b).

- UNI_C to UNI_N MEs (IPa and IPb) between the customer and provider.
- Inter-operator ME (IOa).

Bibliography

- [b-ITU-T G.808.2] Recommendation ITU-T G.808.2 (2008), *Generic protection switching – Ring protection*.
- [b-IETF RFC 5951] IETF RFC 5951 (2010), *Network Management Requirements for MPLS-based Transport Networks*.
- [b-IETF RFC 6370] IETF RFC 6370 (2011), *MPLS-TP Identifiers*. [b-IETF tp id] —
IETF draft-ietf-mpls-tp-identifiers-04 (2013), *MPLS-TP Identifiers following ITU-T Conventions*.
<http://tools.ietf.org/html/draft-ietf-mpls-tp-itu-t-identifiers-04>
- [b-IETF RFC 6423] IETF RFC 6423 (2011), *Using the Generic Associated Channel Label for Pseudowire in the MPLS Transport Profile (MPLS-TP)*.
- [b-IANA PW Reg] Pseudowire Associated Channel Types,
<http://www.iana.org/assignments/pwe3-parameters/pwe3-parameters.xml#pwe3-parameters-10>
-