INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2013-2016

STUDY GROUP 15

TD 400 (PLEN/15)

English only

Original: English

Question(s): 10/15 22 June - 3 July 2015

TD

Source: Editors G.8113.2/Y.1372.2

Title: Draft revised Recommendation ITU-T G.8113.2/Y.1372.2 (for Consent, 3 July 2015)

Abstract

This document provides draft revised G.8113.2/Y.1372.2, incorporating the amendment into the main body of the text and updating some references that have been published in the time since the publication of the amendment. The changes shown with red change bars are those that result from bringing the text of the amendment into the main body. Changes to update references (not updated in the amendment) are shown with blue change bars.

Contact: Tom Huber
Coriant GmbH & Co.
Germany
Tel: +1 630 798 6625
Email: tom.huber@coriant.com

Draft revised Recommendation ITU-T G.8113.2/Y.1372.2

Operations, administration and maintenance mechanisms for MPLS-TP networks using the tools defined for MPLS

Summary

Recommendation ITU-T G.8113.2/Y.1372.2 specifies operations, administration and maintenance (OAM) mechanisms based on the tools defined for MPLS for data-plane OAM in multi-protocol label switching transport profile (MPLS-TP) networks. It also specifies the MPLS-TP OAM packet formats, syntax and semantics of MPLS-TP OAM packet fields. The OAM mechanisms defined in this Recommendation assume common forwarding of the MPLS-TP user packets and MPLS-TP OAM packets.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T G.8113.2/Y.1372.2	2012-11-20	15
1.1	ITU-T G.8113.2/Y.1372.2 (2012) Amd.1	2013-08-29	15
2.0	ITU-T G.8113.2/Y.1372.2 (2015)		15

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/.

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	4
6	Functional components	5
6.1	Maintenance entity (ME)	5
6.2	Maintenance end group (MEG)	5
6.3	MEG end points (MEPs)	5
6.4	MEG intermediate points (MIPs)	7
7	OAM functions	9
7.1	Identification of OAM packets from user-traffic packets	9
7.2	OAM functions specification	9
8	OAM PDU formats	14
8.1	Continuity check and connectivity verification	14
8.2	Transport plane loopback formats	14
8.3	Alarm indication signal (AIS) and link down indication (LDI) formats	14
8.4	Lock instruct (LI) and lock report (LKR) formats	14
8.5	Test (TST) formats	14
8.6	Loss measurement message/loss measurement reply (LMM/LMR) formats	15
8.7	One-way delay measurement (1DM) formats	15
8.8	Two-way delay measurement measure/delay measurement reply (DMM/DMR) formats	15
8.9	Client signal fail (CSF) formats	15
8.10	Experimental message/experimental reply (EXM/EXR) formats	15
8.11	Management communication channel and signalling communication channel formats	15
9	MPLS-TP OAM procedures	15
9.1	Continuity check and connectivity verification	15
9.2	Transport plane loopback procedures	15
9.3	Alarm indication signal (AIS) and link down indication (LDI) procedures	16
9.4	Lock indication (LI) and lock report (LKR) procedures	16
9.5	Test (TST) procedures	16

9.6 Loss measurement message/loss measurement reply (LMM/LMR) procedures 16

Page

9.7 One-way delay measurement (1DM) procedures 16
9.8 Two-way delay measurement message/delay measurement reply (DMM/DMR) procedures 16
9.9 Client signal fail (CSF) procedures 16
Appendix I – MPLS-TP network scenarios 17
I.1 Maintenance entity group (MEG) nesting example 17
Appendix II – Requirements traceability 18
Bibliography 21

Draft revised Recommendation ITU-T G.8113.2/Y.1372.2

Operations, administration and maintenance mechanisms for MPLS-TP networks using the tools defined for MPLS

1 Scope

This Recommendation specifies operations, administration and maintenance (OAM) mechanisms based on the tools defined for MPLS in IETF Requests for Comments, for data-plane OAM in multi-protocol label switching transport profile (MPLS-TP) networks to meet the MPLS-TP OAM requirements defined in [IETF RFC 5860]. It also specifies the MPLS-TP OAM packet formats, syntax and semantics of MPLS-TP OAM packet fields.

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

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

2 References

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

[ITU-T G.805] Recommendation ITU-T G.805 (2000), *Generic functional architecture of transport networks*.

[ITU-T G.806] Recommendation ITU-T G.806 (~~2004~~2012), *Characteristics of transport equipment – Description methodology and generic functionality*.

[ITU-T G.7712] Recommendation ITU-T G.7712 (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*, plus Amendment 1 (2006) and Amendment 2 (2010).

[ITU-T G.8110.1] Recommendation ITU-T G.8110.1/Y.1370.1 (2011), *Architecture of MPLS Transport Profile (MPLS-TP) layer networks*.

[ITU-T G.8121.2] Recommendation ITU-T G.8121.2/Y.1381.2 (2013), *Characteristics of MPLS-TP equipment functional blocks supporting G.8113.2/Y.1372.2*.

[IETF RFC 3692] IETF RFC 3692 (2004), *Assigning Experimental and Testing Numbers Considered Useful*.

---

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

[IETF RFC 4379] IETF RFC 4379 (2006), *Detecting Multi-Protocol Label Switched (MPLS) Data Plane Failures*.

[IETF RFC 5226] IETF RFC 5226 (2008), *Guidelines for Writing an IANA Considerations Section in RFCs*.

[IETF RFC 5586] IETF RFC 5586 (2009), *MPLS Generic Associated Channel*.

[IETF RFC 5654] IETF RFC 5654 (2009), *Requirements of an MPLS Transport Profile*.

[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 OAM in MPLS Transport Networks*.

[IETF RFC 5881] IETF RFC 5881 (2010), *Bidirectional Forwarding Detection (BFD) for IPv4 and IPv6 (Single Hop)*.

[IETF RFC 5884] IETF RFC 5884 (2010), *Bidirectional Forwarding Detection (BFD) for MPLS Label Switched Paths (LSPs)*.

[IETF RFC 5921] IETF RFC 5921 (2010), *A Framework for MPLS in Transport Networks*.

[IETF RFC 6215] IETF RFC 6215 (2011), *MPLS Transport Profile User-to-Network and Network-to-Network Interfaces*.

[IETF RFC 6370] IETF RFC 6370 (2011), *MPLS Transport Profile (MPLS-TP) Identifiers*.

[IETF RFC 6371] IETF RFC 6371 (2011), *Operations, Administration and Maintenance Framework for MPLS-based Transport Networks*.

[IETF RFC 6374] IETF RFC 6374 (2011), *Packet Loss and Delay Measurement for MPLS Networks*.

[IETF RFC 6375] IETF RFC 6375 (2011), *A Packet Loss and Delay Measurement Profile for MPLS-based Transport Networks*.

[IETF RFC 6423] IETF RFC 6423 (2011), *Using the Generic Associated Channel Label for Pseudowire in the MPLS Transport Profile (MPLS-TP)*.

[IETF RFC 6426] IETF RFC 6426, *MPLS On-Demand Connectivity Verification and Route Tracing*.

[IETF RFC 6427] IETF RFC 6427, *MPLS Fault Management Operations, Administration, and Maintenance (OAM)*.

[IETF RFC 6428] IETF RFC 6428, *Proactive Connectivity Verification, Continuity Check and Remote Defect Indication for the MPLS Transport Profile*.

[IETF RFC 6435] IETF RFC 6435, *MPLS Transport Protocol Lock Instruct and Loopback Functions*.

[IETF RFC 6923] IETF RFC 6923, *MPLS Transport Protocol (MPLS-TP) Identifiers Following ITU-T Conventions*.

3 Definitions

This Recommendation introduces some terminology which 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 elsewhere:

3.1.1 defect: [ITU-T G.806]

3.1.2 failure: [ITU-T G.806]

3.1.2 MPLS transport profile [b-ITU-T G.8113.1]: A set of multi-protocol label switching (MPLS) functions used to support packet transport services and network operations.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

1DM One-way Delay Measurement
A Adaptation function
ACH Associated Channel Header
AIS Alarm Indication Signal
BFD Bidirectional Forwarding Detection
C Customer
CC Continuity Check
CSF Client Signal Fail
CV Connectivity Verification
DM Delay Measurement
DMM Delay Measurement Message
DMR Delay Measurement Reply
DT Diagnostic Test
EXM Experimental OAM Message
EXP Experimental
EXR Experimental OAM Reply
G-ACh Generic Associated Channel
GAL G-ACh Label
IANA Internet Assigned Numbers Authority
IETF Internet Engineering Task Force
IP Internet Protocol
LCK Locked Signal
LER Label Edge Router
LI Lock Instruct
LKR Lock Report

LM	Loss Measurement
LMM	Loss Measurement Message
LMR	Loss Measurement Reply
LOC	Loss Of Continuity
LSP	Label Switched Path
LSR	Label Switch Router
MCC	Management Communication Channel
ME	Maintenance Entity
MEG	Maintenance Entity Group
MEL	MEG Level
MEP	MEG End Point
MIP	MEG Intermediate Point
MMG	Mismerge
MPLS	Multi-Protocol Label Switching
MPLS-TP	MPLS Transport Profile
N	Network
NE	Network Element
OAM	Operation, Administration & Maintenance
OTN	Optical Transport Network
PDU	Protocol Data Unit
PSN	Packet Switched Network
PW	Pseudowire
RDI	Remote Defect Indication
RFC	Request for Comments
SCC	Signalling Communication Channel
SDH	Synchronous Digital Hierarchy
Sk	Sink
So	Source
SPME	Sub-Path Maintenance Element
SSF	Server Signal Fail
TCM	Tandem Connection Monitoring
TTL	Time To Live
UNI	User Network Interface
UNM	UNexpected MEP
UNP	UNexpected Period

5 Conventions

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

6 Functional components

6.1 Maintenance entity (ME)

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

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

6.2 Maintenance ~~end~~ entity group (MEG)

A maintenance entity group (MEG) is the 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 element (SPME), as described in section 3.2 of [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 were previously in between becomes an intermediate node for the SPME.

TCMs can nest but not overlap.

6.3 MEG end points (MEPs)

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

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

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

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

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

Per-interface MEP is a MEP which is located on a specific interface within the node. In particular a per-interface MEP is called an "Up MEP" or a "Down MEP" depending on its location relative to the connection function[2], which is shown in Figure 6-1.

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

---

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

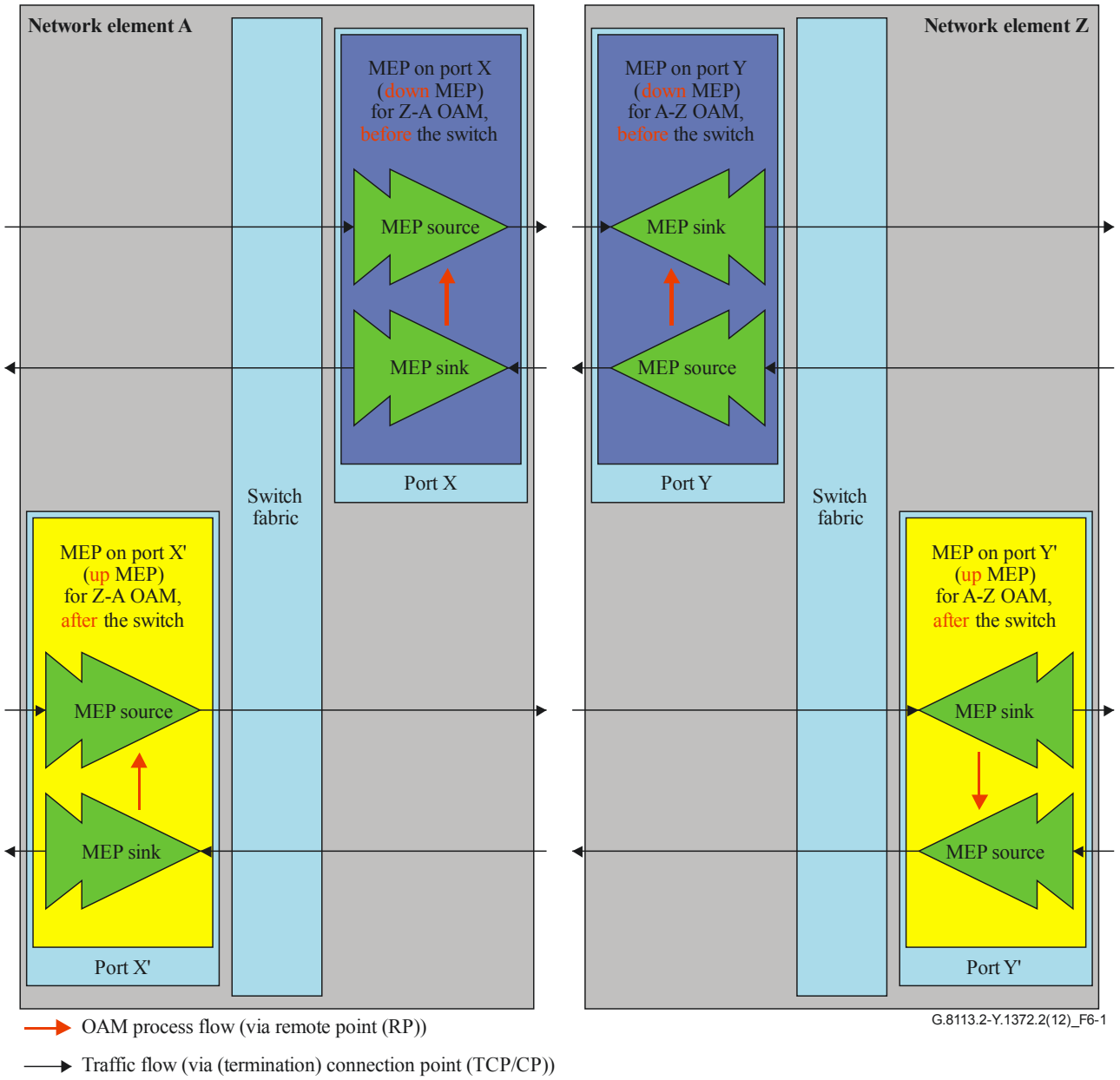

Figure 6-1 – Up/Down MEPs

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

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

therefore the connection function of NE-Z is involved in this OAM flow. Similarly, the OAM packets from $MEP_{ZY'}$ to $MEP_{AX'}$ will be processed by $MEP_{AX'}$ and transit the connection function of NE-A.

More details are described in section 3.3 of [IETF RFC 6371].

6.4 MEG intermediate points (MIPs)

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

A MIP does not initiate unsolicited OAM packets, but may be addressed by OAM packets initiated by one of the MEPs of the MEG. A MIP can generate OAM packets only in response to OAM packets that are sent on the MEG to which it belongs.

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

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

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

Per-interface MIP is a MIP which is located on a node interface, independently from the connection function[3]. The MIP can be placed at the ingress interface or at the egress interface of any node along the MEG.

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

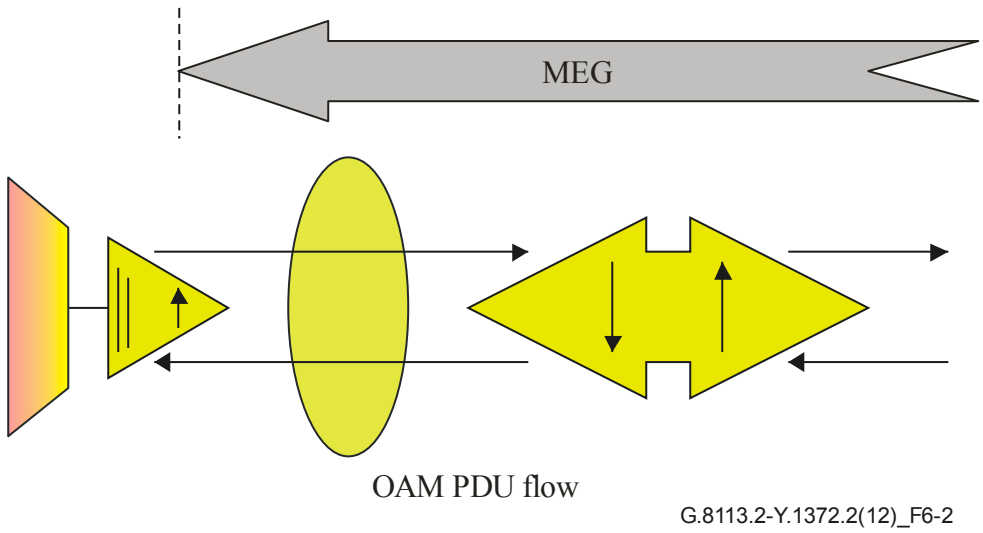

Figure 6-2 – Per-interface Up MEP and MIP in a node at the edge of a MEG

An intermediate node within a MEG can either:

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

– support per-interface MIPs (i.e., two MIPs per node, one on each side of the forwarding engine, for co-routed point-to-point bidirectional connections).

---

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

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

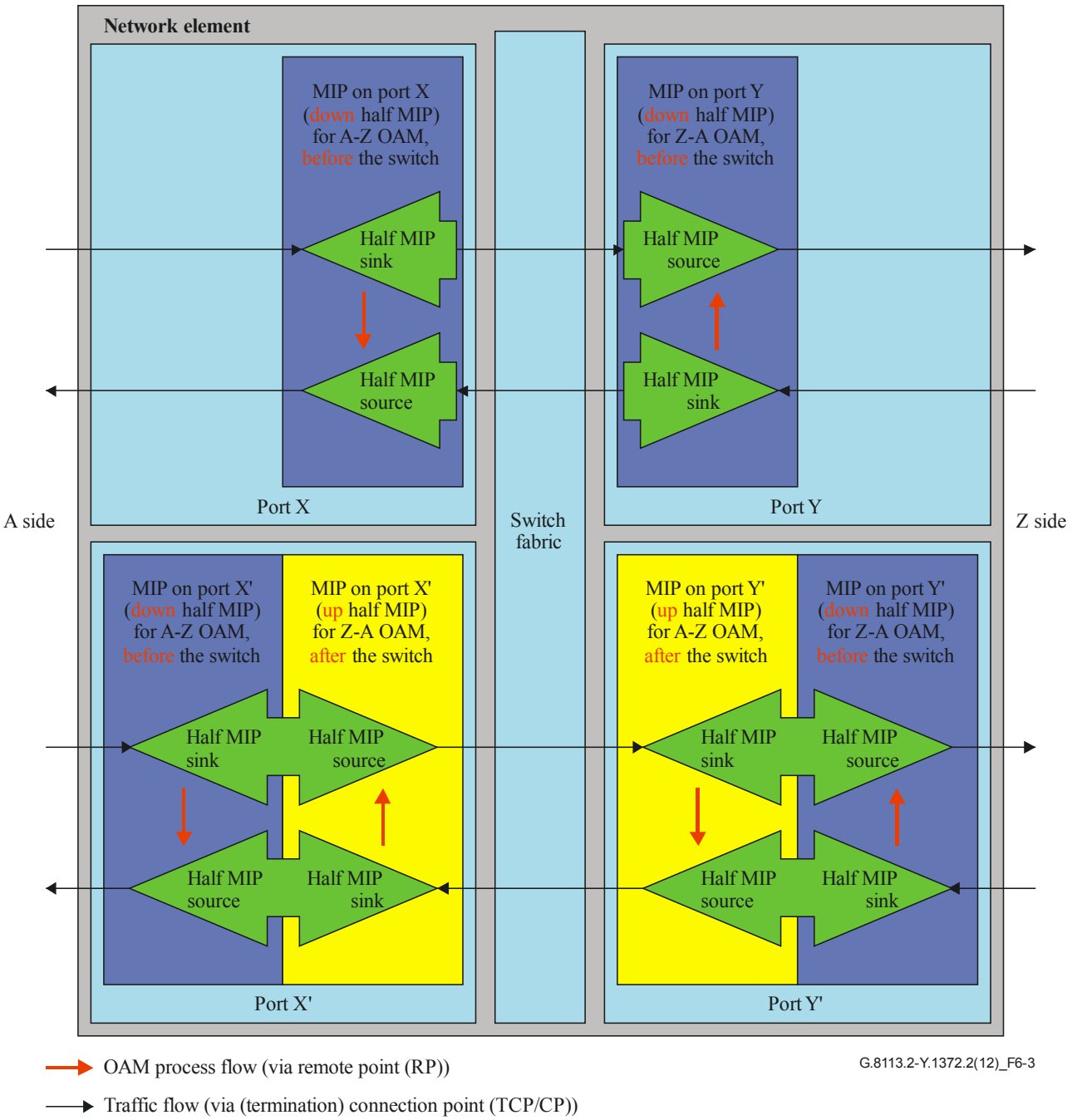

Figure 6-3 – Up/Down half MIPs

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

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

More details are described in section 3.4 of [IETF RFC 6371].

7 OAM functions

The requirements for MPLS-TP OAM are specified in [IETF RFC 5654] and [IETF RFC 5860]. Appendix II contains a table showing the mapping between those requirements and the OAM functions described in this clause.

7.1 Identification of OAM packets from user-traffic packets

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

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

The GAL is a label-based exception mechanism to alert label edge routers/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 G-ACh

The operation of the MPLS-TP generic associated channel (G-ACh) is described in section 3.6 of [IETF RFC 5921] and is defined in [IETF RFC 5586].

As defined in [IETF RFC 5586], Channel Types for the associated channel header (ACH) are allocated through the IETF consensus process. The IETF consensus process is defined in [IETF RFC 5226], where it is termed "IETF Review."

A number of experimental G-ACh channel types are provided for experimental use in product development without allocation; refer to [IETF RFC 3692] for further detail.

NOTE – The use of G-ACh channel types other than in accordance with the IANA allocation [b-IANA PW Reg] is not recommended.

7.1.2 GAL

The use of the GAL is defined in section 4.2 of [IETF RFC 5586] and section 3 of [IETF RFC 6423].

7.2 OAM functions specification

Table 7-1 provides a summary of MPLS-TP OAM functions, protocols used, and the corresponding IETF RFCs. All control messages are carried using G-ACh. Functional processing of these messages is described in [~~b-~~ITU-T G.8121.2].

Table 7-1 – OAM functions

Fault management (FM) OAM functions			
Proactive FM OAM functions	OAM functions	Protocol definitions	IETF RFCs
	Continuity check (CC)	Bidirectional Forwarding Detection (BFD) extensions	[IETF RFC 6428]
	Connectivity verification (CV)	Bidirectional Forwarding Detection (BFD) extensions	[IETF RFC 6428]
	Remote defect indication (RDI)	Flag in CC/CV message	[IETF RFC 6428]
	Alarm indication signal (AIS)	AIS message	[IETF RFC 6427]
	Link down indication (LDI)	Flag in AIS message	[IETF RFC 6427]
	Lock report (LKR)	LKR message	[IETF RFC 6427]
On-demand FM OAM functions	Connectivity verification (CV)	LSP Ping extensions	[IETF RFC 6426]
	Route trace (RT)	LSP Ping extensions	[IETF RFC 6426]
	Transport plane loopback	Management control	[IETF RFC 6435]
	Lock indication (LI)	In-band Lock Instruct messages	[IETF RFC 6435]
Performance management (PM) OAM functions			
Proactive PM OAM functions and **On-demand PM OAM functions**	OAM functions	Protocol definitions	IETF RFCs
	Packet loss measurement (LM)	LM and DM query messages	[IETF RFC 6374] [IETF RFC 6375]
	Packet delay measurement (DM)	LM and DM query messages	
	Throughput measurement	Supported by LM	
	Delay variation measurement	Supported by DM	

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 CC/CV OAM functions are supported by the use of bidirectional forwarding detection (BFD) control packets.

The source MEP sends BFD control packets periodically at the configured rate. The sink MEP monitors for the arrival of these BFD control packets at the configured rate and detects the defect of loss of continuity (LOC).

The following connectivity verification defects are detected using the CV message:

a) Mismerge (MMG): unintended connectivity between two MEGs

b) Unexpected MEP (UNM): unintended connectivity within the MEG with an unexpected MEP.

The following misconfiguration defect is detected using the continuity check/connectivity verification (CC/CV) function:

a) Unexpected period (UNP): BFD control packets are received with a period field value that is different from the configured BFD control packet rate.

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

a) 3.33ms: default transmission period for protection switching application (transmission rate of 300 packets/second)

b) 100ms: default transmission period for performance monitoring application (transmission rate of 10 packets/second)

c) 1s: default transmission period for fault management application (transmission rate of 1 packet/second).

CV messages use a default transmission period of 1s.

Other CC/CV transmission periods are not precluded. For a discussion of periodicity see [IETF RFC 6371].

For further information on BFD procedures for proactive continuity check and connectivity verification, see section 3 of [IETF RFC 6428].

7.2.1.1.2 Remote defect indication

Remote defect indication (RDI) is defined in this Recommendation for bidirectional connections and is associated with proactive CC/CV activation. RDI for other connection types is for further study.

The RDI OAM function is supported by the use of BFD control packets.

RDI is an indicator that is transmitted by a MEP to communicate to its peer MEP that a signal fail condition exists. When a MEP detects a signal fail condition, it sets the Diagnostic field of the BFD control packets it is transmitting to its peer MEP to one of the values defined in section 5 of [IETF RFC 6428]. The particular value depends on the cause of the signal fail condition.

Detailed procedures for setting diagnostic codes in BFD messages are described in sections 3.2 and 3.7 of [IETF RFC 6428].

7.2.1.1.3 Alarm indication

This function is used to suppress downstream alarms following detection of defect conditions at the server layer/sublayer. The detection of LOC or server signal fail (SSF) by a server layer/sublayer MEP causes the generation of OAM packets with alarm indication signal (AIS) information that are forwarded to the downstream MEP(s) in the client layer/sublayer, which allows the suppression of secondary alarms (LOC, etc.) in the client layer/sublayer.

A link down indication (LDI) flag in the AIS message is set when a failure is detected in the server layer.

Procedures for sending AIS messages and setting the LDI flag (L-Flag) are defined in sections 2.2, 2.3, and 6 of [IETF RFC 6427].

7.2.1.1.4 Locked signal

The lock report (LKR) function is used to communicate to the client layer/sublayer MEPs the administrative locking of a server layer/sublayer MEP and consequential interruption of data traffic forwarding in the client layer/sublayer. It allows a client layer/sublayer MEP receiving packets with locked signal (LCK) information to differentiate between a defect condition and an administrative locking action at the server layer/sublayer MEP. Details of sending LKR messages are described in [IETF RFC 6427].

7.2.1.1.5 Client signal fail (CSF)

For further study.

7.2.1.2 On-demand OAM functions for fault management

7.2.1.2.1 Connectivity verification

LSP-Ping [IETF RFC 4379] is an OAM mechanism for MPLS LSPs. [IETF RFC 6426] describes extensions to LSP-Ping to include MPLS-TP LSPs. It describes how LSP-Ping can be used for on-demand connectivity verification (CV) and route tracing functions for MPLS-TP LSPs required in [IETF RFC 5860] and specified in [IETF RFC 6371].

In certain MPLS-TP deployment scenarios, an IP address scheme may not be available or it may be preferred to use some form of non-IP encapsulation for on-demand CV and route tracing. In such scenarios, on-demand CV and/or route-tracing functions are operated without IP addresses, using the ACH as specified in sections 1.3 and 3.3 of [IETF RFC 6426].

Procedures for on-demand CV are defined in sections 1.2, 1.3, and 3 of [IETF RFC 6426]. Procedures for on-demand route tracing are defined in sections 1.2, 1.3, and 4 of [IETF RFC 6426]

7.2.1.2.2 Diagnostic test

For further study.

7.2.1.2.3 Transport plane loopback

The transport plane loopback function is controlled by the management plane. For further information see section 4 of [IETF RFC 6435].

7.2.1.2.4 Lock indication

The lock indication function uses the lock instruct message defined in [IETF RFC 6435] to communicate from a MEP that has been locked by the management or control function to its peer that the peer should enter the administratively locked state.

The management or control function is expected to lock all MEPs in the MEG.

7.2.2 OAM functions for performance monitoring

7.2.2.1 Proactive OAM functions for performance monitoring

The protocol for MPLS-TP loss and delay measurement functions is defined in [IETF RFC 6374] as profiled in [IETF RFC 6375]. These drafts specify how to measure:

- Packet loss
- Packet delay
- Packet delay variation
- Throughput

There are two closely-related protocols, one for packet loss measurement (LM) and one for packet delay measurement (DM). These protocols have the following characteristics and capabilities:

- The same LM and DM protocols can be used for both proactive and on-demand measurement.
- The LM and DM protocols use a simple query/response model for bidirectional measurement that allows a single node to measure the loss or delay in both directions.
- The LM and DM protocols use query messages for unidirectional loss and delay measurement. The measurement can either be carried out at the downstream node(s) or at the upstream node if an out-of-band return path is available.
- The LM and DM protocols do not require that the transmit and receive interfaces be the same when performing bidirectional measurement.
- The LM protocol can be used to measure channel throughput as well as packet loss.
- The DM protocol supports varying the measurement message size in order to measure delays associated with different packet sizes.

Throughput and packet delay variation measurements are derived from LM and DM, respectively.

7.2.2.1.1 Proactive loss measurement

The theory of loss measurement is described in section 2.1 of [IETF RFC 6374].

The protocol procedures are defined in section 4.1 of [IETF RFC 6374].

The profile applicable to MPLS-TP is defined in section 2 of [IETF RFC 6375].

7.2.2.1.2 Proactive delay measurement

The theory of delay measurement is described in section 2.3 of [IETF RFC 6374].

The protocol procedures are defined in section 4.2 of [IETF RFC 6374].

The profile applicable to MPLS-TP is defined in section 3 of [IETF RFC 6375].

7.2.2.2 On-demand OAM functions for performance monitoring

The on-demand OAM functions for performance monitoring are identical to the proactive OAM performance monitoring functions.

7.2.2.2.1 On-demand loss measurement

The on-demand loss measurement function is identical to the proactive loss measurement function defined in 7.2.2.1.1.

7.2.2.2.2 On-demand delay measurement

The on-demand delay measurement function is identical to the proactive delay measurement function defined in 7.2.2.1.2.

7.2.2.3 Throughput and packet delay measurement

Throughput and packet delay measurement are derived from LM and DM, respectively.

7.2.2.3.1 Throughput measurement

In service throughput can be derived using LM as described in section 2.3 of [IETF RFC 6374]. Out of service throughput measurement is for further study.

7.2.2.3.2 Packet delay variation measurement

Packet delay variation can be derived using DM as described in section 2.5 of [IETF RFC 6374].

7.2.3 Other functions

7.2.3.1 Management communication channel/signalling communication channel

The management communication channel (MCC) and signalling communication channel (SCC) are defined in [IETF RFC 5718] and [ITU-T G.7712].

7.2.3.2 Vendor-specific OAM functions

Vendor-specific OAM functions are not supported in this Recommendation.

7.2.3.3 Experimental

A number of experimental G-ACh channel types are provided for product development. Use of these is defined in [IETF RFC 3692].

8 OAM PDU formats

The packet formats for MPLS-TP OAM are defined in the corresponding IETF RFCs as listed below. These formats use IP-based identifiers as specified in [IETF RFC 6370]. The use of ICC-based identifiers is for further study; see [~~b-~~IETF RFC ~~itu-t-identifiers~~6923].

8.1 Continuity check and connectivity verification

8.1.1 Bidirectional forwarding detection (BFD) message formats

The BFD message format is defined in [IETF RFC 5884]. Descriptions of carrying this message on an MPLS-TP LSP and appending TLVs to carry MEP identification are described in [IETF RFC 6428].

8.1.2 On-demand connectivity verification (CV) formats

The formats for on-demand CV are defined in [IETF RFC 6426]. Messages may be encapsulated as defined in section 3.2 (Using IP encapsulation over ACH) and in section 3.3 (Non-IP-based on-demand CV using ACH).

Although section 3.3 of [IETF RFC 6426] defines encapsulation for the case where IP addresses are not used, the identifiers defined for use in [IETF RFC 6426] are IP-based identifiers (as defined in [IETF RFC 6370] to the extent that they are compatible with values typically used by IP-based equipment.

Support for use of ICC-based identifiers is FFS.

8.2 Transport plane loopback formats

Because loopback is management controlled, there are no control message formats associated with this function

8.3 Alarm indication signal (AIS) and link down indication (LDI) formats

The AIS message format and LDI flag are defined in section 4 of [IETF RFC 6427].

8.4 Lock instruct (LI) and lock report (LKR) formats

The lock instruct message format is defined in section 5 of [IETF RFC 6435].

The lock report message format is defined in section 4 of [IETF RFC 6427].

8.5 Test (TST) formats

For further study.

8.6 Loss measurement message/loss measurement reply (LMM/LMR) formats

The loss measurement message/reply formats are defined in section 3.1 of [IETF RFC 6374].

The profile applicable to MPLS-TP is defined in section 2 of [IETF RFC 6375].

Note that loss and delay measurements may be combined as described in section 3.3 of [IETF RFC 6374].

8.7 One-way delay measurement (1DM) formats

The 1DM message formats are defined in section 3.2 of [IETF RFC 6374].

The profile applicable to MPLS-TP is defined in section 3 of [IETF RFC 6375].

Note that loss and delay measurements may be combined as described in section 3.3 of [IETF RFC 6374].

8.8 Two-way delay measurement measure/delay measurement reply (DMM/DMR) formats

The delay measurement message formats are defined in section 3.2 of [IETF RFC 6374].

The profile applicable to MPLS-TP is defined in section 3 of [IETF RFC 6375].

Note that loss and delay measurements may be combined as described in section 3.3 of RFC [IETF RFC 6374].

8.9 Client signal fail (CSF) formats

For further study.

8.10 Experimental message/experimental reply (EXM/EXR) formats

A number of experimental G-ACh channel types are provided for product development. Use of these is defined in [IETF RFC 3692].

8.11 Management communication channel and signalling communication channel formats

The packet format for carrying management communication (i.e., management communication channel (MCC) packets) or signalling communication (i.e., signalling communication channel (SCC) packets) over an ACH and associated procedures are defined in [IETF RFC 5718]. The associated channel type assigned to this channel is maintained by IANA [b-IANA PW Reg]. The value assigned for MCC is 0x0001. The value assigned for SCC is 0x0002.

9 MPLS-TP OAM procedures

The procedures for MPLS-TP OAM are defined in the corresponding IETF RFCs.

9.1 Continuity check and connectivity verification

9.1.1 Bidirectional forwarding detection (BFD) message procedures

The BFD message format is defined in [IETF RFC 5884]. The procedures are based upon [IETF RFC 5881] as updated by [IETF RFC 6428].

9.1.2 On-demand connectivity verification (CV) procedures

The on-demand CV procedures are defined in section 3 of [IETF RFC 6426].

9.2 Transport plane loopback procedures

The loopback procedures are described in section 4 of [IETF RFC 6435].

9.3 Alarm indication signal (AIS) and link down indication (LDI) procedures

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 Fault OAM messages with the message type set to AIS until the aAIS consequent action is cleared. Procedures for sending MPLS Fault OAM can be found in [IETF RFC 6427].

It is recommended that AIS be generated once per second.

When a MEP receives an AIS message, it detects the dAIS defect as described in clause 6.1 of [~~b-~~ITU-T G.8121.2].

9.4 Lock indication (LI) and lock report (LKR) procedures

The lock instruct procedures are defined in section 6 [IETF RFC 6435].

The lock report procedures are defined in section 5 of [IETF RFC 6427].

9.5 Test (TST) procedures

For further study

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

The loss measurement procedures are defined in section 4.1 of [IETF RFC 6374].

The profile applicable to MPLS-TP is defined in section 2 of [IETF RFC 6375].

9.7 One-way delay measurement (1DM) procedures

The one-way delay measurement procedures are defined in section 4.2 of [IETF RFC 6374].

The profile applicable to MPLS-TP is defined in section 3 of [IETF RFC 6375].

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

The two-way delay measurement procedures are defined in section 4.2 of [IETF RFC 6374].

The profile applicable to MPLS-TP is defined in section 3 of [IETF RFC 6375].

9.9 Client signal fail (CSF) procedures

For further study

10 Security

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

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

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

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

Appendix I

MPLS-TP network scenarios

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

I.1 Maintenance entity group (MEG) nesting example

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

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

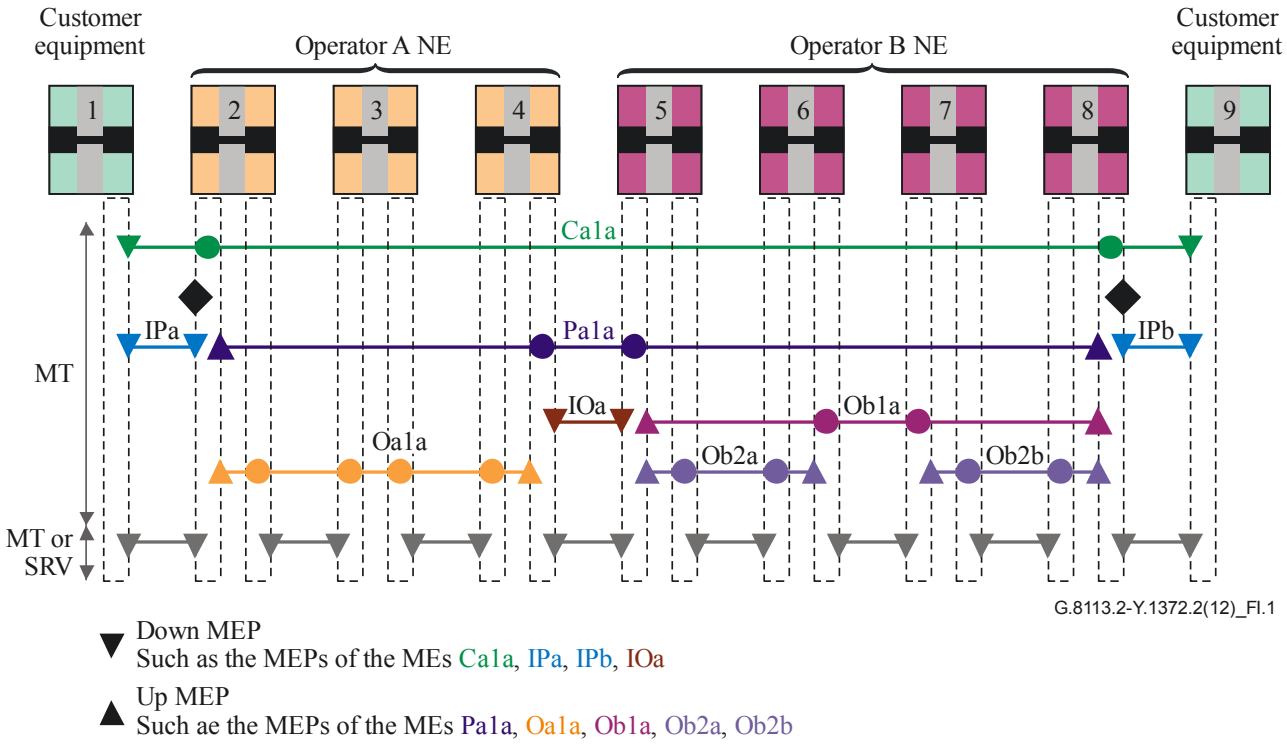

Figure I.1 – Example of MEG nesting

– UNI_C to UNI_C customer ME (Ca1a).
– UNI_N to UNI_N provider ME (Pa1a).
– End-to-end operator MEs (Oa1a and Ob1a).
– Segment operator MEs in operator B's network (Ob2a and Ob2b).
– UNI_C to UNI_N MEs (IPa and IPb) between the customer and provider.
– Inter-operator ME (IOa).

Appendix II

Requirements traceability

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

Table II.1 is provided to assist the reader in evaluating the suitability of this Recommendation for his application environment.

This table provides a quick reference table to show which MPLS-TP OAM functional requirements are addressed in this Recommendation. It is expected that the table will be updated as necessary whenever this Recommendation is revised or amended.

The requirements listed in this table are drawn from [IETF RFC 5654] and [IETF RFC 5860] which were developed jointly by ITU-T and IETF.

Table II.1 – Requirements traceability

Source document	Source section	Requirement number	Level of support	Solution clause(s)	Notes
[IETF RFC 5654]	2.1	1	Full	All	Note 1
[IETF RFC 5654]	2.1	2	Full	All	Note 1
[IETF RFC 5654]	2.1	3	Full	All	Note 1
[IETF RFC 5654]	2.1	4	Partial	8	Note 2
[IETF RFC 5654]	2.1	5	Full	All	
[IETF RFC 5654]	2.1	6	Partial	All	Note 9
[IETF RFC 5654]	2.1	7	Full	All	
[IETF RFC 5654]	2.1	8	FFS		
[IETF RFC 5654]	2.1	15	Partial	All	Note 10
[IETF RFC 5654]	2.1	17	FFS		
[IETF RFC 5654]	2.1	21	Partial		Note 11
[IETF RFC 5654]	2.1	22	Full	All	Note 1
[IETF RFC 5654]	2.1	23 B	Partial		Note 4
[IETF RFC 5654]	2.1	23 C	Full	All	
[IETF RFC 5654]	2.1	27	Full	All	
[IETF RFC 5654]	2.1	28	Full	All	
[IETF RFC 5654]	2.1	29	Full	7.2.1.1.1, 7.2.1.2.1, 8.1, 9.1	
[IETF RFC 5654]	2.3	36	FFS	8	
[IETF RFC 5654]	2.3	44	Partial	7.2.1.2.1, 7.2.2.1.1	Note 3
[IETF RFC 5654]	2.3	45	Partial	7.2.1.2.1, 7.2.2.1.1	Note 3
[IETF RFC 5654]	2.3	46	Full	7.1	
[IETF RFC 5654]	2.5	56 A	Partial	All	Note 11

Table II.1 – Requirements traceability

Source document	Source section	Requirement number	Level of support	Solution clause(s)	Notes
[IETF RFC 5654]	2.5	58	Full	7.2.1.1, 7.2.1.1.2, 7.2.1.1.3, 8.1.1, 9.1.1, 8.3, 9.3	
[IETF RFC 5654]	2.5.3	75	Partial	7.2.1.1.2, 7.2.1.1.3, 7.2.1.1.5	Note 4
[IETF RFC 5654]	2.5.4	88	FFS		Note 12
[IETF RFC 5654]	2.5.5	90 A	Partial	7.2.1.2.4	Note 5
[IETF RFC 5654]	2.5.5	90 B	FFS		
[IETF RFC 5860]	2		Partial	All	Notes 1, 11
[IETF RFC 5860]	2.1.1		Partial	All	Note 6
[IETF RFC 5860]	2.1.2		Full	All	
[IETF RFC 5860]	2.1.3		Full	7.1	
[IETF RFC 5860]	2.1.4		Partial	All	Note 6
[IETF RFC 5860]	2.1.5		Partial	All	Note 6
[IETF RFC 5860]	2.1.6		Partial	All	Note 7
[IETF RFC 5860]	2.2		Full	All	Note 8
[IETF RFC 5860]	2.2.1		Partial	7.2.1.1	Note 4
[IETF RFC 5860]	2.2.2		Partial	7.2.1.1.1, 8.1.1, 9.1.1	Note 9
[IETF RFC 5860]	2.2.3		Partial	7.2.1.2.1, 8.1.2, 9.1.2	Note 9
[IETF RFC 5860]	2.2.4		Full	7.2.1.2.1, 8.1.2, 9.1.2	
[IETF RFC 5860]	2.2.5		FFS		
[IETF RFC 5860]	2.2.6		Partial	7.2.1.2.4, 8.4, 9.4	Note 9
[IETF RFC 5860]	2.2.7		FFS		
[IETF RFC 5860]	2.2.8		Partial	7.2.1.1.3, 8.3, 9.3	Note 9
[IETF RFC 5860]	2.2.9		Full	7.2.1.1.2, 8.1.1, 9.1.1	
[IETF RFC 5860]	2.2.10		FFS		
[IETF RFC 5860]	2.2.11		Partial	7.2.2.1, 7.2.2.1.1, 7.2.2.2.1, 8.6, 9.6	Note 9

Table II.1 – Requirements traceability

Source document	Source section	Requirement number	Level of support	Solution clause(s)	Notes
[IETF RFC 5860]	2.2.12		Partial	7.2.2.1, 7.2.2.2.2, 8.7, 8.8, 9.7, 9.8	Note 9
[IETF RFC 5860]	3				Note 7
[IETF RFC 5860]	4		FFS		

NOTE 1 – RFCs that define MPLS-TP extensions constitute a subset of MPLS, are part of existing MPLS standards, and are inherently interoperable with MPLS.

NOTE 2 – Interworking between MPLS-TP OAM, as defined in this Recommendation, and OAM defined elsewhere is not explicitly defined in either this Recommendation, nor in any referenced RFC. Interfaces (internal and external) are thus not defined but evidence suggests that at least some degree of interworking is possible.

NOTE 3 – Currently referenced RFCs support connectivity verification and packet loss measurement. Packet corruption and/or reordering are not addressed in referenced RFCs and are FFS.

NOTE 4 – This version supports remote defect indication and alarm indication. Client signal fail is FFS.

NOTE 5 – This version supports lock instruct.

NOTE 6 – ICC (and Global ICC) format identifiers are FFS in this Recommendation.

NOTE 7 – Some requirements apply to implementation.

NOTE 8 – Experimental OAM function support is explicitly described in clause 7.2.3.3.

NOTE 9 – Point-to-multipoint support is FFS.

NOTE 10 – Separation of management and data planes is supported in MPLS, hence it is also supported in MPLS-TP. Separation of control and data planes is supported for MPLS-TP LSPs, but not for MPLS-TP PWs.

NOTE 11 – It is difficult to specify full support for requirements stating a need for "*similarity*".

NOTE 12 – It is unclear how the requirement – "*the management plane MUST allow the current protection status of all transport paths to be determined*" – applies to, or impacts on, OAM as defined in this Recommendation.

Bibliography

[b-ITU-T G.8113.1] Recommendation ITU-T G.8113.1/Y.1372.1 (2012), *Operations, administration and maintenance mechanism for MPLS-TP in packet transport networks.*

~~[b-ITU-T G.8121.2] Recommendation ITU-T G.8121.2/Y.1381.2 (2011), *Characteristics of MPLS-TP equipment functional blocks.*~~

~~[b-IETF RFC itu-t-identifiers] IETF Internet Draft draft-ietf-mpls-tp-itu-t-identifiers-06 (2012), *MPLS-TP Identifiers Following ITU-T Conventions*~~
~~http://tools.ietf.org/html/draft-ietf-mpls-tp-itu-t-identifiers-06~~

[b-IANA PW Reg] Internet Assigned Numbers Authority (IANA), Pseudowire Associated Channel Types, http://www.iana.org/assignments/pwe3-parameters/pwe3-parameters.xml#pwe3-parameters-10.

[b-IETF RFC 6941] IETF RFC 6941 (2013), *MPLS-TP Security Framework*

_____