

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

G.8113.1/Y.1372.1

Corrigendum 1
(11/2016)

SERIES G: TRANSMISSION SYSTEMS AND MEDIA,
DIGITAL SYSTEMS AND NETWORKS

Packet over Transport aspects – MPLS over Transport
aspects

SERIES Y: GLOBAL INFORMATION
INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS,
NEXT-GENERATION NETWORKS, INTERNET OF
THINGS AND SMART CITIES

Internet protocol aspects – Transport

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

Corrigendum 1

Recommendation ITU-T G.8113.1/Y.1372.1 (2016) –
Corrigendum 1

ITU-T G-SERIES RECOMMENDATIONS

TRANSMISSION SYSTEMS AND MEDIA, DIGITAL SYSTEMS AND NETWORKS

INTERNATIONAL TELEPHONE CONNECTIONS AND CIRCUITS	G.100–G.199
GENERAL CHARACTERISTICS COMMON TO ALL ANALOGUE CARRIER-TRANSMISSION SYSTEMS	G.200–G.299
INDIVIDUAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON METALLIC LINES	G.300–G.399
GENERAL CHARACTERISTICS OF INTERNATIONAL CARRIER TELEPHONE SYSTEMS ON RADIO-RELAY OR SATELLITE LINKS AND INTERCONNECTION WITH METALLIC LINES	G.400–G.449
COORDINATION OF RADIOTELEPHONY AND LINE TELEPHONY	G.450–G.499
TRANSMISSION MEDIA AND OPTICAL SYSTEMS CHARACTERISTICS	G.600–G.699
DIGITAL TERMINAL EQUIPMENTS	G.700–G.799
DIGITAL NETWORKS	G.800–G.899
DIGITAL SECTIONS AND DIGITAL LINE SYSTEM	G.900–G.999
MULTIMEDIA QUALITY OF SERVICE AND PERFORMANCE – GENERIC AND USER-RELATED ASPECTS	G.1000–G.1999
TRANSMISSION MEDIA CHARACTERISTICS	G.6000–G.6999
DATA OVER TRANSPORT – GENERIC ASPECTS	G.7000–G.7999
PACKET OVER TRANSPORT ASPECTS	G.8000–G.8999
Ethernet over Transport aspects	G.8000–G.8099
MPLS over Transport aspects	G.8100–G.8199
Synchronization, quality and availability targets	G.8200–G.8299
Service Management	G.8600–G.8699
ACCESS NETWORKS	G.9000–G.9999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T G.8113.1/Y.1372.1

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

Corrigendum 1

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 specified 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 described 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 edition of this Recommendation.

This Recommendation is compliant with the transport profile of MPLS as specified by the Internet Engineering Task Force (IETF RFC 5654). 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 requests for comments (RFCs) will take precedence.

Corrigendum 1 removes text implying that MEG Level configurability is needed.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T G.8113.1/Y.1372.1	2012-11-20	15	11.1002/1000/11323
1.1	ITU-T G.8113.1/Y.1372.1 (2012) Amd. 1	2013-08-29	15	11.1002/1000/12032
2.0	ITU-T G.8113.1/Y.1372.1	2016-04-13	15	11.1002/1000/12803
2.1	ITU-T G.8113.1/Y.1372.1 (2016) Cor. 1	2016-11-13	15	11.1002/1000/13099

Keywords

MPLS-TP, OAM, PTN.

* 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 2017

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.....	3
4	Abbreviations and acronyms	3
5	Conventions	5
6	Functional components	5
	6.1 Maintenance entity	5
	6.2 Maintenance entity group	5
	6.3 Maintenance entity group end points	6
	6.4 Maintenance entity group intermediate points	7
	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	24
	8.4 Signalling communication channel	24
9	MPLS-TP OAM procedures	24
	9.1 MPLS-TP OAM procedures based on ITU-T G.8013 PDUs.....	24
10	Security	33
	Annex A – MPLS-TP OAM for a packet transport network applicability statement.....	34
	Appendix I – MPLS-TP network scenarios	35
	I.1 MEG nesting example	35
	Bibliography.....	36

Recommendation ITU-T G.8113.1/Y.1372.1

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

Editorial note: This is a complete-text publication. Modifications introduced by this corrigendum are shown in revision marks relative to Recommendation ITU-T G.8113.1/Y.1372.1 (2016).

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 specifies mechanisms for user-plane OAM in MPLS-TP networks to meet the MPLS-TP OAM requirements specified 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 described 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 edition 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 (2012), *Characteristics of transport equipment – Description methodology and generic functionality*.
- [ITU-T G.808.1] Recommendation ITU-T G.808.1 (2014) *Generic protection switching – Linear trail and subnetwork protection*.
- [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*.

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

- [ITU-T G.7710] Recommendation ITU-T G.7710/Y.1701 (2012), *Common equipment management function requirements*.
- [ITU-T G.7712] Recommendation ITU-T G.7712/Y.1703 (2010), *Architecture and specification of data communication network*.
- [ITU-T G.8010] Recommendation ITU-T G.8010/Y.1306 (2004), *Architecture of Ethernet layer networks*.
- [ITU-T G.8013] Recommendation ITU-T G.8013/Y.1731 (2015), *Operations, administration and maintenance (OAM) functions and mechanisms for Ethernet-based networks*.
- [ITU-T G.8021] Recommendation ITU-T G.8021/Y.1341 (2015), *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 Multi-Protocol Label Switching transport profile layer network*.
- [ITU-T M.1400] Recommendation ITU-T M.1400 (2015), *Designations for interconnections among operators' networks*.
- [IEC 61588] IEC 61588 (2009), *Precision clock synchronization protocol for networked measurement and control systems*.
- [IETF RFC 3032] IETF RFC 3032 (2001), *MPLS Label Stack Encoding*.
- [IETF RFC 3443] IETF RFC 3443 (2003), *Time To Live (TTL) Processing in Multi-Protocol Label Switching (MPLS) Networks*.
- [IETF RFC 4385] IETF RFC 4385 (2006), *Pseudowire Emulation Edge-to-Edge (PWE3) Control Word for Use over an MPLS PSN*.
- [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 5718] IETF RFC 5718 (2010), *An In-Band Data Communication Network For the MPLS Transport Profile*.
- [IETF RFC 5860] IETF RFC 5860 (2010), *Requirements for Operations, Administration, and Maintenance (OAM) in MPLS Transport Networks*.
- [IETF RFC 6371] IETF RFC 6371 (2011), *Operations, Administration and Maintenance Framework for MPLS-Based Transport Networks*.
- [ISO 3166-1] ISO 3166-1 (2013), *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
ACH	Associated Channel Header
AIS	Alarm Indication Signal
AP	Access Point
APS	Automatic Protection Switching
CC	Continuity Check; Country Code
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
EXM	Experimental OAM Message
EXP	Experimental
EXR	Experimental OAM Reply
FC	Frame Count
G-ACh	Generic Associated Channel
GAL	G-ACh Label
ICC	ITU-T Carrier Code
ID	Identifier
IF	Interface
LBM	Loopback Message
LBR	Loopback Reply
LCK	Locked Signal
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
NE	Network Element
Num	Number
OAM	Operations, Administration and Maintenance
OpCode	Operations Code
OSS	Operations Support System
OTN	Optical Transport Network
PD	Packet Delay
PDU	Protocol Data Unit
PDV	Packet Delay Variation
PHB	Per-Hop Behaviour
PRBS	Pseudo-Random Bit Sequence
PTN	Packet Transport Network
PW	Pseudowire
RDI	Remote Defect Indication
RT	Route Tracing
Rx	Receive
SCC	Signalling Communication Channel
SDH	Synchronous Digital Hierarchy
SES	Severely Errored Second
Sk	Sink
SLA	Service Level Agreement
So	Source
SPME	Sub-Path Maintenance Entity

TC	Traffic Class
TCM	Tandem Connection Monitoring
TLV	Type, Length and Value
TrCP	Traffic Conditioning Point
TST	Test
TTL	Time To Live
Tx	Transmit
UNI	User Network Interface
UNL	Unexpected MEL
UNM	Unexpected MEP
UNP	Unexpected Periodicity
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 (MEG) 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

A maintenance entity (ME) can be viewed as the association between two 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 specified to monitor both directions congruently.

6.2 Maintenance entity group

An 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

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 Maintenance entity group end points

An MEP marks the end point of an MEG that is responsible for initiating and terminating OAM packets for fault management and performance monitoring.

An 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 an MEG at the given (sub-) layer, OAM packets never leak outside of an MEG in a properly configured error-free implementation.

An MEP may be a per-node MEP or a per-interface (per-IF) MEP.

A per-node MEP is located somewhere within one node. There is no other MIP or MEP in the same MEG within the same node.

A per-IF MEP is located on a specific IF within the node. In particular a per-IF MEP is called "Up MEP" or "Down MEP" depending on its location relative to the connection function,² as shown in Figure 6-1.

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

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

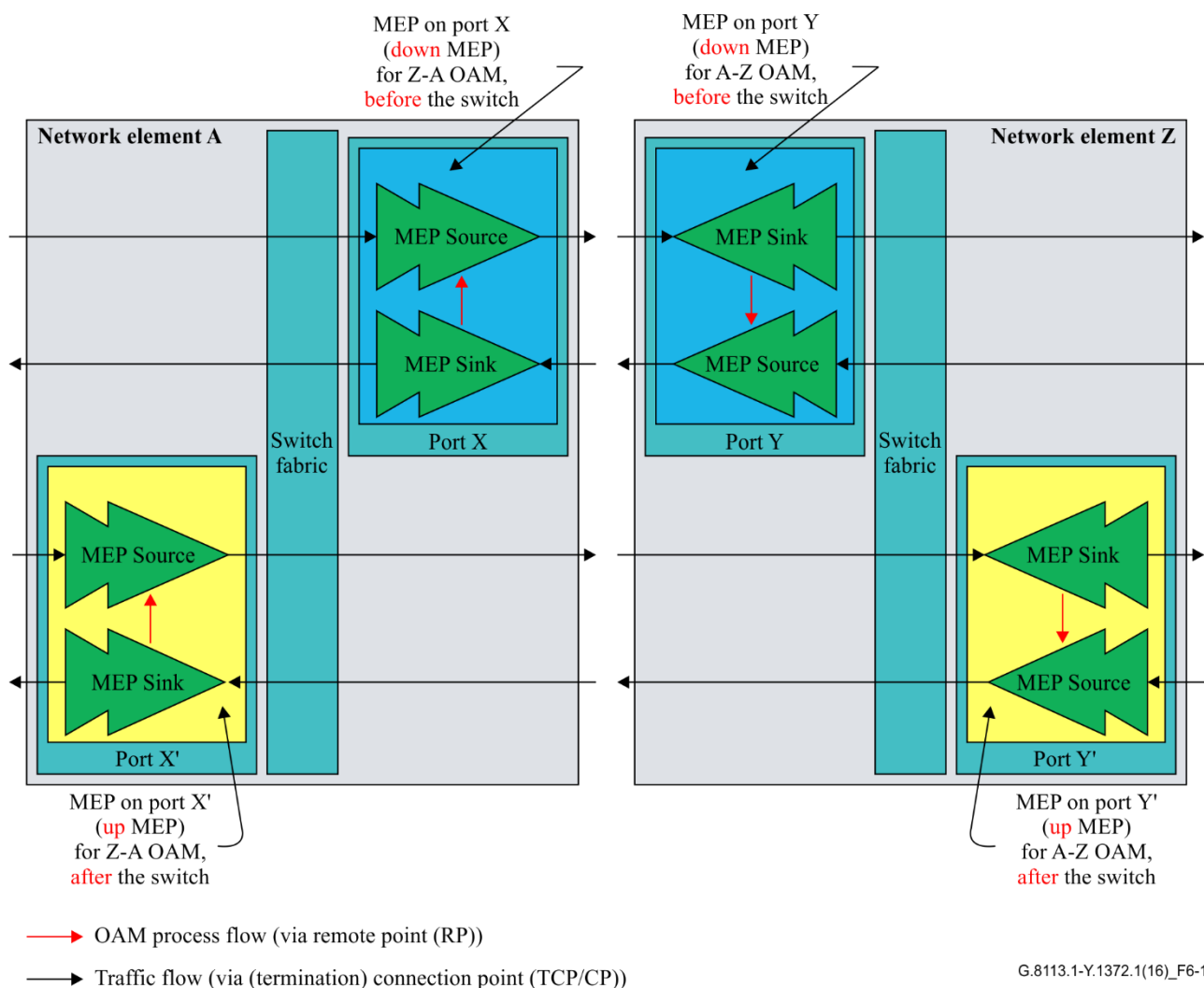


Figure 6-1 – Up/Down MEPs

In Figure 6-1, the MEP of the transport entity traversing IF port X of network element A (NE-A) is a Down MEP. Similarly, the MEP of IF port Y of NE-Z is also a Down MEP. Note that an IF port may support multiple transport entities. In Figure 6-1, 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 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, the MEP of the transport entity traversing IF port X' of NE-A is an Up MEP. Similarly, the MEP of IF 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 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 given in [IETF RFC 6371].

6.4 Maintenance entity group intermediate points

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

An MIP does not initiate unsolicited OAM packets, but may be addressed by OAM packets initiated by one of the MEPs of the MEG. An 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 (Rx) and process OAM packets addressed to them.

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

A per-node MIP is located somewhere within one node. There is no other MIP or MEP on the same MEG within the same node.

A per-IF MIP is located on a node IF, independently from the connection function.³ The MIP can be placed at the ingress IF or at the egress IF of any node along the MEG.

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

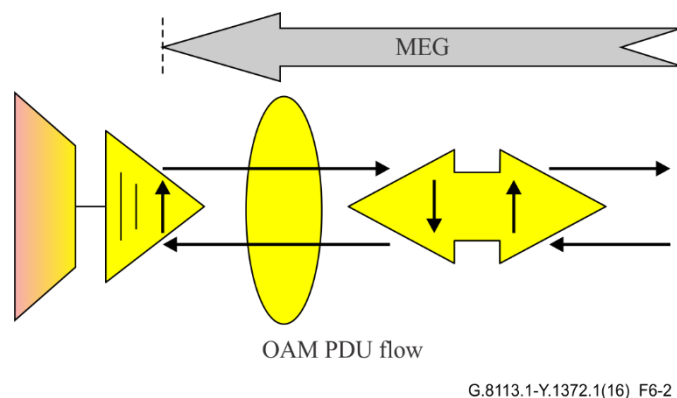


Figure 6-2 – Per-interface Up MEP and MIP in a node at the edge of an MEG

An intermediate node within an MEG can either:

- support a per-node MIP (i.e., a single MIP per node in an unspecified location within the node);
- support per-IF 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], an 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].

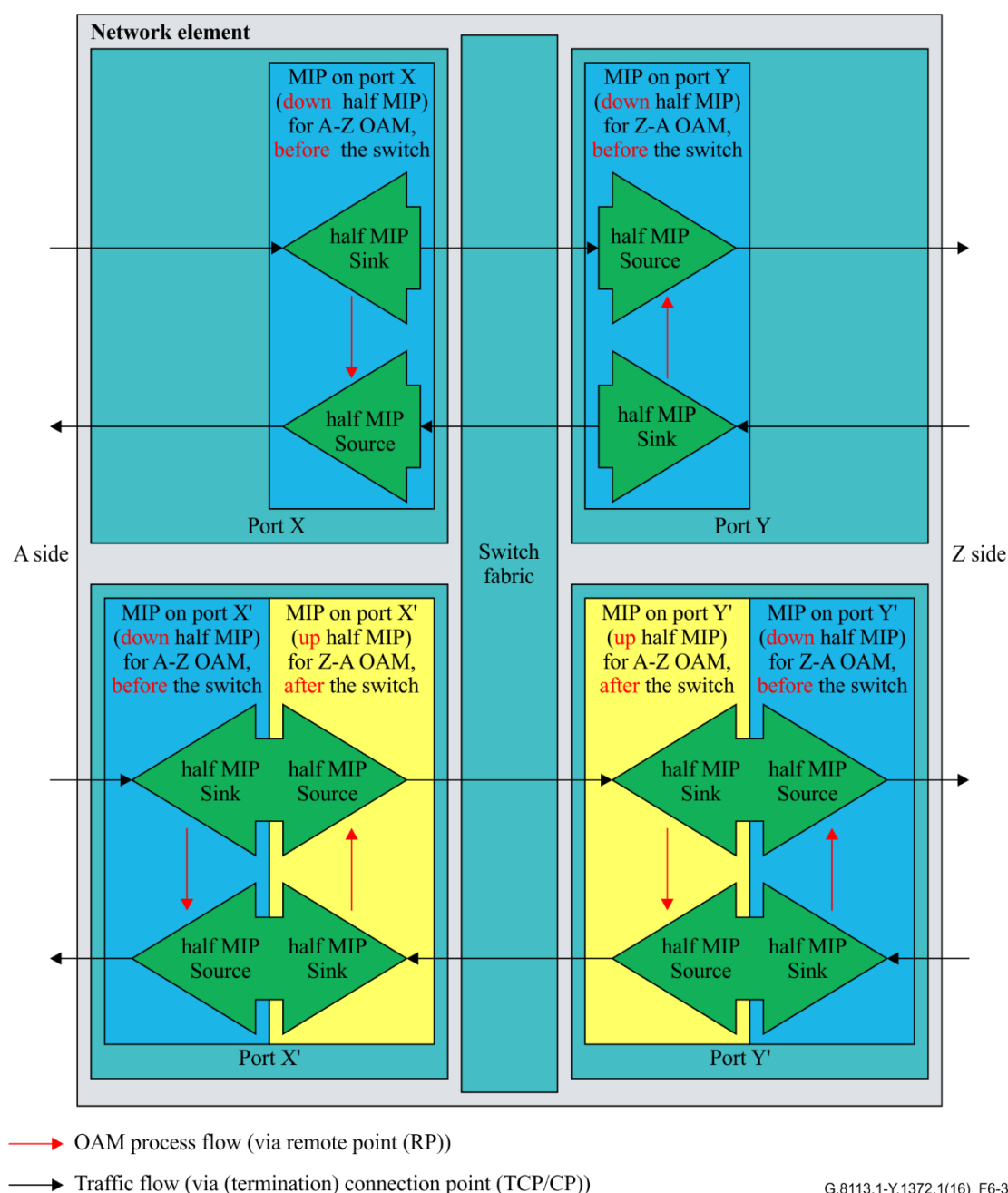


Figure 6-3 – Up/Down half MIPs

In Figure 6-3, MIP_{AX} is on IF port X on the A-side of the NE, MIP_{ZY} is on IF port Y on the Z-side of the NE, $MIP_{AX'}$ is on IF port X' on the A-side of the NE, and $MIP_{ZY'}$ is on IF 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 an MEP of an MEG that is either:

- defined in a layer network that is "below", i.e., that 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", i.e., that encapsulates and transports the sub-layer being referenced.

A server MEP can coincide with an MIP or an 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 NEs 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 user traffic packets. These OAM packets can be distinguished from the user traffic packets by using the generic associated channel (G-ACh) and the G-ACh label (GAL) constructs, as specified in [IETF RFC 5586].

The G-ACh is a generic associated control channel mechanism for Sections, 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/label switch routers (LERs/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 Generic associated channel

The 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 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 Generic associated channel label

A 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, data communication channel (DCC), automatic protection switching (APS)] 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 format of the GAL is specified in clause 8.1 in alignment with [IETF RFC 5586].

NOTE – Using a 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 can be used with PWs.

7.2 OAM functions specification

See Table 7-1.

Table 7-1 – OAM functions

Application	OAM function	
Fault management	Proactive	Continuity check and connectivity verification (CC/CV)
		Remote defect indication (RDI)
		Alarm indication signal (AIS)
		Client signal fail (CSF) ^a
	On-demand	Connectivity verification (CV)
		Route tracing (RT)
		Diagnostic test (DT)
		Locked signal (LCK) ^b
Performance management	Proactive	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)	
	Experimental (EXP)	
^a Client signal fail (CSF) is called client failure indication (CFI) in [IETF RFC 5860].		
^b Locked signal (LCK) is called lock reporting in [IETF RFC 5860].		

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 (So) MEP sends continuity check/connectivity verification (CC/CV) OAM packets periodically at the configured rate. The sink (Sk) 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 CV defects are also detected by this function:

- a) Mismatch (MMG): unintended connectivity between two MEGs.
- b) Unexpected MEP (UNM): unintended connectivity within the MEG with a UNM.

The following misconfiguration defect is also detected by this function:

- i) Unexpected periodicity (UNP): 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 fault management, performance monitoring and protection switching. An MEP periodically transmits the proactive CC/CV OAM packet at the configured transmission period. In transport networks, the following default transmission periods are defined:

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

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 an MEP to communicate to its peer MEPs that a signal fail condition exists. When an MEP detects a signal fail condition, it sends an RDI to its peer MEPs.

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

7.2.1.1.3 Alarm indication

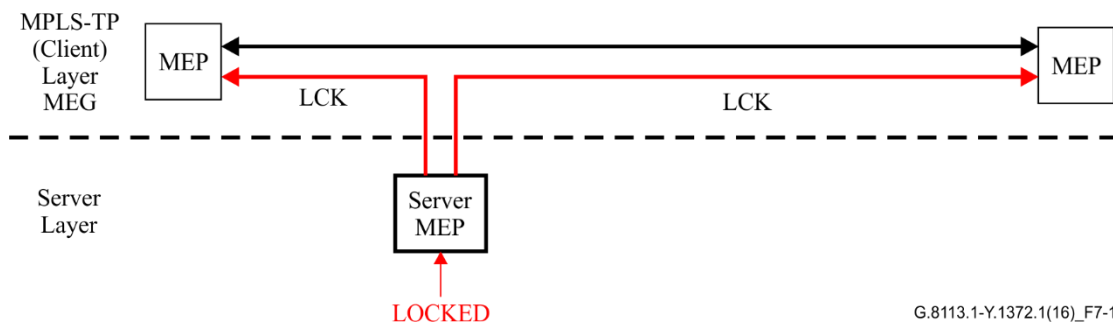
The alarm indication (AI) function is mainly used to suppress alarms following detection of defect conditions at the server (sub-)layer. When a server MEP asserts LOC or signal fail, it sets a flag that results in generation of OAM packets with alarm indication signal (AIS) information that are forwarded 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 an MEP is the out-of-service diagnostic test (DT), 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-Y.1372.1(16)_F7-1

Figure 7-1 – Example of locked signal 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 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 an MEP and a specific MIP. When the on-demand CV function is invoked on an 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 DT function is used to perform DTs, such as bandwidth throughput, packet loss and bit errors estimation by sending OAM DT 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 DT packets are sent to realize this function.

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

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

NOTE 2 – When the in-service test is performed, the DT packets can impact the data traffic.

When the DT function is invoked on an MEP, a test signal generator associated with the MEP can transmit (Tx) OAM DT 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 1 min.

When an MEP receives OAM DT packets, it examines them to ensure that they are valid. If the receiving MEP is configured for the DT function, the test signal detector associated with the MEP detects bit errors from the pseudo-random bit sequence (PRBS) 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 an MEP to discover the ordered sequence of MIPs (if any) and MEP(s) within an MEG.

The RT OAM function can be implemented using the loopback message (LBM) OAM PDU with the Discovery ingress/node MEP/MIP or the Discovery egress MEP/MIP TLVs in the target MEP/MIP identifier (ID) TLV that 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 (LM) function is for performance-monitoring purposes. It is performed continuously and its result is used to verify the performance of the connection against the service level agreement (SLA). This function is used to measure packet loss on a connection. To perform the LM function, 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 LMs, 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 LMs.

NOTE – For an 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 LMs contribute to near-end severely errored seconds (near-end SESs) and far-end SESs, respectively, which together contribute to unavailable time, in a manner similar to [ITU-T G.826] and described in [ITU-T G.7710].

7.2.2.1.2 Proactive delay measurement

The proactive delay measurement (DM) function is for performance-monitoring purposes. It is performed continuously and its result is used to verify the performance of the connection against the SLA. This function is used to measure packet delay (PD) and packet delay variation (PDV) on a connection. The DM function can be performed by two methods: one-way DM and two-way DM.

To perform the proactive DM function, the MEP periodically sends OAM packets with DM information (such as timestamps) to its peer MEP. It also expects to receive packets with DM information from its peer MEP. PD and PDV measurements are derived from the DM information in the DM packets. The PD and PDV summary statistics will be reported for performance monitoring.

7.2.2.2 On-demand OAM functions for performance monitoring

7.2.2.2.1 On-demand loss measurement

The on-demand LM function is for maintenance purposes. 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 packet 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 LMs, but the measurements do not contribute to the SES and unavailable time of the connection.

For an 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 DM function is for maintenance purposes. 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 PD and PDV on a connection. The DM function can be performed by two methods: one-way DM and two-way DM.

When an MEP is invoked to perform the on-demand DM function, 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. PD and 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 communications

APS communications allow MPLS-TP nodes to exchange protection switching control via the 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 G-ACh.

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

NOTE – MPLS-TP MCC and SCC are described 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 VS functionality is not expected across different vendors' equipment.

The protocol design allows different VS protocols to be distinguished or separated from standard protocols and experimental protocols, as well as from other VS protocols.

The specific application of VS 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 EXP functionality is not expected across different administrative domains.

The protocol design allows different EXP protocols to be distinguished or separated from standard protocols and VS protocols, as well as from other EXP protocols.

The specific application of EXP 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.

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 – Generic associated channel label 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].

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

The 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 an ACH is described in Figure 8-2.

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
0001				Version (0)				Reserved (0)								Channel Type															

Figure 8-2 – Associated channel header 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 the Internet Assigned Numbers Authority [b-IANA G-ACh prms]. The values used in this Recommendation are described in Table 8-1.

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 ITU-T Carrier Code- (ICC-)based MIP and MEP identifiers. MPLS-TP also supports IP-based formats for MIP and MEP identifiers.⁴ 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 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.

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

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

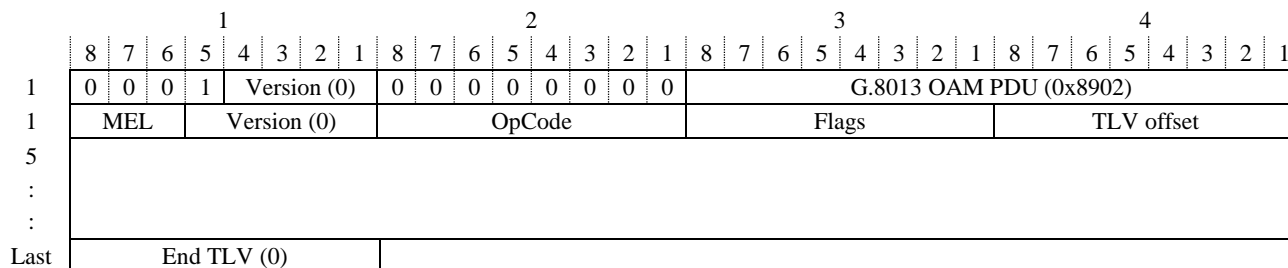


Figure 8-3 – Common OAM packet format based on [ITU-T G.8013]

The MEL field is set to the only valid binary value "111".

~~The MEG level (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 G.8013]. The values used in this Recommendation are described in Table 8-2.

Table 8-2 – OpCode values

OpCode value	OAM PDU type	OpCode relevance for MEPs/MIPs
1	CCM	MEPs
3	LBM	MEPs and MIPs (CV)
2	LBR	MEPs and MIPs (CV)
33	AIS	MEPs
35	LCK	MEPs
37	TST	MEPs
39	APS	MEPs
43	LMM	MEPs
42	LMR	MEPs
45	1DM	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.

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
36	Test ID TLV

8.2.1 Continuity check message

The continuity check message (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:

- Proactive CC (section 2.2.2 of [IETF RFC 5860]).
- Proactive CV (section 2.2.3 of [IETF RFC 5860]).
- Proactive RDI (section 2.2.9 of [IETF RFC 5860]).
- Proactive packet LM (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 proactive CV, the CCM packet contains a globally unique identifier of the source MEP, which is the combination of a globally unique MEG ID with an MEP ID that is unique within the scope of the MEG.

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 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.

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 CV (section 2.2.3 of [IETF RFC 5860]);
- Bidirectional in-service or out-of-service DT (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

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.

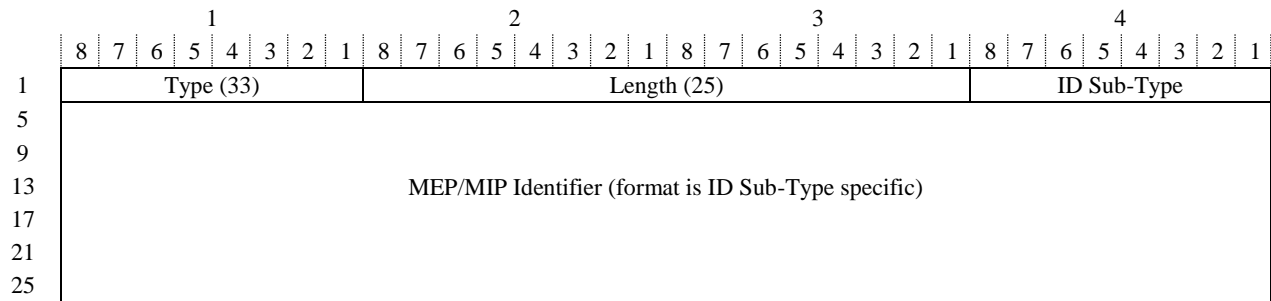


Figure 8-6 – Target MEP/MIP ID TLV format

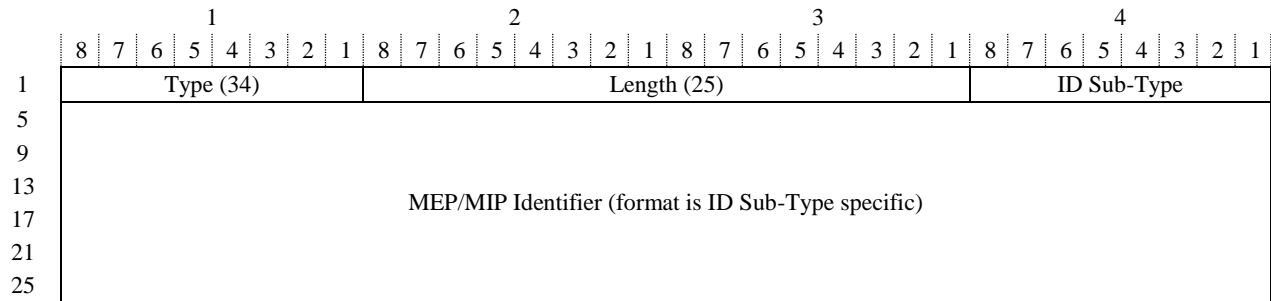


Figure 8-7 – Replying MEP/MIP ID TLV format

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	MEP ID	2 bytes
0x03	MIP ID	16 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) to discover 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.

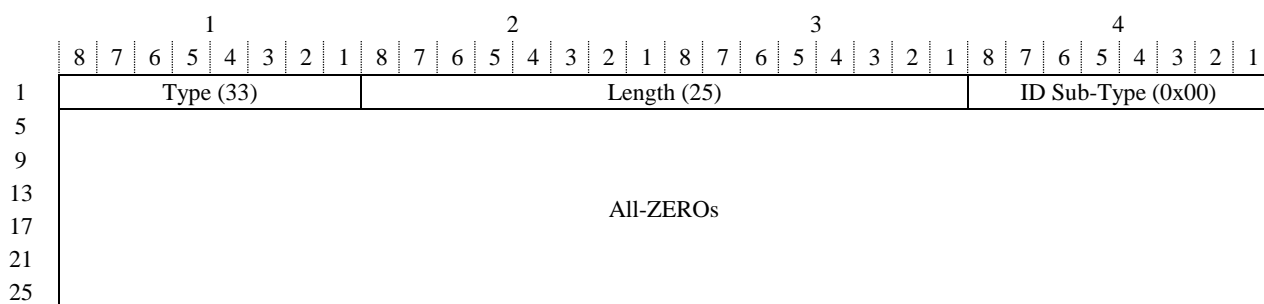


Figure 8-8 – Target MEP/MIP ID TLV format for Discovery ingress/node MEP/MIP

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

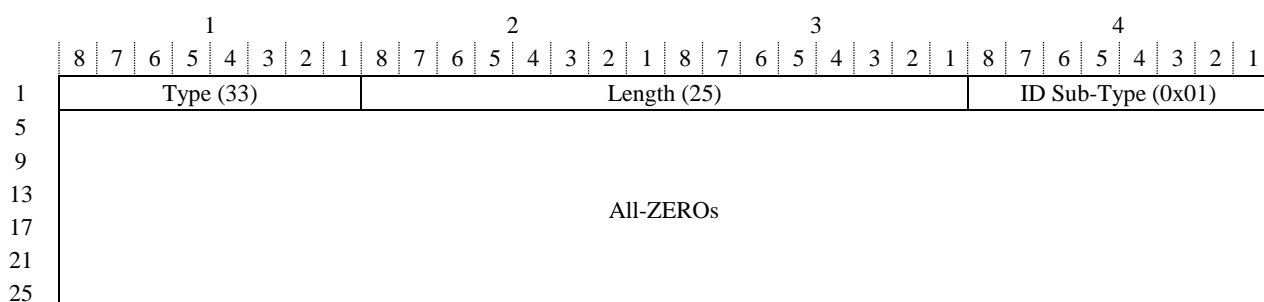


Figure 8-9 – Target MEP/MIP ID TLV format for Discovery egress MEP/MIP

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

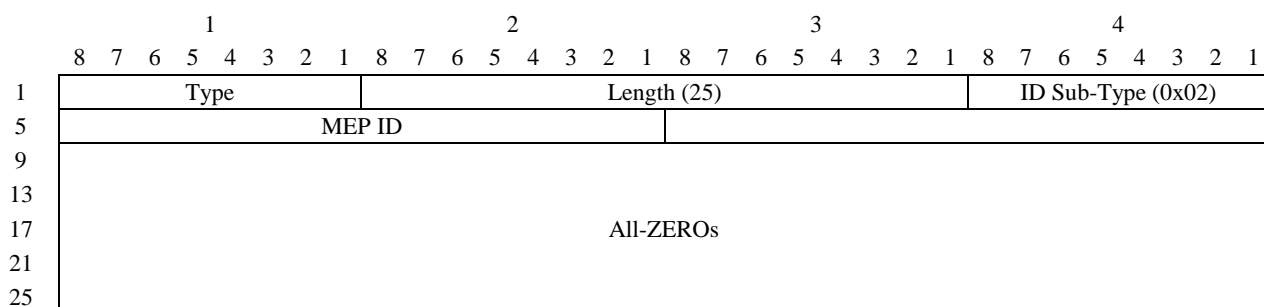


Figure 8-10 – Target or replying MEP/MIP ID TLV format for MEP ID

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 MIP ID is shown in Figure 8-11.

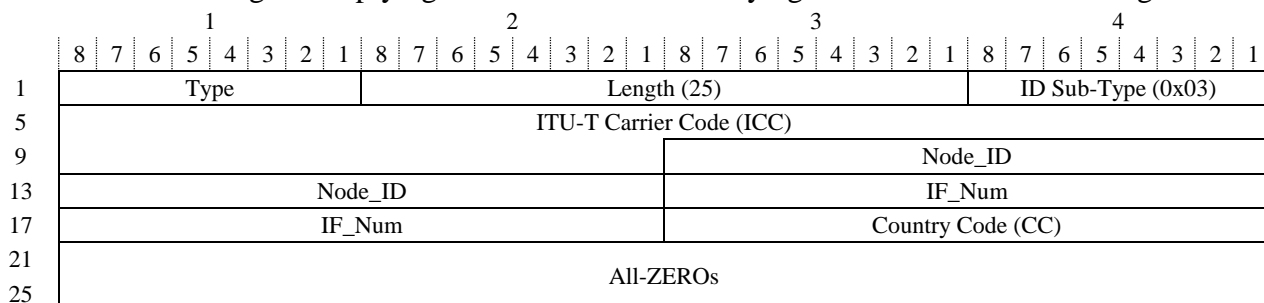


Figure 8-11 – Target or replying MEP/MIP ID TLV format for MIP ID

The ICC is a code assigned to a network operator or service provider and maintained by [ITU-T M.1400]. The ITU field in Figure 8-11 consists of between one and six 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-IF 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.

The country code (alpha-2) is a string of two upper case letters (i.e., A-Z). The country code format is specified 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.

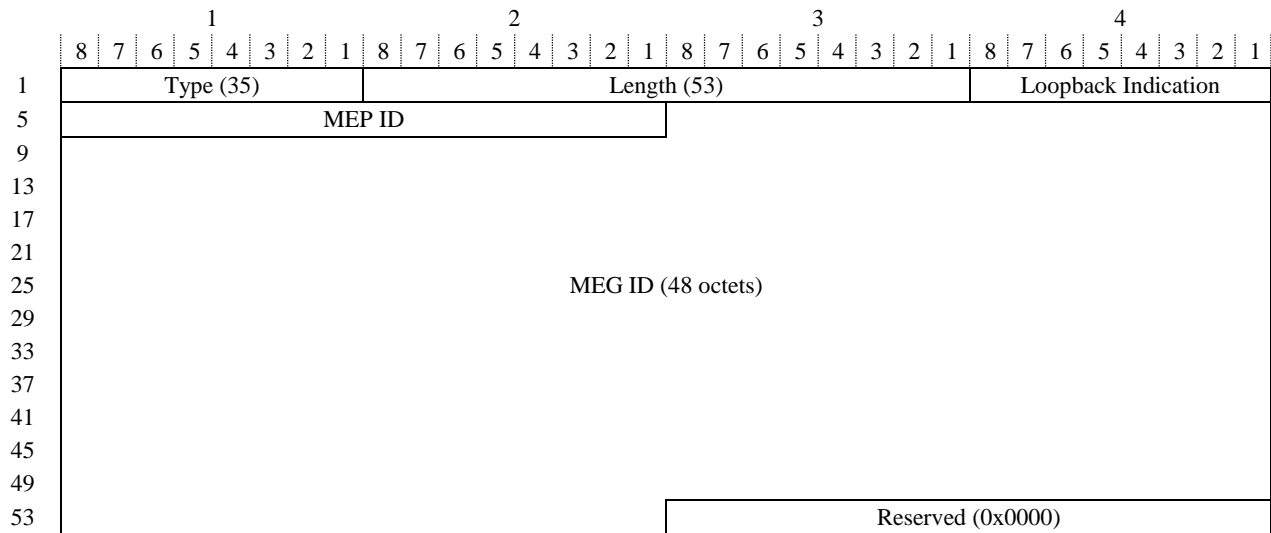


Figure 8-12 – Requesting MEP ID TLV format

The globally unique identifier for an MEP can be provided by the combination of a globally unique MEG ID with an 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 an 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

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 the 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

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

The test (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 DT 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

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 proactive packet LM 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

The one-way delay measurement (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 proactive packet 1DM 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) 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 proactive packet two-way DM 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

The client signal fail (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 (CFI) 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

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

The experimental OAM message/experimental OAM reply (EXM/EXR) PDUs support the requirement to support 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

The vendor-specific OAM message/vendor-specific OAM reply (VSM/VSR) PDUs support the requirement for support of MPLS-TP VS 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

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

8.4 Signalling communication channel

The packet format for carrying signalling communication (i.e., SCC packets) over an ACH, and associated procedures, are described 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 those defined in [ITU-T G.8013] and [ITU-T G.8021] that are technology-independent.

9.1.1 Continuity check message 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 per-hop behaviour (PHB) configured by the operator:

- The MEL field is set ~~as specified in clause 8.2. 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 fail. 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 LM 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 LM 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 LM 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 the CCM PDU is transmitted with a value of the transmission period configured at the transmitting MEP.

When an MEP receives a CCM OAM packet, it checks the various fields (see Figure 8-19 of [ITU-T G.8021] with the MI MEL set as specified in clause 8.2). The following defects are detected as described in clause 6.1 of [ITU-T G.8021]: loss of continuity defect (dLOC); unexpected MEL defect (dUNL); ⁵ 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 proactive LM 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 LM, an MEP periodically transmits CCM packets with the following information elements: TxFCf, RxFCb, TxFCb, as described above.

When configured for proactive LM, an MEP, upon receiving a CCM packet, uses the following values to make near-end and far-end LMs:

- Received CCM packet 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 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.

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

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

NOTE 2 – For dual-ended LM (based on CCM), the counters do not count OAM packets that can be used for on-demand functions (e.g., LBM/LBR, LMM/LMR, DMM/DMR, IDM and TST) as well as OAM packets used only for proactive functions by termination functions (e.g., CCM). However, proactive OAM packets used by adaptation functions (e.g., APS) are counted. This behaviour is aligned with the Ethernet dual-ended LM as defined in clause 8.2 of [ITU-T G.8013].

9.1.2 Loopback message/loopback reply procedures

The 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.

⁵ ~~The dUNL defect will not be raised if the default value for MEL is used.~~

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 can be mutually agreed between the user of the LBM/LBR function and the user of the service.

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

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

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

- The MEL field is set ~~as specified in clause 8.2~~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 PRBS (2³¹-1) 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 that is copied from the last received LBM PDU.
- The Version field is set to the value that 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 that is copied from the last received LBM PDU.
- The TLV Offset field is set to the value that is copied from the last received LBM PDU.
- The Transaction field is set to the value that is copied from the last received LBM PDU.
- The target MEP/MIP ID and originator MEP ID fields are set to the value that is copied from the last received LBM PDU.
- The Optional TLV field is set to the value that 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 that 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 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 ~~as specified in clause 8.2 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 configured 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 a (valid) AIS packet, it detects the alarm indication signal defect (dAIS), as described in clause 6.1 of [ITU-T G.8021].

~~When an 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 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 ~~as specified in clause 8.2 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 configured 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 a (valid) LCK packet, it detects the dLCK defect as described in clause 6.1 of [ITU-T G.8021].

~~When an 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 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.

An 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 an 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 as specified in clause 8.2~~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 that 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 PRBS ($2^{31}-1$) as specified in clause 5.8 of [ITU-T O.150] and all '0' pattern.
- The end TLV field is set to all-ZEROes.

9.1.6 Loss measurement message/loss measurement reply procedures

The LMM/LMR function allows measurement of on-demand and proactive 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 proactive LM is enabled at an 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 ~~as specified in clause 8.2~~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 (proactive or on-demand) of the operation (see clause 9.12.2 of [ITU-T G.8013]).
- 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 single-ended LM (based on LMM/LMR), the counters do not count OAM packets that can be used for on-demand functions (e.g., LBM/LBR, LMM/LMR, DMM/DMR, 1DM and TST). Instead, OAM packets used by termination functions for proactive functions (e.g., CCM) as well as proactive OAM packets used by adaptation functions (e.g., APS) are counted. This behaviour is aligned with the Ethernet single-ended LM as defined in clause 8.2 of [ITU-T G.8013].

~~An LMM packet with a valid MEL is considered to be a valid LMM packet. An LMM packet is discarded if not valid. Whenever a valid LMM packet is received by an MEP (i.e., the receiving MEP), an LMR packet is generated and transmitted by the receiving MEP to the requesting MEP. 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 that is copied from the last received LMM PDU.
- The Version field is set to the value that 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 that is copied from the last received LMM PDU.
- The TLV Offset field is set to the value that is copied from the last received LMM PDU.
- The TxFCf field is set to the value that 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 the 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 copied from the LMM PDU.

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

- Received LMR packet 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 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.

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

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

9.1.7 One-way delay measurement procedures

The 1DM function allows measurement of on-demand and proactive one-way PD and PDV for point-to-point unidirectional or bidirectional MPLS-TP connections.

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

When on-demand or proactive packet DM is enabled at an 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 ~~as specified in clause 8.2~~to the configured value (see clause 8.2).
- The Version field is set to 1 (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 LSB bit (Type) of the Flags field (see clause 8.2) is set according to the type (proactive 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.
- Optional TLVs: If present, a Test ID TLV or a data TLV, with configurable size, in octets, can be present. When a Test ID TLV is included in this area, it is recommended that the Test ID TLV be put first (prior to data TLV). The value part of the data TLV is unspecified.
- 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 PD. A 1DM packet with a valid MEL is considered to be a valid 1DM packet.~~

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. The one-way PD is calculated as:

$$PD = RxTime_f - TxTimeStamp_f$$

PDV measurement is calculated based on the difference between subsequent PDmeasurements.

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 DMM/DMR function allows measurement of on-demand and proactive two-way PD and PDV 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 proactive two-way PD measurement is enabled at an 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 ~~as specified in clause 8.2~~to the configured value (see clause 8.2).
- The Version field is set to 1 (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 (proactive or on-demand) of the operation (see clause 9.15.2 of [ITU-T G.8013]).
- The TLV Offset field is set to 32 (see clause 8.2.8).
- The TxTimeStamp_f field is set to the timestamp at the transmission of the DMM packet. The format of TxTimeStamp_f is equal to the TimeRepresentation format in [IEC 61588].
- The Reserved field is set to all-ZEROes.
- Optional TLVs: If present, a Test ID TLV or a data TLV, with configurable size, in octets, can be present. When a Test ID TLV is included in this area, it is recommended that the Test ID TLV be put first (prior to data TLV). The value part of the data TLV is unspecified.
- 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 MEL is considered to be a valid DMM packet. A DMM packet is discarded if not valid. Whenever a valid DMM packet is received by an MEP (i.e., the receiving MEP), a DMR packet is generated and transmitted by the receiving MEP to the requesting MEP. 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 that is copied from the last received DMM PDU.
- The Version field is set to the value that 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 that is copied from the last received DMM PDU.
- The TLV Offset field is set to the value that is copied from the last received DMM PDU.
- The TxTimeStamp_f field is set to the value that is copied from the last received DMM PDU.
- The RxTimeStamp_f field is optional. If used, it is set to the timestamp of DMM reception. If not used, it is set to all-ZEROes.
- The TxTimeStamp_b 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.
- Optional TLVs: If present in the DMM PDU, these are copied from the DMM PDU. The order of optional TLVs is preserved.
- The end TLV is copied from the DMM PDU.

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

$$PD = RxTimeeb - TxTimeStampf$$

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 PD (i.e., excluding the local processing time at the receiving MEP) is calculated to be:

$$PD = (RxTimeeb - TxTimeStampf) - (TxTimeStampb - RxTimeStampf)$$

PDV measurement is calculated based on the difference between subsequent PD measurements.

9.1.9 Client signal fail 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 if 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 an MEP, upon receiving signal fail information from its client layer. Detection rules for CSF events are by definition client-specific and outside the scope of this Recommendation. Upon receiving a signal fail indication from its client layer, the MEP can immediately start transmitting periodic CSF packets. An 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 an MEP. The period of CSF generation is client layer specific and outside the scope of this Recommendation.

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

The clearing conditions of a 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.

An 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, 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 an 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 an 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 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, 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

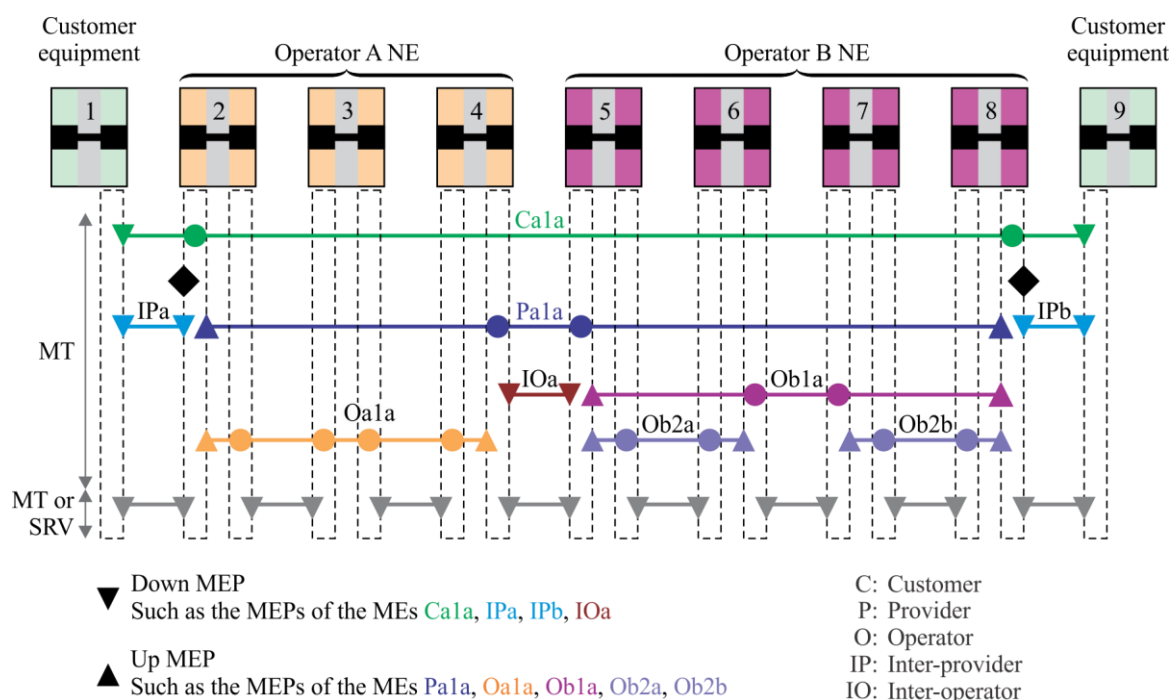
MPLS-TP network scenarios

(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 MEL~~, of nested MEGs for customer, provider and operator roles, in which 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 IF, not per node. Upside-down triangles (▼) indicate Down MEPs and normal triangles (▲) indicate Up MEPs.



G.8113.1-Y.1372.1(16)_FI.1

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 MEGs (Oa1a and Ob1a).
- Segment operator MEGs in operator B's network (Ob2a and Ob2b).
- UNI_C to UNI_N MEGs (IPa and IPb) between the customer and provider.
- Inter-operator MEG (IOa).

Bibliography

- [b-ITU-T G.808.2] Recommendation ITU-T G.808.2 (2013), *Generic protection switching – Ring protection*.
- [b-ITU-T M.20] Recommendation ITU-T M.20 (1992), *Maintenance philosophy for telecommunication networks*.
- [IETF RFC 3031] IETF RFC 3031 (2001), *Multiprotocol Label Switching Architecture*.
- [b-IETF RFC 5654] IETF RFC 5654 (2009), *Requirements of an MPLS Transport Profile*.
- [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 Transport Profile (MPLS-TP) Identifiers*.
- [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 G-ACh prms] IANA (2016). *Generic Associated Channel (G-ACh) Parameters*. Los Angeles, CA: Internet Assigned Numbers Authority.

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT- GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	Y.4800–Y.4899
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks, Internet of Things and smart cities
Series Z	Languages and general software aspects for telecommunication systems