

MPLS Working Group
Internet Draft
Intended status: Informational
Expires: April 2009

M. Vigoureux (Editor)
Alcatel-Lucent

D. Ward (Editor)
Cisco Systems, Inc.

M. Betts (Editor)
Nortel Networks

October 31, 2008

Requirements for OAM in MPLS Transport Networks
draft-vigoureux-mpls-tp-oam-requirements-01

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress".

The list of current Internet-Drafts can be accessed at
<http://www.ietf.org/ietf/1id-abstracts.txt>

The list of Internet-Draft Shadow Directories can be accessed at
<http://www.ietf.org/shadow.html>

This Internet-Draft will expire on April 31, 2009.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Abstract

This document lists the requirements for Operations, Administration and Maintenance functionality in MPLS networks that are used for packet transport services and network operations.

These requirements are derived from the set of requirements specified by ITU-T and first published in the ITU-T Supplement Y.Sup4 [5].

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC 2119](#) [1].

Table of Contents

1.	Introduction.....	3
1.1.	Terminology.....	3
1.2.	Definitions.....	4
1.3.	Context and Motivations.....	4
2.	OAM Requirements.....	5
2.1.	Architectural Requirements.....	6
2.2.	Functional Requirements.....	7
2.2.1.	General requirements.....	8
2.2.2.	Connectivity and Continuity Verification.....	8
2.2.3.	Client Failure Indication.....	8
2.2.4.	Remote Defect Indication.....	8
2.2.5.	Alarm Suppression.....	9
2.2.6.	Packet Loss.....	9
2.2.7.	Delay Measurement.....	9
2.2.8.	Route Determination.....	10
2.2.9.	Diagnostic.....	10
2.3.	Operational Requirements.....	10
2.4.	Performance Requirements.....	11
3.	Security Considerations.....	11
4.	Congestion Considerations.....	12
5.	IANA Considerations.....	12
6.	Acknowledgments.....	12
7.	References.....	13
7.1.	Normative References.....	13
7.2.	Informative References.....	13
	Authors' Addresses.....	13
	Contributing Authors' Addresses.....	14
	Intellectual Property Statement.....	15
	Disclaimer of Validity.....	16

1. Introduction

This document lists the requirements for Operations, Administration and Maintenance functionality in MPLS networks that are used for packet transport services and network operations.

1.1. Terminology

AC Attachment Circuit

CSF Client Signal Fail

FCAPS Fault, Configuration, Accounting, Performance, Security

LER Label Edge Router

LSP Label Switched Path

LSR Label Switching Router

ME Maintenance Entity

MEP Maintenance End Point

MIP Maintenance Intermediate Point

MP Maintenance Point

MS-PW Multi Segment Pseudowire

OAM Operations, Administration and Maintenance

PE Provider Edge

PSN Packet Switched Network

PW Pseudowire

SLA Service Level Agreement

SS-PW Single Segment Pseudowire

S-PE PW Switching Provider Edge

T-PE PW Terminating Provider Edge

TCME Tandem Connection Maintenance Entity

1.2. Definitions

In this document we refer to a fault as the inability of a function to perform a required action. This does not include an inability due to preventive maintenance, lack of external resources, or planned actions. See also ITU-T G.806 [3].

In this document we refer to a defect as the situation for which density of anomalies has reached a level where the ability to perform a required function has been interrupted. See also ITU-T G.806 [3].

In this document, we refer to MPLS Transport Profile (MPLS-TP) as the set of MPLS functions used to support packet transport services and network operations.

In this document we refer to a MPLS Section as a network segment between two LSRs that are immediately adjacent at the MPLS layer.

For definitions of OAM functional components such as Maintenance Point, Maintenance End Point and Maintenance Intermediate Point, please refer to [7].
Additional definitions can also be found in [8].

1.3. Context and Motivations

Important attributes of MPLS-TP are that

- o it is able to function regardless of which client signals are using its connectivity service or over which transmission media it is running. The client, transport network and server layers are, from a functional point of view, independent layer networks. That is, demarcation points exist between MPLS-TP and the client layer, and between MPLS-TP and the underlying server layer.
- o it provides means to commit to Service Level Agreements (SLAs) negotiated with customers, as well as means to monitor compliance with these SLAs.
- o it is consistent with existing transport network OAM models.

In the context of MPLS-TP, the rationale for OAM mechanisms are twofold as they can serve:

- o as a network-oriented mechanism (used by a transport network operator) to monitor his network infrastructure and to implement internal mechanisms in order to enhance the general behaviour and the level of performance of his network (e.g. protection mechanism in case of node or link failure). For example fault localization is typically associated to this use case.
- o as a service-oriented mechanism (used by a transport service provider) to monitor his offered services to end customers in order to be able to react rapidly in case of a problem and to be able to verify some of the SLA parameters (i.e. performance monitoring) negotiated with the end customer. Note that a transport service could be provided over several networks or administrative domains that may not be all owned and managed by the same transport service provider.

More generally, OAM is an important and fundamental functionality in transport networks as it contributes to:

- o the reduction of operational complexity and costs, by allowing efficient and automatic detection, localisation, handling, and diagnosis of defects, and by minimizing service interruptions and operational repair times.
- o the enhancement of network availability, by ensuring that defects, for example resulting in misdirected customer traffic are detected, diagnosed and dealt with before a customer reports the problem.
- o meet service and performance objectives, by running OAM functionality which allows SLA verification in a multi-maintenance domain environment and allows the determination of service degradation due to, for example, packet delay or packet loss.

This is achieved through the support of FCAPS functionality, as described in ITU-T M.3400 [2], itself relying on OAM related information.

2. OAM Requirements

This section lists the requirements by which the OAM functionality of MPLS-TP should abide. Some requirements for this application are similar to some of those listed in [RFC 4377](#) [6].

The requirements listed below may be met by one or more OAM protocols, the definition or selection of these protocols is outside

the scope of this document. However, the specified solution **MUST** inter-work with the existing MPLS and PW OAM protocols.

2.1. Architectural Requirements

OAM functions **SHOULD** be independent of the underlying tunnelling or point-to-point technology or transmission media.

OAM functions **SHOULD** be independent of the service a pseudowire may emulate.

The set of OAM functions operated on each Maintenance Entity **SHOULD** be independent one from another.

Note that independence should not be understood here in terms of isolation but in terms of separate running processes. There should be one OAM process running per Maintenance Entity but different OAM running processes could interact (e.g. alarm summarization).

OAM functionality **MAY** be deployed in a variety of environments. In some of these IP routing and forwarding capabilities are inherently present (e.g. IP/MPLS) and the OAM functionality **MUST** also support their use. Other deployment scenarios exist where IP routing and forwarding capabilities are not necessarily present (e.g. MPLS-TP). In these latter cases, the operation of OAM functions **MUST NOT** rely on IP routing and forwarding capabilities. Further, it is **REQUIRED** by this document that OAM interoperability is achieved across these environments. It is also **REQUIRED** by this document that the two above requirements are still met and still hold when interoperability is achieved.

Furthermore, in case OAM packets need to incorporate identification information of source and/or destination nodes, an IP addressing structure **MUST** be supported.

When MPLS-TP is run with IP routing and forwarding capabilities, all existing IP/MPLS OAM functionality (e.g. LSP-Ping, BFD and VCCV) **MUST** be able to operate seamlessly.

OAM functions **MUST** operate and be configurable even in the absence of a control plane. Conversely, OAM functions **SHOULD** be configurable as part of connectivity (LSP or PW) management. Note that means for configuring OAM functions and for connectivity management are outside the scope of this document.

The service emulated by a single segment or a multi-segment pseudowire may span multiple domains. A LSP may also span multiple domains. It **MUST** be possible to perform OAM functions on a per domain

basis and across multiple domains. More generally it MUST be possible to perform OAM functions between any two switching elements of a PW or of a LSP. This is referred to as segment (or tandem connection) monitoring (see [7]). Furthermore, in case of a fault or defect on the service, means MUST be available for the service provider to be informed of the fault even if the fault is located outside of his domain.

OAM functions operate in the data plane. OAM packets MUST run in-band. That is, OAM packets for a specific Maintenance Entity MUST follow the exact same data path as user traffic of that Maintenance Entity. This is known as fate sharing.

It MUST be possible to discriminate data traffic from OAM packets. This includes a means to differentiate OAM packets from user traffic as well as the capability to apply specific treatment, to OAM packets, at the MIPs or MEPs targeted by these OAM packets.

As part of the design of OAM mechanisms for MPLS-TP, a mechanism that enables the realization of a channel for general purpose signalling, e.g. for control, management and OAM information, associated with the data plane paths, MUST be provided. Such mechanism SHOULD support the operation of existing IP/MPLS OAM.

OAM functions MUST be able to be used for PWs, LSPs and Sections. Furthermore, since LSPs MAY be stacked, OAM functions MUST be able to run on each LSP, regardless of the label stack depth.

2.2. Functional Requirements

Hereafter are listed the required functions composing the MPLS-TP OAM tool-set. The list may not be exhaustive and as such the OAM mechanisms developed in support of the identified requirements SHALL be extensible and thus SHALL NOT preclude the definition of additional OAM functions in the future. Furthermore, the design of OAM mechanisms for MPLS-TP MUST allow the ability to support vendor specific and experimental OAM functions. Vendor specific and experimental OAM functions MUST be disabled by default and explicitly enabled by a service provider or network operator, between nodes that support them.

Moreover, the use of OAM functions SHOULD be optional for the service provider or network operator. A network operator or service provider SHOULD be able to choose which OAM functions to use and which Maintenance Entities to apply them to.

Note that the functions listed below can serve the purpose of fault and/or performance management. For example, connectivity verification can be used for fault management application by detecting failure conditions, but may also be used for performance management application through its contribution to the evaluation of performance metrics (e.g. unavailability time). Nevertheless, it is outside the scope of this document to specify which function should be used for which application.

2.2.1. General requirements

If a defect or fault occurs, mechanisms **MUST** be provided to detect it, diagnose it, localize it, and notify the appropriate entities. Corrective actions **SHOULD** be taken according to the type of defect or fault.

In the case of the PW Maintenance Entity, OAM mechanisms **SHOULD** be provided to ensure that customers do not have to detect faults. The OAM functions **SHOULD** allow the service provider to automatically detect and notify the faults associated with a PW Maintenance Entity.

2.2.2. Connectivity and Continuity Verification

The MPLS-TP OAM tool-set **MUST** provide a function to enable service providers to detect loss of continuity but also mis-connectivity between two points of a Maintenance Entity.

2.2.3. Client Failure Indication

The MPLS-TP OAM tool-set **MUST** provide a function to enable a MEP to propagate a client failure indication to its peer MEP when alarm suppression in the client layer is not supported.

In cases where the OAM of the native service of an AC or a PW type does not provide mechanisms to propagate failure condition information, while a downstream indication of such state is needed, MPLS-TP OAM **SHOULD** provide mechanisms for propagating AC failures and their clearance across a MPLS-TP domain.

2.2.4. Remote Defect Indication

The MPLS-TP OAM tool-set **MUST** provide a function to enable a MEP to notify its peer MEP of the detection of a defect on a bi-directional connection between them.

2.2.5. Alarm Suppression

The MPLS-TP OAM tool-set MUST provide a function to enable a server layer MEP to notify a failure condition or an administrative locking to its client layer MEP(s) in order to suppress alarms that may be generated by maintenance domains of the client layer as a result of the failure condition or of the administrative locking in the server layer.

The MPLS-TP OAM tool-set MUST allow the client layer to differentiate between a defect condition and an administrative locking action at the server layer ME.

The server layer MEP and the client layer MEPs MAY reside on the same node or on different nodes. A mechanism MUST be provided for both cases.

An alarm suppression and summarization mechanism MUST be provided. For example, a fault detected at the LSP level MUST NOT trigger various alarms at the PW level.

2.2.6. Packet Loss

The MPLS-TP OAM tool-set MUST provide a function to enable service providers to measure packet loss ratio between a pair of MEPs. Packet loss ratio is the ratio of the user-plane packets not delivered to the total number of user-plane packets transmitted during a defined time interval. The number of user-plane packets not delivered is the difference between the number of user-plane packets transmitted by the source node and the number of user-plane packets received at the destination node.

2.2.7. Delay Measurement

The MPLS-TP OAM tool-set MUST provide a function to enable service providers to measure the one-way or two-way delay of a packet transmission between a pair of MEPs. Where,

- o One-way packet delay is the time elapsed from the start of transmission of the first bit of the packet by a source node until the reception of the last bit of that packet by the destination node.

- o Two-way packet delay is the time elapsed from the start of transmission of the first bit of the packet by a source node until the reception of the last bit of the loop-backed packet by the same source node, when the loopback is performed at the packet's destination node.

2.2.8. Route Determination

The MPLS-TP OAM tool-set MUST provide a function to enable service providers to determine the route of a connection across the MPLS transport network.

2.2.9. Diagnostic

The MPLS-TP OAM tool-set MUST provide a function to enable service providers to verify bandwidth throughput (and other diagnostic tests) between a pair of MEPs.

2.3. Operational Requirements

OAM functions such as connectivity and continuity verification MUST NOT rely on user traffic. Dedicated OAM flows SHOULD be used to detect connectivity and continuity defects. See also ITU-T G.806 . [3].

This document does not mandate the use of a particular OAM function, however, it is RECOMMENDED that connectivity and continuity verification is performed on every Maintenance Entity in order to reliably detect connectivity defects.

OAM functions MUST be applicable to bidirectional point-to-point connections, and a subset of these OAM functions MUST be applicable to unidirectional point-to-point and point-to-multipoint connections. This subset is based on the nature of both the OAM functions and the connections to which they can apply.

The following table describes how, on which Maintenance Entity and between which points of the Maintenance Entity SHOULD the required OAM functions be applied. In these tables, MEP stands for monitoring from MEP to MEP, MIP stands for monitoring from MEP to MIP, U stands for unidirectional, B stands for bidirectional. Crosses (x) indicate the way the considered function should be applied, numbers indicate the way the considered function should be applied while pointing to a footnote providing additional details.

	on-demand								proactive							
	MEP				MIP				MEP				MIP			
	P2P	P2MP	P2P	P2MP	P2P	P2MP	P2P	P2MP	P2P	P2MP	P2P	P2MP	P2P	P2MP	P2P	P2MP
	U	B	U	U	B	U	U	B	U	U	B	U	U	B	U	U
cc verification		x			x		x	x	x							
client fail. indic.								x								
remote defect indic.								x								
alarm suppression							x	x	x							
packet loss measure		1					x	2	x							
delay measurement	x	3	x													
route determination		x			x											
diagnostic	x	x	x													

1: single-ended packet loss measurements

2: in both directions of the bi-directional connection

3: one-way and two-way packet delay measurements

Table 1 : OAM functions and their applicability scope

2.4. Performance Requirements

OAM functions SHOULD continue to meet their objectives regardless of congestion conditions. See also ITU-T Y.1541 [4].

Additional requirements will be incorporated in a future revision of this document.

3. Security Considerations

Mechanisms SHOULD be provided to ensure that unauthorized access is prevented from triggering any OAM function.

OAM messages MAY be authenticated.

An OAM packet for a Maintenance Entity MUST NOT leak out of the ME, i.e. go beyond the terminating MEP.

4. Congestion Considerations

A mechanism (e.g. rate limiting) MUST be provided to prevent OAM messages from causing congestion in the PSN.

5. IANA Considerations

There are no IANA actions required by this draft.

6. Acknowledgments

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

7. References

7.1. Normative References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997
- [2] ITU-T Recommendation M.3400 (2000), TMN management functions
- [3] ITU-T Recommendation G.806 (2006), Characteristics of transport equipment - Description methodology and generic functionality
- [4] ITU-T Recommendation Y.1541 (2006), Network performance objectives for IP-based services
- [5] ITU-T Supplement Y.Sup4 (2008), Transport Requirements for T-MPLS OAM and considerations for the application of IETF MPLS Technology

7.2. Informative References

- [6] Nadeau, T., et al., "Operations and Management (OAM) Requirements for Multi-Protocol Label Switched (MPLS) Networks", [RFC 4377](#), February 2006
- [7] Busi, I., Niven-Jenkins, B., "MPLS-TP OAM Framework and Overview", [draft-busi-mpls-tp-oam-framework](#), October 2008
- [8] Niven-Jenkins, B., Brungard, D., Betts, M., "MPLS-TP Requirements", [draft-jenkins-mpls-mpls-tp-requirements](#), October 2008

Authors' Addresses

Martin Vigoureux
Alcatel-Lucent

Email: martin.vigoureux@alcatel-lucent.com

David Ward
Cisco Systems, Inc.

Email: dward@cisco.com

Malcolm Betts
Nortel Networks

Email: betts01@nortel.com

Contributing Authors' Addresses

Matthew Bocci
Alcatel-Lucent

Email: matthew.bocci@alcatel-lucent.com

Italo Busi
Alcatel-Lucent

Email: italo.busi@alcatel-lucent.it

Huib van Helvoort
Huawei Technologies Co.Ltd.

Email: hhelvoort@huawei.com

Marc Lasserre
Alcatel-Lucent

Email: mlasserre@alcatel-lucent.com

Lieven Levrau
Alcatel-Lucent

Email: llevrau@alcatel-lucent.com

Han Li
China Mobile Communications Corporation (CMCC)
Email: lihan@chinamobile.com

Julien Meuric
Orange

Email: julien.meuric@orange-ftgroup.com

Philippe Niger
Orange

Email: philippe.niger@orange-ftgroup.com

Benjamin Niven-Jenkins
BT

Email: benjamin.niven-jenkins@bt.com

Jing Ruiquan
China Telecom
Email: jingrq@ctbri.com.cn

Nurit Sprecher
Nokia-Siemens Networks

Email: nurit.sprecher@nsn.com

Yuji Tochio
Fujitsu

Email: tochio@jp.fujitsu.com

Yaacov Weingarten
Nokia-Siemens Networks

Email: yaacov.weingarten@nsn.com

Intellectual Property Statement

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights

might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Disclaimer of Validity

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Copyright Statement

Copyright (C) The IETF Trust (2008).

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.

